WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 17

May 28, 2024

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

$7^{-1} \bmod 23 = 7^{23-2} \bmod 23 = 7^{21} \bmod 23$

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

Solution (conti...)

$$7^1 = 7$$

$$7^2 = 3$$

$$7^4 = 9$$

$$7^8 = 12$$

$$7^{16} = 6$$

$\rightarrow 7^1 = 7 \bmod 23$

$7^2 = 49 \bmod 23 = 3.$

$\rightarrow 7^4 \equiv 9 \bmod 23$

$\Rightarrow 7^8 = 81 = 12$

$\Rightarrow 7^{16} = 144 \bmod 23 = 6$

Thus $7^{21} = 7^{16+4+1}$

$= 7^{16} \times 7^4 \times 7^1$

$= 6 \times 9 \times 7$

$= 10$

$7^{21} = 7^{16+4+1}$

$= 7^{16} \times 7^4 \times 7^1 = 6 \times 9 \times 7$

$= 10$

$\therefore 7^{-1} \bmod 23 = 10$

Verify $7 \times 10 \bmod 23 = 1$

$7.x \equiv 1 \bmod 23$

$x = 10$

Example 55

Compute the inverse of $12^{-1} \bmod 19$

Solution

$12^{-1} \bmod 19 = 12^{17} \bmod 19$

Using fast powering algorithm we get

$$
\begin{aligned}
12^1 &= 12 \\
12^2 &= 11 \\
12^4 &= 7 \\
12^8 &= 11 \\
12^{16} &= 7
\end{aligned}
$$

Thus, $12^{17} = 12^{16+1}$

$$
\begin{aligned}
&= 12^{16} \times 12^1 \\
&= 7 \times 12 = 8
\end{aligned}
$$

Therefore, $12^{-1} \bmod 19 = 8 \bmod 19$

$12^{-1} \bmod 19 = 12^{19-2} \bmod 19$
$= 12^{17} \bmod 19$

$12^1 = 12$
$12^2 = 144 \bmod 19 = 11$
$12^4 = 121 \bmod 19 = 7$
$12^8 = 49 \bmod 19 = 11$
$12^{16} = 121 \bmod 19 = 7$

$12^{17} = 12^{16+1}$
$= 12^{16} \times 12^1$
$= 7 \times 12$
$= 84 \bmod 19$
$= 8$

$12^{-1} \bmod 19$
$= 8$

Verify

$12 \times 8 = 96$
$96 \bmod 19 = 1$

Example 56

Find $35^{-1} \bmod 29$

$35 \bmod 29 = 6 \bmod 29$

$35^{-1} \bmod 29 = 6^{-1} \bmod 29$

Solution

$35^{-1} \bmod\ 29 = 6^{-1} \bmod\ 29 = 6^{27} \bmod\ 29$

Using fast powering algorithm we get

$$6^1 = 6$$
$$6^2 = 7$$
$$6^4 = 20 = -9$$
$$6^8 = 23 = -6$$
$$6^{16} = 7$$
$$\therefore\ 6^{27} = 6^{16+8+2+1}$$
$$= 6^{16} \times 6^8 \times 6^2 \times 6^1$$
$$= 7 \times 23 \times 7 \times 6$$
$$= 5 \bmod 29$$

Thus, $35^{-1} \bmod 29 = 5 \bmod 29$

$6^{-1} \bmod 29 = 6^{27} \bmod 29$

$6^1 = 6 \bmod 29$

$6^2 = 36 \bmod 29 = 7$

$6^4 = 49 \bmod 29 = 20$

$6^8 = 400 \bmod 29 = 23$

$6^{16} = 529 \bmod 29 = 7$

$= -6 \times -6 = 36 \bmod 29 = 7$

$6^{27} = 6^{16+8+2+1}$

$= 6^{16} \times 6^8 \times 6^2 \times 6^1$

$= \underbrace{\underbrace{7 \times (-6)}_{16} \times \underbrace{7 \times 6}_{13}}_{5}$

-2

$29 \overline{)\,-42}$

-58

16

$\therefore 35^{-1} = 5$

verify

$35 \times 5 = 1 \bmod 29$

Example 57

Compute the inverse of 381 modulo 47

$381 \bmod 47 = 5 \bmod 47$

$381^{-1} \bmod 47 = 5^{-1} \bmod 47$

Solution

$381 \bmod 47 \equiv 5 \bmod 47$ and so $381^{-1} \bmod 47 \equiv 5^{-1} \bmod 47 = 5^{45} \bmod 47$.

$5^{-1} \bmod 47 = 5^{45} \bmod 47$

By fast powering algorithm we have,

$$5^1 = 5$$
$$5^2 = 25$$
$$5^4 = 14$$
$$5^8 = 8$$
$$5^{16} = 17$$
$$5^{32} = 7$$

$\Rightarrow 5^1 = 5$

$\Rightarrow 5^2 = 25 \bmod 47$

$\Rightarrow 5^4 = 625 \bmod 47 = 14$

$\Rightarrow 5^8 = 196 \bmod 47 = 8$

$\Rightarrow 5^{16} = 64 \bmod 47 = 17$

$\Rightarrow 5^{32} = 289 \bmod 47 = 7$

$\therefore 5^{45} = 5^{32+8+4+1}$

$= 5^{32} \times 5^{8} \times 5^{4} \times 5^{1}$

$= 7 \times 8 \times 14 \times 5$

$= 3920 \bmod 47 = 19$

$\therefore 381^{-1} \bmod 47$

$= 19 \bmod 47$

verify

$381 \times 19 \bmod 47$

$7239 \bmod 47$

$= \underline{1}$

Solution (conti...)

$$
\begin{aligned}
\therefore\ 5^{45} &= 5^{32+8+4+1} \\
&= 5^{32} \times 5^{8} \times 5^{4} \times 5^{1} \\
&= 7 \times 8 \times 14 \times 5 \\
&= 19 \bmod 47
\end{aligned}
$$

Example 58

17 18 17447

Compute the inverse of 7814 modulo 17449

Solution

7814 17447 7811

$7814^{-1} \bmod 17449$ is given by

$7814^{17447} \bmod 17449 = 1284.$

But $17447_{10} = \cancel{100010000101000_2}.$ = 1000100 00100 111

Let us use fast powering algorithm

17447 = 8 + 32 + 1024 + 16384

Solution (conti...)

7814^{1}	7814
7814^{2}	4545
7814^{4}	14858
7814^{8}	12865
7814^{16}	4460
7814^{32}	17189
7814^{64}	15253
7814^{128}	6492
7814^{256}	6729
7814^{512}	16735
7814^{1024}	3775
7814^{2048}	12241
7814^{4096}	7518
7814^{8192}	3013
7814^{16384}	4689

17449

~~3244~~

3499
1183
12651
9485
1139
16932
13333
2415
2594
16050
816
8587
3239
520

Solution (conti...)

$$
\begin{aligned}
\text{Thus, } 7814^{17447} &= \boxed{7814^{16384+1024+32+4+2+1}} \\
&= 7814^{16384} \times 7814^{1024} \times 7814^{32} \times 7814^{4} \times 7814^{2} \times 78 \\
&= (4689 \times 3775 \times 17189 \times 14858 \times 4545 \times 7814) \bmod \\
&= \underline{1284} \mod \underline{17449}
\end{aligned}
$$