Foundation of Cryptography

Session 15

Date: 08 March 2021

Dr. V. K. Pachghare

Number Theory

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

Euler Totient Function: ø(n)

- In cryptography, Euler's totient function plays an important role.
- The totient of a positive integer n is the total number of the positive integer numbers which are less than n and are relatively prime to n.
- It is shown as **ø**(n), where **ø**(n) is the number of positive integers less than n and relatively prime to n.

- when doing arithmetic modulo n, complete set of residues (positive integer only) is: 1..n-1
- Reduced set of residues is those numbers (residues) which are relatively prime to n i.e. GCD is 1.

Eg. for $n = 8$,

Eg. for $n = 8$,

complete set of residues is $\{0, 1, 2, 3, 4, 5, 6, 7\}$

Eg. for $n = 8$,

complete set of residues is $\{0, 1, 2, 3, 4, 5, 6, 7\}$

reduced set of residues is $\{1, 3, 5, 7\}$

Eg. for $n = 8$,

complete set of residues is $\{0, 1, 2, 3, 4, 5, 6, 7\}$

reduced set of residues is $\{1, 3, 5, 7\}$

Therefore $ø(8) = 4$

Suppose $n = 7$.

Complete set of residues is $\{0, 1, 2, 3, 4, 5, 6\}$

Suppose $n = 7$.

Complete set of residues is $\{0, 1, 2, 3, 4, 5, 6\}$

As 7 is a prime number, all the positive integers from 1 to 6 are relatively prime to 7.

Therefore, reduced set of residues is $\{1, 2, 3, 4, 5, 6\}$

Suppose n = 7.

Complete set of residues is {0, 1, 2, 3, 4, 5, 6}

As 7 is a prime number, all the positive integers from 1 to 6 are relatively prime to 7.

Therefore, reduced set of residues is {1, 2, 3, 4, 5, 6}

Thus, ø(7) = 6

Suppose $n = 7$.

Complete set of residues is $\{0, 1, 2, 3, 4, 5, 6\}$

As 7 is a prime number, all the positive integers from 1 to 6 are relatively prime to 7.

Therefore, reduced set of residues is $\{1, 2, 3, 4, 5, 6\}$

Thus, $ø(7) = 6$

For any prime number n, $ø(n) = n – 1$.

ø(n) = how many numbers there are between 1 and n-1 that are relatively prime to n.

ø(4) = 2 (1, 3 are relatively prime to 4)

ø(5) = 4 (1, 2, 3, 4 are relatively prime to 5)

ø(6) = 2 (1, 5 are relatively prime to 6)

ø(7) = 6 (1, 2, 3, 4, 5, 6 are relatively prime to 7)

- As you can see from the above examples that if n is a prime number $ø(n) = n – 1$.
- This helps to calculate the totient function when the factors of n are two different prime numbers.
- For example, suppose n has two factors A and B, **where A and B are primes**, then

$$ø(n) = ø(A * B)$$

$$= ø(A) * ø(B)$$

$$= (A – 1)*(B – 1)$$

Find the totient function of *n* = 91

$ø(91) = ø(13 * 7)$

Find the totient function of *n* = 91

$\text{ø}(91) = \text{ø}(13 * 7)$

$= \text{ø}(13) * \text{ø}(7)$

Find the totient function of *n* = 91

ø(91) = ø(13 * 7)

= ø(13) * ø(7)

= (13 – 1)*(7 – 1)

Find the totient function of *n* = 91

$\text{ø}(91) = \text{ø}(13 * 7)$

$= \text{ø}(13) * \text{ø}(7)$

$= (13 - 1)*(7 - 1)$

$= 12 * 6$

Find the totient function of *n* = 91

$$
\begin{aligned}
ø(91) &= ø(13 * 7)\\
&= ø(13) * ø(7)\\
&= (13 - 1)*(7 - 1)\\
&= 12 * 6\\
ø(91) &= 72
\end{aligned}
$$

