MATHEMATICS OF COMPUTATION
VOLUME 51, NUMBER 183
JULY 1988, PAGES 331-337

# Weak Uniform Distribution for Divisor Functions. II

By Francis J. Rayner

**Abstract.** The author's methods (reference [4]) are developed further to apply to divisor functions $\sigma_i$ for even values of $i$. The results of calculations for even values of $i$ in the range $4 \leq i \leq 50$ are tabulated.

**1. Introduction.** Throughout, the notation and definitions of the author's previous paper [4] will be used. For a full account of the background, see [2].

The function $\sigma_i(x)$ is defined for positive integers $i, x$ by

$$\sigma_i(x) = \sum_{d \mid x} d^i.$$

An arithmetic function $f$ is defined to be weakly uniformly distributed modulo $n$ (WUD (mod $n$), for short) if the set

$$\{x \in \mathbf{Z} \colon x > 0, (f(x), n) = 1\}$$

is infinite and for every pair of integers $a_1, a_2$ with $(a_1, n) = (a_2, n) = 1$,

$$\#\{x\colon\ 0 < x < t,\ f(x) \equiv a_1 \bmod n\} \sim$$
$$\#\{x\colon\ 0 < x < t,\ f(x) \equiv a_2 \bmod n\}$$

as $t \to \infty$.

In [4] the weak uniform distribution properties of $\sigma_i$ were studied for odd values of $i$. The algorithm embodied in [4, Lemmas 1–4] and derived from Narkiewicz [2] applies equally well to even values of $i \geq 4$. The improvement contained in [4, Propositions 1 and 2] extends to the even case, and a somewhat weaker version of [4, Proposition 3] can be proved (see Section 3 below).

The result of these calculations is that we find, for even $i \geq 4$, sets $K_1$, $K_2$ and $K_4$ of positive integers such that $\sigma_i$ is weakly uniformly distributed modulo $n$ if and only if

(i) $n$ is odd and not divisible by an element of $K_1$, or

(ii) $n$ is even, not divisible by 6 and not divisible by any element of $K_2$, or

(iii) $n$ is divisible by 6 and not divisible by any element of $K_4$.

At the end of this paper, tables are given of the sets $K_1, K_2$ and $K_4$ for each $i$ in the range $4 \leq i \leq 50$.

Received August 23, 1984; revised September 15, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B99; Secondary 11-04, 11A25, 11F30, 11N69, 11Y99.

For completeness, we recall the property of $\sigma_2$ proved by Narkiewicz and Rayner [3]:

The function $\sigma_2$ is WUD (mod $n$) if and only if either

(i) $n$ is odd and not divisible by 15, or

(ii) $n$ is even, not divisible by 6, and not divisible by 8 or 28, or

(iii) $n$ is divisible by 6, and not divisible by 12, 30, 42, or 66, or

(iv) $n$ is divisible by 8 and not divisible by 40, or

(v) $n$ is divisible by 40 and not divisible by any prime $p \geq 7$ for which the order of 4 modulo $p$ is odd.

Thus, $\sigma_2$ does not fit the general pattern described above in respect of moduli divisible by 8, where a more complicated version of [4, Lemma 1] applies. However, as can be seen in the tables of results below, for every even $i \geq 4$, the set $\{15\}$ in (i) is contained in $K_1(i)$, the set $\{8, 28\}$ in (ii) is contained in $K_2(i)$, and the set $\{12, 30, 42, 66\}$ in (iii) is contained in $K_4(i)$. (Note that for $i, k > 2$, and all $j$, if $i \mid k$, then $K_j(i) \subset K_j(k)$.)

As in [4], the calculations of the present paper depend on properties of a set of primes bounded above by $(i+1)^2$ in the case of $K_1$, by $(2i+1)^2$ in the case of $K_2$, and by $(4i+1)^2$ in the case of $K_4$ (see [4, Lemma 4]). In the course of the calculations it became clear that these bounds are too high and that a bound of $5i^{1.5}$ in all three cases would be consistent with the primes actually found. Indeed, something slightly stronger might be true. This is in line with [4, Observation 3]. If such better bounds could actually be proved, it would be easy to carry the calculations considerably further.

