MATH 3800, INTRO NUMBER THEORY, SPRING 2020

Hensel's Lemma: Supplemental notes

Based on your questions in office hours, here are some more details on a few points. First, let's discuss the terminology "lift". We sometimes use the word lift to describe preimages of functions, which we sometimes also call "maps", especially surjective (or onto) functions. For example, as we just saw in class, there are natural functions $f\colon \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for any $m, n \in \mathbb{N}$. Specifically, you can take an integer mod mn and reduce it mod m and then reduce it mod n. For instance, if $m = 3$ and $n = 7$, then $f(11) = (11 \pmod 3, 11 \pmod 7) = (2 \pmod 3, 4 \pmod 7)$. The Chinese Remainder Theorem (CRT) says that given a pair of congruence classes mod m, n, then if m, n are coprime, there is a unique *lift* to a congruence class mod mn. In this case, the lift of $(2 \pmod 3, 4 \pmod 7)$ is $11 \pmod{21}$, and the CRT gives an algorithm for computing these lifts.

More generally, given any $d|n$, there is a natural map $\pi_{n\to d}\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$ given by reducing a congruence class mod n to one mod d. This basically "throws away" some information. For example $\pi_{21\to 3}\colon \mathbb{Z}/21\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$ takes the class $19 \pmod{21}$ and sends it to $\pi_{21\to 3}(19 \pmod{21}) \equiv 19 \equiv 1 \pmod 3$. More generally, every integer which is $19 \pmod{21}$ is of the form $19 + 21k$, and hence is also of the form $19 + 3 \cdot (7k) \equiv 1 \pmod 3$. A lift of a congruence class mod d is a choice of a preimage under this map. For example, the lifts of $1 \pmod 3$ to $\mathbb{Z}/21\mathbb{Z}$ are $1, 4, 7, 10, 13, 16, 19 \pmod{21}$. Note that the number of lifts is $21/3 = n/d$.

Hensel's Lemma is used in the special case when n, d are prime powers. For instance, if $a \equiv 0 \pmod{p^k}$, then in particular,

$$a \equiv 0 \pmod p, \quad a \equiv 0 \pmod{p^2}, \quad \dots, \quad a \equiv 0 \pmod{p^{k-1}}.$$

Thus, if we solve a congruence modulo p^k, of any type, then it must also reduce to a congruence mod $p^1, p^2, \dots, p^{k-1}$. That is, it must be a lift of solutions mod lower prime powers. Hensel's Lemma gives a way to determine all of the lifts of polynomial congruences mod p^k to solutions mod p^{k+1}.

Let's talk a little more about p-adic numbers now. In the context of Hensel's Lemma, suppose we solve a polynomial equation $f(x) \equiv 0 \pmod{p^k}$, and that $r = r_0$ is a simple root of the equation $f(x) \equiv 0 \pmod p$. Then Hensel's Lemma gives an inductive procedure to build a sequence of integers $r_1, r_2, r_3, \dots$ such that

$$f(r_i) \equiv 0 \pmod{p^i}, \quad i = 1, 2, 3 \dots.$$

That is, in terms of the p-adic norm, we have $f(r_i) = p^i k$ for some $k \in \mathbb{Z}$. If $p \nmid K$, then $|f(r_i)|_p = p^{-i}$. If $p|k$, say $k = p^a$ with $k = p^a \ell$ and $p \nmid \ell$, then $|f(r_i)|_p = |p^{i+a}\ell|_p = p^{-(i+a)} < p^{-i}$. [In this case, we have $f(r_i) \equiv 0 \pmod{p^{i+a}}$ but $f(r_i) \not\equiv 0 \pmod{p^{i+a+1}}$. There will always be some such a, usually 0, but sometimes by coincidence a is positive.] In either case, Hensel's Lemma guarantees precisely that

$$|f(r_i)|_p \leq p^{-i}.$$

In other words, p-adically, we have the limit $f(r_i) \to 0$, and this decay to zero happens exponentially fast. Moreover, we have that each r_i is a lift of r_{i-1} (for example, look at the formula defining r_i in Hensel's Lemma). That is, we have

$$r_i \equiv r_{i+1} \pmod{p^i}.$$

Similarly,

$$r_{i+2} \equiv r_{i+1} \pmod{p^{i+1}},$$

and so

$$r_{i+2} \equiv r_{i+1} \pmod{p^i}.$$

Thus,

$$r_{i+2} \equiv r_{i+1} \equiv r_i \pmod{p^i}.$$

Continuing in this way, we find that all higher r_i terms are congruent to $r_i \pmod{p^i}$:

