

# 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 examples.) It and related number-theoretic results are often used to establish facts about periodic points in dynamical systems. (See, for example, [1], p. 119.) Our goal in this paper 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 [4] has shown the arithmetic progression theorems of van der Waerden and of Szemerédi can be derived from generalizations of the recurrence theorems of Birkhoff and of Poincaré. The results we present here are of a much more elementary nature.

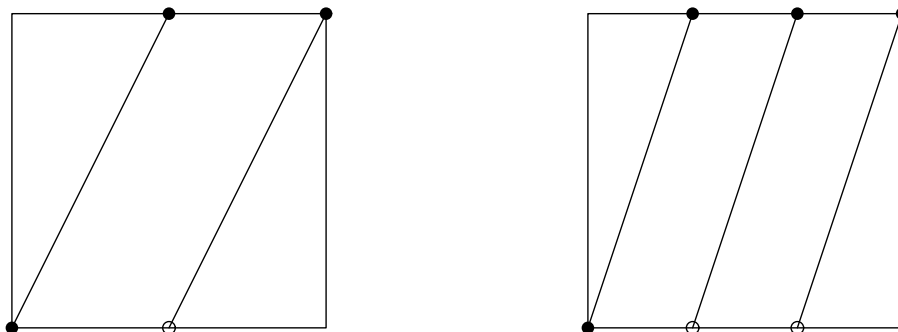
Our new proof of Fermat's little theorem will involve analyzing the fixed and periodic points of the functions  $g_a$  defined here. For each integer  $a \geq 2$ , let  $g_a : [0, 1] \rightarrow [0, 1]$  be given by

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

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  $g_a : S^1 \rightarrow S^1$  by

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

However the previous definition will be easier to use in the fixed point arguments that we wish to make. Figure 1 shows the graphs of  $g_2$  and  $g_3$ . To analyze the  $g_a$  we use the following ideas from dynamical systems.



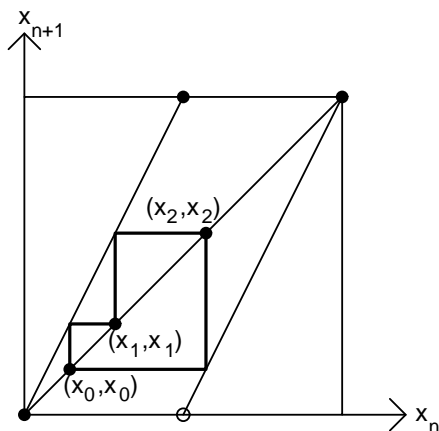
**Figure 1.** The graphs of  $g_2$  and  $g_3$ .

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

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

A *point of period  $n$*  is a point for which  $f^n(x) = x$ . A *point of minimal period  $n$*  is a point of period  $n$  such that  $f^k(x) \neq x$  for all  $k$ ,  $0 < k < n$ . We will let  $\mathcal{N}_n(f)$  denote the number of points of minimal period  $n$ , for the function  $f$ . (We will 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  $x_{k+1} = f(x_k)$ . In other words, one obtains the orbit of  $x_0$ . If  $x_0$  is a point of period  $n$ , then this sequence will repeat 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 periodic point proofs of Fermat’s little theorem and some of its relatives.

**Lemma 1.**

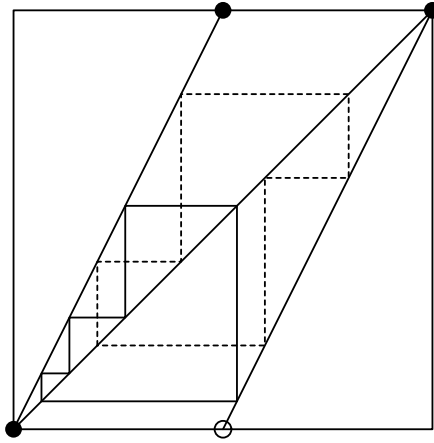
- (i) If  $x_0$  is a point of period  $n$  that has minimal period  $m$ , then  $m|n$ .
- (ii) Two minimal  $m$ -cycles are either disjoint or identical.
- (iii) For all  $m \geq 1$ ,  $m|\mathcal{N}_m$  whenever  $\mathcal{N}_m$  is finite.

*Proof:* Let  $x_0$  be a point of minimal period  $m$ , and consider the minimal  $m$ -cycle  $\{x_0, x_1, \dots, x_{m-1}\}$ . The sequence of points  $x_i, f(x_i), f^2(x_i), \dots, f^{m-1}(x_i)$  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  $x_0, f(x_0), \dots, f^{m-1}(x_0), \dots, f^n(x_0)$ . 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  $m|n$  because the points  $x_0, \dots, x_{m-1}$  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 there is an integer number of cycles, we have  $m|\mathcal{N}_m$ . ■

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  $n \geq 1$ ,  $a^n = \sum_{m|n} \mathcal{N}_m(g_a)$ .

