CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049
SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF MATHEMATICS
DN PG COLLEGE MEERUT

Dr Satish Kr Gupta

H-4649, CH-09 Number Theory (1)

Perfect Numbers

Divisors of 6 are 1, 2, 3, 6

Improper divisor of 6 is 6

proper divisors of 6 are 1, 2, 3

Perfect Number

A positive integer n is called perfect if the sum of its proper divisors is equal to n.

Ex. Take $n = 6$

Its proper divisors are 1, 2, 3

Sum of proper divisors of 6 $= 1+2+3$
$= 6$

$\therefore$ 6 is perfect Number

Note. A number n is called perfect if

$$\sigma(n) = 2n$$

ex $n=6$, $\sigma(6) = \frac{2^2-1}{2-1} \times \frac{3^2-1}{3-1} = 3 \times 4 = 12$

$\sigma(6) = 2 \times 6$ [i.e $\sigma(n) = 2n$]

Take $n = 496 = 2^4 \times 31$

$$\sigma(n) = \frac{2^5-1}{2-1} \times \frac{31^2-1}{31-1}, \quad n = 496$$

$= 31 \times 32$

$= 2 \times 496$

$\sigma(n) = 2n$

$\therefore$ 496 is a perfect number.

Theorem 1, If (2^k-1) is a prime $(k>1)$, The $2^{k-1}(2^k-1)$ is a perfect Number

Proof, Let $2^k - 1 = p$, p is prime

To prove $2^{k-1}(2^k-1)$ is perfect

So $\sigma\{2^{k-1}(2^k-1)\} = \sigma(2^{k-1} \cdot p)$

$= \sigma(2^{k-1}) \cdot \sigma(p)$

$$\sigma(2^{k-1}(2^k-1)) = \sigma(2^{k-1})\,\sigma(p)$$

$$= \frac{2^{k-1+1}-1}{2-1} \times (p+1)$$

$$= (2^k-1)(2^k)$$

$$= 2 \times 2^{k-1}\cdot(2^k-1)$$

$\sigma(n) = 2n$, $n = 2^{k-1}(2^k-1)$.

i.e. $n = 2^{k-1}(2^k-1)$ is a perfect number.

Note: A number of the form $2^{k-1}(2^k-1)$ $(k>1)$ is called Euclid type number, Here k we mean the natural number greater than one.

Theorem 2. Prove that every even perfect number is of the form $2^{k-1}(2^k-1)$ where (2^k-1) is a prime. 2018

Proof. Let n be an even perfect number then $n = 2^{k-1} \times a$ for some $k>1$ and for some odd integer a.

Since $(2^{k-1}, a) = 1$, we have

$$\sigma(n) = \sigma(2^{k-1}\cdot a)$$

$$= \sigma(2^{k-1})\,\sigma(a) \quad [\because \sigma(p_1p_2) = \sigma(p_1)\sigma(p_2) \text{ if } (p_1,p_2)=1]$$

$$= \frac{2^{k-1+1}-1}{(2-1)} \cdot \sigma(a)$$

$$\sigma(n) = (2^k-1)\,\sigma(a) \quad \text{---(1)}$$

$$\Rightarrow 2n = (2^k-1)\,\sigma(a) \quad [\because \sigma(n) = 2n, \text{ as it is given } n \text{ is perfect}]$$

$$\Rightarrow 2\cdot 2^{k-1}\cdot a = (2^k-1)\,\sigma(a) \quad [n = 2^{k-1}\times a]$$

$$\Rightarrow 2^k \cdot a = (2^k-1)\,\sigma(a) \quad \text{---(2)}$$

$$\Rightarrow 2^k \mid (2^k-1)\,\sigma(a)$$

$$\Rightarrow 2^k \mid \sigma(a) \text{ as } (2^k, 2^k-1) = 1$$

H-4049 Ch-09 Number Theory (03)
Dr Satish Kr Gupta

$2^k \mid \sigma(a)$

$\Rightarrow \sigma(a) = 2^k \times q$ for some integer q — (3)

equation (2) and (3) implies

$2^k \cdot a = (2^k - 1)\sigma(a)$

$2^k \cdot a = (2^k - 1)[2^k \times q]$, from (3)

$\Rightarrow a = (2^k - 1)q$ ——— (4)

