3.1 Keeping the ball rolling

Last time, gave a new definition $\mathbb{Q}_p$, as the completion of $\mathbb{Q}$ with respect to the absolute value $|\cdot|_p$. So $\mathbb{Q}_p$ was the set of equivalence classes of Cauchy sequences $(x_n)_{n\in\mathbb{N}}$ of rational numbers, where two Cauchy sequences are equivalent if their difference converges to 0 in norm.

The completion $\mathbb{Q}_p$ is equipped with addition and multiplication where the sum and product of two elements is given by the elementwise sum and product of Cauchy sequences representing them (you can check that the sum or product of Cauchy sequences is again a Cauchy sequence, and that replacing a Cauchy sequence by an equivalent one would not change the sum and product). These operations extend addition and multiplication on $\mathbb{Q}$. Note that, with this definition of $\mathbb{Q}_p$, it is much quicker to show that $\mathbb{Q}_p$ is a field, simply by taking elementwise differences and quotients of Cauchy sequences. We can further equip $\mathbb{Q}_p$ with a norm.

The absolute value of an element of the completion, so an absolute value of a Cauchy sequence, is defined as

$$|(x_n)_{n\in\mathbb{N}}| := \lim_{n\to\infty} |x_n|$$

When completing $\mathbb{Q}$ with respect to $|\cdot|_\infty$, we obtain the norm on $\mathbb{R}$. When completing $\mathbb{Q}$ with respect to $|\cdot|_p$, we obtain a norm on $\mathbb{Q}_p$ that extends the p-adic norm on $\mathbb{Q}$ and is again nonarchemidean.

For example, for $|\cdot|_\infty$, $-\sqrt{2}$ can be defined as the limit of the sequence

$$-1, -1.4, -1.41, -1.414, -1.4142, ...$$

so $|-\sqrt{2}|_\infty$ is the limit of the sequence

$$|-1|_\infty, |-1.4|_\infty, |-1.41|_\infty, |-1.414|_\infty, |-1.4142|_\infty, ...$$

which is the real number $\sqrt{2}$.

In lecture 1, we computed a square root of 2 in $\mathbb{Q}_7$ with a 3 in the "ones" position. We calculate its absolute value:

$$\begin{aligned} |3 + 1\cdot 7 + 2\cdot 7^2 + 6\cdot 7^3 + ...|_7 &= \lim(|3|_7, |3+1\cdot 7|_7, |3+1\cdot 7+2\cdot 7^2+6\cdot 7^3|_7, ...) \\ &= \lim(1,1,1,...) \\ &= 1. \end{aligned}$$

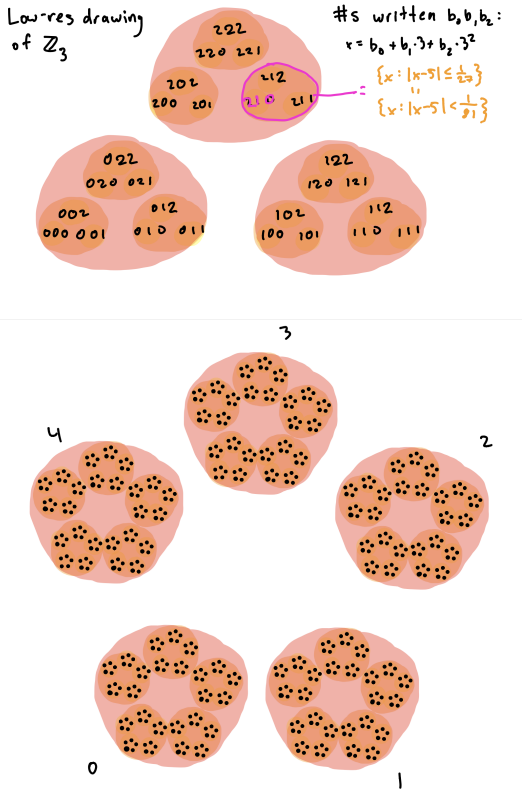
We have only seen a limited type of number occur as p-adic absolute values. Indeed, the way we defined $|\cdot|_p$ on $\mathbb{Q}$, the only possible absolute values of rational numbers were 0

or p^n for $n \in \mathbb{Z}$. And if $r \in \mathbb{R}_{>0}$ is not a power of p, then there exists $i \in \mathbb{Z}$ such that $p^i < r < p^{i+1}$ and hence r cannot occur as a limit of p-adic absolute values of elements of $\mathbb{Q}$. This can be summed up as follows:

