On the least quadratic non-residue of a prime $p \equiv 3 \pmod 4$

By *Richard H. Hudson* at Columbia and *Kenneth S. Williams**) at Ottawa

Dedicated to Alfred Brauer on his 86th birthday

1. Introduction and summary

The problem of finding an upper bound for the least quadratic non-residue of an odd prime p is of historical interest because of a remark of Gauss [7] (see, for example, [3], p. 27), regarding its difficulty. Upper bounds of the order of $p^{\frac{1}{2}}$ have been given by numerous authors including Vinogradov [21], Brauer and Reynolds [4], Kanold [13], Nagell [14], [15], [16], [17], Rédei [18], Skolem [19], and Hudson [10].

The well-known method of Vinogradov [20], used in conjunction with the character sum estimates of Burgess [5], [6], yields a sharp bound for the least quadratic non-residue of "sufficiently large" primes. Only one author, Brauer [1], has exhibited a purely combinatorial method for bounding the least quadratic non-residue of a prime which yields a bound that is $o(p^{\frac{1}{2}})$. In 1931, Brauer [1] showed that the smallest positive quadratic non-residue q of an odd prime $\not\equiv 1 \pmod 8$ must satisfy

$$q < (2p)^{\frac{2}{5}} + 3(2p)^{\frac{1}{5}} + 1 \approx 1.3195\, p^{\frac{2}{5}} + 3.446\, p^{\frac{1}{5}} + 1. \tag{1. 1}$$

Using this method, Brauer [2], Whyburn [22], and Hudson [8], were able to obtain bounds for the second and third smallest prime k-th power non-residues in certain cases, and this method was used by Hudson [9], [11], [12] in related problems, for example, in providing upper bounds for the first three consecutive quadratic residues of a prime $p > 17$ and for the least k-th power non-residue $(\operatorname{mod} p)$ in an arithmetic progression.

Brauer informs us that several authors (unpublished) have been able to obtain slight improvements in the coefficient of $p^{\frac{1}{5}}$ in (1. 1), with easy refinements of his proof. This is, of course, not of great interest as it does not appreciably improve Brauer's bound for large p. In his classes, for more than 40 years, Brauer gave the proof of (1. 1) and challenged his students to improve this bound. In this paper we give a method which yields a small improvement (approximately 24%). In particular, we prove in section 2, that if q is the least positive quadratic non-residue of an odd prime $\not\equiv 1 \pmod 8$, then

$$q < p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33. \tag{1. 2}$$

*) Research supported by Grant A-7233 of the Natural Sciences and Engineering Research Council Canada.

0075-4102/80/0318-0007\$02.00

(At the cost of complicating the proof, the coefficients 12 and 33 in (1. 2) can be improved slightly.)

We expect that many of the aforementioned results which depend on Brauer's method can be similarly improved using (essentially) the simple technique given in section 2.

2. A bound for the least non-residue of odd primes $p \not\equiv 1 \pmod 8$

Theorem. *Let p be an odd prime* $\not\equiv 1 \pmod 8$ *and let q denote the least quadratic non-residue of p. Then*

(2. 1) $$q < p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33.$$

Proof. Assume otherwise, so that

(2. 2) $$q > p^{\frac{2}{5}} + 12p^{\frac{1}{5}} + 33.$$

Since $q > 2$ we may take p to be $\equiv 7 \pmod 8$. Also (2. 2) implies that $p > 71$. Now 8 is a quadratic residue and -1 is a quadratic non-residue of p, so that the $q-1$ positive integers

(2. 3) $$p-8(q-1),\ p-8(q-2), \ldots, p-8$$

are quadratic non-residues $\equiv 7 \pmod 8$. (The integers in (2. 3) are positive since

$$q < p^{\frac{1}{2}} \quad \text{if} \quad p > 23,$$

see [3], p. 27.)

Let r be an odd positive integer of the form

(2. 4) $$r = [p^{\frac{1}{5}}] + \alpha,$$

where α is a positive integer $\leqq 8$ to be chosen later.

Since

(2. 5) $$p^{\frac{1}{5}} < r \leqq p^{\frac{1}{5}} + 8,$$

we must have

(2. 6) $$r \leqq q-1$$

in view of (2. 2).

