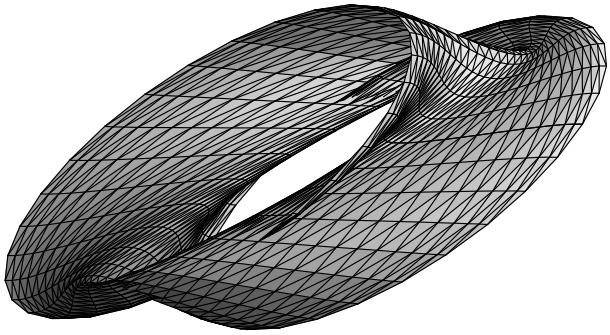
ISSN 1980-024X

BOLETIM DE INICIAÇÃO CIENTÍFICA EM MATEMÁTICA – BICMAT



VOLUME III
OUTUBRO DE 2006
DEPARTAMENTO DE MATEMÁTICA
IGCE – RIO CLARO

unesp

ISSN 1980-024X

Boletim de Iniciação Científica em Matemática – BICMat

Realização

Conselho de Curso de Graduação em Matemática

Departamento de Matemática

IGCE – Unesp – Rio Claro

PET-Matemática / Programa de Educação Tutorial

EDITORIAL

O Boletim de Iniciação Científica em Matemática – BICMat é uma publicação que se destina a difundir prioritariamente trabalhos de iniciação científica que fazem parte de projetos desenvolvidos por alunos do Curso de Graduação em Matemática do IGCE – Unesp – Rio Claro. Eventualmente trabalhos de Iniciação Científica realizados em outras instituições poderão também ser publicados neste Boletim.

O BICMat foi criado em 1998 e foram publicados dois volumes; o primeiro no ano de criação e o segundo em 2000.

Considerando a importância da Iniciação Científica para o graduando, e o sempre crescente número de projetos desta natureza desenvolvidos em nossa instituição, resolvemos reativar a publicação do BICMat neste ano. Para fortalecer o caráter institucional deste Boletim, iniciamos esta nova versão com ISSN 1980-024X.

Destacamos que a autoria dos trabalhos apresentados no BICMat é dos alunos. O orientador figura apenas como responsável científico.

Este Boletim também está aberto à divulgação de trabalhos que não sejam frutos de projetos de iniciação científica, mas que sejam de interesse dos alunos do curso de graduação em Matemática. Estes trabalhos serão selecionados pelos Editores.

Este número teve o apoio do Grupo de Pesquisa: Topologia Algébrica, Diferencial e Geométrica e estará disponibilizado eletronicamente na página do Departamento de Matemática no endereço `www.rc.unesp.br/igce/matematica`

SUMÁRIO

O Problema dos 3-corpos – Estudo da Estabilidade do Movimento Próximo dos Pontos Lagrangianos

Adriano João da Silva* e João Paulo Cerri†
Orientador(a): Prof. Dr. Tadashi Yokoyama

Resumo: Consideremos um sistema formado por 3 corpos, tomando um deles como de massa desprezível em comparação aos demais (massa infinitesimal). Sabemos que num sistema girante de coordenadas existem soluções particulares (estacionárias). Lagrange estabeleceu duas classes de soluções particulares distintas para o Problema dos 3-Corpos: solução Triângulo Equilátero e solução Colinear. Ou seja, pontos estabelecidos nos vértices de um triângulo equilátero e certas posições numa linha reta que une os primários. Tais soluções são os Pontos Lagrangianos de equilíbrio do sistema. Dessa forma, será desenvolvido um estudo da estabilidade do movimento da massa infinitesimal nas proximidades dos Pontos Lagrangianos. Isto será proposto e desenvolvido a seguir para os pontos L_4 e L_1. É importante destacar que este trabalho trata de um estudo detalhado da referência [1], "Introduction to Celestial Mechanics" - Mc Cuskey, S.W., em específico no que diz respeito ao tópico Problema dos 3-Corpos e tendo ainda como apoio as demais referências: [2, 3, 4].

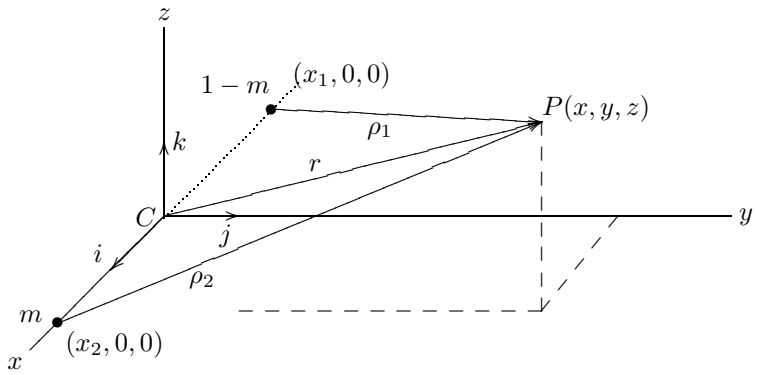
Palavras-chave: Problema de Três Corpos, Problema Restrito de Três Corpos, Pontos Lagrangianos, Soluções Estacionárias, Solução Colinear, Solução Triângulo Equilátero.

