
The Modular Tree of Pythagoras

Roger C. Alperin

1. INTRODUCTION. The Pythagorean triples $[x, y, z]$ of integers satisfying the equation $x^2 + y^2 = z^2$ have been studied and enumerated since Babylonian times. Since Diophantus, it has been known that this set of triples is related to the standard rational parameterization of the circle of radius one, namely,

$$t \mapsto \left(\frac{t^2 - 1}{t^2 + 1}, \frac{2t}{t^2 + 1} \right).$$

The Pythagorean triples that are relatively prime (called the *primitive triples*) have the elementary and beautiful characterization as integers $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$ (when y is even) for relatively prime integers m and n of opposite parity. One can think of this as replacing the parameter t for the circle with the fraction m/n and then scaling.

Our motivation for understanding the triples stems from the realization that one can enumerate the rational numbers on the line by using the modular group, in a sense reversing the Euclidean algorithm [2]. Now the line can be transformed by a linear fractional transformation to the circle. This transformation changes fractions to rational points on the circle, and after scaling this process gives rise to Pythagorean triples. Roughly speaking, we can establish a correspondence of a Pythagorean triple $[m^2 - n^2, 2mn, m^2 + n^2]$ in which m and n are relatively prime with a matrix belonging to $SL_2(\mathbb{Z})$ (the group of two-by-two integral matrices of determinant one) whose entries depend on m and n . Since the modular group $\Gamma = PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$ is essentially a free group, it follows that there is an underlying tree structure to Pythagorean triples. Making this tree structure and its connection to the modular group explicit is a bit delicate, but the payoff is worth the effort.

Our main results can be summarized as follows:

Theorem 1. *The set of positive primitive Pythagorean triples has the structure of a complete, infinite, rooted ternary-tree.*

For the proof we use the action of Γ by conjugation on the set of all two-by-two integer matrices $M_2(\mathbb{Z})$. By studying this action we show (Theorem 5) that the Pythagorean triples can be identified with an orbit of $\Gamma(2)$, the normal subgroup of Γ obtained as the kernel of reduction modulo 2. Then, since the group $\Gamma(2)$ is freely generated by the images of the $SL_2(\mathbb{Z})$ matrices

$$U^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad L^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$

we can use the tree structure for the group elements to make a tree for the Pythagorean triples (see Figure 1).¹

¹After a version of this article was made available as a preprint, it was pointed out to the author that this tree structure was noticed earlier by Hall using three-by-three matrices [4]. The connection between our use of two-by-two matrices versus Hall's three-by-three matrices is presumably a reflection of the isomorphism between the group of linear fractional transformations and a subgroup of the Lorentz group preserving the quadratic form $x^2 + y^2 - z^2$.

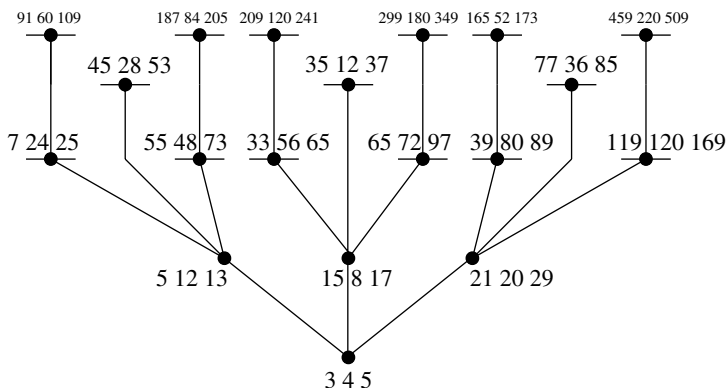


Figure 1. Tree of Pythagoras.

2. CONJUGATION ACTION AND SIMILARITY. In this section we develop some fundamental properties of the action of Γ on $M_2(\mathbb{Z})$. We start with an elementary but important observation.

Proposition 2. *An integer matrix X satisfies $X^2 = 0$ if and only if X has the form*

$$X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}$$

for integers x , y , and z such that $x^2 + yz = 0$.

