Chapter 1: SQUARE NUMBER

At first, we will take a review at some properties of square number:

1.The basic properties:

- Suppose that $n \in N$ and $n = x^2$ then:

$n = x^2 \equiv a \in \{0;1\} \pmod 3$;

$n = x^2 \equiv a \in \{0;1\} \pmod 4$;

$n = x^2 \equiv a \in \{0;1;4\} \pmod 5$;

$n = x^2 \equiv a \in \{0;1;3;4\} \pmod 6$;

$n = x^2 \equiv a \in \{0;1;2;4\} \pmod 7$;

$n = x^2 \equiv a \in \{0;1;4\} \pmod 8$;

$n = x^2 \equiv a \in \{0;1;3;4;7\} \pmod 9$;

$n = x^2 \equiv a \in \{0;2; 3; 7; 8\} \pmod{10}$;

$n = x^2 \equiv a \in \{0;1;3;4;5;9\} \pmod{11}$;

$n = x^2 \equiv a \in \{0;1;4;9\} \pmod{16}$;

.

.

.

- *Suppose that $n \in N$, $n = x^2$ and n is divisible by a prime number a then n is divisible by a^2 or:*
  For n is square, a is prime: $a \mid n \Leftrightarrow a^2 \mid n$.

Problem for applying:

1/ Prove that $A = 7^{2n}+5$ can't be a square number for every positive integral number m.

Guide: Suppose that $A = 7^{2n}+5 = k^2$ then $k^2 \equiv a \in \{0,1;2;4\}$ (mod 7}, yet $A = 7^{2n}+5 \equiv 5 \pmod 7$. That's illogical!

2/Is there any square number that has sum of its digits is 537?

Guide: The answer is no, proof:

Suppose n is square, n has sum of its digits is 537.

Let S(n) be the sum of its digits then S(n) = 537 = 59.9+6

- ⇨ n ≡ 6 (mod 9) so n can't be a square number, contradict with our supposition that n is square and we got the proof.

3/ Find all the positive integer x such that x^2+4 is the product of two consecutive odd number.

Guide: Suppose that $x^2 + 4 = n.(n+2)$ with n is odd then:

$$x^2 + 5 = (n + 1)^2$$

n is odd so $(n + 1)^2$ is divisible by 4 => x is odd => $x^2 \equiv 1 \pmod 4$, yet $5 \equiv 1 \pmod 4$ => $(x^2 + 5) \equiv 2\ (mod\ 4)$, yet $(n + 1)^2 \equiv 0\ (mod\ 4)$.That's illogical!

In conclusion, we got no positive integer x that x^2+4 is the product of two consecutive odd number.

2.Some other special properties:

1: For every integer n:

- there's no integer x satisfied $n^2 < x^2 < (n+1)^2$.
- If $n^2 < x^2 < (n+2)^2$ then $x = n+1$.

Example:

2: If $xy = z^2$ and $(x, y) = 1$ then x, y are square.

We use this property to prove that:

3: There does not exist two consecutive positive integers that their product is a square number.

Proof: Suppose there are two consecutive positive integer x and $x + 1$ such that $x(x + 1) = n^2$, then:

x and $x + 1$ are relatively prime, so: $x = x'^2$; $x + 1 = y^2$ => $x'^2 + 1 = y^2$

- ⇨ $(y + x').(y - x') = 1$
- ⇨ $y + x' = y - x' = 1$
- ⇨ $x' = 0$
- ⇨ $x = x'^2 = 0$

Contradict with the supposition: x is positive integral!

Example: Find 3 consecutive natural number that their product is a square number.

Guide: Suppose that these 3 consecutive natural number are $x - 1;\ x;\ x + 1$

Then $(x - 1).x.(x + 1) = y^2$ (1)

And: $(x;\ x-1) = (x;\ x+1) = 1.$ (2)

Suppose gcd$(x-1; x+1) = d$ then $d \mid [(x-1)+(x+1)]$ => $d \mid 2 => d = 1$ $or\ d = 2.$

- $d = 2$: $2|(x-1) and\ 2|(x+1)$ .Combine this with (1) and (2) we got: $x = a^2;\ x-1 = 2b^2;\ x+1 = 2c^2\ with\ a, b, c \in Z$, a, b, c are relatively prime $=> 2c^2 - 2b^2 = 2 => (c+b).(c-b) = 1$

⇨ $c = 1;\ b = 0 => x-1 = 0.$

⇨ The three number we need to find are 0; 1 ;2.

