p-adic Numbers

Christopher Davis

July 31, 2000

After exploring a variety of different areas in number theory, I ended up concentrating for the last two weeks on p-adic numbers. p-adic numbers show up in a variety of ways, from the study of certain Diophantine equations to modern physics. In this paper I will define p-adic numbers, explain some of their properties, and present the definition of the p-adic absolute value, which with more time could be used for the creation of $\mathbb{Q}_p$, the completion of the rational numbers with respect to the p-adic absolute value.

First of all, we define the p-adic expansion $f_p(x)$ of a rational number x to be the unique way of expressing x as the sum

$$\sum_{n \geq n_0} a_n p^n,$$

with $a_i \in \mathbb{Z}, 0 \leq a_i < p$. Before we can take this too seriously, we should be sure that all $x \in \mathbb{Q}$ have such an expansion.

Theorem *Every rational number x has a p-adic expansion as defined above.*

PROOF: First, note that if both x_1 and x_2 have a p-adic expansion, then $x_1 x_2$ will have a p-adic expansion. With this in mind, to show that a number $x = \frac{a}{b}$ has a p-adic expansion, all we need to show is that $x_1 = a$ and $x_2 = \frac{1}{b}$ have p-adic expansions.

The proof that a positive integer a has a p-adic expansion can be shown by induction. First of all, the numbers 0 and 1 have p-adic expansions for every prime, namely:

$$f_p(0) = 0 \, and \, f_p(1) = 1.$$

Next we assume that all natural numbers x, for $1 \leq x < a$, have a p-adic expansion. To prove that a also has a p-adic expansion, we rely on the fact that for any combination of a and p, there is a unique whole number λ such that

$$\lambda p \leq a < (\lambda + 1)p.$$

Let $a_0 = a - \lambda p$. By the inductive hypothesis, λ has a p-adic expression. Assuming we know the p-adic expansion of λ, we can explicitly find the p-adic expansion of a:

$$f_p(a) = a_0 + p f_p(\lambda).$$

The proof that a positive number $\frac{1}{b}$ has a p-adic expansion is a little more difficult. From the first part of this proof, we know that b has a p-adic expansion.

$$\frac{1}{b} = \frac{1}{f_p(b)} = \frac{1}{a_0 + a_1 p + a_2 p^2 + \cdots + a_n p^n + \cdots}.$$

We need some different way of expressing this fraction. To get this, recall that $\frac{1}{1-z} = \sum_{n=0}^{\infty} z^n$. If $a_0 \neq 0$, then a_0 has an inverse mod p. (An inverse mod p is fine, rather than a traditional inverse, because say $a_0 a_0^{-1} = mp+1$, then the 1 is all that will remain out front, while the m p's will be carried over to the a_1 term.) Therefore, multiplying the top and bottom of the fraction by a_0^{-1} will put it into a form from which we can quickly see that there will be a p-adic expansion. If $a_0 = 0$ we don't have to do much more, just multiply the top and bottom of the fraction by $p^{-1}a_1^{-1}$.

Finally, we observe that

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

That allows us to express negative numbers as their p-adic expansions. With that, we have shown that every rational number indeed has a p-adic expansion. ♣

At the moment we have

$$\mathbb{Q} \subset \mathbb{Q}_p,$$

and we do not know whether there are elements of $\mathbb{Q}_p$ which are not equivalent to elements of $\mathbb{Q}$. There are more things we can realize about $\mathbb{Q}_p$. First of all, $\mathbb{Q}_p$ is a field. Because it seems rather intuitive, the proof is omitted. For a proof, see [Vladimirov 94]. Also, in order for infinitely long p-adic numbers to converge, we must deal with p-adic numbers in a context in which p^n will get smaller as n gets larger.

This next section will be devoted to showing that $\mathbb{Q}_p$ is strictly bigger than $\mathbb{Q}$. To do this, we introduce a new method for obtaining the p-adic expansion of rational numbers, and show that this method can be used for numbers which are *not* rational.

