Triple System and Fano Plane Structure in $\mathbb{Z}_n^*$

Dennis Kinoti Gikunda, Benard Kivunge

Kenyatta University, Kenya

***Abstract: -* A triple system is an absolutely fascinating concept in projective geometry. This paper is an extension of previously done work on triple systems, specifically the triples that fit into a Fano plane and the (*i, j, k*) triples of the quaternion group. Here, we have explored and determined the existence of triple systems in $\mathbb{Z}_n^*$ for $n = p$, $n = pq$ and $n = 2^m p$ with m εN, $p, q \varepsilon \mathbb{P}$, and $p > q$, where N is the set of natural numbers, $\mathbb{P}$ is the set of primes and $\mathbb{Z}_n^*$ is the set of units in Z*n*. A triple system in $\mathbb{Z}_n^*$ has been denoted by (k_1,k_2,k_3) where there exists $k_i > 1$, $i = 1,2,3$, such that $k_i^2 \equiv 1 (\text{mod } n)$ with $k_1k_2 \equiv k_3 (\text{mod } n)$, $k_1k_3 \equiv k_2 (\text{mod } n)$ and $k_2k_3 \equiv k_1 (\text{mod } n)$. We have also investigated the number of triples in $\mathbb{Z}_n^*$ and determined the general formula for getting the triples. Further, we have fitted the triples into Fano planes and established the projective geometry structure for the above defined $\mathbb{Z}_n^*$.**

***AMS Subject Classification:* 20B05**

***Key Words:* Geometry, Triple Systems, Fano Planes, Prime Numbers, Units.**

I. INTRODUCTION

Any natural number n can be expressed as a product of primes, for $n \neq 0,1$. This implies that prime factors are the 'building blocks' for any $n \in$ N. Mathematician find delight in understanding the composition properties of the primes and try to figure out the structure of their sequence (if any exists). The nature of their existence makes them useful in puzzles, cryptography and generation of security codes. Any discovery of their nature is always a lead to new application.

In recent years, mathematicians have made a considerably great progress in a sub-branch of mathematics that concern finite geometries. Herein, we find the concept of triple systems referring to a vector space V over a field K together with K- trilinear mapping $V \otimes V \otimes V \rightarrow V$. Girard Desargues (1591 − 1661) discovered the projective geometry derived from Euclidean geometry, which involved 3- dimension finite geometry. An Italian mathematician, Gino Fano (1871 − 1952) later discussed the 3-dimension finite geometry with 3 points in each line and 7 points on each plane. The total number of points was 15, with 35 lines and 15 planes. The 3 points on each line form unique triple systems.

Another interesting triple is the (i,j,k) triples of the quaternion group, denoted by H = $\{\pm1,\pm i,\pm j,\pm k\}$. The discovery of H is quite a famous story in mathematics. William Rowen Hamilton, an Irish mathematician spent much of his life seeking a 3-dimension number system. On 16th Oct 1843, he discovered the fundamental formula for quaternion (action on 3*D*);

$$i^2 = j^2 = k^2 = ijk = -1,$$

where i,j,k are imaginary points and $1 \in$ R. The equation above, satisfactorily linked the imaginary part to the commonly known real part. A very useful relationship of the i,j,k triples in H is also given by:

$$ij = k = -ji,\ jk = i = -kj,\ ki = j = -ik.$$

The main aspect of this research is the question, "how does the ring Z^*_n, $n=p$ (prime), $n = pq$, $n = 2^m p$, $p > q$ for $p,q \in \mathbb{P}$, $m \in$ N, connect to the concept of the triple systems in projective geometry?"

II. PRELIMINARIES

Definition 1. A **geometry** can be defined by a set $G = (P,I)$, where P is the set of points and lines and I the incidence relation that is both reflective and symmetric. We say a point is incident to the line it lies on and two lines are incident only when they have all points in common. A relation R on a set A is called **reflexive** if $(a,a) \in R$ holds for every element $a \in A$ while a relation R on a set A is called **symmetric** if $(b,a) \in R$ holds when $(a,b) \in R$.

Definition 2. Let a triple $G = (P,L,I)$ be a rank 2 geometry with P = set of points and L = set of lines. Any geometry satisfying the following axioms is a type of **projective geometry**.

G_1 : Any 2 distinct points are incident to a unique line.

G_2 : Any 2 lines on the plane meet.

G_3 : Any line is incident with at least 3 points.

G_4 : There are at least 2 lines.

Definition 3. A **projective space** is a projection of a 2 - dimensional space to a 3 - dimensional space by adding a point at infinity so that there exists no parallel lines. A projective space with at least 2 lines, such that any 2 distinct lines are incident to a unique point is called a **projective plane**

Definition 4. The **order** of a finite projective space is given by the number of points that are incident to each line, minus one. Any finite projective plane of order n contains $n^2 + n + 1$ points. A **Fano plane** is the smallest finite projective plane. It is of order $n = 2$. the total number of points is 7.

