MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 181
JANUARY 1988, PAGES 335-342

Weak Uniform Distribution for Divisor Functions. I

By Francis J. Rayner

Abstract. Narkiewicz (reference [3, pp. 204–205]) has proposed an algorithm for determining the moduli with respect to which a given arithmetic function (of suitable type) has weak uniform distribution. The class of functions to which this algorithm applies includes the divisor functions σ_i. The present paper gives an improvement to the algorithm for odd values of i, which makes computation feasible for values of i up to 200. The results of calculations for odd values of i in the range $1 \leq i \leq 199$ are reported.

1. Introduction. Let $\sigma_i(x)$ be defined for positive integers i, x by

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

For odd values of i, the functions σ_i occur as Fourier coefficients of Eisenstein series.

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

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

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

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

as $t \to \infty$.

The integers n for which $\sigma_i(x)$ is WUD (mod n) have been determined by Sliwa [6] for $i = 1$, by Narkiewicz and Rayner [5] for $i = 2$, and by Narkiewicz [2] for $i = 3$. In the present paper the methods of [2] are further improved. For each odd integer $i > 0$, there exist two finite sets of integers K_1 and K_2 such that σ_i has WUD (mod n) if and only if either n is odd and not divisible by an element of K_1 or n is even and not divisible by an element of K_2.

Calculations of the sets K_1 and K_2 for σ_i for all odd values of i from 5 to 199 have been carried out in the University of Liverpool Computer Laboratory. The results are tabulated at the end of this paper, and the earlier results of Sliwa ($i = 1$) and Narkiewicz ($i = 3$) have been incorporated.

Observation 1. Within the range of the table, it can be seen that if i is prime and $2i + 1$ is composite, then K_1 is empty, and that if i and $2i + 1$ are both prime, then $K_1 = \{2i + 1\}$ for $i \equiv 3 \bmod 4$, and $K_1 = \{6i + 3\}$ for $i \equiv 1 \bmod 4$.

Observation 2. Within the range of the table, if i is prime and $2i+1$ is composite, then $K_2 = \{6\}$, with the sole exception of $i = 43$, where $K_2 = \{6, 2066\}$. Further, if i is prime and $2i + 1$ is prime, then $K_2 = \{6, 4i + 2\}$.

Received October 11, 1983; revised April 22, 1987.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11B99; Secondary 11-04, 11A25, 11F30, 11N69, 11Y99.

Observation 3. The upper bound of Lemma 4 below, $(2i+1)^2$, for the set of primes involved in the calculations is much higher than necessary. A value of $(2i+1)^{1.6}$ would be consistent with the values actually found. It would be possible to make calculations for higher values of i if this observed upper bound could be proved to hold in general.

Since this paper was originally submitted, Narkiewicz's book [4] has appeared. It describes the background and motivation for these calculations and refers to the original version of this paper in which the calculations were carried out for values of $i \leq 107$.

Narkiewicz records that Observation 1 concerning K_1 has been shown to be true generally by E. Dobrowolski (see [4, p. 110, Theorem 6.12]). (See also Narkiewicz [2] for part of this result.)

In [4, p. 112, Problem V] Narkiewicz asks for a characterization of those odd integers i such that σ_i fails to have WUD (mod n) if and only if 6 divides n. Since for composite i the set of moduli for which WUD fails is at least the union of the corresponding sets for the factors of i, one might first consider prime values for i. However, even for prime i, there seems to be no easily observed pattern of behavior of K_2. As in Observation 2 above, in the case in which i is prime and $2i+1$ is composite, while K_1 is always empty it is not always true that $K_2 = \{6\}$, since σ_{43} is not WUD (mod 2066), although this seems to be a rare exception. Calculations for prime values of i are easier than for composite ones, and a search beyond the limits of the present tables, assuming a reduced upper bound as in Observation 3, shows that the next primes i for which K_2 behaves in this way are

$$\begin{aligned} i &= 467, \quad \text{where } K_2 = \{6, 24286\}, \\ i &= 503, \quad \text{where } K_2 = \{6, 24146\}, \text{ and} \\ i &= 883, \quad \text{where } K_2 = \{6, 38854\}. \end{aligned}$$

It is worth noticing in connection with Observation 2 and Dobrowolski's result cited above from [4] that for $i = 809$ we have $K_2 = \{6, 3338, 38834\}$. Thus, although here i and $2i+1$ are both prime, it is not always true that under these conditions $K_2 = \{6, 4i+2\}$, 809 being the first exception.

