International Journal of Algebra, Vol. 12, 2018, no. 8, 333 - 336
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2018.81238

On Integer Solutions of the Cubic Equations Over Certain Fields $\mathbb{Z}_n$

Dilek Namlı

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

Abstract

In this paper, we find the integer solutions of the cubic equations $ax^3+bx^2+cx+d=0$ in $\mathbb{Z}_n$, for $n=\frac{3ac-b^2}{3a^2}$, by using the index function. Also, we give some examples.

Mathematics Subject Classification: 11A41, 11A15

Keywords: Cubic equations, index function

1 Introduction

A cubic equation has the form

$$ax^3+bx^2+cx+d=0$$

where $a,b,c,d\in\mathbb{Z}$ and $a\neq 0$. All cubic equations have either one real root, or three real roots.

Here, we are interesting with the cubic equations over a finite field $\mathbb{Z}_n$, for integer $n\geq 2$.

In the literature, there are many papers on the cubic equations over a finite field $\mathbb{Z}_n$, for integer $n\geq 2$ (for example,please see, [2] and [4]).

On the other hand, let g be a primitive root in $\mathbb{Z}_n$, for integer $n\geq 2$. If there exist an integer t such that $0\leq t\leq \varphi(n)-1$ and $g^t\equiv a(mod\ n)$ when $(a,n)=1$, then t is called the index of a and it is denoted by $t=I(a)$.

The properties of the index function are similar to the logarithm function. These properties are the followings.

1) $I(a.b) = I(a) + I(b)\ (mod\ \varphi(n))$.

2) If $(a, b) = 1$ then $I(a/b) = I(a) - I(b)\ (mod\ \varphi(n))$.

3) If $r \geq 1$ then $I(a^r) \equiv r.I(a)\ (mod \varphi(n))$.

4) $I(1) = 0$ and $I(g) = 1$.

5) If $n > 2$ then $I(-1) = \varphi(n)/2$.

6) If g' is a primitive root different from g in $\mathbb{Z}_n$ then $I_g(a) = I_g(g').I_{g'}(a)$ $(mod\ \varphi(n))$.

For more detailed information on the index function, please see [1] and [3].

In this paper, we find the integer solutions of the cubic equations $ax^3 + bx^2 + cx + d = 0$ in $\mathbb{Z}_n$, for $n = \frac{3ac-b^2}{3a^2}$,by using the index function. Also, we give some examples.

2 Main Results

Theorem 2.1 *Let $ax^3+bx^2+cx+d = 0$ be a cubic equation for $a, b, c, d \in \mathbb{Z}$ and $a \neq 0$. For $k = \frac{9abc-27a^2d-2b^3}{27a^3}$ and $n = \frac{3ac-b^2}{3a^2}$,*

i) if $k \equiv 0\,(mod\ n)$ then unique solution of this cubic equation is $x \equiv \frac{b}{3a}\,(mod\ n)$.

ii) if $k \not\equiv 0\,(mod\ n)$ then this cubic equation is solvable $\Longleftrightarrow (3, \varphi(n)) \mid I(k)$.

Proof. Firstly, we divide both sides of the $ax^3 + bx^2 + cx + d = 0$ by a.

Now, if we write $x - \frac{b}{3a}$ instead of x in the equation, i.e.,

$$a(x - \frac{b}{3a})^3 + b(x - \frac{b}{3a})^2 + c(x - \frac{b}{3a}) + d = 0$$

then we find

$$x^3 + \frac{3ac - b^2}{3a^2}x = \frac{9abc - 27a^2d - 2b^3}{27a^3}.$$

Therefore, we can write the congruence

$$x^3 \equiv \frac{9abc - 27a^2d - 2b^3}{27a^3} \left(mod\ \frac{3ac - b^2}{3a^2}\right).$$

Here, if we say

$$k = \frac{9abc - 27a^2d - 2b^3}{27a^3}$$

and

$$n = \frac{3ac - b^2}{3a^2}$$

then we have the congruence

$$x^3 \equiv k \,(mod\ n)\,.$$

If $k \equiv 0\,(mod\ n)$ then $x^3 \equiv 0\,(mod\ n)$ and $x \equiv 0\,(mod\ n)$. Thus, the unique solution is $x \equiv \frac{b}{3a}\,(mod\ n)$.

