APORTACIONES MATEMÁTICAS
Serie Comunicaciones 25 (1999) 199–202

A dynamical systems proof of Euler's generalization of the little Theorem of Fermat

H. Carrillo[1] and J. R. Guzmán[2]

[1] Laboratorio de Dinámica No Lineal
Facultad de Ciencias
Universidad Nacional Autónoma de México
Ciudad Universitaria
04510, México, D.F.
México
carr@servidor.unam.mx

[2] Instituto de Investigaciones Económicas
Universidad Nacional Autónoma de México
Ciudad Universitaria
04510 México, D.F.
México
jrg@servidor.unam.mx

Abstract. Counting the periodic orbits of a one parameter family of dynamical systems generated by linear expansions of the circumference we prove the following Euler-Fermat theorem: If a and n are positive integers, with no common prime divisor, then $a^{\varphi(n)} \equiv 1 \bmod (n)$, where φ is the Euler function.

Using an ad hoc one-parameter family of circle maps, we proved in [1] the "Little Theorem of Fermat": *If a is an integer and p is a prime number such that $(a,p) = 1$, then*

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

Euler invented the function $\varphi(n)$ that counts the numbers smaller than n, which are relatively prime to it and observed that the following generalization of the little theorem is also true.

1.1 Theorem. (Euler-Fermat). *If $(a,n) = 1$, then*

$$a^{\varphi(n)} \equiv 1 \ mod(n).$$

1991 Mathematics Subject Classification: 11, 58 .

The proof of this theorem is based on the following lemma.

1.2 Lemma. *If a is an integer and $p_1, \ldots, p_k$ are prime numbers, not factors of a, then for any $i = 1, \ldots, k$, we have that*

$$a^{\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k})} \equiv 1 \ mod(p_i^{\alpha_i}).$$

For the sake of completeness we recall here some basic properties of congruences, as well as of the functions of Euler and Möbius, that will be used in the following discussion.

(i) *For $i = 1, \ldots, n$, let a_i, b_i, m_i, be integers such that $a_i \equiv b_i \ mod(m_i)$. Then we have that $a_i \equiv b_i \ mod([m_1, m_2, \ldots, m_n])$, where the function $[\cdot]$ represents the least common multiple.*

(ii) *If p is a prime number and α is a positive integer then $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

(iii) *If $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, where each p_i is a prime number and α_i is a positive integer, then*

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k})).$$

(iv) *Möbius inversion formula: if f and F are arithmetic functions and if $f(n) = \sum_{d|n} F(d)$, then $F(n) = \sum_{d|n} \mu(d) f(\frac{n}{d})$ where $\mu(d)$ is the Möbius funtion:*

$$\mu(n) = \begin{cases} 1 \text{ if } n = 1, \\ 0 \text{ if there exist } a \in Z^+ \text{ such that } a^2 \mid n, \\ (-1)^k \text{if } n = p_1 \ldots p_k \text{ where the } p_i \text{ are distinct prime number}. \end{cases}$$

Proof: To prove this result we consider the monoparametric family of dynamical systems in the circunference whose orbits are recursively determined, for each initial condition $q \in R$, by the rule:

$$x(0) = q,$$
$$x(n) = ax(n-1) \bmod (1),$$

where the parameter a is a positive integer. For each fixed a, a point $q \in \mathbb{R}$ is called periodic of period n, if $x(n) = q \bmod (1)$, that is to say, if $a^n q = q + k$, for some some integer k. We say that d is the minimal period of the point q, if it is the minimal natural with this property. Therefore, the set of periodic points q, of period n is:

$$\begin{aligned} Per(n) &= \left\{ \frac{k}{a^n - 1} \bmod (1) : k \in N \right\}, \\ &= \left\{ 0, \frac{1}{a^n-1}, \frac{2}{a^n-1}, \ldots, \frac{a^n-2}{a^n-1} \right\} \cup \left\{ \frac{k}{a^n-1} \bmod (1) : k \geq a^n - 1 \right\}, \\ &= \left\{ 0, \frac{1}{a^n-1}, \frac{2}{a^n-1}, \ldots, \frac{a^n-2}{a^n-1} \right\}. \end{aligned}$$