Say, for instance, that we want to find the 5-adic expansion for $x = -7$. We can find this by considering the congruences:

$$x^2 = 49 \mod 5^n$$

for every $n \geq 1$. Now, for the first congruence,

$$x^2 = 49 \mod 5^1,$$

we have, as could have been expected, two different solutions: $x = 2$ and $x = 3$. Because $7 = 2 \mod 5$, we can guess that it is going to be the beginning of the 5-adic expansion of 7. Solving

$$x^2 = 49 \mod 5^2$$

gives us $x = 7$ and $x = 18$. The 5-adic expansion of 7 is already done, because as n gets larger, $x = 7$ will remain a solution. Remembering the $x = 2$ from the first solution, we can get the 5-adic expansion of 7:

$$7 = 2 + 1{\times}5.$$

The 5-adic expansion of -7, which is what we were after in the first place, will be more interesting. Continuing in the same way as before we will get:

$$-7 = 3 + 3{\times}5 + 4{\times}5^2 + 4{\times}5^3 + \cdots.$$

To analyze our results further, we will use the following definition:

Definition: *Let p be a prime. We say a sequence of integers α_n such that $0 \leq \alpha_n \leq p^n - 1$ is coherent if, for every $n \geq 1$, we have*

$$\alpha_{n+1} = \alpha_n \mod p^n.$$

Note that a sequence which will give us a p-adic expansion must be coherent (simply because of what a p-adic expansion is). As examples, both of our sequences above were coherent. Now we try to obtain a (coherent) p-adic expansion for a number which is not rational. Let's try to determine a 7-adic expansion of the square root of 2. We begin with the equation

$$x^2 = 2 \mod 7.$$

3 provides us with a solution to this (and we will ignore the second solution). Now, for the sequence to be coherent, the next solution must be of the form $x = 3 + 7k$.

$$\begin{aligned} (3+7k)^2 &= 2 \mod 7^2 \\ 9 + 42k + 49k^2 &= 2 \mod 49 \\ 7 + 42k &= 0 \mod 49 \\ k &= 1. \end{aligned}$$

That means that the second number in our (coherent) sequence is 10. The third number, if it exists, will have to be of the form $x = 10+49k$, but rather than grinding out solutions, we will settle for proving that the sequence can be continued indefinitely.

Theorem: *If one has a solution of the form*

$$x^2 = b \mod p,$$

with $p > 2$, then the solutions obtained when raising p to higher powers exist, and will form a coherent sequence.

PROOF: The proof will be by induction. The hypothesis of the theorem takes care of the first part of the induction. Now assume we have $x_n^2 = b \mod p^n$, so $x_n^2 = b + k_1 p^n$ for some k_1. We want to know if there exists a k_2 such that

$$(x_n + k_2 p^n)^2 = b \mod p^{n+1}.$$

Expanding and replacing x_n^2 with $b + k_1 p^n$ we get

$$b + k_1 p^n + 2x_n k_2 p^n + k_2 p^{2n} = b \mod p^{n+1}.$$

Cancelling out the b's and the term divisible by p^{n+1} we get

$$k_1 p^n + 2x_n k_2 p^n = 0 \mod p^{n+1}.$$

Now, dividing by p^n we get

$$k_1 + 2x_n k_2 = 0 \mod p.$$

We will now show that no matter what k_1 is, we can choose k_2 so that the equality is true. Assume $k_1 = 2m$ (i.e., is even). Then let $k_2 = (p - m)x_n^{-1} \mod p$. Assume $k_1 = 2m + 1$, then let $k_2 = \frac{p-k}{2} x_n^{-1}$. Of course, x_n^{-1}

will exist because p is a prime. Therefore we will be able to carry on the sequence infinitely. ♣

Even with just our one solution of $x^2 = 2$ (the 7-adic solution), we have shown that there is at least one element in $\mathbb{Q}_p$ which is not in $\mathbb{Q}$, and therefore $\mathbb{Q}_p$ is strictly bigger than $\mathbb{Q}$.

In what will at first seem to take us in a new direction, we define the p-adic valuation v_p on the rational numbers.

Definition *The p-adic valuation of a non-zero integer n is the unique number $v_p(n)$ such that*

$$n = p^{v_p(n)} n' \text{ with } p \nmid n'.$$

We extend this definition to a rational number $x = \frac{a}{b}$ by saying

$$v_p(x) = v_p(a) - v_p(b).$$

Finally, we define $v_p(0) = +\infty$.

