THE RECIPROCALS OF INTEGRAL POWERS OF PRIMES AND NORMAL NUMBERS

R. G. STONEHAM

1. Introduction. Numerical studies [1] indicate that the distribution of digits in the recurring period of the reciprocal of an integral power of an odd prime to a base which is a primitive root (of p^n) has properties analogous to that of a normal number. Consider the expansion of $1/p^n$ to a base g which is a primitive root mod p^2, then g is a primitive root mod p^n where p is any odd prime and n a positive integer [7, p. 69]. Let $N(B_j, E_n)$ denote the number of occurrences of any block B_j consisting of j digits chosen from the integers 0, 1, 2, $\cdots$, $g-1$ in the set of digits $\{E_n\}$, the recurring period of $1/p^n$, which contains $\lambda=(p-1)p^{n-1}$ digits. We find that the relative frequency of any block B_j is approximately $1/g^j$ for all block sizes $j=1, 2, \cdots, [n \log_g p]$ when the primitive root g is chosen so that $2 \leqq g < p^n$. Consider any sequence of reciprocals of a given fixed odd prime where the exponents in $1/p^{s_1}, 1/p^{s_2}, \cdots, 1/p^{s_n}, \cdots$ are any strictly monotonic increasing sequence of positive integers $s_1 < s_2 < \cdots < s_n < s_{n+1} \cdots$ and each reciprocal is expanded to the same base g which is a primitive root mod p^2. Under these conditions, a result we prove is that the sequence of relative frequencies of the counts of a given fixed block B_j of j digits for some fixed j evaluated successively over the sets of digits in the recurring periods $E_{s_1}, E_{s_2}, \cdots, E_{s_n}, \cdots$ in the reciprocals $1/p^{s_1}, 1/p^{s_2}, \cdots, 1/p^{s_n}, \cdots$ is such that

$$\lim_{n \to \infty} N(B_j, E_{s_n})/\lambda = 1/g^j \tag{1.1}$$

for any $j \geqq 1$, where $s_n \geqq [j \log_p g]$ for all $n \geqq 1$ and $\lambda=(p-1)p^{s_n-1}$.

In general, the distribution of the digits in E_n, the recurring period of the reciprocal of an integral power of an odd prime, expanded to a base g which is a primitive root mod p^2 and $2 \leqq g < p^n$, can be characterized by the (k, ϵ)-normal concept of Besicovitch [2] given in 1934. We shall define this concept in §2. The expansions are (k, ϵ)-normal for a given $\epsilon > 0$ and a bounded sequence of integers k.

We shall establish a number of corollaries based on inequalities derived from a central theorem which concerns the counts of a block of digits B_j in the period of $1/p^n$. We use $[x]$ to represent the greatest integer not exceeding x.

Presented to the Society, February 23, 1963; received by the editors August 14, 1961 and, in revised form, November 19, 1962.

THEOREM. *Let g be a primitive root* mod p^2 *such that* $2 \leqq g < p^n$, *where p is an odd prime and n is any positive integer, then the number of occurrences of any block of j digits chosen from* $0, 1, 2, \cdots, g-1$ *in the recurring period of* $1/p^n$ *will be one of the alternatives given by*

$$N(B_j, E_n) = [p^n/g^j] - [p^{n-1}/g^j] + m, \tag{1.2}$$

where $|m| \leqq 2$ *and all* $j \leqq [n \log_g p]$. *If* $n=1$ *and* $j=1$, *then* $m=0$ *or* 1; *if* $n=1$ *and* $2 \leqq j \leqq [\log_g p]$, *then* $m=-1, 0,$ *or* 1; *if* $n>1$ *and* $j=1$, *then* $m=-1, 0,$ *or* 1; *and if* $n>1$ *and* $2 \leqq j \leqq [n \log_g p]$, *then* $m=-2, -1, 0,$ *or* 1. *For block sizes j such that* $[n \log_g p] < j \leqq (p-1)p^{n-1}$, *we have* $N(B_j, E_n)=0$ *or* 1.

