Visualizing the p-adic Integers

ALBERT A. CUOCO*
Mathematics Department, Woburn High School, Woburn, MA 01801

Algebra and analysis in the p-adic integers provide us with examples of mathematical phenomena that are hard to find in one package elsewhere. $\mathbb{Z}_p$ is a regular local ring; it is uncountable, and the non-archimedean valuation induced by its maximal ideal, $p\mathbb{Z}_p$, makes it into a compact, totally disconnected topological ring that contains the ordinary integers as a dense subring. How can one visualize such a creature?

Pictures that inspire images of p-adic objects are rare (see the frontispiece of **[3]** for an example). In this note, we show how to represent, for any prime p, the elements of $\mathbb{Z}_p$ as the points on a fractal in $\mathbb{R}^2$. The resulting correspondence captures many of the important algebraic and topological facets of $\mathbb{Z}_p$.

The pictures. Computer graphics enthusiasts have discovered a wonderful pastime. The idea is to plot an inductively defined (nondeterministic) sequence of points $\{Q_n\}$ in the plane. The sequence depends on an initial set of fixed vertices $\{A_0, A_1, \dots, A_{k-1}\}$, the initial point Q_0 in the sequence and a real number e between 0 and 1. Suppose that Q_0 is one of the A_i and that Q_j has been defined. To find Q_{j+1}, pick one of the fixed vertices, say A_h, at random (that is, so that the probability of choosing any one vertex is $1/k$), and let δ be the distance between Q_j and A_h. Then Q_{j+1} is the point on the segment between Q_j and A_h at a distance of $e\delta$ from A_h. If $k = 3$, $e = .5$, and the A_i are vertices of an equilateral triangle, then the Q_n lie on a Sierpiński triangle (see **[1]** for the definition of Sierpiński triangles and Figure 1 for a picture of one).

We'll be concerned with the figures that occur when $k = p$ (a prime $\geqslant 3$), $e = 1/p$, and the A_i are vertices of a regular p-gon of side length 1. Call such a set of points S_p; a Macintosh computer running for a few minutes produced the approximations to S_3 in Figures 2a and 2b.

Figure 2a shows the process after 50 and 100 iterations; Figure 2b shows the results of 500 and 1000 iterations. Figure 2 shows the general shape of S_3; our definition of S_3 implies that it is the attractor for a system of three mappings on $\mathbb{R}^2$ (each mapping is a contraction with magnitude $1/3$ toward one of the A_i).[1]

A deterministic method to obtain S_p is to approximate it with sets $S_{p,n}$. Suppose, for example, that $p = 3$. Then $S_{3,0}$, $S_{3,1}$, $S_{3,2}$, $S_{3,3}$ and $S_{3,4}$ are depicted in Figure 3. Here, $S_{3,n}$ contains 3^n triangular regions. It is constructed from $S_{3,n-1}$ by replacing each triangular region T in $S_{3,n-1}$ with three small triangles, one from each corner of T, each with side-length $1/3$ that of T. S_3 is then the intersection of all the $S_{3,n}$. Similarly, S_p is the intersection of all the $S_{p,n}$. A few of the $S_{5,n}$ are illustrated in Figure 4.

Using this method for constructing S_p shows that S_p, as a subset of $\mathbb{R}^2$, is compact and totally disconnected.

*Work supported by NSF Grant MDR-895-4647

[1] To generate the images in Figure 2, the initial point Q_0 is chosen to be one of the vertices $\{A_0, A_1, A_2\}$; if Q_0 is not a vertex, the resulting sequence $\{Q_n\}$ will converge to S_3 in the sense that $\lim_{n\to\infty}(\inf_{P\in S_3} dist(P, Q_n)) = 0$.

