A Count of Triples and Fano Planes in z_n^* for General n

Felix Komu[1], Benard M. Kivunge[2], Fredrick O. Nyamwala[3]

[1,3] Moi University

[2] Kenyatta University

DOI: https://doi.org/10.51244/IJRSI.2026.1311000032

Received: 31 October 2026; Accepted: 05 November 2026; Published: 20 November 2026

ABSTRACT

This paper gives an extension of our earlier established results on the projective geometric structure of Z_n^* for $n = pqrs$. It will focus on the triples and fano planes generated by order 2 elements in Z_n^*, for a general n, where n is the product of distinct odd primes all greater than 2.We shall count the number of the triples and and fano planes in Z_n^* as we establish the relationship between them.The results are presented in terms of theorems and formulas. The proof of the results is based on the established results. This paper focuses on the actual count of the the triples and fano planes and not the geometric structure of the triples and fano planes. We have used mathematical deduction to roof the two theorems.

Key Phrases: Primes, Triple Systems, Fano Planes.

INTRODUCTION

Projective geometry structure of various permutation groups has been also computed. Projective geometry structure for the group Z_n^*, $n = pq, n = pqr$ *and* $n = pqrs$ has been computed This paper seeks to extent the established results for the group Z_n^*.We shall investigate the relationship between order 2 elements in the ring *of* units modulo n, the triples and the fano planes, where n is the product of distinct odd primes greater than 2. In our study, we shall be interested on the non unity element solutions of Z_n^*, with n being the product of prime numbers all greater than two.This is due to the fact that if $n = 2$, the units in this ring $\{1\}$ only, which in turn is the unity element. For $n = 1$, the ring will have only one element which is $\{0\}$. Zero is not a unit element. This research is applying the computations of number theory.

Preliminaries

A unit in a ring is an element with a multiplicative identity 1 in the same ring

A unity element in this research refer to the multiplicative identity element in a ring, basically the element one (1). A non unity element in $\boldsymbol{Z_n^*}$ means all other elements in $\boldsymbol{Z_n^*}$ apart from the multiplicative identity element.

The group $\boldsymbol{Z_n = \{0, 1, \dots, n-1\}}$ is the group of integers modulon $\boldsymbol{n}$. The group $\boldsymbol{Z_n^*}$ is the group of units in the group. It satisfies the properties of a ring, and so mostly referred to as the ring of units modulo $\boldsymbol{n}$.

Order 2 element say $\boldsymbol{k \in Z_n^*}$ is an element that satisfies $\boldsymbol{k^2 \equiv 1\ (mod\ n)}$.

Fano plane (Komu et. al, 2025)

A fano plane is the smallest finite projective plane of order 2, containing 7 points and 7 lines that involves the set of integers and the modulus operations.

Triple system (Komu et.al, 2025)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue XI November 2026

A triple system in Z_n^* is denoted by (a_1, a_2, a_3) where there exists $k_i > 1$, $i = 1, 2, 3$, such that $a^2 \equiv 1 (\text{mod } n)$ with $a_1a_2 \equiv a_3 (\text{mod } n)$, $a_1a_3 \equiv a_2 (\text{mod } n)$ and $a_2a_3 \equiv a_1 (\text{mod } n)$.

2.3 Euler phi function Fano plane (Komu et. al, 2025)

Let a be an elements in Z^+ Then Euler's phi function $\varphi(a)$ denotes the number of positive integers $\leq a$ and relatively prime to a.

Given that a is a natural number with $(a, n) = 1$, $a^{\varphi(n)} \equiv 1 \ (mod\ n)$.

Chinese Remainder Theorem Fano plane (Gino Fano 1895)

Let $n_1, n_2, \ldots, n_3$ be pairwise co-prime positive integers and $x_1, x_2, \ldots, x_k$ be arbitrary integers. The system of simultaneous congruence

$$a \equiv x_1 (mod\ n_1)$$

$$a \equiv x_2 (mod n_2)$$

$$a \equiv x_k (mod\ n_k)$$

has a unique solution modulo $n = n_1n_2 \ldots n_k$

Corollary (Chinese remainder theorem) Fano plane (Komu et. al, 2025)

If n is an odd number with $n = \boldsymbol{p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}}$ where r is the number of distinct primes of n 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 $\boldsymbol{x^2 \equiv 1 (mod p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r})}$, then $\boldsymbol{p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} / x^2 - 1}$. But since $\boldsymbol{p_i'}$ are distinct primes, then $\boldsymbol{p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r} / x^2 - 1}$ only happens iff $\boldsymbol{p_i^{k_i} / x^2 - 1}$, for all $\boldsymbol{1 \leq i \leq r}$. But each of the congruences has two solutions , i.e $\boldsymbol{x = \pm 1 \ (mod p_i^{k_i})}$.

For each i, $1 \leq i \leq r$ choose $y_i = \pm 1$ and utilize the linear congruence's system;

$$x \equiv y_1^{k_1}$$

$$x \equiv y_2^{k_2}$$

.

.

.

$$x \equiv y_r^{k_r}$$

By the Chinese Remainder Theorem, this system has a unique solution $\boldsymbol{mod p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}}$.

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

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue XI November 2026

Assuming that the 2^r choices of x are not distinct ($mod\ n$), i.e. $x_1 \equiv x_2 (mod\ n)$, then

$x_1 \equiv x_2 (\boldsymbol{mod} \boldsymbol{p}_i^{\boldsymbol{k_i}})$ for all i. However, any two values of x are not congruent $\boldsymbol{p}_i^{\boldsymbol{k_i}}$ for at least one i. Therefore, the above system of linear congruence's has 2^r distinct solutions $x(mod\ n)$. Any of the 2^r choices satisfies $x^2 \equiv 1\ (\boldsymbol{mod} \boldsymbol{p}_i^{\boldsymbol{k_i}})$ for $1 \leq i \leq r$. Hence, there are 2^r distinct solutions to $x^2 \equiv 1 (mod\ n)$

Main results

We recall that Kinoti et.al (2020) computed the number of triples of Z_n^*, $n = pq\ and\ n = pqr$. They found that this ring has exactly three non unity solutions which generate one triple and no fano planes for $n = pq$. When $n = pqr$, they found that there are 7 non unit solutions which generate seven triples and one fano plane.

