[16] T. N. Shorey, *Algebraic independence of certain numbers in p-adic domain*, Indag. Math. 34 (1972), p. 423–435 (Nederl. Akad. Wetensch. Proc. Ser. A 75).
[17] R. Tijdeman, *On the algebraic independence of certain numbers*, Indag. Math. 33 (1971), p. 146–162 (Nederl. Akad. Wetensch. Proc. Ser. A 74).
[18] M. Waldschmidt, *Indépendance algébrique des valeurs de la fonction exponentielle*, Bull. Soc. Math. France 99 (1971), p. 285–304.
[19] — *Solution du huitième problème de Schneider*, J. Number Theory, à paraître.
[20] — *Propriétés arithmétiques de fonctions méromorphes*, C. R. Acad. Sci. Paris, Ser. A 273 (1971), p. 544–547.
[21] A. Weil, *Variétés kählériennes*, Paris 1958.

U. E. R. DE MATHÉMATIQUES ET INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
Talence, France

Reçu le 15. 2. 1972 (255)

ACTA ARITHMETICA
XXIII (1973)

Prime k-th power non-residues

by

RICHARD H. HUDSON (Durham, North Carolina)

1. Introduction and summary. Throughout this paper k will denote an integer $\geqslant 2$ and p will be a prime such that $(k, p-1) = v_k(p) > 1$. We denote the nth prime kth power non-residue by $g_n(p, k)$, $n = 1, 2, \ldots$

We attack the problem of finding an upper bound for $g_2(p, k)$ from several vantage points and we consider, in addition, the case $n > 2$.

A large number of authors have given upper bounds for $g_1(p, k)$ under varying hypotheses.

Burgess [6] has shown that for each $\delta > 0$,

$$g_1(p, 2) = O_\delta(p^{1/(4e^{1/2})+\delta}). \tag{1.1}$$

In order to avoid any misunderstanding regarding the nature of our O-estimates, we will always use the notation O_δ to indicate an implied constant depending at most on δ, while O will indicate an absolute constant.

Wang Yuan [18] generalized the method of Burgess. Namely, for each $\delta > 0$, he has shown that

$$g_1(p, k) = O_\delta(p^{(1/(4e^{v-1/v}))+\delta}) \tag{1.2}$$

for every $v = v_k(p) \geqslant 2$,

$$g_1(p, k) < p^{1/12} \tag{1.3}$$

if $v_k(p) \geqslant 21$, and

$$g_1(p, k) < p^{(\log\log v+2)/4\log v} \tag{1.4}$$

if $v = v_k(p) > e^{33}$.

Wang's results (1.2), (1.3), and (1.4), essentially halve the exponent in the upper bounds for $g_1(p, k)$ given by Buchstab [5] and independently by Davenport and Erdös [8].

K. K. Norton [15] has recently generalized the above results by omitting the restriction that p be prime.

Employing analytic methods, Hua [10] and Erdös and Ko [9], have given upper bounds for $g_2(p, 2)$. In particular, Hua has shown that for each $p \geqslant e^{250}$,

$$g_2(p, 2) < (57600\, p)^{5/16}. \tag{1.5}$$

A. Brauer [2], [4], and C. T. Whyburn [17] have given upper bounds for $g_2(p,2)$ using purely elementary methods. The important advantage in the use of elementary methods, is that the results of Brauer and Whyburn hold for small primes as well as for large primes, an advantage which may well be crucial for a given application. Indeed, this was precisely the case in the application of Brauer's results [2] for $g_2(p,2)$ and $g_3(p,2)$ to the problem of determining which quadratic number fields are Euclidean.

Brauer [2] has shown that the following results hold for all p.

(1.6) If $p \equiv 3 \pmod 8$, $g_2(p,2) < 2p^{2/5}+(49/2)p^{1/5}+7$.

(1.7) If $p \equiv 5 \pmod 8$, $g_2(p,2) < 2^{3/5}p^{2/5}+2^{-6/5}(25)p^{1/5}+3$.

C. Whyburn [17] has extended Brauer's results for $g_2(p,2)$ in the following cases.

(1.8) If $p \equiv 7 \pmod{24}$, $g_2(p,2) < (6p)^{2/5}+(86/3)(6p)^{1/5}+59$.

(1.9) If $p \equiv 17 \pmod{24}$, $g_2(p,2) < (3p)^{2/5}+(91/6)(3p)^{1/5}+29$.

(1.10) If $p \equiv 23 \pmod{24}$, $g_2(p,2) < (10p)^{2/5}+(27/2)(10p)^{1/5}-1$.

Unfortunately, neither Brauer nor Whyburn was able to give a non-trivial upper bound for $g_2(p,2)$ if $p \equiv 1 \pmod 4$ and $g_1(p,2) > 3$, i.e., if $p \equiv 1 \pmod{24}$. Furthermore, to the best of our knowledge, no author has given an upper bound sharper than $O(p^{1/2})$ for $g_2(p,k)$, $v_k(p) > 2$, although it is obvious that $g_2(p,k) \leqslant g_2(p,2)$ if $v_k(p)$ is even.

Let $C(p)$ denote the multiplicative group consisting of the residue classes mod p which are relatively prime to p. $C(p)$ has a proper multiplicative subgroup, $C_k(p)$, consisting of the kth power residues. The remaining $v_k(p)-1$ cosets formed with respect to $C_k(p)$ are called classes of kth power non-residues. Let S_n denote the maximum number of consecutive integers in any of the $v_k(p)-1$ classes of non-residues and let S denote the maximum number of consecutive integers in any of the $v_k(p)$ classes of residues or non-residues.

It follows from a paper of A. Brauer [3], that

$$S < (2p)^{1/2}+2 \tag{1.11}$$

for all p.

The author [11] has given a small improvement of (1.11), namely,

$$S_n < p^{1/2}+2^{2/3}p^{1/3}+2^{1/3}p^{1/6}+1. \tag{1.12}$$

The best upper bound for S has been given by Burgess [7]. Employing non-elementary methods, he has shown that

$$S = O(p^{1/4}\log p) \tag{1.13}$$

where the implied constant is absolute.

Unfortunately, an admissible value for the implied constant in (1.13) is not known, a fact which lends significance to specific estimates for S.

In § 2 some useful lemmas will be established which give an upper bound for $g_n(p,k)$ in terms of S_n and $\prod_{r=1}^{n-1} g_r(p,k)$ if $\prod_{r=1}^{n-1} g_r(p,k)$ is a kth power non-residue, and in terms of S and $\prod_{r=1}^{n-1} g_r(p,k)$ otherwise.