1 Introdução

O estudo da formulação matemática do Problema dos 3-Corpos se dá primeiramente através da obtenção das equações do Movimento do Centro de Massa

*Bolsista PET/MEC-SESU. E-mail: ajsilva@rc.unesp.br
†Bolsista PET/MEC-SESU. E-mail: jpcerri@rc.unesp.br

do sistema, da Integral das Áreas ou do Momento Angular, da Integral da Energia e das Equações do Movimento Relativo. No decorrer do estudo é verificado a impossibilidade da obtenção de uma solução analítica para o Problema dos 3-Corpos, já que o movimento é regido por um sistema de 9 equações diferenciais não lineares de segunda ordem. É necessário a obtenção de 18 constantes de integração para sua completa solução, sendo que 10 delas podem ser determinadas através de manipulações algébricas das equações do movimento. Um breve estudo do movimento relativo das 3 massas é realizado juntamente com a determinação da Equação Perturbadora do movimento. É verificado então que o problema não admite solução em sua forma fechada, ou seja, dadas as coordenadas iniciais de posição e velocidade dos 3 corpos movendo somente sob a ação de suas atrações gravitacionais mútuas, não é possível prever o movimento para um instante de tempo qualquer. Como forma alternativa de se abordar o problema, casos especiais são considerados, a saber: as Soluções Estacionárias (Soluções de Lagrange) e o Problema Restrito de 3-Corpos.



Consideremos três corpos posicionados em um sistema referencial de coordenadas fixado com a origem em C, onde as forças atuantes são somente atrações gravitacionais mútuas dos corpos sobre os outros. Suponhamos que uma das três massas seja tão pequena em comparação com as outras duas, podendo ser desconsiderada (massa infinitesimal P), tanto quanto seus efeitos gravitacionais.

Denotaremos por m a massa do menor dos dois corpos e $1-m$ a maior, de forma tal que a soma das massas seja unitária e $m < \frac{1}{2}$. Destacamos ainda que estes dois corpos movem-se ao redor do centro de massa C em órbitas circulares no plano-xy. O corpo infinitesimal movimenta-se então sobre a atração gravitacional combinada dos outros dois corpos, mas não influencia o movimento dos primários.

2 Estudo da estabilidade do movimento próximo dos Pontos Lagrangianos

Analisaremos então a estabilidade do movimento de uma partícula infinitesimal próxima a um ponto Lagrangiano L. Queremos saber se, dado um pequeno deslocamento e uma velocidade, dependendo do tempo, a partícula manter-se-á na vizinhança deste ponto, realizando assim um movimento limitado. Caso isto ocorra o movimento é dito *estável*. Caso contrário, ou seja, a partícula se distancie deste ponto, o movimento será denominado *instável*. A seguir será apresentada uma formulação matemática para a análise do movimento da partícula nas vizinhanças do ponto L. Dois casos serão apresentados: um onde o movimento se dá de forma estável e o outro de forma instável.

Sabemos que, em decorrência da formulação matemática do problema dos 3-corpos, as equações que descrevem o movimento da massa infinitesimal são dadas por

$$\ddot{x} - 2\dot{y} = \frac{\partial U}{\partial x}, \qquad \ddot{y} + 2\dot{x} = \frac{\partial U}{\partial y}, \qquad \ddot{z} = \frac{\partial U}{\partial z}, \tag{1.1}$$

onde

$$U = \frac{1}{2}(x^2 + y^2) + \frac{1-m}{\rho_1} + \frac{m}{\rho_2} \tag{1.2}$$

e

$$\begin{aligned}
\frac{\partial U}{\partial x} &= x - \frac{(1-m)(x-x_1)}{\rho_1^3} - \frac{m(x-x_2)}{\rho_2^3}, \\
\frac{\partial U}{\partial y} &= y - \frac{(1-m)y}{\rho_1^3} - \frac{my}{\rho_2^3}, \\
\frac{\partial U}{\partial z} &= -\frac{(1-m)z}{\rho_1^3} - \frac{mz}{\rho_2^3}, \\
\rho_1 &= [(x-x_1)^2 + y^2 + z^2]^{\frac{1}{2}}, \\
\rho_2 &= [(x-x_2)^2 + y^2 + z^2]^{\frac{1}{2}}.
\end{aligned} \tag{1.3}$$

A partir de (1.1) é possível mostrar que as soluções L_i de equilíbrio está no plano xy. Seja então $(x_o, y_o, z_o = 0)$ um ponto genérico de L_i. Tomemos também α, β e γ pequenos deslocamentos da partícula ao redor de L_i.

