congresso de pesquisa, ensino e extensão

# 12º conpeex

Luz, ciência e vida

# ANAIS DO XII CONPEEX

Congresso de Pesquisa, Ensino e Extensão

Universidade Federal de Goiás

*De 19 a 21 de outubro de 2015*

# PICME


*Apoio:* FUNAPE Fundação de Apoio à Pesquisa - UFG; FAPEG FUNDAÇÃO DE AMPARO À PESQUISA DO ESTADO DE GOIÁS; SED; GOVERNO DE GOIÁS; CNPq Conselho Nacional de Desenvolvimento Científico e Tecnológico; CAPES

BANCO DO BRASIL; CAIXA; GOVERNO FEDERAL BRASIL PÁTRIA EDUCADORA

*Realização:* UFG UNIVERSIDADE FEDERAL DE GOIÁS

# ÍNDICE DE ALUNOS

| Aluno | Trabalho |
|---|---|
| **LUCAS GOMES DE MELLO** | PROPORÇÃO ÁUREA: FATOS E MITOS |
| **MARCOS LUCAS VELOSO JUNQUEIRA** | UMA ABORDAGEM A MODELAGEM MATEMÁTICA: CURVAS DE PERSEGUIÇÃO |
| **TULIO MARCIO GENTIL DOS SANTOS** | CRIPTOGRAFIA DE CHAVE PÚBLICA PARA CURVAS ELÍPTICAS |
| **VICTOR GONÇALVES NETTO** | BRAQUISTÓCRONA |

# Proporção Áurea: Fatos e Mitos

**SERCONEK**, Shirlei[1]

**MELLO**, Lucas Gomes de[2]

7 de setembro de 2015

**Palavras-chave:** Proporção Áurea, Mito.

## INTRODUÇÃO

A proporção áurea foi descoberta por Euclides há cerca de 2300 anos e desde então tem marcado presença nos mais diversos temas.

A proporção áurea possui certamente propriedades incríveis; entretanto, durante séculos muitos mitos foram inventados e propagados através dos mais diversos meios de comunicação, principalmente pela internet na atualidade. Grandes estudiosos tais como Keith Devlin, Donald E. Simanek e Mario Livio vêm tentando desmistificar muitas informações a respeito dessa proporção. Contudo existem também verdades incríveis sobre esse número. Algumas descobertas recentes têm sido feitas e merecem ser destacadas, como por exemplo, a presença desta proporção no trabalho de Daniel Shechtman, ganhador do prêmio Nobel de Química de 2011.

## JUSTIFICATIVA

As descobertas sobre a proporção áurea têm estimulado pesquisas e consequentemente explicações científicas.

## OBJETIVO

Buscamos neste trabalho, esclarecer quais são as atuais descobertas e os mitos que envolvem a proporção áurea.

## METODOLOGIA

Foram realizados encontros semanais de orientação, além de pesquisas e estudos individuais.

1 Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatística, UFG
2 Orientando – lucasgmello@hotmail.com - Escola de Engenharia Elétrica, Mecânica e da Computação, UFG

## RESULTADOS

No estudo da proporção áurea, encontramos diversos mitos pela internet que circulam como se fossem fatos. Diversas áreas tiveram seus elementos colocados de várias maneiras, tudo para que se encaixasse com algum retângulo ou espiral áureo e motivassem a crença em uma razão áurea “oculta”. Áreas como arte, arquitetura, estética e até mesmo sobre o surgimento da proporção áurea.

Apesar de tudo, também encontramos fatos que nos surpreendem, como a beleza da proporção áurea encontrada na natureza, os números de Fibonacci e também nas recentes descobertas da proporção áurea, tais como a primeira aparição da proporção áurea no espaço nas estrelas “RR Lyrae” e também nos quasicristais, que foram estruturas consideradas impossíveis há alguns anos, mas recentemente foram descobertos por Shechtman, o que lhe rendeu o Nobel de Química em 2011.

## CONCLUSÃO

Certamente a proporção áurea foi alvo de muitos mitos, principalmente nos últimos séculos. Entretanto as atuais descobertas sobre esse número fazem dele como Kepler o descreveu, “uma joia preciosa”.

## REFERÊNCIAS

[1] HART, Ernest Huntley. A Divina Proporção. Trad. De Luís Carlos Nunes. Brasília, Editora Universidade de Brasília, 1985.

[2] LIVIO, Mario. The Golden Ratio. New York, BROADWAY BOOKS.

[3] ARBESMAN, Samuel. Math as Myth. Disponível em <http://nautil.us/issue/0/the-story-of-nautilus/math-as-myth>.

[4] RA, Amateo. Scientists Find Fractal Patterns & Golden Ratio Pulses in Stars. Disponível em <http://www.spiritscienceandmetaphysics.com/scientists-find-fractal-patterns-golden-ratio-pulses-in-stars/>.

[5] Israelense ganha o Nobel de Química pelos quasicristais. Revista VEJA, disponível em <http://veja.abril.com.br/noticia/ciencia/israelense-ganha-nobel-de-quimica-por-quasicristais/>.

# Criptografia de Chave Pública com Curvas Elípticas*

**SERCONEK**, Shirlei†

**SANTOS**, Tulio Marcio Gentil dos ‡

3 de setembro de 2015

**Palavras-chave:** Criptografia, Curvas Elípticas.

## INTRODUÇÃO

A *criptografia* é a ciência que estuda, entre outros, métodos para codificar uma mensagem de modo que apenas seu destinatário consiga interpretá-la.

