Projective Geometry Structure of z_n^* (A Case of $n = pqrs$)

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.2025.12020031

Received: 21 January 2025; Review: 29 January 2025; Accepted: 31 January 2025; Published: 05 March 2025

ABSTRACT

The concept of projective geometry has been studied by a number of mathematicians, though the initial focus was on Euclidean and non Euclidean geometries on the relationship between lines and points on a 3D projective space. This paper will focus on the dempotent elements in Z_n^*, for n=pqrs, specifically focusing on the triples, fano planes and order 15 projective structures. We shall count the number of the triples, fano planes and order 15 projective structures, and establish the relationship between them. It extends the results of projective geometry structure of $Z_n^*, n = pqr$.

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^*, $n = pqr$ 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, fano planes and order 15 geometric structures, n= pqrs.

Preliminaries

Fano plane

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

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 $a_2a_3 \equiv a_1 (\text{mod } n)$.

Euler phi function

Let a be an elements in Z_n^*. 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

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

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

$a \equiv x_1 (mod\ n_1)$

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

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

has a unique solution modulo $n = n_1 n_2 \ldots n_k$

Corollary (Chinese remainder theorem)

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 $1 \le i \le r$, 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 $\boldsymbol{1 \le i \le r}$. But each of the congruences has two solutions , i.e $\boldsymbol{x = \pm 1\ (mod p_i^{k_i})}$.

For each i, $1 \le i \le r$ 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.

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

$x_1 \equiv x_2 (\boldsymbol{mod p_i^{k_i}})$ for all i. However, any two values of x are not congruent $\boldsymbol{p_i^{k_i}}$ 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 $x^2 \equiv 1\ (\boldsymbol{mod p_i^{k_i}})$ for $1 \le i \le r$. Hence, there are 2^r distinct solutions to $x^2 \equiv 1 (mod\ n)$

Lemma

For $x^2 \equiv 1 (mod\ n)$ and $y^2 \equiv 1 (mod\ n)$, we have $(xy)^2 \equiv 1 (mod\ n)$

Proof:

$(xy)^2 = x^2 y^2 \equiv 1 * 1 (mod\ n) = 1 (mod\ n)$

Lemma

Given $x(xy) = x^2 y = 1 * y \equiv y (mod\ n)$ and $y(xy) = xy^2 = x * 1 \equiv x (mod\ n)$, then $xy \equiv \pm 1 (mod\ n)$
Hence, $(xy)^2 \equiv 1 (mod\ n)$ if $x^2 \equiv 1 (mod\ n)$ and $y^2 \equiv 1 (mod\ n)$

Proof:

From $x^2 \equiv 1 (mod\ n)$ and $y^2 \equiv 1 (mod\ n)$ we have, $x \equiv \pm 1 (mod\ n)$ and $y \equiv \pm 1 (mod\ n)$.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

Hence, $xy \equiv (\pm 1)(\pm 1)(mod\ n) = (\pm 1)(mod\ n)$

MAIN RESULTS

Theorem

Consider the set Z^*_n $n = pqrs$, where p, q, r, s are distinct odd primes. The equation $x^2 \equiv 1(mod\ n)$ has 16 distinct solutions.

Proof:

By The Chinese Remainder Theorem, there are $2^4 = 16$ distinct solutions to the equation $x^2 \equiv 1(mod\ n)$, for $n = pqrs$, with p, q, r, s being odd prime numbers and $p > q > r > s > 2$. These solutions are of the form:

Case A: We have two trivial solutions that correspond to the following two items;

$x \equiv 1(mod\ p) \equiv 1(mod\ q) \equiv 1(mod\ r) \equiv 1(mod\ s)$

This is the unit solution, and

$x \equiv -1(mod\ p) \equiv -1(mod\ q) \equiv -1(mod\ r) \equiv -1(mod\ )\ s)$

Case B: The non-trivial solutions correspond to the following;

