CATin

READY TO ACE CAT 2026?

Your Complete Self-Study Prep Ecosystem

Exclusive Launch Waitlist Offer:

Join the waitlist today for an exclusive 20% discount on launch! Get priority platform access and all 15 reference sheets delivered directly to your inbox.

JOIN WAITLIST AT CATIN.IN

CAT Remainder Theorems Formulas

Fermat's little Theorem:

➔ 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 $a^{(p-1)} \bmod p = 1 \bmod p$. Which means the remainder is 1.

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

- **Example:** when 2^{256} is divided by 17, the remainder would be_____:

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

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

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

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

Thus, the remainder when 2^{256} is divided by 17 is 1.

- **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, $3^{36} \bmod 37 = 1$

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

  $3^{75} \bmod 37 = 3^{72} \cdot 3^3 \bmod 37 = 3^3 \bmod 37$

  $27 \bmod 37$ is equal to 27.

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

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

$$\phi(n) = n * \left(1 - \frac{1}{a}\right) * \left(1 - \frac{1}{b}\right) *$$....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.

$$\phi(30)=30*\left(\frac{1}{2}\right) * \left(\frac{2}{3}\right) * \left(\frac{4}{5}\right) = 8$$

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

➔ 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 = $15*\left(1 - \frac{1}{3}\right) * \left(1 - \frac{1}{5}\right)$
  = $15*\frac{2}{3}*\frac{4}{5}=8$
  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.

- **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, $\phi(100)$

  $= 100*\left(1 - \frac{1}{2}\right) * \left(1 - \frac{1}{5}\right)$

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

  $\phi(100) = 40$

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.

Wilson's Theorem:

➔ 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 Example:

➔ 4! When divided by 5, we get 4 as remainder.

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

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

➔ 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

- **Examples:**
- Q.1) What will be the remainder when 568! Is it 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! divided by 569 we get 568 as remainder.

  Answer: 568

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

  Solution: We know that for the 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 the remainder as 1.

  Answer: 1

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

  Solution: 19 is a prime number.

➔ From the 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 the same as the remainder of '16' when divided by 19.

Thus 15! Mod 19 = 16

Answer: 16

- 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*.....*25*24*23!] mod 47 = 1

[(-2)*(-3)*(-4)*.....*(-22)*(-23)*23!] mod 47 = 1

➔ We see that there are even numbers of terms from '-2' to '-23'. Thus negative signs cancel 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

Chinese Remainder Theorem:

- The Chinese remainder theorem is useful when the divisor of any number is composite.
- Let M be a number which is divided by a divisor N.
  The theorem states that if N is the divisor which can be expressed as N = a*b where a and b are co-prime
- Then, M mod N = ar_2x+br_1y
  Here r_1 = M mod a
  And r_2 = M mod b
  Here, ax + by = 1

- **Example 1**
- Find the remainder when 344^{237} is divided by 119
  In the first look it looks difficult but if one knows the chinese remainder theorem then the question can be solved very easily.

- 119 = 17*7, so here a = 17 and b = 7

  344^{237} mod 17 = 4^{237} mod 17 = ($4*16^{116}$) mod 17 = 4*1 = 4

  Hence, we get r_1=4

  Now, 344^{237} mod 7 = 1^{237} mod 7 = 1, Hence r_2=1

  We know that M mod N = $ar_2x + br_1y$
- Therefore, 344^{237} mod 119 = 17*1x + 7*4y = 17x + 28y

  We know that 17x + 7y = 1
- We can see that x =5 and y = -12 satisfies the above equation.

  Hence, putting the values of x and y in equation 1, we get 344^{237} mod 119 = 117 * 5 - 28 * 12 = 85-336 = -251

  Converting this into positive remainder we get 357-251=106
- Hence, the required remainder is 106.

Example 2:

- Let's consider another example to understand is better find the remainder when 495^{2517} is divided by 78.
- In this question also, the divisor is 78 which can be written as 13*6. So, we can use the Chinese remainder theorem in this question as well.
  Let's take a = 13 and b = 6
  So we can write $495^{2517} \bmod 78 = 13r_2x+6r_1y$

➔ $r_1=495^{2517} \bmod 13 = 1^{2517} \bmod 13 = 1$

➔ $r_2=495^{2517} \bmod 6 = 3^{2517} \bmod 6 = (2^{2516} \bmod 2)*3 =$
$1*3 = 3$

➔ We also know that $13x+6y=1$
$x = 1$ and $y = -2$ satisfies the above equation.

➔ Hence, we can obtain the remainder as
$495^{2517} \bmod 78 = 13r_2x+6r_1y = 13*3*1 - 6*1-2$
$=39-12 = 27$
Hence, the required answer is 27.