Proposition 3.1

$$\{|x|_p : x \in \mathbb{Q}_p\} = \{p^n : n \in \mathbb{Z}\} \cup \{0\}$$

This immediately gives a result in the case of $\mathbb{Q}_p$ that we noted more generally for nonarchemidean fields in the previous lecture, which is that open balls are closed sets and closed balls are open sets. It even shows that, in $\mathbb{Q}_p$, open balls are closed balls, since $B(x, p^n) = B_{cl}(x, p^{n-1})$ for all $n \in \mathbb{Z}$.
For example, as in the picture from last lecture, the elements we identified as being in a closed ball of radius 1/9 around 1 are in an open ball of radius 1/3 around 1.



We'll begin exploring algebraic characterizations of these balls. To begin with, we'll give a new definition of $\mathbb{Z}_p$, as a ball. We recall that since $|\cdot|_p$ is nonarchimedean, $|n|_p \le 1$ for

all $n \in \mathbb{Z}$. We extend this as follows:

Definition 3.2

$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$

Here are some examples of elements of $\mathbb{Z}_p$ under this definition: n for all $n \in \mathbb{Z}$, $\sqrt{2}$ when $p = 7$, $1/3$ when $p = 5$, $\sqrt{-1}$ when $p = 7$ (these follow from calculations in lecture 1). Something which is **not** in $\mathbb{Z}_p$ is $1/p$, which has absolute value $p > 1$.

3.2 Wearing many hats

We will now unveil $\mathbb{Q}_p$ (defined as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$) as the very same field we defined in lecture 1!

First we will prove some interesting topological facts about about $\mathbb{Q}_p$, which will lead to our result.

Theorem 3.3

i) $\mathbb{Q}$ is dense in $\mathbb{Q}_p$

ii) $\mathbb{Z}$ is dense in $\mathbb{Z}_p$

iii) Every element in $\mathbb{Z}_p$ can be written **uniquely** in the form

$$b_0 + b_1 p + b_2 p^2 + ...$$

with $b_i \in \{0, 1, ..., p-1\}$, and every such series $b_0 + b_1 p + b_2 p^2 + ...$ with $b_i \in \{0, 1, ..., p-1\}$ represents an element of $\mathbb{Z}_p$.

iv) Every element in $\mathbb{Q}_p$ can be written **uniquely** in the form

$$b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + ...$$

for some $n_0 \in \mathbb{Z}$ and $b_i \in \{0, 1, ..., p-1\}$, and every such series $b_{n_0} p^{n_0} + b_{n_0+1} p^{n_0+1} + ...$ for some $n_0 \in \mathbb{Z}$ and $b_i \in \{0, 1, ..., p-1\}$ represents an element of $\mathbb{Q}_p$.

Proof: i) $\mathbb{Q}$ embeds inside $\mathbb{Q}_p$ by mapping $a \in \mathbb{Q}$ to the constant Cauchy sequence $(a, a, a, a, \dots)$. Different elements of $\mathbb{Q}$ map to different elements of $\mathbb{Q}_p$ since the distance

between them is a positive constant.
Now suppose $x \in \mathbb{Q}_p$. Let (x_n) be a Cauchy sequence in $\mathbb{Q}$ representing x and let $\epsilon > 0$. We wish to exhibit some $a \in \mathbb{Q}$ such that $|x - a|_p < \epsilon$. Recall that $|x - a|_p$ is the limit of $|x_n - a|_p$. Since (x_n) is Cauchy, we can choose N such that $|x_n - x_m|_p < \epsilon$ for $n, m \geq N$. Then $a = x_N$ does the job.

ii) Exercise.

iii) Let $x \in \mathbb{Z}_p$ and let $n \geq 0$. By ii), there exists $a \in \mathbb{Z}$ such that $|x - a|_p \leq p^{-(n+1)}$. In fact, we claim that there is a unique such choice of a mod p^n. Indeed, given $b \in \mathbb{Z}$ we note that $|x - a + b|_p \leq p^{-n}$ if and only if $|b|_p \leq p^{-(n+1)}$ if and only if $p^(n+1)|b$, using the nonarchemidean property. So we let a_n be the unique integer such that $|x - a_n|_p \leq p^{-(n+1)}$ and $0 \leq a_n < p^{n+1}$.

