Unifying Two Proofs of Fermat's Little Theorem

Article *in* Mathematics Magazine · April 2015

DOI: 10.4169/math.mag.88.2.152

1 author:

Massimo Galuzzi
University of Milan
29 PUBLICATIONS **79** CITATIONS

SEE PROFILE

Unifying Two Proofs of Fermat's Little Theorem

MASSIMO GALUZZI
Dipartimento di Matematica
Università Statale di Milano
Via Saldini, 50 - 20133 Milano
galuzzim@gmail.com

Two interesting papers in this MAGAZINE [**2, 3**] have proposed unusual proofs of a famous result of Fermat.

Fermat's Little Theorem. *If $n \in \mathbb{N}$ and p is prime, then*

$$n^p - n \equiv 0 \pmod{p}.$$

It may be worthwhile to observe that the two proofs can be simplified and generalized with the help of a simple lemma. We begin with a definition.

Definition. Given a set S and a function $\varphi : S \to S$, we consider the iterates φ, $\varphi(\varphi)$, $\varphi(\varphi(\varphi))$, ... A point x is called *k-periodic* if

$$\underbrace{\varphi(\varphi(\cdots(\varphi}_{k \text{ times}}(x)))) = x,$$

where k is the number of iterations.

Lemma. *Let S be a set, and suppose that a family of functions $f_n : S \to S$, indexed by $n \geq 2$, has the following properties:*

- *For every n the function f_n has exactly n fixed points in S;*
- *For every n, m we have $f_n(f_m) = f_{nm}$.*

Then, given $n \geq 2$ and p prime, the number of p-periodic points of f_n is exactly $n^p - n$.

Proof. The number of fixed points of f_{n^p} is n^p, and we have to subtract the number of fixed points of f_n, which is n, to obtain the number of p-periodic points of f_n. ■

Assuming that such a family exists, we can now prove Fermat's little theorem.

Proof. We assume the existence of a family of functions as described in the lemma. Let n, p be as before.

The function f_n acts as a permutation on the fixed points of f_{n^p} so those that are not also fixed points of f_n must be in disjoint orbits of length p. The number of orbits of length p is given by

$$\frac{n^p - n}{p}.$$

Since this number is an integer, we conclude that p divides $n^p - n$. ■

Math. Mag. **88** (2015) 152–153. doi:10.4169/math.mag.88.2.152.
MSC: 11A25, 11B75

So everything depends on the existence of a family of functions with the properties given in the lemma. The papers mentioned at the beginning offer two possibilities, and the existence of these families allows us to conclude the proof.

In Levine's paper [**3**], the domain is $S = \mathbb{C}$ and the family of functions is given by $f_n(z) = z^n$, for $z \in \mathbb{C}$.

In Iga's paper [**2**], the domain is $S = [0, 1]$ and the family is given by

$$T_n(x) = \begin{cases} \{nx\} & \text{if } x \in [0, 1), \text{ and} \\ 1 & \text{if } x = 1, \end{cases}$$

where $x \in [0, 1]$ and $\{nx\}$ denotes the fractional part of nx.

Another family that has the properties described in the lemma consists of the Chebyshev polynomials. The main properties of these polynomials are described by Rivlin [**4**]. They are defined recursively by

$$\begin{aligned} T_0(x) &= 1, \\ T_1(x) &= x, \\ T_{n+1}(x) &= 2xT_n(x) - T_{n-1}(x). \end{aligned}$$

These polynomials satisfy the identity $T_n(T_m) = T_{nm}$, and when $n \geq 2$, the polynomial T_n has n fixed points in the domain $S = [-1, 1]$. So these polynomials may be used to obtain another proof of Fermat's little theorem.

The situation analyzed in the preceding lemma is similar to the one of Lemma 1 of [**1**], in which Fermat's little theorem is proved by counting certain necklaces. We are given a function $f : S \to S$, where S is a finite set (of objects), such that $f^{(p)}(x) = x$ for every x in S, where $f^{(p)}$ is the p-fold composition of f and p is a prime number.

It is proved that $|S| = |F| \bmod p$, where F is the set of fixed points of f. In this proof, the domain of f is different for each pair (n, p).

REFERENCES

1. P. G. Anderson, A. T. Benjamin, J. A. Rouse, Combinatorial proofs of Fermat's, Lucas's, and Wilson's theorems, *Amer. Math. Monthly* **112** (2005) 266–268. http://dx.doi.org/10.2307/30037444
2. K. Iga, A dynamical systems proof of Fermat's little theorem, *Math. Mag.* **76** (2003) 48–51, http://dx.doi.org/10.2307/3219132
3. L. Levine, Fermat's Little Theorem: A proof by function iteration, *Math. Mag.* **72** (1999) 308–309, http://dx.doi.org/10.2307/2691226
4. T. J. Rivlin, *The Chebyshev Polynomials*. Second edition. John Wiley, New York, 1990.

Summary. A new simple proof of Fermat's little theorem is given that generalizes the proofs given in this MAGAZINE by Levine (1999) and Iga (2003).

MASSIMO GALUZZI (MR Author ID: 243363) after retirement, became an adjunct professor of History of Mathematics at the Department of Mathematics at the Università Statale di Milano. He is the author of many articles about the mathematical contents of the work of, among others, Descartes, Newton, and Galois.