Math 115. The Stronger General Hensel's Lemma

This handout gives the stronger version of the general Hensel's Lemma (Theorem 2.24), a variant of it, and also a corollary.

Theorem (Hensel's lemma, general version). *Let $f \in \mathbb{Z}[x]$, let p be a prime, and let $a \in \mathbb{Z}$. Assume that $f(a) \equiv 0 \pmod{p^j}$ for some j, $p^\tau \parallel f'(a)$ for some $\tau \in \mathbb{N}$, and that $j \ge 2\tau + 1$. Then:*

(a). *There is an integer t, unique modulo $p^{j-2\tau}$, such that $f(a + tp^{j-\tau}) \equiv 0 \pmod{p^{2j-2\tau}}$. Also, t is the (unique) solution to the congruence*

$$\frac{f'(a)}{p^\tau} t \equiv -\frac{f(a)}{p^j} \pmod{p^{j-2\tau}} .$$

(b). *If $b \equiv a \pmod{p^{j-\tau}}$, then $f(b) \equiv f(a) \pmod{p^j}$.*

(c). *If $b \equiv a \pmod{p^{\tau+1}}$, then $p^\tau \parallel f'(b)$. In particular, this holds if $b \equiv a \pmod{p^{j-\tau}}$.*

Proof. (a). Let $b = a + tp^{j-\tau}$ (with $t \in \mathbb{Z}$ unknown). By Taylor's formula,

$$f(b) = f(a) + f'(a)(tp^{j-\tau}) + \frac{f''(a)}{2}(tp^{j-\tau})^2 + \cdots + \frac{f^{(n)}(a)}{n!}(tp^{j-\tau})^n . \qquad (*)$$

Each coefficient $f^{(i)}(a)/i!$ is an integer; this is because the polynomial $f^{(i)}(x)/i!$ has integer coefficients (this can be checked term by term, using Theorem 1.21 on page 36). Therefore the third and subsequent terms are all $\equiv 0 \pmod{p^{2j-2\tau}}$ (since $j \ge 2\tau + 1$ implies $j \ge \tau$).

Setting $f(b)$ congruent to zero modulo $p^{2j-2\tau}$ then gives the congruence

$$0 \equiv f(a) + f'(a)(tp^{j-\tau}) \pmod{p^{2j-2\tau}} ;$$

rearranging terms and dividing by p^j then gives

$$\frac{f'(a)}{p^\tau} t \equiv -\frac{f(a)}{p^j} \pmod{p^{j-2\tau}} .$$

Note that $f(a)/p^j \in \mathbb{Z}$ and that $f'(a)/p^\tau$ is an integer prime to p, hence prime to $p^{j-2\tau}$. This gives t uniquely modulo $p^{j-2\tau}$, as was to be shown.

(b). If $b \equiv a \pmod{p^{j-\tau}}$, then we have $b = a + tp^{j-\tau}$, so the equation (*) is true. This part then follows from the fact that all terms on the right-hand side other than the first are multiples of p^j. Indeed, for the terms $(f^{(i)}(a)/i!)(tp^{j-\tau})^i$ with $i \ge 2$, this is true because $f^{(i)}(a)/i! \in \mathbb{Z}$ and $i(j-\tau) \ge 2j - 2\tau > j$, and when $i = 1$ it is true because $f'(a)(tp^{j-\tau})$ is a multiple of p^j.

(c). By Theorem 2.2,

$$b \equiv a \pmod{p^{\tau+1}} \implies f'(b) \equiv f'(a) \pmod{p^{\tau+1}} ,$$

and it then follows that $p^\tau \parallel f'(b)$ since $p^\tau \parallel f'(a)$. The last part is true because $j - \tau \ge \tau + 1$. □

Since t is only unique modulo $p^{j-\tau}$, $a+tp^{j-\tau}$ is unique modulo $p^{2j-3\tau}$, and so the congruence $f(x)\equiv 0 \pmod{p^{2j-2\tau}}$ has p^τ solutions modulo $p^{2j-2\tau}$ corresponding to a given value of a.

It is interesting (although perhaps beyond the scope of this course) to see how this plays out in the situation of Example 13, especially the diagram on page 90. We have $f(x)=x^2+x+223$, so $f'(x)=2x+1$. First look at the node 13 in the mod 27 level. We have $f'(13)=27$, so $\kappa=3$ there. So Hensel's lemma can't be applied unless we have solutions modulo $3^7=2187$. (We can't even count on κ being constant on this subtree, and in fact going up to the next level, $f'(40)=81$, so $\kappa=4$ there. But in any case, the presence of dead ends above this node is not surprising.)

At the other two nodes on the mod 27 level, we have $f'(4)=9$ and $f'(22)=45$, so $\kappa=2$ at both of them. Also, if $x\equiv y \pmod{27}$ then $f'(x)\equiv f'(y) \pmod{27}$, so $\kappa=2$ everywhere in the tree above each of those two nodes.

When $\kappa=2$, we need $j\ge 5$, so we can only apply Hensel's lemma at the modulus 243 level and above. But why are there dead ends when going up to 729?

Let's look at what happens at the node $a\equiv 4 \pmod{243}$. Here $j=5$ and $\tau=2$. Let $a=4$. We have $f(4)=243$ and $f'(4)=9$, so we obtain t by solving the congruence $t\equiv -1 \pmod 3$. Taking $t=-1$ gives $b=a+tp^{j-\tau}=4-3^3=-23$. Then $f(b)=729=3^6$, and $6=2j-2\tau$, as expected. To express the residue -23 as a positive number, we have $729-23=706$. This lies above 220 at the 243 level, which in turn lies above 58 at the 81 level. Or, we could have taken $t=2$ to get $4+2\cdot 3^3=58$, which of course lies over 58 at the 243 level. In fact, different choices of t in that same congruence class mod 3 can give any of the nine congruence classes modulo 729 on the left half of the diagram.

So the upshot of this example is that it's better to look at solutions modulo $p^{j-\tau}$ instead of mod p^j. To do that, consider what happens when we let $k=j-\tau$ and restate Hensel's lemma using k and τ instead of j and τ.

Theorem (Hensel's lemma, new general version). *Let $f\in\mathbb{Z}[x]$, let p be a prime, and let $a\in\mathbb{Z}$. Let τ be such that $p^\tau \parallel f'(a)$, and assume that $f(a)\equiv 0 \pmod{p^{k+\tau}}$ for some $k\ge\tau+1$. Then:*

(a). *there is an integer t, unique modulo $p^{k-\tau}$, such that $f(a+tp^k)\equiv 0 \pmod{p^{2k}}$, and moreover t is the (unique) solution to the congruence*

$$\frac{f'(a)}{p^\tau}t\equiv -\frac{f(a)}{p^{k+\tau}} \pmod{p^{k-\tau}}\;;$$

(b). *if $b\equiv a \pmod{p^k}$, then $f(b)\equiv f(a) \pmod{p^{k+\tau}}$; and*

(c). *if $b\equiv a \pmod{p^k}$, then $p^\tau \parallel f'(b)$.*

Corollary. *Let $f\in\mathbb{Z}[x]$, let p be a prime, and let $a\in\mathbb{Z}$. Let τ be such that $p^\tau\parallel f'(a)$, and assume that $f(a)\equiv 0 \pmod{p^{k+\tau}}$ for some $k\ge\tau+1$. Then, for any $\alpha\ge k$ there is an integer b, unique modulo p^α, such that $b\equiv a \pmod{p^k}$ and $f(b)\equiv 0 \pmod{p^{\alpha+\tau}}$.*