Math 55a, Fall 2004

Third Assignment, Solutions
Adapted from Andrew Cotton, George Lee, and Tseno Tselkov

Problem 1.
(a) Here are a few observations and terms used often in this proof:

(1) Note that we can rework conditions to show that a Cauchy sequence $\{x_k\}$ converges to a rational x_∞ exactly when $\{v_p(x_k - x_\infty)\} \to \infty$. Specifically, $\{x_k\} \to 0$ exactly when $\{v_p(x_k)\} \to \infty$.

(2) We claim that for $a, b \in \mathbb{Q}, v_p(a+b) \geq \min(v_p(a), v_p(b))$, where equality occurs if (although not necessarily only if) $v_p(a) \neq v_p(b)$. Suppose without loss of generality that $v_1 = v_p(a) \leq v_2 = v_p(b)$. If $v_2 = \infty$ then $b = 0$ and the claim is obvious. Otherwise, v_1 and v_2 are both finite integers so we can write $a = p^{v_1} \cdot \frac{c}{d}$ and $b = p^{v_2} \cdot \frac{e}{f}$ for integers c, d, e, f not divisible by p. Then

$$a + b = p^{v_1}\left(\frac{c}{d} + p^{v_2 - v_1}\frac{e}{f}\right) = p^{v_1} \cdot \frac{cf + de \cdot p^{v_2 - v_1}}{df}.$$

Since $p \not| \, df$, we have $v_p(a+b) \geq v_1 = \min(v_1, v_2)$. And if $v_1 \neq v_2$, then p divides $de \cdot p^{v_2 - v_1}$ but not cf so p doesn't divide the numerator — and $v_p(a+b) = v_1$, as claimed.

(3) It is easily verified that $v_p(ab) = v_p(a) + v_p(b)$ for $a, b \in \mathbb{Q}$.

Lemma 1. *If the Cauchy sequence $\{x_k\}$ does not converge to 0, then the sequence $\{v_p(x_k)\}$ eventually equals some finite constant.*

Proof: $\{x_k\} \to 0$ if $\forall t \in \mathbb{Z}$, $\exists N$ s.t. $i \geq N \Rightarrow v_p(x_i) \geq t$.

Thus if $\{x_k\}$ does *not* converge to 0, then $\exists t \in \mathbb{Z}$ s.t. $\forall N$, $\exists i \geq N$ s.t. $v_p(x_i) < t$. Set this t in stone.

Now, since $\{x_k\}$ is a Cauchy sequence, $\exists N$ s.t. $i, j \geq N \Rightarrow v_p(x_i - x_j) > t$. Set this N is stone as well. Then we know by the choice of t that $\exists m \geq N$ with $v_p(x_m) = r < t$. Set m and r in stone.

Now if there were some $i \geq N$ such that $v_p(x_i) = s \neq r$, then $v_p(x_i - x_m) = \min(r, s) \leq r < t$, a contradiction. Thus $v_p(x_N), v_p(x_{N+1}), \ldots$ all equal the same value r, and $\{v_p(x_k)\}$ *does* become constant, as claimed. □

Corollary 1. *For a Cauchy sequence $\{x_k\}$, there exist N and T such that $i \geq N \Rightarrow v_p(x_i) \geq T$.*

Proof: If $\{v_p(x_i)\}$ becomes a constant α, then we can choose $T = \alpha$ and N sufficiently large. Otherwise $\{x_k\}$ converges to 0 so $\{v_p(x_i)\}$ converges to ∞ — so for *any* T, we can find such an N. □

Theorem 1. *Given Cauchy sequences $X = \{x_k\}$ and $Y = \{y_k\}$, the following are also Cauchy sequences:*

(i) $X + Y = \{x_k + y_k\}$.
(ii) $XY = \{x_k y_k\}$.
(iii) $\frac{1}{X} = \left\{ \begin{array}{ll} \frac{1}{x_k} & \textit{if } x_k \neq 0 \\ 1 & \textit{if } x_k = 0 \end{array} \right\}$ *if X does not converge to* 0.
(iv) $-X = \{-x_k\}$.

Proof:
(i) Given t, eventually both $v_p(x_i - x_j)$ and $v_p(y_i - y_j)$ always exceed t. Thus for such i,

$$\begin{array}{rcl} v_p((x_i + y_i) - (x_j + y_j)) & = & v_p((x_i - x_j) + (y_i - y_j)) \\ & \geq & \min(v_p(x_i - x_j), v_p(y_i - y_j)) \\ & > & t \end{array}$$

as well — so $X + Y$ is a Cauchy sequence also.

(ii) First suppose that either X or Y converges to 0 — WLOG, X. Then $v_i = v_p(x_i) \to \infty$ while $v_p(y_i)$ eventually is always at least some constant T; so that $v_p(x_i y_i) \geq v_i + T$ converges to infinity. Thus $XY \to 0$, and since it converges it must be a Cauchy sequence.

Now suppose that neither X nor Y converges to 0; then $v_p(x_i)$ and $v_p(y_i)$ eventually equal some finite constants α and β.

