WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 5

April 30,2024

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.

Solution (conti...)

$$
\begin{aligned}
7^1 &= 7\\
7^2 &= 3\\
7^4 &= 9\\
7^8 &= 12\\
7^{16} &= 6
\end{aligned}
$$

$$
\begin{aligned}
\text{Thus } 7^{21} &= 7^{16+4+1}\\
&= 7^{16} \times 7^4 \times 7^1\\
&= 6 \times 9 \times 7\\
&= 10
\end{aligned}
$$

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

Example 56

Compute the inverse of 7814 modulo 17449

Solution

The workings are left for the leaner to show. $7814^{-1} \bmod 17449 = 7814^{17447} \bmod 17449 = 1284$

1.13 Fermat's Primality Test

To test whether p is prime, pick a random integers a not divisible by p and see whether the congruence $a^{p-1} \equiv 1 \bmod p$ holds. If it fails hold for a value of a, then p is composite. The random a chosen should be in the interval $1 < a < p - 1$. It is unlikely that this congruence will hold for a random a if p is composite.

If any random a holds $a^{n-1} \equiv 1 \bmod n$ when n is composite then such a is known as a Fermat liar. In this case n is called Fermat pseudoprime to base a. In this case, if we pick another random a which gives $a^{n-1} \not\equiv 1 \bmod n$ then such a is known as a Fermat witness for the compositeness of n.

Example 57

Let us use Fermat's Primality Test to test whether 7 is prime.

Since $1 < a < n$, the values of a can be $2, 3, 4, 5, 6$. So let's check for the these numbers.

$2^6 \equiv 1 \bmod 7$

$3^6 \equiv 1 \bmod 7$

$4^6 \equiv 1 \bmod 7$

$5^6 \equiv 1 \bmod 7$

$6^6 \equiv 1 \bmod 7$

So 7 is prime since every a has confirmed.

Example 58

Determine whether 221 is prime.

Since $1 < a < 220$, let us take $a = 38$.

$38^{220} \equiv \mod 221$, since Fermat's statement has been upheld, either 221 is prime, or 38 is a Fermat liar, so we take another a, say 24 and check again

$24^{220} \equiv 81 \not\equiv \mod 221$

So 221 is composite and 38 was indeed a Fermat liar. Here, 24 is a Fermat witness for the compositeness of 221.

Exercise 5

a) Show that the following algorithm will compute the value of $a^k \pmod m$. It is a more efficient way to do successive squaring, well-suited for implementation on a computer.

   (1) Set $b = 1$
   (2) Loop while $k \geq 1$
   (3) If k is odd, set $b = a \cdot b \pmod m$
   (4) Set $a = a^2 \pmod m$.
   (5) Set $k = k/2$ (round down if k is odd)
   (6) End of Loop
   (7) Return the value of b (which equals $a^k \pmod m$)

b) Implement the above algorithm on a computer.

c) Use your program to compute the following quantities:

(i) $2^{1000} \pmod{2379}$ (ii) $567^{1234} \pmod{4321}$

(iii) $47^{258008} \pmod{1315171}$

Exercise (conti...)

d) Compute $7^{7386} \pmod{7387}$ by the method of successive squaring. Is 7387 prime?

e) Compute $7^{7392} \pmod{7393}$ by the method of successive squaring. Is 7393 prime?

f) Write a program to check if a number n is composite or probably prime as follows. Choose 10 random numbers $a_1, a_2, \cdots, a_{10}$ between 2 and $n-1$ and compute $a_i^{n-1} \bmod n$ for each a_i. If $a_i^{n-1} \not\equiv 1 \pmod n$ for any a_i, return the message "n is composite." If $a_i^{n-1} \equiv 1 \pmod n$ for all the a_i's, return the message "n is probably prime.

g) Compute $2^{9990} (\bmod\ 9991)$ by successive squaring and use your answer to say whether you believe that 9991 is prime.

1.14 Euler's Theorem

Theorem 16 (Euler's Theorem)

Let $m \in \mathbb{Z}$ and a be an integer relatively prime to m. Then

$$a^{\phi(m)} \equiv 1 \bmod m$$

Example 59

Find the last digit of 27^{71}.

Solution

To find the last digit of 27^{71} we reduce $27^{71} \bmod 10 = 7^{71} \bmod 10$.
Since $\gcd(7, 10) = 1$, we use Euler's Theorem.
Thus, $7^{\phi(10)} \equiv 1 \bmod 10$ or $7^4 \equiv 1 \bmod 10$.
By division algorithm, $71 = 4 \cdot 17 + 3$.
Thus $7^{71} \bmod 10 = 7^3 \bmod 10$

$$= 343 \bmod 10 = 3$$

Therefore, last digit of 27^{71} is 3.

Example 60

Find the last digit of 55^{29}.

Solution

To find the last digit of 55^{29} we reduce $55^{29} \bmod 10$

We want to use Euler's Theorem but $\gcd(55, 10) = 5$ so we can't use it directly. So first, $55 = 5 \cdot 11$.

Thus, $55^{29} = 5^{29} \times 11^{29}$.