Then $\lim_{n\to\infty} a_n = x$, and the decompositions $a_n = \sum_{i=0}^{n} b_i p^i$ are *coherent*, thus representing in the limit the infinite series $\sum_{i=0}^{\infty} b_i p^i$ for some sequence $b_i \in \{0, \ldots, p-1\}$.

iv) Let $x \in \mathbb{Q}_p$. As we've noted $|x|_p = p^n$ for some $n \in \mathbb{Z}$, so $p^{-n}x \in \mathbb{Z}_p$, and the result follows from iii). □

We note some interesting differences with the reals here: $\mathbb{Z}$ is not dense in any open subset of the reals, and some real numbers have multiple decimal representations ($1 = .9999..$ for example), which doesn't happen for the p-adics.

We can make a connection between the series expansion for a p-adic number and its absolute value:

Proposition 3.4

For $x \in \mathbb{Q}_p$ of the form $x = \sum_{i=n_0}^{\infty} b_i p^i$ with $b_{n_0} \neq 0$ (so n_0 is the lowest power of p with a nonzero coefficient), $|x|_p = p^{-n_0}$.

Proof: we use induction and the "all triangles are isosceles" equality from last lecture.

$$\begin{aligned} |b_{n_0}p^{n_0} + b_{n_0+1}p^{n_0+1} + ... + b_k p^k|_p &= \max\{|b_{n_0}p^{n_0}|_p, |b_{n_0+1}p^{n_0+1} + ... + b_k p^k|_p\} \\ &= \max\{p^{-n_0}, p^{-n_0-1}\} \\ &= p^{-n_0}. \end{aligned}$$

So

$$|x|_p = \lim_k |b_{n_0}p^{n_0} + b_{n_0+1}p^{n_0+1} + ... + b_k p^k|_p = p^{-n_0}.$$

□

Examples: $|2 \cdot 3^{-2} + 3^{-1} + 0 + 1 \cdot 3^1 + ...|_3 = 3^2$, $|4 \cdot 5^3 + 2 \cdot 5^4 + 3 \cdot 5^5 + ...|_5 = 5^{-3}$.

3.3 A more algebraic viewpoint

We now explore the links between the algebra and topology of $\mathbb{Z}_p$ and $\mathbb{Q}_p$.

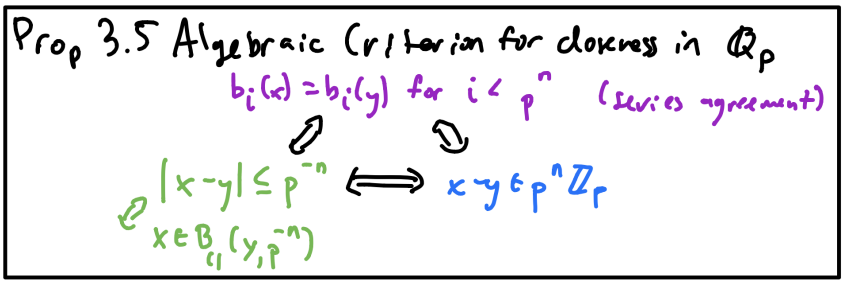
For $n \in \mathbb{Z}$, let $p^n\mathbb{Z}_p := \{x \in \mathbb{Q}_p : x = p^n \cdot y \text{ for some } y \in \mathbb{Z}_p\}$. Note that when $n \in \mathbb{N}$, this is a subset of $\mathbb{Z}_p$; indeed, it is an **ideal** of $\mathbb{Z}_p$: that is, it's closed under addition as well as multiplication by elements of $\mathbb{Z}_p$.

By Proposition 3.2, we see that $p^n\mathbb{Z}_p$ is the closed ball around 0 of radius p^{-n}. In fact, every ideal of $\mathbb{Z}_p$ is of this form, so ideals are balls! (this is an exercise in this week's problem set).

Similarly, we can conclude that an element $x \in \mathbb{Z}_p$ is in the same closed ball of radius p^n as an element y if and only if $x - y \in p\mathbb{Z}_p$. So this gives an algebraic criterion for when two elements of $\mathbb{Q}_p$ are within a specified distance of each other, which we sum up as follows:

Proposition 3.5

For $x, y \in \mathbb{Q}_p$, $|x - y| \leq p^{-n}$ if and only if $x - y \in p^n\mathbb{Z}_p$.