For each $t \in \mathbb{Z}^+$, eventually $v_p(x_i - x_j) > t + \alpha$ and $v_p(y_i - y_j) > t + \beta$. For such i, j, write $x_i = p^\alpha \frac{a}{c}$ and $x_j = p^\alpha \frac{b}{c}$ for integers a, b, c not divisible by p. Then $t + \alpha < v_p(x_i - x_j) = v_p\left(p^\alpha \cdot \frac{a-b}{c}\right)$, so $a \equiv b \pmod{p^t}$. Next write $y_i = p^\beta \frac{d}{f}$ and $y_j = p^\beta \frac{e}{f}$ for integers d, e, f not divisible by p. As above, we must have $d \equiv e \pmod{p^t}$.

Now $x_i y_i - x_j y_j = p^{\alpha+\beta}(\frac{ad-be}{cf})$. But $ad \equiv be \pmod{p^t}$ while $p \not| cf$, so eventually $v_p(x_i y_i - x_j y_j) \geq \alpha + \beta + t$. And since we can choose arbitrarily large t, this implies that XY is indeed a Cauchy sequence.

(iii) Since X does not converge to 0, from the lemma $v_p(x_i)$ eventually equals finite some constant α. At this point no x_i equals 0 so we can safely take their reciprocals.

Let $\{y_k\} = \left\{\frac{x_k}{p^\alpha}\right\}$ so that $v_p(y_i)$ and $v_p(y_i y_j)$ eventually equal 0. Since X is a Cauchy sequence, for any $t \in \mathbb{Z}$ eventually $v_p(x_i - x_j) > t + 2\alpha$.

Thus for any t, eventually

$$\begin{aligned} v_p\left(\frac{1}{x_i} - \frac{1}{x_j}\right) &= v_p\left(p^{-2\alpha}\frac{x_j - x_i}{y_i y_j}\right) \\ &> \underbrace{-2\alpha}_{p^{-2\alpha}} + \underbrace{t + 2\alpha}_{x_j - x_i} + \underbrace{0}_{y_i y_j} \\ &= t. \end{aligned}$$

Thus $\frac{1}{X}$ is indeed a Cauchy sequence.

(iv) For every integer t eventually $v_p(x_i - x_j) > t$ so that $v_p(-x_i - (-x_j)) = v_p(x_i - x_j) > t$ as well. $-X$ is indeed a Cauchy sequence. □

As described in class, we can view $\mathbb{Q}_p$ as the set of equivalence classes of Cauchy sequences of — where $\{x_k\}$ and $\{y_k\}$ are equivalent when $\{\|x_k - y_k\|_p\}$ converges to 0 in $(\mathbb{R}, ||)$. So for any such equivalence class $\overline{X}$, let $X = \{x_1, x_2, \dots\} \in \overline{X}$ be a representative Cauchy sequence; and for any Cauchy sequence $X = \{x_1, x_2, \dots\}$ of elements in $\mathbb{Q}$, let $\overline{X}$ denote the equivalence class containing that sequence. So simply define

$$\begin{array}{ll} v_p(\overline{X}) = \lim_{k\to\infty} v_p(x_k) & \|\overline{X}\|_p = \lim_{k\to\infty} \|x_k\|_p \\ \overline{X} + \overline{Y} = \overline{X + Y} & \overline{X} \cdot \overline{Y} = \overline{XY} \\ \frac{1}{\overline{X}} = \overline{\frac{1}{X}} & -\overline{X} = \overline{-X}, \end{array}$$

where $\lim_{k\to\infty} v_p(x_k)$ can also be ∞. From the theorem, the bottom four operations indeed yield equivalence classes of Cauchy sequences; and from the lemma, the top two quantities indeed exist since $v_p(x_k)$ either eventually equals some constant v (so that $\lim k \to \infty \|x_k\|_p = p^{-v}$), or converges to ∞ (so that $\lim k \to \infty \|x_k\|_p = 0$).

All that remains (sigh...) is to verify that these definitions are independent of the choice of representatives for $\overline{X}$ and $\overline{Y}$, and also that these operations work on the "rational p-adics" the same way that they work for regular rationals. First we prove the choice of representatives is irrelevant — notice that since $\overline{X} + \overline{Y}$ and $\overline{X} \cdot \overline{Y}$ are symmetrically defined, we can just prove that the addition is independent of $\overline{X}$'s representative. (Thus if $\overline{X_1} = \overline{X_2}$ and $\overline{Y_1} = \overline{Y_2}$, then $\overline{X_1} + \overline{Y_1} = \overline{X_2} + \overline{Y_1} = \overline{X_2} + \overline{Y_2}$, and similarly $\overline{X_1} \cdot \overline{Y_1} = \overline{X_2} \cdot \overline{Y_1} = \overline{X_2} \cdot \overline{Y_2}$.)

- *p-adic Absolute Value.*

  Suppose without loss of generality that $v = \lim_{k\to\infty} v_p(a_k) < \lim_{k\to\infty} v_p(b_k)$. If $v_p(a_k) = \infty$ then $v_p(b_k) = \infty$ so $\|\overline{\{a_k\}}\|_p = \|\overline{\{b_k\}}\|_p = 0$. Otherwise eventually $v_p(b_i) > v_p(a_i) = v$, so that $v_p(a_i - b_i) = \min(v_p(a_i), v_p(b_i)) = v$ and $\{v_p(a_k - b_k)\} \not\to \infty$, a contradiction. Thus $v_p(\overline{\{a_k\}}) = v_p(\overline{\{b_k\}})$ and therefore $\|\overline{\{a_k\}}\|_p = \|\overline{\{b_k\}}\|_p$.
- *Addition.* Suppose that $\overline{X} = \overline{\{a_k\}} = \overline{\{b_k\}}$, and $\overline{Y} = \overline{\{y_k\}}$. We wish to prove that $\overline{\{a_k + y_k\}} = \overline{\{b_k + y_k\}}$ — that is, $\{d_p(a_k + y_k, b_k + y_k)\} = \{\|a_k - b_k\|_p\}$ converges to 0 in $(\mathbb{R}, ||)$. But this is precisely what $\overline{\{a_k\}} = \overline{\{b_k\}}$ implies!

