(*November 14, 2005*)

Classical definitions of $\mathbb{Z}_p$ *and* $\mathbb{A}$

Paul Garrett garrett@math.umn.edu http://www.math.umn.edu/~garrett/

Expressing the p-adic integers $\mathbb{Z}_p$ as $\mathbb{Z}_p = \lim_e \mathbb{Z}/p^e$ does not instantly show what $\mathbb{Z}_p$ *is* in comparison to even more classical objects such as $\mathbb{Z}$ and $\mathbb{Q}$. [1]

Kurt Hensel's 1897 conception of the p-adic numbers was close to the projective limit definition. His interest was in problems such as finding sequences $\{x_n\}$ of integers such that $x_n^2 = -1 \bmod 5^n$, constructed recursively. His approach is exactly parallel to the Newton-Raphson method of *sliding down the tangent* to better-and-better approximate zeros of differentiable functions of a *real* variable.

No abstract notion such as *projective limit* existed in Hensel's time time, leaving Hensel to hunt for analogies. The sort of recursion just mentioned led him to express p-adic integers x as *fake power series*

$$x = y_0 + py_1 + p^2y_2 + p^3y_3 + \dots \quad (\text{with } y_i \in \{0, 1, 2, \dots, p-1\})$$

Power series *were* part of the mathematical idiom of the time. The falsity of the model is that multiplication and addition mess up the choice of representatives y_i, which seems to have made Hensel's presentation unconvincing at the time.

The more usual and seemingly more pedestrian description of $\mathbb{Z}_p$ and $\mathbb{Q}_p$ (and somewhat more general related objects) expresses them as *completions* of $\mathbb{Z}$ and $\mathbb{Q}$ with respect to *metrics*. This description had to wait until the development of point-set topology and the notion of *metric* by Hausdorff, Fréchet, and many others in the 1920's and 1930's, and for Hasse's resurrection of Hensel's work, which had been essentially forgotten, not having caught on in the first place. It is ironic that a *redefined* (metric) version of p-adic numbers became acceptable decades before the original and operationally *relevant* definition as projective limit could be given in terms of standard mathematics.

In addition to discussion of the elementary analysis of the metric definition of p-adic numbers, we will show that the (unique) topology on $\lim_e \mathbb{Z}/p^e$ *can* be given by a metric which makes the homeomorphism to the metric definition of $\mathbb{Z}_p$ clear.

While the topology on $\lim_e \mathbb{Z}/p^e$ is uniquely determined, *many different metrics can give the same topology.* Thus, the notion of *topology* is intrinsic, while that of *metric* is not, despite the physical intuition that metrical notions conjure up. We might conclude that many notions that we imagine to be metrical are in fact topological.

---

1. *Hensel's lemma*

Kurt Hensel's 1897 interest in the p-adic numbers was for systematic solution of problems such as $x^2 = -1 \bmod 5^n$ for *all* powers 5^n of 5.

Starting with $x_1 = 2$ (whose square is 4, which is -1 mod 5), one hopes to *adjust* this solution mod 5 to be a solution mod 5^2. Namely, one hopes that for some y the modified value $x_2 = x_1 + 5y$ will satisfy

[1] At the same time, one should not necessarily insist on reduction of new ideas to old.

$x^2 = -1 \bmod 25$. This condition simplifies

$$\begin{array}{rcll} (x_1 + 5y)^2 & = & -1 & \bmod 5^2 \\ x_1^2 + 10x_1y + 25y^2 & = & -1 & \bmod 5^2 \\ (x_1^2 + 1) + 10x_1y & = & 0 & \bmod 5^2 \\ \frac{x_1^2+1}{5} + 2x_1y & = & 0 & \bmod 5 \end{array}$$

since $x_1^2 + 1$ is divisible by 5. A critical point is that the y^2 term *disappears* mod 5^2, leaving in any case a linear problem in y. Then, since $-2x_1 = 1 \bmod 5$ is invertible mod 5, we can solve for

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

and then

$$x_2 = x_1 + 5y = 2 + 1 \cdot 5 = 7$$

satisfies

$$x_2^2 = (x_1 + 5y)^2 = -1 \bmod 5^2$$

In fact, we can continue this process of *improvement* indefinitely, imitating the example just done, as follows. Suppose that

$$x_n^2 = -1 \bmod 5^n$$

We try to find y mod 5 such that

$$(x_n + 5^n y)^2 = -1 \bmod 5^{n+1}$$

An essentially identical rearrangement gives

$$\begin{array}{rcll} (x_n + 5^n y)^2 & = & -1 & \bmod 5^n \\ x_n^2 + 10x_ny + 5^{2n}y^2 & = & -1 & \bmod 5^n \\ (x_n^2 + 1) + 2 \cdot 5^n x_n y & = & 0 & \bmod 5^n \\ \frac{x_n^2+1}{5^n} + 2x_ny & = & 0 & \bmod 5 \end{array}$$

using the fact that $x_n^2 + 1$ is already divisible by 5^n, and the fact that the y^2 term goes away. The last equation has a unique solution

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

where the inverse need be taken only mod 5, not modulo any higher power of 5. The new solution is

$$x_{n+1} = x_n + 5^n y$$

and satisfies

$$x_{n+1} = x_n \bmod 5^n$$

We obtain the sequence of integers

$$2,\ 7,\ 57,\ 182,\ 1482,\ 13057,\ 25182,\ \ldots \sim \sqrt{-1}$$

Remark: The technical point that inverse needed to be taken only modulo 5, not modulo any higher power of 5, is relevant in some applications. Similarly, in the following somewhat more general claim, the inverse is taken only modulo p, not modulo any higher power of p.

This procedure to find the sequence of integers x_n is an example of *Hensel's lemma*. A little more generally:

Claim: Let $f(x) \in \mathbb{Z}[x]$, p a prime, and x_1 such that

$$f(x_1) = 0 \bmod p \qquad \text{and} \qquad f'(x_1) \neq 0 \bmod p$$

Then the recursion [2]

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

(where $f'(x_1)^{-1}$ is an inverse modulo p) determines a sequence of integers x_n such that

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

and

$$x_{n+1} = x_n \bmod p^n$$

Remark: Note that the assertion is that only a single multiplicative inverse is needed, namely $f'(x_1)^{-1}$ modulo p.

Proof: Amusingly, we need a *Taylor series expansion*

$$f(x+h) = f(x) + h \cdot f'(x) + (\text{error term})$$

legitimate for purely algebraic reasons, for polynomials, specifically of the form

$$f(x+h) = f(x) + f'(x) \cdot h + E \cdot h^2$$

where E is a polynomial in x and h with coefficients in $\mathbb{Z}$. [3] Assuming we have such an expression, let [4] $\delta = -f'(x_n)^{-1} \cdot f(x_n)$ and evaluate

$$f(x_{n+1}) = f(x_n + \delta) = f(x_n) + f'(x_n) \cdot \delta + E \cdot \delta^2$$

$$= f(x_n) - f'(x_n) \cdot f'(x_n)^{-1} \cdot f(x_n) + E \cdot \delta^2 = f(x_n) - f(x_n) + E(x_n) \cdot \delta^2 = E \cdot \delta^2$$

Since $f(x_n) = 0 \bmod p^n$, certainly $x_{n+1} = x_n \bmod p^n$, and $f'(x_n) \neq 0 \bmod p$, so has an inverse mod p^n, since f and f' have coefficients in $\mathbb{Z}$. And then $\delta = 0 \bmod p^n$, so $\delta^2 = 0 \bmod p^{2n}$. Since E is a polynomial with coefficients in $\mathbb{Z}$, $E \cdot \delta^2 = 0 \bmod p^{2n}$. That is,

$$f(x_{n+1}) = 0 \bmod p^{2n}$$

For $n \geq 1$, we have $2n \geq n+1$, so this meets our requirement on the recursion.

Note that in the expression

$$x_{n+1} = x_n - f(x_n) \cdot f'(x_n)^{-1} \bmod p^{n+1}$$

since $f(x_n) = 0 \bmod p^n$, we do only need to know $f'(x_n)^{-1}$ modulo p in order to know $x_{n+1} \bmod p^{n+1}$. Thus, it suffices to check that

$$f'(x_1)^{-1} = f'(x_n)^{-1} \bmod p$$

Indeed, since $x_{n+1} = x_n \bmod p^n$, for all n we have $x_n = x_1 \bmod p$. Since f' has coefficients in $\mathbb{Z}$, we have $f'(x_n) = f'(x_1)$ for all n. Since $f'(x_1) \neq 0 \bmod p$, the inverses mod p are all the same.