Now we define the p-adic absolute value.

Definition *For any $x \in \mathbb{Q}$ not equal to 0, we define the p-adic absolute value of x to be*

$$| \ x \ |_p = p^{-v_p(x)},$$

and if $x = 0$, we set $| \ x \ |_p = 0$.

We refer to that as an absolute value, but to ensure that it is an absolute value we must verify the following three properties (which, if true, will show that this absolute value is a non-archimedian absolute value.)

1. $| \ x| = 0$ if and only if $x = 0$.
2. $|xy| = |x \ || \ y \ |$ for all $x, y \in \mathbb{Q}$.
3. $|x + y| \leq \max\{| \ x \ |, | \ y \ |\}$.

To show this is true, we will rely on the following Lemma:

Lemma *For all x and $y \in \mathbb{Q}$, we have*

1. $v_p(xy) = v_p(x) + v_p(y)$
2. $v_p(x + y) \geq \min\{v_p(x), v_p(y)\}$.

PROOF: We begin by assuming that both x and y are integers. Let $x = p^a x'$ and $y = p^b y'$, with both x' and y' not divisible by p. Now

$$xy = p^{a+b} x' y',$$

and therefore $v_p(xy) = v_p(x) + v_p(y)$. To prove the second part of the Lemma, we assume that $a \leq b$. (We can always reverse the roles of x and y if we need to.) With this in mind,

$$x + y = p^a (x' + p^{b-a} y').$$

Therefore, $v_p(x+y) = a = \max\{v_p(x), v_p(y)\}$. Now we must make sure this is also true when x is not an integer but a rational number. Assume $x = \frac{a}{b}$ and $y = \frac{c}{d}$, then:

$$v_p(xy) = v_p(\frac{ac}{bd}) = v_p(a) + v_p(c) - v_p(b) - v_p(d) = v_p(\frac{a}{c}) + v_p(\frac{b}{d}).$$

And,

$$v_p(\frac{a}{b} + \frac{c}{d}) = v_p(\frac{ad+bc}{bd}) \geq \min\{v_p(ad), v_p(bc)\} - v_p(bd).$$

Now, assume that the $min\{v_p(ad), v_p(bc)\} = v_p(ad)$. Then,

$$v_p(\frac{a}{b} + \frac{c}{d}) \geq v_p(ad) - v_p(bd) = v_p(\frac{a}{b}).$$

This concludes the proof of the Lemma. ♣

We are now ready to show that the p-adic absolute value as we defined it is, in fact, an absolute value and, more specifically, is a non-archimedian absolute value.

Theorem: *Our definition* $| \ x \ |_p$ *above defines a non-archimedian absolute value on* $\mathbb{Q}$.

PROOF:

1. For the first property, note that the absolute value cannot equal zero for any finite $v_p(x)$. Therefore $|x|_p = 0$ if and only if $x = 0$.

2. We can prove the second property simply by using the Lemma and manipulating the definitions.

$$|xy|_p = p^{-v_p(xy)} = p^{-v_p(x)-v_p(y)} = |x|_p |y|_p.$$

3. Once again, we can prove this property directly from the Lemma.

$$|x+y| = p^{v_p(x+y)} \leq p^{-\min\{v_p(x),v_p(y)\}} = \max\{p^{-v_p(x)}, p^{-v_p(y)}\} = \max\{|x|, |y|\}.$$

This concluces the proof. ♣

With more time it could be shown that the p-adic numbers dealt with in the first half of the paper are a completion of $\mathbb{Q}$ with respect to the p-adic absolute value dealt with in the second half of the paper.

Acknowledgements: I would like to thank Harvey Keynes for telling me about this program, the University of Minnesota for paying me to attend lectures and read math texts, and most of all Professor Paul Garrett for giving me the opportunity to work here this summer and for his daily lectures and assistance.

Created using LaTeX.

References

[Gouvêa 93] Fernando Q. Gouvêa, *p-adic Numbers*, [Berlin Heidelberg, Springer-Verlag, 1993]

[Vladimirov 94] V.S. Vladimirov, I. V. Volovich, E.I. Zelenov, *p-adic Analysis and Mathematical Physics*, [Singapore, World Scientific Publishing Co., 1994]