North Asian International Research Journal of Multidisciplinary

IRJIF IMPACT FACTOR:7.001

ISSN: 2454-2326 Vol.10, Issue, 10 October-2025

Fourth Power of Stufe and Unit Stufe of Z/nZ

***SIDDARAMU R**

**Government First Grade College, Holenarasipur, Hassan Dist- 573211.*

E-mail: sidramu@rediffmail.com, drsrmysore@gmail.com

ABSTRACT:

The Stufe and Pythagoras number of fields and rings are well known invariants in the study of sums of squares. We introduced a related notion of Unit Stufe for commutative rings with identity and compute the unit Stufe of Z/nZ, where Z/nZ denotes the ring of integer modulo the numbern.

2000 Mathematics subject classification: 11A07, 11E04,11E25,11E81 Keywords and Phrases: Stufe Pythagoras number, Residue class rings Chinese Remainder Theorem.

KEYWORDS: Modular arithmetic, Ring Z/nZ\mathbb{Z} /n \mathbb { Z} Z/nZ, Units of Z/Nz \ mathbb {Z} /n \mathbb {Z} Z/nZ, Group of units (Z/nZ)×(\mathbb {Z} /n \mathbb {Z})^{\times} (Z/nZ)×, Fourth powers modulo nnn, Power residues, Fourth power residues, Unit stufe, Stufe of a ring, Structure of unit groups

1 INTRODUCTION:

The study of sums of squares and more generally of sums of nth power has one of the longest history beginnings with Pythagoras Theorem. One can say Lagrange's Four Squares Theorem, E.Artin's proof of Hilbert's 17th Problem Pfister's Structure Theorems are some of the important landmarks in the subject. This has lead to systematic study of two field quadratic invariants Stufe and Pythagoras number of fields. The Stufe of a field F, denoted by $s(F)$, is defined to be the smallest positive integer s such that-1 is a sum of s- squares of elements in F. When no such s exists, that is, if F is formally real, we take $s(F) = \infty$. Pfister's results on the Stufe of fields were a major breakthrough: if $s(F)$ is finite then it is a power of 2 and all 2-powers occur as Stufe of suitable fields.

For higher powers, this problem is related to the classical Waring problem: Given a positive integer k, every positive integer is a sum of r number of kth power of positive integers, for some r depending only on k. The smallest such r is traditionally denoted by $g(k)$ has been computed explicitly for all $k \neq 4$.The related problem is the Waring problem mod n: computation of $g(k,n)$ when $g(k,n)$

is the smallest integer r such that every integer is a sum of r number of kth power mod n. $g(k,n)$ was introduced and investigated by C. Small.

Definition: Let Abeacommutative ring with identity $1 \neq 0$. For $k \geq 2$, $s(k,A)$ and $s_u(k,A)$ are defined as follows:

$$s(k,A) = min\{s : -1 = a_1^k + \cdots + a_s^k, \quad a_i \in A \; for \; 1 \leq i \leq s\}$$

$$s_u(k,A) = min\{t : -1 = a_1^k + \cdots + a_t^k, \quad a_i \in U(A) \; for \; 1 \leq i \leq t\}$$

where $U(A)$ denotes the multiplicative group of units of A.

If $k = 2$, then$s(k,A)$and $s_u(k,A)$ are the Stufe and the Unit Stufe of the ring of A.Unit Stufe was defined and evaluated when $A = Z_n$, the ring of integers mod n. We have investigated $s(k,A)$ when $k = 4$ and $A = Z_n$. Note that when $k \geq 3$ and k odd, $s(k,Z_n) = s_u(k,Z_n) = 1$. We have done the computation of $s_u(4,Z_n)$. We write $s(k, Z_n)$and $s_u(k, Z_n)$ simply as $s(k, n)$ and$s_u(k, n)$ respectively.

Now we can define as:

$g(k,n)$
$= min\{s: every\ element\ of\ Z_n\ is\ a\ sum\ of\ s\ number\ of\ kth\ powers\ of\ element$ In $Z_n\}$

and so clearly $s(k,n) \leq g(k,n)$and $s(k,n) \leq s_u(k,n)$.

