A DISCUSSION OF HOMOGENOUS QUADRATIC EQUATIONS

by

LANCE KAMINSKI

B.S., University of Missouri-Rolla, 2007

A THESIS

submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2009

Approved by:

Major Professor
Christopher Pinner

Abstract

This thesis will look at Quadratic Diophantine Equations. Some well known proofs, including how to compute all Pythagorean triples and which numbers can be represented by the sum of two and four squares will be presented. Some concepts that follow from these theorems will also be presented. These include how to compute all Pythagorean Quadruples, which number can be represented by the difference of two squares and the Crossed Ladders problem. Then, Ramanujan's problem of finding which positive integers, a, b, c and d which allow $aw^2 + bx^2 + cy^2 + dz^2$ to represent all natural numbers will be shown. The paper will conclude with a lengthy discussion of Uspensky's proof on which numbers can be represented by the sum three squares.

Table of Contents

List of Figures

List of Tables

Chapter 1

Basics of Diophantine Equations

In this chapter, I will introduce Diophantine Equations. Methods of generating all solutions of Pythagorean triples and Pythagorean quadruples will be shown. The chapter will conclude with an application of Pythagorean triples involving two ladders crossing, resting on opposite buildings.

1.1 Explaining Diophantine Equations

The term "Diophantine Equation" generally refers to indeterminate equations with integer coefficients in which only integer solutions are allowed. Some mathematicians are concerned with finding rational solutions to indeterminate equations; however, Mordell points out that finding rational solutions is equivalent to finding integer solutions. Thus only integer solutions will be considered in this thesis.[5] Some examples of Diophantine equations are:

$$ax + by = c \tag{1.1a}$$
$$a^x + b^y = c^z \tag{1.1b}$$
$$x^n + y^n = z^n \tag{1.1c}$$
$$ax^2 + xy + y^2 = cz^2 \tag{1.1d}$$

where $a, b, c \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. In each of these examples, a, b, c are given and the objective is to find integers x, y, z that satisfy each equation. If the indeterminate equation is a polynomial, the Diophantine Equation is labeled based on the highest degree that is in the equation. The indeterminate equation can involve other functions and will derive its name from that function. Equation (1.1a) is called a linear Diophantine Equation. The next example, (1.1b), is an example of an exponential Diophantine Equation. An exponential Diophantine Equation is an indeterminate equation in which at least one of the desired variables appears in an exponent. Catalan's conjecture, which was proven in 2002 by Preda Mihăilescu, states that the only solution, in natural numbers, of

$$x^a - y^b = 1 \tag{1.2}$$

for $x, a, b, y > 1$ is $x = 3$, $a = 2$, $y = 2$ and $b = 3$. The third example given is dealt with in Fermat's Last Theorem. In 1995, Andrew Wiles proved that Fermat was correct is stating that (1.1c) has infinitely many solutions for $n = 2$ and no nontrivial solutions for $n > 2$. The final example, (1.1d) is called a quadratic Diophantine Equation, the main focus of this thesis. As stated previously, these are called quadratic since the highest degree is two.

Quadratic Diophantine Equations can be labeled as either homogeneous or inhomogeneous. A homogenous quadratic Diophantine Equation is a quadratic indeterminate equation in which every term has degree two. In the two variable case the only possible terms are x^2, xy, y^2 with a coefficient in front of each term. This clearly means that a homogeneous quadratic has no constant term. An inhomogeneous quadratic Diophantine Equation is any quadratic Diophantine Equation that is not homogeneous.

1.2 Pythagorean Triples

The well known equation

$$x^2 + y^2 = z^2 \tag{1.3}$$

is from Pythagoras' Theorem. Every high school Geometry student uses this at one time or another to find one side of a right triangle when the two other sides are given. What if none of the sides are given? Looking at this as a Diophantine Equation will allow for all solutions to be generated such that x, y and z are all positive integers.

Lemma 1.1. *Let $x, y, z \in \mathbb{Z}^+$. If x, y, z is a primitive triple of solutions, i.e. $(x, y, z) = 1$, of equation (1.3) then x and y have opposite parity and z is odd.*

Proof. Assume that x and y are both even. Then $x = 2k$ and $y = 2m$ for some $k, m \in \mathbb{N}$. Substituting this into equation (1.3) yields

$$x^2 + y^2 = (2k)^2 + (2m)^2 = 2(2k^2 + 2m^2) = z^2. \tag{1.4}$$

This would imply that z is also even which contradicts $(x, y, z) = 1$. Therefore, for primitive solutions, x and y are not both even.
Next, assume that x and y are both odd. Then $x = 2k - 1$ and $y = 2m - 1$ for some $k, m \in \mathbb{N}$. Thus:

$$\begin{aligned} x^2 + y^2 &= (2k-1)^2 + (2m-1)^2 && \text{(1.5a)} \\ &= 4k(k-1) + 4m(m-1) + 2 && \text{(1.5b)} \\ &\equiv 2 \pmod 8. \qquad \text{(either k(m) is even or k-1(m-1) is)} && \text{(1.5c)} \end{aligned}$$

Case 1: If z is even, then $z = 2n$ for some $n \in \mathbb{N}$, and

$$z^2 = 4n^2 \equiv 0 \text{ or } 4 \pmod 8, \tag{1.6}$$

which contradicts equation (1.5c) which shows that $z^2 = x^2 + y^2 \equiv 2 \pmod 8$.

Case 2: If z is odd, then $z = 2n - 1$ for some $n \in \mathbb{N}$ and

$$z^2 = 4n(n-1) + 1 \equiv 1 \pmod 8 \qquad \text{(either n or n-1 is even)}, \tag{1.7}$$

which again contradicts equations (1.5c). Thus x and y are not both odd.

Thus x and y have opposite parity. Assume, without loss of generality, y is even. Let $x = 2k - 1$ and $y = 2m$ for some $k, m \in \mathbb{N}$.

$$\begin{aligned} z^2 &= x^2 + y^2 && \text{(1.8a)} \\ &= (2k-1)^2 + (2m)^2 && \text{(1.8b)} \\ &= 2(2k^2 - 2k + 2m^2) + 1 && \text{(1.8c)} \end{aligned}$$

Thus, by equations (1.8), z is odd. □

Theorem 1.2. *All nontrivial, positive integer primitive solutions of $x^2 + y^2 = z^2$, with y even, are given by the parameterized equations:*

$$\begin{aligned} x &= m^2 - n^2 && \text{(1.9a)} \\ y &= 2mn && \text{(1.9b)} \\ z &= m^2 + n^2, && \text{(1.9c)} \end{aligned}$$

with $m, n \in \mathbb{Z}^+$, $m > n$, $(m, n) = 1$ and m and n having opposite parity.

Proof. Let x, y, z be such that $x^2 + y^2 = z^2$ with $(x, y, z) = 1$. As in Lemma 1.1, one can let y be even without loss of generality. Let m, n be integers defined such that

$$\frac{m}{n} = \frac{z + x}{y} \tag{1.10}$$

with $(m, n) = 1$. Clearly $z + x > y$ so $m > n$. Manipulating equation (1.10) yields,

$$\begin{aligned} \frac{m}{n}y - x &= z && && \text{(1.11a)} \\ ym - xn &= zn && && \text{(1.11b)} \\ y^2m^2 - 2ymxn + x^2n^2 &= z^2n^2 && \text{(squaring both sides)} && \text{(1.11c)} \\ y^2m^2 - 2ymxn + x^2n^2 &= (x^2 + y^2)n^2 && \text{(since } z^2 = x^2 + y^2\text{)} && \text{(1.11d)} \\ y^2m^2 - 2ymxn &= y^2n^2 && && \text{(1.11e)} \\ y(m^2 - n^2) &= x(2mn). && && \text{(1.11f)} \end{aligned}$$

Since $(m, n) = 1$, either m and n have opposite parity or m and n are both odd (if they are both even then $(m, n) \neq 1$). If m, n are both odd, then $m^2 - n^2$ is even and $\frac{m^2-n^2}{2}$ is an integer. Rewriting equation (1.11f) yields

$$y\left(\frac{m^2 - n^2}{2}\right) = x(mn). \tag{1.12}$$

Since x is odd, then xmn is odd, but y was assumed to be even. This is a contradiction. Thus m, n can not both be odd. So, m, n have opposite parity. Then $m^2 - n^2$ is odd. This means that $(2, m^2 - n^2) = 1$. Using this with the fact that, $(mn, m^2 - n^2)$, implies that $(2mn, m^2 - n^2) = 1$. Thus $2mn \mid y$. It is also clear that $y \mid 2mn$ since $(x, y) = 1$. Therefore $y = 2mn$. If this is the case, then it is clear that $x = m^2 - n^2$. Finally, substituting both of these back into equation (1.11a) obtains

$$z = \frac{m}{n}(2mn) - (m^2 - n^2) = m^2 + n^2 \tag{1.13}$$

Thus x, y, z satisfy the equations (1.9) and m, n are defined in such a way that they satisfy the restrictions. □

To find all solutions of equation (1.3), simply multiply each parameterized solution by the same constant. The x, y and z which satisfy equation (1.3) are called Pythagorean triples.

Now that all Pythagorean triples have been found, it seems logical to look at Pythagorean quadruples.

1.3 Pythagorean Quadruples

$$x^2 + y^2 + z^2 = t^2 \tag{1.14}$$

Theorem 1.3. *All positive integer solutions to equation (1.14) are given by the parameterized equations:*

$$x = d(m^2 + s^2 - n^2 - r^2) \tag{1.15a}$$
$$y = d(2mn - 2rs) \tag{1.15b}$$
$$z = d(2mr + 2ns) \tag{1.15c}$$
$$t = d(m^2 + n^2 + r^2 + s^2) \tag{1.15d}$$

with $m, n, r, s \in \mathbb{N}$, $d \in \mathbb{Z}^+$, *and* $(m, n, r, s) = 1$.

Proof. Suppose x, y, z, t exist such that they satisfy equation (1.14) with $(x, y, z, t) = 1$. Equations (1.14) can be rewritten as

$$y^2 + z^2 = t^2 - x^2 \tag{1.16}$$

If t is even, then at least one of x, y or z is also even. Without loss of generality, assume x is even. Then, $4|t^2 - x^2$, and, by equation (1.16), $4|y^2 + z^2$ which can only happen if y and z are both even. This means that x, y, z, t are all even, but this contradicts $(x, y, z, t) = 1$. Thus t is odd.
Equation (1.16) can be written

$$(t - x)(t + x) = y^2 + z^2. \tag{1.17}$$

Assume $(t-x)$ and $(t+x)$ have a common prime factor, p with $p \equiv 3 \pmod 4$. So

$$p|[(t+x)+(t-x)] \Rightarrow p|2t. \tag{1.18}$$

Since p is an odd prime, $p|t$. Similarly, $p|x$. So,

$$y^2 + z^2 \equiv 0 \pmod p. \tag{1.19}$$

If $p \nmid z$, then there exists an α such that

$$z\alpha \equiv 1 \pmod p. \tag{1.20}$$

So,

$$(y\alpha)^2 + 1 \equiv 0 \pmod p \Rightarrow (y\alpha)^2 = -1 \pmod p. \tag{1.21}$$

But as it will be shown in Lemma 2.3, this is impossible. This contradicts the assumption that $p \nmid z$, therefore $p|z$. By a similar argument, $p|y$. This makes a factor of x, y, z and t which contradicts the assumption that $(x, y, z, t) = 1$. Thus $t-x$ and $t+x$ have no common prime factor, p with $p \equiv 3 \pmod 4$.
For a prime, q, with $q \equiv 3 \pmod 4$, if q divides either $x+t$ or $x-t$, then

$$y^2 + z^2 \equiv 0 \pmod q. \tag{1.22}$$

By the argument given above, this implies $q|y$ and $q|z$ or $q^2|y^2$ and $q^2|z^2$. Thus, $q^2|y^2+z^2 = (x-t)(x+t)$. Therefore, if either $x+t$ or $x-t$ contains a prime factor, q, with $q \equiv 3 \pmod 4$, then it contains that factor to an even power. By Theorem 2.8, which is presented in Chapter 2, $(t-x)$ and $(t+x)$ can both be represented as the sum of two squares. Since $x+t$ and $x-t$ are even, there exists $m, n, r, s \in \mathbb{N}$ such that:

$$t + x = 2(m^2 + s^2) \tag{1.23a}$$
$$t - x = 2(n^2 + r^2). \tag{1.23b}$$

So:

$$t = m^2 + n^2 + r^2 + s^2 \tag{1.24a}$$
$$x = m^2 + s^2 - n^2 - r^2. \tag{1.24b}$$

Substituting this into equation (1.17) yields

$$y^2 + z^2 = 4(m^2 + s^2)(n^2 + r^2) = (2mn - 2rs)^2 + (2mr + 2ns)^2. \tag{1.25}$$

Since y and z are even, without loss of generality:

$$y = 2mn - 2rs \tag{1.26a}$$
$$z = 2mr + 2ns. \tag{1.26b}$$

To find all Pythagorean quadruples, simply multiply each parameterized solution by the same constant, d. □

1.4 Crossed Ladders

In the Crossed Ladders Problem, two ladders, one of length α and one of length β are resting between two walls. The ladders' bases are resting on opposite sides, leaning on opposite buildings and crossing midair. This can be seen in Fig. 1.1.

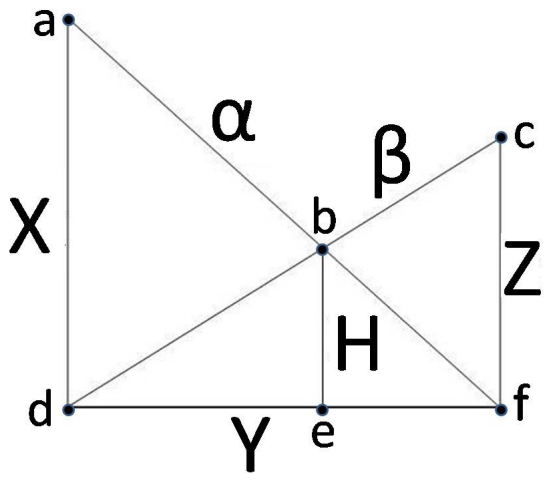

Figure 1.1: *Crossed Ladders Problem*

The origins of this problem are unknown. In *Mathematical Circus*, Gardner discovered a source dating back to 1941. Usually this problem is given as a mathematical brain teaser in which the lengths of the ladders, α and β, as well as the height of their intersection, H, are given.[2] However, when no lengths are given, looking for all general solutions leads to a system of simultaneous quadratic Diophantine Equations. It is clear that this problem involves two right triangles that share a base. Solving this problem consists of solving the two simultaneous equations:

$$Y^2 = \alpha^2 - X^2 \tag{1.27a}$$

$$Y^2 = \beta^2 - Z^2 \tag{1.27b}$$

which are obtained by Pythagorean's Theorem. Using only these two equations makes it a little difficult to solve for the general solution, but using similar triangles gives us a third equation which aids in solving it.

Theorem 1.4. $\frac{1}{X} + \frac{1}{Z} = \frac{1}{H}$

Proof. It is clear that $\triangle adf$ and $\triangle bef$ are similar triangles and $\triangle cfd$ and $\triangle bed$ are also similar triangles. Using the proportionality of the sides of similar triangles produces the equations:

$$\frac{Y}{X} = \frac{ef}{H} \tag{1.28a}$$

$$\frac{Y}{Z} = \frac{de}{H} \tag{1.28b}$$

Adding equation (1.28a) to equation (1.28b) and realizing that $de + ef = Y$ produces:

$$\frac{Y}{X} + \frac{Y}{Z} = \frac{de}{H} + \frac{ef}{H} = \frac{Y}{H} \Longrightarrow \frac{1}{X} + \frac{1}{Z} = \frac{1}{H} \tag{1.29}$$

□

When α, β, and H are given, using (1.29), this problem becomes nothing more than a simple computation. As stated, consider what happens when no lengths are given. That is, instead of finding one solution, find all possible solutions in which α, β, X, Y, Z and H are integers. In 1999, Sutcliffe found a proof of the Crossed Ladders Theorem.

Theorem 1.5 (Solutions to the crossed ladder problem by Sutcliffe)**.** *Given the equations derived from Figure 1.1, with $\alpha \geq \beta$ and $X \geq Z$, then:*

(I) If $\alpha = \beta$, then $X = Z$ and all primitive solutions, i.e. solutions with $(\alpha, H, Y) = 1$, in which α, X, Y, and H are integers are given by the parameterized equation:

$$\alpha = m^2 + n^2 \tag{1.30a}$$
$$H = mn \tag{1.30b}$$
$$Y = m^2 - n^2, \tag{1.30c}$$

with $m, n \in \mathbb{N}$, $m > n$.

