Chapter 3: SOME ESSENTIAL DIOPHANTINE EQUATIONS

A: Pythagorean equation:

The Pythagorean equation, is important in all type of area: mathematics, physics, and astronomy and has practical applications in surveying. It is associated with the name of the Greek philosopher and mathematician Pythagoras, who lived during the 7th century BC. Though, there is evidence show that it was known at least 1,000 years before him. Babylonian texts dating from as early as 1800 BC contain discussions of Pythagorean triples.

In number theory, it's a important theorem, which help solving a lot of Diophantine equation and proving many others important theorem like Fermat last teorem for n = 4, Fermat-like equation,ect....

a) Pythagorean equation:

Pythagorean equation is the equation which has the form of:

$$x^2 + y^2 = z^2 \quad (1)$$

with x, y, z *are positive integral. Such triples of solutions are called Pythagorean triples, and here,of course, we only concern about its primitive roots, which means* $\gcd(x,y,z) = 1$.

Now, we gonna find the fomular that can gives us all the primitive solution of this equation.

1. *First, we got a lemma: If* (x,y,z) *is a primitive Pythagorean triple then x, y, z are pairwise coprime; x, y have different parity and z is odd.*

Indeed, assume that $gcd(x; y) > 1$. *If p is a prime with* $p \mid x;\ p \mid y$ *then* $p^2 \mid x^2 + y^2 = z^2 \Rightarrow p \mid z$, *contradict with the supposition* $\gcd(x,y,z) = 1$ .. *Thus* $gcd(x; y) = 1$.
Similarly for $gcd(x; z) = 1;\ gcd(y,z) = 1$.
Since $gcd(x; y) = 1$ *then* x, y *can't be concurrently even. Assume that* x, y *are odd then* $x^2 \equiv y^2 \equiv 1(\mod 4) \Rightarrow z^2 \equiv 2 \pmod 4$ *and this is impossible so* x, y *are differrent about odd – even parity so* z *is odd.*
Without any lost of generality, we assume that x is even.

2. *Secondly, we will now prove that* (x,y,z) *is a primitive Pythagorean triple (with x is even) if and if only:*

$$x = 2mn$$

$$y = m^2 - n^2$$

$$z = m^2 + n^2$$

with $gcd\,(m,n) = 1;\ m,n$ *have different parity.*

Proof: We have that:

$x^2 = (z + y)(z - y)$

$$\Leftrightarrow \left(\frac{x}{2}\right)^2 = \frac{z+y}{2}.\frac{z-y}{2} \quad (2)$$

Since z, y are odd and relatively prime so $\frac{(z+y)}{2}; \frac{(z-y)}{2}$ *are relatively prime. (readers self evidence). Combine this with (2), we have that* $\frac{(z+y)}{2}; \frac{(z-y)}{2}$ *are all squares.*

Let $\frac{(z+y)}{2} = m^2; \frac{(z-y)}{2} = n^2$ *with m, n are relatively prime then:*

$$z = m^2 + n^2 \;\; ; \;\; y = m^2 - n^2$$

Since y, z is odd so m, n is different about odd-even parity.

Since $gcd(m^2, n^2) = 1$ *then* $gcd(m, n) = 1$.

In conclusion:

$$x = 2mn$$

$$y = m^2 - n^2$$

$$z = m^2 + n^2$$

with $gcd(m, n) = 1;\ m > n; m, n$ *have different parity.*

Reverse, (x, y, z) *is a triple satisfied (1).*

b) Application of Pythagorean equation:

Now, we will come back to prove the theorem that I've mentioned at chapter 2: *Prove that the equation* $p = x^2 + y^2$ *for p is prime,* $p = 4k + 1, k \in Z$ *has one and only one solution in Z (not count its interchange).*

Proof: Suppose that the equation $p = x^2 + y^2$ has two different solutions on N: $(x;\ y) = x_1; y_1)$ *and* $(x;\ y) = (x_2;\ y_2)$ then: $gcd(x_1; y_1) = gcd(x_2;\ y_2) = 1$; $p = {x_1}^2 + {y_1}^2 = {x_2}^2 + {y_2}^2$.

Since p is prime and $p = x_1^2 + y_1^2 = x_2^2 + y_2^2$ then one of ($x_1; y_1$) and one of $(x_2;\ y_2)$ is odd and the other is even. Suppose that x_1 *and* x_2 are even and $y_1;\ y_2$ are odd.

$$p^2 = ({x_1}^2 + {y_1}^2).(x_2^2 + y_2^2) = (x_2.y_1 - x_1.y_2)^2 + (x_1.x_2 + y_1.y_2)^2 \quad (*)$$

It's definitely that $(x_2.y_1 - x_1.y_2)$ *and* $(x_2.x_2 + y_1.y_2)$ are relatively prime, because if gcd$[(x_2.y_1 - x_1.y_2); (x_2.x_2 + y_1.y_2)] > 1$ then suppose d is a prime that p | $(x_2.y_1 - x_1.y_2)$ *and* $p|(x_2.x_2 + y_1.y_2)$ then from (*), we got $d \mid p^2$ and since d, p are prime then $d = p$.

If $d = p$ then: $\left(\frac{x_2.y_1 - x_1.y_2}{p}\right) \in Z; \left(\frac{x_1.x_2 + y_1.y_2}{p}\right) \in Z$ and:

$$(*) \Leftrightarrow \left(\frac{x_2.y_1 - x_1.y_2}{p}\right)^2 + \left(\frac{x_1.x_2 + y_1.y_2}{p}\right)^2 = 1$$

$$\Rightarrow \frac{x_2.y_1 - x_1.y_2}{p} = 0 \;\; (1) \;\; ; \frac{x_1.x_2 + y_1.y_2}{p} = 1 \;\; (2)$$

(1)⇒ $x_2.y_1 - x_1.y_2 = 0$ => $x_2.y_1 = x_1.y_2$. Combine this with $\gcd(x_1; y_1) = \gcd(x_2; y_2) = 1$ we got this is illogical.

Thus, $\gcd[(x_2.y_1 - x_1.y_2); (x_2.x_2 + y_1.y_2)] = 1$. Then (*) is the Pythagorean equation with primitive roots. So:

$x_2.y_1 - x_1.y_2 = 2x_3.y_3$ ('cuz x_1 *and* x_2 are even) (3)

$x_1.x_2 + y_1.y_2 = |{x_3}^2 - {y_3}^2|$

$p = {x_3}^2 + {y_3}^2$

With $(x_3, y_3) = 1$ and x_3, y_3 are different about odd-even parity.

Without any lost of generality, we got that if $x_3 = x_1$ then $y_3 = y_1$

(3) ⇔ $x_2.y_1 - x_1.y_2 = 2x_1y_1$ ⇔ $y_1|(x_1.y_2)$ and since $(x_1; y_1) = 1$ then $y_1|y_2$, so $y_1<y_2$ (4). We also got that $x_1|x_2.y_1$ and since $(x_1; y_1) = 1$ then $x_1|x_2$ or $x_1 < x_2$ (5).

From (4) and (5), we got that $({x_1}^2 + {y_1}^2) < ({x_2}^2 + {y_2}^2)$, which is illogical.