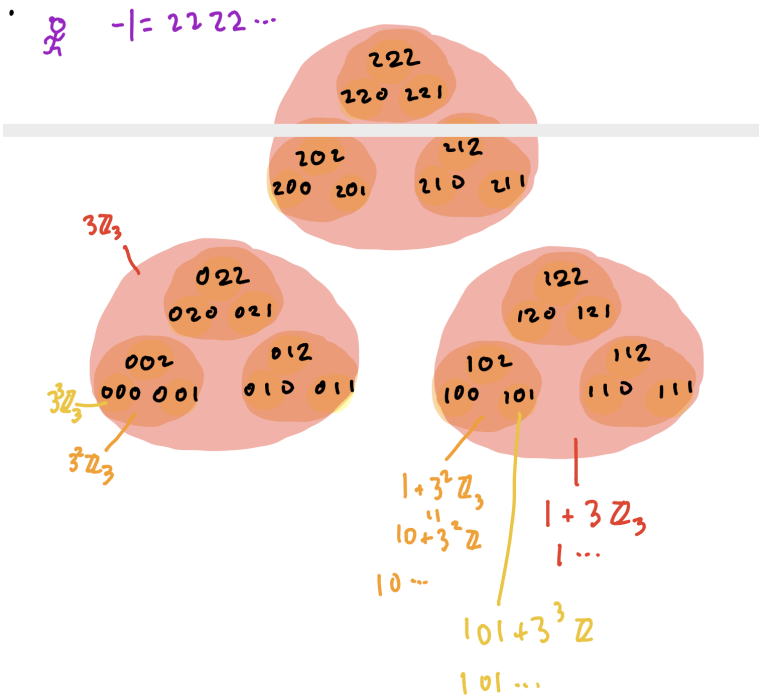
For example, in $\mathbb{Q}_7$, we found a square root of 2 in lecture 1: $3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + ...$, and this is in $(3 + 1 \cdot 7 + 2 \cdot 7^2) + 7^3\mathbb{Z}_p$.

Our proof of Theorem 3.3.iii) showed the following:

Proposition 3.6 Balls are cosets

Let $n \in \mathbb{N}$. Then

$$\mathbb{Z}_p = \bigsqcup_{a=0}^{p^n-1} B_{cl}(a, p^{-n}) = \bigsqcup_{a=0}^{p^n-1} (a + p^n\mathbb{Z}_p)$$



This gives us a map $\pi_n : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ sending

$$\sum_{i=0}^{\infty} b_i p^i \mapsto \overline{\sum_{i=0}^{n-1} b_i p^i}.$$

This map is surjective; for $\bar{a} \in \mathbb{Z}/p^n\mathbb{Z}$, the preimage of $\bar{a}$ under π_n is the closed ball of radius p^{-n}, or $a + p^n\mathbb{Z}_p$.

It is an exercise to check that that π_n respects addition and multiplication, that it is a homomorphism of rings.

Of course, π_n is not injective for any n, since $\ker \pi_n = p^n\mathbb{Z}_p$. However, any distinct elements of $\mathbb{Z}_p$ map to different elements under π_n **for n large enough**. So if we piece together

compatible elements of $\mathbb{Z}/p^n\mathbb{Z}$ as n ranges over $\mathbb{N}_{>0}$, we can "recover" all of $\mathbb{Z}_p$. We state this precisely by introducing a definition.

Definition 3.7

The **inverse limit** of the system $(\mathbb{Z}/p^n\mathbb{Z})_{n>0}$ is the ring

$$\varprojlim \mathbb{Z}/p^n\mathbb{Z} := \{(\overline{a_i})_{i>0} : \overline{a_i} \in \mathbb{Z}/p\mathbb{Z}^{i+1} \text{ and } \overline{a_i} \equiv \overline{a_{i+1}} \pmod{p^{i+1}}\}$$

where

$$(\overline{a_i})_{i>0} + (\overline{\alpha_i})_{i>0} := (\overline{a_i} + \overline{\alpha_i})_{i>0}$$

and

$$(\overline{a_i})_{i>0} \cdot (\overline{\alpha_i})_{i>0} := (\overline{a_i} \cdot \overline{\alpha_i})_{i>0}$$

You can check that the addition and multiplication operations defined above indeed make the inverse limit into a ring.

Note: an analogous definition realizes power series $k[[x]]$ as the "inverse limit" of the system $k[x]/x, k[x]/x^2, k[x]/x^3, ...$ You can formalize this for yourself!