In one of our earlier papers (Felix Komu et.al. 2025), we extended these results to count the number of triples and fano planes in Z_n^*, $n = pqrs$, product of four distinct primes. We found that this result gives 15 non unity element solutions from the corollary (Chinese Remainder Theorem). The 15 non unit element solutions give 35 triples and 15 fano planes all done modulo $n = pqrs$.

We wish to extent these results in order to count the number of triples and fano planes for a general n, where n is a product of distinct odd primes all greater than 2.

Triples in Z_n^* for a general n

Theorem 3.1.1

If n is an integer and with $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ with $p_1, \dots, p_r$ being distinct odd primes, and $k_i > 0$ for $1 \leq i \leq r$. Then

(i) The equation $x^2 \equiv 1$ (mod n) has exactly 2^k solutions

(ii) The number of non unit solutions is $2^k - 1$

(iii) The number of triples per point is $\frac{2^k - 2}{2}$

(iv) The number of triples in Z_n^* is $\frac{(2^k - 1`)(2^k - 2)}{6}$

Proof

(i) From the Chinese Remainder Theorem and its corollary, if there are k distinct odd primes, then the number of non unity solutions is 2^k.

(ii) From the proof (i) above, there are 2^k solutions including the unity element 1. There fore if we exclude the unity element, the remaining elements are non unity solutions which are $2^k - 1$.

(iii) A triple has three points on a straight line. To form a triple in Z_n^*, we fix one point, We now need two more points to complete the triple. Since there are $2^k - 1$ non unity solutions and we have already fixed one solution or point, the remaining points are $2^k - 2$ .Since we need we only need two points to complete the triple, therefore the number of triples per point is given by $\frac{2^k - 2}{2}$.

(iv) Since a triple has three points on a straight and using sections (i) and (iii) above, the result follows immediately that the number of triples is obtained by multiplying the two and dividing the result by 3, which gives;

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XIII Issue XI November 2026

$$\frac{(\text{Number of non unity elements})(\text{Number of triples per element})}{3}$$

Which gives $\frac{(2^k-1`)(2^k-2)}{6}$

Remark : The ring Z_n^* has triples if n is a product of two or more distinct primes which greater than 2

Example 1.

Let k = 4, then the geometric structure has 4 distinct prime numbers. Therefore the number of triples is given by $\frac{(2^4-1`)(2^4-2)}{6} = 35\ triples.$

Example 2.

Let k = 9, then the geometric structure has 9 distinct prime numbers. Therefore the number of triples is given by $\frac{(2^9-1`)(2^9-2)}{6} = 43435\ triples.$

Fano planes in Z_n^* for a general n

***Theorem* 3.2.1**

(i) The number of times a triple appears in a fanio plane is given by $\frac{2^k-4}{4}$

(ii) The number of fano planes for general n is $\frac{(2^k-1)(2^k-2)(2^k-4)}{168}$

Proof

(i) To form a fano plane, we fix three points which leaves us with 4 points to complete a fano plane. Since we have 2^k-1 non unity elements and we have fixed three, we now have $2^k-1-3=2^k-4$ remaining points.Therefore, the total number of distinct fano planes for each triple is $\frac{2^k-4}{4}$.

(ii) The number of triples in Z_n^* for general n from theorem 3.1.1 above has been established to be $\frac{(2^k-1`)(2^k-2)}{6}$ .The number of times a triple appears in a fano plane is $\frac{2^k-4}{4}$. The number of distinct points in a fano plane is 7. Therefore the number of fano planes in Z_n^* is given by the multiplication of the number of triples and the number of times a triple appears in a fano plane and finally dividing the result by 7, that is;

$$\frac{(\text{Number of triples})(\text{Number of distinct fano planes per triple})}{7}$$

Which gives $\frac{(2^k-1)(2^k-2)(2^k-4)}{168}$

Remark: The ring Z_n^* has fano planes if n is a product of three or more distinct primes which greater than 2

Example 3

Let k = 5, then there are five distinct primes greater than 2. Therefore the number of fano planes is given by $\frac{(2^5-1)(2^5-2)(2^5-4)}{168} = 155\ fano\ planes$

Example 4

Let k = 20, then there are 20 distinct primes greater than 2. Therefore the number of fano planes is given by $\frac{(2^{20}-1)(2^{20}-2)(2^{20}-4)}{168} = \mathbf{6862582190715075}$ fano planes.

CONCLUSIONS

We have generated the formulas that give the number of triples and fano planes for a general n in Z_n^*.

REFERENCES

1. **Gikunda, D.K., & Kivunge, B. (2020)**. *Triple system and Fano Plane structure in Z_n.* Inter- national Journal of Research and Innovation in Social Science. ISSN No. 2454 – 6186, VOLUME V Issue IV, Page 23-29.
2. **Komu, F, Kivunge B. & Nyamwala F. (2025)** Projective geometry of Z_n^*, (a case of $n = pqrs$). Inter- national Journal of Research and Scientific innovation. ISSN No. 2321-2705 VOLUME XII ISSUE II Page 356-363.
3. **Gino Fano, (1895),** Sulle superficie algebriche con infinite transformazioni projective in se' stesse RendicontiAcc. Nazz. Lincei (V)41 149-15