ACTA ARITHMETICA
XXVI (1974)

Some further results concerning (j, ε)-normality in the rationals

by

R. G. STONEHAM (New York, N. Y.)

1. Introduction. In this paper, we present a significant improvement in our fundamental theorem on the existence of residue progressions in the rational fractions $Z/m < 1$ in lowest terms which we proved in [5, Th. 4, p. 227]. One essential difference between the new result presented here and the original theorem is that they agree if m in Z/m is an odd integer but differ if m is even.

For broad classes of rational fractions Z/m, the existence of residue progressions is fundamental in establishing the uniform ε-distribution of fractional parts $\{Zg^i/m\}$ for $i = 0, 1, \ldots, \mathrm{ord}_m g - 1 = \omega(m) - 1$ on $[0, 1]$ which is a necessary and sufficient condition for (j, ε)-normality [5, Th. 2, p. 224]. Based on this phenomenon of (j, ε)-normality in the rationals, we found it possible to construct transcendental non-Liouville normal numbers [6] from any given rational fraction.

By means of the improved theorem which we present in this paper concerning residue progressions, we can show that there does exist broad classes of rational fractions of Type B [5, def., p. 229] which *do possess* residue progressions. This statement is an amendment to our statement in [5, p. 229, below def.] wherein we said that residue progressions "do not exist for Type B". We can prove (j, ε)-normality by other means for the Type B, nth power residue case mod p for appropriate bases g or Z/p where p is an odd prime and the base of expansion is a primitive root. We, therefore, present as well the uniform ε-distribution of fractional parts and (j, ε)-normality for this new class of Type B rational fractions.

Furthermore, in this paper, we give a precise definition and a useful factorization for the much used $\omega(m) = \mathrm{ord}_m g$ where m is any positive integer. This factorization leads to a number of improvements in notation and methods of proof as well as giving precise factorizations for $\omega(m)$, D, and $\omega(D)$ which constitute the fundamental parameters in all residue progressions. These are stated in Definition 3.

Since the classification of all rational fractions Z/m into Types A, B, and C is essentially dependent only on the type of positive integer m in the denominator, we also set down the notion here that we may equivalently partition all positive integers m into Types A, B, and C and use this classification and description interchangeably. Thus, we can say here that we have shown that there exists a new even Type B positive integer m which possesses residue progressions. The odd Type B do not possess residue progressions as stated in [5, p. 229].

Finally, we present the theorem on residue progressions for Type C, i.e. $Z/m = Z/2^n$ which we promised in [5, p. 231, above Th. 5], and as well, the consequent uniform ε-distribution and (j, ε)-normality for this type.

2. Definitions and residue progressions. The period of the sequence of power residues in $Zg^x \equiv R_x \bmod m$ is given by $\mathrm{ord}_m g = \omega(m)$ where $m = 2^n \prod_{i=1}^{r} p_i^{n_i}$ with odd primes p_i, $n_i \geqslant 0$, $n \geqslant 0$, and any base g such that $(g, m) = 1$ with $2 \leqslant g < m$. Briefly, $\omega(m)$ is the exponent to which g belongs mod m, i.e. the least positive exponent such that $g^{\omega(m)} \equiv 1 \bmod m$ for any g such that $(g, m) = 1$. The universal exponent $\lambda(m)$ [4, pp. 53–54] has often been used in random number generator studies [2, p. 105] to determine the conditions for so-called "maximal" periods. However, the definition of say $\lambda(p^a)$ where p is an odd prime restricts the choice of g to a primitive root mod p^2 in the range $2 \leqslant g < m$, i.e. $\lambda(p^a) = \varphi(p^a) = (p-1)p^{a-1}$ where $\varphi(x)$ denotes the Euler φ-function of x. We shall state a completely general definition for any composite m and any g contained in $2 \leqslant g < m$ such that $(g, m) = 1$. Therefore, since for arbitrary g, $\omega(p^a) = \mathrm{ord}_{p^a} g = dp^{a-z}$ if $a > z$, and $\omega(p^a) = d$ if $a \leqslant z$ where $p^z \mid (g^d - 1)$ but $p^{z+1} \nmid (g^d - 1)$ (subsequently, we will denote such a statement by $p^z \| (g^d - 1)$). Therefore, we have $\omega(p^a) \mid \lambda(p^a)$ or $\omega(p^a) \leqslant \lambda(p^a)$ since $a - z \leqslant a - 1$ and $d \mid (p-1)$ for arbitrary $g \in 2 \leqslant g < m$. Also, $\lambda(2^a)$ is defined for those particular g such that $\lambda(2^a) = 2^{a-2}$ if $a \geqslant 3$. Since, in general, we may have [3, Th. 7–11] exponents to which g belongs mod 2^a for $a \geqslant 3$ such that $\omega(2^a) = 2^{a-s} \mid \lambda(2^a)$ for $s = 2, 3, \ldots, a-1$ for $g \equiv \pm 1 \bmod 2^s$, we may show without particular difficulty the computationally convenient result $\omega(2^a) = 2^{a-s}$ for $a > 3$ where $2^s \| (g - (-1)^t)$ with $t = (g-1)/2$. Therefore, in general for any odd $g \in 2 \leqslant g < m$, we have $\omega(2^a) \leqslant \lambda(2^a) = \varphi(2^a)/2 = 2^{a-2}$ for $a \geqslant 3$. Hence, we have for any g such that $(g, m) = 1$, the following definition:

