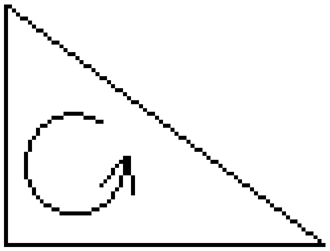
More (a, b, c)'s of Pythagorean triples

Darryl McCullough

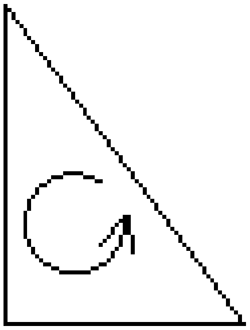
University of Oklahoma

March 3, 2003

A *Pythagorean triple* (PT) is an ordered triple (a, b, c) of positive integers such that $a^2 + b^2 = c^2$.



(3,4,5)



(4,3,5)

When a and b are relatively prime, the triple is called a *primitive* PT (PPT). Each PT is a positive integer multiple of a uniquely determined PPT.

Starting, for example, from $(8, 15, 17)$, we obtain the following nonprimitive PT's:

$$(16, 30, 34), (24, 45, 51), (32, 60, 68), \ldots$$

There is a method for generating all PPT's, which dates to antiquity (it is sometimes credited to Euclid). You can find a proof in almost any book on elementary number theory, and you can find proofs or discussions of the method on hundreds of websites of amateur mathematicians.

Take a pair of relatively prime positive integers (m, n) with $m > n$. Put:

1. $T(m, n) = (m^2 - n^2, 2mn, m^2 + n^2)$ if one of m or n is even.

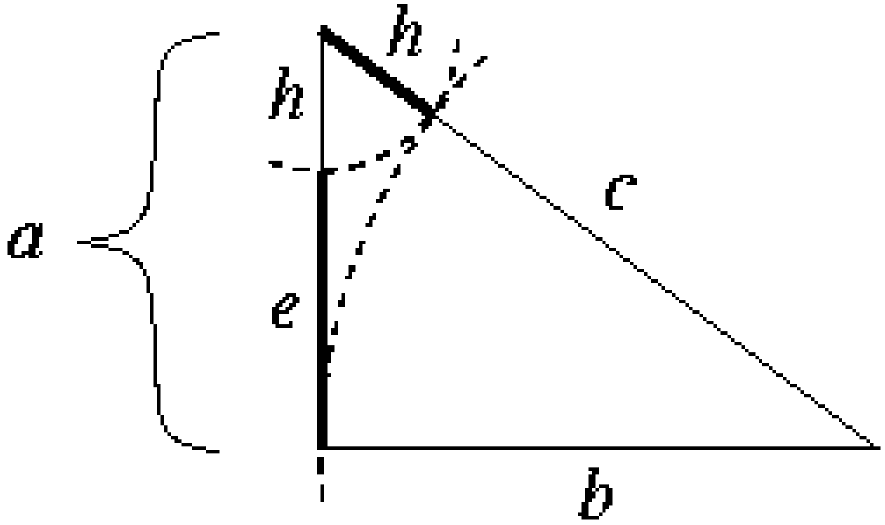
2. $T(m, n) = \left(\frac{m^2-n^2}{2}, mn, \frac{m^2+n^2}{2}\right)$ if both of m and n are odd.

For example, $T(2, 1) = (3, 4, 5)$ and $T(3, 1) = (4, 3, 5)$. This gives each PPT once, and taking all their multiples gives all the PT's.

To me, these parameters do not seem very natural. There is a different enumeration of PT's based on two very natural parameters called the *height* and the *excess.*

The *height* of (a, b, c) is $h = c - b$.

The *excess* of (a, b, c) is $e = a + b - c$.



This name "excess" is used for e, because e is the extra distance that you must travel if you go along the two legs of the triangle, instead of along the hypotenuse.

Not all combinations of h and e can occur in an integer-sided triangle. For a given h, the possible values of e are *exactly the integer multiples of a certain integer d.*

The integer d is called the *increment,* and it is related to h in a simple way: d is the smallest positive integer whose square is divisible by $2h$.

Since e is a multiple of d, we can write $e = kd$ for a positive integer k. Associating k and h to (a, b, c) sets up a one-to-one correspondence of the PT's with the pairs of positive integers (k, h).

For example, everybody's favorite PT $(3, 4, 5)$ corresponds to the pair $(1, 1)$, and $(4, 3, 5)$ and $(5, 12, 13)$ correspond to $(1, 2)$ and $(2, 1)$ respectively. The non-primitive PT's $(48, 189, 195)$ and $(459, 1260, 1341)$ correspond to $(7, 6)$ and $(21, 81)$.

Here is a computational description of the increment d.

Write $h = pq^2$ where q is as large as possible (that is, so that p is not divisible by the square of any prime).

Define $d = \begin{cases} pq & \text{if } p \text{ is even} \\ 2pq & \text{if } p \text{ is odd.} \end{cases}$

Lemma 1 *The numbers* $\{d, 2d, 3d, \ldots\}$ *are exactly the positive integers whose squares are divisible by* $2h$.

