Proof. Suppose that $|m| > 1$ for some integer $m > 1$. Fix any other integer $b > 1$, and then define $B := \max\{|c| : 0 \le c \le b-1\}$. Any integer N can be written in base b as $m_0 + m_1 b + \cdots + m_d b^d$ where each $m_j \in \{0, 1, 2, \ldots, b-1\}$ and $m_d \ge 1$. Therefore

$$|N| \ \le \ \sum_{i=0}^{d} |m_i b^i| \ = \ \sum_{i=0}^{d} |m_i||b|^i \ \le \ (d+1)\ B\ \max\{1, |b|^d\},$$

as there are $d+1$ terms in the sum, each $|m_i| \le B$, and each $|b|^i \le 1$ if $|b| \le 1$, with each $|b|^i \le |b|^d$ if $|b| > 1$.

We let $N = m^n$ for any integer $n \ge 1$, so that $|N| = |m|^n$. Now $b^d \le N$ and so $d \le \frac{\log N}{\log b} = n\frac{\log m}{\log b}$. Substituting this into the inequality above gives

$$|m|^n \ \le \ \left(1 + n\frac{\log m}{\log b}\right)\ B\ \max\{1, |b|^{n\frac{\log m}{\log b}}\}.$$

We will take nth roots of both sides and let $n \to \infty$. We notice that $(u+nv)^{1/n} \to 1$ as $n \to \infty$ for any $v > 0$ and so deduce that

$$|m| \ \le \ \max\{1, |b|^{\frac{\log m}{\log b}}\}.$$

Since $|m| > 1$ this implies that $|b| > 1$ and therefore, taking logarithms, we have

$$\frac{\log |m|}{\log m} \ \le \ \frac{\log |b|}{\log b}.$$

Since $|b| > 1$ we may run the same argument with the roles of b and m reversed and obtain the opposite inequality, and combining these we get equality. But this holds for all integers $b > 1$. Hence there exists a number κ for which $|b| = b^\kappa = |b|_\infty^\kappa$ for all integers $b > 1$.

As $|m| > 1$ we deduce that $\kappa > 0$. Since $2^\kappa = |2|_\infty^\kappa \le |1|_\infty^\kappa + |1|_\infty^\kappa = 2$, therefore $\kappa \le 1$. One can show that the triangle inequality holds whenever $0 < \kappa \le 1$.

If $|n| = 1$ for all $n > 1$, then $|n| = |n|_\infty^0$.

We may now assume that $|n| \le 1$ for all integers $n > 1$, and that $|m| < 1$ for some $m > 1$. By multiplicativity we know that $|p| < 1$ for some prime p dividing m. There can be no other prime q with $|q| < 1$, or else we select a large power e, so large that $|q|^e < 1 - |p|$. Since $(p, q) = 1$ there exist integers a, b for which $ap + bq^e = 1$ and therefore

$$1 \ = \ |1| \ = \ |ap + bq^e| \ \le \ |ap| + |bq^e| \ = \ |a||p| + |b||q|^e \ \le \ |p| + |q|^e < 1,$$

a contradiction. Therefore, if $|p| = p^{-\kappa} = |p|_p^\kappa$, then $|.| = |.|_p^\kappa$. Taking powers of (16.1.3) we see that any norm $|.|_p^\kappa$ satisfies the ultrametric triangle inequality and therefore satisfies the Euclidean triangle inequality. □

16.6. Power series convergence and the p-adic logarithm

Theorem 16.4. *Let $(a_n)_{n\ge 0}$ be an infinite sequence of p-adic numbers. The infinite sum $\sum_{n\ge 0} a_n$ converges to some number L (in the p-adics) if and only if $a_n \to 0$ as $n \to \infty$.*

Proof. Suppose that $a_n \to 0$ as $n \to \infty$. Fix $\epsilon > 0$ and M_0 so that $|a_n| < \epsilon$ whenever $n \geq M_0$. Using the ultrametric inequality we have that if $N > M \geq M_0$, then

$$\left| \sum_{n \leq N} a_n - \sum_{n \leq M} a_n \right|_p \leq \max_{M < n \leq N} |a_n|_p < \epsilon.$$

Therefore the partial sum of the a_n form a Cauchy sequence, and therefore $\sum_{n \geq 0} a_n$ converges to some number L.

