TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 194, 1974

POWER RESIDUES AND NONRESIDUES IN ARITHMETIC PROGRESSIONS

BY
RICHARD H. HUDSON

ABSTRACT. Let k be an integer ≥ 2 and p a prime such that $v_k(p) = (k, p-1) > 1$. Let $bn + c (n = 0, 1, \ldots; b \geq 2, 1 \leq c < b, (b,p) = (c,p) = 1)$ be an arithmetic progression. We denote the smallest kth power nonresidue in the progression $bn + c$ by $g(p,k,b,c)$, the smallest quadratic residue in the progression $bn + c$ by $r_2(p,b,c)$, and the nth smallest prime kth power nonresidue by $g_n(p,k)$, $n = 0, 1, 2, \ldots$.

If $C(p)$ is the multiplicative group consisting of the residue classes mod p, then the kth powers mod p form a multiplicative subgroup, $C_k(p)$. Among the $v_k(p)$ cosets of $C_k(p)$ denote by T the coset to which c belongs (where c is the first term in the progression $bn + c$), and let $h(p,k,b,c)$ denote the smallest number in the progression $bn + c$ which does not belong to T so that $h(p,k,b,c)$ is a natural generalization of $g(p,k,b,c)$.

We prove by purely elementary methods that $h(p,k,b,c)$ is bounded above by $2^{7/4}b^{5/2}p^{2/5} + 3b^3p^{1/5} + b^2$ if p is a prime for which either b or $p-1$ is a kth power nonresidue. The restriction on b and $p-1$ may be lifted if $p > (g_1(p,k))^{7.5}$. We further obtain a similar bound for $r_2(p,b,c)$ for every prime p, without exception, and we apply our results to obtain a bound of the order of $p^{2/5}$ for the nth smallest prime kth power nonresidue of primes which are large relative to $\prod_{j=1}^{n-1} g_j(p,k)$.

1. **Introduction.** In 1924 C. Stengel [12] showed that, with a few identifiable exceptions, the least quadratic nonresidue $\equiv 1 (\mathrm{mod}\ 8)$ of a prime p is less than p, a very weak result. A. Brauer has informed me that he has independently obtained our slightly less trivial Lemma 1, but that he has been unable to improve this result.

We adopt the following notation. Throughout the paper k will be an integer ≥ 2 and without loss of generality p will be a prime $\equiv 1 (\mathrm{mod}\ k)$. Also $bn + c$, $n = 0, 1, \ldots$, will always be an arithmetic progression for which $b \geq 2$, $1 \leq c < b$, and $(b,p) = (c,p) = 1$. Let $g(p,k,b,c)$ denote the smallest kth power nonresidue in the progression $bn + c$ and let $r_2(p,b,c)$ denote the smallest quadratic residue in the progression $bn + c$. Let $C(p)$ be the multiplicative group consisting of the residue classes mod p and let $C_k(p)$ denote the subgroup of the kth powers mod p. The $k-1$ cosets (not including the zero coset) formed with respect to $C_k(p)$ are frequently called the classes of nonresidues. Let S_n be the maximum number of consecutive elements in any of the $k-1$ classes of nonresidues and let S be the maximum number of consecutive elements in any of the k cosets.

Received by the editors July 10, 1972.

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

Key words and phrases. kth power residue, arithmetic progressions, subgroup of kth powers, elementary methods, smallest kth power nonresidue in arithmetic progressions.

In §2 we establish a preliminary lemma from which it follows that $g(p,k,b,c)$ and $r_2(p,b,c)$ are bounded above by $b(2S+1)+c$. Clearly, if one uses D.A. Burgess's [5] well-known algebraically obtained bound for S, and if b is fixed and p is "sufficiently large", then Lemma 1 immediately yields the bound $O(p^{1/4}\log p)$ for $g(p,k,b,c)$ and $r_2(p,b,c)$. Using A. Brauer's [2] purely elementary bound for S, namely,

$$S < (2p)^{1/2} + 2, \tag{1.1}$$

one only obtains from Lemma 1 the much weaker bound for $g(p,k,b,c)$ and $r_2(p,b,c)$,

$$2b((2p)^{1/2}+3), \tag{1.2}$$

although this bound holds for all values of p.

The surprising fact is that for almost all primes we are able to improve rather dramatically on the bound (1.2) by generalizing a purely elementary method first used by Brauer [1].

Specifically, in §3, we show that if p is a prime for which b or $p-1$ are kth power nonresidues then $g(p,k,b,c)$ is bounded above by

$$2^{7/4}b^{5/2}p^{2/5} + 3b^3p^{1/5} + b^2. \tag{1.3}$$

This bound is also shown to hold for $r_2(p,b,c)$ for every prime p and, in fact, a slightly sharper bound is given if $p \equiv 1 \pmod 4$ and $(b/p) = -1$.

