AN ABSTRACT OF THE THESIS OF

RASHIDAH ISMAIL for the MASTER OF SCIENCE

in MATHEMATICS presented on MARCH 29, 1989

Title : REPRESENTATION OF INTEGERS AS SUM OF SQUARES .

Abstract approved : Essam Abotteen

The purpose of this thesis is to investigate the problem of representing an integer as sum of two, three, and four squares.

First the necessary and sufficient conditions for an integer to be representable as the sum of two and four squares are considered. Then I investigate the problem of the representation of integers as a sum of two and four nonvanishing squares. Next the problem of representing integers as a sum of two and four unequal squares is studied. The uniqueness of representations is also be discussed. Formulas for the total number of representation of an integer as a sum of two and four squares are given. For the sum of three squares problem I characterize the integers that can be represented as a sum of three squares, and only give formulas without proofs for the number of representations of an integer as a sum of three squares, since their proofs are beyond the scope of this thesis.

REPRESENTATION OF INTEGERS AS SUM OF SQUARES

A Thesis

Presented to

the Division of Mathematical and Physical Sciences

EMPORIA STATE UNIVERSITY

In Partial Fulfillment

of the Requirements for the Degree

Master of Science

by

Rashidah Ismail

May 1989

Essam Abattam

Approved for the Major Division

James L Wolfe

Approved for the Graduate Council

ACKNOWLEDGEMENTS

In the Name of Allah, Most Gracious, Most Merciful, without Whose help and guidance this work would not been accomplised.

I would like to express my thanks and my deep appreciation to my advisor Dr. Essam Abotteen for his expert guidance, recommendations, assistance and encouragement in conducting this research. I express my gratitute to my committee and my professors at Emporia State University.

A thank you also goes to my family and all brothers and sisters in Islam for their prayers and support.

Finally a very special thanks and love goes to my husband, Ariff, and my children, Abbas and Fatimah. Without their limitless support, patience and love it would not have been possible for me to carry out this study.

TABLE OF CONTENTS

CHAPTER 1

THE STATEMENT OF THE PROBLEM AND A BRIEF HISTORY

The representation of an integer as a sum of kth power integers has fascinated several generations of mathematicians, and its generalizations and analogues occupy a central place in number theory today.

In this study we confine ourselves to the problem of the representation of a positive integer as a sum of two squares,three squares and four squares. The main problems of the representation of an integer as a sum of squares can be formulated as follows:

1) Given a positive integer k, what integers can be represented as a sum of k squares?.
2) If an integer is so representable, how many representations are there?.

The problems of representation of integers as a sum of kth powers can be stated more generally in terms of Quadratic Forms.

Given a quadratic form Q in k variables $x_1,..,x_k$ with integral coefficients. Let N_Q be the set of values of Q. Then the two problems of representation can now be formulated as follows:

1') Given a quadratic form Q, determine N_Q.

2') Given Q and $n \in N_Q$, determine the number of representation of n by Q, i.e determine the number of vectors $(a_1,....a_k) \in Z^k$ for which $Q(a_1,...,a_k) = n$.

Another equivalent formulation of these problems is as follows:

1") Given a quadratic form Q in k variables and an integer n, determine whether the Dophantine equation $Q(x_1,..,x_k)= n$ has solution.

2") Given Q and a representable integer n, find the number of solutions of the Diophantine equation, $Q(x_1,..,x_k) = n$.

In this study we confine ourselves to the cases where k = 2, 3 and 4. Both problems of representation , will be completely solved for k = 2 and 4 in chapters 2 and 3. For k =3,we will characterize the integers that can be represented as a sum of three squares, and we will only give formulas without proofs for the number of representations of an integer as a sum of three squares, since their proofs are beyond the scope of this thesis.

Before going any further we need to make few remarks:

1) In this study by the word "square" we mean the square of integers (positive, negative or zero).

2) Two representations of an integer n are regarded as being <u>not essentially distinct</u> if they only differ trivially (i.e by the order of the summands, or by the sign of a term), otherwise they are said

to be essentially distinct. For example $5 = 2^2 + 1^2$ $=(-2)^2 + (-1)^2 = (-2)^2 + 1^2$ $=2^2 +(-1)^2 = 1^2 + 2^2 = (-1)^2 + (-2)^2 = 1^2 + (-2)^2$ $= (-1)^2 + 2^2$ has a total of 8 representations as a sum of two squares.However, any two of these representations differ only by the order of the summands, or by a sign of one of the terms, and therefore they are not essentially distinct. On the hand, $5 = 2^2 + 1^2$ is the only essentially distinct representation of 5.

3) If a number is representable by a sum of k squares then it is representable by a sum of m squares for any m >=k.

We will show in chapter 3, the least value of k , for which all numbers are representable as a sum of k squares is k = 4,that is to say that any number is representable by a sum of four squares and that four is the least number of squares by which all numbers are representable. This is a special case of well known problem called Waring`s problem, stated by Waring in 1770:

Suppose r > 1 is an integer. Does there exist a positive integer k, such that every positive integer n is a sum of k rth powers of integers, i.e such that the Diophantine equation $n = x_1^r + x_2^r + \dots + x_k^r$ has a solution for all n > 0?

The problem of representing an integer as a sum of kth power integers has a very lengthy history. In this brief historical introduction, we will give a very short sketch of the history of the representation of an integer as a sum of squares. For a more detail acount of the early history the reader may consult Dickson's treatise[3] and a more recent book by A.Weil[16].

The problem of representing an integer as sums of 2, 3, and 4 squares goes back as far as Diophantus. Eventhough Diophantus (325 - 409 A.D) knew and made several statements related to the problem of sum of two squares, but Girard in 1625 and Fermat a few years later, were first to recognize the problem and stated the correct necessary and sufficient conditions on an integer n to be representable as a sum of two squares. Fermat also knew how to determine the number of ways in which a given number of the proper form is a sum of two squares. He stated that he could prove that every prime of the form 4n + 1 is a sum of two squares by the method of indefinite descent. Euler in 1749 was the first to succed in finding a complete proof after struggling with this problem for seven years.

Diophantus stated that no number of the form 8m + 7 is a sum of three squares, a fact easily verified by Descartes. It was Fermat who finally gave the complete proof and formulated the correct conditions that a number is a sum of three squares if and only if it is not of the form $4^n(8m + 7)$. Euler and Langrange tried for many years to prove this theorem but neither Euler nor Lagrange found a proof for all cases. In 1798 Legendre gave a complicated proof for this theorem. Finally in 1801, Gauss gave a complete proof which depended on more difficult results in his extensive theory of quadratic forms. He also obtained a formula for the number of primitive representation for an integer as a sum of three squares. Other proofs have since been given, but none of them can be described as both elementary and simple.

Some historians believed that the fact that every natural number is representable as the sums of four squares was first known to Diophantus of Alexandria because he expressed 5, 13, and 30 as sum of four squares in two ways without mention of any conditions on a number in order to be a sum of four squares whereas he gave necessary conditions for representation as a sum of two and three squares. Hence Bachet and Fermat ascribed to Diophantus a knowledge of the beautiful theorem that every positive integer is a sum of four squares. Bachet verified this theorem for an integer up to 325. The theorem was stated to be true by Girard in 1625 and Fermat claimed that he possesed a proof by indefinite descent. Euler gave serious attention on this theorem for more than 40 years. Not until twenty years after he began the study of the theorem did he publish some important facts about it. The first proof published was by Lagrange in 1772, who gave a lot of credits to Euler's paper. The following year Euler published a proof which is much simpler than Lagrange and which has not been improved upon to date.

CHAPTER 2

SUM OF TWO SQUARES

1.Representation Of Integers As Sum Of Two Squares.

In this chapter we confine ourselves to the case $k = 2$, i.e the representation of a positive integer as a sum of two squares. In this case the two representation problems are:

1) To find the necessary and sufficient conditions for an integer n to be representable as the sum of two squares. That is to say, we want to characterize the set of integers N_Q , for which the Diophantine equation $Q(x,y) = x^2 + y^2 = n$ has a solution.
2) Let $N_Q = \{n \in Z \quad x^2 + y^2 = n$, has integral solution$\}$. The problem is: for $n \in N_Q$, determine the number $r_2(n)$ of solutions of $x^2 + y^2 = n$, where $r_2(n)$ is the total number of solutions that are not essentially distinct.

The problem of determining which numbers are representable as the sum two square is a very old one. In the Arithmetic of Diophantus (325-409 A.D) there are several statements connected with this problem, but their precise meaning is not clear[3]. It was Girard (1595-1632) who first stated the correct necessary and sufficient conditions on an integer n to be representable as a sum of two squares. But it seems that there is no indication that Girard had a proof for his statement. The first proof we know of was published by Euler in 1749[3].

The Main theorem of this section is the following:

Theorem 2.1:

A positive integer n is representable as the sum of two squares if and only if the factorization of n into prime factors does not contain any prime of the form 4k+3 that has an odd exponent in the canonical form of n. That is an integer $n = \prod p_i^{\alpha_i}$ is representable as the sum of two squares if and only if α_i is not odd for every i for which p_i is of the form 4k+3.

As an illustration of the theorem, we note that 3 has no representation as a sum of two squares. On the other hand 90 has, in fact $90 = 3^2 + 9^2$. Note that the prime factorization of 90 is $90 = 2.3^2.5$.

Our objective in this section is the proof of Theorem 2.1. It is an easy matter to rule out certain numbers as incapable of being represented as the sum of two squares.

Lemma 2.01:

Any integer of the form 4m + 3 can not be represented as a sum of two squares.

Proof:

First note that if x is any even integer then $x^2 \equiv 0 (\mathrm{mod} 4)$ and for any odd integer y we have $y^2 \equiv 1 (\mathrm{mod}\ 4)$. Hence the sum of any two squares must be congruent either to 0 + 0 or 0 + 1 or 1+1 (mod4) that is $x^2 + y^2 \equiv 0, 1,$ or 2 (mod4). Thus any number of the form 4m + 3 can not be the sum of two squares.

Lemma 2.02:

If the prime factors of an integer n can be written as the sum of two squares, then n is the sum of two squares.

Proof:

This follow immediately from the identity applied several times if necessary to the prime factors of n.

$(x^2 + y^2)(x_1^2 + y_1^2) = X^2 + Y^2,$

where $X = xx_1 + yy_1$, $Y = xy_1 - yx_1$.

Lemma 2.03:

If p is a prime of the form 4k + 1, then there exists an integer z such that $z^2 + 1 \equiv 0$ (modp).

Proof:

This is equivalent to proving that the congruence $z^2 + 1 \equiv 0$ (modp) is solvable for any prime p of the form 4k+1, which follows directly from Euler's Criterion for an integer to be quadratic residue (modp).

Lemma 2.03 implies that if p is a prime of the form 4k + 1, there exists a positive integer m such that $z^2 + 1 = mp$, $0<m<p$. Hence $x^2+y^2= mp$ is solvable in integers x,y,and m.

Our next objective is to show that a prime of the form 4k + 1 is representable as a sum of two squares. But first we need a lemma.

Lemma 2.04:

If p is a prime of the form 4k + 1 and if $x^2 + y^2 = mp$ with $1<m<p$, then there exist integers x_1, y_1 and n such that $x_1{}^2 + y_1{}^2 = np$ with $1 \leq n < m$.

Proof:

There are two cases to consider according as m is even or odd.

When m is even, then both x and y are even or both are odd, and we may write the equation of the hypothesis in the form :

$$((x+y)/2)^2 + ((x-y)/2)^2 = (m/2)p$$

Thus $x_1 = (x+y)/2$, $y_1 = (x-y)/2$ and $n= m/2$ are integers satisfying the conclusions of the lemma.

When m is odd, we use modified division algorithm for least absolute value remainder to write:

$$x = am + r_1 \text{ and } y = bm + r_2$$

$$\text{where } |r_1| < m/2 \text{ and } |r_2| < m/2$$

If these expression are substituted in the given equation we find $(ma + r_1)^2 + (bm + r_2)^2 = mp$

$r_1{}^2 + r_2{}^2 + 2m(ar_1 + br_2) + (a^2+b^2)m^2 = mp.$

Hence $r_1{}^2 + r_2{}^2 = m(p-2(ar_1+br_2) - (a^2 + b^2)m)$

That is there exists a nonnegative integer n such that $r_1{}^2 + r_2{}^2 = mn$, and we may write

$$n + 2(ar_1 + br_2) + (a^2 + b^2)m = p.$$

By multiplying both sides by n, we have

$$n^2 + 2n(ar_1 + br_2) + (a^2 + b^2) mn = np,$$

this implies $n^2 + 2n(ar_1 + br_2)+(a^2+b^2)(r_1{}^2+r_2{}^2) = np.$

This implies $(n+(ar_1+ br_2))^2+ (ar_2- br_1)^2= np$.

If $n = 0$ we would have $r_1 = r_2 = 0$, so that m^2 would divide $x^2+y^2 = mp$ and m would divide p. But since p is a prime and $1<m<p$, this is a contradiction. Hence we have $1 \leq n$. But also we have $nm = r_1^2 + r_2^2 < m^2/2 < m^2$. Hence $n < m$.

Thus $x_1= n + ar_1 + br_2$, $y = ar_2- br_1$ and n are integers satisfying the conclusion of the lemma.

Lemma 2.05:

Every prime of the form $4k + 1$ can be represented as the sum of two squares.

Proof:

By lemma 2.03 we can find integers x,y such that $x^2 + y^2= mp$, where $1\leq m<p$. If $m>1$, we can apply Lemma 2.04 a finite number of times (say with $m>n = n_1 > n_2>..>n_k=1$) to " descend" to the situation : $x_k^2 + y_k^2 = p$.

As an illustration of Lemma 2.04 and Lemma 2.05 we give the following examples.

Example 1: (m is even)

Let $p = 13$. Consider the equation $x^2 + y^2 = mp$.

$p = 13$ is of the form $4k + 1$, therefore by lemma 2.03 $z^2 + 1 = 0 \pmod{p}$ has solution which is $z = 5$ or $z = 8$.

Let $z = 5$, then $5^2 + 1^2 = 2.13$ .Then we apply lemma 2.04

$x_1 = (5+1)/2 = 3$

$y_1 = (5-1)/2 = 2$

$n = m/2 = 2/2 = 1$

Hence we have $x_1^2 + y_1^2 = np = 3^2 + 2^2 = 1.13$.

Example 2: (m is odd)

From example 1, another solution for z is $z = 8$.

Therefore we have $8^2 + 1^2 = 5.13$.

We apply lemma 2.04 , $x = 8 = am + r_1 = (1)5 + 3$

$y = 1 = bm + r_2 = (0)5 + 1$

$n = p - 2(ar_1 + br_2) - (a^2 + b^2)m$

$= 13 - 2(1.3 + 0.1) - (1^2 + 0^2)5$

$= 13 - 2.3 - 5 = 2.$

$x_1 = n + (ar_1 + br_2) = 4 + (1.3 + 0.1) = 2 + 3 = 5$.

$y_1 = (ar_2 - br_1) = (1.1 - 0.3) = 1.$

Hence $x_1{}^2 + y_1{}^2 = 5^2 + 1^2 = 2.13.$

From here we apply lemma 2.04 as shown in example 1.

Remarks:

1) The method used in the proof of the theorem is sometimes called "proof by finite descent" or "Fermat's method of descent". This type of proof which also occurs at other places in number theory, is based on the well-ordering principle, which states that every nonempty set of positive integers contains a least element.

2) We will see later that the representation of a prime p of the form $4k + 1$ as the sum of two squares is unique, apart from the obvious possibility of interchanging x and y and changing their signs.

In Lemma 2.01 we have shown that no prime of the form $4k + 3$ is the sum of two squares. But since the product of two primes of the form $4k + 3$ is of the form $4k + 1$, further investigation is required to see if such products are representable as the sum of two squares.

Definition 2.1:

A representation of a positive integer n as the sum of two squares is called primitive(or proper) if and only if there exist relatively prime integers x and y such that $n = x^2 + y^2$, otherwise it is called imprimitive representation.

Lemma 2.06:

If $p = 4m + 3$ is a prime number and $p|n$, then n has no primitive representations.

Proof:

Assume that n has a primitive representation, then there exist integers x,y such that $x^2 + y^2 = n$ with $(x,y) = 1$. Now $p|n$ implies $p|x$ and $p|y$.

By Fermat's theorem, $x^{p-1} \equiv 1$ (modp);

hence $yx^{p-1} \equiv y$ (modp).

Let $h = yx^{p-2}$, then we have $xh \equiv y$ (modp) and so

$$x^2(1+h^2) \equiv x^2 + y^2 \equiv n \equiv 0 \text{ (modp)}.$$

But since $p \nmid x$ we obtain $h^2 + 1 \equiv o$ (modp)

i.e $h^2 \equiv -1$ (modp). Therefore -1 is a quadratic residue of p,which is a contradiction.

(Recall :the number -1 is a quadratic residue of primes of the forms $4k + 1$ and a quadratic non-residue of the primes of the forms $4k +3$.)

Lemma 2.07:

If $p = 4m + 3$, $p^c \mid n$, $p^{c+1} \nmid n$ where c is odd, then n has no representation (primitive or imprimitive) as the sum of two squares.

Proof:

The proof is by contradiction. Suppose there is a representation $n = x^2 + y^2$ with $(x,y) = d$. Set $x = du$ and $y = dv$. Then $n= d^2(u^2 + v^2) = d^2N$ and $(u,v) = 1$.

Let p^k be the highest power of p such that $p^k \mid d$.

Now $p^c \mid n$. This implies $p^c \mid d^2N$.

This implies $p^{c-2k} \mid N$ and since c is odd, c-2k is positive.

Hence we have $N = u^2 + v^2$, where $(u,v)=1$ and $p \mid N$ which contradict Lemma 2.06.

Let us restate the main theorem again:

Theorem 2.1:

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

Proof:

For $n = 1$, we have $1 = 1^2 + 0^2$. For the only even prime 2, we have $2 = 1^2 + 1^2$. For every prime of the form $4k + 1$ a representation as the sum of two squares exists by Lemma 2.05. An even power P^{2r} of a prime of the form $p = 4k + 3$ is a sum of two squares since $p^{2r} = (p^r)^2 + 0^2$. By Lemma 2.02 , every composite number n in which prime factors of the form $4k + 3$ appears only to even powers is representable as a sum of two squares. On the other hand if one prime factor of the form $p = 4k + 3$ appears to an odd power, and not to a higher power as a factor of n, then n is not representable as a sum of two squares, for this is the content of Lemma 2.07.

As the first example of theorem 2.1,

consider $n = 234 = 2.3^2.13$

$2 = 1^2 + 1^2$

$3^2 = 3^2 + 0^2$

$13 = 3^2 + 2^2$. Then by lemma 2.02 $n = 234$ is also a sum of two squares where $234 = 15^2 + 3^2$.

$90 = 2.3^2.5$ is also representable as a sum of two squares.

$90 = 9^2 + 3^2$.

$30 = 2.3.5$ is not representable as a sum of two squares since 3 has odd exponent and 3 is not representable as a sum of two squares.

Proposition:

If a positive integer n is not the sum of two square integers, then it is not the sum of two square of rational numbers either.

Proof:

If n is not the sum of two square integers, then by the previous theorem, there exist a prime p of the form $4k + 3$ that divides n to an odd power exactly. Now assume that n = $(s_1/m_1)^2+(s_2/m_2)^2$, where m_1, m_2 are positive integers and s_1,s_2 are integers. Then $(m_1m_2)^2n = (s_1m_2)^2 + (s_2m_1)^2$. But p must appear with an odd exponent in the factorization of the left hand side of the equality, and by the previous theorem, this cannot be true regarding the right hand side of the equality, thus we have a contradiction and so the proposition is proved.

2.The Total Number Of Representations As The Sum Of Two Squares

In this section we are going to find in how many ways a positive integer n can be represented as the sum of two squares. First we will find the total number of not essentially distinct representations of n. Then in section 4 we find what positive integers has exactly one essentially distinct representation as a sum of two squares. Recall that we consider two representations of n as being not essentially distinct if they differ only by the order of the summands, or by the sign of a term, otherwise we regard them being essentially distinct (or different).

Before attacking this problem we are going to show that it is enough only to consider primitive (proper) representations. Let $Q(x_1,x_2,..,x_n)$ be a quadratic form. Let $R_Q(n)$ be the number of primitive solutions of the Diophantine equation, $Q(x_1,x_2,..,x_n) = n$, and let $r_Q(n)$ denote the total number of solutions (primitive and imprimitive solutions). Then we have:

Theorem 2.2:

$$r_Q(n) = \sum_{d^2|n} R_Q(n/d^2)$$

Proof:

Let $s = \langle s_1, s_2, \ldots, s_k \rangle$ be any imprimitive solution of $Q(x_1,..,x_n) = n$. Set $d = (s_1, s_2, .., s_k)$ and write $s_i = ds'_i, i=1,2,..,k$, then $(s_1', s_2', \ldots, s_k') = 1$. Then d^2 n and hence $n = d^2m$ for some integer m and $Q(s_1', .., s_k) = m$, that is $s' = \langle s_1', .., s_k' \rangle$ is a primitive solution of $Q(x_1,..,x_k) = m$.

Thus all solutions of $Q(x_1,..,x_k) = n$ can be obtained from primitive solutions of $Q(x_1,...,x_k) = n/d^2$, when d ranges over all divisor of n such that $d^2 \mid n$. Hence we have,

$$r_Q(n) = \sum_{d^2|n} R_Q(n/d^2).$$

Our next objective is to find the number of primitive solutions of $x^2 + y^2 = n$, where n is any positive integer. First we need a Lemma.

Lemma 2.08:

Let n be any positive integer. The number of solutions N(n) of the quadratic congruence $x^2 \equiv -1 (\mathrm{mod} n)$ is given by :

$$N(n) = \begin{cases} 0 \text{ if } 4|n \text{ or if } n \text{ has a prime factor of the form } 4k+3. \\ 2^s \text{ if } 4\nmid n, \text{ and } n \text{ has no prime factor of the} \\ \quad \text{form } 4k + 3 \text{ and } s \text{ is the number of distinct} \\ \quad \text{odd prime factors of } n. \end{cases}$$

Proof:

For n = 1, the statement is true (the number of solutions is 1). For n>1 let $n = 2^{a_0}P_1^{a_1}\ldots P_r^{a_r}$ be the canonical decomposition of n. Then the number of solutions of $x^2 \equiv -1(\text{mod} n)$ equals the product of the number of solutions of the family of congruence equations:

$x^2 \equiv -1(\text{mod} 2^{a_0})$, $x^2 \equiv -1(\text{mod } P_1^{a_1}),\ldots,x^2 \equiv -1(\text{mod } P_r^{a_r})$.

Also we have $x^2 \equiv -1$ (modp) is solvable if and only if p=2 or p is an odd prime of the form p = 4k +1. For the case p = 2 the equation $x^2 \equiv -1$ (mod 2) has one solution and hence the statement is true. For odd primes p of the form p= 4k + 1 the equation $x^2 \equiv -1(\text{mod } p)$ has two incongruent solutions. Thus the statement is true.

Lemma 2.09:

Let n > 1 be such that congruence $q^2 \equiv -1$ (mod n) has a solution. Then there exist unique positive integers x,y with (x,y) = 1 and satisfying $x^2 + y^2 = n$ and $y \equiv hx$ (mod n).

To prove this Lemma we need to use the following theorem whose proof can be found in [8].

Theorem 2.3:

Given real numbers $\eta \geq 1$ and ξ then there exist a fraction a/b such that (a,b) = 1, $0 < b \leq \eta$ and

$|\xi - (a/b)| < 1/(b\eta)$.

Proof of Lemma 2.09:

In theorem 2.3 Let $\eta = \sqrt{n}$ and $\xi = (-q/n)$. Then there exist two integers a and b for which $(a,b) =1$, $0 <b \leq \sqrt{n}$ and $|-q/n - a/b| < (1/b\sqrt{n})$.

Let us set $qb + na = c$ then $|c|=|qb + na|< \sqrt{n}$ and $c \equiv qb \pmod{n}$.

Consider $b^2 + c^2 \equiv b^2 + q^2b^2 \equiv (1 + q^2)b^2 \equiv 0 \pmod{n}$

Thus $b^2+ c^2 \geq n$, but since $0<b \leq\sqrt{n}$ and $|c|< \sqrt{n}$ then $b^2+ c^2 \leq n$. Hence it follows that $b^2 + c^2 = n$.

Furthermore we have $(b,c) =1$.

Since $n = b^2 + c^2 = b^2 + (qb +na)^2$

$= b^2 (1+q^2) + 2 qnba +n^2a^2$

implies $1= ((1+q^2)/n)b^2 + 2qba + na^2$

$= ((1 + q^2)/n)b^2 + qba + qba + na^2$

$= ub + a(qb + na)$

$= ub + ac$, where $u = ((1+q^2)/n)b + qa$

hence $(b,c) = 1$.

Now $c\neq 0$, for otherwise we would have $b^2 = n> 1$ and $(b,c) > 1$.

In case $c> 0$ the choice $x =b$, $y = c$ will satisfy the conclusion of the theorem.

In case $c< 0$ the choice $x = -c$, $y = b$ does it, since $n =(-c)^2 + b^2$, $-c>0$, $b>0$, $(-c,b) = 1$ and $b\equiv -q^2b \equiv -qc \pmod{n}$.

To prove uniqueness , we assume there are two pairs of positive integers (x',y') and (x",y") that satisfying the given condition of the theorem. Then we have

$n = (x')^2 + (y')^2$ and $n = (x'')^2 + (y'')^2$

$$n^2 = (x'^2 + Y'^2)(X''^2 + Y''^2)$$

$$= (x'x'' + y'y'')^2 + (x'y'' - y'x'')^2$$

$$x'x'' + y'y'' \equiv x'x'' + qx'\,qx'' \equiv (1 + q^2)x'x'' \equiv 0(\mathrm{mod}n)$$

But since $x'x'' + y'y'' > 0$ we have $x'x'' + y'y'' = n$

and $x'y'' - y'x'' = 0$

$$x'n = x'(x'x'' + y'y'') - y'(x'y'' - y'x'') = x''(x'^2 + y'^2) = x''n$$

Hence $x' = x''$ and $y' = y''$.