- *Multiplication.* Again, suppose that $\overline{X} = \overline{\{a_k\}} = \overline{\{b_k\}}$, and $\overline{Y} = \overline{\{y_k\}}$. We wish to prove that $\overline{\{a_k y_k\}} = \overline{\{b_k y_k\}}$ — that is, $\{d_p(a_k y_k, b_k y_k)\} = \{\|(a_k - b_k) y_k\|_p\}$ converges to 0 in $(\mathbb{R}, ||)$ . . . or in other words, that $\{v_p((a_k - b_k) y_k)\} \to \infty$. But there is some T such that eventually $y_i \geq T$. Then for any $t \in \mathbb{Z}$, eventually $v_p(a_i - b_i) > t - T$ as well, so $v_p((a_i - b_i) y_i) > t$, as desired.
- *Reciprocation.* Again, suppose that $\overline{X} = \overline{\{a_k\}} = \overline{\{b_k\}}$. From the work on the p-adic absolute value above, $\{v_p(a_k)\} \to \infty \iff \{v_p(b_k)\} \to \infty$ so that $\{a_k\} \to 0 \iff \{b_k\} \to 0$. Thus reciprocation is *defined* for $\overline{\{a_k\}}$ if and only if it is defined for $\overline{\{b_k\}}$.

  Now suppose that $\{a_k\}, \{b_k\} \not\to 0$ but $\{a_k - b_k\} \to 0$. Since $v_p(b_k - a_k) = v_p(a_k - b_k) \to \infty$, but $v_p(a_k b_k) = v_p(a_k) + v_p(b_k)$ eventually equals some constant $\alpha + \beta$, the sequence $\left\{ v_p \left(\frac{1}{b_k} - \frac{1}{a_k} \right) \right\} = \left\{ v_p \left(\frac{a_k - b_k}{a_k b_k} \right) \right\} \to \infty$, as desired.
- *Negation.* Again, a nice easy proof: if $\overline{\{a_k\}} = \overline{\{b_k\}}$, then $\{v_p(-a_k - (-b_k))\} = \{v_p(a_k - b_k)\} \to 0$ so $\overline{\{-a_k\}} = \overline{\{-b_k\}}$, as desired.

Finally, for any rationals x, y, the corresponding p-adics are $\overline{X}$ containing $(x) = \{x, x, \dots\}$ and $\overline{Y}$ containing $(y) = \{y, y, \dots\}$. Then $\overline{X} + \overline{Y} = \overline{(x)} + \overline{(y)} = \overline{(x + y)}$, so addition on the "rational p-adics" corresponds to addition on rationals. Similar arguments apply to the other operations, and we are finally, finally done.

(b) These properties follow fairly immediately from the definitions of the operations in part (a). Given p-adics $\overline{X}$, $\overline{Y}$, $\overline{Z}$ with Cauchy-sequence-representatives $X = \{x_k\}$, $Y = \{y_k\}$, $Z = \{z_k\}$ we have

- $\overline{X} + (\overline{Y} + \overline{Z}) = \overline{\{x_k + (y_k + z_k)\}} = \overline{\{(x_k + y_k) + z_k\}} = (\overline{X} + \overline{Y}) + \overline{Z}$
- $\overline{X} \cdot (\overline{Y} \cdot \overline{Z}) = \overline{\{x_k(y_k z_k)\}} = \overline{\{(x_k y_k) z_k\}} = (\overline{X} \cdot \overline{Y}) \cdot \overline{Z}$
- $\overline{X} + \overline{\{0,0,0,\dots\}} = \overline{\{0,0,0,\dots\}} + \overline{X}$
  $= \overline{\{x_1 + 0, x_2 + 0, x_3 + 0, \dots\}} = \overline{\{x_1, x_2, x_3, \dots\}} = \overline{X}$
- $\overline{X} \cdot \overline{\{1,1,1,\dots\}} = \overline{\{1,1,1,\dots\}} \cdot \overline{X}$
  $= \overline{\{x_1 \cdot 1, x_2 \cdot 1, x_3 \cdot 1, \dots\}} = \overline{\{x_1, x_2, x_3, \dots\}} = \overline{X}$
- $\overline{X} \cdot \overline{1/X} = \overline{\{x_k \cdot 1/x_k\}} = \overline{\{1,1,1,\dots\}}$
- $\overline{X} + \overline{-X} = \overline{\{x_k + -x_k\}} = \overline{\{0,0,0,\dots\}}$
- $\overline{X} \cdot (\overline{Y} + \overline{Z}) = \overline{\{x_k(y_k + z_k)\}} = \overline{\{x_k y_k + x_k z_k\}} = \overline{XY} + \overline{XZ}$.

(For $\overline{X} \cdot \overline{\frac{1}{X}}$, we assume that $\overline{X} \neq \overline{\{0,0,0,\dots\}}$, and we take k large enough so that $x_k \neq 0$.)