If Two cases arise

(1) $q > 1$ (2) $q = 1$

(1) $q > 1$ then a has atleast four factors namely $1, 2^k - 1, q, (2^k - 1)q$

$\Rightarrow \sigma(a) \geq$ sum of those factors

$= 1 + 2^k - 1 + q + 2^k q - q$

$\sigma(a) \geq 2^k(1 + q)$

which is a contradiction as $\sigma(a) = 2^k \cdot q$

So $q = 1$

i.e. $a = (2^k - 1)$ (from (4))

Hence $n = 2^{k-1} \cdot a = 2^{k-1}(2^k - 1)$

To show $(2^k - 1)$ is prime

We have $2^k - 1 = a$ ——— (5)

From (3) $\sigma(a) = 2^k \times q$

$\Rightarrow \sigma(a) = 2^k$ ——— (6) [$\because q = 1$]

from (5) and (6) we observe that

$a = (2^k - 1)$ has only two factor 1 & $(2^k - 1)$

$\Rightarrow (2^k - 1)$ is prime

Perfect Number

Theorem 3 If (a^k-1) is prime. $(a>0, k>1, 2$

then $a=2$ and k is a prime

Proof. We know

$(a^k-1) = (a-1)(a^{k-1} + a^{k-2} + \dots + a+1)$

since it is given $a>0 \Rightarrow \dots a>1$ (must be)

$\therefore (a^{k-1} + a^{k-2} + \dots + a+1) > a+1 > 2$

It is given (a^k-1) is prime

$\therefore$ $a-1$ must be equal to 1 [$\because$ Any prime has only two factors 1 & itself]

$\Rightarrow a-1=1$

$\Rightarrow a=2$.

To prove k is prime

suppose if possible k is not prime

$\Rightarrow k = rt$, where $r \neq 1, t \neq 1$

$a^k-1 = a^{rt-1}$

$= (a^r)^t - 1$

$a^k-1 = (a^r-1)(a^{r(t-1)} + a^{r(t-2)} + \dots + a^r+1)$

$= A \cdot B$ say $A>1, A = a^r-1$

$B>1, B = (a^{r(t-1)} + \dots + a^r+1)$

which is not possible.

as a^k-1 is prime

$\therefore$ k must be prime

Perfect Number

Theorem 4. Every even perfect number has the last digit either 6 or 8.

Proof. Let n be an even perfect number.

It is of the form $2^{k-1}(2^k-1)$ for some prime number k.

$\Rightarrow$ k will be of the form $(4q+1)$ or $(4q+3)$, where $q \in N$.

If $k = 4q+1$ then

$$n = 2^{k-1}(2^k-1)$$

$$\Rightarrow n = 2^{4k}\left(2^{4q+1}-1\right]$$

$$\Rightarrow n = (16)^q\left[2\cdot 16^q - 1\right] \quad \left[\begin{array}{l} 2^{4q} = (2^4)^q \\ 2^{4q+1} = 2\cdot 2^{4q} \\ \qquad = 2\cdot(2^4)^q \end{array}\right]$$

The last digit of $(16)^q$ will be 6

and last digit of $(2\cdot 16^q - 1)$ will be 1

$\therefore$ last digit of n in this case will be 6

If $k = 4q+3$ then

$$n = 2^{k-1}(2^k-1)$$

$$\Rightarrow n = 2^{4q+2}\left[2^{4q+3}-1\right]$$

$$n = 4\cdot(16)^q\left[8\cdot(16)^q - 1\right]$$

Here we observe that

the last digit of $4\cdot(16)^q$ will be 4

and the last digit of $8\cdot(16)^q$ will be 7

$\therefore$ In this case

last digit of n will be 8 $\quad [4\times 7 = 28]$

Hence every even perfect number has the last digit either 6 or 8.

Theorem 08. Every even perfect number $n = 2^{k-1}(2^k-1)$ is the sum of first $\left(\frac{k-1}{2}\right)$ odd cubes.

Proof Let n is a perfect number then we have

Let $n = 2^{k-1}(2^k-1)$, k is odd prime

$2^{\frac{1}{2}(k-1)} = a$

then to prove $1^3+3^3+\cdots\cdots(2a-1)^3 = n$, where $a = \left(\frac{k-1}{2}\right)$.