Como α, β e γ são funções do tempo, podemos ter então $(\dot{\alpha}, \dot{\beta}, \dot{\gamma})$ e $(\ddot{\alpha}, \ddot{\beta}, \ddot{\gamma})$. Assim,

$$\begin{aligned}
x &= x_0 + \alpha, & \dot{x} &= \dot{x_0} + \dot{\alpha}, & \ddot{x} &= \ddot{x_0} + \ddot{\alpha}, \\
y &= y_0 + \beta, & \dot{y} &= \dot{y_0} + \dot{\beta}, & \ddot{y} &= \ddot{y_0} + \ddot{\beta}, \\
z &= z_0 + \gamma, & \dot{z} &= \dot{z_0} + \dot{\gamma}, & \ddot{z} &= \ddot{z_0} + \ddot{\gamma}.
\end{aligned} \tag{1.4}$$

Admitiremos que os deslocamentos sejam suficientemente pequenos de forma que as expansões de Taylor para U_x, U_y e U_z possam ser escritas como

$$\begin{aligned}
U_x &= (U_x)_0 + \alpha(U_{xx})_0 + \beta(U_{xy})_0 + \gamma(U_{xz})_0, \\
U_y &= (U_y)_0 + \alpha(U_{yx})_0 + \beta(U_{yy})_0 + \gamma(U_{yz})_0, \\
U_z &= (U_z)_0 + \alpha(U_{zx})_0 + \beta(U_{zy})_0 + \gamma(U_{zz})_0,
\end{aligned} \tag{1.5}$$

onde as derivadas parciais são calculadas no ponto (x_o, y_o, z_o) para o ponto L.

No ponto de equilíbrio devemos ter: $(U_x)_0 = (U_y)_0 = (U_z)_0 = 0$. Além disso, pelo fato de (x_0, y_0, z_0) serem constantes, temos que $\dot{x_0} = \dot{y_0} = \dot{z_0} = \ddot{x_0} = \ddot{y_0} = \ddot{z_0} = 0$.

Desta forma as equações do movimento da partícula infinitesimal, na vizi-

nhança do ponto L, para pequenos deslocamentos são dadas por

$$\begin{aligned} \ddot{\alpha} - 2\dot{\beta} &= \alpha(U_{xx})_0 + \beta(U_{xy})_0 + \gamma(U_{xz})_0, \\ \ddot{\beta} + 2\dot{\alpha} &= \alpha(U_{yx})_0 + \beta(U_{yy})_0 + \gamma(U_{yz})_0, \\ \ddot{\gamma} &= \alpha(U_{zx})_0 + \beta(U_{zy})_0 + \gamma(U_{zz})_0. \end{aligned} \tag{1.6}$$

Além disso,

$$\begin{aligned} U_{xx} &= 1 - \frac{(1-m)}{\rho_1^3} - \frac{m}{\rho_2^3} + \frac{3(1-m)(x-x_1)^2}{\rho_1^5} + \frac{3m(x-x_2)^2}{\rho_2^5}, \\ U_{xy} &= \frac{3(1-m)(x-x_1)y}{\rho_1^5} + \frac{3m(x-x_2)y}{\rho_2^5}, \\ U_{xz} &= \frac{3(1-m)(x-x_1)z}{\rho_1^5} + \frac{3m(x-x_2)z}{\rho_2^5}, \\ U_{yy} &= 1 - \frac{(1-m)}{\rho_1^3} - \frac{m}{\rho_2^3} + \frac{3(1-m)y^2}{\rho_1^5} + \frac{3my^2}{\rho_2^5}, \\ U_{yz} &= \frac{3(1-m)zy}{\rho_1^5} + \frac{3mzy}{\rho_2^5}, \\ U_{zz} &= -\frac{(1-m)}{\rho_1^3} - \frac{m}{\rho_2^3} + \frac{3(1-m)z^2}{\rho_1^5} + \frac{3mz^2}{\rho_2^5}. \end{aligned} \tag{1.7}$$

Podemos agora aplicar as equações obtidas ao estudo de dois casos: os pontos L_i estão sobre o eixo-x (solução colinear) e os pontos L_i estão fora deo eixo x, formando um triângulo equilátero com os primários.