So, $x_3 \neq x_1$, $y_3 \neq y_1$the equation has another root (x; y) = $(x_3; y_3)$.

The problem are now return to: $p = {x_1}^2 + {y_1}^2 = {x_3}^2 + {y_3}^2$

Continue proving like this, we have the equation has infinitely solution on Z which is illogical because there're just finitely the number of the positive integers that smaller than p.

So, it must be: $x_1 = x_2 = \cdots = x_n;\ y_1 = y_2 = \cdots = y_n\ (n \in N)$

Or the equation has only one solution on N (not counting its interchange) and the problem has been proved.■

B. Fermat equations:

Fermat equation or Fermat's Last Theorem was proposed by the French mathematician Pierre de Fermat. In mathematics, it's a famous theorem for its difficulty and the proving process of this theorem has led to many important discoveries in both algebra and analysis.

While studying the work of the ancient Greek mathematician Diophantus, Fermat wrote in pencil in the margin of his copy of a book by Diophantus, "The equation $a^n + b^n = c^n$ has no positive integral root for $n \geq 3$. I have discovered a truly remarkable proof which this margin is too small to contain." This equation is called Fermat equation.

For more than 350 years, many mathematicians tried to prove Fermat's statement or to disprove it by finding an exception. In June 1993, Andrew Wiles, an English mathematician at Princeton University, claimed the proof the theorem; however, in December of that year reviewers found a gap in his proof. On October 6, 1994, Wiles sent a revised proof to three colleagues. On October 25, 1994, after his colleagues judged it complete, Wiles published his proof.

Theorem 3.1:

The equation: $x^4 + y^4 = z^2$ has no positive integral root. And from that, get the proof of Fermat theorem for $n = 4$.

Proof: Suppose that the equation above does has integral root. Then let $(x_0;\ y_0;\ z_0)$ is the set of root that z_0 is the smallest one. Then:

Firstly, we got that $(x_0;\ y_0) = 1$. Indeed, if $gcd(x_0;\ y_0) > 1$ then let p is a prime that $p|x_0;\ p|y_0$. We have $p^4|x_0^4 + y_0^4 = z_0^2 => p^2|z_0 => x_0 = px_1;\ y_0 = py_1;\ z_0 = pz_1$=> $x_1^4 + y_1^4 = z_1^2$. So $(x_1;\ y_1;\ z_1)$ is a solution with $z_1 < z_0$. That's contradict with our supposition that z_0 is the smallest one.

Thus, $({x_0}^2;\ {y_0}^2;\ z_0)$ is a primitive Pythagorean triple. Suppose that x_0 is even and y_0 is odd then :

$$ {x_0}^2 = 2mn $$

$$ {y_0}^2 = m^2 - n^2 \quad (*) $$

$$ z_0 = m^2 + n^2 $$

with $gcd(m,n) = 1;\ m > n$; m,n are positive integral ;m,n is different about odd-even parity.

From ${y_0}^2 = m^2 - n^2$, we got $(y_0; m; n)$ is a a primitive Pythagorean triple, so:

$$ y_0 = a^2 - b^2 $$

$$ n = 2ab $$

$$ m = a^2 + b^2 \qquad (*) $$

with $(a;\ b) = 1;\ a > b; a, b$ are positive integral; a, b have different parity.

Assume that $x_0 = 2x_1$. Combine this with (*), we got that ${x_0}^2 = 4{x_1}^2 = 2mn = 4ab(a^2 + b^2)$ => ${x_1}^2 = ab(a^2 + b^2) = abm$. Yet, $(a;\ b) = 1 => (a;\ m) = (b;\ m) = 1. =>$ $a = {a_1}^2, b = {b_1}^2, m = {m_1}^2$. Combine this (**), we got that ${m_1}^2 = a_1^4 + b_1^4$. So, $(a_1; b_1; c_1)$ is a solution of the equation with $m_1 < m_1^2 = m < m^2 + n^2 = z_0$, contradict with our supposition that z_0 is the smallest one.■

From this, we got this corollary: Fermat last theorem is right for every $n = 2^k, k \geq 2$ 'cuz:

$x^{2^k} + y^{2^k} = z^{2^k} \Leftrightarrow (x^{2^{k-1}})^4 + (y^{2^{k-1}})^4 = (z^{2^{k-1}})^4$

Theorem 3.2:

The equation: $x^4 - y^4 = z^2$ (5)

has no positive integral root.

Proof: Suppose that the equation above does has integral root. Then let $(x_0;\ y_0;\ z_0)$ is the set of root that z_0 is the smallest one. Then:

Firstly, we got that $(x_0;\ y_0) = 1$. Indeed, if $\gcd(x_0;\ y_0) > 1$ then let p is a prime that $p|x_0;\ p|y_0$. We have $p^4|x_0^4 - y_0^4 = z_0^2 => p^2|z_0 => x_0 = px_1;\ y_0 = py_1;\ z_0 = pz_1$=> $x_1^4 - y_1^4 = z_1^2$. So $(x_1;\ y_1;\ z_1)$ is a solution with $z_1 < z_0$. That's contradict with our supposition that x_0 is the smallest one.

Thus, $({y_0}^2;\ z_0; {x_0}^2)$ is a primitive Pythagorean triple.

If x_0 is even and y_0 is odd then there exist positive integers m, n such that $(m,n) = 1;\ m > n$; m,n is different about odd-even parity and ${y_0}^2 = m^2 - n^2;\ {x_0}^2 = m^2 + n^2$. Hence, $m^4 - n^4 = (x_0y_0) => (m,n,x_0y_0)$ is a solution of (5) but $m^2 < m^2 + n^2 = {x_0}^2 => m < x_0$. That contradict with our supposition that z_0 is the smallest one.

If $y_0 = 2y_1$ is even then there exist positive integers m,n such that $(m,n) = 1;\ m > n$; m,n have different parity and $y_0^2 = 2mn;\ {x_0}^2 = m^2 + n^2$. Thus, $(m;\ n; x_0)$ is a primitive Pythagorean triple so there exist positive integers a,b such that $(a,b) = 1;\ a > b$; a,b have different parity and ${x_0}^2 = a^2 + b^2;\ and\ m = a^2 - b^2, n = 2ab$ or $n = a^2 - b^2, m = 2ab$. In every case, we all got that $mn = 2ab(a^2 - b^2) => y_0^2 = 2mn = 4ab(a^2 - b^2) => y_1^2 = ab(a^2 - b^2)$. Since (a, b) = 1 then $(a; a^2 - b^2) = 1;\ (b; a^2 - b^2) = 1$. Thus $a = a_1^2; b = b_1^2; a^2 - b^2 = r^2 => a_1^4 - b_1^4 = r^2$. Hence, $(a_1; b_1; r)$ is a solution of (5) but $a_1 < a_1^2 + b_1^2 = a + b \le a^2 + b^2 = x_0$. That contradict with our supposition that x_0 is the smallest one.■

Theorem 3.3:
Prove that the equation $x^4 - 4y^4 = z^2$ has no positive integral solution:

Proof: Suppose the equation does have positive integral solution. Let (x_0, y_0, z_0) is a solution with z_0 is the smallest one, similarly to the proof of the previous theorem, we get that $\gcd(x_0, y_0) = 1$. Assume that x_0 is even , let $x_0 = 2k\ then\ 16k^4 - 4y_0^4 = z_0^2 \Rightarrow z_0 = 2h, 4k^4 - y_0^4 = h^2$. Since $gcd\ (x_0, y_0) = 1$ then y_0 is odd. We get: $(x_0^2)^2 = z_0^2 + (2y_0^2)^2$. Since x_0 is odd and $\gcd(x_0, y_0) = 1$ so $gcd(x_0^2, 2y_0^2) = 1$.Thus, $(z^2, 2y_0^2, x_0^2)$ is a primitivePytagorean triple. Thus, there exist the positive integers a,b such that a> $b, \gcd(a,b) = 1$ and a,b has different odd-even parity such that $2y_0^2 = 2ab, x_0^2 = a^2 + b^2 \Rightarrow a = r^2, b = s^2 \Rightarrow x_0^2 = r^4 + s^4$, contradict with theorem 3.1 .

