Def: A Diophantine equation is one where the unknowns are integers.

Examples:
- \( x^2 + y^2 = z^2 \)
- \( x^3 + y^3 = z^3 \)
- \( x^4 + y^4 = z^4 \)

Results:
- \( 6x + 7y = 15 \) has no solutions.
- \( 2x = 7 \) has no solutions.
- \( 217 \) is a solution.
- \( 6x + 7y = 15 \) has solutions since \((6, 7) = 1\).
- \( x^2 + y^2 = z^2 \) has many solutions (e.g., \( 3^2 + 4^2 = 5^2 \)).
- \( x^4 + y^4 = z^4 \) has no solutions beyond \( xy = 0 \).
- \(-x^3 + y^3 = z^3 \) (Fermat) has no non-trivial solutions (Euler).
Example: \( x^2 + y^2 = z^2 \)

**Step (1): Common Factors**

Say prime \( p \) divided two of \( x, y, z \). Then \( p \) divides the square of the third. So \( p \) divides the third (if \( p \) divides the square of the third, then \( p \) divides the third and divides the third). Then \( p^2 \mid x^2, p^2 \mid y^2, p^2 \mid z^2 \) so can divide \( x, y, z \) by \( p \).

Still have \( \left( \frac{x}{p} \right)^2 + \left( \frac{y}{p} \right)^2 = \left( \frac{z}{p} \right)^2 \)

Keep doing this until no common factors

\( \Rightarrow \) can write soln as \( x = d \cdot x', y = d \cdot y', z = d \cdot z' \)

where \( d \in \mathbb{Z}, x', y', z' \) pairwise relatively prime

**Step (2): Constraints from Congruence**

\( x, y \) can't both be even

Now if \( x, y, z \) pairwise prime, \( x, y \) can't both be even

HW: If \( x \) is even, \( x^2 \) is divisible by \( 4 \)

If \( x \) is odd, \( x^2 \) has remainder 1 when divided by \( 4 \)

If \( x, y \) were both odd, \( x^2, y^2 \) would each have form \( 4q + 1 \)

So \( z^2 = x^2 + y^2 \) would have form \( 4q + 2 \) impossible
So can't have both even or both odd wlog x is odd, y is even. So \(x^2 + y^2\) is odd, so \(z\) is odd.

**Step (3): Unique Factorization**

\[
x^2 + y^2 = z^2 \Rightarrow y^2 = 2^2 - x^2 = (2-x)(2+x)
\]

Both \(x, z\) odd, \(y\) even, so also have

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

Can \(a\) prime \(p\) divide both \(\frac{2-x}{2}, \frac{2+x}{2}\)?

No: if \(p|\frac{2+x}{2}\), and \(p|\frac{2-x}{2}\) then \(p|z = \frac{2+x}{2} + \frac{2-x}{2}\)

and \(p|x = \frac{2+x}{2} - \frac{2-x}{2}\).

So if we write

\[
\frac{2+x}{2} = p_1 \cdot p_2 \cdots p_r
\]

\[
\frac{2-x}{2} = q_1 \cdot q_2 \cdots q_s
\]

in the factorization \(\left(\frac{y}{2}\right)^2 = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdots q_s\)

all \(p, q\) distinct. But in \(\frac{y}{2}\) every prime occurs an even number of times, so \(e_i, f_i\) are even.

\[
36 = 2^2 \cdot 3^2, \quad 300 = 2^2 \cdot 3^2 \cdot 5^2 = (2^2 \cdot 3^2) \cdot (5^2)
\]
So \( \frac{7+x}{2}, \frac{7-x}{2} \) are squares.

Say \( \frac{7+x}{2} = n^2, \frac{7-x}{2} = m^2 \).

Then, \( m, n \) have no common factors (any common factors would divide \( x \) and \( t \)).

**Bottom line:** If \( \frac{7+x}{2} = n^2, \frac{7-x}{2} = m^2 \) then

\[ z = n^2 + m^2, \quad x = n^2 - m^2, \quad y = 2mn \]

Revert assumption \( \text{if primality} \)

\[ \left( \frac{y}{2} \right)^2 = m^2n^2 \]

i.e., if \( x^2 + y^2 = z^2 \) then have \( d, m, n \) with \( (m, n) = 1 \), \( n > m \), one for \( m, n \) even

\[ x = d \cdot (n^2 - m^2) \]
\[ y = d \cdot 2mn \]
\[ z = d \cdot (m^2 + n^2) \]

**Eq.**

\[ 3 = 2^2 - 1^2 \]
\[ 4 = 2 \cdot 2 \cdot 1 \]
\[ 5 = 2^2 + 1^2 \]

