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. Fouvry 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^2 is a basis of order at most 5.

References

[1] J. G. van der Corput, *Neue zahlentheorische Abschätzungen*, Math. Zeitsch. 29 (1929), pp. 397–426.

[2] J. F. Koksma, *Some theorems on Diophantine inequalities*, Math. Centrum Amsterdam Script. 5 (1950).

[3] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe*, J. Reine Angew. Math. 194 (1955), pp. 111–140.

[4] I. M. Vinogradov, *The Method of Trigonometrical Sums in the Theory of Numbers*, London 1954.

Received on 29. 5. 1974
and in revised form on 2. 12. 1974 (593)

ACTA ARITHMETICA
XXX (1976)

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 χ be a non-principal character (mod p) of fixed order k and let $n_2(k,p)$ denote the smallest positive integer satisfying

(1.1) $$\chi(n_2(k,p)) \neq 0 \text{ or } 1, \quad \chi(n_2(k,p)+1) \neq 0 \text{ or } 1.$$

The first significant success in providing an upper bound for $n_2(k,p)$ 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

(1.2) $$n_2(k,p) = O(p^{1/4+\varepsilon})$$

for each $\varepsilon > 0$ and $p \geqslant 5$.

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

(1.3) $$n_2(k,p) = O\left(p^{\frac{1}{4}\left(1-\frac{e^{-10}}{2}\right)+\varepsilon}\right)$$

for each $\varepsilon > 0$ and $p \geqslant 5$.

2. A new bound for $n_2(k,p)$. An "alternative bound" for $n_2(k,p)$ was provided in [7] where I proved that

(2.1) $$n_2(k,p) \leqslant (q_1(k,p)-1)(q_2(k,p))$$

where $q_1(k,p)$ and $q_2(k,p)$ are, for each fixed k, respectively the smallest and the second smallest positive primes with $\chi(q_1(k,p)) \neq 0$ or 1, $\chi(q_2(k,p)) \neq 0$ 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 Erdös [2], to prove the following

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

$$n_2(k, p) = O(p^{\frac{1}{2u_k}+\varepsilon}) \tag{2.2}$$

where u_k is the (unique) solution of $\varrho(u) = 1/k$ and $\varrho(u)$ is Dickman's function, defined by $\varrho(u) = 1$ for $0 \leqslant u \leqslant 1$, $u\varrho'(u) = -\varrho(u-1)$ for $u > 1$.

In other words, combining Burgess's remarkable work with (2.1), I have succeeded in reducing the bound on $n_2(k, p)$ so that it is now as sharp as Davenport and Erdös' bound for the least kth power non-residue. For $k = 4$ and 5 the exponents are approximately .2357 and .2215 while for $k > e^{33}$ 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 $k \geqslant 2$, $\varepsilon > 0$, and $1 \leqslant m \leqslant \dfrac{\log n}{\log\log n}$,*

$$q_m(k, n) = O_{k,\varepsilon}(p^{\frac{1}{4u_k}+\varepsilon}). \tag{2.3}$$

In Theorem 2, $q_m(k, n)$ is the mth prime such that, for each fixed k, $\chi(q_m(k, n)) \neq 0$ or 1; n may be composite, and u_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 $p^{1/4+\varepsilon}$ holds for no less than $k-1$ consecutive kth power non-residues of non-principal characters (mod p) of order $k > 2$.

References

[1] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), pp. 179–192.

[2] H. Davenport and P. Erdös, *The distribution of quadratic and higher power residues*, Pub. Math. (Debrecen) 2 (1951–1952), pp. 252–265.

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

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

[5] Richard H. Hudson, *Prime k-th power non-residues*, Acta Arith. 23 (1973), pp. 89–106.

[6] — *A bound for the first $k-1$ consecutive k-th power non-residues* (mod p), Acta Arith. 28 (1975), pp. 341–343.

[7] — *The least pair of consecutive character non-residues*, to appear in Journ. Reine Angew. Math.

[8] K. K. Norton, *Estimates for prime k-th power non-residues*, Notices Amer. Math. Soc. 21 (1974), January, 74T–A12.

UNIVERSITY OF SOUTH CAROLINA

Received on 23. 7. 1974
and in revised form on 27. 1. 1975 (603)