In §4 we show that $g(p,k,b,c)$ is bounded by

$$2^{11/4}b^{5/2}p^{2/5} + 6b^3p^{1/5} + 2b^2 \tag{1.4}$$

even if b and $p-1$ are both kth power residues, provided that $p > (g_1(p,k))^{7.5}$, where $g_1(p,k)$ denotes the smallest kth power nonresidue. Thus, for example, if $k=2$ and $p \not\equiv 1 \pmod{24}$ or if $k=3$ and $p \neq x^2+27y^2$, $g(p,k,b,c)$ is bounded above by (1.4).

Moreover, in §4, we generalize the concept of $g(p,k,b,c)$ as follows. Among the k cosets denote by T the coset to which c belongs (where c is the first term in the progression $bn+c$), and let $h(p,k,b,c)$ denote the smallest number in the progression $bn+c$ which does not belong to T. It follows that $g(p,k,b,c) = h(p,k,b,c)$ if and only if T is the zero coset (i.e. c is a kth power residue). In Theorem 6 of §4 we show that all of the above mentioned results for $g(p,k,b,c)$ hold, in fact, for $h(p,k,b,c)$.

Let $g_n(p,k)$, $n = 1, 2, \ldots$, denote the nth smallest *prime* kth power nonresidue. In [10] the author noted that the problem of finding an upper bound for $g_n(p,k)$ using only elementary methods appears to be very difficult if $n > 2$. In §5, however, we show that if $Q = \prod_{j=1}^{n-1} g_j(p,k)$ and, if $p > (g_1(p,k))^{7.5}$, or if Q or $p-1$ are kth power nonresidues, then $g_n(p,k)$ is bounded above by

$2^{11/4}Q^{5/2}p^{2/5} + 6Q^3p^{1/5} + 2Q^2$. Consequently, if $\prod_{j=1}^{n-1} g_j(p,k)$ is small relative to p we find a bound for $g_n(p,k)$, by purely elementary methods, considerably better than $p^{1/2}$.

2. **Preliminaries.** Frequently we will use the following abbreviations; g for $g(p,k,b,c)$, r for $r_2(p,b,c)$, h for $h(p,k,b,c)$, and g_n, $n = 1, 2, \ldots$, for $g_n(p,k)$. $[x]$ will denote the greatest integer $\leq x$, $[x_1,\ldots,x_n]$ will denote an integer interval which includes x_1 and x_n if and only if they are integers, and $(x_1,\ldots,x_n)$ will denote an integer interval that includes neither x_1 nor x_n.

Lemma 1. *Let p be a prime and let $bn + c$ be an arithmetic progression with $b \geq 2$, $1 \leq c < b$, and $(b,p) = (c,p) = 1$. Let $C_k(p)$ denote the subgroup of kth powers* mod *p and let S be the maximum number of consecutive elements in any of the k cosets of $C_k(p)$. Then, among the numbers in the arithmetic progression $bn + c$, $n = 0, 1, \ldots, 2S + 1$, there are representatives from at least two different cosets.*

Proof. Let x be the unique integer solution to the congruence $bx \equiv c \pmod p$ such that $1 \leq x < p$. Let t be the smallest positive integer such that c and $bt + c$ are in different cosets and note that $b(x + n) \equiv bn + c \pmod p$, $n = 0, 1, 2, \ldots, t - 1$, so that

$$x, x + 1, x + 2, \ldots, x + t - 1 \tag{2.1}$$

are t consecutive elements in the same coset excepting possible multiples of p which do not belong to any of the cosets. Clearly, at most one integer of the form (2.1) is a multiple of p, in which case it is equal to p, for obviously $x < p \Rightarrow x + t < 2p$. At worst, p is exactly half-way between x and $x + t - 1$ and it follows immediately that $(t - 1)/2 \leq S$ or $t \leq 2S + 1$, establishing Lemma 1.

Remark 1. The proof simplifies and $2S + 1$ may be replaced by S if b is "small" relative to p or by $S + 1$ if -1 is a kth power nonresidue. However the advantage of stating the lemma in the above form is that one can speak of the size of $g(p,k,b,c)$ even when $b > p$.

As an immediate consequence of Lemma 1 and (1.1) we obtain the following corollaries.