In § 3 we show, by purely elementary methods, that under very general conditions; in fact, whenever $g_1(p,k) < 2p^{1/5}+3$, that

$$g_2(p,k) < 12p^{2/5}+42p^{1/5}+43. \tag{1.14}$$

More generally, we show that for all p,

$$g_2(p,k) < 4p^{7/16}(4.7\log p)^{3/4}+37.6p^{1/4}\log p+1. \tag{1.15}$$

We also show that the sharper result (1.14) holds whenever $v_k(p) \geqslant 13$ and p is larger than a constant which can be made specific. The coefficients in (1.14) and (1.15) can be approximately cut in half if -1 is a kth power residue.

The results in Section 3 are more general and the proofs are simpler than the numerous special results of Brauer and Whyburn, for not only do they extend to all values of k, but they also encompass the difficult case, $p \equiv 1 \pmod{24}$.

In § 4 we turn away from elementary methods and specific estimates and use the O-estimates, (1.2), (1.3), (1.4), and (1.13). Combined with the lemmas established in Section 2 we are able to obtain upper bounds for $g_2(p,k)$ superior to (1.14).

In fact we are able to show that for each $\delta > 0$ and p "sufficiently large",

$$g_2(p,k) = O_\delta(p^{a_v+\delta}), \tag{1.16}$$

where, for example, $a_3 = .378354\ldots$, $a_{21} = 1/3$, and $a_v = 1/4$ for "large" v.

In addition, we show that if p is a "sufficiently large" prime for which $g_1(p,k), \ldots, g_{n-1}(p,k)$ are "small" (in a sense to be made precise later),

$$g_n(p,k) = O(p^{1/4}\log p). \tag{1.17}$$

For example, if $v_k(p) = 2$ and $p \not\equiv \pm 1 \pmod{24}$, or if $v_k(p) = 3$ and $p \neq x^2+27y^2$ so that $g_2(p,k)$ is the smallest odd cubic non-residue, then

$$g_2(p,k) = O(p^{1/4}\log p). \tag{1.18}$$

Similar results are discussed when $n > 2$.

Finally, we note that if any one of several conjectures is true, then (1.16) can be improved. For example, if the extended Riemann hypothesis is true, then for all k and "sufficiently large" p,

$$g_2(p,k) = O(p^{1/4}\log^3 p). \tag{1.19}$$

2. Preliminaries. We often will abbreviate $g_n(p,k)$, by g_n and $v_k(p)$ by v. $[x]$ will denote the greatest integer $\leqslant x$. $(y_1, \ldots, y_n)$ will denote an integer interval which does not include y_1 or y_n; $[y_1, \ldots, y_n]$ will include y_1 and y_n if and only if they are integers. We assume the fact, which is trivial to verify, then $g_2(p,k) < p$ if $p \geqslant 5$.

LEMMA 1. *Let $p \geqslant 5$ be a prime for which $g_1(p,k) = 2$ so that $g_2(p,k)$ is the smallest odd k-th power non-residue, and let S_n denote the maximum number of consecutive integers in any of the $v_k(p)-1$ non-residue classes. Then*

$$g_2(p,k) \leqslant 2S_n+1 \tag{2.1}$$

if -1 is a k-th power non-residue, and

$$g_1(p,k) \leqslant S_n+1 \tag{2.2}$$

if -1 is a k-th power residue.

Proof. The odd integers less than g_2 are kth power residues and, consequently,

$$(p+1)/2,\ (p+3)/2,\ \ldots,\ \big(p+(g_2-2)\big)/2 \tag{2.3}$$

are $(g_2-1)/2$ consecutive integers belonging to precisely one of the $v-1$ classes of kth power non-residues, call it C.

If -1 is a kth power residue, then

$$\big(p-(g_2-2)\big)/2, \ldots, (p-1)/2, (p+1)/2, \ldots, \big(p+(g_2-2)\big)/2 \tag{2.4}$$

are g_2-1 consecutive integers belonging to C.

It follows that if -1 is a kth power non-residue,

$$g_2 \leqslant 2S_n+1, \tag{2.5}$$

since $(g_2-1)/2 \leqslant S_n$. Similarly, if -1 is a kth power residue,

$$g_2 \leqslant S_n+1 \tag{2.6}$$

since $g_2-1 \leqslant S_n$.

Combining (1.11) or (1.12) with (2.5) and (2.6) one obtains immediately an elementary upper bound for $g_2(p,k)$ which may be of some interest for small p, but which will be substantially improved in the next section.

There is clearly nothing magical about the choice $g_1 = 2$ in the above proof and, in fact, Lemma 1 generalizes in the following fashion.

LEMMA 2. *Let $p \geqslant 5$. Then*

$$g_2(p,k) \leqslant g_1 S_n+1 \tag{2.7}$$

if -1 is a k-th power non-residue, and

$$g_2(p,k) \leqslant (g_1/2) S_n+1 \tag{2.8}$$

if -1 is a k-th power residue.

Proof. Let t_1 be the largest positive integer such that $t_1 g_1+1 < g_2$. Then the integers

$$1,\ g_1+1,\ \ldots,\ t_1 g_1+1, \tag{2.9}$$

are kth power residues. Let x be the unique integer solution to the congruence $g_1 x \equiv 1 \pmod p$ such that $1 < x < p$. Then

$$x, x+1, \ldots, x+t_1, \tag{2.10}$$

are t_1+1 consecutive integers belonging to exactly one of the $v-1$ classes of kth power non-residues, call it C'.

Let t_2 be the largest positive integer such that $1-t_2 g_1 > -g_2$. If -1 is a kth power residue,

$$x-t_2,\ \ldots,\ x-1,\ x,\ x+1,\ \ldots,\ x+t_1, \tag{2.11}$$

are t_1+t_2+1 consecutive integers belonging to C'.

It follows that if -1 is a kth power non-residue,

$$g_2 \leqslant (t_1+1) g_1+1 \leqslant g_1(S_n+1), \tag{2.12}$$

since t_1 is the largest integer such that $t_1 g_1+1 < g_2$ and, obviously, $t_1+1 \leqslant S_n$.

Similarly, if -1 is a kth power residue,

$$g_2 \leqslant (g_1/2)(S_n+1) \tag{2.13}$$

since

$$1-(t_2+1)g_1 \leqslant -g_2 \Rightarrow g_2 \leqslant (t_2+1)g_1-1 \Rightarrow 2g_2 \leqslant (t_1+t_2+2)g_1$$
$$\leqslant (S_n+1)(g_1) \Rightarrow g_2 \leqslant (g_1/2)(S_n+1).$$

With some minor additional complications, Lemmas 1 and 2 generalize still further.

