An Introductory Exploration of Diophantine Equations

Clyde Kertzer

May 2021

Contents

1 Introduction

A pivotal branch of number theory, Diophantine equations, deals with equations that only allow for integer solutions. These were first studied by Diophantus of Alexandria in the third century AD. The most prominent types of these equations were quadratic. Diophantus studied the following three quadratic equations:

$$ax^2 + bx = c \qquad ax^2 = bx + c \qquad ax^2 + c = bx$$

These three equations are in fact equivalent, but Diophantus had no concept of zero and thus avoided negative coefficients by only looking at positive solutions.[1] This goes to show that even with some of the most rudimentary mathematical techniques, Diophantus left his mark on the world of number theory. In this paper, I will discuss Euclid's formula and extensions, linear Diophantine equations, systems of linear Diophantine equations, Diophantine equations of degree two or more, the Jacobi-Madden equation, and some applications these equations carry.

Lemma 1 (Euclid's Lemma)**.** Let p be a prime. If $p \mid ab$, $a, b \in \mathbb{Z}$, then p must divide either a or b.[2]

Lemma 2 (Euclid's Formula)**.** The combination of every $m, n \in \mathbb{N}$ generates a set of Pythagorean triples[3] through

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

where

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

2 Linear Diophantine Equations

Linear Diophantine equations are the most simple variant of Diophantine Equations and have the form

$$ax + by = c$$

where a, b and c are given integers. This equation will have a solution if and only if c is a multiple of $gcd(a, b)$. If (x, y) is a solution, then other solutions must be of the form $(x + kv, y - ku)$, $k \in \mathbb{Z}$, where u and v are the quotients of a and b (respectively), $\gcd(a, b)$.

1. L. J. Mordell, "Pure and Applied Mathematics," in Diophantine Equations (London, England: Academic Press, 1969), 30:345.

2. Euclid, "Proposition 30," in Book VII (Alexandria: Euclid, 300 BC), 30, accessed November 4, 2020. https://mathcs.clarku.edu/djoyce/java/elements/bookVII/bookVII.html#:text=Proposition%2030,one%20of%20the%20original%20numbers.

3. Kenneth E. Caviness and R. Lewis Caviness, "Euclid's Formula and Properties of Pythagorean Triples," Wolfram Demonstrations Project, last modified March 8, 2017, accessed February 12, 2021, https://demonstrations.wolfram.com/EuclidsFormulaAndPropertiesOfPythagoreanTriples/.

Let's prove this result. To simplify this process, we will first prove a similar case called Bézout's Identity.[4]

Theorem 1 (Bézout's Identity)**.** Let a and b be integers with greatest common divisor d. Then $\exists$ integers x and y such that $ax + by = c$. More generally, the integers of the form $ax + by$ are exactly the multiples of d.

Proof. Given any nonzero integers a and b, let the set $S = \{ax + by \mid x, y \in \mathbb{Z}\}$. Because S is nonempty, it has a minimum element of $d = as + bt$ by the well-ordering principle. To prove that $d = \gcd(a, b)$, we must first show that d is a common divisor of a and b and that for any other common divisor c, $c \leqslant d$. Write $a \mid d$

$$a = dq + r$$

where r is the remainder and $q \in \mathbb{N}$. We know that $S \cup \{0\}$ contains r because

$$\begin{aligned} r &= a - dq \\ r &= a - q(as + bt) \\ r &= a(1 - qs) - bqt \\ r &= a(1 - qs) + b(-qt). \end{aligned}$$

Thus, r is of the form $ax + by$ and therefore $r \in S \cup \{0\}$. However, $0 \leq r < d$ and d is the smallest integer contained by S, therefore r cannot be in S. This means that r must be 0, proving that d is a divisor of a. Thus, d is a divisor of b and is therefore a common divisor of a and b. We must now show that $c \leq d$. Because c is also a common divisor of a and b, $\exists$ u and v s.t. $a = cu$, $b = cv$. Then

$$\begin{aligned} d &= as + bt \\ d &= cus + dvt \\ d &= c(us + vt). \end{aligned}$$

Therefore, c is a divisor of d and $c \leq d$. □

Now to begin the original proof. Once again our intention is to show that the equation $ax + by = c$ will have a solution if and only if c is a multiple of $\gcd(a, b)$.

