Unit 11: NUMBERS OF SPECIAL FORM

UNIT STRUCTURE

11.1 Learning Objectives
11.2 Introduction
11.3 Perfect numbers
11.4 Mersenne primes
11.5 Fermat number
11.6 Pythagorean triplets
11.7 Fermat's last theorem
11.8 Let Us Sum Up
11.9 Answers to Check Your Progress
11.10 Further Reading
11.11 Model Questions

11.1 LEARNING OBJECTIVES

After going through this unit, you will be able to:

- Understand the concept of perfect numbers and identify their fundamental properties.
- Describe Mersenne primes and explain their connection with even perfect numbers.
- Understand the definition and properties of Fermat numbers and their relevance in number theory.
- Identify and generate Pythagorean triplets, and understand their algebraic and geometric significance.
- Understand the statement, historical background, and significance of Fermat's Last Theorem.

11.2 INTRODUCTION

In this unit, we begin with the concept of **perfect numbers**, which are integers equal to the sum of their proper divisors. These numbers were studied by ancient Greek mathematicians and continue to be of interest even today. Closely related to perfect numbers are **Mersenne primes**, a special class of prime numbers that help in generating even perfect numbers.

The unit then introduces **Fermat numbers**, another important sequence of integers proposed by Pierre de Fermat, which are closely connected with primality and modern computational number theory. After this, we study **Pythagorean triplets**, which are sets of three positive integers satisfying the famous relation $a^2 + b^2 = c^2$, and explore methods to generate such triplets.

Finally, the unit concludes with an introduction to **Fermat's Last Theorem**, one of the most celebrated results in the history of mathematics.

11.3 PERFECT NUMBERS

Definition 11.3.1: A positive integer n is called a perfect number if it equals the sum of all its positive divisors ≥ 1 excluding itself.
i.e.$\sigma(n) - n = n \Leftrightarrow \sigma(n) = 2n$.
where $\sigma(n)$denotes the sum of all positive divisors of$n$.
For example, 6 and 28 are both perfect numbers, since
$6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$.
Similarly, 496 and 8128 are also perfect numbers.
Theorem 11.3.1: (Euclid): If $2^k - 1$ is a prime $(k > 1)$,then $2^{k-1}(2^k - 1)$ is a perfect number.
Proof: Let $p = 2^k - 1$ be a prime. Let $n = 2^{k-1}(2^k - 1)$.We have to show that n is a perfect number.
We have

$$\sigma(n) = \sigma[2^{k-1}(2^k - 1)]$$
$$= \sigma[2^{k-1}p]$$

$= \sigma(2^{k-1})\sigma(p)$[by multiplicativity of σ]

$$= (2^{k-1})(p + 1)$$
$$= (2^{k-1})2^K$$
$$= 2.2^{K-1}(2^{k-1})$$
$$= 2n$$

This shows that $n = 2^{k-1}(2^k - 1)$ is a perfect number.
Note:
A number of the form $2^{k-1}(2^k - 1)$ is called Euclid type number.
Theorem 11.3.2: (Eulers): Every even perfect number has the form $2^{k-1}(2^k - 1)$ where $2^k - 1$.
Proof: Let n be an even perfect number. Therefore $n = 2^{k-1} \times a$ for some $k > 1$ and for some odd integer a.Since $(2^{k-1}, a) = 1$,we have

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

$= (2^k - 1)\,\sigma(a)$ (1)
Also n is a perfect number.
Therefore, $\sigma(n) = 2n$
$\Longrightarrow (2^k - 1)\,\sigma(a) = 2^k \times a$ (2)
$\Longrightarrow 2^k | \sigma(a)$ $[\because ((2^{k-1}, 2^k) = 1)$
$\Longrightarrow \sigma(a) = 2^k \times q$ for some integer q. (3)
Now, from (2) using (3), we have

$$(2^k - 1)\,\sigma(a) = 2^k \times q$$

$\Rightarrow a = (2^k - 1)q.$ (4)

Now if $q > 1$,then a has at least four factors $1, 2^{k-1}, q$and$(2^k - 1)q$.

Therefore,

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

This contradicts (3). So, our assumption was wrong.

So $q = 1$ and therefore $a = 2^k - 1$.

Hence,

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

We have $a = 2^k - 1$ and $\sigma(a) = 2^k$.

Therefore,$2^k - 1$ will have only two divisions 1 and $2^k - 1$.

Hence, $a = 2^k - 1$ is a prime.

Theorem 11.3.3: Let a be a positive integer and k is an integer≥ 2.If $a^k - 1$ is a prime, then $a = 2$ and k is a prime.

