Name: _____

UW Math Circle

Week 25 – Diophantine Equations

Today, we will talk about Diophantine equations and some interesting applications!

1 Diophantine Equations

Before we start, we will need some definitions.

- The *integers*, denoted $\mathbb{Z}$, is the set of positive and negative whole numbers, along with 0, i.e. $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
- The *rational numbers*, denoted $\mathbb{Q}$, is the set of fractions of integers, i.e. $\mathbb{Q} = \{\frac{a}{b} : a, b \text{ are integers}\}$
- A *polynomial* is a sum of products and non-negative powers of variables. For example, $x^2 + 3yz - 10$ is a polynomial in the variables x, y, z. The expressions $\sin(x) - z^3$ and $\frac{y}{x}$ are not polynomials.

A *Diophantine equation* is an equation of the form $f = 0$ where f is a polynomial and all the coefficients of f are integers, and where we are interested in the solutions which are integers (called *integral* solutions). For example, $x^2 - 1 = 0$ is a Diophantine equation with integral solutions $1, -1$.

Diophantine equations derive their name from the Greek mathematician Diophantus of Alexandria, who lived some time between 150 and 350 CE. Diophantus wrote a treatise, called *Arithmetica*, on what are now called Diophantine equations.

1. What are the integral solutions to the following Diophantine equations?

   (a) $x - y = 0$

   (b) $z^2 = 0$

   (c) $x^2 + y^2 - 1 = 0$
   Hint: Draw a picture.

2. Do the following Diophantine equations have any solutions? Are there any integer solutions?

   (a) $3x - 1 = 0$

   (b) $x^2 - 2 = 0$

   (c) $x^2 + 1 = 0$

3. Rewrite the following equations as Diophantine equations of the form $f = 0$. What are the integral solutions?

   (a) $x^2 = 4$

   (b) $\frac{1}{2}x = 1$

   (c) $\frac{x^4}{30} - \frac{x^2}{3} + \frac{5}{6} = 0$

   (d) $3\frac{x}{y} + \frac{y}{3x} = \frac{3}{xy}$

   (e) $\frac{1}{x} = \frac{x}{y} + \frac{1}{xy}$

4. Do the following equations correspond to a Diophantine equation? If so, is the solution set of each equation below the same as the solution set of the corresponding Diophantine equation?

   (a) $\frac{x}{y} = 0$

   (b) $\frac{x}{y} = 1$

   (c) $\frac{x}{y} - 2 = -\frac{y}{x}$

2 Some History

A famous Diophantine equation is the following: $x^n + y^n = z^n$. When $n = 2$, positive integer solutions are called *Pythagorean triples*, because they are the sidelengths of a right triangle, and the equation becomes the Pythagorean Theorem. For $n > 2$, there are no integral solutions at all; this is known as *Fermat's Last Theorem*. In the 1630's, Pierre de Fermat wrote the following note in the margins of his copy of Diophantus' *Arithmetica*:

> "It is impossible... for any number which is a power greater than the second to be written as the sum of two like powers
> [$x^n + y^n = z^n$ for $n > 2$]. I have a truly marvelous demonstration of this proposition which this margin is too narrow to contain."

This note was discovered by his son thirty years after Fermat's death, but Fermat seems not to have written down his proof. The theorem was not completely proven until some three and a half centuries later. Many mathematicians worked on Fermat's Last Theorem, and the final piece of the puzzle was put into place by a British mathematician named Andrew Wiles in 1995.

We will now investigate the $n = 2$ case, i.e. the Pythagorean Theorem.

3 The Pythagorean Theorem

If you haven't seen it before, the Pythagorean Theorem states that if a, b are two legs (shorter sides) of a right triangle and c is the hypotenuse (longest side), then $a^2+b^2 = c^2$. Pythagoras of Samos was a Greek mathematician who lived in the 6th century BCE, roughly eight centuries before Diophantus. He is likely not the first person to have proven the theorem that bears his name.

5. Can you find a right triangle with integral legs but non-integral hypotenuse? Is the hypotenuse rational?

6. Suppose (a, b, c) is a Pythagorean triple and $k > 0$

   (a) When is (ka, kb, kc) a Pythagorean triple?

   (b) Can you explain your answer geometrically?

   (c) Algebraically?

7. Say $m > n > 0$ are integers. If one of the legs of a right triangle has length $m^2 - n^2$ and the other has length $2mn$, what is the length of the hypotenuse?

