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

ISSN: 2454-7514 Vol. 3, Issue-3, March-2017

IRJIF. I.F. : 3.821

Sixth power of Stufe and Unit Stufe of $\mathbb{Z}/n\mathbb{Z}$

Siddaramu R
Government First Grade College, Holenarasipur,
Hassan Dist - 573211, Karnataka, India

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.

1 Introduction:

The study of sums of squares and more generally of sums of n^{th} 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 landmark 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 k^{th} 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 k^{th} power mod n. $g(k,n)$ was introduced and investigated by C. Small.

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

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

$s_u(k,A) = \min\{t : -1 = a_1^k + \cdots + a_t^k,\ a_i \in U(A) \text{ for } 1 \leq i \leq t\}$ 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 $A = \mathbb{Z}_n$, the ring of integers mod n, in [7]. We have investigated $s(k,A)$ when $k = 4$ and $A = \mathbb{Z}_n$. Note that when $k \geq 3$ and k odd, $s(k,\mathbb{Z}_n) = s_u(k,\mathbb{Z}_n) = 1$. We have done the computation of $s_u(4,\mathbb{Z}_n)$. We write $s(k,\mathbb{Z}_n)$ and $s_u(k,\mathbb{Z}_n)$ simply as $s(k,n)$ and $s_u(k,n)$ respectively.
Now we can defined as:
$g(k,n) = \min\{s :$ every element of $\mathbb{Z}_n$
is a sum of s number of kth powers of elements in $\mathbb{Z}_n\}$
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 $G = \mathbb{Z}_p^* = U(\mathbb{Z}_p)$ is a cyclic group of order $p-1$. Let g be a generator for G. Put $u = p-1$ and $l = (u,k)$.
Let $G^k = \{x^k \mid x \in G\}$ and ${}_kG = \{x \mid x^k = 1\}$. Then, $G^k \cong G/{}_kG$. Also $|{}_kG| = |{}_lG| = l$. Hence, we have $[G : G^k] = l$.
If $G_i = \{x \in G \mid x$ is a sum of i kth powers in $\mathbb{Z}_p\}$, 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 $|G_{i+1}| \geq |G_i| + |G^k| = |G_i| + \dfrac{u}{l}$.

iv) there are atmost $l-1$ strict containments in (i) and so, we have,

$G^k = G_1 \leq G_2 \leq \ldots \leq G_l = G_{l+1} = \ldots$ and further $G = G_l$ 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 $l = 1, 2, \dfrac{u}{2}, u$.

e

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 $0 \neq b \in \mathbb{Z}_p$, 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) $g(k,p) \leq 2$ if $p > (k-1)^4$.

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

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

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

Due to a theorem of Vaspor, we have:

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

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 $\mathbb{Z}_p$ is a unit. Note that $s(k,2) = 1$ for all $k \geq 1$. For odd primes p, we consider different cases:

Case(i): $p \equiv 1 (\mathrm{mod}\ 8)$.
In this case $G = \mathbb{Z}_p^* = (g)$ 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 4^{th} power proving $s(4,p) = s_u(4,p) = 1$.

Case(2): $p \equiv 5 \ (\mathrm{mod}\ 8)$.
Now $l = (4, p-1) = 4$. If $s(4,p) = 1$, then -1 most be a 4^{th} power and so, $-1 = g^{\frac{p-1}{2}} = g^{4l}$, where g is the generator for $G = \mathbb{Z}_p^*$. This implies, on squaring $p - 1$ divides $8l$ which is a contradiction, since $p \equiv 5 \ (\mathrm{mod}\ 8)$. Thus $s(4,p) \geq 2$. Now by proposition 3, $g(4,p) \leq 2$ if $p > (k-1)^4 = 81$. 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): $p \equiv 3 (\mathrm{mod}\ 4)$.
Since -1 is not a square mod p, it is not a 4^{th} power either and so $s(4,p) \geq 2$. Now $l = (k, p-1) = (4, p-1) = 2$. Now by proposition 1, $g(4,p) \leq l = 2$ which implies $s(4,p) \leq 2$. Hence $s(4,p) = 2$. Thus we have established:

3

We now come to the computation of $s(6,p)$ for odd primes p, we observe

that $s(6,p) = s_u(6,p)$, since every non zero element in $\mathbb{Z}_p$ is a unit. Note that $s(k,2) = 1$ for all $k \geq 1$. For odd prime p we consider different cases for the computation of $s(6,p)$.

