A Review Study on Presentation of Positive Integers as Sum of Squares

Ashwani Sikri
Department of Mathematics,
S. D. College Barnala-148101

ABSTRACT

It can be easily seen that every positive integer is written as sum of squares. In 1640, Fermat stated a theorem known as "Theorem of Fermat" which state that every prime of the form $4n+1$ can be written as sum of two squares. On December 25, 1640, Fermat sent proof of this theorem in a letter to Mersenne. However the proof of this theorem was first published by Euler in 1754, who also proved that the representation is unique. Later it was proved that a positive integer *n* is written as the sum of two squares iff each of its prime factors of the form $4k+3$ occurs to an even power in the prime factorization of n.

Diophantus stated a conjecture that no number of the form $8\lambda+7$ for non negative integer λ, is written as sum of three squares which was verified by Descartes in 1638. Later Fermat stated that a positive integer can be written as a sum of three squares iff it is not of the form $4^m(8\lambda+7)$ where *m* and λ are non-negative integers. This was proved by Legendre in 1798 and then by Gauss in 1801 in more clear way.

In 1621, Bachet stated a conjecture that "Every positive integer can be written as sum of four squares, counting 0^2" and he verified this for all integers upto 325. Fifteen years later, Fermat claimed that he had a proof but no detail was given by him. A complete proof of this four square conjecture was published by Lagrange in 1772. Euler gave much simpler demonstration of Lagrange's four squares theorem by stating fundamental identity which allow us to write the product of two sums of four squares as sum of four squares and some other crucial results in 1773.

Keywords

Integers, Prime, Squares, Sum, Euler

1. INTRODUCTION

First we characterize the positive integers which can be represented as the sum of two squares, the sum of three squares and the sum of four squares by considering the first few positive integers.

$$1 = 1^2$$
$$2 = 1^2 + 1^2$$
$$3 = 1^2 + 1^2 + 1^2$$
$$4 = 2^2$$
$$5 = 2^2 + 1^2$$
$$6 = 2^2 + 1^2 + 1^2$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2$$
$$8 = 2^2 + 2^2$$
$$so\ on \ldots\ldots$$

So, we see that positive integers are expressed as sum of four or less than four squares.

Sum of two squares

We begin with problem of expressing positive integers as sum of two squares, for this we will first consider the case when positive integer is prime.

Theorem

No prime p of the form $4k+3$ is written as a sum of two squares[1].

Proof

Let $p = 4k+3$

$\Rightarrow p \equiv 3 \pmod 4$ …… (1)

Suppose if possible that p is written as sum of two squares

i.e. $p = a^2 + b^2$ where a, b are positive integers.

Now, for any integer 'a', we have

$a \equiv 0,1,2, or\ 3 \pmod 4$

$\Rightarrow a^2 \equiv 0\ or\ 1 \pmod 4$ …… (2)

Similarly, $b^2 \equiv 0\ or\ 1 \pmod 4$ …… (3)

From (2) and (3), we have $a^2 + b^2 \equiv 0, 1\ or\ 2 \pmod 4$, which contradict (1).

So, our supposition is wrong. Hence, p is not written as sum of two square.

Wilson's Theorem

If p is a prime then $(p-1)! \equiv -1 \pmod p$ [1]

Thue's Theorem[1]

Let p be a prime and a be any integer such that $\gcd(a,p) = 1$. Then the congruence $ax \equiv y \pmod p$ has an integral solution x_0, y_0, where, $0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}$

Theorem of Fermat[2]

An odd prime p is represented as sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proof

Let p be written as sum of two squares say $p = a^2 + b^2$ … (1)

Claim $p \nmid a\ and\ p \nmid b$

Suppose $p|a$
Then p|a2 …… (2)
Also $p|p$ …… (3)

So, (2) & (3) implies p|p- a2
Which implies that p|b2 by (1)

Which further implies that $p|b$ (because p is prime)

Now $p|a \text{ and } p|b$

⇨ $p^2|a^2 \text{ and } p^2|b^2$

⇨ p2|a2 +b2

⇨ p2|p by (1)

