Ex. (i) $22 = 2 	imes 11$ 
\[ \phi(22) = 22 \times \left(1 - \frac{1}{2}\right) \times \left(1 - \frac{1}{11}\right) = 22 \times \frac{1}{2} \times \frac{10}{11} = 10 \]

(iii) $120 = 2^3 \times 3 \times 5$
\[ \phi(120) = 120 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} = 32 \]

(iii) $1024 = 2^{10}$
\[ \phi(1024) = 2^{10} \times \frac{1}{2} = 2^9 = 512 \]

---

Chap 7 Primitive Roots

Ex. 1. $\phi(16) = 4$, $\{1, 3, 7, 9\}$ is a reducible syst. mod 10.

We also note that
\[ \{3, 3^2, 3^3, 3^4\} \] are reducible syst. mod 10.
\[ \{7, 7^2, 7^3, 7^4\} \]

Def. If $h$ is the smallest positive integer such that $a^h \equiv 1 \pmod{m}$.

We say that $a$ belongs to exponent $h$ mod $m$.

Thm. 7.1 In order for that $a^b \equiv 1 \pmod{m}$ for some $b$, it is necessary and sufficient that $\gcd(a, m) = 1$. 
Thm 7.2. If \( a \) belongs to exponent \( h \) mod \( m \), and \( a^r \equiv 1 \pmod{m} \), then \( h \mid r \).

Def. If \( g \) is an integer that belongs to exponent \( \varphi(m) \mod m \), then \( g \) is called a primitive root mod \( m \).

Thm 7.3. If \( g \) is a primitive root modulo \( m \), then \( \{ g, g^2, \ldots, g^{\varphi(m)} \} \) form a reduced rep. by \( m \mod m \).

Ex. modulus 7
1. \( 2, 2^2, 2^3 \equiv 1 \pmod{7} \) no
2. \( 3 \), yes
3. \( 4 \), yes
4. \( 4^3 \equiv 64 \equiv 1 \pmod{7} \) no
5. \( 5 \), yes
6. \( 6^2 \equiv 1 \pmod{7} \) no

Q. Does primitive root exist for every modulus?

Unfortunately, no!
Ex. There is no primitive root mod 8.

because
\[ 1 \equiv 1 \pmod{8} \]
\[ 3^2 \equiv 1 \pmod{8} \]
\[ 5^2 \equiv 1 \pmod{8} \]
\[ 7^2 \equiv 1 \pmod{8} \]

Thm 7.4 If \( a \) belongs to the exponent \( h \) mod \( m \), and \( \gcd(k, h) = d \), then \( a^k \) belongs to exponent \( h/d \) mod \( m \).

Cor. 1 If \( g \) is a primitive root modulo \( m \), then \( g^r \) is a primitive root modulo \( m \) if and only if \( \gcd(r, \phi(m)) = 1 \).

Thm 7.5 There exist any primitive root modulo \( m \), there are exactly \( \phi(\phi(m)) \) mutually incongruent primitive roots.

Ex. modulus | primitive roots | \( \phi(\phi(m)) \)  
---|---|---
1 | 1 | 1  
2 | 1 | 2  
3 | 2 | 1  
4 | 2, 3 | 2  
5 | 5 | 1  
6 | 3, 5 | 2  
7 | no | x  
8 | 2, 5 | 2  
9 | 3, 7 | 2  
10 | 3, 7 | 2
Thm 7.6 A modulus m has primitive roots if and only if
m is 2 or 4 or a number of the form $p^a$ or $2p^a$
where p is an odd prime.

The proof of this theorem is hard. We omit it here.

Proof of Thm 7.6

Let $k_i = \frac{k_i}{d}$, $h_i = \frac{h_i}{d}$. Suppose that $a^k$ belongs to exponent $f$.

First of all, $(a^k)^{h_i} \equiv a^{k_i h_i} \equiv (a^h)^{k_i} \equiv 1 \pmod{m}$

Then by Thm 7.2 $f | h_i$.

On the other hand,

$1 \equiv (a^k)^2 \equiv a^{2k} \pmod{m}$.

So by Thm 7.2 $h | k_j$ so $h_i | k_i j$.

But $\gcd(h_i, k_i) = 1$, we have $h_i | j$.

Therefore $h_i = 0$

Ex

$m = 11$

By Thm 7.5. There are $\phi(\phi(11)) = \phi(10) = 4$ primitive roots.

We can check that 2 is a primitive root.

So the other three primitive roots are given by

$2^3, 2^7, 2^9$ which are congruent to

$8, 7, 6$ modulo 11.