Theorem 3.4:
Prove that the equation $x^4 + 4y^4 = z^2$ has no positive integral solution.

Proof: Suppose the equation does have positive integral solution. Let (x_0, y_0, z_0) is a solution with z_0 is the smallest one, similarly to the proof of the previous theorem, we get that $\gcd(x_0, y_0) = 1$. Assume that x_0 is even , let $x_0 = 2k\ then\ 16k^4 + 4y_0^4 = z_0^2 \Rightarrow z_0 = 2h, 4k^4 + y_0^4 = h^2$. So, we get (y_0, k, h) is a soltuion with $h < 2h = z_0$, a contradiction. Thus, x_0 is odd. We get: $(x_0^2)^2 + (2y_0^2)^2 = z_0^2$. Since x_0 is odd and $\gcd(x_0, y_0) = 1$ so $gcd(x_0^2, 2y_0^2) = 1$.Thus, $(x_0^2, 2y_0^2, z_0)$ is a primitive

Pytagorean triple. Thus, there exist the positive integers a, b such that a> $b, \gcd(a, b) = 1$ and a, b has different odd-even parity such that $2y_0^2 = 2ab, x_0^2 = a^2 - b^2 \Rightarrow a = r^2, b = s^2 \Rightarrow x_0^2 = r^4 - s^4$, contradict with theorem 3.2 .

Excercise:

We note that the theorem 3.1 and 3.2 are right not only for just x, y, z are pairwise coprime but also for the case of $\gcd(x;\ y;\ z) > 1$.

We have some excercise from that:

- Application of theorem 3.1:

Excercise 1: Solve these equation **on N**:

a) $15y^4 - z^2 - 2y^2z + 1 = 0$

b) $x^4 + y^4 - x^2y^2 - z^2 - 2xyz = 0$

c) $x^4y^4 - 2x^2y^2 + 1 = x^4 + y^4$

d) $x^8 + y^8 - 3x^4y^4 = 625$

e) $y^4 = 168x^4 + 338x^2y + y^2$

Guide: a) $15y^4 - z^2 - 2y^2z + 1 = 0$

$\Leftrightarrow 1 + (2y)^4 = (z + y^2)^2$

According to the theorem 3.1, we got that: this equation doesn't has positive integral root so: $2y = 0; z + y^2 = 1$

Thus, $y = 0;\ z = 1$ is the only root of this equation on N.

b) $x^4 + y^4 - x^2y^2 - z^2 - 2xyz = 0$

$\Leftrightarrow x^4 + y^4 = (xy + z)^2$

From theorem 3.1, we got that: this equation doesn't has positive integral root so: $x = 0 \vee y = 0;$

- If $x = 0$ then $y^2 = xy + z = z$ .Let $y = t$ then this fomula:

$$x = 0;\ y = t;\ z = t^2$$

give us sets of roots of the equation.

- If $y = 0$ then $x^2 = xy + z = z$. Let $x = v$ then this fomula:

$$x = v;\ y = 0;\ z = v^2$$

is the second fomula that give us sets of roots of the equation.

c) $x^4y^4 - 2x^2y^2 + 1 = x^4 + y^4$

$\Leftrightarrow x^4y^4 + 1 = (x^2 + y^2)^2$

so $xy = 0 => x = 0 \vee y = 0;\ x^2 + y^2 = 1$

The equation has two solution on N: $(x;\ y) = (0;\ 1) \vee (x;\ y) = (1;\ 0)$

d) $x^8 + y^8 - 3x^4y^4 = 625$

$\Leftrightarrow 625 + x^4y^4 = (x^4 - y^4)^2$

So $xy = 0;\ |x^4 - y^4| = 25.$

Roots: $(x;\ y) = (0;\ 5) \vee (x;\ y) = (5;\ 0)$

e) $y^4 = 168x^4 + 338x^2y + y^2$

$\Leftrightarrow x^4 + y^4 = 169(x^2 + y)^2 = [13(x^2 + y)]^2$

$\Leftrightarrow x = 0 \vee y = 0$

Roots: $(x;\ y) = (0;\ 13) \vee (x;\ y) = (0;\ 0)$

- Application of theorem 3.2:

Excercise 2: Solve these equation **on N**:

a) $2x^4 + 2x^2 + 1 = z^4$

b) $-14x^2 + y^4 = 49$

c) $3x^4+y^4 - 102x^2 + 2061 = 0$

d) $3x^4 - 4x^2 + 1 = y^4$

e) $x^4 + 4x^3 + 297x^2 + 4x + 1 = y^4$

Guide: a) $2x^4 + 2x^2 + 1 = z^4$

$\Leftrightarrow x^4 + (x^2 + 1)^2 = z^4$

According to the theorem 3.2, we got that: this equation doesn't has positive integral root, yet $x^2 + 1 > 0$ so: $x = 0 => z = x^2 + 1 = 1$

Thus, $x = 0; z = 1$ is the only root of this equation on N.

b) $-14x^2 + y^4 = 49$

$\Leftrightarrow (x^2 - 7)^2 + y^4 = x^4$

$\Leftrightarrow x^4 - y^4 = (x^2 - 7)^2$

From theorem 3.1, we got that: this equation doesn't has positive integral root so: $x = 0 \vee y = 0;$

In both instances, we all got that the equation has no solution on N.

c) $3x^4+y^4 - 102x^2 + 2061 = 0$

$\Leftrightarrow (2x^2 - 51)^2+y^4 = x^4$

$\Leftrightarrow x^4 - y^4 = (2x^2 - 51)^2$

So $x = 0 \vee y = 0;$

But in both instances, we all got that the equation has no solution on N.

d) $3x^4 - 4x^2 + 1 = y^4$

$\Leftrightarrow x^4 - y^4 = (2x^2 - 1)^2$

So $x \vee y = 0$

Roots: $(x; y) = (0; 1) \vee (x; y) = (1; 0)$

e) $x^4 + 4x^3 + 297x^2 + 4x + 1 = y^4$

$\Leftrightarrow y^4 - (x + 1)^4 = (17x)^2$

From theorem 3.1, we got that: this equation doesn't has positive integral root, yet, this equation must be solve on N, so $x + 1 > 0$ so: $y = 0$, then:

$$(x + 1)^4 + (17x)^2 = 0$$

That's illogical so the equation has no solution on N.

