NOTES ON HENSEL'S LEMMA AND p-ADICS

Vanderbilt University, Spring 2023

We have seen that by combining the results on solving a single linear congruence with the Chinese Remainder Theorem (CRT), we can solve any system of linear congruences. This naturally leads to the question: what about polynomial congruences for polynomials of higher degree? These very naturally arise in all subjects in number theory. For instance, many many number theory problems can be phrased as a question of solving a polynomial equation in the integers, also known as a *Diophantine equation*. If you want to show that such an equation does *not* have a solution, for instance think of Fermat's Last Theorem, then a number theorists' first tool is to try to show that a solution does not exist modulo m for some m. This is called a congruence *obstruction*; an elementary reason why something cannot exist. For example, you showed on the homework that a number of the form $n \equiv 3 \pmod 4$ cannot be a sum of two squares.

We will later have much to say about quadratic congruences, which have many beautiful applications. First, however, we should discuss the general situation. Suppose throughout that $f(x)$ is a polynomial with integer coefficients. To solve the equation $f(x) \equiv 0 \pmod m$, the first step is to note that by the Chinese Remainder Theorem, this is the same as solving the system of equations $f(x) \equiv 0 \pmod{p_i^{e_i}}$, where the $p_i^{e_1}$ are the prime powers occurring in the factorization of m. Each of these will either not have a solution or the solution will be a collection of congruence classes modulo $p_i^{e_i}$. If at least one has no solutions, then the original congruence will have no solutions. If they all have solutions, then one can use the Chinese Remainder Theorem to determine the set of $x \pmod m$ satisfying the original equation.

Thus, it is sufficient in general to study congruences modulo powers of primes. Sometimes, this is all that one can say. However, most of the time, there is a way to build solutions mod a power of a prime from solutions modulo just the prime. That is, there is a general method to bootstrap to build solutions modulo higher and higher powers. This should be a surprise; for instance, it is quite strange that we can study a congruence modulo 2, i.e., just a parity condition, and easily obtain sequences of congruences modulo all powers of 2. However, as we shall see, the proof, though split into several cases, is fairly elementary, and simply uses properties of Taylor expansions.

Theorem 0.1 (Hensel's Lemma)**.** *Suppose $f(x)$ is an integral polynomial of degree at least 2, p is a prime, and r is a solution of the congruence $f(x) \equiv 0 \pmod{p^{k-1}}$. Also suppose that not all coefficients of $f(x)$ are divisible by p. Then we have the following.*

(1) *If r is a simple root modulo p, then the solution r lifts to a unique solution modulo p^k. That is, if $f'(r) \not\equiv 0 \pmod p$, then there is a unique number $0 \leq t < p$ such that $f(r + tp^{k-1}) \equiv 0 \pmod{p^k}$. Specifically, we have*

$$t \equiv -\overline{f'(r)} \cdot \frac{f(r)}{p^{k-1}} \pmod p.$$

(2) *If $f'(r) \equiv 0 \pmod p$ and $f(r) \equiv 0 \pmod{p^k}$, then every lift of r is a root modulo p^k, that is, for all $t \in \mathbb{Z}$, we have*

$$f(r + tp^{k-1}) \equiv 0 \pmod{p^k}.$$

(3) *If $f'(r) \equiv 0 \pmod p$ and $f(r) \not\equiv 0 \pmod{p^k}$, then no lifts of r are a root modulo p^k. That is, the equation $f(x) \equiv 0 \pmod{p^k}$ has no solutions with $x \equiv r \pmod{p^{k-1}}$.*

Note that the condition in part (1) doesn't depend on k, lending this theorem to recursion.

