Available at
http://pvamu.edu/aam
Appl. Appl. Math.
ISSN: 1932-9466

Applications and Applied
Mathematics:
An International Journal
(AAM)

Vol. 3, Issue 1 (June 2008), pp. 100 – 112
(Previously, Vol. 3, No. 1)

Rethinking Pythagorean Triples

William J. Spezeski
Department of Computer Science
Massachusetts College of Liberal Arts
375 Church Street, North Adams, MA 01247 USA
w.spezeski@mcla.edu

Received August 2, 2007; accepted February 5, 2008

Abstract

It has been known for some 2000 years how to generate Pythagorean Triples. While the classical formulas generate all of the primitive triples, they do not generate all of the triples. For example, the triple $(9, 12, 15)$ can't be generated from the formulas, but it can be produced by introducing a multiplier to the primitive triple (3, 4, 5). And while the classical formulas produce the triple (3, 4, 5), they don't produce the triple (4, 3, 5); a transposition is needed. This paper explores a new set of formulas that, in fact, do produce all of the triples i.e. every triple can be produced with a unique set of integer generators; there is no need for multipliers or transpositions. An unexpected result is an application to cryptology.

Keywords: Pythagorean Triple, primitive, hypotenuse-leg twin triple

AMS 2000 Subject Classification Numbers: 11-02, 11D09, 14G50

1. Introduction

The classical Pythagorean Triples have the form $\left(r^2 - s^2, 2rs, r^2 + s^2\right)$. Yet neither the triple $(9,12,15)$ nor the triple $(4,3,5)$ conform to that pattern. Why? This paper revisits the classically developed concept of Pythagorean Triples, comparing and contrasting the classical method of generating them with a newly developed approach that produces both $(9,12,15)$ and $(4,3,5)$ directly. Before looking at the new formulas, let's recall some of the basic properties of classical Pythagorean Triples; most texts on Number Theory will serve as a reference. Named after the Greek mathematician Pythagoras, these triples are defined as

Definition: Three positive integers (a, b, c) are called a Pythagorean Triple whenever $a^2 + b^2 = c^2$. A triple is said to **primitive** if $\gcd(a, b, c) = 1$.

The Classical Greek formula: $(r^2 - s^2, 2rs, r^2 + s^2)$ is a Pythagorean Triple whenever $0 < s < r$; $r, s \in Z^+$. The generating pair of integers in this case is denoted by $[r, s]$ so that $[r, s] = (r^2 - s^2, 2rs, r^2 + s^2)$. The triple is primitive iff $(r, s) = 1$ (are relatively prime) and $(r - s)$ is odd. While $(r, s) = 1$ is a necessary condition for producing primitives, we must also require that $(r - s)$ be odd. A case in point: if $r = 7$ and $s = 3$, then $(7, 3) = 1$ but the pair $[7, 3]$ produces the non-primitive triple $(40, 42, 58)$. We shall refer to the collection of triples generated by $[r, s]$ above as the **classical triples** or **classically generated triples**.

2. A Variant of the Classical Formula

Proposition 1: The classical Pythagorean Triples can be generated by the relationships

$$\begin{aligned}[p+q,\ q] &= \left((p+q)^2 - q^2 ,\, 2q(p+q), (p+q)^2 + q^2 \right) \\ &= (p^2 + 2pq, 2q^2 + 2pq, p^2 + 2q^2 + 2pq),\end{aligned} \tag{1}$$

where $p \,.\, q \in Z^+$.

The two systems of generating triples are completely equivalent in the sense that they produce exactly the same triples. Any triple that can be produced by one system can be produced by the other. Let's compare the two:

The $[r, s]$ System	**The $[p+q, q]$ System**
$r, s \in Z^+; 0 < s < r$ (forcing $r \geq 2$)	$p, q \in Z^+$; no other restrictions
For primitives	
$(r, s) = 1$ (relatively prime)	$(p, q) = 1$
$r - s$ is odd	p is odd
Can only generate finite subsets of triples for fixed value of r	Can generate infinite subsets of triples for each value of p

- As one might guess, there are some distinct advantages to using the variant $[p + q, q]$.

