

Q2a: We will prove this via induction on e . For when $e = 1$, we have the simultaneous equations $x^{p-1} \equiv 1 \pmod{p}$ and $x \equiv i \pmod{p}$. For each i nonzero we have that $i^{p-1} \equiv 1 \pmod{p}$ by Fermat's little Theorem. Now suppose that for e , there is some x_e such that $x_e^{p-1} \equiv 1 \pmod{p^e}$ and $x_e \equiv i \pmod{p}$ for some i . Take $x_{e+1} = x_e + p^e \cdot k$, for some $k \in \mathbb{Z}$. We have that

$$\begin{aligned}
 f(x_{e+1}) &= f(x_e + kp^e) \\
 &= (x_e + kp^e)^{p-1} - 1 \\
 &= \sum_{j=0}^{p-1} \binom{p-1}{j} x_e^{p-1-j} (kp^e)^j - 1 \\
 &= x_e^{p-1} + (p-1)x_e^{p-2} \cdot kp^e \cdots - 1 \\
 &= x_e^{p-1} - 1 + (p-1)x_e^{p-2} \cdot kp^e \\
 &= f(x_e) + f'(x_e)kp^e \pmod{p^{e+1}}
 \end{aligned}$$

By assumption, $f(x_e) \equiv 0 \pmod{p^e}$, we can write $f(x_e) = ap^e$ for some $a \in \mathbb{Z}$. Therefore, $ap^e + f'(x_e)kp^e \equiv 0 \pmod{p^{e+1}}$ and so $a + f'(x_e)k \equiv 0 \pmod{p}$. Since $f'(x_e)$ is nonzero since $x_e \equiv i \not\equiv 0$, so we can take $k = (-a) \cdot (f'(x_e))^{-1}$. Inverses are unique hence x_{e+1} is unique.

Q2b: For each e_i we take $x_{e_i} \equiv -1 \pmod{p^{e_i}}$. We can clearly see that $x_{e_i}^2 \equiv 1 \pmod{3^{e_i}}$ and $x_{e_i} \equiv 2 \pmod{3}$