COLLOQUIUM MATHEMATICUM

VOL. XXVII 1973 FASC. 2

ON DISTRIBUTION OF VALUES OF $\sigma(n)$ IN RESIDUE CLASSES

BY

JAN ŚLIWA (WROCŁAW)

1. Let $N \geqslant 3$ be an integer. A sequence of integers $a_1, a_2, \ldots$ is *weakly uniformly distributed* (mod N) if and only if, for every pair of integers j_1, j_2 with $(j_1, N) = (j_2, N) = 1$,

$$\lim_{x\to\infty} \frac{\sum_{\substack{a_n \equiv j_1 \pmod N \\ n<x}} 1}{\sum_{\substack{a_n \equiv j_2 \pmod N \\ n<x}} 1} = 1,$$

provided the set $\{j: (j, N) = 1\}$ is infinite. For shortness we write that such a sequence is WUD(mod N).

We use the following modification of the theorem of Narkiewicz [2]:

Let $f(n)$ be a multiplicative, integer-valued function such that, for every integer $k \geqslant 1$, there exists a polynomial $W_k(x) \in Z[x]$ and $f(p^k) = W_k(p)$ for all primes p. Let, moreover,

$$R_k(f, N) = \{r \in G(N): W_k(x) \equiv r \pmod N \text{ has a solution in } G(N)\},$$

where $G(N)$ denotes the multiplicative group of residue classes relatively prime to N, and let $A_k(f, N)$ be the subgroup of $G(N)$ generated by the set $R_k = R_k(f, N)$.

If $R_1(f, N) = \ldots = R_{m-1}(f, N) = G$ and $R_m(f, N) \neq \emptyset$ for some m, then the sequence $f(1), f(2), \ldots$ is WUD(mod N) *if and only if, for every non-principal character χ of $G(N)$ which is trivial on A_m, there exists a prime p such that*

$$1 + \sum_{j=1}^{\infty} \chi(f(p^j)) p^{-j/m} = 0.$$

In paper [2] those numbers N for which functions $d(n)$ and $\varphi(n)$ are WUD(mod N) were also found.

2. The aim of this note is to prove the following

THEOREM 1. *The sequence* $\sigma(1), \sigma(2), \ldots$ *is* WUD$(\bmod N)$ *if and only if* $6 \nmid N$.

Proof. For $f(n) = \sigma(n)$, we have $W_j(x) = 1 + x + x^2 + \ldots + x^j$.

(i) Let at first $2 \nmid N$. In this case

$$R_1 = \{n \leqslant N\colon (n, N) = (n-1, N) = 1\}$$

is non-void as $2 \in R_1$. Let $N = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ $(p_i \neq 2)$. Then

$$G(N) = G(p_1^{a_1}) \oplus G(p_2^{a_2}) \oplus \ldots \oplus G(p_k^{a_k}),$$

and so we can represent every element y of $G(N)$ in the form $(y_1, y_2, \ldots, y_k)$ with $y_i \in G(p_i^{a_i})$, $y_i \equiv y (\bmod p_i^{a_i})$.

In this notation A_1 is a subgroup of $G(N)$ generated by the set

$$\{(y_1, y_2, \ldots, y_k)\colon y_i \not\equiv 1 (\bmod p_i), y_i \in G(p_i^{a_i})\}.$$

Denote by $g_1, g_2, \ldots, g_k$ the primitive roots $\bmod p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$, respectively. Since $g_i \not\equiv 1 (\bmod p_i)$, the elements

$$(-1, \ldots, -1, g_i, -1, \ldots, -1) \quad \text{for } i = 1, 2, \ldots, k$$

belong to R_1, and so the elements

$$(1) \quad (-1, \ldots, -1, g_i^{2s+1}, -1, \ldots, -1) = (-1, \ldots, -1, g_i, -1, \ldots, -1)^{2s+1}$$

and

$$(1') \quad (1, \ldots, 1, g_i^{2s}, 1, \ldots, 1) = (-1, \ldots, -1, g_i, -1, \ldots, -1)^{2s}$$

belong to A_1.