Corollary 1. *Let $g(p,k,b,c)$ be the smallest kth power nonresidue in the progression $bn + c$. Then*

$$g(p,k,b,c) \leq b(2S + 1) + c < 2b((2p)^{1/2} + 3). \tag{2.2}$$

Corollary 2. *Let $r_2(p,b,c)$ be the smallest quadratic residue in the progression $bn + c$. Then*

$$r_2(p,b,c) \leq b(2S + 1) + c < 2b((2p)^{1/2} + 3). \tag{2.3}$$

Remark 2. If b is a kth power nonresidue then S may be replaced by S_n in (2.2) and if b is a quadratic residue then S may be replaced by S_n in (2.3). Slightly better elementary bounds are known for S_n than for S (cf. [8] and [9]).

Note that Corollary 2 is certainly not always valid if $r_2(p,b,c)$ is replaced by $r(p,k,b,c)$, the smallest kth power residue in the progression $bn + c$. For example, if $k = p - 1$ then $S = 1$, so that $r(p,k,b,c) > p$ for every $b \geq 2$ provided $c > 1$.

3. **An upper bound for $g(p,k,b,c)$ and $r_2(p,b,c)$.**

Theorem 1. *Let $bn + c$, $n = 0, 1, \ldots$, be an arithmetic progression with $b \geq 2$, $(b,p) = (c,p) = 1$, and $1 \leq c < b$. Let p be a prime for which either b or $p - 1$ is a kth power nonresidue and let $g(p,k,b,c)$ denote the smallest kth power nonresidue in the progression $bn + c$. Then*

$$g(p,k,b,c) < 2^{7/4}b^{5/2}p^{2/5} + 3b^3p^{1/5} + b^2. \tag{3.1}$$

Proof. Assume that Theorem 1 is false.

We may assume that $b < p^{1/15}$ since, otherwise, Theorem 1 follows from Lemma 1. Let $g = bz + c$ and let x be the unique integer solution to the congruence $bx \equiv c \pmod{p}$ such that $1 \leq x < p$. Then the interval

$$[x, x + 1, \ldots, x + z - 1] \tag{3.2}$$

contains only kth power nonresidues if b is a kth power nonresidue. If b is a kth power residue and $p - 1$ is a kth power nonresidue the interval

$$[-x, -x - 1, \ldots, -x - z + 1] \tag{3.3}$$

contains only kth power nonresidues.

Henceforth, J will denote the interval (3.2) if b is a kth power nonresidue and the interval (3.3) if $p - 1$ is a kth power nonresidue. Note that J contains z integers and

$$z = (g - c)/b > (g/b) - 1 > 2^{7/4}b^{3/2}p^{2/5} + 3b^2p^{1/5}. \tag{3.4}$$

In the interval

$$(p^{1/5}, \ldots, p^{1/5} - b), \tag{3.5}$$

there is an integer of the form $bn + c$, $n \geq 0$, call it s. Of course s is a kth power residue by virtue of our assumption. Consider the multiples of s in the interval J, say

$$(a)s, (a + 1)s, \ldots, (a + t - 1)s. \tag{3.6}$$

Since integers of the form (3.6) are kth power nonresidues and s is a kth power

residue, the integers

$$a, a+1, \ldots, a+t-1 \tag{3.7}$$

are kth power nonresidues. Furthermore,

$$t \geq [2^{7/4} b^{3/2} p^{1/5} + 3b^2] \tag{3.8}$$

since $s < p^{1/5}$ and any h consecutive integers must contain at least $[h/s]$ multiples of s.

It is easy to verify that

$$\begin{aligned} a + t - 1 &< p/s < p/(p^{1/5} - b) \\ &= p^{4/5} + bp^{3/5} + b^2 p^{2/5} + b^3 p^{1/5} + b^4 + b^5/(p^{1/5} - b) < 2p^{4/5} \end{aligned} \tag{3.9}$$

since $b < p^{1/10}$ and, thus, $p > 2^{10}$. It follows that there exists an integer f such that

$$(bf + c)^2 < a < \cdots < a + t - 1 < (b(f+1) + c)^2. \tag{3.10}$$

For, by (3.9) and because of our assumption, $bf + c < g - b$ and, consequently, $bf + c$ and $b(f+1) + c$ are kth power residues.

Let $d = b(f+1) + c$ and subdivide the interval $[(d-b)^2, \ldots, d^2]$ using the integers

$$d^2, d^2 - b^2, d^2 - (2b)^2, \ldots, d^2 - (mb)^2, d^2 - ((m+1)b)^2 \tag{3.11}$$

where m is the largest positive integer such that $d^2 - (mb)^2 > (d-b)^2$. Clearly,

$$m < (2d/b - 1)^{1/2}. \tag{3.12}$$

Now the number of integers lying between two integers of the form (3.11) is given by

$$((d^2 - (w+1)^2 b^2) - (d^2 - w^2 b^2)) - 1 = (2w+1)b^2 - 1, \tag{3.13}$$

$w = 0, 1, \ldots, m$. Furthermore, all numbers of the form (3.11) are kth power residues for, by (3.12),

