On Some Diophantine Equations

Sabyasachi Mukherjee
Undergraduate
Shiv Nadar University,India
math.sabyasachi12@gmail.com

December 16, 2013

Abstract

In this expository article, we wish to investigate certain Diophantine equations arising from the Pythagorean theorem for integers and look at ways of investigating some of them. We also offer a proof of Fermat's Last Theorem for the case $n = 4$. The contents in this document are neither new nor original; it is merely an attempt to test my own understanding of the material.

1 The equation of the form $x^2 + y^2 = z^2$

The Pythagoras theorem tells us a fact about right angled triangles: that if two side lengths of a right angled triangle (other than that of the hypotenuse) be x and y and the hypotenuse be of length z, then $x^2 + y^2 = z^2$. This motivates us to find all positive integral solutions of the form $x^2 + y^2 = z^2$.

More specifically, we shall investigate equations of the form $x^2 + y^2 = z^2$ where $\gcd(x, y, z) = 1, x, y, z > 0$. Such triples (x, y, z) are known as primitive Pythagorean triples.

Two lemmas are in order.

1.1 Two Lemmas

Lemma 1: In a Pythagorean triple,one and only one of x and y is even.

Proof:Note that $\gcd(x, y, z) = 1$ by the definition of a primitive Pythagorean triplet. If both are even, $2|z \implies \gcd(x, y, z) \geq 2$. If both are odd, $x^2 + y^2 \equiv 2 \bmod 4$, a contradiction as any square is either 0 or 1 mod 4 .So one of them is even, the other is odd.

Lemma 2: If $a, b, c \in \mathbb{N}, \gcd(a, b) = 1$ and $ab = c^n$, then there exist positive integers e, f such that $e^n = a, f^n = b$.

Proof: The proof is left to the reader.However, looking at the prime representation of a and b is helpful.

1.2 An Important Theorem

Theorem 1:The solutions to the equation $x^2 + y^2 = z^2$ where $x, y, z > 0$, $\gcd(x, y, z) = 1$, is given by

$$x = 2st$$
$$y = s^2 - t^2$$
$$z = s^2 + t^2$$

for some naturals $s, t, s > t > 0, \gcd(s, t) = 1$ and $s \not\equiv t \bmod 2$.

Proof: $x^2 = z^2 - y^2 \implies \dfrac{x^2}{4} = \dfrac{z-y}{2} \cdot \dfrac{z+y}{2}$. Note that $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ If not, let $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = d$. Then $d|\frac{z-y}{2} + \frac{z+y}{2} = z$ and $d|\frac{z+y}{2} - \frac{z-y}{2} = y$.

Thus $d|y, z$. As $x^2 + y^2 = z^2$, d also divides x which forces $\gcd(x, y, z) \geq d$ which is not true as their gcd is 1.

Using lemma 2,

$\frac{z+y}{2} = s^2$ and $\frac{z-y}{2} = t^2$ for some positive integers s, t. So, $z = s^2 + t^2$ and $y = s^2 - t^2$, $z^2 - y^2 = 4s^2t^2 \implies x = 2st$. Note that $y > 0 \implies s^2 - t^2 > 0 \implies s > t > 0$.Further, $\gcd(\frac{z-y}{2}, \frac{z+y}{2}) = 1$ forces $\gcd(s, t)$ to be 1 as well. QED.

2 Two More Theorems

Theorem 2: There is no solution to $x^4 + y^4 = z^2$ in positive integers x, y, z.

The proof of this theorem will need some work. We will see repeated application of theorem 1 and the two lemmas preceding it.

Proof: We prove this by contradicton.

Suppose that the equation has a solution (x, y, z). Further let $\gcd(x, y) = d$. So there exist natural numbers x_0, y_0 such that $\gcd(x_0, y_0) = 1$ so that $x = dx_0, y = dy_0$. That implies $z = d^2 z_0$ for some z_0 in naturals.

