Fixed Points and Fermat: A Dynamical Systems Approach to Number Theory
Author(s): Michael Frame, Brenda Johnson, Jim Sauerberg

Source: *The American Mathematical Monthly*, Vol. 107, No. 5 (May, 2000), pp. 422-428
Published by: Mathematical Association of America
Stable URL: http://www.jstor.org/stable/2695297
Accessed: 24/03/2010 21:33

Fixed Points and Fermat: A Dynamical Systems Approach to Number Theory

Michael Frame, Brenda Johnson, and Jim Sauerberg

Standard fare in undergraduate number theory courses usually includes Fermat's Little Theorem:

For every prime p and all positive integers a, $a^p \equiv a \pmod{p}$.

There are many proofs of this result; see [2] for some of them. It and related number-theoretic results are often used to establish facts about periodic points in dynamical systems [1, p. 119]. Our goal is to show at an elementary level how this process can be reversed: we use fixed and periodic point arguments to prove number-theoretic facts, including Fermat's Little Theorem. The idea of obtaining number theoretic results via dynamical systems is not new. For instance, Furstenberg has shown the arithmetic progression theorems of van der Waerden and of Szemeredi can be derived from generalizations of the recurrence theorems of Birkhoff and of Poincaré [4]. The results we present here are of a much more elementary nature.

Our new proof of Fermat's Little Theorem involves analyzing the fixed and periodic points of the following functions g_a. For each integer $a \geq 2$, let $g_a : [0,1] \to [0,1]$ be given by

$$g_a(x) = \begin{cases} a \cdot x & \text{for } 0 \leq x \leq \dfrac{1}{a} \\ a \cdot x - j & \text{for } \dfrac{j}{a} < x \leq \dfrac{j+1}{a} \end{cases} \tag{1}$$

for $1 \leq j \leq a - 1$. One could also identify the endpoints of the interval $[0,1]$ to create a circle, S^1, and define $g_a : S^1 \to S^1$ by

$$g_a(x) \equiv a \cdot x (\operatorname{mod} 1).$$

However definition (1) is easier to use in our fixed point arguments. Figure 1 shows the graphs of g_2 and g_3. To analyze the g_a we use the following ideas from dynamical systems.

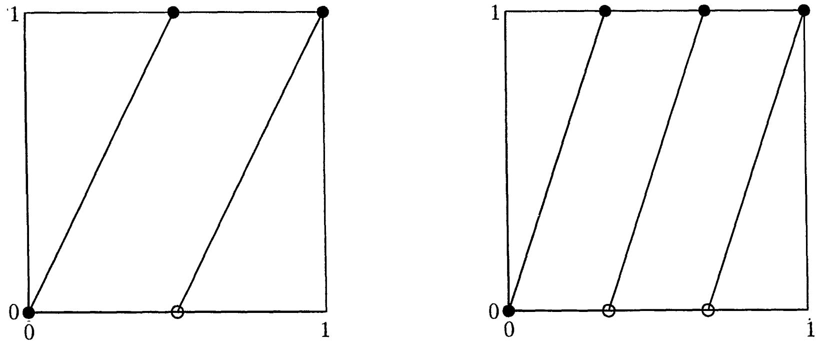

Figure 1. The graphs of g_2 and g_3.

Given a function $f:[0,1] \to [0,1]$, x is a *fixed point* of f if $f(x) = x$. To describe periodic points of the function, we use the n-fold composition of f with itself,

$$f^n = \overbrace{f \circ f \circ \cdots \circ f}^{\text{iterated } n \text{ times}}\ .$$

A *point of period n* is a point x for which $f^n(x) = x$. A *point of minimal period n* is a point x of period n such that $f^k(x) \neq x$ for all k, $0 < k < n$. We let $\mathcal{N}_n(f)$ denote the number of points of minimal period n, for the function f; we drop the f when the function is clear from context. Associated with each point $x \in [0,1]$ is its *orbit*, $\{x, f(x), f^2(x), \dots\}$. If x has period n, then the orbit of x contains at most n distinct elements. Such orbits are called *n-cycles*. If x has minimal period n, then the orbit of x contains n distinct elements: $x, f(x), f^2(x), \dots, f^{n-1}(x)$. Such orbits are called *minimal n-cycles*.