Which is not possible

So $p \nmid a$

In Same way $p \nmid b$

Now $p \nmid b$

⇨ $\gcd(b, p) = 1$

⇨ Congruence $bx \equiv 1(mod\ p)$ has unique

Solution say $x \equiv c\ (mod\ p)$

⇨ $bc \equiv 1\ (mod\ p)$ …… (4)

(1) ⇨ $pc^2 = (ac)^2 + (bc)^2$

$(ac)^2 + (bc)^2 = pc^2$

Modulo p above equation by use of four becomes;

$(ac)^2 + 1 \equiv 0\ (mod\ p)$

⇨ $(ac)^2 \equiv -1\ (mod\ p)$

⇨ $x^2 \equiv -1\ (mod\ p)$ has sol $x \equiv ac\ (mod\ p)$

⇨ -1 is quadratic residue of p

⇨ $p \equiv 1\ (mod\ 4)$

Converse Let $p \equiv 1\ (mod\ 4)$

⇨ $p = 1 + 4\lambda$ **where** λ is a positive integer

Now p is prime so by Wilson theorem we have

$(p-1)! \equiv -1\ (mod\ p)$

1.2.3 …………… $(p-1) \equiv -1(mod\ p)$

⇨ 1.2. ………. $\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)$ ……….

$(p-2)(p-1) \equiv -1(mod\ p)$

[Because $p = 1 + 4\lambda$

⇨ $p-1|2 = 2\lambda = \text{integer}$]

⇨ 1.2………. $\left(\frac{p-1}{2}\right)$ $\left(p - \frac{p-1}{2}\right)$ …………

$(p-2)(p-1) \equiv -1(mod\ p)$

⇨ 1.2………. $\left(\frac{p-1}{2}\right)$ $\left(0 - \frac{p-1}{2}\right)$ …………

$(0-2)(0-1) \equiv -1(mod\ p)$

⇨ $\left[1.2 \ldots\ldots\ldots \left(\frac{p-1}{2}\right)\right]^2 (-1)^{\left(\frac{p-1}{2}\right)} \equiv -1\ (mod\ p)$

⇨ $\left[1.2 \ldots\ldots\ldots \left(\frac{p-1}{2}\right)\right]^2 \equiv -1\ (mod\ p)$

[Because $-1|2 = 2\lambda = \text{even}$ ⇨ $(-1)^{\left(\frac{p-1}{2}\right)} \equiv 1$]

$a^2 \equiv -1(mod\ p) \ldots\ldots\ldots (5)$ where a = 1.2…………

$\left(\frac{p-1}{2}\right)$

⇨ $(a^2, p) = (-1, p)$

⇨ $(a^2, p) = 1$ [Because $(-1, p) = 1$]

⇨ $(a, p) = 1$

So by Thue's theorem implies that the congruence

$ax \equiv y\ (mod\ p)$ has solution x_0, y_0

Where $0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}$ and x0, y0 are integers.

i.e. $ax_0 \equiv y_0\ (mod\ p)$

⇨ $a^2 x_0^2 = y_0^2 (mod\ p)$

⇨ $-1\ x_0^2 \equiv y_0^2 (mod\ p)$ by use of (5)

⇨ $y_0^2 \equiv -x_0^2\ (mod\ p)$ [Because congruence ≡ is symmetric relation]

⇨ p|x02+y02

⇨ $x_0^2 + y_0^2 = mp$ …….. (6) [for some $m \in N$]

Now $0 < |x_0| < \sqrt{p}, 0 < |y_0| < \sqrt{p}$

⇨ $0 < x_0^2 < p,\quad 0 < y_0^2 < p$

⇨ $0 < x_0^2 + y_0^2 < 2p$

⇨ $0 < m < 2$ but m is a natural number.

So this implies that $m = 1$

Put in (6) $x_0^2 + y_0^2 = p$

⇨ $p = x_0^2 + y_0^2$

⇨ p is sum of two square.

Corollary[2]

Any prime p of the form 4n+1 can be represented in a unique way as a sum of two squares (aside from the order of the summands).

