Unfolding Pythagorean Triples from the Unit Circle

Sayan Dutta

Department of Mathematics and Statistics
Indian Institute of Science Education and Research, Kolkata

April 14, 2022

IISER KOLKATA

Table of Contents

Introduction

We want to find all the integer solutions to the equation

$$X^2 + Y^2 = Z^2 \tag{1}$$

Introduction

We want to find all the integer solutions to the equation

$$X^2 + Y^2 = Z^2 \tag{1}$$

We will focus mainly on the solutions that satisfy one more condition, namely,

$$\gcd(x, y, z) = 1$$

Introduction

We want to find all the integer solutions to the equation

$$X^2 + Y^2 = Z^2 \tag{1}$$

We will focus mainly on the solutions that satisfy one more condition, namely,

$$\gcd(x, y, z) = 1$$

These solutions are called *primitive solutions*.

Rational Hunt

Let us divide (1) by Z^2, set $x = X/Z$, $y = Y/Z$ and look at the equation

$$x^2 + y^2 = 1 \tag{2}$$

Let us divide (1) by Z^2, set $x = X/Z$, $y = Y/Z$ and look at the equation

$$x^2 + y^2 = 1 \tag{2}$$

We only need to find all the rational solutions of (2).

Rational Hunt

Let us divide (1) by Z^2, set $x = X/Z$, $y = Y/Z$ and look at the equation

$$x^2 + y^2 = 1 \tag{2}$$

We only need to find all the rational solutions of (2).
Clearly, $(-1, 0)$ is one such solution.

Rational Hunt

Let us divide (1) by Z^2, set $x = X/Z$, $y = Y/Z$ and look at the equation

$$x^2 + y^2 = 1 \tag{2}$$

We only need to find all the rational solutions of (2).
Clearly, $(-1, 0)$ is one such solution.

If (u, v) is another rational solution of (2), we can join these two points and get the straight line

$$y = \frac{v}{u+1}(x+1)$$

Rational Hunt continues

This straight line has a *rational* slope

$$t = \frac{v}{u+1}$$

Rational Hunt continues

This straight line has a *rational* slope

$$t = \frac{v}{u+1}$$

This line meets the Y-axis at the *rational* point $(0, t)$.

Rational Hunt continues

This straight line has a *rational* slope

$$t = \frac{v}{u+1}$$

This line meets the Y-axis at the *rational* point $(0, t)$.

The converse of this is also true. The line through $(-1, 0)$ having a rational slope t is given by

$$y = t(x+1)$$

Rational Hunt continues

This straight line has a *rational* slope

$$t = \frac{v}{u+1}$$

This line meets the Y-axis at the *rational* point $(0, t)$.

The converse of this is also true. The line through $(-1, 0)$ having a rational slope t is given by

$$y = t(x+1)$$

Plugging this into (2), we get

$$x^2 + t^2(x+1)^2 = 1, \qquad x = -1, \ \frac{1-t^2}{1+t^2}$$

Rational treasure found

So, $y = t(x+1)$ meets the unit circle at the *rational* point

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \tag{3}$$

Rational treasure found

So, $y = t(x+1)$ meets the unit circle at the *rational* point

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \tag{3}$$

So, by drawing **all** such lines of rational slope, we can be sure that we have accounted for **every** rational point on our circle!

Integer Hunt

Integer Hunt

X	Y	Possible?	Reason
even	even	✗	$\gcd(x, y, z) = 1$

Integer Hunt

X	Y	Possible?	Reason
even	even	✗	$\gcd(x, y, z) = 1$
odd	odd	✗	$Z^2 = X^2 + Y^2 \equiv 2 \pmod 4$

Integer Hunt

X	Y	Possible?	Reason
even	even	✗	$\gcd(x, y, z) = 1$
odd	odd	✗	$Z^2 = X^2 + Y^2 \equiv 2 \pmod 4$
odd	even	✓	$(3, 4, 5)$ is one such solution

Integer Hunt

X	Y	Possible?	Reason
even	even	✗	$\gcd(x, y, z) = 1$
odd	odd	✗	$Z^2 = X^2 + Y^2 \equiv 2 \pmod 4$
odd	even	✓	$(3, 4, 5)$ is one such solution
even	odd	✓	$(4, 3, 5)$ is one such solution

Parity Analysis

Integer Hunt continues

Given a rational point (x, y) parameterized by t, write $t = m/n$ in its lowest terms, i.e. $\gcd(m, n) = 1$.