Proof: We have

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

Since $a > 0$.We have $a \geq 1$ and therefore

$$a^{k-1} + a^{k-1} + \cdots + a + 1 \geq a + 1 \geq 2.$$

By hypothesis $a^k - 1$ is a prime. Therefore, the other factor

$$a - 1 = 1$$
or $a = 2$.

Suppose if possible k is a composite number.

Then $k = rt$ with $r, t > 1$.Thus,

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

Each factor on the right-hand side is greater than 1 which is possible because $a^r - 1$ is a prime.

Thus, we have a contradiction.

Hence,k must be a prime.

The list of perfect numbers known so far:

SL No	Perfect Number	Digits in the Number
1	$2[2^1-1]=6$	1
2	$2^2[2^3-1]=28$	2
3	$2^4[2^5-1]=496$	3
4	$2^6[2^7-1]=8126$	4
5	$2^{12}[2^{13}-1]=33550336$	8
6	$2^{16}[2^{17}-1]=8589869056$	10
7	$2^{18}[2^{19}-1]=137438691328$	12
8	$2^{30}[2^{31}-1]$	19
9	$2^{60}[2^{61}-1]$	37
10	$2^{88}[2^{89}-1]$	54
11	$2^{106}[2^{107}-1]$	65
12	$2^{126}[2^{127}-1]$	77
13	$2^{520}[2^{521}-1]$	314
14	$2^{605}[2^{607}-1]$	366
15	$2^{1278}[2^{1279}-1]$	770
16	$2^{2202}[2^{2203}-1]$	1327
17	$2^{2280}[2^{2281}-1]$	1373
18	$2^{3216}[2^{3217}-1]$	1937
19	$2^{4252}[2^{4253}-1]$	2561
20	$2^{4422}[2^{4423}-1]$	2663
21	$2^{9688}[2^{9689}-1]$	5834
22	$2^{9940}[2^{9941}-1]$	5985
23	$2^{11212}[2^{11213}-1]$	6751
24	$2^{19936}[2^{19937}-1]$	12003
25	$2^{21700}[2^{21701}-1]$	13,006
26	$2^{23208}[2^{23209}-1]$	13,973
27	$2^{44496}[2^{44497}-1]$	26,790
28	$2^{86242}[2^{86243}-1]$	51,924
29	$2^{110502}[2^{110503}-1]$	66,530
30	$2^{132048}[2^{132049}-1]$	79,502
31	$2^{216090}[2^{216091}-1]$	130,100
32	$2^{756838}[2^{756829}-1]$	455,663

Example 1: Show that the integer $n=2^{10}(2^{11}-1)$ is not a perfect number.
Solution: We have

$$\sigma(n)=\sigma[2^{10}(2^{11}-1)]$$
$$=\sigma[2^{10}.23.89][\because 2^{11}-1=23.89]$$
$$=\sigma[2^{10}]\sigma(23)\,\sigma(89)$$

$= [2^{11} - 1].24.90$

$$\neq 2^{10}(2^{11} - 1)$$
$$\neq n$$

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

Example 2: If n is an even perfect number, then prove that $\sum_{d|n} \frac{1}{d} = 2$.

Solution: We have

$$\sum_{d|n} \frac{1}{d} = \sum_{d|n} \left(\frac{d}{n}\right)$$
$$= \frac{1}{n} \sum_{d|n} d$$
$$= \frac{\sigma(n)}{n}$$

$= \frac{2n}{n}$ [$\because n$ is a perfect number]

$= 2$.

11.4 MERSENNE PRIMES

The numbers of the form $M_n = 2^n - 1$,where$n > 1$ are called Mersenne numbers. A Mersenne number that is also a prime number is known as a **Mersenne prime**.

If M_k is a Mersenne number, then the number $2^{k-1}M_k$ is a perfect number. Thus, there exists a one–to–one correspondence between Mersenne primes and even perfect numbers.

For example, the first few Mersenne numbers are

$3 = 2^2 - 1,7 = 2^3 - 1,15 = 2^4 - 1,31 = 2^5 - 1,63 = 2^6 - 1,127 = 2^7 - 1.$

Among these, 3,7,31 and127 are prime and hence are Mersenne primes.

Marin Mersenne claimed that M_p is prime for $p = 2,3,5,7,13,17,19,31,67,127$ and $257$and composite for all other prime values of p less than 257. However, it was later shown that M_{67} and $M_{257}$are composite. Moreover, M_{61}, M_{89} and M_{107}which were not included in his list, were subsequently found to be prime.

