

# **WEB3CLUBS FOUNDATION LIMITED**

---

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

## **Foundational Mathematics for Web3 Builders**

**Lecture 18**  
**May 30, 2024**

# Euler's Theorem

## 1.1 Euler phi function, $\phi(n)$

### Definition 1

Euler phi function, denoted  $\phi(n)$ , is the number of positive integers less than  $n$  which are relatively prime to  $n$ .

Some texts use the symbol  $\varphi(n)$ .

The following table gives  $\phi(n)$  for  $n = 1, 2, 3, \dots, 14$ .

$n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6

In general, if  $p$  is a prime number,  $\phi(p) = p - 1$ .

If  $n$  is a positive integer with prime factors  $p_1, p_2, p_3, \dots, p_k$  then

$$\phi(n) = \underbrace{(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})(1 - \frac{1}{p_3}) \cdots (1 - \frac{1}{p_k})}_{} n.$$

$$\begin{aligned}\phi(6) &= (1 - \frac{1}{2})(1 - \frac{1}{3}) \\ &= \frac{1}{2} \times \frac{2}{3} \times 6 \\ &= 2\end{aligned}$$

2/45

## Example 1

Denote the Euler phi function by  $\phi(n)$ . Find:

a)  $\phi(19)$

b)  $\phi(840)$

c)  $\phi(930)$

## Solution

Since 19 is prime,  $\phi(19) = 19 - 1 = 18$

$$\begin{aligned}\phi(840) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{6}{7} \times 840 \\ &= 192\end{aligned}$$

$$\begin{aligned}\phi(930) &= \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \times \frac{30}{31} \times 930 \\ &= 240\end{aligned}$$

## Example 2

Find:

a)  $\phi(4900)$

b)  $\phi(765)$ .

$$\begin{array}{r} 24900 \\ \hline 22450 \\ \hline 51225 \\ \hline 5245 \\ \hline 49 \end{array}$$

**Solution**  $\phi(4900) = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) 4900$

a) Since  $4900 = 2^2 \times 5^2 \times 7^2$ , we have

$$\phi(4900) = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) 4900$$

$$= \frac{1}{2} \times \frac{4}{5} \times \frac{6}{7} \times 4900 = 1680$$

b) Since  $765 = 3^2 \times 5 \times 17$ , we have

$$\phi(765) = \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{17}\right) \times 765$$

$$= \frac{2}{3} \times \frac{4}{5} \times \frac{16}{17} \times 765 = \underline{\underline{384}}$$

$$\begin{array}{r} 7 \\ \phi(765) \\ \hline 765 \\ \hline 513 \\ \hline 351 \\ \hline 17 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 5765 \\ \hline 3153 \\ \hline 351 \\ \hline 17 \\ \hline 1 \end{array}$$

3, 5, 17

## Revision Questions 1

Show that

a)  $\phi(15) = 8$

b)  $\phi(29) = 28$

c)  $\phi(20) = 8$

d)  $\phi(715) = 480$

e)  $\phi(716) = \underline{356}$

f)  $\phi(718) = 358$

## Solution

A handwritten diagram showing the prime factorization of 15. It starts with 15 at the top left, with a vertical line down to 5, and another vertical line from 5 to 1. To the right, there is a circle containing the number 1, with a diagonal line through it. Below the circle, there is a circle containing the number 3, with a diagonal line through it. To the right of the circle containing 3, there is a circle containing the number 5, with a diagonal line through it. Below the circle containing 5, there is a circle containing the number 1, with a diagonal line through it. To the right of the circle containing 1, there is a circle containing the number 5, with a diagonal line through it. Below the circle containing 5, there is a circle containing the number 1, with a diagonal line through it. This pattern repeats, with circles containing 1, 3, 5, and 1 appearing in sequence. To the right of the final circle containing 1, there is a multiplication sign followed by the number 15, indicating that the product of these factors is 15.

