**Ingeniería y Ciencia**, ISSN 1794–9165
Volumen 6, número 12, julio-diciembre de 2010, páginas 43–49

# A simple proof of Abel's theorem on the lemniscate

## Uma prova simples do teorema de Abel sobre a lemniscata

## Demostración simple del teorema de Abel sobre la lemniscata

Leonardo Solanilla[1], Óscar Palacio[2] y
Uriel Hernández[3]

*Recepción: 27-feb-2010/Modificación: 19-oct-2010/Aceptación: 06-dic-2010*
*Se aceptan comentarios y/o discusiones al artículo*

### Abstract

Since Abel's original paper of 1827, his remarkable theorem on the constructibility of the lemniscate splitting has been proven with the aid of Elliptic Functions. Nowadays, Rosen's proof of 1981 is considered definitive. He also makes use of (modern and more elaborate) Class Field Theory. Here we present a novel, short and simple proof of Abel's Theorem on the lemniscate and its converse. Our only ingredients are the addition formulas of Gauss lemniscatic functions and some basic facts of Galois Theory.

**Key words:** Abel's theorem on the lemniscate, Gauss lemniscatic functions, geometric constructions.

[1] Doctor en Matemáticas, leonsolc@ut.edu.co, profesor, Universidad del Tolima, Ibagué–Colombia.
[2] Profesional en Matemáticas con énfasis en Estadística, tikomania86@hotmail.com, estudiante de Especialización en Matemáticas, Universidad del Tolima, Ibagué–Colombia.
[3] Profesional en Matemáticas con énfasis en Estadística, uriel501@hotmail.com, estudiante de pregrado, Universidad del Tolima, Ibagué–Colombia.

## Resumo

Desde o artigo original de Abel em 1827, seu notável teorema sobre a construtibilidade da divisão da lemniscata tem sido provado com ajuda das funções elípticas. Hoje, a prova de Rosen (1981) é considerada definitiva. Ele também faz uso da moderna e mais elaborada teoría dos corpos de classes. Neste trabalho, nós apresentamos uma prova nova, curta e simples do Teorema de Abel sobre a lemniscata e seu recíproco. Nossos ingredientes são apenas as fórmulas de adição das funções lemniscáticas de Gauss e alguns fatos básicos da teoría de Galois.


**Palavras chaves:** teorema de Abel sobre a lemniscata, funções lemniscáticas de Gauss, construções geométricas.


## Resumen

Desde la publicación original de Abel en 1827, su notable teorema sobre la constructibilidad de la división de la lemniscata se ha demostrado con ayuda de la teoría de las funciones elípticas. La prueba dada por Rosen en 1981 se considera, hoy por hoy, como definitiva. En ella se utiliza, además, la moderna e intrincada *Class Field Theory*. Aquí se presenta una demostración nueva, corta y simple del teorema de Abel para la lemniscata junto con su recíproco. Las únicas herramientas son las propiedades aditivas de las funciones lemniscáticas de Gauss y algunos elementos de teoría de Galois.


**Palabras claves:** teorema de Abel sobre la lemniscata, funciones lemniscáticas de Gauss, construcciones geométricas.

## 1 Introduction

In 1801, Gauss [1, section 7] proved his celebrated theorem on the construction of the regular polygons by using the trigonometric or circular functions. He also announced that the theory applies to a wider class of transcendental functions including the lemniscatic arc length. Some years later, Abel [2, pp. 361–362] showed indeed clearly his famous theorem. More recently, Rosen [3, p. 388] has claimed to be the first of having the converse of Abel's theorem appeared in print. In what follows, we prove comprenhensively the theorem and its converse from very elementary facts. Our proof improves substantially the technique employed by Hernández and Palacio [4, chapter 4].

**Theorem 1.1.** *The lemniscate can be divided into $n$ equal arcs by means of a compass and an unmarked straightedge if and only if $n = 2^k p_1 p_2 \cdots p_t$, where the $p_i'$s are distinct Fermat primes.*

In section 2 we define the lemniscate, discuss its arc length and recast the lemniscatic functions to fit the later work. In section 3 we give our proof of the "if" part of theorem 1.1 by examining the Galois group of a suitable extension of $\mathbb{Q}(i)$. Section 4 is devoted to the "only if" part of the theorem. At the end we draw some conclusions regarding the possibility of generalizing the procedure to a whole class of curves comprising the circle and the lemniscate.