M_p is prime and composite for all other primes below 257.Since then it has been shown that M_{67} and M_{257} are composite. Furthermore,M_{61}, M_{89} and M_{107} are primes which were excluded in his list.

Theorem 11.3.4: (Fermat): If $p > 2$ is a prime then any prime divisor of M_p must be of the form $2kp + 1$ for $k = 1,2,3, \cdots$.

Proof: Let q be a prime divisor of M_p.Then $q|2^p - 1$.Obviously q is an odd integer.

By Fermat's theorem, we have $2^{q-1} \equiv 1(mod\ q)$ i.e., $q|(2^{q-1} - 1)$.

If $d = (p, q - 1)$,then $d|p$ and $d|q - 1$.

Since p is a prime we have $d = p$ or $d = 1$.

If $d = p$ and $q = dt + 1$,then t must be even (as p and q both are odd).

Therefore,$q = 2pk + 1$ for some $k = 1,2, \cdots$.

If $d = 1$,then

$$(2^p - 1, 2^{q-1} - 1) = 2^{(p,q-1)-1} = 2 - 1 = 1.$$

This is false because q divides $2^p - 1$ and $2^{q-1} - 1$.So,$d \neq 1$.

Theorem 11.3.5: If$q = 2m + 1$ is prime then$q|M_m$provided$q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$.

Proof: We know that

$$\left(\frac{2}{q}\right) = 1$$

when $q \equiv 1(mod\ 8)$ or $q \equiv 7(mod\ 8)$

This gives $2^m \equiv 1(mod\ q)$

$$\Longrightarrow 2^m \equiv 1(mod\ q)$$

$$\text{or } 2^{\left(\frac{q-1}{2}\right)} \equiv 1(mod\ q)$$

$\Longrightarrow q|M_m$.

Thus, we see that $q|M_m$ when $q \equiv 1(mod\ 8)$

or $q \equiv 7(mod\ 8)$.

Theorem 11.3.6: For $p > 2$ every prime divisor of M_p is of the form $8k \pm 1$.

Proof: Since M_p is an odd number, any prime divisor q of it is also odd.

Let $q = 2m + 1$

If $a = 2^{\frac{(p+1)}{2}}$,then

$$a^2 - 2 = 2^{p+1} - 2$$

$$= 2M_p$$

$$\equiv 0(mod\ q) \quad [\because q|M_p \Longrightarrow q|2M_p]$$

$$\Longrightarrow a^2 \equiv 2(mod\ q)$$

$$\Longrightarrow a^{2m} = 2^m(mod\ q)$$

$$\Longrightarrow a^{q-1} = 2^m(mod\ q) \qquad (1)$$

Since q is an odd integer, we have

$$(a, q) = 1$$

Therefore,$a^{q-1} \equiv 1(mod\ q)$ (2)

From (1) and (2), we have

$$2^m \equiv 1(mod\ q)$$

$$\Longrightarrow q|M_m$$

Hence,$q \equiv \pm 1(mod\ 8)$ or $q = 8k \pm 1$.

Theorem 11.3.7: (Euler): Ifn is an odd perfect number, then

$$n = p_1^{a_1} p_2^{2a_2} p_3^{2a_3} \cdots p_r^{2a_r}$$

where p_i are distinct odd primes and $p_1 \equiv a_1 \equiv 1(mod\ 4)$.

Proof: Let $n = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}$ be the prime factorization of n.Since n is a perfect number, we have

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

$$= \sigma\left(p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_r^{a_r}\right)$$

$$= \sigma\left(p_1^{a_1}\right)\sigma\left(p_2^{a_2}\right) \cdots \sigma\left(p_r^{a_r}\right)$$

Since n is an odd number, we have

$n \equiv 1(mod\ 4)$ or $n \equiv 3(mod\ 4)$

$$\Rightarrow 2n \equiv 2(mod\ 4)$$

Thus,$\sigma(n) = 2n$ is divisible by 2, but not by 4.This implies that one of the $\sigma(p_i^{a_i})$,say $\sigma(p_1^{a_1})$,must be an even integer (but not divisible by 4) and all the remaining $\sigma(p_i^{a_i})'s$ are odd integers.

Now for a given p_i,we have

$p_i \equiv 1(mod\ 4)$ and $p_i \equiv 3(mod\ 4)$

$\equiv -1(mod\ 4)$.