Proof

Since p is prime of the form 4n+1, so it is represented as sum of two squares, Now we will prove the uniqueness, assume that

p= a2+b2 =c2+d2 (1)
Where a,b,c, d are all positive integers, (a,b)=1, (c,d)=1
Now a2d2 - b2c2 = a2d2+b2d2 - b2d2- b2c2
=(a2+b2)d2-b2(d2+c2)
= pd2 - b2p
(by 1)
= p (d2-b2)
≡0(modp) (because d2 – b2 is an integer)
a2d2-b2c2 ≡ 0 (mod p)
=> p|a2d2 - b2c2
=> p| (ad-bc) (ad+bc)
but p is prime
=> p|ad-bc or p|ad+bc (2)

(1) => a,b,c,d are all less than $\sqrt{p}$
=> 0≤ad-bc <p & 0< ad+bc <2p
So (2) => ad-bc=0 or ad+bc =p (3)
If ad+bc=p then we would have ac=bd; for,
p2= (a2+b2) (c2+d2) = (ad+bc) 2+ (ac-bd) 2
= p2+ (ac -bd) 2
=> p2= p2+ (ac-bd) 2
=> (ac-bd)2 =0
=> ac-bd =0
=> ac=bd
So (3) => either ad=bc or ac=bd - (4)
Suppose if possible that ad=bc - (5)
=> bc= ad, d is integer

=> a|bc
=> a|c [Because (a,b)=1]
=> $\exists$ +ve integer λ s.t
c=λa (6) Put in (5)
ad=bλa
=> d= λb -(7)
Now p= c2+d2 by (1)
p = λ2 (a2+b2) by (6), (7)
=> (a2+b2) = λ2 (a2+b2) by (1) because a2+ b2 is not equal to zero
=> λ=1
Put in (6), (7)
c=a, d=b
In same way the condition ac=bd impliess to a=d, b=c
Which proves uniqueness

Lemma[3]

If positive integers ∝ and β are written as sum of two squares then ∝ β is also written as sum of two squares.

Proof

Let $\propto = a^2 + b^2$ and $\beta = c^2 + d^2$ where a, b, c, d are integers.

$$\propto\beta = (a^2 + b^2)(c^2 + d^2)$$
$$= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2$$
$$= a^2c^2 + b^2d^2 + 2abcd + a^2d^2 + b^2c^2 - 2abcd$$
$$= (ac + bd)^2 + (ad - bc)^2$$

⇨ ∝ β is sum of two squares.

Theorem[4]

A positive integer n is written as the sum of two squares if and only if each of its prime factors of the form $4k + 3$ occurs to an even power in the prime factorization of n.

Proof

Suppose n is written as sum of two squares i.e. $n = a^2 + b^2$ …. (i)

where a & b are integers.

Let p be prime factor of n of the form $4k + 3$ which occurs in prime factorization of n.

Claim

Power of p is even

Let $(a, b) = d$

$$\Rightarrow \left(\frac{a}{d}, \frac{b}{d}\right) = 1$$
…….. (ii)

Let $\frac{a}{d} = x$ and $\frac{b}{d} = y$ ⇨ $a = dx$ and $b = dy$
…….. (iii)

(ii) and (iii) ⇨ $(x, y) = 1$

Now either p does not divide x or p does not divide y

[because otherwise if p | x and p | y then p|(x,y) which implies that p|1 not possible]

then $p|(x, y)$ which implies that $p|1$ not possible as p is a prime]

Let us suppose p does not divide x ⇨ gcd $(p, x) = 1$

⇨ $\propto_1 p + \beta_1 x$ =1 where $\propto_1, \beta_1$ are integers

⇨ $\beta_1 x \equiv 1 (mod\ p)$
……….. (iv)

(i) & (iii) ⇨ $n = d^2(x^2 + y^2)$

$n = d^2 m$ where $m = x^2 + y^2$

Now we will prove p does not divide m

Suppose if possible p divides m which implies p divides x2+y2

⇨ p| β12(x2+y2)

⇨ p| β12x2+ β12y2

⇨ $\beta^2{}_1 x^2 + \beta^2{}_1 y^2 \equiv 0\ (mod\ p)$
………..(v)

(iv) & (v) ⇨ $1 + \beta^2{}_1 y^2 \equiv 0\ (mod\ p)$

⇨ $(\beta_1 y)^2 \equiv -1\ (mod\ p)$

⇨ Congruence $z^2 \equiv -1\ (mod\ p)$ has a solution $z = \beta_1 y$

⇨ -1 is quadratic residue mod p

⇨ $p \equiv 1 (mod\ 4)$

Not possible [because $p = 4k + 3$ ⇨ $p \equiv 3\ (mod\ 4)$]

Our supposition is wrong

Hence p does not divide m ⇨gcd $(p, m) = 1$ [because p is prime]

Now $p|n$ ⇨ p|d2m
⇨ p|d2 because gcd $(p, m) = 1$
⇨ $p|d$ because p is prime

Let λ be the highest power of p in prime factorization of d, where λ is a positive integer.