---

[2] This recursive formula is exactly the Newton-Raphson formula, easily derived geometrically in the real-number case, by finding the intersection of the horizontal axis with the tangent line to the curve $y = f(x)$ at the point $(x_n, f(x_n))$.

[3] The *derivative* of a polynomial can be defined without taking any limits, via the usual formula $\frac{d}{dx}(x^n) = nx^{n-1}$, and requiring that this map be linear over whatever commutative ring the polynomials' coefficient lie in.

[4] Yes, for the moment we use $f'(x_n)^{-1} \bmod p$ rather than $f'(x_1)^{-1}$, since the former occurs more naturally. We will check in a moment that the two expressions have identical values mod p.

To obtain a Taylor expansion, since we can't divide by p, the factorials occurring in the usual form of the Taylor expansion would appear to be a problem. But, in fact, any polynomial $P(x) = \sum_i b_i x^i$ with coefficients in $\mathbb{Z}$ can be written in the form

$$P(x+h) = c_0 + c_1 \cdot h + c_2 \cdot h^2 + \dots \qquad \text{(a finite expansion)}$$

with c_i polynomials in x by substituting $x+h$ in P and expanding in powers of h. Thus, the issue is to see that, in this expansion

$$c_1(x) = f'(x)$$

Since the requisite expansion is *linear* [5] in the polynomial P, it suffices to consider $P(x) = x^n$. Then by the Binomial Theorem

$$(x+h)^n = x^n + nx^{n-1} \cdot h + E \cdot h^2$$

where, indeed, E is a polynomial in x and h, with coefficients in $\mathbb{Z}$. Since nx^{n-1} is the derivative of x^n, we have the desired sort of Taylor expansion, and Hensel's procedure will succeed. ///

Remark: No special properties of the ring $\mathbb{Z}$ were used above, so the same argument succeeds, and this simple case of Hensel's lemma applies, to prime ideals in arbitrary commutative rings with identity.

Remark: This case of Hensel's lemma is merely the simplest, meant to illustrate the point.

Example: Let k be an integer relatively prime to a prime p. Let x_1 be an inverse of k mod p. Then the recursion

$$x_{n+1} = x_n - x_1^{-1} k x_n$$

produces a sequence of integers x_n such that

$$kx_n = 1 \bmod p^n$$

Indeed, letting $f(x) = kx - 1$, we can apply the previous claim. That is, we have the recursion

$$x_{n+1} = x_n - f(x_n) \cdot f'(x_1)^{-1} = x_n - (kx_n - 1) \cdot k^{-1} = x_n - (kx_n - 1) \cdot x_1$$

making use of the fact that we only need the inverse mod p, not any higher power of p. Thus, for $k \neq 0 \bmod p$ we have a sequence of integers x_n such that

$$x_{n+1} = x_n \bmod p^n \qquad \text{and} \qquad k \cdot x_n = 1 \bmod p^n$$

---

2. *The p-adic numbers*

The p-adic **norm** or **absolute value** $|n|_p$ of and integer $n = p^e m$ (with m prime to p) is

$$p\text{-adic norm of } n = |n|_p = p^{-\mathrm{ord}_p n} = p^{-e}$$

where

$$\mathrm{ord}_p n = \text{largest positive integer } e \text{ such that } p^e | n$$

[5] This *linearity* is that the expansion for the sum of two polynomials is the sum of the corresponding expansions.

We must additionally declare that $|0|_p = 0$, or else declare that $\mathrm{ord}_p 0 = +\infty$. [6] The p-adic **metric** [7] on $\mathbb{Z}$ is

$$p\text{-adic distance } m \text{ to } n = |m-n|_p$$

The p-adic norm on $\mathbb{Q}$ extends that on $\mathbb{Z}$, namely

$$|p^n \cdot \frac{c}{d}|_p = p^{-n}$$

where c, d are integers prime to p, and n can be a positive or negative integer. Again, counter-intuitively, p is small and $1/p$ is large:

$$|p|_p = \frac{1}{p} \qquad |\frac{1}{p}|_p = p$$

In summary, *high divisibility by p* means *small*.

Remark: In a context where the p-adic norm is the only norm used, we may suppress the subscript.

Example: The sequences $\{x_n\}$ produced via Hensel's lemma to achieve $f(x_n) = 0 \bmod p^n$ (for given $f(x) \in \mathbb{Z}[x]$) are *Cauchy sequences* [8] in the p-adic metric, since $x_{m+1} = x_m \bmod p^m$ implies that for all pairs of indices $m \leq n$

$$|x_m - x_n|_p \leq |p^m|_p = p^{-m}$$

And, the fact that $f(x_n) = 0 \bmod p^n$ gives

$$\lim_n f(x_n) = 0 \qquad \text{(in the } p\text{-adic metric)}$$

We will define p-adic things as *completions* [9]

$$\begin{array}{rcl} p\text{-adic integers } \mathbb{Z}_p & = & p\text{-adic metric completion of } \mathbb{Z} \\ p\text{-adic numbers } \mathbb{Q}_p & = & p\text{-adic metric completion of } \mathbb{Q} \end{array}$$

but we should check that the p-adic metric really is a metric. The positivity and symmetry of the associated p-adic metric are immediate, but the triangle inequality is not so immediate.

Example: Partly for the visual effect, we note that

$$1 + 2 + 4 + 8 + 16 + \ldots = -1 \qquad (\text{in } \mathbb{Z}_2)$$

This really is valid in $\mathbb{Z}_2$. Superficially, thinking of the real numbers, this might be perceived as a *corruption* of the identity

$$1 + r + r^2 + r^3 + \ldots = \frac{1}{1-r} \quad (\text{for } |r| < 1)$$

[6] Saying that $\mathrm{ord}_p 0 = +\infty$ is common, but invites trouble in arithmetic manipulations of $+\infty$. Similar issues arise in trying to define *degree* for the zero polynomial.

[7] A *metric* $d(,)$ on a set X is a real-valued function d on $X \times X$ meeting some reasonable conditions: *positivity:* $d(x,y) \geq 0$, and $d(x,y) = 0$ only for $x = y$; *symmetry:* $d(x,y) = d(y,x)$; and, least trivial, the *triangle inequality* condition $d(x,y) \leq d(x,z) + d(z,y)$.

[8] This sense of *Cauchy sequence* is completely analogous to that in the real numbers or $\mathbb{R}^n$, namely, that a sequence $\{x_n\}$ is *Cauchy* if for every $\varepsilon > 0$ there is N such that for all $m, n \geq N$ we have $|x_m - x_n|_p < \varepsilon$.

[9] A metric space is **complete** if every *Cauchy sequence* converges. A *completion* of a metric space X is often defined by a construction (given in the appendix below), but, as discussed shortly, the *idea* is that the completion is the smallest complete metric space containing the given one.

which is most familiar for *real* or *complex* r, and with the usual real or complex absolute value $|r|$. But it is *not* a flawed version at all, since it is literally correct 2-adically.

Regarding the triangle inequality, in fact, we have a strange stronger property: [10]

Proposition: *(ultrametric inequality)* For x, y in $\mathbb{Q}$,

$$|x+y| \leq \max\{|x|,\ |y|\}$$

In fact, *equality* occurs in this last inequality, except possibly when $|x| = |y|$. Thus, in terms of the p-adic metric $d(x,y)$,

$$d(x,y) \leq \max\{d(x,z),\ d(z,y)\}$$

with *equality* except possibly when $d(x,z) = d(z,y)$.

