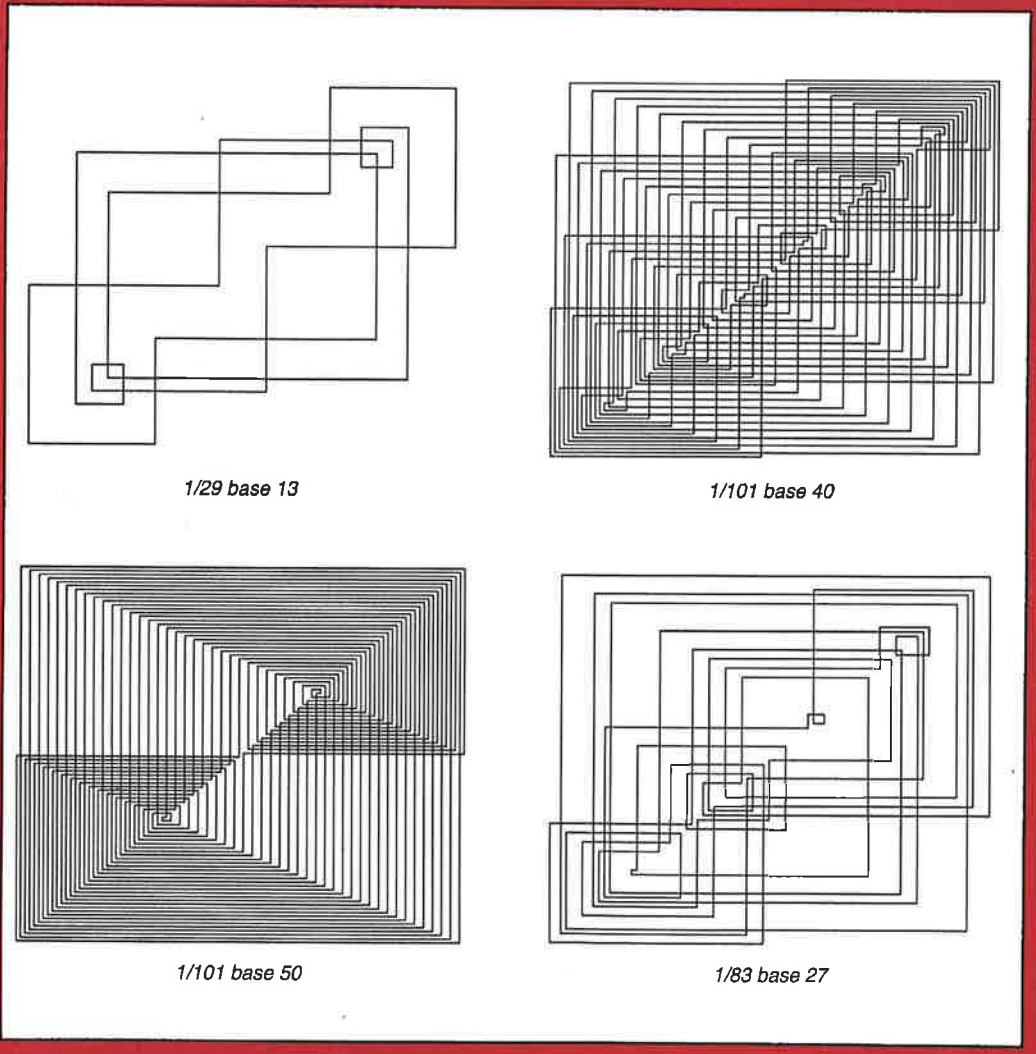
Vol. 73, No. 2, April 2000

MATHEMATICS MAGAZINE



1/29 base 13

1/101 base 40

1/101 base 50

1/83 base 27

- Fractions: A Postmodern View
- Counting on Continued Fractions
- Venn Said it Couldn't be Done
- Superexponentiation
- Oblong Numbers

An Official Publication of The MATHEMATICAL ASSOCIATION OF AMERICA

ARTICLES

A Postmodern View of Fractions and the Reciprocals of Fermat Primes

RAFE JONES
Brown University
Providence, RI 02912

JAN PEARCE
Berea College
Berea, KY 40404

Introduction and preliminaries

In America's visually-oriented, quantitatively illiterate culture, images have a great deal of power, so if a picture is today worth a thousand words, it must be worth at least a billion numbers. This power of the image is a hallmark of the postmodern era, in which the critical role of the observer has come to be recognized, and an understanding of the viewpoint has become inseparable from that of the object.

In some ways, the blossoming of chaos theory marked the arrival of mathematical postmodernism. Not so long ago, mathematical ideas were virtually unseen in American popular culture, and it took the enthralling fractal images of chaos theory to change that: the studies of chaos and fractals became some of the most widely discussed mathematical topics ever, and pictures of fractal images such as the

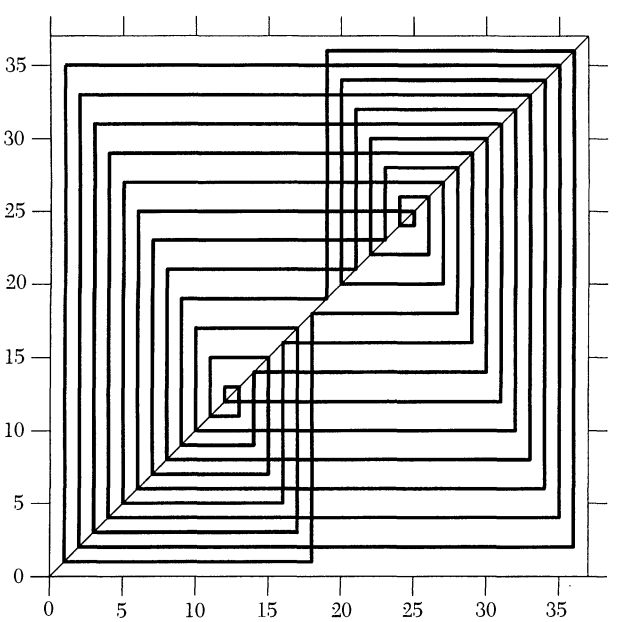


FIGURE 1
Graphical analysis of 1/37 base 35.

Mandelbrot set began cropping up on T-shirts and posters selling in American malls. The power of an image is difficult to underestimate, particularly when it comes to creating interest in a topic widely regarded as bland. Perhaps we could fuel a greater excitement in traditionally underappreciated areas of mathematics if only we could present them in a flashier graphical fashion. Take fractions, for instance, which to many people appear to be merely seas of numbers; after all, infinitely many fractions have infinitely long strings of digits as their decimal expansions. Wouldn't it be nice if we could see complicated fractions, like $\frac{1}{37}$ base 35, as simple images? Wouldn't it be even nicer if, as for the Mandelbrot set, those graphical images exposed something about the inherent mathematical structure that the concise algebraic expression only implied?

