Continuing the pre/review ...

Riemann's explicit formula: *complex zeros* of zeta functions (and L-functions) versus properties of *primes*.

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

Factorization of Dedekind zeta functions of quadratic extensions of $\mathbb{Q}$ and of cyclotomic fields, as *Reciprocity Laws*.

Continuing: solving equations mod p^n ... and p-adic numbers. This is *Hensel's Lemma*, a version of *Newton-Raphson* in a different context. Both *completions* and *projective limits*.

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: 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:

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

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

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

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

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

and $|0|_p = 0$. The p-adic *metric* is made from the norm as usual: $d(x,y) = |x-y|_p$. Note that $|n|_p \le 1$ for all $n \in \mathbb{Z}$.

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 $|*|_p$.

For example, 2-adically,

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

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

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

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

Even though such representations have occasional use, this is potentially misleading: *no* number of x^k's can add up to x^{k+1}, but adding p p^k's gives p^{k+1}.

Ultrametric inequality: All p-adic triangles are isosceles!!!

Stronger than the *triangle inequality*, the *ultrametric inequality* holds:

$$|x \pm y|_p \;\; \le \;\; \max\left(|x|_p, |y|_p\right) \qquad \text{(with } \textit{equality} \text{ unless } |x|_p = |y|_p\text{!!!)}$$

To discuss this the p-adic *valuation* or *ord(er)* is useful:

$$\mathrm{ord}_p(p^\ell \cdot \frac{a}{b}) \;=\; \nu_p(p^\ell \cdot \frac{a}{b}) \;=\; \ell \qquad\qquad \text{(with } a, b \text{ prime to } p\text{)}$$

And $\mathrm{ord}_p 0 = \infty$. Then $|x|_p \;=\; p^{-\mathrm{ord}_p x}$.

To see the ultrametric inequality, observe that, for p^m the largest power of p dividing x, and p^n the largest power of p dividing y, taking $m \;\le\; n$ without loss of generality, p^m divides $x \pm y$. If $m < n$, then p^m is the *largest* power dividing $x \pm y$. That is,

$$\mathrm{ord}_p(x \pm y) \;\ge\; \min\left(\mathrm{ord}_p x, \mathrm{ord}_p y\right)$$

$$\text{(with } \textit{equality} \text{ unless } \mathrm{ord}_p x = \mathrm{ord}_p y\text{)}$$

Rewriting in terms of the norm reverses the inequality, giving the ultrametric inequality.

Ring structure of $\mathbb{Z}_p$

All integers n *prime to* p become p-adic *units!!!*

Proof: Let $f(x) = nx - 1$. Integers a, b with $ap + bn = 1$ give solution $x_1 = b$ to $f(x) = 0 \bmod p$. Since $f'(x) = n \neq 0 \bmod p$, Hensel gives a (compatible!) sequence x_n such that $nx_n = 1 \bmod p^n$. The compatibility $x_{n+1} = x_n \bmod p^n$ assures the sequence is Cauchy, and the limit is the p-adic n^{-1}. ///

Or: computing in $\mathbb{Q}_p$, from $bn = 1 - ap$, $b^{-1}n^{-1} = (1 - ap)^{-1}$ and

$$n^{-1} = b \cdot (1 - ap)^{-1} = b \cdot (1 + ap + a^2p^2 + a^3p^3 + \ldots) \in \mathbb{Z}_p$$

For example, to find 11-adic 7^{-1}, from $2 \cdot 11 - 3 \cdot 7 = 1$,

$$7^{-1} = (-3) \cdot (1 - 2 \cdot 11)^{-1} = (-3) \cdot (1 + 2 \cdot 11 + 4 \cdot 11^2 + 8 \cdot 11^3 + \ldots)$$

But wait: zero divisors in $\mathbb{Z}_p$? Is $\mathbb{Q}_p$ really a field?

Use the p-adic norm: if $\alpha \cdot \beta = 0$ for p-adic integers α, β, then by multiplicativity

$$0 \;=\; |0|_p \;=\; |\alpha \cdot \beta|_p \;=\; |\alpha|_p \cdot |\beta|_p$$

This is an equality of rational numbers, so either $|\alpha|_p \;=\; 0$ or $|\beta|_p = 0$, so either $\alpha = 0$ or $\beta = 0$.

Just to be sure that $|\alpha|_p = 0 \Rightarrow \alpha = 0$: the completion is Cauchy sequences modulo $\{x_n\} \sim \{y_n\}$ when $\lim_n |x_n - y_n|_p = 0$. For non-zero rationals, $|p^\ell \frac{a}{b}|_p \to 0$ requires $\ell \to +\infty$ (with a, b prime to p), and a, b have no impact. Then $|p^\ell \frac{a}{b} - 0|_p \to 0$, and $p^\ell \frac{a}{b} \to 0$ in $\mathbb{Q}_p$. That is, the Cauchy sequence is identified with 0.