The proof uses nothing more than the unique factorization of positive integers into primes. You can prove it yourself, or read a proof on my website.

Theorem 2 (The height-excess enumeration) *As one takes all pairs (k, h) of positive integers, the formula*

$$P(k,h) = \left(h + dk, dk + \frac{(dk)^2}{2h}, h + dk + \frac{(dk)^2}{2h}\right)$$

produces each Pythagorean triple exactly once.

Notice that h is the height of $P(k, h)$, and dk is the excess.

Stated as a recipe, the enumeration is this:

To find (k, h) from (a, b, c)

1. Put $h = c - b$.
2. Write $h = pq^2$ with q square-free and positive.
3. Put $d = 2pq$ if p is odd, and $d = pq$ if p is even.
4. Put $k = (a - h)/d$.

The proof of the height-excess enumeration theorem is just Lemma 1 + college algebra.

First, we need to know that $P(k,h)$ is a PT. By Lemma 1, $\frac{d^2}{2h}$ is an integer, so the coordinates of $P(k,h)$ are integers. The fact that $P(k,h)$ satisfies the Pythagorean relation $a^2+b^2=c^2$ is just college algebra.

Second, we need to know that every PT is $P(k,h)$ for a unique pair (k,h). College algebra shows that for any PT,

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

The Pythagorean relation implies that $e^2 = 2(c-a)(c-b) = 2h\,(c-a)$, so $2h|e^2$. By lemma 1, e can be written as dk for some k. So $(a,b,c) = P(k,h)$ for that pair (k,h).

The uniqueness of (k,h) is just the fact that the recipe exists: (a,b,c) determines $h=c-b$ and $e=a+b-c$, h determines d, and e and d determine k since $e=dk$.

As far as I can determine, the first version of this enumeration for PTs appears in a paper of M. G. Teigan and D. W. Hadwin in the *American Math. Monthly* in 1971. It appears several more times in the literature, although none of its discoverers seems to have recognized the usefulness of the height and excess.

The term "height" seems to appear first in a paper written by the father-and-son combination of P. W. Wade and W. R. Wade. They found the number d, developed a recursion formula that produces all PTs of height h, and used the classical enumeration to give a full verification that the recursion produces all PTs in the cases $h = q^2$ and $h = 2q^2$. In a paper that I wrote with an OU undergraduate Elizabeth Wade (who is no relation to P. W. Wade and W. R. Wade), we used the height-excess enumeration for PTs to give a quick verification of the Wade-Wade recursion for all positive h. In fact, their recursion just gives $P(k+1, h)$ in terms of $P(k, h)$.

I have written another paper, “Height and Excess of Pythagorean Triples,” which gives many other uses of height and excess. Most of these are simpler proofs of known theorems about PT’s, but some are new results. Today, I will talk about one of these applications.

One kind of structure we could seek on the set of PT’s is algebraic structure. Can we put an operation on the set of PT’s that makes it into a group? Of course, there are many meaningless “junk” ways to do this— just take a bijection from the set of PT’s to any countable group, and use it to define the operation. But we want operations that have geometric meaning. A few such operations have been found on the set of PT’s.

In a 1996 paper in the *College Math. J.*, Beauregard and Suryanarayan examined an operation on a set of "generalized" PT's (i. e. a, b, or c can be 0 or negative), defined by

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) =$$
$$(a_1 a_2, b_1 c_2 + b_2 c_1, b_1 b_2 + c_1 c_2)$$

This is geometrically meaningful, because it is multiplicative for a.

The $*$-operation has an identity element, $(1, 0, 1)$, so it makes the set of PT's into a monoid. But it does not produce a group structure— no element except $(1, 0, 1)$ has an inverse. Also, a $*$-product of primitive elements need not be primitive. For example,

$$(4, 3, 5) * (4, 3, 5) = (16, 30, 34) = 2\,(8, 15, 17)$$

There is a way to improve this situation, using a common mathematical device— the same device used to obtain the rational numbers from the fractions.

Declare two nonzero GPT's to be *equivalent* when they are positive multiples of the same primitive PT. Each equivalence class consists of one primitive PT, plus all its multiples.

Putting this equivalence relation on a set is called *projectivization.*

The $*$-operation produces an operation on the equivalence classes, which then form a group. The inverse of (a, b, c) is $(a, -b, c)$, since

$$(a, b, c) * (a, -b, c) = (aa, bc + c(-b), b(-b) + cc)$$
$$= (a^2, 0, c^2 - b^2) = (a^2, 0, a^2) \sim (1, 0, 1)$$

By very clever arguments using the classical enumeration, Beauregard and Suryanarayan proved that the group that results from the GPT's of the form (a, b, c) with $a > 0$ and $c > 0$ is isomorphic to the group of positive rational numbers $\mathbb{Q}_{>0}$.

This result and many more about the $*$-operation can be understood much more easily, however, if one uses h as one of the coordinates.

A simple calculation just using the Pythagorean relation, together with the fact that $h = c - b$, shows that

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

By the height-excess enumeration theorem, a *and* h *determine a GPT exactly when* a *is of the form* $a = h + kd$*.* We denote this GPT by $[a, h]$, and call these the ah-*coordinates* of the GPT.