Integer Hunt continues

Given a rational point (x, y) parameterized by t, write $t = m/n$ in its lowest terms, i.e. $\gcd(m, n) = 1$.Plugging this into (3), we have

$$x = \frac{X}{Z} = \frac{m^2 - n^2}{m^2 + n^2}, \qquad y = \frac{Y}{Z} = \frac{2mn}{m^2 + n^2}$$

Integer Hunt continues

Given a rational point (x, y) parameterized by t, write $t = m/n$ in its lowest terms, i.e. $\gcd(m, n) = 1$.Plugging this into (3), we have

$$x = \frac{X}{Z} = \frac{m^2 - n^2}{m^2 + n^2}, \qquad y = \frac{Y}{Z} = \frac{2mn}{m^2 + n^2}$$

So, there must be some integer k such that

$$kX = m^2 - n^2, \qquad kY = 2mn, \qquad kZ = m^2 + n^2$$

Integer treasure found

Now,

$$\begin{aligned} & k \mid m^2 - n^2 \quad \text{and} \quad k \mid m^2 + n^2 \\ \Rightarrow \quad & k \mid 2m^2 \qquad\quad \text{and} \quad k \mid 2n^2 \\ \Rightarrow \quad & k \mid 2 \end{aligned}$$

Integer treasure found

Now,

$$\begin{aligned} & k \mid m^2 - n^2 \quad \text{and} \quad k \mid m^2 + n^2 \\ \Rightarrow \quad & k \mid 2m^2 \qquad\quad \text{and} \quad k \mid 2n^2 \\ \Rightarrow \quad & k \mid 2 \end{aligned}$$

Thus, $k = 1$ or $k = 2$.

Integer treasure found

Now,

$$\begin{aligned} & k \mid m^2 - n^2 \;\text{ and }\; k \mid m^2 + n^2 \\ \Rightarrow\quad & k \mid 2m^2 \qquad\;\text{ and }\; k \mid 2n^2 \\ \Rightarrow\quad & k \mid 2 \end{aligned}$$

Thus, $k = 1$ or $k = 2$.

But, if $k = 2$, then

$$\begin{aligned} 2X &= m^2 - n^2 \\ \implies \quad 2 &\equiv m^2 - n^2 \pmod 4 \end{aligned}$$

Integer treasure found

Now,

$$\begin{aligned} & k \mid m^2 - n^2 \ \text{ and } \ k \mid m^2 + n^2 \\ \Rightarrow \quad & k \mid 2m^2 \qquad \text{ and } \ k \mid 2n^2 \\ \Rightarrow \quad & k \mid 2 \end{aligned}$$

Thus, $k = 1$ or $k = 2$.

But, if $k = 2$, then

$$\begin{aligned} & 2X = m^2 - n^2 \\ \implies \quad & 2 \equiv m^2 - n^2 \pmod 4 \end{aligned}$$

which is a contradiction.

Integer treasure found

Now,

$$\begin{aligned} & k \mid m^2 - n^2 \;\text{ and }\; k \mid m^2 + n^2 \\ \Rightarrow \quad & k \mid 2m^2 \qquad \text{ and }\; k \mid 2n^2 \\ \Rightarrow \quad & k \mid 2 \end{aligned}$$

Thus, $k = 1$ or $k = 2$.

But, if $k = 2$, then

$$\begin{aligned} 2X &= m^2 - n^2 \\ \implies \quad 2 &\equiv m^2 - n^2 \pmod 4 \end{aligned}$$

which is a contradiction.

Hence, we must have $k = 1$.

Final Parametrization

Plugging in $k = 1$, we get the final solution as

$$(X, Y, Z) = (m^2 - n^2, 2mn, m^2 + n^2)$$

for coprime m, n, one odd and the other even.

Jargon

1. Rational points are those of the form (p, q) with $p, q \in \mathbb{Q}$.
2. Rational lines are those of the form $ax + by + c = 0$ with $a, b, c \in \mathbb{Q}$.
3. Rational conics are those of the form $ax^2 + bxy + cy^2 + dx + fy + g = 0$ with $a, b, c, d, f, g \in \mathbb{Q}$.

