International Mathematical Forum, Vol. 8, 2013, no. 2, 67 - 72

Cubic Residue Characters

Dilek Namli

Balikesir Universitesi, Fen-Edebiyat Fakultesi
Matematik Bolumu, 10145 Balikesir, Turkey
dilekd@balikesir.edu.tr

Abstract

In this study, we investigate for cubic residues of the known results on quadratic residues. We find solutions conditions the equations of cubic residues of the form $x^3 \equiv a(p)$ and $x^3 \equiv a(\pi)$.

Mathematics Subject Classification: 11A41; 11A15

Keywords: Rational prime; comlex prime; non-cubic residue

1 Introduction

The solutions conditions of linear and quadratic congruence are very well known. In this study we obtain the related to the results.solution conditions of the cubic congruence in D modes prime and rational prime.

2 Results

Definition 2.1 *If π, is the prime number in D, and if it is $\pi \nsim 1-\omega$ (i.e. N $\pi \neq 3$), the cubic character of α in mode π will be as follows:*

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & ,if\ \alpha\ divided\ by\ \pi \\ \alpha^{(n\pi-1)/3}\ (\pi) & ,if\ \alpha\ not\ divided\ by\ \pi \end{cases}$$

Here, $\alpha^{(n\pi-1)/3}\ (\pi)$ is found to be 1 in π mode ,or it is equal to ω or ω^2. This character functions the role of quadratic residue theory of Legendre symbol in according to the cubic residue theory.

Definition 2.2 *If it is $\left(\frac{\alpha}{\pi}\right)_3 = 1, \alpha$ is a cubic residue in the π modes. Otherwise, it will be called as non-cubic residue. In the literature, $\chi_\pi(\alpha)$ can be replaced with $\left(\frac{\alpha}{\pi}\right)_3$.*

Conclusion 2.3 *The multiplication of two cubic residues two elements which are non-cubic residues (ω andω^2) from different types will be a cubic residue. Besides, the multiplication of a cubic residue and a non-cubic residue (ω orω^2) and two non-cubic residues from the same types (ω and ω or ω^2andω^2) will be a non-cubic residue. It is very significant here to know that this case is different from quadratic residues.*

Proof. This can be seen in the definition of cubic residue character.? ■

Theorem 2.4 *Suppose that π is the prime in D and that it is $N\pi = p$. If the congruence of $x^3 \equiv a\ (p)$ can be solved, then the congruence of $x^3 \equiv a\ (\pi)$ can also be solved.*

Proof. That can be seen in the $p = \pi\overline{\pi}$. ■

Example 2.5 *Let's suppose tat is $\alpha = 5 + 8\omega$ and $\pi = 1 + 3\omega$. In that case, it is $N(\alpha) = 49$ and $N(\pi) = 7$. As it is $7|49$, as part of description, it will be $\left(\frac{\alpha}{\pi}\right)_3 = 0$. In the reality; it is $\left(\frac{5+8\omega}{1+3\omega}\right)_3 = (5+8\omega)^{\frac{7-1}{3}} = (5+8\omega)^2\ (7)$and as it is $\omega \equiv 2\ (7)$, the following conguence will be obtained;*

$$(5+8\omega)^2 \equiv (5+8.2)^2 \equiv (21)^2 \equiv 0\ (7).$$

Theorem 2.6 *i) It is $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$*
ii) If $\alpha \equiv \beta\ (\pi)$ then is $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Proof. i) It will be $\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{(N\pi-1)/3} \equiv \alpha^{(N\pi-1)/3}.\beta^{(N\pi-1)/3} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$
ii) If $\alpha \equiv \beta\ (\pi)$, it will be $\left(\frac{\alpha}{\pi}\right)_3 = \alpha^{(N\pi-1)/3} \equiv \beta^{(N\pi-1)/3} \equiv \left(\frac{\beta}{\pi}\right)_3$. ■

Theorem 2.7 *i) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\alpha}{\pi}\right)_3^2 = \left(\frac{\alpha^2}{\pi}\right)_3$ and*
i) $\overline{\left(\frac{\alpha}{\pi}\right)_3} = \left(\frac{\overline{\alpha}}{\pi}\right)_3$.

