Recall : Let u be a unit in $\mathbb{Z}_n$. The smallest positive integer k satisfying $u^k \equiv 1 \pmod{n}$ is called the order of u modulo n, denoted by $\text{ord}_n(u)$.

Let p be a prime and g be a unit in $\mathbb{Z}_p$. The followings are equivalent:

$$\left.\begin{array}{l} 1.\ g \text{ generates all the units of } \mathbb{Z}_p \text{, i.e.} \\ \{1,2,3,\dots,p-1\} \equiv \{g, g^2, g^3, \dots, g^{p-1}\} \pmod{p} \\ \\ 2.\ \text{ord}_p(g) = p-1 \end{array}\right\} \text{primitive root}$$

We proved for a primitive root g modulo p that

$$k \geqslant 0 \text{ and } g^k \equiv 1 \pmod{p} \iff p-1 \mid k$$

Take a unit modulo p, it can be written g^a in $\mathbb{Z}_p$ for some $1 \leqslant a \leqslant p-1$. What is $\text{ord}_p(g^a)$?

$$(g^a)^k \equiv 1 \pmod{p} \iff g^{ak} \equiv 1 \pmod{p}$$

$$\iff p-1 \mid ak \longrightarrow ak \equiv 0 \pmod{p-1}$$

$$\frac{ak}{a} \equiv \frac{0}{a} \left(\text{mod } \frac{p-1}{(p-1,a)}\right)$$

$$\iff \frac{p-1}{(p-1,a)} \mid k \longleftarrow k \equiv 0 \left(\text{mod } \frac{p-1}{(p-1,a)}\right)$$

Theorem : $\text{ord}_p(g^a) = \dfrac{p-1}{(p-1,a)}$.

Example:

- In $\mathbb{Z}_3$: $\{ 2, 2^2 \} \pmod 3$

  orders: $2 \quad 1$

- In $\mathbb{Z}_5$: $\{ 2, 2^2, 2^3, 2^4 \} \pmod 5$

  orders: $4 \quad 2 \quad 4 \quad 1$

- In $\mathbb{Z}_7$: $\{ 3, 3^2, 3^3, 3^4, 3^5, 3^6 \} \pmod 7$

  orders: $6 \quad 3 \quad 2 \quad 3 \quad 6 \quad 1$

Remark: Order of a unit modulo p always divides $p-1$.

Theorem: Let d be a positive divisor of $p-1$, then there are exactly $\phi(d)$ units modulo p of order d.

Proof:

$$\operatorname{ord}_p(g^a) = d \iff \frac{p-1}{(p-1, a)} = d$$

$1 \leq a \leq p-1$

$$\iff (p-1, a) = \frac{p-1}{d}.$$

We should have $a = n \cdot \frac{p-1}{d}$ for that

$1 \leq n \leq d$

$$\left(p-1, n \cdot \frac{p-1}{d}\right) = \frac{p-1}{d} \iff (d, n) = 1$$

There are $\phi(d)$ values of n such that $(d, n) = 1$ and $1 \leq n \leq d$.

Corollary: There are $\phi(p-1)$ primitive roots modulo p.

Corollary: $\sum_{d \mid p-1} \phi(d) = p - 1$. (Both sides give the number of units mod p).

We have the following more general results regarding the order of units in $\mathbb{Z}_n$.

Theorem: We have

$$k \geqslant 0 \text{ and } u^k \equiv 1 \pmod{n} \iff \operatorname{ord}_n(u) \mid k.$$

In particular, $\operatorname{ord}_n(u) \mid \phi(n)$.

Proof: Write $k = \operatorname{ord}_n(u) \cdot m + r$, $0 \leq r < \operatorname{ord}_n(u)$

Then, $u^k \equiv 1 \pmod{n} \iff \left(u^{\operatorname{ord}_n(u)}\right)^m \cdot u^r \equiv 1 \pmod{n}$

$$\iff u^r \equiv 1 \pmod{n}$$

$$\iff r = 0$$

$$\iff \operatorname{ord}_n(u) \mid k.$$

Theorem: $\operatorname{ord}_n(u^a) = \dfrac{\operatorname{ord}_n(u)}{(\operatorname{ord}_n(u), a)}$.

Proof: Exercise.

Now, we'll prove the existence of a primitive root modulo p.

Strategy: to prove a stronger result: "There are $\phi(d)$ units of order d modulo p when $d \mid p-1$". (and 0 units when $d \nmid p-1$)

We'll prove by induction on d.

If $d=1$: $\operatorname{ord}_p(u) = 1 \iff u \equiv 1 \pmod p$.

Assume our claim is true up to d, where $d \mid p-1$.

$$\operatorname{ord}_p(u) = d \Rightarrow u^d \equiv 1 \pmod p$$
$$\Rightarrow u^d - 1 \equiv 0 \pmod p$$

How many u satisfies this congruence?
Answer is d by Q1 of PS 4.
If $u^d \equiv 1 \pmod p$, then $\operatorname{ord}_p(u) \mid d$. We should subtract the units of order d' such that

.

$d' \mid d$ but $d' \neq d$. (and $d' > 0$)

$\Rightarrow$ There are $d - \sum_{\substack{d' \mid d \\ 0 < d' \neq d}} \phi(d')$ units of

order d by induction hypothesis.