International Journal of Algebra, Vol. 9, 2015, no. 5, 245 - 249
HIKARI Ltd, www.m-hikari.com
http://dx.doi.org/10.12988/ija.2015.5525

Some Results on Cubic Residues

Dilek Namlı

Balıkesir Üniversiresi Fen-Edebiyat Fakültesi
Matematik Bölümü
10145 Çağış Kampüsü , Balikesir, Turkey

Abstract

In this paper, we examine the solubility of the cubic congruence $x^3 \equiv a\ (p)$ where p is a rational prime and a and x are integers. Here, we give some results and examples related with the cubic residues.

Mathematics Subject Classification: 11A41, 11A15

Keywords: Rational prime, cubic residue, primitive root

1. Introduction

Let p be a rational prime and a be an integer. If there is an integer x such that $x^3 \equiv a\ (p)$ then a is said to be a cubic residue in mod p.

$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$ where $\omega = \frac{-1+\sqrt{-3}}{2}$. For $p \in \mathbb{Z}[\omega]$, the norm of p is given by $Np = p.\overline{p} = a^2 - ab + b^2$ where $\overline{p}$ is the complex conjugate of p. If $\theta \in \mathbb{Z}[\omega]$, then the cubic residue character $\left(\frac{\theta}{p}\right)_3$ of θ in modulo p is defined by

$$\begin{cases} 0 & \text{if } p \mid \theta \\ \omega^i & \text{if } \theta^{(Np-1)/3} \equiv \omega^i\ (p) \end{cases}$$

where $i \in \{0, 1, 2\}$.

Cubic residues have been studied by several authors in [1],[2],[3],[4] and [5].

In this paper, we obtaine some results and examples related with the cubic residues.

2. Main Results

Theorem 1. *Let p be a rational prime for which $p \equiv 1\ (3)$. Then the equivalence $x^3 \equiv a\ (p)$ is solvable if and only if $a^{(p-1)/3} \equiv 1\ (p)$.*

Proof. This theorem is the special case $k = 3$ of the Euler's Criterion. □

Theorem 2. *If p is a rational prime and $a \in \mathbb{Z}$, then $\left(\frac{a^3}{p}\right) = 1$.*

Proof. We know that $\left(\frac{a^3}{p}\right) = \left(\frac{a}{p}\right)^3$. As $\left(\frac{a}{p}\right)$ is equivalent to ω or to ω^2, we find

$$\left(\frac{a^3}{p}\right) = \left(\frac{a}{p}\right)^3 = 1.$$

□

Example 1. *Let us consider whether 9 is a cubic residue in mod 7 or not. Since*

$$\left(\frac{9}{7}\right)_3 \equiv \left(\frac{2}{7}\right)_3 \equiv 2^{\frac{7-1}{3}} \equiv 2^2 \equiv 4,$$

$\omega^2 \equiv 4\ (7)$. Thus $\left(\frac{9}{7}\right)_3 \equiv \omega^2$. Therefore 9 is not a cubic residue in mod 7.

Example 2. *We consider the equivalence $x^3 \equiv 7\ (15)$.*

$$\left(\frac{15}{7}\right)_3 \equiv \left(\frac{1}{7}\right)_3 \equiv 1^{\frac{7-1}{3}} \equiv 1^2 \equiv 1(7).$$

Then, 15 is a cubic residue in mod 7. In other words, the equivalence $x^3 \equiv 15\ (7)$ is solvable. In fact, $x = 1$, $x = \omega$ and $x = \omega^2$ are the roots of the equivalence $x^3 \equiv 15 \equiv 1\ (7)$. Since $\omega = \frac{-1+\sqrt{-3}}{2}$, we get the roots of this equivalence as

$$x \equiv 1(7),\ x \equiv 4(7) \text{ and } x \equiv 2(7).$$

Example 3. *Is the equivalence $x^3 \equiv 41\ (73)$ solvable? Since*

$$\left(\frac{73}{41}\right)_3 \equiv 41^{\frac{73-1}{3}} \equiv 41^{24} \equiv (41^2)^{12} \equiv 2^{12} \equiv 8(73),$$

we obtain $\omega \equiv 8\ (73)$ and $\left(\frac{73}{41}\right)_3 = \omega$. Therefore $x^3 \equiv 41\ (73)$ is unsolvable.

