1 Introduction

To ask for one or two Pythagorean triples is not a hard nor deep question at all. Common examples, like \((3, 4, 5)\), \((5, 12, 13)\), or \((8, 15, 17)\), can easily be found, but what if I was asked to find all the Pythagorean triples? That is precisely the motivating question for this lecture; we wish to find a way to generate all the Pythagorean triples.

**Definition 1.** A Pythagorean triple is any triple \((a, b, c)\) of integers such that \(a^2 + b^2 = c^2\). If \(\gcd(a, b, c) = 1\), then \((a, b, c)\) is a primitive Pythagorean triple.

To ask for all the Pythagorean triples is to ask for all integer solutions to the equation \(a^2 + b^2 = c^2\). Instead of solving a three-variable equation in integers, however, we can divide by \(c^2\) on both sides to get \((\frac{a}{c})^2 + (\frac{b}{c})^2 = 1\), let \(x = \frac{a}{c}\) and \(y = \frac{b}{c}\), and solve for rational solutions on the unit circle \(x^2 + y^2 = 1\). Each pair of rational solutions \((x, y)\) will correspond to exactly one primitive Pythagorean triple \((a, b, c)\).

**Exercise 1.** What is the rational pair \((x, y)\) that corresponds to the primitive Pythagorean triple \((3, 4, 5)\)?

**Definition 2.** A point \((x, y)\) is rational if both \(x\) and \(y\) are rational. A line \(l : y = mx + b\) is rational if both \(m\) and \(b\) are rational. In the same way, any other polynomial or shape is rational if all of its coefficients are rational.

**Proposition 1.** Any line drawn through two rational points is a rational line.

**Proof.** Let the two rational points be \((x_1, y_1)\) and \((x_2, y_2)\). Then the line must have the equation \(y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)\). As \(x_1, x_2, x_3, x_4\) are all rational, the line must also have rational coefficients and therefore be rational.

**Example 1.** Show that the intersection of any two rational lines must be rational.

Let one line be \(y = m_1x + b_1\) and the other be \(y = m_2x + b_2\). Then \(m_1x + b_1 = m_2x + b_2\), so \(x = \frac{b_2 - b_1}{m_1 - m_2}\). As \(b_1, b_2, m_1, m_2\) are all rational, \(x\) must also be rational and thus, \(y\) must also be rational.

**Exercise 2.** Show that if a rational quadratic and rational line intersect at exactly one point, that it must be at a rational point.
Exercise 3. Show that if a rational quadratic and rational line intersect at exactly two points, then either both points are rational or both points are irrational.


Let us return to the problem at hand. With the previous examples and exercises, we are now in a very good position to tackle the next step.

2 Method of Sweeping Lines

Lemma 1. Let \( C \) be the unit circle \( x^2 + y^2 = 1 \) and \( l \) be a line intersecting \( C \) at \((-1,0)\) and \((x,y)\) and intersecting \( x = 0 \) at \((0,t)\). Then, \((0,t)\) is rational if \((x,y)\) is rational.

Proof. If \((x,y)\) is a rational point, then Proposition 1 tells us that \( l \), a line passing through \((-1,0)\) and \((x,y)\) will also be rational. Hence, the intersection of \( l \) and \( x = 0 \) will be rational as shown in Example 1, so \((0,t)\) must be rational.

Lemma 2. Let \( C \) be the unit circle \( x^2 + y^2 = 1 \) and \( l \) be a line intersecting \( C \) at \((-1,0)\) and \((x,y)\) and intersecting \( x = 0 \) at \((0,t)\). Then, \((x,y)\) is rational if \((0,t)\) is rational.

Proof. If \((0,t)\) is a rational point, then Proposition 1 tells us that \( l \), a line passing through \((-1,0)\) and \((0,t)\), is rational. Hence, the intersection of \( l \) and \( C \) will be rational by Exercise 3, so \((x,y)\) must be rational.