In this paper, we apply to the study of certain fractions the same graphical techniques used to transform the Mandelbrot set from algebra to image. This will enable us to turn arcane algebraic objects into eye-catching designs, such as the one pictured in FIGURE 1. What's more, the mathematics behind this metamorphosis is not very hard to describe. We begin by describing a somewhat unusual method of representing a fraction, which will be useful for our purposes. Fractions can be viewed in a number of ways, many of which are base-dependent: reduced or unreduced, as pieces of a pie, expanded into decimal, binary, octal, etc. The method we adopt is quite base-dependent, and relies upon the remainders generated at each stage of the long-division process in base b. Consider $\frac{1}{7}$, which has a base 10 (decimal) expansion of $0.\overline{142857}$. We can calculate this using the usual long division process in base 10 as follows:

$$
\begin{array}{r}
0.142857 \\
7\overline{)1.000000} \\
\underline{7} \\
30 \\
\underline{28} \\
20 \\
\underline{14} \\
60 \\
\underline{56} \\
40 \\
\underline{35} \\
50 \\
\underline{49} \\
1
\end{array}
$$

We can equivalently represent $\frac{1}{7}$ base 10 by writing the sequence of remainders produced in the above long division: $1 \to 3 \to 2 \to 6 \to 4 \to 5 \to 1$, a cycle that repeats infinitely. Note that what makes this a base ten long division is that we multiply the dividend by ten at every step; we could easily make it into a base b long division by multiplying by b at each step. This new long division would yield the sequence of remainders for $\frac{1}{7}$ base b; in fact, one can find the sequence of remainders for any fraction in any base simply by performing the appropriate long division. However, the laboriousness and iterative nature of long division make it desirable to have a simpler, more concise method of finding sequences of remainders. Happily, such a method exists, and it is simply the evaluation of the following function:

DEFINITION. Let a, b, and n be positive integers with $(n, a) = 1$ and $b > 1$. If r_i is the remainder produced at step i of the base b long division of $\frac{a}{n}$, the remainder produced at the $(i+1)$st step is given by $r_{i+1} = F_{b:n}(r_i) = b \times r_i (\text{mod } n)$. We call $F_{b:n}$ the *remainder function*, since if we begin with $r_0 = a$, iteration of $F_{b:n}$ yields the sequence of remainders of $\frac{a}{n}$ long divided in base b.

Note that a and n are relatively prime, so $\frac{a}{n}$ is a reduced fraction; we will assume throughout that all fractions are reduced. We can see the remainder function in action with the fraction used above, $\frac{1}{7}$ base 10. We begin with $r_0 = 1$. Next we have $r_1 = F_{10:7}(r_0) = 10 \times 1 \pmod 7 = 3$, followed by $r_2 = F_{10:7}(r_1) = 10 \times 3 \pmod 7 = 2$, $r_3 = F_{10:7}(r_2) = 10 \times 2 \pmod 7 = 6$, $r_4 = F_{10:7}(r_3) = 10 \times 6 \pmod 7 = 4$, $r_5 = F_{10:7}(r_4) = 10 \times 4 \pmod 7 = 5$, and $r_6 = F_{10:7}(r_5) = 10 \times 5 \pmod 7 = 1$.

Since $r_6 = r_0 = 1$, the sequence repeats. Note that each iteration of the remainder function simply multiplies by b and mods by n. Then, since r_0 is a, we can calculate the ith remainder directly using the formula $r_i = ab^i \pmod n$. This compact formula simplifies many arguments involving sequences of remainders, and you will see it often in the pages to come.

In the analysis above, our friend $\frac{1}{7}$ base 10 displays some surprising qualities. For example, $r_i + r_{i+3} = 7$ for all i. Moreover, if we let d_i represent the digit of the decimal expansion that is i places to the right of the decimal point, then in this example $d_i + d_{i+3} = 9$ for all i. These symmetries, as we shall see, have more than a numerical significance.

Before moving on to graphical topics, it will serve us well to discuss the three kinds of behavior a sequence of remainders (as well as the corresponding expansion) can exhibit. Each of these behaviors corresponds to a particular kind of graphical analysis graph, a concept we introduce in detail below. First, the sequence of remainders of $\frac{a}{n}$ in base b (as well as the corresponding base b expansion) may terminate; this happens if each remainder (and digit) is zero after some point, and such a fraction will have a graphical analysis graph that begins at some point and ends at some different point. This is the case if and only if every prime factor of n is also a prime factor of b. Second, the sequence may have a repeating cycle, but one that begins only after some initial string of remainders that never reappears. In this case, the graphical analysis graph will be an infinitely repeated figure, but with a tail created by the initial unrepeated string of remainders. This happens if and only if n has some factors that divide b and some that do not. Thirdly, the sequence may have only repeated cycles with no initial unrepeated string of remainders; this occurs if and only if n and b are relatively prime. This sort of fraction produces the neatest graphical analysis graph: a figure that retraces itself infinitely, with no unrepeated points.

The remainder function described above will allow us to work more easily with sequences of remainders. That it is a function also makes it a nice candidate for a graphical technique we will now introduce.

Graphical analysis

Graphical analysis or graphical iteration **[2]** gives us a visual way to explore function iteration. To graphically analyze a function $F(r)$, one does the following: Let r_0 be some number. Then, beginning with $i = 0$, draw a vertical line from (r_i, r_i) to the point $(r_i, F(r_i)) = (r_i, r_{i+1})$. (See FIGURE 2) From there, draw a horizontal line to $(F(r_i), F(r_i)) = (r_{i+1}, r_{i+1})$. Then increase i by one iteratively and repeat the preceding steps. Here, we will apply graphical analysis to our function $F_{b:n}(r)$. In order to avoid minor difficulties, we will say that if the remainder becomes zero at r_n, we stop the process at r_{n-1}. Although graphical analysis works only on functions, the remainder function associated with a given fraction is so closely tied to the fraction that we will refer to the graphical analysis of $F_{b:n}(r_i) = b \times r_i \pmod n$, with $r_0 = a$, as the graphical analysis of $\frac{a}{n}$ in base b.

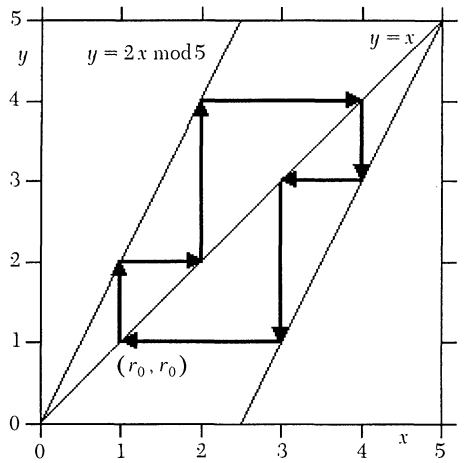


FIGURE 2

Graphical analysis of $\frac{1}{5}$ in base 2.

