A brief note on Hensel’s lemma: it’s statement and examples

In class we proved

**Theorem** (Hensel’s lemma). Let \( p \) be a prime, \( k \geq 2 \) an integer, and \( f(x) \) a polynomial with integer coefficients. Suppose \( r \) is an (integer) solution to the congruence \( f(x) \equiv 0 \pmod{p^{k-1}} \). Then there are three possible cases for the system of congruences

\[
\begin{cases}
  f(x) & \equiv 0 \pmod{p^k} \\
  x & \equiv r \pmod{p^{k-1}}.
\end{cases}
\]  

(\(^*\))

The cases are:

(i) \( f'(r) \not\equiv 0 \pmod{p} \). In this case, there is a unique solution \( s \) modulo \( p^k \) to \((\ast)\). Moreover, we can find \( s \) by letting

\[
s = r + tp^{k-1}
\]

with \( 0 \leq t < p \) such that

\[
t \equiv \frac{f'(r)f(r)}{p^{k-1}} \pmod{p}
\]

where \( f'(r) \) is any inverse of \( f'(r) \) modulo \( p \). Thus the solutions to \((\ast)\) in this case are all integers \( x \) such that

\[
x \equiv s \equiv r - f'(r)f(r) \pmod{49}.
\]

(ii) \( f'(r) \equiv 0 \pmod{p} \) and \( f(r) \equiv 0 \pmod{p^k} \). In this case, there are \( p \) many distinct solutions modulo \( p^k \) to \((\ast)\). In particular, the solutions are all of the form

\[
r + tp^{k-1}
\]

where \( t \) is any integer.

(iii) \( f'(r) \equiv 0 \pmod{p} \) and \( f(r) \not\equiv 0 \pmod{p^k} \). In this case, there are no solutions to \((\ast)\).

Let’s do an example showing how to apply Hensel’s lemma. Let us solve

\[
f(x) = x^2 + 4x + 2 \equiv 0 \pmod{49}.
\]

Since \( 49 = 7^2 \), we first solve the congruence

\[
f(x) \equiv 0 \pmod{7},
\]

since any solution to \( f(x) \equiv 0 \pmod{49} \) must also be a solution to \( f(x) \equiv 0 \pmod{7} \).

By inspection, we find \( x \equiv 1 \pmod{7} \) and \( x \equiv 2 \pmod{7} \) are the solutions to the congruence \( f(x) \equiv 0 \pmod{7} \). We compute

\[
f'(x) = 2x + 4.
\]

In particular, \( f'(1) = 6 \not\equiv 0 \pmod{7} \) and \( f'(2) = 8 \equiv 1 \not\equiv 0 \pmod{7} \). For future reference, we now compute (using either the Euclidean algorithm, or guess and check) that an inverse of \( f'(1) \) modulo \( 7 \) is

\[
\overline{f'(1)} = 6 = 6,
\]

and an inverse of \( f'(2) \) modulo \( 7 \) is

\[
\overline{f'(2)} = 1.
\]

Since \( f'(1) \not\equiv 0 \pmod{7} \), case (i) of Hensel’s lemma applies. It tells us that there is a unique solution (mod 49) to \( f(x) \equiv 0 \pmod{49} \) that is congruent to 1 mod 7. In fact, the solution is

\[
x \equiv 1 - \overline{f'(1)}f(1) \equiv 1 - 6 \cdot 7 \equiv -41 \equiv 8 \pmod{49}.
\]
Just to be sure, we might double check: surely $8 \equiv 1 \mod 7$, and also

$$f(8) = 8^2 + 4 \cdot 8 + 2 = 64 + 32 + 2 = 98 \equiv 0 \mod 49.$$ 

So $x \equiv 8$ is one solution to $f(x) \equiv 0 \mod 49$.

By the same reasoning as before, since $f'(2) \not\equiv 0 \mod 7$, case (i) of Hensel’s lemma tells us there is a unique solution (mod 49) to $f(x) \equiv 0 \mod 49$ that is congruent to 2 mod 7, and this solution is

$$x \equiv 2 - \frac{f'(2)f(2)}{f'(2)} \equiv 2 - 1 \cdot 14 \equiv -12 \equiv 37 \mod 49.$$ 

Since any solution to $f(x) \equiv 0 \mod 49$ has to come from a solution to $f(x) \equiv 0 \mod 7$ in the manner of Hensel’s lemma, we conclude that the solutions are

$$x \equiv 8 \mod 49 \text{ and } x \equiv 37 \mod 49.$$