

# Fermat's Little Theorem and Euler's Totient function

# Fermat's little theorem

- The little theorem is often used in number theory in the testing of large primes .
- If p is a prime which does not divide a( positive integer) , then  $a^{p-1} \equiv 1 \pmod{p}$
- If p is a prime that is not a factor of a, then when a is multiplied together p-1 times, and the result divided by p, we get a remainder of one.
- For example, if we use a=7 and p=3, the rule says that  $7^2$  divided by 3 will have a remainder of one. In fact  $49/3$  does have a remainder of one.

# Fermat's little theorem

- We can test  $3^{90}$  using Fermat's Little Theorem without ever finding out what the actual value of  $3^{90}$  is, by using the patterns of remainders for powers of 3 divided by 91...
- $a=3 \ p = 7 \ 3^6=729$  remainder on division by 7 is 1
- Since  $3^6 = 1 \pmod{91}$  then any power of  $3^6$  will also be  $=1 \pmod{91}$ , and  $3^{90} = (3^6)^{15}$ .

# Solve

1. Find  $3^{31} \bmod 7$ .
2. Find  $2^{35} \bmod 7$ .
3. Find  $128^{129} \bmod 17$ .
4. The number  $2^{1000}$  is divided by 13. What is the remainder?
5. Find  $29^{25} \bmod 11$ .
6. Find  $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \bmod 7$ .

1. Find  $3^{31} \bmod 7$ .

[Solution:  $3^{31} \equiv 3 \bmod 7$ ]

By Fermat's Little Theorem,  $3^6 \equiv 1 \bmod 7$ . Thus,  $3^{31} \equiv 3^1 \equiv 3 \bmod 7$ .

2. Find  $2^{35} \bmod 7$ .

[Solution:  $2^{35} \equiv 4 \bmod 7$ ]

By Fermat's Little Theorem,  $2^6 \equiv 1 \bmod 7$ . Thus,  $2^{35} \equiv 2^5 \equiv 32 \equiv 4 \bmod 7$ .

3. Find  $128^{129} \bmod 17$ .

[Solution:  $128^{129} \equiv 9 \bmod 17$ ]

By Fermat's Little Theorem,  $128^{16} \equiv 9^{16} \equiv 1 \bmod 17$ . Thus,  $128^{129} \equiv 9^1 \equiv 9 \bmod 17$ .

4. (1972 AHSME 31) The number  $2^{1000}$  is divided by 13. What is the remainder?

[Solution:  $2^{1000} \equiv 3 \pmod{13}$ ]

By Fermat's Little Theorem,  $2^{12} \equiv 1 \pmod{13}$ . Thus,  $2^{1000} \equiv 2^{400} \equiv 2^{40} \equiv 2^4 \equiv 16 \equiv 3 \pmod{13}$ .

5. Find  $29^{25} \pmod{11}$ .

[Solution:  $29^{25} \equiv 10 \pmod{11}$ ]

By Fermat's Little Theorem,  $29^{10} \equiv 7^{10} \equiv 1 \pmod{11}$ . Thus,  $29^{25} \equiv 7^5 \equiv 7(-4)^4 \equiv 7 \cdot 256 \equiv 7 \cdot 3 \equiv 21 \equiv 10 \pmod{11}$ .

6. Find  $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \pmod{7}$ .

[Solution:  $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 0 \pmod{7}$ ]

By Fermat's Little Theorem,  $2^6 \equiv 3^6 \equiv 4^6 \equiv 5^6 \equiv 6^6 \equiv 1 \pmod{7}$ . Thus,  $2^{20} + 3^{30} + 4^{40} + 5^{50} + 6^{60} \equiv 2^2 + 3^0 + 4^4 + 5^2 + 6^0 \equiv 4 + 1 + 2^8 + 25 + 1 \equiv 4 + 1 + 4 + 4 + 1 \equiv 14 \equiv 0 \pmod{7}$ .

# Euler's totient function

- In number theory, **Euler's totient function** counts the positive integers up to a given integer  $n$  that are relatively prime to  $n$ .
- It is written using the Greek letter phi as  $\varphi(n)$  or  $\phi(n)$ , and may also be called **Euler's phi function**.
- It can be defined more formally as the number of integers  $k$  in the range  $1 \leq k \leq n$  for which the greatest common divisor  $\gcd(n, k)$  is equal to 1
- The integers  $k$  of this form are sometimes referred to as totatives of  $n$

Rule 1: If  $p$  is a prime then  $\phi(p) = p - 1$ .