**2. Values of $d$.** As in [4], let $V_j(x) = 1 + x^i + x^{2i} + \cdots + x^{ji}$, let $R_j(n) = \{V_j(a) \bmod n \colon\ a \in Z,\ (aV_j(a), n) = 1\}$, as a subset of the multiplicative group $G(n)$ of residue classes prime to $n$, let $\Lambda_j(n)$ be the subgroup of $G(n)$ generated by $R_j(n)$, and let $d(n)$ be the least value of $j \geq 1$ for which $R_j(n) \neq \varnothing$.

In order to apply [4, Lemmas 1–4] to the case of even values of $i \geq 4$, we need first to determine the values of $d(n)$ for each $i$.

LEMMA 1. *Let $m, n$ be positive integers. Then $R_j(n)$ is the image of $R_j(mn)$ under the mapping induced by $x \bmod mn \to x \bmod n$.*

COROLLARY 1. *$\Lambda_j(n)$ is the image of $\Lambda_j(mn)$.*

COROLLARY 2. *The following statements are equivalent:*

(i) $R_j(n) \neq \varnothing$;

(ii) *For all primes $p$ which divide $n$, $R_j(p) \neq \varnothing$.*

COROLLARY 3. *Let $4 \mid i$ and $30 \mid n$. Then $R_4(n) = \varnothing$.*

*Proof.* (Corollary 3) $G(30)$ is an abelian group of exponent 4; the only value of $x^i \bmod 30$ is 1, and so $V_4(x) = 5$ for all $x$. Hence, $R_4(30) = \varnothing$, and the result follows from Lemma 1.

LEMMA 2. *For any prime $p$, if, for all $x \in G(p)$, $x^i = 1$, then $R_{p-1}(p) = \varnothing$. If there exists $x \in G(p)$ with $x^i \neq 1$, then $R_{p-1}(p) = \{1\}$.*

*Proof.* In the second case, calculating in the field of $p$ elements, $V_{p-1}(x) = (1 - (x^i)^p)/(1 - x^i) = 1$.

COROLLARY. *Let $q$ be the least prime for which $(q-1)$ does not divide $i$. Then $d \leq q-1$.*

*Proof.* Lemma 1, Corollary 3 shows that it is enough to prove that for all $p$ dividing $n$ we have $R_{q-1}(p) \neq \varnothing$. For $p \neq q$ we have $q \in R_{q-1}(p)$; for $p = q$, Lemma 2 gives $R_{q-1}(p) = \{1\}$.

(This Corollary is due to Narkiewicz [1, Lemma 1].)

PROPOSITION 1. *Let $i$ be even.*
(i) *if $n$ is odd then $d(n) = 1$;*
(ii) *if $n$ is even and not divisible by 6, then $d(n) = 2$;*
(iii) *if $n$ is divisible by 6 and not divisible by 30, then $d(n) = 4$.*

*Proof.* In case (i), $2 \in R_1(n)$; in case (ii), $3 \in R_2(n)$; and in case (iii), $R_2(6) = \varnothing$ and so, by Lemma 1, $R_2(n) = \varnothing$. Now $5 \in R_4(n)$.

PROPOSITION 2. *Let $30 \mid n$, and let $i$ be even. Then $\sigma_i$ is not WUD* $(\operatorname{mod} n)$.

*Proof.* Note that $d = d(n)$ is even and $\geq 4$.

Firstly, if $i \equiv 2 \pmod 4$, numerical calculation shows $R_4(30) = \{11\}$, so that $d = 4$ and $\Lambda_4(30)$ is cyclic. Since $G(30)$ is not cyclic, $R_4(30)$ does not generate $G(30)$. Secondly, if $i \equiv 0 \pmod 4$, then in $G(30), x^4 = 1$ for all $x$, so that $R_d(30) = \{d+1\}$. Thus $\Lambda_d(30)$ is cyclic, and (again) $R_d(30)$ does not generate $G(30)$.

In either case, it follows from [4, Lemma 1] that $\sigma_i$ is not WUD (mod $n$).

**3. Squares of Primes.** Here the objective is to show that, in [4, Lemma 3], and in the calculation of the sets $k_j$ it is only necessary to consider squares of primes in a few cases (see the Corollary to Proposition 4 below).