Lemma 3. Let \( C \) be the unit circle \( x^2 + y^2 = 1 \) and \( l \) be a line intersecting \( C \) at \((-1,0)\) and \((x,y)\) and intersecting \( x = 0 \) at \((0,t)\). Then, \((x,y)\) is rational if and only if \( t \) is rational.
Proof. By Lemma 1 and Lemma 2, we know that \((x, y)\) is rational if and only if \((0, t)\) is rational. However, since \((0, t)\) is rational if and only if \(t\) is rational, we can conclude that \((x, y)\) is rational if and only if \(t\) is rational.

Note that if \(t = \infty\), then \((x, y) = (−1, 0)\). Therefore, we have just shown that there is a one-to-one correspondence between the rational points on the unit circle \(x^2 + y^2 = 1\) and the rational numbers. As a result, we hope to parameterize all the primitive Pythagorean triples in terms of this single variable \(t\).

**Exercise 5.** Let \(C\) be the unit circle \(x^2 + y^2 = 1\) and \(l\) be a line intersecting \(C\) at \((−1, 0)\) and \((x, y)\) and intersecting \(x = 0\) at \((0, t)\). Show that

(a) \(y = t(x + 1)\),  
(b) \(x = \frac{t^2 + 1}{t^2 + 1}\),  
(c) \(y = \frac{2t}{t^2 + 1}\).

By Exercise 5, we know that \(x = −1\) or \(x = \frac{1 - t^2}{1 + t^2}\). The solution \(x = −1\), however, simply results in the point \((−1, 0)\) that we already know of, so we choose \(x = \frac{1 - t^2}{1 + t^2}\) instead. As a result, we can generate all rational solutions to \(x^2 + y^2 = 1\) by setting \(x = \frac{1 - t^2}{1 + t^2}\) and \(y = \frac{2t}{1 + t^2}\) and plugging in rational values of \(t\). Moreover, since \(t\) is rational, \(t = \frac{m}{n}\) where \(m, n\) are relatively prime integers, so

\[
x = \frac{1 - \left(\frac{m}{n}\right)^2}{1 + \left(\frac{m}{n}\right)^2} = \frac{m^2 - n^2}{m^2 + n^2} \quad \text{and} \quad y = \frac{2\left(\frac{m}{n}\right)}{1 + \left(\frac{m}{n}\right)^2} = \frac{2mn}{m^2 + n^2}.
\]

Referring back to the beginning of the lecture, we know that \(x = \frac{a}{c}\) and \(y = \frac{b}{c}\). Therefore, \(a = m^2 - n^2\), \(b = 2mn\), and \(c = m^2 + n^2\). We can plug in relatively prime integers \(m, n\) to generate Pythagorean triples \((a, b, c)\). As we only wish to generate primitive Pythagorean triples, we choose \(m, n\) of different parity (otherwise, \(2|a\), \(2|b\), and \(2|c\)). For instance, \(m = 3, n = 2\) yields \(a = 9 - 4 = 5, b = 2(3)(2) = 12\), and \(c = 9 + 4 = 13\).

At this point, we are almost done. We have generated all primitive Pythagorean triples, so to generate all Pythagorean triples, we simply multiply \(a, b, c\) by a constant \(k\) to get

\[
a = k(m^2 - n^2), \quad b = k(2mn), \quad c = k(m^2 + n^2)
\]

3 Applications

In the process of parameterizing the Pythagorean triples, we have unveiled many useful things.

3.1 Stereographic Projection

The method we used to parameterize the Pythagorean triples is called stereographic projection. It relied on the fact that we had a rational quadratic, in our case \(x^2 + y^2 = 1\), and an initial rational point, which we chose to be \((−1, 0)\). As a result, we should be able to extend this method to other rational quadratics as long as we can find an initial solution.