Definition 1. Let $\omega(m) = \mathrm{ord}_m g$ be defined as follows:

$$
(2.0)\qquad
\begin{aligned}
\omega(1) &= 1,\\
\omega(2) &= 1, \text{ for odd } g,\\
\omega(2^2) &= 1, \text{ if } g \equiv 1 \bmod 4;\ \ \omega(2^2) = 2, \text{ if } g \equiv 3 \bmod 4,\\
\omega(2^n) &= 2^{n-s} \text{ for } (g, 2) = 1, \text{ if } n = 3,\ s = 2;\\
&\qquad \text{if } n > 3, \text{ then } s = 2, 3, \ldots, n-1\\
&\qquad \text{where } 2^s \| (g - (-1)^t) \text{ with } t = (g-1)/2;\\
&\qquad \text{if } g = 2^n - 1, \text{ then } s = n-1,\\
\omega(p^n) &= dp^{n-z}, p \text{ an odd prime, } d = \mathrm{ord}_p g,\\
&\qquad n > z \geqslant 1, (g, p) = 1,\\
&= d, \text{ if } n \leqslant z \text{ where } p^z \| (g^d - 1) \text{ with } d \mid (p-1),\\
\omega\Big(2^n \prod_{i=1}^{r} p_i^{n_i}\Big) &= \langle \omega(2^n), \omega(p_1^{n_1}), \ldots, \omega(p_r^{n_r}) \rangle \text{ where}\\
&\qquad p_1 < p_2 < \ldots < p_r \text{ are } r \text{ distinct odd primes.}
\end{aligned}
$$

In the notation $a^b \| d_i$ for $i = 1, 2, \ldots, r$; let b denote the maximum power of a which divides any one of $d_1, d_2, \ldots, d_r$. Thus, in $p_i^{s_i} \| d_{i+k}$ for $k = 1, 2, \ldots, r-i$; s_i will denote the maximum power of p_i which divides any $d_{i+1}, d_{i+2}, \ldots, d_r$ for a fixed i.

A more convenient evaluation of $\omega(m) = \langle \omega(2^n), \ldots \omega(p_i^{n_i}), \ldots \rangle = \langle 2^{n-s}, \ldots, d_i p_i^{n_i - z_i} \text{ or } d_i, \ldots \rangle$ can be obtained as follows: we separate the even and odd m, and therefore, if m is odd, we have

$$
(2.1)\qquad \omega(m) = 2^M \prod_{(i)} p_i^{\max(s_i,\, n_i - z_i)} \prod_{(k)} q_k^{r_k}
$$

where $2^M \| d_i$ for $i = 1, 2, \ldots, r$ and the s_i are defined so that $p_i^{s_i} \| d_{i+k}$ for $k = 1, 2, \ldots, r-i$ and some fixed $i = 1, 2, \ldots, r-1$. We also define $q_k^{r_k} \| d_i$ with $r_k \geqslant 0$ as those odd primes $q_k \neq p_i < p_r$ which could occur in the d_i. If m is even, then for $n > 0$

$$
(2.2)\qquad \omega(m) = \max(\omega(2^n),\ 2^M) \prod_{(i)} p_i^{\max(s_i,\, n_i - z_i)} \prod_{(k)} q_k^{r_k}.
$$

The forms in (2.1) and (2.2) have a further simplification. For a given set of odd primes $p_i \in m$, note that the M, s_i, and z_i are fixed for a given m and choice of $g \in 2 \leqslant g < m$. Therefore, the given powers n_i of the p_i in m distinguish 2 types of odd primes in $p_1 < p_2 < \ldots < p_r$, i.e. those p_j such that $n_j > z_j + s_j$ and those remaining p_i for $i \neq j$ such that $n_i \leqslant z_i + s_i$. Making these assumptions, we have the convenient result in

Definition 2. *A factorization of* $\omega(m) = \mathrm{ord}_m g$.

I. If m is odd such that $m = \prod_{(j)} p_j^{n_j} \prod_{(i \neq j)} p_i^{n_i}$ where $n_j \geqslant 1$ and $n_i \geqslant 1$, then

$$
(2.3)\qquad \omega(m) = 2^M \prod_{(j)} p_j^{n_j - z_j} \prod_{(i \neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k}
$$

where $2^M \| d_i = \omega(p_i)$ with $M \geq 0$, $p_i^{z_i} \| (g^{d_i}-1)$ for $i = 1, 2, \ldots, r$ with $z_i \geq 1$, $p_i^{s_i} \| d_{i+k}$ for $k = 1, 2, \ldots, r-i$ with $s_i \geq 0$ for some fixed i in the ordered sequence $p_1 < p_2 \ldots < p_r$, $\prod_{(k)} q_k^{r_k}$ with $r_k \geq 0$ contains those odd primes $q_k \neq p_i < p_r$ such that $q_k^{r_k} \| d_i$ for any $i = 1, 2, \ldots, r$; the p_j are those odd primes in m such that $n_j > z_j + s_j$ and the remaining p_i in m for $i \neq j$ are such that $n_i \leq z_i + s_i$.

II. If m is even such that $m = 2^n \prod_{(j)} p_j^{n_j} \prod_{(i \neq j)} p_i^{n_i}$ with $n > 0$, then

$$\omega(m) = \max\big(\omega(2^n), 2^M\big) \prod_{(j)} p_j^{n_j - z_j} \prod_{(i \neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k}. \tag{2.4}$$

It is clear from the above definition that the powers n_i of some given fixed set of odd primes p_i can be taken sufficiently large so that $n_i > z_i + s_i$ for all $i = 1, 2, \ldots, r$. In this case, the value of $\omega(m)$ is particularly simple. In [7, p. 328], we defined the notion of a "complete" rational fraction, i.e. some $Z/m < 1$ in lowest terms such that $n_i > z_i + s_i$ for *all* p_i in m. On the basis of this assumption, we proved in [7] the existence of what we called "absolute (j, ε)-normality" in the rational fractions. Essentially what this amounts to is to show that there are rational fractions which are (j, ε)-normal in a bounded consecutive set of positive integers. This apparently is the analog in the rationals for Borel's existential result that almost all real numbers are absolutely normal, i.e. normal in every positive integer base with the exceptional set of measure zero.

