A NOTE ON THE SECOND SMALLEST PRIME $k$ TH POWER NONRESIDUE

RICHARD H. HUDSON

ABSTRACT. Upper bounds for the second smallest prime $k$th power nonresidue, which we denote by $g_2(p, k)$, have been given by many authors. Theorem 1 represents an improvement of these bounds, at least for odd $k$. We also give specific estimates for $g_2(p, k)$, and an upper bound for the $n$th ($n \geq 2$) smallest prime $k$th power nonresidue as a function of the first $n - 1$ prime nonresidues. Upper bounds for $g_2(p, k)$ should take on new interest since the author has shown elsewhere that the first two consecutive $k$th power nonresidues are bounded above by the product of the first two prime nonresidues.

1. Introduction. Throughout $k$ will be an integer $\geq 2$ and $p$ will be a prime $= 1$ (mod $k$). The $n$th smallest prime $k$th power nonresidue, $n \geq 2$, will be denoted by $g_n(p, k)$. In [4] the author investigated at some length the problem of finding upper bounds for $g_2(p, k)$. The major purpose of this paper is to improve the bounds given in [4, Theorem 4], which are, to the best of our knowledge, the sharpest upper bounds known for $g_2(p, k)$ for odd $k$. In particular, we are now able to prove the following result.

Theorem 1. For each $\epsilon > 0$ and $p > 5$,

\[ g_2(p, k) = O_{\epsilon, k}(p^{k/4(k-1)+\epsilon}). \]

We also note that several other theorems in [4] can be improved using recent work of P. D. T. A. Elliott [2], [3], Hugh L. Montgomery [8], and K. K. Norton [9], [10].

In the following proof, $h_j(p, k)$, $j = 0, 1, \ldots, k - 1$, will denote the smallest positive representative of the $j$th coset formed with respect to the subgroup of the $k$th powers mod $p$. In particular, for all $k$, $h_0(p, k) = 1$, $h_1(p, k) = g_1(p, k)$, $g_2(p, k)$ denotes the smallest positive $k$th power nonresidue in a coset different than the coset to which $h_1(p, k)$ belongs, $h_{k-1}$ denotes the
smallest positive \( k \)th power nonresidue in a coset different than the cosets to which \( h_1, h_2, \ldots, h_{k-2} \) belong. In the following proof we assume that \( k \geq 3 \) since Theorem 1 is well known for \( k = 2 \). We also observe that \( g_2(p, k) \) is less than \( p \) if \( p \geq 5 \), since otherwise the \( k \)th power nonresidues of \( p \) consist only of powers of \( g_1(p, k) \) and these are clearly insufficiently numerous.

2. Proof of Theorem 1. We want to show that for each \( \epsilon > 0 \) and \( k \geq 3 \) there exists a constant \( c_1(\epsilon, k) \) such that for every prime \( p > 5 \),

\[
(2.1) \quad g_2(p, k) < c_1(\epsilon, k)p^{k/4(k-1)+\epsilon}.
\]

Assume first, that for each \( \epsilon > 0 \) and \( k \geq 3 \), there exists a constant \( c_2(\epsilon, k) \) such that for every odd prime \( p \),

\[
(2.2) \quad g_1(p, k) < c_2(\epsilon, k)p^{1/4(k-1)+\epsilon/(k-1)}.
\]

It follows from [4, Lemma 2] that

\[
(2.3) \quad g_2(p, k) \leq g_1(p, k) \cdot s_n + 1
\]

where \( s_n \) denotes the maximum number of consecutive integers in any of the nonresidue cosets formed with respect to the subgroup of \( k \)th powers mod \( p \). It is well known that \( s_n < c_3p^{1/4}\log p \) for all \( k \) where \( c_3 \) is an absolute constant (in fact \( c_3 < 3.230 \); see [6]). Of course, \( \log p = o(p^{\epsilon/(k-1)}) \) and, consequently, if (2.2) holds, (2.1) follows at once from (2.3).

Conversely, assume there exists \( \epsilon > 0 \) or \( k \geq 3 \) such that for every constant \( c_4(\epsilon, k) \), there exist infinitely many primes with

\[
(2.4) \quad g_1(p, k) > c_4(\epsilon, k)p^{1/4(k-1)+\epsilon/(k-1)}.
\]

Norton [9] has shown that for each \( \epsilon > 0 \) and \( k \geq 2 \) there must exist a constant \( c_5(\epsilon, k) \) such that for every odd prime \( p \),

\[
(2.5) \quad h_{k-1}(p, k) < c_5(\epsilon, k)p^{1/4+\epsilon}.
\]

If (2.4) and (2.5) both hold, we must have \( h_{k-1}(p, k) < (g_1(p, k))^{k-1} \).

