Bounds for Pairs of Cubic Residues
Author(s): M. Dunton
Source: *Proceedings of the American Mathematical Society*, Vol. 16, No. 2 (Apr., 1965), pp. 330-332
Published by: American Mathematical Society
Stable URL: http://www.jstor.org/stable/2033874
Accessed: 01/04/2011 17:09

BOUNDS FOR PAIRS OF CUBIC RESIDUES

M. DUNTON

The purpose of this paper is to prove Theorems 1–4. To this end one first establishes the following simple lemma.

LEMMA. *Let k be an odd prime, and m, n any two nonzero integers. Then for a prime modulus p, at least one member of the set, $S=\{m, n, mn, mn^2, \cdots, mn^{k-1}\}$, is a kth power residue.*

PROOF. If p is not of the form $tk+1$, every residue is a kth power residue, and the lemma is trivial. So suppose $p=tk+1$.

Let χ be a kth power character function defined on residues modulo p. Let $\chi(m)=\theta^\alpha$, $\chi(n)=\theta^\beta$, where θ is a primitive kth root of unity. If $\beta\equiv 0 \bmod k$, $\chi(n)=1$. If not, $\chi(mn^j)=\theta^\alpha$, $\theta^{j\beta}=\theta^{\alpha+j\beta}$, and as j takes values in $\{0, 1, \cdots, k-1\}$, $\alpha+j\beta$ runs over a complete set of residues modulo k, i.e., there is some j_0 such that $\alpha+j_0\beta\equiv 0 \bmod k$. Then $\chi(mn^{j_0})=1$ and mn^{j_0} is a kth power residue modulo p.

In the following theorems, it is assumed that residues are the least positive representatives of their classes and the ordering implied by a "bound" is that of the real integers.

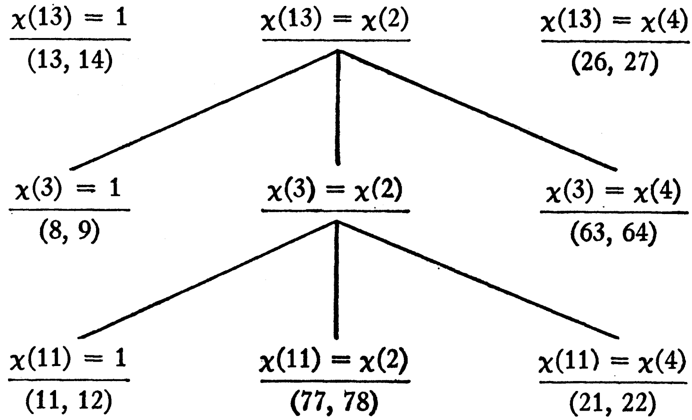
THEOREM 1. *If $p\nmid 7\cdot 13$, then there exists a consecutive pair of nontrivial cubic residues $\leqq$ (77, 78) modulo p.*

PROOF. In the lemma, let $k=3$, $n=2$, $m=7$. Then at least one of the following is a cubic residue: 2, 7, 14, 28. If $\chi(2)=1$, (1, 2) is a consecutive pair; if $\chi(7)=1$, (7, 8) is a consecutive pair; and if $\chi(28)=1$, (27, 28) is a consecutive pair. In the remaining case $\chi(14)=1$, $\chi(2)=\omega$ and $\chi(7)=\omega^2$. To get the shortest proof, one looks at 13, 3 and 11 in that order. The results are summarized in the diagram on the next page.

THEOREM 2. *There are infinitely many primes which have* (77, 78) *as their first pair of consecutive nontrivial cubic residues; this implies that* (77, 78) *is the best possible bound.* 13,817,029 *is the smallest such prime.*

Note. The calculation of this prime was made possible by a grant of free time from the University of California at Berkeley Computer Center. The University of California, Davis Center provided card punching.

Received by the editors September 13, 1963.