Proof. The sufficiency is clear. Suppose that a nonzero integer matrix X has $X^2 = 0$. Since the matrix X satisfies its characteristic polynomial, it follows that $\text{tr}(X)X = \det(X)I$. Because X is not a nonzero multiple of the identity matrix, it follows that $\text{tr}(X) = \det(X) = 0$. The conclusion is now immediate. ■

An element T of the group $GL_2(\mathbb{Z})$ of invertible two-by-two integer matrices acts by conjugation on the set $M_2(\mathbb{Z})$ via $X \mapsto TXT^{-1}$. This action preserves the “cone” of nilpotent matrices $\mathcal{N}_2 = \{X \in M_2(\mathbb{Z}) : X^2 = 0\}$ as described by Proposition 2. In what follows $[X]$ signifies the similarity class of the matrix X (i.e., $[X] = \{TXT^{-1} : T \in GL_2(\mathbb{Z})\}$).

Consider the matrix

$$E = \begin{pmatrix} 0 & -1 \\ 0 & 0 \end{pmatrix}.$$

Notice that the transpose E^t and $-E$ belong to $[E]$ (conjugate by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},$$

respectively). Let $\mathbf{N}$ denote the set of nonnegative integers. If $\mathcal{E}_\lambda = [\lambda E]$ ($\lambda \in \mathbf{N}$) it is clear that $\mathcal{E}_\lambda = \lambda[E]$. Moreover it is an easy exercise to check that $\mathcal{E}_\lambda$ and $\mathcal{E}_\mu$ are disjoint when $\lambda \neq \mu$.

Proposition 3. *Each matrix X in $\mathcal{N}_2$ is similar to λE for a unique λ in $\mathbf{N}$. Thus $\mathcal{N}_2 = \bigcup_{\lambda \in \mathbf{N}} \mathcal{E}_\lambda$ is the disjoint union of similarity classes.*

Proof. Consider a matrix X from $\mathcal{N}_2$. If any entry of X is zero, then it follows immediately from Proposition 2 that X is the zero matrix, a multiple of E , or a multiple of E' . Thus, in this case X is similar to either the zero matrix or E .

Suppose next that none of the entries of X is zero. Write

$$X = \begin{pmatrix} x & y \\ z & -x \end{pmatrix}.$$

Since the determinant of X is zero, the rows are linearly dependent over the rationals. Furthermore, after factoring out the greatest common divisor of the entries of X , call it λ , we find that there are relatively prime integers m and n such that $mx = nz$ and $my = -nx$.

Now exploiting the relative primality of m and n we conclude: $m \mid z$, $m \mid x$, $n \mid x$, $n \mid y$. Rewriting $x = mnx_1$, $y = ny_1$, $z = mz_1$ and then canceling common factors wherever possible, we see that $mx_1 = z_1$ and $-nx_1 = y_1$. Thus $m \mid z_1$ and $n \mid y_1$, whence $x = mn\lambda$, $y = -n^2\lambda$, and $z = m^2\lambda$ for some integer λ .

The original matrix X is therefore an integral multiple of a matrix that admits a special factorization:

$$X = \lambda \begin{pmatrix} mn & -n^2 \\ m^2 & -mn \end{pmatrix} = \lambda \begin{pmatrix} n \\ m \end{pmatrix} (m \quad -n).$$

Consequently, the action of conjugation reduces to a mixture of the usual actions on $\mathbb{Z}^2$ through matrix multiplication with column- and row-vectors, respectively:

$$TXT^{-1} = \lambda T \begin{pmatrix} n \\ m \end{pmatrix} (m \quad -n) T^{-1}.$$