Note that the remainder function $F_{2:5}(x) = 2x \pmod 5$ plays a crucial role in FIGURE 2. However, you may have noticed that $F_{35:37}(x)$ does not appear in the graphical analysis graph of $\frac{1}{37}$ in base 35 (see FIGURE 1). The reason is that for so complex a picture, the slanted parallel lines of the remainder function become so dense as to obscure the image. Thus, despite their importance, for the sake of clarity we will omit them in the images to come.

Also, although the remainder function is theoretically important, one may graphically analyze a fraction without drawing the graph of the remainder function itself. In effect, the graphical analysis begins at the point (r_0, r_0), proceeds first vertically then horizontally to (r_1, r_1), then moves vertically then horizontally again to (r_2, r_2), and continues in this fashion. Hence in practice one can graphically analyze a fraction in a given base as follows: Compute the sequence of remainders; for each remainder, draw the appropriate dot on the line $y = x$; then connect the dots (following the order of the sequence of remainders), moving vertically then horizontally. Thus *the sequence of remainders entirely determines the graphical analysis graph of the fraction.* So when proving certain properties of graphical analysis graphs, such as various symmetries, we need not consider the entire image, but only the distribution of remainders.

Since the graphical analysis of a fraction varies from base to base, one might wonder how many distinct graphical pictures exist for a given fraction $\frac{a}{n}$. Bases zero and one are exempt from consideration. If b_1 and b_2 are bases such that $b_1 \equiv b_2 \pmod n$, then $ab_1^{\,m} \equiv ab_2^{\,m} \pmod n$, so $\frac{a}{n}$ will generate identical sequences of remainders in both bases. Thus, we only have to consider for our bases a single representative from each congruence class modulo n. This means, of course, that at most n bases may produce distinct graphs. Further narrowing the field is the fact that if b is a base such that $b \equiv 0 \pmod n$ or $b \equiv 1 \pmod n$, the pictures are not very interesting: in the former case, all remainders save the first are zero, so the graphical analysis graph is merely a single point, since the analysis ends with the last nonzero remainder. In the latter case, if m is a positive integer, then $\frac{1}{n}$ written in base $mn + 1$ is $0.\overline{1}$, and the sequence of remainders is an infinite string of ones; again, the graphical analysis graph is a single point. We will exclude bases in the 0 congruence class in many later considerations. However, we will often be interested in all bases in which a fraction has a repeating expansion, and thus we will include bases in the 1 congruence class in spite of their graphical shortcomings.

The various graphs of a fraction in different bases often bear some relation to one another. The following definition will help us relate some of them to others.

Rotational graph pairs

DEFINITION 1. $\frac{a_1}{n_1}$ and $\frac{a_2}{n_2}$ are *rotational graph pairs* if the graphical analysis graph of $\frac{a_1}{n_1}$, when rotated 180° about the point $\left(\frac{n}{2}, \frac{n}{2}\right)$, produces the graphical analysis graph of $\frac{a_2}{n_2}$.

These pictures exemplify rotational graph pairs:

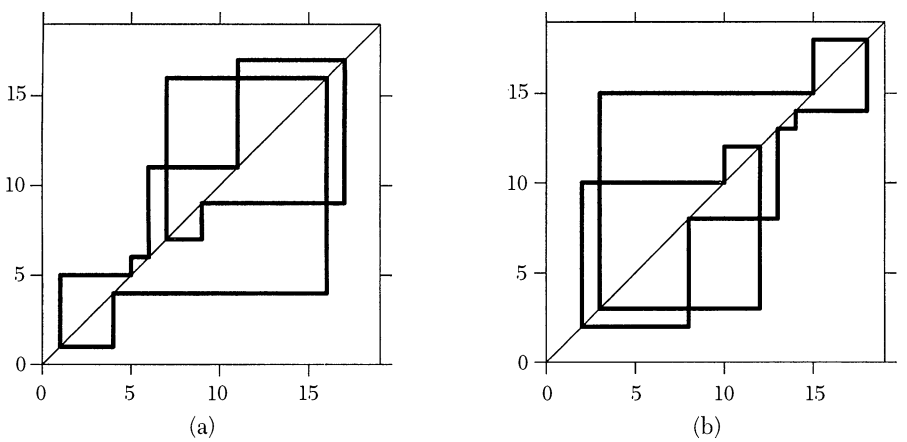


FIGURE 3
Graphical analysis of 17/19 base 5 vs. 2/19 base 5.

Since the graph of a fraction in base b depends entirely on its sequence of remainders, we can show that two fractions are rotational graph pairs simply by showing that "rotating" the sequence of remainders of one fraction about the point $\left(\frac{n}{2}, \frac{n}{2}\right)$ produces precisely the other sequence. In other words, the sequences must be zero in exactly the same places, and whenever the ith remainders of both sequences are nonzero, they must be equidistant from the point $\left(\frac{n}{2}, \frac{n}{2}\right)$. This is true if and only if the remainders in question sum to n. Thus we need only show that adding corresponding nonzero terms in the two sequences of remainders invariably yields n.

THEOREM 1. *In each base b, $\frac{a}{n}$ and $\frac{n-a}{n}$ are rotational graph pairs.*

Proof. First note that the only possible remainders at any stage of the long division of $\frac{a}{n}$ in base b belong to the set $\{0, 1, 2, \ldots, n-1\}$. Now, for any i, $ab^i \pmod n + (n-a)b^i \pmod n = (ab^i + (n-a)b^i) \pmod n = nb^i \pmod n$. Since $nb^i \equiv 0 \pmod n$ we have that the sum of the ith remainders of each sequence must be either 0 or n. Note that it is impossible for the ith remainder of one sequence to be zero and the ith remainder of the other nonzero: the nonzero remainder would make the sum necessarily greater than zero, and the zero remainder would make the sum necessarily less than n. Hence the sequences are zero in precisely the same places. Finally, if corresponding terms in the two sequences are nonzero, they cannot sum to zero, and so must sum to n. ∎

Part of the appeal of Theorem 1 lies in its breadth: it applies to any fraction in any base, regardless of the behavior of the fraction's sequence of remainders. However, in order to have breadth, one often must sacrifice depth. If we consider more restricted classes of fractions, we will be able to prove several stronger, more penetrating results.

