Fermat's little Theorem

Tip 1

Fermat's theorem is an important remainder theorem which can be used to find the remainder easily.

Fermat's theorem states that for any integer 'a' and prime number 'p', a^p-a is always divisible by 'p'.

Also, if a is not divisible by p, i.e. if a and p are relatively prime, then

$$a^{(p-1)} \ mod\ p \ = \ 1\ mod\ p$$

which means the remainder is 1.

The second part of the theorem is very useful in solving problems.

Fermat's Theorem

Example:

When 2^{256} is divided by 17, the remainder would be _: (CAT 2002)

Here, 7 is a prime number and 2, 17 are relatively prime.

Therefore, $2^{16}\ mod\ 17 = 1$.

2^{256} can be written as $(2^{16})^{16}$.

Since, $2^{16}\ mod\ 17 = 1$, $(2^{16})^{16}\ mod\ 17 = 1$.

Thus, the remainder when 2^{256} is divided by 17

Fermat's Theorem

Example:

Find the remainder when 3^{75} is divided by 37.

Here, 37 is a prime number. Hence, Fermat's theorem can be used. Also, 3 and 37 are relatively prime.
Therefore,
$3^{36}\ mod\ 37 = 1$

$3^{72}\ mod\ 37 = (3^{36})^2\ mod\ 37 = 1$

$3^{75} mod\ 37 = 3^{72}.3^3 mod\ 37 = 3^3 mod\ 37$, $27\ mod\ 37$ is equal to 27.

Hence, the remainder when 3^{75} is divided by 37 is 27.

Tip 2

Euler's totient

Euler's theorem is one of the most important remainder theorems. It is imperative to know about Euler's totient before we can use the theorem.

Euler's totient is defined as the number of numbers less than 'n' that are co-prime to it.
It is usually denoted as $\phi(n)$.

The formula to find Euler's totient is $\phi(n) = n*(1 - \frac{1}{a}) * (1 - \frac{1}{b})*\ldots$ where a, b are the prime factors of the numbers.

Eg) Find the number of numbers that are less than 30 and are co-prime to it.

30 can be written as 2*3*5.
$\phi(30) = 30 * 1/2 * 2/3 * 4/5$
$= 8$

Therefore, 8 numbers less than 30 are co-prime to it.

Euler's Theorem

Euler's theorem

Euler's theorem states that $a^{\phi(n)} \pmod{n} = 1 \pmod{n}$ if 'a' and 'n' are co-prime to each other.
So, if the given number 'a' and the divisor 'n' are co-prime to each other, we can use Euler's theorem.

Example 1:
What is the remainder when 2^{256} is divided by 15?
2 and 15 are co-prime to each other. Hence, Euler's theorem can be applied.
15 can be written as 5*3.

Euler's totient of 15 = $15*(1 - \frac{1}{3})* (1 - \frac{1}{5}) = 15*\frac{2}{3}*\frac{4}{5} = 8$

Therefore, we have to try to express 256 as 8k + something. 256 can be expressed as 8*32

We know that, $a^{\phi(n)} \pmod{n} = 1 \pmod{n}$
$2^{8*32} \pmod{15} = 1 \pmod{15}$.

Therefore, 1 is the right answer.

Euler's Theorem

Example

Example 2:
What are the last 2 digits of 7^{2008} ?

Finding the last 2 digits is similar to finding the remainder when the number is divided by 100.
100 and 7 are co-prime to each other. Hence, we can use Euler's theorem.

100 can be written as $2^2 * 5^2$.
Euler's totient of 100, $\phi(100) = 100*(1 - \frac{1}{2}) * (1 - \frac{1}{5})$.

$$= 100* (\frac{1}{2}) * (\frac{4}{5})$$

$$\phi(100) = 40.$$

7^{2008} can be written as $7^{2000}*7^8$

7^{2000} can be written as $7^{40*(25)}$. Hence, 7^{2000} will yield a remainder of 1 when divided by 100.
The problem is reduced to what will be the remainder when 7^8 is divided by 100.
We know that $7^4 = 2401$.
$7^8 = 7^4*7^4 = 2401*2401$.

As we can clearly see, the last 2 digits will be 01.

Tip 3

According to Wilson's theorem for prime number 'p',
[(p-1)! + 1] is divisible by p.

In other words, (p-1)! leaves a remainder of (p-1) when divided by p.

Thus, **(p-1)! mod p = p-1**

For e.g.
4! when divided by 5, we get 4 as a remainder.

6! When divided by 7, we get 6 as a remainder.

10! When divided by 11, we get 10 as a remainder.

Wilson's Theorem

If we extend Wilson's theorem further, we get an important corollary
(p-2)! mod p = 1

As from the Wilson's theorem we have, (p-1)! mod p = (p-1)

Thus, [(p-1)(p-2)!] mod p = (p-1)

This will be equal to [(p-1) mod p] * [(p-2)! mod p] = (p-1)

For any prime number 'p', we observe that (p-1) mod p = (p-1).

For e.g. 6 mod 7 will be 6.
Thus, (p-1) * [(p-2)! mod p] = (p-1)
Thus, for RHS to be equal to LHS,

(p-2)! mod p = 1
Hence, 5! mod 7 will be 1 and 51! mod 53 will be 1

Wilson's Theorem

Examples:

Q.1) What will be the remainder when 568! Is divided by 569?

Solution: According to Wilson's theorem we have,
For prime number 'p', (p-1)! mod p = (p-1)

In this case 569 is a prime number. Thus, 568! mod 569 = 568.
Hence, when 568! is divided by 569 we get 568 as remainder.
Answer: 568

Q.2) What will be the remainder when 225! Is divided by 227?

Solution: We know that for prime number 'p', (p-2)! mod p = 1.
In this case, 227 is a prime number.

Thus, 225! mod 227 will be equal to 1. In other words, when 225! Is divided by 227 we get remainder as 1.
Answer: 1

Wilson's Theorem

Q.3) What will be the remainder when 15! is divided by 19?

Solution:19 is a prime number.
From corollary of Wilson's theorem, for prime number 'p',
(p-2)! mod p = 1

Thus, 17! mod 19 = 1
[17*16*15!] mod 19 = 1
[17 mod 19]* [16 mod 19]* [15! mod 19] = 1
[-2]*[-3]* [15! mod 19] = 1
[6 * 15!] mod 19 = 1

Multiplying both sides by 3, we get
[18*15!] mod 19 = 3
[-1*15!] mod 19 = 3

Multiplying both sides by '-1', we get
15! mod 19 = -3

Remainder of '-3' when divided by 19 is same as remainder of '16' when divided by 19.
Thus 15! mod 19 = 16
Answer: 16

Wilson's Theorem

Q.4) What will be the remainder when $(23!)^2$ is divided by 47?

Solution: 47 is a prime number.
From corollary of Wilson's theorem, for prime number 'p',
(p-2)! mod p = 1

Thus, 45! mod 47 = 1
[45*44*43*42*...*25*24*23!] mod 47 = 1
[(-2)*(-3)*(-4)*(-5)*...*(-22)*(-23) * 23!] mod 47 = 1

We see that, there are even number of terms from '-2' to '-23'. Thus, negative sign cancels off.

We get,
[23!*23!] mod 47 = 1
Thus, $(23!)^2$ mod 47 =1

Hence, when $(23!)^2$ is divided 47, we get 1 as a remainder.
Answer: 1