C. Fermat - like equations:

Inspired from Fermat last thorem, we have another problem: Let n be a positive integers greater than 1. Find all distinguish the positive integers (a, b, c) so that a^n, b^n, c^n) make up a arithmetic progression.

This problem is equivalent to this one:

Find all the positive integral solution of the equation: $x^n + y^n = 2z^n$ which is called Fermat-like equations.

Here, we only talk about this equation with the primitive roots and mainly for n = 2, then:

$$x^2 + y^2 = 2z^2$$

It's easy to see that: x, y are not divisible by 2. Assume that x is odd, then y is odd, too. Then the left-side hand of the equation $\equiv 2\ (mod\ 4) \Rightarrow z$ is odd. If $p \mid x, p \mid y$ then $p \mid z \Rightarrow p = 1$. Thus $\gcd(x, y) = 1$ so $x \neq y\ or\ x = y = 1$.

If $x = y = 1$ then obviously , $(x; y; z) = (1; 1; 1)$ is a solution satisfied the theme.

If $x \neq y$ then assume that $x > y$. Let u = $\frac{x+y}{2}$; v = $\frac{x-y}{2}$ then: $u^2 + v^2 = z^2$. From $(x, y) = 1, x = u + v, y = u - v \Rightarrow (u, v) = 1$. So (u, v, z) is a primitive Pythagorean triple so:

$$u = m^2 - n^2\ (= 2mn)$$

$$v = 2mn\ (= m^2 - n^2)$$

$$z = m^2 + n^2$$

with $(m, n) = 1;\ m > n$; m, n are positive integral ;m, n is different about odd-even parity.So:

$$x = m^2 - n^2 + 2mn$$

$$z = m^2 + n^2$$

x, y has equal roles in the equation so we can conclude the solution is:

$$x = m^2 - n^2 + 2mn$$

$$y = n^2 - m^2 + 2mn$$

$$z = n^2 + m^2$$

with $(m, n) = 1;\ m, n$ are positive integral ;m, n is different about odd-even parity.

Example: with $m = 5, n = 4$ *then* $(49^2; 31^2; 41^2)$ make a number theory progression or $49^2 + 31^2 = 41^2$.

Chapter 4: APPLYING GEOMETRY IN NUMBER THEORY

There are many ways to solve the Diophantus equation like using divisibility; inequalities or the familiar like Fermat or Wilson,... theorem;... but sometimes these method can give us long and complex solutions. Meanwhile, by using geometric, we can have the simple , interesting solutions.

1) Example:

For an example: the Minkovsky theorem:" let $a, b,$ *and* c *are the integer such that* $a > 0$ *and* $ac - b^2 = 1$ *. Then, the equation* $ax^2 + 2bxy + cy^2 = 1$ *has integral roots" had been prove like this:*

Consider the perpendicular Cartesian coordinate system where scalar product is caculated by fomula:

$$((x, y), (x', y')) = axx' + bxy' + bx'y + cyy'$$

This scalar give us the distance from the origin of coordinates to (x, y) is

$$D((0,0); (x, y)) = \sqrt{((x, y); (x, y)} = \sqrt{ax^2 + 2bxy + cy^2}$$

We find the shortest distance from origin of coordinates to a certain point that differrent from (0; 0) of the integral net (m; n) (m, n are integers). Let's call this distanceis d^* *and the point is* $(m^*; n^*)$ *then:*

$$am^{*2} + 2bm^*n^* + cn^{*2} = d^{*2}(4)$$

The set of point (x, y) of the plane satisfied equality:

$ax^2 + 2bxy + cy^2 \leq d^{*2}$

is ab ellipse.If we this ellipse with ratio $1/2$*. Bring this contractive ellipse to the centers on the integral points (advance equally) then if all the ellipse we got intersect, they will intersect at edge-points only.*

IT's easy to see that the intersecting area of the ellipse with the triangle which has its summits at $(0, 0), (1, 0)$ *and* $(1, 1)$ *equal to a haft area of the whole ellipse , yet, this area equal to :*

So, the area that the ellipse taking in the triangle is $\pi d^{*2}/8$ *and this is just a part of the triangle's area, equal to* $1/2$*, which mean* $\pi d^{*2}/8 < ½ \Rightarrow d^{*2} < 4/\pi$

But d^{*2} *is positive integral so* $d^* = 1$*! Thus, the Minkowsky theorem are now proved.*

And now, I will introduce some application of geometry in number theory with the secant method which is a typical example of applying coordinate geometry in number theory, study about the integral points and the rational points on the curves – the method which lead to the notion of Elliptic curve, set the foundation for proving Fermat last theorem.

At first, we will get acquainted with through the fist example:

Example 1:Find all roots that different from (0,0,0) of the equation:

$$x^2 + 3y^2 = z^2 \quad (1)$$

Solution: At first, we alter the equation in to: $(\frac{x}{z})^2 + 3\,(\frac{y}{z})^2 = 1$

Let $u = x/z;\ v = y/z$ then $u^2 + 3v^2 = 1.$

With u, v are rational numbers. Our problem are now turn into finding all rational points on the curve (C): $u^2 + 3v^2 = 1$. It's easy to see that, (½; ½) is a rational point of the curve. So, if (u_0; v_0) is a another rational point of the curve then the angular coefficient of straight line between (½; ½) and (u_0; v_0) would be rational.On the other hand, if $v = k(u - ½) + ½$ is the straight line go through (½; ½) with the angular coefficient k then applying Viéte theorem for the abscissa equation, we will got that the second intersection point of this line with (E) would have integral co-ordinate s, which means:

$$u^2 + 3.[k.(u - \frac{1}{2}) + \frac{1}{2}]^2 = 1$$

$$\Leftrightarrow (3k^2 + 1).u^2 - 3.2.ku..(\frac{k-1}{2}) + 3.(\frac{k-1}{2})^2 = 1$$

$$\Leftrightarrow (3k^2 + 1).u^2 - 3.(k^2 - k).u + 3.(\frac{k-1}{2})^2 - 1 = 0$$

$$\Leftrightarrow (3k^2 + 1).u^2 - 3.(k^2 - k).u + \frac{3k^2 - 6k - 1}{4} = 0$$

By using Viéte theorem, we got:

$$u.u_0 = \frac{\frac{3k^2 - 6k - 1}{4}}{3k^2 + 1} = \frac{3k^2 - 6k - 1}{4.(3k^2 + 1)}$$

yet $u_0 = ½$ so we got that:

$$u = \frac{3k^2 - 6k - 1}{6k^2 + 2};$$

$$v = k.(u - \frac{1}{2}) + \frac{1}{2} \Rightarrow v = \frac{-3k^2 - 2k + 1}{6k^2 + 2}$$

We can also find the set of roots of (1) from this.

For an example: with $k = 3$ we got: $u = 1/7;\ v = -4/7$ and we have $(1;\ 4;\ 7)$ as a root of (1).

And now, we will talk some more about its application in:

2) Ilovi theorem:

a) IloVi theorem:

This theorem talk about the set of roots of the equation has type of $ax^2 + y^2 = z^2$ with a doesn't has quadratic submultiple that bigger than one.

