UNIT 12: SUM OF SQUARES OF INTEGERS

UNIT STRUCTURE

12.1 Learning Objectives

12.2 Introduction

12.3 Sum of Two Square

12.4 Sum of More Than Two Squares

12.5 Let Us Sum Up

12.6 Answers to Check Your Progress

12.7 Further Reading

12.8 Model Questions

12.1 LEARNING OBJECTIVES

By the end of Unit, you will be able to:

- understand the concept of writing a positive integer as a sum of two or more than two squares.
- understand and explain the conditions under which a positive integer can be expressed as the sum of two squares or three squares or four squares.
- recognize the limitations and exceptions for integers that cannot be represented as the sum of two squares and three squares.
- construct examples and counterexamples of integers expressible as sums of two, three, or four squares
- understand Lagrange's Four-Square Theorem and its significance in number theory.
- extend the concept to sums of more than two squares, examining universal quadratic forms.

12.2 INTRODUCTION

The study of expressing integers as sums of squares is a classical topic in number theory, rich with deep results and elegant proofs. This unit is divided into two interconnected parts: the sum of two squares and the sum of more than two squares.

In the first section, we will understand the concept of sum of two squares and then investigate which integers can be represented as the sum of two squares. We also explore how the property involving sum of two squares extends to certain composite numbers and how the representation is affected by the prime factorization of the integer.

The second section broadens our perspective to the representations of integers or primes as a sum of three or more squares. For greater flexibility, adding more terms like three squares, it has been found that still not all numbers can be expressed as a sum of three squares. Meanwhile, Lagrange's Four Square Theorem guarantees that every positive integer can be expressed as the sum of four squares, where a few of them may be zero, which closes the door on non- representability in this broader context.

Together, these two sections provide not only a historical and theoretical foundation but also a tool-kit for understanding the deeper arithmetic structure of the integers.

12.3 SUM OF TWO SQUARES

Starting with the question that how can we write a positive integer as a sum of two squares That is, in how many ways we can write a positive integer as a sum of two squares? For example 1 can be written as a sum of two squares in the following ways:

$$1 = 1^2 + 0^2$$
$$= 0^2 + 1^2$$
$$= (-1)^2 + 0^2$$
$$= 0^2 + (-1)^2$$

Let $r_2(n)$ be the number of representation of n as a sum of two squares where different order and signs are considered to be distinct representation. Then $r_2(1) = 4$. Similarly, the representation of 2 as a sum of two squares are

$$2 = 1^2 + 1^2$$
$$= 1^2 + (-1)^2$$
$$= (-1)^2 + 1^2$$

$= (-1)^2 + (-1)^2$

Therefore $r_2(2) = 4$. Also it can be observed that 3 can not be written as a sum of two squares and hence $r_2(3) = 0$.

Lemma 12.3.1. If a, b are two each the sum of two squares then their product ab is also the sum of two squares.

Proof. Let a and b be the sum of two squares them a and b can be written as $a = m^2 + n^2$ and $b = x^2 + y^2$ for integers m, n, x, y.

Then $ab = (m^2 + n^2)(x^2 + y^2)$ which can be simplified in the form $ab = (mx + ny)^2 + (my - nx)^2$. Thus ab is also a sum of two squares.

It is to be noted that 3 can not be written as a sum of two squares, that is, $3 = m^2 + n^2$ has no solution for any integral value of a and b. Also it can be thought that not every prime can be written as a sum of two squares. More generally, it can be seen that the prime of the form $4k + 3$ can not be expressed as a sum of two squares.

Theorem 1. The prime p of the form $4k + 3$ can not be expressed as a sum of two squares.

Proof. Let p be a prime of the form $4k + 3$ that is $p \equiv 3(mod4)$. If possible, we consider that p can be expressed as a sum of two squares, that is, $p = m^2 + n^2$. Then on modulo $4, m, n \equiv 0, 1, 2 \; or \; 3(mod\ 4)$, so that $m^2, n^2 \equiv 0 or 1(mod4)$. Then $p = m^2 + n^2 = 0, 1 \; or \; 2 \; (mod\ 4)$. It contradicts that $p \equiv 3(mod\ 4)$. Hence any prime p of the form $4k + 3$ can not be expressed as a sum of two squares.

On the other hand, any prime of the form $4k + 1$ can be expressed as a sum of two squares. The proof of this theorem involves a known principle and a result.

Pigeon-hole principle: If n objects are placed in m pigeon-holes and if $n > m$, then some pigeon-hole will contain at least two objects.

Mathematically, the above principle can also be treated as if there is a set with n elements which is the union of m of its subsets and if $n > m$, then some subsets will have more than one element.

