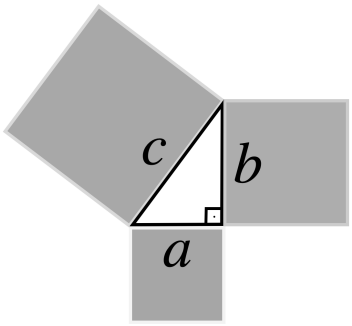
Arithmetic Geometry

By DiBeos

This video was based on the Princeton Companion to Mathematics.

Let's start with something basic: the right triangle. We know that the square of the length of the hypotenuse is equal to the sum of the squares of the lengths of the other two sides.



This can be written as an equation $a^2 + b^2 = c^2$. This theorem has been proven many times using different methods, and we won't go into them. What's important to note is that there are infinitely many solutions to this equation

This is because we can use these formulas, which generate all primitive Pythagorean triples (triples where (a), (b), and (c) are coprime, i.e., have no common factor other than 1):

$$a = m^2 - n^2 \qquad b = 2mn \qquad c = m^2 + n^2$$

m and n are positive integers

$$m > n > 0$$

m and n have opposite parity

m and n are coprime.

By substituting different values of m and n, we can get all of these different examples:

When m = 2, n = 1 : the result is (3, 4, 5)

$a = 2^2 - 1^2 = 3 \qquad b = 2 \cdot 2 \cdot 1 = 4 \qquad c = 2^2 + 1^2 = 5$

When m = 3, n = 2 : the result is (5, 12, 13)

$a = 3^2 - 2^2 = 5 \qquad b = 2 \cdot 3 \cdot 2 = 12 \qquad c = 3^2 + 2^2 = 13$

When m = 4, n = 1 : the result is (15, 8, 17)

$a = 4^2 - 1^2 = 15 \qquad b = 2 \cdot 4 \cdot 1 = 8 \qquad c = 4^2 + 1^2 = 17$

Now, let's change that equation a little bit, and insert a 7 in there. We'll replace a b c with x y and z.

$x^2 + y^2 = 7z^2$

What we will do with just this simple equation will demonstrate the essential ideas we need of arithmetic geometry.

The only difference between this equation and the Pythagorean equation is that the coefficient 1 was replaced with 7.

We want to show that $x^2 + y^2 = 7z^2$ has no solution in nonzero rational numbers x, y and z.

Rational Numbers meaning numbers of the form $\frac{p}{q}$, where p and q are integers and $q \neq 0$.

The equation is a **Diophantine equation**, a type of equation where we seek integer or rational solutions. If no such rational solutions exist, the equation is unsolvable in rational numbers.

Now, suppose x, y and z are rational numbers that satisfy the equation, will we get to a contradiction?

If *n* is the least common denominator of x y and z we can write that $x = \frac{a}{n}$, $y = \frac{b}{n}$, $z = \frac{c}{n}$ such that a b c and n are integers. Now, our original equation has become this:

$$\left(\frac{a}{n}\right)^2 + \left(\frac{b}{n}\right)^2 = 7\left(\frac{c}{n}\right)^2$$

By multiplying through n^2, it becomes

$a^2 + b^2 = 7c^2$

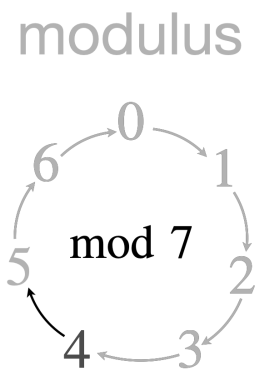
If these have a common factor m, we're able to replace them by $a/m,\ b/m$ and c/m and the new equation $a^2 + b^2 = 7c^2$ still holds for these new numbers. We may therefore suppose that *a*, *b*, and *c* are integers with no common factor.

Now here's something interesting we can do: arithmetic geometry frequently uses the local-to-global principle, meaning that by checking solutions modulo 7 (a local property), we deduce global consequences: if no solutions exist modulo 7, then no integer solutions exist globally. Here, we will reduce the equation modulo 7.

By reducing modulo 7, we check whether the equation is even consistent within this modular system. If no solutions exist modulo 7, then there cannot be any integer (or rational) solutions in general. The reduction modulo 7 is natural here because the coefficient 7 appears explicitly in $7c^2$.