(c) **First Solution:** Suppose that $\sum_{k=0}^{M} a_k p^k = \sum_{k=0}^{N} b_k p^k$ with $a_i, b_i \in S_p$. WLOG assume that $M \leq N$, and write $a_{M+1} = a_{M+2} = \cdots = a_N = 0$. Then

$$\sum_{k=0}^{N} a_k p^k = \sum_{k=0}^{N} b_k p^k. \tag{1}$$

If $(a_0, \dots, a_N) \neq (b_0, \dots, b_N)$ then let j be the smallest number such that $a_j \neq b_j$. Taken mod p^{j+1}, (1) becomes $a_j p^j \equiv b_j p^j \pmod{p^{j+1}} \Rightarrow a_j \equiv b_j \pmod{p}$. But since a_j and b_j are between 0 and $p-1$, we must have $a_j = b_j$ — a contradiction. Thus our assumption was false and $(a_0, \dots, a_N) = (b_0, \dots, b_N)$. This implies that a positive integer can be expressed as a finite sum $\sum_{k=0}^{N} a_k p^k$ in at most one way.

Now, given a positive integer n, choose an integer $N \geq 0$ so that $n \leq p^{N+1} - 1$. There are p^{N+1} possible $(N+1)$-tuples $(a_0, a_1, \dots, a_N)$ with $a_0, a_1, \dots, a_N \in S_p$. From our argument, these $(N+1)$-tuples must correspond to different sums $\sum_{k=0}^{N} a_k p^k$. On the other hand, each of these sums is at least 0 (when all the $a_i = 0$) and at most $p^{N+1} - 1$ (when all the $a_i = p - 1$). There are *exactly* p^{N+1} integers between 0 and $p^{N+1} - 1$ inclusive, so each integer between 0 and $p^{N+1} - 1$ can be expressed as a finite sum of the desired form. Specifically, n can, which was to be proved.

Second Solution: We use generating functions. Define

$$F(x) = \prod_{i=0}^{\infty} \sum_{j=0}^{p-1} x^{jp^i}.$$

When this infinite product is expanded out, the coefficient of x^n is the number of representations of n as $\sum_{i=0}^{\infty} a_i p^i$. But:

$$\begin{aligned} F(x) &= \prod_{i=1}^{\infty} \frac{1 - x^{p^{i+1}}}{1 - x^{p^i}} \\ &= \frac{1}{1-x} \\ &= \sum_{i=0}^{\infty} x^i \end{aligned}$$

So each n has one representation.

(d) We prove a more general result:

Lemma 2. *Given a nonzero p-adic $q \in \mathbb{Q}^p$ represented by a Cauchy sequence $\{q_k\}$ of rationals, we can write q as a convergent infinite series $\sum_{k=v_p(q)}^{\infty} a_k p^k$ where each $a_k \in S_p$.*

Proof: Intuitively, to write a rational number $p^\alpha \frac{s}{t}$ as such a series, we first ignore the p^α term (which we repair at the end by shifting powers of p); then calculating st^{-1} modulo p, p^2, p^3, and so on to decide the rightmost digits — in essence, we are taking st^{-1} modulo "p^∞" . . . and a little work shows that we can *consistently* decide the digits this way. As for a general Cauchy sequence of rationals, we repeat the trick for each rational — and discover that the series used to represent the rationals eventually share arbitrarily many digits.

Now for the math. Since $\{q_k\} \not\to 0$, $v_p(q_k)$ eventually becomes some constant α; for simplicity, we can assume without loss of generality that *all* the $v_p(q_k) = \alpha$ (since if we ignore any other terms, our new Cauchy sequence will still converge to the same p-adic).

So for each k, write $q_k = p^\alpha \frac{s_k}{t_k}$ for integers s_k, t_k relatively prime to p. Then for all $k, K \geq 1$, there exists a unique value $m_K^{(k)}$ between 0 and $p^K - 1$ inclusive such that $m_K^{(k)} \cdot t_k \equiv s_k \pmod{p^K}$ — in other words, such that $m_K^{(k)} \equiv s_k t_k^{-1} \pmod{p^K}$.

Also, for each $K \geq 1$ we know that eventually $v_p(q_i - q_j) \geq K + \alpha$. For such i, j we have

$$v_p(q_i - q_j) = v_p\left(p^\alpha \frac{s_i}{t_i} - p^\alpha \frac{s_j}{t_j}\right) = \alpha + v_p\left(\frac{s_i t_j - s_j t_i}{t_i t_j}\right).$$

We know $p \not| \, t_i t_j$, so

$$\begin{aligned} K+\alpha \leq v_p(q_i-q_j) &= \alpha + v_p(s_it_j - s_jt_i) \\ &\Rightarrow v_p(s_it_j-s_jt_i) \geq K \\ &\Rightarrow s_it_j \equiv s_jt_i \pmod{p^K} \\ &\Rightarrow m_K^{(i)} \equiv s_it_i^{-1} \equiv s_jt_j^{-1} \equiv m_K^{(j)} \pmod{p^K} \end{aligned}$$

and $m_K^{(i)} = m_K^{(j)}$. Thus eventually the $m_K^{(i)}$ all equal some value m_K between 0 and $p^K - 1$. Also, from part (c) we can write each m_K as a finite sum $\sum_{i=0}^{K-1} a_i^{(K)} p^i$.