We can extend Theorem 1 significantly if we restrict ourselves to fractions and bases that produce purely repeating sequences of remainders—that is, those satisfying $(b, n) = 1$. Since the graphs of these fractions consist of a single repeated figure, beginning with any point in the cycle will yield the same image. Thus if c_1 is a term in the sequence of remainders for $\frac{a}{n}$ base b, then the sequence of remainders of $\frac{c_1}{n}$ base b will go through exactly the same cycle, beginning at c_1 instead of a. Hence the two fractions $\frac{a}{n}$ and $\frac{c_1}{n}$ will produce identical graphs. Similarly, if c_2 is a term in the sequence of remainders of $\frac{n-a}{n}$, then $\frac{c_2}{n}$ and $\frac{n-a}{n}$ will produce identical graphs. This corollary then follows immediately from Theorem 1:

COROLLARY 2. *Suppose b and n are relatively prime. If* $ab^i \equiv c_1 \pmod{n}$ *for some i and* $(n-a)b^j \equiv c_2 \pmod{n}$ *for some j, then* $\frac{c_1}{n}$ *and* $\frac{c_2}{n}$ *are rotational graph pairs in base b.*

For example, $2 \times 100 \equiv 10 \pmod{19}$ and $17 \times 10 \equiv 18 \pmod{19}$, so $\frac{10}{19}$ base 10 and $\frac{18}{19}$ base 10 are rotational graph pairs.

Although we will return to this limited class of fractions later, in the next section we enlarge our consideration to include all sequences of remainders that do not terminate. The discussion hinges on a different sort of symmetry in the graphical analysis graph of a fraction: a rotational symmetry of a single graph, rather than of one graph to another.

Rotational symmetry

Consider the following two very different images in FIGURE 4:

The lovely rotational symmetry present in the graphical analysis graph of $\frac{1}{7}$ base 10 is strikingly absent in the graph of $\frac{1}{37}$. One might wonder why: after all, both 7 and 37

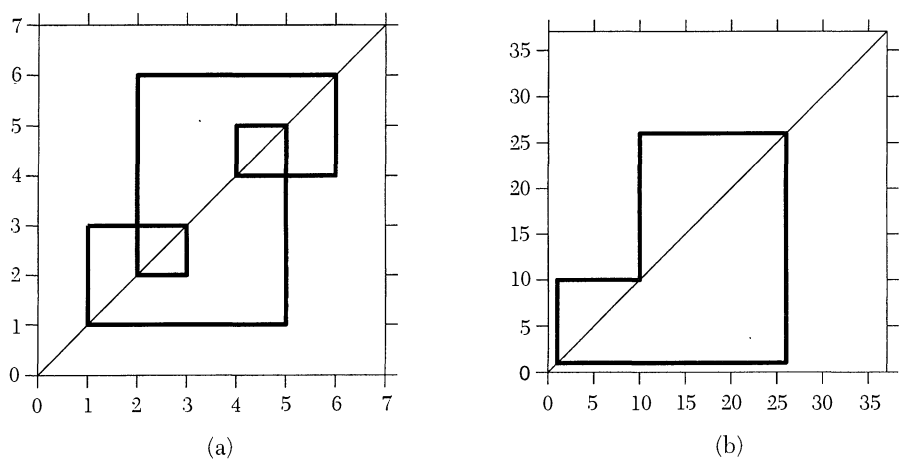


FIGURE 4
Graphical analysis of 1/7 base 10 vs. 1/37 base 10.

are not only relatively prime to 10, but also prime numbers. The following theorem will help to explain this difference.

THEOREM 3. *If* $(n, a) = 1$ *and* n *contains at least one prime factor that does not divide* b *then the following are equivalent*:

A. $n - a$ *appears in the sequence of remainders produced by the long division in base* b *of* $\frac{a}{n}$ (*i.e.*, $r_m = n - a$ *for some* m).
B. *There exists an* m, $0 < m < n$, *such that for each natural number* i, *we have* $r_i + r_{i+m} = n$.
C. *The graphical analysis graph of the function* $F_{b:n}$ *beginning with* $r_0 = a$ *has* 180° *rotational symmetry about the point* $\left(\frac{n}{2}, \frac{n}{2}\right)$.

Proof. We will show A $\Rightarrow$ B by induction on i. By hypothesis, $r_0 + r_m = a + (n - a) = n$, so induction begins. Assuming that $r_i + r_{i+m} = n$, we must show that $r_{i+1} + r_{i+m+1} = n$. Using the remainder function, we have

$$r_{i+1} + r_{i+m+1} = F_{b:n}(r_i) + F_{b:n}(r_{i+m}) = b \times r_i \pmod{n} + b \times r_{i+m} \pmod{n}$$
$$= b \times (r_i + r_{i+m}) \pmod{n} = b \times n \pmod{n} = 0.$$

Thus $r_{i+1} + r_{i+m+1} \equiv 0 \pmod{n}$. Since n contains at least one prime factor that does not divide b, the sequence of remainders of $\frac{a}{n}$ base b does not terminate, so no remainder can be zero. Therefore $0 < r_{i+1} + r_{i+m+1} < 2n$, implying that $r_{i+1} + r_{i+m+1} = n$.

We now turn to B $\Rightarrow$ C. Condition B guarantees the existence of some positive integer m such that $r_i + r_{m+i} = n$ for each i. Let s be the smallest such integer. Since $r_s + r_{2s} = n = r_s + r_0$, it follows that $r_0 = r_{2s}$, and thus the length of the repeating cycle of the sequence of remainders is $2s$. Furthermore, the cycle is composed of the two halves $r_0, r_1, \ldots, r_{s-1}$ and $r_s, r_{s+1}, \ldots, r_{2s-1}$. Since $r_i + r_{s+i} = n$ for each i, these halves are essentially rotational graph pairs, and thus the whole graph is rotationally symmetric by itself.

Finally we address C $\Rightarrow$ A. Condition C means that our graph is rotationally symmetric about $\left(\frac{n}{2}, \frac{n}{2}\right)$, and since $r_0 = a$, (a, a) must be a point on the graph. Because of the graph's symmetry, $(n - a, n - a)$ must also be a point on the graph, implying that $n - a$ is a term in the sequence of remainders. Thus $r_m = n - a$ for some m. ■

Remarks and observations

In the example given above, 36 is indeed nowhere to be found in the sequence of remainders for $\frac{1}{37}$ base 10, which is $1 \to 10 \to 26$, whereas 6 is the fourth number in the sequence for $\frac{1}{7}$ base 10. The equivalence of parts A and B thus predicts the visual discrepancy. In general, one need not go to the trouble of graphically analyzing a fraction to see if its graph is symmetric: it's enough to compute the sequence of remainders and examine it for a single number, $n - a$.

Interestingly, the symmetry among the remainders mentioned in part B of Theorem 3 is related to a similar symmetry among the digits. Suppose that the condition described in part B holds for a fraction $\frac{a}{n}$ in base b. The long division algorithm tells us that for each i, $b \times r_{i-1} = nd_i + r_i$ where d_i is the ith digit in the decimal

expansion of $\frac{a}{n}$ in base b. Thus $nd_i + nd_{i+m} = b(r_{i-1} + r_{i+m-1}) - (r_i + r_{i+m}) = bn - n$. This implies that $d_i + d_{i+m} = b - 1$ for each i, a symmetry that we noted regarding $\frac{1}{7}$ base 10. A similar argument shows that the symmetry of remainders follows from the symmetry of digits, implying that the two are inseparable.

