SYSTEMS OF PYTHAGOREAN TRIPLES

CHRISTOPHER TOBIN-CAMPBELL

Abstract. This paper explores systems of Pythagorean triples. It describes the generating formulas for primitive Pythagorean triples, determines which numbers can be the sides of primitive right triangles and how many primitive right triangles those numbers can be a side of, and finally explores systems of three and four right triangles that fit together in three dimensions.

Acknowledgements

I would like to thank Professor Laura Schueller for advising and guiding me through this project. I would also like to acknowledge Professor Pat Keef and Lindsey Witcosky for their help in the editing process.

1. Introduction

Pythagoras lived during the late 6th century B.C.E. His most famous discovery by far is that on a right triangle, the sum of the squares of the lengths of the two legs is equal to the square of the length of the hypotenuse. This theorem, which has come to be known as the Pythagorean Theorem, is not only incredibly powerful, but rich with mathematical extensions that still fascinate mathematicians today. Moreover, at times, seemingly unrelated problems can be reduced to problems involving the Pythagorean Theorem and the many discoveries related to it.

The motivation for this paper stems from the following problem. Consider the ellipsoid

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 + \left(\frac{z}{c}\right)^2 = 1$$

with $a > b > c > 0$ and $a, b, c \in \mathbb{Z}$. Note that if $x = 0$, then

$$(y/b)^2 + (z/c)^2 = 1$$

is an ellipse with focal points at $(0, \pm\sqrt{b^2 - c^2}, 0)$. Similarly, if $y = 0$, then

$$(x/a)^2 + (z/c)^2 = 1$$

is an ellipse with focal points at $(\pm\sqrt{a^2 - c^2}, 0, 0)$ and if $z = 0$, then

$$(x/a)^2 + (y/b)^2 = 1$$

is an ellipse with focal points at $(\pm\sqrt{a^2 - b^2}, 0, 0)$. We are interested in ellipsoids whose focal points have integer coordinates. In other words, we are interested in the system

$$\begin{aligned} b^2 - c^2 &= n_1^2, \\ a^2 - b^2 &= n_2^2 \text{ and} \\ a^2 - c^2 &= n_3^2 \end{aligned} \tag{1.1}$$

where $a, b, c, n_1, n_2, n_3 \in \mathbb{Z}$.

Rearranging these equations gives us a system of equations, each of the form given in the Pythagorean Theorem:

$$\begin{aligned} n_1^2 + c^2 &= b^2, \\ n_2^2 + b^2 &= a^2 \text{ and} \\ n_3^3 + c^2 &= a^2. \end{aligned} \tag{1.2}$$

Therefore, the motivation for this paper stems from trying to find integral solutions to System 1.2. However, we start with the basics of the Pythagorean Theorem. We begin by looking at generating formulas for Pythagorean triples. From there, we explore the properties of each side of a primitive right triangle, focussing on how it is possible to fit two right triangles together so that they share either a leg or the hypotenuse. We show that with each side of a primitive right triangle, the total number of triangles that can share that side is 2^{n-1}, where n is the number of distinct primes in the standard prime factorization of the length of that side. We follow with a proof that the lengths of the two legs of one right triangle cannot be the lengths of the leg and hypotenuse of another right triangle.

From there we move into three dimensions where we first consider the Euler Brick, giving a few simple results as well as considering the perfect cuboid. Lastly, we return to System 1.2 and give Euler's solution to the problem.

2. Generating All Pythagorean Triples

When asked to give examples of Pythagorean triples, a typical math student can usually give two or three examples: (3,4,5), (5,12,13) and maybe (15,8,17). Not many students can come up with more triples off the top of their heads. It is therefore desirable to find a way of generating Pythagorean triples that is simpler than the guess and check method. We begin with some basic definitions and introductory lemmas.

Definition 2.1. *A* ***Pythagorean triple*** *is a triple of positive integers* (a, b, c) *satisfying* $a^2 + b^2 = c^2$*.*

We call a triple *primitive* when the three integers (a, b, c) have no common factor. To describe Pythagorean triples, it is only necessary to find the primitive triples, since any non-primitive triple is just a multiple of a primitive triple, as is proved in Lemma 2.4.

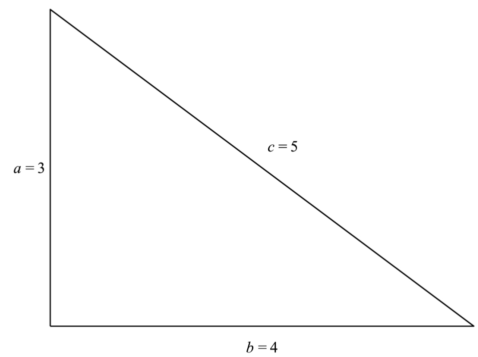
The following basic result will be used frequently throughout this paper.

Lemma 2.2. *For integers* a*,* b *and* d*, if* d *divides* a *and* d *divides* b*, then* d *divides any linear combination of* a *and* b*.*

Proof. Suppose $d|a$ and $d|b$, then $a = dx$ for some integer x, and $b = dy$ for some integer y. Therefore, for any α and β, $\alpha a + \beta b = (\alpha x + \beta y)d$ and thus $d|(\alpha a + \beta b)$. This completes the proof. □

Note that if $d|a$ and $d|b$, then $d|(a^2 + b^2)$ and $d|(a^2 - b^2)$. Also, if a and b are relatively prime and if $d|(a + b)$ and $d|(a - b)$, then either $d = 2$ or $d = 1$, since the sum and difference of $(a + b)$ and $(a - b)$ are $2a$ and $2b$ respectively.

FIGURE 1. The Smallest Primitive Pythagorean Triple



The next lemma is important when dealing with numbers that can be written as the sum of two squares.

Lemma 2.3. *Suppose $x^2 = kl$ where x, k and l are all positive integers. If $gcd(k,l) = 1$, then both k and l must be squares.*

Proof. By the unique factorization of the integers, there exist unique primes

$$p_1, p_2, \ldots, p_m$$

and unique positive integers

$$\alpha_1, \alpha_2, \ldots, \alpha_m$$

such that

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_m^{\alpha_m}$$

and

$$x^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \ldots p_m^{2\alpha_m}.$$

Since $x^2 = kl$ and $gcd(k,l) = 1$, we know that if $p_i | k$, then $p_i \nmid l$. Thus, k and l are both equal to the product of some of the p_i's, where each p_i is raised to an even power. Thus, the square roots of both k and l are integers, and therefore, both k and l are squares. $\square$

Using mathematical induction, it is easy to show that if $x^2 = k_1 k_2 \dots k_n$ where the k_i are pairwise relatively prime, then each k_i is a perfect square. We now prove the following lemma about the primitivity of Pythagorean triples.