On the other hand if $\sum_{n \geq 0} a_n$ converges to some number L, then for any $\epsilon > 0$ there exists M_1 such that $|\sum_{n \leq M} a_n - L| < \epsilon$ whenever $M \geq M_1$. Therefore if $N \geq M_1 + 1$, then we have $a_N = (\sum_{n \leq N} a_n - L) - (\sum_{n \leq N-1} a_n - L)$ so that

$$|a_N|_p \leq \max \left\{ \left| \sum_{n \leq N} a_n - L \right|_p, \left| \sum_{n \leq N-1} a_n - L \right|_p \right\} < \epsilon.$$

We deduce that $a_n \to 0$ as $n \to \infty$. □

Exercise 16.6.1. Let p be a given prime.
(a) Prove that $\sum_{n \geq 0} z^n / a_n$ converges when $|z|_p < p^{-\tau}$, where $\tau = \limsup_{n \to \infty} v_p(a_n)/n$.
(b) Deduce that $\sum_{n \geq 1} z^n / n$ converges if $|z|_p < 1$. (In $\mathbb{C}$ this also converges inside $|z| < 1$.) Exercise 3.10.1(b) states that $v_p(n!) = \frac{n - s_p(n)}{p-1}$ where $s_p(n)$ is the sum of the digits of n when written in base p.
(c) Deduce that $\sum_{n \geq 1} z^n / n!$ converges if $|z|_p < p^{-1/(p-1)}$.

We define the *p-adic logarithm* to be

$$\log_p(z) := -\sum_{n \geq 1} \frac{(1-z)^n}{n}$$

whenever $|1 - z|_p < 1$ with $z \in \mathbb{Z}_p$ (this sum converges by exercise 16.6.1(b)). Similarly we define the *p-adic exponential* to be

$$\exp_p(z) := \sum_{n \geq 1} \frac{z^n}{n!}$$

wherever $|z|_p < p^{-1/(p-1)}$ (this sum converges by exercise 16.6.1(c)).

Exercise 16.6.2. Suppose that $|1 - a|_p, |1 - b|_p < p^{-1/(p-1)}$.
(a) Prove that $|1 - ab|_p < p^{-1/(p-1)}$.
(b) Deduce that $\exp_p(ab) = \exp_p(a) \exp_p(b)$.

In exercise 2.5.9(b) we saw that $\frac{1}{p}\binom{p}{j} \equiv (-1)^{j-1}/j \pmod{p}$ for $1 \leq j \leq p-1$, so that if $z \in \mathbb{Z}_{(p)}$, then

$$\sum_{n=1}^{p-1} \frac{z^n}{n} \equiv -\frac{1}{p} \sum_{n=1}^{p-1} \binom{p}{n} (-z)^n = -\frac{1}{p}((1-z)^p - 1 + z^p) \pmod{p}.$$

This suggests that there might be a convenient expression of this type for $\log_p(z)$.

Exercise 16.6.3. Suppose that $v_p(x) > 0$.
(a) Prove that if $p^k \leq m < p^{k+1}$, then $v_p(x^m/m) \geq p^k v_p(x) - k$, for each integer $k \geq 0$.
(b) Suppose that $v_p(x) \geq 2r/p^r$ for some integer $r \geq 1$. Deduce that $v_p(x^m/m) \geq k$ for all $m \geq p^k$, whenever $k \geq r$.

Lemma 16.6.1. *For any $z \in \mathbb{Z}_{(p)}$ for which $|1-z|_p < 1$, we have*

$$\log_p(z) = \lim_{k\to\infty} \frac{z^{p^k}-1}{p^k}.$$

Proof. Let $x = 1-z$ so that $v_p(x) > 0$. We can select an integer $r \geq 1$ for which $v_p(x) \geq 2r/p^r$, as $i/p^i \to 0$ as $i \to \infty$. Let k be any integer $\geq 3r$ and let ℓ be the largest integer $\leq k/3$, so that $\ell \geq r$. Therefore if $m \geq p^{\ell+1}$, then $v_p(x^m/m) \geq \ell+1 > k/3$ by exercise 16.6.3(b).

