PYTHAGOREAN DESCENT

KEITH CONRAD

Theorem 1. *Let $Q(x,y,z) = x^2 + y^2 - z^2$. The group $\mathrm{O}_Q(\mathbf{Z})$ acts transitively on the primitive null vectors.*

Note a member of $\mathrm{O}_Q(\mathbf{Z})$ preserves the primitivity of an integral vector since it is an invertible linear transformation over $\mathbf{Z}$.

Proof. We will argue by descent, using reflections in $\mathrm{O}_Q(\mathbf{Z})$ to decrease the overall size of the coordinates of a vector.

For $w \in \mathbf{Q}^3$ such that $Q(w) \neq 0$, the reflection $s_w \colon \mathbf{Q}^3 \to \mathbf{Q}^3$ is defined by the formula

$$s_w(v) = v - \frac{2}{B(v,w)}w,$$

where $B(v,w) = \frac{1}{2}(Q(v+w) - Q(v) - Q(w))$ is the bilinear form associated to Q. The transformation s_w is linear, fixes the plane $w^\perp = \{v : v \perp w\}$, and acts by negation on the line through w. These properties characterize s_w. We will use reflections associated to the four vectors $e_1 = (1,0,0)$, $e_2 = (0,1,0)$, $e_3 = (0,0,1)$, and $e_1 + e_2 + e_3 = (1,1,1)$.

The vectors e_1, e_2, and e_3 form an orthogonal basis for Q and the three reflections s_{e_1}, s_{e_2}, and s_{e_3} are all in $\mathrm{O}_Q(\mathbf{Z})$. Starting with an integral vector (a,b,c), the vectors $(\pm a, \pm b, \pm c)$ are obtained from it by applying these three reflections. After making suitable sign changes, any integral null vector (a,b,c) can be assumed to have nonnegative coefficients, so $0 \leq a, b \leq c$ because $c^2 = a^2 + b^2$. Assume a and b are both positive. Then

$$a < c, \quad b < c, \quad c < a + b. \tag{1}$$

The reflection $s_{e_1+e_2+e_3}$ is given by the formula

$$s_{e_1+e_2+e_3}(v) = v - 2(a+b-c)(1,1,1),$$

so

$$s_{e_1+e_2+e_3}(a,b,c) = (-a-2b+2c, -2a-b+2c, -2a-2b+3c). \tag{2}$$

The coordinates of this reflection satisfy

$$-a < -a-2b+2c < a, \quad -b < -2a-b+2c < b, \quad -c < -2a-2b+3c < c,$$

as these inequalities are all equivalent to one of the inequalities in (1) or, in the case of $-c < -2a-2b+3c$, this is equivalent to $a+b < 2c$, which is immediate from $a < c$ and $b < c$.

Since the coordinates of $s_{e_1+e_2+e_3}(a,b,c)$ are, in absolute value, less than the corresponding coordinates of (a,b,c), we can apply the reflections s_{e_i} to make the new coordinates all nonnegative and then, if the first two coordinates are both positive, use the reflection $s_{e_1+e_2+e_3}$ once again to shrink the absolute value of the coordinates further. Eventually by descent we will reach an integral null vector for Q with one of the first two coordinates being 0. If we had started with an integral null vector that is primitive then the null vector

we eventually reach is primitive too, so it must be one of $(0, \pm 1, \pm 1)$ or $(\pm 1, 0, \pm 1)$. We can pass from $(0,1,1)$ to $(-1,0,1)$ using $s_{e_1+e_2}$ (whose general effect is to send (a,b,c) to $(-b,-a,c)$), so the primitive integral null vectors are all in the same orbit of $\mathrm{O}_Q(\mathbf{Z})$. □

Corollary 2. *The group $\mathrm{O}_Q(\mathbf{Z})$ is generated by the five reflections*

$$s_{e_1}, \quad s_{e_2}, \quad s_{e_3}, \quad s_{e_1+e_2+e_3}, \quad s_{e_1+e_2}.$$

Proof. The proof of Theorem 1 used only these five reflections to carry any primitive null vector to $(0,1,1)$, so $\mathrm{O}_Q(\mathbf{Z})$ is generated by these reflections and the matrices fixing $(0,1,1)$. A calculation shows the stabilizer subgroup of $(0,1,1)$ in $\mathrm{O}_Q(\mathbf{Z})$ consists of matrices of the form

$$\begin{pmatrix} 1 & 2b & -2b \\ -2b & 1-2b^2 & 2b^2 \\ -2b & -2b^2 & 1+2b^2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}^b$$

for $b \in \mathbf{Z}$ and

$$\begin{pmatrix} -1 & 2b & -2b \\ 2b & 1-2b^2 & 2b^2 \\ 2b & -2b^2 & 1+2b^2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}^b \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so the stabilizer subgroup is generated by

$$\begin{pmatrix} 1 & 2 & -2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}. \tag{3}$$

The second matrix in (3) is s_{e_1}. By (2), the matrix for $s_{e_1+e_2+e_3}$ is

$$\begin{pmatrix} -1 & -2 & 2 \\ -2 & -1 & 2 \\ -2 & -2 & 3 \end{pmatrix}, \tag{4}$$

so the first matrix in (3) is $s_{e_1+e_2+e_3}s_{e_1}$. □

In [3], all (positive) primitive Pythagorean triples with even second term are shown to be generated from the triple $(3,4,5)$ by a 3-fold ascent using the three matrices

$$\begin{pmatrix} 1 & -2 & 2 \\ 2 & -1 & 2 \\ 2 & -2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 2 \\ 2 & 1 & 2 \\ 2 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} -1 & 2 & 2 \\ -2 & 1 & 2 \\ -2 & 2 & 3 \end{pmatrix}. \tag{5}$$

That is, applying these three matrices in arbitrary order on $(3,4,5)$ leads to all the positive primitive Pythagorean triples. This was found by Berggren [2] and is set out as an exercise with solution in [4, pp. 84-85]. The motivation in [3] which leads to these matrices comes from algebraic relations among sides of right triangles. No geometric interpretation of the matrices in (5) is indicated in [3] or [4]. (I have not been able to look at [2] to check there.) Since $s_{e_1+e_2+e_3}$ is represented by the matrix (4), the matrices in (5) must be related to this reflection. A short search shows the matrices in (5) are $s_{e_1+e_2+e_3}s_{e_1}$, $s_{e_1+e_2+e_3}s_{e_1}s_{e_2}$, and $s_{e_1+e_2+e_3}s_{e_2}$, respectively.

In addition to using 3×3 matrices in $\mathrm{O}_Q(\mathbf{Z})$ to generate the primitive Pythagorean triples, these triples can be generated by 2×2 matrices from the principal congruence subgroup of level 2 in $\mathrm{SL}_2(\mathbf{Z})$. See [1].

References

[1] R. C. Alperin, The Modular Tree of Pythagoras, *Amer. Math. Monthly* **112** (2005), 807–816.
[2] B. Berggren, Pytagoreiska triangular, *Tidskrift för elementär matematik, fysik och kemi* **17** (1934), 129–139.
[3] A. Hall, Genealogy of Pythagorean Triads, *The Math. Gazette* **54** (1970), 377–379.
[4] J. Roberts, "Elementary Number Theory: A Problem Oriented Approach," MIT Press, Cambridge, MA 1977.