8. What happens if m, n are both odd? What happens if they're both even?

9. For two integers a, b, we say b *divides* a if we can write $a = b \cdot c$ where c is also an integer. We write $b \mid a$ to denote b divides a. For example, 2 divides 6 because $6 = 2 \cdot 3$, so we write $2 \mid 6$. The *greatest common divisor* of two integers a, b, written $\gcd(a, b)$ is the greatest d such that $d \mid a$ and $d \mid b$. Find the greatest common divisor of the following pairs of numbers

   (a) $\gcd(2, 4) =$

   (b) $\gcd(5, 5) =$

   (c) $\gcd(15, 6) =$

   (d) $\gcd(0, 14) =$

   (e) $\gcd(1, 9) =$

   (f) $\gcd(2, 3) =$

   (g) $\gcd(123456789, 123456789) =$

   (h) $\gcd(1, 0) =$

   (i) $\gcd(0, 0) =$

10. Two numbers a, b are *coprime* if their greatest common divisor is 1. Three numbers a, b, c are coprime if all three pairs of gcd's are 1, i.e.

$$\gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1.$$

    A Pythagorean triple (a, b, c) is *primitive* if a, b, c are coprime.

    (a) Is $(3, 4, 5)$ primitive?

    (b) Is $(7, 24, 25)$ primitive?

    (c) Is $(45, 24, 51)$ primitive?

11. Let (a, b, c) be a Pythagorean triple.

    (a) Is it possible for exactly one pair of these numbers to be coprime? For example, is it possible to have $\gcd(a, b) = 1,\ \gcd(a, c) = j > 1,\ \gcd(b, c) = k > 1$? If so, give an example.

    (b) Is it possible for exactly two pairs of these numbers to be coprime? For example, is it possible to have $\gcd(a, b) = \gcd(a, c) = 1,\ \gcd(b, c) = j > 1$? If so, give an example.

12. Challenge Problem: Given m, n with $m > n > 0$, you showed in 7 that $(m^2 - n^2, 2mn, m^2 + n^2)$ was a Pythagorean triple. When do m, n generate a primitive Pythagorean triple in this way?

3.1 Parametrizing Pythagorean Triples

Let's take another view of primitive Pythagorean triples. If (a, b, c) is a primitive Pythagorean triple, then $(\frac{a}{c}, \frac{b}{c}, 1)$ are the side lengths of a right triangle with hypotenuse 1. If we put one corner at the origin and put the leg of length $\frac{a}{c}$ on the x-axis, as in Figure 1 then the remaining corner will land exactly on the unit circle! We can see this

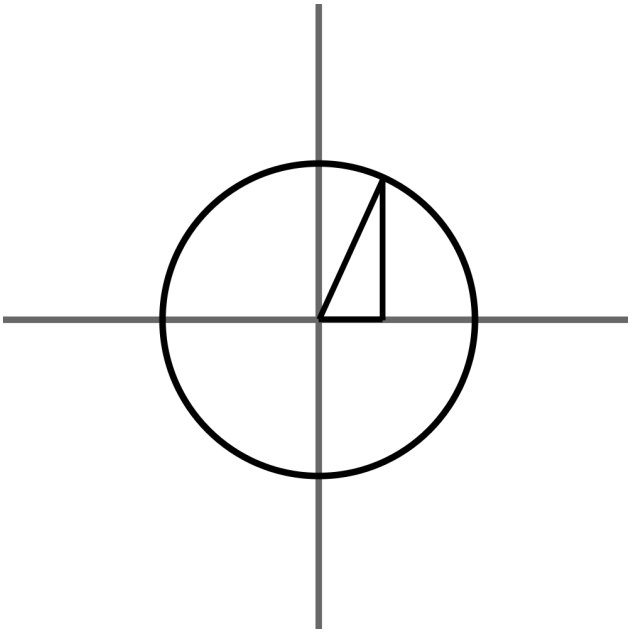


Figure 1: a triangle on the unit circle

algebraically because $x^2 + y^2 = 1$ is the equation of the circle.

13. Call a fraction $\frac{a}{b}$ *reduced* if $\gcd(a, b) = 1$. If $\frac{a}{b}$ is not reduced, then $a = j \cdot \gcd(a, b)$ and $b = k \cdot \gcd(a, b)$, so $\frac{a}{b} = \frac{j}{k}$. Use your answer from question 11 to show that any point on the unit circle of the form $(\frac{a}{b}, \frac{c}{d})$, where $\frac{a}{b}$ and $\frac{c}{d}$ are reduced, must satisfy $\gcd(a, c) = 1$ and $b = d$.