- This system helps to organize the triples into countable families or cosets indexed by the value of p:

$$\left(A_p(q), B_p(q), C_p(q)\right), \qquad p, q \in Z^+.$$

- When p = 1, we obtain the following sets of triples:

$$\left(2q+1, 2q(q+1), 2q(q+1)+1\right), \qquad q \in Z^+.$$

Every triple that is generated here is primitive. This subset is not exhaustive, but it demonstrates easily and clearly that the set of primitive triples is infinite. Since p must be odd in order to produce a primitive triple, the time searching for triples is halved because there is no need to consider the even values of p.

3. Families of Triples

For each $p \in Z^+$, we can define three continuous functions in the variable t as follows:

$$A_p(t) = 2pt + p^2, \qquad B_p(t) = 2t^2 + 2pt, \qquad C_p(t) = 2t^2 + 2pt + p^2 \tag{2}$$

These three functions are a variant of the three functions in (1) replacing q with the more commonly used parameter t.

For fixed values of p, $A_p(t)$ is a linear function in t while both $B_p(t)$ and $C_p(t)$ are quadratic functions in t. When graphed on the same axis for a fixed p value, we wind up with a display like the one in Figure 1. The following shows the relationship between the functions when $p = 3$: The p_3-Family $\left(A_3(t), B_3(t), C_3(t)\right)$.

For each integer value of t there coincides three integer values, one point from each curve, that yields a Pythagorean Triple. The graph also gives us a visual insight into why the first member of a triple is sometimes larger than its second member. For the initial values of t, $A_3(t) > B_3(t)$; at some point, however, $A_3(t) < B_3(t)$, for all subsequent values of t.

Despite its advantages, this variant system still has some of the limitations that the Classical Greek system has, and in particular, can not produce the triples $(9, 12, 15)$ or $(4, 3, 5)$ directly from its formulas. Tong (2003) has explored other aspects of this system.

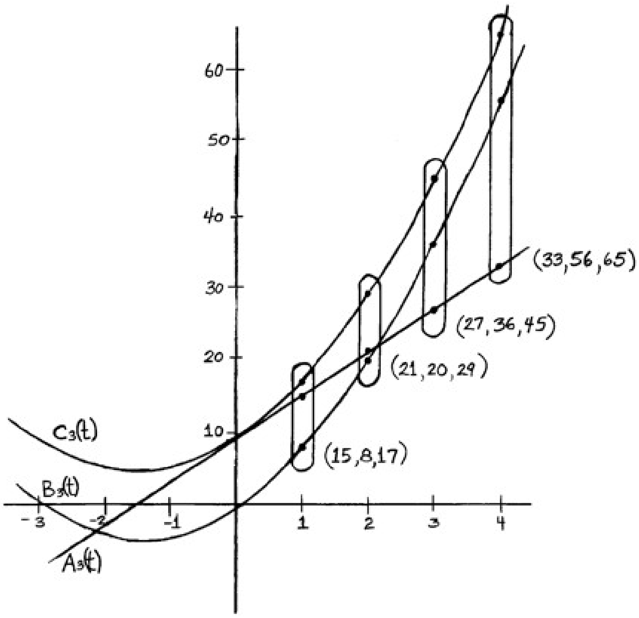

Figure 1.

4. Some Observations of the Classical System and its Variant

The formulas as stated above generate all of the primitive triples as well as many non-primitive ones. However, they do not generate all of the possible triples! This can be seen in the classical Greek system by considering the difference $c-b=(r-s)^2$; it must be a perfect square. Consequently, there are no integer values of r and s that will produce $(9,12,15)$; the difference $15-12=3$ is not a perfect square. To get around this in the classical literature, an integer multiplier $d>0$ is introduced so that

$$a=(r^2-s^2)d\,,\, b=2rsd, \qquad c=(r^2+s^2)d\,.$$

The same phenomenon exists in the variant $[p+q,q]$ system. The formulas will generate families of triples for each positive integer p, but in this case, $c-b=p^2$ so that the actual values of $c-b$ are $1^2, 2^2, 3^2$, etc. Looking at the families of triples that are generated from the point of view of the hypotenuse-side difference $c-b$,

$$c-b\in\{1,4,9,16,25,36,49,64,81,100,\ldots,p^2,\ldots\}\,.$$

There are no 'difference' families of triples for the integers $2,3,5,6,7,8,10,11,12,\ldots$. For example, there is no '$c-b=3$' family, and in particular, the triple $(9,12,15)$ cannot be generated by the variant system unless we resort to multipliers.

So, now an interesting question arises: is it possible to find formulas that will generate all of the families of triples without resorting to multipliers? The answer is – yes!