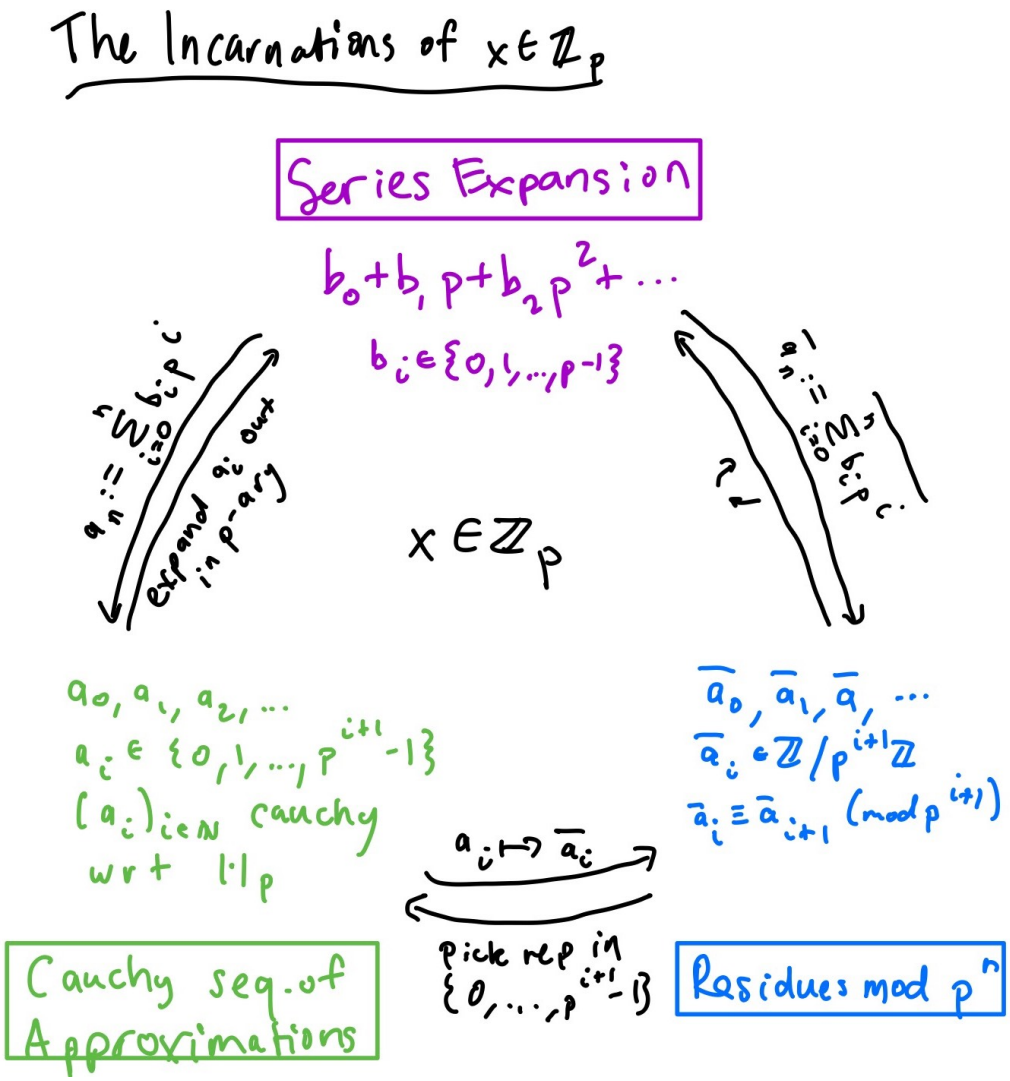
We rephrase the above discussion in the following theorem:

