CONGRUENCE PROPERTIES OF σ_a (N)

By K. G. Ramanathan*

(*Annamalainagar*)

Received August 31, 1946

(Communicated by Prof. B. S. Madhava Rao, D.Sc., F.A.Sc.)

§ 1. Introduction

The object of this paper is to investigate completely the congruence properties of $\sigma_a(N)$,[1] the sum of the 'a'th powers of the divisors of the positive integer N. The two fundamentals theorems of this theory were announced by me,[2] 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

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

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

$$x^{2a} \equiv 1 \pmod k \tag{2}$$

for every x prime to k.

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

$$l^a \equiv -1 \pmod k$$
$$x^{2a} \equiv 1 \pmod k$$

for every x prime to k.

These congruences of σ_a (N) have not, as far as I know, been noticed before in mathematical literature. Mr. Hansraj Gupta,[3] 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 $\frac{1}{2} \sum_{\delta \cdot N} \left| \delta^a - \left(\frac{N}{\delta}\right)^a \right|$; '$a$' may be also negative and then $\sigma_a(N) = N^{-a} \sigma_{-a}(N)$.

[2] *Mathematics Student*, 1945.

[3] *Mathematics Student*, 1945.

It is shown in the sequel that the moduli k for which congruences of σ_a(N) exist belong to a set of numbers called by me, sigma numbers. Also if k is a sigma number it is shown that 'a' has a least value $\frac{1}{2}\lambda$ all the other values of 'a' being got by multiplying this least value by an odd number. The converse problem of determining the value of k when 'a' 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 α is any integer greater than zero then R (p^α) is cyclic; R (2^α) is cyclic if $\alpha = 1$ or 2 but if $\alpha \geqslant 3$ then it is a direct product of two cyclic groups of orders 2 and $2^{\alpha-2}$ represented respectively by (1, – 1) (mod 2^α) and (1, 5, 5^2,....) (mod 2^α). If $k = 2^\alpha p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ then R (k) itself is the direct product of R (2^α), R ($p_1^{\alpha_1}$).... R ($p_r^{\alpha_r}$). The exponent[5] 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

$$\begin{aligned}\lambda(k) &= \text{l.c.m.}\,[2, 2^{\alpha-2}, \phi(p_1^{\alpha_1}), \ldots \phi(p_r^{\alpha_r})] && \text{if } \alpha \geqslant 3 \\ &= \text{l.c.m.}\,[\phi(p_1^{\alpha_1}), \ldots \phi(p_r^{\alpha_r})] && \text{if } \alpha \leqslant 2 \qquad (3)\end{aligned}$$

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

From the definition of exponent it is evident that λ is the least value of y such that

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

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

Consider now the congruence

$$x^{\frac{\lambda}{2}} \equiv -1 \pmod{k}. \qquad (4)$$

This implies the congruences

$$x^{\frac{\lambda}{2}} \equiv -1 \pmod{2^\alpha} \qquad (5)$$

$$\equiv -1 \pmod{p_t^{\alpha_t}} \; (t = 1, \ldots r) \qquad (6)$$

---

[4] E. Hecke, *Theorie der Algebraischen Zahlen*, Leipzig, p. 51 *et seq.*

[5] A. A. Albert. *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 $x \equiv -1 \pmod 2$. Further since $\frac{\lambda}{2}$ involves $\phi(p_1^{a_1})\ldots$etc., we see that if $a \geqslant 2$ then $a \leqslant 3$ 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

$$x^{\frac{\lambda}{2}} \equiv -1 \pmod k$$

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

$$\begin{aligned} x &\equiv t_s \pmod{p_s^{a_s}} \quad (s = 1, \ldots r) \\ &\equiv -1 \pmod{2^a} \end{aligned}$$

where t_s is any quadric non-residue (mod $p_s^{a_s}$). The number of solution is thus $\frac{\phi(k)}{2^t}$ where[7]

$$\begin{aligned} t &= r \text{ if } a = 0 \text{ or } 1 \\ &= r + 1 \text{ if } a = 2 \\ &= r + 2 \text{ if } a \geqslant 3. \end{aligned}$$

k being equal to $2^a p_1^{a_1} \ldots p_r^{a_r}$.

