On The Least K-th Power Non-Residue

RICHARD H. HUDSON

University of South Carolina, U.S.A.

Abstract

Let $C_k(p)$ denote the group of the k-th powers (mod p), p a prime with $(k, p-1) > 1$. A new elementary result for the least k-th power non-residue is given and the result is applied to finding a new elementary bound for the maximum number of consecutive integers in any coset of $C_k(p)$.

1. Introduction

Throughout this paper k will be an integer ≥ 2 and p a prime with $(k, p-1) > 1$. Let $C_k(p)$ denote the group of k-th powers (mod p) and let S be the maximum number of consecutive integers in any coset of $C_k(p)$. Finally, let $g(p, k)$ denote the least positive k-th power non-residue.

Vinogradov [12], A. Brauer [2], Davenport and Erdös [5], Rédei [10], Burgess [4], and the author [6], [7], have given estimates for S. In particular, Vinogradov [12] showed that there exists at least one quadratic non-residue in each set of $3[p^{1/2}] - 1$ consecutive integers (mod p).

A. Brauer [2], using purely elementary arguments, showed that for every p and k,

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

Using deep and non-elementary algebraic arguments, Burgess [4] showed that $S = O(p^{1/4} \log p)$, an enormously stronger result than has been obtained using elementary methods alone.

The major contribution of this paper is to give a small improvement of the elementary upper bounds of Brauer and Reynolds [3], Skolem [11], Nagell [9], and Rédei [10], for $g(p, k)$. Namely, we show that

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

for all p except $p = 23$ and $p = 71$. While much stronger results are known using analytic methods, the proof of (1.2) for each prime p for which -1 is a k-th power residue is not only elementary, but synthetic, and possibly even simple enough to be included in a textbook on elementary number theory.

We also note that (1.2) can be used to improve (1.1), for the author has given a purely elementary argument in [7] that

$$S < \max\{p^{1/2} + (3/4)2^{1/2}p^{1/4} + 2, (1/2)(g(p, k) + (g(p, k)^2 + 4p)^{1/2})\}. \tag{1.3}$$

From (1.2) and (1.3) it follows that

$$S < ((\sqrt{13} + 1)/2\sqrt{3})p^{1/2} + (p/3)^{1/4} + 2 \cong 1.3295\, p^{1/2} + (p/3)^{1/4} + 2. \tag{1.4}$$

Results such as (1.2) and (1.4) are of interest almost solely for the method by which they are obtained. However, they have additional interest for small primes where results such as Burgess's may be un-informative.

2. The proof of (1.2) and (1.4)

THEOREM 1. For each $k \geq 2$ and $p \neq 23$ or 71, $g(p, k) < (p/3)^{1/2} + 2$.

Proof. Henceforth, for simplicity, we denote $g(p, k)$ by g. Let p be a prime for which -1 is a k-th power residue and assume that $g > (p/3)^{1/2} + 2$ so that $g > 3$. Then each integer I, such that $(p - g)/3 < I < (p + g)/3$, is a k-th power residue. Further, each odd integer J satisfying either of the following inequalities is a k-th power residue.

$$(p - 2g)/3 < J < (p - g)/3. \tag{2.1}$$

$$(p + g)/3 < J < (p + 2g)/3. \tag{2.2}$$

For if, (2.1) holds, then the positive integer $(p - 3J)/2$ is less than g, and since -1, 2, and 3 are k-th power residues, it follows that J is a k-th power residue. Likewise, if (2.2) holds, J is a k-th power residue since, then, $(3J - p)/2$ is a positive integer less than g.

Now the number of integers in the closed integer interval $A = [(p - 2g)/3, (p + 2g)/3]$ exceeds g and, consequently, A must contain a multiple of g, say ag. Note that $a > 0$ for obviously $g < p/2$. Now

$$a < (p/3)^{1/2} + 1 < g - 1. \tag{2.3}$$

For if $a > (p/3)^{1/2} + 1$, then

$$ag > ((p/3)^{1/2} + 1)((p/3)^{1/2} + 2) = p/3 + (3p)^{1/2} + 2 > (p + 2g)/3 \tag{2.4}$$

