North Asian International Research Journal of Sciences, Engineering & I.T.

IRJIF. I.F. : 3.821

ISSN: 2454-7514 Vol. 11, Issue-3, March-2025

# UNIT FOURTH POWER OF STUFE $Z/nZ$

***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 number$n$.

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

**KEYWORDS:** Unit, 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 power, Fourth powers modulo nnn, Fourth power residues, Power residues,

## 1 INTRODUCTION:

The study of sums of squares and more generally of sums of $nth$ power has one of the longest history beginning 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 $g(k)$. The value of $g(k)$ has been computed explicitly for all $k \neq 4$.The related problem is the Waring problem mod $n$: computation of $g(k,n)$ when $g(k,n)$ isthe 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 $A$beacommutative 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.$g(k,n)$ can be defined 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 $s(k,n) \leq s_u(k,n)$.

For finding $s_u = (4,n)$ of $Z/nZ$ it becomes necessary not only to find the $s(4,p^k)$ of $Z/p^kZ$ but also all possible ways in which -1 can expressed as sums of fourth power of units in $Z/p^kZ$. For this we need to determine the sets $S_4(n)$ for $n \geq 2$ defined by:

$$S_4(n) = \{t \in N: -1 \; is \; a \; sum \; of \; t \; number \; of \; fourth \; power \; of \; units \; in \; Z/nZ\}.$$

**Proposition 1.1:** Let $n \geq 2$. Then:

1. $s_u(4,n)$ is the least element of $S_4(n)$.
2. $If \;\; k,l \in S_4(n)$ then $k + l + 1 \in S_4(n)$.
3. $S_u(4,p) = s(4,p)$ for all primes $p$ and hence

$$s_u(4.p) = \begin{cases} 1 \;\; when \; p \equiv 1(mod\; 8) \\ 2 \;\; when \; p \equiv 5(mod\; 8) \; and \; p \equiv 3(mod\; 4) \\ 3 \;\; if \; p = 29 \; and \; 4 \; if \; p = 5 \end{cases}$$

**Proof:** (1) follows from the definition of $s_u(4,n)$. Every non-zero elements in $Z/pZ$ is a unit and so (2) follows. If -1 is a sum of $k$ as well as $l$ fourth powers of units, say, $-1 = x_1^4 + \cdots + x_k^4 = y_1^4 + \cdots + y_l^4$, then, $-1 = x_1^4 + \cdots + x_k^4 + y_1^4 + \cdots + y_l^4 + 1$. Hence -1 is a sum of k+l+1 fourth power of units. This proves (3).

As a consequence of Prop 1.1 we note that if $1 \in S_4(n)$ then $S_4(n)$ contains all odd numbers and if $1,2 \in S_4(n)$ then $S_4(n)$is the set of all nature numbers. We now determine $S_4(p)$ for all primes p.

Let $U^4(Z/nZ)$ denote the subgroup of $U(Z/nZ)$ consisting of fourth powers of elements in $U(Z/nZ).i.e.,U^4(Z/nZ) = \{x^4 | \, x \in U(Z/nZ)\}$. Then, $U^4(Z/3Z) = U^4(Z/5Z) = \{\bar{1}\}$ and hence $S_4(3) = \{2,5,8,11,\dots\}$ and $S_4(5) = \{4,9,14,19,\dots\}$.

Let $p \equiv 3(mod\ 4)$ and $p > 3$. Then quadratic residue and quartic residues are identical mod $p$ and so the sets $S(p)\ and\ S_4(p)$ are identical. Thus $S(p) = \{2,3,4,5,\dots\}$.

Let $p \equiv 1(mod\ 4)\ and\ p > 5$. Note that $a \in U(Z/pZ)$ is quartic residue if and only if $a^{\frac{p-1}{4}} = 1(mod\ p)$. Also -4 is a quartic residue when $p \equiv 1(mod\ 4)$. Hence -4+1+1+1=-1 implies $4 \in S_4(p)$.

Let $p \equiv 5(mod\ 8)$ by Thm 2.5. $s_u(4,p) = 2$ and so $2 \in S_4(p)$. To prove $3 \in S_4(p)$. we use the fact that, consecutive quartic residues exist for $p > 41$. If $a^4$ and $b^4$ are consecutive quartic residues modulo $p$, then, $1 + a^4 = b^4$ and so $-1 = a^4 - b^4$. Now, $2 \in S_4(p), -1 = x^4 + y^4$ for some $x, y$ and so $-1 = a^4 + (x^4 + y^4)b^4$. Hence $3 \in S_4(p)$. As 2,3,4$\in S_4(p)$, by Prop 1.1 we have $S_4(p) = \{2,3,4,5,6,\dots\}$.

