p-ADIC CONTINUITY

Berkeley Math Circle class with Masha Vlasenko. April 3, 2019.

Notation.

$$
\begin{array}{l}
\mathbb{N} = \{1, 2, 3, \ldots\} \quad \text{(natural numbers)} \\
\cap \\
\mathbb{Z} \quad \text{(integers)} \\
\cap \\
\mathbb{Q} \quad \text{(rational numbers)} \\
\cap \\
\mathbb{R} \quad \text{(real numbers)} \\
\cap \\
\mathbb{C} \quad \text{(complex numbers)}
\end{array}
$$

$a \equiv b \mod m$ or $m|(a-b)$ means that m divides $a-b$
$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$ is the set of remainders modulo m
$p \in \{2, 3, 5, 7, 11, \ldots\}$ is a prime number
$\triangleright$ denotes an exercise
★ are harder exercises; they usually require a few steps and you might need an extra sheet (or a notebook) to solve them

1. Algebra with p-adic numbers

1.1. **Definition, operations, examples.** The set of p-adic integers is defined as

$$\mathbb{Z}_p = \left\{ x = (x_1, x_2, \ldots) \;\middle|\; x_n \in \mathbb{Z}/p^n\mathbb{Z}\,,\ x_{n+1} \equiv x_n \mod p^n \right\}.$$

Compare this to thinking about real numbers as being approximated by sequences of decimal fractions, e.g.

$$\pi = (3, 3.1, 3.14, 3.141, 3.1415, \ldots)$$

Remark. The following question is still a mystery for number theorists: what is the p-adic analogue of π? If you follow our discussion to the very end, you will learn some tools for thinking about this problem.

Observe:

- For each n the component x_n defines all preceding components: $x_1 = x_n \mod p$, $x_2 = x_n \mod p^2$, and so on up to $x_{n-1} = x_n \mod p^{n-1}$.
- For each n, if one knows x_n then there are p choices for x_{n+1}.
- One can add, subtract and multiply p-adic numbers:

$$x \pm y = (x_1 \pm y_1, x_2 \pm y_2, \ldots)$$
$$x \cdot y = (x_1 \cdot y_1, x_2 \cdot y_2, \ldots)$$

- p-adic integers contain the usual integers:

$$\mathbb{Z} \subset \mathbb{Z}_p$$
$$m \in \mathbb{Z} \mapsto x = (x_1, x_2, \ldots) \text{ with } x_n = m \mod p^n$$

- An equivalent way to write a p-adic number $x = (x_1, x_2, \ldots) \in \mathbb{Z}_p$ is its <u>p-adic expansion</u>
$$x = z_0 + z_1 p + z_2 p^2 + z_3 p^3 + \ldots$$
where $z_0, z_1, z_2, \ldots \in \{0, \ldots, p-1\}$ and $x_n = z_0 + z_1 p + \ldots + z_{n-1} p^{n-1}$. Note that a p-adic integer whose expansion is finite is a non-negative integer.

$\triangleright$ *Write the p-adic expansion of* -1.

$\triangleright$ *Give an example of a p-adic integer which is not an integer, that is* $x \in \mathbb{Z}_p \setminus \mathbb{Z}$.

$\triangleright$ *Show that* <u>*p-integral fractions*</u>
$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \;\middle|\; p \nmid n \right\} \subset \mathbb{Q}$$
are contained in $\mathbb{Z}_p$.

$\triangleright$ *Give an example of a p-adic integer which is not a p-integral fraction, that is* $x \in \mathbb{Z}_p \setminus \mathbb{Z}_{(p)}$.
Hint: look at the next section.

1.2. **Hensel's lemma:** Let $P(x) = a_m x^m + a_{m-1} x^{m-1} + \ldots + a_1 x + a_0$ be a polynomial with $a_m, \ldots, a_0 \in \mathbb{Z}$ (or even $\mathbb{Z}_p$). Suppose that $z_0 \in \mathbb{Z}/p\mathbb{Z}$ is such that $P(z_0) \equiv 0 \mod p$ but $P'(z_0) \not\equiv 0 \mod p$. Then there is a unique $x \in \mathbb{Z}_p$ such that $P(x) = 0$ and $x \equiv z_0 \mod p$.