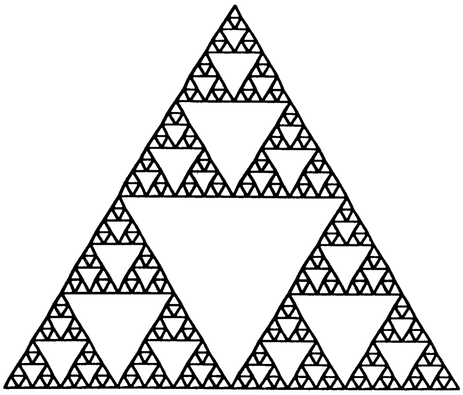

FIG. 1.

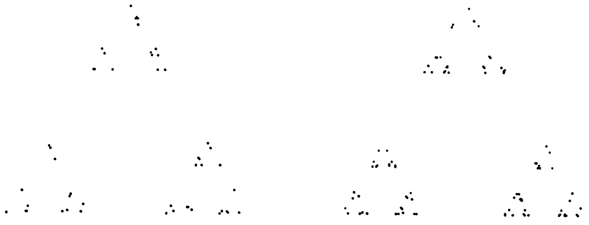

FIG. 2A.

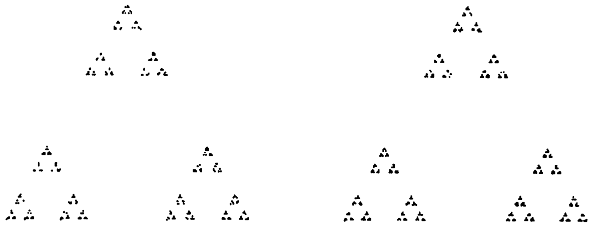

FIG. 2B.

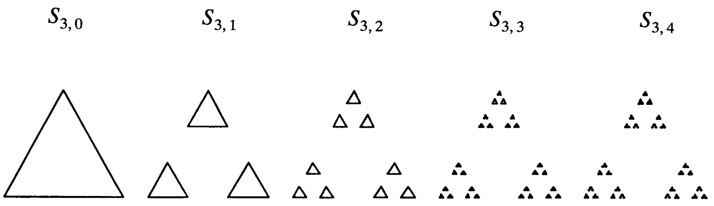

FIG. 3.

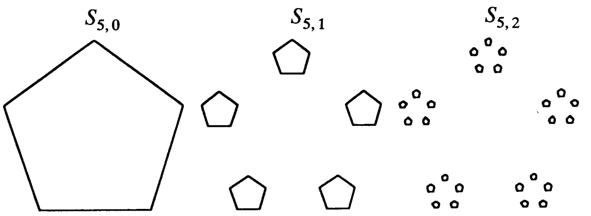

FIG. 4.

p-adic integers. For precise definitions of $\mathbb{Z}_p$, see **[3]**, **[4]** or **[2]**. We'll think of $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to the absolute value $| \ |_p$. Here,

$$|n|_p = p^{-\operatorname{ord}_p(n)}$$

where $\operatorname{ord}_p(n)$ is the highest exponent to which p divides n. The idea is that two integers are close if their difference is 0 modulo a high power of p. The completion contains the subring of $\mathbb{Q}$ known as the "p-integral" numbers (rational numbers whose denominators aren't divisible by p), as well as some irrational numbers.

If m is a positive integer, m has a finite base p expansion

$$m = m_0 + m_1 p + m_2 p^2 + m_3 p^3 + \cdots + m_r p^r,$$

where the m_i are integers between 0 and $p - 1$. This expansion (the *p-adic expansion* for m) will be denoted by its digits, and we'll write

$$m = m_0 m_1 m_2 m_3 \cdots m_r.$$

It's easy to see that $\operatorname{ord}_p(m)$ is the smallest integer k such that $m_k > 0$. It follows that two integers are close if their p-adic expansions agree for many places. In particular, the sequence

$$1, 11, 111, 1111, 11111, \ldots$$

is Cauchy, and its limit in $\mathbb{Z}_p$ can be calculated from the usual formula for the limit of a convergent geometric series