For $1 \leq m \leq p^k$ we have

$$(-1)^{m-1}\frac{1}{p^k}\binom{p^k}{m} = (-1)^{m-1}\prod_{j=1}^{m-1}\frac{p^k-j}{j}\cdot\frac{1}{m} = \frac{c_m}{m} \text{ where } c_m := \prod_{j=1}^{m-1}\left(1-\frac{p^k}{j}\right).$$

We let $c_m = 0$ for all $m > p^k$, so that $-\log_p(z) = -\log_p(1-x) = \sum_{m\geq 1}\frac{x^m}{m}$, and

$$\frac{1-z^{p^k}}{p^k} = \frac{1-(1-x)^{p^k}}{p^k} = \sum_{m=1}^{p^k}(-1)^{m-1}\frac{1}{p^k}\binom{p^k}{m}x^m = \sum_{m=1}^{p^k} c_m\frac{x^m}{m}.$$

Therefore

$$-\log_p(z) - \frac{1-z^{p^k}}{p^k} = \sum_{m\geq 1}(1-c_m)\frac{x^m}{m}.$$

Now if $1 \leq j < m \leq p^k$, then $1-\frac{p^k}{j} \in \mathbb{Z}_{(p)}$, and so $1-c_m \in \mathbb{Z}_{(p)}$ for all $m \geq 1$; that is, $|1-c_m|_p \leq 1$. Therefore if $m \geq p^{\ell+1}$, then

$$\left|(1-c_m)\frac{x^m}{m}\right|_p \leq \left|\frac{x^m}{m}\right|_p < p^{-k/3},$$

by the first paragraph.

If $1 \leq j < m < p^{\ell+1}$, then $1-\frac{p^k}{j} \equiv 1 \pmod{p^{k-\ell}}$, and so $|1-c_m| \leq p^{\ell-k}$. Now $|m|_p \geq p^{-\ell}$ and so

$$\left|(1-c_m)\frac{x^m}{m}\right|_p \leq p^{2\ell-k} \leq p^{-k/3}.$$

Combining these last two estimates, we deduce that

$$\left|\log_p(z) + \frac{1-z^{p^k}}{p^k}\right|_p = \left|\sum_{m\geq 1}(1-c_m)\frac{x^m}{m}\right|_p \leq \max_{m\geq 1}\left|(1-c_m)\frac{x^m}{m}\right|_p \leq p^{-k/3},$$

and the result follows, letting $k \to \infty$. □

Exercise 16.6.4. Prove that $\sum_{m\geq 1} 2^m/m = 0$ in the 2-adics.

Exercise 16.6.5. Assume that $|a-1|_p, |b-1|_p < 1$.

(a) Prove that $\lim_{k\to\infty} a^{p^k} = 1$.
(b) Deduce that $\log_p(ab) = \log_p(a) + \log_p(b)$.
(c) Deduce that if $a = b^n$, then $\log_p(a) = n\log_p(b)$.
(d)† Suggest an algorithm for the discrete log problem in the p-adics.

At the moment the function $\log_p(z)$ is defined only when $|z-1|_p < 1$. For any $\beta \in \mathbb{Z}_p$ with $|\beta|_p = 1$, there exists an integer b with $b \equiv \beta \pmod p$ and $b \not\equiv 0 \pmod p$. Therefore, by Fermat's Little Theorem, $\beta^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$, and so $\log_p(\beta^{p-1})$ is well-defined. Taking our lead from exercise 16.6.5(c) we therefore define

$$\log_p(\beta) \;:=\; \frac{\log_p(\beta^{p-1})}{p-1} \;=\; \lim_{k\to\infty} \frac{\beta^{p^k(p-1)}-1}{p^k(p-1)}.$$

Exercise 16.6.6. Assume that $\alpha, \beta \in \mathbb{Z}_p$.
(a) Prove that $\log_p(-\alpha) = \log_p(\alpha)$.
(b) Prove that $\log_p(\alpha\beta) = \log_p(\alpha) + \log_p(\beta)$.

Any $\gamma \in \mathbb{Z}_p$ can be written in the form $\gamma = p^e\beta$ where $|\beta|_p = 1$, so we define[3]

$$\log_p(\gamma) \;=\; e\log_p(p) + \log_p(\beta).$$

16.7. The p-adic dilogarithm

For each $k \geq 1$, define

$$\mathcal{L}_k(x) := \sum_{m\geq 1} \frac{x^m}{m^k}.$$

The case $k = 2$ is the *dilogarithm function*.