- d = 1 so $(x-1) = u^2; x = v^2;\ x+1 = t^2.$ This is similiar to d = 2 and we found the three number are 0; 1; 2.

  In conclusion, The three number we need to find are 0; 1 ;2.

Excercise:

Let x, y, z are the positive integers.Prove $that\ (xy+1).(yz+1).(zx+1)$ is a square number if and if only $(xy+1);\ (yz+1); (zx+1)$all are squares.

Chapter 2: SUM OF TWO SQUARE NUMBERS.

1) Review:

In this chapter, we will learn how to write a positive integer into the form of sum of two square.

At first, we will study about the problem: which positive integer can be write down to the form of two quadratic number or for which n that the equation $x^2 + y^2 = n \, with \, n \in N$ has integral root.

Theorem 2.1:

"If p prime then p is the sum of two integral squares if and only if only $p \neq 4k + 3$ (k$\in Z$)."

Proof: suppose that the equation $x^2 + y^2 = p$ has integral roots $(x;\, y)$. We know that $g \equiv a \in \{0; 1\}(mod\ 40) => (x^2 + y^2) \equiv b \in \{0; 1; 2\}(mod\ 4)$, so $p \neq 4k + 3, k \in Z$.

Now, we suppose that $p \neq 4k + 3, k \in Z$. If $p = 2$ then $(1;\ 1)$ is a solution. Now, consider so $p = 4k + 1, k \in Z$. Since -1 is not a square (mod p) then there exist a $\in Z$ that $a^2 \equiv -1\ (mod\ p)$. Let $q = |\sqrt{p}|$. Consider $(q + 1)^2$ numbers $\{x + ay\}, x = 0, 1, \ldots, q;\ y = 0,1, \ldots, q$. Since $(q + 1)^2 > p$ then there exist $x_1 + ay_1 \equiv x_2 + ay_2$ $(mod\ p)$

⇨ $(x_1 - x_2) \equiv a(y_2 - y_1)$ (mod p) => u² $\equiv a^2v^2 \equiv -v^2(mod\ p)$

⇨ $u^2 + v^2 \equiv 0(mod\ p)$ where u = $|x_1 - x_2| \leq q < \sqrt{p}$;

v = $|y_2 - y_1| \leq q < \sqrt{p}$. So $p|\ u^2 + v^2$. Since 0 < u² $+v^2$< $p + p = 2p$ then u² $+v^2 = p^2$

<u>Several things you need to know:</u>

With m = $a^2 + b^2$, n = $c^2 + d^2$:

mn = $(a^2 + b^2).(c^2 + d^2) = (ac+bd)^2 + (ad - bc)^2$.

- If p is a prime number such p=4k +3 and (a,b) = 1 then a^2+b^2 is undivisible by p, so:If a positive number that its fractorization into primes is $p_1{}^{a_1}.p_2{}^{a_2} \ldots .p_k{}^{a_k}$ với p_1, p_2,..., $p_k$are primes and $a_1, a_2, \ldots, a_k$ are positve integers then the p = $x^2 + y^2$ doesn't have solution if its fratorization into primes has a factor q= $(4t + 3)^{2r+1}$ with 4t + 3 is prime .

  From these comments, we have the method of forming a positive integer into sum of two squares:

1)If p is a prime:

Of course, here, the equation $p = x^2 + y^2$ has solution if and if only $p = 4k + 1$, k $\in$ Z. We will solve this equation by using modulo number theory, limiting the root's region,....

Example: Solve: $x^2 + y^2 = 881$

Guide: Assume that x, y all are undivisible by 5 then $t^2\ (t = x \vee y) \equiv a \in \{1; 4\}$ (mod 5) so $x^2 + y^2 \equiv b \in \{0; 2; 3\}\ (mod\ 5)\ , yet\ 881 \equiv 1(mod\ 5)$. That's illogical! S, there's must be x or y is divisible by 5, suppose that's x then $0 \leq x < 30$ (because $30^2 >$

881). Since then, $x \in \{0; 5; \ldots; 25\}$. By trying all the possible values, we got one solution $(x; y) = (25; 16)$.

In conclusion, the equation has two roots: $(x, y) = (25; 16); (16; 25)$.

Theorem 2.2: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).