Proof. Any polynomial, say of degree n, can be expanded as a Taylor series, say around a:

$$f(x) = f(a) + f'(a)(x-a) + \ldots + f^{(n)}(a)\frac{(x-a)^n}{n!}.$$

Note that this series terminates as $f^{(k)} = 0$ for all $k \geq n+1$. Letting $x = a + b$, we have

$$f(a+b) = f(a) + f'(a)b + \ldots + f^{(n)}(a)\frac{b^n}{n!}.$$

We claim that all expressions in this formula are integral. To see this, by linearity of the differentiation operator, and since $f(x)$ is an integral linear combination of powers of x, it is enough to show this for powers of x. But then note that

$$\frac{d^j}{dx^j}(x^m)|_{x=a} = m \cdot (m-1) \cdot \ldots \cdot (m-j+1)a^{m-j}.$$

Thus,

$$\frac{d^j}{dx^j}(x^m)|_{x=a} \cdot \frac{1}{j!} = \binom{m}{j} a^{m-j},$$

and we know that binomial coefficients are always integral.

With these observations at hand, we now prove the main results. Suppose that q is a root of f modulo p^k. Then as usual it is also a root modulo p^{k-1}. Thus, if r is the reduction of q modulo p^{k-1}, then we must have that $q = r + tp^{k-1}$ (since they are congruent mod p^{k-1}). Our goal is to determine the conditions on t. Plugging into our second expansion above, we find

$$f(r + tp^{k-1}) = f(r) + f'(r)tp^{k-1} + \ldots + f^{(n)}(r)\frac{(tp^{k-1})^n}{n!},$$

where each term of the form $f^{(k)}(r)/r!$ is an integer. Now most of these terms vanish mod p^k. Specifically, for each $m \geq 2$, the terms $p^{(k-1)m}$ vanish mod p^k, as $(k-1)m > k$. Thus, this last equation reduces to

$$f(r + tp^{k-1}) \equiv f(r) + f'(r)tp^{k-1} \pmod{p^k}.$$

Since $r + tp^{k-1}$ is a root of f mod p^k, this further reduces to

$$f'(r)tp^{k-1} \equiv -f(r) \pmod{p^k}.$$

Since, by assumption, $f(r) \equiv 0 \pmod{p^{k-1}}$, we can divide this congruence through by p^{k-1}, obtaining

$$f'(r)t \equiv -\frac{f(r)}{p^{k-1}} \pmod{p}.$$

This is a linear congruence equation in t, and is especially easy to study as the gcd condition only can involve a divisor of the modulus, namely 1 or p. If $f'(r)$ is not a multiple of p, then $(f'(r), p) = 1$ which divides the right hand side, and so there is a unique t satisfying the congruence mod p. Moreover, using the invertibility of $f'(r)$ mod p and solving gives the explicit formula in (1).

Cases (2) and (3) concern the situation when $p|f'(r)$. Then $(f'(r), p) = p$, and so the equation is solvable if and only if $p| - \frac{f(r)}{p^{k-1}}$, i.e., if and only if $p^k|f(r)$. If it does not divide, then there are no solutions, as claimed, and if it does, then there are p different solutions t mod p, i.e., it holds for all t, as claimed. □

It is perhaps not surprising that one can often use congruences mod a power of a prime to get congruences mod one higher power. However, the true strength of Hensel's Lemma is made apparent by the following immediate consequence.

Corollary 0.2. If r solves $f(x) \equiv 0 \pmod{p}$ but $f'(r) \not\equiv 0 \pmod{p}$, then for each $k \geq 2$, there is a unique solution r_k to the congruence $f(x) \equiv 0 \pmod{p^k}$ where $r_1 = r$, and $r_{k+1} \equiv r_k \pmod{p^{k-1}}$.

Proof. The proof is immediate once one notices that the condition in (1) of the theorem is independent of k. □

As an example, consider the equation $x^2 = 7$. There is no rational solution x, and so certainly there is no integral solution. However, there are congruence solutions. For instance, modulo 3, this becomes the equation $x^2 \equiv 1 \pmod{3}$. As usual for a prime, this reduces to $x \equiv \pm 1 \pmod{3}$. Take the solution $x \equiv 2 \pmod{3}$. If we want to lift this solution to higher prime powers, then we rewrite the equation as $x^2 - 7 \equiv 0 \pmod{3}$, and look at the derivative of the polynomial modulo 3. Thus, we have