Lemma 1.3.2. Let p be a prime and let $\gcd(\mathrm{a},\mathrm{p}) = 1$. Then the linear congruence $ax \equiv y(modp)$ admits a solution x_0, y_0, where $0 < |x_0| < \sqrt{p}$, and $0 < |y_0| < \sqrt{p}$.

Proof. Let $m = [\sqrt{\{p\}} + 1$ and let us consider the set of integers $A = \{ax - y \leq 0$

$\leq \mathrm{m} - 1, 0 \leq \mathrm{y} \leq \mathrm{m} - 1\}$.

Now since $ax - y$ takes on $m^2 > p$ possible values so from pigeonhole principle we have that at least two members of the set A must be congruent modulo *p*; let us call the two members as $ax_1 - y_1$ and $ax_2 - y_2$, where $x_1 \neq x_2$ or $y_1 \neq y_2$. Thus we have

$$a(x_1 - x_2) = y_1 - y_2(mod\ p).$$

Let $x_0 = x_1 - x_2$ and $y_0 = y_1 - y_2$ then it is clear from the above equation that x_0 and y_0 is a solution to the linear congruence $ax = y(mod\ p)$. If say $x_0 = 0$ then from the above equation and the fact that $gcd(a,p) = 1$, it is seen that $y_0 = 0$. And so $y_1 = y_2$, which is a contradiction. Hence $0 < |x_0| \leq m - 1 < \sqrt{p}$ and $0 < |x_0| \leq m - 1 < \sqrt{p}$.

Now by using the Pigeonhole principle and the above lemma, Fermat's theorem which states that every prime of the form $4k + 1$ can be expressed as the sum of two squares, can be proved.

Theorem 2. Any odd prime p can be expressed as the sum of two squares if and only if $p \equiv 1(mod\ p)$.

Proof. First suppose that any odd prime *p* can be expressed as a sum of two squares and say $p = a^2 + b^2$. Now if $p|a$ then $p \mid a^2$ and so $p \mid b^2$ which implies that *p*|*b*, and hence $p^2|p$ (*p*|*a* and *p*|*b* implies that $a=pk_1$ and $b=pk_2$ and so $p = a^2 + b^2 = p^2(k_1^2 + k_2^2)$ that means $p^2|p$), which is a contradiction. Thus we have $p \nmid a$ and $p \nmid b$. So by the theory of linear congruences, there exists an integer *c* such that *bc* ≡ 1 (mod *p*). Now the relation $(ac)^2 + (bc)^2 = pc^2$ under modulo *p* becomes

$$(ac)^2 \equiv -1(modp)$$

which shows that −1 is a quadratic residue of *p*, and we have the above equation is solvable only if *p* is of the form 4*k* + 1, that is, $p \equiv 1(mod\ p)$.

Conversely let us take all odd primes *p* that are of the form 4*k* + 1. We recall that −1 is a quadratic residue of *p* if and only if *p* is of the form 4*k* + 1. Thus there exist an integer *a* such that $a^2 \equiv -1$ (mod *p*). Now since gcd(*a*, *p*) = 1 so the linear congruence *ax* ≡ *y* (mod *p*) admits a solution x_0, y_0. Thus we can write

$$-x_0^2 \equiv a^2x_0^2 \equiv (ax_0)^2 \equiv y_0^2(mod p)$$
$$\Rightarrow\ x_0^2 + y_0^2 = 0(mod\ p)$$

From the above expression we can write $x_0^2 + y_0^2 = kp$, where *k* is an integer such that $k \geq 1$. Also we have $0 < |x_0| < \sqrt{p}$ and $0 < |p_0| < \sqrt{p}$. Thus we have $0 < x_0^2 + y_0^2 < 2p$. That is $x^2 + y^2 = kp$, where $k \geq 1$ and $0 < x^2 + y^2 < 2p$ we must conclude that $k = 1$. Hence $x_0^2 + y_0^2 = p$, which says that *p* can be expressed as a sum of two squares.

The uniqueness of the above theorem can be seen as a corollary below.

Corollary 1. Any odd prime *p* of the form $4k + 1$ can be expressed uniquely as a sum of two squares.