Definition 5. A **Steiner system**, denoted by $S(t,k,v)$, is a set X of v points, and a collection of subsets of X of size k (called blocks), such that any t points of X are in exactly one of the blocks. The special case $t = 2$ and $k = 3$ corresponds to a so-called **Steiner triple system.**

Definition 6. Let n be any positive whole number, if 1 and $n \neq 1$ are the only factors of n, n is said to be a **prime number**, denoted by p. We will denote the set of prime numbers by $\mathbb{P}$. If n has more than 2 distinct factors, it is called a **composite number**.

Definition 7. The expression $x \equiv y$ (mod n) implies that $n|(x\text{-}y)$ and is read as 'x is congruent to y modulo n'. In other words, x and y have the same remainders when divided by n.

Definition 8. A **ring** is a non-empty set R with 2 binary operations + (addition) and $\cdot$ (multiplication) such that the following axioms are satisfied.

R_1 : $(R,+)$ is an abelian group. i.e it satisfies the following axioms (G_1 to G_4).

G_1 : closure; $\forall\, a,b \in R : a + b = b + a \in R$.

G_2 : associativity; $\forall\, a,b,c \in R : (a + b) + c = a + (b + c)$.

G_3 : identity; $\exists\, 0_R \in R : 0_R + a = a = a + 0_R$.

G_4 : inverse; $\forall\, a \in R, \exists - a \in R : a + (-a) = 0_R = (-a) + a$

R_2 : multiplication is associative i.e. $(a \cdot b) \cdot c = a \cdot (b \cdot c)\ \forall\, a,b,c \in R$.

R_3 : multiplication is distributive over addition i.e $\forall\, a,b,c \in R$;

$a \cdot (b + c) = a \cdot b + a \cdot c \rightarrow$ left distributive law and

$(a + b) \cdot c = a \cdot c + b \cdot c \rightarrow$ right distributive law.

Definition 9. Let $(R,+,\cdot)$ be a ring. Then the set of units for this ring is denoted by R^*; where the units are elements in R with multiplicative inverse.

Definition 10. Let $k \in Z^+$. Then **Euler's phi function** $\phi(k)$ denotes the number of positive integers $\leq k$ and relatively prime to k.

Theorem 11. *(Euler's Theorem) Given* $k \in \mathrm{N}$ *with* $(k, n) = 1$, $k^{\phi(n)} \equiv 1\ (mod\ n)$.

Theorem 12. *Let gcd* $(p, q) = 1$. *Given* $a,b \in \mathrm{Z}$, *the system of equations* $x \equiv a(mod\ p)$ *and* $x \equiv b(mod\ q)$ *has a unique solution for* $x \equiv (mod\ pq)$

Corollary 13. *Let* $n_1,n_2,\cdots,n_3$ *be pairwise co-prime positive integers and* $x_1,x_2,\cdots,x_k$ *be arbitrary integers. The system of simultaneous congruence* $a \equiv x_1(mod\ n_1)$, $a \equiv x_2(mod\ n_2)$, $\cdots$, $a \equiv x_k(mod\ n_k)$ *has a unique solution modulo* $n = n_1n_2\ldots n_k$

Theorem 14. *If* n *is an odd number with* $n = p_1^{k_1}\ p_2^{k_2}\ \ldots\ldots\ p_r^{k_r}$ *where* $p_1, p_2, \ldots\ldots, p_r$ *are distinct odd primes and* $k_i > 0$ *for* $1 \leq i \leq r$, *then the equation* $x^2 \equiv 1\ (mod\ n)$ *has exactly* 2^r *distinct solutions* $(mod\ n)$

Proof.

Suppose $x^2 \equiv 1(mod\ p_1^{k_1}\ p_2^{k_2}\ \ldots\ldots\ p_r^{k_r})$, then $p_1^{k_1}\ p_2^{k_2}\ \ldots\ldots\ p_r^{k_r} \mid (x^2-1)$. But since $p_i's$ are distinct primes, $p_1^{k_1}\ p_2^{k_2}\ \ldots\ldots\ p_r^{k_r} \mid (x^2-1)$ only happens iff $p_i^{k_i} \mid (x^2-1)$for all i, *where* $1 \leq i \leq r$.

But each of the congruences only has two solutions i.e. $x \equiv \pm 1(mod\ p_i^{k_i})$.

For each i, $1 \leq i \leq r$, choose $y_i = \pm 1$ and utilize the linear congruences system.

$$x \equiv y_1(mod\ p_1^{k_1})x \equiv y_2(mod\ p_2^{k_2}) \cdots x \equiv y_r(mod\ p_r^{k_r})$$

By Theorem 12, the above system has a unique solution $(mod\ n) = (mod\ p_1^{k_1}\ p_2^{k_2}\ \ldots\ldots\ p_r^{k_r})$.

Since we have 2 choices for each y_i (namely ±1), and we have r congruences, then, the possible choices for $y_1 \ldots ,y_r$ are 2^r

Assuming that the 2^r choices of x are not distinct $(mod\ n)$, i.e. $x_1 \equiv x_2(mod\ n)$, then $x_1 \equiv x_2(mod\ p_i^{k_i})$ for all i. However, any 2 values of x are not congruent $p_i^{k_i}$ for at

least one i. Therefore, the above system of linear congruences has 2^r distinct solutions $x(mod\ n)$. Any of the 2^r choices satisfies $x^2 \equiv (mod\ p_i^{k_i})$ for $1 \leq i \leq r$. Hence, there are 2^r distinct solutions to $x \equiv 1(mod\ n)$.