If $k \not\equiv 0\,(mod\ n)$ then we get the linear congruence

$$\begin{aligned} I(x^3) &\equiv I(k)\,(mod\ \varphi(n)) \\ 3.I(x) &\equiv I(k)\,(mod\ \varphi(n))\,. \end{aligned}$$

This linear congruence is solvable if and only if $(3, \varphi(n)) \mid I(k)$.

If $(3, \varphi(n)) \mid I(k)$ then

a) $(3, \varphi(n)) = 1$ and there is a unique solution in $\mathbb{Z}_n$.

b) $(3, \varphi(n)) = 3$, (or, $3 \mid I(k)$) and there are three solutions in $\mathbb{Z}_n$.

Finally, if $3 \nmid I(k))$ then there is no solution in $\mathbb{Z}_n$.

Example 2.2 *Let us consider the cubic equation* $4x^3 + 6x^2 + 6x + 7 = 0$. *Here,* $a = 4$, $b = 6$, $c = 6$ *and* $d = 7$. *Thus, if we write* $x - \frac{b}{3a} = x - \frac{1}{2}$ *instead of* x *in the equation then we found*

$$\begin{aligned} 4(x^3 - \frac{3}{2}x^2 + \frac{3}{4}x - \frac{1}{8}) + 6(x^2 - x + \frac{1}{4}) + 6x - 3 + 7 &= 0 \\ 4x^3 - 6x^2 + 3x - \frac{1}{2} + 6x^2 - 6x + \frac{3}{2} + 6x + 4 &= 0 \\ 4x^3 + 3x + 5 &= 0. \end{aligned}$$

Therefore, we obtain the congruence

$$\begin{aligned} 4x^3 &\equiv -5\,(mod\ 3) \\ x^3 &\equiv 1\,(mod\ 3)\,. \end{aligned}$$

Now we solve this equation by using the index function. Then, we have

$$\begin{aligned} I(x^3) &\equiv I(1)\,(mod\ \varphi(3)) \\ 3.I(x) &\equiv 0\,(mod\ 2) \\ I(x) &\equiv 0\,(mod\ 2) \\ x &\equiv 1\,(mod\ 3)\,. \end{aligned}$$

Since we write $x - \frac{1}{2}$ *instead of* x, *we find the solution as* $x = 1 - \frac{1}{2} = \frac{1}{2} \equiv 2\,(mod\ 3)$ *in the ring* $\mathbb{Z}_3$.

Example 2.3 *Let us consider the cubic equation* $x^3 + 5x + 2 = 0$. *Here,* $a = 1$, $b = 0$, $c = 5$ *and* $d = 2$. *Since* $x - \frac{b}{3a} = x$, *we obtain the same equation. Therefore, we have the congruence*

$$\begin{aligned} x^3 &\equiv -2 \,(mod\ 5) \\ x^3 &\equiv 3 \,(mod\ 5)\,. \end{aligned}$$

If we use the index function, then we have

$$\begin{aligned} I(x^3) &\equiv I(3) \,(mod\ \varphi(5)) \\ 3.I(x) &\equiv 3 \,(mod\ 4) \\ I(x) &\equiv 1 \,(mod\ 4) \\ x &\equiv 2 \,(mod\ 5)\,. \end{aligned}$$

Thus, we find the solution as $x \equiv 2 \,(mod\ 5)$ *in the ring* $\mathbb{Z}_5$.

References

[1] D. E. Flath, *Introduction to Number Theory*, AMS Chelsea Publishing, Providence, RI, 2018.

[2] V. P. Gabrielyan, Linearized coverings for sets of special solutions of one cubic equation over a finite field, *Dokl. Nats. Akad. Nauk Armen.*, **118** (2018), no. 2, 115-118.

[3] D. Namli, *Cubic Residues*, PhD Thesis, Balikesir, 2001.

[4] L. Zhao, Small prime solutions to cubic equations, *Sci. China Math.*, **59** (2016), no. 10, 1909-1918. https://doi.org/10.1007/s11425-016-5150-5

Received: December 21, 2018; Published: December 27, 2018