Proof. Let us suppose if possible that odd number *p* of the form $4k + 1$ can be expressed as a sum of two squares and let there be two representations of such. That is $p = a^2 + b^2 = c^2 + d^2$, where *a*, *b*, *c*, *d* are all positive integers. Now

$$a^2d^2 - b^2c^2 = p(d^2 - b^2) \equiv 0(mod\ p)$$
$$\Rightarrow a^2d^2 \equiv b^2c^2(modp)$$
$$\Rightarrow ad \equiv bc(modp)$$

Or similarly we have $ad \equiv -bc(mod\ p)$. Now since all *a*, *b*, *c*, *d* are all less than $\sqrt{p}$, thus we get

$$ad - bc = 0 \quad \text{or} \quad ad + bc = p$$

Again

$$p^2 = (a^2 + b^2)(c^2 + d^2) = (ad + bc)^2 + (ac - bd)^2$$
$$= p^2 + (ac - bd)^2$$

On equating both side we have $ac - bd = 0$ that is $ac = bd$. Thus we either have $ad = bc$ or $ac = bd$. Suppose that $ad = bc$, then $a|bc$, with $gcd(a,b) = 1$, which implies $a|c$, that is, $c = ka$, for some integer k. Therefore $ad = bc = bka$ which implies that $d = kb$. But

$$p = c^2 + d^2 = k^2(a^2 + b^2)$$

which implies that $k = 1$. Thus we get $a = c$ and $b = d$. On similar approach we can show that if $ac = bd$ then $a = d$ and $b = c$. Hence we can conclude that the representation of p as a sum of two squares is unique.

Example 1.

Say $p = 5$ then p is clearly of the form $4k + 1$ where $k = 1$. We are to find the representation of 5 as a sum of two squares. For this we will follow the steps

from the theorem 2, and so we will have the choice for *a* here is $[(5-1)/2]!$, that is $a = 2$. Now since $gcd(a,p) = gcd(2,5) = 1$ so we are to find the solution to the linear congruence

$$2x \equiv y(mod\ 5)$$

We now find the solution of the above linear congruence. So let $S = \{2x - y | 0 \leq x, y < 3\}$. Then the elements of *S* are given by the set $S = 0,1,2,3,4$. Now we take the element 0 of the set *S* and find the value of x and y for which it gives the value 0. And it can be easily seen that $2.1 - 2 \equiv 0(mod\ 5)$ and so that $x = 1$ and $y = 2$ are the solution of the linear congruence. Hence we can write $5 = 1^2 + 2^2$. If we order and sign are taken into consideration then we can write $5 = (-1)^2 + 2^2 = (-1)^2 + (-2)^2 = 1^2 + (-2)^2 = 2^2 + 1^2 = (-2)^2 + 1^2 = 2^2 + (-1)^2 = (-2)^2 + (-1)^2$. Thus there are 8 representation of 5 as a sum of two squares.

We have demonstrated that any prime number *p* satisfying the condition $p \equiv 1\ (mod\ 4)$ can be represented as the sum of two squares. However, this characteristic is not exclusive to such primes—there are other numbers that also share this property. For example

$$10 = 1^2 + 3^2$$

Our next objective is to give a precise description of all positive integers that can be expressed as the sum of two squares.

Theorem 3. *If a positive integer n be expressed as $n = N^2 m$, where m is square-free. Then n can be represented as the sum of two squares if and only if m has no prime factor of the form $4k + 3$.*

Proof. First suppose that *m* has no prime factor of the form $4k + 3$. If $m = 1$ then $n = N^2 + 0^2$, there is nothing to proof. Suppose, $m > 1$, let $m = p_1 p_2 \cdots p_r$ be the factorization of *m* into a product of distinct primes. Since *m* has no prime factor of the form $4k + 3$ so each of these primes p_i, being equal to 2 or of the form $4k + 1$, and hence can be expressed as the sum of two squares. Now, we have

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

which says that the product of two integers, each of which can be expressed as a sum of two squares, can also be written as a sum of two squares. By induction, this holds true for the product of any finite number of such integers. Thus, there exist integers *x* and *y* satisfying $m = x^2 + y^2$. Now,

$$n = N^2 m = N^2(x^2 + y^2) = (Nx)^2 + (Ny)^2$$

which shows that *n* can be written as a sum of two squares.

For the converse part, assume that *n* can be expressed as the sum of two squares

$$n = a^2 + b^2 = N^2 m$$

and let p be any odd prime divisor of *m*, assume that *m* > 1, without loss of generality. If $d = gcd(a, b)$, then $a = rd, b = sd$, where $gcd(r, s) = 1$. We get

$$d^2(r^2 + s^2) = N^2 m$$

and since *m* is square free so $d^2 \mid N^2$. But then

$$r^2 + s^2 = (\frac{N^2}{d^2})m = tp$$

for some integer *t*, which leads to

$$r^2 + s^2 \equiv 0(mod\ p)$$

Now the condition gcd(*r*, *s*) = 1 implies that one of *r* or *s*, say *r*, is relatively prime to *p*. Let r' satisfy the congruence

$$rr' \equiv 1(mod\ p)$$

Multiplying the equation $r^2 + s^2 \equiv 0 \pmod{p}$ by $(r')^2$, we obtain

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

That is,

$$(sr')^2 \equiv -1(mod\ p)$$

which can be written as $\frac{-1}{p} = 1$. Since we know that -1 is a quadratic residue of p, if and only if p is of the form $4k + 1$, that means the odd prime is must be of the form $4k + 1$. So, we can say that there is no prime of the form $4k + 3$ that divides m.

