CONGRUENCE PROPERTIES OF $\sigma_a(N)$

BY K. G. RAMANATHAN*

(Annamalainagar)

Received August 31, 1946
(Communicated by Prof. B. S. Madhava Rao, D.Sc., F.A.S.

§ 1. INTRODUCTION

The object of this paper is to investigate completely the congruence properties of $\sigma_a(N)$, the sum of the $a$'th powers of the divisors of the positive integer $N$. The two fundamental theorems of this theory were announced by me, recently in the 'Mathematics Student'. They are

**THEOREM A.**—If $k > 2$, $(k, l) = 1$ then a necessary condition that

$$\sigma_a(km + l) \equiv 0 \pmod{k}$$

for every $m > 0$ is

$$l^a \equiv -1 \pmod{k} \quad (1)$$

**THEOREM B.**—If $k > 2$, $(k, l) = 1$ and $l^a \equiv -1 \pmod{k}$ then a necessary and sufficient condition that $\sigma_a(km + l) \equiv 0 \pmod{k}$ for every $m > 0$ is

$$x^{aa} \equiv 1 \pmod{k} \quad (2)$$

for every $x$ prime to $k$.

Thus the problem of congruence properties of $\sigma_a(N)$ is solved if we are able to solve the two binomial congruences

$$l^a \equiv -1 \pmod{k}$$

$$x^{aa} \equiv 1 \pmod{k}$$

for every $x$ prime to $k$.

These congruences of $\sigma_a(N)$ have not, as far as I know, been noticed before in mathematical literature. Mr. Hansraj Gupta, to whom these results were communicated, has published proofs of these. Here I show that these results are natural consequences of Dirichlet's theorem on the infinitude of primes in an arithmetical progression.

---

* The Contents of this paper formed part of a M.Sc. thesis of the Madras University (1946).

1 The arguments of the paper hold good even if $N$ is negative provided we define $\sigma_a(N)$ as

$$\frac{1}{\phi(N)} \sum_{\phi(N)} x^a \equiv (\frac{N}{x})^a$$

'a' may be also negative and then $\sigma_a(N) = N^{-a} \sigma_{-a}(N)$.


3 Mathematics Student, 1945

314
It is shown in the sequel that the moduli \( k \) for which congruences of \( \sigma_n(N) \) exist belong to a set of numbers called by me, sigma numbers. Also if \( k \) is a sigma number it is shown that \( \alpha \) has a least value \( \frac{1}{2} \lambda \) all the other values of \( \alpha \) being got by multiplying this least value by an odd number. The converse problem of determining the value of \( k \) when \( \alpha \) is given is difficult. I give in this paper only some empirical solutions of this problem reserving detailed discussions for a future occasion.

I wish to express my thanks to Dr. Vaidyanathaswamy, Reader in Mathematics, Madras University, for his help in the preparation of this paper.

§2. On the Group \( R(k) \)

We shall begin by deriving some simple results in the theory of the group \( R(k) \) of prime residue classes mod \( k \).

With Hecke\(^4\) we shall call this group \( R(k) \). It is well known that if \( p \) is an odd prime and \( \alpha \) is any integer greater than zero then \( R(p^\alpha) \) is cyclic; \( R(2^\alpha) \) is cyclic if \( \alpha = 1 \) or 2 but if \( \alpha \geq 3 \) then it is a direct product of two cyclic groups of orders 2 and \( 2^{\alpha-2} \) represented respectively by \((1, -1) \pmod{2^\alpha}) \) and \((1, 5, 5^2, \ldots) \pmod{2^\alpha}) \). If \( k = 2^\alpha p_1^{\alpha_1} \cdots p_r^{\alpha_r} \) then \( R(k) \) itself is the direct product of \( R(2^\alpha), R(p_1^{\alpha_1}), \ldots, R(p_r^{\alpha_r}) \). The exponent\(^6\) of \( R(k) \) is the least common multiple (l.c.m.) of the orders of all elements of \( R(k) \) and it is equal to \( \lambda = \lambda(k) \) where

\[
\lambda(k) = \text{l.c.m.} [2, 2^{\alpha-2}, \phi(p_1^{\alpha_1}), \ldots, \phi(p_r^{\alpha_r})] \quad \text{if } \alpha \geq 3
\]

\[
= \text{l.c.m.} [\phi(p_1^{\alpha_1}), \ldots, \phi(p_r^{\alpha_r})] \quad \text{if } \alpha \leq 2 \quad (3)
\]

where \( \phi(n) \) is Euler's totient function.