We first give an account of certain bounds for $g(k,p)$, for odd primes p, obtained in [2].

Let$p$be an odd prime. Then $G = Z_p^* = U(Z_p)$ is a cyclic group of order $p - 1$. Let g be a generator for G. Put $u = p - 1$and $l = (u,k)$.

Let $G^k = \{x^k \,|x \in G\}$ and $kG = \{x|x^k = 1\}$. Then, $G^k \cong G/kG$. Also $|kG| = |lG| = l$. Hence, we have $[G : G^k] = l$.

If $G_i = \{x \in G|x\ is\ a\ sum\ of\ i\ kth\ powers\ in\ Z_p\}$, then,

i) $G^k = G_1 \subseteq G_2 \subseteq \ldots$; $G = \cup G_i$.
ii) $G_i = G_{i+1}$ implies $G_i = G_{i+j}$ for all $j \geq 1$.
iii) $G_i \subsetneq G_{i+1}$ implies $|G_{i+1}| \geq |G_i| + |G^k| = |G_i| + \frac{u}{l}$.
iv) there are atmost $l - 1$ strict containments in (i) and so, we have, $G^k = G_1 \leq G_2 \leq \ldots \leq G_i = G_{i+1} = \ldots$ and further $G = G_i$ implies $g(k,p) \leq l$.

Proposition 1: $g(k,p) \leq l = [G : G^k]$. Consequently,

(1) $g(k,p) = g(l,p)$

(2) $g(k,p) = l$ when $l = 1,2,\frac{u}{2},u.$

For the prime p the other value of k are termed as "k relevant for p" and for such values of k, the following proposition gives bounds for $g(k,p)$.

For a fixed $r \geq 1$ and $0 \neq b \in Z_p$, let $N(r,b)$ denotes the number of solutions to the equation $x_1^k + \cdots + x_r^k = b$where $k$is relevant for p.

Proposition 2: $|N(r,p) - p^{r-1}| \leq (k-1)^r p^{\frac{r-1}{2}}$.

Consequently $N(r,p) \geq p^{r-1} - (k-1)^r p^{\frac{r-1}{2}}$.Hence $N(r,p) > 0$ provided $p^{r-1} > (k-1)^r p^{\frac{r-1}{2}}$ .i.e., if $p > (k-1)^{\frac{2r}{r-1}}$. Since $g(k,p)$ is clearly the smallest r for which $N(r,b) > 0$ for all b, we have for relevant k.

Proposition 3: i) $g(k,p) \leq 2 \quad if \quad p > (k-1)^4$.

ii) $g(k,p) \leq 3 \quad if \quad p > (k-1)^3$.

iii) $g(k,p) \leq r \quad if \quad p > (k-1)^{\frac{2r}{r-1}}$.

$iv) g(k,p) \leq [\frac{k}{2}] \quad if \quad p > (k-1)^{2[\frac{k}{2}]/[\frac{k}{2}]+1}$.

Due to a theorem of Vaspor, we have:

Proposition 4: If $l \neq \frac{u}{2}$, u,then $g(k,p) = g(l,p) = [\frac{i}{2}] + 1$.

We now come to the computation of $s(k,p)$ for odd primes p. We observe that $s(k,p) = s_u(k,p)$,since every non-zero elements in $Z_p$is a unit. Note that $s(k,2) = 1$for all$k \geq 1$. For odd primes p, we consider different cases:

Case (1): $p \equiv 1(mod\ 8)$.

In this case $G = Z_p^8 = (g)$ is a cyclic group of order $u = p - 1 = 8m$, say. Then $g^{8m} = (g^{4m})^2 = 1$ and so $g^{4m} = -1$ and so −1 is a 4th power proving $s(4,p) = s_u(4,p) = 1$.

Case (2): $p \equiv 5(mod\ 8)$.