Quickly, modular arithmetic is basically reducing our available numbers to a certain value called the modulus. In our case 7. So 5+6 mod 7 = 11 mod 7 = 4. And this can be done for any operation, multiplication, subtraction, etc.

$$5 + 6 = 11 \equiv 4 \mod 7$$



Since 7 is divisible by 7, we know that:

$7 \equiv 0\ mod\ 7$.

So, for $7c^2$, no matter what c^2 is, the product $7c^2$ is still divisible by 7, which means $7c^2 \equiv 0\ mod\ 7$.

Now the equation becomes $\bar{a}^2 + \bar{b}^2 = 0\ (mod\ 7)$, where $\bar{a}$ and $\bar{b}$ are the reductions of a and b modulo 7. Now we only have seven possibilities of $\bar{a}$ and seven possibilities for $\bar{b}$.

So the analysis of the solutions of $\bar{a}^2 + \bar{b}^2 = 0 \ (mod\ 7)$ amounts to checking the forty-nine choices of $\bar{a}$ and $\bar{b}$ and seeing which ones satisfy the equation. If you actually calculate it, you'll find that the only solution to the equation $\bar{a}^2 + \bar{b}^2 = 0 \ (mod\ 7)$ is if everything equals 0.

Saying $\bar{a} = 0$ and similarly $\bar{b} = 0$ means that a and b leave no remainder when divided by 7. This is exactly the same as saying that a and b are both multiples of 7.

When this is true, it means that a^2 and b^2 are multiples of 49, since the a and b are squared. It follows that their sum $7c^2$ is a multiple of 49 as well. Therefore, c^2 is a multiple of 7, and this implies that *c* itself is a multiple of 7. Specifically, $a,\ b$ and c share a common factor of 7.

This is a contradiction of something we said earlier: that in the equation $a^2 + b^2 = 7c^2$, we supposed that *a*, *b*, and *c* are integers with **no common factor**.

But here we proved that they actually have a common factor. Because of this contradiction, we have to conclude that there is not, in fact, any solution to $x^2 + y^2 = 7z^2$ consisting of nonzero rational numbers.

In general, the determination of rational solutions to a polynomial equation like $x^2 + y^2 = 7z^2$ is called a *Diophantine problem*. We were able to dispose of the equation pretty quickly, but that turns out to be the exception: in general, Diophantine problems can be extraordinarily difficult.

For instance, we might modify the exponents in $x^2 + y^2 = 7z^2$ and consider the equation

$$x^5 + y^5 = 7c^5$$

I don't actually know whether it has any solutions in nonzero rational numbers. But you can be sure that it would be a piece of work, and it's even possible that the most powerful techniques available to us might not be enough to answer this simple question. Fermat's Last Theorem is an example.

The primary question—whether $x^2 + y^2 = 7z^2$ has nonzero rational solutions—is a classic Diophantine problem, central to Arithmetic Geometry. Techniques such as modular arithmetic, properties of divisibility (e.g., $7z^2 \Rightarrow z$ is divisible by 7) demonstrate how local properties (e.g., modulo primes) influence global conclusions (so the nonexistence of rational solutions).

Though it is not obvious so far, the solution of Diophantine problems is properly classified as part of geometry, because their solutions can be interpreted as points on a geometric object. Which is why this entire thing is called Arithmetic Geometry.

Technically speaking, our equation $x^2 + y^2 = 7z^2$ defines a quadratic curve (specifically, a conic section) in the projective plane $\mathbb{P}^2$.

Finding rational or integer solutions to the equation is equivalent to finding rational points on this curve. However, the failure of $x^2 + y^2 = 7z^2$ to have nonzero rational number solutions corresponds to the non-existence of rational points. We can essentially throw our geometric intuition in the trash when solving it. This is an example of the principle often referred to as **"geometry without geometry"**, where the tools of arithmetic and algebra are sufficient to fully address the problem, making classical geometric interpretation unnecessary.

If we had an equation like $x^2 + y^2 = 1$ we would find that it has infinitely many rational solutions. But geometrically, it describes a circle in real numbers.

Although we solved the problem over $\mathbb{Z}$ and $\mathbb{Q}$, meaning that we were constrained to these specific number systems, the equation can be analyzed over other algebraic structures, like finite fields $\mathbb{Z}/p\mathbb{Z}$ (integers modulo 7), the equation $x^2 + y^2 \equiv 0 \ (mod\ 7)$ has no solutions except when $x \equiv y \equiv 0$. Or polynomials with complex coefficients $\mathbb{C}[t]$, where solutions can be parametrized as $x(t),\ y(t),\ z(t)$, linking arithmetic and geometry in a broader sense.