Therefore,

$$\sigma(p_i^{a_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{a_i}$$
$$= 1 - 1 + (-1)^2 + \cdots + (-1)^{a_i}(mod\ 4)$$
$$= \begin{cases} 0(mod\ 4)\ when\ a_i\ is\ odd \\ 1(mod\ 4)\ when\ a_i is\ even \end{cases}$$

Since $\sigma(p_1^{a_1}) \equiv 2(mod\ 4)$,we have $p_1 \neq 2(mod\ 4)$ i.e., $p_1 \equiv 1(mod\ 4)$

Also, the congruence $\sigma(p_i^{a_i}) \equiv 0(mod\ 4)$ implies that $4|\sigma(p_i^{a_i})$.This is not possible.

This gives that if., $p_i \equiv 3(mod\ 4)$ for $i = 2, \cdots, r$,then a_i is an even integer.

If $p_i \equiv 1(mod\ 4)$ then

$$\sigma(p_i^{a_i}) = 1 + p_i + p_i^2 + \cdots + p_i^{a_i}$$
$$= 1 + 1 + 1^2 + \cdots + 1^{a_r}(mod\ 4)$$
$$= a_i + 1(mod\ 4)$$

Now $\sigma(p_i^{a_i}) \equiv 1\ or\ 3(mod\ 4)$

We have

$a_i \equiv 0\ or\ 2(mod\ 4)$.

Therefore a_i is even.

Thus, in any case a_i is even.

Corollary: If n is an odd perfect number, then$n$ is of the form

$$n = p^k m^2$$

Where p is a prime,$p \nmid m$ and $p \equiv a \equiv 1(mod\ 4)$.

Example 3: Show that the Mersenne number M_{19} is a prime.

Solution: Here $M_{19} = 2^{19} - 1$

$$= 524288 - 1 = 524287$$

We must check whether **524287** has any prime divisor.

Let a prime p divides M_{19}.Then p is of the form

$$p = 2 \times 19 \times k + 1$$

$= 38k + 1$ for some k (1)

So **any possible prime factor must look like** $38k + 1$.

Now, $\sqrt{524287} \approx 724$

Also, we have $724 < \sqrt{M_{19}}$ (2)

So, we only need to check primes of the form $38k + 1$ that are less than 724.

From (1) we can show that primes less than 724 are 191,229,457 and 647.None of these primes divides M_{19}.

Therefore M_{19} is a prime.

11.5 FERMAT NUMBER

An integer of the form
$F_m = 2^{2^m} + 1, m \geq 0$ is called Fermat number.
If a Fermat number is prime, it is called a **Fermat prime**.
So, $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are the only Fermat prime known so far.
Euler in 1732 found that $F_5 = 4294967297$ is divisible by 641. Thus, F_5 is a composite number.
Infact, the largest composite Fermat number known today is F_{23471}. Till the date, it has also not been decided that if there are any more Fermat primes other than F_0, F_1, F_3 and F_4.
Theorem 11.5.1: The Fermat number F_5 is divisible by 641.
Proof: If we take $a = 2^7$ and $b = 5$ then

$$\begin{aligned} 1 + ab &= 1 + 2^7.5 \\ &= 1 + 640 \\ &= 641 \end{aligned}$$

Also,

$$\begin{aligned} 1 + ab - b^4 &= 1 + (a - b^3)b \\ &= 1 + (2^7 - 5^3)5 \\ &= 1 + (128 - 125)5 \\ &= 1 + 3.5 \\ &= 1 + 15 \\ &= 16 \\ &= 2^4 \end{aligned}$$

Now $F_5 = 2^{2^5} + 1$

$$\begin{aligned} &= 2^{32} + 1 \\ &= 2^4.2^{28} + 1 \\ &= 2^4.(2^7)^4 + 1 \\ &= 2^4a^4 + 1 \\ &= (1 + ab - b^4)a^4 + 1 \\ &= (1 + ab)a^4 + 1 - a^4b^4 \\ &= (1 + ab)[a^4 + (1 - ab)(1 + a^2b^2)] \\ &= 641[a^4 + (1 - ab)(1 + a^2b^2)] \end{aligned}$$

So, $F_5 = 641 \times [Some\ integer]$
This shows that $641 | F_5$.
Theorem 11.5.2: For integers $m > n \geq 0$. $(F_m, F_n) = 1$ i.e., Fermat numbers are relatively prime.
Proof: Let $d = (F_m, F_n)$ and $m > n \geq 0$. Then d is odd as F_m and F_n are odd integers.
Let $x = 2^n$ and $r = 2^{m-n}$, then

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

$$= \frac{\left(2^{2^n}\right)^{2^{m-n}} - 1}{2^{2^n} + 1}$$
$$= \frac{x^r - 1}{x + 1}$$
$$= x^{r-1} - x^{r-2} + \cdots - 1$$

This shows that $F_n|(F_m - 2)$.Also,$d|F_m$.Therefore $d|2$.But d is an odd integer so $d = 1$.Thus we have $(F_m, F_n) = 1$.