III. MAIN RESULTS

Proposition 15. If p is prime, 1 and $p - 1$ are the only integers satisfying $k^2 \equiv 1(mod\ p)$ in the set $\mathbb{Z}_p^*$

Proof.

BWOC, assume that 1 and $p - 1$ are not the only integers satisfying $k^2 \equiv 1(mod\ p)$. Consider $\mathbb{Z}_p^*$ with $\mathbb{Z}_p^* = \{1, 2, .., p-1\}$. Say $\exists$ another distinct element m with $m \in \{2, 3, \ldots, p - 2\}$ such that $m^2 \equiv 1(mod\ p)$.

Now, $m^2 = ap + 1$, (where a is a natural number).

$$\Rightarrow m^2 - 1 = ap \Rightarrow p/(m^2 - 1) \Rightarrow p/(m - 1)(m + 1)$$

Since p is a prime, $p/(m - 1)$ or $p/(m + 1)$. But $1 \leq m - 1 \leq p - 3$ and $3 \leq m+1 \leq p-1$. Hence p does not divide $(m-1)$ or $(m+1)$. Therefore, other than 1 and $p - 1$, $\nexists$ integer satisfying $k^2 \equiv 1(mod\ p)$.

Proposition 16. Let $n = 2p$, p (prime), 1 and $2p - 1$ are the only integers satisfying $k^2 \equiv 1(mod\ 2p)$ in the set $\mathbb{Z}_n^*$.

Proof.

BWOC, assume that 1 and $2p - 1$ are not the only integers satisfying $k^2 \equiv 1(mod\ 2p)$ in $\mathbb{Z}_{2p}^* = \{1, 2, .., 2p-1\}$. Suppose $\exists\, m \in \{2, 3, \ldots, 2p - 2\}$ such that $m^2 \equiv 1(mod\ 2p) \Rightarrow m^2 = (2p-1)^2 = 4p^2 - 4p+1 = 1(mod\ 2p)$. We have, $2p/(4p^2 - 4p)$

resulting to $2p - 2$. Now, $m^2 = a(2p) + 1$, where a is a natural number scalar.

$$m^2 - 1 = a(2p) \Rightarrow 2p/(m^2 - 1) \Rightarrow 2p/(m - 1)(m + 1)$$

Since p is prime, p must divide $(m - 1)$ or $(m + 1)$, which means that $m \equiv \pm 1 (mod\ p)$. Which is a contradiction, since, other than 1 and $p - 1$, there exists no other number with $m \equiv \pm 1 (mod\ p)$.

Proposition 17. If $n = 3p$, p (prime) with $p > 3,\ \mathbb{Z}_n^*$ has 2 possible cases of triple system;

Case 1 If $p = 3k + 1$, the triple system is given by $(p + 1, 2p - 1, 3p - 1)$

Proof.

First, we show that $(p + 1)(2p - 1) \equiv (3p - 1)(mod\ n)$

$$(p + 1)(2p - 1) \equiv (3k + 2)(6k + 1)\ (mod\ n)$$

$= 18k^2 + 15k + 2\ (mod\ 3p)$ *since* $n = 3p$

$= 18k^2 + 15k + 2\ (mod\ 9k + 3)$ *since* $p = 3k + 1$

but

$$\frac{18k^2 + 15k + 2}{9k + 3} = 2k + 1\ remainder\ (-1)$$

$$\text{i.e. } 18k^2 + 15k + 2 \equiv -1\ (mod\ 3p)$$

$= 3p - 1$

Now we show that $(p + 1)(3p - 1) \equiv (2p - 1)(mod\ n)$

We already have:

$$(3p - 1) \equiv -1\ (mod\ 3p)$$

Hence,

$(p + 1)(3p - 1) \equiv (p + 1)(-1)\ (mod\ 3p)$

$= (-p - 1)\ (mod\ 3p)$

$= 3p - p - 1$

$= 2p - 1$

Finally, we show that $(2p - 1)(3p - 1) \equiv (p + 1)(mod\ n)$.

We have $(3p - 1) \equiv -1\ (mod\ 3p)$

Hence,

$(2p - 1)(3p - 1) \equiv (2p - 1)(-1)\ (mod\ 3p)$

$= (-2p + 1)\ (mod\ 3p)$

$= 3p - 2p + 1$

$= p + 1$

Example 18. *For* $p = 7$, $n = 3p = 21$ *and the triple is given by* (8,13,20).

$$8 * 13 = 104 \equiv 20\ mod\ (21)$$

$$8 * 20 = 160 \equiv 13\ mod\ (21)\ 13 * 20 = 260 \equiv 8\ mod\ (21)$$

$8^2 \equiv 13^2 \equiv 20^2 \equiv 1(mod\ 21)$

Case 2: If $p = 3k + 2$, the triples are given by $(p - 1, 2p + 1, 3p - 1)$

Proof.

First, we show that $(p - 1)(2p + 1) = (3p - 1)(mod\ n)$.