Proof. If (x, y) is a solution, then other solutions must be of the form $(x+kv, y-ku)$, $k \in \mathbb{Z}$, where u and v are the quotients of a and b (respectively). If $d = \gcd(a, b)$, Bézout's Identity proves that there exists e and f such that $ae + bf = d$. If c is a multiple of d, then $c = dh$, $h \in \mathbb{Z}$ and (eh, fh) must be a solution. Then for all (x, y), d divides $ax + by$. Thus, if $ax + by = c$ has a solution, c must be a multiple of d. If $a = ud$ and $b = vd$, so for all (x, y)

$$\begin{aligned} a(x + kv) + b(y - ku) &= ax + by + k(av - bu) \\ &= ax + by + k(udv - vdu) \\ &= ax + by. \end{aligned}$$

4. Arvin Deravy, "Bezout's Identity (Bezout's Lemma)," GeeksforGeeks, last modified May 20, 2020, accessed February 13, 2021, https://www.geeksforgeeks.org/bezouts-identity-bezouts-lemma/.

Thus $(x+kv, y-ku)$ is another solution. Given the two solutions: $ax_1+by_1 = ax_2+by_2 = c$, we know that $u(x_2 - x_1) + v(y_2 - y_1) = 0$. As u and v are coprime, Euclid's Lemma shows that v divides $x_2 - x_1$ and therefore $\exists\ k \in \mathbb{Z}$, s.t.

$$x_2 - x_1 = kv \qquad y_2 - y_1 = -ku$$
$$x_2 = x_1 + kv \qquad y_2 = y_1 - ku.$$

Therefore $ax + by = c$ will have a solution if and only if c is a multiple of $gcd(a, b)$. If (x, y) is a solution, then other solutions must be of the form $(x + kv, y - ku)$, $k \in \mathbb{Z}$, where u and v are the quotients of a and b (respectively) of $gcd(a, b)$. □

3 Systems of Linear Diophantine Equations

The equation $AX = B$ expresses the general form of a system of linear Diophantine equations. We can prove whether or not this system has solutions, and if it does, we can find all its solutions. We first define what it means for a matrix to be in row-echelon form:

1. The bottom row of the matrix contains all the zeros.
2. The first value in each nonzero row is to the right of all the leading values in the row(s) above it.

The method we wish to detail is: To solve the system of linear Diophantine equations $AX = B$, unimodular (the matrix's determinant is equal to zero) row reduce $[A^t \mid I]$ to $[R|T]$ where R is in row-echelon form. Then the system $AX = B$ has solutions if and only if the system $R^tK = B$ has solutions for K and all the solutions of $AX = B$ are of the form $X = T^tK$.[5] Use substitution for K to solve $R^tK = B$. The general form [6] looks like

$$\begin{bmatrix} d_1 & & & \\ * & d_2 & & \\ * & * & d_3 & \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \\ \vdots \end{bmatrix} = \begin{bmatrix} b_1 \\ b_2 \\ b_3 \\ \vdots \end{bmatrix}$$

First, row reduce A^t s.t. the first column begins with the gcd and all zeros below. Then do the same with the other columns as shown above. The equation $E[A^t \mid I] = [R|T]$ represents the row reduction of $[A^t \mid I]$ to $[R|T]$, where E is an invertible matrix. Thus, $T = E$ and $TA^t = R$. Therefore, $AT^t = R^t$ and $A = R^t(T^t)^{-1}$. The matrix T is a product of matrices that correspond to the performed unimodular row operations. Thus, each of these matrices has a determinant of $\pm$ 1, $\det(T) = \pm 1$. $AX = B$ is equivalent to $R^t(T^t)^{-1}X = B$ and $K = (T^t)^{-1}X$. Thus $X = T^tK$ and X will have integer solutions if and only if K does. Hence, $AX = B$ has integers solutions for X if and only if $R^tK = B$ has integer solutions for K.

5. William J. Gilbert, "Linear Diophantine Equations," University Waterloo California Mathematics, accessed November 5, 2020, https://www.math.uwaterloo.ca/ wgilbert/Research/GilbertPathria.pdf.

6. Gilbert, "Linear Diophantine," University Waterloo California Mathematics.

Example 1. Let's run through an example of a system of linear Diophantine equations.

$$\begin{aligned} 5a + 6b + 8c &= 1 \\ 6a - 11b + 7c &= 9 \end{aligned}$$

Use unimodular row-reduction[7]

$$\left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 6 & -11 & 0 & 1 & 0 \\ 8 & 7 & 0 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cc|ccc} 5 & 6 & 1 & 0 & 0 \\ 1 & -17 & -1 & 1 & 0 \\ 3 & 1 & -1 & 0 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 91 & 6 & -5 & 0 \\ 0 & 5 & 2 & -3 & 1 \end{array}\right]$$

$$\longrightarrow \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & -13 & 2 & 1 & -2 \\ 0 & 52 & 2 & -3 & 1 \end{array}\right] \longrightarrow \left[\begin{array}{cc|ccc} 1 & -17 & -1 & 1 & 0 \\ 0 & 13 & -2 & -1 & 2 \\ 0 & 0 & 10 & 1 & -7 \end{array}\right].$$