Caso I: Movimento em torno de L_4

Consideremos a figura 1.1. Definimos $x_2 - x_1 = 1$ e $\rho_1 = \rho_2 = 1$. Assim,

$$x_0 - x_1 = \frac{1}{2}, \quad x_0 - x_2 = -\frac{1}{2}, \quad y_0 = \sqrt{\frac{3}{2}}, \quad z_0 = 0$$

e as derivadas são

$$U_{xx} = \frac{3}{4}, \quad U_{xz} = U_{zx} = U_{yz} = U_{zy} = 0,$$

$$U_{yy} = \frac{9}{4}, \quad U_{xy} = U_{yx} = \frac{3\sqrt{3}}{2}\left(\frac{1}{2} - m\right), \quad U_{zz} = -1.$$

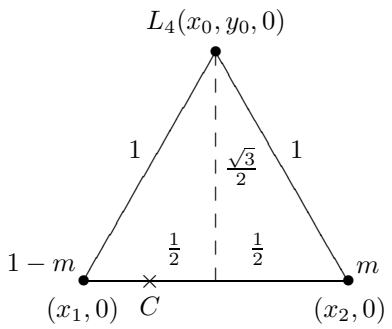


Figura 1.1: Solução Triângulo Equilátero.

As equações do movimento são

$$\begin{aligned} \ddot{\alpha} - 2\dot{\beta} &= \frac{3}{4}\alpha + \frac{3\sqrt{3}}{4}(1-2m)\beta, \\ \ddot{\beta} + 2\dot{\alpha} &= \frac{3\sqrt{3}}{4}(1-2m)\alpha + \frac{9}{4}\beta, \\ \ddot{\gamma} &= -\gamma. \end{aligned} \tag{1.8}$$

Vemos facilmente que a equação em γ possui solução

$$\gamma = c_1 \operatorname{sen} t + c_2 \cos t,$$

onde os c_i são constantes de integração. Assim o deslocamento na direção de z é periódico com período 2π. Portanto, na direção de z o movimento é dito *estável*.

As duas equações restantes formam um sistema de equações diferenciais homogêneas de ordem dois e possuem então solução da forma

$$\alpha = Ae^{\lambda t} \quad \text{e} \quad \beta = Be^{\lambda t}.$$

Assim,

$$\dot{\alpha} = \lambda Ae^{\lambda t} \quad \text{e} \quad \dot{\beta} = \lambda Be^{\lambda t},$$

$$\ddot{\alpha} = \lambda^2 Ae^{\lambda t} \quad \text{e} \quad \ddot{\beta} = \lambda^2 Be^{\lambda t},$$

que substituídas nas equações nos fornecem:

$$\lambda^2 Ae^{\lambda t} - 2\lambda Be^{\lambda t} - \frac{3}{4}Ae^{\lambda t} - \frac{3\sqrt{3}}{4}(1-2m)Be^{\lambda t} = 0$$

ou

$$e^{\lambda t}\left\{A\left[\lambda^2 - \frac{3}{4}\right] + B\left[-2\lambda - \frac{3\sqrt{3}}{4}(1-2m)\right]\right\} = 0.$$

Analogamente para a outra equação:

$$e^{\lambda t}\left\{A\left[2\lambda - \frac{3\sqrt{3}}{4}(1-2m)\right] + B\left[\lambda^2 - \frac{9}{4}\right]\right\} = 0$$

e como $e^{\lambda t} \neq 0$ sempre, temos:

$$\left\{A\left[\lambda^2 - \frac{3}{4}\right] + B\left[-2\lambda - \frac{3\sqrt{3}}{4}(1-2m)\right]\right\} = 0,$$

$$\left\{A\left[2\lambda - \frac{3\sqrt{3}}{4}(1-2m)\right] + B\left[\lambda^2 - \frac{9}{4}\right]\right\} = 0,$$

que possuem solução não trivial se

$$\begin{vmatrix} \lambda^2 - \frac{3}{4} & -2\lambda - \frac{3\sqrt{3}}{4}(1-2m) \\ 2\lambda - \frac{3\sqrt{3}}{4}(1-2m) & \lambda^2 - \frac{9}{4} \end{vmatrix} = 0, \tag{1.9}$$

que simplificada nos dá:

$$\lambda^4 + \lambda^2 + \frac{27}{4}m(1-2m) = 0 \tag{1.10}$$

e esta possui solução na forma quadrática dada por

$$\lambda^2 = \frac{-1 \pm \sqrt{(1)^2 - 4\cdot 1\cdot \frac{27}{4}m(1-m)}}{2} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{1 - 27m(1-m)} \tag{1.11}$$

e α e β serão então limitadas se λ for imaginário puro. Devemos então escolher m de forma que $\lambda^2 < 0$, que nos leva a considerar

$$1 - 27m(1-m) \geq 0, \tag{1.12}$$

mas lembrando que $m < \frac{1}{2}$ então para que o equilíbrio seja estável, devemos ter $1 - 27m(1-m) < 1$.

Resolvendo esta equação e levando em conta a condição $m < \frac{1}{2}$, determinamos $m \leq 0.0385$. Assim, o movimento é **estável** se m não exceder 0.0385. A outra raiz do polinômio acima é aproximadamente 0.9614, sendo então excluída devido a imposição de que $m < \frac{1}{2}$.

Caso II: Movimento em torno de L_1

Consideremos a figura 1.2.

