Indian J Pure Appl Math (2024) 55:388–391
https://doi.org/10.1007/s13226-023-00370-w

ORIGINAL RESEARCH

A note on the sum of cubic residues with even and odd index

V. P. Ramesh · **Gowtham R.** · **Saswati Sinha**

Received: 20 June 2022 / Accepted: 5 January 2023 / Published online: 16 January 2023
© The Indian National Science Academy 2023

Abstract Let p be an odd prime and $\ell \in \mathbb{N}$. We prove that the sum of cubic residues of p^ℓ with even index equals the sum of cubic residues of p^ℓ with odd index if and only if $p \equiv 1 \pmod 4$. We also prove that for $2p^\ell$, $p \equiv 1 \pmod 4$ is sufficient but not necessary for the two sums to be equal. We also present a closed-form expression for the sum and study some properties.

Keywords Cubic residues, Primitive roots, Indices

Mathematics Subject Classification 11A07 · 11A41

1 Introduction

Let us recall some of the relevant definitions first. For any natural number n and any $a \in (\mathbb{Z}/n\mathbb{Z})^*$, a is called the cubic residue of n if the congruence $x^3 \equiv a \pmod n$ has a solution [6]. *Let g be a primitive root of n and $a \in (\mathbb{Z}/n\mathbb{Z})^*$, then the least positive integer m such that $a \equiv g^m \pmod n$ is called the index of a with respect to g* and is denoted by $ind_g\, a$ (see page 163 of [1] or art 57 in page 37 of [3]).

Let g_1 and g_2 be two primitive roots of n. The definition of index of an element a asserts that $2|ind_{g_1}\, a$ if and only if $2|ind_{g_2}\, a$. To see this, note that if $ind_{g_1}\, a = i$ and $ind_{g_2}\, a = j$, then there exists $k \in \mathbb{N}$ such that $g_1^i \equiv g_1^{kj} \pmod n$ if and only if $i \equiv kj \pmod{\phi(n)}$ [1]. Now, since $\phi(n)$ is even and $(\phi(n), k) = 1$ it follows that i is even if and only if j is even.

Throughout this article, p denotes a prime and g denotes a primitive root of n. Dence and Dence [2], denoted the set of all cubic residues of p as $S_p^{(3)}$ and showed that $|S_p^{(3)}|$ is $\frac{(p-1)}{3}$ when $p \equiv 1 \pmod 3$ and $|S_p^{(3)}|$ is $(p-1)$ when $p \equiv 2 \pmod 3$. Later, Ramesh et al. [7] generalised the above result by computing a closed form for $|S_n^{(3)}|$, and showed that, *if $a \in (\mathbb{Z}/p\mathbb{Z})^*$ is a cubic residue of p then $a + kp \in (\mathbb{Z}/p^\ell\mathbb{Z})^*$ is a cubic residue of p^ℓ for all $p \neq 3, k \geq 0$ and $\ell \geq 1$.*

Dence and Dence [2] also showed that $T_p^{(3)}$, the sum of cubic residues of p is jp if $p = 6j + 1$ and $\frac{(3j+1)p}{2}$ if $p = 3j + 2$ for any $j \geq 1$. Křížek and Somer [5] showed that the number of primitive roots of n, $|M(n)|$ equals

Communicated by Sanoli Gun.

These authors contributed equally to this work.

V. p. Ramesh
Department of Mathematics, Central University of Tamil Nadu, Neelakudy, Thiruvarur, Tamilnadu 610005, India
E-mail: vpramesh@gmail.com

G. R.
Department of Mathematics, Indian Institute of Technology Madras, Adyar, Chennai, Tamilnadu 600036, India
E-mail: rgowtham.math@gmail.com

the number of quadratic non-residues of n, $|K(n)|$ if and only if $n = 4$, p or $2p$ where p is a Fermat prime. Later, Gun et al. [4] showed $|M(n)| = |K(n)| - 2^r$ if and only if (i)$n = p$ or $2p$, where p and q are primes such that $p = 2^{r+1}q + 1$; or (ii)$n = p^2$ or $2p^2$, where $p = 2^{r+1} + 1$ is a Fermat prime.

