3.1.2

「$x \equiv y \pmod{p} \Rightarrow x^{p^n} \equiv y^{p^n} \pmod{p^{n+1}}$ $(n \in \mathbb{Z},\ n \geq 0)$」…①

を数学的帰納法で証明する

(i) $n=0$ のとき　仮定より　①が成り立つことは明らか

(ii) $n=k$ $(k \in \mathbb{Z},\ k \geq 0)$ のとき①が成り立つとすると

$x^{p^k} \equiv y^{p^k} \pmod{p^{k+1}}$ より

$x^{p^k} - y^{p^k} = p^{k+1} m$ $(m \in \mathbb{Z})$ とおける

つまり、$x^{p^k} = y^{p^k} + p^{k+1} m$.

$n=k+1$ のとき

$$x^{p^{k+1}} - y^{p^{k+1}} = (x^{p^k})^p - y^{p^{k+1}}$$

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

$$= \sum_{i=1}^{p} {}_pC_i \left(y^{p^k}\right)^{p-i} \left(p^{k+1} m\right)^i$$

$1 \leq i \leq p-1$ のとき　${}_pC_i$ は p で割り切れ、$i \geq 1$ より $\left(p^{k+1} m\right)^{p-i}$ は p^{k+1} で割り切れる

よって ${}_pC_i \left(y^{p^k}\right)^i \left(p^{k+1} m\right)^{p-i}$ は p^{k+1} で割り切れる。

$i=p$ のとき　$\left(p^{k+1} m\right)^p$ は明らかに p^{k+1} で割り切れる

よって　$x^{p^{k+1}} - y^{p^{k+1}}$ は p^{k+1} で割り切れる

ゆえに　$n=k+1$ のときも①が成り立つことが示された。

(i), (ii) より

題意は示された。

合同式のみを使った証明
もしくは
代数構造に着目した証明
はできるのかな