We first saw two algorithms to factor univariate polynomials over finite fields. We shall now get into bivariate factoring over finite fields. Before that, we need to look at a very important and powerful tool called Hensel Lifting.

1 Hensel Lifting

The intuition behind Hensel Lifting is the following - you have a function for which you need to find some root. Suppose you have an $x$ very close to a root $x_0$ in the sense that there is a small error. The question is how can you use $x$ and the polynomial to get a closer approximation?

Recall the Newton Raphson Method you might have done in calculus to find roots of certain polynomials. Let us say $f$ is the polynomial and $x_0$ is our first approximation of a root. We would like to get a better approximation. For this, we just set $x_1 = x_0 + \varepsilon$. And by the Taylor Series,

$$ f(x_1) = f(x_0 + \varepsilon) = f(x_0) + \varepsilon f'(x_0) + \frac{\varepsilon^2 f''(x)}{2!} + \cdots $$

Ignoring the quadratic error terms, we want a better approximation. Thus, in a sense, we would want $f(x_1)$ to be very close to 0. To find the right $\varepsilon$ that would to the trick, we just set $f(x_1) = 0$ and solve for $\varepsilon$. With just some term shuffling, we get

$$ \varepsilon = -\frac{f(x_0)}{f'(x_0)} \implies x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} $$

But one crucial property we need here is that $f'(x_0)$ is not zero for otherwise division doesn’t make sense. In the same spirit, we shall look at version 1 of the Hensel Lifting.
1.1 Hensel Lifting: Version 1

**Theorem 1.** Let \( p \) be a prime and \( c \) and positive integer, and let \( f \) any polynomial. Suppose we have a solution \( x \) that satisfies

\[
f(x) = 0 \mod p^c, \quad f'(x) \neq 0 \mod p
\]

then we can “lift” \( x \) to a better solution \( x^* \) that satisfies

\[
f(x^*) = 0 \mod p^{2c}, \quad x^* = x \mod p^c
\]

It is of course clear that if \( f(x^*) = 0 \mod p^{2c} \) then \( f(x^*) = 0 \mod p^c \) but the converse needn’t be true. Therefore, \( x^* \) is a more accurate root of \( f \). The proof of this is entirely like the proof of the Newton Rhapson Method.

**Proof.** Set \( x^* = x + hp^c \). We need to find out what \( h \) is. Just as in newton rhapson,

\[
f(x^*) = f(x + hp^c) = f(h) + hp^c f'(x) + (hp^c)^2 \frac{f''(x)}{2!} + \cdots
\]

\[
= f(h) + hp^c f'(x) + O((hp^c)^2)
\]

\[
= f(h) + hp^c f'(x) \mod p^{2c}
\]

Since we want \( f(x^*) = 0 \mod p^{2c} \), we just set the LHS as zero and we get

\[
h = \frac{f(x)}{p^c f'(x)}
\]

Note that \( f(x) = 0 \mod p^c \) and therefore it makes sense to divide \( f(x) \) by \( p^c \). Thus our \( x^* = x + hp^c \) where \( h \) is defined as above and by definition \( x^* = x \mod p^c \).

Another point to note here is that since \( x^* = x \mod p^c, f(x^*) \neq 0 \mod p \) as well. Therefore, we could lift even further. And since the accuracy doubles each time, starting with \( f(x) = 0 \mod p \), \( i \) lifts will take us to an \( x^* \) such that \( f(x^*) = 0 \mod p^{2^i} \).

Hensel Lifting allows us to get very good approximations to roots of polynomials. The more general version of Hensel Lifting plays a very central role in Bivariate Polynomial Factoring.
1.2 Hensel Lifting: Version 2

In the first version of the Hensel Lifting, we wanted to find a root of $f$. Finding an $\alpha$ such that $f(\alpha) = 0 \mod p$ is as good as saying that we find a factorization $f(x) = (x - \alpha)g(x) \mod p$. And also, the additional constraint that $f'(\alpha) \neq 0 \mod p$ is just saying that $\alpha$ is not a repeated root of $f$ or in other words $(x - \alpha)$ does not divide $g$. With this in mind, we can give the more general version of the Hensel Lifting.

**Theorem 2.** Let $R$ be a UFD and $a$ any ideal of $R$. Suppose we have a factorization $f = gh \mod a$ with the additional property that there exists $s, t \in R$ such that $sg + th = 1 \mod a$. Then, we can lift this factorization to construct $g^*, h^*, s^*, t^*$ such that

\[
\begin{align*}
g^* &= g \mod a \\
h^* &= h \mod a \\
f &= g^*h^* \mod a^2 \\
s^*g^* + t^*h^* &= 1 \mod a^2
\end{align*}
\]

Further, for any other $g', h'$ that satisfy the above four properties, there exists a $u \in a$ such that

\[
\begin{align*}
g' &= g^*(1 + u) \mod a^2 \\
h' &= h^*(1 - u) \mod a^2
\end{align*}
\]

Therefore, the lifted factorization in some sense is unique.

**Proof.** (sketch) Set $g^* = g + te$ and $h^* = h + se$. Now solve for $e$ and that should do it. Finding $s^*, t^*$ is also similar. (painful!) \qed

Here is a more natural way is to look at this. What we want is a solution to the curve $XY = f$ where $f$ is the function we want to factorize. Let us call $F(X, Y) = f - XY$. We have $X, Y$ as solutions such that $F(X, Y) = f - XY = e$. Now

\[
F(X + \Delta X, Y + \Delta Y) = f - (X + \Delta X)(Y + \Delta Y)
\]

\[
= f - XY - (X\Delta Y + Y\Delta X) + O(\Delta^2)
\]

\[
= F(X, Y) - (X\Delta Y + Y\Delta X)
\]

\[
= e - (X\Delta Y + Y\Delta X)
\]

Further, we also know that $sX + tY = 1$ and therefore, if we just set $\Delta X = se$ and $\Delta Y = te$, we have

\[
F(X + \Delta X, Y + \Delta Y) = e - e(sX + tY) = 0 \mod \Delta^2
\]
One should also be able to look at the lifts of $s$ and $t$ as solving appropriate equations. In the next class, we shall look at this technique put to use in Bivariate Factorization.