If $p \equiv 1(mod\ 8)$, then $1 \in S_4(p)$ and so $3 \in S_4(p)$ by Prop 1.1. Also by above $4 \in S_4(p)$. Let $p > 41$ this consecutive quartic residue exist mod $p$. then $1 + a^4 = b^4$. If -1 is a fourth power, we have $-1 = a^4 - b^4$ and so $2 \in S_4(p)$. Hence, we have $S_4(p) = \{1,2,3,4,5,6,\dots\}$.

By the above consideration it remains compute $S_4(p)$ only when $p = 13,17,29,37,41$.

**Case 1**: $p = 13$: 1,3 and 9 are the quartic residues and

-1=12=9+3=3+3+3+3=1+1+1+3+3+3 and so $2,4,6 \in S_4(13)$ which implies $S_4(13) = \{2,4,5,6,7,8,\dots.\}$.

**Case 2**: $p = 17$: since 3,13 and 16 are quartic residues

-1=16=13+3=16+16+1=13+1+1+1, we have $S_4(17) = \{1,2,3,4,5,\dots.\}$

**Case 3**: $p = 29$: since $s(4,29) = 3$ and 23, 24, 25 are quartic residues mod 29. Thus 3,4,5,6$\in S_4(29)$ and then $S_u(29) = \{3,4,5,6,7,\dots\}$.

**Case 4:**$p = 37$: As 1,9,10,16 and 26 are quartic residues and

-1=36=26+10=26+9+1=10+16+9+1 we have 2,3,4$\in S_4(37)$ and hence $S_4(37) = \{2,3,4,5,6,\dots\}$.

**Case 5:** $p = 41$: As 16,18,37 and 40 are quartic residues, 1,3,4$\in S_4(p)$ and so $S_4(41) = \{1,3,4,5,6,7,\dots\}$. Note that $2 \notin S_4(41)$, as 41 has no consecutive pair of quartic residues. Hence, we have proved.:

**Proposition 1.2:** Let $p$ be an odd prime. Then

(i) $s_4(3) = \{2,5,8,11,14,\dots\}$
(ii) $s_4(5) = \{4,9,14,19,\dots\}$
(iii) $s_4(13) = \{2,4,5,6,7,\dots\}$
(iv) $s_4(29) = \{3,4,5,6,\dots\}$
(v) $s_4(41) = \{1,3,4,5,6,\dots\}$

Further, 1. For $p \neq 3$ and $p \equiv 3(mod\ 4), s_4(p) = \{2,3,4,5,6,\dots\}$

2. For $p \neq 5,13,29$ and $p \equiv 5(mod\ 8), s_4(p) = \{2,3,4,5,6,\dots\}$

3. For $p \neq 41$ and $p \equiv 1(mod\ 8), s_4(p) = \{1,2,3,4,5,6,\dots\}$

We now find $S_4(n)$ when $n$ is a power of a prime.

**Proposition 1.3:** Let $p$ be an odd prime. Then $S_4(p) = S_4(p^k)$ for all $k \geq 1$.

**Proof**: Consider the natural surjective ring projection $\varphi : Z/p^kZ \to Z/pZ$.

Then $\varphi$ is also surjective on the units. $U(Z/p^kZ) \to U(Z/pZ)$. Since $\varphi(-1) = -1$ and $\varphi$ is maps fourth power onto fourth power, $t \in S_4(p^k)$ implies $t \in S_4(p)$. On the other hand, let $t \in S_4(p)$. Then, we show that $t \in S_4(p^k)$.For $e \geq 1$ suppose $-1 = a_1^4 + \cdots + a_t^4 (mod\ p^e)$ for $a_i \in Z$ such that $(p, a_i) = 1, 1 \leq i \leq t$. Then $(p, 4a_i^3) = 1$ and so there exist $x, y \in Z$ such that xp+$4a_i^3 y = 1$.

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

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

And so $(a_1 - qp^e y)^4 + a_2^4 + \cdots + a_t^4 = -1 + ap^e xp + 4qp^e a_1^3 y +$

$$\{-4a_1^3 qp^e y + 6a_1^2 q^2 p^{2e} y^2 - 4a_1 q^3 p^{3e} y^3 + q^3 p^{3e} y^3\}$$

$$\equiv -1(mod\ p^{e+1}).$$

Since $(a_1 - qp^e y, p) = 1$, it follows that $t \in S_4(p^{e+1})$ and so by the repeated application above we have, $t \in S_4(p^k)$. Thus $S_4(p^k) = S_4(p)$ for all $k \geq 1$.

**Proposition 1.4:** Let $n$ be a power of 2. Then $S_4(n)$ is given by:

1. $S_4(2) = \{1,3,5,7,\dots.\}$
2. $S_4(4) = \{3,7,11,15,\dots\}$.