The theorem implies the following inequalities. For counts of blocks in $1/p$, we have

$$-2/p < N(B_j, E_1)/p - 1/g^j < 1/p \tag{1.3}$$

or

$$|N(B_j, E_1)/p - 1/g^j| < 2/p \tag{1.4}$$

which can be written in a form indicating relative frequency since $\lambda = p-1$

$$|N(B_j, E_1)/(p-1) - 1/g^j| < 2/(p-1) + 1/(p-1)g^j. \tag{1.5}$$

If $n>1$, we have for the expansion of $1/p^n$ in the base g

$$-3/(p-1)p^{n-1} < N(B_j, E_n)/(p-1)p^{n-1} - 1/g^j < 2/(p-1)p^{n-1} \tag{1.6}$$

or

$$|N(B_j, E_n)/(p-1)p^{n-1} - 1/g^j| < 3/(p-1)p^{n-1}, \tag{1.7}$$

where in (1.3) to (1.7) for a given p, g, and n the range of block sizes which will satisfy these inequalities are all $j \leqq [n \log_g p]$. The theorem distinguishes two types of blocks of j digits which occur in the expansion of $1/p^n$ in the base g which is a primitive root modulo p^n. Any block B_j of j digits where the block size j is such that $j \leqq [n \log_g p]$ will occur in the distribution of digits in the period with a relative frequency of approximately $1/g^j$. If the block size is such that $[n \log_g p] < j \leqq (p-1)p^{n-1}$ then a particular choice of j digits may or may not occur in the expansion, i.e., have a count of 0 or 1.

We find convenient the definition of (k, ϵ)-normality stated by Hanson [3] in 1954. In our notation, we shall say (j, ϵ)-normality.

2. **Definitions.** *(j, ϵ)-normality.* An integer $m = a_0 a_1 \cdots a_{\lambda-1}$ (represented in the scale g) consisting of λ digits is (j, ϵ)-normal in the

scale g for a given j and a given $\epsilon>0$ if for every j digit sequence $B_j=b_1b_2\cdots b_j$ which occurs in m denoted by $N(B_j, m)$

$$|N(B_j, m)/\lambda - 1/g^j| < \epsilon. \tag{2.1}$$

For $j=1$, we say that m is ϵ-normal in the scale g.

Consider the inequality (1.7). The upper bound $[n \log_g p]$ on the block size provides a convenient measure of the "*degree of normality*" of a given expansion of $1/p^n$ for a given p, g and n since all blocks B_j for $j\leqq[n \log_g p]$ will appear with approximate relative frequency $1/g^j$. A measure of the *degree of approximation* to $1/g^j$ is $\epsilon(p, n)=3/(p-1)p^{n-1}$. We note that $\epsilon(p, n)$ is independent of the choice of the primitive root base g. Let us define the degree of normality of $1/p^n$ to the base g to be $J_g(1/p^n)=[n \log_g p]$ and $\epsilon(p, n)=3/(p-1)p^{n-1}$. Thus, for example, $J_{10}(1/17^{50})=61$ and $\epsilon(17, 50)\cong 10^{-61}$ would indicate that in $1/17^{50}$ to the base 10 all blocks B_j would have a relative frequency of $1/10^j$ such that $\epsilon(17, 50)\cong 10^{-61}$ for all $j\leqq 61$.

In the proof of the theorem and where the context indicates, we shall use the notation B_j to represent either a block of j digits or the same block in place notation to the base g.

3. **Proof of the theorem.** Consider the representation of $1/p^n$, where p is an odd prime, and n a positive integer in the scale g which is a primitive root mod p^n. We have for one period of length $\lambda=(p-1)p^{n-1}$

$$1/p^n = .b_0b_1\cdots b_kb_{k+1}\cdots b_{k+j-1}\cdots b_{\lambda-1} = E_n, \tag{3.1}$$

where $B_j=b_kb_{k+1}\cdots b_{k+j-1}$ is a block of j digits (somewhere in the period) chosen from the integers $0, 1, \cdots, g-1$. The digits b_i in the period E_n of $1/p^n$ are in a 1-1 correspondence with the periodic set of residues r_i mod p^n determined by

$$g^i \equiv r_i \bmod p^n, \tag{3.2}$$

where the b_i are given by

$$b_i = [gr_i/p^n]. \tag{3.3}$$

The residues will be a complete set of reduced power residues relatively prime to p where $i=0, 1, \cdots, \lambda-1=(p-1)p^{n-1}-1$, $1\leqq r_i \leqq p^n-1$ and $0\leqq b_i\leqq g-1$. The number B_j with the initial digit b_k will be given by

