An Investigation of Some Nonlinear Diophantine Equations

by

Sebastiano Galletti

Mathematics Department

California Polytechnic State University

San Luis Obispo

2014

APPROVAL PAGE

TITLE: An Investigation of Some Nonlinear Diophantine Equations

AUTHOR: Sebastiano Galletti

DATE SUBMITTED: June 2014

_____	_____
Senior Project Advisor	Signature
_____	_____
Mathematics Department Chair	Signature

TABLE OF CONTENTS

Section 0: Introduction and Note to the Reader

An equation with the restriction that only integer (or sometimes rational) solutions are sought is called a ***diophantine equation***. When it comes to linear diophantine equations we could easily show how all solutions in integers can be found. But what about nonlinear diophantine equations? That will be the scope of this investigative paper. Many results have been established about particular nonlinear diophantine equations, as well as certain families of nonlinear diophantine equations. We will investigate several types of these types of equations.

First, we will consider the diophantine equation of the form $x^2 + y^2 = z^2$. We will try to find an explicit formula to find all triples (x, y, z) that give solutions to this equation. After studying this particular diophantine equation we will shift our attention to the famous equation $x^n + y^n = z^n$, where n is an integer greater than 2. Fermat stated that there are no solutions of this diophantine equation when $n > 2$ and a proof of that statement had eluded mathematicians for nearly 350 years. We will discuss how the proof of this statement finally came to be and how its discovery ended one of the greatest challenges to mathematics. We will also see an interesting conjecture that will ultimately imply Fermat's last theorem.

Next, we will consider the problem of representing integers as the sums of squares. We will determine which integers can be written as the sum of two squares. Furthermore, we will see that every positive integer is the sum of four squares.

Finally, we will study the diophantine equation $x^2 - dy^2 = 1$, known as Pell's equation. We will show that the solutions of this equation can be found using the simple continued fraction of $\sqrt{d}$, providing an example of the usefulness of continued fractions.

We will be investigating these topics using the following format:

Definition. Definitions will be our key objects during this paper and will facilitate an agreement on the meaning of terms and phrases. The term or phrase that is being defined will always be in ***emphasized text*** and no defined term will ever be used loosely.

Example. Examples will be provided to show emphasis to a new idea and encourage a discussion between readers. These will also be used to show how an abstract statement can be used in a concrete setting.

Fact. Facts will be used without proof and taken to be true statements. We will use these facts to prove what we are investigating and we take them to be true without proof so we do not stray too far from our main objective during the given section.

Lemma. Lemmas will act as propositions that we will prove throughout our discussion and use the results to help us prove grander statements.

Theorem. Theorems are true statements that will be very valuable to our discussion. We will prove every theorem we face during our investigation and the theorems will depend on our definitions, facts, and lemmas.

Now, let us begin...

Section 1: Pythagorean Triples

We will begin our discussion of nonlinear diophantine equations with the idea of Pythagorean Triples. We know from the Pythagorean Theorem that the sum of the lengths squared of a right triangle is equal to the square of the length of the hypotenuse. In fact, any time a triangle has this very special property, we can conclude that it is has to be a right triangle. In this section, we will be interested in finding all right triangles with integral side lengths. In particular, we will want to find all triples of positive integers (x, y, z) that satisfy the diophantine equation

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

These triples of positive integers satisfying this equation are called ***Pythagorean triples*** after the Greek mathematician Pythagoras. Similarly, any right triangle with a Pythagorean triple corresponding to its side lengths and hypotenuse is called a ***Pythagorean triangle***.

Example 1.1. The triples $(3, 4, 5)$, $(5, 12, 13)$, and $(8, 15, 17)$ are Pythagorean triples because $3^2 + 4^2 = 5^2$, $5^2 + 12^2 = 13^2$, and $8^2 + 15^2 = 17^2$. You may remember these as some of your most favorite right triangles from your early academics.

Definition. A Pythagorean triple (x, y, z) is called ***primitive*** if $x, y,$ and z are relatively prime, that is, if $\gcd(x, y, z) = 1$. We call a triangle a ***primitive right triangle*** if its sides have lengths from a primitive Pythagorean triple.

Example 1.2. The Pythagorean triples from the previous example are primitive. However, the Pythagorean triple $(6, 8, 10)$ is not primitive because $\gcd(6, 8, 10) = 2$.

Let (x, y, z) be a Pythagorean triple with $\gcd(x, y, z) = d$, where $d > 1$. Then there exists integers (x_1, y_1, z_1) such that $x = dx_1$, $y = dy_1$, and $z = dz_1$, and $\gcd(x_1, y_1, z_1) = 1$. Now, since

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

we have

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

so that

$$x_1^2 + y_1^2 = z_1^2$$

Therefore, (x_1, y_1, z_1) is a primitive Pythagorean triple and (x, y, z), which was the original triple, is just an integral multiple of the primitive Pythagorean triple.

Furthermore, we would like to take note that any integral multiple of a primitive Pythagorean triple is also a Pythagorean triple. In fact, any integral multiple of any Pythagorean triple—primitive or not—is again a Pythagorean triple. As a consequence of this fact, all Pythagorean triples can be found by forming integral multiples of primitive Pythagorean triples. We will now list some lemmas that will help us in our search for all forms of Pythagorean triples.

Lemma 1.1. If (x, y, z) is a primitive Pythagorean triple, then $\gcd(x, y) = \gcd(x, z) = \gcd(y, z) = 1$.