Because of the reduced upper bound assumed here, these results for $i > 200$ may possibly be incomplete in the sense that the sets K_2 might be larger than stated (and therefore similar results might hold for smaller values of i), but this is extremely unlikely.

Observation 4. Ramanujan's τ function has WUD (mod n) if and only if either n is odd and not divisible by 7 (Serre) or even and divisible neither by 6 nor 46 (Narkiewicz). (See [4, p. 89, Theorem 5.18].) Thus τ behaves with respect to weak uniform distribution in the same way as σ_3 for odd n and in the same way as σ_{11} for even n.

2. Narkiewicz's Algorithm. For a fixed value of $i > 2$, let

$$V_j(x) = 1 + x^i + x^{2i} + \cdots + x^{ji}.$$

Thus, for a prime p, $\sigma_i(p^j) = V_j(p)$. Let

$$R_j(n) = \{V_j(a) \bmod n : a \in \mathbf{Z},\ (aV_j(a), n) = 1\},$$

regarded 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 $R_j(n)$. Let $d(n)$ be the smallest $j \geq 1$ for which $R_j(n) \neq \varnothing$.

The following Lemmas 1–4 are special cases of results proved by Narkiewicz [2], [3].

LEMMA 1. *σ_i has WUD* (mod n) *for $i > 2$ if and only if $\Lambda_{d(n)}(n) = G(n)$.*

Note that for odd $i > 2$, $d(n) = 1$ if n is odd, and $d(n) = 2$ if n is even. Lemma 1 gives a means of calculating whether σ_i is WUD (mod n) for any particular values of i and n.

LEMMA 2. *Let $n = q_1 \cdots q_r$, where $q_1, \dots, q_r$ are powers of distinct primes. Suppose for each q_s, $\Lambda_j(q_s) = G(q_s)$. Then $\Lambda_j(n) \neq G(n)$ if and only if*

(i) *there exist characters χ_s of $G(q_s)$ $(s = 1, \dots, r)$ such that χ_s takes a constant value c_s (say) on $R_j(q_s)$;*

(ii) $\prod_{s=1}^{r} c_s = 1$; *and*

(iii) *not all the characters χ_s are trivial.*

LEMMA 3. *Let $q = p^t$, where p is an odd prime. Then there is a nontrivial character of $G(q)$ taking a constant value on $R_j(q)$ if and only if there is such a character of $G(p^u)$ taking a constant value on $R_j(p^u)$, where $u = \min\{t, 2\}$. For $p = 2$ a similar result holds with $u = \min\{t, 3\}$.*

LEMMA 4. *For any prime p, if there is a nontrivial character of $G(p^t)$ taking a constant value on $R_j(q)$, then $p < (e_j + 1)^2$ where e_j is the degree of $V_j(x)$.*

Remark. A slightly stronger result is due to Fomenko [1].

Let i now denote an odd integer greater than 1. It is easily seen that if $\Lambda_j(n) \neq G(n)$, then $\Lambda_j(mn) \neq G(mn)$ for any integer $m > 1$. It follows that there are finite sets of integers K_1 and K_2 such that σ_i is WUD (mod n) if and only if n is odd and not divisible by an element of K_1 or n is even and not divisible by an element of K_2. The sets K_1 and K_2 can be found in the following way, as follows from Lemmas 1–4.

For $j = 1, 2$, let H_j be the set of primes p satisfying the inequality of Lemma 4 (in which $e_1 = i$ and $e_2 = 2i$).

Let $I_j = H_j \cup \{p^2 : p \in H_j\} \cup \{8\}$, and let

$$J_j = \{m \in I_j : \text{there exists a nontrivial character on } G(m) \text{ constant on } R_j(m)\},$$

including cases in which $\Lambda_j(m)$ is a proper subgroup of $G(m)$.

Then K_j is the set of all products r of elements of J_j (no element being taken more than once in each product) for which $\Lambda_j(r) \neq G(r)$.

Narkiewicz [2] has determined K_1 and K_2 for $i = 3$. Because it may be necessary to examine primes p up to $(2i + 1)^2$ and to calculate values of $R_2(p^2)$ in $G(p^2)$, the calculations become difficult with increasing i. The Propositions in Section 3 below make it unnecessary to consider squares of most odd primes and reduce the number of primes which need to be included in the sets H_j, although the upper bounds are not altered.