since it is well known that $g < p^{1/2}$. (See, for example, Western and Miller [13, pp. xi—xii]). Thus a and $a+1$ are k-th power residues. Now $ag \neq (p-bg)/3$, $b = \pm 1, \pm 2$, for $ag = (p-bg)/3 \Rightarrow p = (3a+b)g$, but p is prime. Hence, ag is an even integer lying either in the interval (2.1) or in the interval (2.2). For ag is a k-th power non-residue since $a < g-1$ and, consequently, cannot be an integer in the interval $[(p-g)/3, (p+g)/3]$, nor can it be an odd integer in either of the intervals (2.1) or (2.2). If ag lies in the interval (2.1) note that $(a+1)g$ is an odd non-residue in the interval (2.2), a contradiction. If ag lies in the interval (2.2), then $(a-1)g$ is an odd non-residue in the interval (2.1), again, a contradiction. We conclude that $g < (p/3)^{1/2} + 2$ if -1 is a k-th power residue.

If -1 is a k-th power non-residue it follows from [1] that

$$g(p,k) < (2p)^{2/5} + 3(2p)^{1/5} + 1. \tag{2.5}$$

It is easy to see that $(2p)^{2/5} + 3\,(2p)^{1/5} + 1 < (p/3)^{1/2} + 2$ for $p > 10^5$ and it can be verified from existing tables, (see, for example, D. H. Lehmer, Emma Lehmer, and Daniel Shanks [8]), that $g < (p/3)^{1/2} + 2$ for $71 < p < 10^5$.

THEOREM 2. $S < ((\sqrt{13}+1)/2\sqrt{3})p^{1/2} + (p/3)^{1/4} + 2$.

Proof. The result is easily checked if $p \leq 71$.

If $p > 71$ we see from Theorem 1 that

$$\begin{aligned}(1/2)(g + (g^2+4p)^{1/2}) &< (1/2)((p/3)^{1/2} + 2 + (13p/3 + 4(p/3)^{1/2} + 4)^{1/2}) \\ &< (1/2)((p/3)^{1/2} + 2 + (13p/3)^{1/2} + 2(p/3)^{1/4} + 2) \qquad (2.6) \\ &= ((\sqrt{13}+1)/2\sqrt{3})p^{1/2} + (p/3)^{1/4} + 2 \cong 1.3295\sqrt{p} + (p/3)^{1/4} + 2,\end{aligned}$$

and the result follows from (1.3).

References

1. BRAUER, A., Über den kleinsten quadratischen Nichtrest, *Math. Z.* 33 (1931), 161—176.
2. —»— Über die Verteilung der Potenzreste, *Math. Z.* 35 (1932), 39—50.
3. BRAUER, A. and REYNOLDS, T. L., On a theorem of Aubrey-Thue, *Canad. J. Math.* 3 (1951), 367—374.
4. BURGESS, D. A., A note on the distribution of residues and non-residues, *J. London Math. Soc.* 38 (1963), 253-256.
5. DAVENPORT, H. and ERDÖS, P., The distribution of quadratic and higher residues, *Publ. Math. Debrecen* 2 (1952), 252—265.
6. HUDSON, R. H., On sequences of consecutive quadratic non-residues, *J. Number Theory* 3 (1971), 178—181.
7. —»— On the distribution of k-th power non-residues, *Duke J.* 39 (1972), 85—88.
8. LEHMER, D. H., LEHMER, E. and SHANKS, D., Integer sequences having prescribed quadratic character, *Math. Comp.* 24 (1970), 433—451.

9. NAGELL, T., Den minste positive n^{te} ikke-potensrest modulo p, *Norsk Mat. Tidsskr.* 34 (1952), p. 13.
10. RÉDEI, L., Die Existenz eines Ungeraden quadratischen Nichtrestes mod p im Interval $1, \sqrt{p}$, *Acta Sci. Math. (Szeged)* 15 (1953), 12—19.
11. SKOLEM, T., Eksistens av en n^{te} ikke-potensrest (mod p) mindre enn $\sqrt{p}$, *Norsk Mat. Tidsskr.* 33 (1951), 123—126.
12. VINOGRADOV, I. M., *Elements of number theory*, Dover Publications, Inc., 1954.
13. WESTERN, A. E. and MILLER, J. C. P., Tables of indices and primitive roots, *Royal Soc. Math. Tables* Vol. 9, Cambridge, 1968.

Received May 26, 1972

Richard H. Hudson
University of South Carolina
U.S.A.