Thus, we find $R^tK = b$

$$\begin{bmatrix} 1 & 0 & 0 \\ -17 & 13 & 0 \end{bmatrix} \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} = \begin{bmatrix} 1 \\ 9 \end{bmatrix}.$$

Solve the system to find

$$\begin{aligned} k_1 &= 1 \\ -17k_1 + 13k_2 &= 9. \end{aligned}$$

By substituting k_1 we find that $k_2 = 2$ and $k_3 \in \mathbb{Z}$. Now we substitute back in to find

$$K = \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} \text{ and } \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = T^tK \begin{bmatrix} -1 & -2 & 10 \\ 1 & -1 & 1 \\ 0 & 2 & -7 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \\ k \end{bmatrix} = \begin{bmatrix} 10k - 5 \\ k - 1 \\ -7k + 4 \end{bmatrix}.$$

The integer solutions in general form where $k \in \mathbb{Z}$ are

$$\begin{aligned} a &= 10k - 5 \\ b &= k - 1 \\ c &= -7k + 4. \end{aligned}$$

4 Applications of Linear Diophantine Equations

Many real-world problems require Diophantine Equations in order to solve for whole number solutions. Problems involving the number of people, houses, etc., where fractional units do not apply (e.g. you cannot have $\frac{1}{2}$ of a person). Consider the following example: James invested a part of his investment in 10% bond A and a part in 20% bond B. His interest income during the first year is \$4,000. If he invests 60% more in 10% bond A and 10%

7. Ibid.

more in 20% bond B, his income during the second year increases by \$2,000. Find his initial investments. We represent his investments into bond A (x) and bond B (y) with[8]

$$10x + .20y = 4000.$$

The income in his second year yields the equation

$$\begin{aligned} .10(1.60x) + .20(1.10y) &= 6000 \\ .16x + .22y &= 6000. \end{aligned}$$

The two equations give the following matrix

$$\underset{A}{\begin{bmatrix} 0.10 & 0.20 \\ 0.16 & 0.22 \end{bmatrix}} \underset{X}{\begin{bmatrix} x \\ y \end{bmatrix}} = \underset{B}{\begin{bmatrix} 4000 \\ 6000 \end{bmatrix}}.$$

We can solve this using the technique proved in the previous section. First, we ensure that A is invertible by taking its determinant

$$\det(A) = (.10 * .22) - (.20 * .16) = .022 - .032 = -.01 \neq 0.$$

Because A is invertible, the technique will work. Begin by setting X equal to $A^{-1}B$ and solvning

$$\begin{aligned} X &= A^{-1}B \\ &= \frac{1}{-0.01} \begin{bmatrix} 0.22 & -0.20 \\ -0.16 & 0.10 \end{bmatrix} \begin{bmatrix} 4000 \\ 6000 \end{bmatrix} \\ &= \frac{1}{-0.01} \begin{bmatrix} -320 \\ 40 \end{bmatrix} \\ &= \begin{bmatrix} 32000 \\ 4000 \end{bmatrix}. \end{aligned}$$

This yields the final solutions of $x = 32000$ and $y = 4000$, meaning his final investments were \$32,000 into bond A and \$4,000 into bond B.

5 Diophantine Equations of Degree Two

Diophantine equations of degree two are Diophantine equations in which all variables are raised to the 2nd power, such as $a^2 + b^2 = 3c^2$. Solving these equations involves three potential outcomes.

1. The equation has no solutions
2. The equation has a finite number of solutions
3. The equation has an infinite number of solutions.

8. Deepinder Kaur and Meenal Sambhor, "Diophantine Equations and Their Applications," International Journal of Mathematics and Its Applications 9, no. 1 (2021): 3, http://ijmaa.in/v5n2-b/217-222.pdf.

5.1 Modular

We can use modular arithmetic to prove that an equation has no solutions. Let's take the previous example, $a^2+b^2 = 3c^2$, and prove that it has no solution, besides the trivial solution $(0, 0, 0)$. Suppose we divide a, b, and c by $gcd(a, b, c)$, s.t. they are now coprime. Let us now deviate to show a separate proof that $x^2 \equiv 0, 1(\text{mod}4)$.