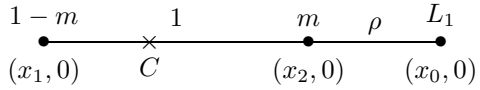


Figura 1.2: Solução Colinear.

Definimos

$$x_0 - x_1 = 1 + \rho = \rho_1, \quad x_0 - x_2 = \rho = \rho_2, \quad y_0 = z_0 = 0.$$

Assim as derivadas parciais são dadas por

$$\begin{aligned}
(U_{xx})_0 &= 1 + \frac{2(1-m)}{(1+\rho)^3} + \frac{2m}{\rho^3}, \\
(U_{yy})_0 &= 1 - \frac{(1-m)}{(1+\rho)^3} - \frac{m}{\rho^3}, \\
(U_{zz})_0 &= -\frac{(1-m)}{(1+\rho)^3} - \frac{m}{\rho^3},
\end{aligned}$$

$$(U_{xy})_0 = (U_{yx})_0 = (U_{xz})_0 = (U_{zx})_0 = (U_{yz})_0 = (U_{zy})_0 = 0.$$

Definimos

$$f = \frac{(1-m)}{(1+\rho)^3} + \frac{m}{\rho^3}. \tag{1.13}$$

Substituindo as derivadas acima nas equações do movimento e utilizando f como

acima, encontramos

$$\begin{aligned} \ddot{\alpha} - 2\dot{\beta} &= \alpha[1+2f], \\ \ddot{\beta} + 2\dot{\alpha} &= \beta[1-f], \\ \ddot{\gamma} &= -f\gamma. \end{aligned} \tag{1.14}$$

Novamente a equação em γ nos mostra que, perpendicularmente ao plano-xy, o movimento é periódico com freqüência $\omega = \sqrt{f}$ e é dado pela equação

$$\gamma = c_3 \cos\sqrt{f}t + c_4 \operatorname{sen}\sqrt{f}t, \tag{1.15}$$

onde os c_i são constantes de integração.

As equações em α e β são homogêneas com coeficientes constantes. Tomemos como solução $\alpha = Ae^{\lambda t}$ e $\beta = Be^{\lambda t}$.

Substituindo nas equações do movimento ficamos com

$$A[\lambda^2 - (1+2f)] + B[-2\lambda] = 0, \tag{1.16}$$

$$A[2\lambda] + B[\lambda^2 - (1-f)] = 0, \tag{1.17}$$

que possuem solução não trivial para A e B se

$$\begin{vmatrix} \lambda^2 - (1+2f) & -2\lambda \\ 2\lambda & \lambda^2 - (1-f) \end{vmatrix} = 0. \tag{1.18}$$

Se resolvermos o determinante acima, encontramos

$$\lambda^4 + (2-f)\lambda^2 + (1+2f)(1-f) = 0. \tag{1.19}$$

Assim, com a condição imposta para a massa m e a definição de f, temos que

$$(1+2f)(1-f) < 0. \tag{1.20}$$

Logo,

$$\lambda^2 = \frac{-(2-f) \pm \sqrt{(2-f)^2 - 4(1+2f)(1-f)}}{2} \tag{1.21}$$

é positivo quando é feita a soma e negativo quando é feita a subtração. As duas raízes numéricas são iguais com sinais opostos e as duas restantes são imaginárias puras.

Tomemos as raízes como sendo

$$\lambda_1 = a, \quad \lambda_2 = -a, \quad \lambda_3 = bi, \quad \lambda_4 = -bi,$$

onde

$$a = \sqrt{\frac{-(2-f) + \sqrt{(2-f)^2 - 4(1+2f)(1-f)}}{2}},$$

$$b = \sqrt{\frac{(2-f) + \sqrt{(2-f)^2 - 4(1+2f)(1-f)}}{2}}.$$

As soluções para α e β são

$$\alpha = A_1 e^{at} + A_2 e^{-at} + A_3 e^{ibt} + A_4 e^{-ibt} \tag{1.22}$$

e

$$\beta = B_1 e^{at} + B_2 e^{-at} + B_3 e^{ibt} + B_4 e^{-ibt}, \tag{1.23}$$

onde os B_j estão relacionados com os A_j na forma

$$B_j = \left(\frac{\lambda_j^2 - (1+2f)}{2\lambda_j}\right) A_j, \quad j = 1, 2, 3, 4, \tag{1.24}$$

obtidos de (1.16).

Os termos e^{at} e e^{-at} nos dizem que o ponto L_1 é um ponto de equilíbrio **instável** já que α e β não são limitados.

Podemos, entretanto, mostrar que por uma escolha apropriada das condições iniciais para o movimento em torno de L_1, esse ponto pode se tornar em um ponto de estabilidade.