$(p - 1)(2p = 1) \equiv (3k + 1)(6k + 5)\ (mod\ n)$

$= 18k^2 + 21k + 5\ (mod\ 3p)$ *since* $n = 3p$

$= 18k^2 + 21k + 5\ (mod\ 9k + 6)$ *since* $p = 3k + 1$

But

$$\frac{18k^2 + 21k + 5}{9k + 3} = 2k + 1\ remainder\ (-1)$$

i.e.

$$18k^2 + 21k + 5 \equiv -1\ (mod\ 3p)$$

$= 3p - 1$

Now we show that $(p - 1)(3p - 1) = (2p + 1)(mod\ n)$

We already have $(3p - 1) \equiv -1\ (mod\ 3p)$.

Hence,

$$(p - 1)(3p - 1) \equiv (p - 1)(-1)\ (mod\ 3p)$$

$= (-p + 1)\ (mod\ 3p)$

$= 3p - p + 1$

$= 2p + 1$

Finally, we show that $(2p + 1)(3p - 1) = (p - 1)(mod\ n)$

We have $(3p - 1) \equiv -1\ (mod\ 3p)$.

Hence,

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

$= (-2p - 1)\ (mod\ 3p)$

$= 3p - 2p - 1$

$= p - 1$

Example 19. *For* $p = 5$, $n = pq = 5 * 3 = 15$ *and the triple is given by* (4,11,14)

$$4 * 11 = 44 \equiv 14\ mod\ (15)$$

$$4 * 14 = 56 \equiv 11\ mod\ (15)$$

$$11 * 14 = 154 \equiv 4\ mod\ (15)$$

$$4^2 \equiv 11^2 \equiv 14^2 \equiv 1(mod\ 15)$$

Proposition 20. If $n = 5p$, p (prime) with $p > 5$, for some $k \in \mathbb{N},\ \mathbb{Z}_n^*$ has 4 possible cases of triple system;

Case 1. if $p = 5k + 1$ the triple is $(2p - 1, 3p + 1, 5p - 1)$ e.g. for $p = 11$, the triple is given by $(21,34,54)$, $n = 55$; $21^2 \equiv 34^2 \equiv 54^2 \equiv 1(mod\ 55)$.

Case 2. if $p = 5k + 2$ the triple is $(p-1, 4p+1, 5p-1)$ e.g. for $p = 7$, the triple is given by $(6,29,34)$, $n = 35$; $6^2 \equiv 29^2 \equiv 34^2 \equiv 1(mod\ 35)$.

Case 3. if $p = 5k + 3$ the triple is $(p + 1, 4p - 1, 5p - 1)$ e.g. for $p = 13$, the triple is given by $(14,51,64)$, $n = 65$; $14^2 \equiv 51^2 \equiv 64^2 \equiv 1(mod\ 65)$.

Case 4. if $p = 5k + 4$ the triple is $(2p + 1, 3p - 1, 5p - 1)$ e.g. for $p = 19$, the triple is given by $(39,56,94)$, $n = 95$; $39^2 \equiv 56^2 \equiv 94^2 \equiv 1(mod\ 95)$.

Proof. Similar to the proof of Proposition 17.

Proposition 21. If $n = 7p$, p(prime) with $p > 7$ for some $k \in \mathbb{N}$, $\mathbb{Z}_n^*$ has 6 possible cases of triple system;

Case 1. if $p = 7k + 1$ the triple is $(2p - 1, 5p + 1, 7p - 1)$ e.g. for $p = 29$, the triple is given by $(57,146,202)$, $n = 203$; $57^2 \equiv 146^2 \equiv 202^2 \equiv 1(mod\ 203)$.

Case 2. if $p = 7k + 2$ the triple is $(p - 1, 6p + 1, 7p - 1)$ e.g. for $p = 23$, the triple is given by $(22,139,160)$, $n = 161$; $22^2 \equiv 139^2 \equiv 160^2 \equiv 1(mod\ 161)$.

Case 3. if $p = 7k + 3$ the triple is $(3p - 1, 4p + 1, 7p - 1)$ e.g. for $p = 17$, the triple is given by $(50,69,118)$, $n = 119$; $50^2 \equiv 69^2 \equiv 118^2 \equiv 1(mod\ 119)$.

Case 4. if $p = 7k + 4$ the triple is $(3p + 1, 4p - 1, 7p - 1)$ e.g. for $p = 11$, the triple is given by $(34,43,76)$, $n = 77$; $34^2 \equiv 43^2 \equiv 76^2 \equiv 1(mod\ 77)$.

Case 5. if $p = 7k + 5$ the triple is $(p + 1, 6p - 1, 7p - 1)$ e.g. for $p = 19$, the triple is given by $(20,113,132)$, $n = 133$; $20^2 \equiv 113^2 \equiv 132^2 \equiv 1(mod\ 133)$.

Case 6. if $p = 7k + 6$ the triple is $(2p + 1, 5p - 1, 7p - 1)$ e.g. for $p = 13$, the triple is given by $(27,64,90)$, $n = 91$; $27^2 \equiv 64^2 \equiv 90^2 \equiv 1(mod\ 91)$.

Proof. Similar to proof of Proposition 17.

