p-ADIC INTERPOLATION

KEITH CONRAD

1. Introduction

Although $\mathbf{N}$ is discrete in $\mathbf{R}$, it is not discrete in $\mathbf{Q}_p$, and in fact has closure $\mathbf{Z}_p$. This raises the possibility of p-adically interpolating a sequence a_n, which is really a function $n \mapsto a_n$ on $\mathbf{N}$, to a continuous function $x \mapsto a_x$ with $x \in \mathbf{Z}_p$. Our basic question is this: when does a function $f\colon \mathbf{N} \to \mathbf{Q}_p$ extend to a continuous function $\mathbf{Z}_p \to \mathbf{Q}_p$? We will look at some concrete examples, then see what a general continuous function $\mathbf{Z}_p \to \mathbf{Q}_p$ looks like, and finally discuss one approach to p-adic integration.

2. p-adic interpolation of a^n

The simplest example of p-adic interpolation occurs for the function $f(n) = a^n$ where $a \in 1 + p\mathbf{Z}_p$.

Theorem 2.1. *Let $a \in 1 + p\mathbf{Z}_p$, so $|a-1|_p \leq 1/p$. For integers $m, n \geq 0$,*

$$|a^m - a^n|_p \leq |a-1|_p |m-n|_p.$$

This shows in a precise form that a^n is p-adically uniformly continuous in n.

Proof. Without loss of generality, $m \geq n$. Since $a \in 1 + p\mathbf{Z}_p \subset \mathbf{Z}_p^\times$, $|a|_p = 1$. Then

$$|a^m - a^n|_p = |a^n(a^{m-n} - 1)|_p = |a^{m-n} - 1|_p.$$

Now that we have m and n only appearing in the context of $m - n$, our task is equivalent to showing

$$|a^k - 1|_p \leq |a-1|_p |k|_p \tag{2.1}$$

for $k \in \mathbf{N}$. This is clear if $k = 0$, so take $k \geq 1$. We will use the factorization

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \cdots + a + 1).$$

Since $|a|_p = 1$, taking absolute values of both sides tells us

$$|a^k - 1|_p \leq |a-1|_p \cdot 1 = |a-1|_p, \tag{2.2}$$

so our goal is reached if p doesn't divide k. If p does divide k, (2.1) is stronger than (2.2) since $|k|_p < 1$. First we treat $k = p$:

$$a^p - 1 = (a-1)(a^{p-1} + a^{p-2} + \cdots + a + 1).$$

The second factor is a sum of p p-adic integers, each being 1 mod p, so modulo p the second factor is $1 + 1 + \cdots + 1 = p \equiv 0 \bmod p$. Thus $|a^p - 1|_p \leq |a-1|_p(1/p) = |a-1|_p |p|_p$, which is (2.1) at $k = p$. By induction, writing $|a^{p^r} - 1|_p$ as $|(a^p)^{p^{r-1}} - 1|_p$, we get (2.2) whenever

k is a power of p. For the general case, write $k = p^r k'$, where p doesn't divide k'. Then by the separate cases for exponent prime to p and exponent a power of p,

$$|a^k - 1|_p = |(a^{p^r})^{k'} - 1|_p \leq |a^{p^r} - 1|_p \leq |a-1|_p \frac{1}{p^r} = |a-1|_p |k|_p.$$

■

Definition 2.2. For $a \in 1 + p\mathbf{Z}_p$ and $x \in \mathbf{Z}_p$, define

$$a^x = \lim_{i \to \infty} a^{n_i},$$

where the limit is taken over any sequence $n_i \in \mathbf{N}$ which converges p-adically to x.

This definition of a^x makes sense because a uniformly continuous function on a dense subset of a compact metric space extends to the whole space. More precisely, we have

Theorem 2.3. *Let X be a compact metric space, Y be a complete metric space, and $f\colon D \to Y$ be a uniformly continuous function on a dense subset D of X. Then f extends uniquely to a continuous function $f\colon X \to Y$ by the formula*

$$f(x) = \lim_{i \to \infty} f(d_i),$$

where the limit is taken over any sequence $\{d_i\}$ in D which converges to x.

We omit the proof, but note that to show the definition of the extended function is well-defined (that is, two sequences in D which tend to x have their function values tend to the same limit) we need the uniform continuity of f on D.

Applying this theorem with $X = \mathbf{Z}_p$, $D = \mathbf{N}$, and $Y = \mathbf{Q}_p$ justifies our definition of a^x for $x \in \mathbf{Z}_p$.

Note it is *false* that a continuous (not uniformly continuous) function on a dense subset of a compact metric space has to extend to the whole space. Consider $f(x) = 1/(x^2 - 2)$ on the rationals in $[1, 2]$. It is continuous on that dense subset but doesn't extend to a continuous function on $[1, 2]$ since it blows up as $x \to \sqrt{2}$.