Proof. In the description of cubic residue character, $\left(\frac{\alpha}{\pi}\right)_3$ is equal to 1, ω or ω^2 and the square of each of these numbers is equal to their conjugate. When we consider that it is $N\overline{\pi} = N\pi$, what we have is i) and ii). ■

Theorem 2.8 *If π, is the prime number in D and let's suppose that it is $N\pi \neq 3$. Then, it is $\left(\frac{-1}{\pi}\right)_3 = 1$.*

Proof. If π is prime number, then it is Nπ=p providing that p≡1 (3) is a rational prime number. If it is p≡1 (3), and then it is p=3k+1, k∈**Z** and as p is a prime number, k will be an even number. Then, as it is

$$\left(\frac{-1}{\pi}\right)_3 = (-1)^{(N\pi-1)/3},$$

it is $N\pi - 1 = p - 1 = 3k + 1 - 1 = 3k$ and therefore, it is

$$\left(\frac{-1}{\pi}\right)_3 = (-1)^{\frac{3k}{3}} = (-1)^k.$$

As the k is an even, then it is

$$\left(\frac{-1}{\pi}\right)_3 = 1.$$

If it is $q \equiv 2(3)$ and q is a rational prime number, then q is a prime number in D. As it is $Nq = q$. $\overline{q} = q^2$, it is $Nq - 1 = q^2 - 1$. As it is $q \equiv 2(3)$ and also it is a prime number, then q is an odd number. In that case, $Nq - 1$ is an even number and therefore, $\frac{Nq-1}{3}$ is also an even number. If this is the case,it is $\left(\frac{-1}{q}\right)_3 \equiv (-1)^{(Nq-1)/3}$=1. ■

Remark 2.9 *The cubic character of -1 in each π mode, will be 1 can be seen from that is $(-1)^3 = -1$. We know that $p \equiv 1(3)$ as a prime number and $N\pi = p$ and $a^{\frac{p-1}{3}} \equiv 1$, ω, ω^2 (p). In other words, the $\frac{p-1}{3}$. powers of the elements of $\mathbb{Z}_p - \{0\}$ are 1, ω, ω^2 which are equivalent to the elements in $\mathbb{Z}_p$. Therefore, the element of $p-1$ are some how gathered under 3 groups. In each of these groups, the number of elements is $\frac{p-1}{3}$.*

$K_p = \{k|\ k, is\ a\ residue\ \frac{p-1}{3}th.a\ different\ from\ zero\ in\ p\ mode\}$ which can be considered to be as a main description. In other words, the K_p, the powers of $\frac{p-1}{3}th.$ of the elements of $\mathbb{Z}_p - \{0\}$ consist of values in p *mode*.

Theorem 2.10 *K_p, is a group depending on the multiplication in $\mathbb{Z}_p$ and in fact it is a subgroup of $\mathbb{Z}_p^*$.*

Proof. We have the following as K_p=$\{1,\omega,\omega^2\}$,

i) We see that it is $a(bc) = (ab)c$ for $\forall a, b, c \in K_p$.

ii) 1 is the unit element of K_p.

iii) As it is $1.1 = 1, x.\omega^2 = 1$, the opposite of 1 is 1, the opposite of ω is ω^2 and the opposite of ω^2 is ω.

K_p from i, ii and iii is a group under the multiplication.

Now let's see that the $\forall a, b \in K_p$ is $ab^{-1} \in \mathbb{Z}_p^*$.

$1.\omega^{-1} = 1.\omega^2 = \omega^2 \in \mathbb{Z}_p^*, 1.(\omega^2)^{-1} = 1.\omega = \omega \in \mathbb{Z}_p^*, \omega.\omega^{-1} = \omega.\omega^2 \equiv 1 \in \mathbb{Z}_p^*,$

$\omega.(\omega^2)^{-1} = \omega.\omega = \omega^2 \in Z_p^*, 1.1^{-1} = 1.1. = 1 \in Z_p^*$ and $\omega^2.(\omega^2)^{-1} = \omega^3 \in Z_p^*$. ■

Example 2.11 *Let's the K_7 and K_{13}. It is $p = 7$ and $\frac{p-1}{3} = 2$. In mode 7, it is $1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 2, 4^2 \equiv 2, 5^2 \equiv 4, 6^2 \equiv 1$ and it is $\omega \equiv 4\ (7), \omega^2 \equiv 2(7)$,*

it is also $K_7 = \{1, 2, 4\} \equiv \{1, \omega, \omega^2\}$. *Now, let's suppose that* $p = 13$. *Then it is* $\frac{p-1}{3}$=*4. In mode*13 , *as it is* $1^4 \equiv 1$, $2^4 \equiv 3, 3^4 \equiv 3, 4^4 \equiv 9, 5^4 \equiv 1, 6^4 \equiv 9, 7^4 \equiv 9, 8^4 \equiv 1, 9^4 \equiv 9, 10^4 \equiv 3, 11^4 \equiv 3, 12^4 \equiv 1$ *and* $\omega \equiv 9(13), \omega^2 \equiv 3(13)$, *what we have is* $K_{13} = \{1, 3, 9\} \equiv \{1, \omega, \omega^2\}$.