Let us point out here that subsequently we may not only speak of the rational fractions $Z/m < 1$ in lowest terms as being of Type A, B, or C as in [5, p. 229] which characterizes the conditions under which power residue progressions exist or not in the congruence $Zg^x \equiv R_x \bmod m$, but we can also refer to these conditions as defining a partition of the class of all positive integers into 3 Types A, B, or C. There would now be 2 kinds of Type A positive integers, complete or incomplete in their prime (odd) decomposition according as $n_i > z_i + s_i$ for *all* i or $n_i > z_i + s_i$ for *at least one* p_i, but not all, respectively. In essence, it is Type A, B or C positive integers m which can lead to residue progressions or not in $Zg^x \equiv R_x \bmod m$ for $x = 0, 1, \ldots, \omega(m)-1$ as prescribed by [5, p. 229]. Types A, B, and C always have residue progressions under suitable conditions [see (2.17) of this paper]. We also have the exceptional case for $m = p$, Type B, [see 5, bottom p. 229 and 230, also top p. 231]. Therefore, we will speak, interchangeably, of rational fractions Z/m or their denominators as being of Type A (complete or incomplete), B, and C. In some results we will present at another time, it turns out that the notion of complete or incomplete Type A is significant for some useful identities envolving $\omega(m)$ and associated trigonometric sums.

The following theorem on residue progressions is an improved form of [5, p. 227, Th. 4]. Basically, there is no difference between the theorem below and [5, p. 227, Th. 4] if m is odd, i.e. $n = 0$, in the definition of the quantity D; but, if m is even, then the value of D given below must be used. The theorem also shows a new class of Type B for which residue progressions exist that has not been noted before.

THEOREM 1. *Let* $m = 2^n \prod_{i=1}^{r} p_i^{n_i}$ *where* $n \geq 0$, $r \geq 1$, $n_i \geq 1$, *and the* p_i *are distinct odd primes* $p_1 < p_2 < \ldots < p_r$. *Let* $d_i = \operatorname{ord}_{p_i} g = \omega(p_i)$ *for each* i *where* $p_i^{z_i} \| (g^{d_i}-1)$ *with* $z_i \geq 1$, $p_i^{s_i} \| (d_{i+1}, d_{i+2}, \ldots, d_r)$ *for* $1 \leq i \leq r-1$, *and* $q_k^{r_k} \| d_i$ *where the* q_k *are those odd primes* $q_k \neq p_i < p_r$.

If $\omega(2^n) = 2^{n-s}$ *where* $n \geq 3$, $2 \leq s \leq n-1$; $2^M \| d_i$ *for* $i = 1, 2, \ldots, r$ *where* $M \geq 0$, $t_i = \min(z_i + s_i, n_i)$, *and for* $n \geq 0$ *with* g *such that* $(g, m) = 1$, $2 \leq g < m$; *we set*

Case 1: $(m$-*odd*$)$, *for* $M \geq 0$, $n = 0$, $D = \prod_{(i)} p_i^{t_i}$;

Case 2: $(m$-*even*$)$, *for* $M = 0$, $n = 1$, *any odd* g, $D = 2^1 \prod_{(i)} p_i^{t_i}$,

$$\text{for } n = 2: \begin{cases} x = 1 \ \text{ if } g \equiv 3 \bmod 4 \\ x = 2 \ \text{ if } g \equiv 1 \bmod 4 \end{cases} \text{ in } D = 2^x \prod_{(i)} p_i^{t_i};$$

Case 3: *for* $M = 1$, $n = 1$ *or* 2, *any odd* g, $D = 2^n \prod_{(i)} p_i^{t_i}$;

Case 4: *for* $M \geq 0$, $n \geq 3$, *any odd* g, $D = 2^{\min(s+M,\, n)} \prod_{(i)} p_i^{t_i}$,

then the complete set of $\omega(m)$ *power residues* $R_j \equiv Zg^j \bmod m$ *where* $(Z, m) = 1$ *and* $2 \leq g < m$ *can be partitioned into* $\omega(D)$ *disjoint arithmetic progressions* P_e *each containing* $\omega(m)/\omega(D) = m/D$ *elements of the form* $r_e + KD$ *where* $Z' \equiv r_e \bmod D$, $Z \equiv Z' \bmod D$ *for* $e = 0, 1, \ldots, \omega(D)-1$ *and* $K = 0, 1, \ldots, \omega(m)/\omega(D) - 1 = m/D - 1$.

Proof. We will prove Theorem 1 in a new way compared to the proof of the original result given in [5, p. 227]. In fact, the approach reveals some new features related to the existence of residue progressions and refines the result in [5, Th. 4, p. 227]. If m is odd, then from (2.3) and choosing $D = \prod_{(j)} p_j^{z_j+s_j} \prod_{(i \neq j)} p_i^{n_i}$ where we have used $D = \prod_{(i)} p_i^{t_i}$ with $t_i = \min(z_i + s_i, n_i)$ stated according to the assumptions concerning the odd primes in m below (2.2), we obtain

$$\frac{m}{D} = \frac{\prod_{(j)} p_j^{n_j} \prod_{(i \neq j)} p_i^{n_i}}{\prod_{(j)} p_j^{z_j+s_j} \prod_{(i \neq j)} p_i^{n_i}} = \prod_{(j)} p_j^{n_j-(z_j+s_j)} \tag{2.5}$$

and

$$\frac{\omega(m)}{\omega(D)} = \frac{2^M \prod_{(j)} p_j^{n_j-z_j} \prod_{(i \neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k}}{2^M \prod_{(j)} p_j^{s_j} \prod_{(i \neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k}} = \prod_{(j)} p_j^{n_j-(z_j+s_j)}. \tag{2.6}$$

Clearly, according to the character of those p_j, i.e. $n_j > z_j + s_j$, we see that D is the least divisor of m such that $m/D = \omega(m)/\omega(D)$ [5, p. 228, (3.4)]. Also shown in (2.5) and (2.6) is the basic requirement for the existence of residue progressions for odd m, i.e. $m/D = \prod_{(j)} p_j^{n_j-(z_j+s_j)} > 1$ which is assured if at least one odd prime in m is such that $n_j > z_j + s_j$ (these are the odd primes belonging to the "j-class" we defined above). We may paraphrase and say that (2.5) and (2.6) show that the number of residues mod m which lie in these $\omega(D)$ residue classes mod D is demonstrated by the fact that $m\omega(D)/D = \omega(m)$ [5, pp. 227–228, (3.2)–(3.4)].

