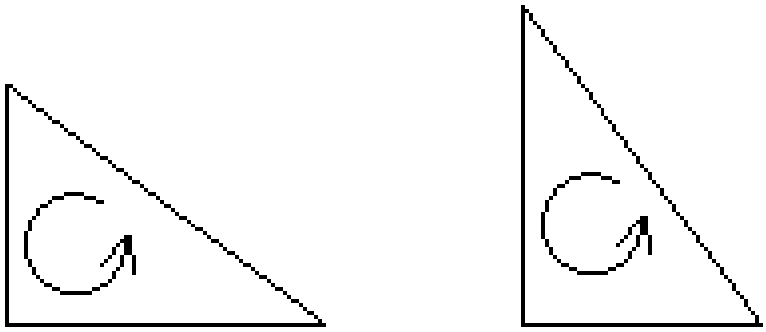
The (a, b, c)'s of Pythagorean triples

Darryl McCullough

University of Oklahoma

September 10, 2001

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



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 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.

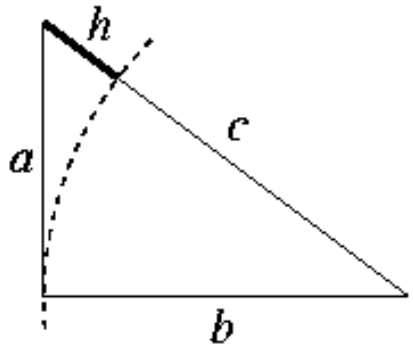
Take a pair of relatively prime positive integers (m, n) with $m > n$. Put:

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.

Recently, a paper of P. Wade and W. Wade in the *College Math. J.* gave another method for generating PT's.

Define the *height* of (a, b, c) to be $h = c - b$.



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

d is called the *increment.*

Start with $(a_0, b_0) = (h, 0)$. Recursively, define

$$(a_{k+1}, b_{k+1}) = \left(a_k + d\,,\ \frac{d}{h}\, a_k + b_k + \frac{d^2}{2h} \right) \ .$$

Then, the $(a_k, b_k, b_k + h)$ with $k \geq 1$ are a list of *all* the PT's of height h. (PPT's can only occur when $p = 1$ or $p = 2$, that is, when h is of the form q^2 or $2q^2$.)

For example, if $h = 72 = 2^3 \cdot 3^2 = 2 \cdot 6^2$, we have $p = 2$ and $q = 6$, so $d = pq = 12$. This gives

$$\frac{d}{h} = \frac{1}{6} \quad \text{and} \quad \frac{d^2}{2h} = 1 \ ,$$

and the recursion is

$$(a_{k+1}, b_{k+1}) = \left(a_k + 12 \, , \, \tfrac{1}{6}\, a_k + b_k + 1\right) \ .$$

Starting from $(72, 0)$, we obtain:

$$
\begin{array}{rcl}
(72, 0, 72) & & \\
\downarrow & & \\
(\mathbf{84}, \mathbf{13}, \mathbf{85}) & & \\
\downarrow & & \\
(96, 28, 100) & = & 4\,(\mathbf{24}, \mathbf{7}, \mathbf{25}) \\
\downarrow & & \\
(108, 45, 117) & = & 9\,(\mathbf{12}, \mathbf{5}, \mathbf{13}) \\
\downarrow & & \\
(120, 64, 136) & = & 8\,(\mathbf{15}, \mathbf{8}, \mathbf{17}) \\
\downarrow & & \\
(\mathbf{132}, \mathbf{85}, \mathbf{157}) & & \\
\downarrow & & \\
(144, 108, 180) & = & 36\,(\mathbf{4}, \mathbf{3}, \mathbf{5}) \\
\downarrow & & \\
(\mathbf{156}, \mathbf{133}, \mathbf{205}) & & \\
\downarrow & & \\
(168, 160, 232) & = & 8\,(\mathbf{21}, \mathbf{20}, \mathbf{29}) \\
\downarrow & & \\
(180, 189, 261) & = & 9\,(\mathbf{20}, \mathbf{21}, \mathbf{29}) \\
\downarrow & & \\
\ldots & &
\end{array}
$$

(the PPT's are in **boldface**)

The proof that P. Wade and W. Wade gave for their recursion formula is a complicated application of the classical enumeration method. Actually, they only gave a complete proof for the cases when h is of the form q^2 or $2q^2$.