Let $q$ denote an odd prime, and (as in [4]) define the homomorphisms $\phi$: $G(q^2) \to G(q)$ and $\phi(x \bmod q^2) = x \bmod q$ and $\psi$: $G(q) \to G(q^2)$ by $\psi(x \bmod q) = x^q \bmod q^2$.

PROPOSITION 3. *Let $q$ be an odd prime not dividing the integer $i$. Let $R_j(q)$ and $R_j(q^2)$ be calculated using the polynomial $V_j$, where $j = 1, 2$, or 4. Then there is a nontrivial character on $G(q^2)$ constant on $R_j(q^2)$ if and only if there is a nontrivial character on $G(q)$ constant on $R_j(q)$. Moreover, for $j = 1$ and 2, the values of the nontrivial character on $G(q^2)$ are $(q-1)$th roots of unity and take the same value on $R(q^2)$ as the values of the nontrivial character on $G(q)$ does on $R(q)$.*

*Proof.* For $j = 1$, this is [4, Proposition 1], and for $j = 2$, this is [4, Proposition 2]. In these cases, it was shown in [4] that, given a nontrivial character $\chi$ on $G(q^2)$ taking a constant value $a$ on $R_j$, the corresponding character on $G(q)$ was $\chi \circ \psi$ taking the value $a^q$ on $R_j(q)$. Since $\chi \circ \psi$ is nontrivial, the values of $\chi$ cannot be $q$th roots of unity. Moreover, if the values of $\chi$ are $q$th roots of unity, then $\chi^t$ will be a nontrivial character constant on $R(q^2)$ with values which are $q$th roots of unity, and we have just seen that this cannot happen. Hence the values of $\chi$ on $G(q^2)$ are all $(q-1)$th roots of unity; since then $a^q = a$, the characters $\chi$ and $\chi \circ \psi$ take the same values on $R(q^2)$ and $R(q)$, respectively.

Now suppose $j \geq 4$, and write $V = V_j$, and let $\chi$ be a nontrivial character on $G(q^2)$ constant on $R_j(q^2)$. Then $\chi \circ \psi \circ \phi$ is again a character constant on $R_j(q^2)$, so that $\chi \circ \psi$ is a character on $G(q)$ constant on $R_j(q)$ which will be nontrivial unless $\ker\chi$ contains the subgroup of $G(q^2)$ of order $(q-1)$. Since $q$ is prime and $\chi$ is nontrivial, the only case which occurs is that in which $\ker\chi$ is the subgroup of order $q-1$. Since all of $R_j(q^2)$ is contained in a single coset of this subgroup, it follows that $R_j(q^2)$ has fewer than $q$ elements. From Taylor's theorem,

$$V(x+qy) \equiv V(x) + qyV'(x) \bmod q^2,$$

so that, if $V'(x)$ is not congruent to 0 modulo $q$, then there are $q$ elements of $R_j(q^2)$ mapped by $\phi$ onto the element $V(x) \bmod q$ of $R_j(q)$. Since this cannot happen, it follows that, whenever $V(x) \bmod q \in R(q)$ (i.e., $V(x)$ does not vanish modulo $q$), we have $V'(x) \equiv 0 \bmod q$. Differentiation of the equation $(1-x^i)V(x) = 1 - x^{ji}$ gives $V(x) \equiv (j+1)x^{ji} \bmod q$ whenever $V'(x) \equiv 0 \bmod q$, so that $V(x)$ is always in the $(j+1)$ coset of the subgroup of squares in $G(q)$, i.e., the quadratic character of $G(q)$ is constant on $R_j(q)$. This completes the proof of Proposition 3.

As a consequence, we can find all primes $q$ for which there is a character mod $q^2$ constant on $R_j(q^2)$ by merely finding those primes for which there is a character mod $q$ constant on $R_j(q)$. Further, for $j = 1$ and 2, if $\sigma_i$ is not WUD (mod $m$), and $m$ has a factor $p^2$, then $\sigma_i$ is not WUD (mod $m/p$).