$$B_j = [r_kg^j/p^n] \tag{3.4}$$

where r_k is the kth remainder. Since $p^n\nmid r_kg^j$, we have from (3.4)

$$p^nB_j/g^j < r_k < p^n(B_j+1)/g^j. \tag{3.5}$$

We shall count the number of residues r_k in the interval (3.5) and then remove from this count, the count of the number of residues not relatively prime to p in the same interval. The residues not relatively prime to p are all $r_k = pR_k$ where $R_k = 1, 2, \cdots, p^{n-1}-1$. Therefore, the R_k are contained in

$$p^{n-1}B_j/g^j < R_k < p^{n-1}(B_j+1)/g^j. \tag{3.6}$$

Let $N^*(B_j, E_n)$ denote the number of occurrences of the block of j digits B_j for a given p, n, and g in $1/p^n$ corresponding to the count of the number of r_k in (3.5) and $N'(B_j, E_n)$ the count of the number of R_k as given by (3.6), then $N(B_j, E_n) = N^*(B_j, E_n) - N'(B_j, E_n)$ will be the counts of the blocks B_j with the initial digit b_k in the period E_n. We distinguish three possibilities for the B_j: $B_j = 0$, $B_j = g^j - 1$ and $B_j \neq 0$, $g^j - 1$. If $B_j = 0$, (3.5) yields

$$0 < r_k < p^n/g^j \tag{3.7}$$

or $N^*(B_j, E_n) = [p^n/g^j]$ since $g^j \nmid p^n$. Similarly, (3.6) gives

$$0 < R_k < p^{n-1}/g^j \tag{3.8}$$

or $N'(B_j, E_n) = [p^{n-1}/g^j]$ since $g^j \nmid p^{n-1}$, and counting the R_k counts the r_k. Therefore, the counts of $B_j = 0$ are given by

$$N(B_j, E_n) = [p^n/g^j] - [p^{n-1}/g^j]. \tag{3.9}$$

For $B_j = g^j - 1$, (3.5) yields

$$p^n - p^n/g^j < r_k < p^n \tag{3.10}$$

or $N^*(B_j, E_n) = p^n - [p^n - p^n/g^j] - 1 = [p^n/g^j]$. Similarly, we find from (3.6) $N'(B_j, E_n) = [p^{n-1}/g^j]$ and therefore

$$N(B_j, E_n) = [p^n/g^j] - [p^{n-1}/g^j]. \tag{3.11}$$

For all other $B_j \neq 0$, $g^j - 1$, we have from (3.5) and (3.6)

$$\begin{aligned} N(B_j, E_n) = {} & [p^n(B_j+1)/g^j] - [p^nB_j/g^j] \\ & - \{[p^{n-1}(B_j+1)/g^j] - [p^{n-1}B_j/g^j]\} \end{aligned} \tag{3.12}$$

since g^j does not divide $p^n(B_j+1)$, p^nB_j, $p^{n-1}(B_j+1)$, and $p^{n-1}B_j$. From the properties of the greatest integer when x and y are not integers, viz. $[x+y] = [x]+[y]$ or $[x]+[y]+1$, we obtain from (3.12) three alternatives independent of the choice of B_j for the counts of the B_j given by

$$N(B_j, E_n) = [p^n/g^j] - \lfloor p^{n-1}/g^j \rfloor + m, \tag{3.13}$$

where m can have the values -1, 0, or $+1$. For $n=1$, and following the previous argument precisely for $B_j=0$, g^j-1 and $B_j\neq 0$, g^j-1, we obtain