Os sistemas de criptografia são classificados em: sistemas simétricos e sistemas assimétricos (ou de chave pública). No sistema de criptografia de chave pública, cada usuário possui um par de chaves: a pública e a privada. Nesse sistema, se o usuário A pretende comunicar-se com B secretamente, A usa a chave pública de B (que todos do sistema conhecem) para cifrar os dados a serem enviado para B. Agora, para que B tenha acesso ao conjunto de dados originais, B usa sua chave secreta para decifrá-los os dados. Esse sistema, foi inicialmente proposto por Diffie e Hellman em 1976.

## JUSTIFICATIVA

O avanço da tecnologia da informação, a questão da privacidade, anonimato e segurança de transmissões de dados mostraram cada vez mais a importância da criptografia.

## OBJETIVOS

Buscamos neste trabalho, entender fundamentos matemáticos para o funcionamento de alguns sistemas criptográficos utilizando curvas elípticas.

---

*Revisado pelo orientador

†Orientadora - shirleik@terra.com.br - Instituto de Matemática e Estatísitca, UFG

‡Orientando - tuliosantosufg@hotmail.com - Instituto de Matemática e Estatísitca, UFG

## METODOLOGIA

Realizamos pesquisas bibliográficas, estudo individual e encontros semanais de orientação.

## RESULTADOS

No estudo de criptografia com curvas elípticas atentamos à dois casos particulares. O primeiro, em que a curva elíptica $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ está definida em um corpo $K$ onde $char(K)$ não é 2 nem 3, e o segundo caso, no qual a curva está definida sobre o corpo $\mathbb{F}_{2^m}$.

Vimos que existem mudanças de variáveis que transformam $E$ em $E_1 : y^2 = x^3 + ax + b$ (no primeiro caso) e em $E_2 : y^2 + xy = x^3 + ax^2 + b$ (no segundo caso). Para cada uma das curvas, $E_1$ e $E_2$, construímos uma estrutura de grupo.

Após essa etapa, estudamos o ECDSA (Elliptic Curve Digital Signature Algorithm) que é um algorítimo de assinatura digital utilizando curvas elípticas. Ele foi proposto inicialmente por Scott Vanstone em 1992 para o NIST (National Institute of Standards and Technology), aceito em 1998 pelo ISO (International Organization for Standardization), e demais órgãos dos Estados Unidos.

## CONCLUSÃO

Nesse trabalho foi possível perceber que a Matemática é uma ciência de grande importância para a sociedade. Sem ela, não teríamos segurança nos tráfegos de dados, e dessa forma estamos vulneráveis à ataques, principalmente na internet.

# Referências


[1] R.L. Rivest, A. Shamir, and L. Adleman *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*.

[2] Don Johnson, Alfred Menezes & Scott Vanstone. *The Elliptic Curve Signature Algorithm*.

[3] Darrel Hankerson, Alfred Menezes & Scott Vanstone. *Guide to elliptic curve cryptography*, Springer, (2004).

[4] Silverman J. H., *An Indroduction to the Theory of Elliptic Curves*, (2006).

[5] Herstein, I.N. *Abstract Algebra*, 3rd ed., Prentice-Hall (1995).

# BAQUISTÓCRONA

**NETTO,** Victor Goncalves; **SILVA,** Rosângela Maria da

**Palavras-chave:** Braquistócrona, Cicloide, Cálculo Variacional, Equação de Euler-Lagrange

**Justificativa:** Durante o primeiro ano do programa de iniciação científica e mestrado (PICME) trabalhamos as curvas do plano e do espaço, do ponto de vista da geometria diferencial. Ao tentar unir os conceitos da geometria diferencial das curvas com a física, optamos por trabalhar o problema da braquistócrona, que tem importância histórica e técnica.

**Objetivos:** O trabalho se propõe a dar uma solução completa do problema da braquistócrona. Além disso, nos propomos a fazer uma breve discussão histórica, e apresentar aplicações.

**Resultado e discussão:** A solução apresentada para o problema da braquistócrona, envolve uma técnica matemática razoavelmente elaborada, que depende de outros conceitos mais básico. Devido a isso, ao longo da solução do problema, fizemos o uso de vários teoremas do cálculo e análise, assim como técnicas de equações diferencias, sem maiores comentários.

Obtivemos a equação de Euler-Lagrange, enunciamos e demonstramos o *Lema fundamental do cálculo das variações*, e utilizamos essas ferramentas para solucionar o problema da braquistócrona.

Outros fatos sobre a cicloide são apresentados, a título de complementação e curiosidade. Comentamos também da hipocicloide, uma generalização natural da cicloide.

**Conclusões:** O trabalho apresentado nos mostra a importância dessa "conversa" entre física e matemática. Uma questão de mecânica, gera avanços na matemática, e esses avanços são utilizados, hoje, em outras áreas da física e da matemática.

**Referências bibliográficas:**

-COELHO, Rejeane Alexandre. A história dos problemas da tautócrona e da braquistócrona. 2008. 107 f. Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, 2008. Disponível em: <http://hdl.handle.net/11449/91134>. Acessado em: 10/07/2015.

-LEMOS, Nivaldo A. Mecânica analítica. 2.ed. São Paulo: Editora Livraria da Física, 2007.

-LIMA, Elon Lages. Curso de análise vol.1. 14.ed. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada, 2014. Projeto Euclides

-TENENBLAT, Keti, Introdução à geometria diferencial. 2.ed. São Paulo: Blucher, 2008.