Theorem 2.5:

The number of primitive solutions of $x^2 + y^2 = n$, is $R_2(n) = 4N(n)$, where $N(n)$ is the number of solutions of the congruence equation $z^2 \equiv -1$ (modn).

Proof:

For $n = 1$ the statement is true, since the number of primitive solution of $x^2 + y^2 = 1$ is 4 namely $1 = (\pm 1)^2 + 0^2$ and $1 = 0^2 + (\pm 1)^2$. On the other hand $N(1) = 1$. Thus $R_2(1) = 4N(1)$.

For $n>1$, if x' and y' is a primitive solution of $x^2 + y^2 = n$, then we necessarily have $x' \neq 0$ and $y' \neq 0$ since $(x',y')=1$. Therefore the total number of primitive solutions of $x^2 + y^2 = n$ must be four times the number of positive primitive solutions .

From Lemma 2.09 above for each q satisfying $q^2 \equiv -1$ (modn), there exists unique $x>0$, $y>0$ such that $(x,y) = 1$, $x^2 + y^2 = n$ and $y \equiv qx(\mathrm{mod}n)$. Conversely, every solution of $x^2 + y^2 = n$ for which $x>0$,$y>0$ and $(x,y) = 1$ yields exactly one solution q (modn) satisfying $q^2 \equiv -1$ (modn) and for which $y \equiv qx$(modn).

To prove the converse is true, note that since $(x,y) = 1$ we have $(x,n) = 1$. Hence the linear congruence $y = qx$ (modn) has a unique solution for q,

$0 \equiv n \equiv x^2 + y^2 \equiv x^2 + q^2x^2 \equiv (1+q^2)x^2$ (modn)

$0 \equiv 1 + q^2$ (modn)

Corollary 2.6:

The total number of solutions of $x^2 + y^2 = n$ is given by the formula $r_2(n) = 4 \sum_{d^2 | n} N(n/d^2)$

Corollary 2.7:

Every prime of the form $p = 4k + 1$ can be written as a sum of two squares in eight ways.

Proof:

By Lemma (2.08), $N(p) = 2$ and since p is a prime all solutions of $x^2 + y^2 = p$ are primitive. Thus $r_2(p) = 8$.

Corollary 2.7 implies any prime of the form $p = 4k+ 1$ can be written as sum of two squares in only one essentially distinct way, since the eight representations can all be obtained from any one of them by changing the sign of x and y and by interchanging the order of the summands. Thus corollary 2.7 may be restated more precisely as:

For any prime p of the form $p = 4k + 1$, the Diophantine equation $x^2 + y^2 = p$ has exactly one essentially distinct solution.

Our main aim in this section is to prove the following theorem:

Theorem 2.8:

Suppose that $n \geq 1$ has the factorization $n = 2^{\alpha} n_1 n_2$, where $n_1 = \prod\limits_{p=4k+1} P^r$, $\quad n_2 = \prod\limits_{q=4k+3} q^s$

$$\text{Then } r_2(n) = \begin{cases} 0 \text{ if any of the exponents } s \text{ is odd} \\ 4\tau(n_1) \text{ if all } s \text{ are even} \end{cases}$$

where $\tau(n_1)$ denotes the number of divisors of n_1.

We shall require some axuiliary Lemmas for the proof of this theorem. We first introduce the function,

$$X(n) = \begin{cases} 0 \text{ if } n \equiv 0(\text{mod}2) \\ 1 \text{ if } n \equiv 1(\text{mod}4) \\ -1 \text{ if } n \equiv 3(\text{mod}4) \end{cases}$$

This function is called the nonprincipal character function modulo 4 . Clearly one can prove the following lemma:

Lemma 2.10:

(1) $X(n) = \begin{cases} 0 \text{ if } 2 \mid n \\ (-1)^{(n-1)/2} \text{ if } 2 \nmid n \end{cases}$

(2) If $n_1 \equiv n_2 \pmod 4$ then $X(n_1) = X(n_2)$

(3) $X(n_1 n_2) = X(n_1) X(n_2)$ for any positive integers n_1, n_2, that is X is completely multiplicative.

Proof:

To prove (1) , clearly if $2 \mid n$ then $n \equiv 0(\text{mod}2)$ and by definition $X(n) = 0$. On the other hand if $2 \nmid n$ then n is odd. Hence n is either of the form $4k + 1$ or the form $4k + 3$. If $n = 4k + 1$, then $(-1)^{(n-1)/2} = (-1)^{4k/2} = 1$. And if $n = 4k + 3$ then $(-1)^{(n-1)/2} = (-1)^{4k+2/2} = -1$.

To prove (2),

1) Assume $n_1 \equiv 0 \pmod{2}$ which implies $n_1 = 2k$.

   $n_1 \equiv n_2 \pmod{4}$ implies $n_1 - n_2 = 4m$.

   Therefore $n_2 = n_1 - 4m = 2k - 4m = 2(k - 2m)$

   which imply $n_2 \equiv 0 \pmod{2}$.

   Hence $\chi(n_1) = \chi(n_2) = 0$.

2) Assume $n_1 \equiv 1 \pmod{4}$ which implies $n_2 \equiv 1 \pmod{4}$.

   This implies $\chi(n_1) = \chi(n_2) = 1$.

3) Assume $n_1 \equiv 3 \pmod{4}$ which implies $n_2 \equiv 3 \pmod{4}$.

   This implies $\chi(n_1) = \chi(n_2) = -1$.

To prove (3), we consider 3 cases.

Case 1: $2\ n_1$ and $2\ n_2$

$\chi(n_1 n_2) = 0$, $\chi(n_1) = 0$, $\chi(n_2) = 0$.

These imply $\chi(n_1 n_2) = \chi(n_1) \cdot \chi(n_2)$.

Case2: $2 \mid n_1$ and $2 \mid n_2$

$\chi(n_1 n_2) = 0$, $\chi(n_1) = 0$, $\chi(n_2) = \pm 1$

These imply $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.

Case3: $2 \nmid n_1$ and $2 \nmid n_2$

Then n_1, n_2 are odd and either of the form $4k + 1$ or $4k + 3$.

Assume $n_1 \equiv 1 \pmod{4}$ and $n_2 \equiv 1 \pmod{4}$.

Then $n_1 n_2 = (4k_1 + 1)(4k_2 + 1) = 4m + 1 \equiv 1 \pmod{4}$

Therefore $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.

Assume $n_1 \equiv 1 (\mathrm{mod} 4)$ and $n_2 \equiv 3 (\mathrm{mod} 4)$.

Then $n_1 n_2 = (4k+1)(4k+3) = 4m + 3 \equiv 3 (\mathrm{mod} 4)$.

Therefore $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.

Assume $n_1 \equiv 3 (\mathrm{mod} 4)$ and $n_2 \equiv 3 (\mathrm{m0d} 4)$.

Then $n_1 n_2 = (4k_1+3)(4k_2+3) = 4m + 1 \equiv 1 (\mathrm{mod} 4)$.

Therefore $\chi(n_1 n_2) = \chi(n_1)\chi(n_2)$.

Now we define $\delta(n) = \sum_{d|n} \chi(d)$, where the sum runs over all positive divisors d of n. $\delta(n)$ is called the Mobius transform of $\chi(n)$, so that it follows from general theorem that $\delta(n)$ is also multiplicative.

Let $n = \prod_{i=1}^{r} P_i^{e_i}$ be the prime factorization of n, then

$$\begin{aligned}\delta(n) &= \sum_{d\ n} \chi(d) \\ &= \prod_{i=1}^{r} (\chi(1) + \chi(P_i) + \chi(P_i^2) + \ldots + \chi(P_i^{e_i}) \\ &= \prod_{i=1}^{r} (1 + \chi(P_i) + \chi(P_i^2) + \ldots + \chi(P_i^{e_i})\end{aligned}$$

Using the function $\chi(n)$ we can restate Lemma (2.08) as follows:

Lemma 2.11:

Let N(n) denote the number of solutions to the congruence equation $x^2 \equiv -1 (\mathrm{mod} n)$. Then

$$N(n) = \begin{cases} 0 \text{ if } 4 \nmid n \\ \prod_{p|n} (1 + \chi(p)) \text{ if } 4 | n \end{cases}$$

where the product runs through all the distinct prime divisors of n.

Lemma 2.12:

$$r_2(n) = 4\,\delta(n)$$

Proof:

From corollary (2.6) and theorem (2.8) we have the total number of solutions of $x^2 + y^2 = n$ is

$$r_2(n) = 4 \sum_{d^2 | n} N\,(n/d^2)$$

where the sum runs over all divisors d of n such that $d^2 | n$

Let $\lambda(d) = 1$ or 0 according to whether d is a square or not .Then $r_2(n) = 4 \sum_{d|n} N(n/d)\ \lambda(d)$

Clearly $\lambda(n)$ is multiplicative and since N(n) is multiplicative it follows that $r_2(n)/4$ is multiplicative. Since $\delta(n)$ is also multiplicative, we need only to show that $r_2(P^e) = 4\,\delta(P^e)$ for any prime p and any positive integer e.

Now if $2|e$, then

$$\frac{r_2(P^e)}{4} = \sum_{d|p^e} N(P^e/d)\ \lambda(d)$$

$$= N(P^e) + N(P^{e-2}) + \ldots + N(P^2) + N(1)$$

$$= \begin{cases} 0 + 0 + \ldots + 0 + 1 = 1 \text{ if } p = 2 \\ 0 + 0 + \ldots + 0 + 1 = 1 \text{ if } p \equiv 3 (\text{mod } 4) \\ 2 + 2 + \ldots + 2 + 1 = e/2.2+1 = e+1 \text{ if } p \equiv 1 (\text{mod } 4) \end{cases}$$

and if $2 \nmid e$ then $\frac{r_2(P^e)}{4} = N(P^e) + N(P^{e-2}) + \ldots + N(P^2) + N(P)$

$$= \begin{cases} 1 \text{ if } p = 2 \\ 0 \text{ if } p \equiv 3 (\text{mod } 4) \\ e+1 \text{ if } p \equiv 1\ (\text{mod } 4) \end{cases}$$

On the other hand we have

$$\delta(P^e) = 1 + \chi(p) + \ldots + \chi(P^e)$$

$$= \begin{cases} 1 + 0 + 0 + \ldots + 0 = 1 \text{ if } p = 2 \\ 1 - 1 + 1 - \ldots + 1 = 1 \text{ if } p \equiv 3 (\mathrm{mod}\, 4)\ , 2 \mid e \\ 1 - 1 + 1 - \ldots - 1 = 0 \text{ if } p \equiv 3 (\mathrm{mod}\, 4)\ , 2 \nmid e \\ 1 + 1 + 1 + \ldots + 1 = e + 1 \text{ if } p \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

Hence $r_2(P^e) = 4\,\delta(P^e)$. Hence we have $r_2(n) = 4\delta(n)$.

Proof of Theorem 2.8:

For $n = 1$, the theorem is true . Now since $\frac{r_2(n)}{4}$ and $\tau(n_1)$ are multiplicative , we only need to prove the statement for $n = P^e$ where p is a prime and $e \geq 1$.

We have

$$\frac{r_2(P^e)}{4} = \begin{cases} 1 = \tau(1) \text{ if } p = 2 \\ 1 = \tau(1) \text{ if } p \equiv 3 (\mathrm{mod}\, 4),\ 2 \mid e \\ 0 = 0 \text{ if } p \equiv 3 (\mathrm{mod}\, 4)\ ,\ 2 \nmid e \\ e+1 = \tau(P^e) \text{ if } p \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

Thus

$$\frac{r_2(P^e)}{4} = \begin{cases} 0 \text{ if } p \equiv 3\ (\mathrm{mod}\, 4)\ ,\ 2 \mid e \\ \tau(P^e) \text{ if } p \equiv 1\ (\mathrm{mod}\, 4) \\ 1 \text{ if } p = 2 \text{ or } p \equiv 3\ (\mathrm{mod}\, 4),\ 2 \mid e. \end{cases}$$

And this complete the proof.

Corollary 2.9:

Let $n = 2^{\alpha} n_1 n_2$, where n_1 and n_2 are as in the theorem, then $r_2(n) = \begin{cases} 4\,\tau(n_1) \text{ if } n_2 \text{ is a square} \\ 0 \text{ if } n_2 \text{ is not a square.} \end{cases}$

The following are some examples to illustrate the above lemma.

$30 = 2.3.5$; $r_2(30) = 0$ since 3 is not a square.

$90 = 2.3^2.5$; $r_2(90) = 4\,\tau(n_1) = 4\,\tau(5) = 4.2 = 8$.

These representations are:

$$90 = 3^2 + 9^2 = (-3)^2 + 9^2 = 3^2 + (-9)^2 = (-3)^2 + (-9)^2$$
$$= 9^2 + 3^2 = 9^2 + (-3)^2 = (-9)^2 + 3^2 = (-9)^2 + (-3)^2$$

Theorem 2.8 is sometimes stated in another form. First we define the following arithmetic functions.

$\tau_1(n)$ = number of divisors of n which are of the form 4k+1.

$\tau_3(n)$ = number of divisors of n which are of the form 4k+3.

Theorem 2.10:

$$r_2(n) = 4(\ \tau_1(n) - \tau_3(n))$$

The proof of this theorem requires some knowledge of the functions τ_1 and τ_3. Neither one of these function is multiplicative. For example $\tau_1(3) = \tau_1(7)=1$ but $\tau_1(21)= 2$

Also $\tau_3(3)= \tau_3(7) = 1$ but $\tau_3(21) = 2$.

On the other hand , these functions do have some interesting properties.

Lemma 2.13:

If $(a,b) = 1$ then

1) $\tau_1(ab) = \tau_1(a)\ \tau_1(b) + \tau_3(a)\,\tau_3(b)$

2) $\tau_3(ab) = \tau_1(a)\ \tau_3(b) + \tau_1(b)\,\tau_3(a)$

Proof:

1) Every divisor d of ab can be written uniquely as $d = AB$ where $A|a$ and $B|b$.

$d \equiv 1 \pmod 4$ if and only if $A \equiv B \equiv 1 \pmod 4$

or $A \equiv B \equiv 3 \pmod 4$

$d \equiv 3 \pmod{4}$ if and only if $A \equiv 1 \pmod{4}$, $B \equiv 3 \pmod{4}$

or $A \equiv 3 \pmod{4}$, $B \equiv 1 \pmod{4}$

Now $\tau_1(ab)$ = number of divisor d of ab where $d = 1 \pmod{4}$

$\tau_1(a)$ = number of divisors A of a where $A \equiv 1 \pmod{4}$

$\tau_1(b)$ = number of divisors B of b where $B \equiv 1 \pmod{4}$

$\tau_3(a)$ = number of divisors A of a where $A \equiv 3 \pmod{4}$

$\tau_3(b)$ = number of divisors B of b where $B \equiv 3 \pmod{4}$

By the multiplication and addition principles of counting we have,

$$\tau_1(ab) = \tau_1(a)\,\tau_1(b) + \tau_3(a)\,\tau_3(b).$$

In similar manner we can prove (2).

Lemma 2.14:

Let $n = 2^{\alpha} n_1 n_2$, where n_1 contains only primes of the form $p = 4k+1$ and n_2 contains only primes of the form $q = 4k+3$.

Then, 1) $\tau_1(n) = \tau_1(n_1 n_2)$

2) $\tau_3(n) = \tau_3(n_1 n_2)$

Proof:

1) From the previous Lemma we have

$$\begin{aligned}\tau_1(n) &= {}_1(2^{\alpha} n_1 n_2)\\ &= \tau_1(2^{\alpha})\,\tau_1(n_1 n_2) + \tau_3(2^{\alpha})\,\tau_3(n_1 n_2)\\ &= 1.\tau_1(n_1 n_2) + 0.\tau_3(n_1 n_2)\\ &= \tau_1(n_1 n_2).\end{aligned}$$

2) $$\begin{aligned}\tau_3(n) &= \tau_3[(2^{\alpha})n_1 n_3]\\ &= \tau_1(2^{\alpha})\,\tau_3(n_1 n_3) + \tau_1(n_1 n_3)\,\tau_3(2^{\alpha})\\ &= 1.\,\tau_3(n_1 n_3) + \tau_1(n_1).0\\ &= \tau_3(n_1 n_3).\end{aligned}$$

Lemma 2.15:

Let $F(n) = \tau_1(n) - \tau_3(n)$,then F is multiplicative.

Proof:

Let a , b be two positive integers such that $(a,b) = 1$,

$$\begin{aligned} F(ab) &= \tau_1(ab) - \tau_3(ab) \\ &= [\tau_1(a)\tau_1(b) + \tau_3(a)\tau_3(b)] \\ &\quad -[\tau_1(a)\tau_3(b) + \tau_1(b)\tau_3(a)] \\ &= [\tau_1(a)\tau_1(b) - \tau_1(b)\tau_3(a)] \\ &\quad + [\tau_3(a)\tau_3(b) - \tau_1(a)\tau_3(b)] \\ &= \tau_1(b)(\tau_1(a) - \tau_3(a)) + \tau_3(b)(\tau_1(a) - \tau_3(a)) \\ &= (\tau_1(a) - \tau_3(a)) - (\tau_1(b) - \tau_3(b)) \\ &= F(a)F(b). \end{aligned}$$

Lemma 2.16:

Let $n = 2^{\alpha} n_1 n_2$, and $F(n) = \tau_1(n) - \tau_3(n)$,

then:

1) $F(2^{\alpha}) = 1$

2) $F(n_1) = \tau(n_1)$

3) $F(n_2) = \begin{cases} 1 \text{ if } n_2 \text{ is a square} \\ 0 \text{ if } n_2 \text{ is not a square} \end{cases}$

Proof:

1) $F(2^{\alpha}) = \tau_1(2^{\alpha}) - \tau_3(2^{\alpha}) = 1 - 0 = 1.$

2) $F(n_1) = \tau_1(n_1) - \tau_3(n_1) = \tau(n_1) - 0 = \tau(n_1).$

3)When n_2 is a square, we let $n_2 = m_2^2$ where $m_2 = 4k + 3$ then $n_2 = 4m + 1$.

Therefore $F(n_2) = \tau_1(n_2) - \tau_3(n_2)$

$$= 2 - 1 = 1,$$

since the divisors of n_2 of the form $4k + 1$ are 1 and $n_2 = m_2^2$, hence $\tau_1(n_2) = 2$. The divisor of n_2 of the form $4k+ 3$ is m_2, hence $\tau_3(n_2) = 1$.

When n_2 is not a square, we let $n_2 = m_2$ where $m_2 = 4k +3$.

Therefore $F(n_2) = \tau_1(n_2) - \tau_3(n_2)$

$$= 1 - 1 = 0,$$

since the divisor of n_2 of the form $4k + 1$ is 1 , and the divisor of n_2 of the form $4k + 3$ is m_2.

roof of the theorem 2.10:

Let $n = 2^{\alpha} n_1 n_2$

$$F(n) = F(2^{\alpha} n_1 n_2) = F(2^{\alpha} F(n_1)F(n_2)$$

$$= \tau(n_1)\ F(n_2)$$

$$= \begin{cases} \tau(n_1) \text{ if } n_2 \text{ is square} \\ 0 \text{ if } n_2 \text{ is not a square} \end{cases}$$

But $r_2(n) = \begin{cases} 4\tau(n_1) \text{ if } n_2 \text{ is a square} \\ 0 \text{ if } n_2 \text{ is not a square} \end{cases}$

Thus we have $r_2(n) = 4(\tau_1(n) - \tau_3(n))$

As an example consider $n = 90 = 2.3^2.5$

$\tau_1(90) = 4$, $\tau_3(90) = 2$.

$r_2(90) = 4(\tau_1(90) - \tau_3(90))$

$= 4(4 - 2) = 8$.

Next consider $n = 18 = 2.3^2$

$r_2(18) = 4(\tau_1(18) - \tau_3(18)) = 4(2- 1) = 4$.

$18 = 3^2 + 3^2 = 3^2 + (-3)^2 = (-3)^2 + 3^2 = (-3)^2 + (-3)^2$.

Now consider $n = 30 = 2.3.5$

$r_2(30) = 4(\tau_1(30) - \tau_3(30)) = 4(2-2) = 4.0 = 0.$

Clearly this theorem implies Theorem 2.1 ,

3. Representation Of Integers As Sum Of Two Nonvanishing Squares:

In this section we consider the problem of representing an integer as a sum of nonvanishing squares.

Theorem 2.11:

A positive integer n is the sum of the squares of two nonvanishing integers if and only if all prime factors of the form $4k + 3$ of the number n has even exponents in the standard factorization of n and either the prime 2 has an odd exponent or n has at least one prime divisor of the form $4k + 1$.

Equivalently: A positive integer n is the sum of the squares of two nonvanishing integers if and only if

$n = 2^a n_1 n_2^2$ provided that $n_1 \nmid 1$ or a is odd,

where $n_1 = \prod\limits_{p_i \equiv 1 (\mathrm{mod}\, 4)} p_i^{\alpha_i}$

$$n_2 = \prod_{q_j \equiv 3 (\mathrm{mod}\, 4)} q_j^{\beta_j}$$

Proof:

Suppose that there exist a positive integer which is the sum of the squares of two nonvanishing integers, and has the following properties: it does not have a prime factor of the form $4k + 1$ (i.e $n_1 = 1$) and in its

factorization into primes 2 has an even exponent. Let h be the least such positive integer with these properties. Since it is the sum of the squares of two nonvanishing integers, by Theorem 2.1 all prime factors of h of the form 4k + 3 have even exponents. Consequently h = $2^{2k}m^2$, where m is an odd integer and k $\geq$ 0. Thus we may write $2^{2k}m^2 = a^2 + b^2$, where a,b are positive integers. If k> 0 , then the left hand side of the last equation is divisible by 4; consequently the numbers a, b are both even ; let a = $2a_1$, b = $2b_1$.
Hence $2^{2k-2}m^2 = a_1^2 + b_1^2 < h$. Contrary to the choice of h. Hence k = 0 and so h = $m^2 = a^2 + b^2 > 1$. The numbers a,b must be relatively prime because if (a,b) = d> 1 we would have a = da_2, b = db_2 where a_2, b_2 are integers , whence m = dm_1 and $m_1^2 = a_2^2 + b_2^2 < m^2 = h$ also contrary to the choice of h. So (a,b) = 1. But since m is odd and greater than 1 (since m has no prime factors of the form 4k + 1), it has a prime factor of the form 4k + 3. Hence $p \mid a^2 + b^2$, or $a^2 \equiv -b^2$ (modp). If we raise each side of the last congruence to the (2k+1)th power, then
$a^{2(2k+1)} \equiv (-1)^{2k+1}b^{2(2k+1)}$ (mod p).
But 2(2k+1) = p-1 hence $a^{p-1} \equiv (-1)^{2k+1}b^{p-1}$(mod p), by Fermat theorem we have $a^{p-1} \equiv 1$ (mod p) and $b^{p-1} \equiv 1$(mod p) , hence we have $1 \equiv (-1)^{2k+1}$(modp) which is impossible. Thus we have proved that a positive integer that is the sum of the squares of two nonvanishing integers has the following properties; either in its factorization

into prime factors the prime 2 has an odd exponent,or it has a prime factor of the form $4k + 1$. Moreover by Theorem 2.1 , it follows that all prime factors of the form $4k + 3$ have even exponents. This shows that the conditions of the theorem are necessary.

Now suppose that a positive integer satisfies the conditions of the theorem. Thus we have either $n = 2m^2$ or $n = 2^{\alpha} m^2 h$, where $\alpha = 0$ or 1 and h is the product of prime factors of the form $4k + 1$.

If $n = 2m^2$, then $n = m^2 + m^2$, and so it is the sum of the squares of two nonvanishing integers.Suppose that $n=2 m^2 h$, where h is the product of prime factors of the form $4k+1$. But each of the factors is the sum of two positive squares, and hence h is again the sum of two positive squares. Recall if $h_1 = a^2 + b^2$, $h_2 = c^2 + d^2$ where h_1 and h_2 are odd, then one of the numbers a or b, say a must be odd, the other being even, the same is true for the numbers c and d; so let c be odd, d is even.

Then $h_1 h_2 = (a^2 + b^2) . (c^2 + d^2)$

$$= (ad + bc)^2 + (ac - bd)^2$$

where $ac - bd$ is odd , and so $ac -bd \neq 0$. Thus the number $h_1 h_2$ is the sum of the squares of two nonvanishing integers. We conclude by induction that h is the sum of the squares of two nonvanishing integers, i.e $h = a^2 + b^2$, Where $m^2 h =(ma)^2 + (mb)^2$ and $2m^2 h =(ma + mb)^2 + (ma - mb)^2$ and $ma - mb \neq 0$ (because a must be different from b since

the number $h = a^2 + b^2$ is odd) .
Thus we see in any case the number n is the sum of the squares of two nonvanishing integers. Therefore the condition is sufficient and the proof is complete.

Here we provide some examples to illustrate theorem 2.11

$10 = 2.5 = 1^2 + 3^2$ is a sum of the squares of two nonvanishing integers since 10 has prime factor of the form 4k + 1 and 2 has odd exponent.

$72 = 2^3.3^2 = 6^2 + 6^2$ is also a sum of the squares of two nonvanishing squares, note here 2 appears with an odd exponent.

$9 = 2^0.3^2 = 3^2 + 0^2$ is not a sum of the squares of two nonvanishing squares since 2 has even exponent and 9 has no prime factor of the form 4k + 1.