Lemma 2.4. *For a Pythagorean triple* (a, b, c)*, the following properties are equivalent:*

(1) *a, b, and c have no common factor, i.e., the triple is primitive,*
(2) *a, b, and c are pairwise relatively prime,*
(3) *two of a, b, and c are relatively prime.*

Proof. We start by showing that (1) implies (2). To do this, we will prove the contrapositive. Let p be prime and suppose that p divides both a and b. Then by Lemma 2.2, p divides $a^2 + b^2 = c^2$. But if p divides c^2, then $p|c$, and thus (1) is violated. Similarly, if $p|a$ and $p|c$, then by Lemma 2.2, $p|(c^2 - a^2) = b^2$, and again, (1) is violated. Obviously the same is true if $p|b$ and $p|c$. Thus, we have shown that (1) implies (2). It is obvious that (2) implies (3). To prove that (3) implies (1), first assume that a and b are relatively prime. Let p be prime and assume that $p|c$ and $p|a$. Then $p|(c^2 - a^2) = b^2$ which implies that $p|b$, which is a contradiction. A similar argument can be used for the other cases. This completes the proof. □

Theorem 2.5 gives us an easy way to generate primitive Pythagorean triples. This is a standard result in number theory and can be found in an article entitled *Pythagorean Triples* by Keith Conrad [1].

Theorem 2.5. *If* (a, b, c) *is a primitive Pythagorean triple, then one of a or b is even and the other is odd. Moreover, taking b to be even,*

$$a = k^2 - l^2, \; b = 2kl, \; c = k^2 + l^2$$

for some integers k and l with $k > l > 0$, $gcd(k, l) = 1$, and $k \not\equiv l$ mod 2. Conversely, for such integers k and l the above formulas yield a primitive Pythagorean triple.

Proof. First, let k and l be positive, relatively prime integers with $k > l > 0$ and $k \not\equiv l \mod 2$. We check that given $a = k^2 - l^2$, $b = 2kl$ and $c = k^2 + l^2$ that (a, b, c) is a primitive Pythagorean triple. We observe that

$$a^2 + b^2 = (k^2 - l^2)^2 + (2kl)^2 = k^4 + 2k^2l^2 + l^4 = (k^2 + l^2)^2 = c^2,$$

showing that $(k^2 - l^2, 2kl, k^2 + l^2)$ is a Pythagorean triple. To show that it is primitive, let d be an integer that divides $(k^2 - l^2)$ and $(k^2 + l^2)$; by Lemma 2.2, d must also divide the sum and difference of $(k^2 - l^2)$ and $(k^2 + l^2)$, which are $2k^2$ and $2l^2$. Since $(k^2 - l^2)$ and $(k^2 + l^2)$ are odd, d must also be odd, and thus $d|k^2$ and $d|l^2$. But since $gcd(k, l) = 1$ and thus $gcd(k^2, l^2) = 1$, we have $d = 1$ and thus $(k^2 - l^2)$ and $(k^2 + l^2)$ are relatively prime. By Lemma 2.4, we can conclude that $(k^2 - l^2, 2kl, k^2 + l^2)$ is a primitive Pythagorean triple.

Next, assume that (a, b, c) is a primitive Pythagorean triple. To show that one of a and b is even and the other is odd, note that if both a and b are even, then they are both divisible by 2, which, by Lemma 2.4, is a contradiction to the fact that (a, b, c) is a primitive Pythagorean triple. Thus, both a and b cannot be even. Next, assume that both a and b are odd. Then $a^2 \equiv b^2 \equiv 1 \mod 4$, so $c^2 = a^2 + b^2 \equiv 2 \mod 4$. However, 2 is not a square modulo 4, thus a and b cannot both be odd. Therefore, one of a and b is odd and the other is even.

Without loss of generality, from now on, we will take b to be even. We rewrite our equation $a^2 + b^2 = c^2$ as

$$b^2 = c^2 - a^2 = (c + a)(c - a). \tag{2.1}$$

Since b is even and $(c + a)$ and $(c - a)$ are both even, we can divide both sides of equation (2.1) by 4. Doing this yields

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

Now we see that the two integers on the right are relatively prime, because by Lemma 2.2 if d divides both $(c + a)/2$ and $(c - a)/2$, it must divide their sum and

TABLE 1. Examples of Pythagorean Triples

k	l	a	b	c
2	1	3	4	5
3	2	5	12	13
4	1	15	8	17
4	3	7	24	25

difference, which are c and a respectively. Since c and a are relatively prime, $d = 1$. Thus $gcd((c+a)/2, (c-a)/2) = 1$. By Lemma 2.3, since the product of $(c+a)/2$ and $(c-a)/2$ is a square, and since $gcd((c+a)/2, (c-a)/2) = 1$, we know that $(c+a)/2 = k^2$ and $(c-a)/2 = l^2$ for some relatively prime positive integers k and l. Doing some simple algebra yields

$$c = k^2 + l^2, \; a = k^2 - l^2.$$

Finally, $(b/2)^2 = k^2l^2$ implies that $b = 2kl$.

Lastly, we must check that $k \not\equiv l \bmod 2$. Since k and l are relatively prime, they are not both even. If they were both odd, then $k^2 + l^2$, $2kl$, and $k^2 - l^2$ would all be even, violating the primitivity of (a, b, c). This completes the proof. $\square$

Example: Let $k = 2$ and $l = 1$. Clearly $gcd(k, l) = 1$ and $k \not\equiv l \bmod 2$. Therefore, Theorem 2.5 tells us that $(2^2 - 1^2, 2 \cdot 2 \cdot 1, 2^2 + 1^2)$ is a primitive Pythagorean triple. This, of course, is just the triple (3,4,5). Table 1 has a list of primitive Pythagorean triples along with their generators.

It is helpful to categorize primitive Pythagorean triples in a slightly different way. Again, this is a standard result in number theory and can be found in the article *Pythagorean Triples* by Keith Conrad [1].

Theorem 2.6. *Given a primitive Pythagorean triple (a, b, c) with b even, there exist s and t where $s > t \geq 1$ are odd integers that are relatively prime such that*

$$a = st, \; b = \frac{s^2 - t^2}{2}, \; c = \frac{s^2 + t^2}{2}.$$

Moreover, for such integers s and t the above formulas yield a primitive Pythagorean triple.