14. We can parametrize the unit circle as follows: for any real number t, the line connecting $(-1, 0)$ and $(0, t)$ will pass through the unit circle in a third point, as seen in Figure 2 . The coordinates of this point are $(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2})$. Call this point $f(t)$. Check that $f(t)$ really is on the unit circle for all t.

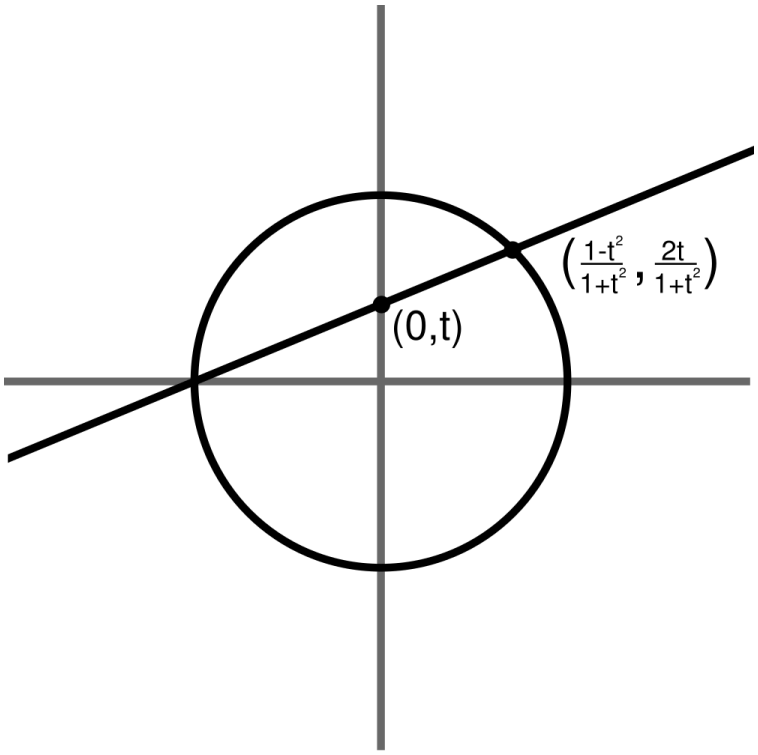


Figure 2: parametrizing the unit circle

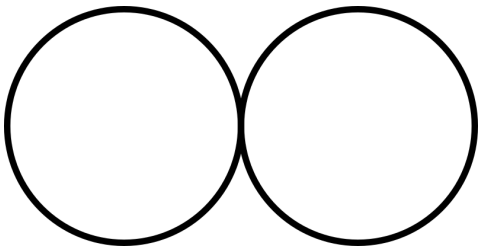
15. Every point on the circle is equal to $f(t)$ for some t, with the exception of $(-1, 0)$. This function f from the real numbers to the circle has an inverse; given a point (x, y) on the unit circle, define $g(x, y)$ to be $\frac{y}{x+1}$. Check that g and f are inverses, namely

$$f(g(x, y)) = (x, y)$$
$$g(f(t)) = t.$$

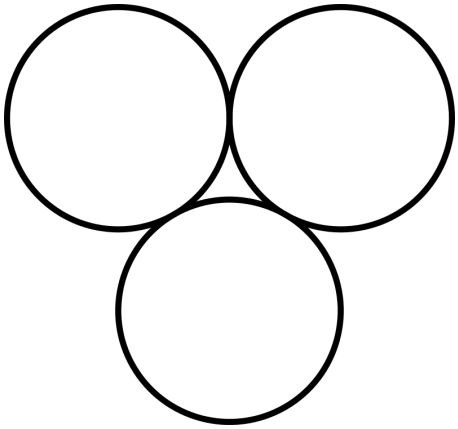
16. Show that the rational points of the circle are parametrized exactly, via f and g, by the rational numbers $\mathbb{Q}$.