Last spring, my undergraduate capstone student Elizabeth Wade and I found a much simpler proof that works for all choices of h. We wrote it up as a paper, "Recursive Enumeration of Pythagorean Triples," which can be downloaded from my website.

Our proof uses a different enumeration of the PT's, which we call the *height-excess enumeration.* After we developed it, we searched for it in the mathematical literature, and were finally able to find it (disguised in much different forms) in two papers published in MAA journals during the 1970's. Also, in the late 1990's it was rediscovered by two other mathematicians, who published it in the *Southern Missouri J. Math. Sci.*

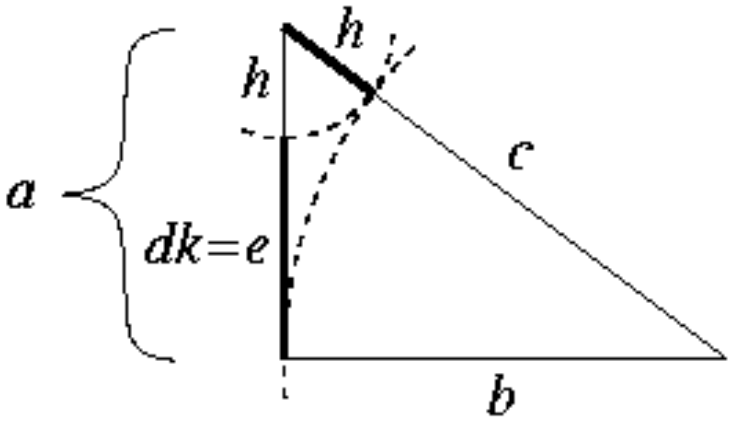
Theorem 1 (The height-excess enumeration) *As one takes all pairs (k, h) of positive integers, the formula*

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

produces each Pythagorean triple exactly once.

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

Also, notice that $dk = a + b - c$. The number $e = a + b - c$ is called the *excess* of the PT, because it is the extra distance you have to travel, if you go along the two legs of the triangle instead of along the hypotenuse.



Here is how the recursion formula follows from the height-excess enumeration theorem:

The theorem tells us that $P(1,h)$, $P(2,h),\ldots,$ are all the PT's of height h. Write (a_k,b_k,c_k) for $P(k,h)$, so that $(a_k,b_k)=\left(h+dk, dk+\frac{(dk)^2}{2h}\right)$. We compute that

$$\begin{aligned}
& (a_{k+1},b_{k+1}) \\
= & \left(h+d(k+1), d(k+1)+\frac{(d(k+1))^2}{2h}\right) \\
= & \left(h+dk+d, dk+d+\frac{(dk)^2}{2h}+dk\,\frac{d}{h}+\frac{d^2}{2h}\right) \\
= & \left(a_k+d, \frac{d}{h}(h+dk)+\left(dk+\frac{(dk)^2}{2h}\right)+\frac{d^2}{2h}\right) \\
= & \left(a_k+d, \frac{d}{h}a_k+b_k+\frac{d^2}{2h}\right) \ .
\end{aligned}$$

That is, the recursion formula just produces $P(k+1,h)$ from $P(k,h)$.

The height-excess enumeration theorem is not difficult to prove. First, we have a lemma that tells the key number-theoretic property of the increment d:

> The numbers $\{d, 2d, 3d, \dots\}$ are exactly the positive integers whose squares are divisible by $2h$.

Lemma 2 *Let h be a positive integer with associated increment d. Then $2h|d^2$. If D is any positive integer for which $2h|D^2$, then $d|D$.*

The proof uses nothing more than the unique factorization of positive integers into primes. You can prove it yourself, or read a proof in the E. Wade-McC paper.

