2020

An In-depth Look at p-adic Numbers

Xiaona Zhou
CUNY New York City College of Technology

An In-depth Look at p-adic Numbers

Xiaona Zhou
Mentor: Professor Satyanand Singh
Department of Mathematics, New York City College of Technology

Abstract

In this study, we consider p-adic numbers. We will also study the p-adic norm representation of real number, which is defined as $\mathbb{Q}_p = \{\sum_{j=m}^{\infty} a_j p^j : a_j \in \mathbb{D}_p, m \in \mathbb{Z}, a_m \neq 0\} \cup \{0\}$, where p is a prime number. We explore properties of the p-adics by using examples. In particular, we will show that $\sqrt{6}, i \in \mathbb{Q}_5$ and $\sqrt{2} \in \mathbb{Q}_7$. p-adic numbers have a wide range of applicationsnin fields such as string theory, quantum mechanics, and transportation in porous disordered media in geology.

Theorems and propositions

Theorem 1 (The p-adic norm)**.** *Given a filed A and a function $f\colon A \to \mathbb{R}$ we say that f is a norm if*

- $f(a) > 0$ *for all* $a \neq 0$ *and* $f(0) = 0$ *(positive-definiteness)*
- *for all* $a, b \in A,\ f(a \cdot b) = f(a) \cdot f(b)$ *(multiplicativity)*
- *for all* $a, b \in A,\ f(a+b) \leq f(a) + f(b)$ *(triangle inequality)*

Theorem 2 (p-adic absolute value)**.** *The p-adic absolute value $|\cdot|\colon \mathbb{Q} \to \mathbb{R}$ is defined as following:*

$$\begin{cases} |\,0\,|_p = 0 \\ |\,q\,|_p = |\,\frac{a}{b}\,|_p = 1; \ \textit{if } (ab,p) = 1 \textit{ and } (a,b) = 1, \textit{where } a \in \mathbb{Z}, b \in \mathbb{N} \\ |\,q\,|_p = |\,\frac{a}{b}\,|_p = p^{-n}; \ \textit{if } p^n \textit{ is the highest power of } p \textit{ that divides} \\ \textit{the numerator } a \\ |\,q\,|_p = |\,\frac{a}{b}\,|_p = p^{m}; \ \textit{if } p^m \textit{ is the highest power of } p \textit{ that divides} \\ \textit{the denominator } b \end{cases}$$

For example,

$$\left| -\frac{5^4 \cdot 7^2}{11^6 \cdot 13 \cdot 3^3} \right|_p = \left| \frac{5^4 \cdot 7^2}{11^6 \cdot 13 \cdot 3^3} \right|_p = \begin{cases} 5^{-4} & \text{if } p = 5 \\ 7^{-2} & \text{if } p = 7 \\ 11^6 & \text{if } p = 11 \\ 13 & \text{if } p = 13 \\ 3^3 & \text{if } p = 3 \\ 1 & \text{else} \end{cases}$$

What is $\frac{98}{5}$ in $\mathbb{Q}_7$?

If $q = \frac{a}{b} \in \mathbb{Q}$ and $(a,b) = 1$, then q can be written as an element of $\mathbb{Q}_p$. To do that, first, we round up q to the nearest integer, so q is equal to the integer minus a fraction. The trick is to have the denominator in the form of $p^t - 1$, and then use a geometric series to solve. Here is one example.

$$\begin{aligned} \frac{98}{5} &= 20 - \frac{2 \cdot 480}{5 \cdot 480} \\ &= 20 - \frac{960}{2400} \\ &= 20 - 960 \cdot \frac{1}{7^4 - 1} \\ &= 20 + 960 \cdot (1 + 7^4 + 7^8 + 7^{12} + \cdots) \end{aligned}$$

Now, we need to write 20 and 960 in base 7.

$$\begin{aligned} 20 &= 6 \cdot 7^0 + 2 \cdot 7^1 = (6.2)_7 \\ 960 &= 1 \cdot 7^0 + 4 \cdot 7^1 + 5 \cdot 7^2 + 2 \cdot 7^3 = (1.452)_7 \end{aligned}$$

