Foundation of Cryptography

Session 16

Date: 09 March 2021

Dr. V. K. Pachghare

Number Theory

- **Euler Totient Function**
- **Extended Euclidean Algorithm**
- **Chinese Remainder Theorem**

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Solution:

$4^{1023} \bmod 100$

As 4 and 100 have common factors, we will take any one factor of 100 such as 5, 10, 20, 25 or 50 as modulus.

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Solution:

$4^{1023} \bmod 100$

As 4 and 100 have common factors, we will take any one factor of 100 such as 5, 10, 20, 25 or 50 as modulus.

Suppose the common factor selected is 25, then

$4^{1023} \bmod 25$

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Solution:

$4^{1023} \bmod 100$

As 4 and 100 have common factors, we will take any one factor of 100 such as 5, 10, 20, 25 or 50 as modulus.

Suppose the common factor selected is 25, then

$4^{1023} \bmod 25$

$4^{1023 \bmod \varnothing(25)} \bmod 25$ $(\varnothing(25) = 20)$

Find the last two digits of 4^{1023}.

Note that 4 and 100 do have a common factor!

Solution:

$4^{1023} \bmod 100$

As 4 and 100 have common factors, we will take any one factor of 100 such as 5, 10, 20, 25 or 50 as modulus.

Suppose the common factor selected is 25, then

$4^{1023} \bmod 25$

$4^{1023 \bmod \varnothing(25)} \bmod 25$ $(\varnothing(25) = 20)$

$= 4^3 \bmod 25$ Since $1023 \bmod 20 = 3$

$= 4^3$ mod 25

=64 mod 25

14, 39, 64

out of these only 64 is divisible by 4.

The number which is power of 4 is selected and that number is the last two digits

So last two digits are 64

Factors of 100 are 5, 10, 20, 25 and 50

4^{1023} mod 5	4^{1023} mod 10	4^{1023} mod 20	4^{1023} mod 50
$4^{1023 \bmod \phi(5)} \bmod 5$	$4^{1023 \bmod \phi(10)} \bmod 10$	$4^{1023 \bmod \phi(20)} \bmod 20$	$4^{1023 \bmod \phi(50)} \bmod 50$
$4^{1023 \bmod 4} \bmod 5$	$4^{1023 \bmod 4} \bmod 10$	$4^{1023 \bmod 8} \bmod 20$	$4^{1023 \bmod 20} \bmod 50$
4^3 mod 5	4^3 mod 10	4^7 mod 20	4^3 mod 50
64 mod 5 = 4 mod 5	64 mod 10 = 4 mod 10	$4^7 = 4^3 * 4^3 * 4$ 4*4*4 mod 20 = 64 mod 20 =4 mod 20	64 mod 50 = 14 mod 50
4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59, **64,** 69, 74, 79, 84, 89, 94, 99	4, 14, 24, 34, 44, 54, **64,** 74, 84, 94	4, 24, 44, **64**, 84	14, **64**
The number which is power of 4 is the last two digits			

What are the last two digits of $\underbrace{3^{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}}_{2012\ times}$?

Solution:

We know that ø(100) = 40;

So, we need to compute $\underbrace{3^{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}}_{2011\ times}$

and raise 3 to that power.

ø(40) = 16; ø(16) = 8; ø(8) = 4; ø(4) = 2

In particular, $3^k = 3 \bmod 4$ for any value of k.

Working backwards

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^3$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3}}$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3}}}$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}}$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3}}}}$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}}}$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}}$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3}}}}}$$

$$3^{3^{3^{3^{3^{\left(3^{3 \bmod \varphi(2)}\right) \bmod 2}}}}}$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \varphi(4)}\right) \bmod 4}}}}$$