Para simplificar, tomemos

$$B_1 = cA_1, \quad B_2 = -cA_2, \quad B_3 = idA_3, \quad B_4 = -idA_4, \tag{1.25}$$

onde

$$c = \frac{a^2 - (1+2f)}{2a} \quad \text{e} \quad d = \frac{b^2 + (1+2f)}{2b}. \tag{1.26}$$

Então, as equações de α e β, juntamente com as respectivas velocidades, são

$$\alpha = A_1 e^{at} + A_2 e^{-at} + A_3 e^{ibt} + A_4 e^{-ibt}, \tag{1.27}$$

$$\beta = cA_1 e^{at} - cA_2 e^{-at} + idA_3 e^{ibt} - idA_4 e^{-ibt}, \tag{1.28}$$

$$\dot{\alpha} = aA_1 e^{at} - aA_2 e^{-at} + ibA_3 e^{ibt} - ibA_4 e^{-ibt}, \tag{1.29}$$

$$\dot{\beta} = acA_1 e^{at} + acA_2 e^{-at} - bdA_3 e^{ibt} - bdA_4 e^{-ibt}. \tag{1.30}$$

Tomando os deslocamentos e velocidades iniciais como sendo α_0, β_0, $\dot{\alpha_0}$ e $\dot{\beta}_0$ em $t = 0$, ficamos com

$$\alpha_0 = A_1 + A_2 + A_3 + A_4, \tag{1.31}$$

$$\beta_0 = c(A_1 - A_2) + id(A_3 - A_4), \tag{1.32}$$

$$\dot{\alpha_0} = a(A_1 - A_2) + ib(A_3 - A_4), \tag{1.33}$$

$$\dot{\beta}_0 = ac(A_1 + A_2) - bd(A_3 + A_4). \tag{1.34}$$

Se o movimento deve ser limitado e periódico, devemos ter $A_1 + A_2 = 0$ e $A_1 - A_2 = 0$. Assim, $A_1 = A_2 = 0$.

Com estas restrições, das equações (1.31-1.32) encontramos A_3 e A_4 sob a forma

$$A_3 = \frac{\alpha_0}{2} - \frac{i\beta_0}{2d} \quad \text{e} \quad A_4 = \frac{\alpha_0}{2} + \frac{i\beta_0}{2d}. \tag{1.35}$$

As equações de α e β são então

$$\alpha = \left(\frac{\alpha_0}{2} - \frac{i\beta_0}{2d}\right) e^{ibt} + \left(\frac{\alpha_0}{2} + \frac{i\beta_0}{2d}\right) e^{-ibt}, \tag{1.36}$$

$$\beta = id\left(\frac{\alpha_0}{2} - \frac{i\beta_0}{2d}\right) e^{ibt} - id\left(\frac{\alpha_0}{2} + \frac{i\beta_0}{2d}\right) e^{-ibt} \tag{1.37}$$

que, por meio da conhecida relação de Euler, estas podem ser simplificadas para

$$\alpha = \alpha_0 \cos bt + \frac{\beta_0}{d} \operatorname{sen} bt, \tag{1.38}$$

$$\beta = \beta_0 \cos bt - d\alpha_0 \operatorname{sen} bt. \tag{1.39}$$

Estas são as equações paramétricas da trajetória da massa infinitesimal em torno de L_1. De acordo com as equações acima o movimento é estável, e portanto L_1 é agora um **ponto de estabilidade**.

Agradecimentos: Agradecemos ao nosso orientador Prof. Dr. Tadashi Yokoyama, docente do DEMAC – Departamento de Estatística, Matemática Aplicada e Computação do IGCE – Unesp Rio Claro, que além de orientar nos ajudou com muita dedicação, incentivando-nos durante todo o tempo em que estivemos trabalhando juntos. Em particular, a atenção voltada ao desenvolvimento do nosso plano de atividades do Projeto de Iniciação Científica do ano de 2005, o qual originou este trabalho. Tal p é parte do plano de pesquisa do Programa de Educação Tutorial – PET do curso de Matemática, programa onde mantemos vínculo como bolsistas. Agradecemos também aos demais professores pelo incentivo e àqueles que contribuíram de forma direta ou indireta na confecção deste trabalho.

Abstract: The aim of this work is just to present some well known solutions of the Restricted Three Body Problem (RTBP). Our presentation is done in a quite elementary way, so that, it is addressed to beginners, undergraduate students who may be interested in some basic topics of two types of stationary solutions of the RTBP. All the material here collect can be found in almost any elementary text book of Celestial Mechanics. Let us consider two point masses (primaries) and a third one (massless) which is under the action the primaries. In this way, it is well known that two particular stationary solutions arise: equilateral triangle solution an collinear solutions.

Usually, the first is a stable solution provided that the masses of the primaries obey some convenient relation. The second class of the solutions are distributed on a straight line connecting the primaries and usually they are unstable.