$$d + (m+1)b < d + (2d-b)^{1/2} b^{1/2} + b. \tag{3.14}$$

But, by (3.9) and (3.10), $d + b < 2^{1/2} p^{2/5} + 2b$ so that

$$\begin{aligned} d + (2d-b)^{1/2} + b &< 2^{1/2} p^{2/5} + 2b + b^{1/2}(2(2^{1/2} p^{2/5} + b) - b)^{1/2} \\ &< 2^{1/2} p^{2/5} + 2b + 2^{3/4} p^{1/5} b^{1/2} + b \end{aligned} \tag{3.15}$$

which is less than g by virtue of our assumption. It follows that numbers of the

form (3.11) are the product of two factors less than g and, consequently, are kth power residues.

It follows from (3.12) and (3.13), since the t consecutive kth power nonresidues given by (3.7) are trapped between kth power residues of the form (3.11), that

$$\begin{aligned} t &\leq (2m+1)b^2 - 1 < 2(2d-b)^{1/2}b^{3/2} + b^2 - 1 \\ &< 2(2^{3/2}p^{2/5} + b)^{1/2}b^{3/2} + b^2 - 1 < 2^{7/4}p^{1/5}b^{3/2} + 3b^2 - 1, \end{aligned} \tag{3.16}$$

contradicting (3.8).

Theorem 2. *Let $r_2(p,b,c)$ be the smallest quadratic residue in the progression $bn + c$. If $p \equiv 3 \pmod 4$ or $(b/p) = +1$,*

$$r_2(p,b,c) < 2^{7/4}b^{5/2}p^{2/5} + b^3p^{1/5} + b^2. \tag{3.17}$$

If $p \equiv 1 \pmod 4$ and $(b/p) = -1$, then

$$r_2(p,b,c) < (384)^{1/4}bp^{2/5} + (3b^3 + 3b/2)p^{1/5}. \tag{3.18}$$

Proof. Assume that Theorem 2 is false.

We may assume that $b < p^{1/15}$ since otherwise Theorem 2 follows from Corollary 2 of Lemma 1. Let z be such that $r_2(p,b,c) = bz + c$ and let x be the unique integer solution to the congruence $bx \equiv c \pmod p$ such that $1 \leq x < p$. Then the interval

$$[x, x+1, x+2, \ldots, x+z-1] \tag{3.19}$$

contains only quadratic nonresidues if b is a quadratic residue, and it contains only quadratic residues if b is a quadratic nonresidue. In the latter case the interval

$$[-x, -x-1, -x-2, \ldots, -x-z+1] \tag{3.20}$$

contains only quadratic nonresidues if $p \equiv 3 \pmod 4$.

If $p \equiv 1 \pmod 4$ and b is a quadratic nonresidue, then the interval

$$[a, a+1, \ldots, a+t-1], \tag{3.21}$$

where ba is the smallest and $b(a+t-1)$ is the largest multiple of b in the interval (3.19), contains only quadratic nonresidues.

Let J denote the interval (3.19) if b is a quadratic residue, the interval (3.20) if b is a quadratic nonresidue and $p \equiv 3 \pmod 4$, and the interval (3.21) if b is a quadratic nonresidue and $p \equiv 1 \pmod 4$. In the first two cases the remainder of the proof is essentially identical with the proof of Theorem 1; in fact, we may simply replace the word kth power by the word quadratic and replace g by r. Indeed, the proof is slightly simpler in the quadratic case since $(bf + c)^2$ and

$(b(f+1)+c)^2$, by virtue of being squares, are immediately quadratic residues (eliminating the need for the argument used in establishing (3.10)). If, however, b and $p-1$ are both kth power residues Theorem 1 fails to give us any information and, consequently, we must consider separately this case in which J is the interval (3.21).

Glancing at (3.21) we see that J contains t consecutive quadratic nonresidues, and it follows that

$$t \geq [z/b] > (z/b) - 1 = ((r - c/b^2) - 1) \geq (r/b^2) - 3/2 \tag{3.22}$$

since $r = bz + c$, $c < b$, and $b \geq 2$.

In the interval

$$((p^{1/5}/b), \ldots, (p^{1/5}/b) - b) \tag{3.23}$$

there clearly is an integer of the form $bn + c$ since $2 \leq b < p^{1/15} \Rightarrow (p^{1/5}/b) - b > 0$. Denote this integer by s and note that s is a quadratic residue for $b < r$ by assumption. Consequently, if ys, $(y+1)s, \ldots, (y+u-1)s$ are the multiples of s in the interval (3.21), then

$$y, y+1, y+u-1 \tag{3.24}$$

are quadratic nonresidues.