Note: From this theorem, we got an experienceis that: when we had already found a solution of the equation $p = x^2 + y^2$ *, we don't have to try the others cases because the equation has only one solution.*

We will come back to prove this at a later chapter.

2)If p is not prime:

We have three steps:

1. Write down it down to the form of: p = $(q_1^{2a_1}.q_2^{2a_2} \ldots . q_h^{2a_h}).(p_1.p_2 \ldots p_k)$ with $q_1, q_2, \ldots, q_h$ are the primes that have the form of $4d + 3$ and $p_1, p_2, \ldots, p_k$ are primes that have the form of $4d + 1$.
2. Express $p_1, p_2, \ldots, p_k$ under the form of sum of two squares.
3. Uses the equality $mn = (a^2 + b^2).(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.

Examples: Express these numbers to sum of two squares:

* 392

$392 = 7.56$ but 7 is prime and $7 = 4.1 + 3$ so 392 can't be express to sum of two squares

* 221

$$221 = 17.13 = (1^2 + 4^2).(2^2 + 3^2)$$
$$= (1.2 + 4.3)^2 + (1.3 - 2.4)^2 = 14^2 + 5^2$$
$$= (1.3 + 4.2)^2 + (1.2 - 3.4)^2 = 11^2 + 10^2.$$

In conclusion, $221 = 14^2 + 5^2 = 11^2 + 10^2$.

* 1225

$1225 = 7^2.5.5$

Yet, 7 is prime with the form of $4t + 3$ and

$$5.5 = (1^2 + 2^2).(1^2 + 2^2)$$
$$= (1.1 + 2.2)^2 + (1.2 - 2.1)^2 = 5^2 + 0^2$$
$$= (1.2 + 2.1)^2 + (1.1 - 2.2)^2 = 4^2 + 3^2.$$

thus, $1225 = 7^2.5.5 = 35^2 + 0^2 = 28^2 + 21^2$.

4. **Theorem 2.3:**(theorem about the number of ways to express a number to forms of sum of two square(if possible)): Let p is the number that p can be expressed to the form of sum of two square; p = $(q_1^{2a_1}.q_2^{2a_2} \ldots . q_h^{2a_h}).(2^m p_1.p_2. \ldots . p_n)$ with

$q_1, q_2, \dots, q_h$ are the primes that have the form of $4d + 3$ and $p_1, p_2, \dots, p_k$ are primes that have the form of $4d + 1$, $p_1, p_2, \dots, p_n$ are the primes that differrent from 2; $\delta(p)$ is the number of ways to express p to forms of sum of two squares then: $\delta(p) = 2^n$.

Proof:

Firstly, we know that with q is product of primes that have the form of $4d + 3$; $q = q_1^{2a_1}.q_2^{2a_2} \dots .q_h^{2a_h}$ then there's only one way to express the number $j = gq$ with j is a prime that has the form of $4d + 1$ to sum of two squares and $j = {j_1}^2 + {j_2}^2$. If not, suppose that there exist j_3, j_4 such that j_1, j_2, j_3, j_4 are pairwise coprime and $j = {j_3}^2 + {j_4}^2$. then ......

We know that $z = u^2 + v^2$ with z is prime , $(u; v) = 1$ has $u = v$ if $u = v = 1$; $z = 2$ or $2 = 1^2 + 1^2$. Then the product gz with $g = c^2 + d^2; (c, d) = 1$ is $g = (c^2 + d^2).(1^2 + 1^2) = (c + d)^2 + (c - d)^2$

- ⇨ There's only one ways to express $k = gz$ to sum of two squares or
- ⇨ $\delta(2^m p_1.p_2. \dots .p_n) = \delta(p_1.p_2. \dots .p_n)$ (2.3.1)

Now, all we have to do is count $\delta(p_1.p_2. \dots .p_n)$.

Let $p_i = a_i^2 + b_i^2;\ i = 1, 2, 3, \dots, n$

from the theorem 2.2, we got that: since p_i is prime then the existence of a_i and b_i is one only.