Now for the proof of the height-excess enumeration theorem:

First, every $P(k,h)$ is a PT. Its coordinates are integers (since $\frac{d^2}{2h}$ is an integer), and the fact that it is Pythagorean is just checked by 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 2, e is divisible by d, that is, e can be written as dk for some k. So $(a,b,c) = P(k,h)$ for that pair (k,h).

The pair (k,h) is uniquely determined: (a,b,c) determines $h = c-b$ and $e = a+b-c$, h determines d, and e and d determine k since $e = dk$.

It turns out that the height-excess enumeration is good for a lot more than just proving the recursion formula. This seems not to have been realized by its previous discoverers. I have written a paper, "Height and Excess of Pythagorean Triples," which details many uses. Most of these are new and simpler proofs of known theorems about PT's, but some are new results.

For many of these applications, it is better not to restrict ourselves to triples with positive entries. A *generalized Pythagorean triple* (GPT) is an ordered triple (a, b, c) of integers such that $a^2 + b^2 = c^2$. If we take *all* (k, h)-pairs of integers, the height-excess enumeration formula produces each GPT exactly once:

Theorem 3 (The height-excess enumeration) *Let* $P(k,0) = (0,k,k)$*, and for* $h \neq 0$ *let*

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

Then P *is a bijection from* $\mathbb{Z} \times \mathbb{Z}$ *to the set of all GPT's.*

This gives us nice "coordinates" on the set of GPT's with $h \neq 0$. A simple calculation just using the fact that $h = c - b$ and the Pythagorean relation $a^2 + b^2 = c^2$ 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. $[1,1] = (1,0,1)$, $[1,-1] = (1,0,-1)$, $[-1,1] = (-1,0,1)$, and $[-1,-1] = (-1,0,-1)$.

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

3. $[q,1] = \left(q, \frac{q^2-1}{2}, \frac{q^2+1}{2}\right)$ with q odd.

   $[5,1] = (5,12,13)$, $[7,1] = (7,24,25)$, $[9,1] = (9,40,41)$.

4. $[q,q^2] = \left(q, \frac{1-q^2}{2}, \frac{q^2+1}{2}\right)$ with q odd.

   $[3,9] = (3,-4,5)$, $[5,25] = (5,-12,13)$.

5. $[2^s,2] = (2^s, 2^{2s-2}-1, 2^{2s-2}+1)$, $s > 1$.

   $[4,2] = (4,3,5)$, $[8,2] = (8,15,17)$, $[16,2] = (16,31,33)$, $[32,2] = (32,63,65)$.

6. $[2^s, 2^{2s-1}] = (2^s, 1-2^{2s-2}, 2^{2s-2}+1)$, $s > 1$. $[4,8] = (4,-3,5)$, etc.

In a 1996 paper in the *College Math. J.*, Beauregard and Suryanarayan examined an operation on the set of GPT's, defined by

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

By very clever arguments using the classical enumeration, they developed a number of properties of the $*$-operation. These properties (and more) can be developed much more easily, however, if one uses ah-coordinates. For 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, the operation is simply:

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

To illustrate the effectiveness of ah-coordinates, we will give a simple proof of one of the theorems of Beauregard and Suryanarayan.

First, we will have to set up the statement of the theorem.

The $*$-operation has an identity element, $[1,1]$. However, no elements except $[\pm 1, \pm 1]$ have inverses. Also, a $*$-product of primitive elements need not be primitive. For example,

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

There is a way to improve this situation, using a common mathematical device.

Declare two nonzero GPT's to be *equivalent* when they are positive multiples of the same primitive GPT.

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

Each equivalence class contains exactly one primitive element. The other elements are just the multiples of that element by positive integers. A typical equivalence class is

$$\{(3,4,5),(6,8,10),\ldots,(3n,4n,5n),\ldots\}\ .$$

What are the 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.

You can check that if you $*$-multiply equivalent GPT's, you obtain equivalent results. That is, the $*$-operation induces an operation on projective equivalence classes.