From the definition of exponent it is evident that \( \lambda \) is the least value of \( \gamma \) such that

\[
x^\gamma \equiv 1 \pmod{k}
\]

for every \( x \) in \( R(k) \) i.e., every \( x \) prime to \( k \).

Consider now the congruence

\[
x^\lambda \equiv -1 \pmod{k} \quad (4)
\]

This implies the congruences

\[
x^2 \equiv -1 \pmod{2^\alpha} \quad (5)
\]

\[
\alpha \equiv -1 \pmod{p_t^{\alpha_t}} \quad (t = 1, \ldots, r) \quad (6)
\]

---


\(^6\) A. A. Albert, \textit{Modern Higher Algebra}, p. 130
The congruences (6) can be satisfied if and only if \( \frac{\lambda}{2} \) is an odd multiple of \( \phi(p_1^{a_1}), \phi(p_2^{a_2}), \ldots \) which means that \( p_1 - 1, p_2 - 1, \ldots \) must all contain the same even elementary block factor.\(^6\) We shall call such primes \( p \) similar primes. Taking (5) we see that \( \frac{\lambda}{2} \) must be odd and \( x = -1 \text{ (mod 2)} \). Further since \( \frac{\lambda}{2} \) involves \( \phi(p_1^{a_1}) \), \ldots, we see that if \( a \geq 2 \) then \( a \leq 3 \) and all the odd prime factors of \( k \) must be of the form \( 4n - 1 \). Hence the important

**Theorem 1.**—The necessary and sufficient condition that the congruence

\[ x^k = -1 \text{ (mod k)} \]

is solvable is

(i) If \( k \) is odd or twice an odd number then all the odd prime factors of \( k \) are similar.

(ii) If \( k \) is divisible by 4 then it should not be divisible by 16 and all the odd prime factors of \( k \) must be of the form \( 4n - 1 \).

We shall call these numbers, the 'sigma numbers'. It is seen that any solution of the congruence when it exists is of the form

\[ x = t_r (\text{mod } p_r^{\alpha_r}) \quad (s = 1, \ldots, r) \]

\[ \equiv -1 \text{ (mod } 2^a) \]

where \( t_r \) is any quadric non-residue (mod \( p_r^{\alpha_r} \)). The number of solution is thus \( \frac{\phi(k)}{2^a} \) where\(^7\)

\[ t = r \text{ if } a = 0 \text{ or } 1 \]

\[ = r + 1 \text{ if } a = 2 \]

\[ = r + 2 \text{ if } a \geq 3, \]

\( k \) being equal to \( 2^a p_1^{\alpha_1} \ldots p_r^{\alpha_r} \).

\section*{3. Parity of \( \sigma_a(N) \)}

Before proving the fundamental theorems A and B we shall consider the parity of \( \sigma_a(N) \) i.e., the oddness or evenness of \( \sigma_a(N) \). We shall also prove some simple elementary congruences of \( \sigma_a(N) \).

**Theorem 2.**—\( \sigma_a(N) \equiv 1 \text{ (mod 2)} \) \( \text{(7)} \)

if and only if the complete odd block factor of \( N \) is a perfect square.

\(^6\) \( b \) is a block factor of \( N \) if \( \left( \frac{b}{N} \right) = 1 \). It is an elementary block factor if it is a prime power.

Proof.---

\[ \sigma_a(N) = \sum_{\delta | N} \delta^a = \sum_{\delta \text{ odd}} \frac{1}{\delta} \pmod{2} \]

Thus \(\sigma_a(N)\) has the same parity as the number of odd divisors of \(N\). But if \(N = 2^a p_1^{s_1} \ldots p_r^{s_r}\) then the number of odd divisors of \(N\) is \((1 + \alpha_1) \ldots (1 + \alpha_r)\). This is odd if and only if \(\frac{N}{2^a}\) is a perfect square.