Corollary 2. A positive integer *n* is representable as a sum of two squares precisely when all prime factors of the form 4*k* + 3 occur to an even power in its prime decomposition.

Example 2.

The integer 459 cannot be written as the sum of two squares, because

$$459 = 3^3 \cdot 17,$$

where the prime 3 having an odd power. On the other hand,

$$153 = 3^2 \cdot 17$$

can be represented as a sum of two squares because the prime 3 being the odd prime of the form $4k + 3$ occurs to an even power, and can also bbe written as

$$153 = 3^2(4^2 + 1^2) = 12^2 + 3^2.$$

There exist some positive integers, though not primes of the form $4k + 1$, admit multiple representations as the sum of two squares. The smallest is

$$25 = 4^2 + 3^2 = 5^2 + 0^2$$

If $x \equiv y \pmod 2$, then the relation

$$xy = \left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2$$

allows us to construct a variety of such examples. For instance, taking *n* = 153, Then *n* can be written as

$$153 = 17 \cdot 9 = \left(\frac{17+9}{2}\right)^2 - \left(\frac{17-9}{2}\right)^2 = 13^2 - 4^2$$

And

$$153 = 51 \cdot 3 = \left(\frac{51+3}{2}\right)^2 - \left(\frac{51-3}{2}\right)^2 = 27^2 - 24^2$$

so that

$$13^2 - 4^2 = 27^2 - 24^2.$$

This yields the two distinct representations

$$27^2 + 4^2 = 24^2 + 13^2 = 745.$$

W CHECK YOUR PROGRESS

Q1) How many ways 13 can be expressed as a sum of two squares?

Q2) Write the representation of $n = 5 \cdot 72 \cdot 13 \cdot 17$, as a sum of two squares.

Q3) How many ways 65 can be written as a sum of two squares?

12.4 SUM OF MORE THAN TWO SQUARES

While not every positive integer can be expressed as the sum of two squares (even allowing 0^2), the situation becomes more interesting when we consider three squares. The additional degree of freedom suggests that three-square representations should exist more universally, though with some important exceptions.

Although not every positive integer can be written as the sum of two squares, what about their representation in terms of three squares (0^2 still permitted)? With an extra square to add, it seems reasonable that there should be fewer exceptions. For instance, when only two squares are allowed, we have no representation for such integers as $14, 33$ and 67, but

$$6 = 2^2 + 1^2 + 1^2 \qquad 14 = 3^2 + 2^2 + 1^2 \qquad 33 = 5^2 + 2^2 + 2^2$$

.

There are integers (possible to find) that cannot be expressed as the sum of three squares.

For this we will see the following theorem.

Theorem 4. *A positive integer n cannot be expressed as the sum of three squares (allowing 0^2) if and only if it has the form*

$$n = 4^a(8b + 7)$$

where a and b are non-negative integers.

Proof. First we show that the integer of the form $8b + 7$ is not expressible as the sum of three squares. For any integer *x*, it can be easily shown that $x^2 \equiv 0,1 \; or \; 4(mod\ 8)$. It follows that

$$x^2 + y^2 + z^2 \equiv 0, 1, 2, 3, 4, 5, or\ 6(mod\ 8)$$

for any choice of integers x, y and z. Thus, we have $8b + 7 \equiv 7 \ (mod 8)$, and so the equation $x^2 + y^2 + z^2 = 8b + 7$ is impossible to form. Hence any integer of the form $8b + 7$ can not be expressible as a sum of three squares. Next, let us first suppose that $n = 4^a(8b + 7)$, where *a* and *b* are non-negative integers, that is, $n \geq 1$, can be written as

$$4^a(8b + 7) = x^2 + y^2 + z^2$$

Then each of the integers *x*, *y*, *z* must be even. Putting $x = 2x_1$, $y = 2y_1$, $z = 2z_1$, we have

$$4^{a-1}(8b+7) = x_1^2 + y_1^2 + z_1^2$$

If $a - 1 \geq 1$, the above process may be repeated until $8b + 7$ is eventually represented as the sum of three squared integers; this, of course, contradicts the result proved in the first paragraph. This proved the result for the necessary part.