Proof. Suppose that (x, y, z) is a Pythagorean triple and that $(x, y) > 1$. Then, there is a prime p such that $p \mid (x, y)$, so that $p \mid x$ and $p \mid y$. Because p divides both x and y, we know that $p \mid (x^2 + y^2) = z^2$. Because $p \mid z^2$, we can conclude that $p \mid z$. This is a contradiction, because (x, y, z) is a primitive Pythagorean triple, which means $\gcd(x, y, z) = 1$. Therefore $\gcd(x, y) = 1$. In a similar manner, we can easily show that $\gcd(x, z) = \gcd(y, z) = 1$.

■

Lemma 1.2. If (x, y, z) is a primitive Pythagorean triple, then x and y have different parity.

Proof. Let (x, y, z) be a primitive Pythagorean triple. By Lemma 1.1, we know that $\gcd(x, y) = 1$, so that x and y cannot both be even. Also, x and y cannot both be odd. If x and y were both odd, then we would have

$$x^2 \equiv y^2 \equiv 1 \ (mod\ 4)$$

so that

$$z^2 = x^2 + y^2 \equiv 2 \ (mod\ 4)$$

This is impossible because if z is even then $z^2 \equiv 0 \ (mod\ 4)$ and if z is odd then $z^2 \equiv 1 \ (mod\ 4)$ for all integers a and in general $a^2 \equiv 0$ or $1 \ (mod\ 4)$. Therefore, x and y must have different parity.

■

Lemma 1.3. If r, s, and t are positive integers such that $\gcd(r, s) = 1$ and $rs = t^2$, then there exists integers m and n such that $r = m^2$ and $s = n^2$.

Proof. If $r = 1$ or $s = 1$ then the lemma is trivial, so we may suppose that $r > 1$ and $s > 1$. Let the prime-power factorization of r, s, and t be

$$r = p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u}$$

$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v}$$

and

$$t = q_1^{b_1} q_2^{b_2} \cdots q_k^{b_k}.$$

Because $\gcd(r, s) = 1$, the primes occurring in the factorizations of r and s are distinct. Because $rs = t^2$, we have

$$p_1^{a_1} p_2^{a_2} \cdots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \cdots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \cdots q_k^{2b_k}$$

From the fundamental theorem of arithmetic, the prime powers occurring on the two sides of the above equation are the same. Hence, each p_i must be equal to q_j for some j with matching exponents, so that $a_i = 2b_j$. Consequently, every exponent a_i is even, and therefore $\frac{a_i}{2}$ is an integer. We see that $r = m^2$ and $s = n^2$, where m and n are the integers

$$m = p_1^{\frac{a_1}{2}} p_2^{\frac{a_2}{2}} \cdots p_u^{\frac{a_u}{2}}$$

and

$$n = p_{u+1}^{\frac{a_{u+1}}{2}} p_{u+2}^{\frac{a_{u+2}}{2}} \cdots p_v^{\frac{a_v}{2}}.$$

■

Now, with the help of these three lemmas, we can prove a major result that will describe all primitive Pythagorean triples.

Theorem 1.4. The triple (x, y, z) of positive integers is a primitive Pythagorean triple, with y even, if and only if there are relatively prime positive integers m and n, with $m > n$ and opposite parity, such that

$$x = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2.$$

Proof. Let (x, y, z) be a primitive Pythagorean triple. We will show that there exists integers m and n that satisfy the statements in the theorem. Lemma 1.2 tells us that x and y have different parity. Because we have assumed that y is even, x and z must both be odd. Hence, $z + x$ and $z - x$ are both even, so that there are positive integers r and s with $r = \frac{z+x}{2}$ and $= \frac{z-x}{2}$.

Because $x^2 + y^2 = z^2$, we have $y^2 = z^2 - x^2 = (z + x)(z - x)$. Hence,

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

Take note that $\gcd(r, s) = 1$. To see this, let $\gcd(r, s) = d$. Because $d \mid r$ and $d \mid s$, $d \mid (r + s) = z$ and $d \mid (r - s) = x$. This means that $d \mid \gcd(x, z) = 1$, so that $d = 1$.

Using Lemma 1.3, we see that there are positive integers m and n such that $r = m^2$ and $s = n^2$. Writing x, y, and z in terms of m and n, we have

$$x = r - s = m^2 - n^2,$$

$$y = \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn,$$

$$z = m^2 + n^2.$$

We also see that $\gcd(m, n) = 1$ because any common divisor of m and n must also divide $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 - n^2$, and we know that $\gcd(x, y, z) = 1$. We also note that m and n cannot both be odd, for if they were, then x, y, and z would all be even, contradicting the condition $\gcd(x, y, z) = 1$. Because $\gcd(m, n) = 1$ and m and n cannot both be odd, we see that m and n cannot both be odd, or vice versa. This shows that every primitive Pythagorean triple has the appropriate form.

To complete the proof, we must show that every triple (x, y, z) with

$$x = r - s = m^2 - n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2,$$

where m and n are positive integers $m > n$, $\gcd(m, n) = 1$ and $m \not\equiv n \pmod 2$, is a primitive Pythagorean triple. First, note that $m^2 - n^2$, $2mn$, $m^2 + n^2$ forms a Pythagorean triple because

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2 \\ &= z^2. \end{aligned}$$

To see that this triple forms a primitive Pythagorean triple, we must show that these values of x, y, and z are mutually relatively prime. Assume for the sake of contradiction that $\gcd(x, y, z) = d > 1$. Then there exists a prime p such that $p \mid \gcd(x, y, z)$. We note that

$p \neq 2$, because x is odd (because $x = m^2 - n^2$, where m^2 and n^2 have opposite parity). Also, note that because $p \mid x$ and $p \mid z$, $p \mid (z + x) = 2m^2$ and $p \mid (z - x) = 2n^2$. Hence, $p \mid m$ and $p \mid n$, contradicting the fact that $\gcd(m, n) = 1$. Therefore, $\gcd(x, y, z) = 1$ and (x, y, z) is a primitive Pythagorean triple.