Let h be the unique integer satisfying

(2. 7) $$8h \equiv 8q - p \pmod r,\ 1 \leqq h \leqq r.$$

By (2. 7), we may define an integer k by

(2. 8) $$k = \frac{p-8(q-h)}{r}.$$

From (2. 6) and (2. 7), we have $1 \leqq h \leqq q-1$, so that the numerator in (2. 8) is one of the integers in (2. 3), and so k is positive.

Now, set $l = [p^{\frac{1}{5}}] + 4$ so that

(2. 9) $$p^{\frac{1}{5}} + 3 < l < p^{\frac{1}{5}} + 4.$$

Further, choose

$$a = [k^{\frac{1}{2}}] + 1. \tag{2. 10}$$

Then $k^{\frac{1}{2}} < a \leqq k^{\frac{1}{2}} + 1$ so that $(a-1)^2 \leqq k < a^2$.

Finally, choose α such that

$$r \equiv 1 (\bmod 8), \quad \text{if} \quad a \equiv 0 \quad \text{or} \quad 3 (\bmod 4), \tag{2. 11}$$

and

$$r \equiv 5 (\bmod 8), \quad \text{if} \quad a \equiv 1 \quad \text{or} \quad 2 (\bmod 4). \tag{2. 12}$$

Provided that

$$(k + 8l - 8)\, r \leqq p - 8, \tag{2. 13}$$

the integers kr, $(k+8)r, \ldots, (k+8l-8)r$ are in (2. 3) and so the l integers

$$k,\ k+8, \ldots,\ k+8l-8 \tag{2. 14}$$

are all quadratic non-residues, which are $\equiv 7 (\bmod 8)$, if $r \equiv 1 (\bmod 8)$, and are $\equiv 3 (\bmod 8)$, if $r \equiv 5 (\bmod 8)$. The condition (2. 13) is satisfied as, by (2. 2), (2. 5), (2. 7), (2. 8), and (2. 9), we have

$$(k + 8l - 8) r < p - 8q + 8r + 8r(p^{\frac{1}{5}} + 4) - 8r < p - 8q + 8(p^{\frac{1}{5}} + 8)\,(p^{\frac{1}{5}} + 4)$$

$$< p - 8p^{\frac{2}{5}} - 96p^{\frac{1}{5}} - 264 + 8p^{\frac{2}{5}} + 96p^{\frac{1}{5}} + 256 = p - 8.$$

If a is even, we consider the sequence of integers

$$(a+1)\,(a-1),\ (a+3)\,(a-3), \ldots,\ (a+2b-1)\,(a-2b+1), \tag{2. 15}$$

where b is the largest integer such that

$$(a+2b-1)\,(a-2b+1) > (a-1)^2; \tag{2. 16}$$

if a is odd, we consider the sequence of integers

$$(a+2)\,a,\ (a+4)\,(a-2), \ldots,\ (a+2c)\,(a-2c+2), \tag{2. 17}$$

where c is the largest integer such that

$$(a+2c)\,(a-2c+2) > (a-1)^2. \tag{2. 18}$$

The integers in (2. 15) are $\equiv 7 (\bmod 8)$, if $a \equiv 0 (\bmod 4)$, and are $\equiv 3 (\bmod 8)$, if $a \equiv 2 (\bmod 4)$. The integers in (2. 17) are $\equiv 3 (\bmod 8)$, if $a \equiv 1 (\bmod 4)$, and $\equiv 7 (\bmod 8)$, if $a \equiv 3 (\bmod 4)$. By the choices made in (2. 11) and (2. 12), we see that the integers in (2. 14) are in the same residue class modulo 8 as those in (2. 15), if a is even, and as those in (2. 17), if a is odd.

Next, we have $(a-1)^2 \leqq k < \dfrac{p}{r} < p^{\frac{4}{5}}$, so that $a < p^{\frac{2}{5}} + 1$. Then

$$a + 2b - 1 < a + \sqrt{2a-1} < p^{\frac{2}{5}} + \sqrt{2}(p^{\frac{1}{5}} + 1) + 1 < q,$$

so that the integers in (2. 15) are all quadratic residues. Similarly the integers in (2. 17) are also quadratic residues.