Here are some properties of a^x for $x \in \mathbf{Z}_p$:

(1) $|a^x - a^y|_p \leq |a-1|_p |x-y|_p$, so in particular $|a^x - 1|_p \leq |a-1|_p |x|_p \leq |a-1|_p \leq 1/p$,
(2) $a^{x+y} = a^x a^y$,
(3) $(a^x)^y = a^{xy}$.

The proofs of these are easy: all expressions are continuous in x and y, so their validity follows by continuity from their validity on $\mathbf{N}$ (where one can verify the properties by induction, say). Notice we need the estimate $|a^x - 1|_p \leq 1/p$ from the first property to make sense of $(a^x)^y$ in the third property. Taking $y = -x$ in the second property gives us $1 = a^x a^{-x}$, so $a^{-x} = 1/a^x$, just as we would expect. In particular, for negative integers x, a^x has its usual meaning!

Remark 2.4. Although we proved a^n is p-adically (uniformly) continuous in n when $|a - 1|_p \leq 1/p$, could it also be p-adically continuous in n for other $a \in \mathbf{Q}_p$? No. Indeed, assume a^n is p-adically continuous in n. Then, since $p^r \to 0$ in $\mathbf{Z}_p$ as $r \to \infty$, $a^{p^r} \to a^0 = 1$, hence $|a^{p^r} - 1|_p \leq 1/p$ for r large. Then $|a^{p^r}|_p = 1$ for r large, so $|a|_p = 1$. We're not done; so far we just have that $a \in \mathbf{Z}_p^\times$. To show $a \in 1 + p\mathbf{Z}_p$, we return to the estimate $|a^{p^r} - 1|_p \leq 1/p$ for large r. Because we know a is a p-adic integer, we can rewrite this estimate as the congruence

$$a^{p^r} \equiv 1 \bmod p\mathbf{Z}_p.$$

By Fermat's little theorem, $a^p \equiv a \bmod p\mathbf{Z}$ for $a \in \mathbf{Z}$. The same result goes through for p-adic integers (since $\mathbf{Z}_p/p\mathbf{Z}_p \cong \mathbf{Z}/p\mathbf{Z}$), so $a^p \equiv a \bmod p\mathbf{Z}$ when $a \in \mathbf{Z}_p$. Repeating the pth power several times, we get

$$a^{p^r} \equiv a \bmod p\mathbf{Z}_p.$$

From the two displayed congruences, $a \equiv 1 \bmod p\mathbf{Z}_p$, so $a \in 1 + p\mathbf{Z}_p$.

Example 2.5. When $p = 2$, we have the continuous function a^x for all $x \in \mathbf{Z}_2$ if $|a-1|_2 \leq 1/2$, which means $a \in \mathbf{Z}_2^\times$. In particular, we can speak about $(-1)^x$ for $x \in \mathbf{Z}_2$. What does this mean? It's this:

$$(-1)^x = \begin{cases} 1, & \text{if } x \in 2\mathbf{Z}_2, \\ -1, & \text{if } x \in 1 + 2\mathbf{Z}_2. \end{cases}$$

After all, when $n \in \mathbf{N}$ we have

$$(-1)^n = \begin{cases} 1, & \text{if } n \in 2\mathbf{Z}, \\ -1, & \text{if } n \in 1 + 2\mathbf{Z}, \end{cases}$$

so $(-1)^n$ is 2-adically locally constant on $\mathbf{N}$, and thus its (unique) continuous extension to $\mathbf{Z}_2$ is the function that's 1 on $2\mathbf{Z}_2$ (the 2-adic closure of the even natural numbers) and -1 on $1 + 2\mathbf{Z}_2$ (the 2-adic closure of the odd natural numbers).

Let's refine the inequality $|a^x - 1|_p \leq |a-1|_p|x|_p$ to an equality.

Theorem 2.6. *For p odd and $a \in 1 + p\mathbf{Z}_p$, $|a^x - a^y|_p = |a-1|_p|x-y|_p$ for all x and y in $\mathbf{Z}_p$. This holds for $p = 2$ when $a \in 1 + 4\mathbf{Z}_2$.*

Proof. Writing $|a^x - a^y|_p$ as $|(a^{x-y} - 1)a^y|_p = |a^{x-y} - 1|_p$, since $a^y \in \mathbf{Z}_p^\times$, we are reduced to the case $y = 0$: show $|a^x - 1|_p = |a-1|_p|x|_p$ for $x \in \mathbf{Z}_p$. Because both sides are continuous in x, it suffices to check the formula when x is a positive integer. It suffices to check two cases:

- if n is not divisible by p then $|a^n - 1|_p = |a-1|_p$,
- $|a^p - 1|_p = |a-1|_p \frac{1}{p}$.

From these two cases, the general formula $|a^k - 1|_p = |a-1|_p|k|_p$ will follow in the same way we proved the inequality (2.1) from the two special cases when k is not divisible by p and when $k = p$.

