APORTACIONES MATEMÁTICAS
Serie Comunicaciones **22** (1998) 63–65

A dynamical systems proof of the little theorem of Fermat

Humberto Carrillo[1] **and José Ramón Guzmán**[2]

[1] Laboratorio de Dinamica No Lineal
Facultad de Ciencias, UNAM
e-mail: carr@servidor.unam.mx

[2] Instituto de Investigaciones Económicas, UNAM
e-mail: jrguzman@economiah2.torre2.unam.mx

Abstract. We use Möbius inversion theorem to count the number of periodic orbits of a family of dynamical systems in the circunference and derive a formula that allows to prove the following Fermat's theorem: If a is an integer number and p a prime number that is not a factor of a then

$$a^{p-1} \equiv 1 \bmod (p)$$

1. In Section 2 we recall a classic result of Number Theory: The Möebius inversion theorem. In Section 3 we associate to Fermat's problem a one parameter family of dynamical systems that is generated by linear expansions of the circunference. Using the Möebius inversion theorem to count the number of periodic orbits of a given period, we derive a formula from which it follows the theorem of Fermat. Simple and elementary proofs of this, so called "Little theorem of Fermat" are well known, but the connection that our proof shows between Number and Dynamical Systems theory is quite interesting, besides, the proof's method might be inspiring to prove other unknown Number Theory results or conjetures.

2. The Möebius function $\mu: \mathbf{N} \to \mathbf{N}$ is defined as follows

$$\begin{aligned}\mu(n) &= 1 && \text{if } n = 1,\\ &= 0 && \text{if exist } p \in \mathbf{N} \text{ such that } p^2 \mid n\\ &= (-1)^k, && \text{if } n = p_1 p_2 \ldots p_k \text{ with } p_i \text{ prime}.\end{aligned}$$

1991 Mathematics Subject Classification: 11, 58.

Assume that f is any function from the natural numbers and that $F\colon \mathbf{N} \to \mathbf{N}$ is such that

$$F(n) = \sum_{d|n} f(d)\,.$$

The Möebius inversion theorem [1] assures that

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right).$$

3. Consider the circunference S of radius one in the complex plane and the 1-parameter family of functions $f_a\colon S \to S$ given by

$$f_a(e^{2\pi i t}) = e^{2\pi i a t}\,,$$

where a is a positive integer number. This function is well defined because if t and s are such that $e^{2\pi i t}$ and $e^{2\pi i s}$ represent the same point in S then $e^{2\pi i a t} = e^{2\pi i a s}$.

We will consider the semi-dynamical determined by iterations of this family of functions of the circunference. Given a point x in S, the set

$$O(x) = \{f^n(x)\colon n \in \mathbf{N}\}\ .$$

is the orbit of the point x, where f^n denotes the repeated composition of the function f with itself, n times. A point x in S is periodic, of period n, if n is the minimun natural number that satisfies $f^n(x) = x$. In this case the set $O(\S)$ is finite (has n elements) and is called a periodic orbit of period n.

For each $a \in \mathbf{N}$ the function f_a has periodic points of all posibles periods, in fact, the set of periodic points of f_a, of period that divides n is

$$Per_n(f_a) = \left\{e^{\frac{2\pi i k}{a^n-1}} \colon k \in \mathbf{N}\right\}\,,$$

and it contains $a^n - 1$ elements.

We can calculate the number, $N(n)$, of periodic orbits of period n observing that

$$\sum_{d|n} N(d) d = a^n - 1\,,$$

and applying the Möbius inversion formula in this equality to obtain:

$$N(n) = \frac{1}{n} \sum_{d|n} \mu(d)(a^{\frac{n}{d}} - 1)\,.$$

When n is equal to a prime number, let say p, we obtain

$$N(p) = \frac{a}{p}(a^{p-1} - 1)\,.$$

Since $N(p)$ is an integer, when p is not a factor of a it necessarily is a factor of the number $a^{p-1} - 1$, which proves the Little theorem of Fermat.

Historical Note.

In the year 1640 Pierre de Fermat wrote a letter to Frénicle de Bessy stating, without proof the result that is now known as the Little Theorem of Fermat. It was not until the year 1736 that a proof of it was made public by Leonard Euler and which was later extended to prove a more general theorem that was named after him.

Acknowledgement. We thank the anonymous referees for their carefull reading and recomendations plus the contribution of the historical note.

Note. This research was supported by projects IN-502096, IN-306596 UNAM and 26629-E CONACyT.

Bibliography

1. I. Niven, H.S. Zuckerman, *An Introduction to the Theory of Numbers*, John Wiley & Sons, Inc. (1966). U.S.A.