MATH8510
Lecture 9 Notes

Charlie Conneen

September 12, 2022

Hensel's Lemma

Recall. If $q(X) \in R[X]$, where R is any ring, then

$$q(X+Y) = q(X) + Yq'(X) + Y^2\widetilde{q}(X,Y),$$

where $\widetilde{q}(X,Y)$ was defined last lecture.

We also had the following corollary:

Corollary. *Let $q(X) \in \mathbb{Z}_p[X]$.*

a. If $c \in \mathbb{Z}_p$, then either $q(c+p\mathbb{Z}_p) \subseteq p\mathbb{Z}_p$ or $q(c+p\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times$.

b. If $c \in \mathbb{Z}_p$ satisfies $q'(c) \in \mathbb{Z}_p^\times$, then there is at most one $x \in c+p\mathbb{Z}_p$ such that $q(x) = 0$.

Theorem (Hensel's Lemma)**.** *Suppose $F(X) \in \mathbb{Z}_p[X]$. If there exists some $\alpha_0 \in \mathbb{Z}_p$ such that $|F(\alpha_0)|_p < 1$ and $|F(\alpha_0)|_p = 1$, then the sequence $(\alpha_n)_n$ given by*

$$\alpha_{n+1} = \alpha_n - \frac{F(\alpha_n)}{F'(\alpha_n)}$$

for all $n \geq 0$ exists, and the sequence converges in $\mathbb{Z}_p$. Moreover, $\alpha := \lim_{n\to\infty} \alpha_n$ is the unique element of $\alpha_0 + p\mathbb{Z}_p$ such that $F(\alpha) = 0$.

Remark. Hensel's lemma is effectively the p-adic version of Newton's method. However, Newton's method can fail in $\mathbb{R}$: take for example $f(x) = x^3 - x$ and the guess $\alpha_0 = \frac{1}{\sqrt{5}}$. So Hensel's lemma says that this process of approximation will always work under some fairly mild conditions.

Proof. Suppose $F(X) \in \mathbb{Z}_p[X]$ admits some α_0 such that $|F(\alpha_0)|_p < 1$ and $|F'(\alpha_0)|_p = 1$. We show by induction that the sequence exists and satisfies

i. $|F(\alpha_n)| \leq p^{-2^n}$;

ii. $|F'(\alpha_n)|_p = 1$; and consequently,

iii. $|\alpha_{n+1} - \alpha_n|_p \leq p^{-2^n}$.

For the case $n = 0$, both (i) and (ii) are given, and $\alpha_1 = \alpha_0 - \frac{F(\alpha_0)}{F'(\alpha_0)}$ exists in $\mathbb{Z}_p$ with $|\alpha_1 - \alpha_0|_p \leq p^{-1} = p^{-2^0}$, so we have (iii).

Now suppose for some $n \geq 0$, α_{n+1} exists in $\mathbb{Z}_p$ and all three of the above conditions hold. Then

$$F(\alpha_{n+1}) = F(\alpha_n) - \frac{F(\alpha_n)}{F'(\alpha_n)} = F(\alpha_n) - \frac{F(\alpha_n)}{F'(\alpha_n)} \cdot F'(\alpha_n) + \left(\frac{-F(\alpha_n)}{F'(\alpha_n)}\right)^2 z$$

for some $z \in \mathbb{Z}_p$. Thus

$$|F(\alpha_{n+1})|_p \leq \left|\frac{-F(\alpha_n)}{F'(\alpha_n)}\right|_p^2 \leq \left(p^{-2^n}\right)^2 = p^{-2^{n+1}}.$$

So (i) holds.

Since (ii) and (iii) hold for n, we know that $F'(\alpha_n) \in \mathbb{Z}_p^\times$, and that $\alpha_{n+1} \in \alpha_n + p\mathbb{Z}_p$. So by part (a) of the Corollary above, $F'(\alpha_{n+1}) \in \mathbb{Z}_p^\times$, so (ii) holds for $n+1$. Hence

$$\alpha_{(n+1)+1} = \alpha_{n+1} - \frac{F(\alpha_{n+1})}{F'(\alpha_{n+1})}$$

exists in $\mathbb{Z}_p$ and $|\alpha_{n+2} - \alpha_{n+1}|_p \leq p^{-2^{n+1}}$. So (iii) holds for $n+1$.

Putting all of these properties together, we see that $(\alpha_n)_n$ is a Cauchy sequence in $\mathbb{Z}_p$ by (iii), so the limit $\alpha \coloneqq \lim_{n\to\infty} \alpha_n$ exists by completeness of $\mathbb{Z}_p$. Furthermore, by continuity of F (polynomials are continuous since $\mathbb{Z}_p$ is a topological ring), we have

$$F(\alpha) = F\left(\lim_{n\to\infty} \alpha_n\right) = \lim_{n\to\infty} F(\alpha_n) = 0,$$

so α is a root of F. Lastly, for each $n \in \mathbb{N}$, we have

$$|\alpha_{n+1} - \alpha_0|_p \leq \max\left\{ |\alpha_{k+1} - \alpha_k|_p \mid 0 \leq k \leq n \right\} \leq p^{-1}$$

by the strong triangle inequality. So $|\alpha - \alpha_0|_p \leq p^{-1} < 1$. So $\alpha \in \alpha_0 + p\mathbb{Z}_p$, and α is the *unique* root in this coset by part (b) of the Corollary. ■