In this article we prove the following results,

Theorem 1 *Let $n = p^\ell$ or $2p^\ell$ where $p \equiv 1 \pmod 4$ and $\ell \in \mathbb{N}$. Then*

$$\sum_{\substack{a \in S_n^{(3)} \\ 2 | ind_g\, a}} a = \sum_{\substack{a \in S_n^{(3)} \\ 2 \nmid ind_g\, a}} a = \begin{cases} \frac{\phi(n)}{12} n, \text{ if } p \equiv 1 \pmod 3 \\ \frac{\phi(n)}{4} n, \text{ if } p \equiv 2 \pmod 3, \end{cases}$$

We observe that when $n = 46 = 2 \times 23$, the sum of all cubic residues of 46 with even index equals the sum of all cubic residues of 46 with odd index and $23 \not\equiv 1 \pmod 4$ so the converse of the above theorem is not true. But in the case of $n = p^\ell$ the converse is also true, which we present in the following result.

Theorem 2 *Let $p \geq 5$ be any prime and $\ell \in \mathbb{N}$. Then,*

$$p \equiv 1 \pmod 4 \iff \sum_{\substack{a \in S_{p^\ell}^{(3)} \\ 2 | ind_g\, a}} a = \sum_{\substack{a \in S_{p^\ell}^{(3)} \\ 2 \nmid ind_g\, a}} a$$

Theorem 3 *Let n be any natural number. Then the number of primitive roots of n is equal to the number of cubic residues of n if and only if $n = 2, p, 2p, 3^\ell$, or $2 \times 3^\ell$ where p is any prime of the form $p = 2^k 3^m + 1$ where k, m, ℓ are natural numbers and $\ell \geq 2$.*

Corollary 1 *Let p be any prime. The number of primitive roots of p is equal to the number of cubic residues of p if and only if $p = 2$ or $2^k 3^m + 1$ where k and m are natural numbers.*

2 Proof of Theorem 1

Before we proceed to the proof of Theorem 1, we first proving the following lemma which will be useful while proving the theorem.

Lemma 1 *Let $n = p^\ell$ or $2p^\ell$ where $p \geq 5$, $\ell \in \mathbb{N}$ and $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Then, $p \equiv 1 \pmod 4$ if and only if $2 | (ind_g\, a + ind_g\, (-a))$.*

Proof Let $n = p^\ell$ or $2p^\ell$, where $p \geq 5$, $p \equiv 1 \pmod 4$, and $\ell \in \mathbb{N}$. Also, let g be a primitive root of n and $a \in (\mathbb{Z}/n\mathbb{Z})^*$.

Since g is a primitive root of n, we know that there exist least positive integers k_1 and k_2 such that $g^{k_1} \equiv a \pmod n$ and $g^{k_2} \equiv -a \pmod n$. In otherwords, let $ind_g\, a = k_1$ and $ind_g\, (-a) = k_2$. Without loss of generality let us assume that $k_1 \geq k_2$, then

$$g^{k_1 - k_2} \equiv -1 \equiv g^{\phi(n)/2} \pmod n$$
$$\implies k_1 + k_2 = 2k_2 + \frac{\phi(n)}{2}$$

Now, if $p \equiv 1 \pmod 4$ then $4 | \phi(n)$ and hence $2 | (k_1 + k_2)$. Conversely, if $2 | (k_1 + k_2)$ then $2 \Big| \left(2k_2 + \frac{\phi(n)}{2}\right)$ and hence $4 | \phi(n)$ which further implies that $p \equiv 1 \pmod 4$. □

We now proceed to the proof of Theorem 1.

Proof Let $n = p^\ell$ or $2p^\ell$ where $p \equiv 1 \pmod 4$ and $\ell \in \mathbb{N}$. We prove the theorem by considering two cases, namely, $p \equiv 1 \pmod 3$ and $p \equiv 2 \pmod 3$.

Case 1. $p \equiv 1 \pmod 3$.

From Corollary 2 and Theorem 3 of [7], it follows that $|S_n^{(3)}| = \dfrac{\phi(p^\ell)}{3}$ for any n of the form p^ℓ or $2p^\ell$.

It is known that for a given primitive root g of n, every cubic residue of n can uniquely be represented by g^{3t} for $1 \le t \le \phi(p^\ell)/3$. Now, since $2|(\phi(p^\ell)/3)$ the number of cubic residues of n with even index equals the number of cubic residues of n with odd index. Furthermore, the number of cubic residues of n with even (odd) index is $\phi(p^\ell)/6$. Since, $p \equiv 1 \pmod 4$, we can see that $2|(\phi(p^\ell)/6)$.