Of course, in this book's framework, we only talk about the orginal set of root or x, y, z are relatively prime. We will find its general fomular by using the secant method:

We alter the equation into:

$$ax^2 + y^2 = z^2$$

$$\Leftrightarrow a.(\frac{x}{z})^2 + (\frac{y}{z})^2 = 1.$$

Let $u = \frac{x}{z}; v = \frac{y}{z}$ with u, v are rational then:

$$au^2 + v^2 = 1$$

It's definitely that this equation always takes $(u_0;\ v_0) = (0;\ -1)$ as its rational root.

This is similar to the problem before, we got:

$v = ku - 1$ with k is rational

$$au^2 + (k.u - 1)^2 = 1$$

$$\Leftrightarrow (k^2 + a).u^2 - 2.ku = 0$$

By using Viéte theorem, we got:

$$u + u_0 = -\frac{-2k}{k^2 + a} = \frac{2k}{k^2 + a}$$

yet $u_0 = 0$ so:

$$u = \frac{2k}{k^2 + a}$$

$$v = k.u + 1 => v = \frac{k^2 - a}{k^2 + a}$$

Because k is rational so: there exist 2 integers e, f such that $(e, f) = 1$ and $k = \frac{e}{f}$

Then: $u = \frac{2k}{k^2 + a} = \frac{2.(\frac{e}{f})}{(\frac{e}{f})^2 + a} = \frac{2ef}{af^2 + e^2} = \frac{x}{z}$ (*)

$$v = \frac{k^2 - a}{k^2 + a} = \frac{(\frac{e}{f})^2 - a}{(\frac{e}{f})^2 + a} = \frac{-af^2 + e^2}{af^2 + e^2} = \frac{y}{z} \quad (**)$$

Suppose that $gcd(-af^2 + e^2; af^2 + e^2) = d$

Then $(-af^2 + e^2) \vdots d$ and $(af^2 + e^2) \vdots d$

so $-af^2 + e^2 + af^2 + e^2 = 2e^2 \vdots d$

$$af^2 + e^2 + af^2 - e^2 = 2af^2 \vdots d$$

yet $gcd(e,f) = 1$ so $d \mid 2a$, combine with (*); (**) and $gcd(x,z) = gcd(y,z) = gcd(x,z) = 1$, we got:

$$x = \frac{2ef}{d}; \quad y = \frac{-af^2 + e^2}{d}; \quad z = \frac{af^2 + e^2}{d} \quad (*)$$

but we just take the integral roots so this fomular can also be write as:

$$x = \frac{2ef}{d};$$

$$y = \frac{|-af^2 + e^2|}{d};$$

$$z = \frac{af^2 + e^2}{d}.$$

with $d \mid 2a$.

We call this is the fomular (I)

Continue expanding (*),we will got fomular (II),concrete :

- Case 1: a is even:
  - If z is even then $z^2 \equiv 0 \ (mod\ 4)$ and y is even => $y^2 \equiv 0 \ (mod\ 4)$ => $ax^2 \equiv 0 \ (mod\ 4)$ but a doesn't have quadratic submultiple that bigger than one, which mean a is not divisible by 4. So, $x \vdots 2$. That is contradict with the supposition $(x,y,z) = 1$.
  So, z is odd ⇒ y is odd.
  - If d is even then $z = \frac{af^2 + e^2}{d} \in Z \Rightarrow e$ is even ⇒ $e^2 \equiv 0 \ (mod\ 4)$ => If $d \vdots 4$ then $af^2 \vdots 4$, yet a is even but has no submultiple that bigger than 1 so $f \vdots 2$ => $gcd(e,f) = 2$, which is contradict with the supposition $gcd(e,f) = 1$.
  So d is not divisible by 4, which means $d \mid a$.

$z = \frac{af^2 + e^2}{d} \in Z$ => d | e. Let $v = d; m = f; a = u.v; e = nv$ then

$$z = um^2 + vn^2$$

$$x = 2mn$$

$$y = -um^2 + vn^2$$

- Case 2: $a \equiv 3\ (mod\ 4)$:
  - If z is odd then: x, y have different parity.

$z^2 \equiv 1 \pmod 4$ => if y is even then $ax^2 \equiv 3 \equiv z^2 \pmod 4$. That's illogical!

⇨ x is even and y is odd.

If d⋮2 then, from $x = \frac{2ef}{d}$, we got that e, f is different about parity.

⇨ $(-af^2 + e^2)$ is odd, yet $y = \frac{|-af^2 + e^2|}{d} \vdots 2$. That's illogical!

So, d is odd, yet $d \mid 2a \Rightarrow d \mid a$.

Let $a = ud\ ;\ e = dn\ ;\ m = f$ then:

$$x = 2nm\ ; \quad y = -um^2 + dn^2; \quad z = um^2 + dn^2$$

Let $d = v$ we got that:

$$x = 2nm\ ; \quad y = -um^2 + vn^2; \quad z = um^2 + vn^2$$

  - If z is even then: x, y, e, f all are odd

⇨ $d \vdots 2$. Let $d = 2v$ then $v \mid a$.

⇨ $x = \frac{ef}{v}\ ; \quad y = \frac{|-af^2 + e^2|}{2v}; \quad z = \frac{af^2 + e^2}{2v}$.

Let $a = uv;\ e = v.n\ ;\ m = f$ then:

$$x = nm\ ; \quad y = \frac{|-um^2 + vn^2|}{2}\ ; \quad z = \frac{um^2 + vn^2}{2}.$$

u, v have equal role so, we can also write like this:

$$x = nm\ ; \quad y = \frac{-um^2 + vn^2}{2}\ ; \quad z = \frac{um^2 + vn^2}{2}.$$

- Case 3: $a \equiv 1\ (mod\ 4)$: it's definitely that z is odd.
  - If d is odd then: e, f is different about odd-even quality ⇒ y is odd.
    $d \mid 2a$, yet d is odd ⇒ $d \mid a$.

Let $a = ud\ ;\ e = dn\ ;\ m = f$ then:

$$x = 2nm\ ; \quad y = -um^2 + dn^2; \quad z = um^2 + dn^2$$

Let $d = v$ then we got:

$$x = 2nm\,; \quad y = -um^2 + vn^2; \quad z = um^2 + vn^2$$

- If d is even then: e, f all are odd

Combine this with $a \equiv 1\ (mod\ 4)$, we got $that\ (-af^2 + e^2) \vdots 4$

⇨ y ⋮ 2. Let $d = 2v$ then $v \mid a$.

⇨ $x = \frac{ef}{v}$; $y = \frac{|-af^2 + e^2|}{2v}$; $z = \frac{af^2 + e^2}{2v}$.

Let $a = uv;\ e = v.n\,;\ m = f$ then:

$$x = nm\,; \quad y = \frac{|-um^2 + vn^2|}{2}\,; \quad z = \frac{um^2 + vn^2}{2}.$$

because u and v have equal role so, we can also write like this:

$$x = nm\,; \quad y = \frac{-um^2 + vn^2}{2}\,; \quad z = \frac{um^2 + vn^2}{2}.$$

2) IloVi fomula:

Conclude: In conclusion, we got two fomular for the type of the equation $ax^2 + y^2 = z^2$ with x, y, z are the positive integer like this:

Fomula **(I):** $x = \frac{2ef}{d}$;

$$y = \frac{|-af^2 + e^2|}{d}.;$$

$$z = \frac{af^2 + e^2}{d}.$$

with $\boldsymbol{d \mid 2a}$ if a is odd and $\boldsymbol{d \mid a}$ if a even.