PROOF. The first part of Theorem 2 follows from Kummer's Theorem that there exist infinitely many primes having prescribed prime power character assigned to a finite set of smaller primes. The computer was programmed to find the smallest prime with the following cubic character: $\chi(2)=\chi(3)=\chi(11)=\chi(13)=\chi(17)=\omega$; $\chi(7)=\chi(19)=\omega^2$; $\chi(5)=1$; $\chi(23)\neq\omega^2$, $\chi(29)\neq\omega^2$; $\chi(37)\neq 1$ and $\chi(73)\neq 1$ if $\chi(37)=\omega^2$; $\chi(41)\neq 1$, $\chi(43)\neq 1$, $\chi(53)\neq 1$, $\chi(59)\neq 1$, $\chi(61)\neq 1$, $\chi(67)\neq 1$, $\chi(71)\neq 1$.

Tables by Cunningham and Gosset [1] provide values of $\mu\equiv L/M$ and $\lambda\equiv M/L$ mod q (where $4p=L^2+27M^2$) for primes $q<50$ such that q will have prescribed cubic character modulo p. For primes >50 a theorem of Emma Lehmer [2] made the necessary extension of the tables a simple matter. Hand calculation provided the machine with 32 possible values of μ mod $60060=2^2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13$. Since 2 is to be a cubic nonresidue of the prime p, L and M must be odd. The machine computed $L\equiv M\mu$ mod 60060 where M is odd and <5000 and μ is taken from the 32 values computed by hand. Next, the machine found $L/M\equiv\mu_q$ mod q for $13<q\leqq 73$ and checked the exclusion tables which had been obtained from Cunningham and Gosset and Lehmer. If μ_q passed all the tests for q up to 73, $(1/4)(L^2+27M^2)=p$ was tested for primality, and in the case of a prime, a card was punched with the values of L, M and p. 13,817,029 was the smallest prime of 28 solutions $<5\cdot 10^8$.

THEOREM 3. *If* $p\nmid 7\cdot 13$, *then there exist* 2 *pairs of nontrivial consecutive cubic residues* $\leqq(125,126)$.

PROOF. At least one of the 10 pairs in the proof of Theorem 1 must occur. Starting from each of these, and considering possible values of

$\chi(2)$, $\chi(3)$, $\chi(5)$, $\chi(7)$, $\chi(11)$, $\chi(13)$, one arrives at a second pair $\leqq(125, 126)$. For example, if (7, 8) occurs, the lemma can be applied to $k=3$, $m=2$, $n=3$. If $\chi(2)=1$, then (1, 2) is another pair; $\chi(3)=1$ implies (8, 9) is a second pair; $\chi(6)=1$ implies (6, 7) is a pair, and $\chi(18)=1$ implies (125, 126) is a second pair. The remaining nine cases can be settled in similar fashion.

THEOREM 4. *If d is a positive integer, $d \not\equiv \pm 3 \bmod 7$ is a necessary condition for the existence of a bound $B(d)$ such that for all except a finite set of primes, there exists a pair of cubic residues r_1, r_2, with $r_1-r_2=d$ and $r_2 \leqq B(d)$.*

PROOF. It must be shown that for all $B(d)>1$ there exist infinitely many primes p such that the first pair of cubic residues which differ by $d\equiv \pm 3 \bmod 7$ are greater than $B(d)$. Such primes can be constructed by taking $\chi(q)=1$ if q is a prime $\leqq B(d)$ and $\equiv \pm 1 \bmod 7$, $\chi(q)=\omega$ if q is a prime $\leqq B(d)$ and $\equiv \pm 2 \bmod 7$, $\chi(q)=\omega^2$ if q is a prime $\leqq B(d)$ and $\equiv \pm 3 \bmod 7$. Kummer's Theorem states that infinitely many such primes p with prescribed character exist and primes so determined cannot have a pair of cubic residues $\leqq B(d)$ which differ by $d\equiv \pm 3 \bmod 7$.

The following table gives values of the bound, $B(d)$, associated with difference d. In each case $B(d)$ was obtained by methods similar to the proof of Theorem 1.

$B(d)$	77	90	none	none	114	21	1	56	72	none
d	1	2	3	4	5	6	7	8	9	10

BIBLIOGRAPHY

1. Lt. Col. Allan Cunningham and Thorald Gosset, *Quartic and cubic residuacity tables*, Messenger of Mathematics 50 (1920–21), 1–30.

2. Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), 20–29.

SACRAMENTO, CALIFORNIA