Theorem 3. *If $p \equiv 2\ (3)$ is a rational prime and a is a positive integer such that $(a, p) = 1$, then a in mod p is a cubic residue.*

Proof. Let $p \equiv 2\ (3)$ be a prime and let a be a positive integer such that $(a, p) = 1$.Since $p \equiv 2\ (3)$, we can write $p = 3k + 2, k \in \mathbb{Z}$. In this case,

$$Np = p.\overline{p} = (3k + 2)(3k + 2) = 9k^2 + 12k + 4$$

and

$$\frac{Np - 1}{3} = 3k^2 + 4k + 1.$$

From $(a,p)=1$ and the Fermat's little theorem, we have

$$a^{p-1}=a^{3k+1}\equiv 1(p).$$

Thus

$$a^{(Np-1)/3}=a^{3k^2+4k+1}=a^{(3k+1)(3k+1)}\equiv (a^{(3k+1)})^{3k+1}\equiv 1^{3k+1}\equiv 1(p).$$

□

Corollary 4. *If $p\equiv 2\ (3)$ is a rational prime, then there are exact p cubic residues in mod p different from each other. In other words, all elements of $\mathbb{Z}_p$ are cubic residues.*

Proof. Let $p\equiv 2\ (3)$ be a rational prime and let g be a primitive root. Also let us choose $a\in\{1,2,...,p-1\}$ and $k\in\{0,1,...,p-2\}$ providing the equivalence $g^k\equiv a\ (p)$.

Since $(3,p-1)=1$, there are integers x' and y' such that $3x'+(p-1)y'=1$. If we take $x=x'k$ and $y=y'k$, then we can write as $3x+(p-1)y=k$.

Since $g^{p-1}\equiv 1\ (p)$, we find

$$a\equiv g^k=g^{3x+(p-1)y}=(g^x)^3(g^{p-1})^y\equiv (g^x)^3\ (p).$$

That is, a is a cube in mod p. Since $0\equiv 0^3\ (p)$, there are exact different p cubes in mod p. □

Example 4. *Let $p=11$. Since $0\equiv 0^3\ (11)$, $1\equiv 1^3\ (11), 2\equiv 7^3\ (11), 3\equiv 9^3\ (11), 4\equiv 5^3\ (11), 5\equiv 3^3\ (11), 6\equiv 8^3\ (11), 7\equiv 6^3\ (11), 8\equiv 2^3\ (11), 9\equiv 4^3\ (11), 10\equiv 4^3\ (11)$ and $11\equiv 10^3\ (11)$, all numbers in $\mathbb{Z}_{11}$ are cubic residues.*

Theorem 5. *If $p\equiv 1(3)$ is a rational prime, then the number of different cubic residues in mod p is $\frac{p+2}{3}$.*

Proof. Let $p\equiv 1(3)$ be a rational prime. For every k element in $\{3,6,9,...,p-1\}$,

$$g^k=g^{3t}=(g^t)^3$$

is a cube where g is a primitive root and $t\in\mathbb{Z}$. Here all these g^k 's are different. Then, there are at least $\frac{p-1}{3}$ nonzero cubes in mod p.

On the other hand, each cube is the form $a\equiv b^3\ (p)$. From $p\equiv 1(3)$ and the Fermat's little theorem,

$$a^{(p-1)/3}\equiv b^{p-1}\equiv 1\ (p).$$

By the Lagrange's Theorem for polynomials, there is the most $\frac{p-1}{3}$ root of the equivalence

$$a^{(p-1)/3}\equiv b^{p-1}\equiv 1\ (p),$$

that is, $\frac{p-1}{3}$ is an upper bound for the total number of cubes in mod p. Then there are exact $\frac{p-1}{3}$ non-zero cubes. When counting the zero, then there are $\frac{p-1}{3}+1=\frac{p+2}{3}$ cubes in mod p. □

Theorem 6. *If p is an odd prime number then $-a \equiv a\ (p)$.if and only if is $a \equiv 0\ (p)$.*

Proof. Since $(2, p) = 1$, we get

$$a \equiv -a\ (p) \Leftrightarrow 2a \equiv 0\ (p) \Leftrightarrow a \equiv 0\ (p).$$

□

Corollary 7. *If p is an odd prime number then cubic residues in $\mathbb{Z}_p$ are*

$$0^3, 1^3, 2^3, 3^3, \cdots, \left(\frac{p-1}{2}\right)^3, \left(\frac{p+1}{2}\right)^3, \cdots, (p-1)^3 \equiv -1.$$

Corollary 8. *Let p be an odd prime number. An integer a is a cubic residue in $\mathbb{Z}_p$ if and only if $-a$ is a cubic residue in $\mathbb{Z}_p$.*