3. Some Improvements. Throughout this paragraph, let $W(x)$ be a polynomial with integer coefficients, and let

$$R(n) = \{W(a) \bmod n\colon\ a \in \mathbf{Z},\ (aW(a), n) = 1\},$$

regarded as a subset of $G(n)$.

For any prime q, let $\phi\colon\ G(q^2) \to G(q)$ be defined, for $x \in \mathbf{Z}$, by $\phi(x \bmod q^2) = x \bmod q$, and let $\psi\colon\ G(q) \to G(q^2)$ be defined, for $x \in \mathbf{Z}$, by $\psi(x \bmod q) = x^q \bmod q^2$. It is easy to see that ϕ and ψ are homomorphisms of abelian groups, that $\psi(\phi(z)) = z$ for all $z \in G(q)$ (so that ϕ is an epimorphism and ψ is a monomorphism) and that $\phi(R(q^2)) = R(q)$.

LEMMA 5. *Let χ be any nontrivial character on $G(q)$ which is constant on $R(q)$. Then $\chi \circ \phi$ is a nontrivial character on $G(q^2)$ which is constant on $R(q^2)$.*

Proof. Immediate.

LEMMA 6. *Let χ be any nontrivial character on $G(q^2)$ taking the constant value 1 on $R(q^2)$, and suppose that $\chi \circ \psi$ is the trivial character on $G(q)$. Then $R(q^2)$ and $R(q)$ have the same cardinal number.*

Proof. First, $R(q^2) \subset \ker \chi$. Again, $\operatorname{im} \psi \subset \ker \chi$. Now $\operatorname{im} \psi$ is a subgroup of $G(q^2)$ of prime index q, so, since χ is not the trivial character, $\operatorname{im} \psi = \ker \chi$. Thus $R(q^2) \subset \operatorname{im} \psi$. The restriction of ϕ to $\operatorname{im} \psi$ is bijective, and $\phi(R(q^2)) = R(q)$. Hence the result.

LEMMA 7. *Suppose that the prime number q and polynomial $W(x)$ are such that $\psi(R(q)) \subset R(q^2)$. Let χ be any nontrivial character on $G(q^2)$ which is constant on $R(q^2)$. Then $\chi \circ \psi$ is a nontrivial character on $G(q)$ which is constant on $R(q)$.*

Proof. Since $\psi(R(q)) \subset R(q^2)$, $\chi \circ \psi$ is a character constant on $R(q)$, and it will be enough to show that it is nontrivial. If it is trivial, then $\chi(\psi(R(q))) = 1$, and so the constant value of χ on $R(q^2)$ is 1. The result now follows from Lemma 6.

PROPOSITION 1. *Let $W(x) = 1 + x^i$, where i is odd and not divisible by the odd prime q. Then there is a nontrivial character on $G(q^2)$ constant on $R(q^2)$ if and only if there is a nontrivial character on $G(q)$ constant on $R(q)$.*

Proof. It is enough to show that Lemma 7 applies. Let $x \in \mathbf{Z}$ be such that $x \bmod q \neq 0$, and let $y_\lambda = x + \lambda q$ for $\lambda = 0, 1, \ldots, q-1$. Then

$$\phi((1 + y_\lambda^i) \bmod q^2) = (1 + x^i) \bmod q$$

and $1 + y_\lambda^i \equiv 1 + y_\mu^i \bmod q^2$ if and only if $\lambda \equiv \mu \bmod q$. Thus $R(q^2)$ contains every element of $G(q^2)$ which is mapped into $R(q)$ by ϕ. Hence $\#R(q^2) = q\#R(q)$ and $\psi R(q) \subset R(q^2)$. Since ψ is a monomorphism and $q > 2$, Lemmas 5 and 7 now give the result.