Theorem 11.5.3 Pepin's test: For $m \geq 1$,the Fermat number $F_m = 2^{2^m} + 1$ is prime iff

$$3^{\frac{(F_m-1)}{2}} \equiv -1(mod\ F_m)$$

Proof: First let us assume that F_m,$m \geq 1$ is prime. Then by quadratic reciprocity law,

We have

$\left(\frac{3}{F_m}\right) = \left(\frac{F_m}{3}\right) = \left(\frac{2}{3}\right) = -1.$

We have

$F_n \equiv (-1)^{2^n} + 1 = 2(mod\ 3).$

Applying Euler's criterion, we have

$$3^{\frac{F_n-1}{2}} \equiv -1(mod\ F_n)$$

Conversely suppose

$3^{\frac{F_m-1}{2}} \equiv -1(mod\ F_m)$ (1)

Then $3^{F_m-1} \equiv 1(mod\ F_m)$

Also, for any prime p divisor of F_m,we get

$3^{F_m-1} \equiv 1(mod\ p).$

Let r be the order of 3 modulo p.Then $r|F_m - 1 \Longrightarrow r|2^{2^m}$.

Therefore, order of r should be 2.

Now $3^r \equiv 1(mod\ p)$

$\Longrightarrow 3^{2^{2^{n-1}}} \equiv 1(mod\ p)$ [By repeated squaring]

or$3^{\frac{F_m-1}{2}} \equiv p(mod\ p)$ (2)

From (1) and (2), we have

$$1 \equiv -p(mod\ p)$$

$$\Longrightarrow p = 2$$

which is a contradiction.

Therefore, the only possibility is that

$$r = 2^{2^m} = F_m - 1$$

By Fermat's theorem, we have

$$r \leq p - 1$$

Which implies

$$F_m = k + 1 \leq p$$

Since $p|F_m$,we have $F_m \geq p$.

Thus, we have

$$F_m = p$$

Therefore,F_m is a prime.

Theorem 11.5.4: Any prime divisor p of the Fermat number $F_m = 2^{2^m} + 1$,where $m \geq 2$, is of the form $p = k.2^{m+2} + 1$.

Proof: Since p is a prime divisor of F_m,we have

$$2^{2^m} \equiv -1(mod\ p)$$

$$\Longrightarrow 2^{2^{m+1}} \equiv 1(mod\ p)$$ [on squaring]

Let a be the order of 2 modulo p.Then

$$a|2^{m+1}$$

Now a cannot be of the form

$$a = 2^r, 1 \leq r \leq m$$

Otherwise

$$2^{2^m} \equiv 1(mod\ p)$$

This provides a contradiction that $p = 2$.This gives that $a = 2^{m+1}$.

We know that the order of 2 modulo p divides $\phi(p) = p - 1$.

Therefore $2^{m+1}|p - 1$ and consequently for $m \geq 2, p \equiv 1(mod\ 8)$ and $\left(\frac{2}{p}\right) = 1$.

By the application of Euler's criterion, we have

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) = 1(mod\ p)$$

Hence,$a|\frac{(p-1)}{2}$ or $2^{m+1}|\frac{(p-1)}{2}$

$$\Longrightarrow 2^{m+2}|(p-1)$$

$\Longrightarrow p = k.2^{m+2} + 1$ where k is an integer.

Theorem 11.5.5: There are infinitely many primes.

Proof: Every pair of Fermat numbers is relatively prime. Hence, for each Fermat number F_n there exists a prime p_n that divides F_n but does not divide any other Fermat number. Therefore, each Fermat number has a distinct prime divisor. Since there are infinitely many Fermat numbers, the number of such primes is also infinite.

Definition (F −number): A composite integer n is said to be an F −number if for each a relatively prime to n.

$$a^{n-1} \equiv 1(mod\ n)$$

The existence of such integers was first shown by R.D. Carmichael and the smallest such number is $561 = 3.11.17$.

11.6 PYTHAGOREAN TRIPLETS

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

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

Definition: A Pythagorean triple is a set of three integers x, y and z such that $x^2 + y^2 = z^2$;the triple is called primitive if $(x, y, z) = 1$.

For example, 3,4,5 and 5,12,13 are Pythagorean triples.

Note: If x, y, z is a Pythagorean triple and $d = (x, y, z)$ then $x_1 = dx$,$y_1 = dy$ and $z_1 = dz$ is also a Pythagorean triples and it is primitive Pythagorean triple.