Proof. The first case, when x is even, $k \in \mathbb{Z}$

$$\begin{aligned} x &= 2k \\ x^2 &= (2k)^2 \\ x^2 &= 4k^2 \equiv 0(\text{mod}4). \end{aligned}$$

The second case, where x is odd, $k \in \mathbb{Z}$

$$\begin{aligned} x &= 2k+1 \\ x^2 &= (2k+1)^2 \\ x^2 &= 4k^2+4k+1 \\ x^2 &= 4(k^2+k)+1 \equiv 1(\text{mod}4). \end{aligned}$$

Because the LHS of the equation $a^2 + b^2$, is the sum of two squares, it will either be equal to $0(\text{mod}4)$ $(even + even)$, $1(\text{mod}4)$ $(even + odd)$, or $2(\text{mod}4)$ $(odd + odd)$. The RHS of the equation $3c^2$, will always have a modulus of $0(\text{mod}4)$ or $3(\text{mod}4)$. Both sides being equivalent to $0(\text{mod}4)$ satisfy the equation, which means that a and b must be even, implying that they share the factor of 2 and are thus not coprime. This is a direct contradiction to what we stated beforehand when we divided a, b, and c by $gcd(a, b, c)$. Thus $a^2 + b^2 = 3c^2$ has no integer solutions. □

5.2 Infinite Descent

Another technique used to prove that an equation has no solutions is *infinite descent*, also known as Fermat's method of descent. This technique is essentially a proof by contradiction in which showing that a statement holds for some number and therefore smaller numbers, leading to an "infinite descent" and finally a contradiction. Put differently, an infinite sequence of decreasing natural numbers cannot exist.[9]

Example 2. Let us utilize this method for the example $x^4 + y^4 = z^2$. Begin by assuming that there are solutions besides the trivial solution $(0, 0, 0)$. Additionally, we assume that x^2, y^2, and z are coprime as we can cancel the common factors if they are not. Then $\exists$ coprime p, $q \in \mathbb{N}$ s.t.

$$\begin{aligned} x^2 &= 2pq \\ y^2 &= p^2 - q^2 \\ z^2 &= p^2 + q^2. \end{aligned}$$

9. Andrew Ellinor, "Fermat's Method of Infinite Descent," Brilliant.org, accessed February 11, 2021, https://brilliant.org/wiki/general-diophantine-equations-fermats-method-of/.

We write $x^4 + y^4 = z^2$ as $(x^2)^2 + (y^2)^2 = z^2$, to see that (x^2, y^2, z) is a Pythagorean triplet. Note that $y^2 = p^2 - q^2$ yields another Pythagorean triplet with coprime a, $b \in \mathbb{N}$ s.t.

$$\begin{aligned} q &= 2ab \\ y^2 &= a^2 - b^2 \\ p &= p^2 + b^2. \end{aligned}$$

We then substitute to get

$$x^2 = 2pq = 4ab(a^2 + b^2).$$

If (a or b) $\mid p$ then it cannot divide $a^2 + b^2$ because a and b are coprime. Thus ab and $a^2 + b^2$ are perfect squares. Because ab is a perfect square, and a, b are coprime, a and b must also be perfect squares. We notate this by letting $a = d^2$, $b = e^2$, and $p = P^2$. Because $a^2 + b^2$ is a perfect square

$$P^2 = a^2 + b^2 = d^4 + e^4$$

and

$$p < p^2 + q^2 = z.$$

Thus we have reached an infinite descent (contradiction) and we have shown that the equation has no solutions.

5.3 Parameterization

In cases where there is at least one solution, one solution can be found, and then other solutions can be derived from the first solution. Parameterization is a common technique used to do this.[10] Start by geometrically interpreting the Diophantine equation. Take $Q = (x_1, \ldots, x_n) = 0$ to be a homogeneous Diophantine equation of degree two. The nontrivial solutions are $(a_1, \ldots, a_n)$, the coordinates of a point on the surface defined by Q. This set can be written as $(\frac{p_1}{q}, \ldots, \frac{p_n}{q})$ where q, $p_1, \ldots, p_n \in \mathbb{Z}$. Thus the integer solutions are $(k\frac{p_1}{d}, \ldots, k\frac{p_n}{d})$, where $k \in \mathbb{Z}$ and $d = gcd(p_1)$. Let us define $A = (a_1, \ldots, a_n)$ to be an integer solution to $Q(x_1, \ldots, x_n) = 0$. We will parameterize the surface by the lines that pass through A. Taking $a_n \neq 0$, the general case is $q(x_1, \ldots, x_{n-1}) = Q(x_1, \ldots, x_n, 1) = 0$ which has the rational point R where

$$R = (r_1, \ldots, r_{n-1}) = (\frac{a_1}{a_n}, \ldots, \frac{a_{n-1}}{a_n}).$$

If this point is singular, all lines that pass through R are contained within the surface and a cone is formed. The general case is a line defined parametrically that passes through R

$$\begin{aligned} x_2 &= r_2 + t_2(x_1 - r_1) \\ \vdots &= \vdots \\ x_{n-1} &= r_{n-1} + t_{n-1}(x_1 - r_1). \end{aligned}$$

10. L. J. Lander, "Geometric Aspects of Diophantine Equations Involving Equal Sums of Like Powers," The American Mathematical Monthly 75, no. 10 (December 1968): 1061-1062, https://doi.org/10.2307/2315731.