Find the totient function of n = 25

$ø(25) = ø(5 * 5)$

Find the totient function of n = 25

$$ø(25) = ø(5 * 5)$$

$$= ø(5) * ø(5)$$

Find the totient function of n = 25

$$
\begin{aligned}
ø(25) &= ø(5 * 5) \\
&= ø(5) * ø(5) \\
&= (5 - 1) * (5 - 1)
\end{aligned}
$$

Find the totient function of n = 25

$$ø(25) = ø(5 * 5)$$

$$= ø(5) * ø(5)$$

$$= (5 - 1) * (5 - 1)$$

$$= 4 * 4$$

Find the totient function of n = 25

$ø(25) \quad = ø(5 * 5)$

$= \; ø(5)* ø(5)$

$= (5 – 1)*(5 – 1)$

$= 4 * 4$

$ø(25) \quad = 16$

Find the totient function of n = 25

$$
\begin{aligned}
ø(25) &= ø(5 * 5) \\
&= ø(5) * ø(5) \\
&= (5 - 1) * (5 - 1) \\
&= 4 * 4
\end{aligned}
$$

$ø(25) = 16$ **but this is wrong**

$ø(n) = ø(A^p) = n(1 – 1/A)$

$n = 25$ and $25 = 5 * 5$

$ø(25) = ø(5 * 5)$

$\phi(n) = \phi(A^p) = n(1 - 1/A)$

$n = 25$ and $25 = 5 * 5$

$\phi(25) = \phi(5 * 5)$

$= \phi(5^2)$ here $A = 5$ and $p = 2$

$ø(n) = ø(A^p) = n(1 – 1/A)$

$n = 25$ and $25 = 5 * 5$

$ø(25) = ø(5 * 5)$

$= ø(5^2)$ here $A = 5$ and $p = 2$

$$= 25\left(1 - \frac{1}{5}\right)$$

$ø(n) = ø(A^p) = n(1 – 1/A)$

$n = 25$ and $25 = 5 * 5$

$ø(25) = ø(5 * 5)$

$= ø(5^2)$ here $A = 5$ and $p = 2$

$$= 25\left(1 - \frac{1}{5}\right)$$

$$= 25\left(\frac{4}{5}\right)$$

$\phi(n) = \phi(A^p) = n(1 - 1/A)$

$n = 25$ and $25 = 5 * 5$

$\phi(25) = \phi(5 * 5)$

$= \phi(5^2)$ here $A = 5$ and $p = 2$

$$= 25\left(1 - \frac{1}{5}\right)$$

$$= 25\left(\frac{4}{5}\right)$$

$$= 20$$

Find the totient value of 100

$$\phi(100) = \phi(25 * 4)$$

$$\phi(100) = \phi(25 * 4)$$
$$= \phi(5^2 * 2^2)$$

$$\begin{aligned}\phi(100) &= \phi(25*4) \\ &= \phi(5^2 * 2^2) \\ &= \phi(5^2) * \phi(2^2)\end{aligned}$$

$$\phi(100) = \phi(25*4)$$
$$= \phi(5^2 * 2^2)$$
$$= \phi(5^2) * \phi(2^2)$$
$$= 5^2\left(1 - \frac{1}{5}\right) * 2^2\left(1 - \frac{1}{2}\right)$$

$$\phi(100) = \phi(25 * 4)$$
$$= \phi(5^2 * 2^2)$$
$$= \phi(5^2) * \phi(2^2)$$
$$= 5^2\left(1 - \frac{1}{5}\right) * 2^2\left(1 - \frac{1}{2}\right)$$
$$= 5^2 * 2^2\left(1 - \frac{1}{5}\right) * \left(1 - \frac{1}{2}\right)$$

$$\phi(100) = \phi(25*4)$$
$$= \phi(5^2 * 2^2)$$
$$= \phi(5^2) * \phi(2^2)$$
$$= 5^2\left(1-\frac{1}{5}\right) * 2^2\left(1-\frac{1}{2}\right)$$
$$= 5^2 * 2^2\left(1-\frac{1}{5}\right) * \left(1-\frac{1}{2}\right)$$
$$= 25*4\left(\frac{4}{5}\right)\left(\frac{1}{2}\right)$$

