WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 4

April 29,2024

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

$$a^{p-1} \equiv 1 (\bmod p)$$

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

$$a^{p} \equiv a (\bmod p)$$

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

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, $1982 = 18 \cdot 110 + 2$.

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

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, $8^{16} \equiv 1 \bmod 17$. Using division algorithm, $1000 = 16 \cdot 62 + 8$

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

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

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

We now find powers of 8

$$8^2 = 13 \bmod 17$$

$$8^3 = 2 \bmod 17$$

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

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

$$= -16 \equiv 1 \bmod 17$$

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

Example 50

Find $524^{9999} \mod 23$

Solution

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

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

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

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

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

Solution (conti...)

We now get powers of 18

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

Thus, $18^{11} = 18^{10+1} = 18^{10} \times 18^1$

$$= 9 \times 18$$
$$= 9 \times (-5) \equiv 1 \mod 23$$

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

Example 51

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

Solution

By Fermat's Little theorem, we have
$2^{10} = 3^{10} = 5^{10} = 8^{10} = 9^{10} \equiv 1 \bmod 11.$
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 $2^{320} + 3^{23} + 5^{79} + 8^{1982} + 9^{2020} \bmod 11 = 3.$

Example 52

Solve the congruence

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

Solution

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

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

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

Thus, we solve $x^3 \equiv 4 \bmod 11$.

We try all values from $x = 0, 1, 2, \cdots 10$. We find $5^3 \equiv 4 \bmod\ 11$.

Thus $x \equiv 5 \bmod 11$.

Example 53

Find all integers x such that

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

Solution

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

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

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

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

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

Thus $x \equiv 8, 21 \bmod 29$.

1.12 Computing Modular Inverses Using Fermat's Little Theorem

Corollary 15

If p is prime and $p \nmid a$, then a^{p-2} is the multiplicative inverse of a. That is, $a^{-1} \equiv a^{p-2} \mathrm{mod}, p$

Notice that this congruence is true because if we multiply a^{p-2} by a we get the statement of Fermat's little theorem that the product is equal to 1 modulo p.

Example 54

Compute the inverse of 7 modulo 23.

Solution

The inverse of 7 modulo 23 is $7^{21} \bmod 23$ which we compute by fast powering algorithm as below.