When substituted into q, we get a second-degree polynomial with a zero at$(x_1 - r_1)$. In x_1 the quotient will be linear and equal to the division of two polynomials with integer coefficients

$$x_1 = \frac{f_1(t_2, \ldots, t_{n-1})}{f_n(t_2, \ldots, t_{n-1})}.$$

To find any x_i where $i = 1, \ldots, n-1$

$$x_i = \frac{f_i(t_2, \ldots, t_{n-1})}{f_n(t_2, \ldots, t_{n-1})}.$$

Thus the homogeneous case is

$$F_i(t_i, \ldots, t_{n-1}) = t_1^2 f_i\left(\frac{t_2}{t_1}, \ldots, \frac{t_{n-1}}{t_1}\right).$$

The polynomials parameterize the surface defined by Q is

$$\begin{aligned} x_1 &= F_1(t_1, \ldots, t_{n-1}) \\ \vdots &= \vdots \\ x_n &= F_n(t_1, \ldots, t_{n-1}). \end{aligned}$$

Because $F_1, \ldots, F_n$ are homogeneous polynomials, the solution point remains unchanged if all t_i are products of the same rational number. Thus $t_n, \ldots, t_{n-1}$ are coprime integers and we let $d = gcd(t_n, \ldots, t_{n-1})$. The solutions are then of the form

$$x_i = k\frac{F_i(t_1, \ldots, t_{n-1})}{d}.$$

Take the example of Pythagorean triples $x^2 + y^2 = z^2$, or $x^2 + y^2 - z^2 = 0$, where $(0, 0, 0)$ is trivial. Note that this is also the homogeneous equation of the unit circle. It is easy to see the nontrivial solution $(-1, 0, 1)$. This solution corresponds to the solution point $(-1, 0)$ on the unit circle. To find the parameterization of this solution, use the slope of the line that passes through this point

$$y = t(x + 1).$$

Plugging this into the circle equation with a radius of 1 we have

$$\begin{aligned} x^2 + y^2 - 1 &= 0 \\ x^2 - 1 + t^2(x + 1)^2 &= 0. \end{aligned}$$

Factoring we have

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

and dividing by $x + 1$ yields

$$x - 1 + t^2(x + 1) = 0.$$

Solve for x in terms of t gives us

$$\begin{aligned} x - 1 + t^2(x+1) &= 0 \\ x - 1 + t^2x + t^2 &= 0 \\ x + t^2x &= 1 - t^2 \\ x(1+t^2) &= 1 - t^2 \\ x &= \frac{1-t^2}{1+t^2}. \end{aligned}$$

Solve for y from $y = t(x+1)$ plugging in the previous equation

$$\begin{aligned} y &= t\left(\frac{1-t^2}{1+t^2} + 1\right) \\ &= t\left(\frac{1-t^2}{1+t^2} + \frac{1+t^2}{1+t^2}\right) \\ &= t\left(\frac{1-t^2+1+t^2}{1+t^2}\right) \\ &= t\left(\frac{2}{1+t^2}\right) \\ &= \frac{2t}{1+t^2}. \end{aligned}$$

Homogenizing as shown before where $k \in \mathbb{Z}$ we have the three solutions

$$x = k\left(\frac{s^2-t^2}{d}\right) \qquad x = k\left(\frac{2st}{d}\right) \qquad x = k\left(\frac{s^2+t^2}{d}\right)$$

where s, $t \in \mathbb{Z}$ and are coprime and $d = gcd(s^2 - t^2, 2st, s^2 + t^2)$. Note that $d = 2$ if s and t are both odd and $d = 1$ if one is even and the other is odd.

6 Euclid's Formula and Extensions

6.1 Euclid's Formula

As stated at the beginning of this paper and used throughout, Euclid's formula can be used to generate an infinite number of Pythagorean triples. Let's prove Euclid's Formula.[11]

Proof. We will ensure that all solutions are primitive by defining a, b, and c to be coprime. Note that as a, b, and c are coprime at least a or b is odd, so let us take a to be odd. It follows that b is even and c is odd. Starting with

$$\begin{aligned} a^2 + b^2 &= c^2 \\ b^2 &= c^2 - a^2 \end{aligned}$$

11. Waclaw Sierpinski, "Obtaining Primitive Pythagorean Triangles," in Pythagorean Triangles, dover ed. (Mineola, N.Y.: Dover Publications, 2003), vi.