We now have $x_0^4 + y_0^4 = z_0^2$ such that $\gcd(x_0, y_0, z_0) = 1, x_0, y_0, z_0 > 0$. So we now have a Pythagorean triple x_0^2, y_0^2, z_0 and so we have (assuming x_0 is even)

$$x_0^2 = 2st$$
$$y_0^2 = s^2 - t^2$$
$$z_0 = s^2 + t^2$$

for some positive naturals $s, t, s > t$ with $\gcd(s, t) = 1$.

y_0 and z_0 are odd by lemma 1. If t is odd, $y_0^2 \equiv 1 \equiv 0 - 1 \equiv 3 \bmod 4$, a contradiction (note that if t is odd, s is even). So, t is even.

Let $t = 2k$. Then $x_0^2 = 2s(2k) \implies \exists u, w \in \mathbb{N}$ such that $s = u^2, k = w^2$

Consider the equation $y_0^2 + t^2 = s^2$, $\gcd(y_0, t, s) = 1$(note that $\gcd(s, t) = 1$ implies that $\gcd(y_0, t, s)$ is 1. So, there exist natural numbers m, n, $m > n >$

0,gcd$(m,n)=1$ such that

$$\begin{aligned} t^2 &= 2mn \\ y_0 &= m^2-n^2 \\ s = m^2+n^2, m &\not\equiv n \bmod 2 \end{aligned}$$

.

Once again, $m=m_1^2$ and $n=n_1^2$ for some natural numbers m_1,n_1 using the previous arguments. So, $s=u^2=(m_1^2)^2+(n_1^2)^2$. Note that this makes (m_1,n_1,u) a solution set to our equation.

$0<m_1^2=m<m^2+n^2=s<2st<x_0^2 \implies 0<m_1<x_0$ i.e for each x_0, there is a smaller m_1 which is part of the solution of the equation. x_0 being finite, $m_1=0$ at some stage, a contradiction.This is the Fermat's method of infinite descent.

So the equation $x^4+y^4=z^2$ has no solution in natural numbers.

Note that this implies that that there is no solution to the equation $x^4+y^4=z^4$, the Fermat's Last Theorem for the exponent 4.

Theorem 3: There is no solution to the equation $x^4-y^4=z^2$ in natural numbers.

Proof: Imitating theorem 1's proof, we consider that case when $x_0^4-y_0^4=z_0^2$ for coprime x_0,y_0,z_0.

So now there are two cases. If y_0 is odd,for some natural numbers m,n

$$\begin{aligned} x_0^2 &= m^2+n^2 \\ y_0^2 &= m^2-n^2 \\ z_0 &= 2mn \end{aligned}$$

where gcd$(m,n)=1$ and $m>n>0$ and $m\not\equiv n \bmod 2$.

Multiplying the first two equations, we get

$$m^4-n^4=(x_0y_0)^2$$

i.e. gcd$(m,n,x_0y_0)=1$, $0<m<\sqrt{m^2+n^2}=x_0$: the Fermat's Method of infinite descent shows that there is a contradiction!

We are left with the case y_0 is even. Then for some natural numbers m,n

$$\begin{aligned} x_0^2 &= m^2+n^2 \\ z_0 &= m^2-n^2 \\ y_0^2 &= 2mn \end{aligned}$$

where gcd$(m,n)=1$ and $m>n>0$. So, gcd$(2m,n)=1$ i.e $2m=w^2$ and $n=r^2$ for some $m,w\in\mathbb{N}$. So, $m=2w_1^2$ for some w_1. We have $x_0^2=(2w_1^2)^2+(r^2)^2$. So, $(2w_1^2,r^2,x_0)$ is a Pythagorean triple. So,

$$\begin{aligned} 2w_1^2 &= 2gh \\ r^2 &= g^2-h^2 \\ x_0 = g^2+h^2, \text{gcd}(g,h)=1, g &\not\equiv h \bmod 2 \end{aligned}$$

That allows us to conclude that g, h are perfect squares. $g = k^2$, $h = l^2$. So $r^2 = k^4 - l^4$ i.e. (k, l, r) is a solution of the original equation. Note that $0 < k = \sqrt{g} < g^2 + h^2 = x_0$ and this produces a contradiction by Fermat's method of infinite descent.

3 Bibliography

1. Fermat's Last Theorem For Specific Exponents
2. *Elementary Number Theory* by David M. Burton(6th edition, McGraw Hill)