For any given relatively prime integers m and n , we can determine integers u and v for which $un + vm = 1$. Let

$$T = \begin{pmatrix} u & v \\ -m & n \end{pmatrix}.$$

Then

$$T \begin{pmatrix} n \\ m \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

and

$$(m \quad -n)T^{-1} = (0 \quad -1).$$

Hence $TXT^{-1} = \lambda E$ and the conclusion of the proposition follows. ■

3. ENUMERATING PYTHAGOREAN TRIPLES. From the proof of Proposition 3 we see that any matrix X in $M_2(\mathbb{Z})$ that is similar to E is in $\mathcal{N}_2$ and has the form

$$\begin{pmatrix} mn & -n^2 \\ m^2 & -mn \end{pmatrix} = \frac{1}{2} \begin{pmatrix} C & S - N \\ S + N & -C \end{pmatrix}, \quad (1)$$

where m and n are relatively prime integers. The integers $S = m^2 - n^2$, $C = 2mn$, and $N = n^2 + m^2$ give a Pythagorean triple satisfying $S^2 + C^2 = N^2$.

We thus have a method of generating all Pythagorean triples. For the matrix product

$$T = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

we find that

$$TET^{-1} = \begin{pmatrix} -28 & -9 \\ 16 & 28 \end{pmatrix},$$

which yields the triple $[-33, -56, 65]$. (However, the triple in the tree in Figure 1 is labelled using absolute values as $[33, 56, 65]$.) For the matrix

$$R = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} T = \begin{pmatrix} -7 & -2 \\ -10 & -3 \end{pmatrix}$$

computing RER^{-1} and using the method just described leads to the Pythagorean triple $S = 51$, $C = 140$, and $N = 149$. In fact, this triple (not shown in Figure 1) occurs at the third level above $[3, 4, 5]$ in the tree, branching from the triple $[33, 56, 65]$.

In order to list the Pythagorean triples we seek an effective way of enumerating the elements of the orbit of E under the action of $GL_2(\mathbb{Z})$ by conjugation. Since we want the triples to exhibit a tree structure, the enumeration should have a recursive structure. Recall that if a group G acts by permutations on a set X and if x_0 is an element of X , then there is a bijection $gH \mapsto g \cdot x_0$ between right cosets of the stabilizer H of x_0 ($\{g \in G : gx_0 = x_0\}$) and the orbit of x_0 . In our case the permutation action is conjugation of matrices TXT^{-1} for T in $GL_2(\mathbb{Z})$ and X in $M_2(\mathbb{Z})$. This fundamental property of group actions now ensures that there is a one-to-one correspondence between the elements of the orbit of E and the cosets of the stabilizer of E .

As we now show, the group $GL_2(\mathbb{Z})$ can be replaced with a simpler group, in fact a free group of rank 2, without changing the set of positive primitive triples obtained from the orbit. First, since conjugation by a diagonal matrix of determinant -1 changes only the sign of E , we may without loss of any triples restrict attention to the subgroup $SL_2(\mathbb{Z})$ of elements having determinant one. In this situation, the stabilizer of E is the subgroup $H = \{T \in SL_2(\mathbb{Z}) : TET^{-1} = E\}$ of $SL_2(\mathbb{Z})$, which is easily seen to be the subgroup generated by

$$U = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and $-I$, the negative of the identity matrix. Since the effect of conjugating by $-I$ on triples S , C , and N is trivial, we factor out that action and work with $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm I\}$ instead of $SL_2(\mathbb{Z})$. It can be shown (see [1]) that the group $PSL_2(\mathbb{Z})$ is isomorphic to the group generated by the images of the matrices U and

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

To enumerate distinct primitive Pythagorean triples $[S, C, N]$ we must start with m and n that are relatively prime and of opposite parity. If m is even and n is odd, then C is even and S is odd. For such m and n there is a matrix T in $PSL_2(\mathbb{Z})$ with $T_{11} = n$ and $T_{21} = m$. If the entry T_{12} is odd, we replace T with the matrix $T' = TU$, which

has even entry T'_{12} . This gives rise to the same Pythagorean triple as T , since U stabilizes E . The elements of $\Gamma = PSL_2(\mathbb{Z})$ with even entries off the diagonal constitute the normal subgroup $\Gamma(2)$, the kernel of the homomorphism $PSL_2(\mathbb{Z}) \rightarrow PSL_2(\mathbb{Z}_2)$ effected by reducing modulo 2. On the basis of earlier remarks we conclude that we need not consider the action of the full modular group Γ to enumerate all triples, just that of $\Gamma(2)$.