$$LHS = 1^3+3^3+5^3+\cdots+(2a-1)^3$$

$$= \sum_{r=1}^{a}(2r-1)^3$$

$$= \sum_{r=1}^{a}\left[8r^3-12r^2+6r-1\right]$$

$$= 8\sum_{r=1}^{a}r^3 - 12\sum_{r=1}^{a}r^2 + 6\sum_{r=1}^{a}r - \sum_{r=1}^{a}1$$

$$= 8\cdot\left[\frac{a(a+1)}{2}\right]^2 - 12\left[\frac{a(a+1)(2a+1)}{6}\right] + 6\,\frac{a(a+1)}{2} - a$$

$$= 8\left[\frac{a^2(a^2+2a+1)}{4}\right] - 2\left[a(2a^2+2a+a+1)\right] + 3(a^2+a) - a$$

$$= 2\left[a^4+2a^3+a^2\right] - 4a^3 - 6a^2 - 2a + 3a^2 + 3a - a$$

$$= 2a^4 + a^3(4-4) + a^2(2-6+3) + a(-2+3-1)$$

$$= 2a^4 - a^2$$

$$= a^2[2a^2-1] \qquad , \; a = 2^{\frac{k-1}{2}}$$

$$= 2^{k-1}(2^k-1) \qquad a^2 = \left(2^{\frac{k-1}{2}}\right)^2 = 2^{k-1}$$

$$= n$$

$LHS = RHS$, Proved.

H-4049, CH-09 (07) Number Theory.
Dr Satish Kr Gupta

Examples on perfect Numbers

(1) Show $n = 2^{10}(2^{11}-1)$ is not a perfect number

Sol We know n is a perfect number

if $\sigma(n) = 2n$

Given $n = 2^{10}(2^{11}-1)$

$$\sigma(n) = \sigma(2^{10}(2^{11}-1))$$
$$= \sigma(2^{10}, 23\times 89) \quad [\because 2^{11}-1 = 23\times 89)$$
$$2048-1 = 2047$$
$$= \sigma(2^{10})\,\sigma(23)\,\sigma(89)$$
$$= \frac{2^{11}-1}{2-1} \times \frac{23^2-1}{23-1} \times \frac{89^2-1}{89-1}$$
$$= (2^{11}-1)(24)(90)$$
$$24 = 2\times 2\times 2\times 3$$
$$90 = 3^3\times 2\times 5$$
$$= (2^{11}-1)(2^4\times 3^4\times 5)$$
$$\neq 2^{10}(2^{11}-1)\cdot 2$$

$\therefore$ $n = 2^{10}(2^{11}-1)$ is not a perfect number.

(2) If n is an even perfect number then prove $\sum_{d|n} \frac{1}{d} = 2$.

Solution. We have $\sum_{d|n} \frac{1}{d} = \sum_{d|n} \left(\frac{d}{n}\right)$

$$= \frac{1}{n} \sum_{d|n} d$$
$$= \frac{1}{n}\sigma(n) \quad [\because \sigma(n) = \sum_{d|n} d]$$
$$= \frac{2n}{n}$$

$$\boxed{\sum_{d|n} \frac{1}{d} = 2}$$ Proved.

(3) Let $n = 2^{k-1}(2^k - 1)$, $k \geq 2$ be any even perfect number. Then show that

$$\prod_{d|n} d = n^k$$

Soln. Let $n = 2^{k-1}(2^k - 1)$, $k > 2$ be any even perfect number ——— (1)

To prove $\prod_{d|n} d = n^k$ ——— (2)

We know that

$$\prod_{d|n} d = n^{\frac{1}{2}\tau(n)} \quad \text{——— (3)}$$

Now $\tau(n) = \tau[2^{k-1}(2^k - 1)]$

$= \tau(2^{k-1})\,\tau(2^k - 1)$

$= (k-1+1)(1+1)$

$= k \cdot 2$

$\tau(n) = 2k$ ——— (4)

(3) and (4) $\Rightarrow$

$$\prod_{d|n} d = n^{\frac{1}{2}\tau(n)}$$

$$= n^{\frac{1}{2}\cdot 2k}$$

$$\prod_{d|n} d = n^k$$

———— , proved.

Ex $n = 496$, $k = 5$ $\left[n = 2^{k-1}(2^k - 1),\ k = 5 \right]$

$n = 2^4(2^5 - 1)$

$\therefore \prod_{d|496} d = (496)^5$

i.e Product of divisors of $496 = (496)^5$. etc

Ex Do yourself

Find $\sum_{d|n} d = ?$ if $n = 8128$, $k = 7$

$n = 33550336$, $k = 13$ etc

$n = 2^{k-1}(2^k - 1)$

(4) Find the last two digits of the perfect number

$$n = 2^{19936}[2^{19937} - 1]$$

Soln $n = 2^{19936}[2 \cdot 2^{19936} - 1]$

$n = 16^{4984}[2 \cdot 16^{4984} - 1]$ $\left[2^{19936} = (2^4)^{4984}\right]$

Now

$2^{19936} = 16^{4984} \equiv 36 \pmod{100}$ ——— (1)

and $2 \times 2^{19936} = 2 \times 16^{4984} - 1 \equiv 71 \pmod{100}$ ——— (2)

$\Rightarrow n = 16^{4484}[2 \times 16^{4984} - 1] \equiv 36 \times 71 \pmod{100}$

$n \equiv 56 \pmod{100}$

Required answer is 56.

