

This is a quick example of Hensel's lemma.

Say we want to solve the equation $f(x) = x^3 + 8x - 5 \equiv 0 \pmod{p^3}$ where $p = 5$. We can check that $f(0) \equiv 0 \pmod{p}$. Also $f'(0) \equiv 3 \pmod{p}$.

Here is one way of doing this: Let $x_1 = 0$. Let $x_2 = 0 + pt$ (since we know $x_2 \equiv x_1 \pmod{p}$). Looking at $f(x_2)$ we get

$$f(x_2) = f(x_1 + pt) = f(x_1) + pt f'(x_1) + \cdots \equiv f(x_1) + pt f'(x_1) \pmod{p^2}.$$

Therefore to find x_2 we need to solve

$$f(x_1) + pt f'(x_1) \equiv 0 \pmod{p^2}.$$

Since $f(x_1) \equiv 0 \pmod{p}$, we can divide the above congruence by p to get

$$\frac{f(x_1)}{p} + t f'(x_1) \equiv 0 \pmod{p}.$$

That is

$$-1 + 3t \equiv 0 \pmod{p},$$

which implies $t \equiv 2 \pmod{p}$. Plugging that back in $x_2 = 0 + 2 \cdot 5 = 10$ is a solution modulo p^2 .

Doing this again, we can let $x_3 = x_2 + p^2 t$, and look at $f(x_3)$. We get

$$f(x_3) = f(x_2 + p^2 t) \equiv f(x_2) + p^2 t f'(x_2) \equiv 0 \pmod{p^3}.$$

Since we know $p^2 | f(x_2)$, we can divide the above equation by p^2 to get

$$\frac{f(x_2)}{p^2} + t f'(x_2) \equiv 0 \pmod{p}.$$

That is

$$3 + 3t \equiv 0 \pmod{p},$$

which implies $t \equiv 4 \pmod{p}$. In particular $x_3 = 10 + 4 \cdot 25 = 110$ should work, and in fact $f(110) = 5^4 \cdot 2131 \equiv 0 \pmod{5^3}$.

And we can continue this way to get x_n such that $f(x_n) \equiv 0 \pmod{p^n}$ and $x_n \equiv x_1 \pmod{p}$.

Notice that this was presented in a fairly general manner. Namely, say we are given a polynomial $f \in \mathbb{Z}[x]$, prime p , and x_1 such that $f(x_1) \equiv 0 \pmod{p}$ and $f'(x_1) \not\equiv 0 \pmod{p}$. Then we can let $x_2 = x_1 + pt$ and solve for $f(x_2) \equiv 0$. Using Taylor expansion we get

$$0 \equiv f(x_2) \equiv f(x_1) + pt f'(x_1) \pmod{p^2},$$

and since $p | f(x_1)$ we get

$$0 \equiv \frac{f(x_1)}{p} + t f'(x_1) \pmod{p},$$

or equivalently

$$-\frac{f(x_1)}{p} \equiv t f'(x_1) \pmod{p}.$$

Let a be an inverse of $f'(x_1)$, then we get

$$t \equiv -a \frac{f(x_1)}{p} \pmod{p},$$

and we get

$$x_2 = x_1 + pt = x_1 - pa \frac{f(x_1)}{p} \equiv x_1 - af(x_1) \pmod{p^2}.$$

Now we can find $x_3 = x_2 + p^2t$ and solve for $f(x_3) \equiv 0 \pmod{p^3}$. Again, using Taylor expansion we get

$$0 \equiv f(x_3) \equiv f(x_2) + p^2tf'(x_2) \pmod{p^3},$$

and since $p^2|f(x_2)$ we get

$$0 \equiv \frac{f(x_2)}{p^2} + tf'(x_2) \pmod{p},$$

or equivalently

$$-\frac{f(x_2)}{p^2} \equiv tf'(x_2) \pmod{p}.$$

Note that since $x_1 \equiv x_2 \pmod{p}$ we get $f'(x_2) \equiv f'(x_1)$, therefore

$$-\frac{f(x_2)}{p^2} \equiv tf'(x_1) \pmod{p}.$$

Note that we let a be the inverse of $f'(x_1)$, so we can rewrite this as

$$-a\frac{f(x_2)}{p^2} \equiv t \pmod{p},$$

and subbing back we get

$$x_3 = x_2 + p^2t \equiv x_2 - af(x_2) \pmod{p^3}.$$

And we can do this again. In fact, assume that $x_n \equiv x_1 \pmod{p}$ such that $f(x_n) \equiv 0 \pmod{p^n}$. Then let $x_{n+1} = x_n + p^nt$, and try to solve for $f(x_{n+1}) \equiv 0 \pmod{p^{n+1}}$. Using Taylor's expansion we get

$$0 \equiv f(x_{n+1}) = f(x_n + p^nt) \equiv f(x_n) + p^ntf'(x_n) \pmod{p^{n+1}}.$$

Since $p^n|f(x_n)$ we can divide by p^n to get

$$0 \equiv \frac{f(x_n)}{p^n} + tf'(x_n) \pmod{p}.$$

Since $x_n \equiv x_1 \pmod{p}$ we get $f'(x_n) \equiv f'(x_1) \pmod{p}$. Therefore we want to solve for

$$0 \equiv \frac{f(x_n)}{p^n} + tf'(x_1) \pmod{p}.$$

Since a is the inverse of $f'(x_1)$ modulo p we get

$$t \equiv -a\frac{f(x_n)}{p^n} \pmod{p},$$

and subbing this back we get

$$x_{n+1} = x_n + p^nt = x_n - p^na\frac{f(x_n)}{p^n} = x_n - af(x_n) \pmod{p^{n+1}}.$$

So, let's try to do another example of Hensel's lifting using the above recurrence:

Let $f(x) = x^3 + 3x - 7$, and let $p = 7$. We can check that f has three roots modulo p , namely 0, 2, and 5. Let's apply Hensel's lifting to $x_1 = 0$. Note that

$f'(x_1) = 3$, and that 5 is an inverse of 3 modulo 7. So, let $a = 5$. Then we get

$$\begin{aligned} x_2 &\equiv x_1 - af(x_1) &= 35, \\ x_3 &\equiv x_2 - af(x_2) &= -214830 \equiv 231 \pmod{7^3}, \\ x_4 &\equiv x_3 - af(x_3) &= -61635154 \equiv 917 \pmod{7^4}, \\ &\vdots & \end{aligned}$$

(Here x_n 's are always chosen as an integer between 0 and 7^n .)

Exercise: Apply two or three steps of Hensel's lifting to $x_1 = 2$. (You should check that $f(x_n) \equiv 0 \pmod{p^n}$).