Using the fact that U and A generate Γ , one can show that $\Gamma(2)$ is generated by the two matrices

$$U^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad L^2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}.$$

Moreover, these elements generate the group as a free product.

Proposition 4. *The group $\Gamma(2)$ is the free product of the infinite cyclic subgroups generated by U^2 and L^2 .*

Proof. This result is easily established using the structure of $PSL_2(\mathbb{Z})$ as the free product of the subgroups of orders 2 and 3 generated by the matrices

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and

$$B = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix},$$

respectively [1]. Since $U = AB$, $U^2 = ABAB$, $L = AB^{-1}$, and $L^2 = AB^{-1}AB^{-1}$, any alternating word in $U^{\pm 2}$ and $L^{\pm 2}$ is also alternating in A and $B^{\pm 1}$, hence is nontrivial. ■

The enumeration of triples is still a bit subtle, since we want to enumerate only the distinct absolute values of the triples $[|S|, |C|, |N|]$. Let

$$D = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Then, for any matrix T in $PSL_2(\mathbb{Z})$, $\delta(T) = DTD^{-1}$ is the matrix with the same off-diagonal entries as T but with signs changed on the diagonal. The two matrices T and $\delta(T)$ give rise to the same absolute Pythagorean triple, as one reads directly from the prescription for S , C , and N given by (1). Because the automorphism δ of order 2 has the effect that $\delta(U^2) = U^{-2}$ and $\delta(L^2) = L^{-2}$, we can avoid using both T and $\delta(T)$ in the enumeration of cosets of $\Gamma(2)$ modulo the stabilizer of E simply by enumerating “half” of the cosets.

To summarize: we have described a listing of Pythagorean triples based on the enumeration of cosets of $\Gamma(2)$ modulo the stabilizer of E , the subgroup generated by U^2 . Because of the free product structure of $\Gamma(2)$ the coset representatives are just the words in $L^{\pm 2}$ and $U^{\pm 2}$. Since we are considering nontrivial left cosets of the subgroup generated by U^2 , the rightmost letter of a coset representative is $L^{\pm 2}$. We do a “breadth-first” enumeration, alternatively concatenating with $U^{\pm 2}$ or $L^{\pm 2}$ on the left of

a string. For example, if the last group element on the left is L^2 , we can concatenate with L^2 , U^2 , or U^{-2} .

We can then effectively describe the distinct coset representatives that enumerate the distinct Pythagorean triples by appealing to the alternating property for the words of the free group $\Gamma(2)$ in the generators L^2 and U^2 . Since we can recover $|n|$ and $|m|$ from $|C|$ and $|N|$, then by use of δ we see that we obtain distinct triples when we initialize with just one of the strings $L^{\pm 2}$. Let $\mathcal{L}_0^+ = \{L^2\}$, $\mathcal{L}_0^- = \mathcal{U}_0^\pm = \emptyset$ and inductively define

$$\begin{aligned}\mathcal{L}_{k+1}^+ &= \{L^2X : X \in \mathcal{L}_k^+ \cup \mathcal{U}_k^\pm\}, \\ \mathcal{L}_{k+1}^- &= \{L^{-2}X : X \in \mathcal{L}_k^- \cup \mathcal{U}_k^\pm\}, \\ \mathcal{U}_{k+1}^+ &= \{U^2X : X \in \mathcal{U}_k^+ \cup \mathcal{L}_k^\pm\}, \\ \mathcal{U}_{k+1}^- &= \{U^{-2}X : X \in \mathcal{U}_k^- \cup \mathcal{L}_k^\pm\}\end{aligned}$$

for $k = 0, 1, \dots$. For example, when $k = 0$, the level-one sets are

$$\mathcal{L}_1^+ = \{L^4\}, \quad \mathcal{L}_1^- = \emptyset, \quad \mathcal{U}_1^+ = \{U^2L^2\}, \quad \mathcal{U}_1^- = \{U^{-2}L^2\}.$$