Theorem 2.12 ***(Cubic reciprocity law)*** *Let* π_1 *and* π_2 *is* 1.*type prime, that* $N\pi_1, N\pi_2 \neq 3$ *and* $N\pi_1 \neq N\pi_2$. *Then is* $\left(\frac{\pi_1}{\pi_2}\right)_3 = \left(\frac{\pi_2}{\pi_1}\right)_3$ *[5].*

Theorem 2.13 *If it is* $\pi = a+b\omega$ *and* $\pi \equiv 2(3)$ *then we have* $\left(\frac{\omega}{\pi}\right)_3 = \omega^{(a+b+1)/3}$ *[4]*

Theorem 2.14 *If it is* $\pi = a + b\omega$ *and* $\pi \equiv 2(3)$ *then it is* $\left(\frac{1-\omega}{\pi}\right)_3 = \omega^{2(a+1)/3}$ *[4].*

Theorem 2.15 *If* π, *is a* 1.*type rational prime number, then it is* $\left(\frac{2}{\pi}\right)_3 = 1$. *In other words,* 2 *is a cubic residue in every* q *mode providing that* $\pi = q > 2$ *it is* 1.*type rational prime number.*

Proof. Suppose that $\pi = q$ is a rational prime number. It cannot be $q = 2$, because then it is $2|2$ and $\left(\frac{2}{q}\right)_3 = 0$. While $q \equiv 2(3)$ is a rational prime number, we know that in mode q, there are q pieces of cubic residue, in other words, in q *mode*, each a number is a cubic residue. Therefore, 2 in mode q is a cubic residue. ■

Theorem 2.16 *If it is* $\pi = a + b\omega$, 1.*type complex prime number, to solve the* $x^3 \equiv 2\ (\pi)$ *the necessary and sufficient condition is* $\pi \equiv 1\ (2)$, *in other words it needs to be* $a \equiv 1\ (2)$ *and* $b \equiv 0\ (2)$.

Proof. Suppose that $x^3 \equiv 2\ (\pi)$ is something which can be solved. Then, it is $\left(\frac{2}{\pi}\right)_3 = 1$. As both of 2 and π are 1.type prime numbers, as required by the cubic reciprocity law, we can write as follows: $\left(\frac{2}{\pi}\right)_3 = \left(\frac{\pi}{2}\right)_3$. As it is $\left(\frac{\pi}{2}\right)_3 \equiv \pi^{(N2-1)/3}\ (2)$ and $N(2) = 2^2 = 4$, it is $\left(\frac{\pi}{2}\right)_3 \equiv \pi\ (2)$. Therefore, it needs to be $\left(\frac{\pi}{2}\right)_3 \equiv \pi \equiv 1\ (2)$ so that we can have the following ;$\left(\frac{\pi}{2}\right)_3 = 1$. The reverse case can also be possible. ■

Example 2.17 *Can the following congruence is a soluble one?*

$$x^3 \equiv 2\ (5 + 6\omega)$$

As $\pi = 5 + 6\omega$ *is* 1.*type, in other words,* $\pi \equiv 2\ (3)$ *and it is* $\pi \equiv 1\ (2)$, *as required by the theorem* 16, *it is* $\left(\frac{2}{5+6\omega}\right)_3 = 1$. *In other words, the congruence of* $x^3 \equiv 2\ (5 + 6\omega)$ *can be solved. By using the Theorem 2.15, it is*

$$\begin{aligned} \left(\frac{2}{5+6\omega}\right)_3 &= \left(\frac{5+6\omega}{2}\right)_3 = (5+6\omega)^{N(2)-1} = 5 + 6\omega\ (2) \\ &\equiv 1 + 0\omega(2) \\ &\equiv 1(2). \end{aligned}$$

Remark 2.18 *Gauss, if it is $p \equiv 1(3)$, that demonstrates that A and B whole numbers exist as in $4p = A^2 + 27B^2$ and that these A and B whole numbers can be determined with only one single way except for signs.*

Theorem 2.19 *Suppose that it is $\pi = a+b\omega$, 1.type prime number and $N\pi = p = a^2 - ab + b^2$. If it is $p \equiv 1(3)$, to be able to solve the congruence of $x^3 \equiv 2$ (p) the necessary and sufficient condition is to find the C and D whole integers to make it $p = C^2 + 27D^2$.*

Proof. If the congruence of $x^3 \equiv 2$ (p) can be solved, then the congruence of $x^3 \equiv 2$ (π) can also be solved and as required by the Theorem 2.15, it is $\pi \equiv 1$ (2). If it is $p = a^2 - ab + b^2$ then it is $4p = 4a^2 - 4ab + 4b^2 = (2a - b)^2 + 3b^2$. Here if it is $2a - b = A$, $\frac{b}{3} = B$, as A is an odd number and b is an even number, A and B are even numbers. Then, can be written as $D = \frac{B}{2}$ and $C = \frac{A}{2}$ and thus obtained $p = C^2 + 27D^2$.