$$N(B_j, E_n) = [p/g^j] + m, \tag{3.14}$$

where now $m=0$ or $+1$. We note that (3.13) includes (3.14) as a special case if we set $m=0$ or 1 in (3.13) when $n=1$ since $[p^{n-1}/g^j]=0$ with $g\geqq 2$ and $j\geqq 1$. Since the width of the interval in (3.5) is p^n/g^j, we can have at least one integral r_k in the interval and thus a count $N(B_j, E_n)$ for every choice of B_j if we seek the positive integral values $j\geqq 1$ such that $p^n/g^j>1$ for a fixed choice of p, g, and n. Therefore, if p is a given odd prime, g a fixed choice of primitive root mod p^2 and n is a fixed positive integer, then each positive integer j such that $j\leqq [n \log_g p]$ will insure that $p^n/g^j>1$. The largest primitive root g_m of p^n which can be used as a base in the expansion of $1/p^n$ must be such that $g_m<p^n$ or $n \log_{g_m} p>1$. This is a necessary condition for all choices of j digits in B_j such that $j\leqq [n \log_g p]$ to have positive counts with the possible exception that when $j=[n \log_g p]$ there can be a few counts which are zero. These counts of zero are associated with blocks which we shall call "anomalous" and they shall be discussed presently. Thus, all blocks B_j such that $j\leqq [n \log_g p]$ will have relative frequency counts of approximately $1/g^j$ as indicated by (1.5) and (1.7). Since the (complete set of) primitive roots of p^n are such that $2\leqq g<p^n$ where p is an odd prime [7, p. 70], we will have positive counts for all $j\leqq [n \log_g p]$ for a given fixed choice of p, n, and all g mod p^2. If $p^n/g^j<1$ for some given p, g, n, and j, then (3.5) may or may not contain a residue depending on the particular choice of digits in B_j. This applies to all possible B_j such that $[n \log_g p]<j\leqq (p-1)p^{n-1}$, the counts of such blocks $N(B_j, E_n)$ can be only 0 or 1.

To the alternatives for m given in (3.13), we have one further consideration. Since the counting of the B_j depends on counting all the r_k in the interval (3.5) including those not relatively prime to p which initiate a particular choice of digits B_j in a period of $1/p^n$, there will be some r_k in the periodic set of residues modulo p^n corresponding to those digits near the end of a period which have been counted in (3.5) and (3.6), yet these r_k initiate blocks which extend into the next period. Consider the sequence of residues commencing with r_k which leads to such blocks of j digits, we have $B_j \sim r_k, r_{k+1}, \cdots, r_{\lambda-1}, r_\lambda, \cdots, r_{k+j-1}$, where the periodic set of residues ends the period at $r_{\lambda-1}$ and $r_\lambda=1$ and all succeeding residues r_i to r_{k+j-1} are such that their corresponding digits are zeros. These are zero since the residues at the beginning of a period or after the end are such that $r_t=g^t$ where $g^t<p^n$ for $t=0, 1, \cdots, [n \log_g p]-1$, i.e., the expansion of

$1/p^n$ begins with $[n \log_g p]$ zeros. This block of $[n \log_g p]$ zeros constitutes one of the all zero blocks such that $j=[n \log_g p]$. Therefore, we have $j-1$ of the g^j possible blocks B_j such that they commence with at least one digit b_k in the period E_n and terminate with zeros that are digits in the next period. We shall designate these $j-1$ blocks which have already been counted using (3.5) and (3.6) but are not to be included in the actual counts "*anomalous*" blocks. Therefore, to include these anomalous blocks, we set $m=-2, -1, 0, 1$ for all possible alternatives since the count of a given anomalous block might have been obtained from (3.13) with $m=-1$ and the actual count in E_n is one less. To summarize, we account for the possible anomalous counts in each case by setting $m=-1, 0, 1$ for $n=1, j>1$ (no anomalous count can occur for $j=1$) and $m=-2, -1, 0, 1$ for $n>1$ and $j>1$. The other counts for $n=1, j=1$ and $n>1, j=1$ remain as in (3.13) and (3.14). The proof of the theorem is now complete.

4. **Some corollaries.** From the inequalities (1.3)–(1.7), we may derive a number of results. Noting (1.5) and (1.7), we obtain using (2.1)

COROLLARY 1. *There are* $\phi\{(p-1)p^{n-1}\}$ *distinct representations of* $1/p^n$, *where* p *is an odd prime and* n *is any positive integer, to bases* g *which are primitive roots* mod p^2 *such that* $2 \leqq g < p^n$ *and each representation is* (j, ϵ)*-normal with* $\epsilon=2/(p-1)+1/(p-1)g^j$ *and all* $j \leqq [\log_g p]$ *for* $n=1$, *and* $\epsilon=3/(p-1)p^{n-1}$ *with all* $j \leqq [n \log_g p]$ *for* $n>1$.