Claim: On $\mathbb{Q}_p^\times$ the p-adic norm (still) takes only the discrete values p^ℓ with $\ell \in \mathbb{Z}$.

... in contrast to the usual $|*|$'s values on $\mathbb{R}$ versus on $\mathbb{Q}$.

Proof: By definition, for Cauchy $\{\alpha_n\}$, $|\lim_n \alpha_n|_p = \lim_n |\alpha_n|_p$. Let α be the limit. For $0 < \varepsilon < |\alpha|_p$ and $|\alpha_n - \alpha|_p < \varepsilon$, by the *ultrametric* inequality

$$|\alpha_n|_p \;=\; |\alpha_n - \alpha + \alpha|_p \;=\; \max(|\alpha_n - \alpha|_p, |\alpha|_p) \;=\; |\alpha|_p$$

Since $|\alpha_n|_p$ are integer powers of p, so is $|\alpha|_p$. ///

The *discreteness* of $|*|_p$ is hugely different from the usual $|*|$.

Claim: The p-adic completion $\mathbb{Z}_p$ of $\mathbb{Z}$ has properties:

$$\begin{array}{rclcl} \mathbb{Z}_p & = & \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p \le 1\} & = & \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p < p\} \\ p\mathbb{Z}_p & = & \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p < 1\} & = & \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p \le \frac{1}{p}\} \\ \mathbb{Z}_p^\times & = & \{\alpha \in \mathbb{Q}_p \,:\, |\alpha|_p = 1\} & = & \{\alpha \in \mathbb{Q}_p \,:\, \frac{1}{p} < |\alpha|_p < p\} \end{array}$$

Each of these sets is *both open and closed.*

Proof: Use discreteness of $|*|_p$.

When a Cauchy sequence $\alpha_n \in \mathbb{Q}^\times$ has $\lim_n |\alpha_n|_p \le 1$, eventually $|\alpha_n|_p < p$, and then necessarily $|\alpha_n|_p \le 1$ by discreteness. Thus, $\alpha_n \in \mathbb{Z}$ from that point, so $\lim_n \alpha_n \in \mathbb{Z}_p$.

[Cont'd]

For a Cauchy sequence $\alpha \in \mathbb{Q}^\times$ with $\lim_n |\alpha_n|_p < 1$, by discreteness eventually $|\alpha_n|_p \le \frac{1}{p}$. Thus, eventually $\alpha_n \in p\mathbb{Z}$. Thus, eventually $\alpha_n = p \cdot \frac{\alpha_n}{p}$ with $\alpha_n/p \in \mathbb{Z}$, exhibiting $\lim_n \alpha_n$ as an element of $p \cdot \mathbb{Z}_p$.

For Cauchy sequence $\alpha \in \mathbb{Q}^\times$ with $\lim_n |\alpha_n|_p = 1$, by discreteness eventually $\frac{1}{p} < |\alpha_n|_p < p$, so $|\alpha_n|_p = 1$, and $\alpha_n = \frac{a_n}{b_n}$ with a, b prime to p. We'd already noted that such things are p-adic units.

The topology is metric, and the above shows that $\mathbb{Z}_p$ is both the *closed ball* of radius 1 centered at 0, and also the *open ball* of any radius r with $1 < r < p$.

$\mathbb{Z}_p$ and $\mathbb{Q}_p$ are totally disconnected

That is, given $\alpha \neq \beta \in \mathbb{Q}_p$, there are disjoint open-and-closed sets $U \ni \alpha$ and $V \ni \beta$ such that $U \cup V = \mathbb{Q}_p$.

... due to the discreteness of the norm/metric/valuation: Let $p^\ell = |\alpha - \beta|_p$, and consider a ball centered at α

$$B \;=\; \{x \in \mathbb{Q}_p \;:\; |\alpha - x|_p < p^\ell\} \;=\; \{x \in \mathbb{Q}_p \;:\; |\alpha - x|_p \leq p^{\ell - 1}\}$$

That is, the ball is both open and closed, so its *complement*, containing β, is both open and closed. ///

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 element of whim.