Assume now that $p_i \neq 3$, $i = 1, 2, \ldots, k$. Then the congruence

$$(2) \quad 2w_i \equiv -1 (\bmod p_i^{a_i})$$

has a solution $w_i \in G(p_i^{a_i})$ such that $w_i \not\equiv 1 (\bmod p_i)$. Indeed, if $w_i \equiv 1 (\bmod p_i)$, then $-1 \equiv 2w_i \equiv 2 (\bmod p_i)$. But it is impossible, since $p_i \neq 3$. Further, we have

$$(-1, \ldots, -1, w_i, -1, \ldots, -1) \cdot (-1, \ldots, -1, 2, -1, \ldots, -1) \cdot (-1, \ldots, -1) = (-1, \ldots, -1, 1, -1, \ldots, -1) \in A_1 \quad \text{for } i = 1, 2, \ldots, k.$$

From (1) and (1') it follows that

$$(1, \ldots, 1, g_i^s, 1, \ldots, 1) \in A_1 \quad \text{for } i = 1, 2, \ldots, k;\ s = 1, 2, \ldots$$

Then

$$(g_1^{s_1}, g_2^{s_2}, \ldots, g_k^{s_k}) \in A_1, \quad s_i = 1, 2, \ldots;\ i = 1, 2, \ldots, k,$$

and so, in this case, $A_1 = G(N)$.

Now, let $N = 3^a \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$, $a \geqslant 1$. In the same way as above we infer that if $a_i \in G(p_i^{a_i})$, $i = 1, 2, \ldots, k$, then

$$(1, a_1, \ldots, a_k) \in A_1 \quad \text{or} \quad (-1, a_1, \ldots, a_k) \in A_1. \tag{3}$$

If $\{w_i\}_{1 \leqslant i \leqslant k}$ is a solution of (2), then $(-1, w_1, \ldots, w_k) \in A_1$ and

$$(-1, 2, \ldots, 2) \cdot (-1, w_1, \ldots, w_k) \cdot (-1, \ldots, -1) = (-1, 1, \ldots, 1) \in A_1.$$

Hence (3) implies

$$(1, g_1^{s_1}, \ldots, g_k^{s_k}) \in A_1 \quad \text{for } s_i = 1, 2, \ldots;\ i = 1, 2, \ldots, k. \tag{4}$$

Now, let g be a primitive root $\bmod 3^a$. Then

$$(g^{2s}, 1, \ldots, 1) = (g, -1, \ldots, -1)^{2s} \in A_1 \tag{5}$$

and

$$(g^{2s+1}, 1, \ldots, 1) = (-1, 2, \ldots, 2) \cdot (-1, w_1, \ldots, w_k) \cdot (g, -1, \ldots, -1)^{2s+1} \in A_1. \tag{6}$$

Comparing (4), (5) and (6), we infer that $A_1 = G(N)$. This, by Narkiewicz [2], implies that the sequence $\sigma(1), \sigma(2), \ldots$ is WUD$(\bmod N)$ for every N odd.

(ii) Now, let N be an even number, $N = 2^a \cdot p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$. We have $R_1 = \emptyset$ but $R_2 \neq \emptyset$. Indeed,

$$W_2(x) = x^2 + x + 1 \quad \text{and} \quad 1 \equiv W_2(N-1) (\bmod N),$$

so $1 \in R_2$. Now, we have

$$G(N) = G(2^a) \oplus G(p_1^{a_1}) \oplus \ldots \oplus G(p_k^{a_k}).$$

We write the elements of this group in the form

$$y = (y_0, y_1, \ldots, y_k), \quad y_s \equiv y (\bmod p_s^{a_s}),\ y_s \in G(p_s^{a_s}),\ s = 0, 1, \ldots, k$$

(here $2^a = p_0^{a_0}$).

In order to prove that $A_2 = G(N)$ it is sufficient to show that, for $i = 1, 2, \ldots, k$ and s $S_i \in \subset \{1, 2, \ldots\}$, there is $(1, 1, \ldots, 1, g_i^s, 1, \ldots, 1) \in R_2$, where $\{g_i^s\}_{s \in S_i}$ generates $G(p_i^{a_i})$, and, for $s \in S_0$, there is $(a_s, 1, \ldots, 1) \in R_2$, where $\{a_s\}_{s \in S_0}$ generates $G(2^a)$. But this holds true if, for $i = 1, 2, \ldots, k$,

the congruences

$$x^2+x+1 \equiv 1 \pmod{p_i^{a_i}}, \tag{7}$$

$$x^2+x+1 \equiv g_i^s \pmod{p_i^{a_i}} \quad \text{for } s \in S_i, \tag{8}$$

$$x^2+x+1 \equiv a_s \pmod{2^a} \quad \text{for } s \in S_0 \tag{8'}$$

have the solutions $x_i \in G(p_i^{a_i})$, $x_0 \in G(2^a)$.