Now let's suppose that there exist C and D whole integers to make the $p = C^2 + 27D^2$, then it is $4p = (2C)^2 + 27(2D)^2$. With this equality, is obtained $B = \mp 2D$. In other words, B, and b are even numbers. If sothe following equality is obtained $\pi = a + b\omega \equiv 1$ (2) (but the following cannot be obtained $a \equiv 0(2)$, because, if so, it is $\pi \equiv 0(2)$) and the results is seen from the Theorem 2.15. ■

Example 2.20 *Let's take $p = 19$. The number p cannot be written as $C^2 + 27D^2$, the congruence of $x^3 \equiv 2$ (19) cannot be solved. In fact, as it is;$\left(\frac{2}{19}\right)_3 = 2^{N(19)-1/3} = 2^{120} \equiv 11(19)$ and $\omega \equiv 11$ (19), the following is obtained; is obtained $\left(\frac{2}{19}\right)_3 \equiv \omega$ (19). Now, let's take $\pi = 5 + 3\omega$, 1. type prime number in which it is $N\pi = 19$.*

$$\left(\frac{2}{5+3\omega}\right)_3 = \left(\frac{5+3\omega}{2}\right)_3 = (5+3\omega)^{N(2)-1/3} = 5 + 3\omega \equiv 1 + \omega \ (2)$$

and

$$1 + \omega = -\omega^2 \equiv (-1).\omega^2 \ (2)$$

$$\equiv 1.\omega^2 \ (2)$$

As it is, the following congruence is obtained

$$\left(\frac{2}{5+3\omega}\right)_3 = \omega^2 \ (2)$$

and therefore, the congruence of $x^3 \equiv 2$ $(5 + 3\omega)$ cannot be solved.

On the other hand, as the number of $p = 31$ *can be written as* $2^2+27.1 = 31$*, in reality, as it is* $\left(\frac{2}{31}\right)_3 = 2^{N(31)-1/3} = 2^{320} \equiv 1(31)$*, the congruence of* $x^3 \equiv 2$ (31) *can be solved and it is easy to see that* $x = 4$*. With the help of the other roots can be found as* $x\omega \equiv 20$ *and* $x\omega^2 \equiv 7(31)$*.*

Let's take now the $\pi = 5 + 6\omega$ $1.$*type prime number which is* $N\pi = 31$ *.*

$$\left(\frac{2}{5+6\omega}\right)_3 = \left(\frac{5+6\omega}{2}\right)_3 = (5+6\omega)^{N(2)-1/3} = 5+6\omega \equiv 1 \ (2)$$

is obtained and thus 2 *is found to be a cubic residue in* $5 + 6\omega$ *mode.*

When $p \equiv 1(3)$*, as* $\omega \in \mathbb{Z}_p$*, we are more interested in the cubic residues in* p *mode rather than the residues in* $\pi = a + b\omega$ *prime mode in* D*. Considering that* $k > 1$ *is a whole integer, as it is* $p = 3k$ *and* $p \equiv 2(3)$*,there is no* $\pi = a+b\omega$ *prime number whose in* D *norm is* p *norm, and as definition of cubic residue concept is described when it is* $N\pi \neq 3$*, there will be no limitations.*

References

[1] Jones, G.A., Jones J.M., Elemantary Number Theory, Springer-Verlag, Newyork , (1998), S.37-140.

[2] Flath, D.E., Introduction to Number Theory, A.Wiley-İnterscience Publication, (1989), s.63-104.

[3] Leveque, W.J., Fundamentals of Number Theory, Dover Publications, Newyork, (1997), s.47-93, 97-120, 270-273.

[4] Stark, H.M., An Introduction to Number Theory, Cambridge, London, (1979), s.51-117.

[5] Sun, Z.H., "On the theory of cubic residues and nonresidues", *Acta Arithmetica J.,* 4 (1998), s.291-335.

Received: September, 2012