Mersenne Prime

The number $M_n = 2^n - 1$, $n > 1$, which is prime is called Mersenne prime

Note. If M_k is Mersenne prime then $2^{k-1} \cdot M_k$ is a perfect number

Few Mersenne primes are → M_2, M_3, M_5, M_7

. As of Feb 2020, 51 Mersenne primes have been obtained. The largest Mersenne prime no is $(2^{82589933} - 1)$, Dec 7, 2018

Theorem 1. If $p > 2$ is a prime then any prime divisor of M_p must be of the form $(2kp+1)$ for $k = 1, 2, 3, \ldots$ ——— (1)

Proof. Let $M_p = (2^p - 1)$

Let q be a prime divisor of M_p

$\Rightarrow q \mid (2^p - 1)$

$\Rightarrow q$ is an odd integer as $2^p - 1$ is odd

By Fermat's theorem, we have

$$2^{q-1} \equiv 1 \pmod{q} \quad [\because (2, q) = 1]$$

If $(p, q-1) = d$

$\Rightarrow d \mid p$ and $d \mid (q-1)$

since p is prime $\Rightarrow d = p$ or $d = 1$ ——— (2)

① $\Rightarrow$ if $d = p$ and $q - 1 = dt$ $[\because d \mid (q-1) \Rightarrow q - 1 = dt$ for some integer $t]$

i.e. $d = p$ and $q = dt + 1$

$q = dt + 1$

$\Rightarrow q = pt + 1 \quad [\because d = p]$

$\Rightarrow t$ must be even as p & q are both odd

Let $t = 2k$ for some integer k

$\therefore q = p \cdot 2k + 1$ for some $k = 1, 2, \ldots$

② $\Rightarrow$ If $d = 1$ then

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p, q-1)} - 1 \quad [(p, q-1) = \text{g.c.d of } p \& (q-1)]$$

$$= 2^d - 1$$

$$= 2^1 - 1 \quad [\because d = 1]$$

$$= 1$$

which is a contradiction as $q \mid (2^p - 1)$ and $q \mid (2^{q-1} - 1)$

So $d \neq 1$.

Fermat Number

An integer of the form

$$f_m = 2^{2^m} + 1, \quad m \geq 0$$ is called fermat number

Note. If f_m is a prime, it is called fermat prime.

ex $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$, $f_4 = 65537$

In 1732, Euler find $f_5 = 4,294,967,297$, a composite number which is divisible by 641.

Theorem 1. Here f_5 is divisible by 641.

Proof. Take $a = 2^7$, $b = 5$ then

$$1 + ab = 1 + 2^7 \cdot 5 = 1 + 640$$
$$= 641$$

Now,

$$1 + ab - b^4 = 1 + (a - b^3) b$$
$$= 1 + (2^7 - 5^3) 5$$
$$= 1 + (128 - 125) 5$$
$$= 1 + 3 \cdot 5$$
$$= 16$$
$$= 2^4 \quad \text{---------- (1)}$$

Now $f_5 = 2^{2^5} + 1 = 2^{32} + 1$

$$= 2^4 \cdot 2^{28} + 1$$
$$= 2^4 \cdot (2^7)^4 + 1 = 2^4 a^4 + 1$$
$$= (1 + ab - b^4) a^4 + 1 \quad [\because 2^4 = 1 + ab - b^4]$$
$$= (1 + ab) a^4 + 1 - a^4 b^4$$
$$= (1 + ab) a^4 + (1 - a^2 b^2)(1 + a^2 b^2) \quad [\because 1 - a^4 b^4 = (1 - a^2 b^2) \times (1 + a^2 b^2)]$$
$$= (1 + ab)[a^4 + (1 - ab)(1 + a^2 b^2)]$$

$$f_5 = 641 [a^4 + (1 - ab)(1 + a^2 b^2)]$$

$\Rightarrow 641 \mid f_5$, Proved.

Theorem 1 H-4049 CH-9, (12)
Dr Satish Kr Gupta

II method.