The two cases above are clear when $a = 1$, so we may assume $a \neq 1$. Set $|a-1|_p = 1/p^r$, so $a = 1 + p^r u$ where $u \in \mathbf{Z}_p^\times$ and $r \geq 1$ for odd p and $r \geq 2$ for $p = 2$. Then

$$\begin{aligned} a^n - 1 &= (1 + p^r u)^n - 1 \\ &= 1 + np^r u + \sum_{j=2}^{n} \binom{n}{j} (p^r u)^j - 1 \\ &= np^r u + \sum_{j=2}^{n} \binom{n}{j} p^{rj} u^j. \end{aligned}$$

Every term past the first term is divisible by p^{2r}, hence by p^{r+1}, so

$$a^n - 1 \equiv np^r u \bmod p^{r+1}.$$

If n is not divisible by p then $np^r u$ is divisible by p^r but not by p^{r+1}, so $a^n - 1$ is divisible by p^r but not by p^{r+1}. Hence $|a^n - 1|_p = 1/p^r = |a-1|_p$.

Now we look at $a^p - 1$:

$$a^p - 1 = (1 + p^r u)^p - 1 = p^{r+1}u + \sum_{j=2}^{p} \binom{p}{j} p^{rj} u^j.$$

The first term on the right is divisible by p^{r+1} but not p^{r+2}. Are the terms in the sum all divisible by p^{r+2}?

Case 1: p odd. For $2 \leq j \leq p-1$, $\binom{p}{j}$ is divisible by p, so the j-th term in the sum is divisible by p^{rj+1} and $rj+1 \geq 2r+1 \geq r+2$. The term for $j = p$ is $p^{rp}u^p$ and $rp \geq 3r \geq r+2$.

Case 2: $p = 2$. The sum is the single term $2^{2r}u^2$, and $2r \geq r+2$ if $r \geq 2$, and that bound on r is correct since $a \in 1 + 4\mathbf{Z}_2$.

Thus all terms in the sum are multiples of p^{r+2}, so $a^p - 1 \equiv p^{r+1}u \bmod p^{r+2}$, which implies $|a^p - 1|_p = 1/p^{r+1} = |a-1|_p(1/p)$. ∎

If $a \in \mathbf{Z}$ and x and y are nonnegative integers, Theorem 2.6 is saying something very concrete about divisibility: if $p \neq 2$ and $a \equiv 1 \bmod p$ then the highest power of p in $a^x - a^y$ is the sum of the highest powers of p in $a - 1$ and $x - y$. This is typical of the way p-adic methods can be used to put otherwise idiosyncratic divisibility properties in a clearer light.

Although the 2-adic function a^x makes sense for all $a \in 1+2\mathbf{Z}_2$, Theorem 2.6 only applies to $a \in 1+4\mathbf{Z}_2$. This restriction is important, since if $a \in (1+2\mathbf{Z}_2) - (1+4\mathbf{Z}_2) = 3+4\mathbf{Z}_2$, the absolute value formula in Theorem 2.6 will fail for some x: since $-a \in 1 + 4\mathbf{Z}_2$, $|a^2 - 1|_2 = |(-a)^2 - 1|_2 = |-a-1|_2|2|_2 = |a+1|_2/2 \leq 1/8$, while $|a-1|_2|2|_2 = 1/4$.

Let's put these ideas to work in a concrete problem that doesn't sound p-adic at all.

Theorem 2.7. *For odd primes p, the group of units $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is cyclic for all $n \geq 1$.*

The group $(\mathbf{Z}/2^n\mathbf{Z})^\times$ is not cyclic for $n \geq 3$, so the restriction to odd p is crucial.

Proof. The size of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is $p^n - p^{n-1} = (p-1)p^{n-1}$. To prove this group is cyclic, we will show it has an element of order $p-1$ and an element of order p^{n-1}. These orders are relatively prime, so the product of those two elements must have order $(p-1)p^{n-1}$.

We begin by viewing the (finite) ring $\mathbf{Z}/p^n\mathbf{Z}$ as $\mathbf{Z}_p/p^n\mathbf{Z}_p$. Taking unit groups, $(\mathbf{Z}/p^n\mathbf{Z})^\times \cong (\mathbf{Z}_p/p^n\mathbf{Z}_p)^\times$. So what? It may look silly to be writing a *finite* group derived from integers in terms of p-adic integers. The advantage of doing this is how we can think about the congruences among units. In $\mathbf{Z}_p$, a unit mod p^n is a bona fide unit in $\mathbf{Z}_p$ (we can't say that in $\mathbf{Z}$, where there are just two units). Moreover, if u and v are in $\mathbf{Z}_p^\times$, then

$$u \equiv v \bmod p^n\mathbf{Z}_p \iff u - v \in p\mathbf{Z}_p \iff \frac{u}{v} - 1 \in p\mathbf{Z}_p \iff \frac{u}{v} \in 1 + p^n\mathbf{Z}_p,$$

and $1 + p^n\mathbf{Z}_p$ is a subgroup of $\mathbf{Z}_p^\times$. So the additive congruence "$u = v$" in $\mathbf{Z}_p/p^n\mathbf{Z}_p$ (with $u, v \in \mathbf{Z}_p^\times$) has been turned into a multiplicative congruence "$u = v$" in $\mathbf{Z}_p^\times/(1 + p^n\mathbf{Z}_p)$. (Think about that and convince yourself it's true.) So

$$(\mathbf{Z}/p^n\mathbf{Z})^\times \cong (\mathbf{Z}_p/p^n\mathbf{Z}_p)^\times \cong \mathbf{Z}_p^\times/(1 + p^n\mathbf{Z}_p).$$

