UNIT 6: FERMAT'S THEOREM

UNIT STRUCTURE

6.1 Learning Objective
6.2 Introduction
6.3 Fermat's factorization method
6.4 Fermat's Little Theorem
6.5 Wilson's Theorem
6.6 Euler's Factorization Method
6.7 Let Us Sum Up
6.8 Answers to check your progress
6.9 Further Reading
6.10 Model Questions

6.1 LEARNING OBJECTIVE

After studying the current unit reader able to

- Understanding the mathematical foundation of Fermat's factorization method, based on expressing a number as a difference of square.
- Developing problem-solving skill to identify when Fermat's method is efficient, especially for numbers with close factors.
- Applying the Fermat's factorization method step-by-step to factorize numbers using integer calculations.
- Understanding the Fermat's Little Theorem.
- Applying the Fermat's Little Theorem to simplify modular exponentiation calculations.
- Understanding the Wilson's Theorem.
- Learn how to apply Wilson's Theorem to verify the primality of small numbers.
- Explore its proof using combinatorial and modular arithmetic techniques.
- Understanding the mathematical basis of Euler's factorization method, which relies on expressing a number as a sum of two squares.
- Learn how to apply the Euler's factorization method to factorize composite numbers particularly those with specific properties.

6.2 INTRODUCTION

Fermat's factorization method is a technique for decomposing an odd composite number N into a product of two factors. It is based an the observation that any odd integer can be expressed as the difference of two squares :

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

The goal is to find integers x and y such that this equation holds, which allows us to determine the factors of N. The method starts by selecting x as the ceiling of $\sqrt{N}$, i.e. the smallest integer x such that $x^2 \geq N$. Then, we iteratively compute $y^2 = x^2 - N$ and check whether y is an integer (i.e. y^2 is a perfect square). If so we have found the factors (x – y) and (x + y). Fermat's method works best when N has factors close to its square root. However for numbers with very small or very large prime factors, it may be inefficient. Despite this, it laid the foundation for later factorization algorithms and remains an elegant example of number theoretic techniques.

Fermat's Little Theorem is a fundamental result in number theory that provides a useful property of prime numbers in modular arithmetic. Fermat's Little Theorem is widely used in number theory, particularly in primality testing and cryptography. It forms the basis of the Fermat primality test, which helps determine whether a number is likely prime. It is also crucial in cryptographic algorithms like RSA encryption, where modular exponentiation plays a key role. The Theorem is named after Pierre De Fermat, who first stated it in a letter in 1640 without providing a proof. The first known proof was given by Euler in the 18th century.

Wilson's Theorem is a fundamental result in number theory that provides a characterization of prime numbers using factorials. It state that an integer p is prime if and only if

$(p - 1)! \equiv -1 \pmod{p}$

This means that the factorial of (p – 1), when divided by p, leaves a remainder of p – 1 (or equivalently; – 1 modulo p). The theorem provides a necessary and sufficient condition for primality, but it is not practical forlarge numbers since computing factorials grows rapidly. However, it has theoretical importance in number theory and is some-times used in primality testing.Wilson's Theorem was first conjectured by John Wilson in the 18th century and later proven by Joseph-Louis Lagrange. Although not widely used in practical applications, it remains an elegant result linking factorials and modular arithmetic.

Euler's factorization method is a number theoretic technique for factoring composite numbers based on the representation of a number as a sum of two squares. It is an extension of Fermat's factorization method and relies on the identity :

$n = a^2 + b2 = c2 + d^2$

If a number N can be expressed as the sum of two different squares in two ways, then it can be factored using the identify :

$$(a - c)(a + c) = (d - b)(d + b)$$

Euler's method is particularly useful for factoring numbers that can be expressed as the sum of two squares in multiple ways.

6.3. FERMAT'S FACTORIZATION METHOD

Let n be an odd positive integer which is the difference of squares of two integers, i.e.,

$n = x^2 - y^2$

$= (x + y)(x - y)$

Conversely, if $n = ab$, $a \geq b \geq 1$, then we can write

$$n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

Since n is an odd integer, we have a and b will be odd integers and consequently $\frac{a+b}{2}$ and $\frac{a-b}{2}$ will be non-negative integers.

One begins the search for possible x and y satisfying the equation $n = x^2 - y^2$

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

by first determining the smallest integer k for which $k^2 \geq n$. Now look successively at the numbers $k^2 - n$, $(k+1)^2 - n$, $(k+2)^2 - n$, ……

until a value of $m \geq \sqrt{n}$ is found making $m^2 - n$ a square. The process cannot go an indentinitely, because we eventually arrive at

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

the representation of n corresponding to the trivial factorization $n = n.1$. If this point is reached without a square difference having been discovered earlier, then n has no factors other than n and 1, in which case it is a prime.

Example 1. Use Fermat's factorization method, factorize 10561.