§ 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.—$\sigma_a(N) \equiv 1 \pmod 2$ (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 $\left(b, \frac{N}{b}\right) = 1$. It is an elementary block factor if it is a prime power.

[7] H. Weber, *Lehrbuch der Algebra*, Bd. 2, I Chapter.

Proof.—

$$\sigma_a(\mathrm{N}) = \sum_{\delta/\mathrm{N}} \delta^a \equiv \sum_{\substack{\delta/\mathrm{N} \\ \delta \text{ odd}}} 1 \pmod 2$$

Thus $\sigma_a(\mathrm{N})$ has the same parity as the number of odd divisors of N. But if $\mathrm{N} = 2^a p_1^{a_1} \ldots . p_r^{a_r}$ then the number of odd divisors of N is $(1+a_1)(1+a_2) \ldots . (1+a_r)$. This is odd if and only if $\frac{\mathrm{N}}{2^a}$ is a perfect square.

Since $x^\lambda \equiv 1 \pmod k$ for every x prime to k we easily deduce that

$$\sigma_a(\mathrm{N}) \equiv \sigma_b(\mathrm{N}) \pmod k \qquad (k, \mathrm{N}) = 1 \tag{8}$$

if $a \equiv b \pmod \lambda$.

In particular if $b = 0$ then

$$\sigma_\lambda(\mathrm{N}) \equiv d(\mathrm{N}) \pmod k. \qquad (\mathrm{N}, k) = 1 \tag{9}$$

$d(\mathrm{N})$ 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

$$\sigma_a(km + l) = 1 + (km + l)^a \equiv 1 + l^a \equiv 0 \pmod k.$$[8]

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 $x^{2a} \equiv (1 \bmod k)$ for every x prime to k then $km + l$ is not a perfect square for any value of $m > 0$.

For if δ and δ^1 be two conjugate divisors of $km + l$ then $\delta\delta^1 \equiv l \pmod k$ and

$$(\delta\delta^1)^a = l^a \equiv -1 \pmod k$$

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

We shall now prove theorem B.

---

[8] This Condition though necessary is not sufficient. For if $k = 35$ and $a = 3$ then $l^3 \equiv -1 \pmod{35}$ has solutions 19, 24, 34. $\sigma_3(3 \cdot 35 + 19)$, $\sigma_3(2 \cdot 35 + 24)$, $\sigma_3(35 + 34) \not\equiv 0 \pmod{35}$.

The condition is sufficient. For if δ and δ^1 be any two conjugate divisors of $km+l$ then

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

Thus $\delta^a+\delta^{1a} \equiv 0 \pmod{k}$ for every two conjugate divisors of $km+l$ and $km+l$ 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

$$pq \equiv l \pmod{k}.$$

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

$$\begin{aligned}\sigma_a(pq) &= (1+p^a)(1+q^a) = 1+p^a+q^a+(pq)^a\\ &\equiv p^a+q^a \pmod{k}.\end{aligned}$$

Multiplying by p^a which does not divide k, we get

$$p^{2a} \equiv 1 \pmod{k}$$

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 σ_a (N) is reduced to a study of the binomial congruences

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

$$x^{2a} \equiv 1 \pmod{k} \qquad (11)$$

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. Then (10) shows that s is an odd number. Now $k > 2$ and hence λ is even and greater than 1. Let $s = 2b+1$. Then

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

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

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

THEOREM 3.—If $\sigma_a(km+l) \equiv 0 \pmod{k}$ 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) $k=3\cdot7=21$. $\lambda(21)=6$. Solutions of $l^3\equiv-1 \pmod{21}$ are 5, 17, 20. Thus $m\geqslant 0$.