Congruence (7) has such solutions: $x_i = p_i^{a_i-1}$.

Observe that $x^2+x+1 \equiv y^2+y+1 \pmod{2^a}$ implies

$$2^a \mid (x-y)\cdot(x+y+1).$$

Since the integer $x+y+1$ is odd for $x, y \in G(2^a)$, there is $x \equiv y \pmod{2^a}$. So, for $x = 1, 3, 5, \ldots, 2^a-1$, we obtain distinct $(\mathrm{mod}\, 2^a)$ values of x^2+x+1. Hence, for every $a \in G(2^a)$, there exists $x \in G(2^a)$ such that

$$x^2+x+1 \equiv a \pmod{2^a}.$$

This solves (8').

Consider the congruence

$$f_s(x) = x^2+x+1-g_j^s \equiv 0 \pmod{p^a}, \tag{9}$$

where $p \neq 2$, and g is a primitive root $\bmod p^a$.

If x_0 satisfies $f_s(x_0) \equiv 0 \pmod{p}$ and $f'(x_0) \not\equiv 0 \pmod{p}$, then the equation $f_s(x) = 0$ has a solution in p-adic integers, and so, for every integer a, congruence (9) has the solution x satisfying $x \equiv x_0 \pmod{p}$ (see [1]).

The congruence

$$f'(x) = 2x+1 \equiv 0 \pmod{p}$$

has the only solution

$$x \equiv \frac{p-1}{2} \pmod{p}.$$

If

$$g^s \not\equiv \left(\frac{p-1}{2}\right)^2 + \frac{p-1}{2} + 1 \pmod{p},$$

then, for such s, congruence (9) is equivalent to the congruence $f_s(x) \equiv 0 \pmod{p}$. If

$$x^2+x+1 \equiv y^2+y+1 \pmod{p} \quad \text{for } x \neq y,\ x,\ y \in G(p),$$

then $p \mid x+y+1$ and $y = p-x-1$. Hence, for $x \in \{1, 2, \ldots, p-1\}$, we get $(p-1)/2$ integers distinct $(\mathrm{mod}\, p)$ which are values of x^2+x+1. Among them may appear 0, so we can assume that $(p-3)/2$ of them belong to $G(p)$.

We prove the following

LEMMA. *Let p be a prime greater than 7, g — a primitive root* mod$p$, *and $A = \{g^{k_1}, g^{k_2}, \ldots, g^{k_s}\} \subset G(p)$ — a set containing at least $(p-3)/2$ distinct elements of $G(p)$ such that at least one of k_i, $i = 1, 2, \ldots, s$, is odd. Then A generates $G(p)$.*

Proof. Let $G(A)$ be a subgroup of $G(p)$ generated by A. For $p > 7$, we have $(p-3)/2 > (p-1)/3$ and $\mathrm{card}G(A) | p-1$. If $G(A) \neq G(p)$, then $\mathrm{card}G(A) = (p-1)/2$. The group $\{g^2, g^4, \ldots, g^{p-1}\}$ is the only subgroup of $G(p)$ which has $(p-1)/2$ elements, but every element of that subgroup has an even order. This gives $G(A) = G(p)$.

It follows from this lemma that integers $k_1, k_2, \ldots, k_s$ generate an additive group $C_{p-1} = \{0, 1, \ldots, p-1\}$. Hence, for some integers $b_1, b_2, \ldots, b_s \geqslant 0$, we have

$$\sum_{i=1}^{s} b_i k_i = 1 + (p-1)t.$$

Let $\{g^{k_1}, g^{k_2}, \ldots, g^{k_s}\}$ be the set of all distinct elements of $G(p)$ such that the congruence

$$x^2 + x - 1 - g^{k_i} \equiv 0 \pmod{p}$$

has a solution $x_i \in G(p) \setminus \{(p-1)/2\}$. Then the congruence

$$x^2 + x - 1 - g^{k_i} \equiv 0 \pmod{p^a}$$

has also a solution $x_i' \in G(p^a)$. If at least one of $k_1, k_2, \ldots, k_s$ is odd, then our lemma implies the existence of non-negative $b_1, b_2, \ldots, b_s$ such that

$$\prod_{i=1}^{s} (g^{k_i})^{b_i} \equiv g^{1+(p-1)t} \pmod{p^a}.$$

Observe, first, that we can assume that at least one of $k_1, k_2, \ldots, k_s$ is not divisible by p. Indeed, if the congruence