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

Proof: Since x, y, z is a primitive Pythagorean triple

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

Suppose x and y are both even, then$2|x$ and $2|y \Longrightarrow 4|x^2 + y^2 \Longrightarrow 4|z^2 \Longrightarrow 2|z$; which is not possible since $(x, y, z) = 1$.

Similarly, if$x$ and y are both odd then $x^2 \equiv 1(mod\ 4)$ and $y^2 \equiv 1(mod\ 4)$.

$$\Longrightarrow x^2 + y^2 = z^2 \equiv 2(mod\ 4)$$

This is impossible because square of any integer is either congruent to 0 or modulo 4. Hence, either$x$ or y is even and the other is odd.

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

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

$a = p_1^{r_1}.p_1^{r_1}.\cdots.p_l^{r_l}$ and $b = q_1^{r_1}.q_1^{r_1}.\cdots.q_k^{r_k}$ be the prime factorizations of a and b.

Since $(a, b) = 1$,all p_i and q_j are distinct primes and integers r_i and s_j are ≥ 1.

Now

$ab = p_1^{r_1}.p_1^{r_1}.\cdots.p_l^{r_l}\ .q_1^{r_1}.q_1^{r_1}.\cdots.q_k^{r_k} = c^2$ is a square.

Therefore, each r_i and s_j must be even integers. This shows that a and b are also squares.

Theorem 11.6.1: All solutions of Pythagorean equations

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

satisfying the conditions

$(x, y, z) = 1,\ 2|y,x > 0,y > 0,z > 0$

are given by

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

where integers r, s are such that $r > s > 0, (r, s) = 1$ and only one of r and s is even and the other is odd.

Proof: Let x, y, z be a primitive Pythagorean triple. By lemma 1, one of x or y is even and the other is odd. Let$y$ is even. Then$x$ and z are both odd. This gives that $z - x$and $z + x$ both are even i.e. $\frac{z-x}{2}$and $\frac{z+x}{2}$ are integers.

Now

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

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

$$\Rightarrow \frac{y^2}{4} = \frac{(z-x)(z+x)}{4}$$

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

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

$$\Rightarrow d = 1$$

By lemma 2, both.$\frac{z-x}{2}$and $\frac{z+x}{2}$ are perfect square.

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

Obviously $(r, s) = 1$ and $r > s$.

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

Since z is odd, $z = r^2 + s^2 \Rightarrow$ only one of r and s is even, other is odd.

Conversely, let$r$, s be any integers satisfying the conditions. Then if $x = r^2 - s^2, y = 2rs$, $z = r^2 + s^2$,we have x, y, z are all positive and

$x^2 + y^2 = (r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2 = z^2$.

Also, if $d = (x, y, z)$,then

$$d|x, y, z \Rightarrow d|r^2 - s^2, 2rs, r^2 + s^2$$

$$\Longrightarrow d|r^2+s^2+r^2-s^2=2r^2$$

and

$$\Longrightarrow d|r^2+s^2-r^2+s^2=2s^2$$

$$\Longrightarrow d|2r^2,rs,2s^2$$

Let p be a prime divisor of d.Then

$$p|2r^2,rs,2s^2$$

$\Longrightarrow p|2$ or $p|r^2$ and $p|s^2$

$\Longrightarrow p|2$ or $p|r$ and $p|s$

If $p=2$,we have a contradiction to x or y being odd and if $p|r$ (and $\therefore p|s$),again we have contradiction, since$(r,s)=1$.

Thus d must be 1$\Longrightarrow$ $x=r^2-s^2$,$y=2rs$ and $z=r^2+s^2$ is a primitive solution of (1).

Example 4: Find all Pythagorean triples where terms are in arithmetic progression.

Solution: Let$x-d$,x,$x+d$ be the required Pythagorean triples. Then

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

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

or $x^2-4xd=0$

or $x(x-4d)=0$

This gives $x-4d=0$

or $x=4d$

Therefore, the required triple is

$3d$,$4d$,$5d$ where $d=1,2,\cdots$.