$$\sigma_3(21m+5),\ \sigma_3(21m+17),\ \sigma_3(21m+20)\equiv 0 \pmod{21}.$$

(ii) $k=2^3\cdot7=56$. $\lambda(56)=6$. Solutions of $l^3\equiv-1 \pmod{56}$ are 31,47,55.

$$\sigma_3(56m+31),\ \sigma_3(56m+47),\ \sigma_3(56m+55)\equiv 0 \pmod{56}.$$

§ 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 λ. Let us denote by $N(t)$ the number of solutions[0] 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 δ runs through all odd divisors of $2a$. The solution of this problem is very difficult. But if 2^α 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^α 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

$$\sum_{\delta/a} N\left(\frac{2a}{\delta}\right)$$

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

3	$7\cdot11$	$3\cdot7\cdot31$
7	$7\cdot31$	$7\cdot11\cdot31$
11	$11\cdot31$	$3^2\cdot7\cdot11$

[0] For solution of similar Problems see another paper by the author.

31	$3^2\cdot 31$	$3^2\cdot 11\cdot 31$
3^2	$3^2\cdot 11$	$3^2\cdot 7\cdot 31$
$3\cdot 7$	$3^2\cdot 7$	$3\cdot 7\cdot 11\cdot 31$
$3\cdot 11$	$3\cdot 7\cdot 11$	$3^2\cdot 7\cdot 11\cdot 31$
$3\cdot 31$	$3\cdot 11\cdot 31$	

together with these multiplied by 2, 4 and 8. Also 4 and 8 are solutions so that there are 94 solutions.

(ii) Let $a=2^a$; since this cannot be an odd multiple of any number we must find a sigma number k such that $\lambda(k)=2^{a+1}$. This means that $2^{a+1}+1$ 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 σ_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 σ_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 $-1 \pmod k$ so that we have the

THEOREM 5[10].—If $k=3, 4, 6, 8, 12$ or 24 then

$$\sigma_a(km-1) \equiv 0 \pmod k, \quad m \geq 0 \qquad (13)$$

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

$$\sigma_a(n) \equiv d(n) \pmod k \qquad (14)$$

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

§7. We have so far been concerned with congruences of the type $\sigma_a(km+l) \equiv 0 \pmod k$, $(k, l)>1$. We shall now prove the

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

$$\sigma_a(km+l) \equiv g \pmod k \qquad (15)$$

for every $m>0$.

---

[10] K. G. Ramanathan, *Mathematics Student*, 1943, 33–35.

Proof.—It is evident from the proof of theorem A that

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

Let us choose two primes p and q not dividing g such that

$$pq \equiv l \pmod{k}.$$

Then $\sigma_a(pq) \equiv g \pmod{k}$ implies

$$g \equiv 1 + p^a + q^a + (pq)^a \pmod{k}.$$

showing that $p^a + q^a \equiv 0 \pmod{k}$.

Multiplying by p^a which does not divide k we get

$$p^{2a} \equiv 1 - g \pmod{k}. \tag{16}$$

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

$$\sum_{n=1}^{\infty} \tau(n)\, x^n = x\,[(1-x)(1-x^2)\ldots.]^{24} \tag{17}$$

THEOREM 8[13].—$\tau(n) \equiv n\sigma_3(n) \pmod{7}$. (18)

This implies Ramanujan's congruence that

$$\tau(n) \equiv 0 \pmod{7}$$

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

THEOREM 9.—$\sigma_{\frac{p-1}{2}}(n) \equiv 0 \pmod{p}$ (19)

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

THEOREM 10.—If $p \nmid n$ then $\sigma_{\frac{p-1}{2}}(n) \equiv \sum_{\delta|n} \left(\frac{\delta}{p}\right) \pmod{p} \sum_{p \nmid \delta}$ (20)

$\left(\frac{\delta}{p}\right)$ 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.*,

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

[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.

[13] Theorem 8 is substantially equivalent to theorem 1 of J. R. Wilton, *Proc. Lond. Math. Soc.*, 1931, p. 1-11.