Furthermore,

$$\begin{aligned} y + u - 1 &< p/bs < p/(p^{1/5} - b^2) \\ &= p^{4/5} + b^2p^{3/5} + b^4p^{2/5} + b^6p^{1/5} + b^8 + b^{10}/(p^{1/5} - b^2) < 6p^{4/5} \end{aligned} \tag{3.25}$$

for $b < p^{1/10} \Rightarrow p^{4/5} + b^2p^{3/5} + b^4p^{2/5} + b^6p^{1/5} + b^8 < 5p^{4/5}$ and $b < p^{1/15} \Rightarrow b^{10}/(p^{1/5} - b^2) < p^{2/3}/(p^{1/5} - p^{2/15}) < p^{4/5}$, the final inequality holding because $p > 2^{15}$.

Since we are restricting ourselves to the case $k = 2$ so that squares are (by definition) residues, it follows that there exists an integer f such that

$$(bf + c)^2 < y < \cdots < y + u - 1 < (b(f+1) + c)^2. \tag{3.26}$$

Letting $d = b(f+1) + c$, subdividing the interval $[(d-b)^2, \ldots, d^2]$ by integers of the form (3.11), and defining m as in Theorem 1, we claim that

$$d + (m+1)b \leq d + (2bd)^{1/2} + b < r. \tag{3.27}$$

For, by (3.25), (3.26), and our assumption,

$$\begin{aligned} d - b = bf + c < (y + u - 1)^{1/2} < 6^{1/2}p^{2/5} &\Rightarrow d < 6^{1/2}p^{2/5} + b \\ \Rightarrow d + (2bd)^{1/2} &< 6^{1/2}p^{2/5} + b + 2^{1/2}b^{1/2}(6^{1/4}p^{1/5} + b^{1/2}) \\ &= 6^{1/2}p^{2/5} + (24)^{1/4}b^{1/2}p^{1/5} + (2^{1/2} + 1)b < r - b \end{aligned} \tag{3.28}$$

from which follows (3.27).

Consequently, every integer of the form $(d + wb)(d - wb) = d^2 - (wb)^2$, $w = 0, 1, \ldots, m$, is a quadratic residue in the interval $[(d - b)^2, \ldots, d^2]$.

Now the interval $[y, y + 1, \ldots, y + u - 1]$ contains at least $[t/s]$ integers so that, by (3.22) and our assumption,

$$\begin{aligned} u &> (t/s) - 1 > (2r - 3b^2)/2b^2s - 1 \geq r/b^2s - 5/2 \\ &> (r/bp^{1/5}) - 5/2 > (384)^{1/4}p^{1/5} + 3b^2 - 1. \end{aligned} \tag{3.29}$$

However, it follows from (3.12) and (3.13) that

$$\begin{aligned} u &\leq (2m + 1)b^2 - 1 < 2(2d - b)^{1/2}b^{3/2} + b^2 - 1 \\ &< 2(2^{3/2}p^{2/5} + b)^{1/2}b^{3/2} + b^2 - 1 \\ &< 2^{7/4}3^{1/4}p^{1/5} + 3b^2 - 1 = (384)^{1/4}p^{1/5} + 3b^2 - 1, \end{aligned} \tag{3.30}$$

contradicting (3.29).

Remark 3. It is clear that the coefficients in Theorem 1 and Theorem 2 may be improved if p is known to be 'large' relative to b. However, the improvement is small, not of great interest, and complicates the proof.

4. Generalizations of Theorem 1. Unfortunately Theorem 1 does not yield a result if b and $p - 1$ are both kth power residues. This is scarcely surprising since, to date, no author has been able to produce an elementary method to show that the smallest kth power nonresidue, $g_1(p, k)$, is less than p^a if $a < 1/2$ unless $p - 1$ is a kth power nonresidue (cf. [11]). However, in special cases we know that $g_1(p, k)$ is small. For example, if $k = 2$ and $p \not\equiv 1 \pmod{24}$, then $g_1(p, k) \leq 3$. Also if $k = 3$ and $p \neq x^2 + 27y^2$, then $g_1(p, k) = 2$. Similar criteria are known for other values of k (see, e.g. [4]).

Theorem 3 is very useful when p is 'large' relative to $g_1(p, k)$, and Theorems 4 and 5 are illustrative examples of the use of Theorem 3. Theorems 6 and 7 give bounds for $h(p, k, b, c)$ analogous to the bounds given for $g(p, k, b, c)$. The proofs of Theorems 6 and 7 are very similar to the proofs of Theorems 1 and 3 and, consequently, we appeal in the proofs of Theorems 6 and 7 to the arguments established in Theorems 1 and 3.