Proposition 22. If $n = 11p$, p(prime) with $p > 11$ for some $k \in \mathbb{N}$, $\mathbb{Z}_n^*$ has 10 possible cases of triple system;

Case 1. if $p = 11k + 1$ the triple is $(2p - 1, 9p + 1, 11p - 1)$ e.g. for $p = 23$, the triple is given by $(45,208,252)$, $n = 253$; $45^2 \equiv 208^2 \equiv 252^2 \equiv 1(mod\ 253)$.

Case 2. if $p = 11k + 2$ the triple is $(p - 1, 10p + 1, 11p - 1)$ e.g. for $p = 13$, the triple is given by $(12,131,142)$, $n = 143$; $12^2 \equiv 131^2 \equiv 142^2 \equiv 1(mod\ 143)$.

Case 3. if $p = 11k + 3$ the triple is $(3p + 1, 8p - 1, 11p - 1)$ e.g. for $p = 47$, the triple is given by $(142,375,516)$, $n = 517$; $142^2 \equiv 375^2 \equiv 516^2 \equiv 1(mod\ 517)$.

Case 4. if $p = 11k + 4$ the triple is $(5p + 1, 6p - 1, 11p - 1)$ e.g. for $p = 37$, the triple is given by $(186,221,406)$, $n = 407$; $186^2 \equiv 221^2 \equiv 406^2 \equiv 1(mod\ 407)$.

Case 5. if $p = 11k + 5$ the triple is $(4p + 1, 7p - 1, 11p - 1)$ e.g. for $p = 71$, the triple is given by $(285,496,780)$, $n = 781$; $285^2 \equiv 496^2 \equiv 780^2 \equiv 1(mod\ 781)$.

Case 6. if $p = 11k + 6$ the triple is $(4p - 1, 7p + 1, 11p - 1)$ e.g. for $p = 17$, the triple is given by $(67,120,186)$, $n = 187$; $67^2 \equiv 120^2 \equiv 186^2 \equiv 1(mod\ 187)$.

Case 7. if $p = 11k + 7$ the triple is $(5p - 1, 6p + 1, 11p - 1)$ e.g. for $p = 29$, the triple is given by $(144,175,318)$, $n = 319$; $144^2 \equiv 175^2 \equiv 318^2 \equiv 1(mod\ 319)$.

Case 8. if $p = 11k + 8$ the triple is $(3p - 1, 8p + 1, 11p - 1)$ e.g. for $p = 19$, the triple is given by $(56,153,208)$, $n = 209$; $56^2 \equiv 153^2 \equiv 208^2 \equiv 1(mod\ 209)$.

Case 9. if $p = 11k + 9$ the triple is $(p + 1, 10p - 1, 11p - 1)$ e.g. for $p = 31$, the triple is given by $(32,309,340)$, $n = 341$; $32^2 \equiv 309^2 \equiv 340^2 \equiv 1(mod\ 341)$.

Case 10. if $p = 11k + 10$ the triple is $(2p + 1, 9p - 1, 11p - 1)$ e.g. for $p = 43$, the triple is given by $(87,386,472)$, $n = 473$; $87^2 \equiv 386^2 \equiv 472^2 \equiv 1(mod\ 473)$.

Proof. Similar to proof of Proposition 17.

Proposition 23. If $n = 13p$, p(prime) with $p > 13$ for some $k \in \mathbb{N}$, $\mathbb{Z}_n^*$ has 12 possible cases of triple system;

Case 1. if $p = 13k + 1$ the triple is $(2p - 1, 11p + 1, 13p - 1)$ e.g. for $p = 53$, the triple is given by $(105,584,688)$, $n = 689$; $105^2 \equiv 584^2 \equiv 688^2 \equiv 1(mod\ 689)$.

Case 2. if $p = 13k + 2$ the triple is $(p - 1, 12p + 1, 13p - 1)$ e.g. for $p = 41$, the triple is given by $(40,493,532)$, $n = 533$; $40^2 \equiv 493^2 \equiv 532^2 \equiv 1(mod\ 533)$.

Case 3. if $p = 13k + 3$ the triple is $(5p - 1, 8p + 1, 13p - 1)$ e.g. for $p = 29$, the triple is given by $(144,233,376)$, $n = 377$; $144^2 \equiv 233^2 \equiv 376^2 \equiv 1(mod\ 377)$.

Case 4. if $p = 13k + 4$ the triple is $(6p + 1, 7p - 1, 13p - 1)$ e.g. for $p = 17$, the triple is given by $(103,118,220)$, $n = 221$; $103^2 \equiv 118^2 \equiv 220^2 \equiv 1(mod\ 221)$.

Case 5. if $p = 13k + 5$ the triple is $(3p - 1, 10p + 1, 13p - 1)$ e.g. for $p = 31$, the triple is given by $(92,311,402)$, $n = 403$; $92^2 \equiv 311^2 \equiv 402^2 \equiv 1(mod\ 403)$.

Case 6. if $p = 13k + 6$ the triple is $(4p + 1, 9p - 1, 13p - 1)$ e.g. for $p = 19$, the triple is given by $(77,170,246)$, $n = 247$; $77^2 \equiv 170^2 \equiv 246^2 \equiv 1(mod\ 247)$.

