MATHEMATICS OF COMPUTATION, VOLUME 27, NUMBER 124, OCTOBER 1973

A Note on Dirichlet Characters

By Richard H. Hudson

Abstract. Denoting by $r(k, m, p)$ the first occurrence of m consecutive kth power residues of a prime $p \equiv 1 \pmod{k}$, we show that $r(k, m, p) > c \log p$ for infinitely many p (c is an absolute constant) provided that k is even and $m \geqq 3$.

1. Introduction. Throughout this paper, k will be an integer $\geqq 2$ and p a prime $\equiv 1 \pmod{k}$. It follows from a theorem of A. Brauer [1] that, for each positive integer m and "sufficiently large" p, there exists a positive integer r and kth power Dirichlet character mod p such that

$$\chi(r) = \chi(r + 1) = \cdots = \chi(r + m - 1) = 1. \tag{1.1}$$

D. H. Lehmer and E. Lehmer [5] denoted by $r(k, m, p)$ the smallest positive integer r satisfying (1.1) and defined $\Lambda(k, m)$ to be the least upper bound of $r(k, m, p)$ where the supremum is taken over all but the finite exceptional set of primes for which no such r exists.

In [8], W. H. Mills noted the obvious connection between the class F_k of all totally multiplicative functions f defined on the positive integers taking on values in the group of kth roots of unity and the class of kth power Dirichlet characters mod p. The author is credited in [11] with preparing for publication a manuscript of I. Schur and using this paper to solve the conjecture of Mills [8] that there are only two functions in F_2 for which there is no positive integer r with

$$f(r) = f(r + 1) = f(r + 2) = 1. \tag{1.2}$$

In [4], the author indicated that the Mills conjecture can be combined with D. A. Burgess's [2] well-known bound for the maximum number of consecutive elements in any of the cosets of the group of kth powers (mod p) to show that

$$r(2, 3, p) \ll p^{1/4} \log p. \tag{1.3}$$

The implied constant in (1.3) is absolute and I have recently calculated an admissible value (approximately 271). However, the proof is long and will not be presented here.

Instead, in this note, we look the other direction and show that

$$r(k, m, p) \neq o(\log p) \tag{1.4}$$

if k is even and $m \geqq 3$. This is, of course, stronger than the result proved by Lehmer and Lehmer [5] that $\Lambda(k, m) = \infty$ if $m \geqq 3$. We conjecture, but are unable to prove, that (1.4) holds for all k if $m \geqq 4$ and we refer the reader to [3] for a possible means of attacking this problem. If $m = 2$ or if k is odd and $m = 3$, it has been conjectured that $r(k, m, p)$ is finite in sharp contrast to (1.4). There is a remarkable asymmetry in the

Received November 1, 1972.

AMS (MOS) subject classifications (1970). Primary 10H35, 10A15.

fact that (1.4) holds if k is even and $m = 3$, but is false if $m = k = 3$ since $\Lambda(3, 3) = 23{,}532$ (cf. [6]).

2. A lower bound for $r(k, m, p)$.

THEOREM. *For each even integer k and each integer $m \geqq 3$, there exist infinitely many primes p such that*

$$r(k, m, p) > c \log p, \tag{2.1}$$

where c is a positive absolute constant.

Proof. It is clearly sufficient to prove the proposition for $r(2, 3, p)$ since $r(k, m, p) \geqq r(2, 3, p)$ if k is even.

Let q_i, $i = 1, 2, \cdots$, denote the ith prime. It is well known that, for each fixed integer n, there exist infinitely many primes p such that

$$(q_i/p) = \alpha_i \tag{2.2}$$

where α_i is either $+1$ or -1 for each $i = 1, 2, \cdots, n$.