Proof. From Theorem 2.5 we know that there exist integers k and l such that

$$a = k^2 - l^2 = (k+l)(k-l)$$

where $k > l > 0$, $gcd(k,l) = 1$, and $k \not\equiv l \pmod 2$. If we take $s = k+l$ and $t = k-l$ we have two odd integers that are relatively prime with $s > t \geq 1$. From Theorem 2.5 we know that $b = 2kl$. Solving for k and l in terms of s and t yields $k = (s+t)/2$ and $l = (s-t)/2$, which implies that $b = (s^2 - t^2)/2$, and $c = k^2 + l^2 = (s^2+t^2)/2$. This completes the proof. □

Example: Let $s = 5$ and $t = 3$. Then Theorem 2.6 tells us that

$$(5 \cdot 3, (5^2 - 3^2)/2, (5^2 + 3^2)/2),$$

or rather $(15, 8, 17)$, is a primitive Pythagorean triple.

3. Primitive Pythagorean Triangles that share a Side

The obvious geometric interpretation of Pythagorean triples is right triangles. The sides of a right triangle with integer lengths form the terms of a Pythagorean triple, and visa versa. In this section, and for the rest of the paper, we will be considering Pythagorean triples with right triangles in mind. The first question that we address concerns primitive right triangles that share a side where sharing a side means that two right triangles have one side that is the same length, while the other two sides are different lengths.

3.1. **Triangles that share the even length side.** From Theorem 2.5, we know that every primitive right triangle has one leg that is even, one leg that is odd, and a hypotenuse that is odd. We first consider those triangles that share the even length side.

Lemma 3.1. *The even side of a primitive right triangle is divisible by 4.*

Proof. The result is clear from Theorem 2.5. □

Theorem 3.2. *Given a number b divisible by 4, let n denote the number of distinct primes in the prime factorization of b. Then b is the even length side of exactly 2^{n-1} primitive right triangles.*

Proof. From Theorem 2.5, we know that given a primitive Pythagorean triple (a, b, c), then

$$a = k^2 - l^2,\ b = 2kl,\ c = k^2 + l^2$$

for some positive integers k and l where $gcd(k, l) = 1$, $k > l$ and one of k and l is even while the other is odd. Moreover, we know that given k and l that meet these criteria, they generate a primitive Pythagorean triple.

Suppose that b is a number divisible by 4, and let n be the number of distinct primes in the prime factorization of b. In other words, let $p_1, p_2, \ldots, p_n$ be the primes in the prime factorization of b such that

$$b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}.$$

Since b is divisible by 4, one of the primes is equal to 2, and moreover, we know that there are at least 2 factors of 2 in the factorization of b. Without loss of generality we can assume that $p_1 = 2$.

With this in mind, we see that the number of primitive right triangles that have a leg of length b is equal to the number of ways we can factor b into $b = 2kl$ where k and l are as in Theorem 2.5. Since b is divisible by 4, and thus $(b/2)$ is divisible by 2, we know one of k and l will be even and the other one will be odd.

Since $gcd(k, l)$ must equal 1, we are simply interested in the number of ways we can partition the n primes into two sets where the product of all the terms in one set is k and the product of the terms in the other set is l. In other words, we are interested in the total number of subsets of an n element set divided by 2, since each subset corresponds to a value for k or l, and the compliment of the subset corresponds to the other. This gives us $(2^n/2) = 2^{n-1}$. The reason we divide by

2 is that k must be greater than l, and the total number of subsets counts those partitions where $l > k$.

It remains to show that each new choice of k and l will give a distinct primitive right triangle. Let k_1, l_1 and k_2, l_2 be generators for two different primitive Pythagorean triples with even term b. If $k_1 = k_2$, then l_1 must also equal l_2, and we would not have two distinct right triangles. Thus, we can assume without loss of generality that $k_1 > k_2$, meaning that $l_1 < l_2$. It does not take much to see that it necessarily follows that $a_1 = k_1^2 - l_1^2 > k_2^2 - l_2^2 = a_2$. Thus, given two different choices of k and l, we necessarily get a different value for a, the odd length leg of our triangle, which necessitates a different hypotenuse, or c value, as well. Therefore, there are 2^{n-1} primitive right triangles that have the even side length equal to b. This completes the proof. $\square$

Example: Consider an example with the number 12. We factor 12 into $3 \cdot 2^2$. Theorem 3.2 tells us that there are $2^{2-1} = 2$ primitive right triangles that have 12 as the even leg. Let $k = 3$ and $l = 2$. Then clearly k and l satisfy the necessary conditions to generate a primitive Pythagorean triple, and indeed, we see that

$$a = 3^2 - 2^2 = 5, \; b = 2 \cdot 3 \cdot 2 = 12, \; c = 3^2 + 2^2 = 13$$

is a primitive right triangle. However, we could choose $k = 6$ and $l = 1$, in which case we get

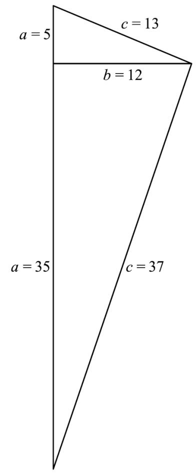
$$a = 6^2 - 1 = 35, \; b = 2 \cdot 6 \cdot 1 = 12, \; c = 6^2 + 1 = 37$$

as our primitive right triangle.

3.2. **Triangles that share an odd length side.** In the same way that we counted the number of triangles that share an even length leg, we can count the number of triangles that share an odd length leg.

Lemma 3.3. *Any odd number can be the odd length leg of a primitive Pythagorean triangle.*

FIGURE 2. Pictorial Example of Theorem 3.2



Proof. By Theorem 2.6, the odd length leg of a primitive Pythagorean triangle can be factored into $a = st$ for relatively prime, odd, positive integers s and t where $s > t$. Thus, given any positive odd integer q, let $t = 1$, and set $s = q$. Therefore, $a = q$. $\square$

Theorem 3.4. *Given an odd number a, let n denote the number of distinct primes in the prime factorization of a. Then a is the odd length leg of 2^{n-1} primitive right triangles.*

Proof. Not surprisingly, the proof of this theorem is similar to the proof given for Theorem 3.2. Because of this, some of the details will be left out. From Theorem 2.6, we know that given a primitive Pythagorean triple (a, b, c), that

$$a = st, \ b = \frac{s^2 - t^2}{2}, \ c = \frac{s^2 + t^2}{2}$$

for some positive odd integers s and t where $gcd(s, t) = 1$, $s > t$. Moreover, we know that given s and t that meet these criteria, they generate a primitive Pythagorean triple.

