BOUNDS OF CUBIC RESIDUES IN A.P.

by SAHIB SINGH,* *Clarion State College, Clarion, Pennsylvania, 16214, U.S.A.*

(Communicated by S. Chowla, F.N.I.)

(*Received 16 June 1969*)

In this paper we define $r = r(k, d, p)$ as the least positive integer such that $r, r+d, r+2d, \ldots r+(k-1)\, d$ are either all cubic residues modulo p or belong to any one of the three cosets obtained with the help of cubic residues. In the former case we define $\Lambda(k, d) = \limsup_{p \to \infty} r\,(k, d, p)$ while in the latter case our notation is $\Lambda^*(k, d)$ instead of $\Lambda(k, d)$. In terms of this notation, a general result $\Lambda^*(2, d) \leqslant (d^3 - d)$ for all $d > 1$ is established and the values of d responsible for $\Lambda(3, d) = \infty$ are derived.

INTRODUCTION

If p is prime, it is well known that a prime field of characteristic p has exactly p elements. We can take these elements as the integers $0, 1, 2, 3, \ldots (p-1)$ where the field operations addition and multiplication are respectively addition modulo p and multiplication modulo p. The non-zero elements of this field, namely $1, 2, 3, \ldots (p-1)$, form a multiplicative group which is cyclic and can be generated by any one of the $\phi(p-1)$ primitive roots of p. We will denote this multiplicative group by G. For our purpose, an element α of G would be defined to be a cubic residue modulo p if $x^3 \equiv \alpha(\text{modulo } p)$ admits integral solutions.

The cubic residues modulo p which occur in G form a sub-group (hereafter called H) of G whose order is $\dfrac{p-1}{(3, p-1)}$. We observe that if $p \not\equiv 1$ (modulo 3), then H is identical with G, which means that every element of G is a cubic residue modulo p. Since this case is not interesting, therefore, the prime p mentioned in the sequel will always be of the form $3m+1$, so that G can be partitioned with the help of H into 3 cosets.

OUR NOTATION AND PROBLEM

Given two positive integers, k and d, we define $r = r(k, d, p)$ as the least positive integer such that $r, r+d, r+2d, \ldots, r+(k-1)\, d$ are all cubic residues modulo p. This notation is different from that followed by Lehmer and

---

* *Present address:* Faculty of Mathematics, Delhi University, Delhi 7.

Lehmer (1962). The existence of these cubic residues in A.P. for every large prime p is a consequence of Theorem due to Brauer (1928).

Finally we define $\Lambda(k, d) = \limsup_{p \to \infty} r(k, d, p)$.

If $r, r+d, r+2d, \ldots r+(k-1)\,d$ do not belong to H, but belong to any one of the cosets, then our notation is $\Lambda^*(k, d)$ instead of $\Lambda(k, d)$.

Our problem is to explore the case as to when $\Lambda(k, d)$ or $\Lambda^*(k, d)$ is finite and when infinite.

This type of problem was first initiated by Dunton (1965) whose results in our notation are as under:

d	1	2	3	4	5	6	7	8	9	10
$\Lambda(2, d)$	77	90	∞	∞	114	21	1	56	72	∞

However, it may be mentioned that the value of $\Lambda(2, 2)$ can be improved to 25 from 90 (Singh 1968).

It is easy to determine the values of $\Lambda^*(2, d)$ when d varies over integral values. Some of these initial results are shown below.

d	1	2	3	4
$\Lambda^*(2, d)$	8	6	12	12

The value of $\Lambda^*(2, 4)$ has been derived below for illustration. Let ψ denote cubic character modulo p and ω the imaginary cubic root of unity defined by $e^{2\pi i/3}$ $(i = \sqrt{-1})$. The implication below on the right-hand side gives the least positive integral valued pair of members belonging to the same coset and differing by 4, against the character values shown on the left hand.

$$\psi(2) = 1 \Rightarrow (4,\ 8)$$
$$\psi(2) = \omega,\ \psi(3) = 1 \Rightarrow (2,\ 6)$$
$$\psi(2) = \omega,\ \psi(3) = \omega \Rightarrow (8,\ 12)$$
$$\psi(2) = \omega,\ \psi(3) = \omega^2 \Rightarrow (12,\ 16)$$

No new values will be obtained by considering $\psi(2) = \omega^2$. Hence $\Lambda^*(2, 4) = 12$.

We assert that $\Lambda^*(2, d) < \infty$ for all positive integral values of d. This is so because we have $\Lambda^*(2,\ 1) = 8$ (Jordan 1964) and by our Theorem 1 below we have $\Lambda^*(2, d) \leqslant (d^3-d)$ for all $d > 1$.

Theorem 1. $\Lambda^*(2, d) \leqslant (d^3-d)$ for all $d > 1$.

Proof: As before, let ψ denote cubic character modulo a prime p and ω, an imaginary cube root of unity. The implication on the right-hand side below gives the integral valued pairs belonging to the same coset (with respect to H) situated at a distance d, against the character values on the left-hand side.

$$\psi(d+1) = 1 \Rightarrow (1,\ d+1)$$
$$\psi(d+1) = \omega,\ \psi(d) = \omega \Rightarrow (d^2,\ d^2+d)$$
$$\psi(d+1) = \omega,\ \psi(d) = \omega^2,\ \psi(d-1) = \omega^2 \Rightarrow (d^2-d,\ d^2)$$
$$\psi(d+1) = \omega,\ \psi(d) = \omega^2,\ \psi(d-1) = \omega \Rightarrow \left(\frac{d(d-1)}{2},\ \frac{d(d+1)}{2}\right)$$
$$\psi(d+1) = \omega,\ \psi(d) = \omega^2,\ \psi(d-1) = 1 \Rightarrow (d^3-d,\ d^3)$$
$$\psi(d+1) = \omega,\ \psi(d) = 1,\ \psi(d-1) = \omega^2 \Rightarrow (d^3-d,\ d^3)$$
$$\psi(d+1) = \omega,\ \psi(d) = 1,\ \psi(d-1) = \omega \Rightarrow \left(\frac{d(d-1)}{2},\ \frac{d(d+1)}{2}\right)$$
$$\psi(d+1) = \omega,\ \psi(d) = 1,\ \psi(d-1) = 1 \Rightarrow (d^2-d,\ d^2).$$

The above values recur when we take $\psi(d+1) = \omega^2$.