But if \( g_2(p, k) > h_{k-1}(p, k) \), and if \( x \) is any \( k \)th power nonresidue such that \( 1 < x \leq h_{k-1}(p, k) \), then clearly \( x = (g_1(p, k))^a y \), where \( y \) is a \( k \)th power residue and \( 1 \leq a \leq k - 2 \). Hence, the inequalities (2.4) and \( g_2(p, k) > h_{k-1}(p, k) \) imply that there are at most \( k - 1 \) cosets of the subgroup of \( k \)th powers mod \( p \), a contradiction. Consequently, if (2.4) holds, we have \( g_2(p, k) \leq h_{k-1}(p, k) \), and (2.1) follows from (2.5).
3. Specific estimates. We shall call an upper bound for \( g_n(p, k) \) a specific estimate if it is of the form \( g_n(p, k) < cp^\alpha \), where \( c \) and \( \alpha \) are specified real numbers and the bound holds for all \( p \) greater than a specified real number. We shall call a specific estimate a universal specific estimate if it is a specific estimate which holds for all \( p \) for which \( g_n(p, k) \) exists.

L. K. Hua [7] has given the best specific estimate for \( g_2(p, k) \) for \( k = 2 \). In particular Hua showed that for \( k = 2 \) (and hence for even \( k \)) and \( p > e^{250} \),

\[
g_2(p, k) < (57600p)^{5/16}.
\]

Using [4, Theorem 3] and K. K. Norton's [10] recently announced improvement of his universal specific estimate for \( g_1(p, k) \), namely \( g_1(p, k) < 1.1p^{1/4}(\log p + 4) \), it is possible to slightly improve Corollary 1 in [4, p. 103].

**Theorem 2.** For each \( k \) and all \( p \geq 5 \),

\[
g_2(p, k) < 4p^{7/16}(1.1 \log p + 4.4)^{3/4} + 8.8p^{1/4} \log p + 36.2.
\]

Norton [10] has also announced a universal specific estimate for the maximum number, \( S \), of consecutive integers in any coset formed with respect to the subgroup of \( k \)th powers mod \( p \), namely \( S < 4.1p^{1/4}\log p \). The author has shown in [6] that this estimate can be improved to \( S < 3.616p^{1/4}\log p \). This allows us to make specific our estimate [4, Lemma 3] for the \( n \)th smallest prime \( k \)th power nonresidue as a function of the first \( n - 1 \) prime nonresidues.

**Theorem 3.** Let \( n \) be any integer \( \geq 2 \). Then

\[
g_n(p, k) < (3.616p^{1/4} \log p + 1) \left( \prod_{r=1}^{n-1} g_r(p, k) \right) + 1.
\]

In [5] the author noted that if \( g_1(p, k) < 2^{1/4}p^{1/4} \), then \( S < 2.9086p^{1/4}\log p \). This yields the following exemplary corollary to Theorem 3.

**Corollary.** Let \( p \) be a prime for which \( g_1(p, k) = 2 \) so that \( g_2(p, k) \) is the smallest odd \( k \)th power nonresidue. Then

\[
g_2(p, k) < 5.8172p^{1/4} \log p + 3.
\]

This universal specific estimate for the smallest odd \( k \)th power nonresidue improves earlier estimates of Brauer [1] and the author [4, Theorem 1].

In conclusion, we note that Theorem 7 of [4] appears rather naive in
R. H. HUDSON

retrospect. In fact Hugh L. Montgomery has informed me that if the generalized Riemann hypothesis is true, then $g_n(p, k) = O((\log^2 p)$ for all $n < \log^2 p / \log \log p$; see also [6].

Note added in Proof (July, 1974). In the near future we hope to improve Theorem 1 considerably. In particular we expect to prove, without hypotheses, that $g_n(p, k) = O(p^{1/4 + \varepsilon})$ for every $p > p_0(\varepsilon)$ and every $n \leq (c \log p) / \log \log p$ (for some positive constant $c$).

REFERENCES


6. ———, The least pair of consecutive $k$th power non-residues (to appear).


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, COLUMBIA, SOUTH CAROLINA 29208

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use