**Exercise 6.** Parameterize the rational solutions to \(x^2 - 2y^2 = 1\).

**Exercise 7.** Parameterize the rational solutions to \(x^2 - 2y^2 = -1\).

**Example 2.** Solve for integer solutions to \(x^2 - 2y^2 = \pm1\).

The parameterizations for Exercise 6 and Exercise 7, respectively, should be
\[
x = \frac{t^2+2}{t^2-2}, \quad y = \frac{2t}{t^2-2} \quad \text{and} \quad x = \frac{1-2t^2}{1-2(t-1)^2}, \quad y = \frac{t^2+(t-1)^2}{1-2(t-1)^2}
\]
or
\[
x = \frac{m^2+2n^2}{m^2-2n^2}, \quad y = \frac{2mn}{m^2-2n^2} \quad \text{and} \quad x = \frac{n^2-2m^2}{n^2-2(m-n)^2}, \quad y = \frac{m^2+(m-n)^2}{n^2-2(m-n)^2}
\]
so, by making the substitution \( n \Rightarrow m \) and \( m \Rightarrow m+n \) on the right side,
\[
x = \frac{m^2+2n^2}{m^2-2n^2}, \quad y = \frac{2mn}{m^2-2n^2} \quad \text{and} \quad x = \frac{m^2-2(m+n)^2}{m^2-2n^2}, \quad y = \frac{(m+n)^2+n^2}{m^2-2n^2}.
\]

As these parameterizations give all the rational solutions, we know that the only integer solutions are when the denominator is \( \pm 1 \), or when \( m^2 - 2n^2 = \pm 1 \). Solving for integer values \( m, n \) such that \( m^2 - 2n^2 = \pm 1 \), however, is precisely the original problem we were trying to solve! As a result, if we know one solution \((x_n, y_n)\) to \(x^2 - 2y^2 = \pm 1\), we can let \( m = x_n \) and \( n = y_n \) so that the denominator is \( x^n - 2y^n = \pm 1 \). Therefore, we can generate two more integer solutions through the numerators of our parameterization:
\[
(x_{2n-1}, y_{2n-1}) = (x_n^2 + 2y_n^2, 2x_ny_n),
\]
\[
(x_{2n}, y_{2n}) = (x_n^2 - 2(x_n + y_n)^2, (x_n + y_n)^2 + y_n^2).
\]

By letting \( x_0 = 1 \) and \( y_0 = 1 \), we can successively generate all the solutions to \( x^2 - 2y^2 = \pm 1 \). Moreover, every \((x_{2n-1}, y_{2n-1})\) is a solution to \( x^2 - 2y^2 = 1 \) and every \((x_{2n}, y_{2n})\) is a solution to \( x^2 - 2y^2 = -1 \).

**Exercise 8.** Solve for integer solutions to \( x^2 - 3y^2 = \pm 1 \).

### 3.2 Parameterizing the Trigonometric Functions

Although the previous application allows for a way to solve Pell’s Equations, it takes an immense amount of work and is impractical because there are much better ways. Using the Pythagorean triples to parameterize Trigonometric functions, however, is quite useful (See [Trigonometry] if needed).

Recall this image, now with an extra line, that we used to find that \( x = \frac{1-t^2}{1+t^2} \) and \( y = \frac{2t}{1+t^2} \).
As $C$ is the unit circle, we know that $x = \cos \theta$, $y = \sin \theta$, and $t = \tan \frac{1}{2} \theta$. Hence,

$$\cos \theta = \frac{1-t^2}{1+t^2}, \quad \sin \theta = \frac{2t}{1+t^2}, \quad t = \tan \frac{1}{2} \theta.$$ \(\text{Example 3.}\) Prove that $\cos^2 \theta + \sin^2 \theta = 1$.

$$\cos^2 \theta + \sin^2 \theta = \left(\frac{1-t^2}{1+t^2}\right)^2 + \left(\frac{2t}{1+t^2}\right)^2 = \frac{t^4-2t^2+1+4t^2}{t^4+2t^2+1} = \frac{t^4+2t^2+1}{t^4+2t^2+1} = 1.$$ \(\text{Example 4.}\) Show that $\sin(\alpha + \beta) = \sin \alpha \cos \beta + \sin \beta \cos \alpha$.