Example 5: Show that if x,y,z is a primitive Pythagorean triples in which x and z are consecutive positive integers, then

$$x=2s(s+1)$$

$$y = 2s + 1$$

$$z = 2s(s + 1) + 1$$

Proof: We know that if x, y, z is a primitive Pythagorean triples, then

$$x = 2rs, y = r^2 - s^2 \text{ and } z = r^2 + s^2. \qquad (1)$$

Since x and z are consecutive integers, we have $z = x + 1$

$$\Rightarrow r^2 + s^2 = 2rs + 1$$

$$\Rightarrow (r - s)^2 = 1$$

$$\Rightarrow r - s = 1$$

$$\Rightarrow r = s + 1$$

Putting the value of r in (1), we get

$$x = 2(s + 1)s$$

$$y = (s + 1)^2 - s^2$$

$$= s^2 + 2s + 1 - s^2$$

$$= 2s + 1$$

and $$z = (s + 1)^2 + s^2$$

$$= s^2 + 2s + 1 + s^2$$
$$= 2s^2 + 2s + 1$$

$$= 2s(s + 1) + 1$$

Thus, we have

$$x = 2s(s + 1)$$

$$y = 2s + 1$$

$$z = 2s(s + 1) + 1$$

11.7 FERMAT'S LAST THEOREM

Over 360 years ago, Fermat stated in the margin of his copy of Diophantus Arithmetician: "It is impossible to write a cube as a sum of two cubes, a fourth power as a sum of two fourth powers and in general any power beyond the second as a sum of two similar powers. For this I have discovered a wonderful proof but the margin is too small to contain it". The theorem can be stated as:
The Diophantine equation

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

has no integral solution for $n > 2$ other than the trivial solution in which x or y is zero.
This theorem is known as Fermat's last theorem. This theorem remained a challenge for mathematical community for a long time. In June 1993 a mathematician Andrew Wales of Princeton University claimed to prove this theorem. The whole mathematics world is excited today because this theorem defied the best minds of several generations of mathematician. It is one of the important theorems.

W CHECK YOUR PROGRESS

Q1) Show that M_{29} is a composite number.

Q2) If n is an even perfect number, then prove that $\sum_{d|n}\frac{1}{d} = 2$.

Q3) Prove that the Mersenne number M_{17} is a prime; hence, the integer $n = 2^{16}(2^{17} - 1)$ is perfect.

Q4) Find all Pythagorean triangles whose areas are equal to their perimeters.

Q5) Prove that if x, y, z is a primitive Pythagorean triple in which the difference $z - y = 2$,then
$x = 2r$, $y = r^2 - 1$,$z = r^2 + 1$ for some $s > 0$.

211.8 LET US SUM UP

- A positive integer n is called a perfect number if it equals the sum of all its positive divisors ≥ 1 excluding itself.
  i.e.$\sigma(n) - n = n \Leftrightarrow \sigma(n) = 2n$,where $\sigma(n)$denotes the sum of all positive divisors of$n$.
- The numbers of the form $M_n = 2^n - 1$,where $n > 1$ are called Mersenne numbers. A Mersenne number that is also a prime number is known as a Mersenne prime.
- If M_k is a Mersenne number, then the number $2^{k-1}M_k$ is a perfect number. Thus, there exists a one–to–one correspondence between Mersenne primes and even perfect numbers.
- An integer of the form
  $F_m = 2^{2^m} + 1, m \geq 0$ is called Fermat number.
  If a Fermat number is prime, it is called a Fermat prime.
  - A Pythagorean triple is a set of three integers x, y and z such that
    $$x^2 + y^2 = z^2$$
  - A Pythagorean triple is a set of three integers x, y and z such that $x^2 + y^2 = z^2$;the triple is called primitive if $(x, y, z) = 1$.

K 11.9 ANSWERS TO CHECK YOUR PROGRESS

Answer to Q 1:

We want to show that the Mersenne number

$M_{29} = 2^{29} - 1$ is composite.

Let a prime p divides M_{29}.Then p is of the form

$$p = 2 \times 29k + 1$$

$= 58k + 1$ for some k (1)

Putting $k = 1,2,3,4,5$ in (1), we get $p = 59,117,175,233,291$ respectively.

Out of these values of$p$, 59 and 233 are prime. By actual division we can see that 233 are prime. By actual division we can see that 233 divides M_{29}.

Hence,M_{29} is a composite number.

Answer to Q 2:

We have

$$\sum_{d|n} \frac{1}{d} = \sum_{d|n} \left(\frac{d}{n}\right)$$

$$= \frac{1}{n} \sum_{d|n} d$$

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

$= \frac{2n}{n}$ [$\because n$ is a perfect number]

$$= 2$$

Answer to Q 3:

Here,$M_{17} = 2^{17} - 1$

Let a prime p divides M_{17}.Then p is of the form

$$p = 2 \times 17k + 1$$

$= 34k + 1$ for some k (1)

Now we test possible values of k such that

$$p \leq \sqrt{131071}$$

Since $\sqrt{131071} \approx 362$

We check primes of the form:

$34k + 1$ for $k = 1,2,3, \cdots$

We get 35, 69, 103, 137, 171, 205, 239, 273, 307, 341, 375...