This is a tool to construct more interesting p-adic numbers!

$$(p = 7) \qquad \sqrt{2} = 3 + 1 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + 2 \cdot 7^5 + \ldots$$
$$\text{or } 4 + 5 \cdot 7 + 4 \cdot 7^2 + 0 \cdot 7^3 + 5 \cdot 7^4 + 4 \cdot 7^5 + \ldots$$

$\triangleright$ *Explain why there are no* $\sqrt{2}$ *in* $\mathbb{Z}_3, \mathbb{Z}_5$. *Is there* $\sqrt{2}$ *in* $\mathbb{Z}_2$*?*

The next p for which $\sqrt{2} \in \mathbb{Z}_p$ are $p = 17$ and $p = 23$, e.g.

$$(p = 23) \qquad \sqrt{2} = 5 + 16 \cdot 23 + 22 \cdot 23^2 + 8 \cdot 23^3 + \ldots$$
$$\text{or } 18 + 6 \cdot 23 + 0 \cdot 23^2 + 14 \cdot 23^3 + \ldots$$

$\triangleright$ *Show that* $\mathbb{Z}_p$ *contains* $p-1$ *different numbers* x *such that* $x^{p-1} = 1$.

$$\begin{aligned} (p=5) \qquad & 1 \\ & 2+1\cdot 5+2\cdot 5^2+5^3+\dots \\ & 3+3\cdot 5+2\cdot 5^2+3\cdot 5^3+\dots \\ -1 =& 4+4\cdot 5+4\cdot 5^2+4\cdot 5^3+\dots \end{aligned}$$

If you solved the last exercise, you should know that for every $z_0 \in \mathbb{Z}/p\mathbb{Z}$, $z_0 \neq 0$ there is a solution to $x^{p-1} = 1$ such that $x \equiv z_0 \mod p$. These p-adic numbers are called Teichmüller units. They are $(p-1)$st roots of unity, similarly to the complex numbers $e^{\frac{2\pi i}{p-1}}, e^{\frac{4\pi i}{p-1}}, \dots, e^{\frac{2(p-1)\pi i}{p-1}} = 1 \in \mathbb{C}$.

★ *Are there other roots of unity in $\mathbb{Z}_p$? Prove that if $x \in \mathbb{Z}_p$ satisfies $x^m = 1$ for some $m \geq 1$ then x is one of the the Teichmüller units, that is, it satisfies $x^{p-1} = 1$.*

1.3. **p-adic numbers and division.** A number $x \in \mathbb{Z}_p$ is called a p-adic unit if there is $y \in \mathbb{Z}_p$ such that $x \cdot y = 1$. The set of p-adic units is denoted $\mathbb{Z}_p^\times$.

▷ *Show that $2 \in \mathbb{Z}_p^\times$ for $p \neq 2$.*

▷ *Prove that $x \in \mathbb{Z}_p^\times$ if and only if $x \not\equiv 0 \mod p$.*

We conclude that $\mathbb{Z}_p = \mathbb{Z}_p^\times \cup p\mathbb{Z}_p$. Every non-zero p-adic integer $x \in \mathbb{Z}_p$, $x \neq 0$ can be uniquely written as $x = p^k \cdot y$ with $y \in \mathbb{Z}_p^\times$ and $k \geq 0$:

$$\begin{aligned} &\mathbb{Z}_p = \{0\} \cup \mathbb{Z}_p^\times \cup p\mathbb{Z}_p^\times \cup p^2\mathbb{Z}_p^\times \cup \dots \\ &\mathbb{Z}_p \setminus \{0\} = \bigcup_{k\geq 0} p^k \mathbb{Z}_p^\times \end{aligned}$$

The minimal set that contains p-adic integers and the fraction $\frac{1}{p}$, and such that we can add and multiply within this set, is called p-adic numbers:

$$\begin{aligned} &\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right] = \mathbb{Z}_p \cup p^{-1}\mathbb{Z}_p^\times \cup p^{-2}\mathbb{Z}_p^\times \cup \dots \\ &\mathbb{Q}_p \setminus \{0\} = \bigcup_{k\in\mathbb{Z}} p^k \mathbb{Z}_p^\times \end{aligned}$$

Now p-adic expansions may contain negative powers of p:

$$\begin{aligned} (p=5) \qquad \frac{1}{50} = 5^{-2}\cdot\frac{1}{2} &= 5^{-2}\cdot(3+2\cdot 5+2\cdot 5^2+2\cdot 5^3+\dots) \\ &= 3\cdot 5^{-2}+2\cdot 5^{-1}+2+2\cdot 5+2\cdot 5^2+2\cdot 5^3\dots \end{aligned}$$

Observe that if $x \in \mathbb{Q}_p$, $x \neq 0$ we have $\frac{1}{x} \in \mathbb{Q}_p$. This property is the same as for the usual rational numbers: if $x \in \mathbb{Q}$, $x \neq 0$ we have $\frac{1}{x} \in \mathbb{Q}$.