Case 7. if $p = 13k + 7$ the triple is $(4p - 1, 9p + 1, 13p - 1)$ e.g. for $p = 59$, the triple is given by $(235,532,766)$, $n = 767$; $235^2 \equiv 532^2 \equiv 766^2 \equiv 1(mod\ 767)$.

Case 8. if $p = 13k + 8$ the triple is $(3p + 1, 10p - 1, 13p - 1)$ e.g. for $p = 47$, the triple is given by $(142,469,610)$, $n = 611$; $142^2 \equiv 469^2 \equiv 610^2 \equiv 1(mod\ 611)$.

Case 9. if $p = 13k + 9$ the triple is $(6p - 1, 7p + 1, 13p - 1)$ e.g. for $p = 61$, the triple is given by $(365,428,792)$, $n = 793$; $365^2 \equiv 428^2 \equiv 792^2 \equiv 1(mod\ 793)$.

Case 10. if $p = 13k + 10$ the triple is $(5p + 1,8p - 1, 13p - 1)$ e.g. for $p = 23$, the triple is given by $(116,183,298)$, $n = 299$; $116^2 \equiv 183^2 \equiv 298^2 \equiv 1(mod\ 299)$.

Case 11. if $p = 13k + 11$ the triple is $(p + 1, 12p - 1, 13p - 1)$ e.g. for $p = 37$, the triple is given by $(38,443,480)$, $n = 481$; $38^2 \equiv 443^2 \equiv 480^2 \equiv 1(mod\ 481)$.

Case 12. if $p = 13k + 12$ the triple is $(2p + 1, 11p - 1, 13p - 1)$ e.g. for $p = 103$, the triple is given by $(207,1132,1338)$, $n = 1339$; $207^2 \equiv 1132^2 \equiv 1338^2 \equiv 1(mod\ 1339)$.

Proof. Similar to proof of Proposition 17

Proposition 24. In the ring $\mathbb{Z}_n^*$ for $n = pq$, where $p, q \in \mathbb{P}$, with $p > q$, the unit elements in $\mathbb{Z}_n^*$ form $q - 1$ triple systems for every $q \geq 3$. The triple system is of the form $(sp + 1, [q - s]p - 1, qp - 1)$, with $1 \leq s \leq q - 1$

The general form of the triples is given by;

$$(p + 1, [q - 1]p - 1, pq - 1)$$
$$(2p + 1, [q - 2]p - 1, pq - 1)$$
$$(3p + 1, [q - 3]p - 1, pq - 1)$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$([q - 1]p + 1, p - 1, pq - 1)$$

Theorem 25. *Consider the set $\mathbb{Z}_n^*$, for $n = pq$, $p,q \in \mathbb{P}$, with $p > q > 2$. We have 4 integer solutions satisfying $x^2 \equiv 1(mod\ n)$, with 3 of the solutions forming a triple for each case of q.*

Proof.

By Theorem 14, there are 2^2=4 distinct solutions to the equation $x^2 \equiv 1(mod\ n)$, for $n = pq$, with $p,q \in \mathbb{P}$ where $p > q > 2$.

By Theorem 12, the solutions are of the form:

Case A: We have two trivial solutions that correspond to items (i) and (ii)

i. $x \equiv 1(mod\ p) \equiv 1(mod\ q) \Rightarrow x \equiv 1(mod\ pq)$

{**(i)** represents the unit solution. The remaining 3 are non-unit solutions, which form the triple system}

ii. $x \equiv -1(mod\ p) \equiv -1(mod\ q) \Rightarrow x \equiv pq - 1(mod\ pq)$

Case B: The non-trivial solutions correspond to items (iii) to (viii) **iii.** $x \equiv -1(mod\ p) \equiv 1(mod\ q)$ **iv.** $x \equiv 1(mod\ p) \equiv -1(mod\ q)$

$\Rightarrow$ There is exactly one triple system for each case of q.

Theorem 26. *Consider the set $\mathbb{Z}_n^*$ for $n = 2^m p$, where p is an odd prime and $m \in \mathbb{N}$ with $m \geq 3$. The equation $x^2 \equiv 1(mod\ n)$ has 8 distinct solutions.*

Proof.

$x^2 \equiv 1(mod\ 2^m p) \Rightarrow x^2 \equiv 1(mod\ 2^m)$ and $x^2 \equiv 1(mod\ p)$

We note that:

i. $x^2 \equiv 1(mod\ 2^3)$ has 4 solutions, namely $x \equiv \pm1,\pm3(mod\ 2^3)$.

ii. $x^2 \equiv 1(mod\ 2^4)$ has 4 solutions, namely $x \equiv \pm1,\pm7(mod\ 2^4)$.

iii. $x^2 \equiv 1(mod\ 2^5)$ has 4 solutions, namely $x \equiv \pm1,\pm15(mod\ 2^5)$.

iv. $x^2 \equiv 1(mod\ 2^6)$ has 4 solutions, namely $x \equiv \pm1,\pm31(mod\ 2^6)$.