⇨ 2 λ is the highest power of p in prime factorization of d^2

⇨ 2 λ is the highest power of p in prime factorization of $d^2 m$

(because p does not divide m)

⇨ 2 λ is the highest power of p in prime factorization of n

⇨ Power of p in prime factorization of n is even.

Converse

Let each prime factor of n of the form $4k + 3$ occurs to an even power in the prime factorization of n

Let

$n = 2^c p_1^{\alpha_1} p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots\ldots p_r^{\alpha_r} q_1^{2b_1} q_2^{2b_2} \ldots\ldots\ldots q_s^{2b_s}$ be prime factorization of n

where pi are primes of the form 4k+1 for all i=1,2,3,……r and qj are primes of the form 4t+3 for all j=1,2,3,……..,s

Since pi is prime of the form 4k+1

⇨ p_i is sum of two squares $\forall\, i = 1, 2, 3, \ldots\ldots r$ by Two squares Theorem of Fermat

⇨ $p_i^2 = p_i\, p_i$ is sum of two squares by Lemma

$\Rightarrow p_i^3 = p_i^2 p_i$ is sum of two squares by Lemma
----
----
pi i=sum of two squares $\forall i = 1, 2, 3, \ldots \ldots r$
……….. (vi)

Now

$2 = 1^2 + 1^2$ = Sum of two squares

$\Rightarrow 2^2 = 2.2 =$ Sum of two squares by Lemma

$\Rightarrow 2^3 = 2^{2.2} =$ Sum of two squares by Lemma

2^c = Sum of two squares
……..(vii)

Also

$$q_1^{2b_1} q_2^{2b_2} \ldots \ldots \ldots q_s^{2b_s} = \left(q_1^{b_1} q_2^{b_2} \ldots \ldots \ldots q_s^{b_s}\right)^2 + 0^2$$

= Sum of two squares – (viii)

(vi), (vii) and (viii) & repeated use of Lemma implies that

$2^c p_1^{a_1} p_1^{a_1} p_2^{a_2} \ldots \ldots \ldots p_r^{a_r} q_1^{2b_1} q_2^{2b_2} \ldots \ldots \ldots q_s^{2b_s}$
is sum of two squares

$\Rightarrow$ n is sum of two squares.

Examples[5]

(i) $135 = 3^{3.5}$ is not written as sum of two squares as power of prime factor 3 of the form $4(k) + 3$ for k=0 in prime factorization of 135 is not even.

(ii) $153 = 3^{2.17}$ is written as sum of two squares as power of prime 3 of the form $4(k) + 3$ for k=0 in the prime factorization of 153 is even

Also $153 = 3^{2.17}$

$153 = 3^2(4^2 + 1^2)$

$153 = 12^2 + 3^2 =$ sum of two squares.

Sum of three squares

Theorem:[6]

No positive integer of the form $4^m(8\lambda + 7)$ is written as sum of three squares where m and λ are non negative integers

Proof:- Let $n = 4^m(8\lambda + 7)$
……….. (1)

Case I $m = 0$

So (1) $\Rightarrow n = 8\lambda + 7$

$\Rightarrow n \equiv 7 \pmod 8$
………….(2)

Suppose n is sum of three squares

Let $n = a^2 + b^2 + c^2$
………….(3)

Where a, b, c are integers

Now a is any integer

$\Rightarrow a \equiv 0, 1, 2, 3, 4, 5, 6 \text{ or } 7 \pmod 8$

$\Rightarrow a^2 \equiv 0, 1 \text{ or } 4 \pmod 8$
………….(4)

In same way $b^2 \equiv 0, 1 \text{ or } 4 \pmod 8$
………….(5)

$c^2 \equiv 0, 1 \text{ or } 4 \pmod 8$
………….(6)

(4), (5) & (6) $\Rightarrow$
$a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5, \text{ or } 6 \pmod 8$

$\Rightarrow n \equiv 0, 1, 2, 3, 4, 5 \text{ or } 6 \pmod 8$
Not possible by (2)

$\Rightarrow$ Our supposition is wrong

$\Rightarrow$ n is not written as sum of three squares.