We got that: $p_i = a_i^2 + b_i^2;\ p_{i+1} = a_{i+1}^2 + b_{i+1}^2$

⇨ $p_i.p_{i+1} = (a_i^2 + b_i^2).(a_{i+1}^2 + b_{i+1}^2)$

$$= (a_1 a_2 + b_1 b_2)^2 + (a_1 b_2 - a_2 b_1)^2$$

$$= (a_1 b_2 + a_2 b_1)^2 + (a_1 a_2 - b_1 b_2)^2$$

- ⇨ If n = 2 then we got $\delta(p) = 4 = 2^2$
- ⇨ $p_i.p_{i+1}.p_{i+2}$ has $4.2 = 2^3$ ways for n = 3
- ⇨ $p_i.p_{i+1}.p_{i+2}.p_{i+3}$ has $2^3.2 = 2^4$ ways.
- ⇨ ...
- ⇨ For n = k, we have 2^n ways. (2.3.2)

From (2.3.1) and (2.3.2) we got the proof.

3.Theorem 2.4:

Lemma 2.1:(The theorem about the integral roots existence of first-degree equation of two unknowns) The equation $ax + by = c$ $(a \neq 0, b \neq 0;\ a, b, c \in Z$ has integral roots if and if only $gcd(a;\ b)|c$.

Proof: Suppose that $(x_0;\ y_0)$ is a solution of the equation, then $ax_0 + by_0 = c$. If $gcd(a;\ b) = d$ then $d \mid ax_0 + by_0 = c$. On the other side, suppose that $d = (a;\ b) \mid c$ then $c = dc_1$ and we got two integers $x_1;\ y_1$satisfied $d = ax_1 + by_1 => dc_1 = a(a_1 c_1) + b(y_1 c_1) = c$ and the equation has integral roots. ☺

Lemma 2.2: Minkowski theorem: For a, b, c are the integers, $a > 0$ and $ac - b^2 = 1$, the $ax^2 + 2bxy + cy^2 = 1$ has integral solution.

Proof: see at chapter: application of geometry in number theory.

Theorem 2.4: If a, b, c are the positive integers such that ac = $b^2 + 1$ then a can be express to sums of two squares and reverse.

Proof:

- ✓ For the propitious part :

We have: $ax^2 + 2bxy + cy^2 = 1$

$\Leftrightarrow (ax + by)^2 + (ac - b^2)y^2 = a$

or $(ax + by)^2 + y^2 = a.('cuz\ ac - b^2 = 1)$

- ✓ For the converse theorem: Suppose $a = f^2 + y^2$ then according to the first lemma, there exist x and b such that: $ax + by = f$.
  And then, we have that $a = f^2 + y^2 = (ax + by)^2 + y^2$

or $a^2x^2 + (b^2 + 1)y^2 + 2abxy = a$

⇨ $a \mid (b^2 + 1)$. Thus, there exist c such that $b^2 + 1 = ac$.
Note: we can also prove this:

For a, b, c are the integers such that $ac = b^2 + 1$ *then, there exist* u, v, p, q *satisfied* $a = u^2 + v^2$; $c = p^2 + q^2$; $b = up + vq$.

(Iran 2001)

4) Excercise:

1.Write these numbers down to the form of sum of two square:

52; 2378; 1105; 5066;

40009; 170; 1993;

Guide:

- $52 = 4^2 + 6^2$
- $170 = 13^2 + 1^2 = 7^2 + 11^2$
- $1105 = 5.13.17 = 23^2 + 24^2 = 32^2 + 9^2 = 33^2 + 4^2 = 31^2 + 12^2$
- $2378 = 43^2 + 23^2 = 47^2 + 13^2$
- $5066 = 71^2 + 5^2 = 65^2 + 29^2$

- $1961 = 40^2 + 19^2 = 44^2 + 5^2$

2.Solve:

$a)\ x^2 + y^2 = 18818$

$b)\ x^2 + y^2 = 5825$

Guide:

a) $18818 = 97^2.2 = (4^2+9^2).(4^2+9^2).2 = 97^2+97^2 = 7^2 + 137^2$.

b) $5825 = 25.233$

yet $25 = (1^2+2^2).(1^2+2^2) = 5^2+0^2 = 3^2+4^2$

so $5825 = (5^2+0^2).(3^2+4^2).(13^2 + 8^2) = 65^2 + 40^2 = 28^2 + 71^2 = 7^2 + 76^2$.