factoring yields

$$(c+a)(c-a) = b^2.$$

Divide both sides by $c-a$

$$(c+a) = \frac{b^2}{c-a}$$

divide both sides by b

$$\frac{c+a}{b} = \frac{b}{c-a}.$$

Because $\frac{c+a}{b}$ is rational, we can set

$$\frac{c+a}{b} = \frac{m}{n} \; m, n \in \mathbb{N}.$$

It then follows that

$$\frac{c-a}{b} = \frac{n}{m}.$$

This yields the system of equations

$$\begin{aligned} \frac{c}{b} + \frac{a}{b} &= \frac{m}{n} \\ \frac{c}{b} - \frac{a}{b} &= \frac{n}{m}. \end{aligned}$$

Rearrange to solve for $\frac{c}{b}$

$$\begin{aligned} \frac{c}{b} &= \frac{m}{n} - \frac{a}{b} \\ \frac{c}{b} &= \frac{n}{m} + \frac{a}{b}. \end{aligned}$$

Set both equation equal to each other

$$\begin{aligned} \frac{m}{n} + \frac{a}{b} &= \frac{n}{m} - \frac{a}{b} \\ \frac{2a}{b} &= \frac{m}{n} + \frac{n}{m} = \frac{m^2}{mn} + \frac{n^2}{mn} = \frac{m^2+n^2}{mn} \end{aligned}$$

leaveing us with equality

$$\frac{a}{b} = \frac{m^2+n^2}{2mn}.$$

Rearrange to solve for $\frac{c}{b}$

$$\begin{aligned} \frac{a}{b} &= \frac{m}{n} - \frac{c}{b} \\ \frac{a}{b} &= \frac{c}{b} - \frac{n}{m} \\ \frac{m}{n} - \frac{c}{b} &= \frac{c}{b} - \frac{n}{m} \\ \frac{2c}{b} &= \frac{m}{n} - \frac{n}{m} = \frac{m^2}{mn} - \frac{n^2}{mn} = \frac{m^2-n^2}{mn} \end{aligned}$$

leaving us with equality

$$\frac{c}{b} = \frac{m^2 - n^2}{2mn}.$$

Because $\frac{m}{n}$ is fully reduced, both m and n cannot be even. If both m and n were odd, $m^2 - n^2$ would be a multiple of 4, as an odd square is congruent to 1(mod4) and $2mn$ would not be a multiple of 4. However, 4 would be the smallest possible factor in the numerator $(m^2 - n^2)$ for the denominator $(2mn)$ it would be 2. This shows a to be even, which is contrary to it being defined as odd. It follows that one of m or n is even and one is odd and $m^2 \pm n^2$ is also odd. This shows us that the fractions are reduced completely and we can set the numerators and denominators equal to each other. This yields Euclid's formula

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

which can also be written as

$$a = \frac{m^2 - n^2}{2} \qquad b = mn \qquad c = \frac{m^2 + n^2}{2}.$$

□

6.2 Pythagorean Quadruples

This naturally leads us to question if we can find generalized solutions of Pythagorean quadruples in the same way. A Pythagorean quadruple is

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

Begin by noting the expansion of

$$(m + n)^2 = m^2 + 2mn + n^2$$

Let $a^2 = m^2$, $b^2 = 2mn$, and $d = m + n$. Thus,

$$a^2 + b^2 + c^2 = m^2 + 2mn + n^2 = (m + n)^2 = d^2$$

However, we can see that this formula cannot generate all Pythagorean quadruples through the example of $(1, 2, 2, 3)$ by noting that there are no integer solutions for m and n that satisfy the equation.[12] Suppose instead we take three numbers a, b, and p s.t. $p \mid (a^2 + b^2)$ and $p^2 < a^2 + b^2$. We can use a precise substitution of $c = \frac{a^2+b^2-p^2}{2p}$

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

12. Chandrahas Halai, "Triples and Quadruples: From Pythagoras to Fermat," Plus Magazine, last modified November 14, 2012, accessed February 14, 2021, https://plus.maths.org/content/triples-and-quadruples.

expand

$$= a^2 + b^2 + \frac{a^2 + a^2b^2 - a^2p^2 + a^2b^2 + b^4 - b^2p^2 - a^2p^2 - b^2p^2 + p^4}{4p^2}$$

factor out $a^2 + b^2$

$$= a^2 + b^2 + \frac{(a^2+b^2)^2 - 2p^2(a^2+b^2) + p^4}{4p^2} = \frac{(a^2+b^2)^2}{4p^2} + \frac{a^2+b^2}{2} + \frac{p^2}{4}$$

factor into a perfect square

$$= \left(\frac{a^2+b^2+p^2}{2p}\right)^2$$

We can now let $d^2 = \left(\frac{a^2+b^2+p^2}{2p}\right)^2$, then $d = \frac{a^2+b^2+p^2}{2p}$ and thus $a^2 + b^2 + c^2 = d^2$. Now we can see why the conditions of p are so important. Note that when both a and b are odd, no quadruples are generated.