Fomular **(II):**

- With a is even:

All the integeral roots of this equation can be found by using this fomula:

$$x = 2mn\,;$$
$$y = um^2 - vn^2;$$
$$z = um^2 + vn^2.$$

With $uv = a;\ u, v, m, n$ is integral; $gcd(m;\ n) = 1$.

- With a is odd:
  All the integeral roots of this equation can be found by using these two fomula:

$$x = mn\,; \quad y = \frac{um^2 - vn^2}{2}; \quad z = \frac{um^2 + vn^2}{2}.$$

wtih $uv = a;\ u,v,m,n$ are odd; $gcd(m;\ n) = 1$.

and $x = 2nm$; $y = -um^2 + vn^2$; $z = um^2 + vn^2$

with $uv = a;\ u,v,m,n$ are integral; $gcd(m;\ n) = 1$.

3) Applications of IloVi theorem:

We'll talk about this more in the next chapter but now, there're some simple example:

Example 1: Sovle :$5x^2 + 6y^2 + 10xy = z^2$ (*)

in integral field, suppose x, y, z are pairwise coprime.

Solution: (*) $\Leftrightarrow 5(x + y)^2 + y^2 = z^2$

It's definitely that $(x + y)$; y; z are relatively prime.

Applying IloVi fomula (II),combine with the equal roles of m and n,we have two case:

Case 1: $x + y = mn$; $y = \frac{|5m^2 - n^2|}{2}$; $z = \frac{5m^2 + n^2}{2}$.

$\Rightarrow$ $x = mn - y = mn - \frac{|5m^2 - n^2|}{2}$ $(x > 0)$;

Case 2: $x + y = 2mn;\ y = |5m^2 - n^2|$; $z = 5m^2 + n^2$

$\Rightarrow$ $x = 2mn - y = 2mn - |5m^2 - n^2|$ $(x > 0)$.

Excercise: Find whole the positive integers x, y such that:

a) $15x^4 + y^2 = 289$

b) $1043x^2 + y^4 = 177^2$

c) $17x^2 + y^2 = 213^2$

d) $51x^2 + y^2 = 900$

e) $73x^2 + y^2 = 49969^2$

f) $11x^2 + 371y^2 = 5929$

g)$39x^2 + 13y^2 = 5476$

h) $68445x^2 + 469y^2 = 1463^2$

i) $117x^2 + y^4 = 361^2$

j)$112x^2 + 111y^2 + 222xy + 22x = 4503$

k) $4x^2 + 14y^2 - 3x + 14xy = 26904$

m)$332x^2 + 331y^2 + 662xy - 2x = 2839224$

l)$11x^2 + 22x + 11 + 2xy + 2y = 494198$

n) $8x^2 + 56y^2 + 2x + 14y = 29583$

p) $2x^4 + 1 = y^2$

q) $26.(2x^2 + 1)^2 + (x^2 + 19^2)^2 = z^2$

g) $12x^4 + 2x^2 + \frac{1}{4} = z^2$

h) $15x^2 + y^2 = z^4$

Guide:

a) $11x^2 + 371y^2 = 5929$

$\Leftrightarrow 10(x + y)^2 + (x - 19y)^2 = 491^2$

b) $39x^2 + 13y^2 = 5476$

$\Leftrightarrow 3(x + 2y)^2 + (6x - y)^2 = 74^2$

c) $68445x^2 + 469y^2 = 1463^2$

$\Leftrightarrow 117(x + 2y)^2 + (234x - y)^2 = 1463^2$

j)$112x^2 + 111y^2 + 222xy + 22x = 4503$

$\Leftrightarrow 111(x + y)^2 + (x + 11)^2 = 68^2$

k) $4x^2 + 14y^2 - 3x + 14xy = 26904$

$\Leftrightarrow 7(x + 2y)^2 + (x - 4)^2 = 232^2$

m) $332x^2 + 331y^2 + 662xy - 2x = 2839224$

$\Leftrightarrow 331(x + y)^2 + (x - 1)^2 = 1685$

l) $11x^2 + 22x + 11 + 2xy + 2y = 494198$

$\Leftrightarrow 10(x + 1)^2 + (x + y + 1)^2 = 703^2$

n) $8x^2 + 56y^2 + 2x + 14y = 29583$

$\Leftrightarrow 7(x - y)^2 + (x + 7y + 1)^2 = 172^2$

CHAPTER 5: HIGH DEGREE EQUATION

A: Some more theorem:

Theorem 5.1: Prove that the equation:

$2ap^4 + q^4 = t^2$ with a is a prime, $a \neq 8k+7, a \neq 8k+1$ has no positive integral set of roots.

Guide: If $gcd(q,t) > 1$ then suppose $1 < b|gcd(q,t)$ and $b^2 \nmid gcd(q,t)$e get $b^2|q^4, b^2|t^2$ so $b^4|q^4, b^2|2ap^4$ while with a is a prime so $b^2|p^4$ or $b|p$. From this, we get $b^4|p^4, b^4|q^4 \Rightarrow b^4|t^2$ or $b^2|gcd(q,t)$, a contradiction with our supposition is $b^2 \nmid gcd(q,t)$.

So, gcd(q, t) =1; p, q, are pairwise coprime.

Now, suppose (x, y, z) is the set of equation with z take the smallest value then $2ax^4 + y^4 = z^2$. By using IloVi fomula, we get:

$x^2 = \frac{2ef}{d}; y^2 = \frac{|2af^2 - e^2|}{d}$; z = $\frac{2af^2+e^2}{d}$ with $d|4a, gcd(e,f) = 1$

- If $d = 4a$ then $4|e^2 \Rightarrow 4|2af^2 \Rightarrow 2|f$ while 2|e and $gcd(e,f) = 1$, a contradiction.
- If $d = 2a$ then we get $2a|e^2$ and from $x^2 = \frac{2ef}{2a} = \frac{ef}{a}$ and $gcd(e,f) = 1$, we get: there exist $e_1, f_1 \in \mathbb{N}^*$ $gcd(e_1, f_1) = 1$ such that $e = 4ae_1^2, f = f_1^2$ then:

$$y^2 = |f_1^4 - 8ae_1^2|$$
$$\Leftrightarrow y^2 = f_1^4 - 8ae_1^2 \text{ or } y^2 = -f_1^4 + 8ae_1^2$$
$$\Leftrightarrow 8ae_1^2 + y^2 = f_1^4 \text{ or } y^2 + f_1^4 = 8ae_1^2$$

But f_1 and y both are odd, so if $y^2 + f_1^4 = 8ae_1^2$ then $y^2 + f_1^4 \equiv 2 \equiv 8ae_1^2 \equiv 0(mod\ 4)$, a contradiction.

So $8ae_1^2 + y^2 = f_1^4$ or $2a(2e_1)^2 + y^2 = f_1^4$.