We know

$$f_5 = 2^{2^5}+1 = 2^{32}+1 \quad \text{—(1)}$$

$$641 = 2^7 \times 5 + 1 \qquad [2^7 \times 5 = 640]$$

$$\therefore 5 \times 2^7 \equiv -1 \pmod{641}$$

$$\Rightarrow (5 \times 2^7)^4 \equiv (-1)^4 \pmod{641} \qquad \left\{ a \equiv b \pmod m \Rightarrow a^4 \equiv b^4 \pmod m \right\}$$

$$\Rightarrow 625 \times 2^{28} \equiv 1 \pmod{641}$$

$$\Rightarrow 2^{28} \equiv \frac{1}{625} \pmod{641}$$

$$\Rightarrow 2^{32} \equiv \frac{2^4}{625} \pmod{641}$$

$$\equiv \frac{2^4 + 641k}{625} \pmod{641} \text{ for some integer } k$$

$$\equiv \frac{2^4 - 641}{625} \pmod{641}, \text{ if } k = -1$$

$$\Rightarrow 2^{32} \equiv -1 \pmod{641}$$

$$\Rightarrow 2^{32} + 1 \equiv 0 \pmod{641}$$

$$\Rightarrow 641 \mid [(2^{2^5}+1) - 1]$$

$$\Rightarrow 641 \mid f_m, \text{ proved}, m = 5.$$

number

$2^n | 2^{m-n} - 1$

Thm For $m, n \geq 0$, $(F_m, F_n) = 1$
i.e Fermat number are relatively prime

Proof. We know the Fermat number

$$F_m = 2^{2^m} + 1$$

To show $(F_m, F_n) = 1$ Let $(F_m, F_n) = d$

We shall show $F_m \nmid F_n$ for $m \neq n$

$$\frac{F_m - 2}{F_n} = \frac{2^{2^m} + 1 - 2}{2^{2^n} + 1} = \frac{2^{(2^n)^{2^{m-n}}} + 1 - 2}{2^{2^n} + 1} = \frac{(2^{2^n})^{2^{m-n}} + 1 - 2}{2^{2^n} + 1}$$

$$= \frac{x^r + 1 - 2}{x + 1}, \quad x = 2^{2^n}, \quad r = 2^{m-n}, \quad m > n$$

$$= x^{r-1} - x^{r-2} + \cdots - 1, \quad r \geq 2 \quad r \text{ is even}$$

$$=$$ an integer $\Rightarrow F_n \mid F_m - 2$, Now $d \mid F_n$
$\Rightarrow d \mid F_m - 2$
$\Rightarrow d \mid 2$
$\Rightarrow d$ must be one.

$\therefore (F_m, F_n) = 1.$

Theorem 3. For each $m > 0$ show that

$$F_{m+1} = F_0 F_1 F_2 \cdots F_m + 2$$

Proof. Let $m > 0$

To prove $F_{m+1} = (F_0 F_1 F_2 \cdots F_m) + 2$

We shall prove this mathematical induction

For $m = 1$ RHS $= F_0 F_1 + 2 = (2^{2^0} + 1)(2^{2^1} + 1) + 2$

$= (2+1)(4+1) + 2 = 17$

$= 2^{2^2} + 1 = F_2 =$ LHS

$\Rightarrow$ theorem is true for $m = 1$

Suppose the theorem is true for $m = k$

To show it will also true for $m = k+1$

i.e $F_k = F_0 F_1 \cdots F_{k-1} + 2$ ——— (2)

Now $f_{k+1} = 2^{2^{k+1}} + 1 = 2^{2^k \cdot 2} + 1$

$= (2^{2^k})^2 + 1 = (F_k - 1)^2 + 1$ $\left[\because F_k = 2^{2^k} + 1\right]$

$= F_k^2 - 2F_k + 1 + 1$

$= F_k[F_k - 2] + 2$

$= F_k[F_0 F_1 F_2 \cdots F_{k-1}] + 2$

$= F_0 F_1 F_2 \cdots F_{k-1} F_k + 2$

This shows that the theorem is true for $m = (k+1)$ also

$\therefore$ $\boxed{f_{m+1} = (F_0 F_1 F_2 \cdots f_m) + 2}$

Theorem 5. Any prime divisor p of the fermat number $F_m = 2^{2^m} + 1$, $m > 0$ is of the form $p = (k \cdot 2^{m+2}) + 1$