Let a be an odd positive integer, and let n be the number of distinct primes in the prime factorization of a. In a similar fashion as in the proof of Theorem 3.2, we see that the number of primitive right triangles that have a leg of length a is equal to the number of ways we can factor a into $a = st$ where $gcd(s,t) = 1$ and $s > t$. Exactly as in the proof of Theorem 3.2, this number is 2^{n-1}.

Checking that each distinct choice of s and t gives a distinct primitive right triangle can be done in the same way as the proof of Theorem 3.2. Thus, given two different choices of s and t, we necessarily get a different value for b, the even length side of our triangle, which necessitates a different hypotenuse, or c value, as well. Therefore, there are 2^{n-1} primitive right triangles that have the odd length leg equal to a. This completes the proof. $\square$

Example: The number 15 factors into $5 \cdot 3$. Theorem 3.4 tells us that there are $2^{2-1} = 2$ primitive right triangles that have 15 as the odd length leg. Let $s = 5$ and $t = 3$. Clearly s and t satisfy the conditions of 2.6, and so

$$a = 5 \cdot 3,\ b = \frac{5^2 - 3^2}{2} = 8,\ c = \frac{5^2 + 3^2}{2} = 17$$

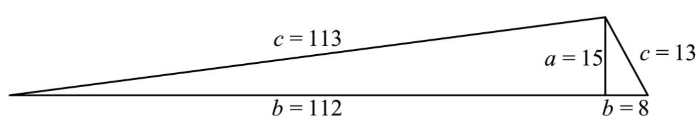
is a primitive right triangle.

However, we could choose $s = 15$ and $t = 1$, in which case we get

$$a = 15 \cdot 1,\ b = \frac{15^2 - 1}{2} = 112,\ c = \frac{15^2 + 1}{2} = 113$$

as our primitive right triangle.

Figure 3. Pictorial Example of Theorem 3.4



3.3. **The Hypotenuse of a primitive right triangle.** The last side of the triangle we consider is the hypotenuse. Determining which numbers can be the hypotenuse of more than one primitive right triangle is more involved than the proofs of Theorems 3.2 and 3.4. Because of this, we include references to proofs, instead of the proofs themselves, for some of the theorems that follow.

Theorem 3.5 uses results from Quadratic Reciprocity. Specifically, it uses the well known result in number theory that the equation $n^2 \equiv -1 \pmod{p}$ for an integer n has a solution if and only if $p \equiv 1 \pmod{4}$. For more information on Quadratic Reciprocity, see Chapter 24 of *A Friendly Introduction to Number Theory* by Joseph H. Silverman[2].

Theorem 3.5. *If c is the hypotenuse of a primitive right triangle, then c is of the form*

$$c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

where $p_i \equiv 1$ (mod 4) for $1 \leq i \leq n$.

Proof. Choose k and l as in Theorem 2.5 so that $c = k^2 + l^2$ where $gcd(k,l) = 1$ and $k \not\equiv l \pmod{2}$. Since c is odd, $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where each p_i is odd. For each $1 \leq i \leq n$,

$$\begin{aligned} k^2 + l^2 &\equiv 0 \ (mod\ p_i) \\ k^2 &\equiv -l^2 \ (mod\ p_i) \\ \text{and } (kl^{-1})^2 &\equiv -1 \ (mod\ p_i). \end{aligned}$$

Here, l^{-1} is the inverse of l under multiplication mod p_i, which we are guaranteed exists since $gcd(k,l) = 1$. By Quadratic Reciprocity, $p_i \equiv 1 \pmod{4}$. This completes the proof. □

Theorem 3.5 has further clarified our understanding of the hypotenuse of primitive right triangles. In the following theorems, we use this result, as well as a result proved by Judith D. Sally and Paul J. Sally Jr. in Chapter 4 of *Roots To Research*[3] to prove that given a number c of the form

$$c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$$

where each $p_i \equiv 1 \pmod{4}$, that c is the hypotenuse of exactly 2^{n-1} primitive Pythagorean triangles.

Definition 3.6. *Given a number $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where each $p_i \equiv 1 \pmod 4$, let $\mathbf{N}(\mathbf{c^2})$ denote the total number of ways, both primitive and non-primitive, that c^2 can be written as the sum of two squares of positive integers, not counting trivial variations ($a^2 + b^2$ does not count separately from $b^2 + a^2$). Let $\mathbf{N_p}(\mathbf{c^2})$ denote the number of primitive ways c^2 can be written as the sum of two squares of positive integers.*

In Theorem 4.12 of *Roots To Research*[3], Judith Sally and Paul Sally Jr. prove that given a number $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where each $p_i \equiv 1 \pmod 4$, that

$$N(c^2) = \frac{1}{2}\left((2e_1 + 1)(2e_2 + 1) \cdots (2e_n + 1) - 1\right).$$

Our task in the remainder of this section is to use this number $N(c^2)$ to find $N_p(c^2)$.

For the sake of brevity, for the remainder of this section we will assume that c is of the form $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ where each $p_i \equiv 1 \pmod 4$.

Lemma 3.7. *Given c,*

$$N_p(c^2) = N(c^2) - \sum N_p\left((c/d)^2\right)$$

where the summation runs through each divisor d of c where $1 < d < c$.

Proof. We must prove that $\sum N_p\left((c/d)^2\right)$ is equal to the number of ways c^2 can be written as the sum of two squares in a non-primitive way, since by removing the non-primitive solutions we are left with only the primitive solutions.

First, note that given a triple $a_1^2 + b_1^2 = (c/d_1)^2$, multiplying through by d^2 gives us a non-primitive solution $(a_1 d_1)^2 + (b_1 d_1)^2 = c^2$ that is counted in $N(c^2)$. This proves that each triple in $\sum N_p\left((c/d)^2\right)$ corresponds to exactly one non-primitive triple in $N(c^2)$.

Next, note that given a non-primitive triple $a_2^2 + b_2^2 = c^2$ with d_2 the greatest common factor of a_2, b_2 and c, that the triple $(a_2/d_2)^2 + (b_2/d_2)^2 = (c/d_2)^2$ is counted in $\sum N_p\left((c/d)^2\right)$ exactly once. This proves that each non-primitive triple in $N(c^2)$ corresponds to exactly one triple in $\sum N_p\left((c/d)^2\right)$.