Corollary 2.13:

A square integer n^2 is the sum of the squares of two nonvanishing integers if and only if the number n has at least one prime factor of the form p = 4k + 1.

This is equivalent to saying:

A positive integer n is a hypotenuse of a pythagorean triangle if and only if n has at least one prime factor of the form p = 4k + 1.

Another interesting problem is the following:
When a positive integer n can be written as the sum of the

squares of two different nonvanishing integers? The anwser is given by the following theorem.

Theorem 2.14:

A positive integer n is the sum of the squares of two different nonvanishing integers if and only if the following conditions are satisfied:

1) The prime factors of n of the form $p = 4k + 3$ have even exponent.
2) The number n has at least one prime factor of the form $4k + 1$.

Proof:

Assume that n is the sum of the squares of two different nonvanishing integers. We need to show the two conditions of the theorem are satisfied.

The necessity of the condition (1) follows from the previous theorem.

Now suppose that a positive integer n does not satisfy condition(2), i.e n has no prime factor of the form $4k + 1$. Consequently , if $n = a^2 + b^2$, with a and b two different nonvanishing integers. Let $(a,b) = d$, then $a = a_1 d$,$b = b_1 d$ and hence $n = d^2(a_1^2 + b_1^2)$ and $a_1 \nmid b_1$, $(a_1,b_1) = 1$, $a_1^2 + b_1^2$ has no prime factor of the form $4k + 1$. Now since $(a_1,b_1) = 1$, then by using the same reasoning used in the proof of the previous theorem (necessary part), we conclude that $a_1^2 + b_1^2$ has no prime factors of the form $4k + 3$ either. Therefore $a_1^2 + b_1^2 = 2^k$

where $k > 1$, since a_1, b_1 are different. Consequently $4 | (a_1^2 + b_1^2)$. Hence the numbers a_1 and b_1 are even, but this contradicts the fact that $(a_1,b_1) = 1$.

Now suppose that a positive integer n satisfies conditions (1) and (2). Then by the previous theorem, we have $n = a^2 + b^2$ where a ,b are nonzero integers. If $a = b$, then $n = 2a^2$, and since n satisfies condition (2) it has a prime factor of the form $4k + 1$, thus a is the hypotenuse of a pythagorean triangle. This means $a^2 = c^2 + d^2$, where c and d are nonzero integers. Clearly $c \neq d$ since if $c = d$, then $a^2 = 2c^2$ which implies $a = \sqrt{2}c$. But since $\sqrt{2}$ is irrational ,this is impossible.

Hence $n = 2a^2 = (c+d)^2 + (c-d)^2$, where $c-d \neq 0$ and $c+d \neq c-d$. Consequently n is the sum of the squares of two different nonzero integers. Thus the conditions (1) and (2) are sufficient . This complete the proof.

To illustrate the theorem 2.14, we provide some examples below:

$10 = 2.5 = 1^2 + 3^2$ is the sum of the squares of two different nonvanishing integers since 10 has prime factor of the form $4k + 1 = 5$.

$18 = 2.3^2 = 3^2 + 3^2$ is not the sum of the squares of two different nonvanishing squares because 18 does not satisfy condition (2) of the theorem.

$90 = 2.3^2.5 = 3^2 + 9^2$, yes since it does satisfy both conditions of the theorem.

$9 = 2^0.3^2 = 3^2 + 0^2$ is not since it does not satisfy condition (2) of the theorem.

The next theorem gives under what conditions a positive integer can be written as the sum of the squares of two relatively prime integers.

Theorem 2.15:

A positive integer n is the sum of the squares of two relatively prime integers if and only if n is neither divisible by 4 nor by a number of the form 4k + 3.

Proof:

Suppose that a positive integer n is the sum of the squares of two relatively prime numbers say, $n = a^2 + b^2$ where $(a,b)= 1$ .If $4|n$, then $n = 4k$, then $4k = a^2 + b^2$, hence both a and b are even , contrary to $(a,b) =1$. If n has a divisor of the form 4k + 3, then as we know it has a prime divisors of this form, which as we have seen in the proof of Theorem 2.11 cannot divide the sum of the squares of two relatively primes numbers. Thus this proves that the condition of the theorem is necessary.

Suppose that a positive integer n satisfies the condition. If $n = 2$, then $2 = 1^2 + 1^2$, and so it is the sum of the square of two relatively prime numbers. If $n>2$, then the condition implies that n is the product of prime numbers of the form 4k + 1 or the product of number 2 and primes of the form 4k + 1. In the first case n is odd and each of the prime factors of n is the sum of the squares of two relatively primes numbers and by induction one can show that n is the sum of the squares of two relatively prime numbers.

In the second case , i.e if n is the product of 2 and the primes of the form 4k + 1, we have $n = 2(a^2 + b^2)$, where a and b are relatively prime. Since $a^2 + b^2$ is odd , one of the numbers a and b is odd and the other is even.

We have $n =(a + b)^2 + (a - b)^2$, where a + b and a - b are odd. Morever, they are relatively prime because if $d|a+b$ and $d|a-b$ then $d|2a$ and $d|2b$ since d is a divisor of an odd number a + b, is odd, we have $d|a$ and $d|b$, but since $(a,b) = 1$, then d =1. Therefore $(a+b, a-b) = 1$.

Thus the condition is sufficient and the proof is complete.

Examples:

10 = 2.5 is the sum of the squares of two relatively prime integers since $4 \nmid 10$ and $c \nmid 10$ where c is of the form 4k + 3. (i.e $10 = 1^2 + 3^2$, $(1,3) = 1$)

$18 = 2.3^2 = 3^2 + 3^2$, $(3,3) = 1$ since $3|18$ and 3 is of the form 4k+3.

29 = 29 is the sum of the squares of two relatively prime integers since $4 \nmid 29$ and 29 has no prime factor of the form 4k+3. (i.e $29 = 2^2 + 5^2$, $(2,5) = 1$)

$90 = 2.3^2.5 = 3^2 + 9^2$, $(3,9) = 1$ since $3|90$ and 3 is of the form 4k+3.

4.The Uniqueness Of Essentially Distinct Representation

In section (2) we found a formula for the total number of representations of a positive integer n as a sum of two squares that are not essentially distinct. In this section we are going to find what positive integers can be written exactly in one way as a sum of two squares apart from the order or the signs of the summands.

Theorem 2.16:

The only positive integers that can be represented as a sum of two squares in exactly one way are of the form : $n = 2^a P n_2^2$, where $a \geq 0$, P is a prime of the form $p = 4k+1$ and n_2 is an integer of the form $n_2 = \prod\limits_{P=4k+3} P^e$.

Proof:

Let n be a positive integer , where $n = 2^a m_1 m_2$, where $a \geq 0$ where $m_1 = \prod\limits_{P_i \equiv 1 (\text{mod } 4)} P_i^{\alpha_i}$, $m_2 = \prod\limits_{q_j \equiv 3 (\text{mod } 4)} q_j^{\beta_j}$

In order that n is a sum of two squares all the $_j$'s must be even. Thus we may write $m_2 = n_2^2$ and hence $n = 2^a m_1 n_2^2$. Let $a = 2b + c$ where $c = 0$ if a is even or $c = 1$ if a is odd. Then $n = 2^c m_1 (2^b n_2)^2$ .Now if $x^2 + y^2 = 2^c m_1$ has a solution, say $x = x_o$ and $y = y_o$ then $x_o^2 + y_o^2 = 2^c m_1$ and hence $(2^b n_2 x_o)^2 + (2^b n_2 y_o)^2 = 2^c m_1 (2^b n_2)^2 = n$. Thus $x_1 = 2^b n_2 x_o$, $y_1 = 2^b n_2 y_o$ is a solution of $x^2 + y^2 = n$. Conversely if $x = x_1$ and $y = y_1$ is a solution of $x^2 + y^2 = n$, then $x_o = x_1/(2^b n_2)$ and $y_o = y_1/(2^b n_2)$ is a solution of $x^2 + y^2 = 2^c m_1$.

Hence it is sufficient to consider only integer of the form $n = 2^c m_1$ where $c = 0$ or $c = 1$ and $m_1 = \prod_{p \equiv 1 (\mathrm{mod}\, 4)} P^{\alpha}$.

Let M be the set of all such integers of the form $n = 2^c m_1$ that can be written as a sum of two square in exactly one way.

Recall that any prime P of the form $p = 4k + 1$ has exactly one representation as a sum of two squares.

If m_1 has two distinct prime factors, P_1 and P_2 of the form $4k+1$, then the representation of $P_1 = a^2 + b^2$ and $P_2 = c^2 + d^2$ are unique.

Hence P_1P_2 has at least two distinct representations

$$x_1 = ac + bd, \quad y_1 = ad - bc$$

$$x_2 = ac - bd, \quad y_2 = ad + bc$$

If these solutions are not distinct then neither we have $ac + bd = ac - bd$ and this would implies $abcd = o$ nor $ac + bd = ad + bc$ which is equivalent to say $(ac + bd) - (ad + bc) = 0$ and this implies $(a-b)(c-d) = 0$.

Both of these will lead to a contradiction.

For let us consider the two possibilities:

Case1:

If $abcd = 0$, then at least one of these must be zero, say $a = 0$, then $P_1 = b^2$, a contradiction.

Case 2:

If $(a-b)(c-d) = 0$ this would imply $a-b = 0$ or $c-d = 0$. Let $a-b = 0$ then $P_1 = 2a^2$ also a contradiction.

Hence m_1 cannot have more than one prime factor of the form $4k + 1$. On the other hand $2 = 1^2 + 1^2$ and if $P = a^2 + b^2$, then $2P = (1^2 + 1^2)(a^2 + b^2) = (a + b)^2 + (a-b)^2$ is the only representation of $2P$ as a sum of two squares. Thus the set M consists of the integers of the form $m = 2^cP$ where $c = 0$ or $c = 1$ and P is a prime of the form $4k + 1$. Finally the set of positive integer that can be represented as a sum of two square in exactly one way are of the form $n = 2^a Pn_2{}^2$, where $a \geq 0$.

Corollary 2.17:

Any prime of the form $p = 4k + 1$ can be represented as a sum of two squares in exactly one way.

Examples:

$10 = 2.5$ can be represented as a sum of two squares in exactly one way i.e $10 = 1^2 + 3^2$.

$25 = 2^0.5^2$ can be represented as a sum of two squares in more than one way since the prime $p = 4k + 1 = 5$ is a square.

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

$90 = 2.3^2.5$ can be represented as a sum of two squares in exactly one way, $90 = 3^2 + 9^2$.

$100 = 2^2.5^2$ can represented as a sum of two squares in more than one way since $p = 4k + 1 = 5$ has even exponent.

$100 = 10^2 + 0^2 = 8^2 + 6^2$ ·

CHAPTER 3

SUM OF FOUR SQUARES

1. Representation Of Integers As Sum Of Four Squares.

In this chapter we consider the representation of a positive integer as a sum of four squares. As in the previous chapter the two Representation problems are:

1) What positive integers n can be represented as the sum of four square integers? That is to say for what positive integers n the Diophantine equation $x^2 + y^2 + z^2 + w^2 = n$ has a solution?
2) To find a formula for $r_4(n)$, the number of representation of an integer n as a sum of four squares.

We shall prove that every positive integer is the sum of four square integers.

It was Girard and Fermat who stated that every natural number is representable as the sum of at most four squares of natural numbers. But some historians have argued that the fact was known already to Diophantus of Alexandria because he made no mention of any condition to be satisfied by a number for it to be representable as a sum of four squares, whereas he was aware that only certain kinds of numbers could be represented by two or three squares. The first proof we know of is that given by Langrange in 1770.

The solution of problem (1) can be broken up into several steps. First we need the following lemmas:

Lemma 3.01:

If every prime is the sum of four squares then every composite integer is the sum of four squares.

Proof:

Using Euler's identity, we can prove this lemma.

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$
$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

This identity can be verified by multiplying out both side. On the left, after multiplying out we have sixteen expressions of the form $x_i^2y_j^2$ ($i = 1..4$, $j= 1..4$). These also appear , among other terms, on the right, for within the four parentheses on the right, each x_i is combined with each y_j with a coefficient of ± 1. The other twenty-four terms on the right , which are all of the form $\pm 2x_ix_jy_ky_h$, $i<j$, $k <h$ cancel each other pairwise , for on the right the coefficient of

$2x_1x_2$ is $y_1y_2 - y_1y_2 - y_3y_4 + y_3y_4 = 0$

$2x_1x_3$ is $y_1y_3 + y_2y_3 - y_1y_3 - y_2y_4 = 0$

$2x_1x_4$ is $y_1y_4 - y_2y_3 + y_2y_3 - y_1y_4 = 0$

$2x_2x_3$ is $y_2y_3 - y_1y_4 + y_1y_4 - y_2y_3 = 0$

$2x_2x_4$ is $y_2y_4 + y_1y_3 - y_2y_4 - y_1y_3 = 0$

$2x_3x_4$ is $y_3y_4 - y_3y_4 - y_1y_2 + y_1y_2 = 0$

This identity show that if X and Y can be expressed as sum of four squares, then so can their product XY. From this identity and math induction, Lemma 3.01 is an immediate consequence , for every composite integer n is the product of primes.

Example:

Let $x = 7 = 2^2 + 1^2 + 1^2 + 1^2$

Let $y = 10 = 1^2 + 1^2 + 2^2 + 2^2$

Then $70 = x.y = 7.10$

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

$$=(2.1 + 1.1 + 1.2 + 1.2)^2 + (2.1 -1.1 + 1.2 - 1.2)^2$$

$$+ (2.2 - 1.1 + 1.1 - 1.2)^2 + (2.2 - 1.1 + 1.2 - 1.1)^2$$

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

$$= 49 + 1 + 4 + 16 = 70 .$$

Therefore if x and y can be expressed as a sum of four squares , then so can their product xy.

Lemma 3.02:

For every $p > 2$ there exist an integer m for which $1 \leq m < p$ and $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable.

Proof:

The $(p+1)/2$ numbers in the set $A = \{0^2, 1^2, \ldots \ldots, ((p-1)/2)^2\}$ are incongruent to each other (modp) in pairs.

Assume $x_1^2 \equiv x_2^2$ (modp) where $0 \leq x_1 < x_2 \leq (p-1)/2$

This implies $x_1^2 - x_2^2 \equiv 0$ (modp)

Thus $p \mid (x_1 - x_2)(x_1 +x_2)$

Since p is a prime, $p \mid (x_1 - x_2)$ or $p \mid (x_1 + x_2)$

This implies $x_1 \equiv x_2$ (modp) or $x_1 \equiv -x_2$ (modp),

a contradiction,

for $x_1 \not\equiv x_2$(modp) since $\{0,1,2,...p-1\}$ forms a complete residue systems modulo p, and $x_1 \not\equiv - x_2$ (modp) because $0 \leq x_1 + x_2 \leq p-1$, hence $(x_1 + x_2) \nmid p$.

Therefore $x_1^2 \not\equiv x_2^2$ (mod p) for all $x_1^2, x_2^2 \in A$.

The same is true for the $(p+1)/2$ numbers in the set

$B = \{-1-0^2, -1-1^2, ..., -1-(p-1)/2^2\}$.

Now $|A \cup B| = (p+1)/2 + (p+1)/2 = p+1$

But there are exactly p incongruence classes mod p.

Therefore there is some number x^2 in A and some $-1-y^2$ in B such that $x^2 \equiv -1-y^2$ (modp) where $|x| < p/2$, $|y| < p/2$

This implies $x^2 + y^2 + 1 \equiv 0$ (mod p),

hence $x^2 + y^2 + 1^2 + 0^2 = mp$ for some integer $m \geq 1$.

$mp = x^2 + y^2 + 1^2 < p^2/4 + p^2/4 + 1$

$= p^2/2 + 1 < p^2/2 + p^2/2 = p^2$,

this implies $m < p$.

If we combine the two results , we have $1 \leq m < p$.

Example:

Let p = 7. Consider the equation $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$.

Let $A = \{0^2, 1^2, 2^2, 3^2\}$ are incongruent to each other mod 7.

Let $B = \{-1-0^2, -1-1^2, -1-2^2, -1-3^2\}$ are incongruent to each other mod 7. But $3^2 \equiv -1-2^2$ (mod7).

This implies $3^2 + 2^2 + 1 \equiv 0$(mod7) implies $3^2 + 2^2 + 1^2 + 0^2 = 2.7$.

Note that $1 \leq 2 < 7$.

Lemma 3.03

If p is an odd prime and if $x^2 + y^2 + z^2 + w^2 = mp$ with $1 < m < p$ then there exist integers x_1, y_1, z_1, w_1 and M such that $x_1{}^2 + y_1{}^2 + z_1{}^2 + w_1{}^2 = Mp$ with $1 \leq M < m$.

Proof:

The proof is divided into two cases according as m is even or odd.

Case 1: m is even

Claim: when m is even then x,y,z,w are all even; or all are odd; or two are even and two are odd.

Proof of claim

Consider the two cases:

1) three of those integers say x,y,z are even and w is odd;

$mp = x^2 + y^2 + z^2 + w^2$

$(\text{even})(\text{odd}) = (\text{even})^2+(\text{even})^2+(\text{even})^2+(\text{odd})^2$

$\text{even} = \text{odd}$

This case cannot happen.

2) three of those integer say x,y,z are all odd and w is even. $mp = x^2 + y^2 + z^2 + w^2$

$(\text{even})(\text{odd}) =(\text{odd})^2+(\text{odd})^2+(\text{odd})^2+(\text{even})^2$

$\text{even} = \text{odd}$

This case cannot happen either.

Now assume x and y are odd and z and w are even.

Then we have,

$((x+y)/2)^2 + ((x-y)/2)^2 + ((z+w)/2)^2 + ((z-w)/2)^2 = (m/2)p$

$x_1 = (x+y)/2, \quad y_1 = (x-y)/2$,

$z_1 = (z+w)/2$ and $w_1 = (z-w)/2$

and $M = m/2$ are integers satisfying Lemma 3.03.

Case 2: m is odd

When m is odd we use division algorithm for least absolute value remainder to write $x = am + r_1$, $y = bm + r_2$

$z = cm + r_3$, $w = dm + r_4$

where $|r_1| < m/2$, $|r_2| < m/2$, $|r_3| < m/2$, $|r_4| < m/2$

If these expressions are substituted in the given equation we find,

$(am + r_1)^2 + (bm + r_2)^2 + (cm + r_3)^2 + (dm + r_4)^2 = mp$

implies $r_1^2 + r_2^2 + r_3^2 + r_4^2 + 2m(ar_1 + br_2 + cr_3 + dr_4)$
$+ (a^2 + b^2 + c^2 + d^2)m^2 = mp$.

Hence $r_1^2 + r_2^2 + r_3^2 + r_4^2 = m(p - 2(ar_1 + br_2 + cr_3 + dr_4)$
$- (a^2 + b^2 + c^2 + d^2)m)$

Let $M = (p - 2(ar_1 + br_2 + cr_3 + dr_4) - (a^2 + b^2 + c^2 + d^2)m$,

then $r_1^2 + r_2^2 + r_3^2 + r_4^2 = mM$. Clearly $M \geq 0$,

if $M = 0$ this would implies $r_1 = r_2 = r_3 = r_4 = 0$ then m^2 would divide $x^2 + y^2 + z^2 + w^2 = mp$ and m would divide p.

Since p is a prime and $1 < m < p$, this is a contradiction.

Hence $1 \leq M$.

We also know that $Mm = r_1^2 + r_2^2 + r_3^2 + r_4^2 < 4\ (m^2/4) = m^2$

Hence $M < m$.

Putting these results together we have $1 \leq M < m$

So far we have

$r_1^2 + r_2^2 + r_3^2 + r_4^2 + 2m(ar_1 + br_2 + cr_3 + dr_4)$
$+(a^2 + b^2 + c^2 + d^2)m^2 = mp$ and $r_1^2 + r_2^2 + r_3^2 + r_4^2 = Mm.$

Therefore $Mm + 2m(ar_1 + br_2 + cr_3 + dr_4)$
$+ (a^2 + b^2 + c^2 + d^2)m^2 = mp.$

Dividing by m , we have $M + 2(ar_1 + br_2 + cr_3 + dr_4)$
$+ (a^2 + b^2 + c^2 + d^2)m = p.$

Multiply both sides by M, we have

$M^2 + 2M(ar_1 + br_2 + cr_3 + dr_4) +(a^2 + b^2 + c^2 + d^2)Mm = Mp.$

This imply $M^2 + 2M(ar_1 + br_2 + cr_3 + dr_4)$
$+ (a^2 + b^2 + c^2 + d^2)(r_1^2 + r_2^2 + r_3^2 + r_4^2) = Mp.$

Using Euler's identity

$(a^2 + b^2 + c^2 + d^2)(r_1^2 + r_2^2 + r_3^2 + r_4^2)$
$= (ar_1 + br_2 + cr_3 + dr_4)^2 + (ar_2 - br_1 + cr_4 - dr_3)^2$
$+ (ar_3 - br_4 - cr_1 + dr_2)^2 + (ar_4 + br_3 - cr_2 - dr_1)^2$

Let $A = (ar_1 + br_2 + cr_3 + dr_4)$
$B = (ar_2 - br_1 + cr_4 - dr_3)$
$C = (ar_3 - br_4 - cr_1 + dr_2)$
$D = (ar_4 + br_3 - cr_2 - dr_1)$

Substitute these in the above equation, we have

$M^2 + 2AM + A^2 + B^2 + C^2 + D^2 = Mp$

$(M + A)^2 + B^2 + C^2 + D^2 = Mp$

Thus $x_1 = M + A$, $y_1 = B$, $z_1 = C$ and $w_1 = D$ and M are integers satisfying the conclusion of Lemma 3.03.

Example1: (m is even)

Consider the equation $x^2 + y^2 + z^2 + w^2 = mp$ where $m = 4$

and p = 7

We have $3^2 + 3^2 + 3^2 + 1^2 = 4.7$

$x_1 = (x+y)/2 = (3+3)/2 = 3$

$y_1 = (x-y)/2 = (3-3)/2 = 0$

$z_1 = (z+w)/2 = (3+1)/2 = 1$

$w_1 = (z-w)/2 = (3-1)/2 = 1$ and $M = m/2 = 4/2 = 2$.

Therefore $x_1{}^2 + y_1{}^2 + z_1{}^2 + w_1{}^2 = 3^2 + 0^2 + 2^2 + 1^2 = 2.7$

We apply the lemma again, we have

$x_2 = (3+0)/2 = 1.5$

$y_2 = (3-0)/2 = 1.5$

$z_2 = (2+1)/2 = 1.5$

$w_2 = (2-1)/2 = 0.5$ and $M_1 = 2/2 = 1$

Hence $x_2{}^2 + y_2{}^2 + z_2{}^2 + w_2{}^2 = 1.5^2 + 1.5^2 + 1.5^2 + 0.5^2 = 1.7$.

Example 2: (m is odd)

Consider the equation $x^2 + y^2 + z^2 + w^2 = mp$ where $p = 7$ and $m = 3$.

Then we have $3^2 + 2^2 + 2^2 + 2^2 = 3.7$

$x = 3 = am + r_1 = 1.3 + 0$

$y = 2 = bm + r_2 = 1.3 + (-1)$

$z = 2 = cm + r_3 = 1.3 + (-1)$

$w = 2 = dm + r_4 = 1.3 + (-1)$

hence
$$M = p - 2(ar_1 + br_2 + cr_3 + dr_4) - (a^2 + b^2 + c^2 + d^2)m$$
$$= 7 - 2[1.0 + 1(-1) + 1(-1) + 1(-1)] - [1^2 + 1^2 + 1^2 + 1^2]3$$
$$= 7 - 2(-3) - 12 = 1.$$

$A = (ar_1 + br_2 + cr_3 + dr_4) = (1.0 + 1(-1) + 1(-1) + 1(-1)) = 3$

$B = (ar_2 - br_1 + cr_4 - dr_3) = (1(-1) - 1.0 + 1(-1) - 1(-1)) = -1$

$C = (ar_3 - br_4 - cr_1 + dr_2) = (1(-1) - 1(-1) - 1.0 + 1(-1)) = -1$

$D = (ar_4 + br_3 - cr_2 - dr_1) = (1(-1) + 1(-1) - 1(-1) - 1.0) = -1$

Hence, $x_1 = \; = 1 \; -3 = 2$

$y_1 = B = -1$

$z_1 = C = -1$

$w_1 = D = -1.$

Therefore we have,

$x_1^2 + y_1^2 + z_1^2 + w_1^2 = 2^2 + (-1)^2 + (-1)^2 + (-1)^2 = 1.7.$

Lemma 3.04:

Every prime can be represented as a sum of four square integers that is to say that for every prime p,

$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is solvable.

Proof:

For $p = 2$, this is obvious since $2 = 1^2 + 1^2 + 0^2 + 0^2$. Therefore let $p > 2$. Now we are going to apply Fermat's method of descent.

By Lemma 3.02 we can find integers x,y,z,w such that

$x^2 + y^2 + z^2 + w^2 = mp$ where $1 \leq m < p$

If $m > 1$, we can apply Lemma 3.03 a finite number of times (say $p > m > M = M_1 > M_2 > \ldots > M_k = 1$)

to descent to the situation ,

$x_k^2 + y_k^2 + z_k^2 + w_k^2 = p$

This shows that every odd prime may be represented as the sum of four squares.

Theorem 3.1:

Every positive integer n is the sum of four square integers.

Proof:

By Lemma 3.04 , every prime can be represented as sum of four squares, Lemma 3.01 guarantees that every composite number may be represented as sum of four squares. For 1 we have,

$1 = 1^2 + 0^2 + 0^2 + 0^2$. Thus we have proved the theorem.

Example:

Let $n = 30 = 2.3.5$. By lemma 3.04, 2,3 ,5 are primes and can be presented as a sum of four squares.