Now, for any $a \in S_n^{(3)}$ we know that $n - a \in S_n^{(3)}$ and by Lemma 1, it follows that $ind_g\ a$ is even (odd) if and only if $ind_g\ (n-a)$ is even (odd). Hence, there exist $\phi(p^\ell)/12$ such pairs of cubic residues of n with even (odd) index and each pair adds up to n. Thus,

$$\sum_{\substack{a \in S_n^{(3)} \\ 2|ind_g\ a}} a = \sum_{\substack{a \in S_n^{(3)} \\ 2\nmid ind_g\ a}} a = \frac{\phi(p^\ell)}{12} n = \frac{\phi(n)}{12} n$$

Case 2. $p \equiv 2 \pmod 3$.

Again, from Corollary 2 and Theorem 3 of [7], it follows that $S_n^{(3)} = (\mathbb{Z}/n\mathbb{Z})^*$ and $|S_n^{(3)}| = \phi(p^\ell)$. Now, for a given primitive root g of n, every cubic residue of n can uniquely be represented by g^t for $1 \le t \le \phi(p^\ell)$. The rest of the arguments are similar to that in Case 1. Since $\phi(p^\ell)$ is even, it is clear that the number of cubic residues of n with even index equals the number of cubic residues of n with odd index. Further, the number of cubic residues of n with even (odd) index is $\phi(p^\ell)/2$. It is also easy to verify that $2|(\phi(p^\ell)/2)$.

Again, from Lemma 1, whenever $a \in S_n^{(3)}$ we have $ind_g\ a$ is even (odd) if and only if $ind_g\ (n-a)$ is even (odd). Hence, there exist $\phi(p^\ell)/4$ such pairs of cubic residues of n with even (odd) index. Thus,

$$\sum_{\substack{a \in S_n^{(3)} \\ 2|ind_g\ a}} a = \sum_{\substack{a \in S_n^{(3)} \\ 2\nmid ind_g\ a}} a = \frac{\phi(p^\ell)}{4} n = \frac{\phi(n)}{4} n$$

3 Proof of Theorem 2

The forward part of this theorem directly follows from Theorem 1 and we prove the converse by the method of contradiction. Suppose there exist a prime $p \ge 5$ and $\ell \in \mathbb{N}$ such that the sum of cubic residues of p^ℓ with even index equals the sum of cubic residues of p^ℓ with odd index and $p \not\equiv 1 \pmod 4$. Since $p \ge 5$ it follows that $p \not\equiv 0 \pmod 3$ and we consider the following two cases to complete the proof.

Case 1. $p \equiv 1 \pmod 3$.

From Corollary 2 of [7], it follows that $|S_{p^\ell}^{(3)}| = \dfrac{\phi(p^\ell)}{3}$. And the sum of all cubic residues of p^ℓ is $\dfrac{\phi(p^\ell)}{6} p^\ell$, since the cubic residues occur in pairs namely a and $p^\ell - a$ adding to p^ℓ. Now, since $p \equiv 3 \pmod 4$, it follows that $2 \nmid \left(\dfrac{\phi(p^\ell)}{6} p^\ell \right)$ which is a contradiction to our assumption that the sum of cubic residues of p^ℓ with even index equals the sum of cubic residues of p^ℓ with odd index.

Case 2. $p \equiv 2 \pmod 3$.

Again from Corollary 2 of [7], it follows that $|S_{p^\ell}^{(3)}| = \phi(p^\ell)$ and a similar argument shows that the sum of all cubic residues of p^ℓ is $\dfrac{\phi(p^\ell)}{2} p^\ell$. Now, since $p \equiv 3 \pmod 4$, it follows that $2 \nmid \left(\dfrac{\phi(p^\ell)}{2} p^\ell \right)$ which is a contradiction to our assumption. □

4 Proof of Theorem 3

Proof Let n be any natural number. We claim that the number of primitive roots of n, $\phi(\phi(n))$ equals the number of cubic residues of n, $|S_n^{(3)}|$ if and only if $n = 2,\ p,\ 2p,\ 3^\ell$, or $2\times 3^\ell$ where p is any prime such that $p = 2^r 3^s + 1$ where r, s, ℓ are natural numbers and $\ell \geq 2$.

