Last time: Diophantine Equations: polynomial eqns, for which
we're only interested in integer or rational solns.

A Method of solving: factoring, e.g. to \( y^2 = x^4 + 9 \)

Another method: using congruences

Example: The eqn \( x^2 - 7y^2 = -1 \) has no integer solns.

Prf: If \((x, y)\) is a soln, then \( x^2 \equiv -1 \pmod{7} \)

But: the \( x^2 \)'s mod 7 are:

\[
\begin{align*}
0^2 & \equiv 0 \\
(\pm 1)^2 & \equiv 1 \\
(\pm 2)^2 & \equiv 4 \\
(\pm 3)^2 & \equiv 9 \equiv 2 \\
\end{align*}
\]

\(6 \equiv -1 \pmod{7}\) does not appear \(\Rightarrow\) no solns.

Thus: Consider \( x^2 - dy^2 = -1 \). Suppose \( d \) is either divisible by 4 or divisible by a prime \( p \equiv 3 \pmod{4} \). Then \( x^2 - dy^2 = -1 \)

has no integer solns.

Prf: Suppose \( 4 \mid d \). Then \( x^2 \equiv -1 \pmod{4} \), if \((x, y)\) is a

soln. But \( x^2 \)'s mod 4 are \( 0^2 \equiv 0, (\pm 1)^2 \equiv 1, 2^2 \equiv 0 \pmod{4} \).

Suppose \( p \equiv 3 \pmod{4} \) & \( p \mid d \). Then if \((x, y)\) is a soln,
Suppose \( p = 3 \pmod{4} + 1 \). Then if \((x, y)\) is a solution, \(x^2 \equiv -1 \pmod{p}\). We proved that this congruence has no solutions.

**Example:** The eq \( x^2 - 5y^2 = 3z^2 \) only has \((x,y,z) = (0,0,0)\) as an integral soln.

**Pf:** Suppose \((x,y,z) \neq (0,0,0)\) is an integral solution. Then \((x,y,z)\) has a gcd, call it \(d\).

\[
\begin{align*}
X &= dx_0 \\
Y &= dy_0 \\
Z &= dz_0
\end{align*}
\]

with \(x_0, y_0, z_0 \in \mathbb{Z}\) and \(\gcd(x_0, y_0, z_0) = 1\).

\[
(dx_0)^2 - 5(dy_0)^2 = 3(dz_0)^2 \implies x_0^2 - 5y_0^2 = 3z_0^2.
\]

\[
0 \equiv x_0^2 - 5y_0^2 \equiv x_0^2 + y_0^2 \pmod{3}
\]

\[
x_0^2 + y_0^2 \equiv \begin{cases} 
0 \pmod{3} & \text{if } x_0 = y_0 = 0 \pmod{3} \\
1 \pmod{3} & \text{if } x_0 = 0 \text{ or } y_0 \not= 0 \pmod{3} \\
2 \pmod{3} & \text{if } x_0 \not= 0 \text{ or } y_0 = 0 \pmod{3}
\end{cases}
\]

\(\implies 3 \mid x_0, 3 \mid y_0 \implies 9 \mid x_0^2 - 5y_0^2 \implies 9 \mid 3z_0^2 \implies 3 \mid z_0^2 \implies 3 \mid z_0.\)
\[ \implies 3 \mid \overline{z_0} \implies 3 \mid \overline{z_0}. \]

This is a contradiction, since \( \gcd(x_0, y_0, z_0) = 1 \).

---

Recall: If \( a, b \in \mathbb{Z}_{>0} \), \( ab = c^n \), and \( (a, b) = 1 \), then \( a = u^n, b = v^n \) for \( u, v \in \mathbb{Z} \).

---

**Pythagorean Triples**

Find all integral solutions to \( x^2 + y^2 = z^2 \).

- **Observe:** By changing sign of \( x, y, z \) can assume that all \( x, y, z > 0 \).

  For example, \((-3)^2 + (4)^2 = (-5)^2 \) and this solution is related to \( 3^2 + 4^2 = 5^2 \).

- If \( d = \gcd(x, y, z) \) and \( x = dx_0, y = dy_0, z = dz_0 \) then \( x_0^2 + y_0^2 = 2_0^2 \) and \( \gcd(x_0, y_0, z_0) = 1 \).

Thus: We'll restrict to the case \( \gcd(x_0, y_0, z_0) = 1 \).

Thus: There are infinitely many positive integer solutions to the equation \( x^2 + y^2 = z^2 \) with \( \gcd(x, y, z) = 1 \). Up to switching \( x, y, z \), these solutions are given by:

\[
\begin{align*}
x &= u^2 - v^2, \\
y &= 2uv, \\
z &= u^2 + v^2
\end{align*}
\]

\( u, v \in \mathbb{Z} \).

**Proof:** First observe that this parametrization really gives solutions, i.e.

\[
(u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2
\]
\[(u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2\]
\[= u^4 + 2u^2v^2 + v^4\]
\[= (u^2 + v^2)^2\]

**Idea to find all solns:**
\[y^2 = z^2 - x^2 = (z - x)(z + x)\]

**Claim:** One of \(x, y\) is even, one is odd, and \(z\) is odd.

**Pf of claim:** \(x^2 + y^2 \equiv z^2 \pmod{4}\)

- If \(2|x, 2|y\) then \(4|x^2 + y^2 = 4|z^2 = 2|z\).
- If \(x, y\) are both odd, then \(x \equiv \pm 1 \pmod{4}, y \equiv \pm 1 \pmod{4}\)
  \[
  \Rightarrow x^2 + y^2 \equiv 1^2 + 1^2 \equiv 2 \pmod{4},\text{ which is not } \equiv 0 \pmod{4}.
  \]
  \[
  \Rightarrow \text{can assume } x \text{ is odd, } y \text{ is even}
  \]
  \[
  \Rightarrow x^2 + y^2 \text{ is odd } \Rightarrow z \text{ is odd.}
  \]

\[
y^2 = (z - x)(z + x) \Rightarrow \left(\frac{y}{2}\right)^2 = \left(\frac{z - x}{2}\right)\left(\frac{z + x}{2}\right)
\]

and \(\frac{y}{2}, \frac{z - x}{2}, \frac{z + x}{2} \in \mathbb{Z}\).

**Claim:** \(\gcd\left(\frac{z - x}{2}, \frac{z + x}{2}\right) = 1\).

**Pf:** Suppose \(p | \frac{z - x}{2}, \frac{z + x}{2}\). Then \(p | \text{sum} = z\)
\[p \mid \text{difference} = x.
\]
\[y^2 = z^2 - x^2 \lor p|y, p|z \Rightarrow p|y^2 \Rightarrow p|y. \quad \square\]
\[ \frac{z + x}{2} = u^2 \]
\[ \frac{z - x}{2} = v^2 \]

\[ z = u^2 + v^2 \]
\[ x = u^2 - v^2 \]
\[ (\frac{y}{2})^2 = u^2 v^2 \]
\[ y = 2uv \]