Symmetries in fractions with $(b, n) = 1$

Already the subject of Corollary 2, this class of fractions and its subclass of fractions with prime denominators will prove worthy of close scrutiny. Members of the larger class share one outstanding quality: in a given base b, rotational symmetry depends only on the denominator of the fraction in question (provided, of course, that the fraction is reduced). We make this precise in the next theorem.

THEOREM 4. *Let $\frac{a}{n}$ be a reduced fraction in base b, where $(b, n) = 1$. Then the graphical analysis graph of $\frac{a}{n}$ is rotationally symmetric in base b if and only if the graphical analysis graph of $\frac{1}{n}$ is rotationally symmetric in base b.*

Proof. Suppose that the graphical analysis graph of $\frac{1}{n}$ is rotationally symmetric in base b. The formula $b^i \pmod n$ gives us the ith remainder of the long division of $\frac{1}{n}$ and $ab^i \pmod n$ gives us the ith remainder of the long division of $\frac{a}{n}$. Since $\frac{1}{n}$ is rotationally symmetric, by Theorem 3 we have $b^i \pmod n + b^{m+i} \pmod n = n$ for each i and for some m satisfying $0 < m < n$. Thus $b^i + b^{m+i} \equiv 0 \pmod n$. Multiplying through by a yields $ab^i + ab^{m+i} = an \equiv 0 \pmod n$, implying that $ab^i \pmod n + ab^{m+i} \pmod n = 0$ or n. Since $(b, n) = 1$, the sequence of remainders of $\frac{a}{n}$ base b does not terminate, and thus no remainders can be zero. We therefore conclude that $ab^i \pmod n + ab^{m+i} \pmod n = n$, proving the rotational symmetry of $\frac{a}{n}$ in base b.

The converse argument is quite similar. Supposing $ab^i \pmod n + ab^{m+i} \pmod n = n$ for all i and for some m, we clearly have $ab^i + ab^{m+i} \equiv 0 \pmod n$. We need only find a positive integer c such that $ca \equiv 1 \pmod n$, and we will be able to

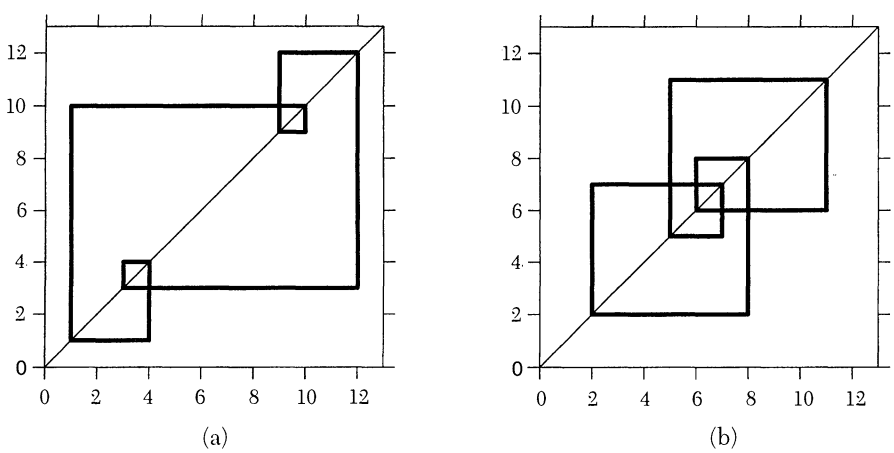


FIGURE 5
Graphical analysis of 1/13 base 10 vs. 5/13 base 10.

multiply through by c and complete the approach used above. Since our fraction is reduced, $(a, n) = 1$, so there exist positive integers c and d such that $ca + dn = 1$. This implies that $ca = 1 - dn \equiv 1 \pmod{n}$, so the desired positive integer does indeed exist. ■

This theorem guarantees that, for our limited class of fractions, if $\frac{1}{n}$ is rotationally symmetric in base b, then $\frac{a}{n}$ will be as well, provided $(a, n) = 1$. It often happens that $\frac{1}{n}$ and $\frac{a}{n}$ in fact produce identical graphs in base b; this is the case for $\frac{1}{7}$ and $\frac{a}{7}$ in base 10, where $(a, 7) = 1$. However, this need not happen, as FIGURE 5 shows.

Theorem 4 allows us to say that every reduced fraction with denominator n is either symmetric or not symmetric in any base b satisfying $(b, n) = 1$, since the value of the numerator plays no role. Thus for short, we will occasionally say simply that n is symmetric or not symmetric in base b.

The Euler totient function

We will be better able to understand symmetries in fractions with prime denominators with the aid of the *Euler totient function*. Denoted $\varphi(n)$, this function takes as input a positive integer n and produces as output the number of positive integers m that are less than or equal to n and satisfy $(m, n) = 1$. Some examples are $\varphi(4) = 2$, $\varphi(6) = 2$, $\varphi(12) = 4$, and, for any prime p, $\varphi(p) = p - 1$. The Euler totient function boasts two convenient properties which allow us to evaluate it easily for any small positive integer: First, if m and n are relatively prime positive integers, then $\varphi(mn) = \varphi(m)\varphi(n)$; and second, if p is prime and j is a positive integer, then $\varphi(p^j) = p^{j-1}(p - 1)$ [3]. Thus, $\varphi(12) = \varphi(2^2 3) = \varphi(2^2)\varphi(3) = 2(2 - 1)2 = 4$. One of the better known theorems involving the Euler totient function is as follows:

LEMMA 5. (EULER'S FORMULA). *If b and m are positive integers and $(b, m) = 1$, then $b^{\varphi(m)} \equiv 1 \pmod{m}$.*

In particular, if p is prime and a not a multiple of p, we have $a^{p-1} \equiv 1 \pmod{p}$. Given a fraction with a purely repeating sequence of remainders, it's natural to be curious about the length of the repeating cycle (also known as the sequence's *period*). Euler's formula gives us some information about this period. Suppose $a < m$ and $\frac{a}{m}$ base b has a purely repeating sequence of remainders; we noted earlier that this is the case if and only if $(b, m) = 1$. The first remainder r_0 in the sequence is $ab^0 = a$, so the period of the sequence is the smallest nonzero k such that $r_k = a$. In other words, the period is the smallest nonzero k such that $ab^k \equiv a \pmod{m}$. Since $(b, m) = 1$, Euler's formula tells us that $b^{\varphi(m)} \equiv 1 \pmod{m}$, and thus $ab^{\varphi(m)} \equiv a \pmod{m}$. Because the period is the smallest nonzero k with $ab^k \equiv a \pmod{m}$, and $\varphi(m)$ satisfies this congruence, it follows that the period must divide $\varphi(m)$. In the special case where p is prime and b is not a multiple of p, we have the useful fact that the period of the sequence of remainders of $\frac{a}{p}$ in base b divides $p - 1$.