$2 = 1^2 + 1^2 + 0^2 + 0^2$

$3 = 1^2 + 1^2 + 1^2 + 0^2$

$5 = 1^2 + 2^2 + 0^2 + 0^2$.

Therefore by lemma 3.01, 30 is also a sum of four squares since 30 is a product of 2.3.5 , $30 = 1^2 + 2^2 + 3^2 + 4^2$.

Theorem 3.2:

Every positive rational number is the sum of the squares of four rational numbers.

Proof:

Let r be a positive rational number $r = k/m$ where k and m are positive integers. By the previous theorem, it follows that every positive integer is the sum of the squres of four or fewer integers.

If $km = a^2 + b^2 + c^2 + d^2$ where a,b,c,d are integers then

$$r = k/m = a^2/m^2 + b^2/m^2 + c^2/m^2 + d^2/m^2$$
$$= (a/m)^2 + (b/m)^2 + (c/m)^2 + (d/m)^2$$

2. Representation of integers as sum of four nonvanishing squares

In this section we consider the problem of representing an integer n as a sum of four nonvanishing squares. It is more convenient to consider the two cases according to whether n is even natural number or n is an odd natural number.

Theorem 3.3:

An odd natural number n is the sum of the squares of four natural numbers if and only if it does not belong to the sequence of numbers 1, 3, 5, 9, 11, 17, 29, and 41.

Proof:(By contradiction)

Assume 29 is the sum of the squares of four natural numbers. Therefore $29 = a^2 + b^2 + c^2 + d^2$ where all $a, b, c, d \geq 1$ and without loss of generality assume $a \geq b \geq c \geq d$. Hence $a^2 < 29 \leq 4a^2$

which implies $3 \leq a \leq 5$.

If $a = 3$ then $29 = 9 + b^2 + c^2 + d^2$

implies $20 = b^2 + c^2 + d^2$

If $a = 4$ then $13 = b^2 + c^2 + d^2$

If $a = 5$ then $4 = b^2 + c^2 + d^2$

By trial an error , all of the above are impossible. Therefore 29 is not the sum of the square of four natural numbers. We can also show none of the numbers

1,3,5,9,17,41, is the sum of four nonvanishing squares by using the same method of proof.

Now suppose that an odd natural n satisfies the condition of the theorem. Therefore $n \neq 1,3,5,9,11,17, 29, 41$.

Since n is odd , it must be of the form $8k + 1$, $8k +3$, $8k + 5$, or $8k +7$.

Consider $n = 8k + 1$.

Let k be of the form $k= 4t, 4t + 1, 4t + 2, 4t + 3$.

If $k = 4t$ we have $n = 8(4t) + 1 = 32t + 1$.

Since $n \neq 1$ then $t \geq 1$. Let $t = x + 1$ where $x \geq 0$

Therefore $n = 32(x+1) + 1 = 4(8x + 6) + 9$

$8x + 6$ is the sum of three squares and also since $8x + 6 = 2(4x + 3)$ cannot be the sum of two squares, this implies each of the integers a, b, c must be nonzero.

$$\begin{aligned}\text{Hence } n &= 4(8x + 6) + 9\\ &= 2^2 (8x + 6) + 9\\ &= 2^2 (a^2 + b^2 + c^2) + 3^2\end{aligned}$$

Therefore $n = 8k + 1$ is the sum of four nonvanishing squares if k is of the form $k = 4t$.

If $k = 4t + 1$, then $n= 8(4t + 1) + 1 = 32t + 9$

Since $n \neq 9$ and $n \neq 41$ we have $t \geq 2$

Let $t = x + 2$ where $x \geq 0$

$$\begin{aligned}\text{Hence } n &= 32(x+2) + 9\\ &= 2^2 (8x + 6) + 7^2\\ &= 2^2 (a^2 + b^2 + c^2) + 7^2\end{aligned}$$

This implies $n = 8k +1$ is the sum of four nonvanishing squares if k is of the form 4t +1.

If $k = 4t + 2$, then $n = 8(4t + 2) + 1 = 32t + 17$

Since $n \neq 17$ then $t \geq 1$. Let $t = x + 1$ and $x \geq 0$.

Therefore $n = 32(x + 1) + 17$

$$= 2^2(8x+6) + 5^2 = 2^2(a^2 + b^2 + c^2) + 5^2$$

This implies $n = 8k + 1$ is the sum of four nonvanishing squares if $k = 4t + 2$.

If $k = 4t + 3$ then $n = 8(4t + 3) + 1 = 32+ + 25$

$$= 2^2(8t + 6) + 5^2$$

This implies $n = 8t + 1$ is the sum of four nonvanishing square if $k = 4t + 3$.

Thus we have proved that the theorem is sufficient provided $n = 8k + 1$.

Now consider $n = 8k + 3$.

Since $n \neq 3$ and $n \neq 11$, this implies $k \geq 2$

Let $k = x + 2$ and $x \geq 0$

Then $n = 8(x+2) + 3 = (8x+3) + 4^2$

$(8x+3)$ is the sum of three squares and since $(8x+3)$ is odd, the three integers must all be odd . For assume two of the integers are even and one is odd then

$$8x + 3 = (2a)^2 + (2b)^2 + (2c+1)^2$$

$$= 4a^2 + 4b^2 + 4c^2 + 4c + 1$$

$$= 4(a^2 + b^2 + c^2 + c) + 1$$

$$8x + 2 = 4(a^2 + b^2 + c^2 + c)$$

$8x + 2 = 4k$ where $k = a^2 + b^2 + c^2 + c$

$2(4x+1) = 4k$

$4x + 1 = 2k$

Contradiction since $4x + 1$ is odd and $2k$ is even.

Hence $(8x + 3)$ is the sum of the squares of three odd integers which is $8k+3 = (2a+1)^2 + (2b+1)^2 + (2c+1)^2$ where a,b,c are nonnegative integers. Consequently $8k + 3$ is the sum of the square of three nonvanishing squares.

Therefore $n = a_1{}^2 + b_1{}^2 + c_1{}^2 + 4^2$ which is the sum of four nonvanishing squares.

Thus we have proved the condition of the theorem is sufficient for $n = 8k +3$.

Consider $n = 8k + 5$.

If $k = 4t$ then $n = 8(4t) + 5 = 32t = 5$

Since $n \neq 5$ this implies $t \geq 3$ 1 . Let $t = x + 1$ where $x \geq 0$.

Therefore $n = 32(x+1) + 5 = 2^2(8x+3) + 5^2$

$$= 2^2(a^2 + b^2 + c^2) + 5$$

This implies $n = 8k + 5$ is the sum of four nonvanishing squares if $k = 4t$.

If $k = 4t + 1$ then $n = 8(4t + 1) + 5 = 32t + 13$.

Since $n \neq 13$ implies $t \geq 1$. Let $t = x+1$ and $x \geq 0$.

Therefore $n = 32(x+1) + 13 = 2^2(8t+3) + 1^2$

This implies n is the sum of four nonvanishing squares if $k = 4t+1$.

If $k = 4t + 2$ then $n = 8(4t+2) + 5 = 2^2(8t+3) + 3^2$

This implies $n = 8k + 5$ is the sum of four non vanishing squares if $k = 4t + 2$.

If $k = 4t + 3$, then $n = 8(4t+3) + 5 = 32t + 29$

Since $n \neq 29$ implies $t \geq 1$. Let $t = x+1$ where $x \geq 0$.

Then $n = 32(x+1) + 29 = 2^2(8x+3) + 7^2$ which implies

$n = 8k+5$ is the sum of four nonvanishing squares if

$k = 4t + 3$.

Thus we have proved that the theorem is sufficient provided

$n = 8k+5$.

Finally consider $n = 8k + 7$.

If $k = 0$ then $n \ \ 7 = 2^2 + 1^2 + 1^2 + 1^2$

If $k = 1$ then $n = 15 = 2^2 + 3^2 + 1^2 + 1^2$

If $k = 2$ then $n = 23 = 3^2 + 3^2 + 2^2 + 1^2$

If $k = 3$ then $n = 31 = 3^2 + 3^2 + 3^2 + 2^2$

If $k = 4$ then $n = 39 = 1^2 + 2^2 + 3^2 + 5^2$

If $k \geq 5$, then $n = 8k + 7 \geq 47$. By Langrange's theorem, there exist integers a,b,c,d such that

$8k + 7 = a^2 + b^2 + c^2 + d^2$.

And we have proved that in order that an odd natural number be the sum of the squares of four nonvanishing integers it should not be any of the number 1,3,5,9,11,17,29 and 41. This implies that any odd natural number of the form $n = 8k + 7$ and > 41 is the sum of the square of four nonvanishing integers.

Next we consider the second case where n is an even number.

Theorem 3.4:

An even natural number n is the sum of the squares of four natural numbers if and only if it is none of the numbers $4^h.2$, $4^h.6$, $4^h.14$ where h = 0,1,2.... .

Proof:(By contradiction)

Let S_4 be the set of all positive integers that can be written as the sum of the squares of four nonvanishing numbers.

Assume $4^h.m \in S_4$ where $h \geq 0$ and $m \in \{2,6,14\}$.
Therefore m is of the form $4k + 2 = 2(2k+1)$ where k =0,1,3
Let h' be the least of such integers.
Since $\{2,6,14\} \notin S_4$ implies $h' \geq 1$.
Hence $4^h.m = a^2 + b^2 + c^2 + d^2$ where all a,b,c,d >0
$4^h.2(2k+1) = a^2 + b^2 + c^2 + d^2$
But $4^{h'}.2(2k+1) \equiv 0 \pmod{8}$ because $h' \geq 1$.
Therefore a,b,c,d are all even ie $a = 2a_1$, $b = 2b_1$, $c = 2c_1$ and $d = 2d_1$ where a_1, b_1 , c_1 ,d_1 are nonvanishing integers. Hence $4^{h'-1}m = a_1{}^2 + b_1{}^2 + c_1{}^2 + d_1{}^2$
$4^{h'-1}m \in S_4$
Contrary to the choice of h'.
Therefore $4^hm \notin S_4$ where m= 2,6,14.

Now let n be an even natural number different from $4^h.2$, $4^h.6$, $4^h.14$ where h= 0,1,2...
Let $4^{h''}$ be the highest power of the number 4 which divides the number n. Then we have $n = 4^{h''}m$ where $m \not\equiv 0 \pmod{4}$
Therefore $m = 4k + 1$, $m = 4k+2$ or $m = 4k + 3$.

If $m = 4k + 1$ and k is even i.e $k = 2t$ then $m = 8t + 1 \in S_4$ as proved previously. In addition if m $\{1,9,17,41\}$ then $4^h m \in S_4$.

But since n is even and $m \not\equiv 0 \pmod{4}$, then $h" > 0$.

Clearly $4 \in S_4$, $4.17 = 68 = 1^2 + 3^2 + 3^2 + 7^2$ and $4.41 = 164 = 1^2 + 1^2 + 9^2 + 9^2$

Hence
$$4^h.1 = 4(2^{h-1})^2$$
$$4^h.9 = 4(2^{h-1}.3)^2$$
$$4^h.17 = 4.17(2^{h-1})^2$$
$$4^h.41 = 4.41(2^{h-1})^2$$ are all in S_4.

Thus if $m = 4k + 1$ and k is even then $n = 4^h m \in S_4$.

Now if $k = 2t + 1$ which is odd then $m = 8t + 5$ as proved is in S_4 provided $m \not\equiv 5$ Or $m \not\equiv 29$.

Since $n = 4^h m$ is even and m is odd this implies $h > 0$.

Hence $4.5 = 20 = 1^2 + 1^2 + 3^2 + 3^2$ and $4.29 = 116 = 1^2 + 3^2 + 5^2$ are both in S_4.

Thus $m = 4k + 1$ with k is odd is in S_4.

If $m = 4k + 2$ and k is even i.e $k = 2t$ then $m = 8t + 2$.

Since $n \not\equiv 4^h.2$ implies $t > 0$. Let $t = u + 1$ where $u \geq 0$.

Then we have $m = 8(u + 1) + 2 = 8u + 6 + 2^2$.

Since $8u + 6$ is the sum of three nonvanishing squares implies $m = 4k + 2 \in S_4$.

If $m = 4k + 2$ and k is odd i.e $k = 2t + 1$ the we have $m = 8t + 6$.

Since $n \not\equiv 4^h.6$ and $n \not\equiv 4^h.14$ we must have $t \geq 2$.

Let $t = u + 2$ where $u \geq 0$.

Therefore $m = 8(u+2) + 6 = 8u + 6 + 4^2$. Since $(8u+6)$ is the sum of three nonvanishing squares, this implies $m \in S_4$.

If $m = 4k + 3$ and k is even i.e $k = 2t$, we have

$m = 8t + 3$.

As proved previously $m \in S_4$ provided $m \neq 3$ or $m \neq 11$.

Since n is even and m is odd implies $h > 0$. Therefore

$4.3 = 12 = 1^2 + 1^2 + 1^2 + 3^2$

$4.11 = 44 = 1^2 + 3^2 + 3^2 + 5^2$ are both in S_4.

Thus if $m = 4k + 3$ then $n = 4^h m \in S_4$.

This complete the proof that an even natural number n is the sum of four nonvanishing squares if and only if it is none of the number $4^h.2$, $4^h 6$, $4^h.14$ where

$h = 0,1,2,\ldots\ldots$.

3. Representation Of Integers As The Sum Of The Squares Of Four Different Integers.

In this section we will consider the problem of representing a positive integer n as the sum of the squares of four different integers.

Theorem 3.5:

The only integers $n > 0$ not the sum of four different squares greater than or equal to 0 are $4^h a$, where $h = 0,1,2\ldots$ and $a = 1,3,5,7,9,11,13,15,17,19,23,25,27,31,$ $33,37,43,47,55,67,73,97,103,2,6,10,18,22,34,58,82$.

Before we prove the theorem we need the following lemmas.

Lemma 3.04:

An odd integer A is a sum of four unequal squares if and only if 4A is a sum of four unequal odd squares.

Proof:

Let A denote a positive odd integer. The system of equations,

$$X = x + y + z + w$$

$$Y = x + y - z - w$$

$$Z = x - y + z - w$$

$$W = x - y - z + w$$, defines a (1,1) correspondence between the set of integers x,y,z,w satisfying

$$A = x^2 + y^2 + z^2 + w^2$$

and the set of integers X ,Y ,Z , W satisfying

$$4A = X^2 + Y^2 + Z^2 + W^2 , \quad X + Y + Z + W \equiv 0 (\bmod 4) \text{ and } X ,Y ,Z ,W \text{ are odd.}$$

Let $U = \{ (x,y,z,w) | x^2 + y^2 + z^2 + w^2 = A\}$

$V = \{ (X,Y,Z,W) | X^2 + Y^2 + Z^2 + W^2 = 4A ,$
$X + Y + Z + W = 4k;$ X ,Y , Z , W are odd$\}$

If we write the above system of equations in a matrix form we have

$$\begin{bmatrix} X \\ Y \\ Z \\ W \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} \text{ with } M = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Let $F : U \longrightarrow V$ be defined by $F(u) = Mu$ for $u \in U$.

CLaim:

$F : U \longrightarrow V$ define a 1-1 correspondence between U and V.

To prove the claim, we will show that

1) If $u' = (x', y', z', w') \in U$ then $F(u) \in V$

2) F is 1-1

3) If $v' = (X', Y', Z', W') \in V$ then $F^{-1}(v') \in U$.

1) Let $(x', y', z', w') \in U$

Now $X^2 + Y^2 + Z^2 + W^2$

$$= (x'+y'+z'+w')^2 + (x'+y'-z'-w')^2 + (x'-y'+z'-w')^2 + (x'-y'-z'+w')^2$$

$$= (x'^2 + y'^2 + z'^2 + w'^2 + 2x'y' + 2x'z' + 2x'w' + 2y'z' + 2y'w' + 2z'w')$$
$$+ (x'^2 + y'^2 + z'^2 + w'^2 + 2x'y' - 2x'z' - 2x'w' - 2y'z' - 2y'w' + 2z'w')$$
$$+ (x'^2 + y'^2 + z'^2 + w'^2 - 2x'y' - 2x'z' - 2x'w' - 2y'z' + 2y'w' - 2z'w')$$
$$+ (x'^2 + y'^2 + z'^2 + w'^2 - 2x'y' - 2x'z' + 2x'w' + 2y'z' - 2y'w' - 2z'w')$$

$$= 4(x'^2 + y'^2 + z'^2 + w'^2) = 4A$$

$X + Y + Z + W$

$$= (x'+y'+z'+w') + (x'+y'-z'-w') + (x'-y'+z'-w') + (x'-y'-z'+w')$$

$$= 4x' \equiv 0 \pmod 4.$$

Since A is odd we must have three of the integers say x', y', z' are odd and w' is even , or three of the integers say x', y', $z'$are even and w' is odd. For the case x', y', z' are odd and w' is even we have,

$X = x'+y'+z'+w' =(2k+1)+(2h+1)+(2m+1)+(2n)$

$= 2(k+h+m+n+1) +1$ which is odd

$Y = x'+y'-z'-w' =(2k+1)+(2h+1)-(2m+1)-(2n)$

$= 2(k+h-m-n) + 1$ which is odd

$Z = x'-y'+z'-w' =(2k+1)-(2h+1)+(2m+1)-(2n)$

$= 2(k-h+m-n) +1$ which is odd

$W = x'-y'-z'+w' =(2k+1)-(2h+1)-(2m+1)+(2n)$

$= 2(k-h-m+n-1)+1$ which is odd

Similarly for the case x',y',z' are even and w' is odd we will have X,Y,Z,W are all odd.

Therefore given $u'= (x',y'z',w') \in U$ then $F(u) \in V$.

2) Matrix M has an inverse because determinant $M \nmid 0$. This implies the mapping $F : U \rightarrow V$ is 1-1.

3) Now we will show that if $v'=(X',Y',Z',W') \in V$ then $F^{-1}(v') \in U$

$$M^{-1} = 1/4 \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

If we multiply M^{-1} to the left of both side of the matrix , we have

$$(1/4) \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} X' \\ Y' \\ Z' \\ W' \end{bmatrix} = \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix}$$

hen $x = (1/4)(X'+Y'+Z'+W')$

$y = (1/4)(X'+Y'-Z'-W')$

$z = (1/4)(X'-Y'+z'-W')$

$w = (1/4)(X'-Y'-Z'+W')$ where all x,y,x,w are integers.

$X'+ Y'+ Z'+ W' \equiv 0 \pmod{4}$

implies $X'+Y'+Z'+W' = 4k$ for some k

Now $x = (1/4)(X'+Y'+Z'+W')$

$= (1/4)(4k) = k$ which is integer.

Now $y = (1/4)(X'+Y'-Z'-W')$

$= (1/4)((X'+Y') +(X'+Y'-4k))$

$= (1/4)(2(2k_1+1) + 2(2k_2 +1) - 4k)$

$= (1/4) (4k_1 + 4k_2 -4k +4)$

$= k_1 + k_2 - k +1$ which is integer.

Similarly it can be shown z and w are integers.

Therefore when we square each x,y,z,w we have

$x^2 + y^2 +z^2 + w^2$

$= (4/16) (X'^2 + Y'^2 + Z'^2 + W'^2) =(1/4)(4A) = A.$

Hence given $v'=(X',Y',Z',W') \in V$ then $F^{-1} (v') \in U$.

Finally we need to show that if $x^2 \neq y^2 \neq z^2 \neq w^2$ then $X'^2 \neq Y'^2 \neq Z'^2 \neq W'^2$ and conversely.

First assume $x^2 \neq y^2 \neq z^2 \neq w^2$.

By symmetry we need to consider only two cases.

Case1:

Assume $X^2 = Y^2$ then $X = Y$ or $X = -Y$.

For $X = Y$, $x + y + z + w = x + y - z - w$

$2z = -2w$

implies $z = -w$

implies $z^2 = w^2$

Contradiction.

For $X = -Y$, $x + y + z + w = -x - y + z + w$

implies $x = -y$

implies $x^2 = y^2$

Contradiction.

Case2:

Assume $Y^2 = Z^2$ then $Y = Z$ or $Y = -Z$

For $Y = Z$, $x + y - z - w = x - y + z - w$

implies $2y = 2z$

implies $y = z$ implies $y^2 = z^2$

Contradiction.

For $Y = -Z$, $x + y - z - w = -x + y - z + w$

implies $2x = 2w$

implies $x = w$ implies $x^2 = w^2$

Contradiction.

We can show that the converse of this is also true by using similar method of proof.

This complete the proof of Lemma 3.04.

Lemma 3.05:

An odd integer A is a sum of four positive squares if and only if 2A is a sum of four different squares.

Proof:

Let A denote a positive odd integer. The system of equations, $s = x + y$, $t = x - y$, $u = z + w$, $v = z - w$, define a (1,1) correspondence between the set of integers x,y,z,w satisfying,

$A = x^2 + y^2 + z^2 + w^2$ and the set of integers s, t, u, v satisfying

$$2A = s^2 + t^2 + u^2 + v^2 \text{ ,} s \equiv t \not\equiv u \equiv v (\text{mod} 2)$$

Let $R = \{(x,y,z,w) | x^2 + y^2 + z^2 + w^2 = A\}$

$S = \{(s,t,u,v) | s^2 + t^2 + u^2 + v^2 = 2A;$

$s \equiv t \not\equiv u \equiv v (\text{mod} 2)\}$

If we write the system of equations in a matrix form we have

$$\begin{bmatrix} s \\ t \\ u \\ v \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} x \\ y \\ z \\ w \end{bmatrix} \quad \text{where B} \quad \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

Let $F : R \rightarrow S$ be defined by $F(r) = Br$ for $r \in R$.

Claim: $R \rightarrow S$ define a 1-1 correspondence between R and S.

To prove the claim, we will show that,

1) If $u' = (x',y',z',w')$ R then $F(r)$ S.

2) F is 1-1

3) If $s'' = (s',t',u',v') \in S$ then $F^{-1}(s'') \in R$.

Let $(x',y',z',w') \in R$

Now $s^2 + t^2 + u^2 + v^2$

$= (x'+y')^2 + (x'-y')^2 + (z'+w')^2 + (z'-w')^2$

$= x'^2 + y'^2 + 2x'y' + x'^2 + y'^2 - 2x'y' + z'^2 + w'^2 + 2z'w' + z'^2$
$+ w'^2 - 2z'w'$

$= 2(x'^2 + y'^2 + z'^2 + w'^2) = 2A$

$s - t = (x'+y') - (x'-y') = 2y \equiv 0 \pmod{2}$

$u - v = (z'+w') - (z'-w') = 2w \equiv 0 \pmod{2}$

$s - u = (x'+y') - (z'+w') \not\equiv 0 \pmod{2}$

Therefore given $r' = (x',y',z',w') \in R$ then $F(r') \in S$.

2) Matrix B has inverse because $\det B \neq 0$. This implies the mapping $F : R \rightarrow S$ is 1-1.

3) Now we will show that if $s'' = (s',t',u',v') \in S$ then $F^{-1}(s'') \in R$

$$B^{-1} = (1/2) \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}$$

If we multiply B^{-1} to the left of both side of the matrix equation we have,

$$(1/2) \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} s' \\ t' \\ u' \\ v' \end{bmatrix} = \begin{bmatrix} x' \\ y' \\ z' \\ w' \end{bmatrix}$$

then $x' = (1/2)(s'+t')$

$y' = (1/2)(s'-t')$

$z' = (1/2)(u'+v')$

$w' = (1/2)(u'-v')$

Clearly x', y', z' and w' are integers.

For $s' \equiv t' \pmod 2$ implies $s'-t' = 2k$ for some k

Now $x' = (1/2)(s+t) = (1/2)(2k+t+t) = (1/2)(2k+2t) = k+t$ which is integer.

$y' = (1/2)(s'-t') = (1/2)(2k) = k$ which is integer

$u' \equiv v' \pmod 2$ implies $u'-v' = 2k$ for some k

Now $z' = (1/2)(u'+v') = (1/2)(2k+v'+v') = k+v'$ which is integer.

$w' = (1/2)(u'-v') = (1/2)(2k) = k$ which is integer

Therefore when we square each $x, y'z'w'$ we have

$$x'^2 + y'^2 + z'^2 + w'^2$$

$$= (1/4)(s^2 + t^2 + 2st) + (1/4)(s^2 + t^2 - 2st)$$

$$+ (1/4)(u^2 + v^2 + 2uv) + (u^2 + v^2 - 2v)$$

$$= (2/4)(s^2 + t^2 + u^2 + v^2) = (1/2)(2A) = A.$$

Hence given $s'' = (s', t', u', v') \in S$ then $F^{-1}(s'') \in R$.

Now we need to show if $x, y, z, w > 0$ then $s^2 \neq t^2 \neq u^2 \neq v^2$ and conversely if $s^2 \neq t^2 \neq u^2 \neq v^2$ then $x, y, z, w > 0$.

We need to consider only four cases.

Case 1:

Assume $x^2, y^2, z^2, w^2 > 0$. But $s^2 = t^2$

This implies $s = t$ or $s = -t$.

If $s = t$ then $x + y = x - y$

implies $y = 0$;Contradiction since $y>0$.

If $s = -t$ then $x + y = y - x$

implies $x = 0$; Contradiction since $x>0$.

Case2:

Assume $x^2, y^2, z^2, w^2 > 0$ but $s^2 = u^2$.

This implies $s = u$ or $s = -u$

If $s = u$, then $s - u = 0$ impossible since $s \not\equiv u (\mathrm{mod} 2)$

If $s = - u$, then $s + u = 0$

implies $(x + y) + (z + w) = 0$ impossible since $x,y,z,w > 0$

Case3:

Assume $x^2, y^2, z^2, w^2 > 0$ but $t^2 = u^2$

This implies $t = u$ or $t = -u$

For $t = u$ then $t - u = 0$ impossible since $t \not\equiv u (\mathrm{mod} 2)$

Since $t \not\equiv u(\mathrm{mod} 2)$ implies $t-u = 2k$ implies $t-u = 2k + 1$.