Solution: From the table of squares, we have

$1022 < 10541 < 1032$

Therefore, we have to consider the values of $k^2 - 10541$ for $k \geq 103$. Taking k = 103, 104, …., we obtain

$1032 - 10541 = 10609 - 10541 = 68$

$1042 - 10541 = 10816 - 10541 = 275$

$1052 = 10541 = 11025 - 10541 = 484 = 222$

$10541 = 1052 = 222$

$= (105 + 22) \times (105 - 22)$

$= 127 \times 83$

Example 2. Factorize $211 - 1$ by using Farmat's factorization method.

Solution: We have $211 - 1 = 2048 - 1$

$= 2047$

From the table of squares we see that $452 < 2047 < 462$. Therefor we find the values of $k2 - 2047$ for $k \geq 46$. Taking $k = 46, 47, \ldots..$ we get

$462 - 2047 = 2116 - 2047 = 69$

$472 - 2047 = 2209 - 2047 = 162$

$482 - 2047 = 2304 - 2047 = 257$

$492 - 2047 = 2401 - 2047 = 354$

$502 - 2047 = 2500 - 2047 = 453$

$512 - 2047 = 2602 - 2047 = 554$

$522 - 2047 = 2704 - 2047 = 657$

$532 - 2047 = 2809 - 2047 = 762$

$542 - 2047 = 2916 - 2047 = 869$

$552 - 2047 = 3025 - 2047 = 978$

$562 - 2047 = 3136 - 2047 = 1089 = 332$

$\therefore 2047 = 562 - 332$

$= (56 + 33)(56 - 33)$

$= 89 \times 23$

W CHECK YOUR PROGRESS

Q.1. Factorize the following numbers by using Fermat's factorization method :

B (a) 119143 KS (b) 23449

6.4. FERMAT'S LITTLE THEOREM

Statement: If p is prime and $p \chi a$, then $a^{p-1} \equiv 1 (mod\ p)$

Proof: We consider the integers a, 2a, 3a, ….., (p – 1)a. None of there is divisible by p. Also no two of these are congruent mod p, because if

ra ≡sa (mod p), for $1 \leq$ r, s $\leq$ p –1

$\Rightarrow$r ≡s (mod p) as (a, p) = 1

Which is impossible as $1 \leq$ r, s $\leq$ p – 1. Therefore the integers a, 2a, 3a, ….. (p – 1) a are congruent (mod p) to the integers 1, 2, 3, ……, (p – 1), taken in some order, i.e.

a. 2a. 3a ……. (p – 1) 1.2.3…… (p – 1) (mod p)

$\Rightarrow a^{p-1}(p-1) \equiv (p-1)!\ \ (mod\ p)$

$\Rightarrow a^{p-1} \equiv 1 (mod\ p)$ $[\because ((p-1)!,\ p) = 1]$

Corollary 6.4.1. If p is prime and a is any integer, then $a^p \equiv a (mod\ p)$

Proof : Let p be prime and a be any integer. Then either p|a of (a, p) = 1.

Case (I). If p|a $\Rightarrow a \equiv 0 (mod\ p)$

$\Rightarrow a^p \equiv 0 (mod\ p)$

$\Rightarrow a^p \equiv a (mod\ p)$

Corollarly 6.4.2. If p and q are distinct primes such that $a^p \equiv a (mod\ q)$ and $a^q \equiv a (mod\ p)$ then $a^{pq} \equiv a (mod\ pq)$

Proof : Let p and q are distinct prime such that $a^p \equiv a (mod\ q)$ and $a^q \equiv a (mod\ p)$

By Corollary 6.4.1.,

$$\left(a^p\right)^q \equiv a^p \,(mod\, q)$$

$$\Rightarrow a^{pq} \equiv a^q \,(mod\, q) \quad [\because a^p \equiv a\,(mod\, q)]$$

$$\Rightarrow q \mid a^{pq} - a \qquad \text{---------- (1)}$$

Similarly

$$\left(a^q\right)^p \equiv a^q \,(mod\, p)$$

$$\Rightarrow a^{pq} \equiv a^q \,(mod\, p) \quad [\because a^q \equiv a\,(mod\, p)]$$

$$\Rightarrow p \mid a^{pq} - a \qquad \text{---------- (2)}$$

From (1) and (2), we get

$$pq \mid a^{pq} - a \qquad [\because \text{ p and q are distinct primes}]$$

$$\Rightarrow a^{pq} \equiv a\,(mod\, pq)$$

Example 1. Prove that $n^6 - 1$ is divisible by 7 if (n, 7) = 1

Solution : Since (n, 7) = 1, so by Fermat's Little theorem,

$$n^7\text{-}1 \equiv 1 \pmod 7$$

$$\Rightarrow n^6 \equiv 1 \pmod 7$$

$$\Rightarrow 7 \mid n^6 - 1$$

i.e. n6 – 1 is divisible by 7.

Example 2. Prove that $n^7 - n$ is divisible by 42.

Solution : We have 42 = 2.3.7.