## Solution (contd...)

$$\begin{aligned}\phi(29) &= \\ \theta(p) &= p-1 \\ &= 29-1 \\ &= \underline{\underline{28}}\end{aligned}$$

## Solution (contd...)

$$\Theta(20)$$

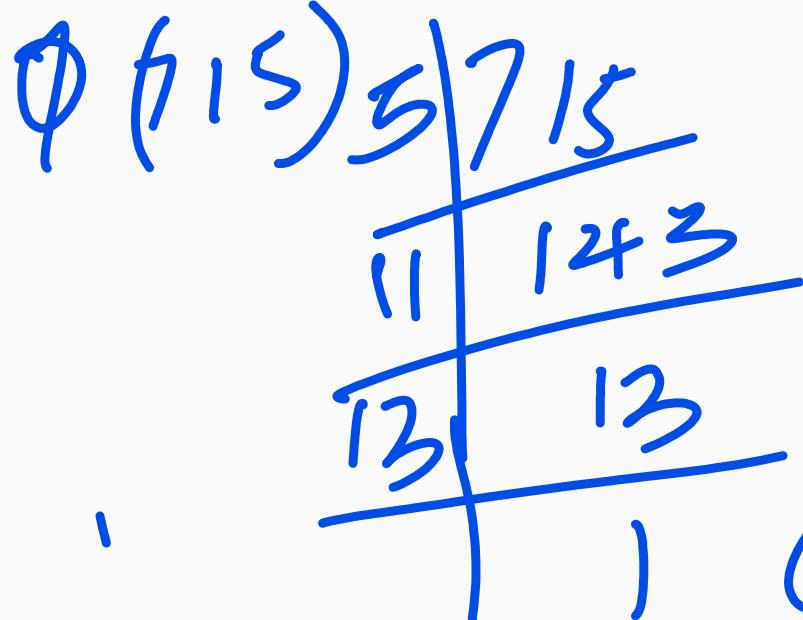
2	20
2	10
5	5

$$2 \times 2 \times 3 = \frac{1}{2^2} \times \frac{5}{(2, 5)}$$

$$\begin{aligned}\Theta(20) &= (1 - \frac{1}{2})(1 - \frac{1}{5})^{20} \\ &= \frac{1}{2} \times \frac{4}{3} \times 2^0 = 4\end{aligned}$$

$$\Theta(20) = (1 - \frac{1}{P_1})(1 - \frac{1}{P_2}) \dots (1 - \frac{1}{P_k})$$

## Solution (contd...)

$\phi(15) = 715$        $5 \times 11 \times 13$   

  
 $\phi(715) = \left(1 - \frac{1}{11}\right) \left(1 - \frac{1}{13}\right) \left(1 - \frac{1}{5}\right)$   
 $\frac{4}{5} \times \frac{10}{11} \times \frac{12}{13} \times 715 \left(1 - \frac{1}{13}\right) 715$   
 $= \cancel{20,280} \quad \underline{\underline{480}}$

## Solution (contd...)

$\phi(16)$

$$\begin{array}{r} 2 \\ \hline 2 | 716 \\ 2 | 358 \\ \hline 179 | 179 \\ \hline \end{array}$$

$$= 4 \times 89 = 356$$

~~356~~

$$\begin{aligned}\phi(716) &= (1 - \frac{1}{2})(1 - \frac{1}{179}) \cdot 716 \\ &= \frac{1}{2} \times \frac{715}{179} \times 716\end{aligned}$$

Solution (contd...)

$$718 = 2 \times 359$$

$$1 \times 358 = 358$$

$$\phi(718)$$

$$\begin{array}{r} 2 | 718 \\ 2 | 359 \\ \hline & 1 \end{array}$$

$$(P-1)(Q-1) = f(n)$$

$$\left(\frac{1-1}{2}\right) \times \left(\frac{1-1}{359}\right) \neq 1 \cdot 1$$

$$\frac{1 \times 358}{2 \times 359} \times 718^2 = \underline{\underline{358}}$$

## Solution (conti...)

## 1.2 Euler's Theorem

### Theorem 2 (Euler's Theorem)

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

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

### Example 3

Find the last digit of  $3^6$ .

### Solution

To find the last digit of  $3^6$  we reduce  $3^6 \pmod{10}$ .

Since  $\gcd(3, 10) = 1$ , we use Euler's Theorem.

Thus,  $3^{\phi(10)} \equiv 1 \pmod{10}$  or  $3^4 \equiv 1 \pmod{10}$ .