If m is even, i.e. $n > 0$, the situation is more complex. Let us define $D = 2^x \prod_{(i)} p_i^{t_i}$ and seek the least value of x using (2.4) such that $D|m$ and $m/D = \omega(m)/\omega(D)$. Using (2.4) and this assumption, leads to

$$\frac{m}{D} = 2^{n-x} \prod_{(j)} p_j^{n_j-(z_j+s_j)} = \frac{\max(\omega(2^n), 2^M)}{\max(\omega(2^x), 2^M)} \prod_{(j)} p_j^{n_j-(z_j+s_j)} \tag{2.7}$$

which defines the crucial relation

$$2^{n-x} = \max(\omega(2^n), 2^M)/\max(\omega(2^x), 2^M) \tag{2.8}$$

from which we seek the least positive integer solution x for some fixed choice of $n \geq 1$, i.e. even m.

A detailed analysis of (2.8) for the cases listed above for $n = 1, 2$, $n \geq 3$ with $M = 0$, $M \geq 1$ leads to the various stated results. For example, in the more frequent case 4 (m-even) for which, we take $n \geq 3 \Rightarrow 2 \leq s \leq n-1$ according to Definition 1 (2.0) for $\omega(2^n)$, $M \geq 0$; (2.8) requires $2^{n-x} \geq 1$, hence $3 \leq x \leq n$ determines the possible range of x values.

In (2.8), we may now write under these assumptions

$$2^{n-x} = \max(2^{n-s}, 2^M)/\max(2^{x-s}, 2^M) \tag{2.9}$$

and in the denominator, let us set $2^{x-s} \geq 2^M$ or $x \geq s+M$ for $n \geq s+M$ which implies $2^{n-s} \geq 2^M$. Hence $\max(2^{n-s}, 2^M) = 2^{n-s}$ and $\max(2^{x-s}, 2^M) = 2^{x-s}$, thus (2.9) becomes $2^{n-x} = 2^{n-x}$ which means that (2.9) is satisfied for *any* $x \geq s+M$. Therefore, we choose the least x, i.e. $x = s+M$ where $D|m$ and thus (2.8) is satisfied if $x = s+M$ for $n \geq s+M$. Also, note that the restriction $3 \leq x = s+M \leq n$ is satisfied since the least possible value for $s+M = 2+0$ obtains for $s = 2$ and $M = 0$.

If $n < s+M$, then $x \leq n < s+M$ or $n-s < M$. Thus, $2^{x-s} < 2^M$, $2^{n-s} < 2^M$, and (2.9) gives $2^{n-x} = 2^M/2^M = 1$ which implies $x = n$ which is, therefore, the least solution for $n < s+M$. Hence stated succinctly, $x = \min(s+M, n)$ for case 4. We have, therefore, disposed of cases 1 and 4.

Cases 2 and 3 are obtained by a detailed analysis of (2.8), considering the possible values of $\omega(2^1)$ and $\omega(2^2)$ as stated in Definition 1 and their relation to 2^M for $M = 0$ or 1.

For example, consider case 2 for $n = 2$, $M = 0$, and the requirement that g be an odd number of the 2 possible types mod 4, $g \equiv 1 \bmod 4$ and $g \equiv 3 \bmod 4$. If $n = 2$ with possible $x = 1$ or 2, we have for $M = 0$, considering the 2 possible values for $\omega(2^2)$

$$\begin{aligned} 2^{2-x} &= \max(\omega(2^2), 1)/\max(\omega(2^x), 1) \\ &= 1/\max(\omega(2^x), 1) \text{ or } 2/\max(\omega(2^x), 1) \end{aligned} \tag{2.10}$$

for $g \equiv 1 \bmod 4$ or $g \equiv 3 \bmod 4$, respectively.

In the first instance, the relation is uniquely satisfied by $x = 2$, $g \equiv 1 \bmod 4$ and $x \neq 1$ since $\omega(2^2) = 1$. In the second, $x = 1$ for $g \equiv 3 \bmod 4$ and $x \neq 2$ since $\omega(2^2) = 2$ and $\omega(2) = 1$. One proceeds in the same way for the rest of cases 2 and 3. The proof of Theorem 1 is now complete.

Let us now assemble together for immediate and future reference, the 4 basic parameters $m, D, \omega(m)$, and $\omega(D)$ stated explicitly which completely determine the structure of the residue progressions for m odd and m even for $n \geq 3$. (We state the m even case for $n \geq 3$. Those for $n = 1$ or 2, etc. can easily be constructed if needed.) Furthermore, we list them for incomplete and complete positive integers m, respectively.

Definition 3. *The residue progression parameters. If m is odd* and incomplete or complete, resp., then assuming the quantities defined in Definition 2, we have based on Theorem 1

$$\begin{aligned} m &= \prod_{(j)} p_j^{n_j} \prod_{(i\neq j)} p_i^{n_i} \text{ or } \prod_{(i)} p_i^{n_i} \quad \text{for all } i, \text{ resp.,} \\ D &= \prod_{(j)} p_j^{z_j+s_j} \prod_{(i\neq j)} p_i^{n_i} \text{ or } \prod_{(i)} p_i^{z_i+s_i}, \\ \omega(m) &= 2^M \prod_{(j)} p_j^{n_j-z_j} \prod_{(i\neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k} \text{ or } 2^M \prod_{(i)} p_i^{n_i-z_i} \prod_{(k)} q_k^{r_k}, \\ \omega(D) &= 2^M \prod_{(j)} p_j^{s_j} \prod_{(i\neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k} \text{ or } 2^M \prod_{(i)} p_i^{s_i} \prod_{(k)} q_k^{r_k}. \end{aligned} \tag{2.11}$$

