On the Bound for a Pair of Consecutive Quartic Residues of a Prime
Author(s): R. G. Bierstedt and W. H. Mills
Source: *Proceedings of the American Mathematical Society*, Vol. 14, No. 4 (Aug., 1963), pp. 628-632
Published by: American Mathematical Society
Stable URL: http://www.jstor.org/stable/2034288
Accessed: 01/04/2011 17:08

ON THE BOUND FOR A PAIR OF CONSECUTIVE QUARTIC RESIDUES OF A PRIME

R. G. BIERSTEDT AND W. H. MILLS

It is easy to show that every prime p greater than 5 has a pair n, $n+1$ of positive consecutive quadratic residues not exceeding 10. Furthermore, any prime p, such as 43, for which 2, 3, 5, 7 are all quadratic nonresidues has 9, 10 as the smallest such pair. M. Dunton [1] has shown that every prime p, except 2, 7, and 13, has a pair n, $n+1$ of positive consecutive cubic residues not exceeding 78, and that there exist an infinite number of primes for which 77, 78 is the smallest such pair.

In this paper we prove the analogous result for quartic residues.[1]

THEOREM. *Every prime p, except* 2, 3, 5, 13, 17, 41, *has a pair n, $n+1$ of positive consecutive quartic residues not exceeding* 1224, 1225. *Furthermore, there exist an infinite number of primes p for which* 1224, 1225 *is the smallest such pair.*

PROOF. If $p\equiv 3 \pmod 4$, then all the quadratic residues of p are quartic residues, and the result follows from the known result for quadratic residues. Hence we may suppose $p\equiv 1 \pmod 4$. Let g be a primitive root modulo p. Let χ be the quartic character modulo p defined by $\chi(n)=i^b$ if $n\equiv g^b \pmod p$. Then n is a quartic residue of p if and only if $\chi(n)=1$.

Suppose p has no pair of positive consecutive quartic residues less than 1226. Then for every integer N, $1\leqq N\leqq 1224$, we have either $\chi(N)\neq 1$ or $\chi(N+1)\neq 1$. Setting $N=1$ we obtain $\chi(2)\neq 1$, and setting $N=80$ we obtain $\chi(5)=\chi(80)\neq 1$. Thus $\chi(2)=-1$, i, or $-i$; and $\chi(5)=-1$, i, or $-i$. Without loss of generality we suppose $\chi(2)=-1$ or i. Furthermore, if $\chi(2)=-1$, we may suppose that $\chi(5)=-1$ or i. This leads to five cases:

Case I. $\chi(2)=\chi(5)=-1$. Putting $N=9$ we obtain $\chi(3)\neq 1, -1$. Without loss of generality we suppose $\chi(3)=i$. The argument indicated by Table I now eliminates this case.

Case II. $\chi(2)=-1$, $\chi(5)=i$. Setting $N=3$ we obtain $\chi(3)\neq 1$, and setting $N=15$ we obtain $\chi(3)\neq -i$. Therefore $\chi(3)=-1$ or i. Thus

Presented to the Society, January 9, 1961, under the title *On the existence of a bound for a pair of consecutive quartic residues modulo a prime*; received by the editors May 1, 1962.

[1] The results for fifth and sixth powers have been obtained by electronic computing machines [4].

we have two subcases which are eliminated by Table II.

TABLE I

The case $\chi(2)=\chi(5)=-1$, $\chi(3)=i$

N	Conclusion
288	$\chi(17)\neq 1, -1$
255	$\chi(17)\neq i$
	$\chi(17)=-i$
51	$\chi(13)\neq 1$
25	$\chi(13)\neq -1$
39	$\chi(13)\neq -i$
	$\chi(13)=i$
195	$\chi(7)\neq 1, -1$
	$\chi(49)=-1$
40	$\chi(41)\neq 1$
81	$\chi(41)\neq -1$
245	$\chi(41)\neq i$
	$\chi(41)=-i$
287	$\chi(7)\neq i$
	$\chi(7)=-i$
10	$\chi(11)\neq 1$
21	$\chi(11)\neq -1$
77	$\chi(11)\neq i$
594	$\chi(11)\neq -i$

TABLE II

The case $\chi(2)=-1$, $\chi(5)=i$

Subcase A: $\chi(3)=-1$		Subcase B: $\chi(3)=i$	
N	Conclusion	N	Conclusion
49	$\chi(7)\neq 1, -1$	288	$\chi(17)\neq 1, -1$
35	$\chi(7)\neq -i$	50	$\chi(17)\neq -i$
	$\chi(7)=i$		$\chi(17)=i$
675	$\chi(13)\neq 1, -1$	49	$\chi(7)\neq 1, -1$
728	$\chi(13)\neq i$	119	$\chi(7)\neq -i$
64	$\chi(13)\neq -i$		$\chi(7)=i$
		168	$\chi(13)\neq 1, -1$
		441	$\chi(13)\neq i$
		64	$\chi(13)\neq -i$

Case III. $\chi(2)=i$, $\chi(5)=-1$. Putting $N=15$ we get $\chi(3)\neq -1$, and putting $N=24$ we get $\chi(3)\neq i$. Therefore $\chi(3)=1$ or $-i$. These subcases are eliminated by Table III.

