Last time: Solutions to diophantine eq's

- Eg., finding all rat'l solns to $x^2 + y^2 = 1$.

Fermat's method of descent/ascent

Idea: go from one soln of a Diophantine eq. to another.

- Descent: can be used to prove certain Diophantine eq's have no soln.
- Ascent: " " " " " " " " " " " " 2/3 many solns.

Thm: There are no solns to the eq $x^4 + y^4 = z^2$ w/ $x, y, z > 0$. In particular, there are no solns to $x^4 + y^4 = w^2$, w/ $x, y, w > 0$.

Recall: There are no solns to $x^n + y^n = z^n$ w/ $n > 2$.

Pf of Thm: Second part of Thm follows from first part by taking $z = w^2$.

Reduction to case: gcd $(x, y) = 1$. Suppose $(x, y, z)$ is a pos int. soln.
Reduction to case: \( \gcd(x, y) = 1 \) Suppose \((x, y, z)\) is a pos int soln

\[ x^4 + y^4 = z^2 \]

with \( \gcd(x, y) = d. \)

Then \( x = dx_1, \quad y = dy_1, \quad x_1, y_1 \in \mathbb{Z}. \) and \( \gcd(x_1, y_1) = 1. \)

\[ z^2 = d^4 (x_1^4 + y_1^4) \Rightarrow x_1^4 + y_1^4 = \left( \frac{z}{d^{2}} \right)^2 \]

Observe: \( \frac{z}{d^{2}} \) is a rat'l #, and its \( \square \) is an integer

\[ \Rightarrow \frac{z}{d^{2}} \in \mathbb{Z} \], set \( \frac{z}{d^{2}} = t_1. \)

Then \( x_1^4 + y_1^4 = t_1^2 \) and \( (x_1, y_1) = 1. \)

**MAIN IDEA:** from \((x_1, y_1, t_1)\) we'll find another soln

\((x_2, y_2, t_2)\) with \( x_2, y_2, t_2 > 0, \) integers

AND \( 0 < t_2 < t_1, \quad (x_2, y_2) = 1. \)

Then can iterate to find \((x_3, y_3, t_3)\), pos int soln with \( t_1 > t_2 > t_3 > 0 \) etc.

Suppose \( x_1^4 + y_1^4 = t_1^2. \) Then \( (x_1^2)^2 + (y_1^2)^2 = t_1^2 \)

so \((x_1^2, y_1^2, t_1)\) is a Pythagorean triple.

Moreover: \( \gcd(x_1^2, y_1^2) = 1 \) b/c \( \gcd(x_1, y_1) = 1. \)

**Thus** One of \( x_1^2, y_1^2 \) is even, one is odd, \( t_1 \) is odd.

Moreover:
Moreover:

\[ x_1^2 = u^2 - v^2 \]
\[ y_1^2 = 2uv \]
\[ z_1 = u^2 + v^2 \]

\[ x_1^2 + v^2 = u^2 \]

\[ u/(u,v) = 1, \] one of \(u,v\) even and one odd

Since \((u,v) = 1\), \((x_1,u,v) = 1\), so this is a primitive Pythagorean triple.

\[ x_1: \text{odd} \implies u: \text{odd}, \ v: \text{even} \]

\[ \implies \exists a,b \in \mathbb{Z} \ u/ \text{one even and one odd s.t.} \]

\[ x_1 = a^2 - b^2 \]
\[ v = 2ab \]
\[ u = a^2 + b^2 \]

Moreover, \((a,b) = 1\).

We'll show that \(u, a, b\) are all \(\square\)'s.

\(\implies\) a smaller soln to the original eqn.

\[ u: \text{a } \square: \text{ Recall } y_1^2 = 2uv, \ v \text{ even}, \ u \text{ odd.} \]
\[ = u(2v) \]

Claim: \((u, 2v) = 1\).

Pf of claim: If \(p | u, \ p | 2v\) then \(p\) is odd b/c \(u\) is odd

\[ \implies p | u, \ p | v \implies x \]

\[ =\]
\[ u = z^2_2 \]
\[ 2v = c^2 \]

\(a, b\) are \(\square\)'s: Recall: \(v = 2ab\)
\(a, b\) are \(\bar{\mathbb{D}}\)s: Recall: \(V = 2ab\)

\[c^2 = 2V = 4ab \implies \left(\frac{c}{2}\right)^2 = a^2 b^2, \quad \frac{c}{2} \in \mathbb{Z}.
\]

But \(gcd(a, b) = 1 \implies a = x^2, \quad b = y^2,\)

Consider \((x_2, y_2, z_2)\).

\[x_2^4 + y_2^4 = (x_2^2)^2 + (y_2^2)^2 = a^2 + b^2 = u = z_2^2.
\]

So: from \((x_1, y_1, z_1)\) we've constructed another soln

\((x_2, y_2, z_2)\) to the same eq^2.

Finally, observe that

- \((x_2, y_2) = 1 \iff p| x_2, \quad p| y_2, \quad \text{then} \quad p| x_2^2, \quad p| y_2^2
\]

\[\implies p|a, \quad p|b \quad \text{but} \quad (a, b) = 1.
\]

- \(z_2 < z_1 \quad \text{by}\)

\[z_1 = u^2 + v^2 > u^2 = z_2^2 \quad \text{by} \quad u = z_2^2
\]

\[\implies z_2 < z_1.
\]

\[\text{Ascent: From one soln to a diophantine eq^2 find another.}
\]

"Larger" solution \(\implies\) there are \(\infty\) many solns.

Thm: Suppose \(d > 0, \quad d \in \mathbb{Z}\). If there is one soln to the eq^2

\[(x^2 - dy^2 = 1) \quad \Rightarrow x, y > 0\]
Theorem 1.

\( x^2 - dy^2 = 1 \) \( w/ \ x, y > 0 \)

then there are \( \infty \) many solutions.

If there is one solution to the equation

\( x^2 - dy^2 = -1 \), then there are only \( \infty \) many solutions to (.5) and (.6).

Idea: Observe:

\[
\begin{vmatrix} a & b \\ db & a \end{vmatrix} = a^2 - db^2
\]

\[
\begin{vmatrix} x & y \\ dy & x \end{vmatrix} = x^2 - dy^2.
\]

\[
\begin{pmatrix} a & b \\ db & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + db \ y \\ db \ y + bx \end{pmatrix} = \begin{pmatrix} x' \\ y' \end{pmatrix}
\]

Thus:

\[
\begin{cases}
  x' = ax + db \ y \\
  y' = db \ y + bx
\end{cases}
\]

Thus, \( (x')^2 - d(y')^2 = (a^2 - db^2)(x^2 - dy^2) \).

Pf of Thm 1. Suppose have solutions \( a, b \) \( w/ \ a^2 - db^2 = 1 \) and \( a, b > 0 \).

Let \( (x_n, y_n) \) be such that \( x_n, y_n > 0 \) and \( x_n^2 - dy_n^2 = 1 \).

Define:

\[
\begin{aligned}
  x_{n+1} &= ax_n + db \ y_n \\
  y_{n+1} &= dy_n + bx_n
\end{aligned}
\]

then \( x_{n+1} > 0 \) and \( x_{n+1} > x_n \).
Define: 
\[ x_{n+1} = cx_n + dy_n \geq ax_n \geq x_n \]
\[ y_{n+1} = ay_n + bx_n \geq ay_n \geq y_n \]

\[ x_{n+1}^2 - dy_{n+1}^2 = (a^2 - d^2)(x_n^2 - dy_n^2) = 1 \cdot 1 = 1. \]

So: there are only many solutions.

Rest is similar.