Therefore, there is a one to one relationship between the non-primitive triples in $N(c^2)$ and $\sum N_p\left((c/d)^2\right)$. Thus, $N_p(c^2) = N(c^2) - \sum N_p\left((c/d)^2\right)$ as was claimed. This completes the proof. $\square$

Lemma 3.7 gives us a formula for finding $N_p(c^2)$, but the formula is recursive. The next two theorems prove that the formula for $N_p(c^2)$ simplifies to 2^{n-1} where n is the number of distinct primes in the prime factorization of c.

Theorem 3.8. *Given $c = p_1 p_2 \cdots p_n$, $N_p(c^2) = 2^{n-1}$.*

Proof. We proceed by induction. Let $c = p_1$ where $p_1 \equiv 1 \pmod 4$. Then by Lemma 3.7, $N_p(c^2) = N(c^2) - \sum N_p\left((c/d)^2\right)$ for each divisor d of c between 1 and c. But since $c = p_1$ (and thus $e_1 = 1$),

$$N_p(c^2) = N(c^2) = \frac{1}{2}\left((2e_1 + 1) - 1\right) = 1.$$

Since $n = 1$ in this base case, $N_p(c^2) = 1 = 2^{n-1}$.

Our induction hypothesis is that $N_p(p_1^2 p_2^2 \cdots p_k^2) = 2^{k-1}$ for all $1 \leq k < n$. Since each $e_i = 1$, note that

$$\begin{aligned}
\sum N_p\left((c/d)^2\right) &= \\
\left(N_p(p_1^2) + N_p(p_2^2) + \cdots + N_p(p_n^2)\right) &+ \\
\left(N_p(p_1^2p_2^2) + N_p(p_1^2p_3^2) + \cdots + N_p(p_1^2p_n^2) + \cdots + N_p(p_{n-1}^2p_n^2)\right) &+ \\
&+ \\
&\vdots \\
&+ \\
\left(N_p(p_1^2p_2^2 \cdots p_{n-1}^2) + \cdots + N_p(p_2^2p_3^2 \cdots p_n^2)\right). &
\end{aligned} \tag{3.1}$$

Since by our induction hypothesis $N_p(p_i^2) = 2^0 = 1$ and $N_p(p_i^2p_j^2p_k^2) = 2^2 = 4$ etc., Equation 3.1 can be simplified to

$$\sum N_p\left((c/d)^2\right) = \binom{n}{1}2^0 + \binom{n}{2}2^1 + \cdots + \binom{n}{n-1}2^{n-2}.$$

The binomial theorem tells us that

$$(1+2)^n = \binom{n}{0}2^0 + \binom{n}{1}2^1 + \cdots + \binom{n}{n-1}2^{n-1} + \binom{n}{n}2^n,$$

and therefore

$$\binom{n}{1}2^0 + \binom{n}{2}2^1 + \cdots + \binom{n}{n-1}2^{n-2} = \frac{(1+2)^n - 1}{2} - \binom{n}{n}2^{n-1}.$$

Therefore, it follows that

$$\begin{aligned} N_p(c^2) &= \\ \frac{(1+2)^n - 1}{2} - \sum N_p\left((c/d)^2\right) &= \\ \frac{(1+2)^n - 1}{2} - \left(\frac{(1+2)^n - 1}{2} - \binom{n}{n}2^{n-1}\right) &= \\ &= 2^{n-1}. \end{aligned}$$

This completes the proof. □

The following theorem is the final result for this section. It is proved by induction on the sum of the powers on each prime in the prime factorization of c, and uses Theorem 3.8 as the base case.

Theorem 3.9. *Suppose* $c = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n}$ *where each* $p_i \equiv 1$ *(mod 4). Then* c *is the hypotenuse of exactly* 2^{n-1} *primitive Pythagorean triangles, or* $N_p(c^2) = 2^{n-1}$.

Proof. We proceed by induction on the sum of the powers on each prime in the prime factorization of c, or rather, we proceed by induction on

$$\sum_{0<i\leq n} e_i.$$

Assume $e_1 = e_2 = \cdots = e_n = 1$. Then by Theorem 3.8, $N_p(c^2) = 2^{n-1}$. This will serve as our base case.

Our induction hypothesis is that $N_p(c^2) = 2^{n-1}$ for $\sum_{0<i\leq n} e_i < K$ for some fixed integer K. Next, notice that the total number of divisors of c with 1 prime in their prime factorization is $(e_1 + e_2 + \cdots + e_n)$, and the total number of divisors of c with 2 primes in their prime factorization is

$$(e_1e_2 + e_1e_2 + \cdots + e_1e_n + e_2e_3 + \cdots + e_{n-1}e_n).$$

This pattern continues until we notice that the total number of divisors of c with all n primes in their prime factorization of c is $(e_1e_2e_3\cdots e_n - 1)$. We subtract 1 since we are only including those divisors which are less than c.

Now that we understand how many divisors of c there are, we can calculate $N_p(c^2)$ using Lemma 3.7. First we compute

$$\begin{aligned}
\sum N_p\left((c/d)^2\right) &= \\
N_p(p_1)(e_1+e_2+\cdots+e_n) + N_p(p_2)(e_1+e_2+\cdots+e_n) &+\cdots+ \\
N_p(p_n)(e_1+e_2+\cdots+e_n) &+ \\
N_p(p_1p_2)(e_1e_2+e_1e_3+\cdots+e_{n-1}e_n) &+ \\
N_p(p_1p_3)(e_1e_2+e_1e_3+\cdots+e_{n-1}e_n) &+\cdots+ \\
N_p(p_{n-1}p_n)(e_1e_2+e_1e_3+\cdots+e_{n-1}e_n) &+ \\
+\cdots+ & \\
N_p(p_1p_2\cdots p_n)(e_1e_2\cdots e_n - 1) &
\end{aligned}$$

which, according to our induction hypothesis, can be rewritten as

$$\begin{aligned}
\sum N_p\left((c/d)^2\right) = \quad & (2^0)(e_1+e_2+\cdots+e_n) && + \\
& (2^1)(e_1e_2+e_1e_3+\cdots+e_{n-1}e_n) && + \\
& +\cdots+ && \\
& (2^{n-1})(e_1e_2\cdots e_n - 1). &&
\end{aligned}$$

Next, consider the expression

$$(2e_1+1)(2e_2+1)\cdots(2e_n+1).$$

Expanding gives us

$$
\begin{aligned}
(2e_1+1)(2e_2+1)\cdots(2e_n+1) &= \\
1+2(e_1+e_2+\cdots+e_n) &+ \\
2^2(e_1e_2+e_1e_3+\cdots+e_{n-1}e_n) &+ \\
+\cdots+ & \\
2^{n-1}(e_1e_2\cdots e_{n-1}+e_1e_2\cdots e_{n-2}e_n) &+ \\
2^n(e_1e_2\cdots e_n) &
\end{aligned}
\tag{3.2}
$$