LEMMA 3. *Let n be any integer $\geqslant 2$ and let p be any prime. If -1 is a k-th power non-residue, then*

$$g_n \leqslant (S+1)\Big(\prod_{r=1}^{n-1} g_r\Big)+1, \tag{2.14}$$

and if -1 is a k-th power residue,

$$g_n \leqslant S\Big(\prod_{r=1}^{n-1} g_r\Big)+1. \tag{2.15}$$

Proof. Let $Z = \prod_{r=1}^{n-1} g_r$ and let t_1 be the largest non-negative integer such that $t_1 Z+1 < g_n$. Then the integers

$$1,\ Z+1,\ 2Z+1,\ \ldots,\ t_1 Z+1, \tag{2.16}$$

are kth power residues (since their prime factorizations clearly contain only kth power residues) provided that they are not multiples of p. Of course, this additional complication arises only if $g_n > p$.

As before, let x be the unique integer solution to the congruence $Zx \equiv 1 \pmod{p}$ such that $1 < x < p$. This exists since it is clear that $(Z, p) = 1$.

Let p be a prime for which -1 is a kth power non-residue. Then

(2.17) $$x,\ x+1, \ldots,\ x+t_1,$$

with the possible exception of $x+t_1$, are t_1+1 consecutive integers belonging to the same coset. For if $x < p$, then $x+t_1 \leqslant p$ since otherwise the interval $[x, \ldots, x+t_1]$ must contain $p+1$ and $p-1$ which are in different cosets. It follows that $t_1 \leqslant S$, and since t_1 is the largest integer such that $t_1 Z+1 < g_n$,

(2.18) $$g_n \leqslant (t_1+1)Z+1 \leqslant (S+1)Z+1.$$

Let p be a prime for which -1 is a kth power residue and let t_2 be the largest non-negative integer such that $1-t_2 Z > -g_n$. Consider the integers,

(2.19) $$x-t_2,\ \ldots,\ x-1,\ x,\ x+1,\ \ldots,\ x+t_1.$$

If $x-t_2 \leqslant 0$, then clearly $x+t_1 < p$ since all the integers between 1 and p cannot belong to the same coset. It follows that $x, x+1, \ldots, x+t_1$ are t_1+1 consecutive integers belonging to the same coset so that $t_1+1 \leqslant S$.

If $x-t_2 \geqslant 1$, then $x, x-1, \ldots, x-t_2$ are t_2+1 consecutive elements belonging to the same coset so that $t_2+1 \leqslant S$.

Since $g_n \leqslant (t_1+1)Z+1$ and $\leqslant (t_2+1)Z-1$, we obtain

(2.20) $$g_n \leqslant SZ+1.$$

If it is known that $g_n < p$, the above proof simplifies. In fact, the proof is then identical with the proof of Lemma 2 with g_2 replaced by g_n, g_1 replaced by Z, and S_n replaced by S. Consequently, one is able to obtain

(2.21) $$g_n \leqslant \Big(\prod_{r=1}^{n-1} g_r\Big)(S+1)$$

if -1 is a kth power non-residue, and

(2.22) $$g_n \leqslant \Big(\prod_{r=1}^{n-1} g_r\Big)\big((S+1)/2\big)$$

if -1 is a kth power residue.

Also, it is obvious that S may be replaced by S_n in Lemma 3 if $\prod_{r=1}^{n-1} g_r$ is a kth power non-residue.

Remark 1. Some curious results, not of great interest, may be read off from the above lemmas if S, S_n, or g_n are specifically known, or if $v = p^a$, $a \geqslant 3/4$. For example, if $k = 2$ and $p \equiv 13 \pmod{24}$, it follows from (2.2) that $S_n \geqslant 4$, since $g_2 = 5$. $p = 13$ is the only known example of a prime for which $S_n > \sqrt{p}$.

If $v = p^a$, $a > 3/4$, and p is "sufficiently large", then by (1.4), $g_1 < p^\varepsilon$ (for each $\varepsilon > 0$), and it follows trivially from Lemma 2 that $g_2 = O(p^{1/4})$ since the maximum number of integers in any coset (consecutive, or otherwise) is $(p-1)/v = O(p^{1/4})$. Indeed, if $v = p^a$, $a > 8/9$, it follows from Lemmas 2 and 3 that $g_2 = O(p^{1/9})$, $g_3 = O(p^{2/9})$, and $g_4 = O(p^{1/3})$!

3. Specific estimates for $g_2(p, k)$. By a specific estimate for $g_2(p, k)$ we will mean an upper bound for $g_2(p, k)$ which is valid for all p and k, or at least for all $p > p_0$ where p_0 is explicitly stated.

THEOREM 1. *If $g_1(p, k) = 2$ so that $g_2(p, k)$ is the smallest odd k-th power non-residue, then for all $p > 2^{15}$,*

(3.1) $$g_2(p, k) < 2^{3/5} + \big((3125/2048)p\big)^{1/5} + 1$$

if -1 is a k-th power residue;

(3.2) $$g_2(p, k) < 2p^{2/5} + (9/8)p^{1/5} + 1$$

if -1 is a k-th power non-residue.

Proof. Let $p > 32768$. Assume that the theorem is false and let r be an odd integer such that $1 \leqslant r < g_2$. Let J denote the interval

(3.3) $$[p-(g_2-2)/2, \ldots, p+(g_2-2)/2]$$

if -1 is a kth power residue, and

(3.4) $$[(p+1)/2, \ldots, p+(g_2-2)/2]$$

if -1 is a kth power non-residue. It follows that J contains only kth power non-residues (in fact, only integers from one of the $v-1$ classes of non-residues). Let

(3.5) $$dr,\ (d+1)r,\ \ldots,\ (d+f-1)r$$

be the integral multiples of r contained in J. Then the integers

(3.6) $$d,\ d+1,\ \ldots,\ d+f-1$$

are all kth power non-residues.

Let $\varepsilon = 1$ if -1 is a kth power residue and let $\varepsilon = 2$ if -1 is a kth power non-residue. Then $f \geqslant [(g_2-1)/\varepsilon r]$ since the interval J contains $(g_2-1)/\varepsilon$ consecutive integers. Let

(3.7) $$C = [\delta p^{1/5}]$$

where $\delta = 2^{-11/5}$ if -1 is a kth power residue and $\delta = 1/8$ if -1 is a kth power non-residue. Note that $C \geqslant 1$ since $p > 8^5$. Finally, let $r = C$ if C is odd and let $r = C-1$ if C is even.