Now, since $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic we know from Gauss's theorem that $n = 2, 4, p^\ell$, or $2p^\ell$ where p is an odd prime and $\ell \geq 1$ (art. 315 in page 379 of [3]). It is easy to verify that $\phi(\phi(2)) = |S_2^{(3)}|$ and $\phi(\phi(4)) \neq |S_4^{(3)}|$ hence n can be 2 and not 4. Now we complete the proof by considering the following two cases.

Case 1. $n = p$ or $2p$.

Let $n = p$ and $\phi(\phi(p)) = |S_p^{(3)}|$. From Corollary 4 of [7] it follows that $p \neq 3$ and $p \not\equiv 2 \pmod 3$. Therefore, $p \equiv 1 \pmod 3$ equivalently, $p - 1 = m3^s$ for some $m, s \in \mathbb{N}$ and $(m, 3^s) = 1$. Now,

$$\begin{aligned}
\phi(\phi(p)) = |S_p^{(3)}| &\iff \phi(p-1) = \frac{p-1}{3} \quad \text{(from Theorem 2 of [2])} \\
&\iff \phi(m3^s) = \frac{m3^s}{3} \\
&\iff \phi(m) = \frac{m}{2} \\
&\iff m = 2^r \quad \text{for some } r \in \mathbb{N}
\end{aligned}$$

Therefore, $p = 2^r 3^s + 1$.

Similarly, when n is of the form $2p$ we get $p = 2^r 3^s + 1$ for some natural numbers r and s, since $\phi(2p) = \phi(p)$ and $|S_{2p}^{(3)}| = |S_p^{(3)}|$. Now, for the converse part, when n is of the form p or $2p$ where $p = 2^r 3^s + 1$ for some natural numbers r and s, it is easy to verfiy that $\phi(\phi(p)) = |S_p^{(3)}|$.

Case 2. $n = p^\ell$ or $2p^\ell$ where $\ell > 1$

Let $n = p^\ell$ and $\phi(\phi(p^\ell)) = |S_{p^\ell}^{(3)}|$. From Corollary 4 of [7], it follows that $p \not\equiv 2 \pmod 3$ and hence $p = 3$ or $p \equiv 1 \pmod 3$. Now, suppose $p \equiv 1 \pmod 3$ then

$$\begin{aligned}
\phi(\phi(p^\ell)) = |S_{p^\ell}^{(3)}| &\iff \phi(p^{\ell-1})\phi(p-1) = \frac{\phi(p^\ell)}{3} \text{ (from Corollary 2 of [7])} \\
&\iff \phi(p-1) = \frac{p}{3} \\
&\Rightarrow \ \Leftarrow p \equiv 1 \pmod 3
\end{aligned}$$

Therefore, $p = 3$ and hence $n = 3^\ell$. Similarly, when $n = 2p^\ell$, it is easy to verify that $p = 3$ since $\phi(2p^\ell) = \phi(p^\ell)$ and $|S_{2p^\ell}^{(3)}| = |S_{p^\ell}^{(3)}|$. Therefore, n can be of the form 3^ℓ or $2 \times 3^\ell$ where $\ell > 1$. Now, for the converse part, when n is of the form 3^ℓ or $2 \times 3^\ell$, it follows from Corollary 2 of [7] that $\phi(\phi(n)) = |S_{3^\ell}^{(3)}| = \phi(3^{\ell-1})$. □

References

1. D. Burton. *Elementary Number Theory*, 7th ed., Tata McGraw-Hill, 2012.
2. T. P. Dence and J. B. Dence. Cubic And Quartic Residues Modulo A Prime, *Missouri Journal of Mathematical Sciences*, Volume 7, Number 1, Pages 24 - 31, 1995. https://doi.org/10.35834/1995/0701024
3. C. F. Gauss. *Disquisitiones arithmeticae*, Translated into English by Arthur A., Clarke, S. J. Yale University Press, New Haven, Conn.-London, 1966.
4. S. Gun, B. Ramakrishnan, B. Sahu and R. Thangadurai. Distribution of quadratic non-residues which are not primitive roots, *Math. Bohem.*, Volume 130, Number 4, 2005.
5. M. Křížek, L. Somer, A necessary and sufficient condition for the primality of Fermat numbers, *Math. Bohem.*, Volume 126, 2001.
6. T. Nagell. *Introduction to Number Theory*, New York: Wiley, 1951.
7. V.P. Ramesh, R. Gowtham and S. Sinha. A note on cubic residues modulo n. *Indian J Pure Appl Math.*, 2022. https://doi.org/10.1007/s13226-022-00230-z

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.