Then if $t = -u$ then $t + u = 0$

$t - u = 2k + 1$ which imply $2t = 2k+1$

which is impossible.

Case 4:

Assume x^2, y^2, z^2, $w^2 > 0$ but $t^2 = v^2$.

This implies $t = v$ or $t = -v$.

If $t = v$ then $t - v = 0$, impossible since $t \not\equiv v (\mathrm{mod} 2)$.

Since $t \not\equiv v(\mathrm{mod} 2)$ implies $t - v = 2k$ implies $t-v= 2k+1$.

Thus if $t = -v$ then $t + v = o$ and

$t - v = 2k + 1$ which imply $2t =2k+1$

which is impossible.

Lemma 3.06:

If $2A$ possesses a representation $2A = s^2 + t^2 + u^2 + v^2$ where $s,t,u,v \neq 0$ and $s^2 > (3A/2)$ then A is a sum of four unequal squares.

Proof:

Assume $2A = s^2 + t^2 + u^2 + v^2$, where $s, t, u, v \neq 0$ and $s^2 > (3A)/2$.

Assume the contrary, that is assume $A = x^2 + y^2 + z^2 + w^2$ is not a sum of four unequal squares.

Case 1:

Assume $x^2 = y^2$ then $x = y$ or $x = -y$

If $x = y$ then $t = 0$ implies $stuv = 0$

If $x = -y$ then $s = 0$ implies $stuv = 0$

A contradiction.

Case 2:

Assume $z^2 = w^2$, then $z = w$ or $z = -w$,

this implies $stuv = 0$, a contradiction.

Case 3:

Assume $x^2 = z^2$, then $x = z$ or $x = -z$

If $x = z$ then $s = x+y$, $u = x + w$, $t = x-y$, $v = x-w$

$s + t = 2x$

$u + v = 2x$

Hence $s + t - u - v = 0$.

If $x = -z$ then $s = x+y$, $u = -x+w$, $t = x-y$, $v = -x-w$

Hence $s + t + u + v = 0$

The rest of the cases will result in

$e_1 s + e_2 t + e_3 u + e_4 v = 0$, where the $e_i = \pm 1$

Now if $2A = s^2 + t^2 + u^2 + v^2$ and $s,t,u,v \neq 0$ then

$stuv \neq 0$ which implies case 1 and case 2 do not occur.

For case 3, we consider

$$(|t| + |u| + |v|)^2$$

$$= t^2 + u^2 + v^2 + 2|t|\ u + 2|t|\,|v| + 2\,|u|\,|v|$$

$$\leq t^2 + u^2 + v^2 + (t^2 + u^2) + (t^2 + v^2) + (u^2 + v^2)$$

$= 3(t^2 + u^2 + v^2)$

$= 3(2A - s^2)$

$= 2(3A) - 3s^2$

$= 2.2(3A/2) - 3s^2$

$< 4s^2 - 3s^2 = s^2$

Thus $(|t| + |u| + |v|)^2 < s^2$.

Take the square root of both sides, we have

$|t| + |u| + |v| - |s| < 0$ which would imply case 3 does not occur since $\pm t \pm u \pm v \pm s = 0$.

Therefore if $2A = s^2 + t^2 + u^2 + v^2$, $s,t,u,v \neq 0$, $s^2 > (3A/2)$ then A is the sum of four unequal squares.

This complete the proof for Lemma 3.06.

4. The Total Number of Representations As The Sum of Four Squares.

In this section we are going to find the total number of representations of a positive integer n as a sum of four squares.

Throughout this section the symbols u_1, u_2, u_3, u_4, h, m, a, α, b, β, a_1, α_1, b_1, β_1 will denote positive odd numbers.

Theorem 3:6:

Let A(u) be number of positive solutions of

$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2$.

Then $A(u) = \sigma(u)$ where $\sigma(u) = \sum_{d|u} d$, the sum of divisors of u.

Proof:

We claim that all the solutions of the given equation can be obtained when we decompose $4u$ into $2h + 2m$ in all posible ways and then solve $u_1^2 + u_2^2 = 2h$; $u_3^2 + u_4^2 = 2m$

To verify the above claim,first note that since u_1, u_2 are odd we have $u_1 = 2k +1$, $u_2 = 2m + 1$.

Hence $u_1^2 + u_2^2$

$= (2k+1)^2 + (2m+1)^2$

$= 4(k^2 + k + m^2 +m) + 2$

$= 2(2k^2 + 2k +2m^2 +2m +1) = 2h$ where h is odd.

Similarly, $u_3^2 + u_4^2 = 2m$ where m is odd.

Thus if $\overline{u_1}$, $\overline{u_2}$, $\overline{u_3}$, $\overline{u_4}$ is a solution of $u_1^2 + u_2^2 + u_3^2 + u_4^2 = 4u$ then $\overline{u_1}$, $\overline{u_2}$ and $\overline{u_3},\overline{u_4}$ are solution for $u_1^2 + u_2^2 = 2h$ and $u_3^2 + u_4^2 = 2m$ respectively, where $2h + 2m = 4u$.

On the other hand if h is an odd number and $2h = u_1^2 + u_2^2$ the numbers u_1, u_2 are odd.

For assume u_1 , u_2 are both even i.e $u_1 = 2v'$, $u_2 = 2v''$ then $2h = (2v')^2 + (2v'')^2$

$= 4v'^2 + 4v''^2$

$2h = 4(v'^2 + v''^2)$,

a contradiction because $4 \mid 4(u'^2 + u''^2)$ but $4 \nmid 2h$ since h is odd.

Also if we assume one of the numbers is even say $u_1 = 2\ v'$ and one is odd say $u_2 = 2v'' + 1$ then

$2h = 2(2v'^2 + 2v''^2 + 2v'') + 1$.

This is a contradiction since $2h$ is even but

$2(2v'^2 + 2v''^2 + 2v'') + 1$ is odd.

Similarly if m is odd and $2m = u_3^2 + u_4^2$ then u_3 and u_4 are both odd.

Thus we see that, in order to find all representation of the number 4u as the sum of four odd squares, it is sufficient to find all possible representation of 4u as a sum of the form $4u = 2h + 2m$ where h and m are both odd numbers, and then to find the number of representation of both numbers 2h, 2m as the sum of two squares.

Now let U(n) = Number of solutions of $n = x^2 + y^2$.

We know from the previous chapter,

$$\frac{U(n)}{4} = \sum_{d/n} \chi(d),$$

$$\frac{U(2h)}{4} = \sum_{a|2h} (a) \quad \text{for } u_1^2 + u_2^2 = 2h$$

$$\frac{U(2m)}{4} = \sum_{b|2m} (b) \quad \text{for } u_3^2 + u_4^2 = 2m$$

Therefore ,

$$A(u) = \sum_{2h+2m=4u} \frac{U(2h)}{4} \frac{U(2m)}{4}$$

$$= \sum_{h+m=2u} \sum_{a|2h} \chi(a) \sum_{b|2m} \chi(b)$$

$$= \sum_{h+m=2u} \sum_{a|h} \chi(a) \sum_{b|m} \chi(b)$$

$$= \sum_{h+m=2u} \left(\sum_{\substack{a|h \\ b|m}} \chi(ab) \right)$$

$$= \sum_{a\alpha + b = 2u} \chi(ab)$$

the last equality hold because

$a|h$ implies $h = a\alpha$

$b|m$ implies $m = b\beta$

Thus $A(u) = \sum_{a\alpha+b\beta=2u} \chi(ab)$

Now we divide the summands in the summation above into two cases the first consisting of the summands for $a \nmid b$ and the second of those for which $a = b$.

Case1: $a \nmid b$

In this case, the equation $2(u/a) = \alpha+\beta$ has (u/a) solutions ($\alpha = 1,3, \ldots\ldots 2(u/a) -1$) and the β determined therefrom);

Since $\chi(aa)=1$, the contribution of each of the u/a solutions is 1.

Thus the total contribution in this case is

$$\sum_{a/u} u/a = \sum_{d/u} d = \sigma(u)$$

Case2 $a \nmid b$

In this case we are going to show $\sum_{\substack{a\alpha+b\beta=2u \\ a\ >(<) b}} \chi(ab) = 0$

By symmetry , it suffices to show $\sum_{\substack{a\alpha+b\beta=2u \\ a\ >\ b}} \chi(ab) = 0$

and for this it suffices to pair off the solutions of $a\alpha + b\beta = 2u$, $a>b$ one to one in such a way that for every quadruple a,b,α,β , we assign a quadruple a_1, b_1 , α_1 , β_1 such that $\chi(ab) + \chi(a_1b_1) = 0$

To achieve this goal, a rule is specified such that

1) to every quadruple a, b, α, β of positive odd numbers , we assign quadruple a_1, b_1, α_1, β_1 such that
$a_1\alpha_1 + b_1\beta_1 = 2u$, $a_1 > b_1$;

2) And also for quadruples a_1, b_1, α_1, β_1 the rule assign the original quadruple a, b, α, β.

3) And the equation must satisfies the following,
$X(ab) + X(a_1b_1) = 0$.

Let us start with the first rule.

1) Let $n = \left[\frac{b}{a-b}\right]$ (≥ 0) ; where $[x]$ is the greatest integer $\leq$ x

Let quadruples (*) be the following

$$a_1 = (n+2)\alpha + (n+1)\beta$$
$$\alpha_1 = -na + (n+1)b$$
$$b_1 = (n+1)\alpha + n\beta$$
$$\beta_1 = (n+1)a - (n+2)b$$

<u>Claim 1</u>

Each of these numbers is odd

$$\begin{aligned} a_1 &= (n+2)\alpha + (n+1)\beta \\ &= n\alpha + 2\alpha + n\beta + \beta \\ &= n(2k+1) + 2(2k+1) + n(2m+1) + 2m+1 \\ &= 2kn + n + 4k + 2 + 2mn + n + 2m + 1 \\ &= 2kn + 4k + 2 + 2mn + 2n + 2m + 1 \\ &= 2(kn + 2k + 1 + mn + n + m) + 1 \\ &= \text{odd}. \end{aligned}$$

$$\begin{aligned}
\alpha_1 &= -na + (n+1)b \\
&= -n(2k+1) + (n+1)(2m+1) \\
&= -2kn-n+2mn+2m+n+1 \\
&= 2(-kn+mn+m) + 1 \\
&= \text{odd}
\end{aligned}$$

$$\begin{aligned}
b_1 &= (n+1)\alpha + n\beta \\
&= (n+1)(2k+1) + n(2m+1) \\
&= 2kn + 2k + n + 1 + 2mn + n \\
&= 2(kn+1+n+mn) + 1 \\
&= \text{odd}
\end{aligned}$$

$$\begin{aligned}
\beta_1 &= (n+1)a - (n+2)b \\
&= (n+1)(2k+1) - (n+2)(2k+1) \\
&= 2kn + 2k + n + 1 - 2kn - 4k - n - 2 \\
&= 2(-k-1) + 1 \\
&= \text{odd.}
\end{aligned}$$

Claim 2:

Each of these number is > 0

$a_1 = (n+2)\alpha + (n+1)\beta$ and $b_1 = (n+1)\alpha + n\beta$ are obviously > 0.

$$\alpha_1 = -na + (n+1)b$$

Since $n = \left[\frac{b}{a-b}\right]$ implies $\frac{b}{a-b} \geq n$

$$\begin{aligned}
b &\geq (a-b)n \\
b &\geq an - bn \\
-an + b + bn &\geq 0 \\
\alpha_1 = -an + (n+1)b &\geq 0
\end{aligned}$$

But α_1 being odd cannot be equal to zero. Consequently $\alpha_1 > 0$.

$$\beta_1 = (n+1)a - (n+2)b$$

Since $n = \left[\frac{b}{a-b}\right]$ implies $n+1 > \frac{b}{a-b} \geq n$

$$(n+1)(a-b) > b$$

$$na + a - nb - b > b$$

$$(n+1)a - (n+2)b = \beta_1 > 0$$

Now we are going to show

$$a_1 \alpha_1 + b_1 \beta_1 = 2u.$$

$$\begin{aligned} a_1 \alpha_1 + b_1 \beta_1 &\\ &= -n(n+2)a\alpha - n(n+1)a\beta + (n+1)(n+2)b\alpha + (n+1)^2 b\beta \\ &\quad + (n+1)^2 2a\alpha + n(n+1)b\beta - (n+1)(n+2)b\alpha - n(n+2)b\beta \\ &= ((n+1)^2 - n(n+2))\,(a\alpha + b\beta) \\ &= a\alpha + b\beta \\ &= 2u. \end{aligned}$$

We also have $a_1 > b_1$. To see that we have,

$$(n+2)\alpha + (n+1)\beta > (n+1)\alpha + n\beta$$

$$n\alpha + 2\alpha + n\beta + \beta > n\alpha + \alpha + n\beta$$

$$a_1 > b_1$$

Now we are going to show $\left[\frac{b_1}{a_1 - b_1}\right] = n.$

$$\begin{aligned} \left[\frac{b_1}{a_1 - b_1}\right] &= \left[\frac{(n+1)\alpha + n\beta}{(n+2)\alpha + (n+1)\beta - (n+1)\alpha - n\beta}\right] \\ &= \left[\frac{n\alpha + \alpha + n\beta}{n\alpha + 2\alpha + n\beta + \beta - n\alpha - \alpha - n\beta}\right] \\ &= \left[\frac{n(\alpha+\beta) + \alpha}{\alpha + \beta}\right] \\ &= \left[\frac{n(\alpha+\beta)}{\alpha+\beta} + \frac{\alpha}{\alpha+\beta}\right] \\ &= \left[n + \frac{\alpha}{\alpha+\beta}\right] = n, \qquad \text{since } \frac{\alpha}{\alpha+\beta} < 1 \end{aligned}$$

If we substitute the value of a_1, α_1, b_1, β_1 in the quadruples (*) , we should have a , b , α , β .

To see that we have

$(n+2)\alpha_1 + (n+1)\beta_1$

$= (n+2)(-na + (n+1)b) + (n+1)((n+1)a - (n+2)b)$

$= -na(n+2) + (n+2)(n+1)b + (n+1)2a - (n+1)(n+2)b$

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

$= a.$

$-na_1 + (n+1)b_1$

$= -n((n+2)\alpha + (n+1)\beta) + (n+1)((n+1)\alpha + n\beta)$

$= -n(n+2)\alpha - n(n+1)\beta + (n+1)^2\alpha + (n+1)n\beta$

$= \alpha(-n(n+2) + (n+1)^2)$

$= \alpha.$

$(n+1)\alpha_1 + n\beta_1$

$=(n+1)((-na) + (n+1)b) + n((n+1)a-(n+2)b)$

$= -na(n+1) + (n+1)^2b + (n+1)na = n(n+2)b$

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

$= b.$

$(n+1)a_1 - (n+2)b_1$

$= (n+1)((n+2)\alpha + (n+1)\beta) - (n+2)((n+1)\alpha + n\beta)$

$= (n+1)(n+2)\alpha + (n+1)^2\beta - (n+2)(n+1)\alpha - (n+2)n\beta$

$= \beta((n+1)^2 - n(n+2))$

$= \beta .$

3) Now we are going to show $\chi(ab) + \chi(a_1b_1) = 0$

For odd v and w we have

$$\begin{aligned}
(v-1)\,(w-1) &\equiv 0 \pmod{4}\\
vw - v - w + 1 &\equiv 0 \pmod{4}\\
vw &\equiv v + w - 1 \pmod{4}
\end{aligned}$$

Hence we have ,

$$a\alpha \equiv a + \quad - 1 \pmod{4}$$

$$b\beta \equiv b + \quad - 1 \pmod{4}$$

$$\begin{aligned}
(a + \alpha - 1) + (b + \beta - 1) &\equiv a\alpha + b\beta \pmod{4}\\
&\equiv 2u \pmod{4}\\
&\equiv 2 \pmod{4}
\end{aligned}$$

$$\begin{aligned}
(a + \alpha - 1) + (b + \beta - 1) &\equiv 2 \pmod{4}\\
a + b + \alpha + \beta &\equiv 0 \pmod{4}
\end{aligned}$$

$$\begin{aligned}
ab + a_1b_1 &\equiv (a + b - 1) + (a_1 + b_1 - 1)\\
&\equiv (a+b-1)+((n+2)\alpha + (n+1)\beta + (n+1)\alpha + n\beta - 1)\\
&\equiv a+b + n\alpha + 2\alpha + n\beta + \beta + n\alpha + \alpha + n\beta + 2\\
&\equiv a + b + (2n + 3)\alpha + (2n+1)\beta + 2\\
&\equiv 2n\,(\alpha + \beta) + a + b + \alpha + \beta + 2 + 2\\
&\equiv 0 \pmod{4}
\end{aligned}$$

This implies $ab + a_1b_1 \equiv 0 \pmod{2}$ which

implies $\chi(ab) = -\chi(a_1b_1)$

This complete the proof of the theorem that

$A(u) = \sigma(u)$.

Corollary 3.7:

If u is a positive odd integer, then the number of all possible representation of 4u as a sum of four odd squares (positive or negative) is ,

$V(4u) = 16\sigma(u)$

Proof:

In the proof of the theorem we have seen that the number of positive odd solutions of

$$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2 \text{ is}$$

$$A(u) = \sum_{2h+2m = 4u} \frac{U(2h)}{4} \quad \frac{U(2m)}{4},$$

where U(2h) and U(2m) is the number of positive solutions of $u_1^2 + u_2^2 = 2h$ and $u_3^2 + u_4^2 = 2m$ respectively.

Now if $v = 2k+1$ is odd, then in the equation $2v = x^2 + y^2$, x and y must be odd. For $2(2k+1) = x^2 + y^2$, then both x and y are odd.

For assume x and y are even where $x = 2h$ and $y = 2n$, then $x^2 + y^2 = 4(h^2 + n^2)$

But $4k+2 = 4(h^2+n^2)$ and $4 \nmid 4k+2$ but $4 \mid 4(h^2+n^2)$.

Contradiction.

If we assume one of the integer is even, say $x = 2s$ and one is odd say $y = 2b + 1$, then we have,

$$\begin{aligned} x^2 + y^2 &= 4s^2 + 4b^2 + 4b + 1 \\ &= 4(s^2 + b^2 + b) + 1 \end{aligned}$$

But $4k + 2 = 4z + 1$ where $z = (s^2 + b^2 + b)$

Therefore both x and y must be odd.

Thus the number of solutions of equation $2v = x^2 + y^2$ equals four times the number of positive solutions in which x and y are odd positive number. Hence the total number of odd solution of

$$4u = u_1^2 + u_2^2 + u_3^2 + u_4^2 \text{ is}$$

$$V(4u) = \sum_{2h+2m=4u} 4\left(\frac{U(2h)}{4}\right) 4\left(\frac{U(2m)}{4}\right)$$

$$= 16 \sum_{2h+2m=4u} \frac{U(2h)}{4} \qquad \frac{U(2m)}{4}$$

$$= 16\,\sigma(u)$$

Theorem 3.8:

$$r_4(2u) = 3r_4(u)$$

Proof:

Consider the equation;

1) $2u = x_1^2 + x_2^2 + x_3^2 + x_4^2$

Since 2u is even two of the x_k must be even and two are odd.

Assume all the x_k are even.

$$2u = 2k_1^2 + 2k_2^2 + 2k_3^2 + 2k_4^2$$

$$= 2(2k_1^2 + 2k_2^2 + 2k_3^2 + 2k_4^2 + 2k_4^2)$$

$$u = 2(k_1^2 + k_2^2 + k_3^2 + k_4^2)$$

Contradiction since u is odd.

Assume all the x_k are odd.

$$2u = (2k_1 + 1)^2 + (2k_2+1)^2 + (2k_3 + 1)^2 + (2k_4+1)^2$$

$$= 2(2k_1^2 + 2k_1 + 2k_2^2 + 2k_2 + 2k_3^2 + 2k_3 + 2k_4^2 + 2k_4 + 2)$$

$$u = 2(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2 + k_3 + k_4^2 + k_4 + 1)$$

Contradiction since u is odd.

Similarly if three of the x_k are even(or odd) and one odd(or even) , then we would have contradiction.

Therefore the number of solution for the equation

$$2u = x_1^2 + x_2^2 + x_3^2 + x_4^2$$ in which x_1 and x_2 are even and x_3 and x_4 are odd is,

$$\frac{1}{{}^{2}C^{4}} r_4(2u) = \frac{1}{6} r_4(2u)$$

Let $y_1 = (x_1 + x_2)/2$

$y_2 = (x_1 - x_2)/2$

$y_3 = (x_4 + x_4)/2$

$y_4 = (x_3 - x_4)/2$

Now consider the equations,

2) $u = y_1^2 + y_2^2 + y_3^2 + y_4^2$

$y_2 + y_1 \equiv 0 \pmod{2}$

$y_3 + y_4 \equiv 0 \pmod{2}$

Claim:

a) Any solution of 2) is a solution of 1)

b) Any solution of 1) is a solution of 2)

a) Let $\overline{y_1}$, $\overline{y_2}$, $\overline{y_3}$, $\overline{y_4}$ be a solution of 2) and

let $x_1 = \overline{y_1} + \overline{y_2}$,

$x_2 = \overline{y_1} - \overline{y_2}$,

$x_3 = \overline{y_3} + \overline{y_4}$,

$x_4 = \overline{y_3} - \overline{y_4}$,

then $x_1^2 + x_2^2 + x_3^2 + x_4^2$

$= (\bar{y}_1+\overline{y_2})^2 + (\bar{y}_1 - \bar{y}_2)^2 + (\bar{y}_3 + \bar{y}_4)^2 + (\bar{y}_3 - \bar{y}_4)^2$

$= (\bar{y}_1^2 + \bar{y}_2^2 + 3\bar{y}_1\bar{y}_2) + (\bar{y}_1^2 + \bar{y}_2^2 - 2\bar{y}_1\bar{y}_2)$

$+(\overline{y}_3^2 + \overline{y}_4^2 + 2\overline{y}_3\overline{y}_4) + (\overline{y}_3^2 + \overline{y}_4^2 - 2\overline{y}_3\overline{y}_4)$

$= 2(\overline{y}_1^2 + \overline{y}_2^2 + \overline{y}_3^2 + \overline{y}_4^2)$

$= 2u.$

$x_1 = \overline{y}_1 + \overline{y}_2 \equiv 0 (\mathrm{mod} 2)$ implies x_1 is even.

$x_2 = \overline{y}_1 - \overline{y}_2$

$= (2k - \overline{y}_2) - \overline{y}_2$ since $\overline{y}_2 + \overline{y}_2 = 2k$ for some k

$= 2(k - \overline{y}_2)$ implies x_2 is even.

$x_3 = \overline{y}_3 + \overline{y}_4 \equiv 1 (\mathrm{mod} 2)$ implies x_3 is odd

$x_4 = \overline{y}_3 - \overline{y}_4$

$= (2k+1 - \overline{y}_4) - \overline{y}_4$ since $\overline{y}_3 + \overline{y}_4 - 1 = 2k$ for some k

$= 2(k - \overline{y}_4) + 1$ implies x_4 is odd.

b) Let x_1, x_2, x_3, x_4 be a solution of 1). And let

$y_1 = (x_1 + x_2)/2$

$y_2 = (x_1 - x_2)/2$

$y_3 = (x_3 + x_4)/2$

$y_4 = (x_4 - x_4)/2$

First note that all y_1, y_2, y_3, y_4 are integers.

$y_1 = (2k_1 + 2k_2)/2 = k_1 + k_2$ is integer

$y_2 = (2(k_1 - k_2))/2 = k_1 - k_2$ is integer.

$y_3 = [(2k_1 + 1) + (2k_2 + 1)]/2 = 2(k_1 + k_2 + 1)$ is integer

$y_4 = [(2k_1 + 1) - (2k_2 + 1)]/2 = [2(k_1 - k_2)]/2$ is integer

Now $y_1^2 + y_2^2 + y_3^2 + y_4^2$

$= [(x_1 + x_2)/2]^2 + [(x_1 - x_2)/2]^2 + [(x_3 + x_4)/2]^2 + [(x_3 - x_4)/2]^2$

$= (1/4)(2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2)$

$= (1/2)(x_1^2 + x_2^2 + x_3^2 + x_4^2)$

$= (1/2)(2u) = u.$

$y_1 + y_2 =(x_1 + x_2)/2 + (x_1 - x_2)/2 = (2x_1)/2 = x_1$

$= 2k \equiv 0 \pmod 2$

$y_3 + y_4 = (x_3 + x_4)/2 + (x_3 - x_4)/2 = (2x_3)/2 = x_3$

$= 2k + 1 \equiv 1 \pmod 2$

Therefore $(1/6)\, r_4(2u)$ is also the number of solution of the equation $u = y_1^2 + y_2^2 + y_3^2 + y_4^2$

In the equation $u = y_1^2 + y_2^2 + y_3^2 + y_4^2$, since u is odd , $u \equiv 1 \pmod 4$ or $u \equiv 3 \pmod 4$ since all the integers can be written in the form of 4k , 4k+1, 4k+2, 4k+3.

Case1:

If $u \equiv 1 \pmod 4$, one of y_k must be odd. And this can be only y_3 or y_4 since $y_3 + y_4 \equiv 1 \pmod 2$ and $y_1 + y_2 \equiv 0 \pmod 2$. Therefore in this case we only have half of the number of possible solutions.

Case2:

If $u \equiv 3 \pmod 4$, one of the y_k must be even and this too can be only y_3 or y_4 since $y_3 + y_4 \equiv 1 \pmod 2$ and $y_1 + y_2 \equiv 0 \pmod 2$.Hence in this case , we only have half of the number of possible solution. Thus the total number of solutions of the equation $u = y_1^2 + y_2^2 + y_3^2 + y_4^2$ with the restriction $y_1 + y_2 \equiv 0 \pmod 4$ and $y_3 + y_4 \equiv 1 \pmod 2$ is $(1/2)\, r_4(u)$ where $r_4(u)$ is the number of solution of the above equation without any restriction.