Exercise 16.7.1. (a) Prove that the sum defining $\mathcal{L}_k(x)$ converges for all $x \in \mathbb{C}$ with $|x|_\infty \leq 1$ for all $k \geq 2$, and for $|x|_p < 1$ in the p-adics.
(b) Establish that $\mathcal{L}_k(x) + \mathcal{L}_k(-x) = 2^{1-k}\mathcal{L}_k(x^2)$ when $|x|_p < 1$.

Theorem 16.5. *If $|1-z|_p < 1$, then*

$$\mathcal{L}_2(1-z) + \mathcal{L}_2(1-z^{-1}) \;=\; -\frac{1}{2}(\log_p z)^2. \tag{16.7.1}$$

In particular $\mathcal{L}_2(2) = 0$ in the 2-adics.

Proof. For $|x|_p < 1$, we have

$$\frac{\mathrm{d}\mathcal{L}_2(x)}{\mathrm{d}x} \;=\; \frac{1}{x}\sum_{m\geq 1}\frac{x^m}{m} = -\frac{\log_p(1-x)}{x}\;,$$

and so, by the chain rule, we have

$$\begin{aligned}\frac{\mathrm{d}}{\mathrm{d}z}(\mathcal{L}_2(1-z)+\mathcal{L}_2(1-z^{-1})) \;&=\; -\mathcal{L}_2'(1-z) + z^{-2}\mathcal{L}_2'(1-z^{-1}) \\ &=\; \frac{\log_p(z)}{1-z} - z^{-2}\frac{\log_p(z^{-1})}{1-z^{-1}} \;=\; -\frac{\log_p z}{z}.\end{aligned}$$

Integrating yields $\mathcal{L}_2(1-z)+\mathcal{L}_2(1-z^{-1}) = -\frac{1}{2}(\log_p z)^2 + C$ for some constant C. Taking $z = 1$ we see that $C = 0$, yielding (16.7.1).

Replacing z by z^2, we obtain

$$\mathcal{L}_2(1-z^2) + \mathcal{L}_2(1-z^{-2}) \;=\; -2(\log_p z)^2 \;=\; 4(\mathcal{L}_2(1-z)+\mathcal{L}_2(1-z^{-1})).$$

When $p = 2$ we may take $z = -1$ in this equation and so $8\mathcal{L}_2(2) = 2\mathcal{L}_2(0) = 0$. □

[3] We can select any value for $\log_p(p)$ as is convenient in context; we do not have to let it be 1.

Exercise 16.7.2. Let $p = 2$ and $|z-1|_2 < 1$.
(a) Prove that $\mathcal{L}_2(1-z) + \mathcal{L}_2(1+z) = \frac{1}{2}\mathcal{L}_2(1-z^2) + C$ for some constant C.
(b) Prove that $C = 0$ using (16.7.1).
(c) Deduce (again) that $\mathcal{L}_2(2) = 0$.

We have now seen that

$$\sum_{n\geq 1} \frac{2^n}{n} = \sum_{n\geq 1} \frac{2^n}{n^2} \;=\; 0$$

in the 2-adics. It is interesting to see how rapidly this convergence happens. If $n \geq N \geq 2^k$, then $v_2(2^n/n) \geq 2^k - k$ so that

$$\sum_{n<N} \frac{2^n}{n} = -\sum_{n\geq N} \frac{2^n}{n} \equiv 0 \pmod{2^{2^k-k}}$$

and similarly

$$\sum_{n<N} \frac{2^n}{n^2} \equiv 0 \pmod{2^{2^k-2k}}.$$

It looks like there might be a pattern here. How about $\sum_{n\geq 1} 2^n/n^3$? Unfortunately the $n = 4$ term gives the unique maximum, 2^2, of $|2^n/n^3|_2$, and so $|\sum_{n\geq 1} 2^n/n^3|_2 = 4$, not 0.

Exercise 16.7.3. Prove that if $|x|_p, |y|_p < 1$, then

$$\mathcal{L}_2(x) + \mathcal{L}_2(y) - \mathcal{L}_2(xy) - \mathcal{L}_2\left(\frac{x(1-y)}{1-xy}\right) - \mathcal{L}_2\left(\frac{y(1-x)}{1-xy}\right) = \log_p\left(\frac{1-x}{1-xy}\right)\log_p\left(\frac{1-y}{1-xy}\right).$$

Further reading on p-adics

[1] Richard M. Hill, *Introduction to number theory*, chapter 4, World Scientific, Singapore, 2018.