Case II $m > 0$

Suppose n is sum of three squares

Let $n = a^2 + b^2 + c^2$ where a, b, c are integers

$\Rightarrow 4^m(8\lambda + 7) = a^2 + b^2 + c^2$
………… (7)

$\Rightarrow a^2 + b^2 + c^2 =$ even because $a^2 + b^2 + c^2$ is multiple of 4

$\Rightarrow$ Either all the a, b, c are even or either two are odd and one is even.

Suppose if possible that a, b are odd and c is even.

Let $a = 2r_1 + 1,\quad b = 2r_2 + 1,\quad c = 2s$
where r1, r2 and s are integers.

$\Rightarrow$
$a^2 + b^2 + c^2 = 4(r_1^2 + r_2^2 + r_1 + r_2 + s^2) + 2$

$\Rightarrow a^2 + b^2 + c^2$ is not multiple of 4, Not true

$\Rightarrow$ all a, b, c are even

Let $a = 2a_1,\quad b = 2b_1,\quad c = 2c_1$ where a1, b1 c1 are integers

Put in (7) $4^m(8\lambda + 7) = 4(a_1^2 + b_1^2 + c_1^2)$

$\Rightarrow 4^{m-1}(8\lambda + 7) = a_1^2 + b_1^2 + c_1^2$
………… (8)

$\Rightarrow a_1^2 + b_1^2 + c_1^2 =$ even

As above we can prove that;

$a_1 = 2a_2,\quad b_1 = 2b_2,\quad c_1 = 2c_2$ where a2, b2 and c2 are integers

Put in (8)

$4^{m-1}(8\lambda + 7) = 4(a_2^2 + b_2^2 + c_2^2)$

$\Rightarrow 4^{m-2}(8\lambda + 7) = a_2^2 + b_2^2 + c_2^2$

Repeat above process $m - 2$ times more, we get

$4^{m-m}(8\lambda + 7) = a_m^2 + b_m^2 + c_m^2$ where am, bm and cm are integers.

Which implies that, $8\lambda + 7 = a_m^2 + b_m^2 + c_m^2$

Which further implies that $8\lambda + 7$ is sum of three squares not possible by Case I.

So, Our supposition is wrong

Hence $4^m(8\lambda + 7)$ is not written as sum of three squares.

Examples

1. 15, which is of the form 8 λ +7 for λ =1 &

$15 = 3^2 + 2^2 + 1^2 + 1^2 \neq$ sum of three squares

2. 240, which is of the form $4^m(8\lambda + 7)$ for m=2 and λ=1 &

$240 = 12^2 + 8^2 + 4^2 + 4^2 \neq$ sum of three squares

3. 459 is not of the form $4^m(8\lambda+7)$ for any m and λ &

459 = $13^2+13^2+11^2$ = sum of three squares

Sum of four squares

For coming to four squares problem we state two Lemmas

Lemma 1 (Fundamental Identity of Euler)[7]

If the positive integers m and n each are written as the sum of four squares, then mn is also written as such a sum.

Lemma 2 (Euler)

[7] If p is an odd prime then the congruence $x^2+y^2+1\equiv 0\ (mod\ p)$ has a solution x_0, y_0 where $0\le x_0<\frac{p-1}{2}$ and $0\le y_0<\frac{p-1}{2}$.

Theorem:[7]

For an odd prime p, there exists a positive integer $m<p$ such that mp is written as the sum of four squares.