Hence, the number of periodic points of period n is $a^n - 1$. Now, if $N(d)$ is the number of periodic orbits of minimal period d, then $|Per(n)| = \sum_{d/n} dN(d)$, where $|.|$ denotes cardinality

Let p be a prime number which is not a factor of a. Then, for all positive integer α, we have that $|Per(p^\alpha)| = a^{p^\alpha} - 1 = \sum_{d/p^\alpha} dN(d)$. Applying Möbius formula to this equation we obtain that:

$$p^\alpha N(p^\alpha) = \sum_{d/p^\alpha} \mu(d)(a^{\frac{p^\alpha}{d}} - 1) = a^{p^{\alpha-1}}(a^{\varphi(p^\alpha)} - 1).$$

From this equation we can conclude that $p^\alpha \mid a^{p^{\alpha-1}}(a^{\varphi(p^\alpha)} - 1)$. On the other hand, $(p, a) = 1$, implies that $(p^\alpha, a^{p^{\alpha-1}}) = 1$ and from this it follows that $p^\alpha \mid (a^{\varphi(p^\alpha)} - 1)$. Then, given a prime number p_i, and a positive integer α_i, we have that $a^{\varphi(p_i^{\alpha_i})} \equiv 1 \bmod (p_i^{\alpha_i})$. Thus, there is $k_i \in \mathbf{Z}$ such that $a^{\varphi(p_i^{\alpha_i})} = 1 + k_i p_i^{\alpha_i}$. From this we get that $a^{\varphi(p_1^{\alpha_1})\ldots\varphi(p_k^{\alpha_k})} = (1 + k_i p_i^{\alpha_i})^{r_i}$, where $r_i = \prod_{\substack{j=1,\ldots,k \\ j\neq i}} \varphi(p_j^{\alpha_j})$. Then

$$\begin{aligned} a^{\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k})} - 1 &= (1 + k_i p_i^{\alpha_i})^{r_i} - 1 \\ &= \binom{r_i}{1}(k_i p_i^{\alpha_i}) + \binom{r_i}{2}(k_i p_i^{\alpha_i})^2 + \ldots + \binom{r_i}{r_i}(k_i p_i^{\alpha_i})^{r_i}, \end{aligned}$$

applying the binomial formula. From the fact that $\binom{r_i}{j}$ is an integer, when $j \leq r_i$, the assertion of the lemma follows. □

Proof of Theorem (1.1).

We assume that $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, with each p_i a prime number and α_i a positive integer, and consider an integer a such that $(a, n) = 1$. Then $(p_i, a) = 1$, for $i = 1, \ldots, k$, and using the lemma we have that $a^{\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_k^{\alpha_k})} \equiv 1 \bmod (p_i^{\alpha_i})$, for any p_i. Using the basic property of congruences, i), we infer that $a^{\varphi(p_1^{\alpha_1})\ldots\varphi(p_k^{\alpha_k})} \equiv 1 \bmod (p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k})$ and then, from the fact that the Euler φ function is multiplicative, the theorem follows. □

Historical Note.

It is known [2] that Leibnitz had proved the Little Theorem 49 years before Euler, who discovered the proof in 1732 and published it in 1738, but, as Leibnitz did not publish it, the credit have been given to Euler.

Aknowledment.

To the anonymous referees for the carefull revision, corrections and the contribution of the historical note.

Bibliography

1. H. Carrillo and J. R. Guzmán, *A dynamical systems proof of the little theorem of Fermat*, Aportaciones Matemáticas. Comunicaciones No. 22, Soc. Mat. Mexicana (1998), 63–65.
2. E.T. Bell, *The development of mathematics*, Mc.Graw-Hill, (1945).
3. I. Niven and H.S. Zuckerman, *An introduction to the theory of Numbers*. Wiley, (1966).