Proof: Let $x = p^m \cdot a/b$ and $y = p^n \cdot c/d$ with a, b, c, d prime to p, and positive or negative integers m, n. Without loss of generality, we can suppose that $m \leq n$. Certainly

$$x + y = p^m \cdot \frac{a}{b} + p^n \cdot \frac{c}{d} = \frac{p^m ad + p^n cb}{bd} = p^m \cdot \frac{ad + p^{n-m} cb}{bd}$$

Note that, by unique factorization, bd is still prime to p. For $m < n$, the numerator in the fraction in

$$x + y = p^m \cdot \frac{ad + p^{n-m} cb}{bd}$$

is prime to p. Thus, for $m < n$, that is, for $|x| > |y|$,

$$|x+y| = p^{-m} = |x| = \max\{|x|,\ |y|\}$$

When $m = n$, that is, when $|x| = |y|$, the numerator may be *further* divisible by p in some cases. Thus, for $|x| = |y|$,

$$|x+y| \leq p^{-m} = \max\{|x|,\ |y|\}$$

Then

$$d(x,y) = |x-y| = |(x-z)+(z-y)| \leq \max\{|x-z|,\ |z-y|\} = \max\{d(x,z),\ d(z,y)\}$$

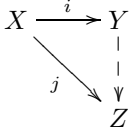
with equality unless possibly when $d(x,z) = d(z,y)$. ///

An **isometry** $f : X \longrightarrow Y$ of metric spaces X, Y is a set map from X to Y such that distances are preserved, namely,

$$d_Y(f(x),\ f(x')) = d_X(x, x')$$

for all x, x' in X. [11] A metric space is **complete** if every Cauchy sequence converges. [12]

Definition: A **completion** Y of a metric space X is a *complete* metric space and an isometry $i : X \longrightarrow Y$ such that, for every isometry $j : X \longrightarrow Z$ to a *complete* metric space Z, there is a unique isometry $J : Y \longrightarrow Z$ giving a commutative diagram



[10] It is traditional at this point to say the the *ultrametric property* proven in the proposition can be construed as asserting that all p-adic triangles are *isosceles*.

[11] Beware that in some contexts an *isometry* is presumed to be a *bijection* to the target, in addition to preserving distance. In our context we specifically do *not* assume that isometries are surjections to the target spaces.

[12] Again, as usual, a sequence $\{x_n\}$ is *Cauchy* if for every $\varepsilon > 0$ there is N such that for all $m, n \geq N$ we have $d(x_m, x_n) < \varepsilon$.

Thus, as usual with mapping-property characterizations, there is at most one completion, up to unique isometric isomorphism. In the appendix below we give the usual construction, which proves *existence*.

Thus, we can define, as expected,

$$\begin{array}{rcl} p\text{-adic integers } \mathbb{Z}_p & = & p\text{-adic metric completion of } \mathbb{Z} \\ p\text{-adic numbers } \mathbb{Q}_p & = & p\text{-adic metric completion of } \mathbb{Q} \end{array}$$

As usual, all operations on the completions are defined as limits, and well-definedness must be proven. That is, for Cauchy sequences of rational numbers x_n and y_n with $x_n \longrightarrow a$ and $y_n \longrightarrow b$ p-adically, define

$$a + b = \lim_n (x_n + y_n) \qquad a \cdot b = \lim_n (x_n \cdot y_n) \qquad |a| = \lim_n |x_n|$$

Proposition: The p-adic norm is a continuous function on the completion. The p-adic norm is *multiplicative* on the completions, that is,

$$|ab| = |a| \cdot |b|$$

Addition, multiplication, and multiplicative inverse (away from 0) are *continuous* maps in the p-adic metric. Also,

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

In particular, $\mathbb{Z}_p$ is both closed and open in $\mathbb{Q}_p$. The p-adic integers $\mathbb{Z}_p$ form an *integral domain*, [13] And $\mathbb{Q}_p$ is its *field of fractions* [14] of $\mathbb{Z}_p$. On $\mathbb{Q}_p$ it is still true that the *ultrametric inequality* holds:

$$|x + y| \leq \max\{|x|, |y|\} \quad \text{(with equality except possibly when } |x| = |y|)$$

Remark: It is the ultrametric property that makes the set of x with $|x| \leq 1$ a subring, since otherwise this set would not be closed under addition. Thus, for example, there is no analogous subring of $\mathbb{R}$.

Proof: From the *general* theory of metric spaces (as in the appendix) the metric $d(,)$ on the completion is defined by taking limits

$$d(a, b) = \lim_n d(x_n, y_n)$$

where x_n, y_n are rational and $x_n \longrightarrow a$ and $y_n \longrightarrow b$. Part of the general assertion is that this is *well-defined*, that is, is independent of the Cauchy sequences approaching a and b. Then, in the present situation, we obtain the extension of the p-adic norms to the completion as a special case, taking $b = 0$, so

$$|a| = d(a, 0) = \lim_n |x_n - 0| = \lim_n |x_n|$$

Then we have the expected

$$|a + b| = |a - (-b)| = d(a, b) \leq d(a, 0) + d(0, b) = |a| + |b|$$

The p-adic continuity of the p-adic norm on $\mathbb{Q}$ is immediate from the continuity of the metric on the completion, which is a general fact about completions.

---

[13] Recall that an *integral domain* is a commutative ring with no proper *zero divisors*, that is, no non-zero elements a, b such that $ab = 0$.

[14] The *field of fractions* of an integral domain R is a field F with an inclusion $i : R \longrightarrow F$ such that any *injection* ring homomorphism of R to a *field* factors through $i : R \longrightarrow F$. A common element-oriented definition of F is as the set of fractions a/b with $a, b \in R$, with $b \neq 0$, modulo the expected equivalence relation that $a/b \sim a'/b'$ if $ab' = a'b$.

The multiplicativity $|xy| = |x| \cdot |y|$ follows for $x, y \in \mathbb{Q}$ from the fact that the ideal $p\mathbb{Z}$ is prime in $\mathbb{Z}$. That is, writing $x = p^m \cdot a/b$ and $y = p^n \cdot c/d$ with a, b, c, d relatively prime to p,

$$xy = p^{m+n} \cdot (ac)/(bd)$$

and by the primality of p the products ac and bd are still prime to p. Then for $x_n \longrightarrow a$ and $y_n \longrightarrow b$ with x_n, y_n in $\mathbb{Q}$,

$$|ab| = \lim_n |x_n y_n| = \lim_n (|x_n| \cdot |y_n|) = \lim_n |x_n| \cdot \lim_n |y_n| = |a| \cdot |b|$$

by continuity of multiplication of real numbers, since $|x_n| \longrightarrow |a|$ and thus $\{|x_n|\}$ is Cauchy in $\mathbb{R}$ (as is $\{|y_n|\}$).

Continuity of addition is easy, from

$$|(x + y) - (x' + y')| \leq |x - x'| + |y - y'|$$

For multiplication,

$$|(xy) - (x'y')| \leq |x(y - y')| + |(x - x')y'| \leq |x(y - y')| + |(x - x')(y' - y)| + |(x - x')y|$$

$$= |x||y - y'| + |x - x'||y' - y| + |x - x'||y|$$

Thus, given x, y in $\mathbb{Q}_p$ and x', y' sufficiently close to them, the products are close.

For multiplicative inverses, let $x \neq 0$. From

$$1 = |1| = |x \cdot x^{-1}| = |x| \cdot |x^{-1}|$$

we have

$$|x^{-1}| = \frac{1}{|x|}$$

and then the continuity of inversion in $\mathbb{R}^\times$ gives our result.

Unsurprisingly, since $\mathbb{Z}$ is a subset of $\mathbb{Q}$, there is the same containment relation between their completions. Since the p-adic absolute value of $x \in \mathbb{Z}$ is at most 1, we immediately have containment in one direction, namely

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

On the other hand, suppose that $y \in \mathbb{Q}_p$ with $|y| \leq 1$. Since $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$, there is $r \in \mathbb{Q}$ arbitrarily close to y. For $|y - r| \leq 1$,

$$|r| \leq \max\{|r - y|, |y|\} = 1$$

so $|r| \leq 1$ itself. Thus, it suffices to show that r itself can be approximated arbitrarily well by elements of $\mathbb{Z}$.

Since $|r| \leq 1$, $r = p^n \cdot \frac{a}{b}$ with $a, b \in \mathbb{Z}$ relatively prime to p and $n \geq 0$. As an example of Hensel's lemma, we saw above that, for $b \neq 0 \bmod p$, there is a sequence of integers x_i such that

$$b \cdot x_i = 1 \bmod p^i$$

That is, x_i is a Cauchy sequence of integers approaching a multiplicative inverse b^{-1} of b in $\mathbb{Q}_p$. By continuity of the norm,

$$|b^{-1}| = \lim_i |x_i| = \lim_n 1 = 1$$

since p does not divide any of the integers x_i. Thus,

$$\lim_i p^n \cdot a \cdot x_i = p^n \cdot a/b = r$$

That is, as i varies the integers $p^n \cdot a \cdot x_i$ get close to r. This proves that $\mathbb{Z}$ is dense in $\{y \in \mathbb{Q}_p : |y| \leq 1\}$, so $\mathbb{Z}_p$ is exactly the latter set, as claimed.