The next step is to multiply out $(1 \cdot 7^0 + 4 \cdot 7^1 + 5 \cdot 7^2 + 2 \cdot 7^3)$ and $(1 + 7^4 + 7^8 + 7^{12} + \cdots)$. That is

$$\begin{aligned} (1 \cdot 7^0 + 4 \cdot 7^1 + 5 \cdot 7^2 + 2 \cdot 7^3) \cdot (1 + 7^4 + 7^8 + 7^{12} + \cdots) \\ = 1 \cdot 7^0 + 4 \cdot 7^1 + 5 \cdot 7^2 + 2 \cdot 7^3 \\ + 1 \cdot 7^4 + 4 \cdot 7^5 + 5 \cdot 7^6 + 2 \cdot 7^7 + \cdots = (\overline{1.452})_7 \end{aligned}$$

Finally, we add $(6.2)_7$ and $(\overline{1.452})_7$. Therefore,

$$\frac{98}{5} = (0.062\overline{1425})_7$$

$(34.\overline{423})_5 = ?$

As we can write $\frac{98}{5}$ in $\mathbb{Q}_7$, we can also work backward and express $(34.\overline{423})_5$ as a rational number. This involves writing the repeating digits in a geometric series. One example is showed below.

$$\begin{aligned} (34.\overline{423})_5 &= (34)_5 + (0.\overline{423})_5 \\ &= 3 \cdot 5^1 + 4 \cdot 5^0 + (0.423)_5 \cdot (\overline{1.000})_5 \\ &= 15 + 4 + (0 \cdot 5^0 + 4 \cdot 5^1 + 2 \cdot 5^2 + 3 \cdot 5^3) \cdot (\overline{1.000})_5 \\ &= 19 + 445 \cdot (1 \cdot 5^0 + 1 \cdot 5^4 + 1 \cdot 5^8 + 1 \cdot 5^{12} + \cdots) \\ &= 19 + 445 \cdot \frac{1}{1 - 5^4} \\ &= 19 - 445 \cdot \frac{1}{5^4 - 1} \\ &= 19 - \frac{445}{624} \\ &= \frac{11411}{624} \end{aligned}$$

Prove $\sqrt{6} \in \mathbb{Q}_5$

If $\sqrt{6}$ can be written in the form of $\sum_{j=m}^{\infty} a_j p^j$, that means $\sqrt{6}$ is an element in $\mathbb{Q}_p$.

$$\mathbb{Q}_p = \left\{ \sum_{j=m}^{\infty} a_j p^j : a_j \in \mathbb{D}_p, m \in \mathbb{Z}, a_m \neq 0 \right\} \cup \{0\}$$

where p is a prime number.

Assume $\sqrt{6} = \alpha = \sum_{k=o}^{\infty} a_k 5^k$, and $6 = \alpha^2 = \left(\sum_{k=o}^{\infty} a_k 5^k\right)^2$. We know that $6 = 1 \cdot 5^0 + 1 \cdot 5^1 = \sum_{k=o}^{\infty} a_k 5^k \cdot \sum_{k=o}^{\infty} a_k 5^k$.

$$\begin{aligned} \sum_{k=o}^{\infty} a_k 5^k \cdot \sum_{k=o}^{\infty} a_k 5^k &= (a_0 + a_1 \cdot 5^1 + a_2 \cdot 5^2 + a_3 \cdot 5^3 + \cdots) \cdot \\ &\quad (a_0 + a_1 \cdot 5^1 + a_2 \cdot 5^2 + a_3 \cdot 5^3 + \cdots) \\ &= a_0^2 + 2a_0 a_1 5^1 + (2a_0 a_2 + a_1^2) 5^2 + (2a_0 a_3 + 2a_1 a_2) 5^3 \\ &\quad + (2a_1 a_3 + a_2^2 + 2a_0 a_4) 5^4 + \cdots \end{aligned}$$

