Finally let \( L \) be a set of positive integers; is it true that there exists a sequence \( A \) such that \( A^n \) is a basis if and only if \( n \) belongs to \( L \)? The answer is yes if there is only a finite number of integers which do not lie in \( L \).

Added in proof. The first named author and E. Poutry proved in a paper which will appear in the J. London Math. Soc. that for any set \( L \) of positive integers there does exist a sequence \( A \) such that \( A^n \) is a basis if and only if \( n \) belongs to \( L \); it is clear from their proof that there exists also a sequence \( H \) which is not a basis such that \( H^3 \) is a basis of order at most 5.

References


Received on 20. 5. 1974
and in revised form on 2. 12. 1974

A sharper bound for the least pair of consecutive \( k \)-th power non-residues of non-principal characters (mod \( p \)) of order \( k > 3 \)

by

RICHARD H. HUDSON (Columbia, S. C.)

1. History of the problem. Let \( \chi \) be a non-principal character (mod \( p \)) of fixed order \( k \) and let \( n_\chi(k, p) \) denote the smallest positive integer satisfying

\[
\chi(n_\chi(k, p)) \neq 0 \quad \text{or} \quad 1, \quad \chi(n_\chi(k, p) + 1) \neq 0 \quad \text{or} \quad 1.
\]

The first significant success in providing an upper bound for \( n_\chi(k, p) \) was that of P. D. T. A. Elliott ([3], p. 52) who showed that for real valued characters (mod \( p \)), i.e. Legendre symbols \( (p > 2) \), that

\[
n_\chi(k, p) = O(p^{1/2 + \varepsilon})
\]

for each \( \varepsilon > 0 \) and \( p \gg 5 \).

Although (1.2) is a relatively easy consequence of D. A. Burgess’s [1] deep and thoroughly remarkable character sum estimates, Elliott improved (1.2) when, in addressing the Number Theory Conference in Boulder, Colorado in 1972 [4], he showed that

\[
n_\chi(k, p) = O(p^{1/2 - \varepsilon/2})
\]

for each \( \varepsilon > 0 \) and \( p \gg 5 \).

2. A new bound for \( n_\chi(k, p) \). An “alternative bound” for \( n_\chi(k, p) \) was provided in [7] where I proved that

\[
n_\chi(k, p) \leq \left( g_1(k, p) - 1 \right) g_2(k, p)
\]

where \( g_1(k, p) \) and \( g_2(k, p) \) are, for each fixed \( k \), respectively the smallest and the second smallest positive primes with \( \chi(g_1(k, p)) \neq 0 \) or 1, \( \chi(g_2(k, p)) \neq 0 \) or 1.

I asserted in [7] which was written in the Fall of 1973, and I announced when I spoke in Oberwolfach, Germany in January, 1974, that (2.1) leads to an improvement of (1.3) for all non-principal characters.
of order $k > 3$. Indeed I am now able, by combining (2.1) with Burgess's estimate ([1], Th. 1) and the method of Davenport and Erdős [2], to prove the following

**Theorem 1.** For each fixed $\varepsilon > 0$, prime $p \geq 5$, and non-principal character (mod $p$) of fixed order $k > 3$,

$$n_k(k, p) = O\left(p^{\frac{k}{2k^{1/2}}}\right),$$

where $n_k$ is the (unique) solution of $g(w) = 1/k$ and $g(w)$ is Dickman's function, defined by $g(0) = 1$ for $0 \leq w < 1$, $g(w) = -g(w-1)$ for $w > 1$.

In other words, combining Burgess's remarkable work with (2.1), I have succeeded in reducing the bound on $n_k(k, p)$ so that it is now as sharp as Davenport and Erdős' bound for the least $k$th power non-residue. For $k = 4$ and 5 the exponents are approximately .2357 and .2215 while for $k > 5$ the exponent is less than 1/12.

I am grateful to the referee for pointing out to me that Karl Norton [8] announced in January of 1974 the following brilliant result which can be combined with (2.1) to provide an immediate proof of Theorem 1.

**Theorem 2 (K. K. Norton).** For $k \geq 2$, $\varepsilon > 0$, and $1 \leq m \leq \frac{\log n}{\log \log n}$,

$$q_m(k, n) = O_n\left(n^{1+\frac{1}{k}}\right).$$

In Theorem 2, $q_m(k, n)$ is the $m$th prime such that, for each fixed $k$, $\varepsilon(q_m(k, n)) \neq 0$ or $1$; $n$ may be composite, and $n_k$ is defined as in Theorem 1.

Remark. The bound (1.2) holds also for $k = 3$ due to work of the author in [6]; more generally, the author shows in [6] that the upper bound $\varepsilon(p^{1+\varepsilon})$ holds for no less than $k-1$ consecutive $k$th power non-residues of non-principal characters (mod $p$) of order $k > 2$.

References