(II) If $\alpha > \beta$ then $X > Z$ and all primitive solutions in which α, β, X, Y, Z and H are integers are given by the following parameters:
Let ϵ be any integer that is not of the form p or $2p$, where p is a prime, and let Γ,Δ, Ψ, and Φ be any positive integers all of the same parity with the restriction that:

$$\begin{aligned} &\Gamma\Delta = \epsilon^2 = \Psi\Phi \\ &\Gamma > \Delta,\ \Gamma > \Psi,\ \textit{and}\ \Psi > \Phi \end{aligned} \tag{1.31}$$

$$X = \mu\omega, \tag{1.32a}$$
$$Y = \epsilon\omega, \tag{1.32b}$$
$$Z = \nu\omega, \tag{1.32c}$$
$$\alpha = \kappa\omega, \tag{1.32d}$$
$$\beta = \lambda\omega, \tag{1.32e}$$
$$H = \mu\nu/d \tag{1.32f}$$

where

$$\kappa = (\Gamma + \Delta)/2, \tag{1.33a}$$
$$\lambda = (\Psi + \Phi)/2, \tag{1.33b}$$
$$\mu = (\Gamma - \Delta)/2, \tag{1.33c}$$
$$\nu = (\Psi - \Phi)/2 \tag{1.33d}$$
$$\omega = (\mu + \nu)/d \tag{1.33e}$$
$$d = (\mu + \nu, \mu\nu). \tag{1.33f}$$

Sutcliffe's Proof of Crossed Ladders (I). [7] If $\alpha = \beta$, then it is clear that $X = Z$ and that equation (1.27a) and equation (1.27b) are the same. Using this fact, equation (1.29) becomes:

$$\frac{1}{Z} + \frac{1}{Z} = \frac{2}{Z} = \frac{1}{H} \Longrightarrow 2H = Z. \tag{1.34}$$

Plugging equation (1.34) back into equation (1.27a) yields

$$Y^2 = \alpha^2 - (2H)^2. \tag{1.35}$$

Thus finding all integer solutions of the Crossed Ladder Problem in this case is equivalent to finding all integer solutions to equation (1.35), which is clearly a Pythagorean triple. In Theorem 1.2 it was shown that all primitive Pythagorean triples to the equation $Y^2 + (2H)^2 = \alpha^2$ are given by the parameterized equations:

$$\alpha = m^2 + n^2 \tag{1.36a}$$
$$2H = 2mn \tag{1.36b}$$
$$Y = m^2 - n^2, \tag{1.36c}$$

with $m, n \in \mathbb{Z}^+$ and $m > n$. □

Lemma 1.6. *"A positive integral square, Y^2, is expressible as the difference between two positive integral squares in at least two distinct ways if and only if it is not of the form p or $2p$, where p is a prime"*[7]

Proof of Lemma. [7] Let Y^2 have two distinct representations, $\alpha^2 - X^2$ and $\beta^2 - Z^2$ with $\alpha \neq \beta$. Another way to write Y is:

$$Y^2 = (\alpha - X)(\alpha + X) = (\beta - Z)(\beta + Z). \tag{1.37}$$

Since $\alpha \neq \beta$ is is clear that these factors are different. Clearly, the factors of the first representation have the same parity as Y^2. Also, the factors of the second representation have the same parity as Y^2. So Y^2 is being represented by two distinct factors of the same parity as Y^2 in two distinct ways.

Case 1: $Y = p$, with p a prime and $p \neq 2$. Then the only distinct factors of Y^2 are 1 and p^2. Thus, if $Y = p$, There are not two distinct ways to factor Y^2 as two distinct factors.

Case 2: $Y = 2$. then there is no way to factor Y^2 as two distinct factors with the same parity as Y^2.

Case 3: $Y = 2p$, with p a prime. Then the only distinct factors of Y^2 with the same parity as Y^2 are 2 and $2p^2$. Thus we have the same problem as Case 1.

Case 4: $Y = qr$, where q and r are any odd numbers greater than 1. Then:

$$Y^2 = (1)(q^2r^2) \qquad Y^2 = (q)(qr^2) \tag{1.38}$$
$$= \left(\frac{q^2r^2+1}{2}\right)^2 - \left(\frac{q^2r^2-1}{2}\right)^2 \qquad = \left(\frac{qr^2+q}{2}\right)^2 - \left(\frac{qr^2-q}{2}\right)^2. \tag{1.39}$$

Since q and r are odd, the fractions above are integers. Clearly these factors are distinct and are all odd: the same parity as Y^2.

Case 5: $Y = 2st$, where s and t are any integer greater than 1. Then:

$$Y^2 = (2)(2s^2t^2) \qquad Y^2 = (2s)(2st^2) \tag{1.40}$$

$$= \left(s^2t^2+1\right)^2 - \left(s^2t^2-1\right)^2 \qquad = \left(st^2+s\right)^2 - \left(st^2-s\right)^2. \tag{1.41}$$

Clearly these factors are distinct and are all even, the same parity as Y^2.

Since these cases go over all possible values of Y, Case 1 through Case 3 show why $Y \neq p$ or $Y \neq 2p$ and Case 4 and 5 show that all other values of Y will give two distinct factorizations Y^2 with two distinct factors. □

Sutcliffe's Proof of Crossed Ladders (II). [7] Let all variables be defined as given in equations (1.32) and (1.33) with all the necessary restrictions. Since $\alpha > \beta$, it is clear that $X > Z$. Using equation (1.27a) with equations (1.32a), (1.32b), and (1.32d) produces:

$$\begin{aligned}
\alpha^2 - X^2 &= (\kappa\omega)^2 - (\mu\omega)^2 && \text{(by Eqns. (1.32d) and (1.32a))} && \text{(1.42a)}\\
&= (\kappa^2 - \mu^2)\omega^2 && \text{(by factoring)} && \text{(1.42b)}\\
&= (\kappa-\mu)(\kappa+\mu)\omega^2 && \text{(by factoring)} && \text{(1.42c)}\\
&= \Delta\Gamma\omega^2 && \text{(by Eqns. (1.33a) and (1.33c))} && \text{(1.42d)}\\
&= \epsilon^2\omega^2 && \text{(by Eqn. (1.31))} && \text{(1.42e)}\\
&= Y^2. && \text{(by Eqn. (1.32b))} && \text{(1.42f)}
\end{aligned}$$

Similarly, it can be shown that

$$\beta^2 - Z^2 = Y^2. \tag{1.43}$$

Combining equations (1.42) and (1.43) obtains

$$\alpha^2 - X^2 = Y^2 = \beta^2 - Z^2. \tag{1.44}$$

This shows that these α, β, X, Y, and Z satisfy the simultaneous system of equations (1.27a) and (1.27b). Also, the way α, β, X, Y, and Z are defined clearly makes them integers. The way H is defined also ensures that it is an integer. It now needs to be shown that H is defined in such a way that it satisfies Theorem 1.4.

$$\begin{aligned}
\frac{1}{X} + \frac{1}{Z} &= \frac{1}{\mu\omega} + \frac{1}{\nu\omega} && \text{(by Eqns. (1.32a) and (1.32c))} && \text{(1.45a)}\\
&= \frac{1}{\omega}\left(\frac{1}{\mu} + \frac{1}{\nu}\right) && \text{(by factoring)} && \text{(1.45b)}\\
&= \frac{d}{\mu+\nu}\frac{\mu+\nu}{\mu\nu} && \text{(by Eqn. (1.33e) and algebra)} && \text{(1.45c)}\\
&= \frac{d}{\mu\nu} && \text{(by algebra)} && \text{(1.45d)}\\
&= \frac{1}{H}. && \text{(by Eqn. (1.32f))} && \text{(1.45e)}
\end{aligned}$$

Thus α, β, X, Y, Z and H are defined in such a way that they all satisfy the necessary equations and are all integers. All that remains to show is that the solutions obtained by the above definition of the variables produces all solutions.
From Lemma 1.6, it is clear that Y^2 can not be of the form p or $2p$ for any prime p. It is also clear that the way $\epsilon, \kappa, \lambda, \mu$, and ν are defined yields the only solutions to $\kappa^2 - \mu^2 = \epsilon = \lambda^2 - \nu^2$. Substituting μ and ν into equation (1.29) yields

$$\frac{1}{\mu} + \frac{1}{\nu} = \frac{\mu + \nu}{\mu\nu} \tag{1.46}$$

This equation needs to be divided by the least expression which will make the right hand side a reciprocal of an integer. This is clearly $\mu + \nu$ divided by the greatest common divisor of $\mu + \nu$ and $\mu\nu$, that is ω. Multiplying all solutions by ω leads to the given solution. Thus, it is the only solution. □

Chapter 2

Sums and Differences of Squares

In this chapter, I will examine which positive integers can be represented as sums of two squares and as the difference of two squares, as well as prove that all positive integers can be represented by the sum of four squares. I will also examine which coefficients can be placed in front of each of the four squares to produce all positive integers.

2.1 Sum of Two Squares

Fermat gave a famous theorem regarding which positive integers can be written as the sum of two squares. This theorem has since been proven by many mathematicians using a variety of different techniques. In order to see which numbers can be represented by the sum of two squares, it is important to start by finding which prime numbers can be written as the sum of two squares.

Theorem 2.1. *If p is an odd prime that can be represented by the sum of two squares, then $p \equiv 1 \pmod 4$.*

Proof. Let p be an odd prime that can be represented by the sum of two squares. So p can be written as

$$p = x^2 + y^2. \tag{2.1}$$

If x and y have the same parity then $x^2 + y^2$ would be an even number, but p is assumed to be an odd prime. Thus, x and y are of opposite parity and it can be assumed without loss of generality that x is odd. Since y is even and x is odd, they can be written as $y = 2k$ and $x = 2m + 1$ where $k, m \in \mathbb{Z}^+$. Substituting this into equation (2.1) and taking it mod 4 obtains:

$$\begin{aligned} p &= (2m+1)^2 + (2k)^2 && \text{(2.2a)} \\ &= 4m^2 + 4m + 4k + 1 && \text{(2.2b)} \\ &\equiv 1 \pmod 4. && \text{(2.2c)} \end{aligned}$$

□

Thus any odd p that can be represented by the sum of two squares is equivalent to 1 (mod 4). Now it needs to be shown which primes p, if any, such that $p \equiv 1 \pmod 4$ can be represented by the sum of two squares. To do this, the following lemmas are needed.

Lemma 2.2 (Wilson's Theorem)**.** *For any prime, p,*

$$(p-1)! \equiv -1 \pmod p. \tag{2.3}$$

Proof. [6] If $p = 2$, then clearly

$$1! \equiv -1 \pmod 2. \tag{2.4}$$

Thus, it can be assumed that p is an odd prime. In the multiplicative group $(\mathbb{Z}/p\mathbb{Z})$, each element has an inverse. In particular, only 1 and $p-1$ are their own inverse. Since each element has an unique inverse, they can each be paired with their respective inverse in $(p-1)!$. As a result, each pair's product evaluates to 1, except for $p-1$, which is its own inverse. Thus:

$$\begin{aligned}(p-1)! &\equiv 1 * (2 * 2^{-1}) * \cdots (p-1) && \text{(2.5a)}\\ &\equiv 1 * 1 * \cdots 1 * (p-1) && \text{(2.5b)}\\ &\equiv p-1 && \text{(2.5c)}\\ &\equiv -1 \pmod p. && \text{(2.5d)}\end{aligned}$$

□

Lemma 2.3. $x^2 \equiv -1 \pmod p$ *has a solution if and only if* $p = 2$ *or* $p \equiv 1 \pmod 4$.
Proof. [6]

Case 1: Let $p = 2$, then

$$-1 \equiv 1 \equiv 1^2 \pmod 2. \tag{2.6}$$

So, for p=2, it is trivial.

Case 2: Assume $p \equiv 1 \pmod 4$. By Wilson's Theorem, Lemma 2.2

$$(p-1)! \equiv -1 \pmod p. \tag{2.7}$$

Also, from modular arithmetic it is clear that

$$\begin{aligned}(p-1)! &= 1 * 2 * 3 * \cdots * (p-1) && \text{(2.8a)}\\ &\equiv 1 * 2 * 3 * \cdots * \frac{p-1}{2} * -\frac{p-1}{2} * \cdots * -2 * -1 && \text{(2.8b)}\\ &\equiv \left(\frac{p-1}{2}!\right)^2 (-1)^{\frac{p-1}{2}} \pmod p. && \text{(2.8c)}\end{aligned}$$

Combining these two facts obtains

$$\left(\frac{p-1}{2}!\right)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p. \tag{2.9}$$

Because $p \equiv 1 \pmod 4$, $\frac{p+1}{2}$ is odd. Thus, $\left(\frac{p-1}{2}!\right)$ is a solution to $x^2 \equiv -1 \pmod p$

Case 3: Assume $p \equiv 3 \pmod 4$. Assume there exists an x such that $x^2 \equiv -1 \pmod p$. Then

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p. \tag{2.10}$$

Fermat's Little Theorem gives us:

$$x^{p-1} \equiv 1 \pmod p. \tag{2.11}$$

Since $p \equiv 3 \pmod 4$, $\frac{p-1}{2}$ is odd. Combining this with the two above facts obtains:

$$1 \equiv x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{2.12}$$

This is a clear contradiction. This means if $p \equiv 3 \pmod p$, then for any x, $x^2 \not\equiv -1 \pmod p$.

□

This lemma gives the following Corollary.

Corollary 2.4. *For p, a prime, if $p \equiv 1 \pmod 4$, then there exists an x such that*

$$1 + x^2 = mp \tag{2.13}$$

for some $0 < m < p$.

Proof. By Lemma 2.3 there exists an x such that $x^2 \equiv -1 \pmod p$ with $0 < x \leq p-1$. By definition, $x^2 + 1 = mp$ for some $m \in \mathbb{Z}^+$ (clearly $m \geq 0$). So

$$0 < mp = x^2 + 1 \leq (p-1)^2 + 1 < p^2. \tag{2.14}$$

Thus $0 < m < p$. □

Once it is known which primes can be written as the sum of two squares, it is important to know if multiplying two such numbers produces another such number. This leads to the following lemma.

Lemma 2.5. *If $a, b, c, d \in \mathbb{Z}^+$, then*

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2 \tag{2.15}$$

Proof.

$$\begin{aligned} (ac - bd)^2 + (ad + bc)^2 &= a^2c^2 + b^2d^2 + a^2d^2 + b^2c^2 && \text{(2.16a)} \\ &= a^2(c^2 + d^2) + b^2(c^2 + d^2) && \text{(2.16b)} \\ &= (a^2 + b^2)(c^2 + d^2). && \text{(2.16c)} \end{aligned}$$

□

Using these lemmas, it can finally be shown that any $p \equiv 1 \pmod 4$ can be written as the sum of two squares.

Theorem 2.6 (Fermat's Theorem on the Sum of Two Squares)**.** *If p is a prime and $p \equiv 1 \pmod 4$, then p can be uniquely represented by the sum of two squares.*

Proof. [1,6] Let $p \equiv 1 \pmod 4$. Consider all non-zero multiples of p that can be written as a sum of two squares. It is know that at least one exists since corollary (2.4) states that there exists a z such that $1 + z^2 = mp$ for some $0 < m < p$. So $z^2 + 1^2 = mp$. Let $x^2 + y^2 = kp$ be the smallest such multiple. By the previous statement, it is clear that $k < p$. If $k = 1$ then p has been represented by the sum of two squares. So, assume that $k > 1$. Consider a, b such that

$$a \equiv x \pmod k \tag{2.17a}$$
$$b \equiv y \pmod k, \tag{2.17b}$$

with $-\frac{k}{2} < a, b \leq \frac{k}{2}$. This means that

$$a^2 + b^2 \equiv x^2 + y^2 \equiv 0 \pmod k \Rightarrow a^2 + b^2 = jk, \tag{2.18}$$

for some $j \in \mathbb{N}$. If $j = 0$, then $a = b = 0$. So $k \mid x$ and $k \mid y$. This means that $k^2 \mid (x^2 + y^2)$, but $x^2 + y^2 = kp$. Thus $k^2 \mid kp$ or $k \mid p$. This is a contradiction since $1 < k < p$. So it can be assumed that $j \neq 0$. Using equation (2.18), a bound on j can be found:

$$jk = a^2 + b^2 \tag{2.19a}$$
$$\leq \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 \tag{2.19b}$$
$$= \left(\frac{k}{2}\right) k. \tag{2.19c}$$

Thus $j \leq \frac{k}{2}$. Using congruences produces:

$$0 \equiv x^2 + y^2 \equiv ax + by \pmod k \tag{2.20a}$$
$$0 = xy - yx \equiv ay - bx \pmod k. \tag{2.20b}$$

Using multiplication and Lemma 2.5 obtains:

$$jk^2p = (a^2 + b^2)(x^2 + y^2) \qquad \text{(multiplying Eqn. (2.18) by } x^2 + y^2) \tag{2.21a}$$
$$= (ax + by)^2 + (ay - bx)^2. \qquad \text{(By Lemma 2.5)} \tag{2.21b}$$