Since the possible values of the p-adic norm are only powers of p, the condition $|x| < p$ implies $|x| \leq 1$.

If $ab = 0$, then $|ab| = 0$, and by multiplicativity $|a| \cdot |b| = 0$. But then a or b is 0. Thus, $\mathbb{Z}_p$ is an integral domain.

Since $\mathbb{Q}$ is a field, it follows fairly easily that its completion $\mathbb{Q}_p$ is a field. To see that $\mathbb{Q}_p$ has no proper subfield that contains $\mathbb{Z}_p$, observe first that we already showed that any element $x \in \mathbb{Q}_p$ with $|x| \leq 1$ lies in $\mathbb{Z}_p$. And for $|x| > 1$, x cannot be 0, so has an inverse (since $\mathbb{Q}_p$ is a field), and $|x^{-1}| < 1$, so lies in $\mathbb{Z}_p$. This proves that $\mathbb{Q}_p$ is the fraction field of $\mathbb{Z}_p$.

Finally, it is not surprising that the ultrametric inequality persists, as follows. Given $a, b \in \mathbb{Q}_p$, let x_n, y_n be rational numbers with $x_n \longrightarrow a$ and $y_n \longrightarrow b$. Given $\varepsilon > 0$, let n be large enough such that $|x_n - a| < \varepsilon$ and $|y_n - b| < \varepsilon$. We can invoke general facts about completions of metric spaces to know that the *triangle inequality* holds, so

$$|x_n + y_n - (a + b)| < |x_n - a| + |y_n - b| < 2\varepsilon$$

Then

$$|a+b| = |(a-x_n)+(b-y_n)|+|x_n+y_n| \leq 2\varepsilon+\max\{|x_n|,|y_n|\} \leq 3\varepsilon+\max\{|x_n|-\varepsilon,|y_n|-\varepsilon\} < 3\varepsilon+\max\{|a|,|b|\}$$

As usual, this is true for every $\varepsilon > 0$, so we obtain the ultrametric inequality. ///

Proposition: The *units* in $\mathbb{Z}_p$ are

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

The ideals in the ring $\mathbb{Z}_p$ are $p^n \cdot \mathbb{Z}_p$ for $0 \leq n \in \mathbb{Z}$. We have $\mathbb{Z} \cap p^n\mathbb{Z}_p = p^n\mathbb{Z}$, and the natural maps

$$\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$$

are *isomorphisms*.

Proof: First, for $x, y \in \mathbb{Z}_p$ such that $xy = 1$, of course

$$1 = |1| = |xy| = |x| \cdot |y|$$

Since $|x| \leq 1$ and $|y| \leq 1$, necessarily they are both 1. Thus,

$$\mathbb{Z}_p^\times \subset \{x \in \mathbb{Z}_p \ : \ |x| = 1\}$$

On the other hand, suppose $|x| = 1$. Let $y \in \mathbb{Z}$ be such that $|x - y| < 1$. Then

$$|y| = |y - x + x| = \max\{|y - x|, \ |x|\} = |x| = 1$$

since the two norms are unequal. Thus, y is an integer not divisible by p. Again, as an example exercise in Hensel's lemma, we found that such y has an inverse in $\mathbb{Z}_p$. And then

$$x = x - y + y = y \cdot (1 + \frac{x - y}{y})$$

gives a way to make a convergent series expression for an inverse to x, namely

$$x^{-1} = y^{-1} \cdot \left((1 - \frac{x - y}{y} + \left(\frac{x - y}{y}\right)^2 - \left(\frac{x - y}{y}\right)^3 + \dots\right)$$

which converges since $|(x-y)/y| < 1$. Thus, x^{-1} exists.

For $x \in \mathbb{Z} \cap p^n\mathbb{Z}_p$, we have $|x| \leq p^{-n}$, so p^n divides x. That is, $x \in p^n\mathbb{Z}$, as claimed. Thus, we have natural *injections*

$$\mathbb{Z}/p^n\mathbb{Z} \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$$

Let $y \in \mathbb{Z}_p$ and consider the coset $y + p^n\mathbb{Z}_p$. Using the density of $\mathbb{Z}$ in $\mathbb{Z}_p$, let $x \in \mathbb{Z}$ with $|y - x| < p^{-n}$. Then $y - x \in p^n\mathbb{Z}_p$, so

$$y + p^n\mathbb{Z}_p = (y-x) + x + p^n\mathbb{Z}_p = p^n\mathbb{Z}_p + x + p^n\mathbb{Z}_p = x + p^n\mathbb{Z}_p$$

which proves the surjectivity. ///

Remark: It is not completely trivial to prove that $\mathbb{Q}_p$ and $\mathbb{Z}_p$ are locally compact from this metric viewpoint.

---

3. *Introductory p-adic analysis*

The behavior of the exponential function for p-adic numbers is quite different from its behavior for real or complex arguments. The details are both amusing and useful. We introduce *formal power series* methods to show that the p-adic exponential and logarithm are mutual inverses.

From the basic metric definition of $\mathbb{Z}_p$ and $\mathbb{Q}_p$, from the ultrametric version of the triangle inequality, we obtain:

Corollary: For p-adic $a_1, \ldots, a_n$,

$$|a_1 + \ldots + a_n| \leq \max\{|a_1|, \ldots, |a_n|\}$$

with equality unless at least two $|a_i|$ are identical. (Induction from the ultrametric property.) ///

Corollary: In the p-adic numbers, Cauchy's *necessary* criterion for the convergence of a sequence $\sum_i a_i$, namely that $|a_i| \longrightarrow 0$, is also *sufficient* for convergence. [15]

Proof: We prove the sufficiency. [16] The difference of the n^{th} and m^{th} partial sums (with $m < n$) is

$$|a_{m+1} + a_{m+2} + \ldots + a_{n-1} + a_n| \leq \max\{|a_{m+1}|, |a_{m+2}|, \ldots, |a_{n-1}|, |a_n|\}$$

Since the individual $|a_n|$ are assumed to go to 0, this maximum goes to 0 as $m \longrightarrow \infty$, so the series converges. ///

Remark: Since an infinite sum converges if the terms go to zero, the distinction between *absolute* and *conditional* convergence disappears here. That is, in effect, any convergent series is absolutely convergent. In particular, *rearrangements* are always permitted. [17]

---

[15] In the real or complex numbers, Cauchy's criterion for convergence of a sum is only *necessary*, and certainly not *sufficient*. It is the fact that p-adic numbers satisfy an *ultrametric* inequality in place of the *triangle* inequality that makes the criterion sufficient in that case.

[16] Necessity is the same as in ordinary calculus, for example, that differences of partial sums, for example $\sum_{i \leq n+1} a_i - \sum_{i \leq n} a_i$, must go to 0 as $n \longrightarrow \infty$. This particular difference is exactly a_{n+1}.

[17] That rearrangements of convergent series are always possible is not hard to see. Suppose that $|a_i|_p \longrightarrow 0$, where i

The **exponential function** does not behave so well p-adically, since the factorials in the denominator which made the power series

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \dots$$

no longer *grow* (helping convergence) but *shrink*, thus impeding convergence.

Recall that $\mathrm{ord}_p x$ is the largest integer e such that $p^e | x$. This still makes sense in $\mathbb{Z}_p$.