Proof:

For an odd prime p, Lemma 2 implies that there exists integers x_0, y_0,

$$0\le x_0<\frac{p}{2}, \qquad 0\le y_0<\frac{p}{2}$$
……….. (1)

Such that

$$x_0^2+y_0^2+1\equiv 0(mod\ p)$$
$$\Rightarrow x_0^2+y_0^2+1=mp$$
………….(2)

where m is a positive integer

$$\Rightarrow mp=x_0^2+y_0^2+1^2+0^2$$
………….(3)

Now (1) and (2) implies that $mp<\frac{p^2}{4}+\frac{p^2}{4}+1$

i.e. $mp=\frac{p^2}{2}+1<p^2$

$$\Rightarrow m<p$$
…………(4)

So, (3) & (4) implies that there exists an integer $m<p$ s.t. mp is sum of four squares.

Theorem:[8]

Any prime p can be written as the sum of four squares.

Proof

The theorem is cleary true for $p=2$,

since $2=1^2+1^2+0^2+0^2$. So we consider the case for odd primes.

Now p is odd prime.

So, above theorem implies that there exists an integer $m<p$ such that mp is the sum of four squares.

Let n be the smallest positive integer such that np is the sum of four squares; say

$$np=a^2+b^2+c^2+d^2$$
………… (1)

Where a, b, c, d are integers and also $n<p$ because $n\le m$ & $m<p$

Claim $n=1$

First we will show that n is an odd integer. For a proof by contradiction, suppose if possible that n is even. Then a,b,c,d are all even; or all are odd; or two are even and two are odd. In all these possibilities we can rearrange them to have

$$a\equiv b(mod\ 2)\ \&\ c\equiv d\ (mod\ 2)$$

It follows that;

$$\frac{1}{2}(a-b),\quad \frac{1}{2}(a+b),\quad \frac{1}{2}(c-d),\quad \frac{1}{2}\ (c+d)$$

are all integers and (1) implies that

$$\frac{1}{2}\ (np)=\left(\frac{a-b}{2}\right)^2+\left(\frac{a+b}{2}\right)^2+\left(\frac{c-d}{2}\right)^2+\left(\frac{c+d}{2}\right)^2$$

is representation of $\left(\frac{n}{2}\right)$p as a sum of four squares for a positive integer $\frac{n}{2}$.

This contradicts the minimal nature of n,

So n is an odd integer

Now we will show that $n=1$. Suppose if possible n is not equal to 1, then n is at least 3 beacause n is an odd integer.

So, there exists integers A, B, C, D such that

$$a\equiv A\ (mod\ n),\qquad b\equiv B\ (mod\ n),\qquad c\equiv C\ (mod\ n),$$
… (2)

and $|A|<\frac{n}{2}$, $|B|<\frac{n}{2}$, $|C|<\frac{n}{2}$, $|D|<\frac{n}{2}$

Here, A, B, C, D are absolute least residue of a, b, c, d respectively moduleo n.

Then

$$a^2+b^2+c^2+d^2\equiv\ A^2+B^2+C^2+D^2\ (mod\ n)$$

So,

$$A^2+B^2+C^2+D^2\equiv a^2+b^2+c^2+d^2(mod\ n)$$

i.e. , $A^2+B^2+C^2+D^2\equiv np\ (mod\ n)$

i.e. $A^2+B^2+C^2+D^2\equiv 0\ (mod\ n)$

and so $A^2+B^2+C^2+D^2\equiv nk$
…………… (3)

for some non-negative integer k.

Because of restrictions on the size of A, B, C, D we have;

$$0\le nk=A^2+B^2+C^2+D^2<4\left(\frac{n}{2}\right)^2=n^2$$

We cannot have $k=0$, because this would implies that $A=B=C=D=0$ and in consequence, that n divides each of the integers a, b, c, d by (2) which implies that n2 divide each of the integers a2, b2 , c2 and d2 which further implies that n2 divides their sum i.e. n2|np by (1)

Or $n|p$ which is impossible because of $1<n<p$.

Also the relation $nk < n^2$ implies that $k < n$.

In sum; $0 < k < n$

& (3) ⇨

$(np)(nk) = (a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2$)(A2+B2+C2+D2)

⇨

$n^2pk = (aA + bB + cC + dD)^2 + (aB - bA - cD + c$ +Dc)2+(aC+bD-cA-Db)2+(aD-bC+cB-dA)2

i.e. $n^2pk = r^2 + s^2 + t^2 + u^2$ ………… (4)

where $r = aA + bB + cC + dD$

$s = aB - bA - cD + dC$

$t = aC + bD - cA - dB$

$u = aD - bC + cB - dA$

Now $r = aA + bB + cC + dD$

$\equiv A^2 + B^2 + C^2 + D^2 (mod\ n)$ by use of (2)

$\equiv 0 (mod\ n)$ by use of (3)

i.e. $r \equiv 0\ (mod\ n)$

i.e. n $|$ r

In same way, n $|$ s, n $|$ t, n $|$ u

⇨ $\frac{r}{n}, \frac{s}{n}, \frac{t}{n}, \frac{u}{n}$ are all integers.