This approach will produce an effective enumeration of nontrivial primitive Pythagorean triples in terms of the coset representatives in the disjoint union

$$\mathcal{P} = \bigcup_{k \geq 0} (\mathcal{L}_k^\pm \cup \mathcal{U}_k^\pm).$$

The recurrence relation that counts the number p_k of elements in $\mathcal{P}$ of level k is $p_k = 3p_{k-1}$, for we can add any one of three elements to the left of a given alternating string to keep it alternating. We use Π to denote the set of matrices obtained from E via conjugation by the elements of $\mathcal{P}$. The entries of each $T = (T_{ij})$ in Π determine a unique primitive Pythagorean triple of positive integers as follows:

$$|S| = |T_{21} + T_{12}|, \quad |C| = |2T_{11}|, \quad |N| = |T_{21} - T_{12}|.$$

Theorem 5. *The primitive Pythagorean triples are in one-to-one correspondence with the set Π of coset representatives of the subgroup generated by U^2 in $\Gamma(2)$. This set Π can be enumerated as a union of subsets Π_k of size 3^k ($k = 0, 1, 2, \dots$), the levels of the tree of Pythagoras.*

We build the tree of Pythagoras by starting with

$$L^2EL^{-2} = \begin{pmatrix} 2 & -1 \\ 4 & -2 \end{pmatrix},$$

so $m = 2$, $n = 1$, and $[S, C, N] = [3, 4, 5]$. At the next level L^4EL^{-4} yields the triple $[15, 8, 17]$, and similarly conjugation of E by U^2L^2 and $U^{-2}L^2$ gives the other triples above $[3, 4, 5]$ (i.e., after taking absolute values we obtain $[21, 20, 29]$ and $[5, 12, 13]$). Further conjugations using L^{-2} , L^2 , U^{-2} , and U^2 of the matrix corresponding to a triple $[S, C, N]$ at level k , where $S = m^2 - n^2$, $C = 2mn$, and $N = m^2 + n^2$, creates three new triples at level $k + 1$ and duplicates one triple from the prior level $k - 1$. In general to make the tree we connect the j th element of level k with the

absolute values of the entries of the three different triples of level $k + 1$ (numbered $3(j - 1) + 1, 3(j - 1) + 2, 3(j - 1) + 3$) obtained from the conjugation action on the j th element.

Alternatively, to get to the next level in the tree when the coordinates of a triple (expressed in terms of m and n) are all positive, it suffices to compute $\mathbf{L}_+$, $\mathbf{U}_-$, and $\mathbf{U}_+$, since if S , C , and N are positive, then the previous triple is $\mathbf{L}_-$. Here

$$\begin{aligned}\mathbf{L}_- &= [m^2 - 4mn + 3n^2, 2mn - 4n^2, m^2 - 4mn + 5n^2], \\ \mathbf{L}_+ &= [m^2 + 4mn + 3n^2, 2mn + 4n^2, m^2 + 4mn + 5n^2], \\ \mathbf{U}_- &= [-n^2 + 4mn - 3m^2, 2mn - 4m^2, n^2 - 4mn + 5m^2], \\ \mathbf{U}_+ &= [-n^2 - 4mn - 3m^2, 2mn + 4m^2, n^2 + 4mn + 5m^2].\end{aligned}$$

This is easy to see, for in this case $m > n \geq 0$, $2mn > 2mn - 4n^2 > -2mn$, and $2mn - 4n^2$ (the second coordinate of $\mathbf{L}_-$) is smaller in absolute value than $C = 2mn$. Similarly, the second coordinate of each of $\mathbf{L}_+$, $\mathbf{U}_-$, and $\mathbf{U}_+$ is greater than C .