Claim: The power series for e^x converges p-adically for

$$\mathrm{ord}_p x > \frac{1}{p-1}$$

Remark: Since $\mathrm{ord}_p x$ is an integer, this gives convergence for $\mathrm{ord}_p x > 0$ for p *odd*, but for $p = 2$ requires $\mathrm{ord}_p x > 1$. [18]

Proof: For a real number r let

$$\mathrm{floor}(r) = \text{greatest integer } n \text{ with } n \le r$$

Then [19]

$$\mathrm{ord}_p n! = \mathrm{floor}(\frac{n}{p}) + \mathrm{floor}(\frac{n}{p^2}) + \mathrm{floor}(\frac{n}{p^3}) + \dots \quad \text{(finitely-many non-zero summands)}$$

This is usefully estimated by

$$\mathrm{ord}_p n! \le \frac{n}{p} + \frac{n}{p^2} + \frac{n}{p^3} + \dots \quad \text{(finitely-many non-zero summands)} = n \cdot \frac{\frac{1}{p}}{1 - \frac{1}{p}} = n \cdot \frac{1}{p-1}$$

Thus, to meet Cauchy's *now-sufficient* criterion for convergence of the series for e^x, we want

$$\lim_n |x^n/n!|_p = 0$$

which is to say that

$$\mathrm{ord}_p x^n/n! \longrightarrow +\infty$$

---

runs through the positive integers. We express a *rearrangement* of the sum $\Sigma_i a_i$ as $\Sigma_i a_{\pi(i)}$ where π be a permutation of the positive integers. To prove that the two sums are equal, first observe that the $a_{\pi(i)}$'s also go to 0, since *going to* 0 means that for each $\varepsilon > 0$ there are only finitely-many $|a_{\pi(i)}| \ge \varepsilon$. Then pick $\varepsilon > 0$, and take N large enough so that both $|a_i| < \varepsilon$ for $i > N$ and $|a_{\pi(i)}| < \varepsilon$ for $i > N$. In the *difference* between partial sums $\sum_{i \le N} a_i$ and $\sum_{i \le N} a_{\pi(i)}$, all the summands with norm at least ε are present in *both* partial sums, so cancel. Thus, the only remaining summands that may not cancel have norm less than ε, and the ultrametric inequality implies that the difference of those partial sums is at most ε. Since these partial sums approach the full sums, and since this holds for every $\varepsilon > 0$, the two infinite sums are equal.

[18] Similarly, for some extension fields k of $\mathbb{Q}_p$, the values of the extension of ord_p to k will not be integers, so the inequality's meaning becomes subtler.

[19] The first summand on the right is (obviously) the number of integers $m \le n$ divisible by p, each contributing at least one factor of p to $n!$. The second summand is the number of integers $m \le n$ divisible by p^2, each such contributing at least one *additional* factor of p to $n!$, and so on.

The estimate we've just derived gives

$$\mathrm{ord}_p x^n/n! = n\mathrm{ord}_p x - \mathrm{ord}_p n! \geq n\mathrm{ord}_p x - n\cdot\frac{1}{p-1} = n\cdot(\mathrm{ord}_p x - \frac{1}{p-1})$$

Thus, for

$$\mathrm{ord}_p x > \frac{1}{p-1}$$

the series for e^x converges. ///

Just to be sure that we understand why the p-adic exponential works as expected, without pretending to invoke differential equations or real-variable calculus accidentally, we prove

Proposition: For $z, w \in \mathbb{Z}_p$ both with ord_p more than $1/(p-1)$

$$e^{z+w} = e^z\, e^w$$

Proof: The most essential point is an application of the binomial theorem, as follows. The condition on ord_p's is to assure convergence, [20] from just above. And, further, $|z+w| \leq \max\{|z|, |w|\}$, so $z+w$ still meets this condition. We compute directly

$$e^{z+w} = \sum_{n\geq 0}\frac{(z+w)^n}{n!} = \sum_n \sum_{0\leq i\leq n}\binom{n}{i} z^{n-i}w^i/n!$$

with binomial coefficients

$$\binom{n}{i} = \frac{n!}{i!\,(n-i)!}$$

as usual. The $n!$'s cancel, leaving

$$e^{z+w} = \sum_n\sum_i \frac{1}{i!\,(n-i)!}\, z^{n-i}w^i = e^z\, e^w$$

as desired. ///

The **logarithm** function's expansion

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \dots$$

behaves less badly than that of e^x, but, still, the denominators become smaller rather than large, so this is still somewhat worse than the real or complex case.

Claim: The usual power series for $\log(1+x)$ converges p-adically for $|x| < 1$.

Proof: The sloppy-but-adequate estimate is

$$\mathrm{ord}_p n \leq \log_p n$$

[20] In fact, the equality is true for *formal power series*, meaning in the projective limit ring $\mathbb{Q}[[z,w]] = \lim_n \mathbb{Q}[z,w]/I^n$ where I is the ideal in $\mathbb{Q}[z,w]$ generated by z and w, and I^n is the ideal generated by n-fold products of elements of I, namely polynomials with all terms of total degree at least n. The same proof works in this context, since only a very limited rearrangement of terms is needed. We use this formal power series viewpoint to prove that the exponential and logarithm are mutual inverses. It bears emphasizing that this formal power series ring is very much akin to the limit construction of $\mathbb{Z}_p$ from $\mathbb{Z}/p^n$.

where the latter logarithm is the usual real-valued one. Then using the *sufficiency* of the p-adic Cauchy's criterion, the series converges if the terms go to 0, which requires that

$$\mathrm{ord}_p(x^n/n) = n \cdot \mathrm{ord}_p x - \log_p n \longrightarrow +\infty$$

This requires that $\mathrm{ord}_p x > 0$, which is $|x| < 1$. ///

Optimistically, apart from the convergence contraints, the following result is exactly as expected.

Proposition: The p-adic exponential and logarithm are mutual inverses on certain regions:

$$\begin{array}{rcll} \log(e^x) & = & x & (\text{for } \mathrm{ord}_p x < 1/(p-1)) \\ e^{\log(1+x)} & = & 1+x & (\text{for } |x| < 1) \end{array}$$

Remark: We will wrap up the combinatorics of a more pedestrian proof of these standard identities, into more intuitive calculus-style arguments by introducing rings of **formal power series** [21]

$$k[[x]] = \lim_n k[x]/(x^n) = x\text{-adic completion of } k[x]$$

over a field k. [22] [23] For our application, $k = \mathbb{Q}_p$. The idea is that we look at power series with coefficients in k without concern for the usual notion of convergence. This does *not* allow us to *evaluate* such series at elements of k, but it *does* allow us to prove many identities that do not actually involve infinite sums of elements of k. The point is to be able to look at *differential equations* satisfied by (formal) power series, even in situations where there are no literal derivatives to be taken. The combinatorial burden is reduced somewhat and organized into the proof (below) of a suitable *chain rule* in a purely algebraic context.

Proof: We have a k-linear map [24]

$$D : k[x] \longrightarrow k[x]$$

given by [25]

$$D(x^n) = nx^{n-1}$$

After verifying the basic properties of D we will prove that D extends to an operator on $k[[x]]$ with the same properties.

The linearity implies that D is additive. Leibniz' rule [26]

$$D(fg) = Df \cdot g + f \cdot Dg$$

[21] We can also define rings of formal power series rings as *metric* completions of $k[x]$, just as $\mathbb{Z}_p$ is often defined as a metric completion of $\mathbb{Z}$. An x-adic *norm* can be defined as $|f(x)| = 2^{-\mathrm{ord}_x f}$ where $\mathrm{ord}_x f = e$ is the maximum integer such that x^e divides the polynomial $f(x)$. Here the constant 2 is irrelevant, and could be replaced by any real number greater than 1.

[22] Sometimes such rings of formal power series are allegedly described as *formal expressions*, but this does not do them justice, and promulgates the notion that mathematics is an activity whose essence is manipulation of strings of marks.

[23] Note that we *cannot* construct the formal power series ring as a *colimit* of (vector spaces of) polynomials of higher and higher degrees, since that colimit would merely be an ascending union, and give us *all* polynomials, rather than any new objects.

[24] Of course we are thinking of *differentiation*, but we are not taking limits of differences.

[25] Viewing x^0 as being 1, this formula implies that D annihilates the copy of k inside $k[x]$ or $k[[x]]$.