Theorem 1: For any prime $p \neq 2,3$ we have $s_u(6,p)$

i) $1 \ if \ p \equiv 1(mod 4)$,

ii) $2 \ if \ p \equiv 11(mod 12)$,

iii) $2 \ if \ p \equiv 7(mod 12), p > 625$

iv) $2 \ if \ p = 19, 43, 103, 127, 151$,

v) $3 \ for \ p = 67, 79, 139, 223$,

vi) $4 \ if \ p = 31$,

vii) $6 \ if \ p = 7$.

Proof: Let $p \equiv 1(mod 4)$. Then $\mathbb{Z}_p^*$ is a cyclic group of order $p-1$. If we put $u = p-1$, then $u = 4t$ for some t. If g is the generator $1 = g^u$ and so $1 = g^{3u} = g^{12t} = (g^{6t})^2$. Thus $g^{6t} = -1$ which implies -1 is the sixth power.

Let $p \equiv 3(mod\ 4)$, if -1 is a sixth power then it is square also since $p \equiv 3(mod\ 4)$, -1 is not a square mod p. Hence -1 can not be a sixth power. Thus $s(6,p) \geq 2$.

Now $s(k,n) \leq g(k,n)$ and $g(k,p) \leq 2$ if $p > (k-1)^4$. Thus for $k = 6$ we have if $p > (k-1)^4 = 5^4 = 625, s(6,p) \leq 2$. Hence for $p > 625$ and $p \equiv 3(mod\ 4)$ we have $s(6,p) = 2$.

Theorem 2: For primes $p = 2,3$ we have $s(6,p^e)$

i) $1 \ for \ p = 2, \ e = 1$.

ii) $2 \ for \ p = 3, \ e = 1$.

iii) $3 \ for \ p = 2, \ e = 2$.

iv) $7 \ for \ p = 2, \ e \geq 3$.

v) $8 \ for \ p = 3, \ e \geq 2$.

Proof: Let $p = 2$ and $e \geq 3$, we first note that if $l \in \mathbb{Z}$ is the sixth power of $mod\ 2^e$, then $l \equiv 0, 1(mod\ 8)$. The group U_{2^e} of units in $\mathbb{Z}_{2^e}$ is given by $U_{2^e} = \{1 \leq l \leq 2^e | \ l \ is \ odd\}$. U_{2^e} is a group of order 2^{e-1} is isomorphic to $C_2 \times C_{2^{e-2}}$. Consider the homomorphism $f : U_{2^e} \longrightarrow U_{2^e}$ defined by $f(x) = x^6$

for $x \in U_{2^e}$. Now $Kerf = \{x \in U_{2^e} \mid x^6 = 1\}$, then there are precisely for elements in U_{2^e} satisfies $x^6 = 1$. In fact $kerf = \{\pm 1,\ 2^{e-1} \pm 1\}$. Thus the number of sixth powers in U_{2^e} is equal to 2^{e-3}. Further each $l,\ 1 \leq l \leq 2^e$ with $l \equiv 1(mod\ 8)$ is a sixth power and in particular $2^e - 7$ is a sixth power. Therefore we have $(2^e - 7) + 6 \cdot 1 \equiv -1(mod\ 2^e)$ and so $s(6, 2^e) = 7$.