Some examples of GPT's in ah-coordinates are:

1. $[3, 1] = (3, 4, 5)$, $[4, 2] = (4, 3, 5)$, while $[2, 1]$ does not represent a GPT.

2. $[1, 1] = (1, 0, 1)$, $[3, 1] = (3, 4, 5)$,
   $[5, 1] = (5, 12, 13)$, $[7, 1] = (7, 24, 25)$,
   $[9, 1] = (9, 40, 41)$, in general for q odd
   $[q, 1] = \left(q, \frac{q^2 - 1}{2}, \frac{q^2 + 1}{2}\right)$.

3. $[3, 9] = (3, -4, 5)$, $[5, 25] = (5, -12, 13)$,
   in general for q odd
   $[q, q^2] = \left(q, \frac{1 - q^2}{2}, \frac{q^2 + 1}{2}\right)$.

4. For $s > 1$,
   $[2^s, 2] = (2^s, 2^{2s-2} - 1, 2^{2s-2} + 1)$.
   $[4, 2] = (4, 3, 5)$, $[8, 2] = (8, 15, 17)$,
   $[16, 2] = (16, 31, 33)$, $[32, 2] = (32, 63, 65)$.

5. For $s > 1$,
   $[2^s, 2^{2s-1}] = (2^s, 1 - 2^{2s-2}, 2^{2s-2} + 1)$,
   $[4, 8] = (4, -3, 5)$, etc.

The $*$-operation

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) =$$
$$(a_1 a_2, b_1 c_2 + b_2 c_1, b_1 b_2 + c_1 c_2)$$

becomes extremely simple in $[a, h]$ coordinates.

The height of $(a_1, b_1, c_1) * (a_2, b_2, c_2)$ is

$$b_1 b_2 + c_1 c_2 - (b_1 c_2 + b_2 c_1) =$$
$$(b_1 - c_1)\,(b_2 - c_2) = (-h_1)(-h_2) = h_1 h_2 \ ,$$

so in ah-coordinates, it is:

$$[a_1, h_1] * [a_2, h_2] = [a_1 a_2, h_1 h_2] \ .$$

What are the projective equivalence classes written in ah-coordinates? Notice that

$$n[a,h] = n[a,c-b] = n(a,b,c) =$$
$$(na,nb,nc) = [na,nc-nb] = [na,nh]\ .$$

(You have to be careful, though, because this formula only makes sense when $[a,h]$ is defined. For example, $[4,2] = (4,3,5)$, while $[2,1]$ is undefined.)

Since $n[a,h] = [na,nh]$, equivalence classes in ah-coordinates just look like:

$$\{[a,h],[2a,2h],[3a,3h],\ldots,[na,nh],\ldots\}\ .$$

where $[a,h]$ is a primitive GPT.

Now we are set up to state and prove the result of Beauregard and Suryanarayan.

Let $\mathcal{G}$ be the projective equivalence classes of GPT's of the form $[a, h]$ with $a > 0$ and $h > 0$. These are the (a, b, c) with $a > 0$ and $c > 0$.

Theorem 3 *Define* ϕ: $(\mathcal{G}, *) \to (\mathbb{Q}_{>0}, \cdot)$ *by sending* $[a, h]$ *to* a/h. *Then* ϕ *is an isomorphism.*

Proof: Since $\phi([na, nh]) = \frac{na}{nh} = \frac{a}{h} = \phi([a, h])$, ϕ is a well-defined injection.

To check that ϕ is a homomorphism:

$$\phi([a_1, h_1]) \cdot \phi([a_2, h_2]) = \frac{a_1}{h_1} \cdot \frac{a_2}{h_2} = \frac{a_1 a_2}{h_1 h_2}$$
$$= \phi([a_1 a_2, h_1 h_2]) = \phi([a_1, h_1] * [a_2, h_2]) \ .$$

$\phi([4, 2]) = 2$, $\phi([4, 8]) = 1/2$, and for q an odd prime, $\phi([q, 1]) = q$ and $\phi([q, q^2]) = 1/q$. The primes and their reciprocals generate $\mathbb{Q}_{>0}$, so ϕ is surjective.

I also used ah-coordinates to analyze the $*$-operation at the unprojectived level, where the operation only gives a monoid structure. This monoid has unique factorization. This was already proven by Beauregard and Suryanarayan. But working with (a,b,c)-coordinates, they did not notice that the monoid breaks into a direct sum of semigroups $\oplus\mathcal{A}_p$, one for each prime. At odd primes, the summand $\mathcal{A}_p$ is generated by the three triples $[p,1]$, $[p,p]$, and $[p,p^2]$. But $\mathcal{A}_2$ is much more complicated. It is not finitely generated, but its structure can be described very precisely. Also, I was able to determine exactly which PT's factor into a product of primitives. Roughly speaking, for odd p about half the PT's in $\mathcal{A}_p$ are products of primitives, but all but 10 of the PT's in $\mathcal{A}_2$ are products of primitives. All of this structure becomes visible when we view the situation in ah-coordinates.

Moral: Always look for the best coordinates.