Proof Technique for : $\mathbb{Z}_{p^e}^*$ is cyclic (p prime, ≥ 3, $e \geq 1$)

- First we determine a generator, say a, of $\mathbb{Z}_p^*$
- Write $a^{p-1} = 1 + pT$ (because $a^{p-1} \equiv 1 \pmod{p}$)

Our objective is to somehow use "a" to get a generator of $\mathbb{Z}_{p^e}^*$ so

- we determine ord a (in $\mathbb{Z}_{p^e}^*$) to be of the form

$$(p-1)p^j$$

where j is necessarily no greater than $e-1$.

The question is whether we can preclude the possibility of $j \leq e-2$.

- Next, under the assumption that $p \nmid T$ we can prove by induction that

$$a^{(p-1)p^\ell} = 1 + p^{\ell+1}u_\ell$$

where u_ℓ is a # NOT divisible by p so that if $\ell \leq e-2$

$$a^{(p-1)p^\ell} - 1 = p^{\ell+1}u_\ell$$

is NOT divisible by p^e. Thus, in this case, the order is $(p-1)p^{e-1} = |\mathbb{Z}_{p^e}^*|$

<u>Remark</u> This induction argument works because the assumption

$$p \nmid T$$

yields the base case, i.e. $l = 0$

- If $p \mid T$ then we consider $a+p$. Since $a \equiv a+p \pmod p$ we can prove that
$$(a+p)^{p-1} = 1 + p u_0$$
where $p \nmid u_0$. This is done with the use of the binomial theorem.

- We now proceed exactly as in the previous case (i.e $p \nmid T$) to obtain the conclusion that $\operatorname{ord}(a+p) = (p-1)p^{e-1}$.