Finally, equations (2.20) imply that $ax + by$ and $ay - bx$ are divisible by k. So dividing both sides of equation (2.21) by k^2 yields

$$\left(\frac{ax + by}{k}\right)^2 + \left(\frac{ay - bx}{k}\right)^2 = jp, \tag{2.22}$$

with $j \leq \frac{k}{2}$. This contradicts k being minimal. Thus $m = 1$, so $p \equiv 1 \pmod 4$ can be represented by the sum of two squares.
To show uniqueness, assume $p = a^2 + b^2 = c^2 + d^2$ with $a, b, c, d \in \mathbb{Z}^+$, $a \neq c$ or d and $b \neq c$ or d. Since p is odd a and b have opposite parity, and c and d have opposite parity. Thus, it can be assumed without loss of generality that a and c are even and b and d are odd. Performing some algebra on p gives:

$$\begin{aligned} p^2 &= (a^2 + b^2)(c^2 + d^2) && && \text{(2.23a)} \\ &= (ac + bd)^2 + (ad - bc)^2 && \text{(By Lemma 2.5)} && \text{(2.23b)} \\ &= (ac - bd)^2 + (ad + bc)^2 && \text{(By Lemma 2.5)} && \text{(2.23c)} \end{aligned}$$

$$\begin{aligned} p(a^2 - c^2) &= a^2(c^2 + d^2) - c^2(a^2 + b^2) && \text{(2.23d)} \\ &= (ad)^2 - (bc)^2 && \text{(2.23e)} \\ &= (ad + bc)(ad - bc) && \text{(2.23f)} \end{aligned}$$

Since a and c are even, and b and d are odd, it is clear that $ac + bd$ and $ac - bd$ are odd and therefore non-zero. Since $a^2 \neq c^2$, equation (2.23f) implies that p divides either $(ad + bc)$ or $(ad - bc)$. It is obvious from equation (2.23b) that $|ad - bc| < p$ and from equation (2.23c) that $ad + bc < p$. The only way for p to divide a number, and for that same number to be less than p is for that number to be 0. This would imply by equation (2.23e) that $a^2 - c^2 = 0$, but with $a, c \in \mathbb{Z}^+$ this can only happen if $a = c$ which contradicts the assumption. Thus, p is uniquely written as a sum of squares. □

Theorem 2.7. *If $p \equiv 3 \pmod 4$ and $p|n = a^2 + b^2$, with $a, b \in \mathbb{N}$, then $p|a$ and $p|b$. In particular, if $p^\alpha \| n$ then α is even.*
Proof. [6] Let $p|n$. Assume $p \nmid a$. This means a has an inverse mod p. Since $p|n$,

$$a^2 + b^2 \equiv 0 \pmod p \Rightarrow b^2 \equiv -a^2 \pmod p \Rightarrow (a^{-1}b)^2 \equiv -1 \pmod p. \tag{2.24}$$

This cannot happen, though, by Lemma 2.3, so this contradicts our assumption that $p \nmid a$. Thus $p|a$ and by a similar argument, $p|b$.
Assume $p^\lambda \| a$ and $p^\mu \| b$ and without loss of generality, $\lambda \geq \mu$. This means that $p^{2\mu}|a^2$ and $p^{2\mu}|b^2$. This implies that

$$p^{2\mu}|a^2 + b^2 = n. \tag{2.25}$$

So,

$$\left(\frac{n}{p^{2\mu}}\right) = \left(\frac{a}{p^{2\mu}}\right)^2 + \left(\frac{b}{p^{2\mu}}\right)^2. \tag{2.26}$$

If $p|\frac{n}{p^{2\mu}}$ then from beginning of this proof, $p|\frac{a}{p^{2\mu}}$ and $p|\frac{b}{p^{2\mu}}$. This contradicts $p^\mu \| b$. This means that $p \nmid \frac{n}{p^{2\mu}}$ and $p^{2\mu} \| n$. □

It should be noted that $2 = 1^2 + 1^2$, so 2 can be written as the sum of two squares. Since it is now known which primes can be written as the sum of two squares, this can be used to show which composite numbers can be written as the sum of two squares using Lemma 2.5.

Theorem 2.8 (Due to Fermat)**.** *n can be written as the sum of two squares if and only if n has a prime factorization of the form*

$$n = 2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} q_1^{2\beta_1} q_2^{2\beta_2} \dots q_t^{2\beta_t} \tag{2.27}$$

where

$$\begin{aligned} p_i &\equiv 1 \pmod 4 \\ q_j &\equiv 3 \pmod 4 \\ \gamma,\, \alpha_l,\, \beta_m &\in \mathbb{N}. \end{aligned}$$

Proof. If $q^{2\alpha+1} \| n$ with $\alpha \in \mathbb{N}$ and $q \equiv 3 \pmod 4$ then by Theorem 2.7 n cannot be written as the sum of two squares. Suppose

$$n = 2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} q_1^{2\beta_1} q_2^{2\beta_2} \dots q_t^{2\beta_t} \tag{2.28}$$

with

$$\begin{aligned} p_i &\equiv 1 \pmod 4 \\ q_j &\equiv 3 \pmod 4 \\ \gamma_k,\, \alpha_l,\, \beta_m &\in \mathbb{Z}^+. \end{aligned}$$

Clearly $2 = 1^2 + 1^2$. Since $p_i \equiv 1 \pmod 4$, by Theorem 2.6, $p_i = a_i^2 + b_i^2$. It is also clear that $q_i^2 = q_i^2 + 0^2$ for $q_i \equiv 3 \pmod 4$. Thus each factor of n can be written as a sum of two squares. By repeated use of Lemma 2.5, it is clear that n is expressible as the sum of two squares. □

2.2 Differences of Two Squares

It has been shown which numbers can be represented as a sum of two squares, it remains to be shown which numbers can be represented by the difference of two squares.

Theorem 2.9. *Any odd positive integer can be written as the difference of two squares.*

Proof. Let ω be an odd positive integer. Let $x = \frac{\omega+1}{2}$ and $y = \frac{\omega-1}{2}$. Clearly since ω is odd, x and y are both integers. Also, it is clear that $x - y = 1$ and $x + y = \omega$. Using these two facts:

$$x^2 - y^2 = (x + y)(x - y) = \omega. \tag{2.29}$$

Thus ω is the difference of the square of two integers. □

Theorem 2.10. *Any number of the form 2ω, where ω is any positive odd integer, cannot be written as the difference of two squares.*

Proof. Let $\alpha = 2\omega$, where ω is an odd positive integer. Assume α can be written as the difference of two squares. $\alpha = x^2 - y^2 = (x-y)(x+y)$. Since x, y are integers, $x+y$ and $x-y$ must have the same parity. Clearly α is even, so $x+y$ and $x-y$ must both also be even. This implies that $\omega = (\frac{x-y}{2})(x+y)$. This is a contradiction, since ω is odd and $x+y$ is even, with $\frac{x-y}{2}$ being an integer. Thus, α cannot be written as the difference of two squares. □

So, any n such that $2\|n$ is not able to be represented by the difference of two squares. It is obvious that

$$2^{2\lambda} = (2^\lambda)^2 - 0^2. \tag{2.30}$$

Thus, 2 raised to any even power can be written as the difference of two squares. Next, consider 2 raised to an odd power.

Theorem 2.11. *For $\lambda \geq 1$, $2^{2\lambda+1}$ can be written as the difference of two squares. In particular,*

$$2^{2\lambda+1} = (2^{\lambda-1}3)^2 - (2^{\lambda-1})^2. \tag{2.31}$$

Proof. For $\lambda \geq 1$,

$$\begin{aligned} 2^{2\lambda+1} &= 2^3 2^{2\lambda-2} && \text{(2.32a)} \\ &= 8(2^{2\lambda-2}) && \text{(2.32b)} \\ &= 9(2^{2\lambda-2}) - 2^{2\lambda-2} && \text{(2.32c)} \\ &= (2^{\lambda-1}3)^2 - (2^{\lambda-1})^2. && \text{(2.32d)} \end{aligned}$$

Thus $2^{2\lambda+1}$ is the difference of two squares. □

It has been shown that if n is an odd integer or if $n = 2^\lambda$, for $\lambda > 1$ then n can be written as the difference of two squares. The following lemma gives a process of combining these two facts into a way of finding all positive integers that can be be represented by a difference of squares.

Lemma 2.12. *For $a, b, x, y \in \mathbb{Z}^+$*

$$(a^2 - b^2)(x^2 - y^2) = (ax + by)^2 - (bx + ay)^2. \tag{2.33}$$

Proof. Let $a, b, x, y \in \mathbb{Z}^+$. Then:

$$\begin{aligned} (a^2 - b^2)(x^2 - y^2) &= (a-b)(a+b)(x-y)(x+y) && \text{(2.34a)} \\ &= (a-b)(x-y)(a+b)(x+y) && \text{(2.34b)} \\ &= ((ax+by) - (bx+ay))((ax+by) + (bx+ay)) && \text{(2.34c)} \\ &= (ax+by)^2 - (bx+ay)^2. && \text{(2.34d)} \end{aligned}$$

□

Theorem 2.13 (Difference of Two Squares)**.** *n is the difference of two squares if and only if n is not of the form 2ω, where ω odd.*

Proof. It has already been shown in Theorem 2.10 that if $n = 2\omega$, and ω is odd, then n is not the difference of two squares. It was also shown in Theorem 2.9 that if n is any odd positive integer, then it can be written as the difference of two squares. Finally it has been shown in equation (2.30) and Theorem 2.11 that 2 raised to any power greater than 1 was able to be represented as the difference of two squares. It just remains to show that $2^\lambda\omega$, where ω is an odd positive integer and λ is an integer greater than one, is representable as the difference of two squares.
Let $n = 2^\lambda\omega$. By Theorem 2.9

$$\omega = \left(\frac{\omega+1}{2}\right)^2 - \left(\frac{\omega-1}{2}\right)^2. \tag{2.35}$$

From equation (2.30) and Theorem 2.11 2^λ can be written as

$$2^\lambda = \alpha^2 - \beta^2. \tag{2.36}$$

Using these two equations, as well as Lemma 2.12 yields:

$$\begin{aligned} n &= 2^\lambda\omega && \text{(2.37a)}\\ &= 2^\lambda\omega && \text{(2.37b)}\\ &= (\alpha^2-\beta^2)\left[\left(\frac{\omega+1}{2}\right)^2 - \left(\frac{\omega-1}{2}\right)^2\right] && \text{(2.37c)}\\ &= \left(\alpha\left(\frac{\omega+1}{2}\right) + \beta\left(\frac{\omega-1}{2}\right)\right)^2 - \left(\beta\left(\frac{\omega+1}{2}\right) + \alpha\left(\frac{\omega-1}{2}\right)\right)^2. && \text{(2.37d)} \end{aligned}$$

Therefore n is the difference of two squares. If $n = 2\omega$, and ω is odd, then n is not the difference of two squares, and if n is anything else, then it can be represented as the difference of two squares. □

This theorem gives the obvious Corollary:

Corollary 2.14. *Any $n \in \mathbb{Z}^+$, can be represented by either:*

$$n = x^2 - y^2 - z^2 \tag{2.38a}$$

or

$$n = x^2 - y^2 + z^2, \tag{2.38b}$$

for some $x, y, z \in \mathbb{N}$.

Proof. Let n be a positive integer.

Case 1: n is odd. If n is odd, then by Theorem 2.13 there exists $x, y \in \mathbb{N}$ such that $n = x^2 - y^2 = x^2 - y^2 \pm 0^2$. Clearly n can be represented by either of the equations (2.38a) or (2.38b) with $z = 0$.

Case 2: n is even. Then both $n \pm 1$ are odd and thus by Theorem 2.13 there exists $x, y \in \mathbb{N}$ such that $n \pm 1 = x^2 - y^2 \Rightarrow n = x^2 - y^2 \mp 1^2$. So clearly n can be represented by either of the equations (2.38a) or (2.38b) with $z = 1$.

□

2.3 Sum of Four Squares

Those numbers that can be represented by the sum of two squares have been examined and the numbers that can be represented by the sum of three squares will be presented in Chapter 3. Unfortunately, with two and three squares, not all numbers can be represented. However all numbers can be represented as a sum of four squares. To show this, a lemma similar to Corollary (2.4) is used as well as an argument similar to the proof of the sum of two squares.

Lemma 2.15. *If p is any odd prime then there exists x, y such that $1 + x^2 + y^2 = mp$ for some integer m with $0 < m < p$.*

Proof. Let p be an odd prime. The set of numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ are all incongruent mod p. If any two numbers of this set were congruent then:

$$r^2 = s^2 \pmod{p} \Rightarrow r = \pm s \pmod{p}. \tag{2.39}$$

It is obvious that with this set of numbers that this only occurs if $r = s$. Similarly, the set of numbers $-1 - 0^2, -1 - 1^2, \ldots, -1 - \left(\frac{p-1}{2}\right)^2$ are all incongruent. The first set contains $\frac{1}{2}(p+1)$ incongruent numbers and the second set contain $\frac{1}{2}(p+1)$ incongruent numbers as well. Both of these sets together then, contain $p+1$ elements, but there are only p residues mod p. By the Pigeon Hole principle, at least of one the numbers in the first set, x^2, is congruent to a number in the second set, $-1 - y^2$, mod p. So there exist $x, y < \frac{1}{2}p$ such that $x^2 \equiv -1 - y^2 \pmod{p}$ or $x^2 + y^2 + 1 = mp$ for some $m \in \mathbb{Z}^+$. Also, $0 < mp = 1 + x^2 + y^2 < 1 + 2\left(\frac{p}{2}\right)^2 < p^2$. So $0 < m < p$. □

Lemma 2.16 (Due to Euler)**.** *For $a, b, c, d, w, x, y, z \in \mathbb{Z}^+$*

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = \\ (aw + bx + cy + dz)^2 + (ax - bw + cz - dy)^2 + \\ (ay - bz - cw + dx)^2 + (az + by - cx - dw)^2\end{aligned} \tag{2.40}$$

Proof. Let $a, b, c, d, w, x, y, z \in \mathbb{Z}^+$

$$(aw + bx + cy + dz)^2 + (ax - bw + cz - dy)^2 + \tag{2.41a}$$
$$(ay - bz - cw + dx)^2 + (az + by - cx - dw)^2 =$$
$$[(aw)^2 + (bx)^2 + (cy)^2 + (dz)^2 + 2(abwx + acwy + adwz + bcxy + bdxz + cdyz)] + \tag{2.41b}$$
$$[(ax)^2 + (bw)^2 + (cz)^2 + (dy)^2 + 2(acxz + bdwy - abwx - adxy - bcwz - cdyz)] +$$
$$[(ay)^2 + (bz)^2 + (cw)^2 + (dx)^2 + 2(adxy + bcwz - abyz - acwy - bdxz - cdwx)] +$$
$$[(az)^2 + (by)^2 + (cx)^2 + (dw)^2 + 2(abyz + cdwx - acxz - adwz - bcxy - bdwy)] =$$
$$[(aw)^2 + (ax)^2 + (ay)^2 + (az)^2] + [(bw)^2 + (bx)^2 + (by)^2 + (bz)^2] + \tag{2.41c}$$
$$[(cw)^2 + (cx)^2 + (cy)^2 + (cz)^2] + [(dw)^2 + (dx)^2 + (dy)^2 + (dz)^2] =$$
$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \tag{2.41d}$$

□

With Lemma 2.16, it is clear that if it can be shown that all primes can be written as the sum of four squares then all positive integers can be written as the sum of four squares.