One can locate fixed points as points of intersection of the graph of f and the diagonal line $y = x$. One can also determine the orbit of a value geometrically by "graphical iteration"; see [3]. Starting at the point (x_0, x_0) on the diagonal, one draws a vertical line segment from (x_0, x_0) to the point $(x_0, f(x_0)) = (x_0, x_1)$ on the graph of f. From this point on the graph of f one draws a horizontal line segment to the diagonal to obtain a new point (x_1, x_1). Repeating this procedure generates a sequence of points $(x_0, x_0), (x_1, x_1), \dots, (x_k, x_k), \dots,$ where $x_{k+1} = f(x_k)$: this is the orbit of x_0. If x_0 is a point of period n, then this sequence repeats itself after n steps, and the points $x_0, x_1, \dots, x_{n-1}$ constitute an n-cycle; see Figure 2.

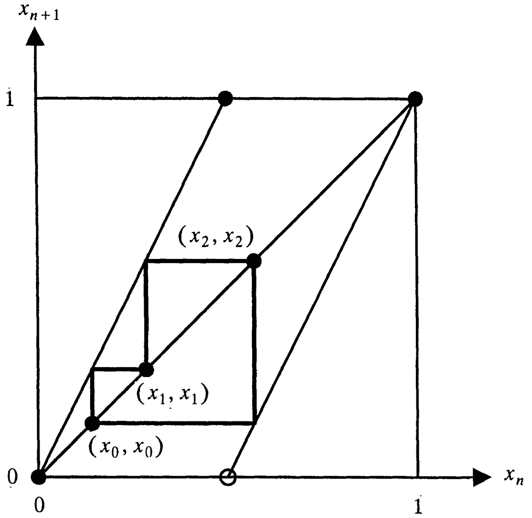

Figure 2. Graphical iteration of g_2 and a 3-cycle.

Our first lemma contains the essential ingredients for our proofs of Fermat's Little Theorem and some of its relatives using periodic points.

Lemma 1.

(*i*) *If x_0 is a point of period n that has minimal period m, then $m \mid n$.*
(*ii*) *Two minimal m-cycles are either disjoint or identical.*
(*iii*) *For all $m \geq 1$, $m \mid \mathcal{N}_m$ whenever $\mathcal{N}_m$ is finite.*

Proof: Let x_0 be a point of minimal period m, and consider the minimal m-cycle $\{x_0, x_1, \ldots, x_{m-1}\}$. The sequence of points $x_i, f(x_i), f^2(x_i), \ldots, f^{m-1}(x_i)$ is completely determined for any of the x_i in the m-cycle, and is simply a reordering of the elements in the original m-cycle. This proves (ii).

To prove (i), consider the sequence $x_0, f(x_0), \ldots, f^{m-1}(x_0), \ldots, f^n(x_0)$. It is clear that the first m points in this n-cycle are the points of the minimal m-cycle, and because $f^m(x_0) = x_0$, the sequence repeats itself every m steps. Thus in order for $f^n(x_0)$ to equal x_0, we must have $m \mid n$ because the points $x_0, \ldots, x_{m-1}$ are distinct.

To prove (iii), note that the points of minimal order m are partitioned into m-cycles, disjoint by (ii). Because each minimal m-cycle contains exactly m points, and the number of cycles is an integer, we have $m \mid \mathcal{N}_m$. ■

Figure 3 illustrates some of these ideas.

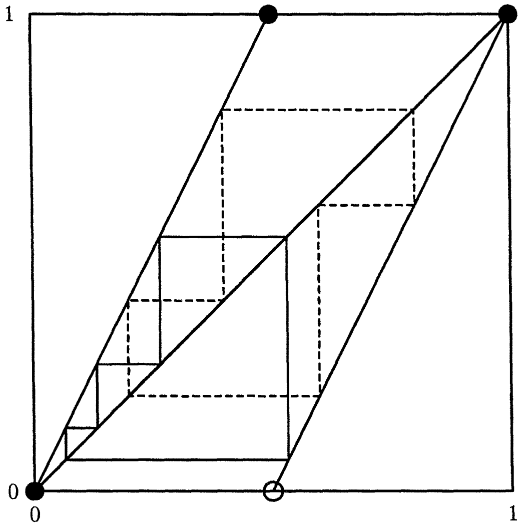

Figure 3. Two (disjoint) 4-cycles for g_2.