By division algorithm,  $6 = 4 \cdot 1 + 2$ .

Thus  $3^6 \pmod{10} = 3^2 \pmod{10} = 9 \pmod{10}$

Therefore, last digit of  $3^6$  is 9.

$$3^6 = 3^{4+2} = 3^4 \cdot 3^2 = 81 \pmod{10} = 9$$

$$\cancel{\text{gcd}(3, 10) = 1} \quad (\cancel{3}, \cancel{10}) \equiv 1$$

$$1 \quad \boxed{3^{\phi(10)} \equiv 1}$$

$$\begin{array}{r} 2 \\ 5 \end{array} \overline{) \begin{array}{r} 10 \\ 5 \end{array}}$$

$$\phi(10) = \frac{1}{2} \times 4 \times 5 = 4$$

$$\underline{3^4 = 1 \pmod{10}}$$

### Example 4

Find the last digit of  $27^{71}$ .

$$\begin{array}{l} \cancel{27^{71} \text{ mod } 10} = 7^{71} \text{ mod } 10 \\ \text{gcd}(7, 10) - 1 \end{array}$$

### Solution

To find the last digit of  $27^{71}$  we reduce  $27^{71} \text{ mod } 10 = 7^{71} \text{ mod } 10$ .

Since  $\text{gcd}(7, 10) = 1$ , we use Euler's Theorem.

Thus,  $7^{\phi(10)} \equiv 1 \text{ mod } 10$  or  $7^4 \equiv 1 \text{ mod } 10$ .

By division algorithm,  $71 = 4 \cdot 17 + 3$ .

Thus  $7^{71} \text{ mod } 10 = 7^3 \text{ mod } 10$

$$= 343 \text{ mod } 10 = 3$$

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

## Example 5

Find the last digit of  $(55^{29})_{10} = (5 \times i^{29})_{10}$

### 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 (cont...)

Note that we can still do these questions using fast powering algorithm. Take example 4 for instance, and compute  $27^{71} \bmod 10$  =  $7^{71} \bmod 10$  by fast powering algorithm.

$$\begin{aligned}7^1 &= 7 \checkmark \\7^2 &= 9 \checkmark \\7^4 &= 1 \checkmark\end{aligned}$$

Since  
 $7^4 = 1$

Since  $7^4 = 1$ , our work has been simplified. ✓

By division algorithm,  $71 = 4 \cdot 17 + 3$

Thus,

$$\begin{aligned}\because 71 &= 4 \cdot 17 + 3 \\7^{71} &= 7^3 \times 7^{2+1} \\&\equiv 9 \times 7\end{aligned}$$

$$\begin{aligned}7^{71} &= 7^3 \\&= 7^{2+1} \\&= 7 \times 9 = 3 \bmod 10\end{aligned}$$

**Example 6**

$$\underline{11}^{11^{71023}} \equiv \underline{11} \pmod{100}$$

$$\left. \begin{array}{l} 11^{\phi(100)} \equiv 1 \pmod{100} \\ 11^{40} \equiv 1 \pmod{100} \end{array} \right\}$$

Find the last two digits of  $\underline{1111}^{71023} \pmod{100}$

**Solution**  $\underline{1111} \pmod{100} \not\equiv 1 \pmod{4}$

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

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

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

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

$$11^1 = 11$$

$$11^8 = 81$$

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

$$11^2 = 21$$

$$11^{16} = 61$$

$$= 61 \times 41 \times 21 \times 11$$

$$11^4 = 41$$

$$= 577731$$

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

## Example 7

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

### Solution

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

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

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

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

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

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

## Revision Questions 2

### 1. Find the last digit of:

a)  $9^9$

b)  $3^{20}$

c)  $4^{10}$

d)  $15^{33}$

2. Find the last two digits of:

a)  $9^9$

b) 3<sup>230</sup>

c)  $4^{53}$

d)  $^{115}\text{S}$

$$q^1 = q^1 \bmod 10$$

$$\left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{4}\right) \dots \left(1 - \frac{1}{10}\right) = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \dots \cdot \frac{9}{10} = \frac{1}{10}$$

$$\cancel{2} \cancel{10} \cancel{5} \cancel{1} \cancel{1/2} \quad \dot{\bar{q}}^{\phi^{10}} = q \quad \phi^{10} = 4$$

$$q^+ = q^- = q$$

$$9 = 4(2) + 1$$

## Solution (contd...)

$$\begin{aligned}3^{q_0} & \quad | \bmod m \\3^{q_1} &= | \bmod 10 \\3^4 &= | \bmod 10 \\3^4 &= | \bmod 10 \\3^{20} &= S(4) + 0\end{aligned}$$

