

February 1, 2005

INTRODUCTION TO p -ADIC NUMBERS

JASON PRESZLER

1. p -ADIC EXPANSIONS

The study of p -adic numbers originated in the work of Kummer, but Hensel was the first to truly begin developing the theory in approximately 1900. Hensel wanted an object analogous to $\mathbb{C}(x)$, the field of rational functions over the complex numbers, so we begin by constructing this field.

A common practice in commutative algebra (and other fields of pure mathematics) is to start with a field, such as \mathbb{C} , and consider the polynomial ring over the field, such as $\mathbb{C}[x]$. This ring consists of all polynomials in one variable and coefficients in the base field. An important fact from algebra is that this polynomial ring in one variable is a unique factorization domain (UFD). Frequently when studying rings, we want to also consider the field of fractions, obtained by adjoining to the ring the multiplicative inverse of every non-zero element in the ring. This process turns $\mathbb{C}[x]$ into $\mathbb{C}(x)$.

If we fix a prime element of $\mathbb{C}[x]$, such as $(x - b)$, then we can consider the Laurent expansion of $f(x) \in \mathbb{C}(x)$ about the prime $(x - b)$. For example, $f(x) = \frac{g(x)}{h(x)}$ and both g and h have Taylor expansions about any prime, in particular $(x - b)$, by then dividing the Taylor series we obtain a Laurent series $f(x) = \sum_{k \geq n_0} c_k(x - b)^k$. Working with a specific function $f(x) = \frac{x}{x-1}$ and the prime $(x - 2)$ we see that $f(x) = \frac{2+(x-2)}{1+(x-2)} = 2 - (x - 2) + (x - 2)^2 - \dots$. This gives us an inclusion of fields

$$i_b : \mathbb{C}(x) \hookrightarrow \mathbb{C}((x - b))$$

for any prime $x - b$ of $\mathbb{C}[x]$.

Since the favorite UFD of most number theorists is \mathbb{Z} we will perform similar operations as above and see what we end up with. First, the fraction field of \mathbb{Z} is \mathbb{Q} and for any prime $p \in \mathbb{Z}$ we can write any $a \in \mathbb{Q}$ as $a = p^{n_0} \frac{u}{v}$, where we have reduced a to lowest terms and then extracted all of the p 's, thus n_0 can be a negative number. As above, we can write a “Taylor” expansion for both the numerator and denominator of a in terms of p and then divide, giving us a “Laurent” series of a in terms of p . This will be referred to as a p -adic

expansion of a . For example, if $a = \frac{24}{17}$ we can consider the 3-adic expansion of a . This gives us

$$a = \frac{24}{17} = \frac{2p + 2p^2}{2 + 2p + p^2} = p + p^3 + 2p^5 + \dots$$

We have not substituted $p = 3$ into anything to avoid the temptation to simply do the arithmetic and get a final answer. We must think of the p -adic expansions as Laurent series in p rather than evaluating a Laurent series. If we take every $a \in \mathbb{Q}$ and compute the p -adic expansion of a , we get a new field, \mathbb{Q}_p analogous to $\mathbb{C}((x-b))$ and we have a similar inclusion

$$i_p : \mathbb{Q} \hookrightarrow \mathbb{Q}_p.$$

This new field \mathbb{Q}_p will be called the field of p -adic numbers and each element is a p -adic expansion. We can also think of a distance on \mathbb{Q}_p analogous to the distance on $\mathbb{C}((x-b))$, which is to consider the order of a zero or pole of a function. In other words, we can define a distance in \mathbb{Q}_p to measure how many times p divides either the numerator or denominator of a .

2. p -ADIC DISTANCE

Before we can really begin talking about distance we must talk about valuations on \mathbb{Q} . Valuations can then be used to define absolute values, which in turn gives rise to a metric.

Definition 2.1. *A valuation $v_p : k \rightarrow \mathbb{R} \cup \{\infty\}$ is a function from any field k to the extended real line such that*

- (i) $v_p(ab) = v_p(a) + v_p(b)$
- (ii) $v_p(a+b) \geq \min(v_p(a), v_p(b))$
- (iii) $v_p(0) = \infty$.

A clear consequence of the first property is that $v_p(a/b) = v_p(a) - v_p(b)$.

Definition 2.2. *An absolute value is a function $|\cdot|_p : k \rightarrow \mathbb{R}_+$ (where \mathbb{R}_+ is the positive reals) such that*

- (i) $|x|_p = 0$ iff $x = 0$
- (ii) $|xy|_p = |x|_p |y|_p$
- (iii) *and one of the following*
 - (a) $|x+y|_p \leq |x|_p + |y|_p$ or
 - (b) $|x+y|_p \leq \max(|x|_p, |y|_p)$.