## 2 Gauss lemniscatic functions

Here, the lemniscate is the locus $\mathcal{L}$ of points $(x, y)$ in the plane satisfying the equation $(x^2 + y^2)^2 = x^2 - y^2$. In polar coordinates $(r, \theta)$, the equation becomes $r^2 = \cos 2\theta$ and its arc length is given by the function

$$\operatorname{arcsl} : [-1, 1] \to \mathbb{R}, \quad r \mapsto \int_0^r \frac{d\rho}{\sqrt{1-\rho^4}}\,.$$

The lemniscatic sine $\operatorname{sl}(x)$ is the odd function resulting from extending $\operatorname{arcsl}^{-1}$ to the real line in such a way it is periodic with period $2\varpi = 4\int_0^1 d\rho/\sqrt{1-\xi^4}$. The lemniscatic cosine is $\operatorname{cl}(x) = \operatorname{sl}\left(\frac{\varpi}{2} - x\right)$.

The most important properties of the lemniscatic functions are their addition formulas

$$\operatorname{sl}(x \pm y) = \frac{\operatorname{sl}(x)\operatorname{cl}(y) \pm \operatorname{sl}(y)\operatorname{cl}(x)}{1 \mp \operatorname{sl}(x)\operatorname{sl}(y)\operatorname{cl}(x)\operatorname{cl}(y)},\ \operatorname{cl}(x \pm y) = \frac{\operatorname{cl}(x)\operatorname{cl}(y) \mp \operatorname{sl}(x)\operatorname{sl}(y)}{1 \pm \operatorname{sl}(x)\operatorname{sl}(y)\operatorname{cl}(x)\operatorname{cl}(y)}\,. \tag{1}$$

By induction on $n \in \mathbb{Z}^+$,

| | if $n$ is odd | if $n$ is even |
|---|---|---|
| $\operatorname{sl}(nx) =$ | $\operatorname{sl}(x)r_1(\operatorname{sl}^2(x))$ | $\operatorname{sl}(x)\operatorname{cl}(x)r_2(\operatorname{sl}^2(x))$ |
| $\operatorname{cl}(nx) =$ | $\operatorname{cl}(x)r_3(\operatorname{sl}^2(x))$ | $r_4(\operatorname{sl}^2(x))$, |

where $r_1, r_2, r_3, r_4$ stand for rational functions in one indeterminate with integer coefficients.

The Pythagorean-like identity

$$\operatorname{sl}^2(x) + \operatorname{cl}^2(x) + \operatorname{sl}^2(x)\operatorname{cl}^2(x) = 1$$

can be visualized as the image $\mathcal{C}$ of the map $x \mapsto \big(\operatorname{cl}(x), \operatorname{sl}(x)\big)$. Figure 1 shows a sketch of this curve. $\mathcal{C}$ possesses a canonical group structure isomorphic to

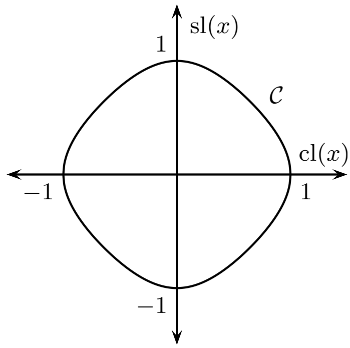


**Figure 1:** The curve $\mathcal{C}$.

the quotient $\mathbb{R}/\langle 2\varpi\rangle$ of the additive group $\mathbb{R}$ into the subgroup generated by $2\varpi$.

Since every point $\big(\mathrm{sl}(x), \mathrm{cl}(x)\big) \in \mathcal{C}$ determines clearly a $(x, y) \in \mathcal{L}$ and the critical point of the lemniscate introduces no confusion, we may use $\mathcal{C}$ to split the lemniscate $\mathcal{L}$. For a fixed positive integer $n$, our problem is then equivalent to the constructibility of the division points $\gamma_k = \mathrm{cl}\big(\frac{2\varpi}{n}k\big) + i\mathrm{sl}\big(\frac{2\varpi}{n}k\big) \in \mathcal{C}$, $k = 0, 1, \ldots, n-1$. The addition formulas (1) provide $\Gamma_n = \{\gamma_k\}_{k=0}^{n-1}$ with a natural group structure isomorphic to $\mathbb{Z}_n$. Writing shortly $\mathrm{cl}(x) + i\mathrm{sl}(x) = z(x)$, the elements of $\Gamma_n$ are just the solutions to the equation $r(z(x)) = z(nx) = 1$.