$$x^2 + x + 1 - g^{k_i} \equiv 0 \pmod{p^a}$$

has a solution in $G(p^a)$, then the congruence

$$x^2 + x + 1 - g^{k_i + p - 1} \equiv 0 \pmod{p^a}$$

also has a solution in $G(p^a)$. So, we can choose the integers $b_1, b_2, \ldots, b_s$ in a way such that p does not divide $\sum_{i=1}^{s} b_i k_i$. Then

$$\Big(\sum_{i=1}^{s} b_i k_i, \varphi(p^a) \Big) = 1,$$

and this means that $g^{b_1 k_1 + \cdots + b_s k_s}$ generates $G(p^a)$.

Now it is sufficient to prove that among the integers $k_1, k_2, \ldots, k_s$, for which the congruence

$$x^2+x+1-g^{k_i} \equiv 0 \pmod{p}$$

has a solution $x \in G(p) \setminus \{(p-1)/2\}$, at least one is odd. Suppose it is not true. First we assume that $p > 7$. If $(3/p) = -1$, then $3 \equiv g^{2s+1} \pmod{p}$ for some s, and as $1^2+1+1 \equiv 3 \pmod{p}$, so

$$x^2+x+1-g^{2s+1} \equiv 0 \pmod{p}$$

has a solution in $G(p) \setminus \{(p-1)/2\}$.

However, if $(3/p) = +1$, then

$$\left(\frac{((p-1)/2)^2+(p-1)/2+1}{p}\right) = \left(\frac{(p^2+3)/4}{p}\right) = \left(\frac{3}{p}\right) = +1,$$

and we infer that

$$\left(\frac{p-1}{2}\right)^2 + \frac{p-1}{2} + 1$$

is a quadratic rest $\bmod p$. Then the polynomial x^2+x+1 gives, for $x = 1, 2, \ldots, p-1$, quadratic rests only. It means that, for every quadratic rest r, there exists $x \in G(p)$ such that

$$x^2+x+1 \equiv r \pmod{p},$$

and, finally,

$$\left(\frac{4r-3}{p}\right) = +1,$$

since the congruence

$$x^2+x+1 \equiv r \pmod{p}$$

is equivalent to the congruence

$$(2x+1)^2 \equiv 4r-3 \pmod{p}.$$

Then also

$$\left(\frac{4r-3}{p}\right) = -1$$

for all quadratic non-rests $\bmod p$.

This implies that, for every r, $1 \leqslant r \leqslant p-1$,

$$\left(\frac{r}{p}\right) = \left(\frac{4r-3}{p}\right)$$

and the element $r(4r-3)$ is a quadratic rest (we put $(0/p) = 1$).

Now, let $rr' \equiv 1 \pmod{p}$. Then

$$4-3r' \equiv r'^2 r(4r-3) \pmod{p}$$

is also a quadratic rest. However, if $r_1 \not\equiv r_2 \pmod{p}$, then also $r_1' \not\equiv r_2' \pmod{p}$, and so, for some integer r', the element $4-3r'$ is a quadratic non-rest. A contradiction.

For $p = 5$, we will show that there exists a primitive root $g \bmod 5^a$ such that the congruence

$$x^2+x+1-g \equiv 0 \pmod{5^a}$$

has a solution $x \in G(5^a)$. Indeed, since 3 is a primitive root mod 5, there exists a primitive root $g \bmod 5^a$ such that $g \equiv 3 \pmod 5$ and that the congruence

$$x^2+x+1-g \equiv 0 \pmod{5^a}$$

is equivalent to

$$x^2+x-1-g \equiv 0 \pmod 5$$

if it has a solution $x = (5-1)/2 = 2$. But $1^2+1+1-g \equiv 0 \pmod 5$. Similarly, for $p = 7$, the primitive root mod 7 is 3, $(7-1)/2 = 3$, and $1^2+1+1-3 \equiv 0 \pmod 7$.

From all this it follows that, for N even such that $3 \nmid N$, the sequence $\sigma(1), \sigma(2), \ldots$ is WUD$(\bmod N)$.