Proof. If a is a solution of $x^3 \equiv k\ (p)$ then $a^3 \equiv k\ (p)$. Since

$$(-a)^3 = -a^3 \equiv -k\ (p) \Leftrightarrow a^3 \equiv k\ (p),$$

$-a$ is a also solution of $x^3 \equiv k\ (p)$. □

Theorem 9. *Let $p \equiv 2\ (3)$ be a prime such that $p \neq 2$. The sum of cubic residues providing the equivalence $x^3 \equiv k\ (p)$ is equivalent to zero in mod p.*

Proof. Let $p \equiv 2\ (3)$ be a prime. From the Corollary 2.4, all cubic residues are different and these are 0, 1, 2, ..., $p-1$. Their sum is

$$0 + 1 + 2 + ... + p - 1 = \frac{p(p-1)}{2}.$$

As p is prime and $p \neq 2$, $p-1$ is an even number, that is, $\frac{p-1}{2} \in \mathbb{Z}$. Then, we find

$$0 + 1 + 2 + ... + p - 1 = \frac{p-1}{2}.p \equiv 0\ (p).$$

□

Theorem 10. *Let $p \equiv 1\ (3)$ be a prime. The sum of the cubic residues providing the equivalence of $x^3 \equiv a\ (p)$ is equivalent to zero in mod p.*

Proof. Let $p \equiv 1\ (3)$ be a prime. From the Theorem 2.5, there are $\frac{p+2}{3}$ different cubic residues.

If $p \equiv 1\ (3)$ then we can write $p = 3k + 1$, $k \in \mathbb{Z}$. As p is a prime, k is an even number. As $\frac{p+2}{3} = k + 1$, $\frac{p+2}{3}$ is an odd number.

One of the cubic residues is zero. Let $a_0 = 0$. Then, there are $\frac{p+2}{3} - 1 = \frac{p-1}{3}$ different cubic residues. Also, from the Corollary 2.8, if a is a cubic residue in $\mathbb{Z}_p$, then $-a$ is a cubic residue in $\mathbb{Z}_p$ too. In this case, the sum of the cubic residues is

$$a_0 + a_1 + \cdots + a_{\frac{p-1}{3}} = a_0 + (a_1 + \cdots + a_{\frac{p-1}{6}}) + (-a_1 - \cdots - a_{\frac{p-1}{6}}) \equiv 0\ (p).$$

□

Theorem 11. *If one of solutions of the equivalence $x^3 \equiv a\ (m)$ is x, then the others are $x\omega$ and $x\omega^2$.*

Proof. If $a = 1$ then, we know that the solutions of $x^3 \equiv 1\ (m)$ are

$$x = 1,\ x\omega = 1.\omega \text{ and } x\omega^2 = 1.\omega^2.$$

If $a \neq 1$ and if one of the solutions of $x^3 \equiv a\ (m)$ is x, then

$$(x\omega)^3 = x^3\omega^3 \equiv x^3 \equiv a\ (m),$$

and

$$(x\omega^2)^3 = x^3\omega^6 \equiv x^3 \equiv a\ (m).$$

□

Corollary 12. *The sum of solutions of the equivalence $x^3 \equiv a\ (m)$ is equivalent to zero in mod m.*

Proof. From the Theorem 2.10, we know that the solutions of the equivalence $x^3 \equiv a\ (m)$ are x, $x\omega$ and $x\omega^2$. Then we have

$$\begin{aligned} x + x\omega + x\omega^2 &= x + x\omega + x(-1 - \omega) \\ &= 0. \end{aligned}$$

□

References

[1] D. S. Xing, Z. F. Cao, X. L. Dong, *Identity based signature scheme based on cubic residues*, Sci. China Inf. Sci. 54 (2011), no. 10, 2001–2012. http://dx.doi.org/10.1007/s11432-011-4413-6

[2] K. Ireland, M. A. Rosen, *A classical introduction to modern number theory*, Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. xiv+389 pp. ISBN: 0-387-97329-X. http://dx.doi.org/10.1007/978-1-4757-2103-4

[3] D. Namli, *Cubic residue characters,* Int. Math. Forum 8 (2013), no. 1-4, 67–72.

[4] Z. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. 84 (1998), no. 4, 291–335.

[5] Z. Sun, *Cubic residues and binary quadratic forms,* J. Number Theory 124 (2007), no. 1, 62–104. http://dx.doi.org/10.1016/j.jnt.2006.08.001

Received: May 27, 2015; Published: June 23, 2015