Since each equivalence class contains exactly one primitive, another way of saying this is that the $*$-operation induces an operation on primitives, where you multiply and then reduce the product, if necessary, as in:

$$(4,3,5) * (4,3,5) = [4,2] * [4,2] = \\ [16,4] \sim [8,2] = (8,15,17) \ .$$

After you projectivize, the $*$-operation becomes much more grouplike. For example,

$$(3,4,5) * (3,-4,5) = \\ [3,1] * [3,9] = [9,9] \sim [1,1]$$

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 4 *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.

To get a group from the Beauregard-Suryanarayan operation, we had to allow GPT's with $b < 0$. Is there a "natural" (that is, geometrically meaningful) operation on GPT's that gives a group structure just on the set of projectivized PT's? Yes, here is one:

$$(a_1, b_1, c_1)\,(a_2, b_2, c_2) =$$
$$(a_1a_2 + a_1b_2 + b_1a_2 + 2b_1b_2 - a_1c_2$$
$$-c_1a_2 - 2b_1c_2 - 2c_1b_2 + 2c_1c_2,$$
$$3a_1a_2 + a_1b_2 + b_1a_2 + b_1b_2 - 3a_1c_2$$
$$-3c_1a_2 - b_1c_2 - c_1b_2 + 3c_1c_2,$$
$$3a_1a_2 + a_1b_2 + b_1a_2 + 2b_1b_2 - 3a_1c_2$$
$$-3c_1a_2 - 2b_1c_2 - 2c_1b_2 + 4c_1c_2)$$

This operation may not look very natural, and it is not obvious, from this description, that it produces a group structure. Again, though, everything is much more transparent if we use better coordinates.

The eh-coordinates of a GPT are just $\langle e, h\rangle$, where e is the excess and h is the height. As with ah-coordinates, only certain pairs represent GPT's (those with $e = dk$). The $\langle e, h\rangle$ with $e > 0$ and $h > 0$ are exactly the PT's.

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

1. $\langle 2, 1\rangle = (3, 4, 5)$, $\langle 2, 2\rangle = (4, 3, 5)$,
   $\langle 2, -2\rangle = (0, 1, -1)$.

2. $\langle 2p, 1\rangle = (1 + 2p, 2p + 2p^2, 1 + 2p + 2p^2)$.
   $\langle 4, 1\rangle = (5, 12, 13)$, $\langle 6, 1\rangle = (7, 24, 25)$.

3. $\langle 2p, 2\rangle = (2 + 2p, 2p + p^2, 2 + 2p + p^2)$.
   $\langle 4, 2\rangle = (6, 8, 10)$, $\langle 6, 2\rangle = (8, 15, 17)$.

4. $\langle 2q, q^2\rangle = (q^2 + 2q, 2q + 2, q^2 + 2q + 2)$.
   $\langle 4, 4\rangle = (8, 6, 10)$, $\langle 6, 9\rangle = (15, 8, 17)$.

5. $\langle 2^s, 2^{2s-1}\rangle = (2^s + 2^{2s-1}, 1 + 2^s, 1 + 2^s + 2^{2s-1})$ with $s \geq 1$.
   $\langle 2, 2\rangle = (4, 3, 5)$, $\langle 4, 8\rangle = (12, 5, 13)$,
   $\langle 8, 32\rangle = (40, 9, 41)$.

You will not be surprised to learn that in eh-coordinates, the operation given above is simply

$$\langle e_1, h_1\rangle \langle e_2, h_2\rangle = \langle e_1 e_2, h_1 h_2\rangle \ .$$

This operation is poorly behaved at the level of GPT's. For example, there is no identity element, since e is always even. However, at the level of projective classes, $\langle 2, 2\rangle = (4, 3, 5)$ is an identity. And, the set of projectived PT's $\mathcal{PT}$ is a group:

Theorem 5 *The function $\psi\colon \mathcal{PT} \to \mathbb{Q}_{>0}$ that sends $\langle e, h\rangle$ to e/h is an isomorphism.*

The proof is essentially the same as for the $*$-operation.

Moral: Always look for the best coordinates.