6.3 Lebesgue's Identity

Pythagorean quadruples also have a close relationship with Lebesgue's identity which states

$$(m^2 + n^2 + p^2 + q^2)^2 = (2mq + 2np)^2 + (2nq - 2mp)^2 + (m^2 + n^2 - p^2 - q^2)^2.$$

Proof. Begin by expanding the base (LHS) of the identity

$$\begin{aligned}(m^2 + n^2 + p^2 + q^2)^2 &= (m^2 + n^2 + p^2 + q^2)(m^2 + n^2 + p^2 + q^2) \\ &= m^4 + m^2n^2 + m^2p^2 + m^2q^2 + m^2n^2 + n^4 + n^2q^2 \\ &+ m^2p^2 + n^2p^2 + p^4 + p^2q^2 + m^2q^2 + n^2q^2 + p^2q^2 + q^4\end{aligned}$$

combine like terms

$$= m^4 + n^4 + p^4 + q^4 + 2m^2n^2 + 2m^2p^2 + 2m^2q^2 + 2n^2p^2 + 2n^2q^2 + 2p^2q^2$$

Organize into factorable groups

$$\begin{aligned}&= (4m^2q^2 + 8mnpq + 4n^2p^2) + (4n^2q^2 - 8mnpq + 4m^2p^2) \\ &+ (m^4 + n^4 + p^4 + q^4 + 2m^2n^2 - 2m^2q^2 - 2m^2p^2 - 2n^2q^2 - 2n^2p^2 + 2p^2q^2) \\ &= (2mq + 2np)^2 + (2nq - 2mp)^2 + (m^2 + n^2 - p^2 - q^2)^2\end{aligned}$$

□

As can be easily seen, Lebesgue's identity is in the exact form of a Pythagorean quadruple, and we can use it to derive an additional method for finding such Pythagorean quadruples. Let $a = 2mq + 2np$, $b = 2nq - 2mp$, $c = m^2 + n^2 - p^2 - q^2$, and $d = m^2 + n^2 + p^2 + q^2$. Thus, the substitution yields $a^2 + b^2 + c^2 = d^2$. However, the formula still cannot generate

all possible Pythagorean quadruples. [13] In fact, it has been shown that no single formula can generate all possible Pythagorean quadruples. We avoid this problem by solving for the ratios of a, b, and c (proof not shown).[14]

$$\frac{a}{d} = \frac{2mp}{m^2+n^2+p^2} \qquad \frac{b}{d} = \frac{2np}{m^2+n^2+p^2} \qquad \frac{c}{d} = \frac{p^2-m^2-n^2}{m^2+n^2+p^2}$$

Similarly, If a scaling factor t is added to Lebesgue's identity, it can generate all possible Pythagorean quadruples.

$$\begin{aligned} a &= t(2mq+2np) \\ b &= t(2nq-2mp) \\ c &= t(m^2+n^2-p^2-q^2) \\ d &= t(m^2+n^2+p^2+q^2) \end{aligned}$$

To write a, b, c, and d in terms of m, n, p, q, and t, we can first set p, $q = 1$, without loss of generality.[15] This yields

$$m = \frac{-b-c}{c-d} \qquad n = \frac{c-b}{a-d} \qquad t = \frac{d-a}{4}$$

When substituted into $t(m^2+n^2-p^2-q^2) = a$, the above solutions are correct if and only if $a^2+b^2+c^2 = d^2$

6.4 The Jacobi-Madden Equation

The Diophantine Equation $a^4+b^4+c^4+d^4 = e^4$ was first explored by Euler in the late 1700s who made the conjecture that 4 was the smallest number of 4th powers that can sum to another 4th power. This is now known as Euler's sum of powers conjecture and was disproved in 1966 by L. J. Lander and T. R. Parkin.[16] Mathematicians Lee Jacobi and Daniel Madden used $a^4+b^4+c^4+d^4 = (a+b+c+d)^4$ to derive a special case of a Pythagorean triple through the following derivation.[17] Beginning with the two identities

$$\begin{aligned} a^4+b^4+c^4+d^4 &= (a+b+c+d)^4 \\ a^4+b^4+(a+b)^4 &= 2(a^2+ab+b^2)^2 \end{aligned}$$

13. Dray Goins and Alain Togbe, "On Pythagorean Quadruples," International Journal of Pure and Applied Mathematics 35, no. 3 (2007): 366, accessed February 14, 2021, https://www.math.purdue.edu/egoins/notes/On-Pythagorean-Quadruplets.pdf.