Obviously e_1, f_1, y are pairwise coprime. Applying loVi fomula we get:

$2e_1^2 = \frac{2e_2f_2}{d_1}$; $f_1^2 = \frac{2af_2^2+e_2^2}{d_1}$ $with\ d_1|4a,\ e_2, f_2 \in \mathbb{N}^*, \gcd(e_2, f_2) = 1$.

- If $d_1 = 4a$ then $f_1 \in \mathbb{N}^* \Rightarrow 2|e_2 \Rightarrow 4|e_2^2 \Rightarrow 4|2af_2^2 \Rightarrow 2|f_2$ while $2|e_2$ and $\gcd(e_2, f_2) = 1$, a contradiction.
- If $d_1 = 2a$ then $e_1^2 = \frac{e_2f_2}{2a}$; $f_1^2 = f_2^2 + \frac{e_2^2}{2a}$ so $2a|e_2^2$, combine with $e_1^2 = \frac{e_2f_2}{2a}$, $\gcd(e_2, f_2) = 1$, we can let: $e_2 = 2ae_3^2$; $f_2 = f_3^2$ then $f_1^2 = f_3^4 + 2ae_3^4$ with f_1, f_3, e_3 are pairwise coprime, which means $(p, q, t) = (e_3, f_3, f_1)$ is of a solution of $2ap^4 + q^4 = t^2$ on $\mathbb{N}^*$.

We also get that z = $\frac{2af^2+e^2}{d}$ = $\frac{2af^2+e^2}{2a} = f^2 + 8ae_1^4 > f \geq f_1$, contradict with our supposition is z is the smallest one.

- If $d_1 = a$ then $e_1^2 = \frac{e_2f_2}{a}$; $f_1^2 = 2f_2^2 + \frac{e_2^2}{a} \Rightarrow a|e_3$. Since $\gcd(e_2, f_2) = 1$, we can let $e_2 = ae_4^2, f_2 = f_4^2$ with $\gcd(e_4, f_4) = 1$ then $f_1^2 = 2f_4^4 + ae_4^4$.
  If $2|f_4$ then $f_1^2 \equiv ae_4^4 \equiv 1(mod\ 8)$ while $a \neq 8k+1$, a contracdiction.
  If $2|e_4$ then $2|f_1 \Rightarrow 4|f_1^2 \Rightarrow 4|2f_4^4 \Rightarrow 2|f_4^4$ while $f_4$is odd , a contracdiction.
- If $d_1 = 1$ then $e_1^2 = e_2f_2$; $f_1^2 = 2af_2^2 + e_2^2$. Let $e_2 = e_5^2, f_2 = f_5^2$ then

$$f_1^2 = 2af_5^4 + e_5^4$$

which means $(p, q, t) = (f_5, e_5, f_1)$ is of a solution of $2ap^4 + q^4 = t^2$ on $\mathbb{N}^*$ with z = $\frac{2af^2+e^2}{d} = f^2 + 8ae_1^4 > f \geq f_1$, contradict with our supposition is z is the smallest one.

- If d = a then $x^2 = \frac{2ef}{a}; y^2 = \frac{|2af^2-e^2|}{a}$.
  Since y is odd, a is odd, we get e is odd, $a|e^2$. Comebine this with $x^2 = \frac{2ef}{a}$ we get : there exist the positive integers e_6, f_6 with $gcd(e_6, f_6) = 1$ such that
  $e = ae_6^2, f = 2f_6^2 \Rightarrow y^2 = |8f_6^4 - ae_6^4|$
  $\Rightarrow y^2 = 8f_6^4 - ae_6^4$ or $y^2 = -8f_6^4 + ae_6^4$
  If $y^2 = 8f_6^4 - ae_6^4$ then $y^2 \equiv 1 \equiv -ae_6^4 \equiv -1(mod\ 8)$, a contradiction.

If $y^2 = -8f_6^4 + ae_6^4$ then $ae_6^4 \equiv y^2 \equiv 1(mod\ 8)$ while $a \neq 8k + 1$, a contradiction.

- If d=1 then $x^2 = 2ef; y^2 = |2af^2 - e^2|$
  Let $e=e_7^2; f = 2f_7^2$ then $y^2 = |8af_7^4 - e_7^2|$.
  From this, we do similiarly to the case d=2a.

In connclusion, the equation:

$2ap^4 + q^4 = t^2$ with a is a prime, $a \neq 8k + 7, a \neq 8k + 1$ has no positive integral set of roots.

From the solution of this problem, we also get that:

$8ap^4 + q^4 = t^2$ with a is a prime, $a \neq 8k + 7, a \neq 8k + 1$ has no positive integral set of roots.

So:

Theorem:

The two equations: $2ap^4 + q^4 = t^2$ and $8ap^4 + q^4 = t^2$ with a is a prime, $a \neq 8k + 7, a \neq 8k + 1$ has no positive integral set of roots.

B: Fouth degree equations and some equations with the even degree:

Example 1*:*
Prove that the equation $867a^4 + 51a^2 + 1 = b^2$ has no positive integral roots.

Guide: Rewrite the equation as

$$3(34\ a^2 + 1)^2 + 1 = (2b)^2\ .$$

Now, applying IloVi theorem, we get:

$$34a^2 + 1 = m_1 n_1$$

and $1 = \frac{3m_1^2 - n_1^2}{2}$ or $1 = \frac{m_1^2 - 3n_1^2}{2}$ with m_1, n_1 are odd and $\gcd(m_1, n_1) = 1$.

- If $1=\frac{m_1^2-3n_1^2}{2}$ then ${3n_1}^2+2={m_1}^2$ which means ${m_1}^2\equiv {3n_1}^2+2\equiv 2(mod\ 3)$, a contradiction.
- If $1=\frac{3m_1^2-n_1^2}{2}$ then combine with $34a^2+1=m_1n_1$, we get $34a^2+\frac{3m_1^2-n_1^2}{2}=m_1n_1$

or $17a^2+{m_1}^2=\left(\frac{m_1+n_1}{2}\right)^2$. Since m_1,n_1 are odd, we get $\frac{m_1+n_1}{2}\in\mathbb{N}^\star$. We have $17a^2+{m_1}^2\equiv 2(mod\ 4) while\ \left(\frac{m_1+n_1}{2}\right)^2\equiv\rho\in\{0,1\}(mod\ 4)$, a contradiction.

In conclusion, the equation above has no positive integral roots.

Example 2:
Prove that the equation $x^4+9x^2y^2+27y^4=z^2$ is not solvable in $\mathbb{N}^*$.

Guide: Here, I'll only talk about the instance in which x, y, z are pairwise coprime, the other is intended for the reader.

We see that if x is even then y,z is odd, then from $x^4+9x^2y^2+27y^4=z^2$, we get that $27y^4\equiv 3y^4\equiv z^2(mod\ 4)$ wile $3y^4\equiv 3(mod\ 4); z^2\equiv 1(mod\ 4)$, a contradiction.

So, x is odd.

