Recall that our goal is to show that $\mathbb{Z}_n$ has a primitive root if and only if

- $n = 1, 2, 4$ or $\longrightarrow$ obvious
- $n = p^m$ or $\longrightarrow$ Step 1
- $n = 2 \cdot p^m$ $\longrightarrow$ Step 2

$\left.\right\}$ p odd prime

Step 3: otherwise no primitive root

For Step-1, we proved for $m = 1, 2$ already.

We finish Step-1 with the following lemma

<u>Lemma:</u> Let $m \geqslant 2$. If g is a primitive root modulo p^m, then it is also a primitive root modulo p^{m+1}.

<u>Proof:</u> Say $\text{ord}_{p^{m+1}}(g) = k$.

By Euler's Theorem,

$$g^{\phi(p^{m+1})} \equiv g^{p^m \cdot (p-1)} \equiv 1 \pmod{p^{m+1}}$$

$\Rightarrow k \mid p^m \cdot (p-1)$

Also,

$$g^k \equiv 1 \pmod{p^{m+1}} \Rightarrow g^k \equiv 1 \pmod{p^m}$$

and $\operatorname{ord}_{p^m}(g) = \phi(p^m) = p^{m-1}\cdot(p-1)$

$\Rightarrow p^{m-1}\cdot(p-1) \mid k$.

From $p^{m-1}\cdot(p-1) \mid k \mid p^m\cdot(p-1)$, we have

$$k = p^{m-1}\cdot(p-1) \quad \text{or} \quad k = p^m\cdot(p-1)$$

we need to prove $k = \phi(p^{m+1}) = p^m\cdot(p-1)$, so

we just need to prove $\operatorname{ord}_{p^{m+1}}(g) = k \neq p^{m-1}\cdot(p-1)$

It is enough to show that

$$g^{p^{m-1}\cdot(p-1)} \not\equiv 1 \pmod{p^{m+1}}$$

Since g is a primitive root in $\mathbb{Z}_{p^m}$, we have

$$g^{p^{m-2}\cdot(p-1)} \not\equiv 1 \pmod{p^m}$$

and by Euler's Theorem we have

$$g^{p^{m-2}\cdot(p-1)} \equiv 1 \pmod{p^{m-1}}$$

$\Rightarrow g^{p^{m-2}\cdot(p-1)} = 1 + t\cdot p^{m-1}$ with $p \nmid t$.

Now,

$$g^{p^{m-1}\cdot(p-1)} = \left(g^{p^{m-2}\cdot(p-1)}\right)^p$$

$$= (1 + t p^{m-1})^p$$

$$= 1 + p\cdot t p^{m-1} + \underbrace{\binom{p}{2}\cdot(t p^{m-1})^2 + \dots + \binom{p}{p}\cdot(t p^{m-1})^p}_{\text{already divisible by } p^{m+1}}$$

$$\equiv 1 + t p^m \pmod{p^{m+1}}$$

$1 + 2(m-1) \geq m+1$

$$\not\equiv 1 \pmod{p^{m+1}} \quad \blacksquare$$

$p \nmid t$

Step-1 is complete. Step-2 is easier

Lemma: Let n be odd. If g is a primitive root modulo n and g is odd, then it is also a primitive root modulo $2n$.

Remark: This finishes Step-2. Take a primitive root modulo p^m, then g or $g + p^m$ will be odd.

Proof: $\phi(2n) = \phi(2)\cdot\phi(n) = \phi(n)$

true anyway

$$g^k \equiv 1 \pmod{2n} \iff g^k \equiv 1 \pmod{n} \text{ and } g^k \equiv 1 \pmod{2}$$

$$\iff g^k \equiv 1 \pmod{n}$$

Smallest positive k is $\phi(n) = \phi(2n)$. $\blacksquare$

Now, we start Step-3: for the other values of n, there is no primitive root.

Remaining values of n:

- $n = 2^e$ with $e \geqslant 3$ → Case B
- $n = 2^e \cdot p^f$ with $e \geqslant 2$, $f \geqslant 1$ → Case A
- n has at least two odd prime factors.

With the following lemma, we can cover Case A.

Lemma: If $n = a \cdot b$ with $(a, b) = 1$ and $a, b > 2$, then $\mathbb{Z}_n$ has no primitive root.

Proof: $a, b > 2 \Rightarrow \phi(a), \phi(b)$ are even (why?)

Let u be a unit in $\mathbb{Z}_n$, then

$$u^{\frac{\phi(a)\phi(b)}{2}} = \left(u^{\phi(a)}\right)^{\frac{\phi(b)}{2}} \equiv 1^{\frac{\phi(b)}{2}} \equiv 1 \pmod{a}$$

$$u^{\frac{\phi(a)\phi(b)}{2}} = \left(u^{\phi(b)}\right)^{\frac{\phi(a)}{2}} \equiv 1^{\frac{\phi(a)}{2}} \equiv 1 \pmod{b}$$

by Euler's Theorem. So, we have

$$u^{\frac{\phi(a)\phi(b)}{2}} \equiv 1 \pmod{n}$$

by CRT.

$$\Rightarrow \mathrm{ord}_n(u) \leq \frac{\phi(a)\phi(b)}{2} = \frac{\phi(n)}{2}.$$

$\Rightarrow \mathrm{ord}_n(u) \neq \phi(n)$, not a primitive root.

<u>Exercise:</u> Finish case A with the lemma.

<u>Next week:</u> Case B and a more detailed investigation of $p=2$ (behaves very differently than odd primes).