Theorem 3.8

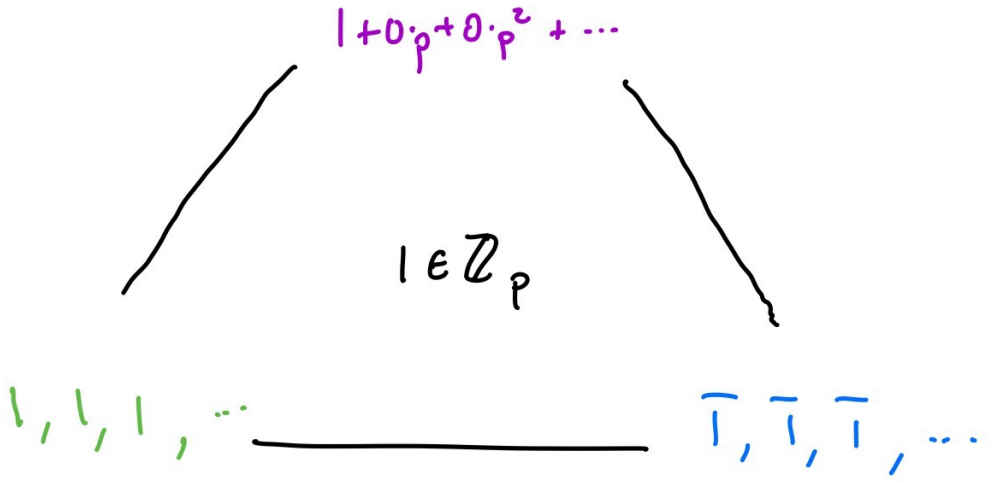
The map $\pi : \mathbb{Z}_p \to \varprojlim \mathbb{Z}/p^n\mathbb{Z}$ defined by $\pi(x) = (\pi_n(x))_n$ is an isomorphism of rings.

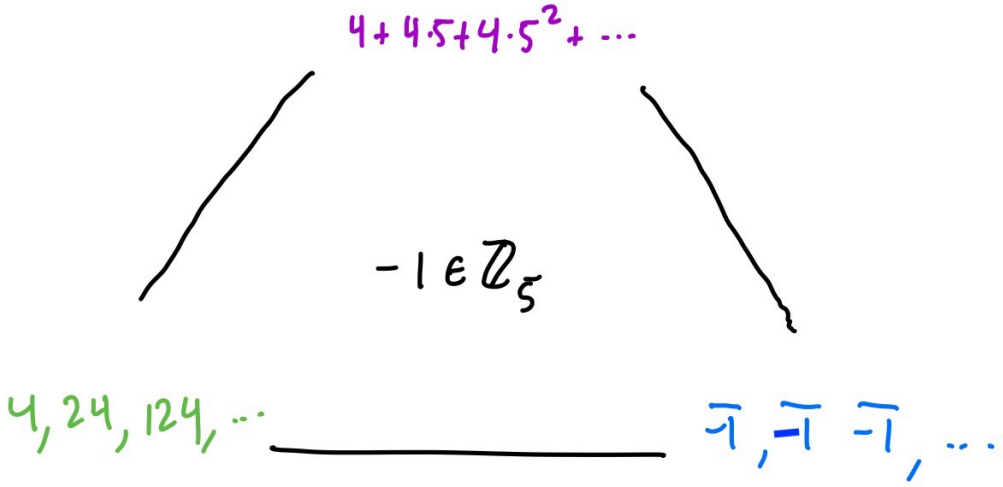
3.4 The Incarnations of $x \in \mathbb{Z}_p$

We have seen three equivalent ways of looking at $\mathbb{Z}_p$, a creature wearing many hats: as series expansions, Cauchy sequences ("increasingly accurate approximations"), and inverse systems of residues mod p^n.



Here are some examples:





We note that, from the perspective of Cauchy sequences as well as from the perspective of inverse limits, addition and multiplication are performed componentwise. However, from the perspective of series expansions, addition and multiplication are *not* performed componentwise, but with carrying.

3.5 Hensel's Lemma

Theorem 3.9 Hensel's Lemma

Let $F(x) = c_0 + c_1x + c_2x^2 + ... + c_mx^m$ be a polynomial with $c_i \in \mathbb{Z}_p$ for all i. Let $F'(x) = c_1 + 2c_2x + 3c_3x^2 + ... + mc_mx^{m-1}$ be the derivative of $F(x)$. Let α_0 be a p-adic integer such that $F(\alpha_0) \equiv 0 \pmod{p\mathbb{Z}_p}$ and $F'(\alpha_0) \not\equiv 0 \pmod{p\mathbb{Z}_p}$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that

$$F(\alpha) = 0 \text{ and } \alpha \equiv \alpha_0 \pmod{p\mathbb{Z}_p}.$$

That is, if we find a root of F mod p which is not a root of F' mod p, we can "lift" it to a root of F in $\mathbb{Z}_p$.

Proof: we will generalize the method we used in the very first lecture to find a square root of 2 in $\mathbb{Z}_7$ (we found better and better approximations of $\sqrt{2}$ as a sequence of integers, adding more and more terms to a sum).