$$r_i \equiv r_{i+1} \equiv r_{i+2} \equiv \dots \pmod{p^i}.$$

In p-adic language for this sequence of integers, this means that for all $j \in \mathbb{N}$, we have

$$|r_{i+j} - r_i|_p \leq p^{-i}. \tag{1}$$

Thus, the sequence of r_i is not only tending to 0 when plugged into f, but the inputs themselves are getting closer and closer to each other. The "real" definition of the p-adic numbers $\mathbb{Q}_p$ is exactly

this: limits of sequences that get really close together in a manner such as in (1). This is similar to our example before of sequences of rational numbers tending to irrational real numbers obtained by chopping off decimal expansions, for example:

$$3, 3.1, 3.14, 3.141, 3.1415, \ldots \to \pi.$$

Each further decimal place we give yields more refined approximations of π. In p-adic language, more refined approximations are similarly given by congruences mod higher p-powers.

Just like in $\mathbb{R}$, we usually think of $\mathbb{Q}_p$, via *expansions*. We can also write $\mathbb{R}$ as:

$$\mathbb{R} := \left\{ \sum_{i=-\infty}^{N} a_i 10^i \mid N \in \mathbb{N}, a_i \in \{0, 1, 2 \ldots, 9\} \right\}.$$

That is, real numbers are essentially the same thing as sequences of digits which extend finitely far to the left of the decimal place but infinitely far to the right. We don't want to allow arbitrarily high positive powers of 10, as $\lim_{n\to\infty} 10^n = \infty$, and if the decimal expansion terminates, we can consider it to fit in the above definition by saying that the digits a_i are all 0 starting at some point. [To be very specific, the above definition is just slightly off, as two different decimal expansions can give the same real number. However, this only happens in one situation, where you have an example like $0.99999\ldots = 1.00000\ldots$. If one is careful to whenever one obtains an infinite sequence of 9's like this to replace it with another expansion with an infinite sequence of 0's, then the above is a proper definition of $\mathbb{R}$.]

It really is tricky to define what a real number is correctly, however the point is that though this is very technical, we compute with real numbers all the time, and just work with such expansions without worrying about these technicalities. That is, we usually just formally manipulate real numbers via decimal expansions. The payoff is that we can do things like calculus, which don't make sense over $\mathbb{Q}$. We will think of $\mathbb{Q}_p$ in the same way. Its another way of filling in "holes" in $\mathbb{Q}$ to allow calculus to happen, and in fact the only other theory of "calculus" like this which exists extending the rational numbers, and one which reflects number-theoretic information like divisibility and congruences.

So let's discuss how we work with p-adic numbers using expansions. Instead of working base 10, p-adic expansions are in terms of powers of p, and the digits are numbers in $\{0, 1, \ldots, p-1\}$. Unlike in $\mathbb{R}$, where for example 10^{100} is huge, $|p^{100}|_p$ is tiny, while $|p^{-100}|_p$ is huge. So to make these expansions converge, we need there to be only finitely many negative powers of p, but allow infinitely many positive powers. We write things then in terms of powers of p^{-1}, so that our decimal expansions go infinitely far to the right instead of the left, and hence they look more like the ones in $\mathbb{R}$ we are used to. That is, we can define the p-adic numbers as a set of expansions analogous to the definition of $\mathbb{R}$:

$$\mathbb{Q}_p := \left\{ \sum_{i=-\infty}^{N} a_i p^{-i} \mid N \in \mathbb{N}, a_i \in \{0, 1, 2 \ldots, p-1\} \right\}.$$

Let's see how to compute p-adic expansions in practice. Let's consider the case of expanding integers first. Let's pick $p = 5$, and pick a random integer, say $a = 12309157913247$. Then a has an expansion of the form

$$a = a_{-N} 5^{-N} + \ldots + a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \ldots.$$