We note that

$$
\begin{aligned}
\frac{1}{2}\left((2e_1+1)(2e_2+1)\cdots(2e_n+1)-1\right) &= \\
(e_1+\cdots+e_n)+\cdots+2^{n-1}(e_1e_2\cdots e_n) &= \\
\sum N_p\left((c/d)^2\right)+2^{n-1}. &
\end{aligned}
\tag{3.3}
$$

Therefore, since

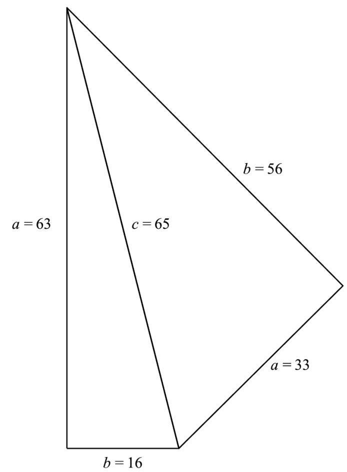
$$N_p(c^2)=\frac{1}{2}\left((2e_1+1)(2e_2+1)\cdots(2e_n+1)-1\right)-\sum N_p\left((c/d)^2\right),$$

$N_p(c^2)=2^{n-1}$ as we set out to prove. This completes the proof. $\square$

Example: Consider the number 65 which factors into $65 = 5\cdot 13$. Both 5 and 13 are primes equivalent to 1 modulo 4. Therefore, 65 can be the hypotenuse of $2^{2-1}=2$ primitive right triangles, namely $(63, 16, 65)$ and $(33, 56, 65)$. Notice that unlike the proofs of Theorems 3.2 and 3.4, the proof of Theorem 3.9 does not provide us with an easy way to find multiple solutions.

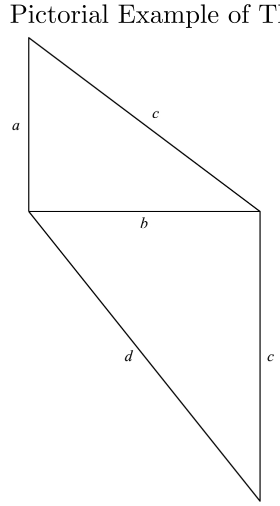
Theorem 3.9 concludes our discussion of the sides of primitive Pythagorean triangles nicely. We have shown that for all three sides, if we have a number that can be a side of a primitive Pythagorean triple, it can be that same side (odd leg, even leg, hypotenuse) of exactly 2^{n-1} primitive Pythagorean triangles, where n is the number of primes in the prime factorization of the number.

FIGURE 4. Pictorial Example of Theorem 3.9



3.4. **Triangles that share a leg and hypotenuse.** Now that we have an understanding of how one number can serve as the side of more than one primitive right triangle, we consider right triangles, primitive or not, which share two sides. In other words, we consider whether it is possible for the lengths of the two legs of one right triangle to be the lengths of the leg and hypotenuse of another right triangle.

FIGURE 5. Pictorial Example of Theorem 3.10



Theorem 3.10 states that this is impossible.

Theorem 3.10. *Given a Pythagorean triple (a, b, c) where $a^2 + b^2 = c^2$, it is never the case that there exists another triple (c, b, d) where $c^2 + b^2 = d^2$.*

Proof. We proceed by contradiction using a reduction argument. Assume that there exists a system of Pythagorean triples (a, b, c) and (c, b, d) where

$$a^2 + b^2 = c^2 \tag{3.4}$$

and

$$c^2 + b^2 = d^2. \tag{3.5}$$

Since we are only interested in positive integers, and since we are assuming that there is at least one solution, there must be a solution for this system where the value of d is smaller than all other values of d that are values in solutions to this system of equations. We call the solution with the smallest d value minimal.

Let a, b, c and d be the minimal solution for equations 3.4 and 3.5. Note that if $p|b$ and $p|c$, then by Lemma 2.2, $p|d$ and $p|a$. This would mean that both triples could be divided through by p resulting in two Pythagorean triples $(a/p, b/p, c/p)$ and $(c/p, b/p, d/p)$ that still share two terms. This would contradict the fact that a, b, c and d is the minimal solution. Thus, we know that (a, b, c) and (c, b, d) are both primitive Pythagorean triples.

Solving equations 3.4 and 3.5 for c^2 and adding the resulting equations together yields

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

Since d and a are both odd, $d - a$ and $d + a$ are both even, and it follows that

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

Note that by Lemma 2.2, $(d + a)/2$ and $(d - a)/2$ are relatively prime. Therefore

$$\left(\frac{d-a}{2}, \frac{d+a}{2}, c\right)$$

is a primitive Pythagorean triple. By Theorem 2.5, either:

$$\text{Case 1: } \frac{d+a}{2} = k^2 - l^2, \ \frac{d-a}{2} = 2kl$$

or

$$\text{Case 2: } \frac{d-a}{2} = k^2 - l^2, \ \frac{d+a}{2} = 2kl$$

where $gcd(k, l) = 1$, $k > l > 0$, and one of k and l is even and the other is odd.

Solving equations 3.4 and 3.5 for b^2 and adding the resulting equations together yields $2b^2 = d^2 - a^2 = (d + a)(d - a)$. Regardless of whether we are in Case 1 or Case 2, we see that $2b^2 = (d + a)(d - a) = 2(k^2 - l^2)2(2kl)$. Using the fact that b is even, it follows that

$$\left(\frac{b}{2}\right)^2 = (k^2 - l^2)kl.$$

Since $gcd(k, l) = 1$, it is clear that $gcd(k^2 - l^2, k) = 1$ and $gcd(k^2 - l^2, l) = 1$, since any divisor of k divides k^2 but not l^2, and visa versa for l. Thus, $k^2 - l^2$, k and l are pairwise relatively prime, and so by Lemma 2.3 each one must itself be a square, since their product is a square.