Fractions with prime denominators

Consider for a moment a reduced fraction with a prime denominator p in a base b that is not a multiple of p. Clearly $(b, p) = 1$, so Theorem 4 applies, showing that the value of the numerator does not affect the symmetry of the fraction's graph. Thus to determine if p is symmetric in base b, it is enough to examine the behavior of $\frac{1}{p}$ in

base b. Although this is nice, we can use our restriction to fractions with prime denominators to get something even nicer: a convenient characterization of rotational symmetry.

Any reduced fraction with prime denominator p in a base b satisfying $(b, p) = 1$ must have a purely repeating sequence of remainders. The period of this sequence has everything to do with the rotational symmetry of the fraction: an even period means symmetry, an odd period no symmetry. We enshrine this convenient characterization in the following theorem:

THEOREM 6. *Let m be the smallest positive integer such that $b^m \equiv 1 \pmod{p}$, where p is an odd prime and $(b, p) = 1$. Then $\frac{1}{p}$ is rotationally symmetric in base b if and only if m is even.*

Proof. First note that because $(b, p) = 1$ and p is prime, it follows from Euler's formula that $b^{p-1} \equiv 1 \pmod{p}$, so there exists some positive integer satisfying $b^m \equiv 1 \pmod{p}$. Hence it makes sense to discuss the smallest such integer. Now suppose $\frac{1}{p}$ is rotationally symmetric in base b, and let c_1 be a term in the sequence of remainders of $\frac{1}{p}$ base b. Then for some i, $b^i \equiv c_1 \pmod{p}$. Since $0 < c_1 < p$, we have $(c_1, p) = 1$, so, by Theorem 6, $\frac{c_1}{p}$ must be rotationally symmetric in base b. Thus, by Theorem 3, $p - c_1$ must appear in the sequence of remainders of $\frac{c_1}{p}$ base b. Hence for some j, $c_1 b^j \equiv p - c_1 \pmod{p}$. Since $b^i \equiv c_1 \pmod{p}$, we have $b^{i+j} \equiv c_1 b^j \equiv p - c_1 \pmod{p}$, implying that $p - c_1$ is in the sequence of remainders of $\frac{1}{p}$ base b. Thus each remainder r in the repeating cycle of $\frac{1}{p}$ base b occurs together with $p - r$. Since p is odd, we cannot have $r = p - r$, so the elements of the cycle occur in distinct pairs. Hence the cycle length must be even. Given that the first remainder is $b^0 \pmod{p} = 1$, this means that the smallest positive integer satisfying $b^m \equiv 1 \pmod{p}$ is even.

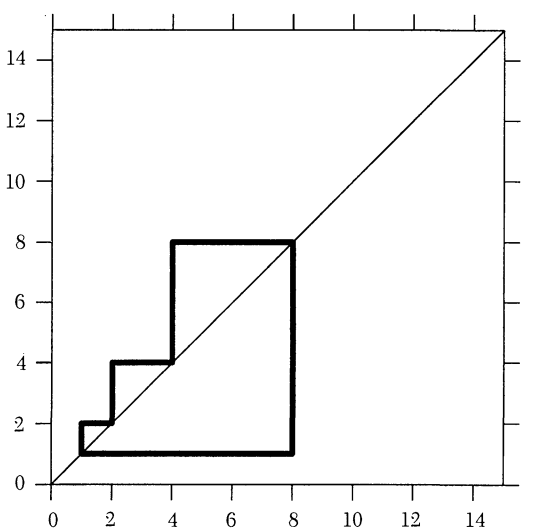


FIGURE 6
Graphical analysis of 1/15 base 2.

To show the converse, let m be the smallest positive integer satisfying $b^m \equiv 1 \pmod{p}$, and suppose m is even. Then $m = 2d$ for some positive integer d. Hence $b^m = b^{2d} = (b^d)^2 \equiv 1 \pmod{p}$. Thus $(b^d + 1)(b^d - 1) \equiv 0 \pmod{p}$ and since p is prime either $b^d \equiv 1 \pmod{p}$ or $b^d \equiv -1 \pmod{p}$. The first case is clearly impossible since $d = \frac{m}{2} < m$, and m was assumed to be the smallest positive integer such that $b^m \equiv 1 \pmod{p}$. Thus we conclude that $b^d \equiv -1 \equiv p - 1 \pmod{p}$. Therefore $p - 1$ is the dth remainder of $\frac{1}{p}$ base b, so by Theorem 3 $\frac{1}{p}$ is rotationally symmetric in base b. ∎

Note that p must be prime for the above theorem to hold. Consider FIGURE 6, which shows that $\frac{1}{15}$ base 2 is not symmetric, though $2^m \equiv 1 \pmod{15}$ gives us a smallest m of 4.

Counting bases that produce symmetry

One might be tempted to guess that a prime number is symmetric in some randomly distributed number of bases; delightfully, this is not so. As we noted earlier, to find the ratio of bases in which a prime p is symmetric, we need only consider a single base b from each congruence class mod p. We will be interested here only in the bases in which $\frac{1}{p}$ has a repeating sequence of remainders. Therefore our considered bases will be all bases except those in the 0 congruence class.

For example, the reciprocal of 19 is symmetric in 9 of the 18 bases between 2 and 20, excluding 19; thus it is symmetric in half of the considered bases. The reciprocals of many other prime numbers are also symmetric in $\frac{1}{2}$ of the considered bases; some examples are 3, 7, 11, 23, 31, and 59. Other primes have reciprocals that are symmetric in $\frac{3}{4}$ of the considered bases; the first few are 5, 13, 29, 37, and 61. Still other primes, including 41, 73, and 89, have reciprocals symmetric in $\frac{7}{8}$ of the considered bases. In fact, one can find prime numbers that are symmetric in $\frac{(2^n - 1)}{2^n}$ of the considered bases for many positive integers n. We can explain this separation of the prime numbers into families, but to do so we will need a couple of number-theoretic results. [For details, see for example **[3]**.]

