Neutrosophic Sets and Systems

Volume 49 Article 15

4-12-2022

Algebraic Properties of Finite Neutrosophic Fields

Chalapathi T

Kumaraswamy Naidu K

Harish Babu D

Neutrosophic Sets and Systems, Vol. 49, 2022
University of New Mexico

Algebraic Properties of Finite Neutrosophic Fields

Chalapathi T [1]*, Kumaraswamy Naidu K [1] and Harish Babu D [1]

[1]Department of Mathematics, Sree Vidyanikethan Engineering College, Tirupathi-517502, A.P. Indian

*Correspondence: chalapathi.tekuri@gmail.com; Tel.: +919542865332

Abstract: We explore a finite Neutrosophic field $\boldsymbol{F_p(I)}$ and its Neutrosophic multiplicative group $\boldsymbol{F_p(I)^\times}$ in this study. We first show $\boldsymbol{\left|F_p(I)^\times\right| = (p-1)^2}$ and then its algebraic properties are studied. The Neutrosophic Fermat's and Little Fermat's theorems over $\boldsymbol{F_p(I)^\times}$ are then proved. Finally, this paper investigates some applications of Neutrosophic Fermat's theorem over $\boldsymbol{F_p(I)^\times}$ with various illustrations.

Keywords: Neutrosophic Field; Neutrosophic Group; Neutrosophic Fermat's Theorem, Neutrosophic Little Fermat's Theorem.

1. Introduction

In the algebraic sense, finite field theory deals with the algebraic concepts and related systems with the properties of different sets of complete residue system $Z_n = \{0, 1, 2, \ldots\ldots, n-1\}$ of integers modulo n. In this paper, we consider some particularly important sets of numbers $Z_p = \{0, 1, 2, \ldots\ldots, p-1\}$ under addition and multiplication modulo a prime p. The theory of these numbers is concerned, at least in its elementary aspects, with properties of the scalars and more particularly with the numbers in Z_p and their related concepts. We shall make no attempt to construct the set of numbers axiomatically, assuming instead that they are already well-known and that any reader of this paper is familiar with many elementary concepts and results about finite fields. Among these some are defined and stated to refresh in algebraic terminology. We can generally define a field F as an abelian group under addition together with multiplicative operation such that the structure $(F-\{0\},\cdot)$ is also an abelian group satisfies the distributive axioms: $a(b+c) = ab + ac$ and $(b+c)a = ba + ca$. Now we shift our attention to the finite field F_p, we are considering in this paper [1]. For a prime p, we represent the number of elements in the field F_p is p. Also, in any finite field of order p, we have $ap = 0$ for every a in F_p. This means that the characteristic of F_p is p. Further, all fields of order p are isomorphic, that is, there is a unique field up to isomorphism of order p.

Classic algebra, control systems, neural networks, decision and estimation issues have all been reformed and adapted to adhere to Neutrosophic logic and systems in recent years [2-7]. In 1980, Smarandache developed his Neutrosophic sets philosophical theory to address many forms of uncertainties in a variety of real-world challenges, and it has since been successfully implemented in a variety of study domains. However, Neutrosophic theory is an extension theory of Fuzzy logic theory in which indeterminacy $\boldsymbol{I}$ is included with $\boldsymbol{I}$ follows some algebraic properties, namely $\boldsymbol{I}+$

$\boldsymbol{I = 2I},\ \boldsymbol{I^2 = I},\ \boldsymbol{I - I = 0},\ \boldsymbol{0I = 0},\ \boldsymbol{1I = I}$ but $\boldsymbol{I^{-1}}$ does not exist. The concept of Neutrosophic field structure was introduced by F. Smarandache and W.B. Vasantha Kandasamy in 2006.

Now we give a brief introduction to Neutrosophic field structures. For any classical field, there exists a Neutrosophic field $F(I)$. The structure $F(I) = (F(I), +, \cdot)$ is called a Neutrosophic field under Neutrosophic operations $+$ and $\cdot$, which are defined as

$(a + bI) + (c + dI) = (a + c) + (b + d)I$ and

$(a + bI)(c + dI) = ac + (ad + bc + bd)I$

for every Neutrosophic elements $a + bI$ and $c + dI$ in $F(I)$. Note that, $F(I)$ is generated by F and I, and it is represented by $F(I) = \langle F \cup I \rangle = F + FI$. If F is a finite field then $F(I)$ is also finite. Otherwise, $F(I)$ is an infinite Neutrosophic field. For example, $Q(I)$, $R(I)$ and $C(I)$ for all infinite fields but $F_p(I)$ is a finite field, where F_p is isomorphic to Z_p. However, for further details about Neutrosophic field, the reader should see [8-13].