We will show that there is a unique sequence of integers $a_0, a_1, a_2, ...$ such that $a_0 \equiv \alpha_0$ mod $p\mathbb{Z}_p$ and for all $n \geq 0$

1. $F(a_n) \equiv 0 \pmod{p^{n+1}}$
2. $a_{n+1} \equiv a_n \pmod{p^{n+1}}$
3. $0 \leq a_n < p^{n+1}$.

We will denote by $(b_n)_{n\in\mathbb{N}}$ the sequence of integers in $\{0, 1, 2, ..., p-1\}$ such that $a_n = \sum_{i=0}^{n} b_i p^i$.

We proceed by induction on n.

For the base case $n = 0$, we define a_0 to be the constant term of the p-adic expansion of α_0; so a_0 is the unique integer in $0, 1, 2, ..., p-1$ which is congruent to $\alpha_0 \pmod{p\mathbb{Z}_p}$, and as a result, $F(a_0) \equiv 0 \pmod{p\mathbb{Z}_p}$.

Now suppose that $a_n = \sum_{i=0}^{n} b_i p^i$ satisfies the criteria 1,2,3. We will find $b_{n+1} \in \{0, 1, ..., p-1\}$ such that the integer $a_{n+1} := a_n + b_{n+1}p^{n+1}$ satisfies the criteria 1,2,3.

Expanding out the criterion 1 for $n+1$:

$$\begin{aligned} F(a_{n+1}) &= F(a_n + b_{n+1}p^{n+1}) \\ &= \sum_{i=0}^{m} c_i(a_n + b_{n+1}p^{n+1})^i \\ &= \sum_{i=0}^{m} c_i(a_n^i + ia_n^{i-1}b_{n+1}p^{n+1} + \text{ terms divisible by } p^{n+2}) \\ &= F(a_n) + b_{n+1}F'(a_n)p^{n+1} + \text{ terms divisible by } p^{n+2}). \end{aligned}$$

By the inductive hypothesis, there exists $k \in \mathbb{Z}$ such that $F(a_n) = kp^{n+1}$, so we want to find b_{n+1} such that

$$0 \equiv kp^{n+1} + b_{n+1}F'(a_n)p^{n+1} \pmod{p^{n+2}}.$$

This is equivalent to finding $b_{n+1} \in \mathbb{Z}$ such that $-k \equiv b_{n+1}F'(a_n) \pmod{p}$. And since $F'(a_n) \equiv F'(a_n) \not\equiv 0 \pmod{p}$ by induction, so there is an integer which we call $(F'(a_n))^{-1}$ such that $(F'(a_n)) \cdot (F'(a_n))^{-1} \equiv 1 \pmod{p}$. We can then define b_{n+1} to be the unique integer in $\{0, 1, ..., p-1\}$ such that $b_{n+1} \equiv -k \cdot (F'(a_n))^{-1} \pmod{p}$.

We are now equipped to answer a very interesting question: when does an integer n have a square root in $\mathbb{Z}_p$? We saw the answer even in lecture 1 for a couple of n's and p's, but now we can address it more completely.

Let p be an odd prime and let $n \in \mathbb{Z}$ such that $p \nmid n$. Is $\sqrt{n} \in \mathbb{Z}_p$?

We let $F(X) = X^2 - n$, and suppose that there exists $\alpha_0 \in \mathbb{Z}$ such that $\alpha_0^2 \equiv n \pmod{p}$, so $F(\alpha_0) \equiv 0 \pmod{p}$. We see that $F'(\alpha_0) = 2\alpha \not\equiv 0 \pmod{p}$. Then by Hensel's Lemma, there exists $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 = n$, so there is a root! This means that $\sqrt{n} \in \mathbb{Z}_p$ if and only if "n is a quadratic residue mod p."

Theorem 3.10 Hensel's Corollary

let $F(X)$ be a polynomial with coefficients in $\mathbb{Z}_p$ and $f(X)$ the corresponding polynomial over $\mathbb{Z}/p\mathbb{Z}$. Suppose that $f = gh$, where the polynomials g and h are relatively prime. Then there are polynomials G and H with coefficients in $\mathbb{Z}_p$ such that g is the reduction of G mod p and $\deg g = \deg G$, h is the reduction of H mod p and $\deg h = \deg H$, and $F = GH$.

Proof: this is an exercise on your problem sheet for this week.