Now by (1.11), (2.1), and (2.2), $g_2 < 2\sqrt{2p}+5$, and it follows that

$$(3.8)\qquad d+f-1 \leqslant (p+g_2-2)/2r < (p+2\sqrt{2p}+1)/2\delta p^{1/5} < (1/2\delta)p^{4/5}+(2^{1/2}p^{3/10}/\delta)+1 < (g_2-2)^2.$$

Consequently, there exists a positive integer a such that

$$(3.9)\qquad a^2 \leqslant d < d+f-1 < (a+1)^2.$$

For if J is not square free so that there exists an integer a such that $a^2 \in J$, then a is an even integer since $a < g_2-2$, by (3.8), and the square of an odd integer less than g_2 is clearly a kth power residue. But then, $a+1$ and $a-1$ are odd integers less than g_2 and so a^2-1 is a kth power residue. Since J contains only kth power non-residues, we are forced to the conclusion that if $a^2 \in J$, then $a^2 = d$.

Now let t be the largest positive integer such that $(a+1)^2-t^2 > a^2$. Then $2a+1-t^2 > 0$ so that $t < (2a+1)^{1/2} < t+1$ and, hence, $t = [(2a+1)^{1/2}]$.

The integers

$$(3.10)\qquad (a+1)^2-v^2 \quad (v = 0, 1, 2, \ldots, t),$$

divide the interval $[a^2, \ldots, (a+1)^2]$ into subintervals. Furthermore, $a+1+t < g_2$. For

$$(3.11)\qquad a \leqslant d^{1/2} < \big((p+2r)/2r\big)^{1/2} < (p/2r)^{1/2}+1,$$

since there must be a multiple of $2r$ between p and $p+2r$, but then

$$(3.12)\qquad a+1+t < a+1+(2a+1)^{1/2} < a+1+(2a)^{1/2}+1 < p^{2/5}/(2\delta)^{1/2}+(2^{1/4}p^{1/5}/\delta^{1/4})+2 < g_2.$$

Hence, every odd integer of the form (3.9) is a kth power residue. The number of integers lying between two consecutive odd integers of the form (3.10) is given by

$$(3.13)\qquad \big((a+1)^2-v^2\big)-\big((a+1)^2-(v+2)^2\big)+1 = 4v+3.$$

It follows that $f \leqslant 4t+3 \leqslant 4(2a+1)^{1/2}+3 < 4(2a-2)^{1/2}+4$ since it is obvious that $a > 19$ if $p > 2^{15}$.

Now, by (3.9), $(a-1)^{1/2} < (p/2r)^{1/4}$ and so

$$4(2a-2)^{1/2}+4 < 2^{5/2}(p/2r)^{1/4}+4.$$

Thus,

$$(3.14)\qquad \big((g_2-1)/\varepsilon r\big)-1 < f < 2^{5/2}(p/2r)^{1/4}+4.$$

If -1 is a kth power residue we obtain from (3.14),

$$(3.15)\qquad g_2 < 2^{9/4}r^{3/4}p^{1/4}+5r+1 < 2^{9/4}(2^{-11/5}p^{1/5})^{3/4}p^{1/4}+5(2^{-11/5})p^{1/5}+1 = 2^{3/5}p^{2/5}+\big((3125/2048)p\big)^{1/5}+1.$$

If -1 is a kth power non-residue we obtain,

$$(3.16)\qquad g_2 < 2^{21/4}r^{3/4}p^{1/4}+9r+1 < 2^{13/4}(p^{1/5}/8)^{3/4}p^{1/4}+(9/8)p^{1/5}+1 = 2p^{2/5}+(9/8)p^{1/5}+1.$$

The contradiction establishes the theorem.

Remark 2. We have not attempted to check (3.15) and (3.16) for $p < 32768$, although tables exist for checking such things; see, for example, Lehmer, Lehmer, and Shanks [12]. We note that (3.15) and (3.16) are, in fact, slightly sharper than (1.6) and (1.7). More significantly, we note that in the proof of Theorem 1 we only need to use the fact that J does not contain any kth power residues, rather than the stronger fact that J contains integers from only one of the $v-1$ classes of non-residues. Implications of the stronger statement will be considered in forthcoming papers.

THEOREM 2. *If* $2 < g_1(p, k) < 2p^{1/5}+3$, *then*

$$(3.17)\qquad g_2(p, k) < 6p^{2/5}+21p^{1/5}+37/2 \quad \textit{if} \quad -1 \textit{ is a } k\textit{-th power residue};$$

$$(3.18)\qquad g_2(p, k) < 12p^{2/5}+42p^{1/5}+43 \quad \textit{if} \quad -1 \textit{ is a } k\textit{-th power non-residue}.$$

Proof. Let p be > 1024. Assume that the theorem is false and let J denote the interval

$$(3.19)\qquad [p-g_2+1, \ldots, p-1, p+1, \ldots, p+g_2-1]$$

if -1 is a kth power residue, and let J denote the interval

$$(3.20)\qquad [p+1, \ldots, p+g_2-1]$$

if -1 is a kth power non-residue.

If $g_1 < p^{1/5}$ there exists a kth power non-residue, which we will denote by n, such that $p^{1/5} < n < 2p^{1/5}+3$ since 2 is a kth power residue. If $g_1 > p^{1/5}$ we let $n = g_1$.

Let

$$(3.21)\qquad dn,\ (d+1)n,\ \ldots,\ (d+f-1)n,$$

be the integral multiples of n contained in J.

We claim that the integers

$$(3.22)\qquad d,\ d+1, \ldots, d+f-1,$$

form a sequence of f consecutive kth power non-residues. For n is obviously a multiple of g_1, say $n = ag_1$. Furthermore, the only integers in the interval J which can fail to be kth power residues are integers of the form $p \pm bg_1$. But integers of the form $p \pm bg_1$ cannot be multiples of n for $p \pm bg_1 = cn = acg_1 \Rightarrow p = (ac \mp b)g_1$, contradicting the fact that p is prime. Consequently, integers of the form (3.21) are all kth power residues which, of course, implies that integers of the form (3.22) are all kth power non-residues.

Now if -1 is a kth power residue, J contains $2g_2-1$ consecutive integers and, thus, $f \geq [(2g_2-1)/n]$ since any x consecutive integers must contain at least $[x/n]$ multiples of n. If -1 is a kth power non-residue, J contains g_2-1 consecutive integers so that $f \geq [(g_2-1)/n]$.