If an absolute value satisfies the triangle inequality ((iii)(a)) then it is said to be Archimedean, and non-Archimedean if the stronger ultrametric inequality ((iii)(b)) is satisfied. By fixing a constant c , we can define an absolute value $|a| = c^{-v_p(a)}$. Thus, the p -adic valuation v_p is the number of p factors in a rational number a (after reducing to lowest terms), i.e. if $x = p^n \frac{u}{v} \in \mathbb{Q}$ and $p \nmid uv$ then $v_p(x) = n$. The p -adic absolute value is defined to be $|x|_p = p^{-v_p(x)}$, where we have chosen the constant to be p in order for future results to look slightly nicer. The appropriate notion of distance then becomes the absolute value of the difference (as usual, except the absolute value is different), $|x - y|_p$ is the p -adic distance between x and y .

The purpose of this paper is to describe the p -adic numbers, but so far we have only established what the p -adic metric is. Before we can ask why \mathbb{Q}_p is important, we must ask why these new metrics (one for each prime p) are important. This was first answered by Ostrowski in 1918, when he classified all absolute values on \mathbb{Q} up to equivalence. Two absolute values are equivalent if they induce the same topology (this amounts to changing the constant that we raise to the valuation).

Theorem 2.3. (*Ostrowski, 1918*) *Let $|\cdot|$ be an absolute value on \mathbb{Q} , then $|\cdot|$ is equivalent to one of the following:*

- (i) *the trivial absolute value, which sends $|0| = 0$ and $|x| = 1 \forall x \neq 0$,*
- (ii) *the usual Euclidean absolute value (denoted $|\cdot|_\infty$), or*
- (iii) *the p -adic absolute value $|\cdot|_p$ for some prime p .*

The following exercise, though similar in topic to Ostrowski's theorem, is much easier than the novice may initially think.

Exercise 2.4. *Classify all absolute values on a finite field.*

Another interesting result concerning the possible absolute values on \mathbb{Q} is the product formula, and it is this result that makes us want to use the constant p to define the absolute value $|\cdot|_p$.

Theorem 2.5. (*Product Formula*) *If $a \neq 0 \in \mathbb{Q}$ then*

$$\prod_{p \leq \infty} |a|_p = 1.$$

PROOF: The proof is very straightforward and the reader is encouraged to supply one. ■

There is a similar result in arbitrary number fields, but one may have more than one prime at infinity (which gives the usual absolute value on \mathbb{Q} , and is referred to as a prime at infinity primarily out of tradition and notational convenience). Also the product formula serves as a natural place to begin a discussion on adèles, but that would be a different paper (see [8] if interested).

3. COMPLETIONS

Once one has an absolute value they have a metric, and a natural thing to begin considering is convergence of sequences. When considering this, the notion of a Cauchy sequence occurs, these are the sequences that “should” converge. By making every Cauchy sequence converge, one has completed the field with respect to the given absolute value. After some preliminary definitions we will make this process of completion more precise, and show several ways to do it.

Definition 3.1. *A sequence $\{x_n\}$ in \mathbb{Q} is Cauchy with respect to $|\cdot|_p$ if $\forall \epsilon > 0 \exists N$ such that $|x_m - x_n|_p < \epsilon \forall m, n \geq N$.*

Cauchy sequences are sequences whose terms become arbitrarily close once you go far enough out. This idea should be closely related to convergence, and in real analysis one sees that this is exactly the notion of convergence, i.e. a sequence converges iff it is Cauchy.

Definition 3.2. *A completion of \mathbb{Q} with respect to $|\cdot|_p$ is a new field, denoted \mathbb{Q}_p such that every Cauchy sequence with respect to $|\cdot|_p$ converges.*

The new field \mathbb{Q}_p is the field of p -adic numbers and is the same as the field of p -adic expansions that we discussed earlier. Thus, elements in \mathbb{Q}_p can be thought of as either Laurent series in p or Cauchy sequences.

If $|\cdot|_p = |\cdot|_\infty$ then the completion of \mathbb{Q} is \mathbb{R} as one learns in real analysis. Also, if $|\cdot|_p$ is trivial then \mathbb{Q} is already complete (this is the main reason for calling this the trivial absolute value). We will now cover how to complete a field, leaving the details up to the reader but clearly informing them of the process. We will cover three methods of completion in this paper, the first two follow immediately but the third will be covered in the next section.

