Lemma: If \( \text{ord}_n(a) = m \), then for any \( k \),
\[
\text{ord}_n(a^k) = \frac{m}{\left( \frac{m}{(m,k)} \right)}
\]

Proof:

\[
(a^k)^{\frac{m}{(m,k)}} = a^{\frac{km}{(m,k)}} = (a^m)^{\frac{k}{(m,k)}} = 1^{\frac{k}{(m,k)}} = 1
\]

So \( \text{ord}_n(a^k) \leq \frac{m}{(m,k)} \) so \( \text{ord}_n(a^k) = r \mid \frac{m}{(m,k)} \).

But if \( b < \frac{m}{(m,k)} \) then \( \frac{bm}{(m,k)} = b \cdot r < \frac{m}{(m,k)} \).

\[
(a^k)^{\frac{bm}{(m,k)}} = a^{bm} = (a^m)^{\frac{b}{(m,k)}} = 1^{\frac{b}{(m,k)}} = 1
\]

But

\[
1 = a^{(m,k)} = a^r \Rightarrow m \mid km \Rightarrow m \mid (km) r
\]

But \( (\frac{m}{(km)} , \frac{k}{(km)}) = 1 \) \( \Rightarrow \frac{m}{(km)} \mid r \Rightarrow \frac{m}{(km)} = r \).

Cor.: The number of primitive roots modulo \( p = \text{prime} \) is \( \phi(p-1) \).

Proof: \( \phi(p) = \text{ord}_p(a) = p-1 \Rightarrow 1 = a^0, a^1, \ldots, a^{p-2} \) are all distinct,

=> they can be rearranged to \( 1, 2, \ldots, p-1 \).

\( k \mid p-1 \) \( \Rightarrow \) \( k \phi(p-1) = 1 \) so the \( k \)

\( a^k \) is a primitive root \( \iff (k,p-1) = 1 \) so there are \( \phi(p-1) \) \( a^k \) which are primitive roots!
In goal, a primitive root \( n \) is on a set.

\[
\text{ord}_n(a) \text{ is as large as it could be } = \phi(n).
\]

Our proof above actually shows that if \( \mathbb{Z}/n \mathbb{Z} \) has a (non) root of

then it has \( \phi(\phi(n)) \) of them!

\section{nth roots mod \( \mathbb{Z}/p \mathbb{Z} \) when can we solve \( x^n \equiv a \pmod{p} \)

\text{If} \( (a,p)=1 \) (ie. \( p \nmid a \)) \text{ then } \boxed{\begin{cases} \text{0 solutions if } a = \frac{p^k + 1}{x} \\ \text{r solutions if } a = \frac{p^k - 1}{x} \end{cases}}

\text{If: } \text{Pick a primitive root of } 1 \text{ mod } p, \ b \text{ Then }

\text{has a for some } k. \text{ If there is } x \text{ with } x^n \equiv a \text{ then since } (a,p) = 1, \ (x,p) = 1. \ \Rightarrow x = b^k \text{ for some } k.

\text{Then } x^n = (b^k)^n = b^{kn} \equiv a \pmod{p} \iff b^{(kn)} \equiv 1 \pmod{p}

\text{Then } b^{-1}(kn-k) \equiv k \pmod{p} \text{ this has exactly } (n,p-1) \text{ solutions } \pmod{p-1} \iff (n,p-1) \mid k, \ \text{or if } \text{it has more}

So it has solutions \( b^k \equiv a \text{ with } k = rw \iff a^r = \left(b^{(rw)}\right)^{\frac{p-1}{r}} = \frac{p-1}{r} \pmod{p} \).
Recall: \( ax \equiv b \mod n \) has a solution \( \iff (a, n) \mid b \)

6/a \( ax - b = ny \implies b = ax_0 + ny \)
\( \iff b \) is a linear combination of \( a \) and \( n \) \( \iff (a, n) \mid b \).

For a particular solution, \( x_0 \), any other solution is
\( x = x_0 + \frac{k}{(a, n)} \).

\( (ax_0 = ay \implies n \mid a(y - x) \implies \frac{n}{(a, n)} \mid (y - x) \implies \text{DO} \)

Example: How many solutions are there to \( x^5 \equiv a \mod \frac{31}{15} \)?
\( p - 1 = 102 \) \( (9, 102) = 6 \) check if \( 15 \equiv 8 \mod \frac{31}{17} \)?

\( 15^6 \equiv 1 \mod \frac{31}{17} \)
\( 15^5 \equiv 225 \equiv 8 \mod \frac{31}{17} \)
\( 15^6 \equiv 8^3 \equiv 512 \equiv \frac{31}{17} \)