Now we use the multiplicative decomposition of $\mathbf{Z}_p^\times$,

$$\mathbf{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbf{Z}_p),$$

to write

$$\mathbf{Z}_p^\times/(1 + p^n\mathbf{Z}_p) \cong \mu_{p-1} \times (1 + p\mathbf{Z}_p)/(1 + p^n\mathbf{Z}_p),$$

so we have split up $(\mathbf{Z}/p^n\mathbf{Z})^\times$ into the direct product of μ_{p-1} and $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$. The whole group has order $(p-1)p^{n-1}$ and μ_{p-1} has order $p-1$, so $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$ must have order p^{n-1}.

It is a theorem in abstract algebra that a finite subgroup of the nonzero elements of a field is a cyclic group. Since the group μ_{p-1} is a finite subgroup of $\mathbf{Q}_p^\times$, it is cyclic. Thus there is an element of μ_{p-1} with order $p-1$. (There is not an effective algorithm to write such an element down.) Now we want to show $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$ contains an element of order p^{n-1}. This we can do effectively, as follows.

We'll show if $a \in 1+p\mathbf{Z}_p$ and $a \notin 1+p^2\mathbf{Z}_p$ (that is, $|a-1|_p = 1/p$), then a is a generator in $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$). In particular, $1+p$ is a generator of $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$.

To prove this, we use the exact formula in Theorem 2.6 for odd p. (This is the first time it matters that $p \neq 2$.) For $m \in \mathbf{Z}^+$, a^m is 1 in $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$ if and only if $a^m \in 1+p^n\mathbf{Z}_p$, which is equivalent to $|a^m-1|_p \leq 1/p^n$. Using Theorem 2.6,

$$|a^m-1|_p = |a-1|_p|m|_p = \frac{1}{p}|m|_p,$$

so

$$|a^m-1|_p \leq \frac{1}{p^n} \Longleftrightarrow |m|_p \leq \frac{1}{p^{n-1}}.$$

Here m is a positive integer, so the final p-adic estimate is equivalent to $p^{n-1}|m$. Thus

$$a^m = 1 \text{ in } (1+p\mathbf{Z}_p)/(1+p^m\mathbf{Z}_p) \Longleftrightarrow p^{n-1}|m.$$

Since $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$ has order p^{n-1}, we see that a is a generator. ∎

Remark 2.8. For $p=2$, $\mathbf{Z}_2^\times = 1+2\mathbf{Z}_2 = \{\pm 1\} \times (1+4\mathbf{Z}_2)$, so for $n \geq 2$ we have

$$(\mathbf{Z}/2^n\mathbf{Z})^\times \cong (\mathbf{Z}_2/2^n\mathbf{Z}_2)^\times \cong \mathbf{Z}_2^\times/(1+2^n\mathbf{Z}_2) = \{\pm 1\} \times (1+4\mathbf{Z}_2)/(1+2^n\mathbf{Z}_2).$$

Using the $p=2$ case of Theorem 2.6, the number 5 (or any $a \in 1+4\mathbf{Z}_2$ not in $1+8\mathbf{Z}_2$) is a generator of $(1+4\mathbf{Z}_2)/(1+2^n\mathbf{Z}_2)$. Thus the group $(\mathbf{Z}/2^n\mathbf{Z})^\times$, of order 2^{n-1}, is a direct product of a group of order 2 and a group of order 2^{n-2}.

The additive group $\mathbf{Z}_p$, while not cyclic, is *topologically* cyclic: the number 1 generates a dense subgroup, so we call 1 a topological generator. More precisely, the (additive) topological generators of $\mathbf{Z}_p$ are exactly the p-adic units (elements of $\mathbf{Z}_p^\times$). The multiplicative group $1+p\mathbf{Z}_p$ also turns out to be topologically cyclic:

Corollary 2.9. *If p is odd and $|a-1|_p = 1/p$, the sequence $\{a^m : m \geq 0\}$ is dense in $1+p\mathbf{Z}_p$, If $|a-1|_p \leq 1/p^2$, a is not a topological generator of $1+p\mathbf{Z}_p$.*

Proof. If $|a-1|_p \leq 1/p^2$, so $a \equiv 1 \bmod p^2$, then $a^m \equiv 1 \bmod p^2$ for all $m \in \mathbf{N}$. Writing this as $a^m \in 1+p^2\mathbf{Z}_p$, we see (since $1+p^2\mathbf{Z}_p$ is closed) no integral power of a will get near a number that's in $1+p\mathbf{Z}_p$ but not in $1+p^2\mathbf{Z}_p$. Thus a is not a topological generator.