Therefore we have,

$$(1/6)\, r_4(2u) = (1/2)\, r_4(u)$$

implies $r_4(2u) = 3\, r_4(u)$

Theorem 3.9:

$$r_4(u) = 8\sigma(u)$$

$$r_4(2^h u) = 24\sigma(u) \text{ for } h > 0$$

Remark.

This determines $r_4(n)$ for $n > 0$, specially for odd n, $r_4(n)$ must be 8 times the sum of positive divisors of n,and for even n, 24 times the sum of the odd positive divisors of n.

Proof:

For $n > 0$, we have $r_4(2n) = r_4(4n)$

For consider the equation,

1) $4n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ then either all the x_k are even or all the x_k are odd.

Assume two of the x_k are odd and two are even.

$$\begin{aligned} 4n &= (2a+1)^2 + (2b+1)^2 + (2c)^2 + (2d)^2 \\ &= 4a^2 + 4a + 4b^2 + 4b + 4c^2 + 4d^2 + 2 \\ &= 4(a^2 + a + b^2 + b + c^2 + d^2) + 2 \\ 4n &= 4(a^2 + a + b^2 + b + c^2 + d^2) + 2 \end{aligned}$$

which is impossible.

Assume three of the x_k are odd and one is even.

$$\begin{aligned} 4n &= (2a+1)^2 + (2b+1)^2 + (2c+1)^2 + (2d)^2 \\ &= 4(a^2 + a + b^2 + b + c^2 + c + d^2) + 3 \\ 4n &= 4(a^2 + a + b^2 + b + c^2 + c + d^2) + 3 \end{aligned}$$

which is impossible.

For the case where three of the x_k are even and one is odd, will result in $4n = 4(a^2 + b^2 + c^2 + d^2 + d) + 1$ which is also impossible.

Consider the equation,

2) $2n = y_2^2 + y_2^2 + y_3^2 + y_4^2$

$$\text{where } y_1 = (x_1 + x_2)/2 \ , \ y_2 = (x_1 - x_2)/2 \ ,$$
$$y_3 = (x_3 + x_4)/2 \ , \ y_4 = (x_3 - x_4)/2$$

Claim:

a) Any solution of 2) is a solution of 1)

b) Any solution of 1) is a solution of 2)

a) Let $\overline{y_1}$, $\overline{y_2}$, $\overline{y_3}$, $\overline{y_4}$ be a solution of 2) and

let $x_1 = \overline{y_1} + \overline{y_2}$, $\quad x_2 = \overline{y_1} - \overline{y_2}$

$x_3 = \overline{y_3} + \overline{y_4}$, $\quad x_4 = \overline{y_3} - \overline{y_3}$

Now $x_1^2 + x_2^2 + x_3^2 + x_4^2$

$= (\overline{y_1} + \overline{y_2})^2 + (\overline{y_1} - \overline{y_2})^2 + (\overline{y_3} + \overline{y_4})^2 + (\overline{y_3} - \overline{y_4})^2$

$= 2(\overline{y_1}^2 + \overline{y_2}^2 + \overline{y_3}^2 + \overline{y_4}^2)$

$= 2\ (2n) = 4n.$

b) Let x_1, x_2, x_3, x_4 be a solution of 1) and

let $y_1 = (x_1 + x_2)/2$, $\quad y_2 = (x_1 - x_2)/2$

$y_3 = (x_3 + x_4)/2$, $\quad y_4 = (x_3 - x_3)/2$

Now $y_1^2 + y_2^2 + y_3^2 + y_4^2$

$= [(x_1 + x_2)/2]^2 + [(x_1 - x_2)/2]^2 + [(x_3 \ \ x_4)/2]^2$

$\quad + [(x_3 - x_4)/2]^2$

$= (1/4)(2x_1^2 + 2x_2^2 + 2x_3^2 + 2x_4^2)$

$= (1/2)(x_2^2 + x_2^2 + x_3^2 + x_4^2)$

$= (1/2)(4n) = 2n.$

Therefore $r_4(2n) = r_4(4n)$.

Furthermore we have $r_4(4u) = 16\sigma(u) + r_4(u)$

For in the equation,

$$4u = x_1^2 + x_2^2 + x_3^2 + x_4^2 ,$$

if all the x_k are even, the equation is then equivalent to

$$u = z_1^2 + z_2^2 + z_3^2 + z_4^2 , \quad z_k = x_k/2$$

Therefore the number of solutions is $r_4(u)$.

If the x_k are all odd then the number of solutions is $16\sigma(u)$ by corollary (3.7).

So far we have

$$\begin{aligned} r_4(2u) &= 3r_4(u) , \\ r_4(2n) &= r_4(4n) \text{ and} \\ r_4(4u) &= 16\sigma(u) + r_4(u) \end{aligned}$$

It follows that $3r_4(u) = r_4(2u) = r_4(4u) = 16\sigma(u) + r_4(u)$

$$\begin{aligned} 3r_4(u) &= 16\sigma(u) + r_4(u) \\ 2r_4(u) &= 16\sigma(u) \\ r_4(u) &= 8\sigma(u). \end{aligned}$$

And from theorem (3.8) $r_4(2u) = 3r_4(u)$ and

$$r_4(u) = 8\sigma(u)$$

It follows that $3r_4(u) = 3(8\sigma(u)) = 24\sigma(u)$

$$r_4(2u) = 24\sigma(u)$$

Finally for $h>0$, from $r_4(2n) = r_4(4n)$ and $_4(2u) = 24\ (u)$ it follows that $r_4(2^h u) = {}_4(2u) = 24\sigma(u)$.

Examples:

As an illustration of Theorem 3.9, consider $u = 7$.

Then $\sigma(7) = 1 + 7 = 8$, $r_4(7) = 8\sigma(7) = 8(8) = 64$

different representations of 7.

$7 = 2^2 + 1^2 + 1^2 + 1^2$. The four summands have 4 distinct permutations and each nonvanishing integer has two choices of sign $(\underline{+}1)^2$ and $(\underline{+}2)^2$ for a total $2^4 = 16$ different choices of signs. Therefore the total number of representation of 7 is $4.16 = 64$.

Now consider $n = 6 = 2^h.u = 2^1.3$.

$u = 3, \sigma(3) = 1 + 3 = 4$.

$r_4(2^1.3) = 24\,\sigma(3) = 24(4) = 96$.

$6 = 1^2 + 1^2 + 2^2 + 0^2$.

The four summands have 12 distinct permutations and each nonvanishing integer has two choices of signs, for a total $2^3 = 8$. Hence the total representation of 6 is $12.8 = 96$.

5.The Uniqueness of Essentially Distinct Representation

In this section we are going to characterize the positive integers that can be written in exactly one way as a sum of four squares apart from order and sign of the summands.

Let us denote $P_k(n)$ the number of partitions of a positive integer n into k integral squares. The term partition implies that we do not consider distinct two decompositions of n into k squares in which the squares are merely permuted. Thus in this section we are concerned with the problem of finding all integers n such that $P_4(n) = 1$. One of the differences between the number of representation $r_4(n)$ and the number of partitions $P_4(n)$ is that when all squares in a particular partition are different from each other and different from zero; to each such partition there corresponds $c_4 = 4!\ 2^4 = 384$ representations counted by $r_4(n)$. Thus we have $P_4 \geq (r_4(n))/384$.

Theorem 4.22:

The only integers with a single partition into four squares are 1,3,5,7,11,15,23 and $4^a r$ where $a \geq 0$ and $r =$ 2,6,14.

Proof:

First note that if $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ then $4n = (2x_1)^2 + (2x_2)^2 + (2x_3)^2 + (2x_4)^2$. Thus for every partition of n into four squares there corresponds a partition of 4n into four square, hence $P_4(4n) \geq P_4(n)$. Recall that if n_1 is an odd integer then, $r_4(n_1) = 8\sigma(n_1)$ and $r_4(2^k n_1) = 24\sigma(n_1)$, $k \geq 1$
and $r_4(2n) = r_4(4n)$ for any integer n.

Now $P_4(n_1 \geq (r_4(n_1/384) = \sigma(n_1)/48$

$P_4(2n_1) \geq r_4(2n_1)/384 = \sigma(n_1)/16$

$P_4(4n_1) \geq r_4(4n_1)/384 = 24\sigma(n_1) = \sigma(n_1)/16$

Thus if $n \not\equiv 0 \pmod 4$, we have $P_4(n) \geq \sigma(n)/48 \geq (n+1)/48$ so that $P_4(n) > 1$ if $n \geq 48$.

If $n \equiv 4 \pmod 8$, then

$P_4(4n_1) = P_4(n) \geq \sigma(n/4)/16 \geq ((n/4)+1)/16 = (n+4)/64$

In this case $P_4(n) > 1$ if $n \geq 60$.

Thus it is sufficient to examine only the integers $n \not\equiv 0 \pmod 4$ for $n < 48$, $n \equiv 4 \pmod 8$ for $n < 60$ and $n \equiv 0 \pmod 8$. By doing so it turns out that none of the integers $n \equiv 4 (\mathrm{mod} 8)$ leads to $P_4(n) = 1$.

For the case $n \equiv 0 (\mathrm{mod} 4)$, with $n < 48$, we have $P_4(n) = 1$ only for $n = 1,2,3,5,6,7,11,14,15,$and 23.

If $n_1 \in \{1,3,5,7,11,15\}$, we have $4n_1 \leq 60$ which implies $P_4(4n_1) > 1$; hence $P_4(4^a n_1) > 1$ for $a \geq 1$.

For $n_1 = 23$, we have $P_4(4.23) = 3 > 1$.

Hence $P_4(4^a.23) > 1$ for $a \geq 1$.

For the integers $n = 2,6,14$ we have,

$P_4(2) = P_4(6) = P_4(14) = 1$.

Hence $P_4(4^a.2) = P_4(4^a.6) = P_4(4^a.14) = 1$ for $a \geq 1$.

If $n \equiv 0 (\mathrm{mod} 8)$, we write $n = 4^a.2m$, where $2m$ is not a multiple of 8. $P_4(n) = P_4(4^a.2m) = P_4(2m)$.

Thus in order that $P_4(n) = 1$, we must have $2m = 2,6,14$.

Thus the proof is complete.

CHAPTER 4

SUM OF THREE SQUARES

1.Representation Of Integers As Sum Of Three Squares.

In this chapter we consider the Representation of a positive integer as a sum of three squares. Unlike the problem of the Representation of an integer as a sum of two squares and four squares the representation of an integer as the sum of three squares is a much more difficult problem.

The two representation problems are:

1) What integers n can be represented as the sum of three squares?
2) Find a formula for $r_3(n)$, the number of representation of an integer n as a sum of three squares.

In this chapter, we will only consider the first representation problem. For the second problem, due to some difficulties, we will be only able to give formulas for the number of representations of an integer as a sum of three squares.

Diaphantus once stated that in order for the equation $x_1^2 + x_2^2 + x_3^2 = n$ to a have solution, n must not equal to (24k + 7). Later Bachet found that this condition was insufficient and added another condition. It was Fermat who finally succeded in formulating the correct condition for this problem. In 1636, Fermat stated that no integer of the form $8k + 7$ is the sum of three squares.

The first attempt to prove that every integer which is not of the form $4^h(8k+7)$ is representable as the sum of three squares was by Legendre in 1798. In 1801 , Gauss gave a complete proof and obtained a formula for the number of primitive representations for an integer as a sum of three squares. Gauss'proof depended on more difficult results in his extensive theory of quadratic forms. Other proofs have since been given , but none of them can be described as both elementary and simple.

First we state the main result in this chapter;

Main Theorem:

A positive integer n is a sum of three squares if and only if n is not of the $4^h(8k+7)$ where k, h are non-negative integers.

First we are going to show that the condition is necessary, which we state in the next theorem:

Theorem 4.1:

If $n = x_1^2 + x_2^2 + x_3^2$, $n > 0$ then n is not of the form $4^h(8k+7)$ where $h,k \geq 0$.

Proof:

Suppose that there exist natural numbers of the form $4^h(8k+7)$ where $h,k \geq 0$ that are the sum of three square integers.

Let n be the least of them. Then we have

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

We will consider four cases.

Case 1:

One of the integers, say a is odd. Then we have,

$$a^2 + b^2 + c^2 = (2k_1 + 1)^2 + (2k_2)^2 + (2k_3)^2$$
$$= 4k_1^2 + 4k_1 + 1 + 4k_2^2 + 4k_3^2$$
$$= 4(k_1^2 + k_1 + k_2^2 + k_3^2) + 1$$

Hence $a^2 + b^2 + c^2$ is of the form $4t + 1$, and it is different from n.

Case2:

Two of the integers say a,b are odd, then we have

$$a^2 + b^2 + c^2 = (2k_1 + 1)^2 + (2k_2 + 1)^2 + (2k_3)^2$$
$$= 4k_1^2 + 4k_1 \; 1 + 4k_2^2 + 4k_2 + 1 + 4k_3^2$$
$$= 4(k_1^2 + k_1 + k_2^2 + k_2 + k_3^2) + 2$$

Hence $a^2 + b^2 + c^2$ is of the form $4t+2$ and it is different from n.

Case 3:

All of the integers are odd . Then we have $a^2 + b^2 + c^2$ is of the form $4t + 3$ and it is different from n.

Case 4:

All of the integers are even.

Let $a = 2a'$, $b = 2b'$, $c = 2c'$ where a' b' c' are integers.

Hence $4^h(8K+7) = h = (2a')^2 + (2b')^2 + (2c')^2$

$$= 4(a'^2 + b'^2 + c'^2)$$

$$4^h(8k+7) = 4(a'^2 + b'^2 + c'^2)$$

$$4^{h-1}(8k+7) = a'^2 + b'^2 + c'^2$$

Contrary to the choice of n.

Thus we have proved that no natural number of the form $4^h(8k+7)$ where $h,k \geq 0$ can be the sum of three squares. On the other hand the proof that the condition is sufficient , i.e if $n \nmid 4^h(8K+7)$, then n is the sum of three squares is difficult. This is due, to a large extent to the fact that in this case, we do not have identity analogous to Euler's identity which we have used in chapters 2 and 3

In order to prove the condition is sufficient we need first to study some basic facts concerning quadratic forms.

2. Quadratic Forms

Definition 4.1:

A homogeneous polynomial of degree 2 in n variables x_1, $x_2,\dots,x_n$, of the type $Q(x_1,\dots,x_n) = \sum\limits_{i,j=1} a_{ij}x_ix_j$ with integer coefficients a_{ij}, is called an integral quadratic form in n variables (or simply quaratic form). It is convinient to assume that $a_{ij} = a_{ji}$ for all $i,j = 1,\dots,n$. Now if we take into account the symmetry of the coefficients, the quadratic forms look like this:

$$Q(x_1,\dots,x_n)$$
$$= a_{11}x_1^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + \dots\dots + 2a_{1n}x_1x_n$$
$$+ a_{22}x_2^2 + 2a_{23}x_2x_3 + \dots\dots + 2a_{2n}x_2x_3 + \dots + a_{nn}x_n^2$$

From this it follows immediately that the quadratic form can be written in a matrix form:

$$Q(x_1,\dots,x_n) = X^TAX ,$$

where $X = \begin{bmatrix} x_1 \\ x_2 \\ \cdot \\ \cdot \\ x_n \end{bmatrix}$

X^T is the transpose of X and $A = [a_{ij}]$ is the symmetric matrix of the coefficients of $x_i x_j$. It is called the coefficient matrix of $Q(x_1,\ldots x_n)$.

Definition 4.2:

Let $Q(x_1,\ldots,x_n) = X^TAX$ be a quadratic form . The rank of A is called the rank of quadratic form and the determinant of A is called the discriminant of Q in what follows it is denoted by $\Delta(Q)$.

Suppose now that $Q = X^TAX$ is a quadratic form. To simplify the quadratic form, we change the variables $x_1,\ldots x_n$ to new variables $y_1,\ldots y_n$ to obtain another quadratic form $Q_1(y_1,\ldots,y_n) = Y^TA_1Y$ with integral coefficient. First we assume that the old variables are related to the new variables by a linear transformation ,

$$x_i = \sum_{j=1}^{n} c_{ij}y_j$$

where $C = [c_{ij}]$ is a matrix with integral coefficient and det $C = 1$. In matrix notation this linear transformation can be written as $X = CY$. Since the det $C = 1$, the linear transformation is invertible and $Y = BX$, where $B = [b_{ij}]$ is a matrix with the $b_{ij's}$ also integers. Now if we replace the $x_{i's}$ in the quadratic form $Q(x_1,\ldots x_n) = X^TAX$ by $X = CY$ we obtain another quadratic form $Q_1(y_1,..,y_n) = (CY)^TA(CY) = Y^T(C^TAC)Y$. Quadratic forms that are related like Q and Q_1 i.e that are transformed into each other by linear transformation X = CY, with $C = \left[c_{ij}\right]$ is a matrix with integer coefficient and det C = 1, are said to be equivalent to each other , in symbols it is written $Q \backsim Q_1$.

The concept of equivalent forms is important enough to reformulate in the following definition:

Definition 4.3:

Let $Q(x_1,..,x_n) = X^TAX$ and $Q_1(y_1,..,y_n) = Y^TDY$

be two quadratic forms, then we say that Q is equivalent to Q_1 if there exist a matrix $C = [c_{ij}]$ with integer coefficients and det C = 1 such that $D = C^TAC$.

Theorem 4.2:

The relation of two quadratic forms being equivalent is an equivalence relation.

Proof:

1) Reflexive : $Q \backsim Q$

$$Q(x_1,...,x_n) = X^TAX \backsim Q(x_1,..,x_n) = X^TAX$$

Recall two quadratic forms $Q = X^TAX$ and $Q' = Y^TDY$ are equivalent if $D = C^TAC$ for some matrix C with det C =1.

Let $C = I = \begin{bmatrix} 1 & 0 & 0 & 0.....0 \\ 0 & 1 & .... & \\ .... & & & \\ 0 & & & 1 \end{bmatrix}$

Then $A = C^TAC$ and $Q \backsim Q$

2) Symmetry : If $Q \backsim Q_1$ then $Q_1 \backsim Q$

Since $Q = X^TAX \backsim Q_1 = Y^TDY$ then $D = C^TAC$ where $\det C = 1$.

Now , $A = (C^{-1})^TD(C^{-1})$ and $\det C^{-1} = (1/\det C) = 1$.

Hence $Q_1 = Y^TDY \backsim Q = X^TAX$.

3)Transitivity: If $Q \backsim Q_1$ and $Q_1 \backsim Q_2$ then $Q \backsim Q_2$.

$$Q(x_1,\ldots,x_n) = X^TAX \backsim Q_1(y_1,\ldots,y_n) = Y^TDY$$

where $D = C^TAC$ for some metrix C with $\det C = 1$.

$$Q_1(y_1,..,y_n) = Y^TDY \backsim Q_2(z_1,..,z_n) = Z^TBZ$$

where $B = P^TDP$ for some metrix P with $\det P = 1$.

Now $Q(x_1,..,x_n) = X^TAX \backsim Q_2(z_1,..,z_n) = Z^TBZ$

Since
$$\begin{aligned} B &= P^TDP \\ &= P^T(C^TAC)P \\ &= (P^TC^T)A(CP) \\ &= (CP)^TA(CP) \end{aligned}$$

$B = (CP)^TA(CP)$ and $\det(CP) = (\det C)(\det P) = 1$.

Example:

Let $Q(x_1,x_2) = x_1^2 + 2x_1x_2 + x_2^2$

$$= \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}^T \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

Let $X = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix}$,

then $x_1 = y_1$, $x_2 = y_1 + y_2$

$$\begin{aligned} Q_1(y_1,y_2) &= y_1^2 + 2(y_1 + y_2) + (y_1 + y_2)^2 \\ &= y_1^2 + 2y_1^2 + 2y_1y_2 + y_1^2y_2^2 + 2y_1y_2 \\ &= 4y_1^2 + 4y_1y_2 + y_2^2. \end{aligned}$$

Theorem 4.3:

If $Q \backsim Q_1$ then $\Delta(Q) = \Delta(Q_1)$

Proof:

$Q(x_1,..,x_n) = X^TAX \quad Q_1(y_1..,y_n) = Y^TDY$

$D = C^TAC$ for some metric C with $\det C = 1$.

$$\begin{aligned}\Delta(Q_1) = \det D &= \det(C^TAC) \\ &= (\det C^T)(\det A)(\det C) \\ &= (\det C)(\det A)(\det C) \\ &= 1(\det A)1 \\ &= \Delta(Q).\end{aligned}$$

Definition 4.4:

A quadratic form $Q(x_1,..,x_n)$ is said to represent the number m if there exist integers $x'_1,..,x'_n$ such that $Q(x_1',...,x_n') = m$.

Theorem 4.4:

If $Q \backsim Q_1$ then Q and Q_1 represent the same numbers.

Proof:

Since $Q = X^TAX \quad Q_1 = Y^TDY$ then $D = C^TAC$ for some matrix C where $\det C = 1$.

Assume m is representable by Q, then there exist integers $x_1',...,x_n'$ such that $Q(x_1',...,x_n') = X'^TAX' = m$

where $X' = \begin{bmatrix} x_1' \\ x_2' \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ x_n' \end{bmatrix}$

Let $Y' = C^{-1}X'$,

$$\begin{aligned} \text{then } Q_1(y'_1,..,y_n) &= Y'^TDY' \\ &= (C^{-1}X')^TD(C^{-1}X') \\ &= X'^T(C^{-1}DC^T)X' \\ &= X'^T(A)X' \\ &= Q(x_1',..,x_n') = m. \end{aligned}$$

Example:

$Q(x_1,x_2) = x_1^2 + 2x_1x_2 + x_2^2$

$Q_1(y_1,y_2) = 4y_1^2 + 4y_1y_2 + y_2^2$

$Q \backsim Q_1$ since $D = C^TAC$ and $C = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$ and det $C = 1$.

$m = 25$ is representable by $Q(x_1,x_2)$ since for $x'_1 = 2$, $x'_2 = 3$ we have $Q(2,3) = 2^2 + 2(2)(3) + 3^2 = 25$.

$m = 25$ is also representable by $Q_1(y_1,y_2)$,

for $y'_1 = 2$, and $y'_2 = 1$ we have,

$4(2)^2 + 4(2)(1) + 1^2 = 25$.

Remark:

The converse of this theorem is not true, that is it is possible for an integer m to be represented by two inequivalent quadratic forms.

Example:

Let $Q(x_1,x_2) = x_1^2 + 161x_2^2$

$Q_1(y_1,y_2 = 9y_1^2 + 2y_1y_2 + 18y_2^2$

$m = 162$ is represented by both Q and Q_1 since $Q(1,1) = 162$ and $Q_1(0,3) = 162$.

But Q and Q_1 are not equivalent. Assume the contrary i.e $Q \backsim Q_1$ then $Q = X^T AX$ and $Q_1 = Y^T DY$ where $D = C^T AC$ for some matrix C with det $C = 1$.

Let $C = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$ and det $C = 1$

Now we have $D = C^T AC$

$$\begin{bmatrix} 9 & 1 \\ 1 & 18 \end{bmatrix} = \begin{bmatrix} x & y \\ z & w \end{bmatrix}^T \begin{bmatrix} 1 & 0 \\ 0 & 161 \end{bmatrix} \begin{bmatrix} x & y \\ x & y \end{bmatrix}$$

$x^2 + 161z^2 = 9$

$xy + 161zw = 1$

$y^2 + 161w^2 = 18$ and also we have $xw - yz = 1$

If we solve the above system of equations, the first equation requires $z = 0$, $x = \pm 3$, the second then yields $y = x^{-1} = \pm 1/3$ and the third equation $w^2 = \pm 1/3$. With an appropriate of sign, we find also $xw - yz = 1$ but $y, w \notin Z$. Therefore Q and Q_1 are not equivalent.

<u>Definition 4.5:</u>

The Quadratic form $Q(x_1,..,x_n)$ is said to be <u>positive definite</u> if $Q(x_1,..,x_n) > 0$ for all integral n-tuples $(x_1,..,x_n) \neq (0,0,..,0)$. $Q(x_1,..,x_n)$ is said to be <u>negative definite</u> if $Q(x_1,..,x_n) < 0$ for all integral n-tuples $(x_1,..,x_n) \neq (0,0,..,0)$.

<u>Example:</u>

$Q(x,y) = x^2 + y^2$ positive definite

$Q(x,y) = -2x^2 - 2y^2$ negative definite

$Q(x,y) = x^2 - y^2$ indefinite

Theorem 4.5:

If $Q \backsim Q_1$ then Q is positive (or negative) definite if and only if Q_1 is positive (or negative) definite.

Proof:

Since $Q \backsim Q_1$ implies Q_1 and Q represent the same number. Therefore it follows that if Q is positive definite then Q_1 is also positive definite.

Reduction of positive definite forms:

We shall be concerned mainly with both binary quadratic forms (i.e forms in two variables) and ternary quadratic forms (i.e forms in three variables).

Now we will restrict ourselves to the study of such forms.

For convenience we shall write the binary quadratic form as $Q(x,y) = ax^2 + 2bxy + cy^2$. The discriminant of Q is,

$$\Delta(Q) = \begin{vmatrix} a & b \\ b & c \end{vmatrix} = ac - b^2$$

Theorem 4.6:

A binary quadratic form $Q(x,y) = ax^2 + 2bxy + cy^2$ is positive definite if and only if both $a>0$ and $\Delta(Q) = ac - b^2 > 0$.

Proof:

We consider all possible values of a and $\Delta(Q)$.

1) If $a \leq o$ then $Q(1,0) = a \leq 0$

Hence $Q(x,y)$ is not positive definite.