In this presentation we discuss, very briefly, the mathematical formulation of the basic aspects of the stability of these stationary points (Lagrangian solutions). Using elementary concepts of ordinary differential equations (EDO) the reader is guided to convince himself about the stability or instability of these

solutions.

Keywords: Three-Body Problem, Restricted Three-Body Problem, Lagrangian Points, Stationary Solution, Collinear Solution, Equilateral-Triangle Solution.

Referências Bibliográficas

[1] Mc Cuskey, S.W., *Introduction to Celestial Mechanics*, Addison-Wesley Publishing Co, Massachusets, 1963.

[2] Brouwer D., Clemence, G., *Methods of Celestial Mechanics*, Editora Academic Press, 1961.

[3] Moulton, F.R., *An Introduction to Celestial Mechanics*, The Macmillan Company, NY.

[4] De Luca, N., *Mecânica Celeste*, Editora da Universidade Federal do Paraná, Curitiba, 1982.

Extensão de Aplicações

Eliana Vieira Norte*
Orientador(a): Prof. Dr. Vanderlei Marcos do Nascimento†

Resumo: Uma questão muito importante na Matemática é saber quando é possível estender uma aplicação continuamente. Estudamos esta questão relacionando-a com o número de voltas de uma aplicação, do que pudemos obter vários resultados interessantes da Topologia Algébrica como, por exemplo, provar que não existe retração de um intervalo fechado sobre sua fronteira.

Palavras-chave: Extensão de funções, número de voltas.

1 Resultados Básicos

Definição 1. Um caminho γ em $U \subseteq \mathbb{R}^2$ é uma aplicação contínua definida num intervalo fechado da reta e tomando valores em U.

Definição 2. Se $\delta : [a,b] \to U$ e $\gamma : [a,b] \to U$, são caminhos com os mesmos pontos finais, definimos uma homotopia de γ para δ como uma aplicação contínua $H : [a,b] \times [0,1] \to U$ tal que:

$$H(t,0) = \gamma(t) \quad \text{e} \quad H(t,1) = \delta(t), \quad a \leq t \leq b;$$

$$H(a,s) = \gamma(a) = \delta(a) \quad \text{e} \quad H(b,s) = \gamma(b) = \delta(b), \quad 0 \leq s \leq 1.$$

Se γ e δ são caminhos fechados em U, definimos uma homotopia de γ para δ como uma aplicação contínua $H : [a,b] \times [0,1] \to U$ tal que:

$$H(t,0) = \gamma(t) \quad \text{e} \quad H(t,1) = \delta(t), \quad a \leq t \leq b;$$

$$H(a,s) = H(b,s)), \quad 0 \leq s \leq 1.$$

*Bolsista FAPESP – Processo 01/14179-5
†Orientadora do projeto FAPESP: Profa. Dra. Alice Kimie Miwa Libardi

Definição 3. Para qualquer caminho $\gamma : [a, b] \to \mathbb{R}^2 - \{P\}$, definimos o número de voltas $W(\gamma, P)$ como segue:

1. Subdividimos o intervalo em $a = t_0 \leq t_1 \leq \cdots \leq t_n = b$, tal que cada subintervalo $[t_{i-1}, t_i]$ é levado em algum setor com vértice em P (tal subdivisão é garantida pelo lema de Lebesgue). Assim, cada ponto da imagem de γ está em algum tal setor.

2. Escolhemos um setor U_i contendo $\gamma([t_{i-1}, t_i])$ e uma correspondente função ângulo θ_i em U_i, para $1 \leq i \leq n$. Seja $P_i = \gamma(t_i)$, $0 \leq i \leq n$. Definimos

$$\begin{aligned} W(\gamma, P) &= \frac{1}{2\pi}[(\theta_1(P_1) - \theta_1(P_0)) + \cdots + (\theta_n(P_n) - \theta_n(P_{n-1}))] \\ &= \frac{1}{2\pi}\sum_{i=1}^{n}(\theta_i(P_i) - \theta_i(P_{i-1})). \end{aligned}$$

Usaremos também os seguintes resultados:

Teorema 4. *Dois caminhos γ e δ em $\mathbb{R}^2 - \{P\}$ são homotópicos se, e somente se, $W(\gamma, P) = W(\delta, P)$.*

Exercício 5. Sejam F_0 e F_1 aplicações de uma circunferência C em U, correspondendo aos caminhos γ_0 e γ_1 de $[0, 1]$ em U. Prove que γ_0 e γ_1 são homotópicos através de caminhos fechados se, e somente se, F_0 e F_1 são aplicações homotópicas, isto é, existe uma aplicação contínua $H : C \times [0, 1] \to U$, com $H(P, 0) = F_0(P)$ e $H(P, 1) = F_1(P)$, para qualquer $P \in C$.