$$1111111 \cdots = 1 + p + p^2 + p^3 + p^4 = \cdots = \frac{1}{1-p}.$$

(Notice that the common ratio in this series is p, and $|p|_p = 1/p$.) Since every p-adic integer is the limit of some Cauchy sequence of integers, and since the p-adic expansions for these integers agree for arbitrarily long initial strings, we can think of a p-adic integer as an infinite p-adic expansion, denoted by an infinite string of digits

$$a_0 a_1 a_2 a_3 a_4 \cdots = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + a_4 p^4 + \cdots,$$

where each a_i is an integer between 0 and $p - 1$. As with all completions, $| \ |_p$ extends to a valuation on $\mathbb{Z}_p$, and its value can be calculated by the same formula that defines it on $\mathbb{Z}$ ($\operatorname{ord}_p(a)$ is the smallest integer k such that $a_k > 0$). So, just as in $\mathbb{Z}$, two p-adic integers are close if their representations agree for many digits (that is, if their difference is 0 modulo a high power of p). An element of $\mathbb{Z}_p$ is a non-negative integer if and only if its digits are eventually 0; an element of $\mathbb{Z}_p$ is in $\mathbb{Q}$ precisely when its digits eventually repeat.

The arithmetic of $\mathbb{Z}_p$ is especially simple. $\mathbb{Z}_p$ has unique factorization, and the only prime is p. Every p-adic integer a can be written uniquely as $p^e u$. Here, $e = \operatorname{ord}_p(a)$, and u is a unit (a p-adic integer whose first digit is not 0). $\mathbb{Z}_p/p\mathbb{Z}_p$ is isomorphic with $\mathbb{Z}/p\mathbb{Z}$. If U is the unit group in $\mathbb{Z}_p$ and U_1 is the subgroup of U consisting of units whose first digit is 1 (the *principal* units), then U/U_1 is isomorphic with $(\mathbb{Z}/p\mathbb{Z})^*$, the multiplicative group of non-zero elements in $\mathbb{Z}/p\mathbb{Z}$ (a cyclic group of order $p - 1$).

Given a p-adic integer a, a fundamental system of neighborhoods for a is the sequence

$$\{a + p^n\mathbb{Z}_p \colon n = 0, 1, 2, 3, \dots\}.$$

Indeed, given an integer $n, \mathbb{Z}_p$ splits up into p^n disjoint disks of diameter $1/p^n$, namely the cosets in $\mathbb{Z}_p/p^n\mathbb{Z}_p$. Two p-adic integers x and y are within $1/p^n$ of each other if and only if they belong to the same disk.

The metric d defined by $|\ |_p$ satisfies a stronger condition than the triangle inequality; if a, b and c are in $\mathbb{Z}_p$, then

$$d(a,b) \leqslant \max\{d(a,c), d(b,c)\}$$

(equality holds if $d(a,c)$ and $d(b,c)$ are unequal). This *non-archimedean* property of d implies that every triangle is isosceles and that every point interior to a circle is its center.

The correspondence. Naïvely, a p-adic integer is an object that can be approximated modulo p^n (that is, within a p-adic distance of $1/p^n$), for any n, by a length n p-adic expansion of an ordinary integer. And, a point on S_p is a point in $\mathbb{R}^2$ which, for any n, is in a connected component of $S_{p,n}$ (so that it can be approximated within a (Euclidean) distance of $1/p^n$ by a vertex on $S_{p,n}$). So, we can build a natural bijection between $\mathbb{Z}_p$ and S_p by setting up, for each n, a bijection between $\mathbb{Z}_p/p^n\mathbb{Z}_p$ and the vertices of $S_{p,n}$ that makes the following diagram commute

$$\begin{tikzcd}
\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \arrow[r] \arrow[d] & \mathbb{Z}_p/p^n\mathbb{Z}_p \arrow[d] \\
S_{p,n+1} \arrow[r] & S_{p,n}
\end{tikzcd}$$

Here, the top row is the usual homomorphism (it amounts to forgetting the last digit in the p-adic expansion), and the bottom row collapses each polygon of side length $1/p^{n+1}$ onto the unique vertex of the polygon of side length $1/p^n$ that it contains. Taking the inverse limit, we have a correspondence between $\mathbb{Z}_p$ and S_p.