Our analysis depends on counting the periodic points of g_a:

Lemma 2.

(*i*) *The function* g_a *has* a^n *points of period* n.

(*ii*) *For all integers* $a > 1$ *and all integers* $n \geq 1$, $a^n = \sum_{m \mid n} \mathcal{N}_m(g_a)$.

Proof: The points of period n are the fixed points of g_a^n. But,

$$g_a^n(x) = \begin{cases} a^n \cdot x & \text{for } 0 \leq x \leq \dfrac{1}{a^n} \\ a^n \cdot x - j & \text{for } \dfrac{j}{a^n} < x \leq \dfrac{j+1}{a^n}, \end{cases}$$

for $1 \leq j \leq a^n - 1$. Thus, the graph of g_a^n consists of a^n line segments of slope a^n. As a consequence, the diagonal intersects this graph in a^n points, giving us a^n fixed points for g_a^n. Hence g_a has a^n n-periodic points.

By Lemma 1 the points of period n are points of minimal period m for some $m \mid n$. Part (ii) now follows from part (i). ■

Now we are ready to use dynamical systems ideas to prove a standard result from number theory.

Theorem 1. *For all integers $a \geq 2$ and all primes p, $a^p \equiv a \pmod{p}$.*

Proof: By Lemma 2, $a^p = \mathcal{N}_1 + \mathcal{N}_p = a + \mathcal{N}_p$. Hence $a^p - a = \mathcal{N}_p$, which is divisible by p by Lemma 1. Thus $a^p \equiv a \pmod{p}$. ■

Hence, Fermat's Little Theorem, for $a \geq 2$, is a simple consequence of counting fixed points of g_a^p.

Some texts state the next result as Fermat's Little Theorem. It follows from Theorem 1 by noting that $a^p - a = a(a^{p-1} - 1)$ and imposing the condition that p does not divide a.

Corollary 1. *For all integers $a \geq 2$ and all primes p such that p does not divide a, $a^{p-1} \equiv 1 \pmod{p}$.*

By using arguments similar to those in the proof of Theorem 1, one can prove the following generalizations of Fermat's Little Theorem for certain types of composites.

Theorem 2.

(*i*) *Let p and q be distinct primes and $a \geq 2$. Then $pq \mid (a^{pq} - a^p - a^q + a)$.*

(*ii*) *Let p be a prime and $a \geq 2$ be an integer. Then p^k divides $a^{p^k} - a^{p^{k-1}}$ for all $k \geq 1$.*

Euler generalized Fermat's Little Theorem to composite numbers. His result, known as Euler's theorem, states that if n is any positive integer relatively prime to a, then $a^{\phi(n)} \equiv 1 \pmod{n}$, where $\phi(n)$ is the number of positive integers not exceeding n that are relatively prime to n. Standard results about $\phi(n)$ include $\phi(p^r) = p^r - p^{r-1}$ for prime p, and $\phi(ab) = \phi(a)\phi(b)$, when a and b are relatively prime; we do not know of any dynamical explanations of these results. With these facts and Theorem 2, we can deduce Euler's theorem: for $n = \prod_i p_i^{r_i}$,

$$a^{\phi(n)} = a^{\prod_i \phi(p_i^{r_i})} = a^{\prod_i (p_i^{r_i} - p_i^{r_i - 1})}$$

But by Theorem 2, $p_i^{r_i} \mid a^{p_i^{r_i-1}}(a^{p_i^{r_i} - p_i^{r_i-1}} - 1)$ and if a and p_i are relatively prime,

$$p_i^{r_i} \big| \left(a^{p_i^{r_i} - p_i^{r_i - 1}} - 1 \right).$$

Then $a^{\prod_j (p_j^{r_j} - p_j^{r_j - 1})} \equiv 1 \pmod{p_i^{r_i}}$ for each i. Since the p_i's are relatively prime, Euler's theorem follows.