COROLLARY. *Let $i$ be even or $j$ be even. Let there be a nontrivial character $\chi$ on $G(q^2)$ taking the constant value 1 on $R_j(q^2)$. Then there is a nontrivial character on $G(q)$ taking the constant value 1 on $R_j(q)$.*

*Proof.* The character is $\chi \circ \psi$ with the required property, unless $\ker\chi$ is the subgroup of $G(q^2)$ of order $q-1$. In this case, the elements of $R_j(q)$ are given by those nonzero values of $V_j(x) \bmod q$ arising from those values of $x$ which satisfy $V_j'(x) \equiv 0 \bmod q$, and we have $V_j(x) \equiv (j+1)x^{ij} \bmod q$. Firstly, let $j \equiv -1 \bmod q$. Then all values of $V_j(x)$ are congruent to zero modulo $q$, so that $R_j(q) = \varnothing$. Secondly, let $j \equiv 0 \bmod q$. Then all values of $V_j(x)$ are congruent to a square modulo $q$ (since $ij$ is even), and the quadratic character on $G(q)$ takes the constant value 1 on $R_j(q)$. Finally, let $j$ be different from $-1$ and 0 modulo $q$. Then $j+1 \in R_j(q)$, since $j+1 = V(j)$. However, $V_j'(1) = ij(j+1)/2$, which is nonzero mod $q$, so that there are $q$ distinct elements of $R_j(q^2)$ mapped onto $j+1 \bmod q$ by $\phi$, which is impossible because cosets of $\ker\chi$ have at most $q-1$ elements.

PROPOSITION 4. *Let $i$ be even. Let $p$ be an odd prime greater than 3 such that $p$ does not divide $i$ and such that there is a character modulo $p^a$ constant on $R_j(p^a)$ with $a = 1$ or 2. Let $t$ be an integer not divisible by $p$, and if $t \neq 1$, such that also $p$ is not a divisor of the order of $G(t)$. Let $R_j(pt)$ generate $G(pt)$. Then $R_j(p^2t)$ generates $G(p^2t)$.*

*Proof.* The case $t = 1$ is the Corollary to Proposition 3. By Lemma 1, $R_j(p)$ generates $G(p)$ and $R_j(t)$ generates $G(t)$; by the Corollary to Proposition 3, $R_j(p^2)$ generates $G(p^2)$. Now suppose $R_j(p^2t)$ does not generate $G(p^2t)$. Then there is a character $\chi_1$ on $G(p^2)$ taking a constant value $\alpha \neq 1$ on $R_j(p^2)$ and another character $\chi_2$ on $G(t)$ taking a constant value $\alpha^{-1}$ on $R_j(t)$. Suppose $e$ is the least exponent for which $\alpha^e = 1$. Then $e > 1$ and $e \mid p(p-1)$ and $e$ divides the order of $G(t)$. Now $p$ does not divide the order of $G(t)$, so that $e \mid (p-1)$, and $\chi_1 \circ \psi$ is a character of $G(p)$ taking the constant value $\alpha$ on $R_j(t)$. Hence $R_j(pt)$ does not generate $G(pt)$, contrary to hypothesis. This completes the proof of Proposition 4.

COROLLARY. *When constructing products $m$ of primes and squares of primes to test as in* [4, *Lemma* 2] (*see Section* 4, *stage* 4 *below*), *it is unnecessary to consider the square of an odd prime $p$ unless $p$ is a divisor of $i$ or a divisor of $s-1$, where $s$ is any other prime divisor of $m$. Further, for $j=1$ or $j=2$ it is unnecessary to consider the square of $p$ unless $p \mid i$.*

*Proof.* For $j=4$ this follows from Proposition 4. For $j=1,2$ this follows from consideration of the characters described in the proof of Proposition 3.

**4. Calculations.** Suppose that $i$ is even and $\geq 4$. The algorithm described in [4] can be carried out with the benefit of Propositions 1 to 4, and is then as follows.

Let $j=1$ or 2 or 4.

*Stage* 1. Determine the set $H_j$ of all primes less than $(1+ij)^2$, excluding 2 in the case $j=1$, and excluding 3 in the case $j=2$.

*Stage* 2. Determine the set $I_j$ consisting of all $p$ in $H_j$ together with $p^2$ (whenever $p \in H_j$ and $p \mid i$) and 8 (whenever $2 \in H_j$).