Theorem 3. *Let g_1 be the smallest kth power nonresidue, and let $g(p, k, b, c)$ be defined as in Theorem* 1. *If $p > g_1^{7.5}$, then*

$$g(p, k, b, c) < 2^{11/4}b^{5/2}p^{2/5} + 6b^3p^{1/5} + 2b^2. \tag{4.1}$$

Proof. Because of Corollary 1 and Theorem 1 we may assume that $b < p^{1/15}$ and that b and $p - 1$ are kth power residues. Let x be the unique integer solution to the congruence $bx \equiv c \pmod{p}$ such that $1 \leq x < p$. Let z be such that $bz + c = g(p, k, b, c)$. Then the interval

$$[x, x+1, \ldots, x+z-1] \tag{4.2}$$

contains only kth power residues.

Assume that Theorem 3 is false. Then there exists a kth power residue, call it s, in the interval

$$(p^{1/5}/g_1, \ldots, (p^{1/5}/g_1) + b) \tag{4.3}$$

since this interval contains an integer of the form $bn + c$, $0 \leq n < z$. Let $k = sg_1$ so that k is a kth power nonresidue with $p^{1/5} < k < p^{1/5} + bg_1 < 2p^{1/5}$ (since $b < p^{1/15}$ and $g_1 < p^{2/15}$).

Consider the multiples of k in the interval (4.2), say

$$ak, (a+1)k, \ldots, (a+t-1)k. \tag{4.4}$$

Since these integers are kth power residues and k is a kth power nonresidue, the integers

$$a, a+1, a+2, \ldots, a+t-1 \tag{4.5}$$

are kth power nonresidues.

Now $a + t - 1 < p/k < p/2p^{1/5} = p^{4/5}/2$ and, moreover,

$$t \geq [2^{7/4} b^{3/2} p^{1/5} + 3b^2] \tag{4.6}$$

since $k < 2p^{1/5}$ and any h consecutive integers must contain at least $[h/s]$ multiples of s.

The remainder of the proof requires only arguments already established in (3.10) through (3.16), with (3.16) providing the desired contradiction to (4.6).

If $p > 3^{7.5} > 3787$, then we obtain immediately from Theorems 1 and 3 the following results.

Theorem 4. *Let p be any prime $\not\equiv 1 \pmod{24}$ and let $k = 2$. Then*

$$g(p,k,b,c) < 2^{11/4} b^{5/2} p^{2/5} + 6b^3 p^{1/5} + 2b^2. \tag{4.7}$$

Theorem 5. *Let p be any prime not of the form $x^2 + 27y^2$, x and y integers, and let $k = 3$. Then*

$$g(p,k,b,c) < 2^{11/4} b^{5/2} p^{2/5} + 6b^3 p^{1/5} + 2b^2. \tag{4.8}$$

Theorem 6. *Let $bn + c$ be defined as in Theorem 1 and let T be the coset to which c belongs. Let z be the smallest positive integer such that $bz + c = h(p,k,b,c)$ where $h(p, k, b, c)$ is the smallest integer in the progression $bn + c$ which belongs to a coset other than T. If p is a prime for which $p - 1$ is a kth nonresidue, then*

$$h(p,k,b,c) < 2^{7/4} b^{5/2} p^{2/5} + 3b^3 p^{1/5} + b^2. \tag{4.9}$$

Proof. Assume that Theorem 6 is false and note that we may take $b < p^{1/15}$ since, otherwise, Theorem 6 follows from Corollary 1 of Lemma 1. Let x be the unique integer solution to the congruence $bx \equiv c \pmod{p}$ such that $1 \leq x < p$. Then the interval

$$[x, x+1, \ldots, x+z-1] \tag{4.10}$$

contains z consecutive integers belonging to exactly one of the k cosets, call it T'. Similarly the interval

$$[-x, -x-1, \ldots, -x-z+1] \tag{4.11}$$

contains z consecutive integers belonging to exactly one of the k cosets, call it T''. Note that $T' \neq T''$ since the cosets form a cyclic group mod k and $p-1$ is not in the zero coset.

Analogous to (3.4) and (3.5), $z = (h-c)/b > 2^{7/4}b^{3/2}p^{2/5} + 3b^2p^{1/5}$, and in the interval $(p^{1/5}, \ldots, p^{1/5} - b)$ there is an integer of the form $bn + c$ with $0 \leq n < z$ which we will again denote by s. Of course, s belongs to the coset T.