Now we take $|a-1|_p = 1/p$. For $t \in 1+p\mathbf{Z}_p$, we want to show the integral powers of a get arbitrarily close to t. Closeness in $\mathbf{Z}_p$ is described by p-power congruences, so it suffices to show for any $n \geq 1$ that we can solve $a^m \equiv t \bmod p^n\mathbf{Z}_p$ for some $m \in \mathbf{N}$. This is easy: in $(1+p\mathbf{Z}_p)/(1+p^n\mathbf{Z}_p)$, a is a generator by the proof of Theorem 2.7, so every coset in this group contains a power of a. Hence $t(1+p^n\mathbf{Z}_p)$ contains some a^m. That means $a^m \in t(1+p^n\mathbf{Z}_p) = t+p^n\mathbf{Z}_p$, so $a^m \equiv t \bmod p^n\mathbf{Z}_p$. ∎

When $|a-1|_p = 1/p$ and $p \neq 2$, the function $\mathbf{Z}_p \to 1+p\mathbf{Z}_p$ given by $x \mapsto a^x$ is continuous and the image is dense (since the nonnegative integral powers of a are dense in $1 + p\mathbf{Z}_p$). The image is compact since $\mathbf{Z}_p$ is compact, so the image is closed. A closed subset of $1+p\mathbf{Z}_p$ containing a dense subset has to be everything, so $a^{\mathbf{Z}_p} = 1 + p\mathbf{Z}_p$. The analogous result when $p = 2$ is: if $|a-1|_2 = 1/4$ then a is a topological generator of $1 + 4\mathbf{Z}_2$.

Example 2.10. Both 7 and 13 are topological generators of $1+3\mathbf{Z}_3$. In particular, $13 = 7^a$ and $7 = 13^b$ for some 3-adic integers a and b. So although 7 and 13 are multiplicatively independent allowing integer exponents (because they are different prime numbers), they are not multiplicatively independent if we allow 3-adic integer exponents. Put differently, the finitely generated group $\langle 7, 13\rangle$ is not cyclic but its 3-adic closure is the topologically cyclic group $1 + 3\mathbf{Z}_3$ with either 7 or 13 as a topological generator.

Incidentally, how do we find $a \in \mathbf{Z}_3$ such that $13 = 7^a$? To estimate a, we can just solve $13 \equiv 7^{a_n} \bmod 3^n$ on a computer with successive values of n. For $n = 2, 3, 4, 5, 6$, the exponent that fits is $2, 5, 14, 14, 176$. These are 3-adically consistent since $176 = 2 + 3 + 3^2 + 2 \cdot 3^4$, whose truncations are 2, 5, and 14. The 3-adic limit of such a_n is a.

3. Representation of p-adically continuous functions

So far we have p-adically interpolated the sequence a^n when $|a-1|_p \leq 1/p$. What about interpolating other sequences?[1] We will describe a simple construction for this purpose using binomial coefficient polynomials: for $n \geq 0$, set

$$\binom{X}{n} = \frac{X(X-1)\cdots(X-n+1)}{n!}. \tag{3.1}$$

The first few of these are $\binom{X}{0} = 1$ (constant polynomial), $\binom{X}{1} = X$, and $\binom{X}{2} = \frac{X(X-1)}{2}$. We can treat these as functions on $\mathbf{Q}_p$ and substitute p-adic numbers for X. When $a \in \mathbf{N}$ with $a \geq n$, we know from combinatorics that $\binom{a}{n} \in \mathbf{N}$, and $\binom{a}{n} = 0$ for $n \geq 1$ when $0 \leq a < n-1$. What can be said about $\binom{x}{n}$ for p-adic integers x? Here is an illustrative example.

Example 3.1. Consider $\binom{1/2}{n}$. For $n = 0, 1, 2, 3, 4, 5$, and 6, the successive values are 1, $1/2$, $-1/8$, $1/16$, $-5/128$, $7/256$, and $-21/1024$. Notice the denominators are purely powers of 2. To show the rational number $\binom{1/2}{n}$ has a 2-power denominator, we will show it is a p-adic integer for any odd prime p. (Make sure you understand why this would explain things!) When $p \neq 2$, $1/2 \in \mathbf{Z}_p$, so $1/2$ is a p-adic limit of positive integers, such as the truncations of its p-adic expansion. Since polynomial functions on $\mathbf{Q}_p$ are continuous, writing $1/2 = \lim_{k\to\infty} a_k$ with $a_k \in \mathbf{N}$ we get

$$\binom{1/2}{n} = \lim_{k\to\infty} \binom{a_k}{n}.$$

The binomial coefficients $\binom{a_k}{n}$ are in $\mathbf{N}$ (by combinatorics), so a p-adic limit of them must be in $\mathbf{Z}_p$. Therefore $\binom{1/2}{n} \in \mathbf{Z}_p$ for all odd primes p, so the only prime which can be in its denominator is 2.