▷ *Observe that $\mathbb{Q} \subset \mathbb{Q}_p$.*

2. p-adic distance and continuous functions

Warm-up:
we are back in the usual world of real numbers.
▷ *Compute* $\lim_{n\to\infty} \frac{3n+5}{9-7n} =$

★ *Compute* $\lim_{n\to\infty} \frac{f_{n+1}}{f_n} =$
where $\{f_n\} = \{1, 1, 2, 3, 5, 8, \ldots\}$ *is the sequence of Fibonacci numbers (it is generated by the rule* $f_n = f_{n-1} + f_{n-2}$*).*

The notation

$$\lim_{n\to\infty} a_n = \alpha \quad \text{or} \quad a_n \to \alpha \text{ as } n \to \infty$$

(in words: the limit of the sequence $\{a_n\}$ is equal to α, or a_n converge to α as n grows) means that the distance $|\alpha - a_n|$ tends to 0 as n increases. Here is the formal definition: for every $\varepsilon > 0$ there exists N such that $|a_n - \alpha| < \varepsilon$ for all $n \geq N$.
▷ *Give an example of a sequence which does not converge to any number.*

A sequence $\{a_n\}$ is called convergent if there exists an α such that $a_n \to \alpha$ as $n \to \infty$. One can detect convergence (without knowing the limit value α) as follows: for every $\varepsilon > 0$ there exists N such that $|a_n - a_m| < \varepsilon$ for all $n, m \geq N$.

With this definition in hand, one can view real numbers $\mathbb{R}$ as the set of possible limits of convergent sequences of rational numbers. This procedure is called completion: $\mathbb{R}$ is the completion of $\mathbb{Q}$.

2.1. p-adic distance.

For $x \in \mathbb{Z}$, $x \neq 0$ we denote

$$\mathrm{ord}_p(x) = \text{ integer } m \text{ such that } p^m | x \text{ but } p^{m+1} \not| x$$

(we say: p-adic order of x). This the exact power of p that divides x.
▷ *Compute* $\mathrm{ord}_3(54)$*,* $\mathrm{ord}_3(-45)$*,* $\mathrm{ord}_5(12)$*.*

The p-adic absolute value is defined as follows. Fix any real number $0 < \nu < 1$ and define

$$|x|_p = \begin{cases} \nu^{\mathrm{ord}_p(x)}, & \text{if } x \neq 0, \\ 0, & \text{if } x = 0. \end{cases}$$

(The standard choice in textbooks would be $\nu = p^{-1}$, but in fact it dos not matter.) Let us try to think of this number as the distance between x and 0! Note that since $\nu < 0$, the bigger $\mathrm{ord}_p(x)$ is the smaller is $|x|_p$. So we now think of an integer as being small when it is divisible by a big power of p.

Though $|x|_p$ seems weird, it satisfies the following properties of the usual absolute value for real (and complex) numbers:

$$\begin{aligned} |x \cdot y|_p &= |x|_p \cdot |y|_p \\ |x|_p &= 0 \Leftrightarrow x = 0 \\ |x + y|_p &\leq |x|_p + |y_p| \quad \text{(triangle inequality)} \end{aligned}$$

The triangle inequality becomes even sharper:

$\triangleright$ *Show that* $|x + y|_p \leq \max(|x|_p, |y|_p)$.

$\triangleright$ *Show that* $|x + y|_p = \max(|x|_p, |y|_p)$ *if* $|x|_p \neq |y|_p$.

If $|x|_p$ is (our new) distance between 0 and x, then one should also think of $|x - y|_p$ as the distance between integers $x, y \in \mathbb{Z}$. So, now x and y are close to each other when their difference is divisible by a large power of p.

2.2. **Limits.** Now we should rethink the idea of limits. The definitions are just as in the warm-up, but with $|\cdot|_p$ in place of $|\cdot|$:

$\triangleright$ *Compute* $\lim_{n\to\infty}(p^n - 1) =$

$\triangleright$ *Compute* $\lim_{n\to\infty}(1 + p + \ldots + p^n) =$

A sequence of integer numpbers $\{a_n\}$ is convergent p-adically (or in p-adic distance) if for every real $\varepsilon > 0$ there is an index N such that $|a_n - a_m|_p < \varepsilon$ for all $m, n \geq N$. Now, the limits are naturally p-adic integers: $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to the p-adic absolute value. To explain this rigorously, let us do two exercises:

$\triangleright$ *Define* $\mathrm{ord}_p(x)$ *for* $x \in \mathbb{Z}_p$, $x \neq 0$ *(so that it takes the same values on* $x \in \mathbb{Z} \subset \mathbb{Z}_p$*).*

One can extend the absolute value: $|x|_p = \nu^{\mathrm{ord}_p(x)}$ if $x \in \mathbb{Z}_p, x \neq 0$.

