WEB3CLUBS FOUNDATION LIMITED

Course Instructor: DR. Cyprian Omukhwaya Sakwa

PHONE: +254723584205 Email: cypriansakwa@gmail.com

Foundational Mathematics for Web3 Builders

Lecture 19
June 3, 2024

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 67

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

Solution

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

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

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

Find $17^{-1} \mod 28$. Use Euler's Theorem.

Solution

Since gcd(17, 28) = 1 we apply Euler's theorem.

$$17^{-1} \mod 28 = 17^{\phi(28)-1} \mod 28 = 17^{11} \mod 28$$

By fast powering algorithm we get;

$$17^{1} = 17$$

$$17^{2} = 9$$

$$17^{4} = 25$$

$$17^{8} = 9$$

$$17^{11} = 17^{8+2+1}$$

$$= 17^{8} \times 17^{2} \times 17^{1}$$

$$= 9 \times 9 \times 17 = 5 \mod 28$$

Thus $17^{-1} \mod 28 = 5 \mod 28$

2957 mon 75

Find $29^{-1} \mod 75$

Solution

$$29^{-1} \mod 75 = 29^{39} \mod 75$$

By fast powering algorithm we obtain

$$29^1 = 29$$

 $29^2 = 16$

$$29^2 = 16^\circ$$

$$29^{4} = 31$$

$$29^8 = 61$$

$$29^{16} = 46$$

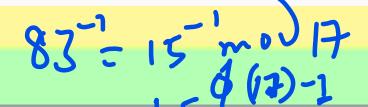
$$29^{32} = 16$$

$$29^{49} = 29^{32+4+2+1}$$

$$= 29^{32} \times 29^4 \times 29^2 \times 29^1$$

$$= 16 \times 31 \times 16 \times 29 = 44 \mod 75$$

Compute $83^{-1} \mod \underline{17}$.



Solution

First,
$$83^{-1} \mod 17 = 15^{-1} \mod 17$$

= $15^{15} \mod 17$

Now,

$$15^{1} = 15$$

 $15^{2} = 4$
 $15^{4} = 16$
 $15^{8} = 1$

$$15^{15} = 15^{8+4+2+1}$$

$$= 15^8 \times 15^4 \times 15^2 \times 15^1$$

$$= 1 \times 16 \times 4 \times 15 = 3$$

Example 71 353 = 115 $\frac{1}{19}$ Evaluate $353^{-1} \mod 119$. = 115 $\frac{1}{19}$

Solution

$$353^{-1} \mod 119 = 115^{-1} \mod 119 = 115^{95} \mod 119$$

By fast powering algorithm we get; $115^1 = 115$

$$115^1 = 115$$

$$115^2 = 16$$

$$115^4 = 18$$

$$>115^8 = 86$$

$$115^{16} = 18$$

$$115^{32} = 86$$

$$115^{64} = 18$$

$$115^{95} = 115^{64+16+8+4+2+1}$$

$$= 18 \times 18 \times 86 \times 18 \times 16 \times 115 = 89 \mod 119$$

$$= 18 \times 18 \times 86 \times 18 \times 16 \times 115 = 89 \mod 119$$

Find inverse of 1787 modulo 215.

Solution

1787⁻¹ mod 215 = 67⁻¹ mod 215 = 67¹⁶⁷ mod 215
Now,
$$167_{10} = 10100111_2$$

 $67^1 = 67$
 $67^2 = 189$
 $67^4 = 31$
 $67^8 = 101$
 $67^{16} = 96$
 $67^{32} = 186$
 $67^{64} = 196$
.
. $67^{128} = 146$
∴ $67^{167} = 146 \times 186 \times 31 \times 189 \times 67 = 138 \mod 215$

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.