3. Solve equations with positive integral roots:

$a)\ 10x^2 + 53y^2 + 38xy = 1765$

$b)\ 97x^2 + 29y^2 - 106xy = 1481$

$c) x^2 + 2xy + 2y^2 = 241$

*Guide:*a) $10x^2 + 53y^2 + 38xy = 1765$ (1)

Note that $10 = 1^2 + 3^2$; $53 = 7^2 + 2^2$; $38 = 2(7.3 - 2.1)$ and we also got this equality: $(ax + by)^2 + (cx + dy)^2 = (a^2+c^2)x^2 + (b^2+d^2)y^2 + 2(ab+cd)xy$. So:

(1)⇔ $(3x + 7y)^2 + (x-2y)^2 = 1765 = 5.353 = (1^2+2^2)(8^2+17^2)$

$$= 1^2 + 42^2 = 26^2 + 33^2.$$

$x, y > 0 => 3x + 7y > x - 2y$. So:

$$\begin{cases} 3x+7y = 42 \\ x - 2y = \pm 1 \end{cases} \quad \text{or} \quad \begin{cases} 3x+7y = 33 \\ x - 2y = \pm 26 \end{cases}$$

By solving these systems of equations, we find out the only solution of (1) is $(x;\ y) = (7;\ 3)$.

$b)\ 97x^2 + 29y^2 - 106xy = 1481$

⇔ $(4x-2y)^2 + (9x-5y)^2 = 1481$

yet, 1481 is prime, $1481 = 35^2 + 16^2$

$c) x^2 + 2xy + 2y^2 = 241$

$$\Leftrightarrow (x+y)^2+y^2=241$$

Yet, $241 = 15^2+4^2$

4.Solve: $n.(n+1).(n+2).(n+3) + m(m+2m) = 17520$ in Z.

Guide: the equation $\Leftrightarrow (n^2+3n+1)^2 + (m+1)^2 = 17522 = 2.8761 = 2.(56^2 + 75^2) = 19^2 + 131^2$.

The equation has 8 sets of roots:
$(n;m) =$
$(3;\ 130);\ (-6;\ 130);\ (3;\ -132);\ (-6;-132);\ (10;\ 18);\ (-13;\ 18);\ (10;\ -20);\ (-13;\ -20)$.

5. Solve: $A = 1.2.3 + 2.3.4 + \ldots. + k.(k+1).(k+2) + (m^2+2).(m^2+4).(m^2+6).(m^2+8) = 54\,629\,835$ on Z.

Guide: Let $S = 1.2.3 + 2.3.4 + \ldots. + k.(k+1).(k+2)$

then $4S + 1 = k.(k+1).(k+2).(k+3) + 1 = (k^2 + 3k + 1)^2$

Let $P = (m^2+2).(m^2+4).(m^2+6).(m^2+8)$

then $P + 2^4 = (m^4 + 5m^2.2 + 5.2^2)^2 = (m^4 + 10m^2 + 20)^2$

Thus: $4A = 4S + 1 + 4.(P + 2^4) - 65$

$= 54\,629\,835$

$$\Leftrightarrow (k^2 + 3k + 1)^2 + 4.(m^4 + 10m^2 + 20)^2 = 218\,519\,405$$

6. Solve: $x^2 + y^2 + z^2 - 2yz = 12\,322$ on N

Guide: the equation $\Leftrightarrow (x - y + z)^2 + (x + y - z)^2 = 12322.2$

Yet, $12322.2 = 61.101.4 = (5^2+6^2).(1^2+10^2).2^2$

$$= 130^2 + 88^2 = 110^2 + 112^2$$

7. Solve: $x^2 = 2y^3 + 21$ on Z.

Guide: the equation $\Leftrightarrow x^2 + (y^3 - 1)^2 = y^6 + 22$

We consider that: x is always odd, then: $x^2 \equiv 1\ (mod\ 8)$

If y is even then $y^3 - 1$ is odd => $(y^3 - 1)^2 \equiv 1 (mod\ 8)$. Thus:

$x^2 + (y^3 - 1)^2 \equiv x^2 + (y^3 - 1)^2 \equiv 1 + 1 \equiv 2\ (mod\ 8)$

While $y^6 + 22 \equiv y6 + 22 \equiv 6\ (mod\ 8)$ .That's illogical!

Then y is odd => $y^6 \equiv 1 \ (mod\ 4)$ => $y^6 + 22$ has the form of 4k +3 so it can't be expressed to sum of two squares while the left –hand side of the equation has the form of sum of two squares. That's illogical!

Thus, the equation above has no integral roots.

Chapter 3: SOME ESSENTIAL DIOPHANTINE EQUATIONS