Theorem 2.17 (Due to Lagrange)**.** *All primes, p, can be written as the sum of four squares.*

Proof. If $p = 2$ then $p = 1^2 + 1^2 + 0^2 + 0^2$. Thus 2 can be written as the sum of four squares. Assume p is an odd prime. Consider all non-zero multiples of p that can be written as a sum of four squares. It is know that at least one exists since Lemma 2.15 states that there exists an a, b such that $0^2 + 1^2 + a^2 + b^2 = mp$ for some $0 < m < p$. Let $w^2 + x^2 + y^2 + z^2 = kp$ be the smallest such multiple. By the previous statement, it is clear that $k < p$. If $k = 1$ then p has been represented by the sum of four squares. Assume that $k > 1$. If k is even then either w, x, y, z are all even, all odd, or two are even and two are odd. Without loss of generality, it can be assumed that w, x have the same parity and that y, z have the same parity. This means:

$$\left(\frac{w+x}{2}\right)^2 + \left(\frac{w-x}{2}\right)^2 + \left(\frac{y+z}{2}\right)^2 + \left(\frac{y-z}{2}\right)^2 = \left(\frac{k}{2}\right)p. \tag{2.42}$$

Since w and x have the same parity and y and z have the same parity, all the terms on the left are integers. This contradicts k being the smallest multiple of p that is representable by the sum of four squares. Thus k is odd. Consider a, b, c, d such that

$$a \equiv w \pmod{k} \tag{2.43a}$$
$$b \equiv x \pmod{k} \tag{2.43b}$$
$$c \equiv y \pmod{k} \tag{2.43c}$$
$$d \equiv z \pmod{k}, \tag{2.43d}$$

with $-\frac{k}{2} < a, b, c, d < \frac{k}{2}$. This means that

$$a^2 + b^2 + c^2 + d^2 \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{k} \Rightarrow a^2 + b^2 + c^2 + d^2 = jk. \tag{2.44}$$

Since

$$jk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2, \tag{2.45}$$

it is known that $j < k$. If $j = 0$ then $a, b, c, d = 0$ and $w, x, y, z \equiv 0 \pmod{k}$. This implies that $k^2 | w^2 + x^2 + +y^2 + z^2 = kp$. So $k|p$, but $1 < k < p$ which is a contradiction. Thus $j \neq 0$. Assume $j > 0$. Using multiplication and Lemma 2.16 obtains:

$$(jk)(kp) = (a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) \tag{2.46a}$$
$$= \alpha^2 + \beta^2 + \gamma^2 + \delta^2 \qquad \text{(By Lemma 2.16)} \tag{2.46b}$$

with:

$$\alpha = aw + bx + cy + dz, \tag{2.47a}$$
$$\beta = ax - bw + cz - dy, \tag{2.47b}$$
$$\gamma = ay - bz - cw + dx \tag{2.47c}$$
$$\delta = az + by - cx - dw. \tag{2.47d}$$

It is clear that $\alpha, \beta, \gamma, \delta \equiv 0 \pmod{k}$ using equations (2.43), so α, β, γ, and δ are all divisible by k. Dividing both sides of equation (2.46) by k^2 results in:

$$jp = \left(\frac{\alpha}{k}\right)^2 + \left(\frac{\beta}{k}\right)^2 + \left(\frac{\gamma}{k}\right)^2 + \left(\frac{\delta}{k}\right)^2. \tag{2.48}$$

Since $j < k$, this is a contradiction of the minimality of k. Thus $k = 1$ and p is expressible as the sum of four squares. □

Because all primes can be represented by the sum of four squares, it is obvious by repeated use of Lemma 2.16 that any positive integer can be represented by the sum of four squares. Knowing this, a natural question to ask is "for what positive integral values of a, b, c, d can all positive integers be expressed in the form" [3] $aw^2 + bx^2 + cy^2 + dz^2$. Finding which values work leads to the following theorem.

Theorem 2.18 (Ramanujan)**.** *The only values of a, b, c, d with $a \leq b \leq c \leq d$ in which*

$$aw^2 + bx^2 + cy^2 + dz^2 \tag{2.49}$$

can be used to produce all positive integers are the 54 values found in Table 2.1.

Proof. [3] Suppose without loss of generality that $a \leq b \leq c \leq d$. The values of a, b, c, d in which an obvious positive integer cannot be represented will be eliminated. Then, it will be shown that these remaining values produce all positive integers.
If $a > 1$ then 1 cannot be expressed by equation (2.49). So

$$a = 1. \tag{2.50}$$

If $b > 2$ then 2 cannot be expressed by equation (2.49). So

$$1 \leq b \leq 2. \tag{2.51}$$

1,1,1,1	1,1,2,4	1,1,2,13	1,2,2,5	1,2,3,9	1,2,4,11
1,1,1,2	1,1,2,5	1,1,2,14	1,2,2,6	1,2,3,10	1,2,4,12
1,1,1,3	1,1,2,6	1,1,3,3	1,2,2,7	1,2,4,4	1,2,4,13
1,1,1,4	1,1,2,7	1,1,3,4	1,2,3,3	1,2,4,5	1,2,4,14
1,1,1,5	1,1,2,8	1,1,3,5	1,2,3,4	1,2,4,6	1,2,5,6
1,1,1,6	1,1,2,9	1,1,3,6	1,2,3,5	1,2,4,7	1,2,5,7
1,1,1,7	1,1,2,10	1,2,2,2	1,2,3,6	1,2,4,8	1,2,5,8
1,1,2,2	1,1,2,11	1,2,2,3	1,2,3,7	1,2,4,9	1,2,5,9
1,1,2,3	1,1,2,12	1,2,2,4	1,2,3,8	1,2,4,10	1,2,5,10

Table 2.1: *Values of* a, b, c, d

Case 1: $b = 1$. If $c > 3$, 3 cannot be expressed by equation (2.49) with $a = 1$ and $b = 1$. So

$$1 \leq c \leq 3. \tag{2.52}$$

Case 1a: $c = 1$. If $d > 7$, 7 cannot be expressed by equation (2.49) with $a = 1$, $b = 1$, and $c = 1$. So

$$1 \leq d \leq 7. \tag{2.53}$$

Case 1b: $c = 2$. If $d > 14$, 14 cannot be expressed by equation (2.49) with $a = 1$, $b = 1$, and $c = 2$. So

$$2 \leq d \leq 14. \tag{2.54}$$

Case 1c: $c = 3$. If $d > 6$, 6 cannot be expressed by equation (2.49) with $a = 1$, $b = 1$, and $c = 3$. So

$$3 \leq d \leq 6. \tag{2.55}$$

Case 2: $b = 2$. If $c > 5$, 5 cannot be expressed by equation (2.49) with $a = 1$ and $b = 2$. So

$$2 \leq c \leq 5. \tag{2.56}$$

Case 2a: $c = 2$. If $d > 7$, 7 cannot be expressed by equation (2.49) with $a = 1$, $b = 2$ and $c = 2$. So

$$2 \leq d \leq 7. \tag{2.57}$$

Case 2b: $c = 3$. If $d > 10$, 10 cannot be expressed by equation (2.49) with $a = 1$, $b = 2$ and $c = 3$. So

$$3 \leq d \leq 10 \tag{2.58}$$

Case 2c: $c = 4$. If $d > 14$, 14 cannot be expressed by equation (2.49) with $a = 1$, $b = 2$ and $c = 4$. So

$$4 \leq d \leq 14 \tag{2.59}$$

Case 2d: $c = 5$. If $d > 10$, 10 cannot be expressed by equation (2.49) with $a = 1$, $b = 2$ and $c = 5$. So

$$5 \leq d \leq 10. \tag{2.60}$$

Thus, all but 55 cases have been eliminated. Ramanujan[3] incorrectly states that the case $w^2 + 2x^2 + 5y^2 + 5z^2$ can be used to represented all positive integers. It can easily be shown that 15 cannot be expressed with this equation. Thus, all but the 54 cases listed in Table 2.1 have been eliminated. All that remains is to show that all positive integers can be expressed by each of these cases. Using Theorem 3.18,

$$\text{If } n \text{ is not of the form } 4^\alpha(8\mu + 7), \text{ then } n = w^2 + x^2 + y^2 \tag{2.61a}$$

According to Ramanujan[3], similar conditions can be found for the values of a, b, c given above. For $\alpha, \mu \in \mathbb{N}$:

$$\text{If } n \text{ is not of the form } 4^\alpha(16\mu + 14), \text{ then } n = w^2 + x^2 + 2y^2. \tag{2.61b}$$

$$\text{If } n \text{ is not of the form } 9^\alpha(9\mu + 6), \text{ then } n = w^2 + x^2 + 3y^2. \tag{2.61c}$$

$$\text{If } n \text{ is not of the form } 4^\alpha(8\mu + 7), \text{ then } n = w^2 + 2x^2 + 2y^2. \tag{2.61d}$$

$$\text{If } n \text{ is not of the form } 4^\alpha(16\mu + 10), \text{ then } n = w^2 + 2x^2 + 3y^2. \tag{2.61e}$$

$$\text{If } n \text{ is not of the form } 4^\alpha(16\mu + 14), \text{ then } n = w^2 + 2x^2 + 4y^2. \tag{2.61f}$$

$$\text{If } n \text{ is not of the form } 25^\alpha(25\mu + 10) \text{ or } 25^\alpha(25\mu + 15), \text{ then } n = w^2 + 2x^2 + 5y^2. \tag{2.61g}$$

This implies that if n is expressible as $aw^2 + bx^2 + cy^2$ then n is not of the form associated with the respective equations. So, for each a, b, c and d, only the cases where n cannot be expressed as three squares with the respective coefficients needs to be considered. To show any $n \in \mathbb{Z}^+$ can be expressed by $w^2 + x^2 + y^2 + dz^2$, it can be assumed that n is of the form $4^\alpha(8\mu + 7)$ for $\alpha, \mu \in \mathbb{N}$. If n is not of this form, then, by Theorem 3.18 , n can be expressed as the sum of three squares and set $z = 0$.

Case 1: $d = 1, 2, 4, 5, 6$. Let $z = 2^\alpha$. Then

$$n - dz^2 = 4^\alpha(8\mu + 7 - d). \tag{2.62}$$

This is clearly not of the form $4^\alpha(8\mu + 7)$, and thus $n - dz^2$, can be expressed in the form $w^2 + x^2 + y^2$ or $n = w^2 + x^2 + y^2 + dz^2$.

Case 2a: $d = 3$, $\mu = 0$. Let $z = 2^\alpha$. Then :

$$n - dz^2 = 4^{\alpha+1}. \tag{2.63}$$

This is clearly also not of the form $4^\alpha(8\mu + 7)$, and thus, $n - 3z^2$ can be expressed in the form $w^2 + x^2 + y^2$ or $n = w^2 + x^2 + y^2 + 3z^2$.

Case 2b: $d = 3$, $\mu \geq 1$ with $\mu \in \mathbb{N}$. Let $z = 2^{\alpha+1}$. Then

$$n - dz^2 = 4^\alpha(8\mu - 5). \tag{2.64}$$

This is clearly not of the form $4^\alpha(8\mu + 7)$, and thus, $n - 3z^2$ can be expressed in the form $w^2 + x^2 + y^2$ or $n = w^2 + x^2 + y^2 + 3z^2$.

Case 3a: $d = 7$, $\mu = 0, 1,$ or 2. Let $z = 2^\alpha$. Then

$$n - dz^2 = 0, 4^{\alpha+1}2 \text{ or } 4^{\alpha+2}. \tag{2.65}$$

These are clearly not of the form $4^\alpha(8\mu + 7)$, and thus, $n - 7z^2$ can be expressed in the form $w^2 + x^2 + y^2$ or $n = w^2 + x^2 + y^2 + 7z^2$.

Case 3b: $d = 7$, $\mu \geq 3$ with $\mu \in \mathbb{N}$. Let $z = 2^{\alpha+1}$. Then

$$n - dz^2 = 4^\alpha(8\mu - 21). \tag{2.66}$$

This is clearly not of the form $4^\alpha(8\mu + 7)$, and thus, $n - 7z^2$ can be expressed in the form $w^2 + x^2 + y^2$ or $n = w^2 + x^2 + y^2 + 7z^2$.

So for $1 \leq d \leq 7$, n is expressible in the form $n = w^2 + x^2 + y^2 + dz^2$
Showing that the other values of a, b, c and d produce all positive integers is similar for all other values of a, b, c and d given. If n is not of the forms listed in equations (2.61), then as Ramanujan states, n is expressible as $w^2 + bx^2 + cy^2$. If n is one of the forms listed in equations (2.61) then the values of z found in Table 2.2 will make $n - dz^2$ not of the associated form and thus $n - dz^2$ is expressible in the form $aw^2 + bx^2 + cx^2$. □

Equation	n is the form	Values of d	Values of μ and α	Values of z
$w^2+x^2+y^2+dz^2$	$4^\alpha(8\mu+7)$	$d=1,2,4,5,6$		$z=2^\alpha$
		$d=3$	$\mu=0$	$z=2^\alpha$
		$d=3$	$\mu\geq 1$	$z=2^{\alpha+1}$
		$d=7$	$\mu=0,1,$ or 2	$z=2^\alpha$
		$d=7$	$\mu\geq 3$	$z=2^{\alpha+1}$
$w^2+x^2+2y^2+dz^2$	$4^\alpha(16\mu+14)$	$2\leq d\leq 5$ or $7\leq d\leq 13$		$z=2^\alpha$
		$d=6$	$\mu=0$	$z=2^\alpha$
		$d=6$	$\mu\geq 1$	$z=2^{\alpha+1}$
		$d=14$	$\mu=0,1,$ or 2	$z=2^\alpha$
		$d=7$	$\mu\geq 3$	$z=2^{\alpha+1}$
$w^2+x^2+3y^2+dz^2$	$9^\alpha(9\mu+6)$	$d=3,4,5$		$z=3^\alpha$
		$d=6$	$\mu=0,1,2,3,4,5$	$z=3^\alpha$
		$d=6$	$\mu\equiv 8 \pmod 9$	$z=3^\alpha$
		$d=6$	$\mu\not\equiv 8 \pmod 9$	$z=2$
$w^2+2x^2+2y^2+dz^2$	$4^\alpha(8\mu+7)$	$d=2,4,5,6$		$z=2^\alpha$
		$d=3$	$\mu=0$	$z=2^\alpha$
		$d=3$	$\mu\geq 1$	$z=2^{\alpha+1}$
		$d=7$	$\mu=0,1,$ or 2	$z=2^\alpha$
		$d=7$	$\mu\geq 3$	$z=2^{\alpha+1}$
$w^2+2x^2+3y^2+dz^2$	$4^\alpha(16\mu+10)$	$3\leq d\leq 9$		$z=2^\alpha$
		$d=10$	$\mu=0,1$	$z=2^\alpha$
		$d=10$	$\mu\geq 2$	$z=2^{\alpha+1}$
$w^2+2x^2+4y^2+dz^2$	$4^\alpha(16\mu+14)$	$d=4,5$ or $7\leq d\leq 13$		$z=2^\alpha$
		$d=6$	$\mu=0$	$z=2^\alpha$
		$d=6$	$\mu\geq 1$	$z=2^{\alpha+1}$
		$d=14$	$\mu=0,1,$ or 2	$z=2^\alpha$
		$d=7$	$\mu\geq 3$	$z=2^{\alpha+1}$
$w^2+2x^2+5y^2+dz^2$	$25^\alpha(25\mu+15)$	$6\leq d\leq 10$		$z=5^\alpha$
	$25^\alpha(25\mu+10)$	$6\leq d\leq 10$	$\mu=0,1$	$z=5^\alpha$
		$6\leq d\leq 10$	$\mu\geq 2$	$z=2(5^\alpha)$

Table 2.2: *Values of z*

Chapter 3

Sum of Three Squares

In this chapter, I will look at which positive integers can be represented as the sum of three squares. Although the proofs given for which positive integers can be represented as the sum of two and four squares are simple, known proofs for which positive integers can be represented as the sum of three squares are much more complicated.

3.1 Fundamental Identity

The numbers that can be represented as the sum of three squares were first discovered by Gauss. Since this discovery, many mathematicians have formulated proofs to verify this idea. The proof discovered by Uspensky and Heaslet will be presented. In this section, the notation $\{X\}_{n=s^2}$ means if $n = s^2$ for $s > 0$ then $\{X\}_{n=s^2}$ equals the quantity X and if n is not a perfect square then $\{X\}_{n=s^2} = 0$.
To begin this proof, what Uspensky calls a "Fundamental Identity" is needed.

Theorem 3.1. *Let $F(x, y, z)$ be an arbitrary real-valued function in which*

$$F(-x, y, z) = -F(x, y, z) \tag{3.1a}$$
$$F(x, -y, -z) = F(x, y, z) \tag{3.1b}$$
$$F(0, y, z) = 0. \tag{3.1c}$$

For any integer, n, consider the partitions of n:

$$n = i^2 + \delta\gamma \tag{3.2a}$$
$$n = h^2 + \alpha\beta \tag{3.2b}$$

with $i, h \in \mathbb{Z}$, $\delta, \gamma, \alpha, \beta \in \mathbb{Z}^+$. *Then,*

$$2 \sum_{(3.2a)} F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta) = \sum_{(3.2b)} F(\alpha + \beta, h, \alpha - \beta) + \left\{ 2 \sum_{j=1}^{2s-1} F(2s - j, s, 2s - j) - \sum_{j=1}^{2s-1} F(2s, j - s, 2j - 2s) \right\}_{n=s^2} \tag{3.3}$$

where the summation indices refer to varying $i, h, \delta, \gamma, \alpha, \beta$ *in the partitions of* n*, and the the summations in the braces are* 0 *unless* $n = s^2$.

Proof. [8] Let n be partitioned as mentioned above. Let

$$S = \sum_{(3.2a)} F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta). \tag{3.4}$$

Split S into three parts, S_1, S_2, S_3, where S_1 corresponds to the partitions in which $2i+\gamma-\delta > 0$, S_2 corresponds to the partitions in which $2i+\gamma-\delta = 0$ and S_3 corresponds to the partitions in which $2i + \gamma - \delta < 0$.