5. A New Approach to Generating Pythagorean Triples

The new approach to generating the triples (a, b, c) primarily concerns itself with the difference $(c-b)$. To this end, and making reference to a right triangle, let's make a formal

Definition: If (a, b, c) is a Pythagorean Triple, then $c-b$ is called its **hypotenuse-leg difference** and is denoted by K. Clearly $c-a$ is also a hypotenuse-leg difference which we will denote by $\widetilde{K}$.

Proposition 2: If (a, b, c) is a Pythagorean Triple with hypotenuse-leg difference K, then the triple can be expressed as

$$\left(a, \frac{a^2-K^2}{2K}, \frac{a^2-K^2}{2K}+K\right). \tag{3}$$

Proof:

$$\begin{aligned} a^2+b^2 &= c^2 \\ &= (b+K)^2 \\ &= b^2+2bK+K^2, \end{aligned}$$

so that $a^2 = 2bK + K^2$. Thus, we have $b = \dfrac{a^2-K^2}{2K}$ and $c = b + K$.

Conversely, given an expression (3) with integers $0 < K < a$, if $2K$ divides $(a^2 - K^2)$, then each term is an integer and (3) is a Pythagorean Triple. So, we will need to know precisely when this integer divisibility exists. To help us, we make the following

Definition: Let $K = D \cdot E^2 \cdot L$, where
$D = \{$ product of the distinct odd factors of K $\}$; each odd factor occurs exactly once,
$E^2 = \{$product of even powers of the remaining factors including 2$\}$ expressed as $[\ ]^2$; each factor has power $2N$ (N an integer, $N > 0$), and
$L = \{$ product of the factors still left $\}$; each factor occurs at most once.

Using this factorization of K, we define a new integer value $M = 2 \cdot D \cdot E$; M is called the **co-value** of K.

To illustrate the construction of M, consider the following:

$$\begin{aligned} K &= 648 = 2\cdot 2\cdot 2\cdot 3\cdot 3\cdot 3\cdot 3 \\ &= 3\cdot(2\cdot 3)^2\cdot 2\cdot 3 = D\cdot E^2\cdot L, \end{aligned}$$

where $D=3$, $E^2=(2\cdot 3)^2$ and $L=2\cdot 3$. Then, $M=2\cdot D\cdot E=2\cdot 3\cdot(2\cdot 3)=36$.

Note that several values of K can have the same value of M. For example, the hypotenuse-leg differences $12, 24, 36$ and 72 each have a co-value of 12. Also note that M is always an even integer. We can deduce that $\sqrt{2K}\le M\le 2K$.

Proposition 3: Let K and M be defined as above; then $2K$ divides M^2.

Proof:
Using the definition of M, we have

$$\frac{M^2}{2K}=\frac{4D^2E^2}{2DE^2L}=\frac{2D}{L}.$$

The term D contains all of the distinct odd factors of K while L contains at most all of the distinct odd factors of K and possibly the factor 2. Thus L divides $2D$ and $2K$ divides M^2.

For example, if $K=648$, then $M=36$ and $\frac{M^2}{2K}=\frac{36\cdot 36}{2\cdot 648}=1$;

if $K=3$, then $M=6$ and $\frac{M^2}{2K}=\frac{6\cdot 6}{2\cdot 3}=6$.

Even though the above result seems rather bland, it is actually quite important. In fact, all of the hard work is done. Now we can combine the ideas of Proposition 2, the definition of M and Proposition 3 to establish a new set of formulas for generating triples.

The question we have been trying to answer is: When does $2K$ divide (a^2-K^2)? The answer is: when $a=Mt+K$. If we make the substitution $a=Mt+K$ in (3), where t is a positive integer-valued parameter, we obtain

$$\left(Mt+K\,,\frac{M^2t^2+2KMt}{2K}\,,\frac{M^2t^2+2KMt}{2K}+K\right),\quad t=1,2,3,.... \tag{4}$$

Proposition 3 guarantees that $2K$ divides M^2, so each term is an integer and thus (4) is a Pythagorean Triple. Are the new generating formulas a little messy? Yes, but there are several ways to simplify. The expression (4) can be equivalently written as

$$\left(M\,t+K\,,\frac{(a+K)(a-K)}{2K}\,,b+K\right), \qquad t=1\,,2\,,3\,,....$$

The latter formula requires that the calculation be done algorithmically, calculating the first term, then the second, and finally the third. On the other hand, the ease of generating the triple is greatly improved.