LEMMA 7. *For any $n \geq 1$, we have $n = \sum_{d|n} \varphi(d)$ where the sum is taken over all divisors of n.*

LEMMA 8. *Let p be a prime number and d a positive divisor of $p - 1$. Then there are exactly $\varphi(d)$ numbers b that are incongruent* (mod p) *and have the property that d is the smallest positive integer satisfying $b^d \equiv 1 \pmod{p}$.*

To illustrate Lemma 8, let $p = 7$ and choose $d = 3$. Lemma 8 tells us that there are $\varphi(3) = 2$ possible bases b which are not congruent (mod 7) and have the property that while b^1 and b^2 are not congruent to 1 (mod 7), b^3 is congruent to 1 (mod 7). In other words, were we to compute the sequence of remainders for $\frac{1}{7}$ in one base from each of the seven congruence classes mod 7, we would find that exactly two of them produce a sequence of period 3. If we want to know how many will yield a sequence with period 6, we simply have to calculate $\varphi(6)$, which is 2. The same holds for any other divisor of 6. To find the number of these bases in which the graph of $\frac{1}{7}$ is rotationally symmetric, Theorem 6 tells us we need only determine in how many of

them $\frac{1}{7}$ has a sequence of remainders of even period. Since we ignore bases in the zero congruence class, all the bases we consider satisfy $(b, 7) = 1$. Since the period of $\frac{1}{7}$ in any of these bases must divide $\varphi(7) = 6$, the only possible even periods are 6 and 2. Thus our answer is $\varphi(6) + \varphi(2) = 3$, and we see that $\frac{1}{7}$ is symmetric in one half of the considered bases. This sort of analysis underlies the following proof.

THEOREM 9. *Suppose p is an odd prime number and n is the largest integer satisfying $2^n | p - 1$. Then, excluding bases $b \equiv 0 \pmod{p}$, $\frac{1}{p}$ is symmetric in $\frac{2^n - 1}{2^n}$ of the remaining bases.*

Proof. We need only consider a single representative base from each nonzero congruence class mod p. By Theorem 6, it suffices to find the number of bases in which $\frac{1}{p}$ produces a sequence of remainders of even period. The period of $\frac{1}{p}$ in any representative base must divide $\varphi(p) = p - 1$, so we want to find for each even divisor m of $p - 1$ the number of bases in which $\frac{1}{p}$ has a sequence of period m. Lemma 8 tells us that for a divisor q of $p - 1$, $\frac{1}{p}$ will produce a sequence of period q in exactly $\varphi(q)$ of the representative bases. Hence we need only compute $\Sigma\varphi(m)$, where m varies over the even divisors of $p - 1$. We will call the value of this sum k.

Suppose 2 divides $p - 1$ exactly n times. Then the prime factorization of $p - 1$ is $2^n p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}$, where each p_j is an odd prime. The largest odd divisor of $p - 1$ is thus $D = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}$. Now every even divisor m of $p - 1$ has the form $2^i t$, where $1 \le i \le n$ and t divides D. So we have

$$k = \sum_{i=1}^{n} \sum_{t|D} \varphi(2^i t).$$

Now since $t|D$ and D is odd, t must be odd. So $(2^i, t) = 1$ for any i, and by the first convenient property of the Euler function, we have $\varphi(2^i t) = \varphi(2^i)\varphi(t)$, so

$$k = \sum_{i=1}^{n} \sum_{t|D} \varphi(2^i)\varphi(t) = \sum_{i=1}^{n} \varphi(2^i) \sum_{t|D} \varphi(t).$$

By Lemma 7, $\Sigma_{t|D} \varphi(t) = D = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}$, so

$$k = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N} \sum_{i=1}^{n} \varphi(2^i).$$

Now $\Sigma_{i=1}^{n} \varphi(2^i) = \varphi(2) + \varphi(2^2) + \cdots + \varphi(2^n)$. By the second convenient property of the Euler function, the right side is $2^0(1) + 2^1(1) + 2^2(1) + \cdots + 2^{n-1}(1) = 2^n - 1$, so we have $\Sigma_{i=1}^{n} \varphi(2^i) = 2^n - 1$. Finally we arrive at our value for k:

$$k = (2^n - 1) p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}.$$

Since we are considering only a single base from each of the $p - 1$ nonzero congruence classes mod p, we have that $\frac{1}{p}$ is symmetric in

$$\frac{k}{p-1} = \frac{(2^n - 1) p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}}{2^n p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_N^{\alpha_N}} = \frac{2^n - 1}{2^n}$$

of the considered bases. ∎

COROLLARY 10. *Suppose p is an odd prime and D is the largest odd divisor of $p-1$. Then, excluding bases $b \equiv 0 \pmod{p}$, $\frac{1}{p}$ fails to be symmetric in $\frac{D}{p-1}$ of the remaining bases.*

Proof. Suppose 2 divides $p-1$ exactly n times. Applying Theorem 9 we get that $\frac{1}{p}$ *fails* to be symmetric in $1 - \frac{2^n - 1}{2^n} = \frac{1}{2^n}$ of all the considered bases. The prime factorization of $p-1$ is $2^n D$. Thus $\frac{1}{p}$ fails to be symmetric in $\frac{1}{2^n} = \frac{D}{2^n D} = \frac{D}{p-1}$ of the possible bases. ∎

We noted earlier that in a base of the form $ap+1$, where a is a positive integer, $\frac{1}{p}$ will have a sequence of remainders that is simply an infinite string of ones. This leads to a graph consisting only of the fixed point $(1,1)$. If $p=2$, this graph is in fact symmetric about $(\frac{p}{2}, \frac{p}{2})$, but for any odd prime it fails to be symmetric. Thus an odd prime must fail to be symmetric in all bases belonging to the 1 congruence class mod p. However, there exist odd primes that are symmetric in *all* of the other considered bases, and thus are as symmetric as it is possible for an odd prime to be.

Perfectly symmetric numbers and Fermat primes

DEFINITION. *A positive integer $n > 1$ is perfectly symmetric if its reciprocal is symmetric in any base b provided $b \not\equiv 0 \pmod{n}$ and $b \not\equiv 1 \pmod{n}$.*

Clearly, 2 is trivially perfectly symmetric. This membership in the set of perfectly symmetric numbers makes 2 a spectacularly rare positive integer, joined only by widely-spaced comrades:

THEOREM 11. *The only perfectly symmetric numbers are 2 and the Fermat primes.*

Proof. Recall that a Fermat prime is a prime of the form $2^{2^m} + 1$, where m is a natural number. Suppose n is a perfectly symmetric number, and suppose also that n is composite. Then there is some base b that divides n and satisfies $1 < b < n$. Clearly b and n are not relatively prime. So the sequence of remainders of $\frac{1}{n}$ in base b cannot be purely repeating: either it terminates or has an initial string of unrepeated remainders. In the latter case, the string of unrepeated digits creates a tail in the graphical analysis graph of $\frac{1}{n}$ base b, and the tail ruins any symmetry. In the former case, $n-1$ cannot appear in the sequence of remainders, for if it did, we would have $r_k = n-1$ for some nonzero k, implying that $r_{2k} = 1$. But the sequence of remainders terminates, so this is not possible. In either case n is not symmetric in base b, contradicting our assumption.

