Continuing the pre/review of the simple (!?) case... Some themes so far:

Riemann's explicit formula connects *complex zeros* of *meromorphic continuations of* zeta functions (and L-functions) to tangible, finitistic properties of primes.

Gauss' *Quadratic Reciprocity* is proven via Gauss sums, which are Lagrange resolvents for cyclotomic fields.

Dedekind zeta functions of quadratic extensions of $\mathbb{Q}$, and of cyclotomic fields, factor into products of Dedekind L-functions. These, too, are *Reciprocity Laws.*

Next: Solving equations mod p^n ... and p-adic numbers. This is *Hensel's Lemma*, a version of *Newton-Raphson* in a different context.

Recall: solving *linear* equations mod N

We need just a simple case: for $\gcd(a,N)=1$, for the equation

$$ax+b \;=\; 0 \bmod N$$

a solution $x \in \mathbb{Z}$ *exists*, and is *unique* up to multiples of N. Proof: recall (!) that there are integers c, d such that

$$\gcd(a,N) \;=\; c\cdot a + d\cdot N$$

Since the *gcd* is 1, this is $1 = ca + dN$. Thus, we have an inverse $c = a^{-1} \bmod N$ for $a \bmod N$. This gives *existence* and *uniqueness* all at once:

$$ax+b \;=\; 0 \bmod N \quad\Longleftrightarrow\quad x = -a^{-1}b \bmod N$$

Comment: The case N *prime* is conceptually simpler, since $\mathbb{Z}/p$ is provably a *field*. However, indeed, some part of the above discussion is exactly what proves $\mathbb{Z}/p$ is a field.

Example: Solving $x^2 + 1 = 0 \bmod 5^n$ for large n.

Since $4|5 - 1$ and $\mathbb{F}_5^\times$ is cyclic, there *exists* an integer solution $x_1 \bmod 5$. In fact, $x_1 = 2$ or $3 \bmod 5$.

Next, given x_1, try to adjust it by multiples of 5 to obtain a solution $x_2 \bmod 5^2$: let $x_2 = x_1 + 5y$ and solve for y:

$$0 \;=\; x_2^2 + 1 \;=\; (x_1 + 5y)^2 + 1 \;=\; x_1^2 + 10x_1y + 5^2y^2 + 1 \bmod 5^2$$

The y^2 term has coefficient $0 \bmod 5^2$, so this becomes a *linear* equation in y:

$$0 \;=\; x_1^2 + 10x_1y + 1 \bmod 5^2$$

By design, $x_1^2 + 1$ is divisible by 5, so we can divide through by 5:

$$\frac{x_1^2 + 1}{5} + 2x_1y \;=\; 0 \bmod 5$$

Since $2x_1$ is invertible mod 5, there is a *unique* solution $y \bmod 5$. Thus, there is *unique* $x_2 \bmod 5^2$ such that both $x_2 = x_1 \bmod 5$ and $x_2^2 + 1 = 0 \bmod 5^2$.

Induction to get a solution x_{n+1} mod 5^{n+1} from a solution x_n mod 5^n. Try to adjust x_n by a multiple of 5^n: $x_{n+1} = x_n + 5^n y$. Solve for y:

$$0 \;=\; x_{n+1}^2 + 1 \;=\; x_n^2 + 2 \cdot 5^n x_n y + 5^{2n} y^2 + 1 \bmod 5^{n+1}$$

Again, the coefficient of y^2 is 0 mod 5^{n+1}, since $2n \geq n+1$ for $n \geq 1$, giving a *linear* equation in y. By induction, $x_n^2 + 1 = 0 \bmod 5^2$, so divide through by 5^n:

$$\frac{x_n^2 + 1}{5^n} + 2x_n y \;=\; 0 \bmod 5$$

For that matter, by induction, $x_n = x_1 \bmod 5$, so

$$y \;=\; -(2x_1)^{-1} \cdot \frac{x_n^2 + 1}{5^n} \quad \bmod 5$$

A somewhat-more-general case:

Theorem: *(Hensel)* For f monic in $\mathbb{Z}[x]$, for prime p, if there is $x_1 \in \mathbb{Z}$ such that $f(x_1) = 0 \bmod p$ but $f'(x_1) \neq 0 \bmod p$, then there is a unique $x_n \bmod p^n$ such that $f(x_n) = 0 \bmod p^n$ and $x_n = x_1 \bmod p$. Specifically, with $f'(x_1)$ inverted mod p,

$$x_{n+1} \;=\; x_n - \frac{f(x_n)}{f'(x_1)} \mod p^{n+1}$$

Proof: As in the example, given x_n, solve for $y \bmod p$ so that $x_{n+1} \;=\; x_n + p^n y$ is a solution mod p^{n+1}. Taylor series for polynomials are legitimate:

$$0 \;=\; f(x_{n+1}) \;=\; f(x_n + p^n y)$$

$$=\; f(x_n) + \frac{f'(x_n)}{1!} p^n y + \frac{f''(x_n)}{2!} (p^n y)^2 + \ldots \mod p^{n+1}$$