So now we have a new way to generate a triple. Conversely, given any triple, its generators can be recovered easily by

$$K=c-b\,(=D\cdot E^2\cdot L)\,, \qquad M=2\cdot D\cdot E\,, \qquad t=\frac{a-K}{M}. \tag{5}$$

Each triple (independent of what system was used to produce it) has a unique generative set of integers $\{K\,,M\,,t\,\}$.

One advantage of this new approach is that there is no need for multipliers, greatest common divisors, or the repositioning terms to generate all of the triples. Each triple is uniquely generated. Notice the triple $(9,12,15)$ when classically generated is $3(3,4,5)$ In the $[K,M,t]$ system it is generated by $\{3,6,1\}$; there is no need for a multiplier. Moreover, $(12,9,15)$ is generated by $\{6,6,1\}$; there is no need for artificial transposition of the 9 and 12.

In order to discuss pairs of triples such as $(3,4,5)$ and $(4,3,5)$, we make the following

Definition: If (a,b,c) is a Pythagorean Triple, then (b,a,c) is called its **co-triple**. In this case, (a,b,c) and (b,a,c) are said to be co-triples of each other. Furthermore, if $\{K,M,t\}$ denotes the set of integers that generates the triple (a,b,c), then the notation $\{\tilde{K},\tilde{M},\tilde{t}\}$ will denote the generative set for the co-triple (b,a,c).

Some of the basic relationships that exist among (b,a,c), $\{K,M,t\}$ and $\{\tilde{K},\tilde{M},\tilde{t}\}$ are shown below. They are either direct results of definitions or can be derived in a straight-forward manner using (4).

$$K=c-b=\frac{\tilde{M}^2\,\tilde{t}^2}{2\tilde{K}}=\frac{a^2}{c+b}, \tag{6}$$

$$\tilde{K}=c-a=\frac{M^2\,t^2}{2K}=\frac{b^2}{c+a},$$

$$a+b-c=a-K=b-\tilde{K}=M\,t=\tilde{M}\,\tilde{t}\,,$$

$$2(c-b)(c-a)=(a+b-c)^2=M^2\,t^2=\tilde{M}^2\,\tilde{t}^2=2K\,\tilde{K}\,,$$

$$(a,b,c)=(M\,t+K,\ \tilde{M}\,\tilde{t}+\tilde{K},M\,t+K+\tilde{K}),$$

$$(a,b,c)=(\sqrt{2K\,\tilde{K}}+K,\ \sqrt{2K\,\tilde{K}}+\tilde{K},\sqrt{2K\,\tilde{K}}+K+\tilde{K}).$$

The last relationship of (6) is probably the most noteworthy. It demonstrates that each term of a Pythagorean Triple can be expressed as a function of only the related hypotenuse-leg differences $K = c - b$ and $\widetilde{K} = c - a$. The geometric relationships corresponding to the formulas above are shown in Figure 2.

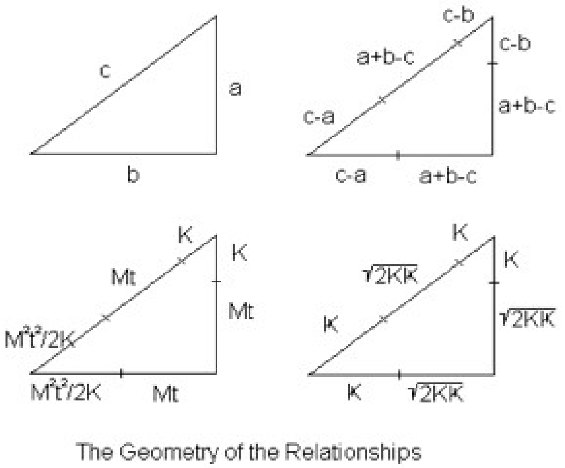

Figure 2.

6. Comparing the Classical System $[r\,s]$ with the $[K\,M\,t]$ System

Using the $[K\,M\,t]$ system, the triple $(3,4,5)$ is generated by $\{1,2,1\}$ while its co-triple $(4,3,5)$ is generated by $\{2,2,1\}$. By contrast, a co-triple of a classical triple $(r^2 - s^2, 2rs, r^2 + s^2)$ can not be produced by the generating formulas. One must physically interchange the first and second terms. The $[K\,M\,t]$ system eliminates the need for this slight of hand. Below are some examples of the relationships in the $[K\,M\,t]$ system shown in (6) along with a comparison to the classical $[r\,s\,d]$ (multiplier) system.