We can prove that the condition of Theorem 13.5 is also sufficient in order that a positive integer be realizable as the sum of three squares; however, the argument...

Lemma 1.4.1 (**Euler.**). *If the integers a and b are each the sum of four squares, then their product ab can also be represented as a sum of four squares.*

Proof. Suppose that the integers *a* and *b* are each represented as a sum of four squares. Then we can write, $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $b = y_1^2 + y_2^2 + y_3^2 + y_4^2$ for integers x_i, y_i. Now their product is given by,

$$ab = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$

$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$

$$+(x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 + (x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1)^2$$

From the above expression it can be concluded that *ab* can also be represented as a sum of four squares.

Lemma 1.4.2. *If p is an odd prime, then the congruence*

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

has a solution a_0, b_0 *where* $0 \leq a_0 \leq (p-1)/2$ *and* $0 \leq b_0 \leq (p-1)/2$.

Proof: To prove the lemma, we consider the following sets:

$$A_1 = \left\{1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2\right\}$$

$$A_2 = \left\{-0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2\right\}$$

Suppose that two elements of A_1 are congruent modulo p, that is, $1 + a_1^2 \equiv 1 + a_2^2(mod\ p)$, then either $a_1 \equiv a_2(mod\ p)$ or $a_1 \equiv -a_2(mod\ p)$. But $a_1 \equiv -a_2(mod\ p)$ is impossible, because $0 < a_1 + b_2 < p$ (unless $a_1 = b_2 = 0$), thus we have $a_1 \equiv b_2(mod\ p)$, which implies that $a_1 = a_2$. No two elements of the set A_1 are congruent modulo *p*. In the similar way, we can show that no two elements of A_2 are congruent modulo *p*. Together the sets A_1 and B_2 contain $2[1 + \frac{1}{2}(p-1)] = p + 1$ number of elements. Hence, by the pigeonhole principle, some integer in A_1 must be congruent modulo *p* to some integer in B_2; that is,

there exist a_0, b_0 such that

$$1 + a_0^2 \equiv -b_0^2 (mod\ p)$$

That is

$$a_0^2 + b_0^2 + 1 \equiv 0 (mod\ p)$$

where $0 \leq a_0 \leq (p-1)/2$ and $0 \leq b_0 \leq (p-1)/2$.

Alt. Approach: We will be using the Quadratic residue approach to prove the above lemma. Let $p \equiv 1(mod 4)$, then -1 is a quadratic residue of +. Then there exits a_0 to be a solution of $a^2 \equiv -1(mod\ p)$ and by choosing $b_0 = 0$ we get our result

$$a_0^2 + b_0^2 + 1 \equiv 0 (mod\ p)$$

Thus, it only needs to show the lemma for the case $p \equiv 3\ (mod\ 4)$. We first consider the integer m to be the smallest positive quadratic non-residue of p, where $m \geq 2$, because 1 is a quadratic residue of p. Now

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

so that $-m$ is a quadratic residue of p. Hence, the congruence

$$a^2 \equiv -m (mod\ p)$$

admits a solution a_0, with $0 < a_0 \leq (p-1)/2$. Now since $m - 1$, is positive and smaller than m, $m - 1$ must be a quadratic residue of p. So, there exists an integer b_0, where $0 < b_0 \leq (p-1)/2$, satisfying

$$b_0^2 \equiv m - 1 (\mathrm{mod}\ p)$$

Hence we have

$$a_0^2 + b_0^2 + 1 \equiv -m + (m-1) + 1 \equiv 0 (mod\ p)$$

where $0 < a_0 \leq (p-1)/2$ and $0 < b_0 \leq (p-1)/2$. This proves the given lemma.

From the above theorem, we get the following corollary.

Corollary 3. For an odd prime p, there exists an integer $k < p$ such that kp is represented as the sum of four squares.

Proof. From the above theorem, we have integers a_0 and b_0 such that

$$0 \leq a_0 < \frac{p}{2} \qquad\qquad 0 \leq b_0 < \frac{p}{2}$$

and

$$a_0^2 + b_0^2 + 1^2 + 0^2 = kp$$

For a suitable choice of k. The restrictions on the size of x_0 and $y_0$imply that

$$kp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2$$

and thus we have $k < p$, which is the required condition.

Example 3.