3.1. How To Complete: Analytically. To complete a field using analytic methods, we begin by letting \mathcal{C}_p be the set of all Cauchy sequences with respect to $|\cdot|_p$. If $\{x_n\}, \{y_n\} \in \mathcal{C}_p$

then we can define an equivalence relation

$$\{x_n\} \sim \{y_n\} \text{ iff } \forall \epsilon > 0, \exists N \text{ such that } n \geq N \implies |x_n - y_n|_p < \epsilon.$$

This makes two Cauchy sequences equivalent if they become arbitrarily close term-wise, having the effect of making two sequences equal if they converge to the same point.

We now define $\mathbb{Q}_p = \mathcal{C}_p / \sim$ where addition is defined $\overline{\{x_n\}} + \overline{\{y_n\}} = \overline{\{x_n\} + \{y_n\}}$ and similarly for multiplication. One must check that the sum of two equivalence classes of Cauchy sequences is again a Cauchy sequence, likewise with the product. Then one must check that these operations make \mathbb{Q}_p into a field.

Next we can identify $a \in \mathbb{Q}$ with the sequence $\{a\} \in \mathcal{C}_p$, thus obtaining the embedding $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ which allows us to consider \mathbb{Q} a dense subfield of \mathbb{Q}_p . Lastly we must extend $|\cdot|_p$ to \mathbb{Q}_p .

3.2. How To Complete: Slightly Algebraic. This method will rely less on the underlying notion of Cauchy sequence, instead using slightly more complicated algebraic techniques. In the next section we will learn an even more algebraic method.

We begin by defining \mathcal{C}_p as above, as well as the operations of addition and multiplication as above (except without equivalence classes), this makes \mathcal{C}_p into a commutative ring with identity. Next we define $N = \{\{x_n\} \in \mathcal{C}_p : x_n \rightarrow 0\}$. First we must verify that N is an ideal of \mathcal{C}_p and then we show that this ideal is maximal. Given a commutative ring and maximal ideal, a natural thing to do is consider the quotient $\mathcal{C}_p/N = \mathbb{Q}_p$ which is a field.

We can then embed $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ as above and we must extend $|\cdot|_p$ to \mathbb{Q}_p , which is the same as above. Thus the two techniques are very similar, just using objects and terminology of different areas of mathematics.

3.3. Some Facts. In Calculus II, we learn that a necessary condition for an infinite series in \mathbb{R} to converge is that the n^{th} term goes to zero as n goes to infinity. The fact that this is not also sufficient causes many problems in analysis, but in \mathbb{Q}_p things are simpler.

As a consequence of the metric being non-Archimedean ((iii)(b)), we have:

Theorem 3.3. *A series $\sum_{n=0}^{\infty} a_n$ in \mathbb{Q}_p converges if and only if $\lim_{n \rightarrow \infty} |a_n|_p = 0$.*

The limit is a limit in \mathbb{R} , so we know exactly how to deal with that. The proof follows directly from the result in \mathbb{R} and the ultrametric inequality that is characteristic of non-Archimedean metrics.

Thus, \mathbb{R} and \mathbb{Q}_p are structurally very similar, but \mathbb{Q}_p is much easier to do analysis in. From this point one could begin the study of \mathbb{Q}_p manifolds, which have a smooth structure but are quite different objects than those studied in differential topology.

4. INVERSE LIMITS

This is a very algebraic method, and is more technical than the above methods. First we must define an inverse system, but to simplify things slightly we will work with a specific example. The more advanced reader should consult a commutative algebra text (such as [4] or [1]), or a text on category theory. Inverse limits, or completions as commutative algebraists call them, can be used in much more generality to obtain very similar results (such as Hensel's Lemma).

Definition 4.1. *Let $A_n = \mathbb{Z}/p^n\mathbb{Z}$ for a fixed prime p and let $\phi_n : A_n \rightarrow A_{n-1}$ be the standard reduction map. We call (A_n, ϕ_n) an inverse system and define the inverse limit of this inverse system to be*

$$\mathbb{Z}_p = \varprojlim (A_n, \phi_n).$$

We call \mathbb{Z}_p the p -adic integers. As one should immediately question, we are not guaranteed that given an inverse system an inverse limit will exist, this gets into more complicated homological algebra. The interesting thing is that the p -adic integers are the ring of integers in \mathbb{Q}_p as defined above.

To define \mathbb{Q}_p in terms of inverse limits, we let \mathbb{Q}_p be the fraction field of \mathbb{Z}_p . The interesting result is that \mathbb{Q}_p as a fraction field is the same object as \mathbb{Q}_p when considered as equivalence classes of Cauchy sequences or as p -adic expansions.