Among these, the primes are:

103, 137, 239, 307

Now check whether any of them divide 131071.

By direct verification (division check), none divides 131071.

Hence $M_{17} = \mathbf{131071}$has no prime divisor $\leq \sqrt{131071}$.

Therefore,M_{17} is prime

Since $2^{17} - 1$is prime and $(2^{16}, 2^{17} - 1) = 1$,

$$\sigma(n) = \sigma(2^{16})\sigma(2^{17} - 1)$$

Now,$\sigma(2^{16}) = 1 + 2 + 2^2 + \cdots + 2^{16} = 2^{17} - 1$

and for prime q, $\sigma(q) = q + 1$

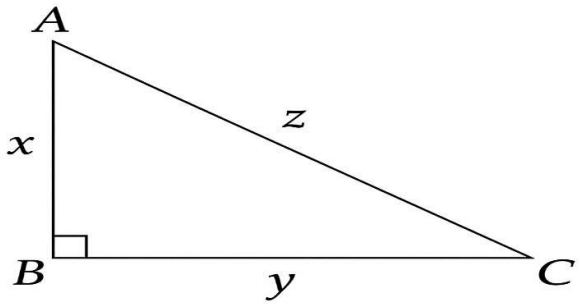
So,$\sigma(n) = (2^{17} - 1)(1 + 2^{17} - 1) = (2^{17} - 1)2^{17} = 2n$

Hence n is perfect.

Answer to Q 4: Let ABC be a Pythagorean triangle whose sides are x, y and $y$respectively. Then we have

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

and $x + y + z = \frac{1}{2}xy$ (2)



Eliminating z from (1) and (2),we have

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

$$= \frac{1}{4}x^2y^2 + x^2 + y^2 + 2\left(-\frac{1}{2}x^2y - \frac{1}{2}xy^2 + xy\right)$$

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

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

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

This gives $x = 12, y = 5$ or $x = 8, y = 6$.

When $x = 12, y = 5$,we have $z = 13$.

When $x = 8, y = 6$, we have $z = 10$.

Thus,$(12,5,13)$ and $(8,6,10)$ are the required Pythagorean triangles.

Answer to Q 5: We know that if x, y, z is a primitive Pythagorean triples, then

$$x = 2rs, y = r^2 - s^2 \text{ and } z = r^2 + s^2. \qquad (1)$$

Since, $z - y = 2$

$$\Rightarrow (r^2 + s^2) - (r^2 - s^2) = 2$$

$$\Rightarrow 2s^2 = 2$$

$$\Rightarrow s^2 = 1$$

$$\Rightarrow s = 1$$

Putting the value of s in (1), we get

$$x = 2r$$

$$y = r^2 - 1$$

and $$z = r^2 + 1$$

11.10 FURTHER READING

1. David M. Burton, Elementary Number Theory (7^{th} Edn.), McGraw Hill Education (India) Private Limited, Chennai-600116, 2018.
2. S. B. Malik, Basic Number Theory (2^{nd} revised Edn.), Vikash Publishing House Private Limited, Noida-201301, 2017.
3. George E. Andrews, Number Theory, Hindustan Publishing Corporation, New Delhi.
4. S. G. Telang, Number Theory, Tata McGraw-Hill Publishing Company Limited.
5. Hardy, G. H. And Wright, E. M., Theory of Numbers, Oxford Science Publications, 2003.

11.11 MODEL QUESTIONS

Q1. Let $n = M_{p_1} M_{p_2}, \cdots, M_{p_k}$ be a product of distinct k –Mersenne primes. Then prove that $\sigma(n) = 2^m$ for some m.

Q2. Prove that M_{23} is composite

Q3. Prove that the Mersenne number M_{13} is a prime; hence, the integer $n = 2^{12}(2^{13} - 1)$ is perfect.

Q4. Prove that the Mersenne number M_{19} is a prime; hence, the integer $n = 2^{18}(2^{19} - 1)$ is perfect.

Q5. Prove that the Mersenne number M_{29} is composite.

Q6. Obtain all primitive Pythagorean triples with $y = 60$.

Q7. Prove that $12|xy$ for any primitive Pythagorean triple x, y, z.

Q8. Find the different Pythagorean triples, not necessarily primitive, of the form $16, y, z$.

Q9. Prove that in a primitive Pythagorean triple x, y, z.the product xy is divisible by 12, hence $60|xyz$.

Q10.If x, y, z is a primitive Pythagorean triple, prove that $x + y$ and $x - y$ are congruent modulo 8 to either 1 or 7.

*** *** ***