Our final results involve determining the locations, not simply the number, of periodic points of g_a. As observed in the proof of Lemma 2, the graph of g_a^n consists of a^n straight line segments, each of slope a^n. We can use similar triangles to find the coordinates of the fixed points of g_a^n, hence of the periodic points of g_a. Figure 4 illustrates the case for $a = 2$ and $n = 2$.

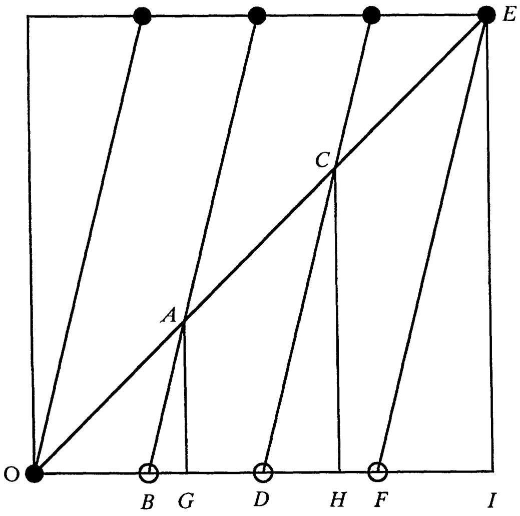

Figure 4. Finding the coordinates of periodic points of g_a by similar triangles.

Remark 1. Observe that $\triangle OAB \sim \triangle OCD \sim \triangle OEF$. From the definition of g_a^n we see that $OB = BD = DF$, so $OA = AC = CE$. This implies $\triangle OAG \sim \triangle OCH \sim \triangle OEI$, from which we see that $OG = GH = HI$. That is, successive fixed points of g_a^n are separated by the same distance. We now use this idea to determine the n-periodic points of g_a precisely, and establish two additional number-theoretic results.

Proposition 1.

(*i*) *The n-periodic points of* g_a *are* $j/(a^n - 1)$ *for* $j = 0, \dots, a^n - 1$.

(*ii*) *If* $\gcd(j, a^n - 1) = 1$, *then* $j/(a^n - 1)$ *is a minimal n-periodic point of* g_a.

Proof: The similar triangle argument in Remark 1 shows that the fixed points of g_a^n must be evenly spaced. As indicated in the proof of Lemma 2, we know there are a^n such points. Since the first and last fixed points are 0 and 1 and the points are evenly spaced, it follows that the fixed points are $j/(a^n - 1)$ for $0 \le j \le a^n - 1$. This proves (i).

Moreover, it must be the case that $j/(a^n - 1)$ is a point of minimal period n if j and $a^n - 1$ are relatively prime. Otherwise, being a point of lower minimal period would require that $j/(a^n - 1)$ could be reduced to a fraction with a smaller denominator of the form $a^k - 1$. This proves (ii). ■

We use Proposition 1 to prove the next result, which is often used in the construction of finite fields [5, p. 82].

Corollary 2. *Let* m, n, a *be integers such that* $m, n \ge 1$ *and* $a \ge 2$. *Then* $m \mid n$ *if and only if* $a^m - 1 \mid a^n - 1$.

Proof: Suppose $m \mid n$ and consider $x_0 = 1/(a^m - 1)$. By Proposition 1, x_0 is a point of minimal period m for g_a, and since $m \mid n$, x_0 is also a point of period n. Thus

$$\frac{1}{a^m - 1} = x_0 = \frac{j}{a^n - 1}$$

for some integer j and so $a^m - 1 \mid a^n - 1$.

Conversely, suppose that $a^m - 1 \mid a^n - 1$ and again consider $x_0 = 1/(a^m - 1)$. By Proposition 1, x_0 is a point of minimal period m. Since $a^m - 1 \mid a^n - 1$, we have

$$x_0 = \frac{1}{a^m - 1} = \frac{k}{a^n - 1}$$

for some integer k. Proposition 1 ensures that x_0 is an n-periodic point, and since x_0 is a minimal m-periodic point, it must be the case that $m \mid n$ by part (i) of Lemma 1. ■

Using Proposition 1, we can partition the n-periodic points into classes by a simple divisibility condition.