$(3^4)^5 \times 3^0$   
 $|^5 \times }^1 = 1$

## Solution (contd...)

$$\cancel{4} \overset{10}{\textcircled{1}} \bmod \underline{10}$$

$$4^1 = 4$$

$$4^0 = 6$$

$$4^{\cancel{0}} = 6$$

$$4^{\cancel{0}} = 6$$

$$4^{\cancel{0}} = 6$$

$$\begin{aligned} 4^{10} &= 4^{(8+2)} \\ &= 4^8 \times 4^2 \\ &= 6 \times 6 \\ &\equiv 36 \bmod 10 \\ &= 6 \end{aligned}$$

## Solution (contd...)

$$15^{33} \bmod 10 \\ (15, 10)$$

$$5^{33} \bmod 10$$

$$5^1 = 5$$

$$5^2 = 25$$

$$5^4 = 625$$

$$5^8 = 390625$$

$$5^{16} = 5 \\ 5^{32} = 25$$

$$5^{33} \bmod 10 \equiv 5^{33} \bmod 10$$

$$5^{33} = 5^{2+1}$$

$$= 5^2 \\ = 25$$

$$= 25 \times 5$$

$$= 25 \bmod 10$$

$$= 5$$

## Solution (contd...)

$$9^4 \pmod{100}$$

$$9^1 = 9$$

$$9^2 = 81$$

$$9^4 = 61$$

$$9^8 = 21$$

$$9^4 = 9^{8+1} = 9^8 \cdot 9^1$$

$$= 21 \times 9 = 189$$

$$189 \pmod{100} \equiv 89$$

## Solution (contd...)

$$3^{230} \pmod{100}$$

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

$$\phi(100) = 40$$

$$3^{40} \equiv 1 \pmod{100}$$

$$3^{230} = 3^{40 \times 5 + 30} = 3^{40} \times 3^{30}$$

$$(3^{40})^5 \times 3^{30} = 1^5 \times 3^{30}$$

$$3^{230} \pmod{100} \quad \boxed{3}$$

$$3^1 = 3$$

$$3^2 = 9$$

~~$$3^3 = 27$$~~

$$3^4 = 81$$

$$3^8 = 61$$

$$3^{16} = 1$$

$$3^{20} = 3^{16+8+4+2} = 3^{16} \times 3^8 \times 3^4 \times 3^2 = 1 \times 61 \times 1 \times 9 = 81$$

## Solution (contd...)

$$3^{16} \times 3^8 \times 3^4 \times 3^2$$

$$\begin{aligned}&= 21 \times 61 \times 81 \times 9 \\&= 933849 \text{ mod } 10\end{aligned}$$

4 4 9

## Solution (contd...)

$$4^{53}$$

$$4^{53} \bmod 100$$

$$4^1 = 4$$

$$4^2 = 16$$

$$4^4 = 56$$

$$4^8 = 36$$

$$4^{16} = 96$$

$$4^{32} = 16$$

$$4^{53} = 4^{32+16+4+1}$$

$$= 16 \times 96 \times 56 \times 4$$

$$= 344064 \bmod 100$$

## Solution (contd...)

15<sup>2</sup> ~~Aast~~  
15<sup>2</sup> and 100

15<sup>2</sup> = 15<sup>2</sup>  
15<sup>2</sup> = 25  
15<sup>2</sup> = 25

## Solution (contd...)

$$15^4 = 25$$

$$15^{16} = 25$$

$$15^{32} = 25$$

$$15^{64} = 25$$

$$72 = 64 + 8$$

## Solution (contd...)

$$\cancel{15^{64} \times 15^8}$$

$$\cancel{25} \times \cancel{25} \text{ net } 100$$

$$625 \text{ net } 100$$

$$25$$