By Fermat's Little Theorem,

$$n^2 \equiv n \pmod 2 \qquad \text{---------- (1)}$$

$$n^3 \equiv n \pmod s \qquad \text{---------- (2)}$$

$$n^7 \equiv n \pmod 7 \qquad \text{---------- (3)}$$

From (1), $(n^2)^3 \equiv n^3 \pmod 2$

$\Rightarrow n^6 \equiv n^2.n \pmod 2$

$\Rightarrow n^6 \equiv n.n \pmod 2$, using (1)

$\Rightarrow n^6 \equiv n^2 \pmod 2$

$\Rightarrow n^6 \equiv n \pmod 2$, using (1)

$\Rightarrow n^6.n \equiv n.n \pmod 2$

$\Rightarrow n^7 \equiv n2 \pmod 2$

$\Rightarrow n^7 \equiv n \pmod 2$, using (1)

From (2), $(n^3)^2 \equiv n^2 \pmod 3$

$\Rightarrow n^6 \equiv n^2 \pmod 3$

$\Rightarrow n^6.n \equiv n^2.n \pmod 3$

$\Rightarrow n^7 \equiv n^3 \pmod 3$

$\Rightarrow n^7 \equiv n \pmod 3$, using (2)

Thus $n7 \equiv n \pmod 2$, $n7 \equiv n \pmod 3$ and $n^7 \equiv n \pmod 7$

$\Rightarrow n^7 \equiv n \pmod{2.3.7}$

$\Rightarrow n^7 \equiv n \pmod{42}$

$\Rightarrow 42 \mid n^7 - n$

i.e. $n^7 - n$ is divisible by 42.

Example 3. Find the remainder when $2^{73} + 14^3$ is divided by 11.

Solution : Since (2, 11) = 1, so by Fermat's Little Theorem,

$2^{11-1} \equiv 1 \pmod{11}$

$\Rightarrow 2^{10} \equiv 1 \pmod{11}$

$\Rightarrow 2^{70} \equiv 1 \pmod{11}$

$\Rightarrow 2^{70}.2^3 \equiv 1.23 \pmod{11}$

$\Rightarrow 2^{73} \equiv 8 \pmod{11}$ ---------- (1)

We have $14 \equiv 3 \pmod{11}$

$\Rightarrow 14^3 \equiv 3^3 \pmod{11}$

$\Rightarrow 14^3 \equiv 5 \pmod{11}$ ---------- (2)

From (1) and (2), we get

$2^{73} + 14^3 \equiv 8 + 5 \pmod{11}$

$\Rightarrow 2^{73} + 14^3 \equiv 2 \pmod{11}$

Therefore required remainder is 2.

Example 4. Find the remainder when 72^{1001} is divided by 31.

Proof : We have $72 \equiv 10 \pmod{31}$

$\Rightarrow 72^{1001} \equiv 10^{1001} \pmod{3}$ ---------- (1)

Since (10, 31) = 1, so by Fermat's Little Theorem,

$10^{31-1} \equiv 1 \pmod{31}$

$\Rightarrow 10^{30} \equiv 1 \pmod{31}$

$\Rightarrow (10^{30})^{33} \equiv 1^{11} \pmod{31}$

$\Rightarrow 10^{990} \equiv 1 \pmod{31}$

$\Rightarrow 10^{990}.10^{11} \equiv 1.10^{11} \pmod{31}$

$\Rightarrow 10^{1001} \equiv 10^8.10^2.10 \pmod{31}$

$\Rightarrow 10^{1001} \equiv (10^4)^2.7.10 \pmod{31}$ -------- (2)

We have $10^4 \equiv 18 \pmod{31}$

$\Rightarrow (10^4)^2 \equiv 18^2 \pmod{31}$

$\Rightarrow (10^4)^2 \equiv 14 \pmod{31}$ -------- (3)

From (2) and (3), we obtain

$10^{1001} \equiv 14 \times 7 \times 10 \pmod{31}$

$\Rightarrow 10^{1001} \equiv 980 \pmod{31}$

$\Rightarrow 10^{1001} \equiv 19 \pmod{31}$ ---------- (4)

From (1) and (4), we get

$$72^{1001} \equiv 19 \pmod{31}$$

Which shows that the remainder is 19 when 72^{1001} is divided by 31.

Example 5. Show that $5^{38} \equiv 4 \pmod{11}$

Solution : Since (5, 11) = 1, by Fermat's Little Theorem,

$$5^{11-1} \equiv 1 \pmod{11}$$

$$5^{10} \equiv 1 \pmod{11}$$

$$5^{11} \equiv 5 \pmod{11}$$

$$(5^{11})^3 \equiv 5^3 \pmod{11}$$

$$5^{33} \equiv 5^3 \pmod{11}$$

$$5^{33}.5^5 \equiv 5^3.5^5 \pmod{11}$$

$$5^{38} \equiv (5^2)^4 \pmod{11}$$

$$5^{38} \equiv 3^4 \pmod{11}$$

$$5^{38} \equiv 81 \pmod{11}$$

$$5^{38} \equiv 4 \pmod{11}$$

Which shows that the remainder is 4 when 538 is divided by 11.