This manuscript makes three contributions. To begin, we propose using finite fields to investigate the algebraic features of the corresponding Neutrosophic field through several cases. Second, we characterise in detail the Neutrosophic Fermat's and Little Fermat's Theorems over finite Neutrosophic fields. Additionally, we present certain necessary and sufficient conditions for the Neutrosophic elements' abilities in the Neutrosophic field $F_p(I)$. Finally, and most importantly, to illustrate three alternative implementations of the Neutrosophic Fermat's Theorem. Additionally, we developed a table comparing classical and neutrosophic fields.

2. Properties of Finite Neutrosophic Fields

Most of the researchers in abstract algebra show how to represent a finite field F_p over its prime characteristic p by clearly representing its additive structure as an abelian group, or a quotient ring of polynomials over F_p. In this section, we represent a Neutrosophic set representation of finite Neutrosophic field that naturally and simply displays both the Neutrosophic additive and multiplicative structures of the finite Neutrosophic field $F_p(I)$ over the classical field F_p under its prime characteristic p.

Let p be a prime number. Then we specify the finite field of order p^2, $F_p(I)$ also denoted by $F_p + F_p(I)$ as follows:

$F_p(I) = \{a + bI : a, b \in F_p, I^2 = I\}$

where the Neutrosophic operations $(a + bI) + (c + dI)$ and $(a + bI)(c + dI)$ are both performed modulo p, this means that $(a + bI) + (c + dI)$ is the remainder of the division $\frac{(a+bI)+(c+dI)}{p}$ and similarly for $(a + bI) + (c + dI)$ remainder of $\frac{(a+bI)(c+dI)}{p}$.

Generally, the following result is well-known with respect to the classical field F_p.

Theorem 2.1[15]: For every element u in $F_p^{\times}$ there exists v in $F_p^{\times}$ such that $uv \equiv 1\ (mod\ p)$.

This result is very useful for studying every result in F_p. But, this result is not true in the Neutrosophic field $F_p(I)$, that is, $(a + bI)(c + dI) \not\equiv 1\ (mod\ p)$ for some elements $(a + bI)$ and $(c + dI)$ in $F_p(I)$, since $I(1 + (p - 1)I) \equiv 0\ (mod\ p)$. A fairly natural question presents itself. Is it possible to enumerate the number of multiplicative inverse elements in the Neutrosophic field $F_p(I)$? The answer is yes and it is contained in the following Theorems. ■

Theorem 2.2: Let $u + vI$ be an element in $F_p(I)^{\times}$ then there exists its multiplicative inverse $(u + vI)^{-1}$ in $F_p(I)^{\times}$ such that $(u + vI)^{-1} = u^{p-2} - vu^{p-2}(u + v)^{p-2}I$.

Proof. Suppose $u + vI$ be an element in $F_p(I)^{\times}$. Then $u, u + v \in F_p$. If possible assume that $u \neq 0$ and $u + v \neq 0$, then there exists u^{-1} and $(u + v)^{-1}$ in $F_p^{\times}$ such that $u^{-1} = u^{p-2}$ and $(u + v)^{-1} = (u + v)^{p-2}$. Because $(u + vI)(u^{p-2} - vu^{p-2}(u + v)^{p-2}I) = 1$, so the definition of multiplication

inverse elements yields the inverse $(u+vI)^{-1}$ of $(u+vI)$ exists in $F_p(I)^{\times}$ such that $(u+vI)^{-1} = u^{p-2} - vu^{p-2}(u+v)^{p-2}I$. ■

Example 2.3: In $F_5(I)^{\times}$, $(4+5I)^{-1} = 4^{5-2} - 2(4^{5-2})(6^{5-2})I = 4 - 3I = 4 + 2I$.

Here is another basic fact extracted from [14] regarding mutual additive inverse elements. Consider an ordered pair (u,v) in$F_p{}^{\times}$. An ordered pair (u,v) in $F_p{}^{\times}$ is called mutual additive pair if $u+v = 0$ in $F_p{}^{\times}$. The set of all mutual additive pairs in $F_p{}^{\times}$ is denoted by $M(F_p{}^{\times})$, particularly, $M(F_p{}^{\times}) = \{(u+vI): u+v=0\}$.
Note that $|F_p(I)^*| = p-1$, where $F_p(I)^* = F_p(I) - \{0\}$. If $u+v=0$ inF_p, then
$uv \not\equiv 1\ (mod\ p)$. Let us see how all this works in a specific instance.

Example 2.4: The following table exhibits the cardinality of the set $F_p(I)^{\times}$ for $p = 2,3,5$.