Now (4) ⇨ $pk = \left(\frac{r}{n}\right)^2 + \left(\frac{s}{n}\right)^2 + \left(\frac{t}{n}\right)^2 + \left(\frac{u}{n}\right)^2$

⇨ pk is sum of four squares.

Since $0 < k < n$, we gets a contradiction because n is the smallest positive integer for which np is the sum of four squares. With this contradiction we have $n = 1$

Put in (1)

$p = a^2 + b^2 + c^2 + d^2$

which implies p is sum of four squares and proof is complete.

Lagrange's four square theorem[1, 9-10]

Statement

Any positive integer n can be written as the sum of four squares, some of which may be zero.

Proof

Clearly, the integer 1 is written as $1 = 1^2 + 0^2 + 0^2 + 0^2,$ a sum of four squares. Assume that $n > 1$ and let $n = p_1 p_2 \dots \dots p_r$ be canonical form of n where pi are not necessarily distinct.

We know that each p_i is written as sum of four squares

So by apply Fundamental Identity of Euler r times we obtain the result that $n = p_1 p_2 \dots \dots p_r$ is written as sum of four squares.

Example

Write 391 as sum of four squares

Solution: we use fundamental identity of Euler to write this.

Fundamental identity of euler:

If m = a2+b2+c2+d2 and n = x2+y2+z2+t2

Where a, b, c, d, x, y, z, t are integers.

Then mn= (a2+b2+c2+d2) (x2+y2+z2+t2)

= (ax+by+cz+dt)2 + (ay – bz – ct + dz)2 + (az + bt – cx – dy)2 + (at – bz + cy – dx)2

We know 391 = 17.23

= (42 + 12 + 02 + 02) (32 + 32 + 22 + 12)

= (4.3 + 1.3 + 0.2 + 0.1)2 + (4.3 – 1.3 – 0.1 + 0.2)2 + (4.2 + 1.1 – 0.3 – 0.3)2 + (4.1 – 1.2 + 0.3 – 0.3)2

= 152 + 92 + 92 + 22

= sum of four squares

2. CONCLUSION AND GENERALIZATION

Every positive integer can be expressed as sum of squares.

Many ideas were involved to generalize the squares to higher powers. Edward Waring stated that each positive integer can be expressed as sum of at least 9 cubes and also as a sum of at least 19 fourth powers and so on. There arises a question , can every positive integer be expressible as the sum of no more than a fixed number g(k) of kth powers. For answering this question, a large body of research in number theory is required. A number of Mathematicians has worked in this research and has been working to find the general formula to find g(k) for all k.

3. REFERENCES

[1] David M. Burton 1999, Elementary Number Theory, 2nd Edition: Wm. C. Brown Company Publishers.

[2] Niven I. and H. Zuckerman, 1980, An Introduction to the theory of Numbers, 4th Edition, New York: John Wiley and Sons.

[3] Hardy, Wright, An Introduction to the Theory of Numbers, Oxford, 1954.

[4] K. Rasen, Elementary Number Theory and its Applications: Addison-Wesley Publishing Co. 1993.

[5] Roberts. Joe 1977 Elementary Number Theory Cambridge Mass: MIT Press.

[6] Starke, Harold. 1970, An Introduction to Number Theory Chicago: Markham.

[7] Stewart, B. M. 1964, Theory of Numbers, 2nd edition, New York: Macmillan.

[8] Landau, E. 1952, Elementary Number Theory Trans. Goodman, New York: Chelsea.

[9] Burton, David. 1985, The History of Mathematics: An Introduction Boston: Allyn and Bacon.

[10] Upensky, J. and M. A. Heaslet. 1939, Elementary Number Theory New York: Mcgraw-Hill.