By deductive reasoning, if $m \geq 3$ then, $x^2 \equiv 1(mod\ 2^m)$ has exactly $2^2 = 4$ solutions

i.e. $x \equiv \pm1,\pm(2^{m-1} - 1)(mod\ 2^m)$.

If $x \equiv \pm1(mod\ 2^m)$, $x^2 \equiv 1(mod\ 2^m)$.

If $x \equiv \pm(2^{m-1} - 1)(mod\ 2^m)$, $x^2 \equiv 2^{2m-2}(2^{m-1}) + 1(mod\ 2^m)$

$$\equiv 2^m(2^{m-2}) - 2^m + 1(mod\ 2^m)$$

$\equiv 1(mod\ 2^m)$, *since* $m \geq 3$.

By Theorem 14, there are 2^1 distinct solutions to the equation $x^2 \equiv 1(mod\ p)$, with $p \in \mathbb{P}$ where $p \geq 3$. Combining with the results above, $x^2 \equiv 1(mod\ 2^m p)$ has exactly $2^{2+1} = 8$ solutions.

Table 1: Triple systems in $n = 2^m p$

2^m	p	$n = 2^m p$	values of x satisfying $x^2 \equiv 1(mod\ n)$						
2^3	3	24	5	7	11	13	17	19	23
2^3	5	40	9	11	19	21	29	31	39
2^3	7	56	13	15	27	29	41	43	55
2^3	11	88	21	23	43	45	65	67	87
2^3	13	104	25	27	51	53	77	79	103
2^4	3	48	7	17	23	25	31	41	47
2^4	5	80	9	31	39	41	49	71	79
2^4	7	112	15	41	55	57	71	97	111
2^4	11	176	23	65	87	89	111	153	175
2^4	13	208	25	79	103	105	129	183	207
2^5	3	96	17	31	47	49	65	79	95
2^5	5	160	31	49	79	81	111	129	159
2^5	7	224	15	97	111	113	127	209	223
2^5	11	352	65	111	175	177	241	287	351
2^5	13	416	79	129	207	209	287	337	415

2^6	3	192	31	65	95	97	127	161	191
2^6	5	320	31	129	159	161	191	289	319
2^6	7	448	97	127	223	225	321	351	447
2^6	11	704	65	287	351	353	417	639	703
2^6	13	832	129	287	415	417	545	703	831

From the table above, we pick 2 examples, from which we illustrate computational analysis for the triples of $n = 2^m p$ for an odd prime p and $m \in$ N where $m \geq 3$ and fit the triples into Fano Planes.

Example 27. *From the* 7 *non-unit solutions in* Z_{24}, *the triples are given by:*

i. $5 * 7 \equiv 11(mod\ 24)$, $5 * 11 \equiv 7(mod\ 24)$, $7 * 11 \equiv 5(mod\ 24) \Rightarrow$ The triple is given by (5,7,11)

ii. $5 * 13 \equiv 17(mod\ 24)$, $5 * 17 \equiv 13(mod\ 24)$, $13 * 17 \equiv 5(mod\ 24) \Rightarrow$ The triple is given by (5,13,17)

iii. $5 * 19 \equiv 23(mod\ 24)$, $5 * 23 \equiv 19(mod\ 24)$, $19 * 23 \equiv 5(mod\ 24) \Rightarrow$ The triple is given by (5,19,23)

iv. $7 * 13 \equiv 19(mod\ 24)$, $7 * 19 \equiv 13(mod\ 24)$, $13 * 19 \equiv 7(mod\ 24) \Rightarrow$ The triple is given by (7,13,19)

v. $7 * 17 \equiv 23(mod\ 24)$, $7 * 23 \equiv 17(mod\ 24)$, $17 * 23 \equiv 7(mod\ 24) \Rightarrow$ The triple is given by (7,17,23)

vi. $11 * 13 \equiv 23(mod\ 24)$, $11 * 23 \equiv 13(mod\ 24)$, $13 * 23 \equiv 11(mod\ 24) \Rightarrow$ The triple is given by (11,13,23)

vii. $11 * 17 \equiv 19(mod\ 24)$, $11 * 19 \equiv 17(mod\ 24)$, $17 * 19 \equiv 11(mod\ 24)$

$\Rightarrow$ The triple is given by (11,17,19)

Fitting the triples into a Fano plane we have:

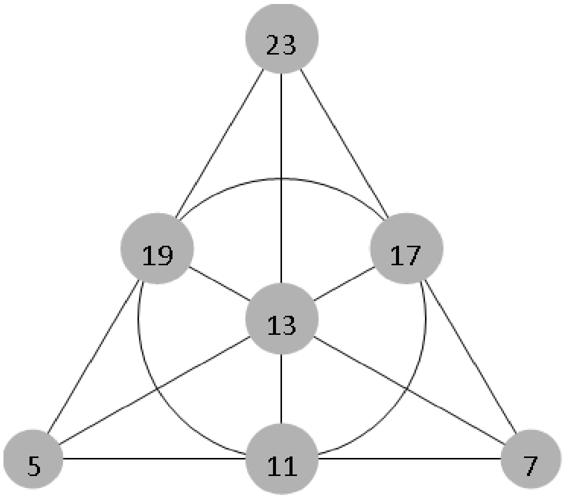

Figure1:Fano Plane Structurefor $\mathbb{Z}^*_{24}$

Example 28. *From the* 7 *non-unit solutions in* Z_{80}, *the triples are given by:*