If y is odd then $x^4\equiv 1(mod\ 8); 9x^2y^2\equiv 9\equiv 1(mod\ 8); 27y^4\equiv 27\equiv 3\ (mod\ 8)\Rightarrow x^4+9x^2y^2+27y^4\equiv 5\ (mod\ 8) while\ z^2\equiv ٧\in\{0;1;4\}(mod\ 8)$, a contradiction.

Rewrite the equation as $4x^4+36x^2y^2+4.27y^4=4z^2$

$$\Leftrightarrow (2x^2+9y^2)^2+27y^4=4z^2$$

So y is even. . Obiously $2x^2+9y^2; 3y^2; 2z$ are pairwise coprime. By using IloVi theorem, we get that:

- $3y^2=2mn;\ 2x^2+9y^2=-3m^2+n^2$: by taking modulo 3 for $2x^2+9y^2=3m^2-n^2$, we eliminate this case.
- $3y^2=2mn;\ 2x^2+9y^2=3m^2-n^2$: From $3y^2=2mn$, we get $2|m$ or $2|n\Rightarrow 3m^2-n^2=4m^2-(m^2+n^2)\equiv -(m^2+n^2)\equiv -1\equiv 3(mod\ 4)\ while\ 2x^2+9y^2\equiv 2(mod\ 4)$('cuz x is odd, y is even), a contradiction.
  Now, the proof is completed .

Note: Another proof of this problem is available in the book: "elementary theory of numbers-PWN-Polish Scientific Publishers, 1998" (page 75).

Example 3:
Prove that the equation: $8a^4+1=b^4$ has no positive integral solution.

Guide:

Now, suppose the equation above does have positive integral solution. Let $(a,b)=(n,m)$ is the set of roots with b is the smallest then b is odd and:

$8n^4+1=m^4\Leftrightarrow 2(2n^2)^2+1=(m^2)^2$

By using IloVi fomular, we get:

$2n^2 = \frac{2ef}{d}; 1 = \frac{|2f^2-e^2|}{d}; m^2 = \frac{|2f^2+e^2|}{d}$ with $d|4$.

- If d=4: $|2f^2 - e^2| = 4 \Rightarrow 2|e^2 \Rightarrow 4|e^2 \Rightarrow 4|2f^2 \Rightarrow 2|f \Rightarrow e, f$ both are divisible for 2 while gcd(e, f)=1, a contradiction.
- If d=2: $m^2 \in \mathbb{N}^* \Rightarrow 2|e$. Combine with $n^2 = \frac{ef}{d} = \frac{ef}{2}$ and $\gcd(e, f) = 1$ we get : there exist the positive integers g, h such that $\gcd(g, h) = 1$ and $e = 2g^2; f = h^2$. Then:

$$|2h^4 - 4g^4| = 2 \; and \; 2h^4 + 4g^4 = 2m^2$$
$$\Rightarrow |h^4 - 2g^4| = 1 \; and \; h^4 = -2g^4 + m^2$$
$$\Rightarrow |-2g^4 + m^2 - 2g^4| = 1$$
$$\Rightarrow |m^2 - 4g^4| = 1$$
$$\Rightarrow m^2 - 4g^4 = 1 \; or \; 4g^4 - m^2 = 1$$

  According to Theorem 3.4:, we get the equation $m^2 - 4g^4 = 1$ or $m^2 = 4g^4 + 1$ has no positive integral solution, so $4g^4 - m^2 = 1$.

$$4g^4 - m^2 = 1$$
$$\Leftrightarrow (2g^2 - m)(2g^2 + m) = 1$$

  $\Leftrightarrow 2g^2 - m = 1 = 2g^2 + m \; (since \; m, g > 0) \Leftrightarrow m = 0$, a contradiction.
- If d=1: m^2 is odd, so $2f^2 + e^2$ is odd which means e is odd.
  Similarly, there exist the positive integers g, h such that $\gcd(p, q) = 1$ and $e = p^2; f = q^2$.
  Then: $|2q^4 - p^4| = 1 \; and \; 2q^4 + p^4 = m^2$ so $2q^4 - (m^2 - 2q^4)| = 1 \Leftrightarrow |m^2 - 4q^4| = 1$.
  Treat this similarly like d=2, we get $|m^2 - 4q^4| = 1$ has no positive integral solution.
  And we completed the proof. ☺

Example 4:
Prove that the equation: $2a^4 + 1 = b^4$ has no positive integral solution.

Guide:

Now, suppose the equation above does have positive integral solution. Let $(a, b) = (n, m)$ is the set of roots with b is the smallest then b is odd and:

$2n^4 + 1 = m^4$

By using IloVi fomular, we get:

$n^2 = \frac{2ef}{d}; 1 = \frac{|2f^2-e^2|}{d}; m^2 = \frac{|2f^2+e^2|}{d}$ with $d|4, e, f$ are the integers, $\gcd(e, f) = 1$.

- If d=4: $|2f^2 - e^2| = 4 \Rightarrow 2|e^2 \Rightarrow 4|e^2 \Rightarrow 4|2f^2 \Rightarrow 2|f \Rightarrow e, f$ both are divisible for 2 while gcd(e, f)=1, a contradiction.
- If d=2: $m^2 \in \mathbb{N}^* \Rightarrow 2|e$. Combine with $n^2 = \frac{2ef}{d} = ef$ and $\gcd(e, f) = 1$ we get : there exist the positive integers g, h such that $\gcd(g, h) = 1$ and $e = 4g^2; f = h^2$. Then:

$$|2h^4 - 16g^4| = 2$$
$$\Rightarrow |h^4 - 8g^4| = 1$$
$$\Rightarrow h^4 - 8g^4 = 1 \; or \; 8g^4 - h^4 = 1$$

  As we had proved before at example 3, $h^4 - 8g^4 = 1$ has no positive integral solutions.
  $8g^4 - h^4 = 1 \Leftrightarrow 8g^4 = h^4 + 1 \Leftrightarrow h^4 \equiv 7 (mod \; 8)$, a contradiction.

If $d = 1$: $n^2 = 2ef\ while\ \gcd(e, f) = 1$, so $m^2 = 2f^2 + e^2$ is odd ⇒ e is odd, f is even. There exist the positive integers p, q such that $\gcd(p, q) = 1$ and $e = p^2; f = 2q^2$. Then $|8q^4 - p^4| = 1$. Treat this similarly like d=2, we get $|8q^4 - p^4| = 1$ has no positive integral solution.
And we complete the proof.☺

Example 5:
Find all positive integral solution of the equation: $y^2 = 8x^4 + 1$

Guide: Obviously $gcd(x, y) = 1$ and y is odd.

Rewrite the equation as: $(y + 1).(y - 1) = 8x^4$

Since y is odd, we get: $\gcd(y + 1; y - 1) = 2$

Combine with $(y + 1).(y - 1) = 8x^4$ we get: there exist the integers a, b such that $\gcd(a, b) = 1$ and :

$$y + 1 = 2a^4\ and\ y - 1 = 4b^4$$

Or

$$y + 1 = 4a^4\ and\ y - 1 = 2b^4$$

If $y + 1 = 2a^4\ and\ y - 1 = 4b^4$ then $2a^4 - 4b^4 = 2 \Leftrightarrow a^4 = 2b^4 + 1$ and as we had proved at example 4, this type of equation has no positive inegral solution.