The sum is finite, but division by factorials...? In fact, for $f \in \mathbb{Z}[x]$, $f^{(k)}(x)$ has coefficients divisible by $k!$(!) It suffices to prove this for monomials:

$$\frac{d^k}{dx^k}x^n \;=\; n(n-1)(n-2)\ldots(n-k+1)\cdot x^{n-k}$$

Hopefully, we recognize

$$\frac{n(n-1)(n-2)\ldots(n-k+1)}{k!} \;=\; \frac{n!}{(n-k)!\,k!}$$

$$=\; \text{binomial coefficient} \;\in \mathbb{Z}$$

As $2n \geq n+1$ for $n \geq 1$, the equation becomes *linear* in y:

$$0 \;=\; f(x_{n+1}) \;=\; f(x_n + p^n y) \;=\; f(x_n) + \frac{f'(x_n)}{1!}p^n y \mod p^{n+1}$$

Inductively, $x_n = x_1 \bmod p$, so $f'(x_n) = f(x_1) \bmod p$. Thus, it is invertible mod p, and mod p^{n+1}. Then

$$p^n y \;=\; -\frac{f(x_n)}{f'(x_n)} \mod p^{n+1}$$

Using $f(x_n) = 0 \bmod p^n$,

$$y \;=\; -\frac{f(x_n)}{p^n \cdot f'(x_1)} \mod p$$

Thus,

$$x_{n+1} \;=\; x_n + p^n y \;=\; x_n - \frac{f(x_n)}{f'(x_n)} \;=\; x_n - \frac{f(x_n)}{f'(x_1)} \bmod p^{n+1}$$

Done.

The sequence of solutions x_{n+1} looks like

$$\begin{array}{rcl} x_1 & = & x_1 \\ x_2 & = & x_1 + py_1 \\ x_3 & = & x_1 + py_1 + p^2 y_2 \\ x_4 & = & x_1 + py_1 + p^2 y_2 + p^3 y_3 \\ & \ldots & \end{array}$$

The adjustments y_i can be in the range $\{0, 1, 2, \ldots, p-1\}$ if we want.

From x_n we can recover all the earlier ones: $x_{n-1}, x_{n-2}, \ldots, x_2, x_1$, at least modulo the respective p^k's.

It would be conceptually economical if the sequence $x_1, x_2, x_3, \ldots$ had a *limit*, x_∞, which somehow solved the equation modulo p^∞, from which we could recover solutions modulo p^n for all finite n.

There are at least two different-looking ways to make the limiting process legitimate.

The more popular, more accessible approach is by making up a metric, the p-adic metric $d(-,-)$, coming from the p-adic *norm* $|*|_p$, in which p^n get *smaller* as n gets *larger*. Then the p-**adic integers** $\mathbb{Z}_p$ are the *completion* of $\mathbb{Z}$ with respect to the p-adic metric, and the p-adic rational numbers $\mathbb{Q}_p$ are the completion of $\mathbb{Q}$. We'll do this first.

The other approach, perhaps less popular, because it is less elementary, is nevertheless more revealing of the true workings of p-adic numbers and other things arising in a similar fashion: $\mathbb{Z}_p$ is the *(projective) limit* of the $\mathbb{Z}/p^n$. We'll look at this second.

The p-adic norm $| * |_p$ is defined on $\mathbb{Q}$ by

$$\left|p^n \cdot \frac{a}{b}\right|_p \;=\; p^{-n} \qquad\qquad \text{(with } a, b \text{ prime to } p,\ n \in \mathbb{Z}\text{)}$$

The p-adic *metric* is made from the norm in the same way that the usual (”real”) metric on $\mathbb{Q}$ is made from the usual absolute value: $d(x, y) = |x - y|_p$. It is obviously symmetric and reflexive, but the *triangle inequality*

$$d(x, z) \;\leq\; d(x, y) + d(y, z)$$

takes a bit of thought. Yes, $|k|_p \leq 1$ for all $k \in \mathbb{Z}$. Examples:

$$\begin{array}{lclclclclcl}
|5|_2 & = & 1 & \quad & |5|_5 & = & \frac{1}{5} & \quad & |5|_3 & = & 1 \\[1ex]
|10|_2 & = & \frac{1}{2} & & |10|_5 & = & \frac{1}{5} & & |10|_3 & = & 1 \\[1ex]
|\frac{2}{3}|_2 & = & \frac{1}{2} & & |\frac{2}{3}|_5 & = & 1 & & |\frac{2}{3}|_3 & = & 3 \\[1ex]
|\frac{35}{18}|_2 & = & 2 & & |\frac{35}{18}|_5 & = & \frac{1}{5} & & |\frac{35}{18}|_3 & = & 9
\end{array}$$

A metric space is *complete* if every Cauchy sequence has a limit.

The *completion* $\widetilde{X}, \tilde{d}$ of a metric space X, d can be *characterized* as a complete metric space with an inclusion $j : X \to \widetilde{X}$ preserving the metric, that is, $\tilde{d}(jx, jy) = d(x, y)$, and such that X is *dense*, that is, every point of $\widetilde{X}$ is a limit of a Cauchy sequence in X.