Let us suppose that $p = 17$, then the sets A_1 and B_2 become

$$A_1 = \{1,2,5,10,17,26,37,50,65\}$$

$$A_2 = \{0, -1, -4, -9, -16, -25, -36, -49, -64\}$$

On taking modulo 17, the set A_1 can be rewritten as $1, 2, 5, 10, 0, 9, 3, 16, 14$, and the set A_2 consist of the elements $0, 16, 13, 8, 1, 9, 15, 2, 4$. From the above Lemma, it can be seen that some member $1 + x^2$ of the first set is congruent to some member $-y^2$ of the second set. Thus we can observe that,

$$1 + 5^2 \equiv 9 \equiv -5^2 (mod\ 17)$$

or $1 + 5^2 + 5^2 \equiv 0 (mod\ 17)$. It follows that

$$3 \cdot 17 = 1^2 + 5^2 + 5^2 + 0^2$$

is a multiple of 17 which can be written as a sum of four squares.

Next we will be observing a few results on the fact that any prime integer can be expressed as a sum of four squares.

Theorem 5. *Any prime p can be written as the sum of four squares.*

Proof. For $p = 2$, we have $2 = 1^2 + 1^2 + 0^2 + 0^2$ and thus 2 can be written as a sum of four squares. Now say $p > 2$, that is, *p* is an odd prime. From the Corollary 3, it can be say that there exist $k < p$, the smallest positive integer say, such that kp is the sum of four squares; say,

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

We just need to show that *k* = 1.

First we will show that *k* is an odd integer. We will be showing it by contradiction. If possible assume that *k* is even. Then the possibilities for *a*, *b*, *c*, *d* are: all even, or all are odd; or two are even and two are odd. In all of the cases we can arrange them as

$$a \equiv b (mod\ 2) \qquad \text{and} \qquad c \equiv d (mod\ 2)$$

From the above condition, we have the integers as follows

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

and thus we have

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

It is clear that $(k/2)p$ can be represented as a sum of four squares. Now since $k/2 < k$, therefore it is a contradiction to the fact of minimal nature of *k*. And hence *k* is an odd integer. Now it is left to show that *k* is nothing but 1, that is $k = 1$. Again let if possible that $k \neq 1$. Then $k \geq 3$, since *k* is an odd integer. It is therefore possible to choose integers a_1, b_1, c_1, d_1 such that

$$a_1 \equiv a(mod\ k) \qquad b_1 \equiv b(mod\ k) \qquad c_1 \equiv c(mod\ k) \qquad d_1 \equiv d(mod\ k)$$

and

$$|a_1| < \frac{k}{2} \qquad |b_1| < \frac{k}{2} \qquad |c_1| < \frac{k}{2} \qquad |d_1| < \frac{k}{2}$$

Then

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0(mod\ k)$$

And therefore we can write

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = nk$$

Where n is some non-negative integer. Thus we have,

$$0 \leq nk = a_1^2 + b_1^2 + c_1^2 + d_1^2 < 4\left(\frac{k}{2}\right)^2 = k^2$$

Now if $n = 0$, it will imply that $a_1 = b_1 = c_1 = d_1 = 0$ and, then k divides each of the integers a, b, c, d and so $k\text{^}2 \mid kp$, that is, $k \mid p$, which is impossible since $3 \leq k < p$. We also have $nk < k^2$, that is, $n < k$. Sine $n \neq 0$ so we have $0 < n < k$. Now we have,

$$k^2np = (kp)(kn) = (a_2^2 + b_2^2 + c_2^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2)$$
$$= x^2 + y^2 + z^2 + w^2$$

where

$$x = aa_1 + bb_1 + cc_1 + dd_1$$

$$y = ab_1 - ba_1 + cd_1 - dc_1$$

$$z = ac_1 - bd_1 - ca_1 + db_1$$

$$w = ad_1 + bc_1 - ab_1 - da_1$$

It is important to observe that all four of x, y, z, w are divisible by k. In the

case of the integer x, for example, we have

$$r = aa_1 + bb_1 + cc_1 + dd_1 \equiv a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv 0(mod\ k)$$

Similarly, $y \equiv z \equiv w \equiv 0\ (mod\ k)$. This leads to the representation

$$np = \left(\frac{x}{k}\right)^2 + \left(\frac{y}{k}\right)^2 + \left(\frac{z}{k}\right)^2 + \left(\frac{w}{k}\right)^2$$

where *x*/*k*, *y*/*k*, *z*/*k*, *w*/*k* are all integers. Since 0 < *n* < *k*, we thus get *k* as the smallest positive integer for which *kp* is the sum of four squares, which is a contradiction, and hence *k* = 1. This completes the proof.