[1] We will only discuss further the *general* concept of interpolation. There are many *particular* sequences in number theory, such as special values of zeta-functions and L-functions, whose p-adic interpolation is a big business. But the background to understand what this means and why anyone should care would be another course.

There is a way to see $\binom{1/2}{n}$ has a 2-power denominator without p-adic considerations. By working from the definition of $\binom{1/2}{n}$ in (3.1) as a long product divided by $n!$, some algebraic manipulation yields

$$\binom{1/2}{n} = \frac{\binom{2n-2}{n-1} - \binom{2n-2}{n-2}}{2^{2n-1}}$$

for $n \geq 2$. The numerator is a difference of binomial coefficients and thus is an integer, so $\binom{1/2}{n}$ has a denominator that is a power of 2. The numerator is sometimes even, so the power of 2 in the denominator of this formula is not necessarily the smallest one possible.

Theorem 3.2. *If $x \in \mathbf{Z}_p$ then $\binom{x}{n} \in \mathbf{Z}_p$ for all $n \geq 0$.*

Proof. Use p-adic continuity as in the example of $\binom{1/2}{n}$. For $x \in \mathbf{Z}_p$, x is a p-adic limit of nonnegative integers, so $\binom{x}{n}$ is a limit of ordinary binomial coefficients, which are nonnegative integers. Thus the limit is in $\mathbf{Z}_p$. ∎

Example 3.3. For $r \in \mathbf{Q}$, the only primes that might appear in the denominator of $\binom{r}{n} \in \mathbf{Q}$ are the primes in the denominator of r: if p is a prime not in the denominator of r then $r \in \mathbf{Z}_p$ so $\binom{r}{n} \in \mathbf{Z}_p$, hence p is not in the denominator of $\binom{r}{n}$. Unlike the special case of $\binom{1/2}{n}$, it doesn't seem worth trying to find a non-p-adic explanation of this very general result.

Now we are in a position to write down many examples of continuous functions $\mathbf{Z}_p \to \mathbf{Q}_p$. If $c_n \in \mathbf{Q}_p$ and $c_n \to 0$ as $n \to \infty$, the series

$$f(x) = \sum_{n \geq 0} c_n \binom{x}{n} = c_0 + c_1 x + c_2 \frac{x(x-1)}{2} + \cdots \tag{3.2}$$

converges on $\mathbf{Z}_p$ since the general term tends to 0. In fact, $|c_n\binom{x}{n}|_p \leq |c_n|_p \to 0$ uniformly in x, so by the Weierstrass M-test this series is uniformly convergent on $\mathbf{Z}_p$. Each summand is a continuous function (polynomials are continuous), so f is continuous.

Let's see how to recover the coefficients c_n from the values of the function on $\mathbf{N}$. When x is a nonnegative integer, the series in (3.2) truncates to a finite sum and we get the successive values

$$f(0) = c_0, \quad f(1) = c_0 + c_1, \quad f(2) = c_0 + 2c_1 + c_2, \quad f(3) = c_0 + 3c_1 + 3c_2 + c_3.$$

These equations can be successively inverted to write the c_n's in terms of f-values:

$$c_0 = f(0), \quad c_1 = f(1) - f(0), \quad c_2 = f(2) - 2f(1) + f(0), \quad c_3 = f(3) - 3f(2) + 3f(1) - f(0).$$

The evident alternating sign and binomial coefficient patterns continue, and it turns out that

$$c_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} f(k) \tag{3.3}$$

for all n. In particular, the coefficients c_n in the series (3.2) are uniquely determined, just like coefficients in a power series expansion are uniquely determined. Amazingly, the simple construction in (3.2) of continuous functions from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ accounts for all of them.

Theorem 3.4 (Mahler, 1958). *If $f\colon \mathbf{Z}_p \to \mathbf{Q}_p$ is continuous then the sequence of numbers c_n defined by* (3.3) *tends to* 0 *and the representation* (3.2) *holds for all x in $\mathbf{Z}_p$.*

The hard part of this proof (which we omit) is showing the sequence c_n in (3.3) p-adically tends to 0 as $n \to \infty$ when f is a continuous function. Once we grant this decay in the c_n's, the rest of the proof is easy: define a continuous function $g\colon \mathbf{Z}_p \to \mathbf{Q}_p$ by $g(x) = \sum_{n\geq 0} c_n\binom{x}{n}$, invert the formula (3.3) to show $f(m) = g(m)$ for all $m \in \mathbf{N}$, and then by continuity of both sides we have $f(x) = g(x)$ for all $x \in \mathbf{Z}_p$.