[26] There is a story that in the first edition of Leibniz' calculus text it was claimed that the derivative of the product is the product of the derivatives. This was quickly corrected in a new printing.

follows from linearity and the easy

$$D(x^m \cdot x^n) = D(x^{m+n}) = (m+n)x^{m+n-1} = mx^{m-1}x^n + nx^m x^{n-1}$$

We also need the *chain rule*

$$D(f(g(x))) = Dg(x) \cdot (Df)(g(x))$$

It suffices to take $f(x) = x^n$, by linearity of D. Let $g(x) = \sum_{i=0}^d c_i x^i$. Then

$$\begin{aligned} D(g(x)^n) &= \sum_{\ell_0+\ldots+\ell_d=n} \tfrac{n!}{\ell_0!\ldots\ell_d!} c_0^{\ell_0} \ldots c_d^{\ell_d}\ x^{\ell_1+2\ell_2+\ldots d\ell_d} \\ &= \sum_{\ell_0+\ldots+\ell_d=n} \tfrac{n!}{\ell_0!\ldots\ell_d!} c_0^{\ell_0} \ldots c_d^{\ell_d}\ (\ell_1+2\ell_2+\ldots d\ell_d)\ x^{\ell_1+2\ell_2+\ldots d\ell_d-1} \\ &= n\sum_{j=0}^d \sum_{\ell_0+\ldots+\ell_d=n} \tfrac{(n-1)!}{\ell_0!\ldots(\ell_j-1)!\ldots\ell_d!} c_0^{\ell_0} \ldots c_d^{\ell_d}\ jx^{j-1}\ x^{\ell_1+\ldots+j(\ell_j-1)+\ldots d\ell_d} \end{aligned}$$

A little more fooling around does indeed rearrange this to

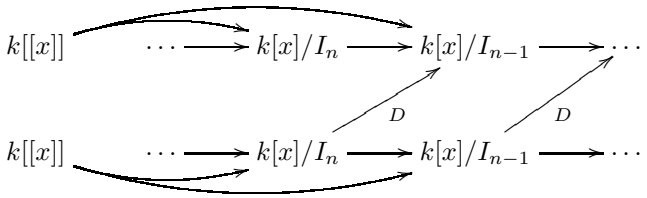
$$Dg(x) \cdot n \cdot g(n)^{n-1}$$

This verifies the chain rule for polynomials.

Now we look at the compatibility of D with the x-adic projective limit. [27] Let I_n be the ideal in $k[x]$ generated by x^n. From Leibniz' rule,

$$D(I_n) \subset I_{n-1}$$

Thus, D gives a map $k[x]/I_n \longrightarrow k[x]/I_{n-1}$, and we have a diagram



This induces a unique (k-linear) map $D : k[[x]] \longrightarrow k[[x]]$. That is, D commutes with taking x-adic limits.

Polynomial multiplication and addition map

$$k[x]/I_n \times k[x]/I_n \longrightarrow k[x]/I_n$$

compatibly with the transition maps $k[x]/I_n \longrightarrow k[x]/I_{n-1}$, so, *as usual*, induce addition and multiplication on $k[[x]]$. The associativity, commutativity, and distributivity follow as usual, also. [28]

The chain rule is more interesting. First, we must be sure not to try to evaluate $f(g(x))$ unless $g \in xk[x]$. Otherwise, we might appear to be taking infinite sums of elements of elements of k, which we eschew. Keeping this in mind, we have the usual *composition*

$$k[x] \times x \cdot k[x] \longrightarrow k[x] \quad \text{by} \quad f(x) \times g(x) \longrightarrow f(g(x))$$

The essential point is that requiring that the argument polynomial be divisible by x gives a (well-defined) map [29]

$$k[x]/I_n \times x \cdot k[x] \longrightarrow k[x]/I_n$$

[27] Charmingly, D does not quite stabilize the ideal generated by x^n, since, after all, it decreases the exponent by 1.

[28] These details were written out in greater detail in the discussion of projective limits of topological groups acting on topological spaces.

[29] If we fail to require that the input polynomial be divisible by x, then the composite will not behave propertly x-adically. For example, for $f(x) = x^m$ and $g(x) = 1 + x$, $f(g(x)) = (1+x)^m$, and the latter is not at all divisible by x.

As usual, [30] this induces a well-defined compatible map

$$k[[x]] \times x \cdot k[[x]] \longrightarrow k[[x]]$$

The compatibility assures that Leibniz' rule and the chain rule still hold.

Now we return to the exponential and logarithm. Now we must assume that the field is of characteristic 0, or else the exponential and logarithm have extra problems due to the denominators in their power series expansions. As in viewing a p-adic integer as the p-adic metric limit of ordinary integers, or, equivalently, as a *compatible* sequence of elements in the limitands of a projective limit, we think of a formal power series as being the sequence of its finite partial sums.

Being careful, observe that

$$\log(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} - \ldots \in x \cdot k[[x]]$$

and that in fact we want inputs to log to be in $1 + x \cdot k[[x]]$ because of this situation. Also, $e^x - 1 \in x \cdot k[[x]]$. As in ordinary analysis, but taking an x-adic limit instead,

$$D(e^x) = \lim_n D(\sum_{i \le n} \frac{x^i}{i!}) == \lim_n \sum_{i \le n} \frac{x^{i-1}}{(i-1)!} = e^x$$

Similarly,

$$D(\log(1+x)) = 1 - x + x^2 - x^3 + \ldots = \frac{1}{1+x}$$

but as an x-adic limit, where x-adically

$$\frac{1}{1+x} = \lim_n (1 - x + x^2 - \ldots \pm x^n)$$

And, unsurprisingly, for $f(x) \in k[[x]]$, if $Df(x) = 0$ then $f(x)$ is in the copy of k inside $k[[x]]$.

Imitating the elementary theory of differential equations, to prove that

$$e^{\log(1+x)} = 1 + x$$

it suffices to show that the constant term of $e^{\log(1+x)}$ is 1, and that (since $D(1+x) = 1$)

$$D\left(e^{\log(1+x)}\right) = 1$$

Use the chain rule to compute

$$D\left(e^{\log(1+x)}\right) = D(\log(1+x)) \cdot e^{\log(1+x)} = \frac{1}{1+x} \cdot e^{\log(1+x)}$$

Now we will see that this differential equation

$$(1+x) \cdot Df = f$$

characterizes f up to scalar multiples, and, in fact, we will see that it must be just $1 + x$. We do this by looking at the power series coefficients. [31] Let $f(x) = \sum_{n \ge 0} c_n\, x^n$. Then the equation is

$$(1+x) \cdot \sum_{n \ge 0} c_n\, n x^{n-1} = \sum_{n \ge 0} c_n\, x^n$$

[30] Yes, limits of products are products of limits, and the multiplication by x likewise commutes with limit-taking.

[31] The case of formal power series is much easier than the case of *convergent* power series, since in the latter a recursive determination of power series coefficients may not lend itself to verification of convergence.

or

$$c_1 + (c_1 + 2c_2)x + (2c_2 + 3c_3)x^2 + (3c_3 + 4c_4)x^3 \ldots = c_0 + c_1 x + c^2 x^2 + \ldots$$

which gives (by equating coefficients) [32]

$$\begin{array}{rcl} c_1 & = & c_0 \\ 2c_2 & = & 0 \\ 3c_3 & = & -c_2 \\ 4c_4 & = & -2c_3 \\ & \ldots & \end{array}$$

Since the characteristic of k is 0, this implies that any $f(x)$ satisfying this differential equation is a constant multiple of $1 + x$. By looking at the 0^{th} coefficient of $e^{\log(1+x)}$, we see that it is exactly $1 + x$. We leave the proof that $\log(e^x) = x$ to the reader. ///

---

4. *Comparison with projective limit definition of $\mathbb{Z}_p$*

Now we connect the classical metric-completion definition of $\mathbb{Z}_p$ with the (projective) limit definition

$$\mathbb{Z}_p = \lim_n \mathbb{Z}/p^n$$

Theorem: The projective limit $\lim_n \mathbb{Z}/p^n$ is isomorphic [33] to the p-adic metric completion $\mathbb{Z}_p$ of $\mathbb{Z}$. The projections are

$$p_n \ : \ \mathbb{Z}_p \xrightarrow{\text{quotient}} \mathbb{Z}_p/p^n\mathbb{Z}_p \xrightarrow{\text{isom}} \mathbb{Z}/p^n$$

where the isomorphism $\mathbb{Z}_p/p^n\mathbb{Z}_p \approx \mathbb{Z}/p^n$ is the natural one proven earlier.

Remark: We give two proofs, one emphasizing the limit viewpoint, the other emphasizing the metric viewpoint.