Consider S_1. If i, γ, and δ are solutions to (3.2a) with $2i + \gamma - \delta > 0$, then i', γ' and δ' are corresponding solutions with:

$$i' = \delta - i \tag{3.5a}$$
$$\gamma' = 2i + \gamma - \delta \tag{3.5b}$$
$$\delta' = \delta \tag{3.5c}$$

since:

$$i = \delta' - i' \tag{3.6a}$$
$$\gamma = 2i' + \gamma' - \delta' \tag{3.6b}$$
$$\delta = \delta'. \tag{3.6c}$$

Also, it is clear that:

$$\delta' - 2i' = -\delta + 2i \tag{3.7a}$$
$$\gamma' + i' = \gamma + i \tag{3.7b}$$
$$2\gamma' + 2i' - \delta' = 2\gamma + 2i - \delta. \tag{3.7c}$$

Using these equations one obtains:

$$S_1 = \sum F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta) \qquad \text{(def. of } S_1\text{)} \tag{3.8a}$$
$$= \sum F(\delta' - 2i', \gamma' + i', 2\gamma' + 2i' - \delta') \qquad \text{(by eqns. (3.5))} \tag{3.8b}$$
$$= \sum F(-\delta + 2i, \gamma + i, 2\gamma + 2i - \delta) \qquad \text{(by eqns. (3.7))} \tag{3.8c}$$
$$= -\sum F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta) \qquad (F \text{ is odd wrt } x) \tag{3.8d}$$
$$= -S_1. \qquad \text{(def. of } S_1\text{)} \tag{3.8e}$$

Thus, $S_1 = 0$.
Now consider S_2. Since $2i + \gamma - \delta = 0$,

$$i = \frac{\delta - \gamma}{2}. \tag{3.9}$$

Plugging this into equation (3.2a) one obtains

$$n = \left[\frac{\gamma + \delta}{2}\right]^2. \tag{3.10}$$

So, if $n \neq s^2$ for some $s > 0$, then S_2 reduces to 0. If $n = s^2$ for some $s > 0$, then:

$$\gamma + \delta = 2s \qquad \text{by eqn. (3.10) and } n = s^2, \tag{3.11a}$$
$$\delta - 2i = 2s - \delta \qquad \text{by eqn. (3.9) and eqn. (3.11a)}, \tag{3.11b}$$
$$\gamma + i = s \qquad \text{by eqn. (3.9) and eqn. (3.11a)}, \tag{3.11c}$$
$$2\gamma + 2i - \delta = 2s - \delta \qquad \text{by eqn. (3.9) and eqn. (3.11a)}. \tag{3.11d}$$

δ can assume all values $1, 2, 3, \ldots 2s - 1$. So:

$$S_2 = \sum_{(3.2a)} F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta) \tag{3.12a}$$
$$= \sum_{j=1}^{2s-1} F(2s - j, s, 2s - j) \tag{3.12b}$$

if $n = s^2$ for $s > 0$.
Finally consider S_3. If i, γ, and δ are solutions to (3.2a) with $2i + \gamma - \delta < 0$, then there exist corresponding solutions h, α, and β with:

$$h = \gamma + i \tag{3.13a}$$
$$\alpha = \gamma \tag{3.13b}$$
$$\beta = \delta - \gamma - 2i. \tag{3.13c}$$

The h, α, and β satisfy equation (3.2b) with $\beta - \alpha + 2h > 0$. Conversely, each solution of (3.2b) with $\beta - \alpha + 2h > 0$ corresponds to:

$$i = h - \alpha \tag{3.14a}$$
$$d = \alpha \tag{3.14b}$$
$$\delta = \beta - \alpha + 2h \tag{3.14c}$$

which satisfy equation (3.2a) with $2i + \gamma - \delta < 0$. Thus, using equations (3.13),

$$S_3 = \sum F(\alpha + \beta, h, \alpha - \beta) \tag{3.15}$$

where the summation is over $n = h^2 + \alpha\beta$ for $\beta - \alpha + 2h > 0$. Therefore:

$$2 \sum_{(3.2a)} F(\delta - 2i, \gamma + i, 2\gamma + 2i - \delta) = 2S \tag{3.16a}$$

$$= 2(S_1 + S_2 + S_3) \tag{3.16b}$$

$$= 2(0 + \{\sum F(2s - j, s, 2s - j)\}_{n=s^2} + \sum F(\alpha + \beta, h, \alpha - \beta)) \tag{3.16c}$$

$$= 2 \sum F(\alpha + \beta, h, \alpha - \beta) + \{2 \sum F(2s - j, s, 2s - j)\}_{n=s^2} \tag{3.16d}$$

where the first summation of equation (3.16d) is summed over $n = h^2+\alpha\beta$ with $\beta-\alpha+2h > 0$ and the second summation of equation (3.16d) is summed over $j = 1, 2, \ldots 2s - 1$. With equation (3.2b), the values of h, α and β run through the same values as $-h, \beta$ and α. Using this, with the fact that F is even with respect to y and z, the first summation of equation (3.16d) can be written

$$\sum F(\beta + \alpha, -h, \beta - \alpha) = \sum F(\beta + \alpha, h, \alpha - \beta) \tag{3.17}$$

where the summation extends over solutions to equation (3.2b) with $\beta-\alpha+2h < 0$. Because the summation in equation (3.16d) is multiplied by 2, one of the summations can be made to extend over $\beta - \alpha + 2h < 0$, and the other summation can be made to extend over $\beta - \alpha + 2h > 0$. If $\beta - \alpha + 2h = 0$, then

$$h = \frac{\alpha - \beta}{2}. \tag{3.18}$$

Plugging this into equation (3.2b) results in

$$n = \left[\frac{\alpha + \beta}{2}\right]^2. \tag{3.19}$$

So, if $n \neq s^2$ for some $s > 0$, then the summation in equation (3.16d) covers all possible values of h, α, β. If $n = s^2$ for some $s > 0$, then:

$$\alpha + \beta = 2s \qquad \text{(by eqn. (3.19) and } n = s^2) \tag{3.20a}$$

$$\alpha - \beta = 2s - 2\beta \qquad \text{(by eqn. (3.20a) and eqn. (3.19))} \tag{3.20b}$$

$$h = s - \beta. \qquad \text{(by eqn. (3.20b) and (3.18)).} \tag{3.20c}$$

Therefore, if $\beta - \alpha + 2h = 0$, then, using the fact that $F(x, y, z)$ is even with respect to y and z, the first summation of equation (3.16d) and $\sum_{(3.2b)} F(\alpha + \beta, h, \alpha - \beta)$ differ by

$$\left\{\sum_{j=1}^{2s-1} F(2s, j - s, 2j - 2s)\right\}_{n=s^2}. \tag{3.21}$$

Thus,

$$2\sum_{(3.2a)} F(\delta-2i,\gamma+i,2\gamma+2i-\delta)=\sum_{(3.2b)} F(\alpha+\beta,h,\alpha-\beta)+ \left\{2\sum_{j=1}^{2s-1}F(2s-j,s,2s-j)-\sum_{j=1}^{2s-1}F(2s,j-s,2j-2s)\right\}_{n=s^2}. \quad (3.22)$$

□

3.2 Necessary Lemmas

Since the above identity is true for any function which satisfies equations (3.1), other identities can be derived using specific functions with Theorem 3.1.

Lemma 3.2. *For any n, let n be partitioned so that*

$$n=i^2+\gamma\delta \text{ with } \delta \text{ odd} \quad (3.23)$$

with $i\in\mathbb{Z}$ and $\gamma,\delta\in\mathbb{Z}^+$. Then,

$$\sum_{(3.23)}(-1)^i f(\gamma+i)=\left\{(-1)^{s-1}sf(s)\right\}_{n=s^2} \quad (3.24)$$

where f is anyodd function.

Proof. [8] Let n be partitioned by equations (3.2). Let

$$F(x,y,z)=\begin{cases}0, & \text{if } x \text{ or } z \text{ is even;}\\ (-1)^{\frac{x+z}{2}+y}f(y), & \text{if } x \text{ and } z \text{ are odd;}\end{cases} \quad (3.25)$$

where $f(y)$ is any odd function of y. Clearly by the way $F(x,y,z)$ is defined it satisfies equations (3.1) so Theorem 3.1 is applicable. If x and z are odd, then $F(x,y,z)$ is equal to the bottom equation of (3.25) and is an odd function with respect to y. For the partition of n given in equation (3.2b), h and $-h$ run through the same set of values. Thus, the right hand side of the first summation of equation (3.3) becomes:

$$\sum_{(3.2b)}F(\alpha+\beta,h,\alpha-\beta)=\sum_{(3.2b)}F(\alpha+\beta,-h,\alpha-\beta) \quad (3.26a)$$

$$=\sum_{(3.2b)}-F(\alpha+\beta,h,\alpha-\beta). \quad (3.26b)$$

Thus, $\sum_{(3.2b)}F(\alpha+\beta,h,\alpha-\beta)=0$. Also, if $n\neq s^2$, then

$$\left\{2\sum_{j=1}^{2s-1}F(2s-j,s,2s-j)-\sum_{j=1}^{2s-1}F(2s,j-s,2j-2s)\right\}_{n=s^2}=0. \quad (3.27)$$

If $n = s^2$ for some $s > 0$, then

$$\left\{\sum_{j=1}^{2s-1} F(2s, j-s, 2j-2s)\right\}_{n=s^2} = 0, \tag{3.28}$$

since $2j - 2s$ and $2s$ are even. Also:

$$\left\{2\sum_{j=1}^{2s-1} F(2s-j, s, 2s-j)\right\}_{n=s^2} = 2\sum_{j=1}^{s} F(2s-(2j-1), s, 2s-(2j-1)) \tag{3.29a}$$

$$= 2\sum_{j=1}^{s}(-1)^{2s-2j+1+s} f(s) \tag{3.29b}$$

$$= 2(-1)^{s-1} s f(s). \tag{3.29c}$$

Using this fact with the left hand side of equation (3.3) as well as equation (3.25) yields

$$\sum_{(3.23)} (-1)^i f(\gamma + i) = \left\{(-1)^{s-1} s f(s)\right\}_{n=s^2}. \tag{3.30}$$

□

Lemma 3.3. *For any odd n, let n be partitioned such that:*

$$n = i^2 + 2\gamma\Delta \text{ with } \gamma \text{ odd} \tag{3.31a}$$

$$n = 4H^2 + \alpha\beta \tag{3.31b}$$

with $i, H \in \mathbb{Z}$, $\gamma, \Delta, \alpha, \beta \in \mathbb{Z}^+$ and γ odd. Then:

$$\sum_{(3.31b)} f\left(\frac{\alpha+\beta}{2}\right) = 2\sum_{(3.31a)} f(\Delta + i) + \{s f(s)\}_{n=s^2} \tag{3.32a}$$

and

$$\sum_{(3.31b)} (-1)^H f\left(\frac{\alpha+\beta}{2}\right) = 2\sum_{(3.31a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} f(\Delta + i) + \left\{(-1)^{\frac{s-1}{2}} f(s)\right\}_{n=s^2} \tag{3.32b}$$

for any odd function $f(t)$.

Proof. [8] Let n be odd and partitioned by equations (3.2). Let $F(x, y, z) = 0$ for x or y odd. It then suffices to only consider x and y even or the partitions in which δ is even, i odd, and γ is odd from equation (3.2a) and h is even from equation (3.2b). Thus δ can be replaced with 2Δ and h can be replaced with $2H$. So, n can now be partitioned by equations (3.31). For even values of x and y, if $F(x, y, z)$ is defined in such a way that it satisfies equations (3.1), then Theorem 3.1 yields

$$2\sum_{(3.31a)} F(2\Delta + 2i, \gamma - i, 2\gamma - 2i - 2\Delta) = \sum_{(3.31b)} F(\alpha+\beta, 2H, \alpha-\beta) + \left\{2\sum_{j=1}^{2s-1} F(2s-j, s, 2s-j) - \sum_{j=1}^{2s-1} F(2s, j-s, 2j-2s)\right\}_{n=s^2}. \tag{3.33}$$

Case 1: Let $F(x,y,z) = f\left(\frac{x}{2}\right)$ for x and y even where $f(t)$ is an arbitrary odd function with $f(0) = 0$.
Clearly the way $F(x,y,z)$ is defined, it satisfies equations (3.1). If $n = s^2$ for $s > 0$, then using this function with the second summation of (3.33) yields

$$2\sum_{j=1}^{2s-1} F(2s-j, s, 2s-j) = 0. \tag{3.34}$$

Since n is odd, s is always odd. Using this function with the third summation of (3.33) yields:

$$\sum_{j=1}^{2s-1} F(2s, j-s, 2j-2s) = \sum_{j=1}^{2s-1} f(s) \qquad \text{for } 2s \text{ and } j-s \text{ even} \tag{3.35a}$$

$$= \sum_{k=1}^{s} f(s) \qquad \text{for } 2s \text{ and } 2k-1+s \text{ even} \tag{3.35b}$$

$$= sf(s). \tag{3.35c}$$

Using this function with the first summation of equation (3.33) and combining it with the second and third summation results in

$$2\sum_{(3.31a)} f(\Delta + i) + \{sf(s)\}_{n=s^2} = \sum_{(3.31b)} f\left(\frac{\alpha+\beta}{2}\right). \tag{3.36}$$

Case 2: Let $F(x,y,z) = (-1)^{\frac{y}{2}} f\left(\frac{x}{2}\right)$ for x and y even where $f(t)$ is any odd function with $f(0) = 0$.
Clearly the way $F(x,y,z)$ is defined satisfies equations (3.1). If $n = s^2$ for $s > 0$, then using this function with the second summation of (3.33) obtains yields

$$2\sum_{j=1}^{2s-1} F(2s-j, s, 2s-j) = 0. \tag{3.37}$$

Since n is odd, s is always odd. Using this function with the third summation of (3.33) yields:

$$\sum_{j=1}^{2s-1} F(2s, j-s, 2j-2s) = \sum_{j=1}^{2s-1} (-1)^{\frac{j-s}{2}} f(s) \qquad \text{for } 2s \text{ and } j-s \text{ even} \tag{3.38a}$$

$$= \sum_{k=1}^{s} (-1)^{\frac{2k-1-s}{2}} f(s) \quad \text{for } 2s \text{ and } 2k-1+s \text{ even} \tag{3.38b}$$

$$= (-1)^{\frac{s-1}{2}} f(s). \tag{3.38c}$$

Modular arithmetic gives the identity

$$\frac{\gamma-i}{2}=\frac{\gamma-1}{2}-\frac{i-1}{2}\equiv\frac{\gamma-1}{2}+\frac{i-1}{2}\pmod 2. \tag{3.39}$$

Using this identity with equations (3.38) and the first summation of equation (3.33) and then combining it with the second and third summation results in

$$2\sum_{(3.31a)}(-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}}f(\Delta+i)+\left\{(-1)^{\frac{s-1}{2}}f(s)\right\}=\sum_{(3.31b)}(-1)^{H}f\left(\frac{\alpha+\beta}{2}\right). \tag{3.40}$$

□

Lemma 3.4. *For any n, let n be partitioned so that:*

$$n=i^2+\eta\theta+\epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.41a}$$
$$n=i^2+\gamma\delta \text{ with } \delta \text{ odd} \tag{3.41b}$$

with $i\in\mathbb{Z}$ and $\gamma,\delta,\eta,\theta,\epsilon,\zeta\in\mathbb{Z}^+$. Then

$$\sum_{(3.41a)}(-1)^i[E(\eta-\epsilon+i)-E(\eta+\epsilon+i)]=\sum_{(3.41b)}(-1)^i i[E(i+\gamma)] \tag{3.42}$$

for any even function $E(t)$.

Proof. [8] Fix $\epsilon,\zeta\in\mathbb{Z}^+$, $m\in\mathbb{Z}$ and ζ odd. Let $E(t)$ be any even function. Then, $f(x)=E(x-\epsilon)-E(x+\epsilon)$ is an odd function, so Lemma 3.2 can be applied with the summation over the partitions of m. Let $n=m+\epsilon\zeta$, then the summation is now over

$$n-\epsilon\zeta=i^2+\eta\theta \text{ with } \theta \text{ odd}. \tag{3.43}$$

Applying Lemma 3.2 with $E(t)$ one obtains

$$\sum_{(3.43)}(-1)^i[E(\eta-\epsilon+i)-E(\eta+\epsilon+i)]=\left\{(-1)^{s-1}s[E(s-\epsilon)-E(s+\epsilon)]\right\}_{n-\epsilon\zeta=s^2}. \tag{3.44}$$

So, summing equation (3.44) over all ϵ and ζ, with $\epsilon\zeta<n$ and ζ odd, results in the right hand side of equation (3.44) to be 0, unless $n-\epsilon\zeta=s^2$ for some $s>0$ or

$$n=s^2+\epsilon\zeta \text{ with } \zeta \text{ odd}. \tag{3.45}$$

The summation on the left hand side of equation (3.44) is now over equation (3.41a) Sum-

ming equation (3.44) over all ϵ and ζ with $\epsilon\zeta < n$ and ζ odd yields:

$$\sum_{(3.41a)} (-1)^i[E(\eta-\epsilon+i)-E(\eta+\epsilon+i)] = \sum_{(3.45)} (-1)^{s-1}s[E(s-\epsilon)-E(s+\epsilon)] \tag{3.46a}$$

$$= \sum_{(3.45)} (-1)^{s-1}s[E(s-\epsilon)-E(-s-\epsilon)] \tag{3.46b}$$

$$= \sum_{(3.41b)} (-1)^{i-1}i[E(i-\gamma)] \tag{3.46c}$$

$$= \sum_{(3.41b)} (-1)^{-i-1}(-i)[E(-i-\gamma)] \tag{3.46d}$$

$$= \sum_{(3.41b)} (-1)^{i}i[E(i+\gamma)]. \tag{3.46e}$$

□

Lemma 3.5. *For any n, let n be partitioned so that:*

$$n = i^2 + \gamma\delta \text{ with } \delta \text{ odd} \tag{3.47a}$$

$$n = h^2 + \alpha\beta \text{ with } \alpha+\beta \text{ odd} \tag{3.47b}$$

with $i, h \in \mathbb{Z}$ and $\gamma, \delta, \alpha, \beta \in \mathbb{Z}^+$. Then:

$$2\sum_{(3.47a)} (-1)^i\delta E(\gamma+i) = \sum_{(3.47b)} (-1)^{\beta-1+h}(2h+\beta-\alpha)E(h)+$$

$$2\{(-1)^{s-1}s^2f(s)\}_{n=s^2} \tag{3.48a}$$

and

$$2\sum_{(3.47a)} (-1)^i(\gamma+i)E(\gamma+i) = \sum_{(3.47b)} (-1)^{\beta-1+h}(h)E(h)+$$

$$2\{(-1)^{s-1}s^2f(s)\}_{n=s^2} \tag{3.48b}$$

for any even function $E(t)$.