Jargon

1. Rational points are those of the form (p, q) with $p, q \in \mathbb{Q}$.
2. Rational lines are those of the form $ax + by + c = 0$ with $a, b, c \in \mathbb{Q}$.
3. Rational conics are those of the form $ax^2 + bxy + cy^2 + dx + fy + g = 0$ with $a, b, c, d, f, g \in \mathbb{Q}$.

Some observations:

1. A line passing through two rational points is a rational line.
2. Two rational lines intersect at a rational point.
3. A rational conic and a rational line (and hence, two rational conics) **may not** intersect at rational points.
   For example, $y = x^2 + 1$ and $y = x + 2$ intersects at $x = \frac{1 \pm \sqrt{5}}{2}$.

An Interesting Question

We want to address the question of whether we can generalize these tricks to find integer solutions to any equation of the form

$$X^2 + Y^2 = nZ^2$$

for some integer n.

An Interesting Question

We want to address the question of whether we can generalize these tricks to find integer solutions to any equation of the form

$$X^2 + Y^2 = nZ^2$$

for some integer n.

It can be done iff there are integers s and t such that $n = s^2 + t^2$.

An Interesting Question

We want to address the question of whether we can generalize these tricks to find integer solutions to any equation of the form

$$X^2 + Y^2 = nZ^2$$

for some integer n.

It can be done iff there are integers s and t such that $n = s^2 + t^2$.

Let us note that, if $n = s^2 + t^2$, then

$$X^2 + Y^2 = (s^2 + t^2)Z^2 = (sZ)^2 + (tZ)^2$$

and hence, $(X, Y) = (sZ, tZ)$ is a solution.

The (not so) Interesting Expression

And, if the equation has a non-trivial integer solution (x, y, z), then

$$x^2 + y^2 = nz^2$$

and so nz^2 is a sum of two squares.

The (not so) Interesting Expression

And, if the equation has a non-trivial integer solution (x, y, z), then

$$x^2 + y^2 = nz^2$$

and so nz^2 is a sum of two squares.
But, since the squarefree part of nz^2 is same as the squarefree part of n, our n must also be a sum of squares.

The (not so) Interesting Expression

And, if the equation has a non-trivial integer solution (x, y, z), then

$$x^2 + y^2 = nz^2$$

and so nz^2 is a sum of two squares.
But, since the squarefree part of nz^2 is same as the squarefree part of n, our n must also be a sum of squares.

And, in that case, given one primitive non-trivial solution (x_0, y_0, z_0), the others are given by the parametrization

The (not so) Interesting Expression

And, if the equation has a non-trivial integer solution (x, y, z), then

$$x^2 + y^2 = nz^2$$

and so nz^2 is a sum of two squares.
But, since the squarefree part of nz^2 is same as the squarefree part of n, our n must also be a sum of squares.

And, in that case, given one primitive non-trivial solution (x_0, y_0, z_0), the others are given by the parametrization

$$\begin{aligned} x &= x_0 np^2 - 2qnz_0 p + 2q^2 y_0 \\ y &= y_0 np^2 - 2qnz_0 p + 2q^2 x_0 \\ z &= z_0 np^2 - 2qx_0 p - 2qy_0 p + 2q^2 z_0 \end{aligned}$$

Another interesting Question

Another interesting Question

Now, we want to ask whether the equation

$$aX^2 + bY^2 = cZ^2$$

has integer solutions.

Another interesting Question

Now, we want to ask whether the equation

$$aX^2 + bY^2 = cZ^2$$

has integer solutions.

We basically want to find at least one rational point on the ellipse

$$ax^2 + by^2 = c$$

Another interesting Question

Now, we want to ask whether the equation

$$aX^2 + bY^2 = cZ^2$$

has integer solutions.

We basically want to find at least one rational point on the ellipse

$$ax^2 + by^2 = c$$

and this turns out to be much more difficult than the last one.

Another Interesting Answer

Another Interesting Answer

Theorem (Legendre)

Let a, b, c be coprime positive integers. Then, the equation

$$aX^2 + bY^2 = cZ^2$$

has a non-trivial rational solution iff

$$\left(\frac{-bc}{a}\right) = \left(\frac{-ac}{b}\right) = \left(\frac{ab}{c}\right) = 1$$

Jacobi Symbol

Definition (Jacobi Symbol)

The Jacobi Symbol written as $\left(\frac{n}{m}\right)$ is defined for positive odd m as

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1} \left(\frac{n}{p_2}\right)^{a_2} \cdots \left(\frac{n}{p_k}\right)^{a_k}$$

where $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $\left(\frac{n}{p_1}\right)$ is the Legendre symbol.