Let $k = r^2$, $l = s^2$ and $k^2 - l^2 = t^2$ and note that $t^2 = k^2 - l^2 = (k + l)(k - l) = (r^2 + s^2)(r^2 - s^2)$. Since one of k and l is even and the other is odd, we know that t^2 is odd. Because of this, $(k + l)$ and $(k - l)$ are relatively prime, since any divisor of the two of them would have to divide their sum and difference, which are $2k$ and $2l$ respectively. But since t^2 is odd, we know that the divisor cannot be 2, thus the divisor would have to divide both k and l, meaning that the divisor is simply 1. It follows that $r^2 + s^2$ and $r^2 - s^2$ are relatively prime. Thus, by Lemma 2.3, $r^2 + s^2$ and $r^2 - s^2$ are squares, since their product is t^2. Thus, $r^2 + s^2 = x^2$ and $r^2 - s^2 = y^2$ for some positive integers x and y.

Therefore, (y, s, r) and (r, s, x) are two Pythagorean triples where $y^2 + s^2 = r^2$ and $r^2 + s^2 = x^2$. In other words, the numbers y, s, r and x yield another solution to equations 3.4 and 3.5. However,

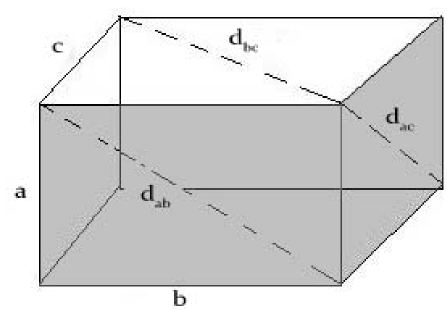
$$x^2 = s^2 + r^2 = k + l < 2k \leq 2kl \leq \frac{d+a}{2} < d \leq d^2.$$

Since a, b, c and d was taken at the beginning to be the minimal solution, the fact that $x^2 < d^2$ is a contradiction. Therefore, given a Pythagorean triple (a, b, c), it is never the case that there is exists another Pythagorean triple (c, b, d). This completes the proof. $\square$

4. Pythagorean Triples in 3-Dimensions

4.1. **The Euler Brick.** We now move our discussion to considering how we can fit three Pythagorean triangles together in 3-dimensions. Consider a cuboid (right parallelepiped) with side lengths a, b, and c, and face diagonals d_{ab}, d_{ac}, and d_{bc}, where d_{ab} is the face diagonal across the face with sides a and b, and so on, as in Figure 6.

Figure 6. Pictorial Example of a Cuboid



From the faces of this cuboid, we find three equations:

$$a^2 + b^2 = d_{ab}^2 \tag{4.1}$$

$$a^2 + c^2 = d_{ac}^2 \tag{4.2}$$

$$b^2 + c^2 = d_{bc}^2 \tag{4.3}$$

When all six values, a, b, c, d_{ab}, d_{ac}, and d_{bc}, are integers, the cuboid is called an *Euler Brick*, and the three equations above are Pythagorean triples.

Euler Bricks have not yet been fully classified, but there are some things we know about them. We call an Euler Brick primitive if all three Pythagorean triples are primitive.

Theorem 4.1. *There are no primitive Euler Bricks.*

Proof. We proceed by contradiction. Suppose we have a primitive Euler Brick, and that in Equation 4.1, b is the even term. Then by Theorem 2.5, both a and c must be odd. This is a contradiction because both a and c cannot be odd in Equation 4.2 by Theorem 2.5. Next, let a be the even term in 4.1. Then by Theorem 2.5, both b and c must be odd. This is a contradiction because both b and c cannot be odd in Equation 4.2. Therefore, there are no primitive Euler Bricks. This completes the proof. □

In 1740, Nicholas Saunderson found a formula for generating different Euler Bricks, although perhaps not all Euler bricks [4].

Theorem 4.2. *If* (x, y, z) *is a Pythagorean triple, then*

$$(a, b, c) = (x(4y^2 - z^2), y(4x^2 - z^2), 4xyz)$$

is an Euler Brick with face diagonals

$$\begin{aligned} d_{ab} &= z^3 \\ d_{ac} &= x(4y^2 + z^2) \\ d_{bc} &= y(4x^2 + z^2). \end{aligned}$$

Proof. The proof is just a matter of computation. □

Theorem 4.2 proves that there are infinitely many Euler Bricks. The smallest Euler Brick (measured by the longest side) has sides $(a, b, c) = (240, 117, 44)$ and face diagonals $d_{ab} = 267$, $d_{ac} = 244$ and $d_{bc} = 125$, and was discovered by Paul Halcke in 1719[4].

If the interior diagonal D of an Euler Brick is also an integer, that is, if

$$D = \sqrt{a^2 + b^2 + c^2}$$

is an integer, then the Euler Brick is called a *Perfect Cuboid.* It is not known whether any Perfect Cuboids exist, despite many efforts to prove it impossible and many efforts to find an example of one.

4.2. **A Tetrahedron of Right Triangles.** Consider the following system of equations:

$$\begin{aligned} n_1^2 + c^2 &= b^2 \\ n_2^2 + b^2 &= a^2 \\ n_3^3 + c^2 &= a^2. \end{aligned} \tag{4.4}$$

These three equations actually describe the edges of a tetrahedron where three of the faces are right triangles. Moreover, with a little algebra, we see that

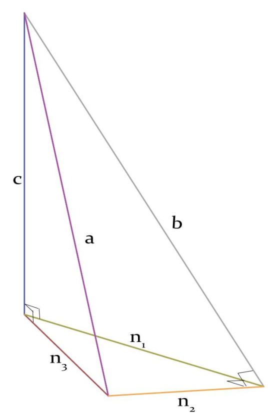
$$n_1^2 + n_2^2 = n_3^2,$$

meaning that the fourth face of the tetrahedron is a right triangle as well. Figure 7 shows how this tetrahedron might look.

The question is whether or not it is possible to have a tetrahedron like this with integer sides. In a paper [E753], Euler proved that this is indeed possible.

Euler, however, was pursuing a different question. He was looking for three integers a, b and c where all three sums and all three differences are squares. However, a solution to this problem also gives us a solution to our tetrahedron problem.

FIGURE 7. Pictorial Example of System 4.4



Suppose we have three integers a, b and c such that

$$\begin{array}{ccc} a+b, & & a-b, \\ a+c, & & a-c, \\ b+c, & \text{and} & b-c \end{array}$$

are all squares. Then,

$$(b+c)(b-c) = b^2 - c^2 = n_1^2$$
$$(a+b)(a-b) = a^2 - b^2 = n_2^2$$
$$(a+c)(a-c) = a^2 - c^2 = n_3^2$$

is a solution to System 4.4, since the product of two squares is a square.

We will not go through the solution that Euler gives for this problem. The interested reader can read *How Euler Did It* by Ed Sandifer[5] for a complete explanation of Euler's solution. The result is stated below.