Since the partial sums $\sum_{n=0}^{N} c_n\binom{x}{n}$ converge uniformly (not just pointwise) to f, and are polynomials, we have a very explicit p-adic Stone-Weierstrass theorem for continuous functions $\mathbf{Z}_p \to \mathbf{Q}_p$. The classical Stone-Weierstrass theorem (well, Weierstrass' part) says any continuous function $[0,1] \to \mathbf{R}$ can be uniformly approximated by real polynomial functions.

Now we have a necessary and sufficient criterion for p-adic interpolation: if a_n is a sequence of p-adic numbers, there is a continuous function $f\colon \mathbf{Z}_p \to \mathbf{Q}_p$ interpolating these values, in the sense that $f(n) = a_n$ for all $n \in \mathbf{N}$, if and only if the sequence of numbers

$$\sum_{k=0}^{n}(-1)^{n-k}\binom{n}{k}a_k$$

tends to 0 in $\mathbf{Q}_p$ as $n \to \infty$.

Example 3.5. The sequence $n!$ tends to 0 in $\mathbf{Q}_p$ as $n \to \infty$, so

$$\sum_{n\geq 0} n!\binom{x}{n} = 1 + x + x(x-1) + x(x-1)(x-2) + \cdots$$

is a continuous function on $\mathbf{Z}_p$ (for all p). This is, as far as I am aware, a *useless* function.

Example 3.6. Another sequence tending to 0 p-adically is p^n. The continuous function $\sum_{n\geq 0} p^n\binom{x}{n}$ is something very familiar. It's just $(1+p)^x$:

$$(1+p)^x = \sum_{n\geq 0} p^n\binom{x}{n}.$$

It's easy to check this: since both sides are continuous in x, it suffices to check they agree on $\mathbf{N}$ to know they agree on $\mathbf{Z}_p$. When $x = m$ is a natural number, the right side truncates to the finite sum $\sum_{n=0}^{m} p^n\binom{m}{n}$, which is $(1+p)^m$ by the binomial theorem!

In fact, whenever $|a-1|_p < 1$ the powers $(a-1)^n$ tend to 0 and we have

$$a^x = \sum_{n\geq 0}(a-1)^n\binom{x}{n} \tag{3.4}$$

for $x \in \mathbf{Z}_p$ since both sides are continuous and are equal on $\mathbf{N}$. We could have bypassed the whole original interpolation business with powers of a and just written down the formula $\sum_{n\geq 0}(a-1)^n\binom{x}{n}$ as an obvious (!) continuous function of $x \in \mathbf{Z}_p$ which has the values a^m when $x = m$ is a natural number. This provides an alternate proof that the nonnegative powers of a have a p-adic interpolation when $|a-1|_p < 1$, because we can simply write down a continuous function with the integral powers of a as its special values on nonnegative integers.

Example 3.7. Taking $a = -1$, so $a - 1 = -2$, our knowledge of $(-1)^x$ for $x \in \mathbf{Z}_2$ gives us

$$\sum_{n\geq 0}(-2)^n\binom{x}{n} = \begin{cases} 1, & \text{if } x \in 2\mathbf{Z}_2, \\ -1, & \text{if } x \in 1 + 2\mathbf{Z}_2. \end{cases}$$

The series (3.4) begins as $a^x = 1 + (a-1)x + (a-1)^2\binom{x}{2} + \ldots$, so

$$|a^x - 1|_p \leq \max_{n\geq 1}\left|(a-1)^n\binom{x}{n}\right|_p \leq \max_{n\geq 1}|(a-1)^n|_p \leq |a-1|_p,$$

which is one of the estimates we found earlier by another method.

Remark 3.8. Although $\binom{x}{n}$ is a polynomial, it is not at all the case that a series $\sum_{n\geq 0} c_n\binom{x}{n}$ with $c_n \to 0$ can generally be rearranged to become a power series in x. Indeed, series of the type $\sum_{n\geq 0} c_n\binom{x}{n}$ describe all continuous functions $\mathbf{Z}_p \to \mathbf{Q}_p$ but most continuous functions are not p-adic analytic (that is, are not given by a single power series convergent on all of $\mathbf{Z}_p$).

The most important property of the expansion (3.2) for continuous functions is that the natural concept of size for a function is the same as the natural concept of size for its sequence of coefficients (which are going to 0):

$$\max_{x\in\mathbf{Z}_p}|f(x)|_p = \max_{n\geq 0}|c_n|_p. \tag{3.5}$$

The proof of this is trivial: from the series $f(x) = \sum_{n\geq 0} c_n\binom{x}{n}$ we get

$$|f(x)|_p \leq \max_{n\geq 0}\left|c_n\binom{x}{n}\right|_p \leq \max_{n\geq 0}|c_n|_p.$$

This holds for all x, so $\max_{x\in\mathbf{Z}_p}|f(x)|_p \leq \max_{n\geq 0}|c_n|_p$. For the reverse inequality, we use (3.3): the binomial coefficients $\binom{n}{k}$ there are integers, so their p-adic size is at most 1, hence

$$|c_n|_p \leq \max_{0\leq k\leq n}|f(k)|_p \leq \max_{x\in\mathbf{Z}_p}|f(x)|_p.$$

This holds for all n, so $\max_{n\geq 0}|c_n|_p \leq \max_{x\in\mathbf{Z}_p}|f(x)|_p$.

