Pacific Journal of Mathematics

CONGRUENCE PROPERTIES OF $\sigma_r(N)$

VINCENT C. HARRIS AND M. V. SUBBA RAO

Vol. 12, No. 3 March 1962

CONGRUENCE PROPERTIES OF $\sigma_r(N)$

V. C. HARRIS AND M. V. SUBBA RAO

1. Introduction. Let $\sigma_r(N)$ denote as usual the sum of the rth powers of the divisors of N. Let d be a divisor of N with $1 \leqq d \leqq \sqrt{N}$ and d' its conjugate, so that $dd' = N$. By a component of $\sigma_r(N)$ we mean the quantity $d^r + d'^r$ or d^r according as $1 \leqq d < \sqrt{N}$ or $d = \sqrt{N}$. Components corresponding to distinct divisors $d \leqq \sqrt{N}$ are distinct and $\sigma_r(N)$ is their sum.

If every component of $\sigma_r(N)$ is congruent to the integer a, modulo K, we say that $\sigma_r(N)$ is componently congruent to a $(\bmod K)$ and indicate this by writing

$$\sigma_r(N) \underline{\equiv} a \pmod{K} .$$

This does not necessarily imply that also $\sigma_r(N) \equiv a \pmod{K}$. For example $\sigma_4(8) \underline{\equiv} 2 \pmod 3$ but $\sigma_4(8) \equiv 1 \pmod 3$. Similarly ordinary congruence does not imply component congruence, as the same example shows.

2. THEOREM 1. *If r, K, L are fixed positive integers with $K \geqq 3$ and $(L, K) = 1$, and if a is a nonnegative integer, then a necessary and sufficient condition that*

(1) $\sigma_r(nK + L) \underline{\equiv} a \pmod{K}$ *for all integral values of* $n \geqq 0$

is that

(2) *L is a quadratic nonresidue of K*

(3) $1 + L^r \equiv a \pmod{K}$

(4) $(w^r - 1)(w^r + 1 - a) \equiv 0 \pmod{K}$ *for all w such that* $(w, K) = 1$

all hold.

We first show necessity. Assume that $\sigma_r(nK + L) \underline{\equiv} a \pmod{K}$ and L is a quadratic residue of K. Then there exists q such that $q^2 \equiv L \pmod{K}$ and consequently n_1 such that $n_1K + L = q^2$. Consider q^2 and $n_2K + L = (n_1K + n_1 + L)K + L = (K + 1)q^2$, both occurring in the sequence $nK + L$. Since $\sigma_r(q^2) \underline{\equiv} a \pmod{K}$ we have with $d = q$ that $q^r \equiv a \pmod{K}$ and since $\sigma_r([K + 1]q^2) \underline{\equiv} a \pmod{K}$ we have with $d = q$ and $d' = (K + 1)q$ that $q^r + (K+1)^r q^r \equiv a \pmod{K}$. Thus $q^r + (K+1)^r q^r \equiv q^r$, or, $2 \equiv 1 \pmod{K}$. This is a contradiction and (2) is necessary. Assume next (1) holds. Then in particular for $n = 0$ we have $\sigma_r(L) \underline{\equiv} a \pmod{K}$. By condition (2) just proved $L \neq 1$ and the component with $d = 1$ and $d' = L$ gives $1 + L_r \underline{\equiv} a \pmod{K}$ which is (3).

Received May 11, 1961, and in revised form November 1, 1961.

Next to show (4). Given any w such that $(w, K) = 1$, there exists an $x \not\equiv w \pmod{K}$ such that $wx \equiv L \pmod{K}$. Let this x be denoted by w_1.

Then

$$ww_1 \equiv L \pmod{K}$$

and by our assumption $\sigma_r(nK + L) \equiv a \pmod{K}$ applied to ww_1 it follows that

$$1 + w^r w_1^r \equiv a \pmod{K}$$
$$w^r + w_1^r \equiv a \pmod{K} .$$

Eliminating w_1^r gives $1 + w^r(a - w^r) \equiv a \pmod{K}$. Rewriting this gives (4) and shows (4) is necessary.

To show sufficiency, we need to show for any divisor d of $N = nK + L$ with $1 \leqq d \leqq \sqrt{N}$ and conjugate divisor d' that $d^r + d'^r \equiv a \pmod{K}$ or $d^r \equiv a \pmod{K}$ according as $1 \leqq d < \sqrt{N}$ or $d = \sqrt{N}$ provided (2), (3) and (4) hold. But (2) insures that N cannot be a square, so the second alternative cannot occur. Now

$$\begin{aligned} d^r(d^r + d'^r) &= d^{2r} + (dd')^r \\ &\equiv (1 + ad^r - a) + L^r \end{aligned}$$

by (4) and the fact that $dd' \equiv L \pmod{K}$. Then using (3),

$$d^r(d^r + d'^r) \equiv (1 + ad^r - a) + a - 1 \equiv ad^r \pmod{K} .$$

Since $(d, K) = 1$ it follows that

$$d^r + d'^r \equiv a \pmod{K}$$

for each d as specified. But this shows (1) holds and completes the proof.