Triple	***K***	***M***	***t***	**Co-triples**	$\widetilde{K}$	$\widetilde{M}$	$\widetilde{t}$	$2K\widetilde{K}$	***Mt***	$\widetilde{M}\widetilde{t}$	***r***	***s***	***d***
(21, 20, 29)	9	6	2	(20, 21, 29)	8	4	3	144	12	12	5	2	1
(77, 36, 85)	49	14	2	(36, 77, 85)	8	4	7	784	28	28	9	2	1
(9, 12, 15)	3	6	1	(12, 9, 15)	6	6	1	36	6	6	2	1	3
(15, 8, 17)	9	6	1	(8, 15, 17)	2	2	3	36	6	6	4	1	1
(27, 36, 45)	9	6	3	(36, 27, 45)	18	6	3	324	18	18	6	3	1
(40, 42, 58)	16	8	3	(42, 40, 58)	18	6	4	576	24	24	7	3	1
(63, 60, 87)	27	18	2	(60, 63, 87)	24	12	3	1296	36	36	5	2	3

7. Comparing the Variant System $[p+q, q]$ with the $[K\,M\,t]$ System

Like the formulas (2) for the Variant system, the formulas (4) for the $[K\,M\,t]$ system can be parameterized so that they produce families of triples for each positive integer *K*:

$$A_K(t) = Mt + K, \qquad B_K(t) = \frac{M^2t^2 + 2KMt}{2K}, \qquad C_K(t) = \frac{M^2t^2 + 2KMt}{2K} + K. \quad (7)$$

There might be a need to clear up what might lead to a little confusion – while both generative systems produce families of triples that are indexed by integers, a closer look shows that each family of $[p+q, q]$ corresponds to the integer index *K* where $K = p^2$. That makes sense because the variant system can only generate triples whose hypotenuse-leg difference is a perfect square. A case in point is the earlier-appearing graph of the p_3-family $(A_3(t), B_3(t), C_3(t))$; this is also the graph of the K_9-family $(A_9(t), B_9(t), C_9(t))$. Thus the variant $[p+q, q]$ system only organizes the triples that it generates into cosets; that is not the same as all of the triples as produced by the $[K\,M\,t]$ system.

Whenever *K* is a perfect square, then $4K = M^2$ and the formulas (4) of the $[K\,M\,t]$ system reduce to those of the Variant system (2) where $K = p^2$ and $M = 2p$. One might say that the $[K\,M\,t]$ system 'extends' the $[p+q, q]$ system, generalizing its formulas, and allowing for families of triples indexed by all positive integers *K*, rather than just the integers that are perfect squares $(K = p^2)$.

Now remember that the neither the Classical $[r,s]$ system nor its variant $[p+q, q]$ system produce co-triples – if one generates a triple (a, b, c), then it does not generate (b, a, c). In this sense, these systems produce only half of all of the triples. Considering this in more detail, if

$$(a, b, c) = \left(r^2 - s^2, 2rs, r^2 + s^2\right), \text{ then } K = c - b = (r-s)^2$$

indicating that *K* is a perfect square. For its co-triple (b, a, c) we have

$$(b, a, c) = \left(2rs, r^2 - s^2, r^2 + s^2\right), \text{ then } K = c - a = 2s^2$$

indicating that the hypotenuse-leg difference *K* is an even integer that is twice a perfect square *p* :

$$K \in \{2, 8, 18, 32, 50, 72, 98, \ldots, 2p^2, \ldots\}.$$

All of the triples (including all co-triples) generated by $\{K, M, t\}$ come from exactly one set of formulas. Thus, we have two conditions under which a primitive triple will occur:

A triple generated by $\{K, M, t\}$ is primitive whenever
(i) K is an odd perfect square $(K \in \{1, 9, 25, 49, 81, ...\})$ and $(K, t) = 1$, and
(ii) K is twice a perfect square $(K \in \{2, 8, 18, 32, 50, ...\})$ and $(K, t) = 1$.

8. Some Observations and Applications

The preceding mathematical gymnastics are straightforward and comprise the 'heavy lifting'. The behind-the-scenes effort that took some doing was coming up with a way to describe *K*'s co-value *M*. What follows are some interesting, easily proved observations. Consequently, in the interest of brevity, they are stated without proofs.