PROPOSITION 2. *Let $W(x) = 1 + x^i + x^{2i}$, where i is odd and not divisible by the odd prime q. Then there is a nontrivial character on $G(q^2)$ constant on $R(q^2)$ if and only if there is a nontrivial character on $G(q)$ constant on $R(q)$.*

Proof. For $q = 3$, it is easily seen that such characters exist both on $R(q)$ and on $R(q^2)$. Now suppose $q \geq 5$. It is enough to show that if χ is a nontrivial character on $G(q^2)$ taking a constant value a on $R(q^2)$, then $\chi \circ \psi$ is a nontrivial character on $G(q)$ taking a constant value on $R(q)$. Putting $x = q-1$, we see that $1 \in R(q^2)$, so that $a = \chi(1) = 1$. Now let x be such that $x \bmod q \neq 0$, and put $y_\lambda = x + \lambda q$ for $\lambda = 0, 1, \ldots, q-1$. Clearly, $W(y_\lambda) \equiv W(y_\mu) \bmod q^2$ if and only if

$$(\lambda - \mu) i x^{i-1}(1 + 2x^i) \equiv 0 \bmod q.$$

If x is such that $1 + 2x^i \bmod q \neq 0$, it follows that q distinct elements of $R(q^2)$ are mapped onto $W(x) \bmod q$ by ϕ. On the other hand, if x is such that $1+2x^i \bmod q = 0$, then exactly one element of $R(q^2)$ is mapped onto $W(x) \bmod q$ by ϕ. Note that in this case $W(x) \bmod q$ is uniquely determined. Thus, provided $R(q)$ has at least two elements, we can conclude that $\#R(q^2) > \#R(q)$. But q is a prime greater than 3, and $1 \in R(q)$, $3 \in R(q)$. Lemma 6 now shows that $\chi \circ \phi$ is nontrivial. Now let $z \bmod q$ be any element of $R(q)$, so that $z = W(x) \bmod q$ for suitable $x \in \mathbf{Z}$. Then $z \bmod q^2 \in R(q^2)$, and

$$\chi(\phi(z \bmod q)) = \chi(z^q \bmod q^2) = (\chi(z \bmod q^2))^q = 1^q = 1.$$

Thus $\chi \circ \phi$ is constant on $R(q)$, and the proposition is proved.

PROPOSITION 3. *Let i be odd, and let q be a prime greater than 3, and let $W(x)$ be either $1+x^i$ or $1+x^i+x^{2i}$. Suppose that there is a nontrivial character on $G(q)$ which is constant on $R(q)$. Then $(i, q-1) \neq 1$.*

Proof. Suppose that $(i, q-1) = 1$. Then $x \to x^i$ is an automorphism of $G(q)$.

For $W(x) = 1 + x^i$ we have $R(q) = \{2, 3, \ldots, q-1\}$ and the only character constant on this set is trivial, so that the proposition holds in this case.

For $W(x) = 1 + x^i + x^{2i} = (x^i + \alpha)^2 + \beta$, where α and β are calculated in the finite field $\mathbf{Z}_q$, we have $1 = W(-1) \in R(q)$, so that there will only be a nontrivial character constant on $R(q)$ if $R(q)$ generates a proper subgroup of $G(q)$. As x^i runs through all the nonzero elements of $\mathbf{Z}_q$, $x^i + \alpha$ runs through all except α (but including 0 and $-\alpha$), so that $(x^i + \alpha)^2$ runs through all the quadratic residues, and also takes the value 0. Thus $(x^i + \alpha)^2 + \beta$ takes $(q-1)/2$ values in $G(q)$ if $-\beta$ is a quadratic residue, and $(q+1)/2$ values otherwise. If $R(q)$ generates a proper subgroup of $G(q)$, this can only be the subgroup of order $(q-1)/2$, that is, the group of quadratic residues. Thus, for every quadratic residue r^2, $r^2 + \beta$ is also a quadratic residue. It follows that every element of $G(q)$ is a quadratic residue. This contradiction completes the proof of the proposition.

4. Results. With the help of Propositions 1, 2 and 3, the algorithm of Section 2 can be simplified as follows.

For an odd integer $i > 1$, let H_1 (respectively, H_2) be the set consisting of the primes p of the form $1 + \lambda r$ (where r is a nontrivial divisor of i and λ is an integer) for which $p < (i+1)^2$ (respectively, $p < (2i+1)^2$), together with the prime divisors of i and their squares.