If *m is even* with $n \geq 3$ and complete or incomplete, resp., then

$$\begin{aligned} m &= 2^n \prod_{(j)} p_j^{n_j} \prod_{(i\neq j)} p_i^{n_i} \text{ or } 2^n \prod_{(i)} p_i^{n_i} \quad \text{for all } i, \text{ resp.,} \\ D &= 2^{\min(s+M, n)} \prod_{(j)} p_j^{z_j+s_j} \prod_{(i\neq j)} p_i^{n_i} \text{ or } 2^{\min(s+M, n)} \prod_{(i)} p_i^{z_i+s_i}, \\ \omega(m) &= 2^{\max(n-s, M)} \prod_{(j)} p_j^{n_j-z_j} \prod_{(i\neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k} \text{ or } 2^{\max(n-s, M)} \prod_{(i)} p_i^{n_i-z_i} \prod_{(k)} q_k^{r_k}, \\ \omega(D) &= 2^M \prod_{(j)} p_j^{s_j} \prod_{(i\neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k} \text{ or } 2^M \prod_{(i)} p_i^{s_i} \prod_{(k)} q_k^{r_k}. \end{aligned} \tag{2.12}$$

For the odd case, the parameters were stated in (2.5) and (2.6). For the even case, by construction using the stated m, D, and $\omega(m)$ and the fact that $\omega(D) = D\omega(m)/m$, we find that

$$\omega(D) = 2^{\min(s+M,n)+\max(n-s,M)-n} \prod_{(j)} p_j^{s_j} \prod_{(i\neq j)} p_i^{s_i} \prod_{(k)} q_k^{r_k}. \tag{2.13}$$

For the 2 alternatives $n \geqslant s+M$ and $n < s+M$, we have for $\omega(D)$ in (2.12)

$$\min(s+M, n)+\max(n-s, M)-n = M \tag{2.14}$$

for either alternative, i.e. if $n \geqslant s+M \Rightarrow s+M+n-s-n = M$ and $n < s+M \Rightarrow n+M-n = M$. The parameters for complete positive integers as stated are easily obtained when $n_i > z_i+s_i$ for *all* p_i in m. The requirements of Definition 3 are now complete.

In 1971, Dieter [2, pp. 105–106] stated something similar to the progressions in Theorem 1 appropriate to so-called "maximal" periods in a study of congruential random number generators using the universal exponent $\lambda(m)$ which, of course, restricts g to being a primitive root mod p^2 (for *every* odd prime in m) among other requirements for a so-called "primitive" element. However, as we have seen above, the result we gave in 1970 [5, p. 227, Th. 4] and Theorem 1 stated here applies to all $(g, m) = 1$. Also in Dieter [2, p. 105, (3.5)], we find $\lambda(m)/\lambda(f) = m/f$ which is the analog for $\omega(m)/\omega(D) = m/D$ found in [5, p. 228, (3.4)] where f is the least divisor of m.

This is a convenient place to emphasize again that our aim (or program) in the results we have been building since 1964 in [5–9] in relation to normal numbers is to determine those fundamental arithmetic properties with respect to the uniform ε-distribution of convergent sequences of rational approximations to a given irrational.

In this, it is clear, that we must have results of a quite general nature with respect to the base of expansion since the positive integers q_n which would appear in the denominators of p_n/q_n where $\lim_{n\to\infty} p_n/q_n = \theta$ with θ an algebraic or transcendental irrational will vary considerably for increasing n in their character (or "Types" A, B, C, etc. as we call them) with respect to the base of expansion g which would be fixed for each q_n such that $(g, q_n) \geqslant 1$.

For example in [7], we showed that the non-periodic parts which arise when $(g, m) \geqslant 1$ did not affect the normality of the construction [6, 7, 8] that we have studied in detail. In fact, we were lead to absolute (j, ε)-normality in the rationals by assuming that $(g, m) > 1$.

Therefore, we want as few restrictions on the base g with respect to m, as possible, and yet still have uniform ε-distributions.

From Definition 3 (or case 4 in Theorem 1), assuming $n > s+M$, we may obtain for incomplete positive even integers, the requirement for the existence of residue progressions

$$m/D = 2^{n-(s+M)} \prod_{(j)} p_j^{n_j-(z_j+s_j)} > 1. \tag{2.15}$$

Also, $m/D = \omega(m)/\omega(D)$ is the number of elements in each of the $\omega(D)$ residue progressions P_ε. The form in (2.15) reveals a number of conclusions. First, we can obtain $m/D > 1$ by having Type B [5, p. 229, Def.] where $n_i \leqslant z_i+s_i$ for *all* odd primes p_i in $m = 2^n \prod_{(i)} p_i^{n_i}$ since $\prod_{(j)} p_j^{n_j-(z_j+s_j)} = 0$ and, therefore, we can now have residue progressions by choosing n as large as we please in $m/D = 2^{n-(s+M)} > 1$ for $n > s+M$. Second, since s and M are fixed for a given set of p_i and g, we can make the number of elements m/D in each P_ε arbitrarily large by taking n sufficiently large. Third, if m is Type A, we could increase both n and n_j (the exponent of at least one odd prime in m), or fix n and increase n_j, or fix n_j and increase n, and thus, by any of these 3, again increase the number of elements in any P_ε.

Of most interest here is that Theorem 1 in the form of (2.15) shows that there exists a new Type B integer m which generates residue progressions. It appears we must revise the statement we made in [5, p. 229] that "residue progressions do not exist for Type B". As we said above for Type B, (2.15) becomes simply

$$m/D = 2^{n-(s+M)} > 1. \tag{2.16}$$

It is clear that this new result follows from our more precise value of D for the even m case. Before in [5, p. 228, (3.4)] for even m, we had $m/D = \prod_{(i)} p_i^{n_i-t_i}$ since we gave $D = 2^n \prod_{(i)} p_i^{t_i}$, and $t_i = \min(n_i, z_i+s_i)$. Therefore, if $n_i \leqslant z_i+s_i$ for Type B, we had $m/D = \prod_{(i)} p_i^{n_i-n_i} = 1$, i.e. no residue progressions.