Proof: First, the maps $q_n : \mathbb{Z}_p \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p \approx \mathbb{Z}/p^n$ give a compatible family of (continuous!) maps to the limitands in $\lim_n \mathbb{Z}/p^n$, so induce a map of $\mathbb{Z}_p$ to the limit. For each non-zero element $x \in \mathbb{Z}_p$, there is some exponent n such that the image of x in $\mathbb{Z}_p/p^n\mathbb{Z}_p$ is non-zero, so $\mathbb{Z}_p$ *injects* to the limit. Thus, we might guess that $\mathbb{Z}_p$ *is* the limit, and try to verify this. [34] Let $f_n : Z \longrightarrow \mathbb{Z}/p^n$ be a compatible family of maps from another object [35] For fixed $z \in Z$, for each n choose $x_n \in \mathbb{Z}$ such that [36]

$$x_n + p^n\mathbb{Z}_p = f_n(z)$$

We claim that the sequence x_n is a *Cauchy* sequence in $\mathbb{Z}_p$, so by completeness we could take a limit

$$f(z) = \lim_n x_n \in \mathbb{Z}_p$$

[32] Yes, unsurprisingly, two formal power series are equal if and only if all their coefficients are equal, for if the coefficients of x^n were different, then the series would be different modulo x^{n+1}.

[33] Isomorphic as topological *ring*, in fact.

[34] Note that the argument so far applies as well to $\mathbb{Z}$ itself, which does indeed inject to the limit, but is a proper subobject.

[35] We can give this argument for topological groups, or for topological rings, etc.

[36] That there exists such x_n is the content of the assertion that the natural map $\mathbb{Z}/p^n \longrightarrow \mathbb{Z}_p/p^n\mathbb{Z}_p$ is an isomorphism.

The Cauchy-ness follows from the compatibility of the f_n's, and, then, the necessary compatibility of the integer representatives x_n. This defines a map $f : Z \longrightarrow \mathbb{Z}_p$ compatible with the f_n's and the projections. We still need to show that there is a *unique* such f to have proven that $\mathbb{Z}_p$ is the limit. Indeed, if f and g were two maps compatible with the projections and f_n's, then

$$0 = p_n\left(f(z) - g(z)\right) \in \mathbb{Z}/p^n \approx \mathbb{Z}_p/p^n\mathbb{Z}_p$$

Taking the intersection over n gives the uniqueness $f(z) = g(z)$. This proves that $\mathbb{Z}_p$ is the limit. ///

Proof: (Second) For a second sort of proof, we will prove that the limit is also a completion of $\mathbb{Z}$ with respect to a metric which agrees on $\mathbb{Z}$ with the p-adic metric, and is complete, so (by the uniqueness of *completions*) naturally isomorphic to the completion $\mathbb{Z}_p$ of $\mathbb{Z}$. We need a bit of general discussion of products and limits of metric spaces:

Claim: A *countable* product $\prod_i X_i$ of metric spaces X_i is *metrizable*. If every X_i is *complete*, then the product is complete.

Remark: Further, we will use explicit expressions for the metric on the product. For example, letting $d_i(,)$ be the metric on X_i, the expression

$$d(\{x_i\},\{y_i\}) = \sum_{n\geq 1} 2^{-n}\,\frac{d_n(x_n,y_n)}{1+d_n(x_n,y_n)}$$

will give a metric on the product. The oddness of this expression is put into context better by realizing several things. First, the powers of 2 appearing can be replaced by *any* sequence of positive real numbers whose sum converges. Second, the expressions

$$\frac{d_i(x_i,y_i)}{1+d_i(x_i,y_i)}$$

have the effect of giving new metrics (giving the same topology) on the X_i which are *bounded* by 1. Further, the 1 in the denominator of the latter expression can be replaced by any positive real number if we want, still giving the same topology. Indeed, for notational ease, let us replace each $d_i(,)$ by $d_i(,)/(1+d_i(,))$, so that we effectively assume that the metric on each of the factors is *already* bounded by 1. Thus, we won't need to carry along the more complicated expressions.

Remark: The extreme ambiguity of the constants reminds us that many different metrics can give the same topology. Thus, a topology cannot possibly specify a canonical metric, in general. The uniqueness of the *topology* on a product has no canonical metric analogue.

Proof: (of claim) It is easy and not so interesting to verify that $d(,)$ gives a metric on the product. It is more interesting to see that it gives the product topology. [37] The trick is that a condition of the form

$$d(\{x_i\},\{y_i\}) < \varepsilon$$

gives no condition whatsoever on x_i and y_i for i large enough such that $2^{-i} < \varepsilon/2$, since

$$\frac{1}{2^i} + \frac{1}{2^{i+1}} + \frac{1}{2^{i+2}} + \frac{1}{2^{i+3}} + \ldots = \frac{2^i}{1-\frac{1}{2}} = 2\cdot 2^{-i} < \varepsilon$$

[37] It is especially interesting to see that this metric gives the product topology if one still thinks of the product topology as being disappointingly coarse. That is, it might seem unlikely that it could arise from a metric, but it does.

and since $d_i(x_i, y_i)/(1 + d_i(x_i, y_i)) < 1$ for all inputs. [38] Thus, for fixed $x = \{x_i\}$ in the product, the collection of $y = \{y_i\}$'s within distance $\varepsilon > 0$ of x includes the whole $X_i \times X_{i+1} \times \ldots$ for some large-enough index i.

More precisely, given $d(x, y) < \varepsilon$, necessarily $d_i(x_i, y_i) < 2^i \cdot \varepsilon$ for all i. Thus, given a collection of open balls in the individual X_i's, almost all [39] of them being the whole X_i, we can choose $\varepsilon > 0$ such that the resulting ball in the $d(,)$ metric is *contained in* the product of those balls.

Conversely, given x in the product and $\varepsilon > 0$, taking n large enough such that $2^{-n} < \varepsilon/2$, the product

$$(\varepsilon\text{-ball at } x_1) \times (\varepsilon\text{-ball at } x_2) \times \ldots (\varepsilon\text{-ball at } x_n) \times X_{n+1} \times X_{n+2} \times \ldots$$

is contained in the ε-ball at x. Thus, the two topologies are the same.

The more serious part of the claim is the completeness. [40] Given a Cauchy sequence $\{x^{(k)}\}$ in the product with the funny metric, since the metric on the product dominates the (bounded-by-1) metrics on the factors, for each index i the i^{th} components $\{x_i^{(k)}\}$ are Cauchy in X_i, so have a limit x_i in X_i. It is irresistible to suspect that the point $x = \{x_i\}$ in the product is the limit of the original Cauchy sequence. Indeed, given $\varepsilon > 0$, take n large enough such that $2^{-n} < \varepsilon/2$. Let N be large enough such that for $k \geq N$ for each of the *finitely*-many $i \leq n$

$$d(x_i^{(k)}, x_i) < \varepsilon$$

Then it easily follows that for $k \geq N$

$$d(\{x_i^{(k)}\}, \{x_i\}) < \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \ldots + \frac{\varepsilon}{2^n} + \frac{2^{-(n+1)}}{1 - \frac{1}{2}} < \frac{\varepsilon}{2} + \frac{\varepsilon}{4} + \ldots + \frac{\varepsilon}{2^n} + \frac{\varepsilon}{2} = \varepsilon$$

That is, the original Cauchy sequence does indeed have the anticipated limit. Thus, with this funny metric, the product is *complete*. ///

Keep in mind that projective limits are subsets of the corresponding products, and can be given the metric from the product by restriction. Since *closed* subsets of complete metric spaces are complete, [41]

Now we can complete the metric-space proof that the projective limit definition of $\mathbb{Z}_p$ is the same as the metric one. The discussion just completed shows that $\lim_n \mathbb{Z}/p^n$ does have a structure of complete metric space. What remains is to show that this is the same as that on $\mathbb{Z}_p$. To do so, we show that we can choose a particular form of the metric on the limit such that the restrictions of the two metrics to $\mathbb{Z}$ are identical. We also must show that $\mathbb{Z}$ is *dense* in $\lim_n \mathbb{Z}/p^n$, and then we're done, by the uniqueness of metric completions.

Returning to the funny expressions for metrics on a countable product, give $\mathbb{Z}/p^n$ the natural metric that *any* discretely topologized set can be given, namely

$$d_n(x, y) = \begin{cases} 1 & (\text{for } x \neq y) \\ 0 & (\text{for } x = y) \end{cases}$$

[38] A nearly identical phenomenon occurs no matter what constants we use to define the metric on the product. This *cut-off* phenomenon is the crucial mechanism.