Now$l = (4,\ p-1) = 4$.If $s(4,p) = 1$, then −1 most be a 4th power and so, $-1 = g^{\frac{p-1}{2}} = g^{4l}$, where $g$is the generator for $G = Z_p^*$.This implies, on squaring $p-1$ divides$8l$which is a contradiction, since $p \equiv 5\ (mod\ 8)$. Thus $s(4,p) \geq 2$. Now by Proposition 3, $g(4,p) \leq 2 \quad if \quad p > (k-1)^4 = 81$. Consequently, $s(4,p) = 2$ for primes p such that $p > 81$. Hence, we need to compute the value of$s(4,p)$for the primes 5,13,29,37,53,61. It can be established (also shown in [2]) that the value of $s(4,p)$is 4 for $p = 5$ and 3 for$p = 29$and in all other cases it is 2.

Case (3): $p \equiv 3(mod 4)$.

Since −1 is not a square mod p, it is not a 4th power either and so $s(4,p) \geq 2$. Now $l = (k,\ p-1) = (4,\ p-1) = 2$. Now by proposition1,$g(4,p) \leq l = 2$which implies$(4,p) \leq 2$.Hence$s(4,p) = 2$.Thus, we have established:

Theorem1: For any prime$p$,

$$s_u(4,p) = s(4,p) = \begin{cases} 1 & if \quad p = 2 \quad or \quad if \quad p \equiv 1(mod\ 8) \\ 2 & if\ p \equiv 3(mod\ 4) \quad or\ p \equiv 5(mod\ 8), p \neq 5, 29 \\ 3 & if\ p = 29\ , \quad 4 \quad if \quad p = 5. \end{cases}$$

We now compute$s(4,n)$ when$n$isapowerofaprime.

Theorem2: Let$p$be an odd prime. Then$s(4,p^e) = s(4,p)$foralle≥ 1.

Proof:Toprovethe theorem, it sufficient toestablishthat:−1isasumof$t$4th powersinZ_{p^e}ifandonlyif−1isasumof$t$4th powers in$Z_{p^{e+1}}$.

Then at uralmap$\varphi: Z_{p^{e+1}} \to Z_{p^e}$ takes4th powersto4th powersand$\varphi(-1) = -1$. Hence$s(4,p^e) \leq s(4,p^{e+1})$.

On the other hand, suppose$s(Z_{p^e}) = t$.Then, we have$-1 \equiv a_1^4 + \cdots + a_t^4 (mod\ p^e)$ forsome$a_i \in Z$.Clearlythereexistsome$i$ suchthat$p \nmid a_i$andsowecansuppose $(p, 2a) = 1$.Then$(p, 4a_1^3) = 1$andsothereexist$x, y \in Z$suchthat$xp + 4a_i^3 y = 1$.

Now,

$a_1^4 + \cdots + a_t^4 = -1 + qp^e$, forsome$q \in Z$

$= -1 + qp^e(xp + 4a_1^3 y)$ Andso

$$\begin{aligned}(a_1 - qp^e y)^4 + a_2^4 + \cdots + a_t^4 \\ = -1 + ap^e xp + 4qp^e a_1^3 y\ + \{-4a_1^3 qp^e y + 6a_1^2 q^2 p^{2e} y^2 \\ - 4a_1^2 q^3 p^{3e} y^3 + q^3 p^{3e} y^3\} \equiv -1(mod\ p^{e+1}).\end{aligned}$$

Hences$(4,p^{e+1}) \leq s(4,p^e)$and the rebyproving the equality. Now the theorem follows.

We now consider thes$(4,n)$whennisapowerof2.Aneasycomputationgives:

$$s(4,2^e) = s_u(4,2^e) = \begin{cases} 1 \ if \ \ e=1 \\ 3 \ if \ \ e=2 \\ 7 \ if \ \ e=3 \ \ and \ 15 \ if \ \ e=4. \end{cases}$$

Lete $\geq$ 5.Wenotethat$m \in Z$isa4th powermod2^e, then,$m \equiv 0,1(mod16)$. ThegroupU_{2^e}ofunitsofZ_{2^e} isgivenby$U_{2^e} = \{\pm 5^i (mod\ 2^e) | 0 \leq i < 2^{e-2}\}$.