$\triangleright$ *Let* $\{a_n\}$ *be a* p*-adically convergent sequence of integer numbers. Construct* $\alpha \in \mathbb{Z}_p$ *such that* $|\alpha - a_n|_p \to 0$ *as* $n \to \infty$.

Now we are done. One interesting computational exercise at the end:

$\triangleright$ *Take some integer* $a \in \mathbb{Z}$*. Show that the sequence* $a_n = a^{p^n}$ *is* p*-adically convergent and compute its limit.*

Remark. The notion of p-adic order $\mathrm{ord}_p(x)$ can be defined for $x \in \mathbb{Q}$ and $x \in \mathbb{Q}_p$. Namely, for a fraction $\frac{n}{m} \in \mathbb{Q}$ one has $\mathrm{ord}_p(\frac{n}{m}) = \mathrm{ord}_p(n) - \mathrm{ord}_p(m)$. If $x \in \mathbb{Q}_p$, $x \neq 0$ one can uniquely write this number as $x = p^k y$ with $k \in \mathbb{Z}$ and $y \in \mathbb{Z}_p^\times$. We then put $\mathrm{ord}_p(x) = k$. ▷ *As an exercise, you could check that on $\mathbb{Q} \subset \mathbb{Q}_p$ this agrees with the definition for fractions given in the previous sentence.* Since we have $\mathrm{ord}_p(\cdot)$, we have the p-adic absolute value $|\cdot|_p$ on $\mathbb{Q}_p$. ▷ *Another exercise: show that for $x \in \mathbb{Q}_p$ the statements $|x|_p \leq 1$ and $x \in \mathbb{Z}_p$ are equivalent; also, $|x|_p = 1$ if and only if $x \in \mathbb{Z}_p^\times$.* Finally, let us say that $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, just as $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the usual absolute value $|\cdot|$.

2.3. **Continuous functions.** A function $f : \mathbb{R} \to \mathbb{R}$ is called continuous if for every convergent sequence of arguments $x_n \to x$ the values of the function also converge: $f(x_n) \to f(x)$.

Equivalently, one can say that if the two arguments x, y are close, then the values $f(x), f(y)$ are close.

Most functions that you know (polynomials, e^x, $\sin(x)$, ...) are continuous.

▷ *Give an example of a function, which is not continuous.*

Of course, the same definition can be given for $f : \mathbb{Z}_p \to \mathbb{Z}_p$ or $f : \mathbb{Q}_p \to \mathbb{Q}_p$. But what is it useful for, if we can't even draw their graphs?

Let us call a function $f : \mathbb{N} \to \mathbb{Z}$ or $f : \mathbb{Z} \to \mathbb{Z}$ continuous p-adically if for every integer $M > 0$ there exists an integer $N > 0$ such that $p^N | (x - y)$ implies $p^M | (f(x) - f(y))$.

▷ *Show that the sum of continuous functions is continuous.*

▷ *Show that polynomials are continuous.*

★ *Let $a \in \mathbb{N}$. Prove that $f(n) = a^n$ is p-adically continuous if and only if $a \equiv 1 \mod p$.*

Here is a curious fact about such functions. Suppose you have a p-adically continuous $f : \mathbb{N} \to \mathbb{Z}$. This is just a sequence of integers $\{f(n)\}$, but due to continuity our function can be evaluated at any $x \in \mathbb{Z}_p$. To see this,

▷ *Observe that any $x \in \mathbb{Z}_p$ is a p-adic limit of a sequence of natural numbers.*

In particular, there are well defined values $f(-1), f(-2), \ldots$ at negative integers and values $f(m/n)$ at rational numbers without p in the denominator (remember, $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$). Well, this perspective does not sound exciting for polynomial functions. But what if $f(n) = n!$ was p-adically continuous? This is not quite true, but in the next section we will make a modification of the factorial which works.