These results also imply the uniform ε-distribution over a whole period and within the period according to our recent results in [8]; and, in consequence, (j, ε)-normality for Type B rational fractions $Z/m = Z/2^n \prod_{(i)} p_i^{n_i}$. It also follows that there are no odd Type B positive integers, in general, that have residue progressions since $m/D = 1$, other than the exceptional case we noted in [5, p. 229, bottom] where p is an odd prime in Z/p and g is a primitive root mod p^2 and the complete periodic set can be re-arranged into a sequence whose elements differ by one (see also, Type B(a), below).

However, the difficulty in proving the uniform ε-distribution of normalized residues r_i/m for the odd Type B discussed in [5, p. 230, at top] still remains.

Let us gather together our present knowledge of the types of positive integers m which produce residue progressions in $Zg^i \equiv r_i \bmod m$. In Type B, we have some unpublished results concering nth power residues [see 5, p. 230] for $d = (p-1)/n$ where $n > 1$.

Definition 4. *Existence of residue progressions.* Residue progressions for the complete periodic sets of power residues in $Zg^i \equiv r_i \bmod m$ exist for the following positive integers m using those g such that $(g, m) = 1$, $2 \leqslant g < m$, and $(Z, m) = 1$:

1. *Type* A. m (even or odd) $= 2^n \prod_{(i)} p_i^{n_i}$, $n \geqslant 0$, complete or incomplete, i.e. $n_i > z_i + s_i$ for all i, or at least one, resp.

(2.17) 2. *Type* B. (a) $m = p$, $p \| (g^{p-1}-1)$ where g is a primitive root $\bmod p^2$,

(b) m(even) $= 2^n \prod_{(i)} p_i^{n_i}$, $n > s+M \geqslant 2$, $n_i \leqslant z_i + s_i$ for all i.

3. *Type* C. $m = 2^n$, for $n \geqslant 4$, and any odd g.

In the next section, we will present the theorem on Type C which we promised in [5, p. 231]. (This result for Type C was stated in an unpublished ms. of 1964 communicated to D. A. Burgess.)

3. (j, ε)-normality for Types A, B, and C. First, let us present the new result for Type B.

If we follow the proof of [5, Th. 5, p. 231] and we introduce the D for Type B based on Def. 3 (2.12) as well as (2.16) for $m/D = \omega(m)/\omega(D)$, then we have demonstrated

Theorem 2. *In the rational fraction $Z/m = Z/2^n \prod_{(i)} p_i^{n_i}$ of Type* B *where $n_i \leqslant z_i + s_i$ for all i, let s be defined by $\omega(2^n) = 2^{n-s}$ for $n \geqslant 3$, $2^M \| d_i$ for all i, and choose $n > s+M \geqslant 2$, then the fractional parts $\{Zg^i/m\}$ for $i = 0, 1, \ldots, \omega(m)-1 = 2^{n-s} \prod_{(i)} p_i^{s_i} \prod_{(k)} q_k^{r_k} - 1$ have a uniform ε-distribution for all bases g such that $(g, m) = 1$, $2 \leqslant g < 1/\delta$ where $\varepsilon = \delta = \omega(D)/\omega(m) = D/m = 1/2^{n-(s+M)}$, $D = 2^{s+M} \prod_{(i)} p_i^{n_i}$, and $\omega(D) = 2^M \prod_{(i)} p_i^{s_i} \prod_{(k)} q_k^{r_k}$.*

Therefore, using [5, Th. 2, p. 224] and Theorem 2 (above), we have (j, ε)-normality over a full period $\omega(m)$ for this even Type B. Assuming the definitions of the quantities s and M as given in Theorem 2, and essentially paraphrasing [5, Th. 6, p. 233] we have established

Theorem 3. *A rational fraction $Z/m = Z/2^n \prod_{(i)} p_i^{n_i} < 1$ in lowest terms of the even Type* B *for $n > s+M \geqslant 2$ is (j, ε)-normal in all bases g such that*

$$(g, m) = 1, \quad 2 \leqslant g < m/D = 2^{n-(s+M)} = 1/\varepsilon \textit{ for all } j \leqslant [\log_g 2^{n-(s+M)}]$$

where

$$\varepsilon = D/m = 1/2^{n-(s+M)}, \quad \omega(2^n) = 2^{n-s}, \quad \textit{and} \quad D = 2^{s+M} \prod_{(i)} p_i^{n_i}.$$

Implicit in Theorems 2 and 3 is the structure of the associated residue progressions for the even Type B. Since these were not explicitly stated, we do so in the following corollary:

Corollary to Theorem 2. *If $m = 2^n \prod_{(i)} p_i^{n_i}$ in $Zg^i \equiv r_i \bmod m$ where $n \geqslant 3$, $n_i \leqslant z_i + s_i$ for all i, and $n > s+M$, then we have $\omega(D) = 2^M \prod_{(i)} p_i^{s_i} \prod_{(k)} q_k^{r_k}$ residue progressions P_e each consisting of $\omega(m)/\omega(D) = 2^{n-(s+M)}$ elements of the form $r_e + KD = r_e + K \cdot 2^{s+M} \prod_{(i)} p_i^{n_i}$ where $Z \equiv Z' \bmod D$, $Z'g^e \equiv r_e \bmod D$, and $K = 0, 1, \ldots, 2^{n-(s+M)}-1$.*

For Type C, i.e. $Z/m = Z/2^n < 1$ in lowest terms, we prove the following theorem concerning the associated residue progressions. The residue progressions lead to the uniform ε-distribution of fractional parts $\{Zg^i/2^n\}$ for $i = 0, 1, \ldots, \omega(2^n)-1$ which, consequently, establishes the (j, ε)-normality of $Z/2^n$ under suitable conditions using [5, Th. 2, p. 224].