$$\begin{aligned}
\phi(100) &= \phi(25*4) \\
&= \phi(5^2*2^2) \\
&= \phi(5^2)*\phi(2^2) \\
&= 5^2\left(1-\frac{1}{5}\right)*2^2\left(1-\frac{1}{2}\right) \\
&= 5^2*2^2\left(1-\frac{1}{5}\right)*\left(1-\frac{1}{2}\right) \\
&= 25*4\left(\frac{4}{5}\right)\left(\frac{1}{2}\right) \\
&= 100\left(\frac{4}{10}\right)
\end{aligned}$$

$$
\begin{aligned}
\phi(100) &= \phi(25*4) \\
&= \phi(5^2*2^2) \\
&= \phi(5^2)*\phi(2^2) \\
&= 5^2\left(1-\frac{1}{5}\right)*2^2\left(1-\frac{1}{2}\right) \\
&= 5^2*2^2\left(1-\frac{1}{5}\right)*\left(1-\frac{1}{2}\right) \\
&= 25*4\left(\frac{4}{5}\right)\left(\frac{1}{2}\right) \\
&= 100\left(\frac{4}{10}\right) \\
&= 10*4
\end{aligned}
$$

$$\begin{aligned}
\phi(100) &= \phi(25*4) \\
&= \phi(5^2*2^2) \\
&= \phi(5^2)*\phi(2^2) \\
&= 5^2\left(1-\frac{1}{5}\right)*2^2\left(1-\frac{1}{2}\right) \\
&= 5^2*2^2\left(1-\frac{1}{5}\right)*\left(1-\frac{1}{2}\right) \\
&= 25*4\left(\frac{4}{5}\right)\left(\frac{1}{2}\right) \\
&= 100\left(\frac{4}{10}\right) \\
&= 10*4 \\
&= 40
\end{aligned}$$

The generalise formula to calculate $\Phi(n)$ of a number n is:

$$\Phi(n) = A_1^{m_1} * A_2^{m_2} * A_3^{m_n} * \ldots * A_n^{m_n}$$

$$= n * \left(1 - \frac{1}{A_1}\right) * \left(1 - \frac{1}{A_2}\right) * \left(1 - \frac{1}{A_3}\right) * \ldots \left(1 - \frac{1}{A_n}\right)$$

$$\Phi(n^m) = n^{m-1}\Phi(n) \text{ [identity relating to } \Phi(n^m) \text{ to } \Phi(n)\text{]}$$

400 = 100 x 4

= 10 x 10 x 2 x 2

= 2 x 5 x 2 x 5 x 2 x 2

= 2^3 x 5^2

$$\phi(400) = 400\left[\left(1-\frac{1}{5}\right)\left(1-\frac{1}{2}\right)\right]$$