3. $S_4(8) = \{7,15,23,\ldots.\}$.
4. $S_4(16) = \{15,31,47,\ldots\}\ and\ S_4(2^k) = \{15,31,47,\ldots\}\ for\ k \geq 5.$

**Proof:** The sets $S(2), S(4), S(8)$ and $S(16)$ can be easily computed, since, the fourth power of any unit is the identity element. $\bar{1}$ in all the groups $U(Z/2Z), U(Z/4Z), U(Z/8Z)\ and\ U(Z/16Z)$.

For $k \geq 5$, $m$ is a fourth power of a unit in $Z/2^kZ$ if and only if $m \equiv 1(mod\ 16)$. Hence if $m = 2^k - 15$ then m is a fourth power in $Z/2^kZ$ and $-1 = \bar{m} + 14\bar{1}$ in $Z/2^kZ$ and so $15 \in S_4(2^k)$. The other numbers in $S_4(2^k)$ can be found using prop 1.1 providing the Proposition.

Using these values of $S_4(p^k)\ for\ p = 2\ and\ p$ an odd prime, we now compute $S_4(n)$ by making use of the Chinese Remainder Theorem.

**Theorem 1.5:** Let $n = p_1^{k_1}\ldots.p_r^{k_r}$ denote the canonical representation of $n$ into product of powers of distinct primes. Then $S_u(4,n)$ is given by $s_u(4,n) = min\{m: m \in \bigcap_{i=1}^{r} S_4(p_i^{k_i})\}$.

**Proof:** Since $S_u(4,n)$ is the least integer in $S_4(n)$ it is enough to show that $S_4(n) = \bigcap_{i=1}^{r} S_4(p_i^{k_i})$. Consider the natural surjective ring projection

$\varphi : Z/nZ \to Z/p_i^{k_i}Z$ thus $\varphi$ is also surjective on the units: $U(Z/nZ) \to U(Z/p_i^{k_i}Z)$. Hence $m \in S_4(n)$ implies $m \in S_4(p_i^{k_i})$. On the other hand, let $m \in \bigcap_{i=1}^{r} S_4(p_i^{k_i})$. This implies -1 can be expressed as a sum of $m$ fourth power of units in each $Z/p_i^{k_i}Z,\ 1 \leq i \leq r$.Using the Chinese Remainder Theorem, we now show that-1 can be expressed as a sum of $m$ fourth power of units in $Z/nZ$. Suppose $-1 = a_{i1}^{-4} + \cdots + a_{im}^{-4}$, where $a_{i1}^{-}, \ldots, a_{im}^{-} \in U(Z/p_i^{k_i}Z)\ for\ 1 \leq i \leq r$. By Chinese Remainder Theorem we choose $a_j{}^{-} \in Z/nZ$ such that $a_j \equiv a_{ij}\ (mod\ p_i^{k_i}), 1 \leq i \leq r, 1 \leq j \leq m$.Then, $a_1{}^{-}, \ldots, a_m{}^{-}$ are units in $Z/nZ$ and

$$\sum_{j=1}^{m} a_j^4 \equiv a_{i1}^4 + \cdots + a_{im}^4 \equiv -1(mod\ p_i^{k_i})\ for\ all\ i, 1 \leq i \leq k$$

$$\equiv -1(mod\ n)$$

Thus $m \in S_4(n)$. This completes the proof of the theorem.

Thus, for computing $s_u(4,n), where\ n = p_1^{k_1} \cdots p_r^{k_r}$ we need to find the least element in $\bigcap_{i=1}^{r} S_4(p_i^{k_i})$. By using Prop 1.3, 1.4 and 1.5, we obtain:

**Corollary 1.6:** If $n \geq 2$, then,

$s_u(4,n) = 1,2,3,4,5,7,9,11,14,15,19,23,29,39,47,50,79,119\ or\ 239$. In fact, if $n$ is odd not divisible by 15, then, $S_u(4,n) = 1,2,3\ or\ 4$.

**REFERENCES:**


1. C. Small, Waring's problem mod n, AMS Monthly, 84 (1977) p 12-25.
2. C. Small, Waring's Problem, Maths. Magazine, 50 (1977).
3. C. Small, Powers mod n, Maths. Magazine, 50 (1977) p 12.
4. C. Small, Solution of Waring's Problem mod n, AMS MONTHLY, 84 (1977) p 356-359.
5. H. Devanport, On Warning's Problems for fourth powers, Ann. of Math, 40 (1939) p 731-747.
6. W. J. Ellison, Waring's Problem, AMS MONTHYLY, 78 (1971) p 10-36.
7. R. Siddaramu and H.N. Ramaswamy, On the Stufe, Unit Stufe and Pythagoras 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.
8. D.H. Lehmer, E. Lehmer, W.H. Mills, Pairs of Consecutive Powers Residue, Can Jr. Maths. Vol. XV (No 1) 1963, p 172-177.
9. R.G. Bierstedt and W. Mills, On the bound for a pair of consecutive quartic residue modulo a prime Proc. AMS 14 (1963), p 628-652.