■

Example 1.3. Let $m = 5$ and $n = 2$, so that $\gcd(m, n) = \gcd(5, 2) = 1$, $m \not\equiv n \pmod 2$ and $m > n$. Hence, theorem 1.4 tells us that (x, y, z) with

$$x = m^2 - n^2 = 5^2 - 2^2 = 21,$$

$$y = 2mn = 2 \cdot 5 \cdot 2 = 20,$$

$$z = m^2 + n^2 = 5^2 + 2^2 = 29$$

is a primitive Pythagorean triple.

We will list the primitive Pythagorean triples generated using theorem 1.4 with $m \leq 6$ in the following table:

m	n	$x = m^2 - n^2$	$y = 2mn$	$z = m^2 + n^2$
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25
5	2	21	20	29
5	4	9	40	41
6	1	35	12	37
6	5	11	60	61

Section 2: Fermat's Last Theorem and an Interesting Conjecture

In this section we will discuss one of the biggest "celebrities" in the world of mathematics, which is *Fermat's Last Theorem*. The French lawyer and mathematician, Pierre de Fermat, had many contributions to number theory as well as other fields of mathematics, but this may be his most celebrated theorem. This is mostly because the quest for a proof had challenged mathematicians for more than 350 years. We have already shown, in the previous section, that the diophantine equation $x^n + y^n = z^n$ has infinitely many solutions in nonzero integers x, y, z when $n = 2$. But what about when $n > 2$? In Fermat's copy of the works of Diophantus, he commented in the margin next to a discussion of the above equation. Fermat wrote:

> However, it is impossible to write a cube as the sum of two cubes, a fourth power as the sum of two fourth powers and in general any power as the sums of two similar powers. For this I have discovered a truly wonderful proof, but the margin is too small to contain it.

Fermat did include a proof of the special case of $n = 4$ which we will discuss later in this section using his *method of infinite descent*. Although it is believed to be highly unlikely that Fermat actually had a proof for this result for all integers $n > 2$, we will never know for certain. We will now state the theorem.

Theorem 2.1. ***Fermat's Last Theorem.*** The Diophantine equation

$$x^n + y^n = z^n$$

has no solutions in nonzero integers x, y, and z when n is an integer with $n \geq 3$.

The Proof for $n = 4$

The proof we will give for the case when $n = 4$ uses the *method of infinite descent* devised by Fermat. This method is an offshoot of the well-ordering property, and shows that a Diophantine equation has no solutions by showing that for every solution there is a "smaller" solution, contradicting the well-ordering property.

Using the method of infinite descent, we will show that the diophantine equation $x^4 + y^4 = z^2$ has no solutions in nonzero integers x, y, and z. This is stronger than showing Fermat's last theorem is true for $n = 4$, because any $x^4 + y^4 = z^4 = (z^2)^2$ gives a solution of $x^4 + y^4 = z^2$.

Theorem 2.2. The diophantine equation

$$x^4 + y^4 = z^2$$

has no solutions in nonzero integers x, y, and z.

Proof. Assume that this equation has a solution in nonzero integers x, y, and z. Because we may replace any number of the variables with their negatives without changing the validity of the equation, we may assume that x, y, and z are positive integers.

We may also suppose that $\gcd(x, y) = 1$. To see this, let $\gcd(x, y) = d > 1$. Then $x = dx_1$ and $y = dy_1$, with $\gcd(x_1, y_1) = 1$, where x_1 and y_1 are positive integers. Because $x^4 + y^4 = z^2$, we have

$$(dx_1)^4 + (dy_1)^4 = z^2,$$

so that

$$d^4(x_1^4 + y_1^4) = z^2.$$

Hence, $d^4 \mid z^2$, which implies $d^2 \mid z$. Therefore, $z = d^2 z_1$, where z_1 is a positive integer. Thus,

$$d^4(x_1^4 + y_1^4) = (d^2 z_1)^2 = d^4 z_1^2,$$

so that

$$x_1^4 + y_1^4 = z_1^2.$$

This gives a solution of $x^4 + y^4 = z^2$ in positive integers $x = x_1$, $y = y_1$, and $z = z_1$ with $\gcd(x_1, y_1) = 1$.

So suppose that $x = x_0, y = y_0$, and $z = z_0$ is a solution of $x^4 + y^4 = z^2$, where x_0, y_0, and z_0 are positive integers with $\gcd(x_0, y_0) = 1$. We will show that there is another

solution in positive integers $x = x_1, y = y_1$, and $z = z_1$ with $\gcd(x_1, y_1) = 1$, such that $z_1 < z_0$. Because $x_0^4 + y_0^4 = z_0^2$, we have

$$(x_0^2)^2 + (y_0^2)^2 = z_0^2$$

so that (x_0^2, y_0^2, z_0) is a Pythagorean triple. Furthermore, we have $\gcd(x_0^2, y_0^2) = 1$, for if p is a prime such that $p \mid x_0^2$ and $p \mid y_0^2$, then $p \mid x_0$ and $p \mid y_0$, contradicting the fact that $\gcd(x_0, y_0) = 1$. Hence, (x_0^2, y_0^2, z_0^2) is a primitive Pythagorean triple, and by Theorem 1.4, we know that there exists positive integers m and n with $\gcd(m, n) = 1$, $m \not\equiv n \ (mod\ 2)$, and

$$x_0^2 = m^2 - n^2,$$

$$y_0^2 = 2mn,$$

$$z_0 = m^2 + n^2,$$

where we have interchanged x_0^2 and y_0^2, if necessary, to make y_0^2 the even integer of this part.

