Hensel's Lemma

Let $n = p_1^{e_1} \cdots p_r^{e_r}$. The problem of solving a polynomial congruence

$$f(x) \equiv 0 \bmod n$$

$\Downarrow$ reduced by Chinese Remainder Theorem to solving a system of congruences

$$f(x) \equiv 0 \bmod p_i^{e_i} \qquad (i = 1, \dots, r).$$

To solve $f(x) \equiv 0 \bmod p^K$ we start with a solution modulo p, then move to a solution modulo $p^2, \dots,$ up to p^K.

Suppose that $x = a$ is a solution to $f(x) \equiv 0 \bmod p^J$ and we want to use it to get a solution modulo p^{J+1}. The idea is try to get a solution ~~modulo~~ $x = a + tp^J$, where t is to be determined, by use of Taylor's expansion

$$f(a+tp^J) = f(a) + tp^J f'(a) + t^2 p^{2J} \frac{f''(a)}{2!} + \cdots + t^n p^{nJ} \frac{f^{(n)}(a)}{n!} \qquad (*)$$

where degree $(f) = n$. All derivatives beyond the n^{th} are identically zero.

Now with respect to the modulus p^{J+1}, equation $(*)$ gives

$$f(a+tp^J) \equiv f(a) + tp^J f'(a) \pmod{p^{J+1}} \qquad (**)$$

as the following argument shows. What we want to establish is that the coefficients of $t^2, t^3, \dots, t^n$ in $(*)$ are divisible by p^{J+1} and so can be ~~omitted~~ omitted in $(**)$. This is almost obvious because the powers of p in those terms are $p^{2J}, p^{3J}, \dots, p^{nJ}$. But this is not quite immediate because of the denominators $2!, 3!, \dots, n!$ in these terms.

The explanation is that $\dfrac{f^{(k)}(a)}{k!}$ is an integer for each value of k, $2 \le k \le n$. (

To see this, let cx^r be a representative term from $f(x)$. The corresponding term in $f^{(k)}(a)$ is

$$cr(r-1)(r-2)\cdots(r-k+1)\,a^{r-k}.$$

It is a well-known fact that the product of k consecutive integers is divisible by $k!$ and the argument is complete. Thus we have proved that the coefficient of $t^2, t^3, \ldots, t^n$ in $(*)$ are divisible by p^{J+1}.

The congruence $(**)$ reveals how t should be chosen if $x = a + tp^J$ is to be a solution of $f(x) \equiv 0 \bmod p^{J+1}$. We want

$$f(a) + tp^J f'(a) \equiv 0 \pmod{p^{J+1}}.$$

Since $f(x) \equiv 0 \bmod p^J$ is presumed to have a solution $x = a$, we see that p^J can be removed as a factor to give

$f(a) \equiv 0 \bmod p^J$

$f(a) = kp^J$

$$t f'(a) \equiv -\frac{f(a)}{p^J} \pmod p \qquad (***)$$

which is a linear congruence in t. This congruence may have no solution, one solution or p solutions. If $f'(a) \not\equiv 0 \pmod p$, then this congruence has exactly one solution an we obtain

<u>Thm 2.73 (Hensel's Lemma)</u>: Suppose $f(x) \in \mathbb{Z}[x]$. If $f(a) \equiv 0 \pmod{p^J}$ and $f'(a) \not\equiv 0 \bmod p$, then there is a unique $t \pmod p$ s.t.

$$f(a + tp^J) \equiv 0 \pmod{p^{J+1}}.$$

If $f(a) \equiv 0 \bmod p^J$, $f(b) \equiv 0 \pmod{p^K}$, $J < K$ and (

$a \equiv b \pmod{p^J}$, then we say that b *lies above* a, or a lifts to b.

If $f(a) \equiv 0 \pmod{p^J}$, then the root a is called *nonsingular* if $f'(a) \not\equiv 0$ (

otherwise it is *singular*.

By Hensel's lemma we see that a non singular root a (mod p) lifts to a unique root $a_2 \pmod{p^2}$. Since $a_2 \equiv a \bmod p$, it follows from the fact that (if $a \equiv b \bmod m \Rightarrow f(a) \equiv f(b) \bmod m$) that $f'(a_2) \equiv f'(a) \not\equiv 0 \bmod$

By a second application of Hensel's lemma we may lift a_2 to form a root a_3 of $f(x)$ modulo p^3, and so on. In general we find that a nonsingular root a modulo p lifts to a unique root a_J modulo p^J for $J = 2, 3, \ldots$.

By (***) we see that

$$a_{J+1} = a_J - f(a_J)\,\overline{f'(a)} \qquad (****)$$

where $\overline{f'(a)}$ is an integer chosen so that $f'(a)\,\overline{f'(a)} \equiv 1 \bmod p$.

Example: We want to solve $x^2 \equiv -1 \mod 5^4$.

This is the same as solving $f(x) \equiv 0 \mod 5^4$, where $f(x) = x^2+1$.

First we note that $x = \pm 2$ are solutions to $f(x) \equiv 0 \mod 5$

and that $f'(x) = 2x$.

We also have that $f'(2) = 4 \not\equiv 0 \mod 5$ and $f'(-2) = -4 \not\equiv 0 \mod 5$

and therefore $x = \pm 2$ are nonsingular roots.

Let $a \equiv 2 \mod 5$. So we have that

$$a_2 = a - f(a)\overline{f'(a)}, \text{ where } \overline{f'(a)} \text{ is s.t. } f'(a)\overline{f'(a)} \equiv 1 \mod p$$

So, $a_2 = 2 - f(2)\overline{f'(2)} = 2 - 5 . 4$ (we can choose $\overline{f'(2)} = 4$)

$$a_2 = -18$$

Since we consider $a_2 \mod 5^2$, we have $a_2 \equiv 7 \mod 5^2$.

Now we have

$$a_3 = a_2 - f(a_2)\overline{f'(a)} = 7 - f(7) . 4 = 7 - 200 = -193$$

Since we are considering $a_3 \mod 5^3$, we have

$$-193 \equiv -68 \mod 5^3 \equiv 57 \mod 5^3.$$

Now we want to compute a_4.

$$a_4 = a_3 - f(a_3) . 4 = 57 - f(57) . 4 = 57 - 13.000 = -1294$$

We consider a_4 mod 5^4, then we have

$$-12943 \equiv -443 \bmod 5^4 \equiv 182 \bmod 5^4.$$

Therefore $x = 182$ is one root.

If we start with $a = -2$ then we obtain the solution $x = -182$.

Hence we may conclude that ± 182 are the desired roots.