Thus, subdividing the integer interval

$$\begin{cases} [(a-1)^2, \ldots, a^2-1], & \text{if } a \text{ is even,} \\ [(a-1)^2, \ldots, a^2+2a], & \text{if } a \text{ is odd,} \end{cases}$$

by the quadratic residues in (2. 15) and (2. 17) respectively, we must have, by (2. 14), that $8l-8$ is less than the maximum difference between integers in the subdivided interval. This gives the required contradiction; we just give the details for a odd. In this case, the difference between integers in (2. 17) in the subdivided interval $[(a-1)^2, \ldots, a^2-1]$ is at most

$$(a+2c)(a-2c+2)-(a+2c+2)(a-2c)=8c<4+8a^{\frac{1}{2}}<8p^{\frac{1}{5}}+12<8p^{\frac{1}{5}}+16<8l-8.$$

References

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

[2] *A. Brauer*, On the Non-Existence of the Euclidean Algorithm in Certain Quadratic Number Fields, Amer. J. Math. **62** (1941), 697—716.

[3] *A. Brauer*, Combinatorial Methods in the Distribution of k-th Power Residues, Combinatorial Mathematics and its Applications, Chapel Hill 1969, 14—37.

[4] *A. Brauer* and *T. L. Reynolds*, On a Theorem of Aubry-Thue, Canad. J. Math. **3** (1951), 367—374.

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

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

[7] *C. F. Gauss*, Werke I, Disquitiones Arithmeticae, 2nd ed., Göttingen 1870, art. 125 and 129 (see also *Dirichlet-Dedekind*, Vorlesungen über Zahlentheorie, 4th ed., Braunschweig 1894, 116).

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

[9] *Richard H. Hudson*, A bound for the first occurrence of three consecutive integers with equal quadratic character, Duke Math. J. **40** (1973), 33—39.

[10] *Richard H. Hudson*, On the Least K-th Power Non-Residue, Arkiv för matematik **12** (1974), 217—220.

[11] *Richard H. Hudson*, Power Residues and Nonresidues in Arithmetic Progressions, Trans. Amer. Math. Soc. **194** (1974), 277—289.

[12] *Richard H. Hudson*, Totally multiplicative sequences with values ± 1 which exclude four consecutive values of 1, J. reine angew. Math. **271** (1974), 218—220.

[13] *H.-J. Kanold*, Sätze ueber Kreisteilungspolynome und ihre Anwendungen auf einige zahlentheoretische Probleme. I, J. reine angew. Math. **187** (1950), 169—182.

[14] *T. Nagell*, Sur les restes et les non-restes quadratiques suivant un module premier, Arkiv Mat. **1** (1950), 185—193.

[15] *T. Nagell*, Sur un théorème d'Axel Thue, Arkiv Mat. **1** (1951), 489—496.

[16] *T. Nagell*, Sur le plus petit non-reste quadratique impair, Arkiv Mat. **1** (1951), 573—578.

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

[18] *L. Rédei*, Die Existenz eines ungeraden quadratischen Nichtrestes mod p im Intervall 1, $\sqrt{p}$, Acta Math. Sc. Szeged **15** (1953), 12—19.

[19] *Th. Skolem*, Eksistensen av en n^{te} ikke-potensrest (mod p) mindre enn $\sqrt{p}$, Norsk Mat. Tidsskrift **33** (1951), 123—126.

[20] *I. M. Vinogradov*, On the bound of the least non-residue of n^{th} powers, Bull. Acad. Sci. USSR **20** (1926), 47—58 (Trans. Amer. Math. Soc. **29** (1927), 218—226).

[21] *I. M. Vinogradov*, Elements of Number Theory, New York 1954.

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

Department of Mathematics, Computer Science, and Statistics, University of South Carolina, Columbia, S. C., 29208, USA

Department of Mathematics and Statistics, Carleton University, Ottawa, Ontario K1S 5B6, Canada

Eingegangen 17. Oktober 1979