What is number theory:

Study of arithmetic properties of the integers.

- Primes: How they're distributed

\[ \pi(x) = \text{number of prime numbers } p \leq x \]

\[ \text{Fact: } \pi(x) \text{ approximated by } \frac{x}{\log x} \]

Dirichlet. Given integers \( a, d \),

There are only many primes of the form \( a + nd \), \( n \in \mathbb{N} \)

\( a, a+d, a+2d, \ldots \)

- Solutions to polynomial equations

Diophantine equations.

Fermat equation: \( x^n + y^n = z^n \)

\( n = 2 \) solved by Euclid

\( n > 2 \): no solutions, solved by

Wiles 1995.
**Pythagorean Triples.**

**Defn.** A Pythagorean triple (PT) is a triple \((a,b,c)\) of positive integers such that

\[a^2 + b^2 = c^2\]

**E.g.**

\[
\begin{align*}
&\text{3} \quad &\text{5} \\
&\text{4} \\
&\text{12709} \quad &\text{18541} \\
&\text{13500}
\end{align*}
\]

\[
\begin{align*}
&\text{3} \quad &\text{5} \\
&\text{4} \\
&\text{8} \quad &\text{10} \\
&\text{6}
\end{align*}
\]

**Note.** If \((a,b,c)\) is a PT, so is \((b,a,c)\).

- If \((a,b,c)\) is a PT, so is \((na,nb,nc)\) for any \(n \in \mathbb{N}\).

**Defn.** A primitive PT is a PT \((a,b,c)\) \(a',b',c'\) such that if \((a,b,c) = (a'n,nb',nc')\) for \(n \in \mathbb{N}\) then \(n = 1\).
Problem: Find all primitive \( P_T(a, b, c) \) (possibly up to switching \( a \) \& \( b \))

i.e. if I find \((a, b, c)\), I have found \((b, a, c)\).

First Insight: A primitive \( P_T(a, b, c) \) is equivalent to a point \((x, y)\) on \( x^2 + y^2 = 1 \); \( x, y \in \mathbb{Q} \). "rational point"

\[(a, b, c) \text{ primitive } P_T \quad \mapsto \quad \left( \frac{a}{c}, \frac{b}{c} \right) \]

\[(a, b, c) \quad \mapsto \quad (x, y) \]

with \( x, y \in \mathbb{Q} \)

common denominator

\[x = \frac{a}{c} \quad y = \frac{b}{c} \]

Second Insight:

A line through \((0, 1)\) \(w/\) rational slope intersects the unit circle at a rational point!

pf. \( y = mx + d \) be such a line. \( d = 1 \).

Note that \( x \)-intercept is \( t = -\frac{1}{m} \).
Then:

\[ y = 1 - \frac{x}{t} \]

\[ x^2 + y^2 = 1 \]

\[ x^2 + \left(1 - \frac{x}{t}\right)^2 = 1 \]

\[ x^2 + 1 - 2 \frac{x}{t} + \frac{x^2}{t^2} = 1 \]

\[ 2 \frac{x^2}{t^2} = x^2 \left(t^2 + 1\right) \]

either \( x = 0 \)
\[ x = \frac{2t}{t^2 + 1} \] rational!

\[ y = 1 \]
\[ y = 1 - \frac{x}{t} = \frac{t^2 - 1}{t^2 + 1} \] rational!

Further, every rational point \((x, y)\) can be gotten this way.

**Proof.** Take the line through \((0, 1)\) & \((x, y)\)

its slope is \(\frac{y-1}{x} = m\).

Thus every rational point \((x, y)\) in 1st quadrant except \((0, 1)\)
is \((x, y) = \left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1}\right) \quad t \in \mathbb{Q} \quad t \geq 1. \)

\((1, 0) \quad t = \frac{1}{2}\)
Writing \( t = \frac{p}{q} \) in lowest terms, the corresponding \( PT \) is similar to

\[
(2pq, p^2-q^2, p^2+q^2), \quad p, q \in \mathbb{N}, \quad p > q.
\]

Check:

\[
(2pq)^2 + (p^2-q^2)^2 = (p^2+q^2)^2
\]

\[
4p^2q^2 + p^4 - 2p^2q^2 + q^4 = p^4 + q^4 + 2p^2q^2 \quad \checkmark
\]

Almost done .

(1) \( (*) \) may not be primitive

(2) Different \( p, q \) may yield similar \( (*) \)

Every

\[\text{Every} \]

\[\text{primitive} \] \( PT \) \((a, b, c)\) can

be written uniquely (possibly after switching \( a, b))\)

as

\[
(2pq, p^2-q^2, p^2+q^2) \quad \text{for } p, q \in \mathbb{N}, \quad p > q,
\]

\( p, q \) opposite parity \( 2 \) \( \text{w/ no common factor.} \)
<table>
<thead>
<tr>
<th>(2,1)</th>
<th>(4, 3, 5)</th>
<th>(4/5, 3/5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(3,1)</td>
<td>(6, 8, 10)</td>
<td>(6/10, 8/10) = (3/5, 4/5)</td>
</tr>
<tr>
<td>(3,2)</td>
<td>(12, 5, 13)</td>
<td>(12/13, 5/13)</td>
</tr>
<tr>
<td>(4,1)</td>
<td>(8, 15, 17)</td>
<td>(8/17, 15/17)</td>
</tr>
<tr>
<td>(4,2)</td>
<td>(16, 12, 20)</td>
<td>(16/20, 12/20) = (4/5, 3/5)</td>
</tr>
</tbody>
</table>

**Proof**. All that is left is to show:

\[(2pq, p^2 - q^2, p^2 + q^2) \text{ for } p, q \in \mathbb{N}, \ p > q\]

is primitive iff \(p, q\) have opposite parity and no common factors.

If \(p, q\) have same parity \(\Rightarrow\) not primitive

\(\text{no common factor} \Rightarrow \text{not primitive}\)

Assume different parity, \(d \neq 2\)

If \(d \mid 2p^2\) and \(d \mid 2q^2\)

\[\Rightarrow d \mid p \quad \text{and} \quad d \mid q\]