Proof. Since p is a prime divisor of F_m

$\Rightarrow F_m \equiv 0 \pmod p \Rightarrow 2^{2^m} \equiv -1 \pmod p$

$\Rightarrow (2^{2^m})^2 \equiv 1 \pmod p \Rightarrow 2^{2^{m+1}} \equiv 1 \pmod p$ — (1)

Let a be the order of 2 mod p

$\Rightarrow a \mid 2^{m+1}$ [if $a(a) = k$ then $a^h \equiv 1 \pmod p \Rightarrow a \mid k$]

Now, a can not be of the form $a = 2^s$, $1 \le s \le m$

Otherwise $2^{2^m} \equiv 1 \pmod p$ whereas a contradiction that $p = 2$

$\therefore a = 2^{m+1}$ ——— (2)

We know $2^{p-1} \equiv 1 \pmod p$, p is prime

$\Rightarrow a \mid (p-1)$ [$\because$ order of 2 is $a \pmod p$]

$\Rightarrow 2^{m+1} \mid (p-1)$ [$\because a = 2^{m+1}$, from (2)]

and consequently for $m > 2$, $p \equiv 1 \pmod 8 \Rightarrow \left(\frac{2}{p}\right) = 1$

i.e. $\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}} \equiv 1 \pmod p$

$\Rightarrow a \mid \left(\frac{p-1}{2}\right) \Rightarrow 2^{m+1} \mid \left(\frac{p-1}{2}\right) \Rightarrow \frac{p-1}{2} = 2^{m+1} \cdot k$

$\Rightarrow p = (k \cdot 2^{m+2} + 1)$, k is an integer.

Pythagorean Triples. A Pythagorean triple is a set of ~~three~~ three integers x, y and z such that

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

This triplet is said to be primitive if $(x, y, z)=1$

Ex ① 3, 4, 5 ② 5, 12, 13

Lemma 1. If x, y, z is primitive Pythagorean triple then one of x or y is even and the other is odd.

Proof. Suppose x and y are both even, then

$2|x$ and $2|y \Rightarrow 4 | x^2+y^2 \Rightarrow 4 | x^2+y^2=z^2$

$\Rightarrow 4|z^2 \Rightarrow 2|z$, which is not possible because $(x,y,z)=1$.

Similarly, if x and y are both odd then

$x^2 \equiv 1 \pmod 4$ and $y^2 \equiv 1 \pmod 4$

$\Rightarrow (x^2+y^2) \equiv 2 \pmod 4$, which is not possible because square of any integer is either congruent to 0 mod 4 or 1 mod 4 Hence either x or y is even and other is odd.

Lemma 2. If $ab=c^2$ and $(a,b)=1$ then a & b are also squares.

Proof. Let $a>1$, $b>1$ and

$a = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$ and $b = q_1^{s_1} q_2^{s_2} \cdots q_t^{s_t}$

be the prime factorisation of a & b. Since $(a,b)=1$ then

$ab = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} q_1^{s_1} q_2^{s_2} \cdots q_t^{s_t}$

$= c^2$, a square

$\Rightarrow$ each s_i and each s_j must be square

$\Rightarrow$ a & b must be both squares.

Theorem 1. All solutions of Phythagorean equations $x^2+y^2=z^2$ satisfying the conditions $(x,y,z)=1$, $2|x$, $x>0$, $y>0$, $z>0$ are given by

$x=2ab$, $y=a^2-b^2$, $z=a^2+b^2$.

For integers $a>b>0$ such that $(a,b)=1$ and $a \not\equiv b \pmod 2$ (2004)

Proof. Let $(x,y,z)=1$, $x>0, y>0, z>0$

Let x,y,z be a Primitive Pythagorean triple then one one of x and y is even and other is odd

Let x be even then both y and z are odd

$\Rightarrow$ $z-y$ and $z+y$ are both even

$\Rightarrow$ $\frac{z-y}{2}$ and $\frac{z+y}{2}$ are integers

Now, $x^2+y^2=z^2$ (given)

$\Rightarrow x^2=z^2-y^2$

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

If $d=\left(\frac{z-y}{2}, \frac{z+y}{2}\right)$ then

$d \mid \frac{z-y}{2}$, $d \mid \left(\frac{z+y}{2}\right)$

$\Rightarrow d \mid \left(\frac{z-y}{2}+\frac{z+y}{2}\right)$ and $d \mid \left(\frac{z+y}{2}-\frac{z-y}{2}\right)$