Since $6 = 1 \cdot 5^0 + 1 \cdot 5^1 = \sum_{k=o}^{\infty} a_k 5^k \cdot \sum_{k=o}^{\infty} a_k 5^k$, we have following equations.

$$\begin{aligned} a_0^2 5^0 &= 1 \cdot 5^0 \\ 2a_0 a_1 5^1 &= 1 \cdot 5^1 \\ (2a_0 a_2 + a_1^2) 5^2 &= 0 \\ (2a_0 a_3 + 2a_1 a_2) 5^3 &= 0 \\ (2a_1 a_3 + a_2^2 + 2a_0 a_4) 5^4 &= 0 \\ &\vdots \end{aligned}$$

By solving the equations, we can find the first five 5-adic digits of $\sqrt{6}$. There are two answers because $a_0 = \pm 1$. In the case of $a_0 = 1$, we have $a_1 = 3$; $a_2 = 0$; $a_3 = 4$; $a_4 = 2$. Therefore, $\sqrt{6} = 1 + 3 \cdot 5^1 + 0 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + \cdots$. We have showed that $\sqrt{6}$ can be written in the form of $\sum_{j=m}^{\infty} a_j 5^j$, so we concluded that $\sqrt{6}$ is an element in $\mathbb{Q}_5$.

Prove $i \in \mathbb{Q}_5$

Similar to proving $\sqrt{6}$, we need to show that i can be written in the form of $\sum_{j=m}^{\infty} a_j p^j$. Assume $i = \alpha = \sum_{k=o}^{\infty} a_k 5^k$, and $-1 = \alpha^2 = \left(\sum_{k=o}^{\infty} a_k 5^k\right)^2$. The problem here is that how do we find -1 in base 5. We can do that by following the procedures below.

Claim: $\alpha + \beta = 0$
$\alpha = a_0 \cdot p^0 + a_1 \cdot p^1 + a_2 \cdot p^2 + \cdots + a_j \cdot p^j$
$\beta = t_0 \cdot p^0 + t_1 \cdot p^1 + t_2 \cdot p^2 + \cdots + t_j \cdot p^j + t_{j+1} \cdot p^{j+1} + \cdots$
Choose: $t_0 = p - a_0$

Choose: $t_k = \begin{cases} p - a_k - 1, & \text{if } 1 \leqslant k \leqslant j \\ p - 1, & \text{if } k \geqslant j + 1 \end{cases}$

Proof. To show the procedures above works, we need to show that $\alpha + \beta = 0$. First, we know that
$\alpha + \beta = (a_0 + t_0) + (a_1 + t_1)p + (a_2 + t_2)p^2 + \cdots$
Since $t_0 = p - a_0$, we know that $a_0 + t_0 = p$. Since $t_1 = p - a_1 - 1$, we know that $t_1 + a_1 = p - 1$. Similarly, we know that $a_2 + t_2 = p - 1$. Substitute back to $\alpha + \beta$ we have

$$\begin{aligned} \alpha + \beta &= p + (p-1)p + (p-1)p^2 + (p-1)p^3 + \cdots \\ &= p + (p-1)p \cdot (1 + p + p^2 + p^3 + \cdots) \\ &= p + (p-1)p \cdot \left(\frac{1}{1-p}\right) \\ &= p + \cancel{(p-1)}p \cdot \left(-\frac{1}{\cancel{p-1}}\right) \\ &= p + (-p) \\ &= 0 \end{aligned}$$

□

To find -1 in base 5, we need first find 1 in base 5. Let $\alpha = 1$ and $\beta = -1$

$$1 = (1)_5 = 1 \cdot 5^0 + 0 \cdot 5^1 + 0 \cdot 5^2 + \cdots$$

That means $a_0 = 1, a_1 = 0, a_2 = 0, \cdots$. According to the procedures above, we have

$$\begin{aligned} t_0 &= p - a_0 = 5 - 1 = 4 \\ t_1 &= p - a_1 - 1 = 5 - 0 - 1 = 4 \\ t_2 &= p - a_2 - 1 = 5 - 0 - 1 = 4 \\ &\vdots \end{aligned}$$