Now since there are no negative powers of 5 in a (it is an integer, so there is no denominator), there are no negative powers of 5 in the expansion. That is, the expansion in this case is of the form

$$a = a_0 + a_1 \cdot 5 + a_2 \cdot 5^2 + \ldots.$$

We can determine the digits inductively by reducing mod powers of 5. For example, reducing mod the first few prime powers gives us the equations:

$$a \equiv a_0 \pmod 5,$$

$$a \equiv a_0 + 5a_1 \pmod{25},$$

$$a \equiv a_0 + 5a_1 + 25a_2 \pmod{125},$$

where in each case we have used that mod the power of five on the right hand side, only the first few powers of 5 in the expansion aren't killed and all powers of 5 beyond the modulus are identically 0. In this case, we compute on the computer that

$$a \equiv 2 \pmod 5, \quad a \equiv 22 \pmod{25}, \quad a \equiv 122 \pmod{125}.$$

Thus, the equations above become

$$a_0 \equiv 2 \pmod 5,$$
$$a_0 + 5a_1 \equiv 2 + 5a_1 \equiv 22 \pmod 5 \iff 5a_1 \equiv 20 \pmod 5 \iff a_1 \equiv 4 \pmod 5,$$

and

$$a_0 + 5a_1 + 25a_2 \equiv 2 + 4 \cdot 5 + 25a_2 \equiv 22 + 25a_2 \equiv 122 \pmod{125}$$
$$\iff 25a_2 \equiv 100 \pmod{125} \iff a_2 \equiv 4 \pmod 5.$$

Thus, the first few 5-adic digits of a are $2, 4, 4$. We write this as a decimal expansion notationally as

$$a = 2.44\ldots_5\,.$$

The 2 is before the decimal place since its the "ones" spot, namely, the multiple of p^0 in the expansion, and the subscript 5 reminds us that this is as a 5-adic number. If you continue in this way (of course, I just used a computer), you find that

$$a = 12309157913247 = 2{+}4{\cdot}5{+}4{\cdot}5^2{+}5^4{+}2{\cdot}5^5{+}5^6{+}5^7{+}4{\cdot}5^8{+}3{\cdot}5^9{+}2{\cdot}5^{10}{+}5^{11}{+}3{\cdot}5^{12}{+}3{\cdot}5^{13}{+}5^{14}{+}3{\cdot}5^{15}{+}5^{17}{+}3{\cdot}5^{18}$$
$$= 2.4401211432133130 13_5.$$

As on one of the HW exercises, this expansion eventually repeats, as $a \in \mathbb{Z}$ is rational (the expansion is eventually all 0's as it terminates), and indeed for every integer, there is a unique representation in terms of sums of powers of 5's in this way, which is exactly the same fact that is the basis for decimal expansions of integers making sense in the usual real number sense: given a base, such as 10, every integer has a unique representation as a sum of numbers modulo that base times powers of that base, which we usually use to write integers. There is nothing special about 10, so of course we could work in binary, or 5-ary arithmetic, and the same would hold. Put another way, eventually, the powers p^i will be bigger than any integer a, and at this point, reducing a mod those prime powers always gives the same answer beyond that point. For instance, $120 < 5^3$, so it is the same mod $5^3, 5^4, 5^6$, and so on, and the above equations guarantee that after this point all the 5-adic digits are just 0.

As on the HW, if we now take any rational number, we should find that it has a p-adic eventually repeating expansion. Let's see how we can use congruence equations like above to expand any rational number. Let's take $a = \frac{2}{5}$ and expand it in $\mathbb{Q}_3$. Then as in the last example there are no 3's dividing the denominator, so the expansion is of the shape

$$a = \frac{2}{5} = a_0 + a_1 \cdot 3 + a_2 \cdot 3^2 + \ldots.$$

If we reduce mod successive powers of 3, as above, we find that

$$\frac{2}{5} \equiv a_0 \pmod 3,$$
$$\frac{2}{5} \equiv a_0 + a_1 \cdot 3 \pmod 9,$$
$$\frac{2}{5} \equiv a_0 + a_1 \cdot 3 + a_2 \cdot 9 \pmod{27}.$$

