Introduction to Pythagorean Triples

No doubt you already know about the Pythagorean Theorem: the sides of any right-angled triangle in flat, or Euclidean, space satisfy the relationship

$$a^2 + b^2 = c^2 \tag{1}$$

or, in more traditional terms, the square of the hypotenuse is equal to the sum of the squares of the other two sides. But have you heard of Pythagorean Triples?

A Pythagorean Triple is a set of three integers (or whole numbers) (a, b, c) which satisfy the basic Pythagorean equation:

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

Famous examples of Pythagorean Triples include $(3, 4, 5)$ and $(5, 12, 13)$:

$$\begin{aligned} 3^2 + 4^2 = 9 + 16 &= 25 = 5^2 \\ 5^2 + 12^2 = 25 + 144 &= 169 = 13^2 \end{aligned} \tag{3}$$

A Pythagorean Triple (a, b, c) is said to be *primitive* if the three integers a, b, c do not share a common divisor. Thus $(3, 4, 5)$ is a primitive Pythagorean Triple, while $(6, 8, 10)$ and $(15, 20, 25)$ are not primitive, although they are Pythagorean Triples.

The next question is obvious – how can we find all the primitive Pythagorean Triples? The traditional approach to this problem proceeds by brute force. First, we observe that in any primitive Pythagorean Triple (a, b, c), c must be an odd number, and one of (a, b) must be odd, while the other must be even.

The proof of this assertion is a bit tricky, but basically straightforward. First, let us assume that both a and b are even. But if a is even, then a^2 is also even, and if b is even, then b^2 is also even. The sum of two even numbers is always an even number, so c^2 must be even, since $a^2 + b^2 = c^2$. But c^2 is an even number if and only if c is an even number (the square of every even number is even, and the square of every odd number is odd). Therefore, if a and b are even and $a^2 + b^2 = c^2$, c is also even, and the triplet (a, b, c) cannot be primitive, for each element of the triplet is divisible by two.

What about the case where both a and b are odd numbers? Well, this can't work because the sum of two odd perfect squares can never be a perfect square. To see why, we have to do a little algebra. So let's assume that a and b are odd integers, and that $a^2 + b^2 = c^2$. Now in this case c must be an even number, since the sum of two odd numbers is always even, and we've just shown that if c^2 is even, c must also be even. Let us make a substitution of variables: since a is an odd number, there must be some integer t such that $a = 2t + 1$. Similarly, we may write $b = 2u + 1$, and, since c is even, $c = 2v$. Now

$$\begin{aligned} a^2 + b^2 &= c^2 && ==> \\ (2t+1)^2 + (2u+1)^2 &= (2v)^2 && ==> \\ (4t^2+4t+1) + (4u^2+4u+1) &= 4v^2 && ==> \\ 4(t^2+t+u^2+u) + 2 &= 4v^2 \end{aligned}$$

But this last equation cannot possibly be true, since the right side is obviously divisible by 4, while the left side apparently leaves a remainder of 2 when divided by 4. Since that is impossible if the two sides are in fact equal, we conclude by the principle of *reductio ad absurdum* that if $a^2 + b^2 = c^2$, a and b cannot both be odd integers. So we've seen that a and b can't both be even, and that they can't both be odd, either. The only remaining alternative is that one of (a, b) is even, and the other is odd. That is what we set out to prove. *qed*

With that preliminary result under our belts, let's proceed to do some more algebraic reasoning with our basic equation. Since one of (a, b) must be an odd integer, we can specify which one is odd – for the sake of argument, let us say that a is the odd integer. Our basic relationship is

$$a^2 + b^2 = c^2 \tag{4}$$

or, subtracting $b^2 = b^2$:

$$a^2 = c^2 - b^2 \tag{5}$$

and then factoring:

$$a^2 = (c+b) * (c-b) \tag{6}$$

But now we appeal to the fact that $c+b$ and $c-b$ must both be integers, and to the fact that there are a limited number of ways to separate a^2 into distinct factors to complete our characterization of all primitive Pythagorean Triples. Let us perform another substitution of variables: set $u = c+b$ and set $v = c-b$. Adding these two equations we see that $u+v = 2c$ or $c = \frac{u+v}{2}$, and subtracting the second expression from the first we obtain $u-v = 2b$ or $b = \frac{u-v}{2}$.