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

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

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  $m|n$ . Part (ii) now follows from part (i). ■

Now we are ready to give a dynamical systems proof of 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  $p \nmid a$ ,  $a^{p-1} \equiv 1 \pmod{p}$ .

By using arguments similar to the proof of Theorem 1, one can prove the following generalizations of Fermat's little theorem for certain types of composites. We leave the proofs as exercises for the interested reader.

**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  $k \geq 1$ .

Recall that Euler generalized Fermat's little theorem for all composite numbers. Known as Euler's theorem, this result 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. (At present, we do not know of any dynamical equivalents of these results.) With these facts and Theorem 2, we can deduce Euler's theorem: for  $n = \prod_i p_i^{r_i}$ ,

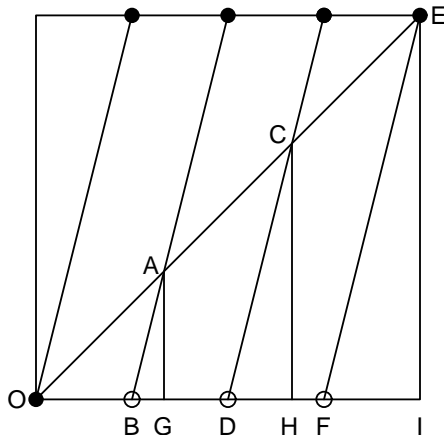
$$\begin{aligned} a^{\phi(n)} &= a^{\prod_i \phi(p_i^{r_i})} \\ &= a^{\prod_i (p_i^{r_i} - p_i^{r_i-1})} \end{aligned}$$

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,

$$p_i^{r_i} \mid (a^{p_i^{r_i} - p_i^{r_i-1}} - 1).$$

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.

First, note  $\triangle OAB \sim \triangle OCD \sim \triangle OEF$ . From the definition of  $g_a^n$  we see  $OB = BD = DF$ , so  $OA = AC = CE$ . This implies  $\triangle OAG \sim \triangle OCH \sim \triangle OEI$ , from which we see  $OG = GH = HI$ . 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  $\frac{j}{a^n - 1}$  for  $j = 0, \dots, a^n - 1$ .
- (ii) If  $\gcd(j, a^n - 1) = 1$ , then  $\frac{j}{a^n - 1}$  is a minimal  $n$ -periodic point of  $g_a$ .

*Proof:* The similar triangle argument above 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  $\frac{j}{a^n - 1}$  for  $0 \leq j \leq a^n - 1$ . This proves (i).

Moreover, it must be the case that  $\frac{j}{a^n - 1}$  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  $\frac{j}{a^n - 1}$  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 (see [5], p. 82).

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

*Proof:* Suppose  $m|n$  and consider  $x_0 = \frac{1}{a^m - 1}$ . By Proposition 1,  $x_0$  is a point of minimal

period  $m$  for  $g_a$ , and since  $m|n$ ,  $x_0$  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  $a^m - 1|a^n - 1$ .

Conversely, suppose that  $a^m - 1|a^n - 1$  and again consider  $x_0 = \frac{1}{a^m - 1}$ . By Proposition 1,  $x_0$  is a point of minimal period  $m$ . Since  $a^m - 1|a^n - 1$ , we have

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

for some integer  $k$ . It follows by Proposition 1 that  $x_0$  is an  $n$ -periodic point, and since  $x_0$  is a minimal  $m$ -periodic point, it must be the case that  $m|n$  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  $\frac{j_1}{a^n - 1}$  and  $\frac{j_2}{a^n - 1}$  belong to the same  $n$ -cycle, then  $\gcd(j_1, a^n - 1) = \gcd(j_2, a^n - 1)$ .

*Proof:* Consider  $x_i = \frac{j}{a^n - 1}$ . 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,  $\{\frac{1}{15}, \frac{2}{15}, \frac{4}{15}, \frac{8}{15}\}$ ,  $\{\frac{7}{15}, \frac{14}{15}, \frac{13}{15}, \frac{11}{15}\}$ , and  $\{\frac{3}{15}, \frac{6}{15}, \frac{12}{15}, \frac{9}{15}\}$ . 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.

Finally, the last result can be proved using ideas from group theory, but is also a direct consequence of the previous two propositions. 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  $n \geq 1$ ,  $n|\phi(a^n - 1)$ .

*Proof:* Consider the points  $\frac{j}{a^n - 1}$  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  $n|\phi(a^n - 1)$ . ■

## 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, 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

Union College, Schenectady, New York, 12308-2311, USA  
framem@union.edu

Brenda Johnson

Union College, Schenectady, New York, 12308-2311, USA  
johnsonb@union.edu

Jim Sauerberg

St. Mary's College, P.O. Box 3517, Moraga, CA 94575-3517, USA  
jim@gauss.stmarys-ca.edu