Prime	2	3	5
$F_p(I)^{\times}$	1	4	16

Here, we observe that the cardinality of $F_5(I)^{\times}$ is 16, whereas the cardinality of $F_2(I)^{\times}$ and $F_3(I)^{\times}$ are 1 and 3 respectively. It is easy to verify that $F_2(I)^{\times} = \{1\}$, $F_3(I)^{\times} = \{1,2,1+I,2+2I\}$, $F_5(I)^{\times} = \{1,2,3,4,1+I,1+2I,1+3I,2+I,2+2I,2+4I,3+I,3+3I,3+4I,4+2I,4+3I,4+4I\}$

One consequence of what has just been proved is that, in those cases in which a multiplicative inverse exists in $F_p(I)^{\times}$, we can now state exactly how many there are.

Theorem 2.5: If $u+iv$ is a multiplicative inverse in $F_p(I)$ has exactly $(p-1)^2$ of them. Particularly,$|F_p(I)^{\times}| = (p-1)^2$.

Proof. Because $\boldsymbol{p}$ is a prime, surely the Neutrosophic field $\boldsymbol{F_p(I)}$ is a disjoint union of the sets $\{\boldsymbol{0}\}, \boldsymbol{F^*I}, \boldsymbol{M(F_p(I)^*)}$ and$\boldsymbol{F_p(I)^{\times}}$, that is, $\boldsymbol{F_p(I) = \{0\} \cup F_p^*I \cup M(F_p(I)^*) \cup F_p(I)^{\times}}$, where $\boldsymbol{F_p^* = F - \{0\}}$ and $\boldsymbol{F_p^*I = \{uI: u\epsilon F_p^*\}}$. Raise both sides of this relation to the cardinality and expand to obtain the relation

$$\boldsymbol{F_p(I) = |\{0\}| + |F_p^*I| + |M(F_p(I)^*)| + |F_p(I)^{\times}|}$$
$$\boldsymbol{\Rightarrow p^2 = 1 + (p-1) + (p-1) + |F_p(I)^{\times}|}$$
$$\boldsymbol{\Rightarrow |F_p(I)^{\times}| = p^2 - 1 - (p-1) - (p-1)}$$
$$\boldsymbol{\Rightarrow |F_p(I)^{\times}| = (p-1)^2}.$$

For an illustration of these ideas, let us demonstrate the cardinality of $F_3(I)^{\times}$. Using the Neutrosophic elements in $F_3(I)$, we observe that
$F_3(I) = \{0,1,2,I,2I,1+I,1+2I,2+I,2+2I\}$,
$F_3^*I = \{I,2I\}$, and $M(F_3(I)^*) = \{u+vI: u+v=0\}$
$= \{1+2I, 2+I\}$.
Therefore,
$$|F_3(I)| = |\{0\}| + |F_3^*I| + |M(F_3(I)^*)| + |F_3(I)^{\times}|$$
$$\Rightarrow 3^2 = 1 + (3-1) + (3-1) + |F_3(I)^{\times}|$$
$$\Rightarrow |F_3(I)^{\times}| = 3^2 - (3-1) - (3-1) = (3-1)^2 = 4,$$
which are listed below
$$F_3(I)^{\times} = \{1,2,1+I,2+2I\}.$$

In view of classical algebraic sense, well-known that $a^{\varphi(n)} \equiv 1\ (mod\ n)$ whenever $(a,n) = 1$, where $\varphi(n)$ is the Euler totient function of n. This supports the following definition in the classical field F_p.

Definition 2.6: Let $u \in F_p$, then there exists a least positive integer k such that $O(u) = k$ with respect to multiplication defined over F_p if and only if $u^k \equiv 1\ (mod\ n)$.
For instance, $2^3 \equiv 1\ (mod\ 7)$ in the field F_7, so that the integer 2 has order 3 modulo 7. According to this classical field systems, we know that every non-zero element in F_p has unique order with respect to multiplication. However, it is not true in the Neutrosophic sense. Now let us see how all this works in the following specific instances.

Example 2.7: The following table exhibits the order of the non-zero elements in the Neutrosophic field
$F_3(I) = \{0, 1, 2, I, 2I, 1 + I, 1 + 2I, 2 + I, 2 + 2I\}$
under Neutrosophic multiplication modulo 3.

Element in $F_3(I)$	1	2	I	$2I$	$1 + I$	$1 + 2I$	2+I	2+2I
Order	1	2	d.e	d.e	2	d.e	d.e	2

where "d.e" represents does not exist.

Particularly, the following table illustrates the orders of each element in $F_3(I)^\times$ exits.

Element in $F_3(I)^\times$	1	2	$1 + I$	$2 + 2I$
Order	1	2	2	2

Theorem 2.9: Let $u, v \in F_p$. Then $u + vI$ has a multiplicative inverse in $F_p(I)$ if and only if $u \neq 0$ and $u + v \neq 0$ in F_p.

