<u>Lemma</u>: If $\mathrm{ord}_n(a) = m$, then for any k,

$$\mathrm{ord}_n(a^k) = \frac{m}{(m,k)}$$

<u>Pf</u>: $\cancel{(a^k)^r \equiv a^{kr} \equiv_n 1}$

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

($\frac{k}{(m,k)}$ → integer!)

So $\mathrm{ord}_n(a^k) \le \frac{m}{(m,k)}$ so $\mathrm{ord}_n(a^k) = r \,\Big|\, \frac{m}{(m,k)}$

~~But if~~ $\cancel{r < \frac{m}{(m,k)}}$ ~~then~~ $\cancel{\frac{m}{(m,k)} = rs \quad s \ge 2 \quad so}$

$\cancel{(a^k)^r = a^{\frac{km}{(m,k)s}} = a^{\frac{k}{(m,k)} \cdot m \frac{1}{s}}}$ ~~But~~ $\cancel{\left(\frac{k}{(m,k)}, m\right) \ne 1}$

$\cancel{k\frac{m}{(m,k)} = rsk = \frac{k}{(m,k)} \cdot m}$

<u>But</u>

$1 \equiv (a^k)^r = a^{kr} \Rightarrow m \mid kr \longrightarrow \frac{m}{(k,m)} \,\Big|\, \frac{k}{(k,m)} r$

But $\left(\frac{m}{(k,m)}, \frac{k}{(k,m)}\right) = 1 \Rightarrow \frac{m}{(k,m)} \,\Big|\, r \Longrightarrow \frac{m}{(k,m)} = r$.

<u>Cor</u>: The number of primitive roots modulo p = prime is $\phi(p-1)$.

Pf: $\mathrm{ord}_p(a) = p-1 \Rightarrow 1 = a^0, a^1, \dots, a^{p-2}$ are <u>all</u> <u>distinct</u>

$\Rightarrow$ they are a rearrangement of $1, \dots, p-1$.

a^k ($1 \le k \le p-1$) is a primitive root $\Longleftrightarrow (k, p-1) = 1$ so there ~~roots~~.

are $\phi(p-1)$ a^k's which are primitive roots!

B

In gen'l, a primitive root of 1 mod n is an a s.t. $\text{ord}_n(a)$ is as large as it <u>could</u> be $= \phi(n)$. ✓

<u>Fact</u>: $\mathbb{Z}_n$ has a primitive root $\iff n = 2, 4, p, p^2, 2p^k$ $\quad p =$ odd prime

Our proof above actually shows that if $\mathbb{Z}_n$ <u>has</u> a prim root of 1 then it has exactly $\phi(\phi(n))$ of them!

(*)

<u>n^{th} roots mod p</u>: when can we solve $x^n \underset{p}{\equiv} a$ for fixed n, p, a?

<u>Thm</u> If $(a,p)=1$ (i.e. $p \nmid a$) then (setting $\boxed{(p-1,n)=r}$)

$$x^n \underset{p}{\equiv} a \text{ has } \begin{cases} r \text{ solutions if } a^{\frac{p-1}{r}} \underset{p}{\equiv} 1 \\ 0 \text{ solutions if } a^{\frac{p-1}{r}} \underset{p}{\not\equiv} 1 \end{cases}$$

<u>Pf</u>: Pick a primitive root of 1 mod p, b. Then $b^k \underset{p}{\equiv} a$ for <u>some</u> k. If there is a x with $x^n \underset{p}{\equiv} a$ then since $(a,p)=1$, $(x,p)=1$. So $x = b^l$ for some l.

So then $x^n = (b^l)^n = b^{ln} \underset{p}{\equiv} a = b^k \iff$ ~~so~~ $b^{(ln-k)} \underset{p}{\equiv} 1$

$\iff$ $p-1 \mid ln-k \iff$ ~~the~~ $nl \underset{p-1}{\equiv} k$ this has <u>exactly</u> $(n,p-1)$ solutions (mod $p-1$) $\iff \underset{\overset{\shortparallel}{r}}{(n,p-1)} \mid k$, o/w it has <u>none</u>

So it has solutions $\iff b^k \underset{p}{\equiv} a$ with $k = rw \iff$

$$a^{\frac{p-1}{r}} = (b^{(rw)})^{\frac{p-1}{r}} = (b^{p-1})^w \underset{p}{\equiv} 1$$

(*) <u>Recall</u> : $ax \underset{n}{\equiv} b$ has a solution $\Longleftrightarrow$ $(a,n) \mid b$

C

b/c $ax - b = ny \Longleftrightarrow b = \cancel{ax}\ a(-x) + ny$
$\Longleftrightarrow b$ is a lin comp of a and n $\Longleftrightarrow (a,n) \mid b$.

For a particular solution, x_0, any <u>other</u> solution is

$$x = x_0 + i\frac{n}{(a,n)} . \quad \left(ax \underset{n}{\equiv} ay \Longleftrightarrow n \mid a(y-x) \right.$$
$$\Longleftrightarrow \frac{n}{(a,n)} \Big| \frac{a}{(a,n)}(y-x)$$
$$\left. \Longleftrightarrow \frac{n}{(a,n)} \Big| y-x \right) \leftarrow \underline{DO}$$

$\Rightarrow$ there are (a,n) incongruent solutions.

<u>Ex</u>! How many solutions of $x^{\overset{n}{\cancel{x}}\,5} \equiv \overset{a}{15} \pmod{\overset{p}{\cancel{103}}\ 31}$?

$p-1 = 102$ $\quad (\cancel{3}\,5, \cancel{102}\,30) = \cancel{3}\,5$ <u>check</u> <u>if</u> $\quad \cancel{15^{51} \underset{103}{\equiv} 1}$?

$15^6 \underset{31}{\equiv} 1$?

$15^2 = 225 \underset{31}{\equiv} 8 \qquad 15^6 \equiv 8^3 \equiv 512 \underset{31}{\equiv} 17$