## 3 Extending $\mathbb{Q}(i)$

The extension field $L_n = \mathbb{Q}(i)(\Gamma_n)$ is Galois over $\mathbb{Q}(i)$. Certainly, $\Gamma_n$ is finite and so, $L_n$ is algebraic and finite dimensional. As $\mathbb{Q}(i)$ has characteristic 0, $L_n$ is separable. Also, if $\sigma$ is a $\mathbb{Q}(i)$-automorphism of $\mathbb{C}$ and $\gamma_k = \alpha_k + i\beta_k \in \Gamma_n$, then $r(\sigma(\alpha_k) + i\sigma(\beta_k)) = \sigma(r(\alpha_k + i\beta_k)) = 1$. Therefore, the equivalence relation

$$\gamma_k \ \sim \ \gamma_l \Leftrightarrow \exists\ \sigma \in \mathrm{Gal}_{\mathbb{Q}(i)} L_n : \sigma(\gamma_k) = \gamma_l$$

partitions $\Gamma_n$ into classes of elements sharing the same irreducible polynomial over $\mathbb{Q}(i)$. Since $L_n$ is the splitting field of the product of these polynomials, it is normal.

Furthermore, the Galois group $\mathrm{Gal}_{\mathbb{Q}(i)} L_n = G_n$ is isomorphic to a subgroup of the multiplicative group $U_n$ of units of $\mathbb{Z}_n$. Actually, the action of $G_n$ on $\Gamma_n$ defined by $\sigma(\gamma_k)$ is a bijection for each fixed $\sigma$, which preserves the group structure on $\Gamma_n$. That is, there is a group homomorphism $G_n \to \mathrm{Aut}(\Gamma_n) \cong \mathrm{Aut}(\mathbb{Z}_n) \cong U_n$. Since $L_n$ is algebraic, this homomorphism is onto.

Now, the order of $U_n$ equals the value of Euler's $\varphi$-function at $n$. Thus, if $n = 2^k p_1 p_2 \cdots p_t$ with different Fermat primes $p_i, 1 \leqslant i \leqslant t$, a simple number-theory calculation shows the order of $U_n$ is a power of two. As a result of Lagrange's theorem and basic Galois theory, $[L_n : \mathbb{Q}(i)]$ is also a power of two. Hence, the elements of $\Gamma_n$ are constructible. A convenient reference for this material is the fifteenth chapter of Hungerford's book [5]. So, we have proved Abel's theorem: if $n$ has the given form, then the lemniscate can be split into $n$ equal parts with ruler and compass.

## 4 Converse

We must elucidate the field structure of $L_n$. To begin, let us consider the orbits $[k]$ of the action $U_n \times \mathbb{Z}_n \to \mathbb{Z}_n, (u,k) \mapsto uk$. We claim that $\gamma_k \sim \gamma_l \Leftrightarrow [k] = [l]$. The implication "$\Rightarrow$" has been already proved: if $\gamma_k \sim \gamma_l$, there is a $u \in U_n$ such that $l = uk$, i.e., $[k] = [l]$. The "$\Leftarrow$" part is more elaborate and relies on a careful scrutiny of the general addition formulas for $\mathrm{sl}(nx), \mathrm{cl}(nx)$. We notice that, when $n$ is odd (respectively, even), the factors $\mathrm{cl}(x), \mathrm{sl}(x)$ yield the solution $\gamma_0 = 1$ (respectively, solutions $\gamma_0 = 1, \gamma_{n/2} = -1$) of equation $r(z(x)) = \mathrm{cl}(nx) + i\mathrm{sl}(nx) = 1 + 0i$. Since the remaining factors depend on $\mathrm{sl}^2(x)$, the elements of $\Gamma_n$ occur in conjugate pairs within the same equivalence class.

Let us resume the proof where we left off. If $[k] = [l]$, then there is a $u \in U_n$ such that $l = uk$. The case $u = 1$ is evident. If $u = n-1$, $\gamma_l$ is the complex conjugate $\bar{\gamma}_k$ of $\gamma_k$. The remaining case is when $u \in U_n \setminus \{1, n-1\}$. In this case, the real and imaginary parts of

$$\gamma_l = \gamma_{uk} = \mathrm{cl}\Big(u\frac{2\varpi}{n}k\Big) + i\ \mathrm{sl}\Big(u\frac{2\varpi}{n}k\Big)$$

are, via the addition formulas, rational expressions of $\mathrm{cl}(\frac{2\varpi}{n}k) = \frac{\gamma_k + \bar{\gamma}_k}{2}$ and $\mathrm{sl}(\frac{2\varpi}{n}k) = \frac{\gamma_k - \bar{\gamma}_k}{2i}$. In this way, given $u \in U_n$, there is a permutation $\gamma_j \mapsto \gamma_{uj}$