Suppose, for the sake of example, that $p = 3$. Figure 5 shows how the correspondence develops.

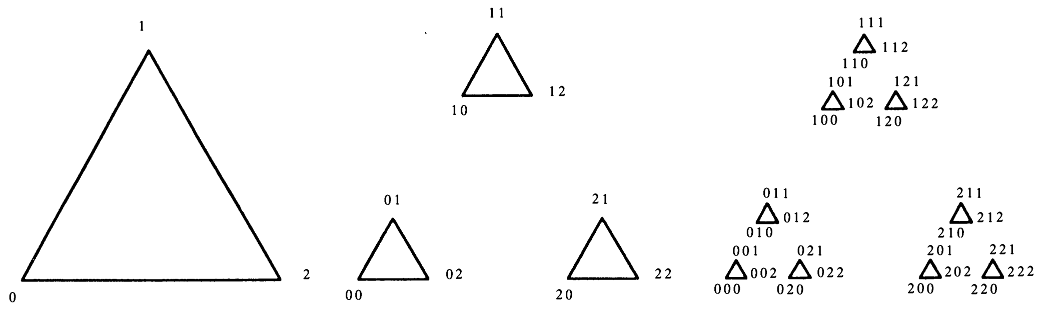

FIG. 5.

Figure 6 shows the skeleton of $S_{3,3}$, but the labeled points are the actual 3-adic integers (expressed as elements of $\mathbb{Q}$) that remain after passing to the limit.

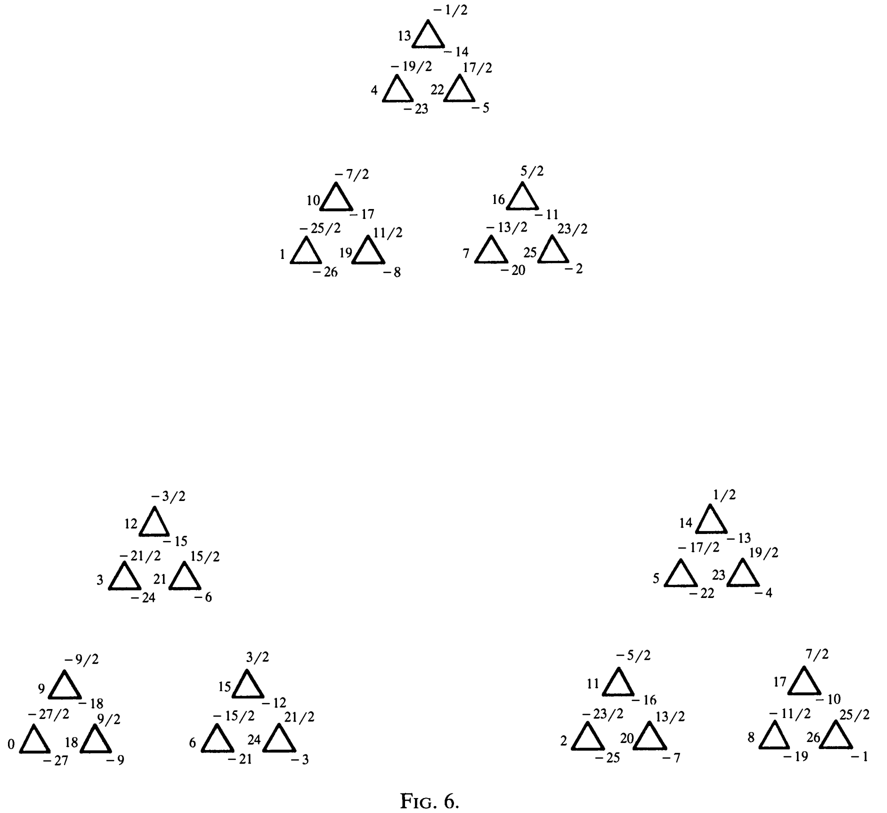

FIG. 6.