14. Goins and Togbe, "On Pythagorean," 366.

15. Tito Piezas to Stack Exchange web forum, "Lebesgue's Identity," November 10, 2012, accessed February 14, 2021, https://math.stackexchange.com/questions/921335/lebesgues-identity

16. L. J. Lander and R. R. Parkin, "Counterexample to Euler's Conjecture," American Mathematical Society 72, no. 6 (June 27, 1966): 1, https://doi.org/10.1090/S0002-9904-1966-11654-3.

17. Lee W. Jacobi and Daniel T. Madden, "On $a^4+b^4+c^4+d^4$," The American Mathematical Monthly 115, no. 3 (March 2008): 226-227, https://doi.org/10.1080/00029890.2008.11920519.

By adding $(a+b)^4 + (c+d)^4$ to both sides of the first equation we have

$$a^4 + b^4 + (a+b)^4 + c^4 + d^4 + (c+d)^4 = (a+b)^4 + (c+d)^4 + (a+b+c+d)^4.$$

The 2nd identity allows us to rewrite this as

$$(a^2 + ab + b^2)^2 + (c^2 + cd + d^2)^2 = \left((a+b)^2 + (a+b)(c+d) + (c+d)^2\right)$$

Which is a very cleverly disguised Pythagorean triple! This form can also be parameterized with an elliptical curve and an infinite set of solutions can be found (not shown).[18]

18. Jacobi and Madden, "On $a^4 + b^4 + c^4 + d^4$," 227-230.

References

[1] L. J. Mordell, "Pure and Applied Mathematics," in Diophantine Equations (London, England: Academic Press, 1969), 30:345.

[2] Euclid, "Proposition 30," in Book VII (Alexandria: Euclid, 300 BC), 30, accessed November 4, 2020. https://mathcs.clarku.edu/djoyce/java/elements/bookVII/bookVII0.html#:text=Proposition%2030,one%20of%20the%20original%20numbers.

[3] Kenneth E. Caviness and R. Lewis Caviness, "Euclid's Formula and Properties of Pythagorean Triples," Wolfram Demonstrations Project, last modified March 8, 2017, accessed February 12, 2021, https://demonstrations.wolfram.com/EuclidsFormulaAndPropertiesOfPythagoreanTriples/.

[4] Arvin Deravy, "Bezout's Identity (Bezout's Lemma)," GeeksforGeeks, last modified May 20, 2020, accessed February 13, 2021, https://www.geeksforgeeks.org/bezouts-identity-bezouts-lemma/.

[5] William J. Gilbert, "Linear Diophantine Equations," University Waterloo California Mathematics, accessed November 5, 2020, https://www.math.uwaterloo.ca/ wgilbert/Research/GilbertPathria.pdf.

[6] Deepinder Kaur and Meenal Sambhor, "Diophantine Equations and Their Applications," International Journal of Mathematics and Its Applications 9, no. 1 (2021): 3, http://ijmaa.in/v5n2-b/217-222.pdf.

[7] Andrew Ellinor, "Fermat's Method of Infinite Descent," Brilliant.org, accessed February 11, 2021, https://brilliant.org/wiki/general-diophantine-equations-fermats-method-of/.

[8] L. J. Lander, "Geometric Aspects of Diophantine Equations Involving Equal Sums of Like Powers," The American Mathematical Monthly 75, no. 10 (December 1968): 1061-1062, https://doi.org/10.2307/2315731.

[9] Chandrahas Halai, "Triples and Quadruples: From Pythagoras to Fermat," Plus Magazine, last modified November 14, 2012, accessed February 14, 2021, https://plus.maths.org/content/triples-and-quadruples.

[10] Dray Goins and Alain Togbe, "On Pythagorean Quadruples," International Journal of Pure and Applied Mathematics 35, no. 3 (2007): 366, accessed February 14, 2021, https://www.math.purdue.edu/egoins/notes/On-Pythagorean-Quadruplets.pdf.

[11] Tito Piezas to Stack Exchange web forum, "Lebesgue's Identity," November 10, 2012, accessed February 14, 2021, https://math.stackexchange.com/questions/921335/lebesgues-identity

[12] L. J. Lander and R. R. Parkin, "Counterexample to Euler's Conjecture," American Mathematical Society 72, no. 6 (June 27, 1966): 1, https://doi.org/10.1090/S0002-9904-1966-11654-3.

[13] Lee W. Jacobi and Daniel T. Madden, "On $a^4 + b^4 + c^4 + d^4$," The American Mathematical Monthly 115, no. 3 (March 2008): 226-227, https://doi.org/10.1080/00029890.2008.11920519.