What does it mean to reduce a fraction modulo a prime? By $2/5$, we mean 2 times the multiplicative inverse of 5, namely, $\frac{2}{5} \equiv 2 \cdot \overline{5} \pmod 3$. The inverse of 5 is $\overline{5} \equiv \overline{-1} \equiv -1 \pmod 3$. Thus, we have $\frac{2}{5} \equiv 2 \cdot (-1) \equiv -2 \equiv 1 \pmod 3$. Alternatively, we can take the first equation in the chain of equations just above and rewrite it as

$$2 \equiv 5a_0 \pmod 3,$$

which is solved by multiplying both sides by $\overline{5} \pmod 3$. Either way of thinking about it works fine. At any rate, we have just computed that $a_0 = 1$. To compute the next digit, we will try the alternative method of computing to mix it up:

$$\frac{2}{5} \equiv a_0 + 3a_1 \equiv 1 + 3a_1 \pmod 9 \iff 2 \equiv 5 + 15a_1 \pmod 9 \iff 2 \equiv 5 + 6a_1 \pmod 9$$
$$\iff -3 \equiv -3a_1 \pmod 9 \iff 1 \equiv a_1 \pmod 3,$$

and hence $a_1 = 1$. We can compute a_2, say by using the multiplicative inverse of 5 modulo 27, which is $\overline{5} \equiv 11 \pmod{27}$, yielding

$$\frac{2}{5} \equiv 2 \cdot \overline{5} \equiv 2 \cdot 11 \equiv 22 \equiv a_0 + 3a_1 + 9a_2 \equiv 1 + 3 + 9a_2 \equiv 4 + 9a_2 \pmod{27}$$
$$\iff 18 \equiv 9a_2 \pmod{27} \iff 2 \equiv a_2 \pmod 3.$$

Hense, $a_2 = 2$. Continuing in this way (eventually you'll want a computer; any computer algebra system can compute multiplicative inverses modulo n), we find that the first few digits are

$$\frac{2}{5} = 1.121012101210\ldots_3\,.$$

This looks like it repeats, namely that

$$\frac{2}{5} = 1.\overline{1210}_3.$$

Indeed, we can check this using a geometric series as on the homework solutions. We compute that

$$1.\overline{1210}_3 = 1 + 3 \cdot 0.\overline{1210}_3 = 1 + 3 \cdot \left(1 + 2 \cdot 3 + 3^2\right) \cdot \left(1 + 3^4 + 3^8 + 3^{12} + \ldots\right)$$
$$= 1 + 3 \cdot 16 \cdot \sum_{i=0}^{\infty} 3^{4i} = 1 + \frac{48}{1 - 3^4} = 1 - \frac{48}{80} = 1 - \frac{3}{5} = \frac{2}{5}.$$

(To see the second equality, write out the first few terms of the product of the two expressions in parentheses; the first expression controls the digits in the repeating pattern and the powers of three at multiples of 4 reflects that the period of the repetition is 4). Thus, this is indeed the precise formula in $\mathbb{Q}_3$ for the number $2/5$.

This example illustrates how to compute the p-adic expansion of any rational number with no p's in the denominator. If there are powers of p downstairs in some rational number, then we can simply multiply that rational number by the power of p to kill the powers in the denominator, repeat the above procedure, and then shift the expansion at the very end. For instance, consider the 3-adic expansion of $b = \frac{2}{135} = \frac{2}{5 \cdot 3^3}$. Then we have that $27 \cdot b = \frac{2}{5}$ has no 3's in the bottom, and so the expansion starts with a 3^0 term (i.e., there are no negative powers of 3 in the expansion). Since we did the computation for the 2-adic expansion of $a = 27b$ above, we then find that

$$b = 3^{-3} \cdot \frac{2}{5} = 3^{-3} \cdot \left(1 + 3 + 2 \cdot 3^2 + 3^3 + 3^5 + \ldots\right) = 3^{-3} + 3^{-2} + 2 \cdot 3^{-1} + 3^0 + 3^2 + \ldots$$
$$= 1121.012101210\ldots_3 = 1121.\overline{0121}_3.$$

That is, multiplying by a power of p just shifts the decimal place, just as multiplying by a power of 10 does for real number decimal expansions. As any rational number has a finite power of p (if any) in the denominator, one can always do this and reduce to the cases like above, where one has to compute the expansion via computing congruences mod higher and higher powers of p.

As a final aside, if you are computing the expansion of a rational number $x = a/b$ in $\mathbb{Q}_p$, then you are finding a root of the polynomial $f(x) = a - bx$, which has derivative $f'(x) = -b$. Thus if $p \nmid b$, then x is a simple root of this polynomial and Hensel's Lemma gives a procedure for computing the p-adic expansion of the rational number. Thus, you could also use Hensel's Lemma to compute p-adic expansions of rational numbers. I prefer the above more "explicit/hands-on" approach above for expositional purposes. However, this is worth mentioning, to further emphasize the connections.