Furthermore, for $N > K+1$ eventually $m_{K+1}^{(i)} = m_{K+1}$ and $m_N^{(i)} = m_N$. Then

$$m_N \equiv s_it_i^{-1} \pmod{p^N} \quad \Rightarrow \quad m_N \equiv s_it_i^{-1} \equiv m_{K+1} \pmod{p^{K+1}}.$$

Thus m_N and m_K have the same final $K+1$ digits in their base-p representations: specifically, the digits in the p^K place are equal and $a_K^{(K)} = a_K^{(N)}$. Thus $a_K^{(K)}, a_K^{(K+1)}, \ldots$ all equal the same value a_K.

We claim that as $N \to \infty$, $\sum_{k=\alpha}^N a_{k-\alpha}p^k$ converges to q — that is, the Cauchy sequences $\{q_k\}_{k=1,2,\ldots}$ and $\{\sum_{k=\alpha}^N a_{k-\alpha}p^k\}_{N=\alpha,\alpha+1,\ldots}$ belong in the same equivalence class q. Observe that

$$\begin{aligned} d\left(\sum_{k=\alpha}^{N} a_{k-\alpha}p^k, q_i\right) &= d\left(p^\alpha \sum_{k=0}^{N-\alpha} a_k p^k, q_i\right) \\ &= d\left(p^\alpha m_{N-\alpha+1}, q_i\right) \\ &= \|p^\alpha m_{N-\alpha+1} - q_i\|_p \\ &= \left\| p^\alpha m_{N-\alpha+1} - p^\alpha \frac{s_i}{t_i} \right\|_p \\ &= \left\| p^\alpha \left(\frac{m_{N-\alpha+1}t_i - s_i}{t_i} \right) \right\|_p \end{aligned}$$

But for sufficiently large i so that $m_{j-\alpha}^{(i)} = m_{j-\alpha}$ and for large $N \geq j-1$, we have $m_{N-\alpha+1} \equiv m_{j-\alpha} \equiv m_{j-\alpha}^{(i)} \equiv s_it_i^{-1} \pmod{p^{j-\alpha}}$, so $p^{j-\alpha}$ divides the numerator of the fraction while p does not divide the denominator. So, the valuation of the messy quantity is at least j.

Sketch of alternative proof Let $v = v_p(q)$.

Suppose we have any p-adic r such that $v_p(r) \geq v$; then there exists a sequence of rationals $\{r_k\}$ converging to r. Because $\{v_p(r_k)\}$ (i) must eventually be constant or converge to ∞ and (ii) converge to $v_p(r)$ by definition, it follows that $v_p(r_k) = v_p(r) \geq v$ for sufficiently large k. Also, though, for any $\epsilon > 0$, $\|r - r_k\|_p < \epsilon$ for sufficiently large k. Specifically, for $\epsilon = p^{-v}$, there must exist a rational α such that $v_p(\alpha) \geq v$ and $\|r - \alpha\|_p < p^{-v}$.

Apply this result to $r = q$ to obtain a corresponding α, say α_0. Then let β_0 be the integer in S_p such that $\beta_0 \equiv \alpha_0 p^{-v} \pmod{p}$ (or equivalently, such that $\|\beta_0 - \alpha p^{-v}\|_p < 1$). We then have $\|\beta_0 p^v - q\|_p \leq \max\{\|\beta_0 p^v - \alpha_0\|_p, \|\alpha_0 - q\|_p\} < p^{-v}$. Hence, $\|\frac{q-\beta_0 p^v}{p}\|_p \leq p^{-v}$.

Next apply the previous result to $r = \frac{q-\beta_0 p^v}{p}$ to obtain a corresponding α, say α_1. Let β_1 be the integer in S_p such that $\beta_1 \equiv \alpha_1 p^{-v} \pmod{p}$. We then have $\|(\beta_0 p^v + \beta_1 p^{v+1}) - q\|_p < p^{-v-1}$. Hence, $\|\frac{q-(\beta_0 p^v + \beta_1 p^{v+1})}{p^2}\|_p \leq p^{-v}$. We can proceed similarly to find $\beta_0, \beta_1, \ldots$ in S_p such that $\sum_{k=v}^{\infty} \beta_k p^k$ converges to q. □

Part (d) now follows immediately from the lemma, since -1 is a p-adic represented by the Cauchy sequence $\{-1, -1, \ldots\}$. Applying this construction we find that

$$-1 = \sum_{k=0}^{\infty} (p-1)p^k.$$

(e) Part (e) also follows immediately from the lemma, since $\frac{1}{n}$ is a p-adic represented by the Cauchy sequence $\{\frac{1}{n}, \frac{1}{n}, \ldots\}$ (and $v_p(\frac{1}{n}) = 0$ so the sum starts at 0).

(f)

- *Unique Representation as a Series.* The lemma implies that any nonzero p-adic can be represented as such a sum; and $0 =$ "$\sum_{k=\infty}^{\infty} 0 \cdot p^k$." Conversely, the series $\sum_{k=v}^{\infty} a_k p^k$ corresponds to the sequence

  $$\{\sigma_N\}_{N \geq v} = \left\{ \sum_{k=v}^{N} a_k p^k \right\}_{N \geq v}.$$

  But given any K, for $N_1 \geq N_2 \geq K$ we have $\sigma_{N_1} - \sigma_{N_2} = \sum_{k=N_2+1}^{N_1} a_k p^k$ which has p-adic valuation at least $N_2 + 1 > K$. Thus $\{\sigma_N\}$ is a Cauchy sequence and indeed converges to some p-adic.