Let

$$I_1 = H_1 \cup \{p^2 : p \in H_1 \text{ is prime and there exists } q \in H_1 \text{ with } q \equiv 1 \pmod p\}$$

and let

$$I_2 = H_2 \cup \{p^2 : p \in H_2 \text{ is prime and there exists } q \in H_2 \text{ with } q \equiv 1 \pmod p\} \cup \{2, 4, 8\}.$$

As before, let J_1 be the subset of I_1 consisting of those elements m for which there is a nontrivial character modulo m constant on the set $R(m)$ of values of the polynomial $1+x^i$, and let J_2 be calculated similarly from I_2 using $1+x^i+x^{2i}$. The sets K_1 and K_2 consist of the products r (say) of elements of J_1 and J_2, respectively, with no repeated factor, for which $\Lambda_1(r) \neq G(r)$ (respectively, $\Lambda_2(r) \neq G(r)$), but omitting from K_1 and K_2 any r which is strictly divisible by another element already known to lie in K_1 or K_2, respectively. It follows from the results of Section 3 that, with K_1 and K_2 found from these smaller sets I_1 and I_2, σ_i fails to have WUD (mod n) if and only if n is odd and divisible by an element of K_1 or n is even and divisible by an element of K_2.

The results tabulated below include the cases $i = 1$, due to Sliwa [6] and $i = 3$ due to Narkiewicz [2].

Table of Results

The notation is as in Section 2. σ_i has WUD (mod n) if and only if n is odd and not divisible by an element of K_1 or n is even and not divisible by any element of K_2.

i	K_1	K_2
1	–	6
3	7	6
5	33	6 22
7	–	6
9	7 57	6 146
11	23	6 46
13	–	6
15	7 31 33	6 22 122 302
17	–	6
19	–	6
21	7 43	6
23	47	6 94
25	33	6 22
27	7 57 109	6 146
29	177	6 118
31	–	6
33	7 23 201	6 46 134
35	33 71	6 22 142
37	–	6
39	7 79 157	6 1874
41	249	6 166
43	–	6 2066
45	7 31 33 57 209	6 22 122 146 302
47	–	6
49	–	6
51	7 103 307	6 206 614
53	321	6 214
55	23 33	6 22 46
57	7 229	6
59	–	6

61	–	6
63	7 43 57 127	6 146
65	33 393 1441	6 22 262
67	–	6
69	7 47 277 417	6 94
71	–	6
73	–	6
75	7 31 33 151	6 22 122 302 1202 2402
77	23	6 46
79	–	6
81	7 57 109 489 3097	6 146
83	167	6 334
85	33	6 22 3742
87	7 177	6 118
89	537	6 358
91	–	6
93	7	6
95	33 191	6 22 382
97	–	6
99	7 23 57 199 201 397 1273	6 46 134 146
101	–	6
103	–	6
105	7 31 33 43 71 633 2321	6 22 122 142 302
107	–	6
109	–	6
111	7 223	6
113	681	6 454
115	33 47	6 22 94
117	7 57 79 157	6 146 1874
119	239	6 478
121	23	6 46
123	7 249	6 166
125	33 251	6 22 502
127	–	6
129	7	6 2066
131	263	6 526
133	–	6
135	7 31 33 57 109 209 271	6 22 122 146 302 542
137	–	6
139	–	6
141	7 283	6
143	23	6 46
145	33 177 649	6 22 118
147	7 43	6
149	–	6
151	–	6
153	7 57 103 307 919	6 146 206 614 1226 1838 7346
155	33 311	6 22 622
157	–	6
159	7 321	6 214

(continues)

(continued)

161	47	6 94
163	–	6
165	7 23 31 33 201 331 737	6 22 46 122 134 302 1322
167	–	6
169	–	6
171	7 57 229	6 146
173	1041	6 694
175	33 71	6 22 142
177	7	6
179	359	6 718
181	–	6
183	7 367 733	6 734
185	33	6 22
187	23	6 46
189	7 43 57 109 127 1137 7201	6 146 1514
191	383	6 766
193	–	6
195	7 31 33 79 157 393 1441	6 22 122 262 302 1874
197	–	6
199	–	6

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

1. O. M. FOMENKO, "The distribution of values of multiplicative functions with respect to a prime modulus," *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov.* (LOMI), v. 93, 1980, pp. 218–224. (Russian)

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

3. W. NARKIEWICZ, "Euler's function and the sum of divisors," *J. Reine Angew. Math.*, v. 323, 1981, pp. 200–212.

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

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

6. J. SLIWA, "On distribution of values of $\sigma(n)$ in residue classes," *Colloq. Math.*, v. 28, 1973, pp. 283–291.