5. LOCAL-GLOBAL RESULTS

Now that we have given a solid idea of what the p -adic numbers are, we will address the question of why they are important objects to study. To do this we note that a very common idea in mathematics is to consider objects "locally" and use this "local" information to obtain information about the entire object. This is a key idea in calculus, since limits and derivatives provide local information (i.e. information about a neighborhood of a point) then we want to see what this tells us about the function as a whole. This is extended beautifully into the study of smooth manifolds and Lie theory, which are locally copies of \mathbb{R}^n . Furthermore, Grothendick's revolution in algebraic geometry makes extensive use of

this local-global idea in schemes. A slightly less geometric use is the classification of finite groups, where local data is information about subgroups.

In our current situation, local information will be information from a “local field.”

Definition 5.1. *A local field is a field K with a non-trivial absolute value such that K is complete and locally compact.*

The following theorem classifies all local fields. We will remark now that \mathbb{R} and \mathbb{C} are peculiar local fields, usually not conforming to the pattern provided by finite extensions of \mathbb{Q}_p .

Theorem 5.2. *If K is a local field then K is isomorphic to one of the following:*

- (i) \mathbb{R} or \mathbb{C} if the absolute value is Archimedean,
- (ii) a finite extension of \mathbb{Q}_p if $\text{char}(K) = 0$ and the absolute value is non-Archimedean,
- (iii) $\mathbb{F}((t))$ if $\text{char}(K) = p > 0$ and the absolute value is non-Archimedean.

When working in a field, one needs to consider functions on that field and automorphisms of the field. The second case, looking at automorphisms, leads us into Galois theory of p -adic numbers which is of great importance in modern number theory but unfortunately far beyond the scope of the present treatise. To see some of the utility of p -adic numbers, we will consider only the first case, looking at p -adic polynomials.

When working with polynomials, the most natural and important questions concern the roots. As a practical means of finding roots there is an analogue of Newton’s method which works in $\mathbb{Z}_p[x_1, \dots, x_m]$. Also there is the important lemma of Hensel (the “creator” of p -adic numbers).

Theorem 5.3 (Analogue of Newton’s Method). *Let $f \in \mathbb{Z}_p[x_1, \dots, x_m]$ and $a \in \mathbb{Z}_p^m$, $n, k, j \in \mathbb{Z}$ such that $0 \leq j \leq m$. If $0 \leq 2k \leq n$ and*

$$f(a) \equiv 0 \pmod{p^n} \quad v_p \left(\frac{\partial f}{\partial x_j}(a) \right) = k,$$

then \exists a zero, y , of f in \mathbb{Z}_p^n such that $y \equiv a \pmod{p^{n-k}}$.

Lemma 5.4 (Hensel’s Lemma). *Let $f \in \mathbb{Z}_p[x]$ be monic. If $a_0 \in \mathbb{Z}$ is a simple root of*

$$f(x) \equiv 0 \pmod{p},$$

then $\exists y \in \mathbb{Z}_p$ such that $y \equiv a_0 \pmod{p}$ and $f(y) = 0$.

Hensel's lemma is an important component in the proof of the above theorem (essentially providing the initial case for induction), however we will focus on a more interesting consequence, namely that \mathbb{Z}_p contains the $(p-1)^{th}$ roots of unity after proving Hensel's lemma. Also, there are more general versions of Hensel's lemma, as one can find in any standard commutative algebra text that discusses completions and the I -adic topology.

PROOF: Our proof will be by induction. Suppose that $\exists a_n$ such that $f(a_n) \equiv 0 \pmod{p^n}$. We must show that a_n can be lifted uniquely to $a_{n+1} \pmod{p^{n+1}}$ such that $a_{n+1} \equiv a_n \pmod{p^n}$ and $f(a_{n+1}) \equiv 0 \pmod{p^{n+1}}$, then y will simply be the limit of this sequence of $\pmod{p^k}$ solutions.

Since f is a polynomial we can write it in the form $f(x) = \sum_i c_i x^i$. Also consider $tp^n + a_n$ as a possible lift of a_n . Then

$$(1) \quad \begin{aligned} f(tp^n + a_n) &= \sum_i c_i (tp^n + a_n)^i \\ &\equiv f(a_n) + p^n t f'(a_n) \pmod{p^{n+1}}. \end{aligned}$$

The equivalence above is a result of using Taylor series. We must now solve for t in

$$p^n t f'(a_n) + f(a_n) \equiv 0 \pmod{p^{n+1}}.$$

Thus $t f'(a_n) \equiv -(f(a_n)/p^n) \pmod{p}$. Since $f(a_n) \equiv 0 \pmod{p}$ (since $a_n \equiv a_0 \pmod{p}$) and $f'(a_n) \not\equiv 0 \pmod{p}$ (simple root), then t has a unique \pmod{p} solution. Thus $a_{n+1} = a_n + tp^n$ is a unique lift of $a_n \pmod{p}$.