2.4. **p-adic factorial.** The following exercise might be difficult, it requires a few steps:
★ *Prove that function $f : \mathbb{N} \to \mathbb{Z}$ given by*

$$f(n) = (-1)^{n+1} \prod_{1 \le m \le n, p \nmid m} m = (-1)^{n+1} \frac{n!}{\lfloor \frac{n}{p} \rfloor! \, p^{\lfloor \frac{n}{p} \rfloor}}$$

is p-adically continuous. More precisely, $p^N | (n-k)$ implies $p^N | (f(n) - f(k))$.

A proof can be found in books on p-adic analysis such as "p-adic numbers, p-adic analysis and zeta functions" by Neal Koblitz (this is a truly great book!) or in my notes. We shall discuss it in class if there is time left.

One should think of $f(n)$ as the p-adic analogue of $n!$
▷ *Let $p = 3$. Compute $f(2)$, $f(3)$, $f(10)$.*

▷ *Observe that $f(n)$ is not divisible by p.*

Due to the last observation, we obtain a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p^\times$. We make a shift in the argument and define the <u>p-adic gamma function</u> as

$$\Gamma_p(x) = f(x-1).$$

This is again a continuous function $\Gamma_p : \mathbb{Z}_p \to \mathbb{Z}_p^\times$ satisfying

$$\mathrm{ord}_p(\Gamma_p(x) - \Gamma_p(y)) \ge \mathrm{ord}_p(x-y)$$

and

$$\Gamma_p(n) = f(n-1) = (1)^n \prod_{1 \le m < n, \; p \nmid m} m \quad \text{for all } n \in \mathbb{N}.$$

(The shift in the argument is just a convention. It is motivated by the analogy with the classical gamma function, see the remark below.)

Here are a few useful properties of the p-adic gamma function:

- For any $x \in \mathbb{Z}_p$ one has
$$\frac{\Gamma_p(x+1)}{\Gamma_p(x)} = \begin{cases} -x, & x \in \mathbb{Z}_p^\times, \\ -1, & x \in p\mathbb{Z}_p. \end{cases}$$
- If $x \in \mathbb{Z}_p$, write $x = x_0 + px_1$ where $x_0 \in \{1, 2, \dots, p\}$ is the first digit in the expansion of x unless $x \in p\mathbb{Z}_p$, in which case $x_0 = p$ rather than 0. Then
$$\Gamma_p(s)\Gamma_p(1-s) = (-1)^{s_0}.$$
- Let $m \in \mathbb{N}$ is not divisible by p. Then
$$\frac{\Gamma_p(\frac{x}{m})\Gamma_p(\frac{x+1}{m}) \dots \Gamma_p(\frac{x+m-1}{m})}{\Gamma_p(x)\Gamma_p(\frac{1}{m}) \dots \Gamma_p(\frac{m-1}{m})} = m^{1-x_0} \cdot (m^{-(p-1)})^{x_1}$$
with x_0 and x_1 defined for $x \in \mathbb{Z}_p$ in the previous property.

$\triangleright$ *Explain why the right-hand side in the last property is written in this weird way.* (Recall our exercise on p-adic continuity of $n \mapsto a^n$.)

$\triangleright$ *Compute* $\Gamma_p(0)$, $\Gamma_p(-1)$, $\Gamma_p(\frac{1}{2})$.

Remark. Let us go back to the world of real numbers. The classical gamma function is a function $\Gamma : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ defined by the integral

$$\Gamma(x) = \int_0^\infty t^{x-1}e^{-t}dt.$$

Let us list some of its properties:

- *Show that* $\Gamma(x+1) = x\Gamma(x)$. *Conclude that* $\Gamma(n) = (n-1)!$ *for* $n \in \mathbb{N}$.

- For $0 < x < 1$ one has $\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin(\pi x)}$.
- For $m \in \mathbb{N}$ we have

$$\frac{\Gamma(\frac{x}{m})\Gamma(\frac{x+1}{m})\dots\Gamma(\frac{x+m-1}{m})}{\Gamma(x)} = (2\pi)^{\frac{m-1}{2}} m^{\frac{1}{2}-x}.$$

Proofs can be found in Wikipedia. Now you can see this as a motivation for proving similar properties for p-adic gamma functions. As another exercise, you could

$\triangleright$ *rewrite the last property with the left-hand side being the same as in the p-adic case, that is*

$$\frac{\Gamma(\frac{x}{m})\Gamma(\frac{x+1}{m})\dots\Gamma(\frac{x+m-1}{m})}{\Gamma(x)\Gamma(\frac{1}{m})\dots\Gamma(\frac{m-1}{m})} =$$

Finally, compute

$$\Gamma\left(\frac{1}{2}\right) =$$