Proof. [8] Let n be partitioned by equations (3.47a) and (3.47b) Let $F(x,y,z) = 0$ if x or z is even.

Case 1: Let

$$F(x,y,z) = (-1)^{\frac{x-1}{2}+\frac{2y-z-1}{2}}(2y-z)E(y) \text{ if } x \text{ and } z \text{ are odd} \tag{3.49}$$

Clearly, equation (3.49) satisfies equations (3.1), so Theorem 3.1 can be applied. Using this definition of $F(x,y,z)$ in Theorem 3.1 produces equation (3.48a).

Case 2: Let

$$F(x,y,z) = (-1)^{\frac{x-1}{2}+\frac{2y-z-1}{2}}(y)E(y) \text{ if } x \text{ and } z \text{ are odd} \tag{3.50}$$

Clearly, equation (3.50) satisfies equations (3.1), so Theorem 3.1 can be applied. Using this definition of $F(x,y,z)$ in Theorem 3.1 produces equation (3.48b).

□

Lemma 3.6. *For any n, let n be partitioned so that:*

$$n = i^2 + \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.51a}$$

$$n = i^2 + \gamma\delta \text{ with } \delta \text{ odd} \tag{3.51b}$$

with $i \in \mathbb{Z}$ and $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. Then

$$\sum_{(3.51a)} (-1)^i[E(\eta - \epsilon + i) - E(\eta + \epsilon + i)] = \sum_{(3.51b)} (-1)^i[(\delta - \gamma)E(\gamma + i) + (\gamma - \delta)E(i)] \tag{3.52}$$

for any even function $E(t)$

Proof. [8] Let n be partitioned by equations (3.47b), (3.51a), and (3.51b). Let $E(t)$ be an arbitrary even function. In equation (3.47b), n is summed over h and $-h$, so it is clear that

$$\sum_{(3.47b)} (-1)^{\beta-1+h}(h)E(h) = 0. \tag{3.53}$$

Because in equation (3.47b), the summation only happens if $\alpha + \beta$ is odd, n can either be partitioned so:

$$n = h^2 + \alpha\beta \text{ with } \alpha \text{ odd and } \beta \text{ even} \tag{3.54a}$$

or

$$n = h^2 + \alpha\beta \text{ with } \beta \text{ odd and } \alpha \text{ even} \tag{3.54b}$$

Also, partition n so that

$$n = i^2 + \gamma\delta \text{ with } \gamma \text{ and } \delta \text{ odd} \tag{3.55a}$$

and

$$n = i^2 + \gamma\delta \text{ with } \delta \text{ odd and } \gamma \text{ even} \tag{3.55b}$$

If n is partitioned by equation (3.55a), then since δ and γ can be interchanged, it is clear that

$$\sum_{(3.55a)} (-1)^i(\delta - \gamma)E(i) = 0 \tag{3.56}$$

So, it is evident that:

$$\sum_{(3.47b)} (-1)^{\beta-1+h}(2h+\beta-\alpha)E(h) \tag{3.57a}$$

$$= \sum_{(3.47b)} (-1)^{\beta-1+h}(2h)E(h) + \sum_{(3.47b)} (-1)^{\beta-1+h}(\beta-\alpha)E(h) \tag{3.57b}$$

$$= 0 + \sum_{(3.47b)} (-1)^{\beta-1+h}(\beta-\alpha)E(h) \tag{3.57c}$$

$$= \sum_{(3.54a)} (-1)^{\beta-1+h}(\beta-\alpha)E(h) + \sum_{(3.54b)} (-1)^{\beta-1+h}(\beta-\alpha)E(h) \tag{3.57d}$$

$$= \sum_{(3.54a)} (-1)^{h-1}(\beta-\alpha)E(h) + \sum_{(3.54b)} (-1)^{h}(\beta-\alpha)E(h) \tag{3.57e}$$

$$= -2 \sum_{(3.54b)} (-1)^{h}(\alpha-\beta)E(h) \tag{3.57f}$$

$$= -2 \sum_{(3.55b)} (-1)^{i}(\gamma-\delta)E(i) + 0 \tag{3.57g}$$

$$= -2 \sum_{(3.55b)} (-1)^{i}(\gamma-\delta)E(i) - 2 \sum_{(3.55a)} (-1)^{i}(\delta-\gamma)E(i) \tag{3.57h}$$

$$= -2 \sum_{(3.51b)} (-1)^{i}(\gamma-\delta)E(i). \tag{3.57i}$$

Subtracting equation (3.48b) by equation (3.48a) and using equations (3.53) and (3.57) results in

$$\sum_{(3.51b)} (-1)^{i}(i)E(\gamma+i) = \sum_{(3.51b)} (-1)^{i}(\delta-\gamma)E(\gamma+i) + \sum_{(3.51b)} (-1)^{i}(\gamma-\delta)E(i) \tag{3.58}$$

Plugging this into equation (3.42) produces

$$\sum_{(3.51a)} (-1)^{i}[E(\eta-\epsilon+i) - E(\eta+\epsilon+i)] = \sum_{(3.51b)} (-1)^{i}[(\delta-\gamma)E(\gamma+i) + (\gamma-\delta)E(i)] \tag{3.59}$$

□

Lemma 3.7. *For any n, let n be partitioned so that:*

$$n = \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.60a}$$

$$n = \gamma\delta \text{ with } \delta \text{ odd.} \tag{3.60b}$$

with $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. For i fixed, let

$$H_i = \sum_{(3.60a)} [E(\eta-\epsilon+i) + E(\eta-\epsilon-i) - E(\eta+\epsilon+i) - E(\eta+\epsilon-i)]$$

$$- \sum_{(3.60b)} (\delta-\gamma)[E(\gamma+i) + E(\gamma-i) - E(i) - E(-i)] \tag{3.61}$$

for any even function $E(t)$.
For any n and any even function, $E(t)$, if $H_0(n) = 0$ then $H_i(n) = 0$ where $i \geq 0$.

Proof. Let n be partitioned by equations (3.60a) and (3.60b). Fix i and let $H_i(n)$ be defined by equation (3.61) with $E(t)$ any even function. Since $E(t)$ is any even function, the only way to get it to cancel with other terms is in equation (3.61) is if there is a $E(t) - E(t)$ or $E(t) - E(-t)$. Assume $H_0(n) = 0$. The first summation of equation (3.61) becomes

$$H_0 = \sum_{(3.60a)} [E(\eta - \epsilon) + E(\eta - \epsilon) - E(\eta + \epsilon) - E(\eta + \epsilon)]. \tag{3.62}$$

The first two terms of this equation can cancel in a couple of ways.

Case 1: $E(\eta - \epsilon) + E(\eta - \epsilon)$ cancels with $E(\eta' + \epsilon') + E(\eta' + \epsilon')$. This implies that either $\eta - \epsilon = \eta' + \epsilon'$ or $-(\eta - \epsilon) = \eta' + \epsilon'$.

Case 1a: $\eta - \epsilon = \eta' + \epsilon'$. If this is the case, then $\eta - \epsilon + i = \eta' + \epsilon' + i$. Hence the terms in $H_i(n)$ of the form $E(\eta - \epsilon + i) + E(\eta - \epsilon - i)$ will cancel out with the terms $E(\eta' + \epsilon' + i) + E(\eta' + \epsilon' - i)$.

Case 1b: $-(\eta - \epsilon) = \eta' + \epsilon'$. If this is the case, then $-(\eta - \epsilon + i) = \eta' + \epsilon' - i$. Hence the terms in $H_i(n)$ of the form $E(\eta - \epsilon + i) + E(\eta - \epsilon - i)$ will cancel out with the terms $E(\eta' + \epsilon' + i) + E(\eta' + \epsilon' - i)$.

Case 2: $E(\eta - \epsilon) + E(\eta - \epsilon)$ cancels with $2E(\gamma)$ from the second summation. In order for this to happen, n is even. If this is the case then either $\eta - \epsilon = \gamma$ or $-(\eta - \epsilon) = \gamma$. By the same argument as above, $E(\eta - \epsilon + i) + E(\eta - \epsilon - i)$ will cancel out with the terms $E(\gamma + i) + E(\gamma - i)$.

Case 3: $E(\eta-\epsilon)+E(\eta-\epsilon)$ cancels with $2E(0)$ from the second summation. If this is the case then $\eta-\epsilon = 0$ or $\eta = \epsilon$ Hence the terms in $H_i(n)$ of the form $E(\eta-\epsilon+i)+E(\eta-\epsilon-i)$ will cancel out with the terms $E(i) + E(-i)$.

Therefore, if $E(\eta - \gamma) + E(\eta - \gamma)$ cancel with other terms in $H_0(n)$, then $E(\eta - \gamma + i) + E(\eta - \gamma - i)$ will cancel in $H_i(n)$.
By the same argument as above, if $E(\eta + \gamma) + E(\eta + \gamma)$ cancel with other terms in $H_0(n)$, then $E(\eta + \gamma + i) + E(\eta + \gamma - i)$ will cancel in $H_i(n)$.
The terms $2E(\gamma)$ can not cancel out with $2E(\gamma')$ since this would imply that $\gamma = \gamma'$, which can not happen.
The terms $2E(\gamma)$ can also not cancel out with $2E(0)$ since this would imply that $\gamma = 0$, which can not happen.
If n is odd, the the second summation is clearly 0 since δ and γ can be interchanged.
If n is even, the terms $E(0)$ can only cancel with terms from the first summation since they can not cancel with $2E(\gamma)$ or themselves. Thus all terms in $H_0(n)$ have been paired up with terms they cancel with which in turn corresponds with pairs that will cancel in $H_i(n)$. Since all terms in $H_0(n)$ cancel, and there are the exact same number of terms in $H_i(n)$, all the terms in $H_i(n)$ cancel. Thus if $H_0(n) = 0$ then $H_i(n) = 0$. □

Lemma 3.8. *Let $H_i(n)$ be defined by equation (3.61). For any $n \in \mathbb{Z}^+$ and any even function, $E(t)$, if $H_0(n) + 2\sum_{i=1}^{\lfloor\sqrt{n-1}\rfloor}(-1)^i H_i(n-i^2) = 0$, then $H_0(n) = 0$.*

Proof. Let $H_0(n) + 2\sum_{i=1}^{\lfloor\sqrt{n-1}\rfloor}(-1)^i H_i(n-i^2) = 0$. Proceed by induction on n.
For $n = 1$, $H_0(1)$ clear equals 0.
Assume $H_0(n-1) = 0$ for all $n \geq 2$. By Lemma 3.7, since $H_0(n-1) = 0$ for all $n \geq 2$, $H_i(n-1) = 0$ for all $n \geq 2$. This clear makes the summation, $\sum_{i=1}^{\lfloor\sqrt{n-1}\rfloor}(-1)^i H_i(n-i^2) = 0$.
Thus $H_0(n) = 0$. Thus by induction $H_0(n) = 0$ □

Lemma 3.9. *For any n, let n be partitioned so that:*

$$n = \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.63a}$$

$$n = \gamma\delta \text{ with } \delta \text{ odd.} \tag{3.63b}$$

with $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. Then

$$\sum_{(3.63a)} [E(\eta-\epsilon) - E(\eta+\epsilon)] = \sum_{(3.63b)} (\delta-\gamma)[E(\gamma) - E(0)] \tag{3.64}$$

for any even function $E(t)$.
Proof. [8] Let n be partitioned by equations (3.63a) and (3.63b). Let $E(x)$ be an arbitrary even function. Let

$$G_i(x) = E(x+i) + E(x-i), \tag{3.65}$$

which, for a given i, is even with respect to x. For a fixed i, let

$$H_i = \sum_{(3.63a)} [G_i(\eta-\epsilon) - G_i(\eta+\epsilon)] - \sum_{(3.63b)} (\delta-\gamma)[G_i(\gamma) - G_i(0)]. \tag{3.66}$$

Then

$$H_i = \sum_{(3.63a)} [E(\eta-\epsilon+i) + E(\eta-\epsilon-i) - E(\eta+\epsilon+i) - E(\eta+\epsilon-i)] - \sum_{(3.63b)} (\delta-\gamma)[E(\gamma+i) + E(\gamma-i) - E(i) - E(-i)]. \tag{3.67}$$

Clearly, using this equation, equation (3.52) from Lemma 3.6 is equivalent to

$$H_0(n) + 2\sum_{i=1}^{\lfloor\sqrt{n-1}\rfloor}(-1)^i H_i(n-i^2) = 0. \tag{3.68}$$

By Lemma 3.8

$$H_0(n) = 0. \tag{3.69}$$

Thus,

$$\sum_{(3.63a)} [G_0(\eta-\epsilon) - G_0(\eta+\epsilon)] = \sum_{(3.63b)} (\delta-\gamma)\,[G_0(\gamma) - G_0(0)]\,. \tag{3.70}$$

Since G_0 is an arbitrary even function, G_0 can be replaced by E. □

Lemma 3.10. *For any m, let m be partitioned so that:*

$$2m = \lambda\mu + \nu\xi \text{ with } \lambda, \mu, \nu, \xi \text{ odd} \tag{3.71a}$$

$$m = \rho\sigma \text{ with } \sigma \text{ odd} \tag{3.71b}$$

with $\lambda, \mu, \nu, \xi, \rho, \sigma \in \mathbb{Z}^+$. Then

$$\sum_{(3.71a)} [J(\lambda - \nu) - J(\lambda + \nu)] = \sum_{(3.71b)} \rho[J(0) - J(2\rho)] \tag{3.72}$$

for an even function $J(t)$ with $J(t) = 0$ if t is odd.

Proof. [8] Let $J(t)$ be an even function with $J(t) = 0$ if t is odd. Let n be an even number, so $n = 2m$ for some m. Let $2m$ be partitioned by:

$$2m = \lambda\mu + \nu\xi \text{ with } \mu, \xi \text{ odd} \tag{3.73a}$$

$$2m = \phi\sigma \text{ with } \sigma \text{ odd.} \tag{3.73b}$$

Equation (3.73b) clearly implies that ϕ is even. Replacing ϕ with 2ρ, equation (3.73b) can be written

$$m = \rho\sigma \text{ with } \sigma \text{ odd.} \tag{3.74}$$

Since Lemma 3.9 applies for any even function and any n, it can be applied here for $n = 2m$. So,

$$\sum_{(3.73a)} [J(\lambda - \nu) - J(\lambda + \nu)] = \sum_{(3.74)} (\sigma - 2\rho)[J(2\rho) - J(0)] \tag{3.75}$$

Equation (3.73a) implies that either λ and ν are both even or both odd. If they are both even, then they can be replaced with 2λ and 2ν and equation (3.75) can be written

$$\sum_{(3.77a)} [J(2\lambda - 2\nu) - J(2\lambda + 2\nu)] + \sum_{(3.77b)} [J(\lambda - \nu) - J(\lambda + \nu)] = \sum_{(3.74)} (\sigma - 2\rho)[J(2\rho) - J(0)] \tag{3.76}$$

with:

$$m = \lambda\mu + \nu\xi \text{ with } \mu, \xi \text{ odd} \tag{3.77a}$$

and

$$2m = \lambda\mu + \nu\xi \text{ with } \lambda, \mu, \nu, \xi \text{ odd.} \tag{3.77b}$$

Using Lemma 3.9 with $E(2x)$ yields

$$\sum_{(3.77a)} [J(2\lambda - 2\nu) - J(2\lambda + 2\nu)] = \sum_{(3.74)} (\sigma - \rho)[J(2\rho) - J(0)]. \tag{3.78}$$

Subtracting equation (3.76) from equation (3.78) results in

$$\sum_{(3.77b)} [J(\lambda-\nu)-J(\lambda+\nu)] = \sum_{(3.74)} \rho[J(0)-J(2\rho)]. \tag{3.79}$$

□

Lemma 3.11. *For any n, let n be partitioned so that:*

$$n = i^2 + \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.80a}$$
$$n = i^2 + \gamma\delta \text{ with } \delta \text{ odd} \tag{3.80b}$$

with $i \in \mathbb{Z}$ and $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. Then:

$$\sum_{(3.80a)} (-1)^{i+\frac{\zeta-1}{2}} [O(\eta-\epsilon+i)+O(\eta+\epsilon+i)] = -\sum_{(3.80b)} (-1)^{i+\frac{\delta-1}{2}} i[O(i+\gamma)] \tag{3.81}$$

for any arbitrary odd function $O(t)$.