Thus we can construct an infinite sequence of a_i such that $f(a_i) \equiv 0 \pmod{p^i}$, $f'(a_i) \not\equiv 0 \pmod{p^i}$ and $a_{i+1} \equiv a_i \pmod{p}$. This sequence is Cauchy, and therefore converges to a unique limit $y \in \mathbb{Z}_p$ that has the properties of each element in the sequence. ■

Corollary 5.5. *The ring \mathbb{Z}_p contains the $(p-1)^{th}$ roots of unity.*

PROOF: In order to prove this, we note that if $\exists \omega_j \in \mathbb{Z}_p$ such that $\omega_j^{p-1} = 1$ and $\omega_j \equiv j \pmod{p}$ for every $j = 1, 2, \dots, p-1$ then $\omega_j = \zeta_j$. Thus, we will show the existence of ω_j .

We will show the existence of ω_j by applying Hensel's lemma to $f(x) = x^{p-1} - 1$. Consider the congruence

$$f(x) = x^{p-1} - 1 \equiv 0 \pmod{p}.$$

By Fermat's little theorem, $j^{p-1} \equiv 1 \pmod{p} \forall j = 1, \dots, p-1$. Therefore, each j is a root of the above congruence, and by Hensel's lemma, $\exists \omega_j \in \mathbb{Z}_p$ such that $\omega_j \equiv j \pmod{p}$ and $f(\omega_j) = \omega_j^{p-1} - 1 = 0$ so $\omega_j^{p-1} = 1$. ■

Now is an appropriate time to mention the significance of p -adic numbers, manifested in the Hasse-Minkowski theorem.

Theorem 5.6 (Hasse-Minkowski). *Let $f(x, y) \in \mathbb{Q}[x, y]$ be a quadratic polynomial. Then $f(x, y) = 0$ has a solution in \mathbb{Q}^2 iff it has a solution in $\mathbb{Q}_p^2 \forall p \leq \infty$.*

This theorem provides a "local-global" principal that makes the p -adic numbers very useful in modern number theory. By Hensel's lemma, checking for solutions in \mathbb{Q}_p for finite primes is relatively easy and Newton's method allows an effective algorithm for $p = \infty$, i.e. \mathbb{R} . This theorem can be generalized to the Hasse principal. We must note that the above theorem is false for a cubic, but the idea is still very useful in many geometric settings.

6. THE MULTIPLICATIVE GROUP \mathbb{Q}_p^\times

In this section we will simply state the structure theorem for the group \mathbb{Q}_p^\times , as there is an interesting description, unlike in the case of \mathbb{R} .

Theorem 6.1.

$$\mathbb{Q}_p^\times \simeq \begin{cases} \mathbb{Z} \times \mathbb{Z}_p \times \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \neq 2, \\ \mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}/2\mathbb{Z} & \text{if } p = 2. \end{cases}$$

One can naturally inquire about the squares of \mathbb{Q}_p^\times and discover an analogue of the Legendre symbol. Or one can deviate into any of the numerous tangents mentioned above. For this paper however, this seems a decent place to end our discussion.

REFERENCES

1. David Eisenbud, *Commutative algebra with a view toward algebraic geometry*, first ed., Springer-Verlag, 1995.
2. Fernando Gouvea, *p -adic numbers*, second ed., Springer-Verlag, 1997.
3. Kazuya Kato, Nobushige Kurokawa, and Takeshi Saito, *Number theory 1: Fermat's dream*, first ed., American Mathematical Society, Providence, Rhode Island, USA, 1996.
4. Hideyuki Matsumura, *Commutative ring theory*, first ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, 1986.

5. Barry Mazur, *Passage from local to global in number theory*, Bulletin of the American Mathematical Society (1993).
6. Paulo Ribenboim, *Classical theory of algebraic numbers*, first ed., Springer-Verlag, New York, 2001.
7. Jean-Pierre Serre, *A course in arithmetic*, first ed., Graduate Texts in Mathematics, vol. 7, Springer-Verlag, 1973.
8. Tom Weston, *An idelic approach to number theory*, unpublished, available online.