Proof. We denote multiplicative identity in F_p by 1. Consider a nonzero pair of elements u, v in F_p and write it in the form $(u + vI)$ in $F_p(I)$. Then

$(u + vI)$ has a multiplicative inverse $\Leftrightarrow$ $(u + vI)(x + yI) = 1$ has a solution in $F_p(I)$

$\Leftrightarrow$ $ux \equiv 1\ (mod\ p)$ has a solution in Z and
$vx + (u + v)y \equiv 0\ (mod\ p)$ has a solution in Z.

$\Leftrightarrow$ $u \neq 0$ and $u + v \neq 0$ in F_p. ■

Let us now employ the unique technique of this section to enumerate the number of elements in $F_p(I)^\times$ of the form $(u + vI)^2 = 1$. To start, we know that there is only one element 1 in $F_2(I)^\times$ with $1^2 = 1$. Now, our enumeration starts from $p > 2$, which explore the following theorem.

Theorem 2.10: If $p > 2$ is a prime number, then the congruence$(u + vI)^2 - 1 \equiv 0\ (modulo\ p)$ has exactly 4 solutions in $F_p(I)^\times$.

Proof. Because p is an odd prime, it follows that $F_p(I)^\times$ contains at least one element of order 2. Suppose that $u + vI$ is an element in $F_p(I)^\times$ of order 2, then the Neutrosophic multiplication inverse of $u + vI$ is itself $u + vI$ in $F_p(I)^\times$. Therefore,

$(u + vI)^2 = 1$ $\Leftrightarrow$ $u^2 + v^2I + 2uvI = 1 + 0I$

$\Leftrightarrow$ $u^2 = 1,\ v^2 + 2uv = 0$

$\Leftrightarrow$ $u^2 = 1, v^2 = 4$, since $v^2 \neq 0$

$\Leftrightarrow$ $u = 1, p - 1, v = 2, p - 2$ in F_p.

So, there exists six $\left[\binom{4}{2} = 6\right]$Neutrosophic elements, namely
$1 + 0I, (p - 1) + 0I, 1 + 2I, 1 + (p - 2)I, (p - 1) + 2I$

and $(p-1)+(p-2)I$ in $F_p(I)^\times$.

Out of these six elements, four elements $1, p-1, 1+(p-2)I$ and $(p-1)+2I$ satisfies the Neutrosophic equation $(u+vI)^2=1$ in $F_p(I)^\times$, because $(1+2I)^2 \neq 1$ and $\big((p-1)+(p-2)I\big)^2 \neq 1$is true in $F_p(I)^\times$. ■

As an immediate consequence of Theorem [2.10], we deduce the following corollary.

Corollary 2.11: The set $\mathcal{J}_p(I)=\{u+vI \epsilon F_p(I)^\times : (u+vI)^2=1\}$ is a Neutrosophic subgroup of the Neutrosophic group $F_p(I)^\times$.

Proof. It is clear from the well-known result:

$(u+vI)^2=1,\ (u'+v'I)^2=1$ implies that $[(u+vI)(u'+v')]^2=1$ in $F_p(I)^\times$. ■

Remark 2.12: (1) $\mathcal{J}_p(I)=F_p(I)^\times \Leftrightarrow p=3$.

(2) $|\mathcal{J}_p(I)| \leq |F_p(I)^\times|$ for every $p \geq 3$.

Let us see what happens if $0(u+vI)=2$ is evaluated for each $u+vI$ in $F_p(I)^\times$ of $p \geq 3$ and the required results are added. In the case $p=3$, the answer is easy; here

$$0(u+vI)=2 \iff u+vI \epsilon F_p(I)^\times - \{1\}.$$

Suppose that $p>3$, then the non-empty subset

$$H_p(I)=\{u+vI \epsilon F_p(I)^\times : 0(u+vI)=2\}$$

exists in $F_p(I)^\times$ but it is not a Neutrosophic subgroup of $F_p(I)^\times$ because $1 \notin H_p(I)$ (since $o(1)=1 \neq 2$).

3. Neutrosophic Fermat's and Little Fermat's Theorems

The above information of the Neutrosophic field $F_p(I)$ seems the opportune moment to mention the Fermat's and Little Fermat's Theorems gave an essentially valid proof of Neutrosophic filed Theory. First of all, we state classical Fermat's and Little Fermat's Theorems in the classical field F_p as follows.

Theorem3.1 [15]: (Fermat's Theorem)

For every u in F_p, we have $u^{p-1} \equiv 1\ (mod\ p)$.

