TAM CHEETHAM-WE

NUMBER THEORY (PROBLEM 4).

$h(x)$ is a polynomial with integer coefficients.
$h(0), h(1), \ldots, h(p^2-1)$ are distinct (mod p^2).
In particular $h(0), h(1), \ldots, h(p^2-1)$ are also distinct mod p^3 [since, if any 2 elements of $\{h(0), h(1), \ldots, h(p^2-1)\}$ are congruent (mod p^3) they are congruent mod p^2 by divisibility].
I consider lifts from $\{0,1,\ldots,p^2-1\}$ to $\{0,1,\ldots,p^3-1\}$ of the form $a+tp^2$ where $a \in \{0,1,\ldots,p^2-1\}, 0<t<$
- In particular with this specification above the smallest lift is $a=0, t=1 \Rightarrow p^2$ and the largest lift is $a=p^2-1$, $t=p-$ $\Rightarrow p^3-1$].

$$h(x) = h(a) + h'(a)(x-a) + \frac{h''(a)}{2!}(x-a)^2 + \frac{h'''(a)}{3!}(x-a)^3 \ldots$$

plugging $x = a+tp^2$.

$$h(a+tp^2) = h(a) + h'(a)tp^2 + \frac{h''(a)}{2!}(tp^2)^2 + \frac{h'''(a)}{3!}(tp^2)^3 \ldots$$

Reducing (mod p^3) yields.

$$h(a+tp^2) = h(a) + \underbrace{h'(a)tp^2 + h''(a)tp^2}_{\not\equiv 0 \pmod{p^3}}.$$

$\Rightarrow h(a+tp^2) \not\equiv h(a) \pmod{p^3}$. Each lift $h(a+tp^2)$ is incongruent to its parent $(h(a))$ (mod p^3). Also the lifts are incongruent to themselves (mod p^3) since each lift can be viewed as a lift from a previous lift (mod p^2).
By the same Taylor series method, we can see that $h(a+tp^2) \not\equiv h(b)$ when $b \in \{0,1,\ldots,p^2-1\}$, $b \neq a$.
We can also see that the lifts from some $a \in \{0,1,\ldots,p^2-1\}$ will be incongruent to all the lifts from $b \neq a \in \{0,1,\ldots,p^2-1\}$ by considering various Taylor series forms.

$\Rightarrow h(0), h(1), \ldots, h(p^3-1)$ are distinct numbers mod p^3 $\square$