  Now suppose that a p-adic could be represented by two sums $\sum_{k=v_1}^{\infty} a_k p^k$ and $\sum_{k=v_2}^{\infty} b_k p^k$. If $v_1 < v_2$ then we can let $v = v_1 = v_2$ and $b_{v_1} = b_{v_1+1} = \cdots = b_{v_2-1} = 0$ so that

  $$\sum_{k=v}^{\infty} a_k p^k = \sum_{k=v}^{\infty} b_k p^k.$$

  (We can similarly do this if $v_1 > v_2$.)
  This implies that the two sequences

$$\left\{\sum_{k=v}^{N} a_k p^k\right\}_{N=v,v+1,\ldots} \quad \text{and} \quad \left\{\sum_{k=v}^{N} a_k p^k\right\}_{N=v,v+1,\ldots}$$

are in the same equivalence class.

Now suppose by way of contradiction that some $a_K \neq b_K$, so that $v_p((a_K - b_K)p^K) = K$. Then for large enough N eventually $v_p\left(\sum_{k=v}^{N}(a_k - b_k)p^k\right) > K$. For such N, for all other $i \neq K$ with $v \leq i \leq N$, we have $v_p((a_i - b_i)p^i) = i$ or ∞. Then by an easy extension of our original Observation 3, we have

$$\begin{aligned} v_p\left(\sum_{k=v}^{N}(a_k - b_k)p^k\right) &= \min_{k=v,v+1,\ldots,N} v_p((a_k - b_k)p^k) \\ &\leq v_p((a_K - b_K)p^K) \\ &= K, \end{aligned}$$

a contradiction. Thus $a_K = b_K$ for *all* $K \geq v$.

Thus any p-adic q can be expressed *uniquely* in the form $\sum_{k=v_p(q)}^{\infty} a_k p^k$, as desired.

- *Addition and Multiplication of* p*-adics as Series.*

We wish to show that we can "add" series as we do with normal numbers — lining up the "p-ecimal" points, starting in the rightmost nonzero column, adding and carrying, and then working our way left. But in normal addition $a + b = c$, the last t digits of c depend only the last t digits of a and b — precisely, if $a = p^v A$ and $b = p^v B$, then we can find the last t digits of $c = p^v C$ by setting $C \equiv A + B \pmod{p^t}$.

Thus applying "normal addition" to the last t digits when adding two series

$$\sum_{k=v}^{\infty} a_k p^k = p^v \sum_{k=0}^{\infty} a_{k+v} p^k$$

and

$$\sum_{k=v}^{\infty} b_k p^k = p^v \sum_{k=0}^{\infty} b_{k+v} p^k$$

yields

$$p^v \sum_{k=0}^{t-1} c_{k+v} p^k,$$

where

$$\sum_{k=0}^{t-1} c_{k+v} p^k \equiv \sum_{k=0}^{t-1} (a_{k+v} + b_{k+v}) p^k \pmod{p^t}.$$

(The sum $\sum_{k=0}^{t-1}(a_{k+v}+b_{k+v})p^k$ is congruent to exactly one value between 0 and p^t-1; and we know from a previous result that there is exactly one way to express this as a sum $\sum_{k=0}^{t-1}c_{k+v}p^k$ for $c_i \in S_p$.) Furthermore, as we increase k, previously defined c_i stay the same since if $\sum_{k=0}^{t}c'_{k+v}p^k \equiv \sum_{k=0}^{t}(a_{k+v}+b_{k+v})p^k \pmod{p^{t+1}}$, then $\sum_{k=0}^{t-1}c'_{k+v}p^k \equiv \sum_{k=0}^{t-1}(a_{k+v}+b_{k+v})p^k \equiv \sum_{k=0}^{t-1}c_{k+v}p^k \pmod{p^t}$.

Similar arguing shows that applying "normal multiplication" to two series also yields a well-defined series in powers of p with coefficients in S_p. And this addition and multiplication corresponds to our previously given definitions of addition and multiplication of p-adics — we view both p-adics as the Cauchy sequence of rationals with the same rightmost t digits (as t goes from 1 to ∞), then add or multiply them term by term. (For example, the p-adic multiplication $\ldots 1072.312 \times \ldots 0326.89$ corresponds to the multiplication $\{P_1, P_2, P_3, P_4, \ldots\} = \{.002 \times .000, .012 \times .090, .312 \times .890, 2.312 \times 6.890, \ldots\}$. Then P_t will have the same rightmost t digits as $\sum_{k=v}^{\infty}c_kp^k$, so the sequence product $\{P_t\}$ and the series product converge to the same p-adic.)

(g)

- *Compactness of* $\mathbb{Z}_p$.

First Solution: We show that $\mathbb{Z}_p$ is sequentially compact. By (f), each $x \in \mathbb{Z}_p$ can be expressed as $\sum_{k=0}^{\infty}a_kp^k$. Consider a sequence $\{x_i\}$. We extract a Cauchy subsequence (the completeness of $\mathbb{Z}_p$ will then ensure it converges). There are finitely many possibilities for a_0, so by the pigeonhole principle one of them occurs infinitely often. Let x_{n_0} have this as its first digit. Then, among these, there will be an a_1 which occurs infinitely often, we choose x_{n_1} with $n_1 > n_0$ such that it has these as its first two digits, and so on. This subsequence is Cauchy since for $i > j \geq N$, $\|x_{n_i} - x_{n_j}\|_p < p^{-N}$.