Let now $N = 2^\alpha \cdot 3^\beta \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$, $\alpha \geqslant 1, \beta \geqslant 1$. If $6s+r \pmod N \in G(N)$, then either $r = 1$ or $r = 5$. We have

$$(6s+1)^2+(6s+1)+1 \equiv 0 \pmod 3$$

and

$$(6s+5)^2+(6s+5)+1 \equiv 1 \pmod 6.$$

Therefore, in R_2 there are only elements of the form $6l+1$. Since the product of two elements of the form $6l+1$ is also of that form, in A_2 there are only elements of the form $6l+1$. In order to prove that $A_2 \neq G(N)$, it is sufficient to show that there exists an integer s such that $6s+5 \in G(N)$. But if $5^\gamma \mid N$ and $5^{\gamma+1} \nmid N$, then $s = N/5^\gamma$ satisfies our condition.

Thus, to complete the proof, it is sufficient to show that, for $N = 6N_1$ and for every non-principal character χ of $G(N)$ which is trivial on A_2, there exists no prime p such that

$$1+\sum_{j=1}^{\infty} \chi\left(\frac{p^{j+1}-1}{p-1}\right) p^{-j/2} = 0. \tag{10}$$

We have

$$\left|\sum_{j=1}^{\infty}\chi\left(\frac{p^{j+1}-1}{p-1}\right)p^{-j/2}\right| \leqslant \sum_{j=1}^{\infty}p^{-j/2} = \frac{1}{\sqrt{p}-1}$$

and, for $p \geqslant 5$, $1/(\sqrt{p}-1) < 1$. Thus, if (10) is satisfied, then $p = 2$ or $p = 3$. If $p = 3$, then, because of $2 \mid (3^{2s}-1)/2$, we have

$$\chi\left(\frac{3^{2s}-1}{2}\right) = 0$$

and

$$\left|\sum_{j=1}^{\infty}\chi\left(\frac{3^{j+1}-1}{2}\right)3^{-j/2}\right| = \left|\sum_{j=1}^{\infty}\chi\left(\frac{3^{2j+1}-1}{2}\right)3^{-j}\right| \leqslant \sum_{j=1}^{\infty}3^{-j} = \frac{1}{2} < 1.$$

If $p = 2$, then $3 \mid 2^{2k}-1$ and

$$\left|\sum_{j=1}^{\infty}\chi(2^{j+1}-1)2^{-j/2}\right| = \left|\sum_{j=1}^{\infty}\chi(2^{2j+1}-1)2^{-j}\right| \leqslant \sum_{j=1}^{\infty}2^{-j} = 1,$$

whence we see that

$$1+\sum_{j=1}^{\infty}\chi(2^{j+1}-1)2^{-j/2} = 0$$

only if, for every j, $\chi(2^{2j+1}-1) = -1$. But this is impossible because if $7 \mid N$, then $\chi(2^{2s+1}-1) = 0$ and if $7 \nmid N$, then $7 \in A_2$ and $\chi(7) = 1$. In the second case $7 \in A_2$ because the congruence

$$x^2+x+1 \equiv 7 \pmod{3^{\beta}}$$

has a solution $x \in G(3^{\beta})$ and because the elements

$$(7,1,\ldots,1),\ (1,1,7,1,\ldots,1),\ (1,1,1,7,1,\ldots,1),\ \ldots,\ (1,\ldots,1,7)$$

belong to A_2.

Hence the proof of our theorem is complete.

3. It would be of interest to know for which N the function

$$\sigma_{\nu}(n) = \sum_{d \mid n} d^{\nu}$$

is WUD(mod N) (**P 844**). For $\nu = 0$, there is $\sigma_0(n) = d(n)$. Those numbers N for which $d(n)$ is WUD(mod N) were found in [2]. The answer in the case $\nu = 1$ is given by Theorem 1. For $\nu > 1$, the following theorem gives a partial answer:

THEOREM 2. *If* $(v, \varphi(N)) = 1$, *then* $\sigma_v(n)$ *is* WUD(mod N) *if and only if* $6 \nmid N$. *If* $\varphi(N) | v$, *then* $\sigma_v(n)$ *is* WUD(mod N) *if and only if* $d(n)$ *is* WUD(mod N) (*see* [2]).

The proof of the first part of Theorem 2 is analogous to the proof of Theorem 1, and the proof of the second part — to the proof of Corollary 1 in [2].

REFERENCES

[1] З. И. Боревич и И. Р. Шафаревич, *Теория чисел*, Москва 1964.

[2] W. Narkiewicz, *On distribution of values of multiplicative functions in residue classes*, Acta Arithmetica 12 (1967), p. 269-279.

Reçu par la Rédaction le 14. 2. 1972