P6578708 (10)

Expand $f(x)$ in a Taylor series
$(\mathrm{mod}\ p^{n-1})$ if r is a soln to $f(x) \equiv 0 (\mathrm{mod}\ p^n)$
Put $x = r + qp^{n-1}$
$f(r+qp^{n-1}) = f(r) + qp^{n-1} f'(r) (\mathrm{mod}\ p^{n+1})$
since higher order terms are
multiplied by $p^{2(n-1)} \equiv 0 (\mathrm{mod}\ p^{n+1})$
$f(r) = k p^{n-1}$ since $f(r) \equiv 0 (\mathrm{mod}\ p^{n-1})$
so $f(r+qp^{n-1}) \equiv (k + qf'(r)) p^{n-1} (\mathrm{mod}\ p^n)$
Hence we must have $k + qf'(r) \equiv 0 (\mathrm{mod}\ p)$
We solve for $q (\mathrm{mod}\ p)$, then the
solution $(\mathrm{mod}\ p^n)$ that we are
looking for is $r + qp^{n-1}$
If $f'(r) = f(r) \equiv 0 (\mathrm{mod}\ p^n)$ then we
can take $q = 0, 1, \ldots, p-1$ in the
equation $r_1 = r + qp^{n-1}$
For the example on the previous
page, we solve
for $r=1$ $\quad 1 + 4q \equiv 0 (\mathrm{mod}\ 5) \Rightarrow q = 1$,
$r_1 = 1 + 1 \cdot 5 \equiv 6 (\mathrm{mod}\ 25)$
for $r=4$ $\quad 7 + 16q \equiv 0 (\mathrm{mod}\ 5) \Rightarrow q = 3$
$r_1 = 4 + 3 \cdot 5 \equiv 19 (\mathrm{mod}\ 25)$
$f(6) = 2 \cdot 6^2 + 3 = 75 \equiv 0 (\mathrm{mod}\ 25)$
$f(19) = 2 \cdot 19^2 + 3 = 725 \equiv 0 (\mathrm{mod}\ 25)$ ✓

You need to discuss solving quadratic congruences, and also to frame the essay with an introduction, describing the problem, and a conclusion summarising the techniques.
(14)