*Stage* 3. Determine the set $J_j$ of all $n$ in $I_j$ for which there is a nontrivial character of $G(n)$ constant on $R_j(n)$.

*Stage* 4. Determine the set $K_j$ of all integers $n=\prod q_i$ for which $R_j(n)$ does not generate $G(n)$, where all the $q_i$ are distinct, and for each $i$, either $q_i \in J_j$ or $q_i=p^2$ where $p \in H_j \cap J_j$ and $p \mid (q_j-1)$ for some $j \neq i$, and furthermore, for $j=2, n$ is even and for $j=4, n$ is divisible by 6.

Then $\sigma_i$ will fail to be WUD (mod $m$) if and only if

(i) $m$ is odd and divisible by an element of $K_1$, or

(ii) $m$ is even, not divisible by 6, but divisible by an element of $K_2$, or

(iii) $m$ is divisible by 6 and not divisible by 30, but divisible by an element of $K_4$, or

(iv) $m$ is divisible by 30 (Proposition 2).

We can incorporate case (iv) in case (iii) by including the integer 30 in each of the sets $K_4$ in the tables below, and can remove as redundant from each $K_d$ any integer properly divisible by another element of the same $K_d$.

Calculations of $K_1, K_2$ and $K_4$ for $4 \leq i \leq 200$ have been carried out in the University of Liverpool Computer Laboratory, and the results for $i \leq 50$ are given below. The general pattern for $50 < i \leq 200$ is similar, with no additional features appearing.

During the course of the calculations for $K_4$ it was observed that whenever the prime $p \geq 5$ was such that there was a nontrivial character on $G(p)$ constant on $R_4(p)$, then $\sigma_i$ failed to be WUD (mod $6p$). Thus it was never necessary to test for WUD (mod $6p^2$), etc., so that the calculations became lighter.

As noted in Section 1 above, in the calculations of $K_1, K_2$ and $K_4$ the upper bounds in stage 1 of the algorithm are much higher than necessary, and a bound of $5i^{1.5}$ would not lead to smaller sets $J_d$ in the range of calculations attempted. The indications are that this bound should apply at least for values of $i$ up to 1225.

It is an unsettled problem to prove that these two observations are true in general.

## Tables of Results

*The sets* $K_1(i)$. For odd $m, \sigma_i$ is not WUD (mod $m$) if and only if $m$ is divisible by an element of $K_1(i)$.

| $i$ | $K_1(i)$ |
|---|---|
| 4 | 15 |
| 6 | 7 15 39 57 65 95 247 |
| 8 | 15 17 |
| 10 | 15 33 41 55 |
| 12 | 7 15 39 57 65 95 183 247 305 793 1159 |
| 14 | 15 87 129 145 215 1247 |
| 16 | 15 17 |
| 18 | 7 15 39 57 65 95 111 185 247 481 703 |
| 20 | 15 33 41 55 |
| 22 | 15 23 201 335 |
| 24 | 7 15 17 39 57 65 73 95 183 247 305 793 1159 |
| 26 | 15 159 265 |
| 28 | 15 87 113 129 145 215 1247 |
| 30 | 7 15 31 33 39 41 55 57 65 95 143 183 209 247 305 671 793 1159 |
| 32 | 15 17 97 193 |
| 34 | 15 137 239 |
| 36 | 7 15 39 57 65 73 95 109 111 183 185 247 305 481 703 793 1159 2257 |
| 38 | 15 |
| 40 | 15 17 33 41 55 |
| 42 | 7 15 39 43 57 65 87 95 127 145 247 337 377 551 1137 1895 4927 7201 10991 |
| 44 | 15 23 89 201 335 |
| 46 | 15 47 417 695 |
| 48 | 7 15 17 39 57 65 73 95 97 183 247 305 793 1159 3033 4381 |
| 50 | 15 33 41 55 151 303 505 1111 |

*The sets* $K_2(i)$. For even $m$ not divisible by $6, \sigma_i$ is not WUD (mod $m$) if and only if $m$ is divisible by an element of $K_2(i)$.