**Step 2:** Check:

\[ (d(n^2 - m^2))^2 + (d \cdot 2mn)^2 = d^2 \left( n^4 - 2m^2n^2 + m^4 \right) + d^2 \left( 4m^2n^2 \right) \]

\[ = d^2 \left( n^4 + 2m^2n^2 + m^4 \right) = d^2 \left( n^2 + m^2 \right)^2 \]

\[ = (d \cdot (n^2 + m^2))^2 \checkmark \]
Simple Version

Consider \( x^2 = 2y^2 \)

has sol'n \( 0^2 = 2 \cdot 0^2 \) Suppose \( x, y \neq 0 \)

let \( p \) be odd prime \( \implies p \mid x \) then \( p \mid x^2 \) so \( p \mid 2y^2 \)

so \( p \mid 2 \) or \( p \mid y \) or \( p \mid y^2 \) so \( p \mid y \)

then \( p^2 \mid x^2 \), \( p^2 \mid y^2 \) and \( \left( \frac{x}{p} \right)^2 = 2 \left( \frac{y}{p} \right)^2 \)

Repetitively doing this, eventually no odd prime divides \( x \) or \( y \)

So \( x \) is power of \( 2 \): \( x = 2^k \) 

and \( y \) is a power of \( 2 \): \( y = 2^l \) so \( x^2 = 2^{2k} \) \( 2y^2 = 2^{2l+1} \)

So can't have \( x^2 = 2y^2 \)

\( \implies \left( \frac{x}{y} \right)^2 = 2 \) has no solutions! (\( \sqrt{2} \) is irrational)

Lemma: If \( x = \prod p^{e_p} \) then \( x^2 = \prod p^{e_p+1} \)

\( \prod (p^{e_p+1}) = \prod p^{e_p + 2} \) (every exponent is even)
Go back to $10x + 7y = 33$

Solved by:

1. Using Bezout to find particular soln:
   
   $(10, 7) = 1 = 3 \cdot 7 - 2 \cdot 10 \Rightarrow 33 = -66 \cdot 10 + 99 \cdot 7$

2. Finding the general soln to homogeneous eqn
   
   $10x + 7y = 0$

   $\Rightarrow t \mid y \Rightarrow t \mid 10x \Rightarrow t \mid x \Rightarrow (t, 10t) = 1 \Rightarrow x = 7t$

   so $y = -10t$.

Put together:

\[
\begin{align*}
2x &= -66 + 7t \\
y &= 99 - 10t
\end{align*}
\]

(consecutive integer pts on line differ by $\pm (\frac{7}{10})$)

New interpretation:

\[10x + \left( \text{multiple of } \frac{7}{10} \right) = 33\]

(implicit unknown: By

Solution was:

\[x = -66 + \left( \text{multiple of } \frac{7}{10} \right)\]

Also $x = 4 + \left( \text{multiple of } \frac{6}{10} \right)$
New notation: Instead of \(10x + \left(\frac{\text{mult}}{7}\right) = 33\) or \(10x = 33 + \left(\frac{\text{mult}}{7}\right)\)

write (Gauss)

\[10x \equiv 33 \pmod{7}\]
\[x \equiv -9 + \left(\frac{\text{mult}}{7}\right)\]

Say "10x is congruent to 33 modulo 7").

Instead of \(x = -66 + \left(\frac{\text{mult}}{7}\right)\)

write \(x \equiv 4 \pmod{7}\)
\(x \equiv 4 \pmod{7}\)
\(x \equiv 4 \pmod{7}\)

Examples: \(365 = 1 + 7 \cdot 52\)
\[\Rightarrow 365 \equiv 1 \pmod{7}\]
Bottom line: Equation $10x + 7y = 33$

has only many solutions: \[ (x, y) = (-66) + (7)k \]

Congruence $10x \equiv 33 \pmod{7}$

has the "unique" solution $x \equiv 4 \pmod{7}$

Aside: One way to solve congruence $10x \equiv 33 \pmod{7}$

is to put back the implicit variable, convert to equation $10x + 7y = 33$

**Def:** Let $a, b, m \in \mathbb{Z}$, with $m > 1$. Say $a \equiv b \pmod{m}$ if $a - b$ is divisible by $m$.

$(\Leftarrow)$ $a - b = m \cdot k$ for some $k$, or $a = b + mk$ for some $k$.

Write $a \equiv b \pmod{m}$.

If $a - b$ not divisible by $m$, say $a$ is not congruent to $b \pmod{m}$, write $a \not\equiv b \pmod{m}$.

**Eg:** $4 \equiv 11 \equiv 18 \equiv -66 \pmod{7}$

but $4 \not\equiv 11 \pmod{6}$
Earlier today (HW): If $x \equiv 1$ (2) then $x^2 \equiv 1$ (4)

Proof: (1) $\equiv \cdot (m)$ is an equivalence relation:

(a) $x \equiv x (m)$ for all $x$
(b) if $x \equiv y (m)$ then $y \equiv x (m)$
(c) if $x \equiv y (m)$ and $y \equiv z (m)$ then $x \equiv z (m)$

(2) If $x \equiv x' (m)$, $y \equiv y' (m)$
then $x + y \equiv x' + y' (m)$
$x \cdot y \equiv x' \cdot y' (m)$