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

$$\cdots \longrightarrow x_{n+1} \longrightarrow \cdots \longrightarrow x_2 \longrightarrow x_1$$

$$\cdots \longrightarrow \mathbb{Z}/p^{n+1} \xrightarrow{\bmod p^n} \cdots \xrightarrow{\bmod p^2} \mathbb{Z}/p^2 \xrightarrow{\bmod p} \mathbb{Z}/p$$

What we want is not so much a metric something-something, but an object X *behind* all the $\mathbb{Z}/p^n$'s, and $x_\infty \in X$,

$$\begin{tikzcd}
x_\infty \arrow[rr, dashed, bend left] \arrow[rrrr, dashed, bend left] \arrow[rrrrr, dashed, bend left] & \cdots \arrow[r] & x_{n+1} \arrow[r] & \cdots \arrow[r] & x_2 \arrow[r] & x_1
\end{tikzcd}$$

making a *commutative diagram* (meaning that the outcome doesn't depend on what route is traversed)

$$\begin{tikzcd}
X \arrow[rr, dashed, bend left] \arrow[rrrr, dashed, bend left] \arrow[rrrrr, dashed, bend left] & \cdots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\bmod p^n"] & \cdots \arrow[r, "\bmod p^2"] & \mathbb{Z}/p^2 \arrow[r, "\bmod p"] & \mathbb{Z}/p
\end{tikzcd}$$

We should tell how this X is to *interact* with other things, probably *topological rings*, meaning rings with topologies so that addition and multiplication are continuous. *Hausdorff*, for sanity.

Now *map* will mean *continuous ring hom.* Require that, for every topological ring Y with a collection of compatible maps (meaning the diagram is commutative)

$$\begin{tikzcd}
Y \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \cdots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\mathrm{mod}\ p^n"] & \cdots \arrow[r, "\mathrm{mod}\ p^2"] & \mathbb{Z}/p^2 \arrow[r, "\mathrm{mod}\ p"] & \mathbb{Z}/p
\end{tikzcd}$$

there is a *unique* map $Y \to X$ giving a commutative diagram

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \cdots \arrow[r] & \mathbb{Z}/p^{n+1} \arrow[r, "\mathrm{mod}\ p^n"] & \cdots \arrow[r, "\mathrm{mod}\ 2"] & \mathbb{Z}/p^2 \arrow[r, "\mathrm{mod}\ p"] & \mathbb{Z}/p \\
& Y \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

A topological ring $X = \lim \mathbb{Z}/p^n$ meeting these conditions is the *(projective) limit* of the $\mathbb{Z}/p^n$'s, and is provably the same $\mathbb{Z}_p$!!!

Note: each finite ring $\mathbb{Z}/p^n$ has a unique Hausdorff topology!!!

How to prove *existence* of projective limits? In this and many other situations, limits $\lim_n X_n$ are *subsets* of the (topological) cartesian products $\prod_n X_n$. Specifically, with

$$\cdots \longrightarrow X_{n+1} \xrightarrow{\varphi_{n+1}} \cdots \xrightarrow{\varphi_3} X_2 \xrightarrow{\varphi_2} X_1$$

a projective limit $X = \lim_n X_n$ can be constructed as

$$X \;=\; \{\{x_n\} \,:\, x_n \in X_n \text{ such that } \varphi_n(x_n) = x_{n-1} \text{ for all } n\}$$

That is, X consists exactly of *compatible sequences*

$$\cdots \longrightarrow x_{n+1} \xrightarrow{\varphi_{n+1}} \cdots \xrightarrow{\varphi_3} x_2 \xrightarrow{\varphi_2} x_1$$

just as produced by Hensel's recursion. For continuous φ_n and *compact* Hausdorff X_n's, *Tychonoff's theorem* says the product is *compact*. Such a projective limit is a closed subset of a compact Hausdorff space, so is *compact*. This proves compactness of $\mathbb{Z}_p$!!!

Uniqueness (up to unique isomorphism) of projective limits

The diagrammatic characterization can be used to assure that there's *no ambiguity* in what $\mathbb{Z}_p$ is, as long as it functions as a projective limit:

First, claim the only map of $X = \lim_n X_n$ to *itself*, compatible with the maps of it to the X_n, is the *identity*. Certainly the identity map is ok. Then the *uniqueness* of the dotted arrow

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \cdots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \cdots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

proves that the identity is the *only* compatible map. Next, ...

Suppose X and X' were *two* projective limits. On one hand, there is a unique $f : X' \to X$ giving commutative diagram

$$\begin{tikzcd}
X \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \cdots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \cdots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X' \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

On the other hand, reversing the roles of X and X', there is a unique compatible map $g : X \to X'$ fitting into

$$\begin{tikzcd}
X' \arrow[rr, bend left] \arrow[rrrr, bend left] \arrow[rrrrr, bend left] & \cdots \arrow[r] & X_n \arrow[r, "\varphi_n"] & \cdots \arrow[r, "\varphi_3"] & X_2 \arrow[r, "\varphi_2"] & X_1 \\
& X \arrow[ul, dashed] \arrow[ur] \arrow[urrr] \arrow[urrrr] & & & &
\end{tikzcd}$$

The composites $f \circ g : X \to X$ and $g \circ f : X' \to X'$ are also compatible, so must be the identities on X and X', by the first part. Thus, f, g are mutual inverses. ///