Let $p = 3$ and $e \geq 2$. We note that $l \in \mathbb{Z}$ is a sixth power $mod\ 3^e$, then $l \equiv 0, 1(mod\ 9)$. In this case the group of units U_{3^e} in $\mathbb{Z}/3^e\mathbb{Z}$ is cyclic. Hence $x^6 = 1$ has six solution in U_{3^e} and so U_{3^e} contain 3^{e-2} sixth power since $\dfrac{\phi(3^e)}{6} = 3^{e-2}$.

Thus the sixth power in U_{3^e} are precisely the integer $l,\ l \equiv 1(mod\ 9)$. Now $(3^e - 8) + 7 \cdot 1 \equiv -1(mod\ 3^e)$ and $s(6, 3^e) = 8$. The other cases are easily verified.

Theorem 3: Let p be a prime $p \neq 2, 3$ then $s(6,\ p^e) = s(6,\ p)$ for all $e \geq 1$.
Proof: To prove the theorem it sufficient to establish that -1 is a sum of t number of sixth powers in $\mathbb{Z}_{p^e}$ if and only if -1 is a sum of t number of sixth power of $\mathbb{Z}_{p^{e+1}}$. The natural map $\phi : \mathbb{Z}_{p^{e+1}} \longrightarrow \mathbb{Z}_{p^e}$ takes sixth power to sixth powers and $\phi(-1) = -1$. Hence $s(6,\ p^e) \leq s(6,\ p^{e+1})$.
On the other hand suppose $s(\mathbb{Z}_{p^e}) = t$, then we have $-1 \equiv a_1^6 + a_2^6 + \cdots + a_t^6 (mod\ p^e)$ for some $a_i \in \mathbb{Z}$, clearly there exist some i such that $p \nmid a_i$ and so we can suppose $(p,\ a_1) = 1$ and $(p,\ 6) = 1$, then $(p,\ 6a_1^5) = 1$ and so there exist $x, y \in \mathbb{Z}$ such that $xp + 6a_1^5 y = 1$
Now $a_1^6 + a_2^6 + \cdots + a_t^6 = -1 + qp^e \quad$ for some $q \in \mathbb{Z}$

$$\begin{aligned}
&= -1 + qp^e(xp + 6a_1^5 y) \\
&= -1 + p^{e+1}qx + 6a_1^5 yqp^e
\end{aligned}$$

and so $(a_1 - qp^e y)^6 + a_2^6 + a_3^6 + \cdots + a_t^6 = -1 + p^{e+1}qx + 6a_1^5 qp^e y$

$$\begin{aligned}
&+\{-6a_1^5 qp^e y + 15a_1^4 q^2 p^{2e} y^2 - 20a_1^3 q^3 p^{3e} y^3 + 15a_1^2 q^4 p^{4e} y^4 \\
&-6a_1 q^5 p^{5e} y^5 + q^6 p^{6e} y^6\} \\
&= -1 + xp^{e+1}q + 15a_1^4 q^2 p^{2e} y^2 - 20a_1^3 q^3 p^{3e} y^3 \\
&+15a_1^2 q^4 p^{4e} y^4 - 6a_1 q^5 p^{5e} y^5 + q^6 p^{6e} y^6 \\
&= -1 + p^{e+1}(xq + 15a_1^5 p^{e-1} q^2 y^2 - 20a_1^3 p^{2e-1} q^3 y^3 \\
&+15a_1^2 p^{3e-1} q^4 y^4 - 6a_1 p^{4e-1} q^5 y^5 + p^{5e-1} q^6 y^6) \\
&\equiv -1 (mod\ p^{e+1}).
\end{aligned}$$

Hence $s(6, p^{e+1}) \leq s(6.p^e)$ and there by proving the equality.

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 Pythagoras numbers of the ring of integers modulo n*: Presented at the the International Conference on Number theory, Theoretical Physics and Special Functions held at Kumbakonam, Tamilnadu during 20-22, Dec 2007.