$\Rightarrow d \mid z$ and $d \mid y$

Now $(x,y,z)=1 \Rightarrow (z,y)=1$

$\Rightarrow d=1$

Now $\frac{z+y}{1} \cdot \frac{z-y}{1}=\left(\frac{x}{2}\right)^2$

$\Rightarrow \frac{z-y}{1}$ and $\frac{z+y}{2}$ are both perfect square

[$ab=c^2 \Rightarrow a, b$ are both perfect square]

Let $\frac{z+y}{2} = r^2$, $\frac{z-y}{2} = s^2$ for some positive integers r and s

Obviously $(r, s) = 1$, $r > 0$, $s > 0$

$$\Rightarrow r^2 s^2 = \frac{z+y}{2}\,\frac{z-y}{2} = \left(\frac{x}{2}\right)^2$$

$$\Rightarrow x^2 = 4r^2 s^2 \Rightarrow \boxed{x = 2sr}$$

Now $r^2 - s^2 = \frac{z+y}{2} - \frac{z-y}{2}$

$$\boxed{r^2 - s^2 = y}$$

$$r^2 + s^2 = \left(\frac{z+y}{2}\right) + \left(\frac{z-y}{2}\right)$$

$$\boxed{r^2 + s^2 = z}$$

$$\therefore \boxed{x = 2rs,\ y = r^2 - s^2,\ z = r^2 + s^2}$$

Converse. Suppose $(r, s) = 1$

$x = 2rs$, $y = r^2 - s^2$, $z = r^2 + s^2$ then.

$(x, y, z) = 1$.

Let $d = (x, y, z)$ then

$\Rightarrow d \mid y$ and $d \mid z$ $\Rightarrow d \mid y + z$

$\Rightarrow d \mid r^2 - s^2 + r^2 + s^2$

$\Rightarrow d \mid 2r^2$

and $d \mid (y + z)$ $\Rightarrow d \mid (r^2 + s^2) - (r^2 - s^2)$

$\Rightarrow d \mid 2s^2$

Now, $d \mid x \Rightarrow d \mid 2rs$, $d \mid 2r^2$, $d \mid 2s^2$

If p is a prime divisor of d then

$p \mid 2r^2, 2rs, 2s^2$

$\Rightarrow p \mid 2$ or $p \mid r^2$ and $p \mid s^2$

$\Rightarrow \underline{p \mid 2}$ or $\underline{p \mid r}$ and $\underline{p \mid s}$

(1) (2)

Now p can not be equal to 2 as y and z are odd

(2) $p \mid x$ and $p \mid s$ which is again a contradiction as $(x, s) = 1$

$\therefore$ d must be equal to 1

$\therefore$ $(x, y, z) = 1$

$\Rightarrow (2rs, r^2 - s^2, r^2 + s^2)$ is a primitive solution of $x^2 + y^2 = z^2$.

where $x = 2rs$, $y = r^2 - s^2$, $z = r^2 + s^2$.

Other Diophantine equation.

(1) Show that the positive integral solution of $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$, where (x, y, z) is of the form $x = a(a+b)$, $y = b(a+b)$, $z = ab$

Sol. Given equation is

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z} \qquad \text{---------- (1)}$$

To show $x = a(a+b)$, $y = b(a+b)$, $z = ab$

let $x = ca$, $y = cb$ such that $(a, b) = 1$

Then $\frac{1}{z} = \frac{1}{x} + \frac{1}{y} = \frac{1}{ca} + \frac{1}{cb}$

$$\frac{1}{z} = \frac{a+b}{cab} \Rightarrow z = \frac{cab}{a+b} \qquad \text{---(2)}$$

(2) $\Rightarrow (a+b) \mid cab$

$\Rightarrow a+b \mid c$ as $(a+b, ab) = 1$ because take $(a, b) = 1$, $a = 2, b = 3$, $(2+3, 2\cdot3) = 1$

$\Rightarrow c = c_1(a+b)$ for some integer c_1

$\therefore z = \frac{cab}{a+b}$

$\Rightarrow z = \frac{c_1(a+b) \cdot ab}{(a+b)} = c_1 ab$

$\Rightarrow z = c_1 ab$

$x = ca$, $y = cb$

$z = c_1 ab$

Now we have

$(x, y, z) = 1$

$\Rightarrow (ca, cb, c_1 ab) = 1$

$\Rightarrow (c_1 a(a+b), c_1 (a+b) b, c_1 ab) = 1$

$\Rightarrow c_1 = 1$

i.e. $c = c_1 (a+b) \rightarrow c = (a+b)$

i.e. $x = ca$ $\quad y = cb$

$\Rightarrow x = (a+b)a$ $\quad \Rightarrow y = (a+b)b$, $z = c_1 ab$

$z = 1 \cdot ab$, as $c_1 = 1$

Hence $\left.\begin{array}{l} x = a(a+b) \\ y = b(a+b) \\ z = ab \end{array}\right\}$ is a solution of (1).

