Visualization of Straight Lines in p-Adic Space

In p-adic space, straight lines analogous to those in $\mathbb{R}^2$ are defined by

$$y = a + b \cdot x, \quad (a, b, x, y \in \mathbb{Q}_p).$$

In Euclidean space, we say that $y = a + bx$ because the Euclidean distance between y and $a + bx$ is zero, and the Euclidean distance is simply the absolute value of their difference. In p-adic space, we also declare y and $a + bx$ equal if their distance is zero; however, here the distance between two numbers is determined by the divisibility of their difference by p. If the difference is divisible by arbitrarily high powers of p, then their p-adic distance approaches zero.
Thus, when we write $y = a + bx$ in p-adic space, we really mean that

$$y - (a + bx)$$

is divisible by every power of p, that is,

$$y \equiv a + bx \pmod{p^n} \quad \text{for all } n > 0.$$

However, there are three practical limitations when visualizing this situation.

1. **Finite precision.** We cannot verify divisibility up to an infinite power of p. In practice, we can only check that $y - (a + bx)$ is divisible up to some finite power p^n, i.e., modulo p^n.

2. **Finite plotting domain.** We cannot explicitly plot x and y in $\mathbb{Q}_p$, because for a given $x \in \mathbb{Q}_p$, the condition $y - (a + bx)$ divisible by p^n yields infinitely many pairs $(x, y) \in \mathbb{Z}_p^2$ satisfying it. Therefore, we can only visualize their images modulo p^n, i.e.

   $$y \bmod p^n = \big(a \cdot (x \bmod p^n) + b\big) \bmod p^n,$$

   and plot the pairs $(x \bmod p^n,\ y \bmod p^n)$.

3. **Disconnectedness of p-adic space.** We cannot connect these plotted points with continuous lines, since the p-adic metric induces a completely disconnected topology. Around each point there exists an open ball that contains no other points, hence no continuous curve can pass through multiple points in p-adic space.

How to Expand a Number in p-Adic Space

The general idea is that we use an infinite amount of p^i to approximate a number x. Different from the Euclidean metric, the notion of closeness here changes to the p-adic metric, so if we are using a sequence s_n to approximate x, we want $x - s_n$ to be more and more divisible by p when n progresses.
So if $s_n = \sum_{i=0}^{n} a_i p^i$, then we want $x - s_n$ to be divisible by p^{n+1}.

However, here the idea of divisibility changes since $x - s_n$ is any rational number. Suppose $x = r/s$. Then $r/s - s_n$ being divisible by p^{n+1} means that $r - as$ is divisible by p^{n+1}, or $x - s = fp^{n+1}$, where $f =$ some integer in $\mathbb{Z}_p$. This is denoted by

$$\frac{r}{s} \equiv s_n \pmod{p^{n+1}}.$$

A useful algorithm for this is to start from a_0, s_0. We want

$$x \equiv s_0 \pmod{p^1}.$$

Then we know $x - a_0 = f_0 p$. Next, we find a_1 such that

$$x \equiv s_1 \pmod{p^2}.$$

Then

$$x - s_1 = x - s_0 - a_1 p = f_0 p - a_1 p.$$

This holds iff $f_0 - a_1$ is divisible by p. So we need

$$a_1 \equiv f_0 \pmod{p}.$$

By induction, it is easy to show that to get a_n,

$$a_n \equiv f_{n-1} \pmod{p},$$

where

$$f_{n-1} = \frac{x - s_{n-1}}{p^n}.$$

(Note that its is the best if we keep f_i in fractional form so that we don't loss any precision) Now the problem is how to find a_n such that $a_n \equiv f_{n-1} \pmod{p}$, where f_{n-1} is a rational number. Remember, divisibility for rational numbers is different from the integer definition, so we have to use another algorithm.

Step I:

We prove that

$$a_n = \big((r \bmod p)\,(u \bmod p)\big) \bmod p,$$

where $r, s \in \mathbb{Z}$ and $r/s = f$ with $(p \nmid s)$. Suppose $u \in \mathbb{Z}$ satisfies

$$s\,u \equiv 1 \pmod{p},$$

that is, $u \equiv s^{-1} \pmod{p}$.

First, we show that for any integers a, b,

$$\big((a \bmod p)\,(b \bmod p)\big) \bmod p = (ab) \bmod p.$$

Let $a = \tilde{a} + kp$ and $b = \tilde{b} + \ell p$, where $\tilde{a} = a \bmod p$ and $\tilde{b} = b \bmod p$. Then

$$ab = (\tilde{a} + kp)(\tilde{b} + \ell p) = \tilde{a}\tilde{b} + p(\tilde{a}\ell + \tilde{b}k + k\ell p).$$