Similarly, Figure 7 shows some elements of $\mathbb{Z}_5$ as they appear on $S_{5,1}$.

Figure 8 shows how to chase down the (irrational) 5-adic integer 0313113111311113111113... in S_5 by tracking the approximation 0, 03, 031, and 0313.

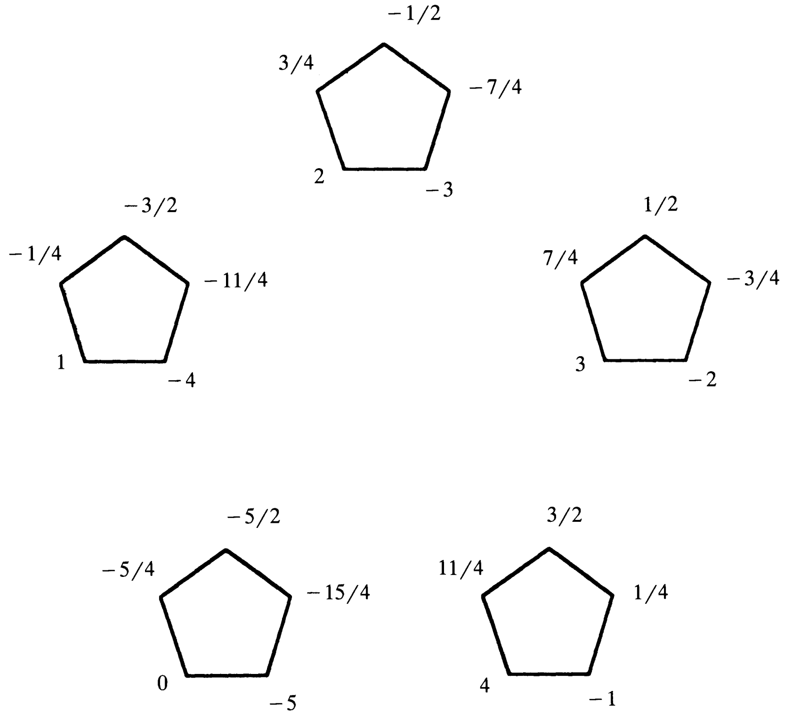

FIG. 7.

The most important aspect of our construction is: *Two p-adic integers are in a disk of diameter* $1/p^n$ *if and only if their images in* S_p *are in the same connected component of* $S_{p,n}$.

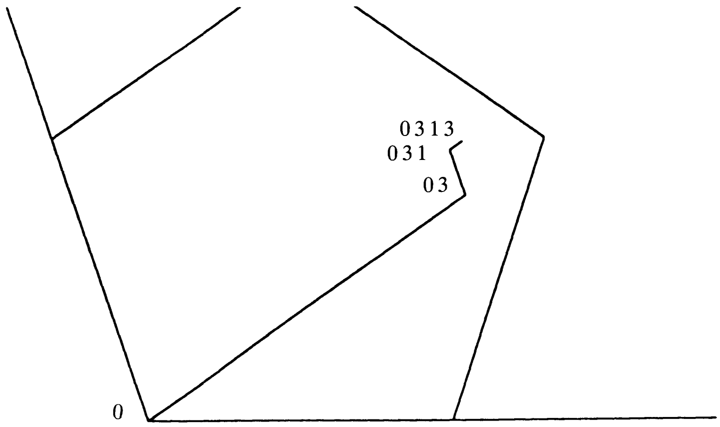

FIG. 8.

Using the correspondence. Looking at Figure 6, for example, the following facts about $\mathbb{Z}_3$ stand out:

1. $\mathbb{Z}_3$ is compact.

2. Every point in $\mathbb{Z}_3$ has a neighborhood that is both open and closed; $\mathbb{Z}_3$ is totally disconnected.

3. The image of the filtration $\{3^n\mathbb{Z}_3: n = 0, 1, 2, 3, \dots\}$ in S_3 is contained in the set of triangles that contain 0 and have sides of length $(1/3^n)$ $(n = 0, 1, 2, \dots)$.