Observation 1:

Let (a, b, c) be a Pythagorean Triple generated by the integer pair $[r, s]$ using the classical Greek formula as well as by $\{K, M, t\}$ using (4). If $4K = M^2$, then we have the cross-over relationships

$$\begin{aligned} K &= (r-s)^2 & \qquad r &= t + \frac{M}{2} \\ M &= 2(r-s) & s &= t \\ t &= s & & \end{aligned}$$

For a given value of *K*, it is useful to know when $B_K(t) > A_K(t)$. Then we can predict when the triple (a, b, c) generated by $\{K, M, t\}$ will be ordered, ie. $a < b < c$.

Observation 2:

Let (a, b, c) be a triple generated by three positive integers $\{K, M, t\}$; then $a > b$ when $t < \frac{\sqrt{2}K}{M}$ and $a < b$ when $t > \frac{\sqrt{2}K}{M}$.

A straightforward calculation shows that $A_K(t) = B_K(t)$ when $t = \pm\frac{\sqrt{2}K}{M}$, and the result follows easily. This result is particularly convincing when viewing a graph where the functions $A_K(t), B_K(t), C_K(t)$ (for a specific *K*) are simultaneously displayed as shown earlier.

Observation 3: Hypotenuse-leg Twins

A triple of the form $(a, b, b+1)$ is called a **hypotenuse-leg twin** – i.e., $(5,12,13)$. The family $\left(A_1(t), B_1(t), C_1(t)\right)$ produces all the hypotenuse-leg twin triples. We have $\left(A_1(t), B_1(t), C_1(t)\right) = (2t+1, 2t^2+2t, 2t^2+2t+1)$ for integer values of $t > 0$. The first 15 $(K=1, M=2, 1 \le t \le 15)$ are shown below:

(3, 4, 5) (5, 12,13) (7, 24, 25) (9, 40, 41) (11, 60, 61)
(13, 84, 85) (15, 112, 113) (17, 144, 145) (19, 180, 181) (21, 220, 221)
(23, 264, 265) (25, 312, 313) (27, 364, 365) (29, 420, 421) (31, 480, 481)

Note that every triple in this family is primitive, making this family unique in this respect. For each odd integer ≥ 3, there exists one hypotenuse-leg twin triple with that integer as its first term. Each such triple is ordered $(a < b)$, making this family unique in that respect as well.

Observation 4: Recursive Relationships

As we have seen in (4), for each positive value of *K*, these formulas generate all of the triples in that particular family or 'coset'. The differences between the related terms of successive triples are given by (for $t \le 2$)

$$\begin{aligned} &A_K(t) - A_K(t-1) = M \\ &B_K(t) - B_K(t-1) = C_K(t) - C_K(t-1) \\ &\qquad\qquad\qquad = \frac{M^2}{2K}(2t-1) + M = \frac{M}{2K}(2A_K(t-1) + M). \end{aligned}$$

These relationships let us generate a family of triples recursively. For example, if $K = 8$, then $M = 4$ and for $t \ge 2$:

$$\begin{aligned} &A_8(t) = A_8(t-1) + 4, \\ &B_8(t) = B_8(t-1) + 2t + 3, \\ &C_8(t) = C_8(t-1) + 2t + 3, \end{aligned}$$

where $\left(A_8(1), B_8(1), C_8(1)\right) = (12, 5, 13)$ is the starting triple.

By comparison, the original generating formulas (4) for the family of triples with $K = 8$ would yield (for $t \ge 1$)