Theorem3.2 [15]: (Fermat's Little Theorem)

For every u in F_p, we have $u^p \equiv u\ (mod\ p)$.

Classical Fermat's theorem contains many applications and it plays a central role in much of what is done in many applied and engineering sciences. However, now we introduce Neutrosophic Fermat's theorem over the Neutrosophic field $F_p(I)$.

We now proceed to state and prove Neutrosophic Fermat's Theorem in $F_p(I)$.

Theorem 3.3: (Neutrosophic Fermat's Theorem for $F_p(I)$)

Let p be a prime and let $u+vI \in F_p(I)$. Then

$$(u+vI)^{p-1} \equiv 1\ (modulo\ p).$$ ■

Before we proceed to the proof of this theorem, we observe that the congruence

$$(u+vI)^{p-1} \equiv 1\ (modulo\ p)$$

fails to hold for some choice of $u+vI$ in $F_p(I)$. As an illustration of this approach, let us look $p=3$. The determination is kept under control by selecting a suitable Neutrosophic element for $u+vI$, say, $u+vI=1+2I$. Because $(1+2I)^{p-1}$ maybe written as, $(1+2I)^{3-1}=(1+2I)^2=1+4I+4I=1+2I\ (mod\ 3)$, but $(1+2I) \not\equiv 1\ (mod 3$. Combining these congruences, we finally obtain

$(1+2I)^{3-1} \not\equiv 1\ (mod\ 3)$. So, Theorem **[3.3]** is not true in $F_p(I)$. However, the upshot of all this is the following Theorem.

Theorem3.4: (Neutrosophic Fermat's Theorem for $F_p(I)^{\times}$)
Let $p > 2$ be a prime. For every Neutrosophic element $u + vI$ in $F_p(I)^{\times}$ such that
$(u+vI)^{p-1} \equiv 1\ (mod\ p)$.

Proof. Let $u + vI$ in $F_p(I)^{\times}$. Then we begin by assuming the first $(p-1)$ multiples of $u + vI$, that is, $u+vI, 2(u+vI), 3(u+vI), \ldots\ldots, (p-1)(u+vI)$. None of these Neutrosophic elements in $F_p(I)^{\times}$ is congruent modulo p to any other element in $F_p(I)^{\times}$. To see this, we consider $r(u+vI) \equiv s(u+vI)\ (mod\ p)$ for some r and s such that $1 \le r < s \le p-1$. Since $u + vI \in F_p(I)^{\times}$, there exists a multiplicative inverse of $u + vI$ in $F_p(I)^{\times}$, so $u + vI$ could be cancelled in $r(u+vI) \equiv s(u+vI)\ (mod\ p)$ to give $r \equiv s\ (mod\ p)$, which is not true because $1 \le r < s \le p-1$. Therefore, the set $u+vI, 2(u+vI), 3(u+vI), \ldots\ldots, (p-1)(u+vI)$ of Neutrosophic elements in $F_p(I)^{\times}$ must be congruent modulo p under the following bijection:

$$r \mapsto (u+vI)r$$

for every r in $\{0, 1, 2, 3, \ldots\ldots, p-1\}$. Now multiply all these elements together, we obtain that

$(u+vI)2(u+vI)3(u+vI)\cdots(p-1)(u+vI) \equiv 1\ 2\ 3\cdots(p-1)\ (mod\ p)$

$\Rightarrow (u+vI)^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$

$\Longrightarrow (u+vI)^{p-1} \equiv 1\ (mod\ p)$, since $gcd(p, (p-1)!\,) = 1$. ■

An application of Neutrosophic Fermat's Theorem leads to the congruences
$(1+I)^2 \equiv 1\ (mod\ 3), (1+I)^6 \equiv 1\ (mod\ 7), (1+I)^{10} \equiv 1\ (mod\ 11)$ and, in turn, to solve the following example.

Example 3.5: In the Neutrosophic multiplicative group $F_{101}(I)^{\times}$, we have
$(1+I)^{100} \equiv 1\ (mod\ 101)$.
Solution. It is easy to see that
$(1+I)^2 \equiv (1+3I)\ (mod\ 101), (1+I)^{10} \equiv (1+13I)\ (mod\ 101)$.
However, we conclude that,

$$\begin{aligned}(1+I)^{100} &= [(1+I)^{10}]^{10} = (1+13I)^{10}\\ &\equiv (1+83I)(1+94I)\ (mod\ 101\\ &\equiv 1\ (mod\ 101).\end{aligned}$$

Now, starts the greatest advances in this direction were made by this manuscript called Neutrosophic Fermat's Little Theorem. We state this more precisely in the following theorem.