Numbers of the form

$$as, (a+1)s, \ldots, (a+t-1)s \tag{4.12}$$

belong either to the coset T' or the coset T'' depending on whether we choose J to be the interval (4.10) or the interval (4.11). Consequently, the numbers

$$a, a+1, \ldots, a+t-1 \tag{4.13}$$

are t consecutive numbers belonging to one coset, say U', if J is the interval (4.10) and to another coset, say U'', if J is the interval (4.11). Clearly $U' \neq U''$ since $T' \neq T''$. Now (3.8) and (3.9) carry over unchanged from Theorem 1 and it follows that there exists an integer f such that (3.10) holds. Consequently $(bf+c)^2$, $(b(f+1)+c)^2$, and all other numbers of the form (3.11) belong to exactly one coset, call it T^*, since (3.12), (3.13), (3.14), (3.15), and (3.16) carry over unchanged from Theorem 1 and, consequently, all numbers of the form (3.11) are the product of exactly two integers belonging to the coset T.

Now if $T^* = U'$ we let J be the interval (4.11) and the contradiction follows from the fact that $T^* \neq U''$. If $T^* = U''$ we let J be the interval (4.10) and the contradiction follows since $T^* \neq U'$.

Theorem 7. *Let p, $bn + c$, and $bz + c = h(p,k,b,c)$ be defined as in Theorem 6 and let g_1 be the smallest kth power nonresidue. If p is any prime $> g_1^{7.5}$, then*

$$h(p,k,b,c) < 2^{7/4}b^{5/2}p^{2/5} + 3b^3p^{1/5} + b^2. \tag{4.14}$$

Proof. Assume that Theorem 7 is false. Note that we may assume that $b < p^{1/15}$ since otherwise Theorem 7 follows from Corollary 1 of Lemma 1. Let x be the

unique integer solution to the congruence $bx \equiv c \pmod{p}$ such that $1 \leq x < p$. Then the interval

$$[x, x+1, \ldots, x+z-1] \tag{4.15}$$

contains integers belonging to exactly one coset, call it T'.

Now there exists an integer belonging to the coset T in the interval

$$(p^{1/5}/g_1, \ldots, (p^{1/5}/g_1) + b) \tag{4.16}$$

since this interval contains an integer of the form $bn + c$, $0 \leq n < z$. Let $k = sg_1$ and note that $p^{1/5} < k < p^{1/5} + bg_1 < 2p^{1/5}$.

Consider the multiples of k in the interval (4.15), say

$$ak, (a+1)k, \ldots, (a+t_1-1)k. \tag{4.17}$$

These, of course, all belong to the coset T'. Denote by U' the coset to which

$$a, a+1, \ldots, a+t_1-1 \tag{4.18}$$

belong and note that as in Theorem 3, $a + t_1 - 1 < p^{4/5}/2$ and $t_1 \geq [2^{7/4}b^{3/2}p^{1/5} + 3b^2]$.

Now, in the interval

$$(p^{1/5}, \ldots, p^{1/5} - b) \tag{4.19}$$

there is an integer belonging to the coset T, namely, an integer of the form $bn + c$, $0 < n < z$. Call this integer y and consider the multiples of y in the interval (4.15), say

$$ey, (e+1)y, \ldots, (e+t_2-1)y. \tag{4.20}$$

These integers belong to T', and we denote by U'' the coset to which the integers

$$e, e+1, \ldots, e+t_2-1 \tag{4.21}$$

belong. Note that $t_2 \geqslant [2^{7/4}b^{3/2}p^{1/5} + 3b^2]$ and $e + t_2 - 1 < 2p^{4/5}$ for the identical reasons given in establishing (3.8) and (3.9).

Now there exist integers f_1 and f_2 belonging to coset T such that

$$(bf_1 + c)^2 < a < \cdots < a + t_1 - 1 < (b(f_1+1) + c)^2 \tag{4.22}$$

and, moreover,

$$(bf_2 + c)^2 < e < \cdots < e + t_2 - 1 < (b(f_2+1) + c)^2. \tag{4.23}$$

Subdividing the intervals (4.22) and (4.23) exactly as in Theorem 1 and denoting by T^* the coset to which the product of two numbers in coset T belong

we obtain, as in (3.16), that the maximum number of integers lying between integers belonging to T^* in either of the intervals (4.22) or (4.23) cannot be greater than $2^{7/4}b^{3/2}p^{1/5} + 3b^2$. The contradiction follows, as in Theorem 6, from the fact that U' and U'' are not the same coset and, consequently, cannot both be equal to T^*.

Remark 4. It is, in fact, unnecessary to treat separately the case where b is a kth power nonresidue. For if $b > p^{1/15}$, (4.14) follows from Corollary 1 of Lemma 1 while if $b < p^{1/15}$, then $g_1 < p^{1/15}$ so that $p > g_1^{7.5}$.