4. For any n, there are precisely 3^n disks of diameter $1/3^n$. These are the translates of $3^n\mathbb{Z}_3$ by $0, 1, 2, \dots, 3^{n-1}$.

Figure 9 suggests that $\mathbb{Z}_p/p\mathbb{Z}_p$ identifies with $\mathbb{Z}/p\mathbb{Z}$, and that U/U_1 identifies with $(\mathbb{Z}/p\mathbb{Z})^*$.

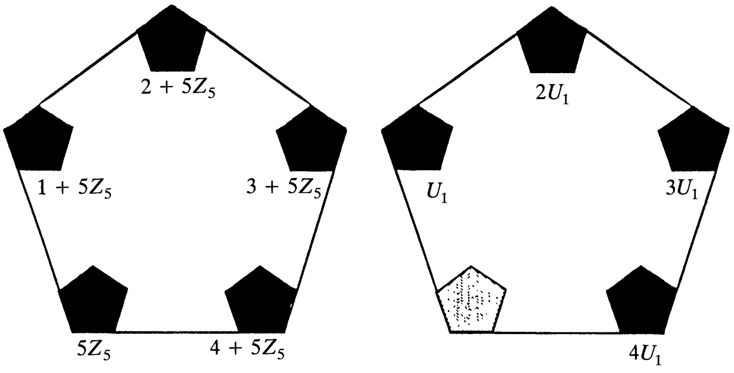

FIG. 9.

One can even use S_p to give examples of the non-archimedean geometry of $\mathbb{Z}_p$. For example, S_5 can be used to illustrate the isosceles triangle property in $\mathbb{Z}_5$. Suppose that we have three points A, B, and C in $\mathbb{Z}_5$ that are not the vertices of an equilateral triangle. Suppose further that

$$\max\{d(A,B), d(B,C), d(A,C)\} = \frac{1}{5^n}$$

and that this maximum distance is between A and C. Then one pair of points, say, A and B, are separated by a distance of at most $1/5^{n+1}$. Using our correspondence, the situation is as in Figure 10.

In Figure 10, we have a disk of diameter $1/5^n$ in $\mathbb{Z}_5$ that contains A, B, and C. This disk is the union of 5 disjoint disks, each of diameter $1/5^{n+1}$. Two elements of the large disk are in the same small disk if and only if the distance between them is at most $1/5^{n+1}$, while two 5-adic integers from the large disk are in *different* small disks if and only if the distance between them is exactly $1/5^n$. It follows that A and B are in the same small disk, and that C is in a different small disk. Therefore,

$$d(A,C) = d(B,C) = \frac{1}{5^n}$$

and our triangle is isosceles.

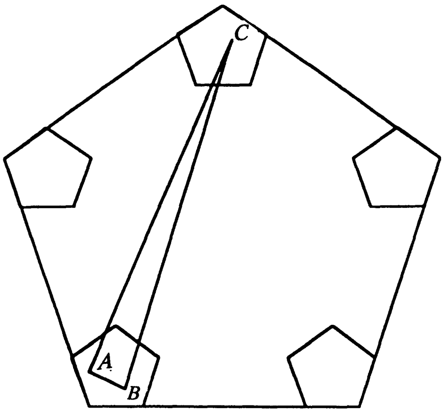

FIG. 10.

Conversely, the arithmetic of $\mathbb{Z}_p$ might be a useful tool in the study of the geometry of S_p. For example, suppose that c is a fixed integer between 1 and $p - 1$. The fact that the neighborhoods of c are just the translates by c of the neighborhoods of 0 can be used to picture the effect of the mapping $x \mapsto c + x$ on S_p. Multiplication by c is a one-to-one mapping of $\mathbb{Z}_p$ onto itself, and there is an algorithm (much like the multiplication algorithm that is taught in elementary school) for obtaining the digits of ca from those of a. Given a p-adic integer a and its location in S_p, can this algorithm be transported to a simple geometric construction that allows one to locate ca in S_p?