(2) Show $x^2 + y^2 = z^2$, $(x, z, z) = 1$ has positive integral solution as

$x = a^4 - b^4$, $y = 2ab(a^4 + b^2)$, $z = 2ab(a^2 - b^2)$

Sol Given equation be

$x^2 + y^2 = z^2$ ——— (1)

$(x, y, z) = 1$ ——— (2)

To show $x = a^4 - b^4$, $y = 2ab(a^2 + b^2)$, $z = 2ab(a^2 - b^2)$ is a positive integral solution of (1)

Let $x^2 = a_1(a_1 + b_1)$, $y^2 = b_1(a_1 + b_1)$ and $z^2 = a_1 b_1$ where $(a_1, b_1) = 1$

Since $z^2 = a_1 b_1 \Rightarrow a_1$ & b_1 must be both squares

& $x^2 = a_1(a_1 + b_1) \Rightarrow a_1$ & $(a_1 + b_1)$ must be both squares

Let $a_1 = a_2^2$, $b_1 = b_2^2$, and $a_1 + b_1 = c^2$

(i) $a_2^2 + b_2^2 = c_2^2$

Using theorem of Pythagorean triplet

$a_2 = a^2 - b^2$, $b_2 = 2ab$, $c_2 = a^2 + b^2$

, $(a, b) = 1$, $a > 0$, $b > 0$

(ii) $x = a_2 c_2$

$x = (a^2 - b^2)(a^2 + b^2) = (a^4 - b^4)$

$y = b_2 c_2 = 2ab(a^2 + b^2)$

$z = a_2 b_2 = 2ab(a^2 - b^2)$

(ii) $x = (a^4 - b^4)$, $y = 2ab(a^4 + b^4)$, $z = 2ab(a^4 - b^4)$

is a positive integral solution of (1).

Example. Find all Phythagorean triples whose terms are in A.P

Solu. Let $x-d, x, x+d$ be the required Pythagorean triplet. Then

$(x+d)^2 = (x-d)^2 + x^2$

$x^2 + d^2 + 2xd = x^2 + d^2 - 2xd + x^2$

$\Rightarrow x^2 - 4xd = 0$

$\Rightarrow x[x - 4d] = 0 \Rightarrow x = 4d$, $x \neq 0$

Therefore, the required triplet is given by

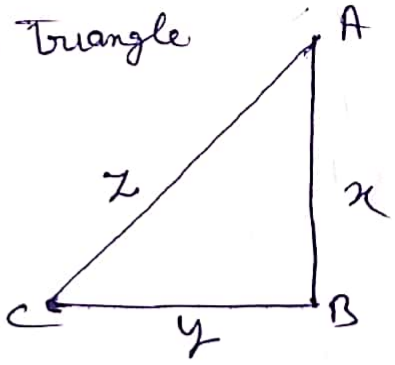
$x-d, x, x+d$

i.e $4d-d, 4d, 4d+d$

i.e $3d, 4d, 5d$; where $d = 1, 2, 3, \ldots$.

Example 3. Find all Pythagorean triangles whose area are equal to their Perimeters.

Solution. Let ABC be the Pythagorean Triangle as in figure then



$$x^2+y^2=z^2 \quad \text{---(1)}$$

and

$$x+y+z=\frac{1}{2}xy \quad \text{---(2)}$$

(1) & (2) $\Rightarrow$

$$x^2+y^2=\left(\frac{1}{2}xy-x-y\right)^2$$

$$x^2+y^2=\frac{1}{4}x^2y^2+x^2+y^2-x^2y-xy^2+2xy$$

$$x^2y^2-4x^2y-4xy^2+8xy=0$$

$$xy-4x-4y+8=0$$

$$x(y-4)-4(y-4)=8$$

$$(x-4)(y-4)=8$$

$\Rightarrow$ $x-4=8$, $y-4=1$ OR $x-4=4$, $y-4=2$

$\Rightarrow$ $x=12$, $y=5$ or $x=8$, $y=6$

$z=\sqrt{5^2+12^2}$ $\quad$ $z=\sqrt{8^2+6^2}$

$z=13$ $\quad$ $z=10$

Thus 5, 12, 13 & 8, 6, 10 are required Pythagorean triangles.