And now the traditional characterization of all primitive Pythagorean Triples is complete. Let a be any odd number. Form the integer a^2 and examine the several ways in which a^2 can be separated into factors. For each pair of factors $u * v = a^2$ (where $u > v$), calculate $b = \frac{u-v}{2}$ and $c = \frac{u+v}{2}$.

If there is no divisor common to (a, b, c), this triplet is a unique primitive Pythagorean Triple. By setting a equal in turn to each of the odd integers $1, 3, 5, 7, 9, \ldots$ it is in principle possible to enumerate all the infinitely many primitive Pythagorean Triples!

Before we give this up entirely, let's work through a few elementary examples to see how it works. If $a = 1, a^2 = 1$, and no solution is possible, since 1 cannot be separated into two integral factors (u, v) such that $u > v$. In fact, substituting $1 = 1*1$ in the above equations we get $a = 1, b = 0, c = 1$; and while it is true that $1^2 + 0^2 = 1^2$ this doesn't exactly define a triangle, since one "side" is of length zero.

What if we set $a = 3$? Well, $3^2 = 9$, and $1 * 9 = 3 * 3 = 9$. Substituting the first of these factorizations into our equations we find that $a = 3, b = 4$, and $c = 5$; this is of course the most famous primitive Pythagorean Triple of them all. (The second factorization is another degenerate case, $3^2 + 0^2 = 3^2$.)

I'll let you work out $a = 5$ and $a = 7$ for yourself – since both 5 and 7 are prime numbers, you'll find just one unique primitive Pythagorean Triple in each of these cases. In fact, for each odd prime integer a there is one and only one primitive Pythagorean Triple which pops out of our procedure. Can you see why? Can you visualize what they look like? (To me, they start out short and squat, but rapidly get taller and skinnier as a takes on the successive values $5, 7, 11, 13, 17, 19, 23, ...$ Does that make sense?)

The picture gets much more interesting when a is an odd composite integer, for then it is possible to factor a^2 in a larger number of ways. The case a = 9 doesn't do much for us since 9 is itself a perfect square – all we get is $(9, 40, 41)$. But look what happens when $a = 15$:

$$15^2 = 225 = 1 * 225 = 3 * 75 = 5 * 45 = 9 * 25 \tag{7}$$

Now $225 = 1 * 225$ yields $(15, 112, 113)$, much like the tall skinny triangles we get out of odd prime numbers a. And neither $225 = 3 * 75$ nor $5 * 45$ will give us a new primitive Pythagorean Triple, because we end up with triplets which share common factors and which, consequently, can be reduced to other cases we have already encountered. But $225 = 9 * 25$ does give us something new: $a = 15, b = \frac{25-9}{2} = 8$, and $c = \frac{25+9}{2} = 17$, or $(8, 15, 17)$ – this is in fact a different looking critter, closer to the $(3, 4, 5)$ shape we started with!

OK, one more, and then I've got to go cook supper. The next interesting wrinkle arises when a is an odd number with three (instead of two) prime factors. The smallest such a is 105:

$$105^2 = 11,025 = 1 * 11,025 = 9 * 1,225 = 25 * 441 = 49 * 225 \tag{8}$$

(I've omitted the factorizations of 11,025 which lead to nothing new.)

This gives us four distinct primitive Triples containing the number 105: (105, 5512, 5513); (105, 608, 617); (105, 208, 233); and (88, 105, 137).

I hope this little homily has helped you gain some insight into Primitive Pythagorean Triples, and why I think they're so much fun. There are a lot of interesting questions about PPTs for the amateur mathematician to explore. For instance, can we find an isosceles PPT? (No, because one of a, b must be odd, and the other even.) Can we find "almost isosceles" PPTs, in which $b = a + 1$? (Yes, we can. The smallest such is (20, 21, 29). Can you find another one?) How about a PPT for which $b = 2 * a + 1$? (I'll let you find some of those without my help.) Enjoy!