By (1.11), (2.7), and (2.8), $g_2 < g_1\sqrt{2p}+2g_1+1$. It follows that

$$(3.23)\quad d+f-1 \leq (p+g_2-1)/n < (p+g_1\sqrt{2p}+2g_1)/p^{1/5} < (g_2-2)^2$$

since $g_1 < 2p^{1/5}+3$. Consequently, there exists a positive integer a such that

$$(3.24)\quad a^2 \leq d < d+f-1 < (a+1)^2.$$

For if $a^2 \in [d, \ldots, d+f-1]$, then a must be a multiple of g_1 since, by (3.24), $a < g_2-2$, and the square of an integer less than g_2 which is not a multiple of g_1 is clearly a kth power residue, whereas $d, \ldots, d+f-1$, are all kth power non-residues. But, then, $a+1$ and $a-1$ are integers less than g_2 which are not multiples of g_1 and so a^2-1 is a kth power residue. As in the proof of Theorem 1, we are forced to the conclusion that if $a^2 \in [d, \ldots, d+f-1]$, then $a^2 = d$.

Now subdivide the interval $A = [a^2, \ldots, (a+1)^2]$ into the overlapping subintervals

$$(3.25)\quad A_1 = [a^2, \ldots, a(a+1)],$$

$$(3.26)\quad A_2 = [(a+2)(a-1), \ldots, (a+1)^2].$$

Note that if either $g_1|a$ or $g_1|a+1$, then $g_1 \nmid a+2$ and $g_1 \nmid a-1$ since $g_1 > 2$. Conversely, if either $g_1|a+2$ or $g_1|a-1$, then $g_1 \nmid a$ and $g_1 \nmid a+1$. Consequently, at least one of the integers $(a+2)(a-1) = a^2+a-2$ or $a(a+1) = a^2+a$ is a kth power residue, since $a+2 < g_2$ by (3.23) and (3.24).

Let t_1 be the largest positive integer such that

$$(a+1)^2-t_1^2 > (a+2)(a-1).$$

Then $a+3-t_1^2 > 0$ so $t_1 < (a+3)^{1/2} \leq t_1+1$ and, hence, $t_1 = [(a+2)^{1/2}]$.

The integers

$$(3.27)\quad (a+1)^2-v^2 \quad (v = 0, 1, 2, \ldots, t_1),$$

divide the interval A_2 into subintervals.

Furthermore, $a+1+t_1 < g_2$. For

$$(3.28)\quad a \leq d^{1/2} < \big((p+n)/n\big)^{1/2} < (p/n)^{1/2}+1$$

since there must be a multiple of n between p and $p+2n$. But then

$$(3.29)\quad a+1+t_1 \leq a+1+(a+2)^{1/2} < p^{2/5}+2+(p^{2/5}+3)^{1/2} < g_2.$$

Now, if $(a+1)^2-v^2$ $(v = 0, 1, 2, \ldots, t_1)$, is a kth power non-residue, then at least one of its factors $a+1+v$ or $a+1-v$ must be a kth power non-residue and, hence, a multiple of g_1 because of (3.29). It follows that either $\big(a+1+(v+1)\big)\big(a+1-(v+1)\big)$ is a kth power residue or $\big(a+1+(v+2)\big)\big(a+1-(v+2)\big)$ is a kth power residue. For, if $a+1+v$ is a multiple of g_1, then $a+1+(v+1)$ and $\big(a+1+(v+2)\big)$ clearly are not, since $g_1 > 2$. By (3.29), then, $a+1+(v+1)$ and $a+1+(v+2)$ are kth power residues. But at least one of the integers $a+1-(v+1)$ or $a+1-(v+2)$ must be a kth power residue since both cannot be multiples of g_1. Similarly, if $a+1-v$ is a multiple of g_1, then $a+1-(v+1)$, $a+1-(v+2)$, and at least one of $a+1+(v+1)$ and $a+1+(v+2)$ are kth power residues.

Consequently, at least one of the integers

$$(a+1)^2-v^2,\ (a+1)^2-(v+1)^2,\ \text{or}\ (a+1)^2-(v+2)^2$$

is a kth power residue for each $v = 0, 1, 2, \ldots, t_1-2$. It follows that the maximum number of integers lying between kth power residues of the form (3.27) cannot exceed

$$(3.30)\quad \big((a+1)^2-v^2\big)-\big((a+1)^2-(v+3)^2\big)+1 = 6v+8.$$

Thus, in the interval A_2,

$$(3.31)\quad f \leq 6t_1+8 \leq 6(a+2)^{1/2}+8 < 6(a^{1/2})+10$$

for $(a+1)^2 > p/n > (1024/11) > 93$ since $p > 1024$ and $n < 2p^{1/5}+3$ $\Rightarrow a \geq 9$, but $6(a+2)^{1/2} < 6(a^{1/2})+2$ if $a \geq 9$.

Let t_2 be the largest positive integer such that $a(a+1)-t_2(t_2+1) > a^2$. Then $t_2^2+t_2 < a$ so that $t_2 \leq [a^{1/2}]$. The integers

$$(3.32)\quad a(a+1)-v(v+1) = (a+1+v)(a-v) \quad (v = 0, 1, 2, \ldots, t_2),$$

divide the interval A_1 into subintervals and by the same argument as before, at least one of the integers

$$(a+1+v)(a-v),\ \big(a+1+(v+1)\big)\big(a-(v+1)\big),\ \text{or}\ \big(a+1+(v+2)\big)\big(a-(v+2)\big)$$

is a kth power residue for each $v = 0, 1, 2, \ldots, t_2-2$. It follows that the maximum number of integers lying between kth power residues of the form (3.32) cannot exceed

$$(3.33)\quad \Big(\big(a^2+a-(v^2+v)\big)-\big(a^2+a-(v^2+7v+12)\big)\Big)+1 = 6v+11.$$

Thus in the interval A_1,

(3.34) $$f \leqslant 6t_2+11 \leqslant 6(a^{1/2})+11,$$

and so $f \leqslant 6(a^{1/2})+11$ in the entire interval A.

Now, if -1 is a kth power residue,

(3.35) $$f \geqslant [(2g_2-1)/n] > \big((2g_2-1)/n\big)-1 > \big((2g_2-1)/(2p^{1/5}+3)\big)-1$$

since $n < 2p^{1/5}+3$. Clearly $a^2 < p/n < p^{4/5}$ since $n > p^{1/5}$ so that $a^{1/2} < p^{1/5}$.