Because we have multiple angles, we need different parameters for each angle. Let the parameter for angle $\alpha$ be $t_\alpha$, the parameter for angle $\beta$ be $t_\beta$, and the parameter for angle $\alpha + \beta$ be $t_{\alpha + \beta}$. Then

$$\sin(\alpha + \beta) = \frac{2t_{\alpha + \beta}}{1 + t_{\alpha + \beta}}$$

and

$$\sin \alpha \cos \beta + \sin \beta \cos \alpha = \left(\frac{2t_\alpha}{1+t_\alpha^2}\right)\left(\frac{1-t_\beta^2}{1+t_\beta^2}\right) + \left(\frac{2t_\beta}{1+t_\beta^2}\right)\left(\frac{1-t_\alpha^2}{1+t_\alpha^2}\right).$$

We wish to solve for the parameter $t_{\alpha + \beta}$ in terms of $t_\alpha$ and $t_\beta$ in order to rewrite $\sin(\alpha + \beta)$ in terms of $t_\alpha$ and $t_\beta$.

The idea is to use the fact that complex multiplication, in its vector representation, adds the angles two vectors form from the horizontal axis (See [Complex Numbers] and [Vectors] if needed). As a result, we translate our plane by 1 unit to the left so that $(-1, 0)$ becomes our origin. Under our new coordinate system, we represent $(1, t_\alpha)$ by the complex vector $1 + it_\alpha$, $(1, t_\beta)$ by $1 + it_\beta$, and $(1, t_{\alpha + \beta})$ by $1 + it_{\alpha + \beta}$. Note that the vector $1 + it_\theta$ forms an angle of $\frac{\theta}{2}$ with the horizontal axis.

As such, the vector $(1 + it_\alpha)(1 + it_\beta) = (1-t_\alpha t_\beta) + i(t_\alpha + t_\beta)$ forms an angle of $\frac{\alpha + \beta}{2}$ with the horizontal axis and is therefore parallel to $1 + it_{\alpha + \beta}$. Therefore, $\frac{(1-t_\alpha t_\beta)+i(t_\alpha + t_\beta)}{1-t_\alpha t_\beta} = 1 + i\left(\frac{t_\alpha + t_\beta}{1-t_\alpha t_\beta}\right)$ is also parallel to $1 + it_{\alpha + \beta}$, and as the real component of both vectors are equal, both vectors must be equal. Hence, the imaginary components of both vectors must also be equal so $t_{\alpha + \beta} = \frac{t_\alpha + t_\beta}{1-t_\alpha t_\beta}$.

From here, we substitute, expand, and find that

$$\sin(\alpha + \beta) = \frac{2t_{\alpha + \beta}}{1 + t_{\alpha + \beta}} = \frac{2\left(\frac{t_{\alpha + \beta}}{1-t_\alpha t_\beta}\right)}{1\left(\frac{t_{\alpha + \beta}}{1-t_\alpha t_\beta}\right)} = \left(\frac{2t_\alpha}{1+t_\alpha^2}\right)\left(\frac{1-t_\beta^2}{1+t_\beta^2}\right) + \left(\frac{2t_\beta}{1+t_\beta^2}\right)\left(\frac{1-t_\alpha^2}{1+t_\alpha^2}\right) = \sin \alpha \cos \beta + \sin \beta \cos \alpha$$

\(\text{Exercise 9.}\) Show that $\cos(\alpha + \beta) = \cos \alpha \cos \beta - \sin \alpha \sin \beta$.

I will leave off with a final use for the Trigonometric parameterizations. As $t = \tan \frac{1}{2} \theta$, we know that $\tan^{-1} t = \frac{1}{2} \theta$ so $\frac{1}{2} \cdot \frac{d\theta}{dt} = \frac{1}{1+t^2}$. Hence, $d\theta = \frac{2dt}{1+t^2}$. This allows us to use our Trig parameterizations to change any integral in terms of Trig functions and $d\theta$ into an integral in $dt$. 