W CHECK YOUR PROGRESS

Q.2. Show that $n^{12} - 1$ is divisible by 7 if (n, 7) = 1.

Q.3. Find the remainder when $2^{1000000}$ is divided by 7.

Q.4. Show that $a^9 \equiv a \pmod{30}$ for all a.

Q.5. Find the unit digit of 3^{100} by using Fermat's Little Theorem.

Q.6. If $7 \chi a$, prove that either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Q.7. If a and b are integers not divisible by the prime p and $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$

Q.8. If p is an odd prime, then

a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv -1 \pmod{p}$

b) $1^p + 2^p + 3^p + \ldots.. + (p-1)^p \equiv 0 \pmod{p}$

Q.9. If p and q are distinct primes, prove that

$$P^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

6.5. WILSON'S THEOREM

Statement : An integer p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Proof : Let p be a prime number. Then 1, 2, 3, …., p – 1 are p – 1 in congruent solution of the algebraic congruence

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

and which gives

$$x^{p-1} - 1 \equiv (x-1)(x-2) \ldots\ldots\ldots\ldots \{x-(p-1)\} \pmod{p}$$

Putting x = p, we get

$$p^{p-1} - 1 = (p-1)(p-2) \ldots.. \{p-(p-1)\} \pmod{p}$$

$$\Rightarrow \quad 0 - 1 \equiv (0-1)(0-2) \ldots\ldots\ldots \{0-(p-1)\} \pmod{p}$$

$$\Rightarrow \quad -1 \equiv (-1)p - 1\,(p-1)! \pmod{p}$$

Either p – 1 is even or p = 2. Since p = 2 obviously satisfies $(p-1)! \equiv -1 \pmod{p}$. If p – 1 is even then $-1 \equiv (p-1)! \pmod{p}$

$$\Rightarrow (p-1)! \equiv -1 \pmod{p}$$

Conversely, let $(p-1)! \equiv -1 \pmod{p}$. To prove p is a prime number. If possible, let p is a composite number let p = rs, where $1 < r, s < p$

Since r is a factor of p, so

$$(p-1)! \equiv -1 \pmod{r}$$

$$(p-1)! \equiv 0 \pmod{r} \quad [\therefore 1 < r < p]$$

$$\Rightarrow \quad -1 \equiv 0 \pmod{r}$$

$$\Rightarrow \quad 0 \equiv -1 \pmod{r}$$

$$\Rightarrow \quad r \mid 0 - (-1)$$

$\Rightarrow$ r/1, which is a contradiction.

Hence our assumption is wrong. Hence p is a prime number.

Example 1. Find the remainder, when

(i) 15 ! is divided by 17,

(ii) 2.26 is divided by 29.

Solution : Since 17 is a prime number. So by Wilson's Theorem,

$(17 - 1)\,! \equiv -1 \pmod{17}$

$\Rightarrow 16\,! \equiv -1 \pmod{17}$

$\Rightarrow 16.15\,! \equiv -1 \pmod{17}$

$\Rightarrow (-1).15\,! \equiv -1 \pmod{17}$

$\Rightarrow 15\,! \equiv +1 \pmod{17}$

Which shows that 1 is remainder when 15! Is divided by 17.

Since 29 is a prime number, so by Wilson's Theorem,

$(29 - 1)! \equiv -1 \pmod{29}$

$\Rightarrow 28\,! \equiv -1 \pmod{29}$

$\Rightarrow 28.27.26\,! \equiv -1 \pmod{29}$

$\Rightarrow (-1).(-2).26! \equiv 0 - 1 \pmod{29}$

$\Rightarrow 2.\,26\,! \equiv (29 - 1) \pmod{29}$

$\Rightarrow 2.\,26\,! \equiv 28 \pmod{29}$

which shows that 28 is remainder wen 2. 26! Is divided by 29.

Corollary 6.5.1. An integer p is a prime number if and only if $2\,(p - 3)\,! + 1 \equiv 0 \pmod{p}$

Proof : By Wilson's Theorem,

Integer p is prime $\Leftrightarrow (p - 1)\,! \equiv -1 \pmod{p}$

$\Leftrightarrow (p-1)! + 1 \equiv 0 \pmod{p}$

$\Leftrightarrow (p-1)(p-2)(p-3)! + 1 \equiv 0 \pmod{p}$

$\Leftrightarrow (0-1)(0-2)(p-3)! + 1 \equiv 0 \pmod{p}$

$\Leftrightarrow 2(p-3)! + 1 \equiv 0 \pmod{p}$

Theorem 6.5.2 Let p be an odd prime. The congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p \equiv 1 \pmod{4}$.

Proof : Suppose $x^2 \equiv -1 \pmod{p}$ has a solution say.