Theorem 4. *Type* C. *If $Z/m = Z/2^n < 1$ in lowest terms where $n \geqslant 4$ and g is any odd number contained in $2 < g < 2^n$ such that $g \neq (2^{n-1} \pm 1)$ or $2^n - 1$, then the complete set of power residues in $Zg^i \equiv r_i \bmod 2^n$ with $(Z, 2) = 1$ are such that in*

Case 1: *if $2^s \| (g+1)$ for $2 \leqslant s \leqslant n-2$, then we have 2 residue progressions consisting of elements $r_e + K \cdot 2^{s+1}$ where $Z \equiv Z' \bmod 2^{s+1}$, $D = 2^{s+1}$, $Z'g^e \equiv r_e \bmod 2^{s+1}$ for $e = 0, 1$; $K = 0, 1, \ldots, 2^{n-(s+1)}-1$, and in*

Case 2: *if $2^s \| (g-1)$ for $2 \leqslant s \leqslant n-2$, then we have one residue progression consisting of 2^{n-s} elements $r_e + K \cdot 2^s$ where $K = 0, 1, \ldots, 2^{n-s}-1$ and $Z'g^e \equiv r_e \bmod 2^s$.*

Proof. Consider the definition of $\omega(2^n)$ found in (2.0). All the $2^{n-1}-1$ odd g contained in $2 < g < 2^n$ can be partitioned into 2 kinds of $g = 2^s r \pm 1$ where $(r, 2) = 1$, i.e. $2^s \| (g-1)$ in case 2 and $2^s \| (g+1)$ in case 1, resp. where $2 \leqslant s \leqslant n-1$. For case 2, we have $\omega(2^s) = 1$ since $g^1 \equiv 1 \bmod 2^s$ for $g = 2^s r + 1$, and for case 1, $g^2 \equiv 1 \bmod 2^{s+1}$, i.e. $\omega(2^{s+1}) = 2$ for $g = 2^s r - 1$. For all such g, we have the usual $\omega(2^n) = 2^{n-s}$ for $n \geqslant 4$ and $2 \leqslant s \leqslant n-1$ where $2 \leqslant \omega(2^n) \leqslant 2^{n-2}$. As in the demonstration for Theorem 1 starting at (2.7), we seek the least divisor of m such that $m/D = \omega(m)/\omega(D)$. In Theorem 4, we have for $D = 2^x$

$$m/D = 2^{n-x} = \omega(2^n)/\omega(2^x) = 2^{n-s}/\omega(2^x) \tag{3.0}$$

where we shall assume $n \geqslant 4$ and $\omega(2^n) = 2^{n-s}$ for which $2 \leqslant s \leqslant n-1$. Therefore, for the 2 kinds of g, we distinguish 2 values for $D = 2^x$, i.e. if $g = 2^s r + 1$ in case 2, $2^{n-x} = 2^{n-s}/1 \Rightarrow x = s$ or $D = 2^s$ and $g = 2^s r - 1$ in case $1 \Rightarrow 2^{n-x} = 2^{n-s}/2 \Rightarrow x = s+1$ or $D = 2^{s+1}$. Thus, in case 2, $\omega(D) = \omega(2^s) = 1$ which implies the existence of one residue progression with differences $D = 2^s$ and in case 1, $\omega(D) = (2^{s+1}) = 2$ which shows the existence of 2 residue progressions. (These values for D are minimal by implication.) In order that we are able to clearly recognize the progressions in the minimal cases, let us require that we have, either one set of 4 elements in progression, or 2 sets of 2 elements in progression, i.e. require the total number of elements $\omega(2^n)$ in the complete periodic set to be such that $\omega(2^n) \geqslant 2^2$. This can be done if we confine ourselves to those s such that $2 \leqslant s \leqslant n-2$, since the number of elements in one progression is $\omega(2^n)/\omega(D)$ or $2^{n-s}/2 > 1$, at most. Hence $2^{n-s} \geqslant 2^2 > 2$ which shows that $s \leqslant n-2$ will suffice. Therefore, as indicated in the theorem, we must remove those $g \in 2 < g < 2^n$ such that $s = n-1$, i.e. $g = 2^{n-1}-1, 2^{n-1}+1$, and $2^n - 1$ since $(2^{n-1} \pm 1)^2 \equiv 1 \bmod 2^n$ and $(2^n-1)^2 \equiv 1 \bmod 2^n$ implies that $\omega(2^n) = 2^{n-(n-1)} = 2$.

The other standard features of the residue progressions follow as well in Theorem 4, i.e. the values for r_e, Z', e, and K, etc. as in [5, Th. 4, p. 227] where in the present result for Type C, we distinguish the 2 values for D, i.e. $D = 2^s$ or 2^{s+1} according to the particular odd $g \in 2 < g < 2^n$. The proof of Theorem 4 is now complete.

Following the proof of [5, Th. 5, p. 231] and noting [5, Th. 6, p. 233], we see that the essential parameters in uniform ε-distributions and (j, ε)-normality theorems for any rational fraction $Z/m < 1$ in lowest terms are $\varepsilon = D/m = \omega(D)/\omega(m)$ for all g such that $2 \leqslant g < 1/\varepsilon = m/D$ and $j \leqslant [\log_g m/D]$. Therefore, we give the following theorem for Type C which combines both of these properties for $Z/2^n$.

THEOREM 5. *The rational fraction $Z/2^n < 1$ in lowest terms of Type* C *for $n \geqslant 5$ is such that the fractional parts $\{Zg^i/2^n\}$ for $i = 0, 1, \ldots, \omega(2^n)-1$ have a uniform ε-distribution on* $[0, 1]$ *and, consequently, is also (j, ε)-normal when represented in any odd number base g where in*

Case 1: *if $2^s \| (g+1)$ for any odd $g \in 2 < g < 2^{n-(s+1)}$, then $\varepsilon = 1/2^{n-(s+1)}$ with $j \leqslant [\log_g 2^{n-(s+1)}]$; and in*

Case 2: *if $2^s \| (g-1)$ for any odd $g \in 2 < g < 2^{n-s}$, then $\varepsilon = 1/2^{n-s}$ with $j \leqslant [\log_g 2^{n-s}]$.*

The only comment that we make about Theorem 5 is that in order for $2 < g < 2^{n-(s+1)}$ to contain at least one odd' g, we require that $n \geqslant 5$ since, minimally, $2^{n-(s+1)} = 2^{5-(2+1)} = 2^2$ for $s = 2$ in case 1, and this requirement also accomodates $2 < g < 2^{n-s} = 2^3$ for case 2. Q.E.D.