From the equation for x_0^2, we see that

$$x_0^2 + n^2 = m^2$$

Because $\gcd(m, n) = 1$, it follows that (x_0, n, m) is a Pythagorean triple, m is odd, and n is even. Again, using Theorem 1.4, we see that there exists positive integers r and s with $\gcd(r, s) = 1, r \not\equiv s \ (mod\ 2)$, and

$$x_0 = r^2 - s^2,$$

$$n = 2rs,$$

$$m = r^2 + s^2$$

Because m is odd and $\gcd(m, n) = 1$, we know that $\gcd(m, 2n) = 1$. We take note that because $y_0^2 = (2n)m$, Lemma 1.3 tells us that there are positive integers z_1 and w with $m = z_1^2$ and $2n = w^2$. Because w is even, $w = 2v$, where $v$is a positive integer, so that

$$v^2 = \frac{n}{2} = rs\,.$$

Because $\gcd(r, s) = 1$, Lemma 1.3 tells us that there are positive integers x_1 and y_1 such that $r = x_1^2$ and $s = y_1^2$. Note that because $\gcd(r, s) = 1$, it easily follows that $\gcd(x_1, y_1) = 1$. Hence,

$$x_1^4 + y_1^4 = r^2 + s^2 = m = z_1^2\,,$$

where x_1, y_1, z_1 are positive integers with $\gcd(x_1, y_1) = 1$. Moreover, we have $z_1 < z_0$, because

$$z_1 \leq z_1^4 = m^2 < m^2 + n^2 = z_0\,.$$

To complete the proof, assume that $x^4 + y^4 = z^2$ has at least one integral solution. By the well-ordering property, we know that among the solutions in positive integers there is a solution with the smallest value z_0 of the variable z. However, we have shown that from this solution we can find another solution with a smaller value of the variable z, leading us to a contradiction. This completes the proof by the method of infinite descent.

■

This process of infinite descent is a really useful tool to show an equation cannot have any positive integer solutions because at a certain point we will run out of positive integers but the process insists there must be a solution. That is what gives us our contradiction and our conclusion that in the case of $n = 4$, there are no positive inter solutions.

Mathematicians continued to work on extending the proof of Fermat's last theorem for a very long time and there were many advancements and general proofs under very specific conditions. However, in 1993, a professor at Princeton University named *Andrew Wiles*, shocked the mathematical world when he provided a complete proof of Fermat's last theorem during a series of lectures in Cambridge, England. Wiles spent seven years working in solitary to complete this proof. Shortly after his presentation a major error was discovered, but less than a year later Wiles revised his proof and was passed through careful review and was then accepted. Finally, after the 350 year long search, we now have a complete proof of Fermat's last theorem.

An Interesting Conjecture

This interesting conjecture was formulated in 1985 by Joseph Oesterle and David Masser. If their conjecture proves to be true, it could be used to resolve questions about many well-known diophantine equations. Before we state the conjecture, we need to introduce some notation.

Definition. If n is a positive integer, then $rad(n)$ is the product of distinct prime factors of n. Note that $rad(n)$ is also called the *squarefree* part of n because it can be obtained from eliminating all the factors that produce squares from the prime factorization of n.

Example 2.1. If $n = 2^5 \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 11^3$, then $rad(n) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$.

■

We can now state the conjecture.

The abc Conjecture For every real number $\epsilon > 0$ there exists a constant $K(\epsilon)$ such that if a, b, and c are integers such that $a + b = c$ and $\gcd(a, b) = 1$, then

$$\max(|a|, |b|, |c|) < K(\epsilon)\big(rad(abc)\big)^{1+\epsilon}.$$

There have been shown to be many consequences of this conjecture that have come from some of its deep results. We will not discuss the background or the motivations that led to this conjecture because it will take us to far from the scope of this project, but in the following example, we will show how the abc conjecture can be used to prove a result related to Fermat's last theorem.

Example 2.2. We can apply the abc conjecture to obtain a partial solution of Fermat's last theorem. Suppose that

$$x^n + y^n = z^n,$$

where x, y, and z are pairwise relatively prime integers. Let $a = x^n$, $b = y^n$, and $c = z^n$. We can estimate $rad(abc) = rad(x^n y^n z^n)$ by noting that

$$rad(x^n y^n z^n) = rad(xyz) \leq xyz < z^3.$$

The equality $rad(x^n y^n z^n) = rad(xyz)$ holds because the primes dividing $x^n y^n z^n$ are the same as the primes dividing xyz. The first inequality follows because $rad(m) \leq m$ for every positive integer m, and the last inequality holds because x and y are positive, so that $x < z$ and $y < z$.

Now applying the abc conjecture and noting that $\max(|a|, |b|, |c|) = z^n$, for every $\epsilon > 0$, there exists a constant $K(\epsilon) > 0$ such that

$$z^n \leq K(\epsilon)(z^3)^{1+\epsilon}.$$

If we take $\epsilon = \frac{1}{6}$ and $n \geq 4$, it is easy to see that $n - 3(1 + \epsilon) \geq \frac{n}{8}\epsilon$

$$z^n \leq K\left(\frac{1}{6}\right)^8,$$

where $K\left(\frac{1}{6}\right)$ is the value of the constant $K(\epsilon)$ for $\epsilon = \frac{1}{6}$. It follows that $z \leq K\left(\frac{1}{6}\right)^{\frac{8}{n}}$. Consequently, in a solution of $x^n + y^n = z^n$ with $n \geq 4$, the numbers x, y, and z are all less than a fixed bound, which implies that there are only finitely many solutions.