Then $a^2 \equiv -1 \pmod{p}$

Since (a, p) = 1, so by Fermat's Little Theorem,

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \quad 1 \equiv a^{p-1} \pmod{p}$$

$$\equiv \left(a^2\right)^{\frac{p-1}{2}} \pmod{p}$$

$$\equiv (-1)^{\frac{p-1}{2}} \pmod{p} \quad [\because a2 \equiv -1 \pmod{p}]$$

Since p is odd, so is $\frac{p-1}{2}$ an integer. But the last equation is true only for $\frac{p-1}{2}$ is even.

So let $\frac{p-1}{2} = 2k$ for some integer k.

$\Rightarrow p - 1 = 4k$

$\Rightarrow 4 \mid p - 1$

$\Rightarrow p \equiv 1 \pmod{4}$

Conversely, Suppose $p \equiv 1 \pmod{4}$

$\Rightarrow$ p = 4k + 1, for some integer k.

Since p is an odd prime, so by Wilson's Theorem,

$(p-1)! \equiv -1 \pmod{p}$

$$\Rightarrow 1.2.3.....\left(\frac{p-1}{2}\right).\left(\frac{p+1}{2}\right).\left(\frac{p+3}{2}\right).....(p-1)\equiv -1(\text{mod}\,p) \quad \text{---------- (1)}$$

We have $\frac{p+1}{2}\equiv -\frac{p-1}{2}\ (\text{mod}\,p)$

$$\frac{p+3}{2}\equiv -\frac{p-3}{2}\ (\text{mod}\,p)$$

……..

……..

P – 2 ≡ – 2 (mod p)

P – 1 ≡ – 1 (mod p)

From (1),

$$1.2.3.....\left(\frac{p-1}{2}\right).\left(-\frac{p-1}{2}\right).\left(-\frac{p+3}{2}\right).....(-2).(-1)\equiv -1(\text{mod}\,p)$$

$$\Rightarrow (-1)^{\frac{p-1}{2}}\left[1.2.3.....\left(\frac{p-1}{2}\right)\right]^2\equiv -1(\text{mod}\,p)$$

$$\Rightarrow (-1)^{2k}\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv -1(\text{mod}\,p)$$

$$\Rightarrow \left[\left(\frac{p-1}{2}\right)!\right]^2\equiv -1(\text{mod}\,p)$$

i.e. $\left(\frac{p-1}{2}\right)!$ is a solution of $x^2\equiv -1(\text{mod}\,p)$

W CHECK YOUR PROGRESS

Q.10. Find the remainder when 2.28! is divided by 31.

Q.11. Prove that an integer n > 1 is prime if and only if $(n-2)!\equiv 1(\text{mod}\,p)$.

Q.12. If n is a composite integer, show that $(n-1)!\equiv 0(\text{mod}\,n)$, except when n = 4.

6.6. EULER'S FACTORIZATION METHOD

Let n be an odd integer to be factorized. Let

$n = a^2 + b^2$ where a is even and b is odd

and $n = c^2 + d^2$ where c is even and d is odd.

Then $a^2 + b^2 = c^2 + d^2$

$\Rightarrow a^2 - c^2 = d^2 - b^2$

$\Rightarrow (a + c)(a - c) = (d + b)(d - b)$

Let $k = (a - c, d - b)$. Then k is an even integer greater than or equal to 2 and $a - c = kr_1$, $d - b = kr_2$ for some integers r_1, r_2 with $(r_1, r_2) = 1$

From (1),

$(a + c)\, kr_1 = (d + b)\, kr_2$

$r_1 (a + c) = r_2 (d + b)$ ---------- (2)

$r_1 \mid r_2 (d + b)$

$r_1 \mid d + b$

$d + b = r_1 t$ for some integer t ---------- (3)

From (2) and (3), we get

$a + c = r_2 t$

Obviously $(a + c, d + b) = t$ is an even integer.

Thus $a - c = kr_1$, $a + c = r_2 t$, $d - b = kr_2$ and $d + b = r_1 t$

$$\Rightarrow a = \frac{r_1 k + r_2 t}{2},\ c = \frac{r_2 t - r_1 k}{2},\ d = \frac{r_2 k + r_1 t}{2},\ b = \frac{r_1 t + r_2 k}{2}$$

Hence $n = a^2 + b^2$

$$\Rightarrow a = \frac{r_1 k + r_2 t}{2},\ c = \frac{r_2 t - r_1 k}{2},\ d = \frac{r_2 k + r_1 t}{2},\ b = \frac{r_1 t + r_2 k}{2}$$

$$= \left(\frac{r_1 k + r_2 t}{2}\right)^2 + \left(\frac{r_1 t + r_2 k}{2}\right)^2$$

$$= \frac{r_1^2k^2 + r_2^2t^2 + r_1t^2 + r_2^2k^2}{4}$$

$$= \frac{r_1^2\left(k^2 + t^2\right) + r_2^2\left(t^2 + k^2\right)}{4}$$

$$= \left(r_1^2 + r_2^2\right)\left(\frac{k^2 + t^2}{4}\right)$$

$$= \left(r_1^2 + r_2^2\right)\left(\frac{k^2}{4} + \frac{t^2}{4}\right)$$

which gives two factors of n.