Second Solution: Given an open cover of $\mathbb{Z}_p$, we must prove there is a finite subcover — but since every open set is the union of open epsilon-balls, it suffices to prove that given an open cover of $\mathbb{Z}_p$ with *ϵ-balls* there is a finite subcover, for, given an open cover, we consider a collection of ϵ-balls such that for each open set in the original cover, there is a subcollection of the ϵ-balls whose union is that open set. These ϵ-balls cover the space, and we take a finite subcover, and then for each ϵ-ball, take an open set in the original cover which contains it, and this is our finite subcover.

Viewing p-adics as infinite series, $\mathbb{Z}_p$ is the set of sums $\sum_{k=0}^{\infty}a_kp^k$ with each $a_k \in S_p$. Also, because p-adic absolute value is a *discrete* function (taking on values of p^t for $t \in \mathbb{Z}$), any epsilon-ball $B(\sum_{k=0}^{\infty}a_kp^k, \epsilon)$ is exactly the same as $B(\sum_{k=0}^{\infty}a_kp^k, p^{-t})$ where p^{-t}

is the smallest value greater than or equal to ϵ. But $B(\sum_{k=0}^{\infty} a_k p^k, p^{-t})$ contains exactly those numbers $\sum_{k=0}^{\infty} b_k p^k$ where $(a_0, a_1, \ldots, a_{t-1}) = (b_0, b_1, \ldots, b_{t-1})$.

Now given an infinite open cover of epsilon-balls, suppose by way of contradiction there is no finite subcover. Then by the pigeonhole principle, $\exists c_0 \in S_p$ such that $\{\sum_{k=0}^{\infty} a_k p^k \mid a_0 = c_0\}$ has no finite subcover (since there are exactly p such sets, a finite number, partitioning all of $\mathbb{Z}_p$); fix this c_0. Then again by the pigeonhole principle, $\exists c_1 \in S_p$ such that $\{\sum_{k=0}^{\infty} a_k p^k \mid (a_0, a_1) = (c_0, c_1)\}$ has no finite subcover. Continuing onward, we can find $c_0, c_1, \ldots$ such that for each N, the set $Z_N = \{\sum_{k=0}^{\infty} a_k p^k \mid (a_0, \ldots, a_N) = (c_0, \ldots, c_N)\}$ has no finite subcover. But $\sum_{k=0}^{\infty} c_k p^k$ must be in some epsilon-ball $B(\sum_{k=0}^{\infty} b_k p^k, p^{-t}) = \{\sum_{k=0}^{\infty} a_k p^k \mid (a_0, \ldots, a_{t-1}) = (b_0, \ldots, b_{t-1})\}$. Thus $(c_0, \ldots, c_{t-1}) = (b_0, \ldots, b_{t-1})$, which implies that this epsilon-ball contains the set Z_{t-1}. But then Z_{t-1} has a finite subcover (of one epsilon-ball), a contradiction.

Third Solution: Complete and totally bounded implies compact. $\mathbb{Z}_p \subset \mathbb{Q}_p$ is complete since it is a closed set (the closure of $\mathbb{Z}$) in a complete space. We show that it is totally bounded. Given any $\epsilon > 0$ we can find $p^{-t} < \epsilon$ so that the following p^t epsilon-balls cover $\mathbb{Z}_p$:

$$\begin{aligned}
&\bigcup \left\{ B\left(\sum_{k=0}^{t-1} a_k p^k, \epsilon \right) \mid a_k \in S_p \right\} \\
&\quad \supset \bigcup \left\{ B\left(\sum_{k=0}^{t-1} a_k p^k, p^{-t} \right) \mid a_k \in S_p \right\} \\
&\quad = \bigcup \left\{ \left\{ \sum_{k=0}^{\infty} b_k p^k \mid (b_0, \ldots, b_{t-1}) = (a_0, \ldots, a_{t-1}) \right\} \mid a_k \in S_p \right\} \\
&\quad = \mathbb{Z}_p,
\end{aligned}$$

so there are finitely many ϵ-balls that cover $\mathbb{Z}_p$ for any $\epsilon > 0$. Thus $\mathbb{Z}_p$ is closed *and* totally bounded, and therefore compact.

- *Openness of* $\mathbb{Z}_p$. Given any p-adic integer $Q = \sum_{k=0}^{\infty} q_k p^k$, we claim that the epsilon-ball $B(q, 1)$ is in $\mathbb{Z}_p$. Suppose by way of contradiction that $R = \sum_{k=v}^{\infty} r_k p^k \notin \mathbb{Z}_p$ were in this epsilon-ball — notice that $v_p(R) < 0$.

  If $Q = 0$ then $d(Q, R) = \|R\|_p = p^{-v_p(R)} > 1$, a contradiction; and since $R \notin \mathbb{Z}_p$, $R \neq 0$. Then Q is represented by the Cauchy sequence $\{\sigma_Q\}_{N=0,1,\ldots} = \{\sum_{k=0}^{N} q_k p^k\}_{N=0,1,\ldots}$, and eventually these terms all have p-adic valuation $v_p(Q) \geq 0$. Similarly, R is represented by the Cauchy sequence $\{\sigma_R\}_{N=v,v+1,\ldots} = \{\sum_{k=v}^{N} r_k p^k\}_{N=v,v+1,\ldots}$, and eventually these terms all have p-adic valuation $v_p(R) < 0$.