Remark. In our definition of the p-adic absolute value

$$|a|_p = \left(\frac{1}{p}\right)^{\operatorname{ord}_p(a)},$$

our choice of the "uniformizing parameter" $1/p$ is somewhat arbitrary. Any real number less that 1 will give an equivalent metric, although our correspondence requires a parameter less than 0.5. In the case $p = 2$, it is sometimes convenient to take $1/4$, so that

$$|a|_2 = \left(\frac{1}{4}\right)^{\operatorname{ord}_2(a)}.$$

Then it is possible to set up our correspondence between $\mathbb{Z}_2$ and the Cantor-like subset of the unit interval obtained by repeatedly removing the middle half.

p-adic numbers. Because $\mathbb{Z}_p$ is an integral domain, it has a quotient field $\mathbb{Q}_p$, the field of p-adic numbers. $\mathbb{Q}_p$ is locally compact, and it contains $\mathbb{Z}_p$ as an open subring. If $|\ |_p$ is viewed as a function on $\mathbb{Q}$ (by defining the absolute value of a quotient as the quotient of the absolute values), $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\ |_p$. We end by sketching a method for extending our embedding of $\mathbb{Z}_p$ into $\mathbb{R}^2$ to an embedding of $\mathbb{Q}_p$ into $\mathbb{R}^2$.

One way to think about a p-adic number is as a p-adic expansion that contains a finite number of terms with negative exponents. If a is the p-adic number

$$a = \sum_{k=-N}^{\infty} a_k p^k,$$

we'll denote a by its digits

$$a = a_{-N}a_{-N+1} \cdots a_{-1}.a_0a_1a_2 \ldots .$$

We can write $\mathbb{Q}_p$ as the increasing union of the sets $\mathbb{Q}_{p,n}$ where

$$\mathbb{Q}_{p,n} = \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leqslant p^n\}.$$

Then

$$\mathbb{Q}_{p,0} = \mathbb{Z}_p = \{0.a_0a_1a_2 \cdots : 0 \leqslant a_i \leqslant p-1\},$$

$$\mathbb{Q}_{p,1} = \{a_{-1}.a_0a_1a_2 \cdots : 0 \leqslant a_i \leqslant p-1\},$$

and, more generally,

$$\mathbb{Q}_{p,n} = \{a_{-n} \cdots a_{-1}.a_0a_1a_2 \cdots : 0 \leqslant a_i \leqslant p-1\}.$$

Geometrically, we can replicate S_p as in Figure 11 (for $p = 3$) to obtain a fractal $S_{p,\infty}$.

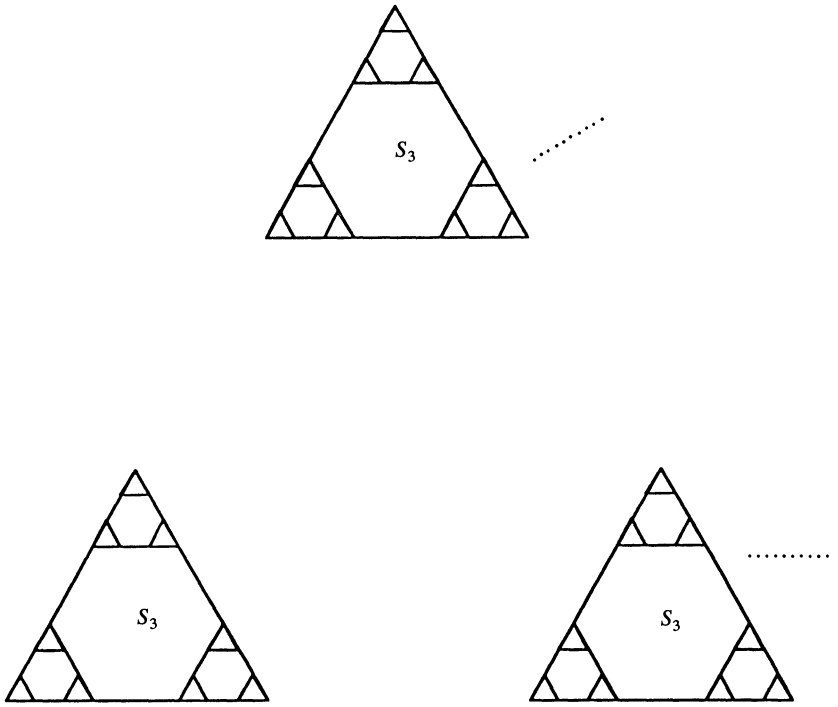

FIG. 11.