Example 1. Factorize 493 by Euler's factorization method.

Solution : We have $493 = 13^2 + 18^2$

$$493 = 3^2 + 22^2$$

Therefore $13^2 + 18^2 = 3^2 + 22^2$

$\Rightarrow 13^2 - 3^2 = 22^2 - 18^2$

$\Rightarrow (13 + 3)(13 - 3) = (22 + 18)(22 - 18)$

$\Rightarrow 16.10 = 40.4$

Now (16, 40) = 8, (10, 4) = 2 and we write

$16 = 2.8,\ 40 = 5.8,\ 10 = 5.2,\ 4 = 2.2$

Here $r_1 = 2$, $r_2 = 5$, $k = 2$, $t = 8$

Thus $493 = \left(r_1^2 + r_2^2\right)\left(\frac{k^2 + t^2}{4}\right)$

$$= \left(2^2 + 5^2\right)\left(\frac{2^2 + 8^2}{4}\right)$$

$$= 29 \times 17$$

W CHECK YOUR PROGRESS

Q.13. Factorize 38025 by Euler's factorization method.

26.7. LET US SUM UP

* Fermat's Factorization Method : Fermat's factorization method is a technique for factoring an odd integer by expressing it as a difference of two squares :

$$n = a^2 - b^2 = (a + b)(a - b)$$

To apply it, start which $a = \left[\sqrt{n}\right]$ and check whether $a^2 - n$ is a perfect square. If it is, set $b = \sqrt{a^2 - n}$ and the factors of n are (a + b) and a – b. Repeat with increasing a until a square is found. It works best when the factors of n are close together.

* Fermat's Little Theorem : If p is prime and $p \chi a$, then $a^{p-1} \equiv 1 \pmod p$

* If p is prime and a is any integer, then $ap \equiv a \pmod p$

* If p and q are distinct primes such that $a^q \equiv a \pmod p$ then $a^{pq} \equiv a \pmod{pq}$.

* Wilson's Theorem : A integer p is prime if and only if $(p-1)! \equiv -1 \pmod p$.

* An integer p is a prime member if and only if $2.(p-3)! + 1 \equiv 0 \pmod p$.

* Let p be an odd prime. The congruence $x^2 \equiv -1 \pmod p$ has a solution if and only $p \equiv 1 \pmod 4$

* Euler's Factorization Method : Let n be a odd integer to be factorized. Let

  $n = a^2 + b^2$, where a is even an b is odd

  and $n = c^2 + d^2$, where c is even and d is odd

  Then $a^2 + b^2 = c^2 + d^2$

  $\Rightarrow (a + b)(a - c) = (d + b)(d - b)$

  If ged $(a - c, d - b) = k$ and ged $(a + c, d + b) = t$

  such that $a - c = kr_1$, $a + c = r_2t$, $d - b = kr_2$

  and $d + b = r_1t$ with $(r_1, r_2) = 1$, then

  n can be factorize as

$$n = \left(r_1^2 + r_2^2\right)\left(\frac{k^2}{4} + \frac{t^2}{4}\right)$$

K 6.8. ANSWERS TO CHECK YOUR PROGRESS

Ans. to Q.1

We have n = 119143. From the table of squares, $345^2 < 119141 < 346^2$. Therefore we fine the values of $k^2 - 119143$ for $k \geq 346$. The calculations begin as follows :

$346^2 - 119143 = 119716 - 119143 = 573$

$347^2 - 119143 = 120409 - 119143 = 1266$

$348^2 - 119143 = 121104 - 119143 = 1961$

$349^2 - 119143 = 121801 - 119143 = 2658$

$350^2 - 119143 = 122500 - 119143 = 3357$

$351^2 - 119143 = 123201 - 119143 = 4058$

$352^2 - 119143 = 123904 - 119143 = 4761 = 69^2$

This last line wxhibits the factorization

$11913 = 352^2 - 69^2$

$= (352 + 69)(352 - 69)$

$=421.283$

(b) Left as an exercise.

Ans. to Q.2

Since (n, 7) = 1, so by Fermat's Little Theorem,

$n^{7-1} \equiv 1 \pmod 7$

$\Rightarrow n^6 \equiv 1 \pmod 7$

$\Rightarrow (n^6)^2 \equiv 1^2 \pmod 7$

$\Rightarrow n^{12} \equiv 1 \pmod 7$

$\Rightarrow 7 \mid n^{12} - 1$

which shows that $n^{12} - 1$ is divisible by 7.

Ans to Q.3

We have (2, 7) = 1. Therefore by Fermat's Little Theorem,

$$2^{7-1} \equiv 1 \pmod 7$$

$$\Rightarrow 2^6 \equiv 1 \pmod 7$$

$$\Rightarrow (2^6)^{166666} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{999996}.2^4 \equiv 1.2^4 \pmod 7$$

$$\Rightarrow 2^{1000000} \equiv 2 \pmod 7$$

which shows that the remainder is 2 when $2^{1000000}$ is divided by 7.

