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 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.

e.g. $5 \equiv 1^2 \pmod 2$, $5 \equiv 1^2 \pmod{2^2}$, but $5 \not\equiv 1^2 \pmod{2^3}$.
5 is not a square at all mod 8, and thus is not a square in $\mathbb{Z}_2$, even though we can "approximate" its root to a certain order.

Consider $7 \in \mathbb{Z}_3$. Notice:

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

In this case, we can continue indefinitely, so 7 is a perfect square in $\mathbb{Z}_p$. In other words, $x^2 - 7$ has a root.

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

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

1. $f(a) \equiv 0 \pmod{p}$, and
2. $f'(a) \not\equiv 0 \pmod{p}$

Then there is a unique $b \in \mathbb{Z}_p$ such that $f(b) = 0$ and $a \equiv b \pmod{p}$.

Ex: $f(x) = x^2 - \alpha$ in $\mathbb{Z}_2[x]$ fails the second hypothesis $\forall \alpha$:

$$f'(x) = 2x \equiv 0 \pmod{p}.$$

So we can't use Hensel's Lemma to find square roots in $\mathbb{Z}_2$.

However, in $\mathbb{Z}_3$, if $f(x) = x^2 - 7$, then $f(1) \equiv 0 \pmod{3}$, and $f'(1) = 2 \not\equiv 0 \pmod{3}$. Thus, 1 lifts to a root in $\mathbb{Z}_3$.

Also, $f(2) = 4 - 7 \equiv 0 \pmod{3}$ and $f'(2) = 4 \not\equiv 0 \pmod{3}$, so 2 lifts to a root as well.

More generally, we can ask: which elements $c \in \mathbb{Z}_p$ are perfect squares?

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

Consider $f(x) = x^2 - b \in \mathbb{Z}_p[x]$.

If $p \neq 2$, suppose b is a square mod p, say

$$b \equiv a^2 \pmod{p},$$

then let $\bar{a}, \bar{b} \in \mathbb{Z}/p\mathbb{Z}$ and we get $\bar{a}^2 = \bar{b}$. $\bar{b} \neq 0$, so $\bar{a} \neq 0$, so $\overline{2a} \neq 0 \Rightarrow f'(a) \not\equiv 0 \pmod{p}$. Thus, Hensel's lemma implies $\bar{a}$ lifts to a root of f in $\mathbb{Z}_p$.

Thus, we conclude that $c = p^n b$ has a root in $\mathbb{Z}_p$ $(p \neq 2)$ iff $n \geq 0$ is even and b is a square mod p.

For the $p=2$ case, we need a more general version of Hensel's Lemma.

__Hensel's Lemma, version 2__: Let R be a ring that is complete with respect to an ideal I. Let $f(x) \in R[x]$ s.t. $f(a) \in f'(a)^2 I$ for some $a \in R$.

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

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

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

Ex: Back to $\mathbb{Z}_2$, $c = 2^n b$, b not divisible by 2.

If b is a square, then

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

Conversely, assume $b \equiv 1 \pmod 8$. Then set $f(x) = x^2 - b$.
We want to show f has a root.

$\mathbb{Z}_2$ is complete w.r.t. (2), so $f'(a)^2 I = 4a^2(2) = (8a^2)$.

Set $a = 1$. Then $f(1) = 1 - b \equiv 0 \pmod 8$, so

$$f(1) \in f'(1)^2 I = (8).$$

Thus, Hensel's Lemma says there's some α s.t.

$$\alpha^2 = b \quad \text{and} \quad \alpha - 1 \in f'(1) I = (4)$$

Thus, we can summarize our findings as follows:

Cor: Let $c \in \mathbb{Z}_p$ and write $c = p^n b$, b not divisible by p, $n \geq 0$.
Then c is a perfect square if and only if either

1. $p = 2$, n even, and $b \equiv 1 \pmod 8$, or

2. $p \neq 2$, n even, and $b \equiv a^2 \pmod p$ for some a.