Theorem 3.6: (Neutrosophic Little Fermat's Theorem)
Let p be a prime. Then for every $u + vI$ in the Neutrosophic field $F_p(I)$,

$$(u+vI)^p \equiv (u+vI)\ (mod\ p).$$

Proof In light of the Binomial theorem, $(u+vI)^p = \binom{p}{0}u^p(vI)^0 + \binom{p}{1}u^{p-1}(vI)^1 + \cdots +$
$\binom{p}{2}u^{p-2}(vI)^2 + \cdots + \binom{p}{p-1}u^{p-(p-1)}(vI)^{p-1} + \binom{p}{p}u^0(vI)^p$.
Because $u + vI \epsilon F_p(I)$, we have $u, v, I \epsilon F_p$. So, by the classical Fermat's Little Theorem [3.2],

$$u^p \equiv u\ (mod\ p),\ u^p \equiv u\ (mod\ p) \text{ and } I^p \equiv I\ (mod\ p).$$

Since $p|\binom{p}{1}$, $p|\binom{p}{2}$,..... $p|\binom{p}{p-1}$. In this sequence, we can obtain easily as
$(u+vI)^p \equiv (u+vI)\ (mod\ p)$. ■

At this stage, when $p = 2,\ 2(u + vI) \equiv 0(mod\ 2)$ for any $u + vI \in F_2(I)$, so $u + vI = -(u + vI)$ for any $u + vI \in F_2(I)$. Therefore, we also have

$(u - vI)^2 \equiv u^2 - v^2 I\ \equiv (u^2 + v^2 I\ )(mod\ 2)$.

Corollary 3.7:

Let p be an odd prime. Then for every $u + vI$ in the Neutrosophic field $F_p(I)$,

$$(u - vI)^p \equiv (u - vI)\ (mod\ p).$$

Proof. By Theorem [3.6], we have

$$\begin{aligned}(u - vI)^p &= (u + (-vI))^p = u^p + (-vI)^p \\ &= u^p + (-1)^p (v)^p (I)^p \\ &= u^p + (-1)^p v^p I.\end{aligned}$$

When $p > 2,\ p$ is odd, we have $(-1)^p \equiv -1(mod\ p)$, and $I^p \equiv I(mod\ p)$. Hence

$(u - vI)^p \equiv (u - vI)\ (mod\ p)$. ■

4. Applications of Neutrosophic Fermat's Theorem

Already, it is well known that the Quadratic congruence $(u + vI)^2 - 1 \equiv 0\ (mod\ p)$ has exactly four solutions whenever p is an odd prime. From this result, we can pass simply to the following application of Neutrosophic Fermat's theorem.

Theorem 4.1: Let $p > 3$ be an odd prime and let $u + vI \in F_p(I)^\times$. If $4|(p - 1)$ and $4d|(p - 1)^2$ then the congruence $(u + vI)^{4d} - 1 \equiv 0\ (mod\ p)$ has exactly $4d$ solutions.

Proof. Since $\left|F_p(I)^\times\right| = (p - 1)^2$. Suppose $u + vI$ be any element in $F_p(I)^\times$. But by hypothesis, $4d|(p - 1)^2$, so we have $(p - 1)^2 = 4dq$ for some positive integer q. Then the expression $(u + vI)^{(p-1)^2} - 1\ = (u + vI)^{4dq} - 1$

$$\begin{aligned}&= ((u + vI)^{4d})^q - 1^q \\ &= ((u + vI)^{4d} - 1) f(u + vI),\end{aligned}$$

where

$f(u + vI) = (u + vI)^{4d(q-1)} + (u + vI)^{4d(q-2)} + \cdots + (u + vI)^{4d} + 1$

is a polynomial of degree

$4d(q - 1) = 4dq - 4d = (p - 1)^2 - 4d$.

We know that any solution $u + vI \equiv (a + bI)(mod\ p)$ of the congruence $(u + vI)^{(p-1)^2} - 1 \equiv 0(mod\ p)$ that is not a solution of $f(u + vI) \equiv 0(mod\ p)$ must satisfy the congruence$(u + vI)^{4d} - 1 \equiv 0\ (mod\ p)$.

For the element $a + bI$ in $F_p(I)^\times$, we have

$0 \equiv (\ a + bI)^{(p-1)^2} - 1 = ((a + bI)^{4d} - 1) f(a + bI)(mod\ p)$

with the condition $p \nmid f(a + bI)$, which implies that $p|((a + bI)^{4d} - 1)$. It follows that the required congruence $(u + vI)^{4d} - 1 \equiv 0\ (mod\ p)$ must have

$(p - 1)^2 - ((p - 1)^2 - 4d) = 4d$ solutions. ■

Example 4.2: For an illustration of these facts, let us solve the congruence

$(u + vI)^4 - 1 \equiv 0\ (mod\ 5)$.