Ans. to Q.4

We have 30 = 5.3.2. Using Fermat's Little Theorem,

$$a^5 \equiv a \pmod 5 \qquad \text{---------- (1)}$$

$$a^3 \equiv a \pmod 3 \qquad \text{---------- (2)}$$

$$a^2 \equiv a \pmod 2 \qquad \text{---------- (3)}$$

From (1), $a^5 \equiv a \pmod 5$

$$\Rightarrow a^5.a^4 \equiv a.a^4 \pmod 5$$

$$\Rightarrow a^9 \equiv a \pmod 5$$

$$\Rightarrow a^9 \equiv a \pmod 5, \text{ using (1)}$$

From (2), $(a^3)^3 \equiv a^3 \pmod 3$

$$\Rightarrow a^9 \equiv a \pmod 3, \text{ using (2)}$$

From (3), $(a^2)^2 \equiv a2 \pmod 2$

$$\Rightarrow a^4 \equiv a \pmod 2, \text{ using (3)}$$

$$\Rightarrow (a^4)^2 \equiv a^2 \pmod 2$$

$$\Rightarrow a^8 \equiv a \text{ (mode 2), using (3)}$$

$$\Rightarrow a^8.a \equiv a.a \pmod 2$$

$\Rightarrow a^9 \equiv a^2 \pmod 2$

$\Rightarrow a^9 \equiv a \pmod 2$, using (3)

Thus, we obtain

$a^9 \equiv a \pmod 5$, $a^9 \equiv a \pmod 3$, $a9 \equiv a \pmod 2$

$\Rightarrow a^9 \equiv a \pmod{5.3.2}$

$\Rightarrow a^9 \equiv a \pmod{30}$ for all a.

Ans to Q.5.

We have $10 = 5.2$

Since $(5, 3) = 1$, so by Fermat's Little Theorem,

$3^{5-1} \equiv 1 \pmod 5$

$\Rightarrow 3^4 \equiv 1 \pmod 5$

$\Rightarrow (3^4)^{25} \equiv 125 \pmod 5$

$\Rightarrow 3^{100} \equiv 1 \pmod 5$ --------- (1)

Also $3 \equiv 1 \pmod 2$

$\Rightarrow 3^{100} \equiv 1 \pmod 2$

From (1) and (2), we obtain

$5 \mid 3^{100} - 1$ and $2 \mid 3^{100} - 1$

$\Rightarrow 5.2 \mid 3^{100} - 1$

$\Rightarrow 10 \mid 3^{100} - 1$

$\Rightarrow 3^{100} \equiv 1 \pmod{10}$

Therefore unit digit of 3^{100} is 1.

Ans. to Q.6

Since $7 \chi a$ so by Fermat's Little Theorem,

$a^{7-1} \equiv 1 \pmod 7$

$\Rightarrow a^6 \equiv 1 \pmod 7$

$\Rightarrow$ $7|(a^3 + 1)(a^3 - 1)$

$\Rightarrow$ $7 \mid a^3 + 1$ or $7|a^3 - 1$ as 7 is prime.

$\Rightarrow$ either $a^3 + 1$ or $a^3 - 1$ is divisible by 7.

Ans to Q.7

Assume $p \chi a$, $p \chi b$ and p be prime. Then by Fermat's Little Theorem,

$a^p \equiv a \pmod p$ and $b^p \equiv b \pmod p$ ------- (1)

Let $a^p \equiv b^p \pmod p$ ------- (2)

From (1), $a \equiv a^p \pmod p$

$\Rightarrow$ $a \equiv b^p \pmod p$ using (2)

$\Rightarrow$ $a \equiv b \pmod p$ using (1)

Ans to Q.8

(a) Since p is prime ≥ 3, so $p \chi a$ if $a < p$. By Fermat's Little Theorem,

$a^{p-1} \equiv 1 \pmod p$

Putting a = 1, 2, 3, …… (p – 1) and adding we get

$1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv (p-1).1 \pmod p$

$\Rightarrow$ $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv (0-1) \pmod p$

$\Rightarrow$ $1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots\ldots + (p-1)^{p-1} \equiv -1 \pmod p$

(b) Left as an exercise.

Ans to Q.9

Since p and q are distinct prime, so and

By Fermat's Little Theorem,

$q \chi p \Rightarrow p^{q-1} \equiv 1 \pmod q$ ---------- (1)

Clearly, $q|q^{p-1}$, so $q^{p-1} \equiv 0 \pmod q$ ---------- (2)

Form (1) and (2), $p^{q-1} + q^{p-1} \equiv 1 \pmod q$ ---------- (3)

Similarly, $p \chi q \Rightarrow q^{p-1} \equiv 1 \pmod p$ ---------- (4)

and $p \mid p^{q-1} \Rightarrow p^{q-1} \equiv 1 \pmod{p}$ ---------- (5)

From (4) and (5), $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$ ---------- (6)

From (3) and (6)

$q \mid p^{q-1} + q^{p-1}$ and $p \mid p^{q-1} + q^{p-1}$

$\Rightarrow$ $pq \mid p^{q-1} + q^{p-1} - 1$ as p and q are prime.

