

# WEB3CLUBS FOUNDATION LIMITED

---

Course Instructor: DR. Cyprian Omukhwaya Sakwa  
PHONE: +254723584205 Email: cypriansakwa@gmail.com

## Foundational Mathematics for Web3 Builders

**Lecture 16/Revision**

**May 27, 2024**

## 1.11 Fermat's Little Theorem

### Theorem 14 (Fermat's Little Theorem)

*Let  $p$  be prime. Then for each integer  $a$  not divisible by  $p$ , we have*

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

If  $a$  is coprime to  $p$ , then we can multiply both sides of  $a^{p-1} \equiv 1 \pmod{p}$  by  $a$  and rewrite the expression into the following equivalent form

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

Note that if  $p$  is prime and  $a$  another integer divisible by  $p$ , then  $a^{p-1} \equiv 0 \pmod{p}$ .

### Example 48

Use Fermat's Little theorem to calculate

$$2^{1982} \bmod 19.$$

### Solution

Since 19 is prime and  $19 \nmid 2$ , Fermat's Little theorem is applicable.

Thus  $2^{19-1} \equiv 1 \bmod 19$ . That is  $2^{18} \equiv 1 \bmod 19$ .

By division algorithm,  $1982 = 18 \cdot 110 + 2$ .

$$\begin{aligned}\text{Therefore, } 2^{1982} &= 2^{18 \cdot 110 + 2} \\ &= (2^{18})^{110} \times 2^2 \\ &= 1^{110} \times 2^2 \\ &= 4\end{aligned}$$

Hence  $2^{1982} \bmod 19 \equiv 4 \bmod 19$

### Example 49

Find the remainder when  $8^{1000}$  is divided by 17.

#### Solution

Since 17 is prime and  $17 \nmid 8$ , by Fermat's Little theorem,  $8^{16} \equiv 1 \pmod{17}$ . Using division algorithm,  $1000 = 16 \cdot 62 + 8$

Thus,  $8^{1000} = 8^{16 \cdot 62 + 8}$

$$= (8^{16})^{62} \times 8^8$$

$$= (1)^{62} \times 8^8 = 8^8$$

We now find powers of 8

$$8^2 = 13 \pmod{17}$$

$$8^3 = 2 \pmod{17}$$

So that  $8^8 = 8^{3+3+2} = 8^3 \times 8^3 \times 8^2$

$$= 2 \times 2 \times (-4)$$

$$= -16 \equiv 1 \pmod{17}$$

Thus,  $8^{1000} \pmod{17} = 1$

### Example 50

Find  $524^{9999} \bmod 23$

### Solution

Here, 23 is prime and  $23 \nmid 524$  so we can apply Fermat's Little theorem.

First, we reduce  $524 \bmod 23 \equiv 18 \bmod 23$  so that  $524^{9999} \bmod 23$  equals to  $18^{9999} \bmod 23$ .

By Fermat's Little theorem,  $18^{22} \equiv 1 \bmod 23$ .

Using division algorithm, we have  $9999 = 22 \cdot 454 + 11$ .

$$\begin{aligned}\text{Thus, } 18^{9999} &= 18^{22 \cdot 454 + 11} \\ &= (18^{22})^{454} \times 18^{11} \\ &= 1^{454} \times 18^{11} = 18^{11}\end{aligned}$$

### Solution (conti...)

We now get powers of 18

$$18^2 = 2$$

$$18^{10} = (18^2)^5 = 2^5 = 9$$

$$\begin{aligned}\text{Thus, } 18^{11} &= 18^{10+1} = 18^{10} \times 18^1 \\ &= 9 \times 18 \\ &= 9 \times (-5) \equiv 1 \pmod{23}\end{aligned}$$

So that  $524^{9999} \pmod{23} = 1$

### Example 51

Find  $2^{320} + 3^{23} + 5^{79} + 8^{1982} + 9^{2020} \pmod{11}$ .

### Solution

By Fermat's Little theorem, we have

$$2^{10} = 3^{10} = 5^{10} = 8^{10} = 9^{10} \equiv 1 \pmod{11}.$$

Since  $320 = 10 \cdot 32 + 0$ ,  $23 = 10 \cdot 2 + 3$ ,  $79 = 10 \cdot 7 + 9$ ,  $1982 = 10 \cdot 198 + 2$ ,  $2020 = 10 \cdot 202 + 0$  we have

$$\begin{aligned} 2^{320} + 3^{23} + 5^{79} + 8^{1982} + 9^{2020} &= 2^0 + 3^3 + 5^9 + 8^2 + 9^0 \\ &= 1 + 5 + 9 + 9 + 1 = 3 \end{aligned}$$

Thus  $2^{320} + 3^{23} + 5^{79} + 8^{1982} + 9^{2020} \pmod{11} = 3$ .

### Example 52

Solve the congruence

$$x^{103} \equiv 4 \pmod{11}$$

### Solution

By Fermat's Little theorem  $x^{10} \equiv 1 \pmod{11}$ .

By division algorithm we have  $103 = 10(10) + 3$

Thus  $x^{103} \equiv x^3 \pmod{11}$ .

Thus, we solve  $x^3 \equiv 4 \pmod{11}$ .

We try all values from  $x = 0, 1, 2, \dots, 10$ . We find  $5^3 \equiv 4 \pmod{11}$ .

Thus  $x \equiv 5 \pmod{11}$ .



### Example 53

Find all integers  $x$  such that

$$x^{86} \equiv 6 \pmod{29}.$$

### Solution

By Fermat's Little theorem  $x^{28} \equiv 1 \pmod{29}$ .

By division algorithm we have  $86 = 28(3) + 2$

Thus  $x^{86} \equiv x^2 \pmod{29}$ .

Thus, we solve  $x^2 \equiv 6 \pmod{29}$ . which is same as  $x^2 \equiv 64 \pmod{29}$

Thus,  $x^2 - 64 \equiv 0 \pmod{29}$  or  $(x - 8)(x + 8) \equiv 0 \pmod{29}$ .

Thus  $x \equiv 8, 21 \pmod{29}$ .