Since $d^3-d > d^2$ when $d > 1$, therefore, it follows that $\Lambda^*(2, d) \leqslant (d^3-d)$ for all $d > 1$.

The case when $k = 3$ and $d = 1$ has already been settled with the help of computer. The value of $\Lambda(3, 1) = 23532$ (Mills 1965).

Our next problem is to examine the value of $\Lambda(3, 2)$. We give below two proofs to show that $\Lambda(3, 2) = \infty$. The first proof is connected with a result due to Dunton (1965) and the second is an obvious deduction from a general result developed in Theorem 2, for determining the values of d such that $\Lambda(3, d) = \infty$.

Proposition. $\Lambda(3, 2) = \infty$.

First Proof: If possible let $\Lambda(3, 2) < \infty$. This implies the existence of a finite upper bound α such that there is always a triplet of cubic residues $(d, d+2, d+4)$ with respect to almost all primes* with $d \lessdot \alpha$. This amounts to the existence of a pair of cubic residues $(d, d+4)$ with $d \leqslant \alpha$ for all primes, thus contradicting the result of Dunton (1965) which states that $\Lambda(2, 4) = \infty$.

Hence our supposition is wrong and the proof is complete.

Second Proof: It follows from Theorem 2 below which uses a result due to Kummer. We call it Kummer Theorem which is stated as under:

Kummer Theorem—Given n, a prime, and m, a positive integer, such that $p_1, p_2, \ldots, p_m$ are distinct and fixed primes and $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ denote nth roots of unity (not necessarily distinct), then there exist infinitely many primes p with corresponding nth power character ψ modulo p satisfying

$$\psi(p_j) = \epsilon \quad (1 \leqslant j \leqslant m).$$

Theorem 2. $\Lambda(3, d) = \infty$ when

(i) $d \equiv \pm 2, \pm 3$ (modulo 7),

(ii) $d \equiv \pm 2, \pm 3, \pm 4, \pm 6$ (modulo 13),

(iii) $d \equiv \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 9$ (modulo 19).

---

* Here 'almost all primes' in this context means all primes with a finite number of exceptions.

PROOF: (i) Let N be any positive arbitrarily selected large integer. We define cubic character ψ for all primes less than N, using ω as the complex cubic root of unity.

$\psi(p_1) = 1$ where p_1 ranges over primes of form $7m \pm 1$,
$\psi(p_2) = \omega$ where p_2 represents all primes of the type $7m \pm 2$,
$\psi(p_3) = \omega^2$ when p_3 represents primes of the form $7m \pm 3$.

With this definition of ψ, if we consider all possible triplets in arithmetic progression with a common difference d and which are all less than N, then we find that if $d \equiv \pm 2$ (modulo 7) or $\equiv \pm 3$ (modulo 7), at least one of the members in the triplet is of the form $7m \pm 2$ or $7m \pm 3$ and is thus not a cubic residue.

Since the selection of N is arbitrary, therefore, the occurrence of a triplet of cubic residues in A.P. with a common difference of form $7m \pm 2$ or $7m \pm 3$ can be postponed as far as we like by using Kummer Theorem.

(ii) We use the fact that 2 is a primitive root of 13 and by this use we observe that the cubic residues can be of type $13m$, $13m \pm 1$ or $13m \pm 8$. The remaining argument is on similar lines as in Proof (i).

(iii) The proof is similar to cases (i) and (ii).

Remark: The values of d determined in the above theorem which make $\Lambda(3, d) = \infty$ are not exhaustive. By a suitable definition of character values, it would be possible to include more values. However, this method does not give us any value of d which can make $\Lambda^*(3, d) = \infty$. The conjecture is that for all positive integral values of d, $\Lambda^*(3, d) < \infty$. It may be that a proof can be developed on the same basis as in Theorem 1.

ACKNOWLEDGEMENT

The author expresses his gratitude to Professor S. Chowla for his inspiration and encouragement during the preparation of this paper.

REFERENCES

Brauer, Alfred (1928). Über sequenzen von potenzresten. *Sber. Akad. Wiss.* 9–16.

Dunton, M. (1965). Bounds for pairs of cubic residues. *Proc. Am. math. Soc.*, **16**, 330–32.

*Hilbert, D. (1932). Zahlentheorie Verlag Von Julius. Springer, Berlin.

Jordan, J. H. (1964). Pairs of consecutive power residues or non-residues. *Can. J. Math.*, **16**, 310–14.

Lehmer, D. H., and Lehmer, E. (1962). On run of residues. *Proc. Am. math. Soc.*, **13**, 102–106.

Mills, W. H. (1965). Bounded consecutive residues and related problems. Proceedings of Symposia in Pure Mathematics, American Mathematical Society, Vol. 8, 170–74.

Singh, Sahib (1968). Bounds of Power Residues in Arithmetic Progression. Ph.D. thesis. Pennsylvania State University.

* Not cited in the text. This is for general reference on the subject.