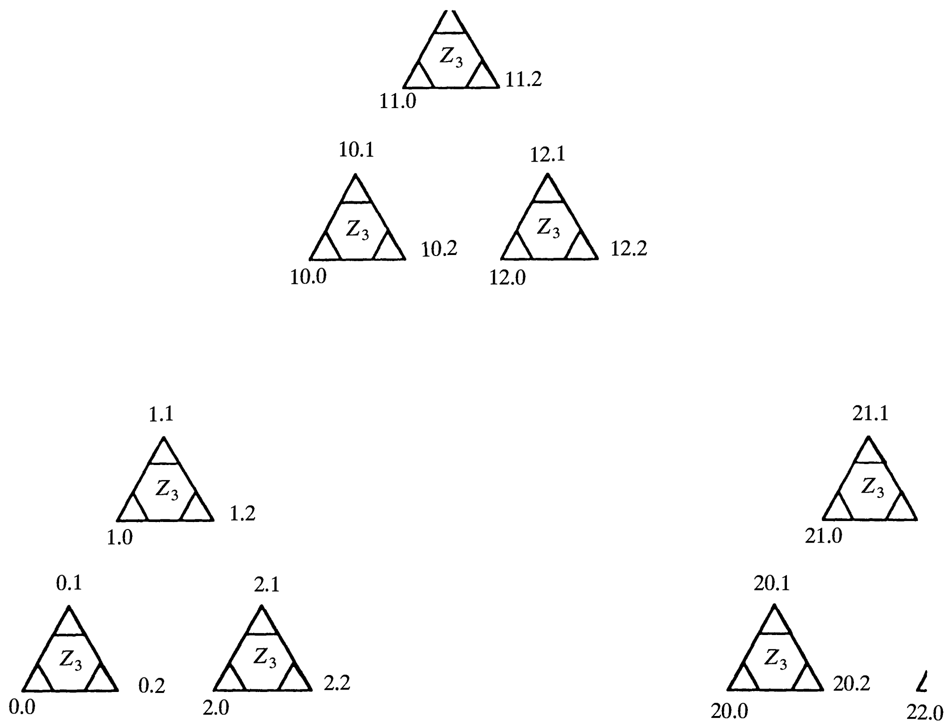

FIG. 12.

The bijection between $\mathbb{Q}_p$ and $S_{p,\infty}$ is shown in Figure 12 for the case $p = 3$.

Special thanks to E. Paul Goldenberg.

REFERENCES

1. Michael Barnsley, Fractals Everywhere, Academic Press, San Diego, 1988.
2. Z. I. Borevich and I. R. Shafarevich, Number Theory, Academic Press, New York, 1966.
3. Neal Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer Verlag, New York, 1977.
4. Jean-Pierre Serre, A Course in Arithmetic, Springer Verlag, New York, 1973.

Editor's note: Several readers have pointed out that the argument presented in Deng Bo's article "The derivation of the Maclaurin series for sine and cosine" in November 1990 issue of the MONTHLY is well known. It appears in some calculus books, including those by Ivan Niven and George Simmons. Niven points out that the argument appears in the 1941 book *What is Mathematics?*, by R. Courant and H. Robbins, but was probably well known several decades earlier. Finally, Niven's book (*Calculus: An Introductory Approach*, 2d edition, Von Nostrand, New York, 1966, pp. 140, 160, 167, 171) shows how the logarithmic, exponential, and arctangent series can all be given similar derivations.