[39] This standard usage of *almost all* means *all but finitely-many*.

[40] But completeness, too, comes down to the odd cut-off phenomenon that already made this metric topology as coarse as it must be to be the product topology.

[41] That topologically closed subsets of complete metric spaces are again complete is straightforward: a Cauchy sequence in the subset does have a limit in the whole space by the completeness of the larger space, and the limit point lies in the subset, by closedness.

Being a little clever in choice of constants, we try

$$d(\{x_n\},\{y_n\}) = \sum_{n\geq 1} p^{-n}\cdot d(x_n,y_n)$$

Unlike points in the whole product $\Pi_n \mathbb{Z}/p^n$, points in the limit have a compatibility condition. Thus, given $\{x_n\} \neq \{y_n\}$ in the limit, there is a largest index N such that $x_n = y_n$ for $n \leq N$ and $x_n \neq y_n$ for $n > N$. With this N,

$$d(\{x_n\},\{y_n\}) = \sum_{1\leq n\leq N} p^{-n}\cdot 0 + \sum n > Np^{-n}\cdot 1 = \frac{p^{-(N+1)}}{1-\frac{1}{p}} = p^{-N}\cdot\frac{1}{p-1}$$

When $\{x_n\}$ and $\{y_n\}$ come from integers x, y, the integer N is the maximal one such that p^N divides $x-y$, so

$$d(x,y) = |x-y|_p \cdot \frac{1}{p-1}$$

That is, up to the easily reparable constant $1/(p-1)$, this contrived metric agrees on $\mathbb{Z}$ with the p-adic one.

Finally, we should show that $\mathbb{Z}$ is dense in the limit. Note that denseness is an intrinsic topological property, not necessarily metric, but since we've already made up the metric we may as well use it on this occasion. Given a compatible sequence $\{x_n\}$ in the limit, and given $\varepsilon > 0$, let n be large enough such that $p^{-(n+1)} < \varepsilon/2$. Let x be an integer such that $x = x_n \bmod p^n$. Then the same sort of calculation gives

$$d(x,\{x_n\}) \leq \sum_{1\leq i\leq n} p^{-i}\cdot 0 + \sum i > np^{-i}\cdot 1 = \frac{p^{-(n+1)}}{1-\frac{1}{p}} = p^{-n}\cdot\frac{1}{p-1} < \varepsilon$$

Thus, $\mathbb{Z}$ is dense in the limit, so the limit is its metric completion. This proves (a second time) that the limit is the same as the metric completion definition of $\mathbb{Z}_p$. ///

---

5. *Comparison of definitions of* $\mathbb{A}$

To understand the comparison of definitions of the adeles $\mathbb{A}$, we should first review the simpler case of $\mathbb{Q}_p$.

The most pedestrian definition of $\mathbb{Q}_p$ is as p-adic completion of $\mathbb{Q}$, from which it follows readily (as earlier, above) that it is the field of fractions of $\mathbb{Z}_p$.

The expression

$$\mathbb{Q}_p = \bigcup_n p^{-n}\cdot\mathbb{Z}_p$$

of $\mathbb{Z}_p$ as a colimit of topological (additive) *groups* does *not* directly express $\mathbb{Q}_p$ as a *ring*, certainly not as a colimit of rings. Nevertheless, the limitands in the colimit behave reasonably, in the sense that

$$p^{-m}\,\mathbb{Z}_p \cdot p^{-n}\,\mathbb{Z}_p \subset p^{-(m+n)}\,\mathbb{Z}_p$$

so that the ring structure on $\mathbb{Z}_p$ (as limit) and the obvious multiplicative properties of powers of p give the colimit a ring structure.

Recall that we have defined the adeles $\mathbb{A}$ as

$$\mathbb{R}\times\mathbb{A}_{\text{fin}}$$

where the *finite* adeles $\mathbb{A}_{\text{fin}}$ are defined to be

$$\mathbb{A}_{\text{fin}} = \text{colim}_n \frac{1}{n}\cdot\widehat{\mathbb{Z}}$$

with the indexing poset being positive integers ordered by *divisibility*, not magnitude, and where, as earlier,

$$\widehat{\mathbb{Z}} = \lim_n \mathbb{Z}/n \approx \Pi_{p \text{ prime}} \mathbb{Z}_p$$

with positive integers again ordered by divisibility, not magnitude. This gives a strict colimit expression for $\mathbb{A}$ as topological group, but not as *ring*.

By contrast, one usual definition of $\mathbb{A}$ is a sort of colimit, but usually without mentioning the notion explicitly, [42] as follows. For a finite set S of primes, [43] including the infinite prime ∞, and let

$$\mathbb{A}_S = \Pi_{\mathfrak{p} \in S} \mathbb{Q}_p \times \Pi_{p \notin S} \mathbb{Z}_p$$

For $S \subset S'$ there is an obvious inclusion

$$\mathbb{A}_S \subset \mathbb{A}_{S'}$$

and the adeles $\mathbb{A}$ are the strict colimit

$$\mathbb{A} = \text{colim}_S \mathbb{A}_S$$

where S is in the poset of finite subsets of the set of all primes (including the nominal prime at infinity) ordered by inclusion. This *is* a countable strict colimit of topological rings, and each limitand is *open* in its successors, so we are in a good situation. But why consider this particular colimit at all?

We can write a slightly different and more natural (ring) colimit to express $\mathbb{A}$. To warm up to this, we first do an easier case. Without using in advance the fact that $\mathbb{Q}_p$ is the field of fractions of $\mathbb{Z}_p$, and that $\mathbb{Z}_p[1/p] = \mathbb{Q}_p$, we can prove that there exists a natural colimit topology on $\mathbb{Z}_p[1/p]$. [44]

Claim: The colimit

$$\text{colim}(\ \mathbb{Z}_p \xrightarrow{\times p} \mathbb{Z}_p \xrightarrow{\times p} \mathbb{Z}_p \xrightarrow{\times p} \cdots\ )$$

of topological *groups* has a natural *ring* structure in which the multiplication is continuous, and the ring structure is

$$\mathbb{Z}_p[\frac{1}{p}] \approx \text{colim}(\ \mathbb{Z}_p \xrightarrow{\times p} \cdots\ )$$

Proof: The idea of the argument is to observe that the colimit is isomorphic, as topological *group*, to

$$\text{colim}(\ \mathbb{Z}_p \xrightarrow{\text{inc}} \tfrac{1}{p} \cdot \mathbb{Z}_p \xrightarrow{\text{inc}} \tfrac{1}{p^2} \cdot \mathbb{Z}_p \xrightarrow{\text{inc}} \cdots\ )$$

Apart from the first one, the limitands are not rings, but the product of an element $p^{-m}x \in p^{-m}\mathbb{Z}_p$ and $p^{-n}y \in p^{-n} \cdot \mathbb{Z}_p$ is definable as

$$(p^{-m}x) \cdot p^{-n}y = p^{-(m+n)}\, x \cdot y \quad (\text{where } x, y \in \mathbb{Z}_p)$$

[42] The usual terminology is something about *restricted direct products*, but, in fact, these are (strict) colimits.

[43] Further, to talk about $\mathbb{R}$ at the same time as all the other completions $\mathbb{Q}_p$, often one talks as though there were a *prime* ∞ whose corresponding completion is $\mathbb{R}$. This has no content apart from allowing a uniform language. It is more proper to speak of *places* rather than *primes* as a generalized notion that includes both genuine primes and the standard metric that yields $\mathbb{R}$, but insisting on using *place* is pointless. Thus, *the infinite prime* is just the index ∞ that allows us to talk about $\mathbb{R}$ in the same manner we talk about $\mathbb{Q}_p$.

[44] We have several choices of characterization of $\mathbb{Z}_p[1/p]$. The *intent* is that this be an enlargement of $\mathbb{Z}_p$ in which p is invertible. One natural choice is that $\mathbb{Z}_p[1/p]$ should be a topological ring with a continuous ring homomorphism $i\mathbb{Z}_p \longrightarrow \mathbb{Z}_p[1/p]$ such that any continuous ring homomorphism $\mathbb{Z}_p \longrightarrow Y$ where p is invertible in Y *factors uniquely* through i. This mapping property characterization immediately shows, by the usual argument, that there is at most one such thing.