$$3^{3^{3^{\left(3^{3 \bmod \varphi(8)}\right) \bmod 8}}}$$

$$3^{3^{\left(3^{3 \bmod \varphi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \varphi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \varphi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}}}$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}}$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}}} \qquad \left(3^{3 \bmod \phi(4)}\right) \bmod 4 = 3^{3 \bmod 2} \bmod 4 = 3$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}}$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}}} \qquad \left(3^{3 \bmod \phi(4)}\right) \bmod 4 = 3^{3 \bmod 2} \bmod 4 = 3$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}} \qquad \left(3^{3 \bmod \phi(8)}\right) \bmod 8 = 3^{3 \bmod 4} \bmod 8 = 3$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}}$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}}} \qquad \left(3^{3 \bmod \phi(4)}\right) \bmod 4 = 3^{3 \bmod 2} \bmod 4 = 3$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}}} \qquad \left(3^{3 \bmod \phi(8)}\right) \bmod 8 = 3^{3 \bmod 4} \bmod 8 = 3$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}} \qquad \left(3^{3 \bmod \phi(16)}\right) \bmod 16 = 3^{3 \bmod 8} \bmod 16 = 11$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40}$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}} \qquad \left(3^{3 \bmod \phi(4)}\right) \bmod 4 = 3^{3 \bmod 2} \bmod 4 = 3$$

$$3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}} \qquad \left(3^{3 \bmod \phi(8)}\right) \bmod 8 = 3^{3 \bmod 4} \bmod 8 = 3$$

$$3^{3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16}} \qquad \left(3^{3 \bmod \phi(16)}\right) \bmod 16 = 3^{3 \bmod 8} \bmod 16 = 11$$

$$\left[3^4 \bmod 40 = 1\right] => \left[3^{11} = \left(3^4\right)^2 3^3 \bmod 40 = 1\right] => \left[3^3 \bmod 40 = 27\right]$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40} \qquad \left(3^{3 \bmod \phi(40)}\right) \bmod 40 = 3^{3 \bmod 16} \bmod 40 = 3^{11} \bmod 40 = 27$$

$$3^{3 \bmod \phi(100)} \bmod 100$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$3^{3^{3^{3^{\left(3^{3 \bmod \phi(2)}\right) \bmod 2}}}} \qquad \left(3^{3 \bmod \phi(2)}\right) \bmod 2 = 3^{3 \bmod 1} \bmod 2 = 1$$

$$3^{3^{3^{\left(3^{3 \bmod \phi(4)}\right) \bmod 4}}} \qquad \left(3^{3 \bmod \phi(4)}\right) \bmod 4 = 3^{3 \bmod 2} \bmod 4 = 3$$

$$3^{3^{\left(3^{3 \bmod \phi(8)}\right) \bmod 8}} \qquad \left(3^{3 \bmod \phi(8)}\right) \bmod 8 = 3^{3 \bmod 4} \bmod 8 = 3$$

$$3^{\left(3^{3 \bmod \phi(16)}\right) \bmod 16} \qquad \left(3^{3 \bmod \phi(16)}\right) \bmod 16 = 3^{3 \bmod 8} \bmod 16 = 11$$

$$\left[3^4 \bmod 40 = 1\right] \Rightarrow \left[3^{11} = \left(3^4\right)^2 3^3 \bmod 40 = 1\right] \Rightarrow \left[3^3 \bmod 40 = 27\right]$$

$$3^{\left(3^{3 \bmod \phi(40)}\right) \bmod 40} \qquad \left(3^{3 \bmod \phi(40)}\right) \bmod 40 = 3^{3 \bmod 16} \bmod 40 = 3^{11} \bmod 40 = 27$$

$$3^{3 \bmod \phi(100)} \bmod 100 = 3^{27 \bmod 40} \bmod 100$$

$$= 3^{27} \bmod 100 =$$

$$3^{3^{3^{3^{3^{3^{3}}}}}}$$

$$27^{11} \bmod \phi(100)$$

$$= 27^{11} \bmod 40 \qquad as\ \phi(100) = 40$$

$$= 3x3^{26} \bmod 100 = 3x(3^{13})^2 \bmod 100$$

$$= 3x(3x(3^3)^2)^2)^2 \bmod 100$$

$$= 87 \bmod 100$$