Rule 2: If  $a = p^n$  is a prime power then  $\phi(p^n) = p^n - p^{n-1}$ .



Rule 3: If  $\gcd(m, n) = 1$  then  $\phi(mn) = \phi(m)\phi(n)$ .

- *Rule 1:*
  - $\phi(41) = 41-1$  since 41 is a prime number
- *Rule 2:*
  - $\phi(32)=2^5=2^5-2^4=16$
  - 32 can be written as a Power of prime number 2
- *Rule 3:*
  - $\phi(35)=7 \times 5 = (7-1)(5-1)=24$ 

 Rule 1
  - 35 is written as product of two primes

# Euler Totient Function $\phi(n)$

- The multiplicative group for  $Z_n$ , denoted with  $Z_{n'}^*$ , is the subset of elements of  $Z_n$  relatively prime with  $n$ .
- The totient function of  $n$ , denoted with  $\phi(n)$ , is the size of  $Z_{n'}^*$
- Example  $Z_{10}^* = \{ 1, 3, 7, 9 \}$   $\phi(10) = 4$
- $\{(2,10), (4,10), (5,10), (6,10), (8,10), (10,10)\}$
- $\{(1,10), (3,10), (7,10), (9,10)\}$

# Euler Totient Function $\phi(n)$

- If  $p$  is prime, we have  $Z_{,p}^* = \{1, 2, \dots, (p - 1)\}$

$$\phi(p) = p - 1$$

- For each element  $x$  of  $Z_n^*$ , we have  $x^{\phi(n)} \bmod n = 1$
- Example ( $n = 10$ )  $\phi(10) = 4$
- $3^{\phi(10)} \bmod 10 = 3^4 \bmod 10 = 81 \bmod 10 = 1$
- $7^{\phi(10)} \bmod 10 = 7^4 \bmod 10 = 2401 \bmod 10 = 1$
- $9^{\phi(10)} \bmod 10 = 9^4 \bmod 10 = 6561 \bmod 10 = 1$

# Euler Totient Function $\phi(n)$

- to compute  $\phi(n)$  need to count number of elements to be excluded
- in general need prime factorization, but
  - for  $p$  (p prime)  $\phi(p) = p-1$
  - for  $p.q$  ( $p,q$  prime)  $\phi(p \cdot q) = (p-1)(q-1)$
- eg.
  - $\phi(37) = 36$
  - $\phi(21) = (3-1) \times (7-1) = 2 \times 6 = 12$

Find the remainder when  $5^{37}$  is divided by 63.

Answer: 5 and 63 are coprime to each other, therefore we can apply Euler's theorem here.

$$63 = 3^2 \times 7 \Rightarrow \phi(63) = 63\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{7}\right) = 18$$

$$\text{Therefore, } \text{Remainder}\left[\frac{5^{18}}{63}\right] = 1 \Rightarrow \text{Remainder}\left[\frac{5^{18} \times 5^{18}}{63}\right] = \text{Remainder}\left[\frac{5^{36}}{63}\right] = 1 \Rightarrow \text{Remainder}\left[\frac{5^{37}}{63}\right] = \text{Remainder}\left[\frac{5^{36} \times 5}{63}\right] = 5$$

---

Find the remainder when  $52^{60}$  is divided by 31.

Answer: 31 is a prime number therefore  $\phi(N) = 30$ . 52 and 31 are prime to each other. Therefore, by Fermat's theorem:

$$\text{Remainder}\left[\frac{52^{30}}{31}\right] = 1 \Rightarrow \text{Remainder}\left[\frac{52^{60}}{31}\right] = 1$$

Find the last three digits of  $57^{802}$ .

Answer: Many a times (not always), the quicker way to calculate the last three digits is to calculate the remainder by 1 000. We can see that 57 and 1 000 are coprime to each other. Therefore, we can use Euler's theorem here if it's useful.

$$1\ 000 = 2^3 \times 5^3 \Rightarrow \phi(1000) = 1000\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 400$$

Therefore,

$$\text{Remainder}\left[\frac{57^{400}}{1000}\right] = 1 \Rightarrow \text{Remainder}\left[\frac{57^{400} \times 57^{400}}{1000}\right] = \text{Remainder}\left[\frac{57^{800}}{1000}\right] = 1$$

$$\Rightarrow \text{Remainder}\left[\frac{57^{802}}{1000}\right] = \text{Remainder}\left[\frac{57^{800} \times 57^2}{1000}\right] = 249$$

Hence, the last two digits of  $57^{802}$  are 249.