to check if $2x \equiv 0 \pmod 3$ for our solution $x \equiv 2 \pmod 3$. As $2 \cdot 2 \not\equiv 0 \pmod 3$, we see by Hensel's Lemma that there is a lift to a solution mod 9. Using the formula given there, we can compute it by first finding the inverse of $f'(r) \equiv 4 \equiv 1 \pmod 3$, which is simply $\overline{f'(r)} \equiv 1 \pmod 3$. Thus, we find that the solution mod 9 lifting this root mod 3 is $r + t \cdot 3$ where $t = -f(r)/3 = -(2^2 - 7)/3 = 1$. That is, the solution mod 9 is $2 + 3 \cdot 1 = 5$. Indeed, we find that $5^2 \equiv 7 \pmod 9$. Similarly, we have already checked that $r = 2$ is not a multiple root modulo 3, and since 5 is a lift of the original root, modulo 3 it is still the same root $r = 2$, and so is still a simple root. We also still have the same computation for the inverse, as that equation took place modulo 3. Thus, applying Hensel's Lemma again gives a root modulo 27 as $5 + 9 \cdot (-(5^2 - 7)/9) = 5 + 9 \cdot (-2) = -13 \equiv 14 \pmod{27}$. Thus, there is a "square root" of 7 modulo every power of 3. Moreover, there are exactly two such square root, by the uniqueness statement in Hensel's Lemma, and the fact that there are two roots modulo 3. Thus, for instance, we can find all solutions modulo $27, 81, \ldots$.

We have discovered something important in this example. Although $\sqrt{7}$ is irrational, we can approximate it modulo any power of 3 to arbitrary precision. The way to think about this is using another number system, called the p-adic numbers. The idea is as follows. In calculus class, you simply assumed that the real numbers were something that exists and which are worthy of study, but you had not seen how they are actually defined. The reason for this is that it is a delicate matter which requires some careful work. The idea, however, is reasonable. Just as there are polynomials which do not have real roots, but we can "fix" the problem by passing to the complex numbers thanks to the Fundamental Theorem of Algebra, the set of rationals (which we take for granted are "natural") has a defect. Namely, since things like $\sqrt{2}$ are irrational, but can be approximated arbitrarily well by sequences of rational numbers (for instance by truncating decimal expansions), the theory of limits, on which all calculus is based, don't really make any sense over $\mathbb{Q}$. In particular, you can build sequences of rational numbers which get arbitrarily close together but whose limit goes outside the set of rationals. Just as the solution to number systems not containing roots of polynomials like $x^2 + 1$ is to "throw in" the roots and consider a bigger number system, here the problem can be fixed by adding in the limits of all sequences of rational numbers like these, and this gives the set of real numbers. This definition is very easy to work with as well, as everything can be expressed as a decimal expansion, just possibly with infinitely many digits. Once one does this, things like continuous functions and derivatives make sense, and calculus is then possible.

However, the set of real numbers is just one possible way to fix the problem of "holes" in $\mathbb{Q}$. Specifically, the construction sketched above relies on the notion of elements in a sequence getting "close" to one another. The standard measure of distance on number like is that the distance from x to y is $|x - y|$. However, this is not the only possibly theory of distance which makes sense. It is a famous theorem that the types of distance that satisfy some standard axioms (these are called *norms*) are precisely the usual Euclidean distance together with the "p-adic" metric for any prime p. This measures the size of any rational number as follows. Any rational numbers r/s can be written as $r/s = p^k u/v$ where $u, v \not\equiv 0 \pmod p$. Then we say that the "size" of r/s is

$$|r/s|_p = p^{-k}.$$

We also define $|0|_p = 0$. Thus, a number is "small" if it is highly divisible by p. For instance $2/5, 6/5, 18/5, 54/5, \ldots$ is a sequence of rational numbers with 3-adic norms $3^0, 3^{-1}, 3^{-2}, 3^{-3}, \ldots = 1, 1/3, 1/9, 1/27, \ldots$. Thus, this sequence tends to 0 3-adically. Similarly, the sequence $1/2, 1/4, 1/8, 1/16, \ldots$ goes to infinity 2-adically.