■

The interesting thing about the abc conjecture is that Fermat's last theorem is a direct consequence of it. This is because the abc conjecture implies there are only finitely many solutions to the equation $x^n + y^n = z^n$ where $\gcd(x, y, z) = 1$ and $n \geq 4$. So the only thing left to check is when $n = 3$ and a solution to this has been around for quite some time. Therefore, the abc conjecture is a very nice way to see how the statement of Fermat's last theorem really is true.

Section 3: Sums of Squares

Since we are discussing the investigation of solutions to nonlinear diophantine equations, we are only interested in solutions of integral type. In this section, we will discuss the representation of integers as sums of squares. We will consider two very important questions that mathematicians have been very interested in throughout history. The first question we will try to answer is: Which integers are the sum of two squares? Once we have found exactly what integers can be represented this way, we will then try to extend this question past the sum of just two squares and ask: What is the least integer n such that every positive integer is the sum of n squares?

This seems to be a very natural questions to ask. Since we are seeking integral solutions to our nonlinear diophantine equations, it would seem necessary to categorize the integers themselves.

Fact. n is not the sum of two squares if it is of the form $4k + 3$.

To see why this fact is true, we know that $a^2 \equiv 0$ or $1\ (mod\ 4)$ for every integer a, which means $x^2 + y^2 \equiv 0, 1,$ or $2\ (mod\ 4)$ for all integers x, and y. Therefore, for any $n = 4k + 3$, $n \equiv 3\ (mod\ 4)$ and cannot be written as a sum of two squares.

Example 3.1. Let's examine the first 20 positive integers

$1 = 0^2 + 1^2$	11 is not the sum of two squares.
$2 = 1^2 + 1^2$	12 is not the sum of two squares.
3 is not the sum of two squares.	$13 = 3^2 + 2^2$
$4 = 2^2 + 0^2$	14 is not the sum of two squares.
$5 = 1^2 + 2^2$	15 is not the sum of two squares.
6 is not the sum of two squares.	$16 = 4^2 + 0^2$
7 is not the sum of two squares.	$17 = 4^2 + 1^2$
$8 = 2^2 + 2^2$	$18 = 3^2 + 3^2$
$9 = 3^2 + 0^2$	19 is not the sum of two squares.
$10 = 3^2 + 1^2$	$20 = 4^2 + 2^2$

Just by looking at this table it is very hard to see any similarities between the integers that can or cannot be represented as a sum of two squares. So, developing a conjecture about when a positive integer can be represented as a sum of squares is in no way trivial.

The first observation we can examine to begin this discussion is whether or not an integer's prime factorization determines whether a particular integer is the sum of squares. This is a natural place to begin because we will see that a product of two integers that can be represented as a sum of two squares will again be a sum of two squares. Also, we will use the fact that a prime is representable as a sum of two squares if and only if it is not of

the form $4k + 3$. We will prove both these statements and then we will state and prove a theorem that will specify which integers are the sum of squares.

Theorem 3.1. If m and n are both sums of two squares, then mn is also the sum of two squares.

Proof. Let $m = a^2 + b^2$ and $n = c^2 + d^2$. Then

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

Since the set of integers is closed under addition, the sums $(ac + bd)$ and $\big(ad + (-bc)\big)$ are also integers. Therefore, if m and n are both sums of squares then so is mn.

■

Example 3.2. Because $5 = 2^2 + 1^2$, and $13 = 3^2 + 2^2$ it follows from Theorem 3.1 that

$$65 = 5 \cdot 13 = (2^2 + 1^2)(3^2 + 2^2)$$
$$= (2 \cdot 3 + 1 \cdot 2)^2 + (2 \cdot 2 - 1 \cdot 3)^2$$
$$= 8^2 + 1^2.$$

Our next essential result will be that every prime of the form $4k + 1$ is the sum of two squares. We will need the following definition and lemma to prove this result.

Definition. If m is a positive integer, we say that an integer a is a ***quadratic residue of m*** if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \ (mod\ m)$ has a solution.

Lemma 3.2. If p is a prime of the form $4m + 1$, where m is an integer, then there exists integers x and y such that $x^2 + y^2 = kp$ for some positive integer $k < p$.

Proof. Since p is an odd prime, we can see that -1 is a quadratic residue of p. Hence, there is an integer a, $a < p$, such that $a^2 \equiv -1 \ (mod\ p)$. It follows that $a^2 + 1 = kp$ for some positive integer k. Hence, $x^2 + y^2 = kp$, where $x = a$ and $y = 1$. Also, we can see that $k < p$ since $kp = x^2 + y^2 \leq (p - 1)^2 + 1 < p^2$.

■

We can now prove the statement from above that suggests all primes not of the form $4k + 3$ are the sum of two squares.

Theorem 3.3. If p is a prime not of the form $4k + 3$, then there are integers x and y such that $x^2 + y^2 = p$.

Proof. Note that 2 is the sum of squares, because $1^2 + 1^2 = 2$. Now, suppose that p is a prime of the form $4k + 1$. Let m be the smallest positive integer such that $x^2 + y^2 = mp$ has a solution in integers x and y. By Lemma 3.2 there is such an integer less that p; by the well-ordering property, a least such integer exists. We will show that $m = 1$.

