Solutions

1. Assume the congruence has $k$ roots $a_1, a_2, \ldots, a_k$.

$f(x) = (x-a_1)\cdots(x-a_k)\, g(x) + p\, r(x)$.

$g(x)$ must be non-zero, since by assumption not all coefficients of $f(x)$ are divisible by $p$.

Consequently, $n = \deg f(x) = k + \deg g(x)$

$\geq k$.

$\Rightarrow k \leq n$.

2. Example: $x^2 \equiv 1 \mod 8 \rightarrow$ has 4 solutions

3. $x^3 + 4x \equiv 4 \pmod{343}$

$343 = 7^3$

We first solve the congruence mod 7, then mod $7^2$ & finally mod $7^3$.

$x^3 + 4x \equiv 4 \mod 7$

$f(x) = x^3 + 4x - 4$

$f'(x) = 3x^2 + 4$

Trying all residue classes, we see that $x^3 + 4x \equiv 4 \mod 7$ has the single sol$^n$ $x \equiv 3 \pmod 7$

$f'(a_1) = 27 + 4 = 31$ $(a_1 = 3)$

$7 \nmid f'(a_1) = 31$.

so, can use the corollary. unique sol.$^n$ for $f(x) \equiv 0 \mod 7^3$

lift $a_1 \equiv 3 \pmod 7$ to a solution mod $7^2$.

$f'(3)\, t \equiv -\dfrac{f(3)}{7} \mod 7$

$$31\,t \equiv -\frac{(3^3+4.3-4)}{7} \bmod 7$$

$$\equiv -5 \bmod 7$$

$$31t \equiv 2 \bmod 7$$

$$\Rightarrow 3t \equiv 2 \bmod 7$$

$$t \equiv 3 \bmod 7$$

$$a_2 = a_1 + 7t$$

$$= 3 + 21 = 24$$

$$a_2 \equiv 24 \bmod 49.$$

Lift $a_2 \equiv 24 \bmod 49$ to a sol.$^n$ mod $7^3$

$$f'(24)\,t \equiv -\frac{f(24)}{49} \bmod 7$$

$$(3.24^2+4)t \equiv -\frac{(24^3+4.24-4)}{49} \bmod 7$$

$$3t \equiv 3 \bmod 7$$

$$t \equiv 1 \bmod 7$$

$$a_3 = a_2 + 7^2 t$$

$$= 24 + 49$$

$$= 73$$

$$\boxed{a_3 \equiv 73 \bmod 7^3}$$