A table of powers of Neutrosophic elements in $F_5(I)^\times$ can be constructed once a modulo 5 is fixed. Using this modulo 5, we simply calculate the powers of elements in $F_5(I)^\times$ as follows.

$1^4 \equiv 1\ (mod\ 5),\ 2^4 \equiv 1\ (mod\ 5),\ 3^4 \equiv 1\ (mod\ 5), 4^4 \equiv 1\ (mod\ 5),$

$(1 + I)^4 \equiv 1\ (mod\ 5),\ (1 + 2I)^4 \equiv 1\ (mod\ 5),\ (1 + 3I)^4 \equiv 1\ (mod\ 5),$

$(2 + I)^4 \equiv 1\ (mod\ 5),\ (2 + 2I)^4 \equiv 1\ (mod\ 5),\ (2 + 4I)^4 \equiv 1\ (mod\ 5),$

$(3 + I)^4 \equiv 1\ (mod\ 5),\ (3 + 3I)^4 \equiv 1\ (mod\ 5),\ (3 + 4I)^4 \equiv 1\ (mod\ 5),$

$(4 + 2I)^4 \equiv 1\ (mod\ 5),\ (4 + 3I)^4 \equiv 1\ (mod\ 5),\ (4 + 4I)^4 \equiv 1\ (mod\ 5).$

Consulting the above list of powers of 4 in each element of $F_5(I)^\times$, we obtain that the original congruence $(u + vI)^4 - 1 \equiv 0\ (mod\ 5)$ possesses the $4d = 4 \cdot 4 = 16$ solutions, namely

$u + vI \equiv 1,2,3,4, 1 + I, 1 + 2I, \ldots,$ and $4 + 4I \ (mod\ 5)$.

Remark 4.3: The congruence $(u + vI)^4 - 1 \equiv 0 \ (mod\ 11)$ is not solvable in $F_{11}(I)^\times$, because $4 \nmid (11 - 1)$.

We would like to close this paper with another application of Neutrosophic Fermat's theorem to the study of quadratic congruence $(u + vI)^2 \equiv 0 \ (mod\ p)$.

Theorem 4.4: Let $u + vI \in F_p(I)^\times$ and let $p > 3$ be a prime. If the quadratic congruence $(u + vI)^2 + 1 \equiv 0 \ (mod\ p)$ has a solution, the prime $p \equiv 1 \ (mod\ 4)$.

Proof: Suppose $a + bI \in F_p(I)^\times$ be any solution of $(u + vI)^2 + 1 \equiv 0 \ (mod\ p)$. Then

$$(a + bI)^2 \equiv -1 \ (mod\ p).$$

By the Neutrosophic Fermat's theorem [15],

$$1 \equiv (a + bI)^{p-1} \equiv [(a + bI)^2]^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \ (mod\ p).$$

If possible assume that $p = 4q + 3$ for some q, then

$$(-1)^{\frac{p-1}{2}} = (-1)^{2q+1} = -1, \text{ hence } 1 \equiv -1 \ (mod\ p).$$

This implies that $p|2$, which is not true because p is an odd prime. Consequently, our assumption that $p = 4q + 3$ is not true, and hence p must be of the form $4q + 1$. ■

The converse of the preceding theorem may not be true. That is if $p = 4q + 1$, then $(u + vI)^2 + 1 \equiv 0 \ (mod\ p)$ is not solvable in $F_p(I)^\times$. For instance, $p = 5$, the congruence $(u + vI)^2 + 1 \equiv 0 \ (mod\ 5)$ is not solvable in $F_5(I)^\times$.

Example 4.5: Consider the case $p = 13$, which is a prime of form $4q + 1$. It is easy to see that $(3 + 4I)^2 + 1 \equiv 0 \ (mod\ 13)$. Thus the congruence $(u + vI)^2 + 1 \equiv 0 \ (mod\ 13)$ is solvable in $F_{13}(I)^\times$.

