1. Fermat's Last Theorem(4)

Theorem 1.1 (Fermat's Last Theorem)**.** Let $n \geq 3$ be an integer. There are no positive integer solutions to

$$x^n + y^n = z^n$$

Fermat showed the case when $n = 4$. He proved that there are no positive integer solutions to $x^4 + y^4 = z^2$ by *infinite descent*, that is, if there is a solution with z minimal, then show there is another solution X, Y, Z, positive integers, with $Z < z$ to make a contradiction.

Note that no solutions to $x^4 + y^4 = z^2$ implies no solutions to $x^4 + y^4 = z^4$.

Proof. Assume $x^4 + y^4 = z^2$ with $x, y, z \in \mathbb{Z}$ positive and z minimal. We claim[1] this would imply that $\gcd(x, y) = 1$.

Proof of claim[1]: Let $d = \gcd(x, y)$. If $d \neq 1$, then there is a smaller solution

$$\left(\frac{x}{d}\right)^4 + \left(\frac{y}{d}\right)^4 = \left(\frac{z}{d^2}\right)^2$$

with $\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2} \in \mathbb{Z}$ and the solution is smaller because if $d > 1$, $\frac{z}{d^2} < z$.

Hence (x^2, y^2, z) is a primitive Pythagorean triple, because $\gcd(x, y) = 1$ implies $\gcd(x^2, y^2, z) = 1$. Thus, by the classification of primitive Pythagorean triple, there exists $u, v \in \mathbb{Z}$ such that

$$x^2 = v^2 - u^2 \tag{1}$$

$$y^2 = 2uv \tag{2}$$

$$z = u^2 + v^2 \tag{3}$$

where $v > u > 0$, $\gcd(u, v) = 1$ and they have opposite parity.

Note that x^2 is odd $\implies$ x is odd $\implies$ $x^2 \equiv 1 \mod 4$. Thus, $v^2 \equiv 1 \mod 4$ and $u^2 \equiv 0 \mod 4$, i.e. v **is odd and** u **is even**. Then, we could rewrite u as $\boxed{u = 2r}$ for some integer $r > 0$.

Substituting $u = 2r$ into (1),

$$x^2 = v^2 - (2r)^2 \tag{4}$$

Substituting $u = 2r$ into (2),

$$y^2 = 4rv$$

Since y is even, $\frac{y}{2} \in \mathbb{Z}$, and

$$\left(\frac{y}{2}\right)^2 = rv$$

Note that $\gcd(u, v) = 1 \implies \gcd(r, v) = 1$, and since $\left(\frac{y}{2}\right)^2$ is a square, we may conclude that r, v are squares. Thus, rewrite them as $\boxed{r = t^2, v = Z^2}$.

Note that

$$v > 0 \implies Z > 0 \tag{5}$$

Substituting $r = t^2, v = Z^2$ into (4),

$$\begin{aligned} x^2 &= Z^4 - (2t^2)^2 \\ \implies x^2 + (2t^2)^2 &= Z^4 \\ \implies x^2 + (2t^2)^2 &= (Z^2)^2 \end{aligned}$$

$(x, 2t^2, Z^2)$ is a primitive[2] Pythagorean triple.

Proof of claim[2] $\gcd(r, v) = 1 \implies \gcd(Z^2, t^2) = 1 \implies \gcd(x, 2t^2, Z^2) = 1$

Hence, by the classification of primitive Pythagorean triple, there exists $U, V \in \mathbb{Z}$ such that

$$x = V^2 - U^2 \tag{6}$$

$$2t^2 = 2UV \tag{7}$$

$$Z^2 = U^2 + V^2 \tag{8}$$

where $V > U > 0$, $\gcd(U, V) = 1$ and they have opposite parity.

(7) implies that $t^2 = UV$, thus, U and V are squares, so rewrite them as

$$\boxed{U = X^2, V = Y^2} \tag{9}$$

Substituting (9) into (8),

$$X^4 + Y^4 = Z^2$$

Remark that (5) and $U, V > 0 \implies X, Y, Z > 0$. In other words, X, Y, Z is a positive integer solution to $x^4 + y^4 = z^2$. Furthermore, we claim[3] that $Z < z$, contradicting the minimality of z.

Proof of claim[3]: $Z^2 = v$ but $u^2 + v^2 = z$ (equation (3)), so $v < \sqrt{z}$, i.e., $Z^2 < z^{\frac{1}{2}} \implies Z < z^{\frac{1}{4}} \leq z$. Hence, $Z < z$.

□