Since \(x^\lambda \equiv 1 \pmod{k}\) for every \(x\) prime to \(k\) we easily deduce that

\[ \sigma_a(N) \equiv \sigma_a(N) \pmod{k} \quad (k, N) = 1 \quad (8) \]

if \(a \equiv b \pmod{\lambda}\).

In particular if \(b = 0\) then

\[ \sigma_b(N) \equiv d(N) \pmod{k} \quad (N, k) = 1 \quad (9) \]

\(d(N)\) being the number of divisors of \(N\).

§ 4. PROOF OF THEOREMS A AND B

We shall make use of the following theorem of Dirichlet in proving our theorems.

**Dirichlet's theorem.**—If \(l < k\) and \((k, l) = 1\) then there are an infinity of values of \(m\) for which \(km + l\) is a prime number.

**Proof of theorem A.**—Consider the series of numbers \(l, k + l, 2k + l, \ldots\), and the corresponding series of numbers \(\sigma_a(l), \sigma_a(k + l), \ldots\) If all the numbers of the second series are divisible by \(k\) then whenever \(km + l\) is a prime, \(\sigma_a(km + l)\) is also divisible by \(k\). For then

\[ \sigma_a(km + l) = 1 + (km + l)^a = 1 + l^a \equiv 0 \pmod{k} \]

**Proof of theorem B.**—To prove this we require the following:

**Lemma.**—If \(k > 2\) \((k, l) = 1\), \(l^a \equiv -1 \pmod{k}\) and \(x^{2a} \equiv (1 \pmod{k})\) for every \(x\) prime to \(k\) then \(km + l\) is not a perfect square for any value of \(m > 0\).

For if \(\delta\) and \(\delta^l\) be two conjugate divisors of \(km + l\) then \(\delta \delta^l \equiv l \pmod{k}\) and

\[ (\delta \delta^l)^a = l^a \equiv -1 \pmod{k} \]

But if \(\delta = \delta^l\) then \(l \equiv \delta^{2a} = (\delta l^a)^a = l^a \equiv -1 \pmod{k}\) which is absurd since \(k > 2\).

We shall now prove theorem B.

---

*This Condition though necessary is not sufficient. For if \(k = 35\) and \(a = 3\) then \(l^a = -1 \pmod{35}\) has solutions 19, 24, 34. \(\sigma_3\left(3 \cdot 35 + 19\right), \sigma_3\left(2 \cdot 35 + 24\right), \sigma_3\left(35 + 34\right) \neq 0 \pmod{35}.*
The condition is sufficient. For if $\delta$ and $\delta^1$ be any two conjugate divisors of $km+1$ then

$$3\delta (\delta + \delta^1) = 3\delta^2 + (\delta^1)^2 = 0 \pmod{k}$$

Thus $\delta^2 + \delta^1 = 0 \pmod{k}$ for every two conjugate divisors of $km+1$ and $km+1$ has an even number of divisors.

The condition is necessary.

Let us choose a prime $p$ not dividing $k$. Then there is a prime $q$ (in fact an infinity of them) such that

$$pq = 1 \pmod{k}.$$  

Now let $\sigma_a (pq) \equiv 0 \pmod{k}$. Then

$$\sigma_a (pq) = (1 + p^a)(1 + q^a) = 1 + p^a + q^a + (pq)^a$$

$$= p^a + q^a \pmod{k}.$$  

Multiplying by $p^\alpha$ which does not divide $k$, we get

$$p^{2\alpha} = 1 \pmod{k}.$$  

But $p$ is any prime not dividing $k$ and in every prime residue class there are an infinity of such primes. Thus the necessity of the condition.

Thus the theory of congruences of $\sigma_a (N)$ is reduced to a study of the binomial congruences

$$l^a \equiv -1 \pmod{k} \quad (10)$$

$$x^{2\alpha} \equiv 1 \pmod{k} \quad (11)$$

for every $x$ prime to $k$.