Therefore, $-1 = (4.\bar{4})_5$. Now, we are ready to write i in the form of $\sum_{j=m}^{\infty} a_j p^j$. Assume $i = \theta = \sum_{k=o}^{\infty} a_k 5^k$, and $-1 = \theta^2 = \left(\sum_{k=o}^{\infty} a_k 5^k\right)^2$. Since $-1 = (4.\bar{4})_5 = 4 \cdot 5^0 + 4 \cdot 5^1 + 4 \cdot 5^2 + \cdots = \sum_{k=o}^{\infty} a_k 5^k \cdot \sum_{k=o}^{\infty} a_k 5^k$, we have the following equations.

$$\begin{aligned} a_0^2 5^0 &= 4 \cdot 5^0 \\ 2a_0 a_1 5^1 &= 4 \cdot 5^1 \\ (2a_0 a_2 + a_1^2) 5^2 &= 4 \cdot 5^2 \\ (2a_0 a_3 + 2a_1 a_2) 5^3 &= 4 \cdot 5^3 \\ (2a_1 a_3 + a_2^2 + 2a_0 a_4) 5^4 &= 4 \cdot 5^4 \\ &\vdots \end{aligned}$$

By solving the equations,we have $a_0 = \pm 2$. In the case of $a_0 = 2$, $a_1 = 1$; $a_2 = 2$; $a_3 = 1$; $a_4 = 3$. Therefore, $i = 2 + 1 \cdot 5^1 + 2 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots$. We have showed that i can be written in the form of $\sum_{j=m}^{\infty} a_j 5^j$, so we concluded that i is an element in $\mathbb{Q}_5$.

Prove $\sqrt{2} \in \mathbb{Q}_7$

Lemma 1 (Hensel's)**.** *Let $f(x) \in \mathbb{Z}_p[X]$ be a p-adic polynomial and assume there exists $\alpha_0 \in \mathbb{Z}_p$ such that $f(\alpha_0) \equiv 0(\mathit{mod}\ p)$, but $f'(\alpha_0) \not\equiv 0(\mathit{mod}\ p)$. Then there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \alpha_0$ mod p*

Claim: There exists $\alpha \in \mathbb{Z}_p$ such that $\alpha^2 \equiv 2(\text{mod } 7)$ and $\alpha \equiv 3(\text{mod } 7)$

Proof. Apply Hensel's lemma above to $f(x) = x^2 - 2$ at $\alpha_0 = 3$. Clearly,

$$\begin{aligned} f(\alpha_0) &= 7 \equiv 0 \text{ mod } 7 \text{ and} \\ f'(\alpha_0) &= 6 \not\equiv 0 \text{ mod } 7 \\ &\Rightarrow \sqrt{2} \in \mathbb{Z}_p \end{aligned}$$

□

We can prove $\sqrt{2} \in \mathbb{Q}_7$ in a similar way as proving $\sqrt{6} \in \mathbb{Q}_5$. Alternatively, we can use Hensel's lemma as shown above. To find the 7-adic digits for $\sqrt{2}$, we solved a similar set of equations as before. We found the first five 7-adic digits: $a_0 = 3$; $a_1 = 1$; $a_2 = 2$; $a_3 = 6$; $a_4 = 1$. That is $\sqrt{2} = 3 + 1 \cdot 7^1 + 2 \cdot 7^2 + 6 \cdot 7^3 + 1 \cdot 7^4 + \cdots$.

References

[1] Campbell, Duff. *An Open Door to Number Theory*. MAA Press,an Imprint of the American Mathematical Society, 2018.

[2] Khrennikov, A., et al. *"Applications of p-Adic Numbers: from Physics to Geology."* . from Physics to Geology." Contemporary Mathematics Advances in Non-Archimedean Analysis, Jan. 2016, pp. 121–131.