Therefore n must be prime. We have already seen that 2 is perfectly symmetric. If n is an odd prime, then, by Corollary 10, $\frac{1}{n}$ will fail to be symmetric in bases belonging to D of the $n-1$ nonzero congruence classes mod n, where D is the largest odd divisor of $n-1$. Any odd prime must fail to be symmetric in at least one of these base congruence classes, but since n is perfectly symmetric, it cannot fail in any of the others; therefore $D=1$. Thus no odd number greater than one can divide $n-1$, implying that $n-1$ is of the form 2^i for some i. Therefore $n = 2^i + 1$ and n is prime. If $i = uv$, where u is odd and $u > 1$, then $2^v + 1 | 2^i + 1$, so $2^i + 1$ fails to be prime. Thus in this case our i must be of the form 2^k, where $k \in \mathbb{N}$. Therefore our prime n is of the form $2^{2^k} + 1$, and is thus a Fermat prime.

Conversely, if n is either 2 or a Fermat prime, then clearly either $n = 2$, and is thus perfectly symmetric, or n is odd. In the latter case, by Corollary 10 we have that $\frac{1}{n}$ fails to be symmetric in bases belonging to D of the $n - 1$ nonzero congruence classes mod n, and must be symmetric in all the rest. Here $n - 1 = 2^i$, so $D = 1$. But the reciprocal of any number m must fail to be symmetric in bases belonging to the 1 congruence class mod m. Hence if $x > 1$ and $b \equiv x \pmod{n}$, $\frac{1}{n}$ is symmetric in base b. Therefore n is perfectly symmetric. ■

Currently there are only five known Fermat primes: 3, 5, 17, 257, and 65537. Thus, only six known perfectly symmetric numbers lurk among all the positive integers greater than one, suggesting that perfect symmetry is among the more unusual properties a number can have. However, precisely how many perfectly symmetric numbers exist remains an open question.

Questions and conclusions

Our discussion of the number of symmetry-producing bases for various fractions raises two questions about certain kinds of prime numbers:

Question 1. *Does there exist, for each positive integer n, a natural number k such that $2^n(2k + 1) + 1$ is prime?*

If so, then for any positive integer n one can find a prime p such that 2 divides $p - 1$ exactly n times. This would mean that for any positive integer n, primes exist that are symmetric in $\frac{2^n - 1}{2^n}$ of the considered bases.

Question 2. *How many Fermat primes are there?*

No one has any idea; we know only that there are at least five. Pierre de Fermat thought that all numbers of the form $2^{2^k} + 1$ were prime, but history has proven otherwise: All the numbers generated using $k = 5, \ldots, 11$ have turned out to be composite, as well as selected others, including the monstrous $2^{2^{23471}} + 1$. There remain, however, infinitely many more as-yet-undetermined possibilities. An answer to this question would also tell how many perfectly symmetric numbers exist.

Thus ends our exploration of fractions and symmetry. Postmodernism has taught us that all ways of looking at a problem are not equivalent: different perspectives highlight different properties. Adopting our society's penchant for images led us to examine more closely the symmetries of certain fractions, and opened our eyes to unexpected visions.

Note on the computer program During the course of this project, we wrote a simple computer program that graphically analyzes any fraction in any base. We found many of the images quite striking and beautiful, and were sorry not to be able to include all of them in this article. For those of you who would like to generate some of these images yourselves, our program is in an electronic supplement at `http://www.maa.org/pubs/mm_supplements/index.html`.

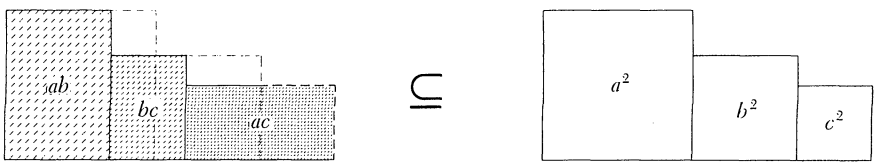
Acknowledgments. We would like to thank Dr. Mark Hanisch for his help with MATLAB, Dr. James Lynch for his interest and encouragement, the Reverend Kent Gilbert for moral support and occasional entertainment, and Dr. Libby Jones for timely sustenance.

REFERENCES

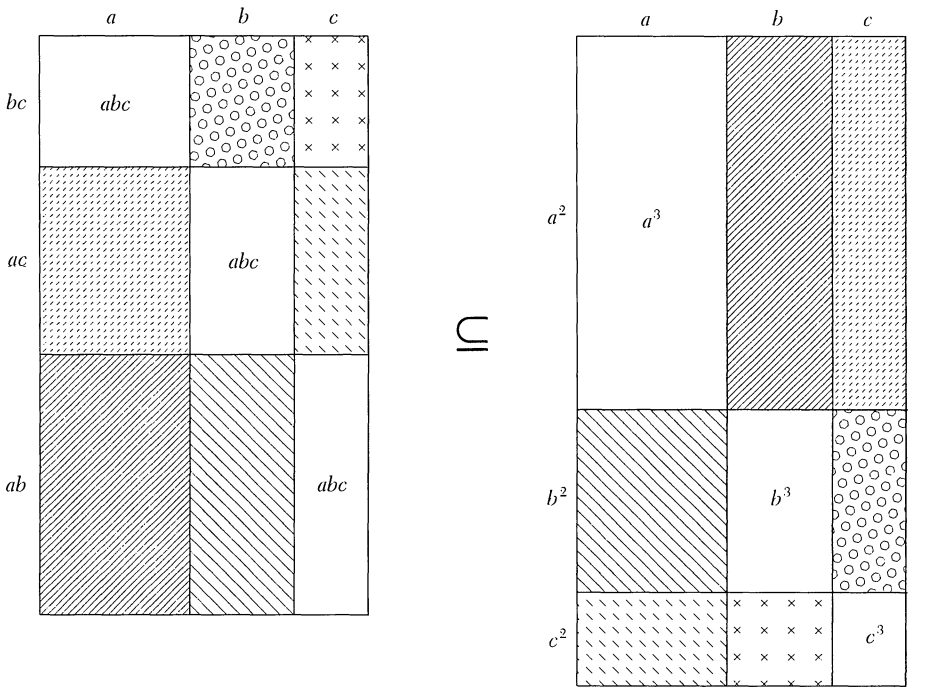
1. K. H. Becker and M. Dörfler, *Dynamical Systems and Fractals*, Cambridge University Press, Cambridge, UK, 1989.
2. R. Devaney, *Chaos, Fractals, and Dynamics*, Addison-Wesley, Reading, MA, 1990.
3. J. Silverman, *A Friendly Introduction to Number Theory*, Prentice-Hall, Upper Saddle River, NJ, 1997.

Proof Without Words: The Arithmetic–Geometric Mean Inequality for Three Positive Numbers

LEMMA 1. $ab + ac + bc \le a^2 + b^2 + c^2$



THEOREM. $3abc \le a^3 + b^3 + c^3$



—CLAUDI ALSINA
UNIVERSITAT POLITECNICA CATALUNYA
DIAGONAL 649, 08028 BARCELONA
SPAIN