Assume that $m > 1$. Let a and b be defined by

$$a \equiv x \ (mod\ m), \qquad b \equiv y \ (mod\ m)$$

and

$$-\frac{m}{2} < a \leq \frac{m}{2}, \qquad -\frac{m}{2} < b \leq \frac{m}{2}.$$

It follows that $a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \ (mod\ m)$. Hence, there is an integer k such that

$$a^2 + b^2 = km.$$

We have

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

By Theorem 3.1, we have

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2.$$

Furthermore, because $a \equiv x \ (mod\ m)$ and $b \equiv y \ (mod\ m)$, we have

$$ax + by \equiv x^2 + y^2 \equiv 0 \ (mod\ m)$$

$$ay - bx \equiv xy - yx \equiv 0 \ (mod\ m).$$

Hence, $\frac{ax+by}{m}$ and $\frac{ay-bx}{m}$ are integers, so that

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ay - bx}{m}\right)^2 = \frac{km^2p}{m^2} = kp$$

is the sum of two squares. If we show that $0 < k < m$, this will contradict the choice of m as the minimum positive integer such that $x^2 + y^2 = mp$ has a solution in integers. We know that $a^2 + b^2 = km, -\frac{m}{2} < a \leq \frac{m}{2}$, and $-\frac{m}{2} < b \leq \frac{m}{2}$. Hence, $a^2 \leq \frac{m^2}{4}$ and $b^2 \leq \frac{m^2}{4}$. We now have

$$0 \leq km = a^2 + b^2 \leq 2\left(\frac{m^2}{4}\right) = \frac{m^2}{2}.$$

Consequently, $0 \leq k \leq \frac{m}{2}$. It follows that $k < m$. All that remains is to show that $k \neq 0$. If $k = 0$, we have $a^2 + b^2 = 0$. This implies that $a = b = 0$, so that $x \equiv y \equiv 0 \ (mod\ m)$, which shows that $m \mid x$ and $m \mid y$. Because $x^2 + y^2 = mp$, this implies that $m^2 \mid mp$, which implies that $m \mid p$. Because $m < p$, this implies that $m = 1$, which is what we wanted to prove.

■

We can now put all the pieces together and prove the fundamental result that classifies the positive integers that are representable as the sum of two squares.

Theorem 3.4. The positive integer n is the sum of two squares if and only if each prime factor of n of the form $4k + 3$ occurs to an even power in the prime factorization.

Proof. Suppose that in the prime factorization of n there are no primes of the form $4k + 3$ that appear to an odd power. We write $n = t^2u$, where u is the product of primes. No primes of the form $4k + 3$ appear in u. By Theorem 3.3, each prime in u can be written as

the sum of two squares. Applying Theorem 3.2 one time fewer than the number of different primes in u shows that u is also the sum of two squares, say,

$$u = x^2 + y^2 .$$

It then follows that n is also the sum of two squares, namely,

$$n = (tx)^2 + (ty)^2 .$$

Now, suppose that there is a prime p, $p \equiv 3\ (mod\ 4)$, that occurs in the prime factorization of n to an odd power, say, the $(2j + 1)$th power. Furthermore, suppose that n is the sum of two squares, that is,

$$n = x^2 + y^2 .$$

Let $\gcd(x, y) = d$, $a = \frac{x}{d}$, $b = \frac{y}{d}$, and $m = \frac{n}{d^2}$. It follows that $\gcd(a, b) = 1$ and

$$a^2 + b^2 = m .$$

Suppose that p^k is the largest power of p that divides d. Then m is divisible by $p^{2j-2k+1}$, and $2j - 2k + 1$ is at least 1 because it is nonnegative; hence, $p \mid m$. We know that p does not divide a, for if $p \mid a$, then $p \mid b$ because $b^2 = m - a^2$, but $\gcd(a, b) = 1$.

Thus, there is an integer z such that $az \equiv b\ (mod\ p)$. It follows that

$$a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1 + z^2)\ (mod\ p).$$

Because $a^2 + b^2 = m$ and $p \mid m$, we see that

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

Because $\gcd(a, p) = 1$, it follows that $1 + z^2 \equiv 0 \ (mod\ p)$. This implies that $z^2 \equiv -1 \ (mod\ p)$, which is impossible because -1 is not a quadratic residue of p, because $p \equiv 3 \ (mod\ 4)$. This contradiction shows that n could not have been the sum of two squares.

■

So, that' it. We have done it. We now know that not every positive integer can be expressed as the sum of two squares but the ones that have a very specific type of prime factorization can. So, your next questions might be the following. What about integers being represented as the sum of three squares? Or four squares? Is there a certain number of squares that when added together can represent any integer you want? The answer is yes and the least integer to make this statement true is $n = 4$. Every integer can be represented as a sum of four squares! We will not prove this statement here but the proof is very similar to what we just did, where the same lemmas hold true in the $n = 4$ case. However, there are no more restrictions on the prime factorization and we are guaranteed to find integers that will work.

Section 4: Pell's Equation

The nonlinear diophantine equation we will examine in this section is of the form

$$x^2 - dy^2 = n\,.$$

where d and n are fixed integers. There are no solutions to this equation when $d < 0$ and $n < 0$. In the case where $d < 0$ and $n > 0$ there can be at most a finite number of solutions, because the equation $x^2 - dy^2 = n$ implies that $|x| \leq \sqrt{n}$ and $|y| \leq \sqrt{\frac{n}{|d|}}$. If d happens to be a square, say, $d = D^2$, then

$$x^2 - dy^2 = x^2 - D^2y^2 = (x + Dy)(x - Dy) = n\,.$$

Hence, any solution when d is a square, corresponds to a simultaneous solution of the equations

$$x + Dy = a\,,$$

$$x - Dy = b\,,$$

where a and b are integers such that $n = ab$. Since for each factorization of n there is at most one integer solution of these two equations, we can conclude that there are only a finite number of solutions.

For the rest of this section, we will be interested in the diophantine equation $x^2 - dy^2 = n$, where d and n are integers and d is a positive integer that is not a square.

Before we state the first theorem, we need some definitions that will be very helpful for the study of this equation.