§ 5. SOLUTION OF THE CONGRUENCES

From (11) it is evident that $2a$ must be a multiple of $\lambda = \lambda (k)$, the exponent of the group of prime residue classes mod $k$. Let $2a = s \cdot \lambda$ where $s$ is an integer. Now $k > 2$ and hence $s$ is even and greater than 1. Let $s = 2b + 1$. Then

$$l^{(2b+1)\lambda} \equiv l \frac{\lambda}{2} \cdot l^\frac{\lambda}{2} = l^\frac{\lambda}{2} \pmod{k}.$$  

so that (10) implies the congruence $l^2 = -1 \pmod{k}$.

The least value of $a$ is thus $\lambda 2$ and $k$ is a sigma number. Thus

THEOREM 3.—If $\sigma_a (km+1) \equiv 0 \pmod{k}$ for $(k, l) = 1$ then

(i) $k$ is a sigma number

(ii) $a'$ is an odd multiple of $\frac{\lambda}{2}$.  

It may be remarked that Mr. Hansraj Gupta in his paper does not get all the values of \( k \) and arrives at the wrong conclusion that \( k \) cannot contain odd prime factors of the form \( 4n+1 \). We shall give some examples illustrating the above theory.

(i) \( k = 3 \cdot 7 = 21 \). \( \lambda (21) = 6 \). Solutions of \( P^3 = -1 \pmod{21} \) are 5, 17, 20. Thus \( m \geq 0 \).

\[ \sigma_3(21m + 5), \sigma_3(21m + 17), \sigma_3(21m + 20) = 0 \pmod{21} \]

(ii) \( k = 2^3 \cdot 7 = 56 \). \( \lambda (56) = 6 \). Solutions of \( P^3 = -1 \pmod{56} \) are 31, 47, 55.

\[ \sigma_3(56m + 31), \sigma_3(56m + 47), \sigma_3(56m + 55) = 0 \pmod{56} \]

§ 6. Determination of \( k \) when ' \( a \)' is given

We have so far been concerned with the determination of ' \( a \)' and ' \( l \)' when \( k \) is given. We shall now take the converse problem. Given ' \( a \)' what are the congruences or what are the possible values of \( k \). It was observed that \( k \) is a sigma number; also ' \( a \)' is an odd multiple of \( \frac{\lambda}{2} \) so that \( 2a \) is an odd multiple of \( \lambda \). Let us denote by \( N(t) \) the number of solutions in sigma numbers of

\[ t = \lambda (x) \]

then it is easily seen that the number of \( k \)'s for a given ' \( a \)' is given by

\[ \Sigma N \left( \frac{2a}{\delta} \right) \]

where \( \delta \) runs through all odd divisors of \( 2a \). The solution of this problem is very difficult. But if \( 2^a \) is the even elementary block factor of \( 2a \) then each one of the prime factors of \( k \) must be such that \( p - 1 \) contains \( 2^a \) as the even elementary block factor. Let us take some important examples.

(i) Let \( a \) be an odd number. Then the number of values of \( k \) is

\[ \Sigma_{2a} N \left( \frac{2a}{\delta} \right) \]

If \( a = 15 \) then solutions in sigma numbers should be found of

\[ 2 = \lambda (x), \ 6 = \lambda (x), \ 10 = \lambda (x), \ 30 = \lambda (x). \]

The solutions are

\[
\begin{array}{ccc}
3 & 7 \cdot 11 & 3 \cdot 7 \cdot 31 \\
7 & 7 \cdot 31 & 7 \cdot 11 \cdot 31 \\
11 & 11 \cdot 31 & 3^2 \cdot 7 \cdot 11 \\
\end{array}
\]

* For solution of similar Problems see another paper by the author.
together with these multiplied by 2, 4 and 8. Also 4 and 8 are solutions so that there are 94 solutions.

(ii) Let \( a = 2^x \); since this cannot be an odd multiple of any number we must find a sigma number \( k \) such that \( \lambda(k) = 2^{x+1} \). This means that \( 2^{x+1} + 1 \) is a prime number. Obviously this must be a Fermat prime.

