Hensel's Lemma

Complete rings satisfy a nice analytic property, similar to Newton's Method, called Hensel's lemma, which we will state but not prove, and then use it to work through some examples.

Motivation: In the p-adics, congruences are approximations: if $a \equiv b \mod p^n$, then they agree in their first n entries. The higher the n, the closer they are.

For example, $5 \equiv 1^2 \pmod 2$, $5 \equiv 1^2 \pmod{2^2}$, but $5 \not\equiv 1^2 \pmod 8$, and in fact, 5 is not a square in $\mathbb{Z}/2\mathbb{Z}$. Thus, 5 is not a perfect square in $\mathbb{Z}_5$, even though we can "approximate" its root up to a certain order.

Now consider $7 \in \mathbb{Z}_3$. Notice that

$$7 \equiv 1^2 \pmod 3$$
$$7 \equiv (1+3)^2 \pmod{3^2}$$
$$7 \equiv (1+3+3^2)^2 \pmod{3^3}$$

And, in fact, in this case we can continue indefinitely.

Hensel's lemma tells us when the root of a polynomial mod p can be lifted to a root in $\mathbb{Z}_p$.

e.g. we saw that $f(x) = x^2 - 5$ has no root in $\mathbb{Z}_2$.

We first state the $\mathbb{Z}_p$ version and then the more general version.

Hensel's Lemma, version 1: If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfies

$$f(a) \equiv 0 \pmod{p}, \quad f'(a) \not\equiv 0 \pmod{p}$$

then there is a unique $b \in \mathbb{Z}_p$ s.t. $f(b) = 0$ and $a \equiv b \pmod{p}$.

Ex: In the case of $f(x) = x^2 - 5$ in $\mathbb{Z}_2$, $f'(x) = 2x \equiv 0 \pmod{p}$ $\forall x$, so we can't find a square root this way.

However, in $\mathbb{Z}_3$, if $f(x) = x^2 - 7$, then $f(1) \equiv 0 \pmod{3}$, and $f'(1) = 2$, which is not 0 mod 3, so f has a root in $\mathbb{Z}_3$. In fact $f(2) = 4 - 7 \equiv 0 \pmod{3}$ and $f'(2) = 4$, so f has 2 roots!

In general, we can ask: which elements $c \in \mathbb{Z}_p$ are perfect squares

We can write $c = p^n b$, where $n \geq 0$, and $p \nmid b$. Then c is a square iff n is even and b is a square.

Consider the polynomial $f(x) = x^2 - b \in \mathbb{Z}_p[x]$. It's derivative is $2x$.

If $p \neq 2$. Then if b is a square mod p, say $b \equiv a^2 \pmod{p}$, then let $\bar{a}$ and $\bar{b}$ be the images in $\mathbb{Z}/p\mathbb{Z}$ and we get $\bar{a}^2 = \bar{b} \pmod{p}$.

$\bar{b} \neq 0$, so $\bar{2}\bar{a} \neq 0$.

Thus, we conclude that $c=p^n b$ has a root in $\mathbb{Z}_p$ $(p \neq 2)$ iff b is a square mod p.

If $p=2$, we can't apply this version of Hensel's Lemma. Here's a generalization.

Hensel's Lemma (more general version): Let R be a ring that is complete with respect to the ideal m, and let $f(x) \in R[x]$ be a polynomial with approximate root a, in the sense that

$$f(a) \in f'(a)^2 m.$$

Then there is a root b of f "near" a in the sense that

$$f(b)=0 \quad \text{and} \quad b-a \in f'(a)m.$$

If $f'(a)$ is a nonzero divisor in R, then b is unique.

Ex: Back to the case of $c=2^n b$, b odd.

If b is a square then

$$b=(1+2k)^2 = 1+4k+4k^2 = 1+4\underbrace{(k+k^2)}_{\text{even}} \Rightarrow b \equiv 1 \pmod 8$$

If $f(x)=x^2-b$, then $f'(x)=2x$, so $f'(a)^2 m = (8a)$, for any a.

Then take $a=1 \implies a^2-b \equiv 0 \pmod 8$, so Hensel's lemma says b has a 2-adic square root.