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

Dilek Namlı

Balıkesir Üniversitesi Fen-Edebiyat Fakültesi, Matematik Bölümü
10145 ÇAĞIŞ Kampüsü, Balıkesir, 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) \( I(a,b) = I(a) + I(b) \pmod{\varphi(n)} \).
2) If \((a, b) = 1\) then \( I(a/b) = I(a) - I(b) \pmod{\varphi(n)} \).
3) If \( r \geq 1 \) then \( I(a^r) \equiv r \cdot I(a) \pmod{\varphi(n)} \).
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 \( I_g(a) = I_g(g') \cdot I_{g'}(a) \pmod{\varphi(n)} \).

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 \( k \equiv 0 \pmod{n} \) then unique solution of this cubic equation is \( x \equiv \frac{b}{3a} \pmod{n} \).

ii) if \( k \not\equiv 0 \pmod{n} \) then this cubic equation is solvable \( \iff (3, \varphi(n)) | I(k) \).

**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.,

\[
 a\left(x - \frac{b}{3a}\right)^3 + b\left(x - \frac{b}{3a}\right)^2 + c\left(x - \frac{b}{3a}\right) + d = 0
\]

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

\[ x^3 \equiv k \pmod{n}. \]

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

If \( k \not\equiv 0 \pmod{n} \) then we get the linear congruence

\[
\begin{align*}
I(x^3) & \equiv I(k) \pmod{\varphi(n)} \\
3I(x) & \equiv I(k) \pmod{\varphi(n)}.
\end{align*}
\]

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

If \((3, \varphi(n)) | I(k)\) then

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

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

Finally, if \(3 \not| I(k)\) 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

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

Therefore, we obtain the congruence

\[
\begin{align*}
4x^3 & \equiv -5 \pmod{3} \\
x^3 & \equiv 1 \pmod{3}.
\end{align*}
\]

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

\[
\begin{align*}
I(x^3) & \equiv I(1) \pmod{\varphi(3)} \\
3I(x) & \equiv 0 \pmod{2} \\
I(x) & \equiv 0 \pmod{2} \\
x & \equiv 1 \pmod{3}.
\end{align*}
\]

Since we write \(x - \frac{1}{2}\) instead of \(x\), we find the solution as \(x = 1 - \frac{1}{2} = \frac{1}{2} \equiv 2 \pmod{3}\) 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

\[
x^3 \equiv -2 \pmod{5} \\
x^3 \equiv 3 \pmod{5}.
\]

If we use the index function, then we have

\[
I(x^3) \equiv I(3) \pmod{\varphi(5)} \\
3I(x) \equiv 3 \pmod{4} \\
I(x) \equiv 1 \pmod{4} \\
x \equiv 2 \pmod{5}.
\]

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

References


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