Hence,

$$ab \equiv \tilde{a}\tilde{b} \pmod{p}.$$

Also, we know that if $u \equiv s^{-1} \pmod{p}$, then $s\,u \equiv 1 \pmod{p}$, since $u - 1/s = kp$ implies that $us - 1 = np$, where n is an integer.
So we know

$$a_n = \big((r \bmod p)\,(u \bmod p)\big) \bmod p$$

is the same as saying

$$a_n \equiv r\,u \pmod{p}. \tag{1}$$

Thus,

$$s\,a_n \equiv r\,u\,s \pmod{p}. \tag{2}$$

Since $s\,u \equiv 1 \pmod{p}$, we have

$$s\,a_n \equiv r \pmod{p},$$

which is our original restriction on a_n.
Step II:
Finding $s\,u \equiv 1 \pmod{p}$ is equivalent to finding integers n and u such that

$$s\,u + n\,p = 1.$$

This only has a solution if $\gcd(s, p) = 1$, because if they have a common factor, any multiple of $(1 + \text{factor})p$ is never going to be 0.
Now, to find such a solution, we have to first understand the normal Euclidean Algorithm that calculates $\gcd(a, b)$. It claims that if we keep dividing with remainders, the last remainder will be $\gcd(a, b)$. Namely, let

$$\begin{aligned} a &= q_0 b + r_1, \\ b &= q_1 r_1 + r_2, \\ r_1 &= q_2 r_2 + r_3, \\ &\vdots \\ r_{k-1} &= q_k r_k + r_{k+1}, \\ r_k &= q_{k+1} r_{k+1}. \end{aligned}$$

Then $r_{k+1} = \gcd(a, b)$.
Proof. First, notice that $r_1 > r_2 > r_3 > \cdots$, so the remainders form a strictly decreasing sequence. Also $r_i \geq 0$. Hence a strictly decreasing sequence bounded below by 0 must eventually reach 0.
Secondly, $\gcd(x, y) = \gcd\big(y,\ x - ny\big)$ for any integer n. Denote by $C(x, y)$ the set of common divisors of x and y. Similarly define $C\big(y, x - ny\big)$. We show $C(x, y) \subseteq C\big(y, x - ny\big)$ and $C\big(y, x - ny\big) \subseteq C(x, y)$.
If $d \mid x$ and $d \mid y$, then

$$\frac{x - ny}{d} \;=\; \frac{x}{d} - n\,\frac{y}{d} \in \mathbb{Z},$$

so $d \mid (x - ny)$. Thus $d \in C\big(y, x - ny\big)$, proving $C(x, y) \subseteq C\big(y, x - ny\big)$.

Conversely, if $d \mid (x - ny)$ and $d \mid y$, then

$$\frac{x}{d} \;=\; \frac{x - ny}{d} + n\,\frac{y}{d} \in \mathbb{Z},$$

so $d \mid x$. Thus $d \in C(x, y)$, proving $C\big(y, x - ny\big) \subseteq C(x, y)$.
Therefore $C(x, y) = C\big(y, x - ny\big)$, and hence $\gcd(x, y) = \gcd\big(y, x - ny\big)$.
Applying this to the Euclidean algorithm gives

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_k, r_{k+1}) = r_{k+1}.$$

Since the remainders strictly decrease and are nonnegative, the process terminates with the last nonzero remainder r_{k+1}h which equals $\gcd(a, b)$.
Step III:
Now with normal Euclidean algorithm, we could solve for x and y such that $ax + by = \gcd(a, b) = r_{k+1}$, this is simple as we already calculated from normal Euclidean algorithm that

$$r_{k+1} = r_{k-1} - q_k r_k,$$
$$= (r_{k-2} - q_{k-1} r_{k-1}) - q_k r_k = \ldots$$

until we expand it to an expression with respect to a and b. Now back to our problem, we want to find n and u such that $su + np = 1 = \gcd(s, p)$, so we first use normal Euclidean algorithm to calculate $\gcd(s, p)$ which we should get 1, in the process we keep track of each q_i and r_i and then we use the extended Euclidean algorithm to solve for n and u. Now plug n back to the original equation in step I, we should get a_n.

Remark

1. If our input fraction is divisible by p, then we just simply factor out the part that is divisible by p, expand the remaining nondivisible part, and multiply p back in.

2. If our input number y is negative, then we first calculate its positive complement $-y$. We want $y - y = 0$, namely we want all of the p-adic digits to carry over to the next digit to infinity so that everything becomes 0.

   Namely, we want

   $$a_i + a_{i,\text{complement}} + 1$$

   (the 1 comes from the previous digit carried over) to be equal to p for all i, so that every digit i is carried over to the next digit and the whole expression vanishes. So,

   $$a_{i,\text{negative}} = p - 1 - a_{i,\text{positive}}.$$

   Note that for the first non-zero digit, we don't have the extra 1 because we don't have the digit carried over from the previous digit, so

   $$a_{k,\text{negative}} = p - a_{k,\text{positive}},$$

   where k is the index of the first nonzero digit.

3. The reverse of expanding, namely finding the Euclidean rational number with known prefix and repeating block is Easy. Suppose I have a prefix A and a repeating digit block of $\{b_0, \ldots, b_{k-1}\}$, and suppose I know that the repeating block starts from digit n_r. Then,

$$x = A + p^{n_r}\big(b_0 + b_1 p + \cdots + b_k p^{k-1} + b_0 p^k + \ldots\big),$$

where

$$(b_0 + b_1 p + \cdots + b_k p^k + b_0 p^{k+1} + \ldots) = B(1 + p^k + p^{2k} + \ldots),$$

with $B = b_0 + b_1 p + \cdots + b_k p^k$. Then, $(1 + p^k + p^{2k} + \ldots)$ is the geometric series in p-adic space that converges to $1/(1 - p^k)$. This can be easily shown by the exact same technique we used in Euclidean space.