We now show how to modify $\mathbf{L}_+$ and $\mathbf{U}_\pm$ to obtain transformations that map triples with positive coordinates to other triples of this sort and so preserve the positive quadrant of the cone $S^2 + C^2 = N^2$. One may use these transformations as the starting point for an alternate description of the tree structure:

$$\begin{aligned}\mathcal{L}_+[S, C, N] &= [m^2 + 4mn + 3n^2, 2mn + 4n^2, m^2 + 4mn + 5n^2] \\ &= [S, -C, N] + 2(N - S + C)[1, 1, 1], \\ \mathcal{U}_-[S, C, N] &= [n^2 - 4mn + 3m^2, 4m^2 - 2mn, n^2 - 4mn + 5m^2] \\ &= [-S, C, N] + 2(N + S - C)[1, 1, 1], \\ \mathcal{U}_+[S, C, N] &= [n^2 + 4mn + 3m^2, 2mn + 4m^2, n^2 + 4mn + 5m^2] \\ &= [-S, -C, N] + 2(N + S + C)[1, 1, 1].\end{aligned}$$

Certain paths in the tree have predictable properties. If, for example, we start at the root and always follow the path dictated by $\mathcal{L}_+$, then we get a sequence that displays quadratic growth in the C coordinate, since the terms are solutions to $x^2 + y^2 = (x + 2)^2$ (or equivalently $x = \frac{1}{4}y^2 - 1$):

$$\begin{aligned}&[3, 4, 5] \\ &[15, 8, 17] \\ &[35, 12, 37] \\ &[63, 16, 65] \\ &[99, 20, 101] \\ &[143, 24, 145] \\ &[195, 28, 197] \\ &\dots\end{aligned}$$

Another path starts at the root $[3, 4, 5]$ and follows a route along which the N coordinate differs by one from either twice the S or twice the C coordinate. It is generated by alternating the application of the transformations $\mathcal{L}_+$ and $\mathcal{U}_-$:

[3, 4, 5]
 [15, 8, 17]
 [33, 56, 65]
 [209, 120, 241]
 [451, 780, 901]
 [2911, 1680, 3361]
 ...

The growth of the N coordinate in the following triples, which are obtained by taking every other triple from the previous list, is visibly exponential. It is left as an exercise to show that these are solutions to the equation $x^2 + y^2 = (2x - 1)^2$ (equivalently, $(3x - 2)^2 - 3y^2 = 1$) and thus related to solving Pell's equation $X^2 - 3Y^2 = 1$.

[3, 4, 5]
 [33, 56, 65]
 [451, 780, 901]
 [6273, 10864, 12545]
 [87363, 151316, 174725]
 [1216801, 2107560, 2433601]
 [16947843, 29354524, 33895685]
 [236052993, 408855776, 472105985]
 [3287794051, 5694626340, 6575588101]
 [45793063713, 79315912984, 91586127425]
 [637815097923, 1104728155436, 1275630195845]
 [8883618307201, 15386878263120, 17767236614401]
 [123732841202883, 214311567528244, 247465682405765]
 [1723376158533153, 2984975067132296, 3446752317066305]
 [24003533378261251, 41575339372323900, 48007066756522501]
 [334326091137124353, 579069776145402304, 668652182274248705]
 [4656561742541479683, 8065401526663308356, 9313123485082959365]
 [64857538304443591201, 112336551597140914680, 129715076608887182401]
 [903348974519668797123, 1564646320833309497164, 1806697949039337594245]
 [12582028104970919568513, 21792711940069192045616, 25164056209941839137025]
 [175245044495073205162051, 303533320840135379141460, 350490088990146410324101]
 ⋮

4. RAYS IN THE TREE. In this section we discuss and sketch some connections between infinite rays in the tree of Pythagoras and Pell's equations. A ray in the tree is an infinite sequence of distinct triples starting at a root or vertex of the tree so that two consecutive terms of the sequence are one level apart in the tree. The root corresponds to the smallest solution to a Pell's equation and the remaining solutions give higher level vertices in the tree. We invite the reader to visit the applet at <http://www.math.sjsu.edu/~alperin/Pythagoras/ModularTree.html>, where he or she may peruse the tree at great length.

