ACTA ARITHMETICA
XXVIII (1975)

A bound for the first $k-1$ consecutive k-th power non-residues (mod p)

by

Richard H. Hudson (Columbia, S.C.)

1. Introduction and summary. Throughout χ will be a non-principal character (mod p) of order k, where p is an odd prime with $p \equiv 1 \pmod k$ and k is an integer $\geqslant 2$.

Let $r(k, m, p)$ denote the smallest positive integer r such that

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

and let $a_j(k, p)$ denote the smallest positive integer a such that

$$\chi(a) \neq 1, \quad \chi(a+1) \neq 1, \quad \ldots, \quad \chi(a+j-1) \neq 1. \tag{1.2}$$

Although knowledge of the exact number of triples of consecutive quadratic residues of primes p is classical and approximate formulae are well-known for the number of occurrences of m consecutive residues (with a markedly improved error term (see [4], p. 198) due to the work of A. Weil [7]), the first non-trivial upper bound for $r(k, m, p)$ when $k = 2$ and $m = 3$ was obtained by the author; see, in particular [5] and [6]. Namely, for $k = 2$ and $m = 3$, I have shown that

$$r(k, m, p) < 270\cdot 5p^{1/4}\log p + 62 \quad \text{for all } p > 17. \tag{1.3}$$

On the other hand, P. D. T. A. Elliott showed in [2], Lemma 12, that

$$a_2(k, p) = O_\varepsilon(p^{1/4+\varepsilon}) \tag{1.4}$$

for $k = 2$, $\varepsilon > 0$, and $p \geqslant 5$.

In [3], Elliott gave a slight improvement of (1.4), namely

$$a_2(k, p) = O_\varepsilon\left(p^{\frac{1}{4}\left(1-\frac{e^{-10}}{2}\right)+\varepsilon}\right) \tag{1.5}$$

for $k = 2$, $\varepsilon > 0$, and $p \geqslant 5$. Unfortunately, Elliott's results applied only to real characters (mod p), and nothing was obtained for $a_j(k, p)$ when j is > 2.

I am deeply indebted to Hugh L. Montgomery for suggesting to m
a technique by means of which a considerable generalization of Elliott
result can be obtained as a relatively easy consequence of Burgess's chara
ter sum estimates.

Specifically, for $\varepsilon > 0$, $k \geqslant 2$, and $p > p_0(\varepsilon, k)$, I will show tha

(1.6) $$a_{k-1}(k, p) = O_{\varepsilon,k}(p^{1/4+\varepsilon}).$$

There are, for example, at least six consecutive seventh power nor
residues less than $p^{1/4+\varepsilon}$! Note also that an immediate consequence c
(1.4) and (1.6) is that the second smallest *prime* character non-residu
of characters of order $\geqslant 2$, $g_2(k, p)$, satisfies the implied inequality i
(1.6) since $g_2(k, p) \leqslant a_2(k, p) + 1$.

2. Consecutive character non-residues.

THEOREM. *For every $\varepsilon > 0$ and each $k \geqslant 2$,*

(2.1) $$a_{k-1}(k, p) = O_{\varepsilon,k}(p^{1/4+\varepsilon})$$

for all primes $p > p_0(\varepsilon, k)$ satisfying $p \equiv 1 (\operatorname{mod} k)$.

Proof. Let X denote the set of complex valued characters (mod p
of order k defined on the positive integers, and order the elements o
X so that $\chi = \chi_1$ is the character with the property that $\chi(n) = e^{2\pi i/k}$ i
n is a character non-residue of order k.

Then, for $(n, p) = 1$ we have

(2.2) $$\sum_{r=1}^{k-1} \chi^r(n) = \begin{cases} k-1 & \text{for} \quad \chi(n) = 1, \\ -1 & \text{for} \quad \chi(n) \neq 1, \end{cases}$$

since $e^{2\pi i/k} + e^{4\pi i/k} + \ldots + e^{(2\pi i/k)(k-1)} = -1$.

Assume that

(2.3) $$p^{1/4+\varepsilon} < (k-1)N < a_{k-1}(k, p).$$

Then, obviously, at least N of the integers n with $n \leqslant (k-1)N$ are charac
ter residues of order k. Consequently, no more than $(k-2)N$ can be charac
ter non-residues of order k.

Thus

(2.4) $$\sum_{n \leqslant (k-1)N} \Big(\sum_{r=1}^{k-1} \chi^r(n)\Big) = \sum_{\substack{n \leqslant (k-1)N \\ \chi(n)=1}} (k-1) - (k-2) \sum_{\substack{n \leqslant (k-1)N \\ \chi(n) \neq 1}} 1$$
$$\geqslant N(k-1) - N(k-2) = N.$$

But, from Burgess [1], if $a_{k-1}(k, p) > p^{1/4+\varepsilon}$ we must have

(2.5) $$\Big|\sum_{n \leqslant (k-1)N} \Big(\sum_{r=1}^{k-1} \chi^r(n)\Big)\Big| = \Big|\sum_{r=1}^{k-1} \Big(\sum_{n \leqslant (k-1)N} \chi^r(n)\Big)\Big|$$
$$\leqslant \sum_{r=1}^{k-1} \Big|\sum_{n \leqslant (k-1)N} \chi^r(n)\Big|$$
$$< \sum_{r=1}^{k-1} \varepsilon(k-1)N = \varepsilon N(k-1)^2.$$

But $N > \varepsilon N(k-1)^2$ for $\varepsilon < \dfrac{1}{(k-1)^2}$ contradicting the assumption (2.3)
and, consequently, the theorem is proved.

References

[1] D. A. Burgess, *A note on the distribution of residues and non-residues*, J. London Math. Soc. 38 (1963), pp. 253–256.

[2] P. D. T. A. Elliott, *On the mean value of $f(p)$*, Proc. London Math. Soc. (3) 21 (1970), pp. 28–96.

[3] — *On the least pair of consecutive quadratic non-residues* (mod p), Proc. Conf. Number Theory, Univ. Colorado, Boulder, Colorado, 1972, pp. 75–79.

[4] A. O. Gelfond and Yu. V. Linnik, *Elementary Methods in Analytic Number Theory*, Chicago, Illinois, 1965.

[5] Richard H. Hudson, *A bound for the first occurrence of three consecutive integers with equal quadratic character*, Duke Math. J. 40 (1973), pp. 33–39.

[6] — *A note on Dirichlet characters*, Math. Comp. 27 (1973), pp. 973–975.

[7] A. Weil, *Riemann hypothesis in function fields*, Proc. Math. Acad. Sci. U. S. A., 27 (1941), pp. 345–347.

UNIVERSITY OF SOUTH CAROLINA

Received on 14.5.1974 (592)