Theorem 4.3. *Given positive integers f and g,*

$$\begin{aligned}
a = & \quad (4f^2g^2((f^4+2f^2g^2+9g^4)+(f^4-2f^2g^2+9g^4)))^2 \\
& \cdot(16f^4g^4-(f^4-2f^2g^2+9g^4)(f^4+2f^2g^2+9g^4))^2 \\
b = & \quad 2(4f^2g^2((f^4+2f^2g^2+9g^4)+(f^4-2f^2g^2+9g^4))) \\
& \cdot(16f^4g^4-(f^4-2f^2g^2+9g^4)(f^4+2f^2g^2+9g^4)) \\
c = & \quad 2(4f^2g^2((f^4+2f^2g^2+9g^4)-(f^4-2f^2g^2+9g^4))) \\
& \cdot(16f^4g^4-(f^4-2f^2g^2+9g^4)(f^4+2f^2g^2+9g^4))
\end{aligned}$$

is a solution to System 4.4.

Proof. The proof is just a matter of calculation. We can factor all the sums and differences to see that they are all indeed squares. That is,

$$\begin{aligned}
a+b = & \quad (f-g)^2(f-3g)^2(f+3g)^2(f+g)^2(f^2+2fg+3g^2)^2(f^2-2fg+3g^2)^2, \\
a-b = & \quad (f^2+9g^2)^2(f^2+g^2)^2(f^4-2f^2g^2+9g^4)^2, \\
a+c = & \quad (f^4+2f^3g+2f^2g^2-6fg^3+9g^4)^2(f^4-2f^3g+2f^2g^2+6fg^3+9g^4)^2, \\
a-c = & \quad (f^4-2f^2g^2+9g^2)^2(f^2+2fg+3g^2)^2(f^2-2fg+3g^2)^2, \\
b+c = & \quad 16f^2g^2(f^2-3g^2)^2(f^2+2fg+3g^2)^2(f^2-2fg+3g^2)^2, \text{ and} \\
b-c = & \quad 16f^2g^2(f^2+3g^2)^2(f^4-2f^2g^2+9g^4)^2.
\end{aligned}$$

□

Example: Consider the following example. Let $f = 2$ and $g = 1$. It follows from Theorem 4.3 that

$$a = 733,025, \; b = 488,000 \text{ and } c = 418,304.$$

Here we see that:

$$a+b = 1105^2, \; a-b = 495^2,$$

$$a+c=1073^2,\ a-c=561^2,$$

$$b+c=952^2,\ b-c=264^2.$$

We then use these values to solve for n_1, n_2 and n_3 in our original equation:

$$n_1^2=(b+c)(b-c)=63,165,763,584=251,328^2,$$

$$n_2^2=(a+b)(a-b)=299,181,650,625=546,975^2,\ \text{and}$$

$$n_3^2=(a+c)(a-c)=362,347,414,209=601,953^2.$$

In Euler's solution, due to the complexity of the problem, he makes assumptions that simplify the problem. Thus, it is not at all clear whether Theorem 4.3 will produce every solution to System 4.4. Moreover, many solutions generated by Theorem 4.3 are trivial. For example, if $f=g$ or $f=3g$, then $a+b=0$, meaning that $n_2=0$, from which it follows that $b=a$ and $n_1=n_3$.

Theorem 4.4. *Suppose that a, b, c, n_1, n_2 and n_3 is a solution set to System 4.4. Then*

$$A=a^2+b^2-c^2,\ B=a^2+c^2-b^2,\ \textit{and}\ C=|b^2+c^2-a^2|$$

and

$$N_1=2cn_2,\ N_2=2an_1,\ \textit{and}\ N_3=2bn_3$$

is also a solution set.

Proof. We need to prove that A^2-B^2, A^2-C^2 and B^2-C^2 are all squares. To see that A^2-B^2 is square, note that

$$A-B=2(b^2-c^2)=2n_1^2,$$

and

$$A+B=2a^2.$$

Thus,

$$A^2-B^2=(A+B)(A-B)=2^2a^2n_1^2=N_2^2.$$

In a similar fashion, we see that

$$A^2 - C^2 = 2^2 b^2 n_3^2 = N_3^2 \text{ and}$$

$$B^2 - C^2 = 2^2 c^2 n_2^2 = N_1^2.$$

This completes the proof. □

Example: From the example above, we know that $a = 733,025$, $b = 488,000$, $c = 418,304$, $n_1 = 251,328$, $n_2 = 546,975$ and $n_3 = 601,953$ is a solution set to System 4.4. By Theorem 4.4,

$$\begin{aligned}
A &= 733,025^2 + 488,000^2 - 418,304^2 &&= 600,491,414,209,\\
B &= 733,025^2 + 418,304^2 - 488,000^2 &&= 474,159,887,041,\\
C &= |488,000^2 + 418,304^2 - 733,025^2| &&= 124,203,414,209,\\
N_1 &= 2 \cdot 418,304 \cdot 546,975 &&= 457,603,660,800,\\
N_2 &= 2 \cdot 733,025 \cdot 251,328 &&= 368,459,414,400, \text{ and}\\
N_3 &= 2 \cdot 488,000 \cdot 601,953 &&= 587,506,128,000
\end{aligned}$$

is also a solution set. The calculations can be verified.

5. Conclusion

Theorems 4.3 and 4.4 give us some solutions to our original problem, but perhaps not all solutions. As was mentioned, Euler made many simplifications before coming up with his solutions to System 4.4, and therefore potentially threw out many solutions. However, we have shown that there are, at least, some solutions to the problem we set out to solve.

Other questions remain unanswered. It is still unknown whether there are any Perfect Cuboids. The solutions to both the Euler Brick and System 4.4 could potentially be classified in much more elegant terms. We leave these, as well as many other questions, for others to pursue.

References

[1] Conrad, Keith: *Pythagorean Triples*

http://www.math.uconn.edu/~kconrad/blurbs/ugradnumthy/pythagtriple.pdf

[2] Silverman, Joseph H.: *A Friendly Introduction to Number Theory.*

New Jersey: Prentice Hall, 1997.

[3] Sally, Judith D.; Sally Jr., Paul J: *Roots To Research.*

Providence, RI: American Mathematical Society, 2007.

[4] "Euler Brick – from Wolfram MathWorld." Wolfram MathWorld.

Web. 14 May 2010.

http://mathworld.wolfram.com/EulerBrick.html.

[5] Sandifer, Ed: *How Euler Did It.*

MAA Online. Web. 2009.