Jacobi Symbol

Definition (Jacobi Symbol)

The Jacobi Symbol written as $\left(\frac{n}{m}\right)$ is defined for positive odd m as

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{a_1} \left(\frac{n}{p_2}\right)^{a_2} \cdots \left(\frac{n}{p_k}\right)^{a_k}$$

where $m = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ and $\left(\frac{n}{p_1}\right)$ is the Legendre symbol.

Definition (Legendre Symbol)

For an odd prime p and an integer a, we define the Legendre Symbol of a with respect to p as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p \text{ and } a \not\equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p \\ 0 & \text{if } a \equiv 0 \pmod{p} \end{cases}$$

Another Interesting Answer

Theorem (Legendre)

Let a, b, c be coprime positive integers. Then, the equation

$$aX^2 + bY^2 = cZ^2$$

has a non-trivial rational solution iff

$$\left(\frac{-bc}{a}\right) = \left(\frac{-ac}{b}\right) = \left(\frac{ab}{c}\right) = 1$$

Another Interesting Answer

Theorem (Legendre)

Let a, b, c be coprime positive integers. Then, the equation

$$aX^2 + bY^2 = cZ^2$$

has a non-trivial rational solution iff

$$\left(\frac{-bc}{a}\right) = \left(\frac{-ac}{b}\right) = \left(\frac{ab}{c}\right) = 1$$

Theorem (Hasse)

A homogeneous quadratic equation in several variables is solvable by integers, not all zero, if and only if it is solvable in real numbers and in p-adic numbers for each prime p.

Fermat's Last Theorem

Can we use this method to see whether the equation

$$X^3 + Y^3 = Z^3$$

has an integer solution?

Fermat's Last Theorem

Can we use this method to see whether the equation

$$X^3 + Y^3 = Z^3$$

has an integer solution?That is, can we ask whether the equation

$$x^3 + y^3 = 1$$

has a rational solution?

Fermat's Last Theorem

Can we use this method to see whether the equation

$$X^3 + Y^3 = Z^3$$

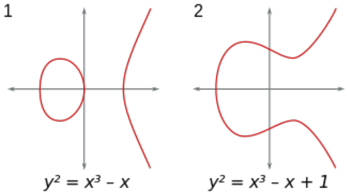
has an integer solution?That is, can we ask whether the equation

$$x^3 + y^3 = 1$$

has a rational solution?

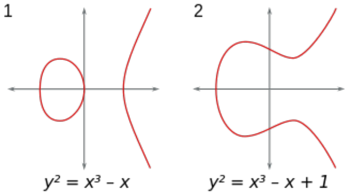
Sadly, we cannot directly use the geometric principle that worked so well for conics because a line generally meets a cubic in three points. And if we have one rational point, we cannot project the cubic onto a line, because each point on the line would then correspond to two points on the curve.

Why Rational points?

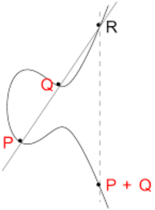


Elliptic Curves

Why Rational points?



Elliptic Curves



Rational Points on Elliptic Curves

Love Poems

Love Poems

Theorem (Mordell)

Let C be a non-singular cubic curve with rational coefficients. Then the group Γ of rational points on C is finitely generated.

Love Poems

Theorem (Mordell)

Let C be a non-singular cubic curve with rational coefficients. Then the group Γ of rational points on C is finitely generated.

Theorem (Nagell-Lutz)

Let

$$y^2 = x^3 + ax^2 + bx + c$$

be a non-singular cubic curve with integer coefficients a, b, c, and let D be the discriminant of the cubic polynomial

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

Let $P = (x, y)$ be a rational point of finite order. Then x and y are integers, and either $y = 0$, or $y | D$.

Thank You!

References

1. Rational Points on Elliptic Curves
   Joseph H. Silverman, John Tate

2. The Desmos Animation

3. Square modulo 4 animation by Satvik Saha

4. Legendre's Theorem