

find solutions (mod m). For each congruence (mod $p_i^{a_i}$) to have solutions it must have solutions mod p_i . $a_i = 1, \dots, r$.
 If it has a soln (mod p), then it will have solns mod p^2 if $f'(r) \not\equiv 0 \pmod{p}$ or $f'(r) \equiv 0 \pmod{p}$ and $f(r) \equiv 0 \pmod{p^2}$.
 In the 1st case each solution (mod p) gives rise to a unique solution (mod p^2), and the second case has each solution (mod p) giving rise to p solns (mod p^2).

The substance of the last paragraph generalises, so if $f(r) \equiv 0 \pmod{p^k}$ has a soln r , and $f'(r) \not\equiv 0 \pmod{p}$, then we can find solns (mod p^{k+1}).
 If $f'(r) \equiv 0 \pmod{p}$, $f(r) \equiv 0 \pmod{p^{k+1}}$ each soln (mod p^k) gives rise to p solutions (mod p^{k+1}).
 If $f'(r) \equiv 0 \pmod{p}$, $0 \not\equiv f(r) \pmod{p^{k+1}}$, then r cannot give rise to a soln (mod p^{k+1}).

For example, find solutions to

$$f(x) = 2x^2 + 3 \equiv 0 \pmod{25}$$

$$\text{Find solns to } f(x) = 2x^2 + 3 \equiv 0 \pmod{5}$$

$$f(0) = 3 \pmod{5}$$

$$f(1) = 5 \equiv 0 \pmod{5}$$

$$f(2) = 2 \cdot 2^2 + 3 = 1 \pmod{5}$$

$$f(3) = 2 \cdot 3^2 + 3 = 1 \pmod{5}$$

$$f(4) = 2 \cdot 4^2 + 3 = 0 \pmod{5}$$

1, 4 are solns

$$\text{Now } f(1) \not\equiv 0 \pmod{25}$$

$$f(4) = 35 \not\equiv 0 \pmod{25}$$

$$f'(x) = 4x \Rightarrow f'(1) = 4 \not\equiv 0 \pmod{5}$$

$$f'(4) = 16 \not\equiv 0 \pmod{5}$$