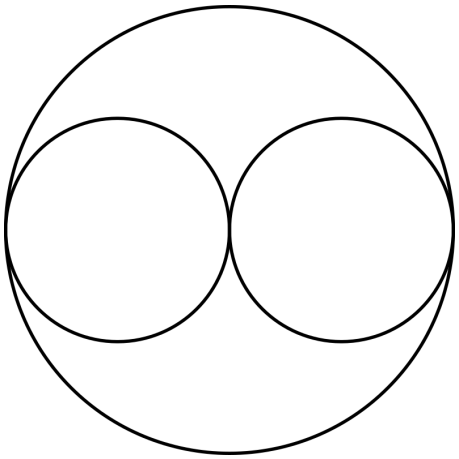
4 Apollonian Circle Packings

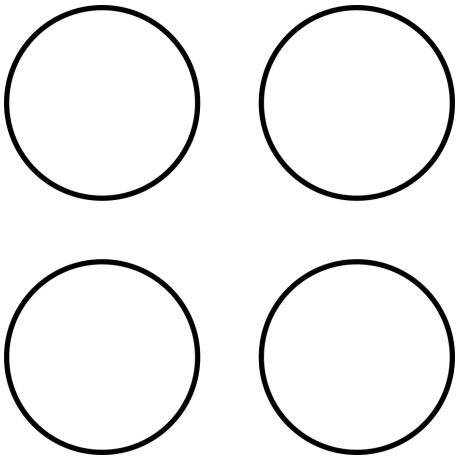
17. Two circles in the plane are *tangent* if they touch at exactly one point. The two circles below are tangent. How many different circles can you draw that are tangent to both?

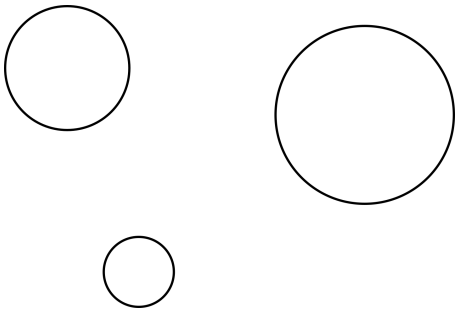


18. How many circles can you draw that are tangent to all of the following sets of circles?







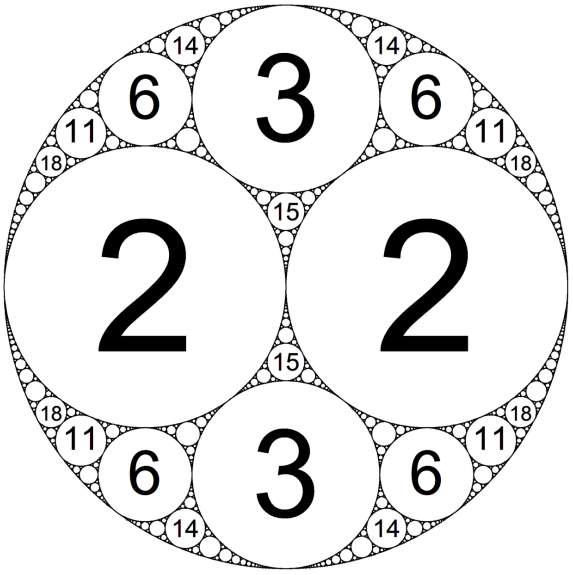


Apollonius of Perga, a Greek mathematician who lived in the third century BCE, posed and solved the problem of finding all the circles tangent to three given circles.

19. Given a circle C of radius r, the *curvature* of C is defined to be $\frac{1}{r}$. In 1643, French mathematician René Descartes stated the following theorem: Given four mutually tangent circles (i.e., every pair of circles are tangent), their curvatures k_1, k_2, k_3, k_4 satisfy the equation

$$(k_1 + k_2 + k_3 + k_4)^2 = 2\left(k_1^2 + k_2^2 + k_3^2 + k_4^2\right)$$

For example, in the picture below the curvatures of the four largest circles (including the circle all others are contained inside) are $-1, 2, 2, 3$.



Negative curvature means that the other circles are contained inside that circle. Check that the picture is correct, i.e. that $-1, 2, 2, 3$ satisfy Descartes' theorem. Check one other collection of four mutually tangent circles.

20. Given k_1, k_2, and k_3, the two possible values of k_4 are

$$k_4 = k_1 + k_2 + k_3 + 2\sqrt{k_1k_2 + k_2k_3 + k_1k_3}$$
$$k_4 = k_1 + k_2 + k_3 - 2\sqrt{k_1k_2 + k_2k_3 + k_1k_3}.$$

If k_1, k_2, and k_3 are integers and one solution is an integer, will the other also be an integer?