5. **Applications to the distribution of prime kth power nonresidues.** In [10] the author noted that the problem of finding an upper bound better than a constant times $p^{1/2}$ for the nth smallest prime kth power nonresidue (by purely elementary methods) appeared to be very difficult if $n > 2$. Bounds for $g_2(p,k)$ have been obtained when $k = 2$ by A. Brauer [3] and C. Whyburn [13] using elementary methods, and by Hua [7] and Erdös and Ko [6] using analytic methods. In [10] the author sharpened the elementary and analytic bounds of the aforementioned authors and extended their results to all k.

We now prove the following theorem.

Theorem 8. *Let $p > g_1^{7.5}$, let $g_n(p,k)$, $n = 1, 2, \ldots$, denote the nth smallest prime kth power nonresidue, and let $Q = \prod_{j=1}^{n-1} g_j(p,k)$. Then*

$$g_n(p,k) < 2^{11/4}Q^{5/2}p^{2/5} + 6Q^3p^{1/5} + 2Q^2. \tag{5.1}$$

If $p - 1$ or Q are kth power nonresidues, then

$$g_n(p,k) < 2^{7/4}Q^{5/2}p^{2/5} + 3Q^3p^{1/5} + Q^2. \tag{5.2}$$

Proof. Consider the arithmetic progression $Qn + 1$, $n = 0, 1, \ldots$. Let z be the smallest positive integer such that $Qz + 1$ is a kth power nonresidue. Then $Qz + 1$ must contain a kth power nonresidue in its prime factorization since any product of kth power residues is a kth power residue. But, clearly, $Qz + 1$ is not divisible by $g_1, g_2, \ldots, g_{n-1}$. If Q or $p - 1$ are kth power nonresidues the result follows immediately from Theorem 1; otherwise it follows from Theorem 3.

The fact, first established by some lengthy arguments of C. Whyburn [13], that $g_2(p,k)$ is bounded by a quadratic polynomial in $p^{1/5}$ if $k = 2$ and $p \not\equiv 1 \pmod{24}$ follows immediately from Theorem 8 (with somewhat weaker coefficients). Of course, Theorem 8 goes a good deal further although, unfortunately, the use of Theorem 8 is limited to special cases where $g_{n-1}(p,k)$ is known to be 'small' relative to p. One of many examples that may be constructed is the following.

Theorem 9. *If $k = 2$ and $p \equiv \pm 53 \pmod{120}$, so that $g_1 = 2$, $g_2 = 3$, and $g_3 = 5$, then*

$$g_4(p,k) < 2^{7/4}(30)^{5/2}p^{2/5} + 3(30)^3p^{1/5} + 900. \tag{5.3}$$

REFERENCES

1. A. Brauer, *Ueber den kleinsten quadratischen Nichtrest*, Math. Z. **33** (1931), 161–176.

2.———, *Ueber die Verteilung der Potenzreste*, Math. Z. **35** (1932), 39–50.

3.———, *On the non existence of the Euclidean algorithm in certain quadratic number fields*, Amer. J. Math. **62** (1941), 697–716. MR **2**, 146.

4. Ezra Brown, *A theorem on biquadratic reciprocity*, Proc. Amer. Math. Soc. **19** (1968), 678–680.

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

6. P. Erdös and Chao Ko, *Note on the Euclidean algorithm*, J. London Math. Soc. **13** (1938), 3–8.

7. L.K. Hua, *On the distribution of quadratic non-residues and the Euclidean algorithm in real quadratic fields*. I, Trans. Amer. Math. Soc. **56** (1944), 537–546. MR **6**, 170.

8. Richard H. Hudson, *On sequences of consecutive quadratic non-residues*, J. Number Theory **3** (1971), 178–181. MR **43** #150.

9.———, *On the distribution of k-th power non-residues*, Duke Math. J. **39** (1972), 85–88.

10.———, *Prime k-th power non-residues*, Acta Arith. **23** (1972), 89–106.

11.———, *On the distribution of k-th power non-residues in the interval* $[1,p^a]$, $2/5 < a \leq 4/9$, J. Reine Angew. Math. **260** (1973), 178–180.

12. C. Stengel, *Über quadratische Nichtreste von der Form* $8h + 1$, J. Reine Angew. Math. **153** (1924), 208–214.

13. C. T. Whyburn, *The second smallest quadratic non-residue*, Duke Math. J. **32** (1965), 519–528. MR **31** #4759.

DEPARTMENT OF MATHEMATICS, DUKE UNIVERSITY, DURHAM, NORTH CAROLINA 27706

Current Address: Department of Mathematics and Computer Science, University of South Carolina, Columbia, South Carolina 29208