$x \equiv 1(mod\ p) \equiv -1(mod\ q) \equiv -1(mod\ r) \equiv 1(mod\ s)$

$x \equiv 1(mod\ p) \equiv 1(mod\ q) \equiv -1(mod\ r) \equiv -1(mod\ s)$

$x \equiv 1(mod\ p) \equiv -1(mod\ q) \equiv 1(mod\ r) \equiv -1(mod\ s)$

$x \equiv -1(mod\ p) \equiv 1(mod\ q) \equiv 1(mod\ r) \equiv 1(mod\ s)$

$x \equiv -1(mod\ p) \equiv -1(mod\ q) \equiv -1(mod\ r) \equiv 1(mod\ s)$

$x \equiv -1(mod\ p) \equiv 1(mod\ q) \equiv -1(mod\ r) \equiv -1(mod\ s)$

$x \equiv 1(mod\ p) \equiv 1(mod\ q) \equiv -1(mod\ r) \equiv 1(mod\ s)$

$x \equiv -1(mod\ p) \equiv -1(mod\ q) \equiv 1(mod\ r) \equiv -1(mod\ s)$

$x \equiv 1(mod\ p) \equiv -1(mod\ q) \equiv 1(mod\ r) \equiv 1(mod\ s)$

$x \equiv 1(mod\ p) \equiv 1(mod\ q) \equiv 1(mod\ r) \equiv -1(mod\ s)$

$x \equiv 1(mod\ p) \equiv -1(mod\ q) \equiv -1(mod\ r) \equiv -1(mod\ s)$

$x \equiv -1(mod\ p) \equiv 1(mod\ q) \equiv -1(mod\ r) \equiv 1(mod\ s)$

$x \equiv -1(mod\ p) \equiv -1(mod\ q) \equiv 1(mod\ r) \equiv 1(mod\ s)$

$x \equiv -1(mod\ p) \equiv 1(mod\ q) \equiv 1(mod\ r) \equiv -1(mod\ s)$

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

Table 1: Non-unit idempotents in Z_n, for $n = pqrs$

p	Q	R	R	N	values of x satisfying $x^2 \equiv 1(mod\ n)$									
3	5	7	11	1155	34	76	274	386	419	461	496	659	694	736
3	5	7	13	1365	64	118	209	274	391	454	664	701	911	974
3	5	7	17	1785	169	239	356	526	596	664	764	1021	1121	1189
3	5	11	13	2145	131	274	571	584	716	859	989	1156	1286	1429
3	5	11	17	2805	254	494	749	934	1121	1189	1376	1429	1616	1684
3	11	13	17	3315	664	766	781	1106	1429	1444	1546	1769	1871	1886

values of x satisfying $x^2 \equiv 1(mod\ n)$				
769	881	1079	1121	1154
1091	1156	1184	1301	1364
1258	1429	1546	1616	1784
1561	1574	1871	2014	2144
1871	2056	2311	2551	2804
2209	2549	2549	2651	3314

Example

Consider the 15 non unit solutions Z^*, n = 1155,, the triples are given by 34, 76, 274, 386, 419, 461, 496,659, 694, 736, 769, 881, 1079, 1121 and 1154. From these solutions, we make the following observations;

The 15 non unit solutions of the group generate 35 triples as follows. These triples are computed 9*mod 1155).*

$34 * 76 \equiv 274$

$34 * 386 \equiv 419$

$34 * 694 \equiv 496$

$34 * 736 \equiv 769$

$34 * 881 \equiv 1079$

$34 * 1121 \equiv 1154$

$76 * 386 \equiv 461$

$76 * 419 \equiv 659$

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

$76 * 496 \equiv 736$

$76 * 694 \equiv 769$

$76 * 881 \equiv 1121$

$76 * 1079 \equiv 1154$

$274 * 386 \equiv 659$

$274 * 419 \equiv 461$

$274 * 496 \equiv 769$

$274 * 694 \equiv 736$

$274 * 881 \equiv 1154$

$274 * 1079 \equiv 1121$

$386 * 496 \equiv 881$

$386 * 694 \equiv 1079$

$386 * 736 \equiv 1121$

$386 * 769 \equiv 1154$

$419 * 694 \equiv 881$

$419 * 736 \equiv 1154$

$419 * 769 \equiv 1121$

$461 * 694 \equiv 1154$

$461 * 736 \equiv 881$

$461 * 769 \equiv 1079$

$496 * 659 \equiv 1154$

$419 * 496 \equiv 1079$

$496 * 461 \equiv 1121$

$659 * 694 \equiv 1121$

$659 * 769 \equiv 881$

$659 * 736 \equiv 1079$

$34 * 461 \equiv 659$

That;