$$= 400\left[\left(\frac{4}{5}\right)\left(\frac{1}{2}\right)\right]$$

$$= 400\left[\left(\frac{4}{10}\right)\right]$$

$$= 160$$

Find Totient value of 9

$$9 = 3^2$$

Find Totient value of 9

$$9 = 3^2$$

$$\phi(9) = 9 * \left(1 - \frac{1}{3}\right)$$

Find Totient value of 9

$$9 = 3^2$$

$$\phi(9) = 9 * \left(1 - \frac{1}{3}\right)$$

$$= 9 * \left(\frac{2}{3}\right)$$

$$= 6$$

Find Totient value of 64

$$64 = 8^2 = 2^6$$

Find Totient value of 64

$$64 = 8^2 = 2^6$$

$$\phi(64) = \phi\left(2^6\right)$$

Find Totient value of 64

$$64 = 8^2 = 2^6$$

$$\phi(64) = \phi\left(2^6\right)$$

$$= 64 * \left(1 - \frac{1}{2}\right)$$

Find Totient value of 64

$$64 = 8^2 = 2^6$$

$$\phi(64) = \phi\left(2^6\right)$$

$$= 64 * \left(1 - \frac{1}{2}\right)$$

$$= 32 * (1)$$

Find Totient value of 64

$$64 = 8^2 = 2^6$$

$$\phi(64) = \phi\left(2^6\right)$$

$$= 64 * \left(1 - \frac{1}{2}\right)$$

$$= 32 * (1)$$

$$= 32$$

$$a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$$

Find the unit place digit of 7^{2013}

$7^{2013} \bmod 10 = 7^{2013 \bmod ø(10)} \bmod 10$

Find the unit place digit of 7^{2013}

$7^{2013} \bmod 10 = 7^{2013 \bmod ø(10)} \bmod 10$ {ø(10)= 4}

Therefore 2013 mod 4 = 1

Find the unit place digit of 7^{2013}

$7^{2013} \bmod 10 = 7^{2013 \bmod ø(10)} \bmod 10$ {ø(10)= 4}

Therefore 2013 mod 4 = 1

$7^{2013 \bmod ø(10)} \bmod 10 = 7^{1} \bmod 10 = 7$

Ex 2:

Find the last two digits of 9^{1573}.

$9^{1573} \bmod 100$

Apply $\quad a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100$

Apply $\quad a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100 = 9^{1573 \bmod \varnothing(100)} \bmod 100$

$9^{1573} \bmod 100$

Apply $a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100 = 9^{1573 \bmod \varnothing(100)} \bmod 100$

Since $\varnothing(100) = 40$; $1573 \bmod \varnothing(100) = 13$

9^{1573} mod 100

Apply $a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

9^{1573} mod 100

$= 9^{1573 \bmod \varnothing(100)} \bmod 100$

Since $\varnothing(100) = 40$; **1573 mod** $\varnothing(100) = 13$

$= 9^{13} \bmod 100$ ($9^{3} \bmod 100 = 29$)

$9^{1573} \bmod 100$

Apply $a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100$

$= 9^{1573 \bmod \varnothing(100)} \bmod 100$

Since $\varnothing(100) = 40$; $1573 \bmod \varnothing(100) = 13$

$= 9^{13} \bmod 100$ $(9^3 \bmod 100 = 29)$

$= (9^3)^4 \times 9 \bmod 100 = 29^4 \times 9 \bmod 100$

9^{1573} mod 100

Apply $a^{b} \bmod p = a^{b \bmod \varnothing(p)} \bmod p$

$9^{1573} \bmod 100$

$= 9^{1573 \bmod \varnothing(100)} \bmod 100$

Since $\varnothing(100) = 40$; 1573 mod $\varnothing(100) = 13$

$= 9^{13} \bmod 100$ ($9^3 \bmod 100 = 29$)

$9^{13} \bmod 100 = (9^3)^4 \times 9 \bmod 100 = 29^4 \times 9 \bmod 100$

$= (41)^2 \times 9 \bmod 100$ Since $(29^2) \bmod 100 = 41$

$= 29$

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!

$4^{1023} \bmod 100$

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

Note that 4 and 100 do have a common factor!

4^{1023} mod 100

As 4 and 100 have common factors, we will take 25 as modulus.

4^{1023} mod 25

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

Note that 4 and 100 do have a common factor!

4^{1023} mod 100

As 4 and 100 have common factors, we will take 25 as modulus.

4^{1023} mod 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.

$4^{1023} \bmod 25$

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

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

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 25 as modulus.

$4^{1023} \bmod 100$

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

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

=64 mod 25

14, 39, 64, 89 out of these only 64 is divisible by 4 and 100.

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**
$4^{1023 \bmod \varnothing(5)} \bmod 5$	$4^{1023 \bmod \varnothing(10)} \bmod 10$	$4^{1023 \bmod \varnothing(20)} \bmod 20$	$4^{1023 \bmod \varnothing(50)} \bmod 50$
$4^{1023 \bmod 4} \bmod 5$	$4^{1023 \bmod 4} \bmod 10$	$4^{1023 \bmod 8} \bmod 20$	$4^{1023 \bmod 20} \bmod 50$
$4^3 \bmod 5$	$4^3 \bmod 10$	$4^7 \bmod 20$	$4^3 \bmod 50$
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 $\underbrace{3^{3^{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}}}}}_{2012\ time}$?

Solution:

We know that ø(100) = 40;

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

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

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

$$3^3$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$= 87 \bmod 100$$