i. $9 * 31 \equiv 39(mod\ 80)$, $9 * 39 \equiv 31(mod\ 80)$, $31 * 39 \equiv 9(mod\ 80) \Rightarrow$ The triple is given by (9,31,39)

ii. $9 * 41 \equiv 49(mod\ 80)$, $9 * 49 \equiv 41(mod\ 80)$, $41 * 49 \equiv 9(mod\ 80) \Rightarrow$ The triple is given by (9,41,49)

iii. $9 * 71 \equiv 79(mod\ 80)$, $9 * 79 \equiv 71(mod\ 80)$, $71 * 79 \equiv 9(mod\ 80) \Rightarrow$ The triple is given by (9,71,79)

iv. $31 * 41 \equiv 71(mod\ 80)$, $31 * 71 \equiv 41(mod\ 80)$, $41 * 71 \equiv 31(mod\ 80) \Rightarrow$ The triple is given by (31,41,71)

v. $31 * 49 \equiv 79(mod\ 80)$, $31 * 79 \equiv 49(mod\ 80)$, $49 * 79 \equiv 31(mod\ 80) \Rightarrow$ The triple is given by (31,49,79)

vi. $39 * 41 \equiv 79(mod\ 80)$, $39 * 79 \equiv 41(mod\ 80)$, $41 * 79 \equiv 39(mod\ 80)$

$\Rightarrow$ The triple is given by (39,41,79)

vii. $39 * 49 \equiv 71(mod\ 80)$, $39 * 71 \equiv 49(mod\ 80)$, $49 * 71 \equiv 39(mod\ 80)$

$\Rightarrow$ The triple is given by (39,49,71)

Fitting the triples into a Fano plane we have:

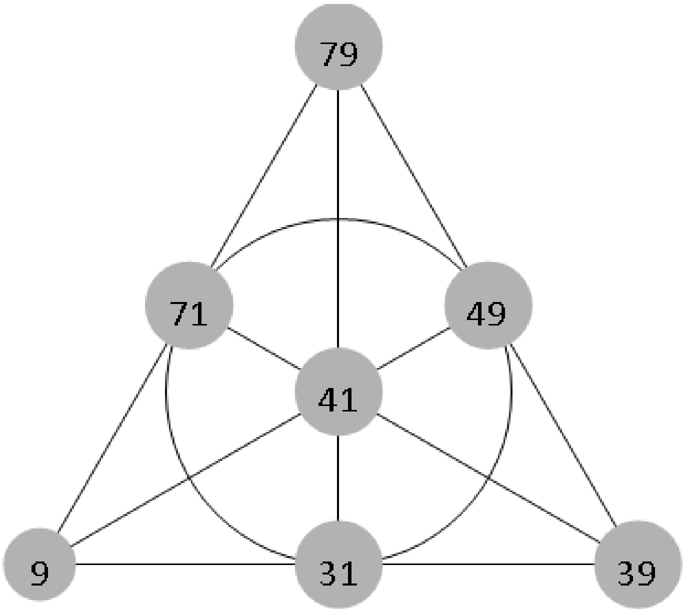

Figure2:Fano Plane Structure for $\mathbb{Z}$*80

IV. CONCLUSION

In this paper, we have successfully proved that there exists no triples in$\mathbb{Z}_n^*$, for $n = p$and $n = 2p$, $p \in \mathbb{P}$. Further, we have established the existence of triples in $\mathbb{Z}_n^*$, for $n = pq$and $n = 2^m p$, where $m \in \mathbb{N}$, p,q are odd primes with $p > q$. Finally, we have fitted the triples in$\mathbb{Z}_n^*$, $n = 2^m p$ into Fano Planes.

REFERENCES

[1] **Doyen, J., & Wilson, R. M. (1973)**. *Embeddings of Steiner triple systems*. Discrete Mathematics, 5(3), 229-239.

[2] **Hung, S. H., & Mendelsohn, N. S. (1973)**. *Directed triple systems.* Journal of Combinatorial Theory, Series A, 14(3), 310-318.

[3] **Johnson, S. J., & Weller, S. R. (2001)**. *Construction of low-density parity-check codes from Kirkman triple systems.* In GLOBECOM'01. IEEE Global Telecommunications Conference (Cat. No. 01CH37270) (Vol. 2, pp. 970-974). IEEE.

[4] **Lehmer, D. H., & Lehmer, E. (1974).** *A new factorization technique using quadratic forms*. MATHEMATICS of computation, 28(126), 625-635.

[5] **Lu, J. X. (1983)**. *On Large Sets of Disjoint Steiner Triple Systems I. J. Comb. Theory*, Ser. A, 34(2), 140-146.

[6] **Ramo, J. M. (2011)**. *On structural aspects of finite simple groups of Lie type* (Doctoral dissertation).

[7] **Skolem, T. (1959)**. *Some Remarks On The Triple Systems Of Steiner*. Mathematica Scandinavica, 6(2), 273-280.