In Corollary 1, we have used the result that the complete set of $\phi\{(p-1)p^{n-1}\}$ positive distinct primitive roots of p^n are all g such that $2 \leqq g < p^n$, where $\phi(x)$ is the Euler ϕ-function, [7, p. 70].

A. Brauer [4, pp. 25, 27, Theorems 7 and 10] in 1954 proved that there exists at least $\{\phi(p-1)\}/2$ positive primitive roots mod p^n for every odd prime and positive integer n which are less than p and if $p>5$ is a prime of the form $4N+1$, then there are at least $3\{\phi(p-1)\}/4$ primitive roots less than p and at least $\{\phi(p-1)\}/4$ less than $p/2$. For all primitive roots such that $2 \leqq g < p$, we have $\log_g p > 1$ or $n \log_g p > n$. Therefore Brauer's results insures that there will exist at least $\{\phi(p-1)\}/2$ expansions of $1/p^n$ to bases g such that g is a primitive root mod p^2 and $2 \leqq g < p$, where the blocks B_j will occur for all $j=1, 2, \cdots, n, \cdots, [n \log_g p]$ or certainly all $j \leqq n$, i.e., the degree of normality for such primitive roots is $J_g(1/p^n) \geqq n$ independent of the particular prime or primitive root. If $p>5$ is a prime of the form $4N+1$ then there are at least $3\{\phi(p-1)\}/4$ expansions of $1/p^n$ to bases g such that $2 \leqq g < p$ with $J_g(1/p^n) \geqq n$ and at least

$\{\phi(p-1)\}/4$ to bases g such that $2 \leqq g < p/2$ with $J_g(1/p^n) \geqq [n \log_g 2g]$. For example, if $p>5$ is a prime of the form $4N+1$ and $g=2$, then $J_2(1/p^n) \geqq 2n$. We have

COROLLARY 2. *If p is an odd prime and n a positive integer, then there exists at least $\{\phi(p-1)\}/2$ representations of $1/p^n$ in a scale g where g is a primitive root* mod p^2 *which are (j, ϵ)-normal with $n>1$ and $\epsilon = 3/(p-1)p^{n-1}$ for all $j \leqq n$.*

COROLLARY 3. *If $p>5$ is an odd prime of the form $4N+1$, n a positive integer, then there exists at least $3\{\phi(p-1)\}/4$ representations of $1/p^n$ in scales g, where g is a primitive root* mod p^2 *such that $2 \leqq g < p$ which are (j, ϵ)-normal for $n>1$ for all $j \leqq n$ and there are at least $\{\phi(p-1)\}/4$ representations of $1/p^n$ which are (j, ϵ)-normal in the scales g such that $2 \leqq g < p/2$ for $j \leqq [n \log_g 2g]$ and $\epsilon = 3/(p-1)p^{n-1}$ in both cases.*

From (1.7), we easily obtain

COROLLARY 4. *Consider the set of digits E_{s_n} in the recurring periods of a sequence of reciprocals $1/p^{s_1}, 1/p^{s_2}, \cdots, 1/p^{s_n}, \cdots$ of positive integral powers of a fixed odd prime p each represented in the same scale $g \geqq 2$ which is a primitive root* mod p^2, *where $s_1 < s_2 < \cdots < s_n < s_{n+1} \cdots$ is any strictly monotonic increasing sequence of positive integers with $s_n \geqq [j \log_p g]$ for $n \geqq 1$ and a given j, then the relative frequency of any block B_j chosen from the digits $0, 1, 2, \cdots, g-1$ evaluated over each successive period is such that*

$$\lim_{n \to \infty} N(B_j, E_{s_n})/(p-1)p^{s_n-1} = 1/g^j \tag{4.1}$$

for any j.

In Corollary 4 we take $s_n \geqq [j \log_p g]$ for $n \geqq 1$ so that for a given p, g and j, the first reciprocal will contain blocks of the chosen size.