Definition. A ***finite continued fraction*** is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

where $a_0, a_1, a_2, \ldots, a_n$ are real numbers with $a_0, a_1, a_2, \ldots, a_n$ positive. The real numbers $a_0, a_1, a_2, \ldots, a_n$ are called ***partial quotients*** of the continued fraction. The continued fraction is called ***simple*** if the real numbers $a_0, a_1, a_2, \ldots, a_n$ are all integers. We use the notation $[a_0; a_1, \ldots, a_n]$ to represent the continued fraction.

Example 4.1. The fraction $\frac{47}{17}$ can be written as a simple finite continued fraction. To see this, we observe that

$$\frac{47}{17} = 2 + \frac{13}{17} = 2 + \frac{1}{\frac{17}{13}} = 2 + \frac{1}{1 + \frac{4}{13}} = 2 + \frac{1}{1 + \frac{1}{\frac{13}{4}}} = 2 + \frac{1}{1 + \frac{1}{3 + \frac{1}{4}}}$$

and in short form, $\frac{47}{17} = [2; 1, 3, 4]$. It should take little convincing that any rational number can be written as a finite continued fraction. This particular fraction corresponds to steps in the Euclidean algorithm. First,

$$47 = 2 \cdot 17 + 13$$

$$17 = 1 \cdot 13 + 4$$

$$13 = 3 \cdot 4 + 1$$

$$4 = 4 \cdot 1 + 0$$

Rewriting, we see that,

$$\frac{47}{17} = 2 + \frac{13}{17}$$

$$\frac{17}{13} = 1 + \frac{4}{13}$$

$$\frac{13}{4} = 3 + \frac{1}{4}$$

Now we can get the continued fraction above by simply substituting.

Example 4.2. The simple continued fraction for π is given by

$[3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 14, 2, 1, 1, 2, 2, 2, 2, \dots]$.

Definition. The continued fraction $[a_0; a_1, \dots, a_n]$, where k is a nonnegative integer less than or equal to n, is called the ***kth convergent*** of the continued fraction $[a_0; a_1, \dots, a_n]$. The kth convergent is denoted by C_k.

Fact. If α is an irrational number and if $\frac{r}{s}$ is a rational number in lowest terms, where r and s are integers with $s > 0$ such that

$$\left|\alpha - \frac{r}{s}\right| < \frac{1}{2s^2},$$

then $\frac{r}{s}$ is a convergent of the simple continued fraction expansion of α.

Theorem 4.1. Let d and n be integers such that $d > 0$, d is not a square, and $|n| < \sqrt{d}$. If $x^2 - dy^2 = n$, then $\frac{x}{y}$ is a convergent of the simple fraction of $\sqrt{d}$.

Proof. First consider the case when $n > 0$. Because $x^2 - dy^2 = n$, we see that

$$(x + y\sqrt{d})(x - y\sqrt{d}) = n.$$

From this, we see that $x - y\sqrt{d} > 0$, so that $x > y\sqrt{d}$. Consequently,

$$\frac{x}{y} - \sqrt{d} > 0,$$

and, because $0 < n < \sqrt{d}$, we see that

$$\begin{aligned} \frac{x}{y} - \sqrt{d} &= \frac{x - \sqrt{d}y}{y} \\ &= \frac{x^2 - dy^2}{y(x + y\sqrt{d})} \\ &< \frac{|n|}{y(2y\sqrt{d})} \end{aligned}$$

$$< \frac{\sqrt{d}}{2y^2\sqrt{d}}$$

$$= \frac{1}{2y^2}.$$

Because $0 < \frac{x}{y} - \sqrt{d} < \frac{1}{2y^2}$, the above fact tells us that $\frac{x}{y}$ must be a convergent of the simple continued fraction of $\sqrt{d}$.

When $n < 0$, we divide both sides of $x^2 - dy^2 = n$ by $-d$, we obtain

$$y^2 - \left(\frac{1}{d}\right)x^2 = -\frac{n}{d}.$$

By a similar argument to that given when $n > 0$, we see that $\frac{y}{x}$ is a convergent of the simple continued fraction expansion of $\frac{1}{\sqrt{d}}$. Therefore, we know that $\frac{x}{y} = \frac{1}{\frac{y}{x}}$ must be a convergent of the simple continued fraction of $\sqrt{d} = \frac{1}{\frac{1}{\sqrt{d}}}$.

■

What we have just shown is that the solutions of the diophantine equation $x^2 - dy^2 = n$, where $|n| < \sqrt{d}$, are given by the convergents of the simple continued fraction expansion of $\sqrt{d}$. Our next theorem will help us use these convergents to find solutions of this diophantine equation.

Fact. Let d be a positive integer that is not a square. Define $\alpha_k = \frac{P_k+\sqrt{d}}{Q_k}$,

$a_k = [\alpha_k]$, $P_{k+1} = a_k Q_k - P_k$, and $Q_{k+1} = \frac{d-P_{k+1}^2}{Q_k}$, for $k = 0, 1, 2, \ldots$, where $a_0 = \sqrt{d}$.

Furthermore, let $\frac{p_k}{q_k}$ denote the kth convergent of the simple continued fraction expansion of $\sqrt{d}$. Then

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1}.$$

The special case of the diophantine equation $x^2 - dy^2 = n$ with $n = 1$ is called ***Pell's equation***, named after the mathematician *John Pell*. The problem of finding the integral solutions to this equation has a very long and rich history. Many famous mathematicians like Euler, Lagrange, and even Fermat have all contributed to the methods of finding solutions to this equation and all of their methods are related to the use of the continued fraction of $\sqrt{d}$. We will show how the use of this continued fraction is used to find the solutions of Pell's equation. We will do this with the use of previous theorems and even look at the solutions of the related equation $x^2 - dy^2 = -1$.