2) If $a > 0$ and $\Delta(Q) \leq 0$, then

$$Q(-b,a) = ab^2 - 2b^2a + ca^2$$

$$= -ab^2 + ca^2 = a(ac-b^2) = a.\Delta(Q) \leq 0.$$

Hence $Q(x,y)$ is not positive definite.

3) If $a > 0$ and $\Delta(Q) > 0$ then

$$a.Q(x,y) = a(ax^2 + 2bxy + cy^2)$$

$$= a^2x^2 + 2bxy + acy^2$$

$$= (ax + by)^2 + (ac-b^2)y^2$$

$$= (ax + by)^2 + \Delta(Q)y^2$$

But $Q(x,y) \leq 0$ only if $(ax + by)^2 + \quad (Q)y^2 \leq 0$ for any x,y. Hence we must have,

$$ax + by = 0$$

$$y = 0$$

Therefore $x = y = 0$ and $Q(x,y)$ is positive definite.

Theorem 4.7:

In every class of a positive definite binary forms there is a form for which $2|b| \leq a \leq c$. Such a form is called reduced.

Proof:

Let $Q(x,y) = a_0x^2 + 2b_0xy + c_0y^2$ belong to a class of a positive definite form. Let n be the smallest positive number representable by this form (and hence any form of the class). Then for some integer r,t we have

$n = a_0r^2 + 2b_0rt + c_0t^2$.

Claim: The g.c.d $(r,t) = 1$

For if $(r,t) = v > 1$ then $v^2 | n$.

Hence $\frac{n}{v^2} = a_o\left(\frac{r}{v}\right)^2 + 2b_o\left(\frac{r}{v}\right)\left(\frac{t}{v}\right) + c_o\left(\frac{t}{v}\right)^2$

But $n\ {}^2/v^2 < n$ is representable by the form, which contradict that n is the smallest number representable by the form. Thus we must have g.c.d$(r,t) = v = 1$. Now since $(r,t) = 1$, there exist integers s, u such that $ru - st = 1$. If u_o, s_o is any solution of $ru - st = 1$, then the general solution is $u = u_o + ht$, $s = s_o + hr$ where h is any integer.

Now let $X = \begin{bmatrix} x \\ y \end{bmatrix}$, $X' = \begin{bmatrix} x' \\ y' \end{bmatrix}$ $C = \begin{bmatrix} r & s \\ t & u \end{bmatrix}$ with det $C = 1$

Consider the transformation $X = CX'$, then by substituting in the form $Q(x,y)$ we have $Q'(x',y') = X'^T(C^TAC)X'$ and hence $Q \backsim Q'$, that is Q and Q' are in the same equivalent class. Let $Q'(x',y') = ax'^2 + 2bx'y' + cy'^2$.

By direct substitution of CX' for X in Q(x,y) we have,

$a = n$ and $b = s(a_or + b_ot) + u(b_or + c_ot)$,

$b = s_o(a_or + b_ot) + u_o(b_or + c_ot)$

$+ h(r(a_or + b_ot) + t(b_or + c_ot)$

Now since the coefficient of h is $a_or^2 + 2b_ort + c_ot^2 = n$ b takes on all values in a certain residue class mod n; hence h may be selected in such a way $2|b| \leq a |b| \leq a/2$ Since c can be represented by the form $Q'(x',y')$, $c = Q'(0,1)$, we have $a \leq c$. This complete the proof.

Proof:

Since $a \leq c$ then by multiplying by $a \geq 0$, we have

$a^2 \leq ac = b^2 + \Delta(Q) \leq (a^2/4) + \Delta(Q)$

this implies $(3/4)a^2 \leq \Delta(Q)$, and $a \leq (2/\sqrt{3})\ \Delta(Q)$.

Corollary 4.9:

Every positive definite binary form having discriminant 1 is equivalent to the form $x'^2 + y'^2 = Q'(x',y')$

Proof:

By the previous corollary , every such form is equivalent to a form for which $0 \leq 2|b| \leq a \leq (2\sqrt{3})$

this implies $0 \leq |b| \leq (a/2) \leq (1/\sqrt{3})$,

and hence $a = 1$, $b = 0$, $c = 1$.

Therefore $Q'(x',y') = x'^2 + y'^2$.

Theorem 4.10:

A ternary quadratic form $Q(x_1,x_2,x_3) = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ is positive definite if and only if all the following hold:

$$d = \Delta(Q) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix} > 0 ,$$

$$b = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0, \text{ and } a_{11} > 0$$

Moreover if $Q(x_1,x_2,x_3)$ is positive definite , then we have $a_{11}Q = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + K(x_2,x_3)$ where $K(x_2,x_3)$ is the binary positive definite form,

$$K(x_2,x_3) = (a_{11}a_{22} - a_{12}^2)x_2^2 + 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3$$
$$+ (a_{11}a_{33} - a_{13}^2)x_3^2$$

Proof:

By completing $a_{11}Q(x_1,x_2,x_3)$ to a square we have

$$a_{11}Q(x_1,x_2,x_3)$$
$$= a_{11}^2\ x_1^2 + 2a_{11}a_{13}x_1x_3 + a_{11}a_{22}x_2^2$$
$$+ 2a_{11}a_{23}x_2x_3 + a_{11}a_{33}x_3^2$$
$$= (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + (a_{11}a_{22} - a_{12}^2)x_2^2$$
$$+ 2(a_{11}a_{23} - a_{12}a_{13})x_2x_3 + (a_{11}a_{33} - a_{13}^2)x_3^2$$
$$= (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + K(x_2,x_3)$$

$$\Delta(K(x_2,x_3)) = \begin{vmatrix} a_{11}a_{22} - a_{12}^2 & a_{11}a_{23} - a_{12}a_{13} \\ a_{11}a_{23} - a_{12}a_{13} & a_{11}a_{33} - a_{13}^2 \end{vmatrix}$$
$$=(a_{11}a_{22} - a_{12}^2)(a_{11}a_{33} - a_{13}^2) - (a_{11}a_{23} - a_{12}a_{13}$$
$$= a_{11}(a_{11}a_{22}a_{33} - a_{11}a_{23}^2 + 2a_{12}a_{13}a_{23} - a_{12}^2a_{33} - a_{12}^2a_{22})$$
$$= a_{11}\ \ (Q(x_1x_2x_3))$$

Thus $Q(x_1,x_2,x_3)$ is positive definite if and only if $K(x_2,x_3)$ is positive definite and $a_{11} > 0$.

Clearly if $a_{11} \leq 0$, then $Q(1,0,0) = a_{11} \leq 0$ and Q is not positive definite.

Now if $a_{11} > 0$ and $K(x_2,x_3)$ is not positive definite, then $K(x_2',x_3') \leq 0$ for some x_2',x_3' not both of which zero. Then also $K(x_2'',x_3'') \leq 0$ with $x_2'' = a_{11}x_2'$and $x_3'' = a_{11}x_3'$. Let $x_1'' = -a_{11}^{-1}(a_{12}x_2'' + a_{13}x_3'')$.

Clearly x_1'' is an integer,also $a_{11}x_1'' + a_{12}x_2'' + a_{13}x_3'' = 0$.

Thus for x_1'',x_2'',x_3'' we have

$a_{11}Q(x_1'',x_2'',x_3'') = 0^2 + K(x_2'',x_3'') \leq 0$

Hence $Q(x_1'',x_2'',x_3'') \leq 0$

On the other hand if $K(x_2,x_3)$ is positive definite and $a_{11} > 0$, but $Q(\overline{x_1},\overline{x_2},\overline{x_3}) \leq 0$ for some $\overline{x_1},\overline{x_2},\overline{x_3}$ not all of which zero then since $a_{11}Q(x_1,x_2,x_3)$

$= (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + K(\overline{x_2},\overline{x_3}) \geq K(\overline{x_2},\overline{x_3})$

We have $K(\overline{x_2},\overline{x_3}) \leq a_{11}Q(x_1,x_2,x_3) \leq 0$

Hence $\overline{x_2} = \overline{x_3} = 0$ and $a_{11}\overline{x_1}^2 \leq 0$ which implies $\overline{x_1} = 0$.

That contradict that not all $\overline{x_1}$, $\overline{x_2}$ and $\overline{x_3}$ are zero.

Now $K(\overline{x_2},\overline{x_3})$ is positive definite if and only if both

$b = a_{11}a_{22} - a_{12}^2 > 0$ and $\Delta(K(x_2,x_3)) > 0$

but $\Delta(K(x_2,x_3)) = a_{11}\Delta(Q(x_1,x_2,{}_3))$,

thus $K(x_2,x_3)$ is positive definite if and only if both

$b = a_{11}a_{22} - a_{12}^2 > 0$ and $\Delta(Q(x_1,x_2,x_3)) = d > 0$.

Lemma 4.01:

Let $C = [a_{ij}]$ be a matrix with integer coefficients. If $g.c.d(c_{11},c_{21}) = 1$, then the six remaining numbers c_{ij} can be chosen in such a way that $\det C = 1$.

Proof:

Let us set $g.c.d(c_{11},c_{21}) = g$.

Since $g.c.d\ (c_{11},c_{21}) = g$ we can choose integers c_{12} and c_{22} in such a way that $c_{11}c_{22} - c_{12}c_{21} = g$

Also since $g.c.d(g,c_{31}) = 1$ we can choose integer u and v such that $gu - c_{31}v = 1$.

Now let $C = \begin{bmatrix} c_{11} & c_{12} & (c_{11}/g)v \\ c_{21} & c_{22} & (c_{21}/g)v \\ c_{31} & 0 & u \end{bmatrix}$

$$\det C = c_{31}\ (c_{12}c_{21} - c_{11}c_{22})\ v + (c_{11}c_{22} - c_{12}c_{21})u$$
$$= -c_{31}v + gu = 1.$$

Example:

Let $c_{11} = 2$, $c_{21} = 4$, $c_{31} = 5$

Hence we have g.c.d$(c_{11}, c_{21}) = (2,4) = g = 2$ and

g.c.d$(g, c_{31}) = (2,5) = 1$.

We can choose integer c_{12} and c_{22} such that

$$c_{11}c_{22} - c_{12}c_{21} = g$$

implies $2c_{22} - c_{12}.4 = 2$

implies $c_{22} = 3$, $c_{12} = 1$

We can also choose integer u and v such that

$gu - c_{31}v = 1$ implies $2u = 5v = 1$ and hence $u = 3$, $v = 1$.

Then $C = \begin{bmatrix} 2 & 1 & 1 \\ 4 & 3 & 2 \\ 5 & 0 & 3 \end{bmatrix}$.

Theorem 4.11:

Every class of positive definite ternary quadratic forms $Q(x_1, x_2, x_3)$ contains at least one reduced form with

$0 < a_{11} \leq (4/3)\sqrt[3]{d}$, $2\ |a_{12}| \leq a_{11}$, $2\ |a_{13}| \leq a_{11}$

where $d = \Delta(Q)$ the discriminant of Q.

Proof:

Let $Q(x_1, x_2, x_3) = \sum_{i,j=1}^{3} a_{ij}x'_i x'_j$ be a fixed ternary form belonging to the class . Let a be the smallest positive integer that can be represented by Q and consequently by any form belonging to the class. Then for suitable integers c_{11}, c_{21}, c_{31} we have $a = Q(c_{11},c_{21}, c_{31})$.

<u>Claim:</u> $\quad$ g.c.d$(c_{11},c_{21},c_{31}) = 1$.

If g.c.d $(c_{11},c_{21},c_{31}) = v > 1$ then $C = (a/v^2) < a$ would be representable by $Q(x_1,x_2,x_3)$, a contradiction.

Next we are going to find a form $Q_1 = \sum_{i,j=1}^{3} a_{ij}x_ix_j$ such that $Q_1 \backsim Q$ and $a_{11} = a$.

Let Q_1 be the form into which Q is carried by the transformation $C = [c_{kl}]$ of determinant 1, constructed in accordance with the previous Lemma 4.01, then we have

$a_{11} = Q_1(1,0,0) = Q(c_{11},c_{21},c_{31}) = a$

Next we construct a matrix

$$N = \begin{bmatrix} 1 & r & s \\ o & \multicolumn{2}{c}{\multirow{2}{*}{B}} \\ o & & \end{bmatrix}$$

with r,s integers to be selected later and B a 2 x 2 matrix with det B = 1. Clearly det N = 1, thus if we set

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = N \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix} = NY$$

then $Q_1(X) = Q_1(NY) = Q_2(Y)$ and we have $Q \backsim Q_1 \backsim Q_2$ are in the same class.

Let $Q_2(y_1,y_2,y_3) = \sum_{i,j=1}^{3} b_{ij}y_iy_j$ where $b_{11} = a_{11}$.

From the previous theorem we have:

$a_{11}Q_1(X) = (a_{11}x_1 + a_{12}x_2 + a_{13}x_3)^2 + k_1(x_2,x_3)$

$a_{11}Q_2(Y) = (b_{11}y_1 + b_{12}y_2 + b_{13}y_3)^2 + k_2(y_2,y_3)$

where $k_1(x_2,x_3)$ and $k_2(x_2,x_3)$ are positive definite.

Now since N carries the form $Q_1(x_1,x_2,x_3)$into $Q_2(y_1,y_2,y_3)$, it follows that $k_1(x_1,x_2)$, is taken into $k_2(y_2,y_3)$ by B.

By the previous theorem $k_2(x_2,y_3)$ has discriminant $=\Delta(k_2(y_2,y_3) = a_{11}d = b_{11}d$, where $d = \Delta(Q_2(y_1,y_2,y_3)$ and the coefficient of y_2^2 is equal to $b_{11}b_{22} - b_{12}^2 = b$. As we have seen in the case of reduced binary forms, B may be selected so that $b \leq (2/\sqrt{3})\sqrt{b_{11}d}$. Also b_{12} and b_{13} are linear forms in a_{11} with coefficient r and s, respectively. Hence these may be selected so that $|b_{ij}| \leq (1/2)a_{11} = (1/2)b_{11}$ for $j = 2,3$.

Finally since $b_{22} = Q_2(0,1,0)$ is representable , hence $b_{22} \geq a_{11}$, we obtain the sequence of inequalities

$$b_{11}^2 \leq b_{11}b_{22} = (b_{11}b_{22} - b_{12}^2) + b_{12}^2$$

$$\leq 2/\sqrt{3}\ \sqrt{b_{11}d} + (1/4)\ b_{11}^2$$

$$b_{11}^2 \leq (2/\sqrt{3})\ \sqrt{b_{11}d} + (1/4)b_{11}^2$$

$$(3/4)\ b_{11}^2 \leq (2/\sqrt{3})\ \sqrt{b_{11}d}$$

$$(3\sqrt{3})/8\ (b_{11}^{(3/2)}) \leq \sqrt{d}$$

$$(27/64)b_{11}^3 \leq d$$

$$b_{11} \leq (4/3)\sqrt[3]{d.}$$

<u>Corollary</u> <u>4.12:</u>

Every positive definite ternary quadratic form

$Q(x_1,x_2,x_2)$ of discriminant $d_3 = 1$ is equivalent to the form, $Q_1(y_1,y_2,y_3) = y_1^2 + y_2^2 + y_3^2$ (i.e equivalent to a sum of three square).

Proof:

By Theorem 4.11, the given quadratic form $Q(x_1,x_2,x_3)$ is equivalent to a form in which $0 \leq a_{11} \leq (4/3)$, $2|a_{12}| \leq a_{11}$, $2|a_{13}| \leq a_{11}$.

From this it follows that $a_{11} = 1$, $a_{12} = 0$, $a_{13} = 0$.

The class therefore contains a form,

$$Q(x_1,x_2,x_3) = x_1^2 + a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$$
$$= x_1^2 + K(x_2, x_3)$$

where $k(x_2,x_3) = a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3$ is positive definite and has discriminant 1.

Hence $k(x_2,x_3)$ goes into a form $K'(y_2,y_3) = y_2^2 + y_3^2$ by suitable transformation $B = \begin{bmatrix} t & u \\ v & w \end{bmatrix}$ with $\det B = 1$.

Thus the transformation $\begin{bmatrix} 1 & 0 & 0 \\ 0 & t & u \\ 0 & v & w \end{bmatrix}$

takes $Q(x_1,x_2,x_3)$ into $Q_1(y_1,y_2,y_3) = y_1^2 + y_2^2 + y_3^2$.

Theorem 4.13:

If $n > 0$ is not of the form $4^a(8b+7)$, $a \geq 0$, $b \geq 0$ then n can be written as a sum of three squares.

In order to prove this theorem, we need Dirichlet's Theorem stated below. We are not going to prove Dirichlet's

Theorem here because its proof is very involved and beyond our objectives. A proof can be found in [12].

Dirichlet's Theorem:

If $(k,m) = 1$ then the arithmetic progression $kr + m$ $(r = 0,1,\ldots)$ contains infinitely many primes.

Proof of Theorem:

If $n = 4^a n_1$, $4 \nmid n_1$ and n_1 is a sum of three squares, say $n_1 = \sum_{i=1}^{3} x_i^2$, then $n = \sum_{i=1}^{3} (2^a x_i)^2$ is also a sum of three squares. Hence it is sufficient to consider only the case $n \not\equiv 0 \text{ (mod4)}$. This is equivalent to consider only the case $n \not\equiv 0,4 \text{ (mod8)}$

$$\left(\begin{array}{l} n \equiv 0 \text{ (mod4) implies } n = 4k = \{0,\ \pm 4,\ \pm\ 8\ldots\} \\ n \equiv 0 \text{ (mod8) implies } n = 8k = \{0,\ \pm\ 8, \pm 16,\ \ldots\} \\ n \equiv 4 \text{ (mod8) implies } n = 8k + 4 = \{\pm 4, \pm 2, \ldots\ldots\} \end{array}\right)$$

If $n \equiv 7 \text{(mod8)}$ then n cannot be written as the sum of three squares as we proved in the theorem(4.1) at the beginning of this chapter. Therefore it is sufficient to consider the cases $n \equiv 1,2,3,5,6 \text{(mod8)}$.

The idea of the proof is, first to show that n can be represented by a positive definite ternary quadratic form $Q = \sum_{i,j=1}^{3} a_{ij} x_i x_j$ of discriminant 1.

Then we use corollory (4.12) (Every positive definite ternary quadratic form of discriminant $d_3 = 1$ is equivalent to sum of three squares) to complete the proof.

We will specify nine numbers $a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33}, x_1, x_2, x_3$ which satisfy the four conditions below:

1) $n = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + a_{22}x_2^2 + 2a_{23}x_2x_3 + a_{33}x_3^2$,

2) $a_{11} > 0$

3) $b = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}^2 > 0$

4) $\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = 1$

Let $a_{13} = 1$, $a_{23} = 0$, $a_{33} = n$.

Then Q can be written in the form,

$Q = a_{11}x_1^2 + 2a_{12}x_1x_2 + 2x_1x_3 + a_{22}x_2^2 + nx_3^2$.

Then if we let $x_1 = x_2 = 0$, and $x_3 = 1$, we have $Q(0,0,1)=n$.

This will satisfy the first condition.

The three remaining unknown which are a_{11}, a_{12}, a_{22} have to satisfy the remaining three conditions:

1) $a_{11} > 0$

2) $b = \begin{vmatrix} a_{11} & a_{21} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}^2 > 0$

3) $\begin{vmatrix} a_{11} & a_{12} & 1 \\ a_{21} & a_{22} & 0 \\ 1 & 0 & n \end{vmatrix}$

$= (a_{11}a_{22} - a_{12}^2)n - a_{22}$

$= bn - a_{22}$

$= 1$, this imply $bn - 1 = a_{22}$.

Claim:

Condition (1) $a_{11} > 0$ is a sequence of the two conditions (2) and (3).

Let $n \geq 2$ (for $n = 1$, $1 = 1^2 + 0^2 + 0^2$).

It follows that $a_{22} = nb - 1 \geq 2b - 1 > 0$ since b is a positive integer.

$a_{11}a_{22} = a_{12}^2 + b \geq b > 0$. Implies $a_{11} > 0$.

Now we need to choose a value of b so that

$a_{11} = (a_{12}^2 + b)/a_{22}$ is an integer.

This implies $a_{22}\ (a_{12}^2 + b)$

which implies $a_{12}^2 \equiv -b\ (\mathrm{mod}\, a_{22})$

hence $a_{12}^2 \equiv -b (\mathrm{mod}\ bn - 1)$ where a_{12} is an arbitrary integer. Therefore we need to find (-b) as a quadratic residue $\mathrm{mod}\, a_{22}$. The easiest way to accomplish this , is to choose b so that

$nb - 1 = p$ where p is a prime and $\left(\frac{-b}{p}\right) = 1$.

We will consider the cases according to n is an even integer or odd integer.

Case1:

n is even , then $n \equiv 2$ or $6\ (\mathrm{mod} 8)$

Claim: $(4n, n-1) = 1$

Proof of claim:

We will show that $(4, n-1) = 1$ and $(n, n-1) = 1$, that is to show there exist integers x,y such that

$x(4) + y(n-1) = 1$ and $x(n) + y(n-1) = 1$.

For $n \equiv 2 (\mathrm{mod} 8)$ we have $n = 8k+2$.

Therefore $x(4) + y((8k+2)-1) = 1$,

this implies $x(4) + y(8k+1) = 1$

hence we can take $y = 1$ and $x = (-2k)$.

For $n = 6(\mathrm{mod}\,8)$ we have $n = 8k+6$.

Therefore $x(4) + y((8k+6)-1)=1$

imply $x(4) + y((8k+5) = 1$

hence we can take $y = 1$ and $x = -(2k+1)$.

And for $x(n) + y(n-1) = 1$, we have $x = 1$ and $y = -1$

Thus $(4n, n-1) = 1$

By Dirichlet's theorem, there exist integer m such that

$4nm + (n-1)= p$, where p is a prime.

We select $b = 4m + 1$ which implis $b \equiv 1(\mathrm{mod}\,4)$

Now we have $p = 4nm + n - 1 = (4m+1)n - 1 = bn - 1$.

$$\begin{aligned} p \equiv 1 \ (\mathrm{mod}\,4) \text{ since for } n \equiv 2(\mathrm{mod}\,8),\ p &= (4m + 1)(8k+2) - 1 \\ &= 32mk + 8m + 8k + 2 - 1 \\ &= 4t + 1 \end{aligned}$$

where $t = 8mk + 2m + 2k$. This implies $p \equiv 1(\mathrm{mod}\,4)$.

$$\begin{aligned} \text{And for } n \equiv 6(\mathrm{mod}\,8)\ ,\ p &= (4m+1)(8k+6) - 1 \\ &= 32mk + 24m + 8k + 6-1 \\ &= 4r + 1 \text{ where } r = 8mk + 6m + 2k. \end{aligned}$$

This implies $p \equiv 1(\mathrm{mod}\,4)$

Thus $b \equiv p \equiv 1(\mathrm{mod}\,4)$.

$$\begin{aligned} \text{Also } \left(\frac{-b}{p}\right) = \left(\frac{-1.b}{p}\right) &= \left(\frac{-1}{p}\right) \left(\frac{b}{p}\right) \\ &= (-1)^{(p-1)/2} \left(\frac{b}{p}\right) \\ &= \left(\frac{b}{p}\right) \end{aligned}$$

$(b,p) = 1$ for $xp + yb = 1$

implies $x(bn-1) + yb = 1$,implies $x = -1$, $y = n$.

Hence$\left(\frac{b}{p}\right) = \left(\frac{p}{b}\right)(-1)^{((p-1)/2)((b-1)/2)}$

$= \left(\frac{p}{b}\right) \cdot 1$

$= \left(\frac{bn-1}{b}\right)$

$= \left(\frac{-1}{b}\right)$ since $bn -1 \equiv -1(\mathrm{mod} b)$

$= (-1)^{(b-1)/2} = 1.$

Therefore $a_{22} = bn - 1 = p > 0$

$a_{12}^2 \equiv -b(\mathrm{mod} p)$ has solution, yielding a_{12}

and $a_{11} = (b + a_{12}^2) \mid a_{22}$ is an integer.

<u>Case</u> <u>2:</u> n is odd.

Then $n \equiv 1,3,5 \ (\mathrm{mod} 8)$

We set $c = 1$ if $n \equiv 3(\mathrm{mod}8)$ and $c = 3$ if $n \equiv 1,5(\mathrm{mod}8)$.

Then we have $(cn-1)/2$ is odd in both cases.

<u>Claim:</u>

$(4n, (cn-1)/2) = 1$

<u>Proof</u> <u>of</u> <u>claim:</u>

For $n \equiv 3(\mathrm{mod}8)$ we have $n = 8k+3$.

We will show that $(n,(cn-1)/2) = 1$.

Consider $x(4) + y((8k+3-1))/2 = 1$

this implies $x(4) + y(4k+1) = 1$,

hence $x = -k$, $y = 1$, and $x(n) + y((cn-1)/2) = 1$

implies $x(8k+3) + y(4k+1) = 1$

implies $x = 1$, $y = -2$.

For $n \equiv 1(\text{mod}8)$ we have $n = 8k+1$ and $c = 3$

$$x(4) + y((3(8k+1)-1)/2) = 1$$

implies $x(4) + y((24k-2 /2) = 1$

$$x(4) + y(12k-1) = 1$$

implies $x = 3k$, $y = -1$ and $x(n) + y((3n-1)/2) = 1$

implies $x(8k+1) + y((24k+2)/2) = 1$

implies $x(8k+1) + y(12k+1) = 1$

implies $x = 3$, $y = -2$.

For $n \equiv 5(\text{mod}8)$ we have $n = 8k+5$ and $c = 3$.

$$x(4) + y(((8k+5)3-1)/2) = 1$$

implies $x(4) + y((24k + 14)/2) = 1$

implies $x(4) + y(12k + 7) = 1$

implies $x = (3k+2)$ and $y = -1$ and $x(n) + y((cn-1)/2) = 1$

implies $x(8k+5) + y(12k+7) = 1$

implies $x = 3$, $y = -2$

Thus $(4n, (cn-1)/2) = 1$ for all cases.