(iii) Let \( S(a) \) denote the set of numbers \( k \) for which congruence properties of \( \sigma_a(N) \) with \( k \) as modulus exist. If \( a \) is odd and \( b \) any divisor of \( a \) then

\[ S(b) \subset S(a) \]

Since unity divides every odd number

\( S(1) \subset S(a) \).

Thus the set \( S(1) \) consists of sigma numbers \( k \) for which congruence properties of \( \sigma_a(N) \) exist whatever odd number \( k \) is. We now prove the

**Theorem 4.** The set \( S(1) \) consists of the numbers 3, 4, 6, 8, 12 and 24 only.

**Proof.** The only solutions of \( \lambda(x) = 2 \) are \( x = 3, 4, 6, 8, 12, \) and 24. In this case there is only one value of \( l \) namely \( -1 \mod k \) so that we have the

**Theorem 5.** If \( k = 3, 4, 6, 8, 12, \) or 24 then

\[ \sigma_a(km - 1) = 0 \mod k, \quad m > 70 \tag{13} \]

whatever odd number \( k \) is.

A companion to this theorem would be.

**Theorem 6.** If \( (n, k) = 1 \) and \( k = 3, 4, 6, 8, 12, \) or 24 then

\[ \sigma_a(n) = d(n) \mod k \tag{14} \]

\( d(n) \) being the number of divisors of \( n \) and \( a \) any even number.

§7. We have so far been concerned with congruences of the type

\[ \sigma_a(km + l) = 0 \mod k, \quad (k, l) > 1 \]

We shall now prove the

**Theorem.** If \( (k, l) = 1 \) and \( g > 0 \) there are no values of \( k \) for which

\[ \sigma_a(km + l) = g \mod k \tag{15} \]

for every \( m > 0. \)

---

Proof.---It is evident from the proof of theorem A that
\( l^n = g - 1 \pmod{k} \).

Let us choose two primes \( p \) and \( q \) not dividing \( g \) such that
\( pq = l \pmod{k} \).

Then \( \sigma_n(pq) = g \pmod{k} \) implies
\( g = 1 + p^q + q^p + (pq)^{\varphi} \pmod{k} \),
showing that \( p^q + q^p = 0 \pmod{k} \).

Multiplying by \( p^\varphi \) which does not divide \( k \) we get
\( p^{\varphi} = 1 - g \pmod{k} \). (16)

It is easily seen from the group property of the residue classes as well as Dirichlet's theorem that this congruence cannot hold good unless \( g = 0 \).

§. In this last article I shall state a congruence property of Ramanujan's function \( \tau(n) \).11 Proof is published elsewhere.12

Ramanujan's function \( \tau(n) \) is defined by
\[
\sum_{x=1}^{\infty} \tau(n) x^n = n \sum_{n=1}^{\infty} (1 - x^2) \ldots \] (17)

**THEOREM 8**: \( \tau(n) = n \varphi (n) \pmod{7} \). (18)

This implies Ramanujan's congruence that
\( \tau(n) = 0 \pmod{7} \)

if \( n \equiv 6, 3, 5, 6 \pmod{7} \). For \( \sigma_3(n) = 0 \pmod{7} \) if \( n \) is a quadratic non-residue of 7. More generally

**THEOREM 9**.---\( \sigma_{p-1}(n) = 0 \pmod{p} \) (19)

if \( n \) is a quadratic non-residue of the odd prime \( p \). This is a particular case of

**THEOREM 10**.---If \( p \mid n \) then \( \sigma_{p-1}(n) = \sum_{d=1}^{p-1} \left( \frac{d}{p} \right) \pmod{p} \sum_{p \in P \atop p \mid n} \) (20)

\( \left( \frac{d}{p} \right) \) being the Legendres-quadratic residue symbol.

---

11 See G. H. Hardy, 'Ramanujan,' Cambridge, 1940, p. 169. Ramanujan has stated such congruences only for the moduli 5 and 691, viz.,
\[
\tau(n) = n \varphi(n) \pmod{5} \quad \tau(n) = n \sigma(n) \pmod{691}.
\]

12 Proofs of theorems 8, 9 and 10 can be found in my Paper to be published in the *Journal of the Indian Mathematical Society*, 1945.