Theorem 6 (**Lagrange's Four Squares Theorem**)**.** Any positive integer m can be written as the sum of four squares, some of which may be zero.

Proof. It is clear that $1 = 1^2 + 0^2 + 0^2 + 0^2$, that means, 1 can be written as a sum of four squares. Assume that $m > 1$ and let $m = p_1 p_2 \cdots p_k$ be the prime factorization of *m*, where p_i's are not necessarily distinct. Since any prime can be written as a sum of four squares, so each p_i can be expressed as a sum of four squares. Also by Euler's identity, which says that product of two integers, which itself can be represented as a sum of four squares, can be expressed as a sum of four squares. This theorem, by induction, can be extends to any finite number of prime factors. Therefore $p_1 p_2$ can be written as a sum of four squares. Repeating the same process, $p_1 p_2 p_3$ can also be expressed as a sum of four squares. So applying the identity for $k - 1$ times, we will get the desired result, that is, any positive integer m can be expressed as a sum of four squares.

Example 4.

As an example we will be representing the integer 459 as a sum of four squares. Thus we can write (by using Euler's identity),

$$\begin{aligned} 459 &= 3^2 \cdot 3 \cdot 17 \\ &= 3^2(1^2 + 1^2 + 1^2 + 0^2)(4^2 + 1^2 + 0^2 + 0^2) \\ &= 3\text{^}2[(4 + 1 + 0 + 0)^2 + (1 - 4 + 0 - 0)^2 \\ &\quad +(0 - 0 - 4 + 0)\text{^}2 + (0 + 0 - 1 - 0)\text{^}2] \\ &= 3^2[5^2 + 3^2 + 4^2 + 1^2] \\ &= 15^2 + 9^2 + 12^2 + 3^2 \end{aligned}$$

The above representation is the required representation of 459 as a sum of four squares.

Lagrange's theorem inspired a deeper exploration into whether every positive integer can be expressed as a quadratic form in four variables with fixed positive integer coefficients, that is, the four variable expression is of the form

$$ax^2 + by^2 + cz^2 + dw^2$$

where a, b, c and d are all given positive integers. In 1916, the famous Indian mathemati- cian Srinivasa Ramanujan identified 53 such "universal quadratic forms", four of which were already known. One example is the quadratic form combining squares of four variables with coefficients 1, 2, 3, and 8, which can represent all positive integers. For instance, the number 39 can be expressed as follows.

$$39 = 2^2 + 2 \cdot 0^2 + 3 \cdot 3^2 + 8 \cdot 1^2$$

In 2005, mathematician Manjul Bhargava made a significant breakthrough by proving that there are exactly 204 number of desired quadratics. Later, in a definitive resolution to the problem, Bhargava and Jonathan Hanke discovered a key criterion: a specific set of 29 positive integers that can be used to test whether any given quadratic form is universal. This provided a complete classification of such forms, settling a long-standing question in number theory.

2. 12.5 LET US SUM UP

- The prime p of the form $4k + 3$ can not be expressed as a sum of two squares, more generally, any odd prime p can be expressed as the sum of two squares if and only if $p \equiv 1(mod\ 4)$.
- If a, b are two each the sum of two squares then their product ab is also the sum of two squares.
- A positive integer n cannot be expressed as the sum of three squares (allowing 0^2) if and only if it has the form

$$n = 4^a(8b + 7)$$

- where a and b are non-negative integers.
- If the integers a and b are each the sum of four squares, then their product ab can also be represented as a sum of four squares.
- Any prime p can be written as the sum of four squares. More generally, Lagrange's Four Squares Theorem states that any positive integer m can be written as the sum of four squares, some of which may be zero.

K 12.6 ANSWERS TO CHECK YOUR PROGRESS

Answer to the Q. no. 1: Here $p = 13$ and *p* is clearly of the form $4k + 1$ where $k = 3$. We are to find the representation of 13 as a sum of two squares. For this we will follow the steps from the theorem 2, and so we will have the choice for *a* here is $[(13 - 1)/2]!$, that is $a = 720$. Now since $gcd(a, p) = gcd(720, 13) = 1$ so we are to find the solution to the linear congruence