It follows that

(3.36) $$(2g_2-1)/(2p^{1/5}+3) < 6(a^{1/2})+12 < 6p^{1/5}+12$$
$$\Rightarrow 2g_2-1 < 6(2p^{1/5}+3)p^{1/5}+12(2p^{1/5}+3) = 12p^{2/5}+42p^{1/5}+36$$
$$\Rightarrow g_2 < 6p^{2/5}+21p^{1/5}+37/2.$$

The contradiction establishes (3.17) for $p > 1024$. If $p < 1024$, $g_1 \leqslant 7$ since $g_1 < 2p^{1/5}+3 < 11$ so by (1.11) and (2.8),

$$g_2 < (7/2)\sqrt{2p}+8 < 6p^{2/5}+21p^{1/5}+37/2.$$

If -1 is a kth power non-residue,

(3.37) $$f \geqslant [(g_2-1)/n] > \big((g_2-1)/n\big)-1 > \big((g_2-1)/(2p^{1/5}+3)\big)-1.$$

Clearly $(a-1)^2 < p/n < p^{4/5}$ so that $(a-1)^{1/2} < p^{1/5}$. Furthermore,

$$6(a^{1/2})+11 < 6(a-1)^{1/2}+13 < 6p^{1/5}+13 \quad \text{since} \quad a > 9.$$

It follows that

(3.38) $$(g_2-1)/(2p^{1/5}+3) < 6p^{1/5}+14 \Rightarrow g_2 < 12p^{2/5}+42p^{1/5}+43.$$

The contradiction establishes (3.18) for $p > 1024$. If $p < 1024$, $g_1 \leqslant 7$, so by (1.11) and (2.7),

$$g_2 < 7\sqrt{2p}+15 < 12p^{2/5}+42p^{1/5}+43.$$

Theorem 2 generalizes Whyburn's results (1.8), (1.9), and (1.10), even when $v = 2$. For if $g_1(p, 2) > 3$, Whyburn was only able to obtain a non-trivial upper bound for $g_2(p, 2)$ if -1 is a quadratic non-residue. Consequently, Theorem 2 is more general than (1.8), (1.9), and (1.10), even when $v = 2$. Theorem 3, combined with a remarkable specific estimate given recently by K. K. Norton [15] for $g_1(p, k)$, namely,

(3.39) $$g_1(p, k) < 4.7p^{1/4}\log p,$$

will yield a non-trivial upper bound for $g_2(p, k)$ for all p and k. We omit details in the proof of Theorem 3 which are identical with arguments already established in the proof of Theorem 2.

THEOREM 3. *If* $g_1(p, k) > 2p^{1/5}+3$, *then*

(3.40) $$g_2(p, k) < 2g_1^{3/4}p^{1/4}+3g_1+1/2$$

if -1 *is a k-th power residue:*

(3.41) $$g_2(p, k) < 4g_1^{3/4}p^{1/4}+8g_1+1$$

if -1 *is a k-th power non-residue.*

Proof. Let p be $\geqslant 257$. Assume that the theorem is false and let J be defined as in Theorem 2. Let

(3.42) $$dg_1,\ (d+1)g_1,\ \ldots,\ (d+f-1)g_1$$

be the integral multiples of g_1 contained in J.

By the same reasoning that was used in the proof of Theorem 2 the integers

(3.43) $$d,\ d+1,\ \ldots,\ d+f-1$$

form a sequence of f consecutive kth power non-residues.

Also, of course, $f \geqslant [(2g_2-1)/g_1]$ if -1 is a kth power residue, and $f \geqslant [(g_2-1)/g_1]$ if -1 is a kth power non-residue.

As before, $g_2 < g_1\sqrt{2p}+2g_1+1$ implies that

(3.44) $$d+f-1 \leqslant (p+g_2-1)/g_1 < (p+g_1\sqrt{2p}+2g_1)/2p^{1/5} < (g_2-2)^2$$

since it is well known that $g_1 < p^{1/2}$, and so there exists a positive integer a such that

(3.45) $$a^2 \leqslant d < d+f-1 < (a+1)^2.$$

Define t_1, t_2, the interval A, and the subintervals A_1 and A_2 as in Theorem 2. Recall that $t_1 = [(a+2)^{1/2}]$ and that $t_2 \leqslant [a^{1/2}]$. It is easy to verify that $a+1+t_1 < g_2$ and so, of course, $a+1+t_2 < g_2$.

However, a new and useful fact is available to us if $g_1 > 2p^{1/5}+3$. Namely, we claim that

(3.46) $$2[(a+2)^{1/2}]+1 < g_1 \quad \text{and} \quad 2[a^{1/2}]+2 < g_1.$$

For if $p > 512$,

(3.47) $$(a-1)^2 < p/g_1 \Rightarrow a-1 < (p/2p^{1/5})^{1/2} \Rightarrow a+2 < (p^{2/5}/2^{1/2})+3$$
$$\Rightarrow 2(a+2)^{1/2}+2 < 2\big((p^{2/5}/2^{1/2})+3\big)^{1/2}+2 < 2^{3/4}p^{1/5}+7/2 < g_1$$

since

$$\big((p^{2/5}/2^{1/2})+3\big)^{1/2} < (p^{1/5}/2^{1/4})+3/4 \quad \text{if} \quad p \geqslant 257.$$

Clearly (3.46) follows from (3.47).

Subdivide the interval A_2 by the integers

(3.48) $$(a+1)^2-v^2 \quad (v = 0, 1, \ldots, t_1).$$

As before, $(a+1)^2-v^2$ can only be a kth power non-residue if at least one of its factors $a+1+v$ or $a+1-v$ is a multiple of g_1. Unlike before, if either $a+1+v$ or $a+1-v$ is a multiple of g_1, then, by using (3.46), we can show that neither $a+1+(v+1)$ nor $a+1-(v+1)$ can be multiples of g_1.

For if $a+1+v$ is a multiple of g_1, then $(a+1+v)-\big(a+1-(v+1)\big) = 2v+1 \leqslant 2t_1+1 = [(a+2)^{1/2}]+1 < g_1$, by (3.46), and so $a+1-(v+1)$ cannot be a multiple of g_1. Obviously $a+1+(v+1)$ is not a multiple of g_1 either. Similarly if $a+1-v$ is a multiple of g_1, then $a+1+(v+1)-(a+1-v) = 2v+1 < g_1$ so that $a+1+(v+1)$ is not a multiple of g_1 and, of course, $a+1-(v+1)$ cannot be either. It follows that at least every other (rather than every third) integer of the form $(a+1)^2-v^2$ $(v = 0, 1, 2, \ldots, t_1)$ is a kth power residue. Consequently, the maximum number of integers lying between kth power residues of the form (3.48) cannot exceed

(3.49) $$\big((a+1)^2-v^2\big)-\big((a+1)^2-(v+2)^2\big)+1 = 4v+3.$$

Thus, in the interval A_2,

(3.50) $$f \leqslant 4t_1+3 \leqslant 4(a+2)^{1/2}+3 < 4(a^{1/2})+5,$$

for $a+1 > (p/g_1)^{1/2} \Rightarrow a+1 > p^{1/4}$ (since it is well known that $g_1 < p^{1/2}$) $\Rightarrow a \geqslant 4$ since $p \geqslant 257$.