| $i$ | $K_2(i)$ |
|---|---|
| 4 | 8 20 26 28 70 |
| 6 | 8 26 28 76 266 |
| 8 | 8 20 26 28 70 164 194 410 574 |
| 10 | 8 22 28 82 124 434 |
| 12 | 8 20 26 28 70 74 76 146 190 266 |
| 14 | 8 28 172 602 |
| 16 | 8 20 26 28 68 70 164 170 194 238 410 574 1394 |
| 18 | 8 26 28 74 76 146 266 362 |
| 20 | 8 20 22 26 28 70 82 122 124 310 434 |
| 22 | 8 28 46 134 |
| 24 | 8 20 26 28 70 74 76 146 164 190 194 266 410 574 1558 |
| 26 | 8 28 316 1106 |
| 28 | 8 20 26 28 70 116 172 290 406 430 602 2494 |
| 30 | 8 22 26 28 76 82 122 124 266 302 434 1178 |
| 32 | 8 20 26 28 68 70 164 170 194 238 386 410 574 1394 |
| 34 | 8 28 206 818 |
| 36 | 8 20 26 28 70 74 76 146 190 218 266 362 866 |
| 38 | 8 28 914 |
| 40 | 8 20 22 26 28 70 82 122 124 194 310 434 482 |
| 42 | 8 26 28 76 172 266 508 602 674 1634 1778 4826 10922 |
| 44 | 8 20 26 28 46 70 134 |
| 46 | 8 28 94 556 1946 |
| 48 | 8 20 26 28 68 70 74 76 146 164 170 190 194 238 266 386 410 574 646 1394 1558 4718 12806 |
| 50 | 8 22 28 82 124 302 434 |

*The sets* $K_4(i)$. For $m$ divisible by $6, \sigma_i$ is not WUD (mod $m$) if and only if $m$ is divisible by an element of $K_4(i)$.

| $i$ | $K_4(i)$ |
|---|---|
| 4 | 12 30 42 66 |
| 6 | 12 30 42 66 78 186 366 |
| 8 | 12 30 42 66 246 |
| 10 | 12 30 42 66 186 246 366 |
| 12 | 12 30 42 66 78 186 366 |
| 14 | 12 30 42 66 174 258 426 |
| 16 | 12 30 42 66 102 246 |
| 18 | 12 30 42 66 78 114 186 366 654 |
| 20 | 12 30 42 66 186 246 366 606 1446 |
| 22 | 12 30 42 66 138 402 534 |
| 24 | 12 30 42 66 78 186 246 366 |
| 26 | 12 30 42 66 786 |
| 28 | 12 30 42 66 174 258 426 |
| 30 | 12 30 42 66 78 186 246 366 906 1086 1446 3246 |
| 32 | 12 30 42 66 102 246 |
| 34 | 12 30 42 66 618 2454 |
| 36 | 12 30 42 66 78 114 186 222 366 654 1086 |
| 38 | 12 30 42 66 1146 1374 |
| 40 | 12 30 42 66 186 246 366 606 1446 2406 |
| 42 | 12 30 42 66 78 174 186 258 366 426 762 1266 2022 2526 |
| 44 | 12 30 42 66 138 402 534 |
| 46 | 12 30 42 66 282 |
| 48 | 12 30 42 66 78 102 186 246 366 1446 |
| 50 | 12 30 42 66 186 246 366 606 1506 3606 4206 7806 |

Department of Pure Mathematics
The University of Liverpool
P.O. Box 147
Liverpool, Great Britain GB-L69 3BX

1. W. NARKIEWICZ, "Distribution of coefficients of Eisenstein series in residue classes," *Acta Arith.*, v. 43, 1983, pp. 83–92.

2. W. NARKIEWICZ, *Uniform Distribution of Sequences of Integers in Residue Classes*, Lecture Notes in Math., vol. 1087, Springer-Verlag, Berlin and New York, 1984.

3. W. NARKIEWICZ & F. RAYNER, "Distribution of values of $\sigma_2(n)$ in residue classes," *Monatsh. Math.*, v. 94, 1982, pp. 133–141.

4. FRANCIS J. RAYNER, "Weak uniform distribution for divisor functions. I," *Math. Comp.*, v. 50, 1988, pp. 335–342.