$\Rightarrow$ $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$

Ans to Q 10.

Since 31 is a prime number, so by Wilson's Theorem,

$(31 - 1)! \equiv -1 \pmod{31}$

$\Rightarrow$ $30! \equiv -1 \pmod{31}$

$\Rightarrow$ $30.\ 29.\ 28! \equiv -1 \pmod{31}$

$\Rightarrow$ $(-1).\ (-2)\ .\ 28! \equiv (31 - 1) \pmod{31}$

$\Rightarrow$ $2.\ 28! \equiv 30 \pmod{31}$

Which shows that 30 is the remainder when 2.28! is divided by 31.

Ans to Q. 11

By Wilson's Theorem,

n is prime $\Leftrightarrow$ $(n - 1)! \equiv -1 \pmod{n}$

$\Leftrightarrow$ $(n - 1)(n - 2)! \equiv (n - 1) \pmod{n}$

$\Leftrightarrow$ $(n - 2)! \equiv 1 \pmod{n}$ [$\because$ ged $(n - 1, n) = 1$]

Ans to Q. 12 Left as an exercise.

Ans to Q. 13

We have $38025 = 1682 + 992$

$38025 = 1562 + 1172$

Therefore $168^2 + 99^2 = 156^2 + 117^2$

$\Rightarrow$ $117^2 - 99^2 = 168^2 + 117^2$

$\Rightarrow$ $(117 - 99) = (117 + 99) = (168 - 156)(168 + 156)$

$\Rightarrow$ $18.216 = 12.324$

We have $(216, 324) = 108$, $(18, 12) = 6$ and

$216 = 2 \times 108$

$324 = 3 \times 108$

$18 = 3 \times 6$

$12 = 2 \times 6$

Here $r_1 = 3$, $r_2 = 2$, $k = 6$ and $t = 108$. Therefore

$$38025 = \left(r_1^2 + r_2^2\right)\left(\frac{k^2}{4} + \frac{t^2}{4}\right)$$

$$= \left(3^2 + 2^2\right)\left(\frac{6^2}{4} + \frac{108^2}{4}\right)$$

$$= (9 + 4)\left(\frac{36 + 11664}{4}\right)$$

$$= 13 \times 2925$$

O 6.9. FURTHER READING

1. David M Burton, Elementary Number Theory (7th Edn.) McGraw Hill Education (India) Private Limited, Chennai – 600116, 2018
2. S.B. Malik, Basic Number Theory (2nd Edn.), Vikash Publishing House Private Limited, Noida – 201301, 2017.
3. H. Kishan, Number Theory, Krishna Prakashn Media (P) Limited, Meerut – 250001 (UP), India, 2017.
4. G.H. Hardy and E.M. Wright, Theory of Numbers, Oxford Science Publication, 2003.

M 6.10. MODEL QUESTIONS

1. Factorize 8927 using Fermat's factorization method.
2. Factorize 340663 using Euler's factorization method.

3. Find the remainder when

   (i) 3^{287} is divided by 23.

   (ii) 41^{75} is divided by 3.

   (iii) 473^{38} is divided by 5.

4. Let (a, p) = (b, p) = 1. If $a^p \equiv b^p \pmod{p}$, then prove that $a^p \equiv b^p \pmod{p^2}$

5. Derive the congruence $a^{13} \equiv a \pmod{3.7.13}$ for all a.

6. Assume that p and q are distinct odd primes such that $p - 1 \mid q - 1$. If ged (a, pq) = 1

   show that $a^{q-1} \equiv 1 \pmod{pq}$.

7. If p is a prime number, then prove that

   $(p-1)! \equiv (p-1) \pmod{1 + 2 + 3 + \ldots + (p-1)}$

8. If p is odd prime, then using Wilson's Theorem, prove that

   $$1^2 + 3^2 + 5^2 \ldots\ldots\ldots (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$$

9. If p is a prime of the form 4k + 3, then prove that either $\left(\frac{p-1}{2}\right)! \equiv 1 \pmod{p}$ or $\left(\frac{p-1}{2}\right)! \equiv -1 \pmod{p}$ and $\left(\frac{p-1}{2}\right)!$ is a solution of the quadratic congruence $x^2 \equiv 1 \pmod{p}$.

10. If p and p + 2 are a pair of twin primes, then prove that $4((p-1)!+1) + p \equiv 0 \pmod{p(p+2)}$

11. If p is an odd prime, $p \equiv 3 \pmod 4$ and $a^2 + b^2 \equiv 0 \pmod p$, then prove that $a \equiv 0 \pmod p$ and $b \equiv 0 \pmod p$

12. Prove Wilson's Theorem by using Fermat's Little Theorem.

*** *** ***