Subdivide the interval A_1 by the integers

(3.51) $$a(a+1)-v(v+1) = (a+1+v)(a-v) \qquad (v = 0, 1, 2, \ldots, t_2).$$

Analogous to the previous argument we can show, using (3.46), that if either of the factors $a+1+v$ or $a-v$ is a multiple of g_1, then neither of the factors $\big(a+1+(v+1)\big)$ nor $\big(a-(v+1)\big)$ can be multiples of g_1.

For if $a+1+v$ is a multiple of g_1, then $(a+1+v)-\big(a-(v+1)\big) = 2v+2 \leqslant 2t_2+2 \leqslant 2[a^{1/2}]+2 < g_1$, by (3.46). Similarly, if $a-v$ is a multiple of g_1, then $\big(a+1+(v+1)\big)-(a-v) = 2v+2 < g_1$.

It follows that the maximum number of integers lying between kth power residues of the form (3.51) cannot exceed

(3.52) $$\big(a^2+a-(v^2+v)\big)-\big(a^2+a-(v^2+5v+6)\big)+1 = 4v+5.$$

Thus, in the interval A_1,

(3.53) $$f \leqslant 4t_2+5 \leqslant 4(a)^{1/2}+5,$$

and so $f \leqslant 4(a^{1/2})+5$ in the entire interval A.

Now, if -1 is a kth power residue,

(3.54) $$f \geqslant [(2g_2-1)/g_1] > \big((2g_2-1)/g_1\big)-1.$$

Also

$$a^2 < p/g_1 \Rightarrow a^{1/2} < (p/g_1)^{1/4}.$$

It follows that

(3.55) $$(2g_2-1)/g_1 < 4(a^{1/2})+6 \Rightarrow 2g_2-1 < 4g_1^{3/4}p^{1/4}+6g_1$$
$$\Rightarrow g_2 < 2g_1^{3/4}p^{1/4}+3g_1+1/2.$$

The contradiction establishes (3.40) for $p > 257$. If $p < 257$, Theorem 3 is vacuously true since g_1 is never greater than $2p^{1/5}+3$. For if $p < 31$, then $g_1 < p^{1/2}$ so that $g_1 \leqslant 5$, but $2p^{1/5}+3 > 5$. If $37 \leqslant p \leqslant 257$, $2p^{1/5}+3 > 7$, but it is easily checked that $g_1 \leqslant 7$ using, e.g., Nagell [14] and well known bounds for $g_1(p, 2)$.

If -1 is a kth power non-residue,

(3.56) $$f \geqslant [(g_2-1)/g_1] > \big((g_2-1)/g_1\big)-1.$$

Furthermore,

$$(a-1)^2 < p/g_1 \Rightarrow (a-1)^{1/2} < (p/g_1)^{1/4}.$$

Now

$$4(a^{1/2})+5 < 4(a-1)^{1/2}+7 \quad \text{since} \quad a \geqslant 4.$$

It follows that

(3.57) $$(g_2-1)/g_1 < 4(a-1)^{1/2}+8 \Rightarrow g_2 < 4g_1^{3/4}p^{1/4}+8g_1+1.$$

The contradiction establishes (3.41) for $p > 257$ and, as noted, the theorem holds vacuously if $p < 257$.

COROLLARY 1. *For every $k \geqslant 2$ and every p such that $(k, p-1) > 1$,*

(3.58) $$g_2(p, k) < 2p^{7/16}(3.9\log p)^{3/4}+11.7p^{1/4}\log p+1/2$$

if -1 is a k-th power residue, and

(3.59) $$g_2(p, k) < 4p^{7/16}(4.7\log p)^{3/4}+37.6p^{1/4}\log p+1$$

if -1 is a k-th power non-residue.

Proof. Noting that Norton [15] has shown that the coefficient 4.7 in (3.39) can be replaced by 3.9 if -1 is a kth power residue, the proof follows immediately from (3.39), (3.40), and (3.41), together with Theorems 1 and 2.

Remark 3. Norton [15] has also given the specific estimate

(3.60) $$g_1(p, k) < (p^{1/2}\log p)^B$$

where

$$B = \exp\{-1+v^{-1}+6/\log p+20/\log^2 p\}.$$

(3.60) is sharper than (3.39) if $v > 3$ and p is larger than a calculable constant c (depending on v). Correspondingly, Corollary 1 can be improved if $v > 3$. In fact, it follows from (3.60) that if $v = v_k(p) \geqslant 13$ and $p > e^{4440}$, then $g_1(p, k) < p^{1/5}$ and, consequently, $g_2(p, k)$ is bounded by the quadratic polynomials in $p^{1/5}$, (3.17) and (3.18).

Remark 4. Although, in theory, elementary methods similar to those used in Theorems 1, 2, and 3 are applicable to g_n, $n > 2$, the additional complications, even for g_3, are overwhelming.

We remark that it follows immediately from an elementary result of Rédei ([16], p. 151) that for each integer $n \geq 1$ there exists an integer m such that for every "sufficiently large" prime p with $g_1(p, 2) > m$, $g_n(p, 2) < 2\sqrt{p}/\sqrt{3}$. In fact, $g_n(p, 2) < 2\sqrt{p}/\sqrt{3}$ for every "sufficiently large" prime p in the arithmetic progression $ax+b$ where $a = 4\cdot 2\cdot 3\cdot 5\cdot 7\cdot 11\cdots m$ and $b = 1$ since for every prime in this progression, $g_1(p, 2) > m$. There are, of course, infinitely many such primes since $(a, b) = 1$. Unfortunately, however, this still leaves us a long way from showing that $g_n(p, 2) < 2\sqrt{p}/\sqrt{3}$ for every "sufficiently large" prime. In the next section we turn away from elementary methods, and we see that $g_n(p, k) = O(p^{1/4}\log p)$ for all "sufficiently large" p for which $g_1, \ldots, g_{n-1}$ assume preassigned values.

4. O-estimates. It follows from Wang's result (1.2), and Theorems 1 and 2, that for each $v \geq 2$ and all "sufficiently large" p,

$$g_2(p, k) < 6p^{2/5} + 21p^{1/5} + 37/2 \tag{4.1}$$

if -1 is a kth power residue;

$$g_2(p, k) < 12p^{2/5} + 42p^{1/5} + 43 \tag{4.2}$$

if -1 is a kth power non-residue.

Our purpose in this section is to improve (4.1), (4.2), for "large" p through the use of the lemmas in Section 2, Burgess's result (1.13), and Wang's results (1.2), (1.3), and (1.4).