Proposition 2. *If $j_1/(a^n - 1)$ and $j_2/(a^n - 1)$ belong to the same n-cycle, then* $\gcd(j_1, a^n - 1) = \gcd(j_2, a^n - 1)$.

Proof: Consider $x_i = j/(a^n - 1)$. Then the numerator of x_{i+1} is $a \cdot j - l \cdot (a^n - 1)$ for some l, $0 \leq l < a$. Then $\gcd(a \cdot j - l \cdot (a^n - 1), a^n - 1) = \gcd(a \cdot j, a^n - 1) = \gcd(j, a^n - 1)$, as desired. ■

For example, consider the minimal 4-cycles for g_2. There are three such cycles,

$$\left\{\tfrac{1}{15}, \tfrac{2}{15}, \tfrac{4}{15}, \tfrac{8}{15}\right\}, \left\{\tfrac{7}{15}, \tfrac{14}{15}, \tfrac{13}{15}, \tfrac{11}{15}\right\}, \text{and } \left\{\tfrac{3}{15}, \tfrac{6}{15}, \tfrac{12}{15}, \tfrac{9}{15}\right\}.$$

In the first two 4-cycles, the numerators and denominators have a greatest common divisor of 1, in the third, a greatest common divisor of 3.

Our final result can be proved using ideas from group theory, but it is also a consequence of Propositions 1 and 2. Recall that $\phi(n)$ is the number of positive integers not exceeding n that are relatively prime to n.

Corollary 3. *For any integers $a \geq 2$ and $n \geq 1$, $n \mid \phi(a^n - 1)$.*

Proof: Consider the points $j/(a^n - 1)$ for which $\gcd(j, a^n - 1) = 1$. By part (ii) of Proposition 1 these points generate minimal n-cycles, and by Proposition 2 these points are the only points in such minimal n-cycles. By the greatest common divisor condition, we know that there are a total of $\phi(a^n - 1)$ points in these minimal n-cycles. Since each minimal n-cycle contains n distinct points, it follows that $n \mid \phi(a^n - 1)$. ■

REFERENCES

1. W. E. Briggs and W. L. Briggs, Anatomy of a Circle Map, *Math. Magazine* **72** (1999) 116–125.
2. D. Burton, *Elementary Number Theory*, McGraw-Hill, New York, 1998.
3. R. Devaney, *A First Course in Chaotic Dynamical Systems. Theory and Experiment*, Addison-Wesley, Reading, MA, 1992.
4. H. Furstenberg, Poincare recurrence and number theory, *Bull. Amer. Math. Soc.* **5** (1981) 211–234.
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.

MICHAEL FRAME received a B.S. from Rensselaer Polytechnic Institute in 1973 and a Ph.D. from Tulane University in 1978. Since 1987 he has been a member of the mathematics department at Union College, and has held several visiting appointments in the mathematics department at Yale University. His principal research interests are geometric topology and fractal geometry, and for over a decade he has been teaching fractal geometry as an introduction to science for liberal arts students.
Union College, Schenectady, New York, 12308-2311
framem@union.edu

BRENDA JOHNSON received a B.A. from Grinnell College in 1985 and a Ph.D. from Brown University in 1991. Since 1992 she has been a member of the mathematics department at Union College. Her principal research interests are in algebraic topology, particularly homotopy theory.
Union College, Schenectady, New York, 12308-2311
johnsonb@union.edu

JIM SAUERBERG received his B.S. from the University of Wisconsin in 1988 and his Ph.D. from Brown University in 1993. After spending three years under the tutelage of his co-authors at Union College, he moved to Saint Mary's College of California. His current interests include the marginal (and tiring) results of procreation.
St. Mary's College, P.O. Box 3517, Moraga, CA 94575-3517
jim@gauss.stmarys-ca.edu

Note added in proof. A proof similar to our proof of Theorem 1 has appeared recently in Lionel Levine, Fermat's Little Theorem: A Proof by Function Iteration, *Math. Magazine* 72 (1999) 308–309. The dynamical aspects of the approach are emphasized differently in Levine's paper and ours, and the results in the latter parts of the two papers diverge.