of the equivalence class $[\gamma_k]$ of $\gamma_k$. For, $\gamma_{uj}$ is obtained from $[\gamma_k]$ and $\mathbb{Q}(i)$ by a finite sequence of field operations. In other words, it belongs to the splitting field $\mathbb{Q}(i)([\gamma_k])$ of the irreducible polynomial associated with $[\gamma_k]$. Then, the permutation induces a linear automorphism of $\mathbb{Q}(i)([\gamma_k])$ which leaves each element of $\mathbb{Q}(i)$ unchanged. By performing the process in the other equivalence classes in $\Gamma_n$, this automorphism extends in turn to a $\sigma_u \in G_n$. As $\sigma_u(\gamma_k) = \gamma_l$, we get $\gamma_k \sim \gamma_l$.

Consequently, $G_n$ is isomorphic to $U_n$. Then, $[L_n : \mathbb{Q}(i)] = \varphi(n)$. If the division of the lemniscate into $n$ equal arcs can be constructed, $\varphi(n)$ is a power of two. By elementary arguments in number theory we conclude that $n = 2^k p_1 p_2 \cdots p_t$, where the $p_i'$s are distinct Fermat primes. Theorem 1.1 follows.

## 5 Conclusions

The plainness of the procedure reveals what might be needed for a closed curve to split like the circle or the lemniscate. First, its arc length should be given by an elliptic integral, say $\int dx/\sqrt{p(x)}$ for a certain polynomial $p$. Second, the locus of the solution to Euler's problem

$$\frac{dx}{\sqrt{p(x)}} + \frac{dy}{\sqrt{p(y)}} = 0,\ y(x=0) = 1\,,$$

should conveniently match the curve. Third, there should be a periodic parametrization $x(t), y(t)$ of the solution locus such that $x(nt), y(nt),\ n \in \mathbb{Z}^+$, are rational functions of $x(t), y(t)$ with rational coefficients. Fourth, the problem should reduce to the constructibility of $x((2\varpi/n)k) + iy((2\varpi/n)k)$, $k = 0, 1, \ldots, n-1$, where $2\varpi$ denotes the parametrization period. Fifth, these numbers should be the zeros of equation $x(nt) + iy(nt) = 1$, etc. For background material on elliptic integrals the reader can consult McKean and Moll [6, chapter 2]. See also [7].

## Acknowledgements

This paper has been partially supported by the Vicerrectoría de Investigaciones of Universidad de Medellín and the Facultad de Ciencias of Universidad del Tolima. The authors also wish to thank the referees for their valuable suggestions and improvements in the paper.

## References

[1] C. F. Gauss. *Disquisitiones Arithmeticæ*, ISBN 958–92–05–15–1. Spanish translation by H. Barrantes, M. Josephy and A. Ruiz, Academia Colombiana de Ciencias Exactas, Físicas y Naturales, Bogotá, 1995. Originally published by Gerh. Fleischer, Leipzig, 1801. Referenciado en 44

[2] N. H. Abel. *Recherches sur les fonctions elliptiques, Œuvres Complètes, Christiania (Oslo)*, 1881. Originally published in Journal für die reine und angewandte Mathematik, herausgegeben von Crelle, Bd. 2, 3; Berlin, 1827, 1828. Referenciado en 44

[3] Michael Rosen. *Abel's Theorem on the Lemniscate*. The American Mathematical Monthly, ISSN 0002–9890, **88**(6), 387–395 (1981). Referenciado en 44

[4] U. Hernández and O. J. Palacio. *División de la lemniscata: geometría, análisis, álgebra*. Facultad de Ciencias, Universidad del Tolima, trabajo de grado del Programa de Matemáticas con énfasis en Estadística, Ibagué–Colombia, 2009. Referenciado en 44

[5] Thomas W. Hungerford. *Abstract Algebra, an Introduction*, ISBN 0–03–010559–5. Brooks/Cole, New York, 1996. Referenciado en 47

[6] Henry McKean and Victor Moll. *Elliptic Curves: Function Theory, Geometry, Arithmetic*, ISBN 978–0521658171. Cambridge University Press, Cambridge, 1999. Referenciado en 48

[7] R. Sridharan. *From Lintearia to Lemniscate II: Gauss and Landen's Work*. Resonance, ISSN 0971–8044, **9**(6), 11–20 (June 2004). Referenciado en 48