Proof. [8] Fix an $\epsilon, \zeta \in \mathbb{Z}^+$, $m \in \mathbb{Z}$ and ζ odd. Let $O(t)$ be an arbitrary odd function. Then, $f(x) = O(x-\epsilon)+O(x+\epsilon)$ is an odd function, so Lemma 3.2 can be applied with the summation over the partitions of m. Let $n = m + \epsilon\zeta$, then the summation is now over

$$n - \epsilon\zeta = i^2 + \eta\theta \text{ with } \theta \text{ odd}. \tag{3.82}$$

Applying Lemma 3.2 with $O(t)$ and multiplying both sides of the equations by $(-1)^{\frac{\zeta-1}{2}}$ one obtains

$$\sum_{(3.82)} (-1)^{i+\frac{\zeta-1}{2}} [O(\eta-\epsilon+i)+O(\eta+\epsilon+i)] = \\ (-1)^{\frac{\zeta-1}{2}} \left\{(-1)^{s-1} s[O(s-\epsilon)+O(s+\epsilon)]\right\}_{n-\epsilon\zeta=s^2}. \tag{3.83}$$

So, summing equation (3.83) over all ϵ and ζ, with $\epsilon\zeta < n$ and ζ odd, results in the right hand side of equation (3.83) being 0, unless $n - \epsilon\zeta = s^2$ for some $s > 0$ or

$$n = s^2 + \epsilon\zeta \text{ with } \zeta \text{ odd}. \tag{3.84}$$

and the summation on the left hand side of equation (3.83) is now over equation (3.80a)

Summing equation (3.83) over all ϵ and ζ with $\epsilon\zeta < n$ and ζ odd yields:

$$\sum_{(3.80a)} (-1)^{i+\frac{\zeta-1}{2}}[O(\eta-\epsilon+i)+O(\eta+\epsilon+i)] \tag{3.85a}$$

$$= \sum_{(3.84)} (-1)^{\frac{\zeta-1}{2}+(s-1)} s[O(s-\epsilon)+O(s+\epsilon)] \tag{3.85b}$$

$$= \sum_{(3.84)} (-1)^{\frac{\zeta-1}{2}+(s-1)} s[O(s-\epsilon)-O(-s-\epsilon)] \tag{3.85c}$$

$$= \sum_{(3.80b)} (-1)^{\frac{\delta-1}{2}+(i-1)} i[O(i-\gamma)] \tag{3.85d}$$

$$= \sum_{(3.80b)} (-1)^{\frac{\delta-1}{2}+(-i-1)} (-i)[O(-i-\gamma)] \tag{3.85e}$$

$$= -\sum_{(3.80b)} (-1)^{i+\frac{\delta-1}{2}} i[O(i+\gamma)]. \tag{3.85f}$$

□

Lemma 3.12. *For any n, let n be partitioned so that:*

$$n = i^2 + \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.86a}$$

$$n = i^2 + \gamma\delta \text{ with } \delta \text{ odd} \tag{3.86b}$$

with $i \in \mathbb{Z}$ and $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. Then:

$$\sum_{(3.86a)} (-1)^{i+\frac{\zeta-1}{2}}[O(\eta-\epsilon+i)+O(\eta+\epsilon+i)] =$$

$$\sum_{(3.86b)} (-1)^i \left[(-1)^{\frac{\delta-1}{2}}\gamma - \frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right] O(i+\gamma) \tag{3.87}$$

for any arbitrary odd function $O(t)$.

Proof. [8] Let n be partitioned by equations (3.86a) and (3.86b)and by

$$n = i^2 + \alpha\beta \text{ with } \alpha+\beta \text{ odd.} \tag{3.88}$$

Let $O(t)$ be an arbitrary odd function. Let

$$F(x,y,z) = \begin{cases} 0, & \text{if } x \text{ or } z \text{ is even;} \\ (-1)^{\frac{x-1}{2}} zO(y), & \text{if } x \text{ and } z \text{ are odd;} \end{cases} \tag{3.89}$$

Clearly, the way $F(x,y,z)$ is defined, it satisfies equations (3.1), so Theorem 3.1 can be

applied. Using this definition of $F(x,y,z)$ in Theorem 3.1 yields

$$2\sum_{(3.86b)}(-1)^{i+\frac{\delta-1}{2}}(2\gamma+2i-\delta)O(\gamma+i)=\sum_{(3.88)}(-1)^{\frac{\alpha+\beta-1}{2}}(\alpha-\beta)O(h)+\left\{2\sum_{j=1}^{s}(-1)^{s-j}(2s-2j+1)O(s)\right\}_{n=s^2}. \quad (3.90)$$

The second summation of equation (3.90) sums over h and $-h$. Since $O(t)$ is odd, $-O(h)=O(-h)$. This implies that

$$\sum_{(3.88)}(-1)^{\frac{\alpha+\beta-1}{2}}(\alpha-\beta)O(h)=0. \quad (3.91)$$

The third summation can be simplified to

$$\left\{2\sum_{j=1}^{s}(-1)^{s-j}(2s-2j+1)O(s)\right\}_{n=s^2}=2\left\{(-1)^{s-1}sO(s)\right\}_{n=s^2}. \quad (3.92)$$

Using these facts with Lemma 3.2 one obtains:

$$\sum_{(3.86b)}(-1)^{i+\frac{\delta-1}{2}}(2\gamma+2i-\delta)O(\gamma+i)=\left\{\sum_{j=1}^{s}(-1)^{s-j}(2s-2j+1)O(s)\right\}_{n=s^2} \quad (3.93a)$$

$$=\left\{(-1)^{s-1}sO(s)\right\}_{n=s^2} \quad (3.93b)$$

$$=\sum_{(3.86b)}(-1)^{i}O(\gamma+i). \quad (3.93c)$$

Rearranging this equation yields

$$-\sum_{(3.86b)}(-1)^{i+\frac{\delta-1}{2}}iO(i+\gamma)=\sum_{(3.86b)}(\gamma-\frac{1}{2}\delta)(-1)^{i+\frac{\delta-1}{2}}O(i+\gamma)-\frac{1}{2}\sum_{(3.86b)}(-1)^{i}O(i+\gamma). \quad (3.94)$$

Using this with Lemma 3.11 yields

$$\sum_{(3.86a)}(-1)^{i+\frac{\zeta-1}{2}}[O(\eta-\epsilon+i)+O(\eta+\epsilon+i)]=\sum_{(3.86b)}(-1)^{i}\left[(-1)^{\frac{\delta-1}{2}}\gamma-\frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right]O(i+\gamma). \quad (3.95)$$

□

Lemma 3.13. *For any n, let n be partitioned so that:*

$$n = \eta\theta + \epsilon\zeta \text{ with } \theta \text{ and } \zeta \text{ odd} \tag{3.96a}$$

$$n = \gamma\delta \text{ with } \delta \text{ odd} \tag{3.96b}$$

with $\gamma, \delta, \eta, \theta, \epsilon, \zeta \in \mathbb{Z}^+$. Then

$$\sum_{(3.96a)} (-1)^{\frac{\zeta-1}{2}}[O(\eta-\epsilon)+O(\eta+\epsilon)] = \sum_{(3.96b)} \left[(-1)^{\frac{\delta-1}{2}}\gamma - \frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right] O(\gamma) \tag{3.97}$$

for any arbitrary odd function $O(t)$.

Proof. [8] Let n be partitioned by equations (3.96a) and (3.96b). Let $O(x)$ be an arbitrary odd function. Let

$$P_i(x) = O(x+i) + O(x-i), \tag{3.98}$$

which, for a given i, is odd with respect to x. Let

$$Q_i = \sum_{(3.96a)} (-1)^{\frac{\zeta-1}{2}}[P_i(\eta-\epsilon) - P_i(\eta+\epsilon)] - \sum_{(3.96b)} \left[(-1)^{\frac{\delta-1}{2}}\gamma - \frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right][P_i(\gamma) - P_i(0)]. \tag{3.99}$$

Then

$$Q_i = \sum_{(3.96a)} (-1)^{\frac{\zeta-1}{2}}[O(\eta-\epsilon+i)+O(\eta-\epsilon-i)-O(\eta+\epsilon+i)-O(\eta+\epsilon-i)] - \sum_{(3.96b)} \left[(-1)^{\frac{\delta-1}{2}}\gamma - \frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right][O(\gamma+i)+O(\gamma-i)]. \tag{3.100}$$

Clearly, using this equation, equation (3.87) from Lemma 3.12 is equivalent to

$$Q_0(n) + 2\sum_{i=1}^{\lfloor\sqrt{n-1}\rfloor} (-1)^i Q_i(n-i^2) = 0. \tag{3.101}$$

By a similar argument to Lemmas 3.7 and3.8,

$$Q_0(n) = 0. \tag{3.102}$$

Thus,

$$\sum_{(3.96a)} (-1)^{\frac{\zeta-1}{2}}[P_0(\eta-\epsilon) - P_0(\eta+\epsilon)] = \sum_{(3.96b)} \left[(-1)^{\frac{\delta-1}{2}}\gamma - \frac{1+(-1)^{\frac{\delta-1}{2}}\delta}{2}\right][P_0(\gamma)]. \tag{3.103}$$

Since P_0 is an arbitrary odd function, P_0 can be replaced by $O(x)$. □

Lemma 3.14. *For any m, let m be partitioned so that:*

$$2m = \lambda\mu + \nu\xi \text{ with } \lambda, \mu, \nu, \xi \text{ odd} \tag{3.104a}$$

$$m = \rho\sigma \text{ with } \sigma \text{ odd} \tag{3.104b}$$

with $\lambda, \mu, \nu, \xi, \rho, \sigma \in \mathbb{Z}^+$. Then

$$\sum_{(3.104a)} (-1)^{\frac{\xi-1}{2}} [R(\lambda - \nu) + R(\lambda + \nu)] = \sum_{(3.104b)} (-1)^{\frac{\sigma-1}{2}} \rho[R(2\rho)] \tag{3.105}$$

for an odd function $R(t)$ with $R(t) = 0$ if t is odd.

Proof. [8] This follows using the same argument shown in Lemma 3.10 using Lemma 3.13. □

3.3 Sum of Three Squares

Theorem 3.15. *For any n, let $4n + 1$ be partitioned so that:*

$$4n + 1 = i^2 + 4\alpha\beta \text{ with } \beta \text{ odd} \tag{3.106a}$$

$$4n + 1 = 4H^2 + \alpha\beta + 2\psi\phi \text{ with } \alpha, \beta, \psi \text{ and } \phi \text{ odd}, \tag{3.106b}$$

with $i, H \in \mathbb{Z}$ and $\alpha, \beta, \psi, \phi \in \mathbb{Z}^+$ then, for any even function $g(t)$:

$$\sum_{(3.106b)} \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.106a)} \alpha[g(i) - g(i - 2\alpha)], \tag{3.107a}$$

and

$$\sum_{(3.106b)} (-1)^H \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.106a)} (-1)^{\frac{\beta-1}{2} + \frac{i-1}{2}} \alpha[g(i - 2\alpha)]. \tag{3.107b}$$

Proof. [8] Let $m \equiv 3 \pmod 4$. Then clearly, m is not a perfect square. If m is partitioned so that:

$$m = i^2 + 2\gamma\Delta \tag{3.108a}$$

$$m = 4H^2 + \alpha\beta \text{ with } \alpha \text{ and } \beta \text{ odd} \tag{3.108b}$$

with $i, H \in \mathbb{Z}$, $\gamma, \Delta, \alpha, \beta \in \mathbb{Z}^+$ and γ odd, then by Lemma 3.3

$$\sum_{(3.108b)} f\left(\frac{\alpha+\beta}{2}\right) = 2 \sum_{(3.108a)} f(\Delta + i) \tag{3.109a}$$

and

$$\sum_{(3.108b)} (-1)^H f\left(\frac{\alpha+\beta}{2}\right) = 2 \sum_{(3.108a)} (-1)^{\frac{\gamma-1}{2} + \frac{i-1}{2}} f(\Delta + i) \tag{3.109b}$$

for any arbitrary odd function $f(t)$. Since $m \equiv 3 \pmod 4$, m can be written as

$$m = 4n + 1 - 2\psi\phi \tag{3.110}$$

with $n \in \mathbb{Z}$, $\psi, \phi \in \mathbb{Z}^+$, ψ, ϕ both odd and $2\psi\phi < 4n + 1$.
Let $g(x)$ be an even function such that

$$f(x) = g(x - \psi) - g(x + \psi). \tag{3.111}$$

Substituting g into equations (3.109a) and (3.109b) and summing over $4n + 1 - 2\psi\phi$ yields:

$$\sum_{(3.113b)} \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.113a)} \left[g(\Delta + i - \psi) - g(\Delta + i + \psi) \right] \tag{3.112a}$$

and

$$\sum_{(3.113b)} (-1)^H \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.113a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} \left[g(\Delta + i - \psi) - g(\Delta + i + \psi) \right] \tag{3.112b}$$

with:

$$4n + 1 - 2\psi\phi = i^2 + 2\gamma\Delta \tag{3.113a}$$

$$4n + 1 - 2\psi\phi = 4H^2 + \alpha\beta \text{ with } \alpha \text{ and } \beta \text{ odd.} \tag{3.113b}$$

Summing these two summations over all ψ and ϕ results in:

$$\sum_{(3.115b)} \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.115a)} \left[g(\Delta + i - \psi) - g(\Delta + i + \psi) \right] \tag{3.114a}$$

and

$$\sum_{(3.115b)} (-1)^H \left[g\left(\frac{\alpha+\beta}{2} - \psi\right) - g\left(\frac{\alpha+\beta}{2} + \psi\right) \right] = 2 \sum_{(3.115a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} \left[g(\Delta + i - \psi) - g(\Delta + i + \psi) \right] \tag{3.114b}$$

with:

$$4n+1 = i^2 + 2\gamma\Delta + 2\psi\phi \text{ with } \gamma,\ \Delta,\ \psi \text{ and } \phi \text{ odd} \tag{3.115a}$$
$$4n+1 = 4H^2 + \alpha\beta + 2\psi\phi \text{ with } \psi \text{ and } \phi \text{ odd.} \tag{3.115b}$$

Since, in the right hand side of equation (3.114a), i and $-i$ run through the same set of numbers,

$$2\sum_{(3.115a)}[g(\Delta+i-\psi)-g(\Delta+i+\psi)] = \sum_{(3.115a)}[G_i(\Delta-\psi)-G_i(\Delta+\psi)] \tag{3.116}$$

where for a given i,

$$G_i(x) = g(x+i)+g(x-i). \tag{3.117}$$

$G_i(x)$ is clearly an even function. Using Lemma 3.10 on the right hand side of equation (3.116) yields:

$$\sum_{(3.115a)}[G_i(\Delta-\psi)-G_i(\Delta+\psi)] = \sum_{(3.119)}\alpha[G_i(0)-G_i(2\alpha)] \tag{3.118a}$$
$$= \sum_{(3.119)}\alpha[g(i)+g(-i)-g(2\alpha+i)-g(2\alpha-i)] \tag{3.118b}$$
$$= 2\sum_{(3.119)}\alpha[g(i)] + \sum_{(3.119)}\alpha[-g(2\alpha+i)] + \sum_{(3.119)}\alpha[-g(2\alpha-i)] \tag{3.118c}$$
$$= 2\sum_{(3.119)}\alpha[g(i)] + \sum_{(3.119)}\alpha[-g(2\alpha-i)] + \sum_{(3.119)}\alpha[-g(2\alpha-i)] \tag{3.118d}$$
$$= 2\sum_{(3.119)}\alpha[g(i)] + 2\sum_{(3.119)}\alpha[-g(i-2\alpha)] \tag{3.118e}$$
$$= 2\sum_{(3.119)}\alpha[g(i)-g(i-2\alpha)], \tag{3.118f}$$

with the summation being over the partition

$$4n+1 = i^2 + 4\alpha\beta \text{ with } \beta \text{ odd.} \tag{3.119}$$

From equation (3.119), it is clear that in order for $4n+1$ to be partitioned in just a manner, that $i^2 \equiv 1 \pmod 4$. Combining equations (3.116) and (3.118) and plugging it into equation (3.114a) one obtains

$$\sum_{(3.115b)}\left[g\left(\frac{\alpha+\beta}{2}-\psi\right)-g\left(\frac{\alpha+\beta}{2}+\psi\right)\right] = 2\sum_{(3.119)}\alpha[g(i)-g(i-2\alpha)]. \tag{3.120}$$