Hensel's big idea was that the rationals still have "holes" with respect to this new measure of size, but that one could still extend $\mathbb{Q}$ to a bigger set by filling in the holes. This leads to the set of p-adic numbers $\mathbb{Q}_p$. To a number theorist, these numbers are almost as important as the set of real numbers themselves, and such people can often be heard saying that we shouldn't be "biased" by always studying only the reals.

As an example, consider the set of solutions to the equation $x^2 - 7$ modulo powers of 3 which we constructed above. What we really showed was that there is a sequence of numbers r_k such that

$$|r_k^2 - 7|_3 = 3^{-k},$$

i.e., such that $\lim_{k\to\infty}(r_k^2 - 7) = 0$. This limit cannot exist within $\mathbb{Q}$, but it does in $\mathbb{Q}_3$. Just as any real number has a decimal expansion which is a linear combination of powers of 10, every p-adic number can be understood explicitly via a *p-adic* expansion of the form

$$x = \sum a_n p^n,$$

where the a_n are essentially unique numbers $0 \leq a_n < p$. For instance, the 3-adic square root of $x^2 - 7$ which we built above has p-adic expansion which starts out as 14 modulo 27, and which we recursively built as $2 + 3 \cdot 1 + 9 \cdot 1 = 14$ (here we replaced the -2 above by its reduced representative mod 3. This is the beginning of the p-adic expansion of our square root, that is, the first few "digits" are $2, 1, 1, \ldots$. Similarly,

$$1 + 3 + 3^2 + 2 \cdot 3^4 + 2 \cdot 3^7 + 3^8 + 3^9 + 2 \cdot 3^{10} = 148891$$

and

$$148891^2 - 7 = 821056662 = 2 \cdot 3^9 \cdot 20857$$

is a multiple of 3^9. Thus, our other square root of 7 in $\mathbb{Q}_3$ has 3-adic expansion with initial digits $1, 1, 1, 0, 2, 0, 0, 2, 1, 1, 2$.

As a quick remark, although we won't have the time to describe it in too much detail, there is a theory of calculus and geometry that can be built out of p-adic norms. What should a continuous function be? Well, one in which if the inputs are congruent modulo a high power of p, then the outputs also must be congruent mod large powers of p. There are very reasonable notions of integration, and many other things. This is frequently useful. However, the resulting geometry is weird. For example, all triangles using $\mathbb{Q}_p$ are isosceles. Many things are easier than in classical calculus, too. For instance, in $\mathbb{Q}_p$, an infinite series converges if and only if its terms tend to zero. Much of Calculus II wouldn't be needed if this also held over $\mathbb{R}$! Moreover, Hensel's Lemma shows that constructing roots of functions often amounts to a finite elementary calculation.

Returning to the problem of studying Diophantine equations in the integers, we can use these ideas to build one of the most powerful techniques in number theory. This technique does not always work, but even when it fails, its nearly-working is still extremely interesting. For instance, this thinking is what leads to the ideas of the zeta and L-functions, and can be thought of as somehow behind two of the seven million dollar Millennium prize problems. To explain, we have to begin with an example whose solution goes back to the ancient Greeks.

We will consider the problem of characterizing the Pythagorean triples. You have probably seen these in school. To recap, they are simply triples of positive integers $a, b, c \in \mathbb{N}$ such that $a^2 + b^2 = c^2$. For instance, a few triples are given by $(3, 4, 5)$ and $(5, 12, 13)$. Of course, these really arise from a geometric problem. Namely, a triple of numbers is a Pythagorean triple if and only if they are the side lengths of a right triangle. How can you write down all such triples? The first observation is that one can rescale triangles by considering similar triangles. That is, any triple (a, b, c) can be rescaled to (Na, Nb, Nc). For instance, $(3, 4, 5)$ also gives rise to the triples $(9, 12, 15)$ and $(30, 40, 50)$. Similarly, one can divide out any common factors from a, b, c. Thus, it is sufficient to determine the set of *primitive Pythagorean triples*, i.e., those for which $(a, b, c) = 1$.

In the following lecture, we shall see how the Greeks devised a brilliant solution to this problem by recasting it as a different geometric problem, and how p-adics and Hensel's Lemma can be used to determine all points on other geometric curves and surfaces as well.