TABLE III

The case $\chi(2)=i$, $\chi(5)=-1$

Subcase A: $\chi(3)=1$		Subcase B: $\chi(3)=-i$	
N	Conclusion	N	Conclusion
48	$\chi(7)\neq 1, -1$	6	$\chi(7)\neq 1$
224	$\chi(7)\neq -i$	35	$\chi(7)\neq -1$
	$\chi(7)=i$	20	$\chi(7)\neq i$
168	$\chi(13)\neq 1, -1$		$\chi(7)=-i$
675	$\chi(13)\neq i, -i$	16	$\chi(17)\neq 1$
		84	$\chi(17)\neq -1$
		119	$\chi(17)\neq i$
		255	$\chi(17)\neq -i$

Case IV. $\chi(2)=\chi(5)=i$. Putting $N=15$ we have $\chi(3)\neq -i$. Thus we have three subcases here—these are eliminated by Table IV.

TABLE IV

The case $\chi(2)=\chi(5)=i$

Subcase A: $\chi(3)=1$		Subcase B: $\chi(3)=-1$		Subcase C: $\chi(3)=i$	
N	Conclusion	N	Conclusion	N	Conclusion
48	$\chi(7)\neq 1, -1$	12	$\chi(13)\neq 1$	16	$\chi(17)\neq 1$
	$\chi(49)=-1$	624	$\chi(13)\neq -1$	255	$\chi(17)\neq -1$
16	$\chi(17)\neq 1$	675	$\chi(13)\neq i, -i$	135	$\chi(17)\neq i$
1224	$\chi(17)\neq i$				$\chi(17)=-i$
255	$\chi(17)\neq -i$			374	$\chi(11)\neq 1$
	$\chi(17)=-1$			99	$\chi(11)\neq -1$
169	$\chi(13)\neq 1, -1$			54	$\chi(11)\neq -i$
26	$\chi(13)\neq -i$				$\chi(11)=i$
	$\chi(13)=i$			384	$\chi(7)\neq -1$
120	$\chi(11)\neq 1, -1$			84	$\chi(7)\neq i$
935	$\chi(11)\neq i$			35	$\chi(7)\neq -i$
143	$\chi(11)\neq -i$				$\chi(7)=1$
				168	$\chi(13)\neq 1, -1$
				220	$\chi(13)\neq i$
				39	$\chi(13)\neq -i$

Case V. $\chi(2)=i$, $\chi(5)=-i$. This last case is eliminated by Table V. We have now shown that every prime p, except 2, 3, 5, 13, 17, 41, has a pair of consecutive positive quartic residues not exceeding 1224, 1225.

TABLE V

The case $\chi(2)=i$, $\chi(5)=-i$

N	Conclusion
9	$\chi(3)\neq 1, -1$
15	$\chi(3)\neq i$
	$\chi(3)=-i$
6	$\chi(7)\neq 1$
35	$\chi(7)\neq i$
224	$\chi(7)\neq -i$
	$\chi(7)=-1$
168	$\chi(13)\neq 1, -1$
624	$\chi(13)\neq i$
	$\chi(13)=-i$
16	$\chi(17)\neq 1$
255	$\chi(17)\neq -1$
135	$\chi(17)\neq i$
	$\chi(17)=-i$
10	$\chi(11)\neq 1$
99	$\chi(11)\neq -1$
33	$\chi(11)\neq i$
351	$\chi(11)\neq -i$

It follows from Theorem 3 of [2] that there exist an infinite number of primes p such that, with appropriate choice of primitive root g, $\chi(3)=1$ and $\chi(q)=i$ for all other primes q less than 1226. Let p be such a prime. Then $\chi(n)$ is determined for all n such that $1\leqq n\leqq 1225$. The only odd values of n in this range for which $\chi(n)=1$ are

$$n = 1, 3, 9, 27, 81, 243, 625, 729, 875, 1225.$$

On the other hand $\chi(n)\neq 1$ for

$$n = 2, 4, 8, 10, 26, 28, 80, 82, 242, 244, 624, 626, 728, 730, 874, 876,$$

and $\chi(1224)=1$. Hence 1224, 1225 is the smallest pair of positive consecutive quartic residues of p. Thus there are an infinity of primes p for which 1224, 1225 is the smallest pair of consecutive quartic residues. This completes the proof of the theorem.

The primes 5, 13, 17, and 41 occurred in the factorizations of the numbers used in the proof. Hence no conclusion can be drawn from this proof concerning them. However a brief calculation shows that these primes do not have pairs of consecutive quartic residues.

It is known from a theorem of A. Brauer [**3**] that every sufficiently large prime p has a pair of consecutive quartic residues. Our result shows that this is true for all primes p greater than 41. Brauer's proof does not establish the existence of an upper bound for the least pair of consecutive quartic residues of p.

D. H. and Emma Lehmer [**5**] have shown that there is no bound for three consecutive positive quadratic residues. In other words there exist primes for which the smallest triplet n, $n+1$, $n+2$ of consecutive positive quadratic residues is arbitrarily large. The same result is therefore true for three consecutive quartic residues.

References

1. M. Dunton, *A bound for consecutive pairs of cubic residues* (to appear).

2. W. H. Mills, *Characters with preassigned values*, Canad. J. Math. **15** (1963), 169–171.

3. A. Brauer, *Über Sequenzen von Potenzresten*, S.-B. Preuss Akad. Wiss. Phys.-Math. Kl. (1928), 9–16.

4. D. H. Lehmer, Emma Lehmer and W. H. Mills, *Pairs of consecutive power residues*, Canad. J. Math. **15** (1963), 172–177.

5. D. H. Lehmer and Emma Lehmer, *On runs of residues*, Proc. Amer. Math. Soc. **13** (1962), 102–106.

Colorado College and
Yale University