In fact, letting

$$d_n = 4q_1 \cdots q_n \tag{2.3}$$

it is known [10] that there exist $\varphi(d_n)/2^n$ integers l with $l < d_n$ and $(l, d_n) = 1$ such that (2.2) holds for every prime $p \equiv l \pmod{d_n}$. Corresponding to each such number l, let p_n denote the smallest prime $\equiv l \pmod{d_n}$. It follows from Linnik [7] that

$$p_n < d_n^s \tag{2.4}$$

where s is an absolute constant. Now

$$(1/s) \log p_n < \log d_n, \tag{2.5}$$

but $\log d_n = \log 4 + \Phi(q_n)$ where $\Phi(x)$ is the Chebyshev function. Since Rosser and Schoenfeld [9] have shown that

$$\Phi(x) < x(1 + 1/(2 \log x)) \quad \text{for every} \quad x > 1, \tag{2.6}$$

it follows that

$$\log d_n < q_n + q_n/(2 \log q_n) + \log 4 < 2(q_n - 2) \tag{2.7}$$

for $n > 4$ ($q_n > 7$).

Now, assume that the values α_i in (2.2) are chosen so that

$$\begin{aligned} \alpha_i &= 1 \quad \text{if} \quad q_i \equiv 1 \pmod 3, \\ &= -1 \quad \text{if} \quad q_i \equiv 2 \pmod 3, \end{aligned} \tag{2.8}$$

for $i = 1, 2, \cdots, n - 1$ and that

$$\begin{aligned} \alpha_n &= -1 \quad \text{if} \quad q_n \equiv 1 \pmod 3, \\ &= 1 \quad \text{if} \quad q_n \equiv 2 \pmod 3. \end{aligned} \tag{2.9}$$

Clearly, $r(2, 3, p_n) \geqq q_n - 2$ and it follows from (2.5) and (2.7) that, for each $n > 4$,

$$r(2, 3, p_n) \geqq (1/2s) \log p_n. \tag{2.10}$$

The result now follows from the obvious fact that $\varphi(d_n)/2^n \to \infty$ as $n \to \infty$.

Remark. It is clear from [10] that the lower bound $c \log p$ holds also for $r_2(p)$, the smallest positive prime quadratic residue. It is curious that large values of the smallest prime quadratic residue and large values of the first run of three consecutive quadratic residues are mutually exclusive. In fact, it is easily checked that if $p \geqq 17$ and $r_2(p) > 7$, then $r(2, 3, p) \leqq 14$, and if $p \geqq 17$ and $r(2, 3, p) > 14$, then $r_2(p) \leqq 7$. Is a similar result true for each $m > 3$?

Department of Mathematics
University of South Carolina
Columbia, South Carolina 29208

1. A. Brauer, "Ueber Sequenzen von Potenzresten," *S.-B. Preuss. Akad. Wiss. Phys. Math. Kl.*, 1928, pp. 9–16.

2. D. A. Burgess, "A note on the distribution of residues and non-residues," *J. London Math. Soc.*, v. 38, 1963, pp. 253–256. MR **26** #6135.

3. P. D. T. A. Elliot, "Some notes on k-th power residues," *Acta Arith.*, v. 14, 1967, pp. 153–162. MR **37** #4000.

4. Richard H. Hudson, "On the first occurrence of three consecutive integers with equal quadratic character," *Duke Math. J.*, v. 40, 1973, pp. 33–39.

5. D. H. Lehmer & Emma Lehmer, "On runs of residues," *Proc. Amer. Math. Soc.* v. 13, 1962, pp. 102–106. MR **25** # 2025.

6. D. H. Lehmer, Emma Lehmer, W. H. Mills & J. L. Selfridge, "Machine proof of a theorem on cubic residues," *Math. Comp.*, v. 16, 1962, pp. 407–415. MR **28** #5578.

7. Ju. V. Linnik, "On the least prime in an arithmetic progression. I. The basic theorem," *Mat. Sb.*, v. 15 (57), 1944, pp. 139–178. (Russian) MR **6**, 260.

8. W. H. Mills, *Bounded Consecutive Residues and Related Problems,* Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc., Providence, R.I., 1965, pp. 170–174. MR **31** #1226.

9. J. B. Rosser & L. Schoenfeld, "Approximate formulas for some functions of prime numbers," *Illinois J. Math.*, v. 6, 1962, pp. 64–94. MR **25** #1139.

10. Hans Salie, "Über den kleinsten positiven quadratischen Nichtrest nach einer Primzahl," *Math. Nachr.*, v. 3, 1949, pp. 7–8. MR **11**, 500.

11. I. Schur, "Multiplikativ signierte Folgen postiver ganzer Zahlen," *Gesammelte Abhandlungen von I. Schur,* Springer, Berlin, 1973.