Let $C(\mathbf{Z}_p, \mathbf{Q}_p)$ be the continuous functions from $\mathbf{Z}_p$ to $\mathbf{Q}_p$ and let $c_0(\mathbf{Q}_p) = \{(c_n) : c_n \in \mathbf{Q}_p, c_n \to 0\}$ be the sequences tending to 0 in $\mathbf{Q}_p$. Both are $\mathbf{Q}_p$-vector spaces under the natural addition and $\mathbf{Q}_p$-scaling. Let $||f|| = \max_{x\in\mathbf{Z}_p}|f(x)|_p$ and $||(c_n)|| = \max_{n\geq 0}|c_n|_p$. Using $||f-g||$ and $||(c_n)-(d_n)||$ as the distances between two functions and two sequences, both $C(\mathbf{Z}_p, \mathbf{Q}_p)$ and $c_0(\mathbf{Q}_p)$ are complete metric spaces. In fact, (3.5) tells us these spaces are isomorphic to each other, with the isomorphism being $f \mapsto (c_n)$ where the c_n's are the coefficients in the expansion of f given by (3.3). This is completely unlike the real case, where $C([0,1], \mathbf{R})$ is (provably) not isomorphic to the space $c_0(\mathbf{R})$ of real sequences tending to 0.[2]

4. p-adic integration

As a final topic, let's briefly discuss p-adic integration. There are two senses one can mean by the phrase "p-adic integration":

- integration of real/complex-valued functions defined on a p-adic space (like $\mathbf{Z}_p$),
- integration of p-adic valued functions defined on a p-adic space (like $\mathbf{Z}_p$).

[2]The proof of this needs functional analysis. The natural map from $C([0,1], \mathbf{R})$ to its double dual space is an isomorphism while the natural map of $c_0(\mathbf{R})$ to its double dual space is not an isomorphism. Here the "dual space" is meant in the sense of analysis: the *continuous* linear functionals.

The first kind of integration is just a special case of the general theory of integration through measure theory. It's the second integration that presents something really new: integrating a function taking p-adic values.

Let's recall the more classical type of integration through linear functionals. Integration of real-valued continuous functions on $[0,1]$ can be regarded as a function $I\colon C([0,1],\mathbf{R}) \to \mathbf{R}$, where

$$I(f) = \int_0^1 f(x)\,\mathrm{d}x.$$

This I is $\mathbf{R}$-linear and satisfies $|I(f)| \leq ||f||$, where $||f||$ denotes the maximum value of $|f(x)|$ for $x \in [0,1]$. Using measure theory, all $\mathbf{R}$-linear functions $I\colon C([0,1],\mathbf{R}) \to \mathbf{R}$ such that $|I(f)| \leq c||f||$ for some nonnegative constant c turn out to be integrals: $I(f) = \int_0^1 f(x)\,\mathrm{d}\mu(x)$ where μ is a measure on $[0,1]$.

In the p-adic framework, we will call any $\mathbf{Q}_p$-linear function $I\colon C(\mathbf{Z}_p,\mathbf{Q}_p) \to \mathbf{Q}_p$ such that $|I(f)|_p \leq c||f||$ for some nonnegative constant c a p-adic integral. It's very easy to write examples of these down. Fixing a *bounded* sequence $\mathbf{b} = (b_n)$ in $\mathbf{Q}_p$, we can take its dot product with the coefficients in the expansion $f(x) = \sum_{n\geq 0} c_n\binom{x}{n}$ of any $f \in C(\mathbf{Z}_p,\mathbf{Q}_p)$:

$$I_{\mathbf{b}}(f) \stackrel{\text{def}}{=} \sum_{n\geq 0} b_n c_n.$$

This series converges in $\mathbf{Q}_p$ since the general term tends to 0. The value of the series is some p-adic number, and $I_{\mathbf{b}}$ is a p-adic integral. It turns out all p-adic integrals have the form $I_{\mathbf{b}}$ for some bounded sequence $\mathbf{b}$ in $\mathbf{Q}_p$.

If we want to turn sequences in $c_0(\mathbf{R})$ into real numbers in a nice way, we can't do as in the p-adic case by a dot product with a bounded real sequence: if (b_n) is bounded in $\mathbf{R}$ and $c_n \to 0$ in $\mathbf{R}$, the dot product $\sum_n b_n c_n$ need not converge. For the series $\sum b_n c_n$ to make sense for *all* sequences (c_n) tending to 0, it would be sufficient for the series $\sum b_n$ to be absolutely convergent, and that sufficient condition is necessary too. It's interesting that in the p-adic setting we had no need for the notion of absolutely convergent series.