$34 \equiv 1(mod\ 3) \equiv -1(mod\ 5) \equiv -1(mod\ 7) \equiv 1(mod\ 11)$

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

$76 \equiv 1(mod\ 3) \equiv 1(mod\ 5) \equiv -1(mod\ 7) \equiv -1(mod\ 11)$

$274 \equiv 1(mod\ 3) \equiv -1(mod\ 5) \equiv 1(mod\ 7) \equiv -1(mod\ 11)$

$386 \equiv -1(mod\ 3) \equiv 1(mod\ 5) \equiv 1(mod\ 7) \equiv 1(mod\ 11)$

$419 \equiv -1(mod\ 3) \equiv -1(mod\ 5) \equiv -1(mod\ 7) \equiv 1(mod\ 11)$

$461 \equiv -1(mod\ 3) \equiv 1(mod\ 5) \equiv -1(mod\ 7) \equiv -1(mod\ 11)$

$496 \equiv 1(mod\ 3) \equiv 1(mod\ 5) \equiv -1(mod\ 7) \equiv 1(mod\ 11)$

$659 \equiv -1(mod\ 3) \equiv -1(mod\ 5) \equiv 1(mod\ 7) \equiv -1(mod\ 11)$

$694 \equiv 1(mod\ 3) \equiv -1(mod\ 5) \equiv 1(mod\ 7) \equiv 1(mod\ 11)$

$736 \equiv 1(mod\ 3) \equiv 1(mod\ 5) \equiv 1(mod\ 7) \equiv -1(mod\ 11)$

$769 \equiv 1(mod\ 3) \equiv -1(mod\ 5) \equiv -1(mod\ 7) \equiv -1(mod\ 11)$

$881 \equiv -1(mod\ 3) \equiv 1(mod\ 5) \equiv -1(mod\ 7) \equiv 1(mod\ 11)$

$1079 \equiv -1(mod\ 3) \equiv -1(mod\ 5) \equiv 1(mod\ 7) \equiv 1(mod\ 11)$

$1121 \equiv -1(mod\ 3) \equiv 1(mod\ 5) \equiv 1(mod\ 7) \equiv -1(mod\ 11)$

$1154 \equiv -1(mod\ 3) \equiv -1(mod\ 5) \equiv -1(mod\ 7) \equiv -1(mod\ 11)$

This establishes theorem 3.3

To get a fano plane, we fix a triple, we premultiply the three points of the triple with a fourth point, we shall generate three more points. In total we shall have 7 points which forms a fano plane. Consider the 35 triples of Z^*, n= 1155. Repeating this procedure for all the 35 triples, we generate 15 fano planes as listed as follows;