These quaresinU_{2^e} astheevenpowersof$5(mod\ 2^e)$andthefourthpowersinU_{2^e} arethe4th powersof$5(mod\ 2^e)$.

The number of 4th powers of $5\ (mod\ 2^e)$ is equal to the number of integers m, such that $m \equiv 1(mod16)$ with $0 \leq m \leq 2^e$. Each m, $0 \leq m \leq 2^e$ with $m \equiv 1(mod16)$is a 4th power of a unit in Z_{2^e}. Now $(2^e - 15) + 14(1) = 2^e - 1 \equiv -1(mod\ 2^e)$, and so $s(4,2^e) = s_u(4,2^e) = 15$, since $2^e - 15$ is a 4th power of a unit in Z_{2^e}. Thus we have proved:

Theorem 3:

$$s_u(4,2^e) = s(4,2^e) = \begin{cases} 1 \ if \ \ e=1 \\ 3 \ if \ \ e=2 \\ 7 \ \ if\ e=3 \ and \ \ 15 \ \ if\ e \geq 4 \end{cases}$$

We now use Chinese Remainder Theorem to compute $s(4,n)$ for all n. We prove:

Theorem 4: Let $n = p_1^{e_1} \cdots p_r^{e_r}$ denotes the canonical representation of n into product of distinct primes. Then, $s(4,n) = max\{s(4,p_1^{e_1}),\cdots,s(4,p_r^{e_r})\}$.

Proof: By Chinese Remainder Theorem, we have, $Z_n \cong \prod_{i=1}^{r} Z_{p_i^{e_i}}$.

If $-1 \equiv a_1^4 + \cdots + a_t^4 (mod\ n)$then $-1 \equiv a_1^4 + \cdots + a_t^4 (mod\ p_i^{e_i})$ and so clearly $s(4,p_i^{e_i}) \leq s(4,n)$.

Let $s = max\{s(4,p_1^{e_1}),\cdots,s(4,p_r^{e_r})\}$,let $s_i = s(4,p_i^{e_i})$. There exist $a_{i,j}$for $1 \leq i \leq r$, $1 \leq j \leq s$(by taking some $a_{i,j} = 0$, if necessary) such that $-1 \equiv \sum_{j=1}^{s} a_{i.j}^4 \ (mod\ p_i^{e_i}), 1 \leq i \leq r$. Using the Chinese Remainder Theorem, we can choose $x_j \in Z$, for $1 \leq j \leq s$ such that $x_j \equiv a_{ij} (mod\ p_i^{e_i})$, $1 \leq i \leq r$. Then $x_1^4 + \cdots + x_s^4 \equiv \sum_{j=1}^{s} a_{ij}^4 \equiv -1(mod\ p_i^{e_i})$ for all i, $1 \leq i \leq r$ and so

$x_1^4 + \cdots + x_s^4 \equiv -1(mod\ n)$. Thus $s(4,n) \leq s$.Hence $s(4,n) = s$and this proves the Theorem.

Theorem 5: The value of $s(4,n)$ is one of the following: 1,2,3,4,7,15.

Further study: By continuing the above investigation we next undertake the computation of$s_u(4,n)$.

REFERENCES:

[1] C. Small, Waring's problem mod n, this MONTHLY, 84 (1977) 12-25.

[2] C. Small, Waring's Problem, Math. Magazine, 50 (January 1977).

[3] C. Small, Powers mod n, Math. Mag., 50 (1977) p12.

[4] H. Devanport, On Waring's problems for fourth powers, Ann. of Math, 40 (1939) 731-747.

[5] W. J. Ellison, Waring's Problem, this MONTHLY, 78 (1971) 10-36.

[6] R. Siddaramu and H. N. Ramaswamy, On the Stufe, Unit Stufe and Pythago ras numbers of the ring of integers modulo n: Presented at the International Conference on Number theory, Theoretical Physics and Special Functions held at Kumbakonam, Tamilnadu during 20-22, Dec 2007.