Then $Q - R$ is represented by the Cauchy sequence $\{(\sigma_Q)_N - (\sigma_R)_N\}$. But eventually $v_p((\sigma_Q)_N) = v_p(Q) \geq 0 > v_p(R) = v_p((\sigma_R)_N)$, so that

$$v_p\left((\sigma_Q)_N - (\sigma_R)_N\right) = \min(v_p(Q), v_p(R)) = v_p(R) < 0.$$

So the p-adic valuation of $Q - R$ is negative, and $d(Q, R) > p^0 = 1$, a contradiction.

Thus our original assumption was false, and indeed every element in $\mathbb{Z}_p$ is the center of some epsilon-ball contained in $\mathbb{Z}_p$. Therefore $\mathbb{Z}_p$ is open, as desired.

- *Noncompactness of* $\mathbb{Q}_p$.
  First, $\mathbb{Q}_p$ is not bounded because $d(0, p^k) = p^{-k}$ which can be made arbitrarily large as $k \to -\infty$. Thus (from part (c) of the solution to Problem 2) it is not totally bounded. But $\mathbb{Q}_p$ is compact if and only if it is closed and totally bounded; and since it is not totally bounded, it cannot be compact.

Problem 2.

(a) (X, d) *is a metric space.*
d indeed satisfies all the properties of a metric distance:

- *Symmetry.* $d(\{x_k\}, \{y_k\}) = \sup_k |x_k - y_k| = \sup_k |y_k - x_k| = d(\{y_k\}, \{x_k\})$.
- *Zeroicity.* $d(\{x_k\}, \{x_k\}) = \sup_k |x_k - x_k| = \sup_k 0 = 0$.
- *Positivity.* If $\{x_k\} \neq \{y_k\}$ then $\exists N$ such that $x_N \neq y_N$. Thus $d(\{x_k\}, \{y_k\}) = \sup_k |x_k - y_k| \geq |x_N - y_N| > 0$.
- *Triangle Inequality.* Suppose we have sequences $\{x_k\}, \{y_k\}, \{z_k\}$ with $d(\{x_k\}, \{z_k\}) = t$. Then $\forall \epsilon > 0, \exists N$ such that $|x_N - z_N| > t - \epsilon$. Thus $d(\{x_k\}, \{y_k\}) + d(\{y_k\}, \{z_k\}) \geq |x_N - y_N| + |y_N - z_N| \geq |x_N - z_N| > t - \epsilon$ for all $\epsilon > 0$, so we must have $d(\{x_k\}, \{y_k\}) + d(\{y_k\}, \{z_k\}) \geq t = d(\{x_k\}, \{z_k\})$. (In the previous steps, $|x_N - y_N| + |y_N - z_N| \geq |x_N - z_N|$ by the triangle inequality for the real numbers.)

(b) (X, d) *is bounded but not totally bounded.*
Given any sequences $\{x_k\}, \{y_k\}$, we have $0 \leq |x_k - y_k| \leq 1$ for every k so that $0 \leq d(\{x_k\}, \{y_k\}) = \sup_k |x_k - y_k| \leq 1$ and thus X is bounded.

However, suppose by way of contradiction that X were totally bounded — that is, for any $\epsilon > 0$ there exists a finite collection of epsilon-balls $B\left(\left\{x_k^{(1)}\right\}, \epsilon\right), B\left(\left\{x_k^{(2)}\right\}, \epsilon\right), \ldots, B\left(\left\{x_k^{(n)}\right\}, \epsilon\right)$ that contain all elements of X. Choose $\epsilon = \frac{1}{2}$ and find the corresponding $\left\{x_k^{(i)}\right\}$. For each i with $1 \leq i \leq n$, if $x_i^{(i)} \leq \frac{1}{2}$ then write $y_i = 1$; otherwise, if $x_i^{(i)} > \frac{1}{2}$ then write $y_i = 0$. The sequence $\{y_k\} = y_1, y_2, \ldots, y_n, 1, 1, 1, \ldots$ is in X. But $d(\{x_k^{(i)}\}, \{y_k\}) \geq |x_i^{(i)} - y_i| \geq \frac{1}{2}$, so $\{y_k\}$ is not in any of the epsilon-balls — a contradiction. Therefore our original assumption was false, and X is not totally bounded.

(c) *Every totally bounded metric space* (X, d) *is also bounded.*

Suppose that (X, d) is totally bounded. Fixing an $\epsilon > 0$, there is a finite collection of epsilon-balls $B(x_1, \epsilon)$, $B(x_2, \epsilon)$, $\ldots$, $B(x_n, \epsilon)$ that contains every element in X. Write $M = \max_{1 \leq i,j \leq n}\{d(x_i, x_j)\}$ and consider any $y, z \in X$. Then $y \in B(x_i, \epsilon)$ and $z \in B(x_j, \epsilon)$ for some i and j, so that

$$d(y, z) \leq d(y, x_i) + d(x_i, x_j) + d(x_j, z) < \epsilon + M + \epsilon$$

by the triangle inequality. Thus any two elements have distance less than $M + 2\epsilon$, so (X, d) is indeed bounded.