$$720x \equiv y(mod\ 13)$$

But on modulo 13, the above equation can be rewritten as

$$5x \equiv y(mod\ 13)$$

We now find the solution of the above linear congruence. For this, let $S = \{5x - y | 0 \leq x, y < 4\}$. Then the elements of *S* are given by the set $S = \{-3, -2, -1, 0, 2, 3, 4, 5, 7, 8, 9, 10, 12, 13, 14, 15\}$. On taking modulo 13, we now have the elements of *S* as $S = \{0, 1, 2, 3, 4, 5, 7, 8, 9, 10, 11, 12\}$. Now we take the element 0 of the set S and find the value of *x* and *y* for which it gives the value 0. And it can be easily seen that $5 \cdot 3 - 2 \equiv 0(mod\ 13)$ and so that $x = 3$ and $y = 2$ are the solution of the linear congruence. Hence we can write $13 = 3^2 + 2^2$. If the order and sign are taken into consideration then we can write $13 = (-3)^2 + 2^2 = (-3)^2 + (-2)^2 = 3^2 + (-2)^2 = 2^2 + 3^2 = (-2)^2 + 3^2 = 2^2 + (-3)^2 = (-2)^2 + (-3)^2$. Thus there are 8 representation of 13 as a sum of two squares.

Answer to the Q. no. 2: Here $n = 5 \cdot 7^2 \cdot 13 \cdot 17$. In this case, we have

$$n = 7^2 \cdot 5 \cdot 13 \cdot 17 = 7^2(2^2 + 1^2)(3^2 + 2^2)(4^2 + 1^2)$$

Two applications of the identity appearing in Theorem 3 give

$$(3^2 + 2^2)(4^2 + 1^2) = (12 + 2)^2 + (3 - 8)^2 = 14^2 + 5^2$$

And

$$(2^2 + 1^2)(14^2 + 5^2) = (28 + 5)^2 + (10 - 14)^2 = 33^2 + 4^2$$

When these are combined, we end up with

$$n = 7^2(33^2 + 4^2) = 231^2 + 28^2$$

Answer to the Q. no. 3: We are to find the representation of 65 as a sum of two squares. For this we write 65 = 13 · 5. In this unit we already have seen the representation of 13 and 5 as sum of two squares such that $13 = 2^2 + 3^2$ and $5 = 1^2 + 2^2$. Thus we have

$$65 = (2^2 + 3^2)(1^2 + 2^2)$$

Now by using the identity used in Theorem 3, the above expression now becomes

$$65 = (2 + 6)^2 + (4 - 3)^2 = 8^2 + 1^2$$

Now it can be observed that if we write $513 = 3^2 + 2^2$ and then write

$$65 = (3^2 + 2^2)(1^2 + 2^2)$$

Then by using the identity used in 3, we get

$$65 = (3 + 4)^2 + (6 - 2)^2 = 7^2 + 4^2$$

So, the there are two distinct representations of 65 as a sum of two squares and they are

$$65 = 8^2 + 1^2 = 7^2 + 4^2$$

O 12.7 FURTHER READING

1. David Burton: Elementary Number Theory, Universal Book Stall, New Delhi.
2. George E. Andrews: Number Theory, Hindustan Publishing Corporation, New Delhi.
3. K.C. Chowdhury: A First Course in Theory of Numbers, Asian Books Pvt. Ltd.
4. Ramanujachary Kumanduri; Cristina Romero: Number Theory with Computer Applica- tions, Prentice Hall, New Jersey.
5. G.H. Hardy; E.M. Wright: An Introduction to the Theory of Numbers, OUP.
6. Thomas Koshy: Elementary Number Theory with Applications, Harcourt Science and Technology Company.
7. S.G. Telang (eds. M.G.Nadkarni & J.S.Dani) : Number Theory, Tata McGraw-Hill Pub- lishing Company Limited .
8. Gareth A. Jones & J. Mary Jones, Elementary Number Theory, Springer.
9. Apostol, T. M. Introduction to Analytic Number Theory. Springer 2014.
10. Niven, I. and Zuckerman, H. S. Introduction to the Theory of Numbers. John Wiley & Sons, 2008.
11. Hardy, G. H. and Wright, E. M. Theory of Numbers. Oxford Science Publications, 2003.

M 12.8 MODEL QUESTIONS

Q. 1: Represent each of the primes 113, 229, and 373 as a sum of two squares.

Q. 2: Prove that a prime *p* can be expressed as a sum of two squares if and only if the congruence $x^2 + 1 \equiv 0(mod\ p)$ admits a solution. (**Hint**: Use the concept of

quadratic residue)

Q. 3: Prove that the positive integer *n* has as many representations as the sum of two squares as does the integer 2*n*. (**Hint**: Find a representation of *n* as a sum of two squares and then show that 2*n* has the same representation.

Q. 4: Prove that every prime number *p* of the form $8k + 1$ or $8k + 3$ can be written as $p = a^2 + 2b^2$, for some choice of integers *a* and *b*. (**Hint**: The proof is very similar to the proof of Theorem 2)

*** *** ***