Theorem 4. *Let* $a_v = 1/4 + 1/(4e^{v-1/v})$, $v \geq 2$. *Then, for each* $\delta > 0$,

$$g_2(p, k) = O_\delta(p^{a_v+\delta}) \quad \textit{if} \quad v \geq 2; \tag{4.3}$$

$$g_2(p, k) = O_\delta(p^{1/3+\delta}) \quad \textit{if} \quad v \geq 21; \tag{4.4}$$

$$g_2(p, k) = O_\delta(p^{1/4+((\log\log v+2)/4\log v)+\delta}) \quad \textit{if} \quad v > e^{33}. \tag{4.5}$$

Proof. Immediate from (1.2), (1.3), (1.4), (1.13), and Lemma 2; $\log p$ in (1.13) is, of course, swallowed up by p^δ since $\log p = o(p^\delta)$.

Computing several values of a_v, we obtain,

$$a_3 = .378354\ldots,$$
$$a_5 = .362332\ldots,$$
$$a_7 = .356093\ldots,$$
$$\cdots\cdots\cdots\cdots$$
$$a_{19} = .346940\ldots$$

If $v > e^{33}$, $(\log\log v+2)/4\log v < .04164$ so that

$$g_2(p, k) = O_\delta(p^{b_v+\delta}) \tag{4.6}$$

where $b_v = 1/4 + (\log\log v+2)/4\log v < .29164$.

In fact, replacing δ by $\delta/2$ in (4.5), and noting that there exists a $v_0 > e^{33}$ such that $(\log\log v_0+2)/4\log v_0 < \delta/2$, we immediately obtain the following theorem for "large" v.

Theorem 5. *Let v_1 be any integer $\geq v_0$. Then for all "sufficiently large" p with $(k, p-1) = v_1$,*

$$g_2(p, k) = O_\delta(p^{1/4+\delta}) \quad \textit{for each } \delta > 0. \tag{4.7}$$

The following theorem is very useful when $g_{n-1}(p, k)$, $n \geq 2$, is small and an upper bound for $g_n(p, k)$ is sought.

Theorem 6. *Let b be a positive integer ≥ 2. Then there exists p_0 such that if p is any prime $\geq p_0$ for which $g_{n-1}(p, k) = b$,*

$$g_n(p, k) = O(p^{1/4}\log p). \tag{4.8}$$

Proof. Immediate from (1.13) and Lemma 3.

Some illustrative applications of Theorem 6 are given below.

If $v_k(p) = 2$, then

$$g_2(p, k) = O(p^{1/4}\log p) \quad \text{if} \quad p \not\equiv \pm 1 \pmod{24} \quad \text{since } g_1 \leq 5, \tag{4.9}$$

$$g_3(p, k) = O(p^{1/4}\log p) \quad \text{if} \quad p \equiv \pm 5 \pmod{24} \quad \text{since } g_2 = 3; \tag{4.10}$$

if $v_k(p) = 3$ and $p \neq x^2+27y^2$, then

$$g_2(p, k) = O(p^{1/4}\log p), \tag{4.11}$$

since $g_1 = 2$, etc.

Remark 5. K. K. Norton ([15], p. 26) suggested that the method used in obtaining the specific estimate (3.39) may generalize to yield an admissible value for the implied absolute constant in (1.13). Obviously, this would give fresh significance to Theorem 6 since examples of the type (4.9), (4.10), and (4.11) would become specific estimates.

Finally, we note that a number of conditional results for $g_1(p, k)$ sharper than (1.2), (1.3), and (1.4) have been given, and because of the nature of Lemma 2, these obviously lead to conditional improvements of Theorem 4. For example, Linnik [13] has given a specific function $f(\varepsilon)$ such that for each $\varepsilon > 0$ and all sufficiently large N, there are at most $f(\varepsilon)$ primes p in the interval $[N^\varepsilon, N]$ for which $g_1(p, 2) > p^\varepsilon$. Ankeny [1] has shown that, conditional on the truth of the extended Riemann hypothesis, $g_1(p, 2) = O(\log^2 p)$.

Lemma 2 combined with Ankeny's result yields the following conditional result.

THEOREM 7. *If the extended Riemann hypothesis is true, then for all p and k,*

$$g_2(p, k) = O(p^{1/4}\log^3 p). \tag{4.12}$$

References

[1] N. C. Ankeny, *The least quadratic non-residue*, Ann. of Math. 55 (1952), pp. 65–72.

[2] A. Brauer, *Ueber den kleinsten quadratischen Nichtrest*, Math. Zeitschr. 33 (1931), pp. 161–176.

[3] — *Ueber die Verteilung der Potenzreste*, Math. Zeitschr. 35 (1932), pp. 39–50.

[4] — *On the non-existence of the Euclidean algorithm in certain quadratic number fields*, Amer. J. Math. 62 (1941), pp. 697–716.

[5] A. A. Buchstab, *On those numbers in an arithmetic progression all prime factors of which are small in order of magnitude*, Dokl. Akad. Nauk SSSR (N. S.) 67 (1949), pp. 5–8.

[6] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), pp. 106–112.

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

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

[9] P. Erdös and C. Ko, *Note on the Euclidean algorithm*, J. London Math. Soc. 13 (1938), pp. 3–8.

[10] 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), pp. 537–546.

[11] R. H. Hudson, *On the distribution of k-th power non-residues*, Duke Math. J. 39 (1971), pp. 85–88.

[12] D. H. Lehmer, Emma Lehmer, and Daniel Shanks, *Integer sequences having prescribed quadratic character*, Math. Comp. 24 (1970), pp. 433–451.

[13] Yu. V. Linnik, *A remark on the least quadratic non-residue*, C. R. (Dokl.) Acad. Sci. USSR (N. S.) 36 (1942), pp. 119–120.

[14] T. Nagell, *Den minste positive n^{te} ikke-potensreste modulo p*, Norsk Mat. Tidsskr. 34 (1952), p. 13.

[15] K. K. Norton, *Numbers with small prime factors, and the least k-th power non-residue*, Mem. Amer. Math. Soc. (1971), # 106.

[16] L. Rédei, *Ueber die Anzahl der Potenzreste* mod p *in Interval* $1, \sqrt{p}$, Nieuw Archief 23 (1950), pp. 150–162.

[17] C. T. Whyburn, *The second smallest quadratic non-residue*, Duke Math. J. 32 (1965), pp. 519–528.

[18] Yuan Wang, *Estimation and application of character sums*, Shuxue Jinzhan 7 (1964), pp. 78–83.

Received on 20. 3. 1972 (265)