3. Examples and some special cases. It is not difficult to show that when $K = p$ is an odd prime, all component congruences are obtained with $r = (p-1)/2$ and $a = 0$ or $r = (p-1)$ and $a = 2$. Thus for example:

$$\sigma_6(13n + L) \equiv 0 \pmod{13},\ L = 2, 5, 6, 7, 8, 11$$
$$\sigma_{12}(13n + L) \equiv 2 \pmod{13},\ L = 2, 5, 6, 7, 8, 11 .$$

When K is composite we have $\sigma_{\varphi(K)}(nK + L) \equiv 2 \pmod{K}$ for any non-quadratic residue L of K.

In the special case $r = 1$ we show

THEOREM 2. *For all integral* $n \geqq 0$, $\sigma_1(nK + L) \equiv a \pmod{K}$ *holds for suitable* L *and* a *if and only if* K *is one of* 3, 4, 6, 8, 12 *and* 24.

The equation in condition (4) becomes

$$w^2 - aw + a - 1 \equiv 0 \pmod K \tag{5}$$

The congruence (5) is equivalent to

$$4x^2 - 4ax + a^2 \equiv (2x - a)^2 \equiv (a-2)^2 \pmod{4K} .$$

With $y = 2x - a$ we have

$$y^2 \equiv (a-2)^2 \pmod{4K} \tag{6}$$

subject to $y \equiv -a \pmod 2$. But this last condition is no restriction so that the number of solutions of (5) is the same as that of (6). Let $S(4K)$ be the number of solutions of (6) and let $4K = p_1^{2+e_1} p_2^{e_2} \cdots p_j^{e_j}$ where $p_1 = 2,\ p_2 = 3, \cdots$ are distinct primes. Then

$$S(4K) = S(p_1^{2+e_1}) S(p_2^{e_2}2) \cdots S(p_j^{e_j}) \text{ and } S(p_1^{2+e_1}) \leqq 2 \text{ for } e_1 = 0 ;$$

$S(p_1^{2+e_1}) \leqq 4$ for $e > 0$; $S(p_i^{e_i}) \leqq 2$ for $p_i > 2$.

Since (5) is to hold for all w such that $(w, K) = 1$, we must have $\phi(p_i^{e_i}) \leqq S(4p_i^{e_i})$ or

$$p_i^{e_i-1}(p_i - 1) = \phi(p_i^{e_i}) \leqq \begin{cases} 2 & p_i = 2,\ e_i = 0 \\ 4 & p_i = 2,\ e_i > 0 \\ 2 & p_i > 2 \end{cases} . \tag{7}$$

But the only values of $p_i^{e_i}$ satisfying these are 1, 2, 4, 8 and 1, 3. Since $K \geqq 3$ these give $K = 3, 4, 6, 8, 12, 24$. The converse can be proved by enumeration. The results are listed:

K	3	4	6	8	8	12	12	24	24
L	2	3	5	3	7	5	11	11	23
a	0	0	0	4	0	6	0	12	0

4. Relation between component congruence and congruence. We have

THEOREM 3. *If* $\sigma_r(nK + L) \mathrel{\underline{\equiv}} a \pmod K$ *for all integral* $n \geqq 0$, *then* $\sigma_r(nK + L) \equiv a \pmod K$ *for all integral* $n \geqq 0$ *if and only if* $a \equiv 0 \pmod K$.

If $a \equiv 0 \pmod K$ then each component is congruent to zero and the sum of the components—that is, $\sigma_r(nK + L)$—is congruent to zero. Conversely, if $\sigma_r(nK + L) \equiv a \pmod K$ as well as $\sigma_r(nK + L) \mathrel{\underline{\equiv}} a \pmod K$, then, $\tau(n)$ standing for the number of divisors of n, we have

$$[\tau(nK + L)/2]a \equiv a \pmod K$$

since there are $\tau(nK + L)/2$ components each congruent to $a \pmod K$. By Dirichlet's theorem, w and w_1 in the proof of Theorem 1 may be taken as primes p and p_1. Then for $nK + L = pp_1$, $\tau(nK + L) = 4$. We must have $2a \equiv a$ or $a \equiv 0 \pmod{K}$.

In the particular case $a = 0$, conditions (2), (3) and (4) reduce to conditions which Gupta [1] and Ramanathan [2] found to be necessary and sufficient in order that $\sigma_r(nK + L) \equiv 0 \pmod{K}$ for r, n, K and L as above. Thus we have the remarkable result:

THEOREM 4. *Let r, K and L be positive integers with $(K, L) = 1$ and $K \geqq 3$. Then $\sigma_r(nK + L) \equiv 0 \pmod{K}$ for all $n \geqq 0$ if and only if $\sigma_r(nK + L) \equiv 0 \pmod{K}$ for all $n \geqq 0$.*

REFERENCES

1. H. Gupta, *Congruence properties of $\sigma(n)$*, Math. Student, XIII, **1** (1945), 25–29.
2. K. G. Ramanathan, *Congruence properties of $\sigma_r(n)$*, Math. Student, XIII, **1** (1945), 30.
3. M. V. Subba Rao, *Congruence properties of $\sigma(n)$*, Math. Student (1950), 17–18.

SAN DIEGO STATE COLLEGE
SRI VENKATESWARA UNIVERSITY AND UNIVERSITY OF MISSOURI

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, L. J. Paige at the University of California, Los Angeles 24, California.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. Effective with Volume 13 the price per volume (4 numbers) is $18.00; single issues, $5.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $8.00 per volume; single issues $2.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Pacific Journal of Mathematics

Vol. 12, No. 3 March, 1962