The results discussed here depend on a close examination of differences between the coordinates of triples that remain constant (up to sign) in a sequence of triples as one proceeds level-by-level up the tree. Here are some examples to motivate the discussion: (a) the sequence of triples $[S, C, N]$ with difference 1 between N and C make up a ray in the tree beginning with $[3, 4, 5]$, $[5, 12, 13]$, and $[7, 24, 25]$; (b) the analogous ray with (absolute) difference 1 between C and S exhibits an alternation of the location of the larger coordinate, as seen in $[3, 4, 5]$, $[21, 20, 29]$, $[119, 120, 169]$,

and [697, 696, 985]; (c) the difference -7 for $S - C$ occurs (alternating sign) for the ray beginning with [15, 8, 17], [65, 72, 97], and [403, 396, 565].

One can easily check that each of the differences between coordinates in $[m^2 - n^2, 2mn, m^2 + n^2]$ —namely, $P = N - C = (m - n)^2$, $Q = N - S = 2n^2$, and $R = C - S = (n + m)^2 - 2m^2$ —persists to the next level (except for a sign change in the last one), for exactly one of the transformations $\mathcal{U}_-$, $\mathcal{L}_+$, or $\mathcal{U}_+$. These three new points at level $k + 1$ are represented in the tree from left to right (see Figure 1) and connected to the level k point.

We indicate an approach to a characterization of all those integers that can be differences of the types just indicated: P , Q , or $\pm R$. This “difference problem” is equivalent to a question about the representations of integers by the forms $P = (m - n)^2$, $Q = 2n^2$, and $R = (m - n)^2 - 2n^2$ for m even and n odd. The first form can take on any odd square value, the second can assume any value that is twice an odd square, but the third case is more restrictive. We shall concentrate our attention on the values of $\pm R$. The values of R are closely related to values of the algebraic norm $a^2 - 2b^2$ of an element $a + b\sqrt{2}$ in the ring $\mathbb{Z}[\sqrt{2}]$.

Suppose that we are given integers a and b such that

$$a > 0, \quad b < 0, \quad a^2 - 2b^2 = d.$$

We can then solve for values of m and n that give rise to a Pythagorean triple by setting $m + n = a$ and $m = b$. Then $n = a - m > 0$ and $n - m = a - 2m > 0$. Hence the Pythagorean triple of positive integers $[n^2 - m^2, -2mn, m^2 + n^2]$ has difference $d = -R = n^2 - m^2 - (-2mn) = a^2 - 2b^2$. For example, to find the first time that the difference $R = -17$ occurs in the Pythagorean tree we use the smallest positive solution (in $\mathbb{Z}[\sqrt{2}]$) $5 - 2\sqrt{2}$ to $a^2 - 2b^2 = 17$. In this instance $m = -2$ and $n = 7$ produce the (positive) triple [45, 28, 53]. To create a triple with $R = 17$, multiply $5 + 2\sqrt{2}$ by $-1 + \sqrt{2}$, the smallest positive unit of norm equal to -1 , to obtain $-1 + 3\sqrt{2}$ of norm -17 . Then, choosing $m = 3$ and $n = -4$ gives the triple [7, 24, 25].

The “norm” equation (or Pell’s equation) $X^2 - 2Y^2 = d$ can be solved for integers X and Y for exactly those integers d that occur as norms for the ring $\mathbb{Z}[\sqrt{2}]$. When d is square-free, we see by reducing this equation modulo d that 2 is a quadratic residue modulo d , and hence also modulo any divisor of d . It now follows from the quadratic reciprocity law that every odd prime factor p of d is congruent to ± 1 modulo 8. Conversely, it is not difficult to see that $\mathbb{Z}[\sqrt{2}]$ is a Euclidean ring with respect to the function $|a^2 - 2b^2|$ and consequently any prime p congruent to ± 1 modulo 8 is a norm (i.e., $p = a^2 - 2b^2$ for integers a and b integers). Since the norm is multiplicative, if we want to show that a particular value of d is a norm we express its prime factors as norms (if possible). By multiplying the minimal positive representation of d as a norm by an arbitrary unit of $\mathbb{Z}[\sqrt{2}]$ we obtain a ray in the Pythagorean tree of constant (up to alternations of sign) differences using the method that we have discussed. The path is infinite since the group of units of $\mathbb{Z}[\sqrt{2}]$ contains an infinite cyclic subgroup of index 2.