Since $\gcd(11, 10) = 1$, we have that $11^{\phi(10)} = 1 \bmod 10$ or $11^4 = 1 \bmod 10$. Since $29 = 4 \cdot 7 + 1$, we have that $11^{29} = 11^1 = 11$.

Thus, $5^{29} \times 11^{29} = 5^{29} \times 11 \bmod 10$

Let us use the fast powering algorithm to solve $5^{29} \bmod 10$.

$5^1 = 5$	$5^4 = 5$	$5^{16} = 5$
$5^2 = 5$	$5^8 = 5$	$5^{29} = 5^{16} \times 5^8 \times 5^4 \times 5^1 = 5$

Thus $5^{29} \times 11 \bmod 10 = 5 \times 11 = 55 \bmod 10$.

The last digit is 5.

Example 61

Find the last two digits of 1111^{71023}.

Solution

To find the last two digits of 1111^{71023} we reduce $1111^{71023} \bmod 100 = 11^{71023} \bmod 100$. Since $\gcd(11, 100) = 1$, we use Euler's Theorem. Here, $\phi(100) = \frac{1}{2} \times \frac{4}{5} \times 100 = 40$

Thus, $11^{\phi(100)} \equiv 1 \bmod 100$ or $11^{40} \equiv 1 \bmod 100$.

By division algorithm, $71023 = 40 \cdot 1775 + 23$.

Thus $11^{71023} \bmod 100 = 11^{23} \bmod 100$.Thus;

$$11^1 = 11 \qquad 11^8 = 81 \qquad 11^{23} = 11^{16} \times 11^4 \times 11^2 \times 11^1$$

$$11^2 = 21 \qquad 11^{16} = 61 \qquad = 61 \times 41 \times 21 \times 11$$

$$11^4 = 41 \qquad = 577731$$

Therefore, last two digits of 1111^{71023} is 31.

Example 62

Find the last three digits of 17^{20001}.

Solution

To find the last three digits of 17^{20001} we reduce $17^{20001} \mod 1000$.

Since $\gcd(17, 1000) = 1$, we use Euler's Theorem. Here, $\phi(1000) = \frac{1}{2} \times \frac{4}{5} \times 1000 = 400$

Thus, $17^{\phi(1000)} \equiv 1 \mod 1000$ or $17^{400} \equiv 1 \mod 1000$.

By division algorithm, $20001 = 400 \cdot 50 + 1$.

Thus $17^{20001} \mod 1000 = 17^1 \mod 1000 = 17$.

Therefore, last three digits of 17^{20001} is 017.

Example 63

Find remainder of 524^{9999} on division by 23.

Solution

Fist reduce $524^{9999} \mod 23 = 18^{9999} \mod 23$.

Since $\gcd(18, 23) = 1$, we use Euler's Theorem. Here, $\phi(23) = 22$.

Thus, $18^{\phi(23)} \equiv 1 \mod 23$ or $18^{22} \equiv 1 \mod 23$.

By division algorithm, $9999 = 22 \cdot 454 + 11$.

Thus $18^{9999} \mod 23 = 18^{11} \mod 23$.

Using fast powering algorithm,

$$
\begin{array}{lll}
18^1 = 18 & 18^4 = 4 & 18^{11} = 18^8 \times 18^2 \times 18^1 \\
18^2 = 2 & 18^8 = 16 & \quad\;\; = 16 \times 2 \times 18 = 1
\end{array}
$$

The remainder is 1.

Example 64

Find remainder of 17^{2028} on division by 20.

Solution

We reduce $17^{2028} \bmod 20$. Since $\gcd(17, 20) = 1$, we use Euler's Theorem. Here, $\phi(20) = \frac{1}{2} \times \frac{4}{5} \times 20 = 8$.

Thus, $17^{\phi(20)} \equiv 1 \bmod 20$ or $17^8 \equiv 1 \bmod 20$.

By division algorithm, $2028 = 8 \cdot 253 + 4$.

Thus $17^{2028} \bmod 20 = 17^4 \bmod 20$.

Using fast powering algorithm,

$17^1 = 17$

$17^2 = 9$

$17^4 = 1$

The remainder is 1.

1.15 Using Euler's Theorem to Compute Inverses

Multiplying $a^{\phi(m)} \equiv 1 \mod m$ by a^{-1} we get $a^{-1}a^{\phi(m)} \equiv a^{-1} \mod m$ or $a^{\phi(m)-1} \equiv a^{-1} \mod m$. Thus $a^{-1} \mod m$ is given by $a^{\phi(m)-1} \mod m$.

Example 65

Use Euler's Theorem to compute $12^{-1} \mod 19$

Solution

Since, $\gcd(12, 19) = 1$,
we have $12^{-1} = 12^{\phi(19)-1} \mod 19 = 12^{17} \mod 19$. By fast powering algorithm we get

$$12^1 = 12 \qquad 12^4 = 7 \qquad 12^{16} = 7$$
$$12^2 = 11 \qquad 12^8 = 11 \qquad 12^{17} = 12^{16} \times 12^1 = 7 \times 12 \mod 19 = 8$$

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

Exercise 6

a) Write a program to compute $\phi(n)$, the value of Euler's phi function. You should compute $\phi(n)$ by using a factorization of n into primes, not by finding all the a's between 1 and n that are relatively prime to n.