Also, since in the right hand side of equation (3.114b), i and $-i$ run through the same set of numbers,

$$2 \sum_{(3.115a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} [g(\Delta+i-\psi)-g(\Delta+i+\psi)] = \sum_{(3.115a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} [P_i(\Delta-\psi)-P_i(\Delta+\psi)] \quad (3.121)$$

where for a given i,

$$P_i(x) = g(x+i) - g(x-i). \quad (3.122)$$

$P_i(x)$ is clearly an odd function. Using Lemma 3.14 on the right hand side of equation (3.121) yields:

$$\sum_{(3.115a)} (-1)^{\frac{\gamma-1}{2}+\frac{i-1}{2}} [P_i(\Delta-\psi)-P_i(\Delta+\psi)] \quad (3.123a)$$

$$= \sum_{(3.115a)} -(-1)^{\frac{i-1}{2}+\frac{\gamma-1}{2}} [P_i(\psi-\Delta)+P_i(\Delta+\psi) \quad (3.123b)$$

$$= -\sum_{(3.119)} (-1)^{\frac{i-1}{2}+\frac{\beta-1}{2}} \alpha P_i(2\alpha) \quad (3.123c)$$

$$= -\sum_{(3.119)} (-1)^{\frac{i-1}{2}+\frac{\beta-1}{2}} \alpha [g(2\alpha+i)-g(2\alpha-i)] \quad (3.123d)$$

$$= \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{-i-1}{2}} \alpha g(-i-2\alpha) + \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha g(i-2\alpha) \quad (3.123e)$$

$$= \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha g(i-2\alpha) + \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha g(i-2\alpha) \quad (3.123f)$$

$$= 2 \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha g(i-2\alpha) \quad (3.123g)$$

Combining equations (3.121) and (3.123) and plugging it into equation (3.114b) one obtains

$$\sum_{(3.115b)} (-1)^H \left[g\left(\frac{\alpha+\beta}{2}-\psi\right) - g\left(\frac{\alpha+\beta}{2}+\psi\right)\right] = 2 \sum_{(3.119)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha [g(i-2\alpha)]. \quad (3.124)$$

□

Theorem 3.16. *Let $T(n)$ be the total number of solutions to both equations:*

$$4n+1 = \alpha\beta + (\alpha+\beta-2)\phi \quad (3.125a)$$

$$4n+1 = \alpha\beta + (\alpha+\beta+2)\phi \quad (3.125b)$$

with $\alpha, \beta, \phi \in \mathbb{Z}^+$ *such that* $\alpha + \beta \equiv 0 \pmod 4$ *and* α, β, ϕ *are all odd. Then:*

$$T(2d) + 2T(2d - 2^2) + 2T(2d - 4^2) + \ldots = 4\sigma(d) \tag{3.126a}$$
$$T(2d - 1^2) + T(2d - 3^2) + T(2d - 5^2) + \ldots = 2\sigma(d) \tag{3.126b}$$
$$T(4d - 1^2) + T(4d - 3^2) + T(4d - 5^2) + \ldots = 4\sigma(d) \tag{3.126c}$$

for any odd d *where* $\sigma(d)$ *is the sum of divisors function.*

Proof. [8] Let $K(x)$ be an even function with:

$$K(x) = 0 \text{ if } x^2 > 1 \text{ or } x = 0; \tag{3.127a}$$
$$K(1) = K(-1) = 1. \tag{3.127b}$$

Since $K(x)$ is an even function, it can be used in Theorem 3.15. Let n be partitioned by:

$$4n + 1 = i^2 + 4\alpha\beta \text{ with } \beta \text{ odd} \tag{3.128a}$$
$$4n + 1 = 4H^2 + \alpha\beta + 2\psi\phi \text{ with } \alpha,\ \beta,\ \psi \text{ and } \phi \text{ odd}. \tag{3.128b}$$

Then by Theorem 3.15

$$\sum_{(3.128b)} \left[K\left(\frac{\alpha+\beta}{2} - \psi\right) - K\left(\frac{\alpha+\beta}{2} + \psi\right)\right] = 2 \sum_{(3.128a)} \alpha[K(i) - K(i - 2\alpha)] \tag{3.129a}$$

and

$$\sum_{(3.128b)} (-1)^H \left[K\left(\frac{\alpha+\beta}{2} - \psi\right) - K\left(\frac{\alpha+\beta}{2} + \psi\right)\right] = 2 \sum_{(3.128a)} (-1)^{\frac{\beta-1}{2} + \frac{i-1}{2}} \alpha[K(i - 2\alpha)]. \tag{3.129b}$$

By the definition of $K(x)$, $K\left(\frac{\alpha+\beta}{2} - \psi\right) = 0$, except for when $\psi = \frac{\alpha+\beta}{2} \pm 1$, in which case the function equals 1. Since ψ is odd, then $\alpha + \beta \equiv 0 \pmod 4$. Let $T(n)$ denote the total number of solutions to the equations:

$$4n + 1 = \alpha\beta + (\alpha + \beta - 2)\phi \tag{3.130a}$$
$$4n + 1 = \alpha\beta + (\alpha + \beta + 2)\phi \tag{3.130b}$$

with $\alpha, \beta, \phi \in \mathbb{Z}^+$ such that $\alpha + \beta \equiv 0 \pmod 4$ and α, β, ϕ are all odd. Thus, the left hand side of equation (3.129a) is clearly equivalent to

$$\sum_{h=-\lfloor\sqrt{n-1}\rfloor}^{\lfloor\sqrt{n-1}\rfloor} T(n - h^2), \tag{3.131}$$

and the left hand side of equation (3.129b) is clearly equivalent to

$$\sum_{h=-\lfloor\sqrt{n-1}\rfloor}^{\lfloor\sqrt{n-1}\rfloor} (-1)^h T(n-h^2). \tag{3.132}$$

Looking at the first term of the right hand side of equation (3.129a), it is clear that

$$2 \sum_{(3.128a)} \alpha K(i) = 4 \sum_{(3.134)} \alpha, \tag{3.133}$$

with the summation being over the partition of n,

$$n = \alpha\beta \text{ with } \beta \text{ odd}. \tag{3.134}$$

The cases where $n = 2d$ or $n = 4d$ with d odd will be considered.

Case 1: $n = 2d$. Then

$$4 \sum_{(3.134)} \alpha = 8\sigma(d) \tag{3.135}$$

where $\sigma(d)$ is the sum of the divisors of d.
Looking now at the second term of the right hand side of equation (3.129a), it is clear, from the definition of K, that $K(i-2\alpha) = 0$ unless $i - 2\alpha = \pm 1$ or

$$i = 2\alpha \pm 1. \tag{3.136}$$

Thus, the partition of n in equation (3.128a) can be written

$$2d = \alpha(\alpha + \beta \pm 1) \text{ with } \beta \text{ odd}. \tag{3.137}$$

Clearly, α and $\alpha + \beta \pm 1$ have the same parity, but this is impossible if $n = 2d$, d odd. Thus

$$-2 \sum_{(3.128a)} \alpha K(i-2\alpha) = 0. \tag{3.138}$$

The same argument implies

$$\sum_{(3.128a)} (-1)^{\frac{\beta-1}{2}+\frac{i-1}{2}} \alpha K(i-2\alpha) = 0. \tag{3.139}$$

Thus for $n = 2d$:

$$\sum_{h=-\lfloor\sqrt{2d-1}\rfloor}^{\lfloor\sqrt{2d-1}\rfloor} T(2d-h^2) = 8\sigma(d) \tag{3.140a}$$

$$\sum_{h=-\lfloor\sqrt{2d-1}\rfloor}^{\lfloor\sqrt{2d-1}\rfloor} (-1)^h T(2d-h^2) = 0. \tag{3.140b}$$

Adding equations (3.140a) and (3.140b) yields

$$T(2d) + 2T(2d - 2^2) + 2T(2d - 4^2) + \ldots = 4\sigma(d). \tag{3.141}$$

Subtracting equation (3.140b) from equation (3.140a) yields

$$T(2d - 1^2) + T(2d - 3^2) + T(2d - 5^2) + \ldots = 2\sigma(d). \tag{3.142}$$

Case 2: $n = 4d$ for d odd. Then

$$4 \sum_{(3.134)} \alpha = 16\sigma(d) \tag{3.143}$$

where $\sigma(d)$ is the sum of the divisors of d.
Looking now at the second term of the right hand side of equation (3.129a), it is clear, from the definition of K, that $K(i - 2\alpha) = 0$ unless $i - 2\alpha = \pm 1$ or

$$i = 2\alpha \pm 1. \tag{3.144}$$

So, the partition of n in equation (3.128a) can be written

$$4d = \alpha(\alpha + \beta \pm 1) \text{ with } \beta \text{ odd}. \tag{3.145}$$

This can only occur if α is even. Let $\alpha = 2\theta$. Then

$$-2 \sum_{(3.128a)} \alpha K(i - 2\alpha) = -4 \sum_{(3.147)} \theta \tag{3.146}$$

with the summation being over the partition of d,

$$d = \theta \left(\theta + \frac{\beta \pm 1}{2} \right) \text{ with } \beta \text{ odd}. \tag{3.147}$$

Similarly,

$$2 \sum_{(3.128a)} (-1)^{\frac{\beta-1}{2} + \frac{i-1}{2}} \alpha [K(i - 2\alpha)] = 4 \sum_{(3.147)} (-1)^{\frac{\beta \pm 1}{2} + \theta} \theta \tag{3.148a}$$

$$= -4 \sum_{(3.147)} \theta \qquad \left(\text{since } \frac{\beta \pm 1}{2} + \theta \text{ is odd}\right). \tag{3.148b}$$

Thus for $n = 4d$,

$$\sum_{h=-\lfloor\sqrt{4d-1}\rfloor}^{\lfloor\sqrt{4d-1}\rfloor} T(4d - h^2) = 16\sigma(d) - 4 \sum_{(3.147)} \theta \tag{3.149a}$$

$$\sum_{h=-\lfloor\sqrt{4d-1}\rfloor}^{\lfloor\sqrt{4d-1}\rfloor} (-1)^h T(4d - h^2) = -4 \sum_{(3.147)} \theta. \tag{3.149b}$$

Subtracting equation (3.149b) from equation (3.149a) results in

$$T(4d - 1^2) + T(4d - 3^2) + T(4d - 5^2) + \ldots = 4\sigma(d). \tag{3.150}$$

□

Theorem 3.17. *The function, $T(n)$, defined in Theorem 3.16 always has a positive value.*
Proof. [8]

Case 1: n is odd. Let $\alpha = 2n+1$, $\beta = 1$ and $\phi = 1$. Then α, β and ϕ are clearly a solution to equation (3.125a) with α, β and ϕ all odd and $\alpha + \beta \equiv 0 \pmod 4$.

Case 2: n is even. Let $\alpha = 2n-1$, $\beta = 1$ and $\phi = 1$. Then α, β and ϕ are clearly a solution to equation (3.125b) with α, β and ϕ all odd and $\alpha + \beta \equiv 0 \pmod 4$.

□

Theorem 3.18 (Sum of Three Squares)**.** *Let n be a positive integer, then n is expressible as the sum of three squares if and only if n is not of the form $4^\lambda(8\alpha+7)$ for $\lambda, \alpha \in \mathbb{N}$.*
Proof. [8] Jacobi's Four Square Theorem deals with the number of representation of a number as the sum of four squares (see[4] for a proof of Jacobi's Theorem). By Jacobi's Theorem, the number of integer solutions to

$$4d = w^2 + x^2 + y^2 + z^2 \tag{3.151}$$

in odd numbers is $16\sigma(d)$ for d odd. Let $N_3(n)$ be the number of representations of n by the sum of three squares. If a number is equivalent to 3 (mod 4) then, if it is representable as the sum of three squares, each must be odd by congruence consideration. Thus, for any odd d

$$N_3(4d-1^2) + N_3(4d-3^2) + N_3(4d-5^2) + \ldots = 8\sigma(d). \tag{3.152}$$

Using equation (3.126c) from Theorem 3.16 it is clear that

$$2[T(4d-1^2)+T(4d-3^2)+T(4d-5^2)+\ldots] = N_3(4d-1^2)+N_3(4d-3^2)+N_3(4d-5^2)+\ldots. \tag{3.153}$$

Since this equation holds for all odd values of d, it is clear that:

$$\text{For } d=1, \qquad 2T(3) = N_3(3). \tag{3.154a}$$
$$\text{For } d=3, \qquad 2T(11) + 2T(3) = N_3(11) + N_3(3). \tag{3.154b}$$
$$\text{For } d=5, \qquad 2T(19) + 2T(11) + 2T(3) = N_3(19) + N_3(11) + N_3(3). \tag{3.154c}$$

Thus, by an induction argument,

$$N_3(4d-1) = 2T(4d-1). \tag{3.155}$$

Since $4d-1$ represents any number of the form $8M+3$,

$$N_3(8M+3) = 2T(8M+3). \tag{3.156}$$

By Theorem 3.17, $2T(8M+3)$ is a positive number, so for any $M \in \mathbb{Z}^+$, any number of the form $8M+3$ can be represented by the sum of three squares.
By Jacobi's Theorem, the number of integer solutions to

$$2d = w^2 + y^2 + x^2 + z^2 \tag{3.157}$$

in which x is positive and odd is $6\sigma(d)$ for d odd. So

$$N_3(2d-1^2)+N_3(2d-3^2)\ldots=6\sigma(d). \tag{3.158}$$

Using equation (3.126b) from Theorem 3.16 it is clear that

$$3[T(2d-1^2)+T(2d-3^2)\ldots]=N_3(2d-1^2)+N_3(2d-3^2)\ldots. \tag{3.159}$$

Since this equation holds for all odd values of d,

$$N_3(2d-1)=3T(2d-1). \tag{3.160}$$

By Theorem 3.17, $3T(2d-1)$ is a positive number, so for any $M\in\mathbb{Z}^+$, any number of the form $4M+1$ can be represented by the sum of three squares.
By Jacobi's Theorem, the number of integer solutions to

$$2d=w^2+y^2+x^2+z^2 \tag{3.161}$$

in which x is even is $12\sigma(d)$ for d odd. So

$$N_3(2d)+2N_3(2d-2^2)+2N_3(2d-4^2)\ldots=12\sigma(d). \tag{3.162}$$

Using equation (3.126a) from Theorem 3.16 it is clear that

$$3[T(2d)+2T(2d-2^2)+2T(2d-4^2)+\ldots]=N_3(2d)+2N_3(2d-2^2)+2N_3(2d-4^2)\ldots. \tag{3.163}$$

Since this equation holds for all odd values of d,

$$N_3(2d)=3T(2d). \tag{3.164}$$

By Theorem 3.17, $3T(2d)$ is a positive number, so for any $M\in\mathbb{Z}^+$, any number of the form $8M+2$ or $8M+6$ can be represented by the sum of three squares.
Looking at the equation $x^2+y^2+z^2 \mod 8$, it is clear that

$$x^2+y^2+z^2\equiv 0,1,2,3,4,5 \text{ or } 6 \pmod 8. \tag{3.165}$$

Thus, numbers of the form $8M+7$ cannot be represented by the sum of three squares by congruence considerations.
Again, looking at the equation $x^2+y^2+z^2 \mod 8$, if at least one of x,y or z is odd then

$$x^2+y^2+z^2\equiv 1,2,3,5,6 \pmod 8. \tag{3.166}$$

Thus, the equation $4e=x^2+y^2+z^2$ can only hold if x,y and z are all even for any $e\in\mathbb{N}$. Let $x=2\hat{x}$, $y=2\hat{y}$, $z=2\hat{z}$. Then the number of solutions to $4e=x^2+y^2+z^2$ is equivalent to the number of solutions to $e=\hat{x}^2+\hat{y}^2+\hat{z}^2$. Thus if e is representable as the sum of three squares, then so is $4e$. So by the previous work in the theorem, all integers can be expressed by the sum of three squares except those of the form $4^\lambda(8\alpha+7)$ for $\lambda,\alpha\in\mathbb{N}$. □

Bibliography

[1] Carmichael, R. D. (1915). *Diophantine Analysis*, volume 16 of *Mathematical Monographs*. John Wiley & Sons, Inc.

[2] Gardner, M. (1979). *Mathematical Circus*. New York: Random House.

[3] Hardy, G. H., Seshu Aiyar, P. V., and Wilson, B. M., editors. *Collected Papers of Srinivasa Ramanujan*. Cambridge:University Press.

[4] Hirschhorn, M. D. A simple proof of jacobi's four-square theorem.

[5] Mordell, L. J. (1969). *Diophantine Equations*, volume 30 of *Pure and Applied Mathematics*. London and New York: Academic Press.

[6] Pinner, C. Class lecture. Introduction to Number Theory, Kansas State University, Manhattan, KS.

[7] Sutcliffe, A. (1963). Complete solution of the ladder problem in integers. *The Mathematical Gazette*, 47(360):133–136.

[8] Uspensky, J. V. and Heaslet, M. A. (1939). *Elementary Number Theory*. McGraw-Hill Book Company, Inc.