The new value of D stated in the residue progression Theorem 1 for the even modulus $m = 2^n \prod_{(i)} p_i^{n_i}$ of Type A not only leads to (j, ε)-normality for a new class of Type B as stated in Theorem 3 based on Theorem 2 but also has its effect on the uniform ε-distribution and (j, ε)-normality statements for Type A given in [5, Th. 5, p. 231; Th. 6, p. 233].

In the following theorem, we introduce Definition 3 for simplicity and combine the two fundamental properties for Type A, i.e. uniform ε-distribution and (j, ε)-normality as we did in Theorem 5 for Type C. We assume the definitions of z_i, s_i, s, M, etc. as stated in Theorem 1. We have

THEOREM 6. *The rational fraction $Z/m = Z/2^n \prod_{(i)} p_i^{n_i} < 1$ in lowest terms of Type* A *is such that the fractional parts $\{Zg^i/m\}$ for $i = 0, \ldots, \omega(m)-1$ have a uniform ε-distribution on* $[0, 1]$*; and, consequently, is (j, ε)-normal where in*

Case 1: *if m is odd, then*

$$\varepsilon = 1 \Big/ \prod_{(j)} p_j^{n_j-(z_j+s_j)} \quad \textit{for all } j \leqslant \Big[\log_g \prod_{(j)} p_j^{n_j-(z_j+s_j)}\Big]$$

where the g are such that $(g, m) = 1$ and $2 \leqslant g < \prod_{(j)} p_j^{n_j-(z_j+s_j)}$; and in

Case 2: *if m is even with $n \geqslant 3$ such that $n \geqslant s+M$, then*

$$\varepsilon = 1/2^{n-(s+M)} \prod_{(j)} p_j^{n_j-(z_j+s_j)} \quad \textit{for all } j \leqslant \Big[\log_g 2^{n-(s+M)} \prod_{(j)} p_j^{n_j-(z_j+s_j)}\Big]$$

where the g are such that $(g, m) = 1$ and $2 < g < 2^{n-(s+M)} \prod_{(j)} p_j^{n_j-(z_j+s_j)}$.

In case 1 above for odd m, the result is identical with our original statement in [5, Th. 6, p. 231]. Also note that in case 2, we can require $n \geqslant s+M$ since if Z/m is Type A, then there is surely at least one odd prime in m such that $n_j > z_j + s_j$ by definition. Therefore, we could permit $n = s+M$ for some s and M and still have a well defined ε and a bounded set of j values for (j, ε)-normality due to the presence of the factor $\prod_{(j)} p_j^{n_j-(z_j+s_j)}$. For the new even Type B integer $m = 2^n \prod_{(i)} p_i^{n_i}$, clearly we must require $n > s+M$ for uniform ε-distribution and (j, ε)-normality as stated in Theorem 4.

In [5, p. 230], we stated that we could prove the (j, ε)-normality for the Type B case of Z/p where $p \| (g^d - 1)$ with $d = (p-1)/n$ for $n \geqslant 1$ and appropriate g. In the near future, we will present these results which envolve character sums and other techniques. In addition, we will prove that certain representations of given irrationals like "$e-2$", $\sqrt{2}$, π, etc.

have representations which are Type A rational fractions. In particular, we show that the partial infinite product representation for $\pi/4$ with n sufficiently large is Type A and, consequently, we obtain results concerning the Brouwer conjecture that we discussed in [5, pp. 234–235].

References

[1] R. D. Carmichael, *The Theory of Numbers and Diophantine Analysis*, New York 1959.

[2] U. Dieter and J. Ahrens, *An exact determination of serial correlations of pseudo-random numbers*, Numer. Math. 17 (1971), pp. 101–123.

[3] H. Griffin, *Elementary Theory of Numbers*, New York 1954.

[4] W. J. LeVeque, *Topics in Number Theory*, Vol. I, Reading, Mass., 1956.

[5] R. G. Stoneham, *On (j, ε)-normality in the rational fractions*, Acta Arith. 16 (1970), pp. 221–237.

[6] — *A general arithmetic construction of transcendental non-Liouville normal numbers from rational fractions*, Acta Arith. 16 (1970), pp. 239–253.

[7] — *On absolute (j, ε)-normality in the rational fractions with applications to normal numbers*, Acta Arith. 22 (1973), pp. 277–286.

[8] — *On the uniform ε-distribution of residues within the periods of rational fractions with applications to normal numbers*, Acta Arith. 22 (1973), pp. 371–389.

[9] — *The reciprocals of integral powers of primes and normal numbers*, Proc. Amer. Math. Soc. 15 (1964), pp. 200–208.

THE CITY COLLEGE OF THE CITY UNIVERSITY OF NEW YORK

Received on 25. 5. 1973 (410)

ACTA ARITHMETICA
XXVI (1974)

Remark to a theorem of P. Erdös

by

P. Szüsz (Stony Brook, N.Y.)

Let $f(n)$ be a real-valued additive arithemtic function, that is,

$$f(nm) = f(n)+f(m) \quad \text{for} \quad (n, m) = 1.$$

Put

$$f^*(n) = \begin{cases} f(n) & \text{for} \quad |f(n)| \leqslant 1, \\ 0 & \text{for} \quad |f(n)| > 1. \end{cases}$$

A remarkable theorem of P. Erdös [1] states, that if

(1) $$\sum_p \frac{f^*(p)}{p} \text{ converges,}$$

(2) $$\sum_p \frac{f^*(p)^2}{p} < \infty$$

and

(3) $$\sum_{|f(p)|>1} \frac{1}{p} < \infty$$

then the distribution-function of $f(n)$ exists, that is, the limit

(4) $$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{k\leqslant N \\ f(k)\leqslant x}} 1 = G(x)$$

exists for every real x. Further he showed that if the additional condition

(5) $$\sum_{f(p)\neq 0} \frac{1}{p} = \infty$$

holds, then $G(x)$ is continuous; if

(6) $$\sum_{f(p)\neq 0} \frac{1}{p} < \infty$$

then $G(x)$ is a discrete distribution.