Completions $\widetilde{X}$ are proven to *exist* by giving a *construction*: $\widetilde{X}$ is Cauchy sequences in X modulo the equivalence relation $\{x_n\} \sim \{y_n\}$ when $\lim_n d(x_n, y_n) = 0$. The metric on this model is $\tilde{d}(\{x_n\}, \{y_n\}) = \lim_n d(x_n, y_n)$. There are things to be checked to certify that this construction succeeds in making a completion.

Another *characterization* of the completion $j : X \to \widetilde{X}$, which makes it easy to prove *uniqueness*, is that any metric-preserving map $f : X \to Y$ to a *complete* metric space Y *factors through* $j : X \to \widetilde{X}$, in the sense that there is a *unique* metric-preserving $F : \widetilde{X} \to Y$ such that

$$\begin{tikzcd}
\widetilde{X} \arrow[rd, dashed, "F"] & \\
X \arrow[u, "j"] \arrow[r, "f"] & Y
\end{tikzcd} \qquad \text{(metric-preserving maps)}$$

The ring of p-**adic integers** $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|*|_p$.

The field of p-**adic rationals** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|*|_p$.

We'll also want to be sure that addition, multiplication, and inversion (of non-zero things) are *continuous* on $\mathbb{Q}$ in the p-adic metric, so that it is legitimate to *extend by continuity* to define addition and multiplication on $\mathbb{Q}_p$:

$$\begin{array}{rcl} (\lim_n a_n) \cdot (\lim_n b_n) & = & \lim_n (a_n \cdot b_n) \\ (\lim_n a_n) + (\lim_n b_n) & = & \lim_n (a_n + b_n) \\ (\lim_n a_n)^{-1} & = & \lim_n (a_n^{-1}) \end{array}$$

By design, the sequence of solutions x_n to $f(x_n) = 0 \bmod p^n$,

$$\begin{array}{rcl} x_1 &=& x_1 \\ x_2 &=& x_1 + py_1 \\ x_3 &=& x_1 + py_1 + p^2 y_2 \\ x_4 &=& x_1 + py_1 + p^2 y_2 + p^3 y_3 \\ & \ldots & \end{array} \qquad \text{(with } x_1,\ y_i \text{ in } \mathbb{Z}\text{)}$$

is *Cauchy* in the p-adic metric: for $m \le n$,

$$|x_n - x_m|_p \;=\; |p^{m+1} y_{m+1} + \ldots p^n y_n|_p$$

$$=\; |p^{m+1}|_p \cdot |y_{m+1} + \ldots p^{n-m-1} y_n|_p \;\le\; |p^{m+1}|_p \cdot 1 \;=\; \frac{1}{p^{m+1}}$$

since $y_{m+1} + \ldots p^{n-m-1} y_n \in \mathbb{Z}$!!!

For example, 2-adically,

$$1+2+4+8+16+\ldots \;=\; \lim_n (1+2+\ldots+2^n)$$

$$=\; \lim_n \frac{1-2^{n+1}}{1-2} \;=\; \frac{1-0}{1-2} \;=\; -1$$

Generally, p-adically,

$$1+p+p^2+p^3+\ldots \;=\; \frac{1}{1-p}$$

In contrast, the usual exponential series

$$e^x \;=\; 1+\frac{x}{1!}+\frac{x^2}{2!}+\ldots$$

converges p-adically only for $|x|_p$ *small*, because the factorials *hurt*, rather than *help* the convergence.

Warning: Yes, it is *possible* to write p-adic integers in a form that makes them look like *power series*:

$$\alpha \;=\; a_o + a_1 p^1 + a_2 p^2 + a_3 p^3 + \ldots \qquad (\text{with } a_i \in \{0, 1, 2, \ldots, p-1\})$$

In fact, this is what Hensel originally emphasized. However, neither addition nor multiplication treat such expressions as power series: the basic discrepancy is that *no* number of x^k's can add up to x^{k+1}, but adding p p^k's gives p^{k+1}.

Hensel's analogy to power series *is correct*, but not quite in the naive way one might think.

Therefore, while the possibility of such expressions is genuine, they do *not* reflect the behavior of p-adic numbers very well!!!

Another viewpoint: Even though the p-adic norm and metric succeed in making the sequences produced by Hensel's lemma *convergent*, there might seem an elementy of whimsicality.

One ambiguity is that many different metrics can give the same topology.

The true state of affairs, addressed candidly, is that Hensel's recursion produces a sequence x_n fitting into a picture

$$\begin{tikzcd}
\cdots \arrow[r] & x_{n+1} \arrow[r] & \cdots \arrow[r] & x_2 \arrow[r] & x_1 \\
\cdots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\text{mod } p^n"] & \cdots \arrow[r, "\text{mod } p^2"] & \mathbb{Z}/p^2 \arrow[r, "\text{mod } p"] & \mathbb{Z}/p
\end{tikzcd}$$