Fermat's Last Theorem : For $n \geq 3$, the equation

$$X^n + Y^n = Z^n$$

has no solutions in positive integers x, y, z

In today's class, we consider $n=4$ case.

The equation becomes: $X^4 + Y^4 = Z^4$

Indeed, we will show:

Theorem 30.1 The equation $x^4 + y^4 = z^2$

has no solutions in positive integers x, y, z.

Remark: This theorem is stronger than "no solutions for $X^4 + Y^4 = Z^4$."

Assume Theorem 30.1 is valid. Suppose that

$X^4 + Y^4 = Z^4$ has a solution

Then set $x = X$, $y = Y$, $z = Z^2$

Then $x^4 + y^4 = z^2$. A contradiction.

Therefore, it suffices to show Theorem 30.1.

Lemma: Let s, t be two odd integers satisfying $\gcd(s,t) = 1$. Then $\gcd(s-t, s+t) = 2$.

Proof: Let $p \mid s-t$, $s+t \Rightarrow p \mid 2s$ and $p \mid 2t$

Since $\gcd(s,t) = 1$, $p = 2$.

Next, assume that $4 \mid s-t$, $s+t$

Then $s \equiv t \pmod 4$.

If $s \equiv t \equiv 1 \pmod 4$, $s+t \equiv 2 \pmod 4$ $4 \nmid s+t$

If $s \equiv t \equiv 3 \pmod 4$, $s+t \equiv 2 \pmod 4$ $4 \nmid s+t$.

A contradiction.

Therefore, $\gcd(s-t, s+t) = 2$. □

Lemma: Assume that $\gcd(a,b) = 1$ and $ab = n^2$

Then both a, b are squares.

Proof: By prime factorization, $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$$ab = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_r^{2\alpha_r}$$

Since $\gcd(a,b) = 1$, a, b share no common divisors.

If $p_i \mid a$, then $p_i^{2\alpha_i} \| a \Rightarrow a$ is a square

If $p_j \mid b$, then $p_j^{2\alpha_j} \| b \Rightarrow b$ is a square. □

Remark: We will again use the "descent" method:

suppose that we can find a solution (x_1, y_1, z_1)

then we can find another solution (x_2, y_2, z_2)

with $z_2 < z_1$

We repeat this process and we get:

$$z_1 > z_2 > z_3 \cdots$$

Finally, we can find $z = 1$, which forces either x or y to be 0. A contradiction.

Therefore, what we prove for the theorem is:

"suppose that we find a solution (x_1, y_1, z_1),

then we can find another solution (x_2, y_2, z_2) such that

(1) $x_2, y_2, z_2 > 0$

(2) $z_1 > z_2$.

Proof: Suppose that we have the solution:

$$x_1^4 + y_1^4 = z_1^2$$

Then this can be written as:

$$(x_1^2)^2 + (y_1^2)^2 = z_1^2$$

Furthermore, we can assume that x_1, y_1, z_1 has no common divisors.

Therefore, (x_1^2, y_1^2, z_1) is a PPT.

Then we can find $s > t \geq 1$ odd such that

(1) $\gcd(s,t) = 1$

(2) $x_1^2 = st \quad y_1^2 = \frac{s^2 - t^2}{2} \quad z_1 = \frac{s^2 + t^2}{2}$

(Lemma: let n be an odd square, then $n \equiv 1 \pmod 4$)

Notice that s, t are odd and $st = x_1^2$

This implies that $st \equiv 1 \pmod 4$

This will show: $s \equiv t \pmod 4$

On the other hand,

$$2y_1^2 = s^2 - t^2 = (s-t)(s+t)$$

Notice that $2 \mid s-t, s+t, \quad 4 \mid (s-t)(s+t) \Rightarrow 4 \mid 2y_1^2$

and hence $2 \mid y_1^2 \Rightarrow 2 \mid y_1 \Rightarrow 8 \mid 2y_1^2$

Notice that $\gcd(s,t) = 1$, and $s \equiv t \pmod 4$

This will show: $s-t \equiv 0 \pmod 4$, $s+t \equiv 2 \pmod 4$

and $\gcd(s-t, s+t) = 2$.

Therefore, we can write $s+t = 2 \cdot A$ A odd.

$$s-t = 4 \cdot B.$$

This gives: $2y_1^2 = 8A \cdot B$ with $\gcd(A, 2B) = 1$

$$\Rightarrow \quad y_1^2 = \underset{\| \; s+t}{A} \cdot 4 \underset{\| \; s-t}{B} \quad \text{with } \gcd(A, 2B) = 1$$

$\Rightarrow$ Both A, B are squares.

We write: $s+t = 2u^2$ with $\gcd(u, 2v) = 1$.

$$s-t = 4v^2$$

This gives: $s = u^2 + 2v^2$

$t = u^2 - 2v^2$

$$z_1 = \frac{s^2+t^2}{2} = \frac{(u^2+2v^2)^2 + (u^2-2v^2)^2}{2}$$

$$= u^4 + 4v^4 > u^2$$

Then $x^2 = st = u^4 - 4v^4$

$$\Rightarrow \quad x^2 + 4v^4 = u^4 \qquad \gcd(u, 2v) = 1$$

Next, we set $A = x$, $B = 2v^2$ $C = u^2$ primitive

The equation becomes: $A^2 + B^2 = C^2$

Then $A = ST$ $\quad B = \dfrac{S^2 - T^2}{2}$ $\quad C = \dfrac{S^2 + T^2}{2}$.

$B = 2v^2$

$\Rightarrow \quad 2v^2 = B = \dfrac{S^2 - T^2}{2} \quad \Rightarrow \quad 4v^2 = S^2 + T^2 = (S-T)(S+T)$

Again: $\gcd(S-T, S+T) = 2$

Then: $S+T = 2X^2 \qquad S-T = 2Y^2$

This gives: $S = X^2 + Y^2$ and $T = X^2 - Y^2$

Then:

$$u^2 = C = \frac{S^2+T^2}{2} = \frac{(X^2+Y^2)^2 + (X^2-Y^2)^2}{2}$$

$$= X^4 + Y^4.$$

We find another solution (X, Y, u) with $u < z_1$.

We finish the proof. $\square$