$$A_8(t) = Mt + K \qquad = 4t + 8$$

$$B_8(t) = \frac{M^2 t^2 + 2KMt}{2K} \qquad = t^2 + 4t$$

$$C_8(t) = \frac{M^2 t^2 + 2KMt + 2K^2}{2K} \qquad = t^2 + 4t + 8$$

Observation 5: Applications to Cryptology

The generation of Pythagorean Triples using (4) can lend itself to the area of cryptology very nicely because two distinct related generating sets, such as $\{1,2,1\}$ and $\{2,2,1\}$, will yield the 'same' triple (allowing transposition), in this case $(3,4,5)$. The various families of (7) (indexed by *K*) can be thought of as an infinite number of code wheels with each wheel (family) having infinite ways to code each letter of the alphabet – 'e' could be coded with some value $t = 5 \bmod 26$ for instance. Together, a value chosen for *K* (wheel) plus the value selected for *t* will produce a triple (a,b,c); remember that *K* will determine its necessary co-value *M*. If 'e' is the plaintext message, the representative cipher sent will be the first two terms of the triple, namely (a_e, b_e). The third value of the triple can easily be calculated from the other two terms and then K_e and t_e can be calculated to decode the cipher. But along with K_e and t_e, there is another pair $\widetilde{K}_e$ and $\widetilde{t}_e$ that produce the 'same' triple. Which 'wheel' did the '*t*' come from? Which '*t*' is the correct one? Even working with the correct '*t*', the '*t*' still needs to be deciphered.

$$e \to \{K_e, t_e\} \to (a_e, b_e) \to --- \to (a_e, b_e, c_e) \to \begin{array}{c} \{K_e, t_e\} \\ ? \\ \{\tilde{K}_e, \tilde{t}_e\}. \end{array}$$

This is not a problem for someone who knows which choice to make, but a savvy hacker, even one who realizes the methodology, still has to make a choice, and this is his/her dilemma. After thirty characters of plaintext, there are over a billion possible combinations to muddle through. In short, a plaintext message can be coded in exactly one way, can be decoded easily, but would require a Herculean effort to crack. Changing the parameters of the ciphering algorithm to spawn a new cipher is easy, and can be done often with little work. Moreover, any number of other code scamblings could be used to further obfuscate the cipher. For example, (a,b) could be sent as $(a+3, b-7)$. Of course, a computer needs to be part of the whole process.

9. Conclusion

Some of the advantages of the $\left[K\,M\,t\right]$ system for generating Pythagorean Triples include the following:

- Every triple has a unique generative set $\{K, M, t\}$, eliminating any need for multipliers or transposition to produce them.
- Each member of a generative set $\{K, M, t\}$ has a geometric relationship to the triangle whose side lengths (a, b, c) they produce.
- It organizes 'all' of the triples into countable families or cosets indexed by the value of K.
- The cosets or families of triples can be graphed to visually display the members of the family. The members of each family are analytically related by the functions $(A_K(t), B_K(t), C_K(t))$.
- As an unintended consequence, it has applications to cryptology.

REFERENCES

Beiler, Albert H. (1966). *Recreations in the Theory of Numbers*, Dover Press.

Burton, David M. (2005). *Number Theory (4th edition)*, McGraw-Hill.

Singh, Simon (1999). *The Code Book*, Fourth Estate Ltd.

Tong, J. (2003). *Conjugates of Pythagorean Triples*, The Mathematical Gazette, Vol. 87, pp.496-499.

Weisserstein, Eric W. (1999). *CRC Concise Encyclopedia of Mathematics*, Chapman & Hall CRC.

APPENDIX

Factorization of K

$$\begin{aligned} K &= 2^{r_0} p_1^{r_1} p_2^{r_2} ... p_k^{r_k} \qquad p_k \neq 2 \ \forall k \\ &= p_1 \cdot p_2 ... p_k \cdot 2^{r_0} p_1^{r_1 - 1} p_2^{r_2 - 1} ... p_k^{r_k - 1} \\ &= p_1 \cdot p_2 ... p_k \cdot (2^{s_0} p_1^{s_1} p_2^{s_2} ... p_k^{s_k})^2 \cdot 2^{t_0} p_1^{t_1} p_2^{t_2} ... p_k^{t_k} \\ &= \prod_{n=1}^{k} p_n \cdot (2^{s_0} \prod_{n=1}^{k} p_n^{s_n})^2 \cdot 2^{t_0} \prod_{n=1}^{k} p_n^{t_n}, \end{aligned}$$

where $s_0 = \frac{r_0}{2}$, $s_n = \frac{r_n - 1}{2}$ (integer division), $t_0 = \frac{r_0}{2} \bmod 2$, $t_n = \frac{r_n - 1}{2} \bmod 2$ for $n = 1, 2, ..., k$. Note that either $t_n = 0$ or $t_n = 1$ for $n = 0, 1, 2, ..., k$. Thus K can be written as the product $K = D \cdot E^2 \cdot L$, where

$$D = \prod_{n=1}^{k} p_n \qquad E = 2^{s_0} \prod_{n=1}^{k} p_n^{s_n} \qquad L = 2^{t_0} \prod_{n=1}^{k} p_n^{t_n}.$$