By Dirichlet's Theorem, it follows that there is a prime

$$p = 4nv + (cn-1)/2,$$

hence $2p = (8v+c)n - 1$.

If we set $b = 8v + c$ then we have $b > 0$, $2p = bn -1$.

For $n \equiv 1(\text{mod}8)$, $b \equiv 3(\text{mod}8)$, $p \equiv 1(\text{mod}4)$

For $n \equiv 3(\text{mod}8)$, $b \equiv 1(\text{mod}8)$, $p \equiv 1(\text{mod}4)$

For $n \equiv 5(\text{mod}8)$, $b \equiv 3(\text{mod}8)$, $p \equiv 3(\text{mod}4)$

For $n \equiv 1,5(\text{mod}8)$, $\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right)$

$$= (1)(-1)^{((8v+3)^2 -1)/8} =(1)(1)=1.$$

For $n \equiv 3(\mathrm{mod}8)$, $\left(\frac{-2}{b}\right) = \left(\frac{-1}{b}\right)\left(\frac{2}{b}\right)$

$$= (1)(-1)^{((8v+1)^2-1)/8)} =(1)(1) =1.$$

It follows that , for any $n \equiv 1 ,3 ,5(\mathrm{mod}8)$

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

$$= (-1)^{(-b-1)/2(p-1)/2}\left(\frac{p}{b}\right)\left(\frac{-2}{b}\right)$$

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

$$= \left(\frac{1-bn}{b}\right)$$

$$= \left(\frac{1}{b}\right) = 1 \text{ since } 1 -bn \equiv 1(\mathrm{modb}).$$

Hence $-b$ is a quadratic residue mod p,

this implies $-b \equiv u^2$ (modp) also we have $-b \equiv 1^2$ (mod2).

Therefore $-b$ is a quadratic residue (mod $2p$),

hence $-b \equiv u^2$ (mod2p) has a solution. If we take one of the solutions $u^2 = a_{12}^2$ then $a_{11} = (a_{12}^2 + b)/a_{22}$ is an integer. Therefore the proof is complete.

As an illustration of the previous theorem, we give two completely worked-out examples, in which we follow step by step the proof just given.

Example 1:

Let $n = 18$, then $n = 18 \equiv 2(\mathrm{mod}8)$.

We choose m such that $4.18(m) + (18-1) = p$.

Let $m = 0$, then $p = 17 = a_{22}$

$b = (p+1)/n = (17+1)/18 = 1$.

For a_{12} we choose the smallest solution of

$-1 \equiv u^2 \pmod{17}$, i.e $u = 4 = a_{12}$

Then $a_{11} = (b + a_{12}{}^2)/a_{22} = 17/17 = 1.$

The quadratic form is now look like this,

$Q = x_1{}^2 + 8x_1x_2 + 2x_1x_3 + 17x_2{}^2 + 18x_3{}^2$

and $Q(0,0,1) = 18.$ Note that

$a_{11} = 1 > 0$,

$$b = \begin{vmatrix} 1 & 4 \\ 4 & 17 \end{vmatrix} = 1 > 0 \text{ and } \begin{vmatrix} 1 & 4 & 1 \\ 4 & 17 & 0 \\ 1 & 0 & 18 \end{vmatrix} = 1$$

By completing the square we obtain

$Q = (x_1 + 4x_2 + x_3)^2 + x_2{}^2 - 8x_2x_3 + 17x_3{}^2$

$\quad = (x_1 + 4x_2 + x_3)^2 + Q_1$

where $Q_1 = x_2{}^2 - 8x_2x_3 + 17\, x_3{}^2$ and $L = x_1 + 4x_2 + x_3$

$a_{11} = 1 = Q(1,0,0)$. Therefore we do not need preliminary transformation to make $a_{11} = a$. $Q_1(1,0)$ is the smallest integer representable by Q_1. Hence we form $B = \begin{bmatrix} 1 & s \\ 0 & u \end{bmatrix}$ such that $|B| = 1$ and this requires $u = 1$ and $s \in Z$ is arbitrary.

Let $\begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$ be defined such that $\begin{bmatrix} x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$

Substitute in $Q_1(x_2,x_3)$

$= (y_2 + sy_3)^2 - 8(y_2 + sy_3)y_3 + 17y_3{}^2$

$= y_2{}^2 + 2y_2y_3s + s^2y_3 - 8y_2y_3 - 8sy_3{}^2 + 17y_3{}^2$

$= y_2{}^2 + (2s-8)y_2 + (s^2 - 8s + 17)y_3$

Set the coefficient $y_2y_3 = 0$. This will requires $s = 4$, and

$$B = \begin{bmatrix} 1 & 4 \\ 0 & 1 \end{bmatrix}.$$

Now let

$$N = \begin{bmatrix} 1 & v & w \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix}$$

Set $x = Ny$. We obtain

$x_1 = y_1 + vy_2 + wy_3$

$x_2 = y_2 + 4y_3$

$x_3 = y_3$

We substitute in $Q(x)$ and obtain

$L = (y_1 + vy_2 + wy_3 + 4(y_2 + 4y_3) + y_3$

$\quad = y_1 + (4+v)y_2 + (w+17)y_3$

We choose $v = -4$, and $w = -17$ then $L = y_1$ and hence

$Q(x_1,x_2,x_3) \backsim Q'(x_1,x_2,x_3) = {y_1}^2 + {y_2}^2 + {y_3}^2$

Since $Q(0,0,1) = 18$ set $x_1 = 0 = y_1 + vy_2 + wy_3$

$\qquad = y_1 - 4y_2 - 17y_3$

$x_2 = 0 = y_2 + 4y_3$

$x_3 = 1 = y_3$

Therefore $y_2 = -4y_3 = -4(1) = -4$

$y_1 = 4y_2 + 17y_3 = 4(-4) + 17 = 1.$

Thus we have $1^2 + (-4)^2 + 1^2 = 18.$

Example 2:

Let $n = 11 \equiv 3(\text{mod}8)$. With $c = 1$, $(cn-1)/2 = 5$

We choose m so that $4(11)m + (cn-1)/2 = p$, a prime.

Therefore we let $m = 0$, $p = 5$ and $2p = 10 = a_{22}$.

$$2p = 10 = bn - 1$$

implies $bn = 11$ implies $b = 1$.

For a_{12} , we choose the smallest positive solution of the congruence $-1 \equiv u^2 \pmod{10}$. Thus $a_{12} = 3$.

$a_{11} = (1+3^2)/a_{22} = (1+9)/10 = 1$.

Then our quadratic form will be,

$Q(x_1,x_2,x_3) = x_1^2 + 6x_1x_2 + 2x_1x_3 + 10x_2^2 + 11x_3^2$.

We verify that all required conditions hold:

$Q(0,0,1) = 11 = n$.

$a_{11} = 1 > 0$

$b = 1 > 0$ and

$$\begin{vmatrix} 1 & 3 & 3 \\ 3 & 10 & 0 \\ 1 & 0 & 11 \end{vmatrix} = 1.$$

We have $Q = (x_1 + 3x_2 + x_3)^2 + Q_1(x_1,x_3)$ where

$Q_1 = x_2^2 - 6x_2x_3 + 10x_3^2$ and $L = x_1 + 3x_2 + x_3$

$Q_1(1,0) = 1$ is the smallest integer representable by Q_1.

Hence we form $B = \begin{bmatrix} 1 & s \\ 0 & u \end{bmatrix}$ and $B = 1$ requires $u = 1$ and $s \in Z$

Define $\begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$ by $\begin{bmatrix} x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix} \begin{bmatrix} y_2 \\ y_3 \end{bmatrix}$

implies $x_2 = y_2 + sy_3$

$x_3 = y_3$

Substitute the above values in Q_1,

$Q_1(x_2,x_3) = y_2^2 + 2y_2y_3(s-3) + y_3^2(s^2 -6s +10)$

Set the coefficient $y_2y_3 = 0$. This requires $s = 3$.

Now $B = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$ and $Q(x) = L^2 + y_2^2 + y_3^2$

Let $N = \begin{bmatrix} 1 & v & w \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}$

and set $x = Ny$, then

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 1 & v & w \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

and we have

$x_1 = y_1 + vy_2 + wy_3$

$x_2 = y_2 + 3y_3$

$x_3 = y_3$

We substitute the above values in L we have

$L = (y_1 + vy_2 + wy_3) + 3(y_2 + 3y_3) + y_3$

$= y_1 (v+3)y_2 + (w+10)y_3$

For $v = -3$ and $w = -10$ then $L = y_1$,

$Q(x) = Q(Ny) = y_1^2 + y_2^2 + y_3^2$

In order to obtain $Q(x) = 11$, we need $x_1=x_2 =0$ and $x_3= 1$.

Under $x = Ny$, $x_3 = y_3 = 1$.

$x_2 = y_2 + 3y_3 = 0$ implies $y_2 = -3y_3 = (-3)(1) = -3$

and $x_1 = 0 = y_2 + vy_2 + wy_3$

$$= y_1 + (-3)y_2 - 10y_3$$

$$= y_1 -3(-3) -10(1)$$

$$= y_1 - 1,$$

this implies $y_1 = 1$.

Hence $1^2 + (-3)^2 + 1^2 = 11$.

Corollary 4.14:

Every non-negative integer is representable as a sum of four squares.

Proof:

From theorem (4.13) we have any positive integer n, where $n \equiv 1$ or $2 \pmod 4$ can be written as a sum of three squares, and hence it can be written as a sum of four squares.

Consequently any positive $n \equiv 3 \pmod 4$ can be written as a sum of four squares since $n = (n-1) + 1^2$ and $n - 1 \equiv 2 \pmod 4$.

If $n \equiv 0 \pmod 4$, then it can be written in the form $n = 4^a(4b + r), r = 1,2,3$. For if $n \equiv 0 \pmod 4$ then $n = 4k$, $k \geq 1$, hence $n = 4^a(4b+r)$, $r = 1,2,3$.

Since $4^a = 2^{a\ 2}$ and $(4b+r) \equiv 1,2$ or $3 \pmod 4$, therefore $n = 4^a(4b+r)$ can be written as a sum of four squares.

Corollary 4.15:

A natural number n is the sum of the squares of three rational numbers if and only if it is the sum of the squares of three integers.

Proof:

Let n be a rational number and n is the sum of three rational numbers. Then n $=\left(\frac{x_1}{x_2}\right)^2 + \left(\frac{y_1}{y_2}\right)^2 + \left(\frac{z_1}{z_3}\right)^2$

By finding the common denominator of the three rational numbers above, we have $n = \frac{x^2 + y^2 + z^2}{w^2}$ where x,y,z are integers.

This implies $w^2n = x^2 + y^2 + z^2$.

If $n = 4^h(8k+7)$ where k,h are integers ≥ 0,

let $w = 2^r(2m+1)$, where $r,m \geq 0$ then

$$\begin{aligned} w^2n &= (2^r(2m+1))^2\ 4^h(8k+7) \\ &= 4^r(2m+1)^2\ 4^h(8k+7) \\ &= 4^r.4^h(2m+1)^2(8k+7) \end{aligned}$$

Note that 2m+1 is odd. Therefore it is of the form (8s+1), (8s+3),(8s+5) or (8s+7).

If (2m+1) is of the form (8s+1) then

$$\begin{aligned} w^2n &= 4^r.4^h(8s+1)^2(8k+7) \\ &= 4^r.4^h(8k+7)(64s^2 + 16s + 1) \\ &= 4^r.4^h(8t+7) \text{ where } r + h,\ t \geq 0 \\ &= 4^{r+h}\ (8t+7) \end{aligned}$$

By using the same method above , we can verify that the other three forms (i.e (8s+3),(8s+5),(8s+7)) will also give us $w^2n = 4^{r+h}(8v+7)$ for some $v \geq 0$.

But from Theorem (4.1), this is impossible because w^2n is the sum of three squares. Hence n cannot be of the form $4^h(8k+7)$ where k,h are integers, and by theorem (4.13) n is the sum of three squares integers.

Conversely, if n is the sum of the squares of three integers, it is also the sum of tthe squares of three rational numbers for $n = x^2 + y^2 + z^2$

$$= (x/1)^2 + (y/1)^2 + (z/1)^2.$$

Corollary 4.16:

If $p \equiv 1 (\mathrm{mod} 4)$ and P is a prime then P is the sum of two squares.

Proof:

$P \equiv 1(\mathrm{mod}4)$. This implies $b^2 \equiv -1(\mathrm{mod}P)$ has a solution since $\genfrac{}{}{0pt}{}{-1}{P} = (-1)^{((4k+1)-1))/2}$

$= (-1)^{2k} = 1.$

Therefore there exist integers b, c such that

$b^2 = -1 + cp.$

Now we consider the quadratic form

$Q(x,y) = Px^2 + 2bxy + cy^2$. If we let $x = 1$ and $y = 0$ then $Q(1,0) = P > 0$ and the discriminant of Q is

$$\Delta(Q(x,y)) = \begin{vmatrix} P & b \\ b & c \end{vmatrix}$$

$$= Pc - b^2 = 1 \text{ since } b^2 = -1 + cP.$$

This implies $Q(x,y) \backsim Q'(x',y') = x'^2 + y'^2$ which implies P is a sum of two squares.

This corollary together with Lemma 2.02 and Lemma 2.07 of chapter 2 gives us a complete solution of the two squares problem.

Definition 4.6:

n is a triangular number if $n = \frac{a(a+1)}{2}$ where $a \in Z$

Corollary 4.17:

Every integer is the sum of three triangular numbers.

Proof:

By theorem (4.13) , any integer of the form 8k+3 is the sum of the squares of three integers,

ie $8k+3 = x^2 + y^2 + z^2$.

Since (8k+3) is odd, this implies x,y,z are all odd.

For assume two of the integers say x, y are even and one is odd say z then,

$$\begin{aligned} (8k+3) &= (2x')^2 + (2y')^2 +(2z'+1)^2 \\ &= 4x'^2 + 4y'^2 + 4z'^2 + 4z + 1 \\ &= 4(x'^2 + y'^2 + z'^2 + z') + 1 \end{aligned}$$

implies $8k+2 = 4(x'^2 + y'^2 + z'^2 + z')$

implies $2(4k+1)= 4m$ where $m = (x'^2 + y'^2 + z'^2 + z')$

implies $4k+1 = 2m$. Contradiction since 4k+1 is odd and 2m is even.

Similarly , if two of the integers are odd and one is even or all the integers are even , we would have a contradiction. Hence (8k+3) is the sum of the squares of three odd integers say

$$(8k+3) = (2x'+1)^2 + (2y' +1)^2 + (2z'+1)^2$$

$$(8k+3) = 4x'^2 + 4x' + 4y'^2 + 4y' + 4z'^2 + 4z' + 3$$

$$8k = 4x'^2 + 4x' + 4y'^2 + 4y' + 4z'^2 + 4z'$$

$$2k = x'^2 + x' + y'^2 + y' + z'^2 + z'$$

$$k = x'\frac{(x'+1)}{2} + y'\frac{(y'+1)}{2} + z'\frac{(z'+1)}{2}$$

Therefore any integer is the sum of three squares triangular numbers.

3.The Number Of Representations Of An Integer As A Sum Of Three Squares.

In this section we are concerned with problem of determining the number of representations of an integer as a sum of three squares. In chapters 2 and 3 we were able to solve the corresponding problems for Two-square and Four-square completely by using elementary methods. On the other hand the known formulae that give the number of representations of an integer as a sum of three squares are difficult to prove. This perhaps, not too surprising if we consider the fact that even the statements depend on the rather deep and difficult concepts of class number, the genus of a quadratic form, etc.

In this section we will restrict ourselves to only the statement of some theorems concerning that problem. The reader can find their proofs in [5],[12] and [8]. We will also give as an application some examples.

Recall $R_3(n)$ is the number of primitive solutions of $x_1^2 + x_2^2 + x_3^2 = n$ and $r_3(n)$ is the total number of all solutions.

Theorem 4.18:

If n is the sum of three squares, then $r_3(n) = r_3(4^k n)$ for any non-negative integer k.

Proof:

Assume $n = x_1^2 + x_2^2 + x_3^2$,

then $4^k n = (2^k x_1)^2 + (2^k x_2)^2 + (2^k x_3)^2$.

Conversely if $4^k n = y_1^2 + y_2^2 + y_3^2$, then all the $y_{i's}$ are even. Let $y_i = 2x_i$, then $4^k n = (2x_1)^2 + (2x_2)^2 + (2x_3)^2$ so that $4^{k-1} n = x_1^2 + x_2^2 + x_3^2$. If $k - 1 \nmid 0$ then all the $x_{i's}$ are even, say $x_i = 2z_i$, then $4^{k-2} n = z_1^2 + z_2^2 + z_3^2$. We continue this process (a finite number of times) and we have $n = x_1^2 + x_2^2 + x_3^2$.

Thus we have shown there is a 1-1 corresponding between the solutions of the two equations,

$x_1^2 + x_2^2 + x_3^2 = n$

$x_1^2 + x_2^2 + x_3^2 = 4^k n$

Hence $r_3(n) = r_3(4^k n)$.

Before we go any further we shall find it more convenient to use Gauss's notation concerning the "discriminant" of the quadratic form. In all of our previous discussion we have defined the discriminant of a quadratic form to be the determinant of the matrix of the coefficients of the form.This is well defined entity for forms in any number of variables. However in the particular case of binary forms the traditional meaning of the discriminat is little different. In this section we will define the discriminate of the quadratic form $Q(x,y) = ax^2 + 2bxy + cy^2$ by $D = -4d_2$ where $d_2 = \begin{vmatrix} a & b \\ b & c \end{vmatrix} = ac - b^2$, is the determinant.

Definition 4.7:

A quadratic form $Q(x,y) = ax^2 + 2bxy + cy^2$ is said to be primitive if $g.c.d(a,b,c) = 1$ and imprimitive otherwise.

Theorem 4.19:

Let $h(D)$ be the number of classes of primitive binary quadratic forms corresponding to the discriminant $D = -1$ if $n \equiv 3(\text{mod}8)$, $D = -4n$ if $n \equiv 1,2,5,\text{or } 6(\text{mod}8)$ then the number of primitive solutions $R_3(n)$ is given by

$$R_3(n) = \begin{cases} 12\,h(D) \text{ if } n \equiv 1,2,5,\text{or } 6(\text{mod}8) \text{ and } n \neq 1 \\ 24h(D) \text{ if } n \equiv 3(\text{mod}8) \text{ and } n \neq 3 \\ 6h(D) \text{ if } n = 1 \\ 8h(D) \text{ if } n = 3 \end{cases}$$

Few remarks concerning the number of classes of primitive binary quadratic forms $h(D)$ are in order:

1) $h(D) = gk$ where $g = 2^{t-1}$ is the number of genera, t is the number of distinct prime factors of D, and k is the number of classes in each genus.

2) If $D = -4n$ and $n \equiv 1, 2, 5$ or $6(\text{mod}8)$ and if n contains t odd prime factors, then D contains $t + 1$ primes, and hence

$g = 2^{(t+1)-1} = 2^t$. If $D = -n$ and $n \equiv 3 \pmod 8$ and if n contains t primes(all odd), then $g = 2^{t-1}$. For $n = 1,3$, $h = 1$.

As a consequence of these remarks we can restate the previous theorem as follows:

Theorem 4.20:

The number of primitive representation of n as a sum of three squares is:

$$R_3(n) = \begin{cases} 3.2^{t+2}k & \text{if } n = 1,2,3,5,\text{or } 6 \pmod 8, n \nmid 1 \text{ or } 3 \\ 6 & \text{if } n = 1 \\ 8 & \text{if } n = 3 \end{cases}$$

For $n = 1$, we have $1 = \underline{+}1^2 + 0^2 + 0^2$

For $n = 3$, we have $3 = (\underline{+}1)^2 + (\underline{+}1)^2 + (\underline{+}1)^2$

Examples:

1) Let $n = 18 \equiv 2 \pmod 8$

$h = 2$, $g = 2$, $k = 1$(see Rose)

$R_3(18) = 12(2) = 24$ (by first theorem)

$R_3(18) = 3(2^{1+2}.1) = 24$ (by second theorem)

2) Let $n = 11 \equiv 3 \pmod 8$

$h = 1$, $g = 1$, $k = 1$ (see Rose)

$R_3(11) = 24$ (by first theorem)

$R_3(11) = 3.2^3 = 24$ (by second theorem)

For square free positive integers Eisenstein proved by using Dirichlet's class number formulae the following:

Theorem 4.21: (Eisenstein)

For square free positive integer n,

$$R_3(n) = 24 \sum_{r=1}^{\left[\frac{n}{4}\right]} \left(\frac{r}{n}\right) \text{ if } n \equiv 1 (\text{mod} 4)$$

$$8 \sum_{r=1}^{\left[\frac{n}{2}\right]} \left(\frac{r}{n}\right) \text{ if } n \equiv 3 (\text{mod} 8)$$

where [x] is the greatest integer less than or equal to x and $\left(\frac{r}{n}\right)$ is the Jacobi symbol.

Example:

$$n = 11 \equiv 3(\text{mod} 8)$$

$$R_3(11) = 8 \sum_{r=1}^{\left[\frac{11}{2}\right]} \left(\frac{r}{11}\right)$$

$$= 8\left[\left(\frac{1}{11}\right) + \left(\frac{2}{11}\right) + \left(\frac{3}{11}\right) + \left(\frac{4}{11}\right) + \left(\frac{5}{11}\right)\right]$$

$$= 8[1 + 0 + 1 + 1 + 0]$$

$$= 24.$$

So far , we have considered only the primitive representations $R_3(n)$. The total number of representations of n as a sum of three squares is given by

$$r_3 = \sum_{d^2 | n} R_3\left(\frac{n}{d^2}\right)$$

For example if n = 18,

$$r_3(18) = \sum_{d^2 | 18} R_3\left(\frac{18}{d^2}\right)$$

$$= R_3(18) + R_3(2)$$

$$= 24 + 12 = 36.$$

$$r_3(11) = \sum_{d^2 | 11} R_3\left(\frac{11}{d^2}\right) = R_3(11) = 24.$$

Final remarks concerning the representation of an integer as a sums of three squares.

1) In chapters 2 and 3, we characterized the positive integers that can be represented as a sum of two and four nonvanishing squares.The complete anwser of characterizing which positive integers are sum of three nonvanishing squares is still not known and depend on the difficult, and still unsolved, problem of the determination of all discriminants of binary , positive definite quadratic forms with exactly one class in each genus. Some partial results and conjectures concerning this problem can be found in [5] and [11].

2) The problem concerning the uniqueness of essentially distinct representation as a sum of three squares and also the problem of determining all integers which are not sum of three unequal squares are not completely solved. Some partial results and conjectures are given in [5].

Summary and Conclusion

In this study, we characterized the integers that can be represented as a sum of two, three and four squares.

In chapter 1, we stated thr problem and give a historical introduction of the problem of representation of integers n as a sum of kth. power integers. In chapter 2, we studied the necessary and sufficient conditions for an integer n to be representable as the sum of two squares. Then we determined the total number of not essentially distinct representation of integer n. Also in this chapter we considered the problem of representing an integer n as a sum of two nonvanishing squares, the sum of two relatively prime squares, and we discussed the uniqueness of essentially distinct representation.

In chapter 3, we proved that every positive integer n is the sum of four squares integers. The representation of an integer n as a sum of four nonvanishing squares and four unequal squares have also been discussed. We also determined the total number of representation of an integer n as a sum of four squares, this followed by the study of the uniqueness of essentially distinct representations.

In chapter 4, we began with the proof of the main result of representation of integer n as a sum of three squares. Then we studied some properties of integral Quadratic forms. We concluded this chapter by only stating some important theorems and results concerning the problem of representation of an integer n as a sum of three squares.

BIBLIOGRAPHY

[1] Chahal, J.S. Topic in Number Theory. New York: Plenum Press, 1988.

[2] Davenport, Harold. The Higher Arithmetic. New York : Harper and Row, 1960.

[3] Dickson, Leonard E. History of the Theory of Numbers. 3vols. New York: Chelsea Publishing Co., 1952

[4] - - - .Modern Elementary Theory of Numbers. Chicago: The University of Chicago Press, 1965.

[5] Grosswald, Emil. Representation of integers as Sum of Squares. New York : Springer-Verlag New York Inc., 1985.

[6] Halter-Koch, F . "Darstellung Naturlicher Zallen als summe von Quadraton." Acta Arithmetica 42 , (1983) : 11 - 20.

[7] Hardy, G.H and Wright, E.M. An Introduction to the Theory of Numbers. Fifth ed. New York: Clarendon Press, 1979.

[8] Landau, Edmund. Elementary Number Theory New York : Chelsea Publishing Co., 1958.

[9] Lehmer, D.H. "On the partition of numbers into squares." American Mathematics Monthly 55(1948) : 476-481.

[10] Niven, Ivan and Herbert S. Zuckerman. An Introduction to the Theory of Numbers. 4th ed. New York: John Wiley & Sons, 1980.

[11] Paul, G. "On sums of squares." American Mathematics Monthly 40 (1933):10-18.

[12] Rose, H.E. A course In Number Theory. New York: Clarendon Press Oxford, 1988.

[13] Sierpinski, Waclaw. Elementary Theory of Numbers. Vol 31 . North Holand : PWN -Polish Scientific Publishers, 1988

[14] Stewart, B. Madison. Theory of Numbers . 2nd. ed. New York : The Macmillan Co. , 1964.

[15] Uspensky, J. V and Heaslet, M.A . Elementary Number Theory. 1st. ed. New York : McGraw-Hill Book Co., 1939.

[16] Weil, Andre. Number Theory. Boston: Birkhauser Boston Inc., 1984.