Theorem 4.2. Let d be a positive integer that is not a square. Let $\frac{p_k}{q_k}$ denote the kth convergent of the simple continued fraction of $\sqrt{d}$, $k = 1, 2, 3, \ldots$, and let n be the period length of this continued fraction. Then, when n is even, the positive solutions of the diophantine equation $x^2 - dy^2 = 1$ are $x = p_{jn-1}, y = q_{jn-1}, j = 1, 2, 3, \ldots$, and the

diophantine equation $x^2 - dy^2 = -1$ has no solutions. When n is odd, the positive solutions of $x^2 - dy^2 = 1$ are $= p_{2jn-1}, y = q_{2jn-1}, j = 1, 2, 3, \dots$, and the solutions of $x^2 - dy^2 = -1$ are $x = p_{(2j-1)n-1}, y = q_{(2j-1)n-1}, j = 1, 2, 3, \dots$.

Proof. We already know that if x_0, y_0 is a positive solution of $x^2 - dy^2 = \pm 1$, then $x_0 = p_k, y_0 = q_k$, where $\frac{p_k}{q_k}$ is a convergent of the simple continued fraction of $\sqrt{d}$. On the other hand, from the fact above, we know that

$$p_k^2 - dq_k^2 = (-1)^{k-1} Q_{k+1},$$

where Q_{k+1} is as defined above.

Because the period of the continued expansion of $\sqrt{d}$ is n, we know that $Q_{jn} = Q_0 = 1$ for $j = 1, 2, 3, \dots$, because $\sqrt{d} = \frac{P_0 + \sqrt{d}}{Q_0}$. Hence,

$$p_{jn-1}^2 - dq_{jn-1}^2 = (-1)^{jn} Q_{nj} = (-1)^{jn}.$$

This equation shows us that when n is even, p_{jn-1}, q_{jn-1} is a solution of $x^2 - dy^2 = 1$ for $= 1, 2, 3, \dots$, and when n is odd, p_{2jn-1}, q_{2jn-1} is a solution $x^2 - dy^2 = 1$ and $p_{2(j-1)n-1}, q_{2(j-1)n-1}$ is a solution of $x^2 - dy^2 = -1$ for $j = 1, 2, 3, \dots$.

To show that the diophantine equations $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$ have no solutions other than those already found, we will show that $Q_{k+1} = 1$ implies that $n \mid k$ and that $Q_j \neq -1$ for $= 1, 2, 3, \dots$.

We first note that if $Q_{k+1} = 1$ then

$$\alpha_{k+1} = P_{k+1} + \sqrt{d}.$$

Because $\alpha_{k+1} = [a_{k+1}; a_{k+2}, \dots]$, the continued fraction expansion of α_{k+1} is purely periodic. Hence, $-1 < \alpha_{k+1} = P_{k+1} - \sqrt{d} < 0$. This implies that $P_{k+1} = \lfloor \sqrt{d} \rfloor$, so that $\alpha_k - \alpha_0$, and $n \mid k$.

To see that $Q_j \neq -1$ for $= 1, 2, 3, \dots$, note that $Q_j = -1$ implies that $\alpha_j = -P_{k+1} - \sqrt{d}$. Because α_j has a purely periodic simple continued fraction expansion, we know that

$$-1 < \alpha_j' = -P_j + \sqrt{d} < 0$$

and

$$\alpha_j = -P_j - \sqrt{d} > 1.$$

From the first of these inequalities, we see that $P_j > -\sqrt{d}$, and from the second, we see that $P_j < -1 - \sqrt{d}$. Because these two inequalities for p_j are contradictory, we see that $Q_j \neq -1$.

Because we have found all solutions of $x^2 - dy^2 = 1$ and $x^2 - dy^2 = -1$, where x and y are positive integers, we have completed the proof.

■

We will illustrate the use of Theorem 4.2 with the following example.

Example 4.3. Because the continued fraction of $\sqrt{14}$ is $[3; \overline{1,\ 2,\ 1, 6}]$, the positive solutions of $x^2 - 14y^2 = 1$ are $p_{4j-1}, q_{4j-1}, j = 1, 2, 3, \dots$, where $\frac{p_{4j-1}}{q_{4j-1}}$ is the jth convergent of the simple continued fraction expansion of $\sqrt{14}$. The least positive solution is $p_3 = 15, q_3 = 4$.

The diophantine equation $x^2 - 14y^2 = -1$ has no solutions, because the period length of the simple continued fraction expansion of $\sqrt{14}$ is even.

We will conclude this section with a theorem that will show us how to find all the positive solutions of Pell's equation using the least positive solution. We will take this theorem as a fact. The proof is left for the reader but the result directly follows from everything we have taken time to prove in this section. We now have all the solutions of Pell's equation and they are exactly as follows:

Theorem 4.3. Let x_1, y_1 be the least positive solution of the diophantine equation $x^2 - dy^2 = 1$, where d is a positive integer that is not a square. Then all positive solutions x_k, y_k are given by

$$x_k + y_k\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^k$$

for $= 1, 2, 3, \ldots$

This concludes our investigation of nonlinear diophantine equations and their integral solutions. Historically, these seem to have been some of the most intriguing and frustrating types of problems for most mathematicians. However, the quest for an understanding and classification of these not-so-trivial solutions has led to some incredible breakthroughs and advancements in the mathematical world. It's no wonder why some of

the greatest minds in human history have spent as much time and energy on these equations as they had. I hope you have enjoyed reading this paper as much as I did writing it.

■

Section 5: Bibliography

[1] Rosen, Kenneth H.. ***Elementary Number Theory & its Applications.*** Addison-Wesley, New York 2011.