Consider (1.5) and (1.7) for a fixed positive integer n. It is worth noting that for p *sufficiently large*, $\epsilon(p, n) = 3/(p-1)p^{n-1}$ is arbitrarily small and the relative frequency of the blocks B_j are as close to $1/g^j$ as we please for all blocks $j \leqq [n \log_g p]$ and any choice of primitive root of p^n such that $2 \leqq g < p^n$ even though we cannot state precisely the primitive root in $1/g^j$ for any prime p. A study of the degree of normality $J_g(1/p^n) = [n \log_g p]$ for a fixed value of n as the primes increase without bound is necessary in order to draw conclusions concerning the upper bound on the j values. For example, does $[n \log_g p]$ increase without bound for a fixed value of n as p increases?

Finally, let us consider the consequences of assuming a well-known conjecture (Le Veque [5, pp. 69, 122]) that there are an infinite number of primes which have a given fixed integer g as a primitive root. In this case, we may fix the primitive root g_0 and allow the primes which have g_0 as a primitive root to increase without bound. Thus, from (1.7) we obtain

COROLLARY 5. *If there exists an infinite number of odd primes each of which has the given integer* g_0 *as a primitive root* mod p^2, *then the relative frequency of any block of* j *digits* B_j *chosen from* $0, 1, \cdots, g_0-1$ *evaluated over the reciprocals of the sequence of the integral powers of such primes for some fixed positive integer exponent* n *(each expanded to the same base* g_0*) is such that*

$$\lim_{p\to\infty} N(B_j, E_n)/(p-1)p^{n-1} = 1/g_0^j \tag{4.2}$$

for all j.

In Niven [6, p. 116], we find the remarks "E. Borel defined an 'absolutely' normal number as one that is normal to every base. However, might it be that, if a number is normal to one base, it is absolutely normal? It would be interesting to have an answer to this question, because it would tell us the depth of the normality concept, whether this concept is associated with the numbers themselves (as are the rational and algebraic concepts) or whether it is dependent upon the particular base of representation used to represent the number." Schmidt [8] in 1960 proved that there exists numbers which are normal to one base but not absolutely normal. Similarly, for our results, $1/p^n$ is (j, ϵ)-normal on a restricted subset of integers, i.e., only those primitive roots in the range $2 \leqq g < p^n$ but is not (j, ϵ)-normal for all integers g in this interval which would be the analog of absolute normality. Further, we see from Corollary 1 that if $1/p^n$ is (j, ϵ)-normal to one scale g which is a primitive root of p^n then it is (j, ϵ)-normal for every primitive root such that $2 \leqq g < p^n$ and also that (j, ϵ)-normality of $1/p^n$ depends intimately on the particular number being represented, i.e., on the particular primitive roots of that p^n for such bases. In a sense every (j, ϵ)-normal expansion (of $1/p^n$) can be transformed into every other (j, ϵ)-normal expansion since any primitive root of p^n can be used to generate all the other members of the complete set of distinct primitive roots of p^n.

These results also offer numerical techniques for the construction of sequences of digits with any desired degree of normality by taking n sufficiently large in $1/p^n$, e.g. $J_{10}(1/17^n) = [n \log_{10} 17]$.

Can we find analogous results for the sums and products of the reciprocals of integral powers of primes and perhaps, eventually, study the (j, ϵ)-normal properties of the distribution of digits in the rational approximations of irrationals?

References

1. R. G. Stoneham and S. Dunin, IBM 650, Western Data Processing Center, Univ. of California, Los Angeles, Calif., project #0030, 1957 (unpublished). R. P. Kelisky, IBM 7090, Thomas J. Watson Research Center, Yorktown Heights, New York, 1962.

2. A. S. Besicovitch, *The asymptotic distribution of the numerals in the decimal representation of the squares of the natural numbers*, Math. Z. **39** (1934), 146–156.

3. H. A. Hanson, *Some relations between various types of normality of numbers*, Canad. J. Math. **6** (1954), 477–485.

4. A. Brauer, *Elementary estimates for the least primitive root*, Studies in mathematics and mechanics, presented to R. von Mises, pp. 20–29, Academic Press, New York, 1954.

5. W. J. Le Veque, *Topics in number theory*, Vols. I and II, Addison-Wesley, Reading, Mass., 1956.

6. I. Niven, *Irrational numbers*, Carus Math. Monographs, No. 11, Wiley, New York, 1956.

7. R. D. Carmichael, *The theory of numbers and diophantine analysis*, Dover, New York, 1959.

8. W. Schmidt, *On normal numbers*, Pacific J. Math. **10** (1960), 661–672.

The City College of the City University of New York