Finally, the difference table for F_p and $F_p(I)$ is displayed below:

	Classical Field F_p		**Neutrosophic Field $F_p(I)$**
1.	$\lvert F_p \rvert = p$.	1.	$\lvert \boldsymbol{F_p(I)} \rvert = \boldsymbol{p^2}$.
2.	$\lvert F_p^\times \rvert = p - 1$.	2.	$\lvert \boldsymbol{F_p(I)^\times} \rvert == \boldsymbol{(p-1)^2}$.
3.	For each u in F_p^*, there exists v in F_p^* such that $uv \equiv 1 \ (mod\ p)$.	3.	For some $\boldsymbol{a + bI}$ and $\boldsymbol{c + dI}$ in $\boldsymbol{F_p(I)^*}$, we have $\boldsymbol{(a + bI)(c + dI) \not\equiv 1 \ (mod\ p)}$.
4.	$F_p^\times$ is a cyclic group.	4.	$\boldsymbol{F_p^\times}$ is not a cyclic group.
5.	The product of all elements in F_p^* is non-zero.	5.	The product of all elements in $\boldsymbol{F_p(I)^*}$ is zero.
6.	The congruence $x^2 + 1 \equiv 0 \ (mod\ p)$ has a solution $\Leftrightarrow$ $p \equiv 1 \ (mod\ 4)$.	6.	If $\boldsymbol{(u + vI)^2 + 1 \equiv 0 \ (mod\ p)}$ has a solution in $\boldsymbol{F_p(I)^\times}$ then $\boldsymbol{p \equiv 1 \ (mod\ 4)}$. But converse need not be true.

5. Conclusions

In this manuscript, we turn to close to another milestone of the development of Fermat's theorem under the Neutrosophic sense. In this regard, we constructed a table to differentiate the field F_p and Neutrosophic field $F_p(I)$. Also, we have given necessary and sufficient conditions for solving Neutrosophic quadratic congruences like

$$(u + vI)^2 + 1 \equiv 0 \ (mod\ p),$$

$$(u + vI)^2 - 1 \equiv 0 \ (mod\ p) \text{ and } (u + vI)^{4d} - 1 \equiv \ (mod\ p)$$

with various illustrations in the Neutrosophic field $F_p(I)$.

Funding: This research has no external Funding.

Conflicts of Interest: The authors declare no Conflict of interest.

References

1. Lidl, R.; Harrald, N. "Finite Fields", *Cambridge University Press*, pp.1-772, 1996.
2. Vasantha Kandasamy, W.B.; Smarandache, F."Basic Neutrosophic Algebraic Structures and Their Application to Fuzzy and Neutrosophic Models", *Hexis, Church Rock*, pp.1-149, 2004.
3. Arena, P.; Baglio, S.; Fortuna, L. Manganaro, G., Hyperchaos from cellular networks, *Electron.Lett*., 31, pp.250-251, 1995.
4. Chalapathi, T.; Madhavi, L. "A study on Neutrosophic Zero Rings", *Neutrosophic Sets and Systems*, Vol.30, pp.191-201, 2019
5. Chalapathi, T.; Madhavi, L."Neutrosophic Boolean Rings", *Neutrosophic Sets and Systems*, Vol.33, pp.59-66, 2020.
6. Sumathi, I.R.; Antony Crispin Sweety, C. "New approach on differential equations via trapezoidal Neutrosophic number", *Complex and Intelligent systems*, Vol. 5, pp.417-424, 2019.
7. Zhong, H.; Wang, J.Q. "Interval Neutrosophic Sets and Their Application in Multicriteria Decision Making Problem", *The Scientific World Journal*, pp.1-16, 2014
8. Chalapathi, T.; Kiran Kumar, R.V. "Neutrosophic Units of Neutrosophic Rings and Fields", *Neutrosophic Sets and Systems*, Vol.21, pp.5-12, 2018.
9. Chalapathi, T.; Kiran Kumar, R.V. "Self Additive Inverse Elements of Neutrosophic Rings and Fields", *Annals of Pure and Applied Mathematics*. Vol. 13(1), pp.63-72, 2017.
10. Ali, M.; Smarandache, F.; Shabir, M.; Vladareanu, L. "Generalization of Neutrosophic Rings and Neutrosophic Fields", *Neutrosophic Sets and Systems*, Vol.5, pp.9-14, 2014.
11. Mohammad, A. "On the Representation of Neutrosophic Matrices by Neutrosophic Linear Transformations", Hindawi-Journal of Mathematics Vol.2021, 1-5, 2021.
12. Agboola, A. A. A.; Akinleye, S. A."Neutrosophic vector spaces," Neutrosophic Sets and Systems, vol. 4, pp. 9–17, 2014.
13. Chalapathi, T.; Sajana, S.; Smarandache, F. "Neutrosophic Quadratic Residues and Non-Residues", Neutrosophic Sets and Systems, Vol. 46, pp. 356-371, 2021.
14. Chalapathi, T.; Sajana, S. "Unitary Invertible Graphs of Finite Rings", *General Algebra and Applications*, Vol. 41, pp. 195-208, 2021.
15. Xian –Wan, Z. " Finite Fields and Galois Rings", *World Scientific Publishers*, pp. 1-388, 2011.

Received: Dec. 25, 2021. Accepted: April 4, 2022.