We should also note from the foregoing discussion that if we chose $m = Y$ with m even, then the Pell’s equation $X^2 - 2Y^2 = d$ can be transformed to the Pell’s equation $x^2 - 8y^2 = d$. We give an example to illustrate a method of solving the latter equation in integers x and y when $d = p$ is a prime congruent to 1 modulo 8. This method of Lagrange is described in [3]. We use $d = 89$ and seek a minimal solution to $x^2 - 8y^2 = 89$. First one finds the smallest positive integer z_0 less than $89/2$ such that $(z_0^2 - 8)/89$ is an integer, say q_1 (here $z_0 = 39$, $q_1 = 17$). One then solves for the smallest z_1 less than $17/2$ such that $(z_1^2 - 8)/17 = q_2$ is integral. In this case $z_1 = 5$ and

$q_2 = 1 < \sqrt{8}$, so the algorithm terminates. It now follows that $(39 - 2\sqrt{2})/(5 + 2\sqrt{2})$ has norm 89. This gives rise to the solution $11 + 4\sqrt{2}$, an element of norm 89 in $\mathbb{Z}[\sqrt{2}]$. The solution $11 + 4\sqrt{2}$ leads to $m = 4$ and $n = 15$, which generates the positive triple [209, 120, 241]. The number $3 - 7\sqrt{2}$ has norm -89 ; with $3 - 7\sqrt{2}$ we use $m = -7$ and $n = 10$ to obtain the positive triple [51, 140, 149]. This triple stems from [33, 56, 65] (not shown in Figure 1). It follows that the triple [51, 140, 149] is a root of those triples with difference $R = -89$.

New mysteries of the Pythagorean triples and their connections with other Pell's equations await readers who delve further into the ideas presented here or explore other aspects of the geometry of the Pythagorean modular tree.

REFERENCES

1. R. C. Alperin, $PSL_2(\mathbb{Z}) = \mathbb{Z}_2 * \mathbb{Z}_3$, this MONTHLY **100** (1993) 385–6.
2. ———, Rationals and the modular group, this MONTHLY **106** (1999) 771–3.
3. G. Chrystal, *Algebra*, Part II, 7th ed., Chelsea, New York, 1964.
4. A. Hall, Genealogy of Pythagorean triads, *Math. Gazette* **54** (1970) 377–379.

ROGER C. ALPERIN grew up in Miami, Florida, graduated from the University of Chicago, and then received a Ph.D. from Rice University under the direction of Professor S. M. Gersten. His main areas of interest in mathematics involve the interplay between algebra and low-dimensional topology or geometry, and sometimes elementary number theory or the Chomsky hierarchy. His main recreational interests are hiking, biking, and occasionally, easy mountaineering or desert backpacking.

Department of Mathematics, San Jose State University, San Jose, CA 95192
alperin@math.sjsu.edu

Finite dimensionality of normed spaces with compact closed disks: A short proof

Theorem 1. *Let X be a real normed vector space. If the closed unit disk D in X is compact, then X is finite dimensional.*

Proof. Let S be the sphere that bounds D . This is a closed subset of D , hence is compact. By the Hahn-Banach theorem, there exists for each x in S a continuous linear transformation $\pi_x : X \rightarrow \mathbb{R}$ such that $\pi_x(x) \neq 0$. Then

$$S \subseteq \bigcup_{x \in S} (\pi_x)^{-1}(\mathbb{R} \setminus 0).$$

The compactness of S reduces this union to a finite one, that is, there are points $x_1, \dots, x_n$ in S such that S is contained in the union of $(\pi_{x_i})^{-1}(\mathbb{R} \setminus 0)$. The continuous linear map $f : X \rightarrow \mathbb{R}^n$ defined by $x \mapsto (\pi_{x_1}(x), \dots, \pi_{x_n}(x))$ is an $\mathbb{R}$ -monomorphism. The result follows.

——Submitted by Shahram Biglari, University of Leipzig, Germany