34, 76, 274, 386, 419, 461, 659

34, 76, 274, 496, 694, 736, 769

34, 76, 274, 881, 1079, 1121, 1154

34, 386, 419, 496, 694, 881, 1079

34, 386, 419, 736, 769, 1121, 1154

34, 461, 659, 496, 694, 1121, 1154

34, 461, 659, 736, 769, 881, 1079

76, 386, 461, 496, 736, 881, 1121

76, 386, 461, 694, 769, 1079, 1154

76, 419, 659, 694, 769, 881, 1121

76, 419, 496, 659, 736, 1079, 1154

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

1274, 386, 496, 659, 769, 881, 1154

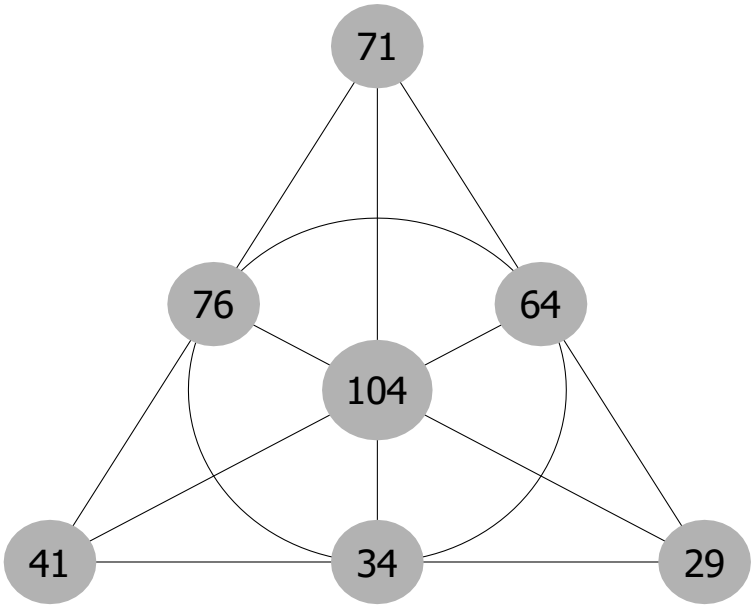
274, 386, 659, 694, 736, 1079, 1121

274, 419, 461, 694, 736, 881, 1154

274, 419, 461, 496, 769, 1079, 1121

Fitting triples into a Fano plane:

The first fano plane can be drawn as follows;



All the other fano planes can be drawn in a similar manner.

Remarks

Every triple will appear in three distinct fano planes.

Order 15 Projective geometry structure of Z_n^*, n= pqrs

To get the order 15 geometric structure, we fix a fano plane, and pick a distinct eighth element and premultiply it with all the elements of the fixed fano plane, we get the required geometric structure.

Example

Consider the 15 non unit solutions of Z_n^*, n= 1155 given by 34, 76, 274, 386, 419, 461, 496, 659,694, 736, 769, 881, 1079, 1121 and 1154. We have already seen that Z_n^*, n= 1155 has 35 triples and 15 fano planes. Consider the first fano plane given by 34,76,274,386,419,461,659. If we fix these elements and premultiply all by 694, we shall get the elements 34, 76, 274, 386, 419, 461,659 ,694,694,736,769,881,1079,1121,1154. Fixing any other fano plane and pre multiplying its elements with a distinct element from, we shall get the same result. Therefore, we have only one order 15 geometric structure given as follows; 34,76,274,386,419,461,659 ,694 ,694,736,769,881,1079,1121,1154

We can make the following observations;

Each fano plane appears once in the order 15 geometric structures

The order 15 projective geometric structure is made up of the 15 fano planes and 35 triples

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue II February 2025

CONCLUSIONS

We have established that Z^*, n= pqrs has 15 non unit solutions. These non unit solutions generate 35 triples. The 35 triples generate 15 fano planes which in turn generate only one order 15 projective geometric stricture.

REFERENCES

1. Doyen, J., & Wilson, R. M. (1973). Embeddings of Steiner triple systems. Discrete Mathematics, 5(3), 229-239.
2. 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, 5(4), 23-29.
3. Hung, S. H., & Mendelsohn, N. S. (1973). Directed triple systems. Journal of Combinatorial Theory, Series A, 14(3), 310-318.
4. 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.
5. Lehmer, D. H., & Lehmer, E. (1974). A new factorization technique using quadratic forms. MATHEMATICS of computation, 28(126), 625-635.
6. Lu, J. X. (1983). On Large Sets of Disjoint Steiner Triple Systems I. J. Comb. Theory, Ser. A, 34(2), 140-146.
7. Ramo, J. M. (2011). On structural aspects of finite simple groups of Lie type (Doctoral disserta- tion).
8. Skolem, T. (1959). Some Remarks On The Triple Systems Of Steiner. Mathematica Scandinavica, 6(2), 273-28