Prova: Suponhamos que F_0 e F_1 sejam homotópicas. Seja $H : C \times [0, 1] \to U$ uma homotopia entre F_0 e F_1. Definimos $\widetilde{H} : [0, 1] \times [0, 1] \to U$ por $\widetilde{H}(t, s) = H(\phi(t), s)$, a qual é uma homotopia entre γ_0 e γ_1, pois $\widetilde{H}(t, 0) = H(\phi(t), 0)$, mas $H(\phi(t), 0) = F_0(\phi(t)) = \gamma_0(t)$, pois H é uma homotopia e $\widetilde{H}(t, 1) = H(\phi(t), 1) = \gamma_1(t)$.

Logo, $\widetilde{H}$ é uma homotopia entre γ_0 e γ_1.

Suponhamos agora que γ_0 e γ_1 sejam homotópicas. Seja $\widetilde{H} : [0, 1] \times [0, 1] \to U$ uma homotopia entre γ_0 e γ_1.

Definimos $H : C \times [0,1] \to U$ uma homotopia entre F_0 e F_1 dada por $H(P,s) = \widetilde{H}(t,s)$, onde $\phi(t) = P$. Notemos que H está bem definida pois, dado $P \neq (0,1) \in C$ existe um único $t \in [0,1]$ tal que $\phi(t) = P$ e $\phi(t) = P = (0,1)$ se, e somente se, $t = 0$ ou $t = 1$, mas $\widetilde{H}(0,s) = \widetilde{H}(1,s)$. ∎

2 Resultado Principal

Teorema 6. *Suponhamos que C seja a fronteira do disco fechado D e $F : C \to \mathbb{R}^2 - \{P\}$ seja uma aplicação contínua. Então F pode ser estendida a uma aplicação contínua de D em $\mathbb{R}^2 - \{P\}$ se, e somente se, $W(F,P) = 0$.*

Prova: Sejam D o disco de raio r e centro (x_0, y_0) e $\gamma : [0,1] \to \mathbb{R}^2 - \{P\}$ o caminho correspondente a F. Se $\widetilde{F} : D \to \mathbb{R}^2 - \{P\}$ é uma tal extensão de F, então

$$H(t,s) = \widetilde{F}((x_0,y_0) + sr(\cos(2\pi t), \operatorname{sen}(2\pi t))), \quad 0 \leq t, s \leq 1,$$

nos dá uma homotopia entre γ e o caminho constante $\widetilde{F}((x_0,y_0))$. Essa homotopia está definida em $I \times I$ com valores em $\mathbb{R}^2 - \{P\}$ e como o número de voltas do caminho constante é zero, então, pelo teorema 4, segue o resultado.

Reciprocamente, seja $F : C \to \mathbb{R}^2 - \{P\}$ uma aplicação contínua em C tal que $\gamma = F \circ \phi$. Seja $\beta : [0,1] \to \mathbb{R}^2 - \{P\}$ um caminho constante. Como $W(\gamma, P) = 0$ então γ é homotópico a β e portanto $W(\beta, P) = 0$.

Seja $\widetilde{F} : C \to \mathbb{R}^2 - \{P\}$ uma aplicação contínua em C tal que $\beta = \widetilde{F} \circ \phi$. Pelo exercício anterior, as aplicações $\widetilde{F}$ e F são homotópicas.

Mostremos que se $F : C \to \mathbb{R}^2 - \{P\}$ é homotópica a uma aplicação constante então F estende-se continuamente ao disco fechado.

Suponhamos que $H : C \times I \to \mathbb{R}^2 - \{P\}$ seja uma homotopia entre F e a aplicação constante $\widetilde{F}$. Consideremos $\psi : C \times I \to D$, definida por $\psi(x,t) = (1-t)x$, ψ é contínua e sobrejetora em $C \times I$.

Para $x, x' \in C$ e $t, t' \in [0,1]$, só se pode ter $(1-t)x = (1-t')x'$ quando $(x,t) = (x',t')$, ou então quando $t = t' = 1$. Portanto, $(1-t)x = (1-t)x'$

implica $H(x,t) = H(x',t')$.

Assim, $\widetilde{F}((1-t)x) = H(x,t)$ define, sem ambigüidade, uma aplicação $\widetilde{F} : D \to \mathbb{R}^2 - \{P\}$, tal que $\widetilde{F} \circ \psi = H$. Para todo $x \in C$ tem-se

$$\widetilde{F}(x) = \widetilde{F}((1-0)x) = H(x,0) = F(x).$$

Logo, $\widetilde{F}$ estende F. Como $C \times I$ e D são compactos e ψ é contínua e sobrejetora então $\widetilde{F} : D \to \mathbb{R}^2 - \{P\}$ é uma aplicação contínua se, e somente se, $\widetilde{F} \circ \psi$ é contínua. ■

Abstract: An important question in Mathematics is to know whether is possible to extend continuously a map. We learned how this question is related to the winding number of a map, then we could solve several exercises that are indeed interesting results of the Algebraic Topology.

Keywords: Extension of applications, winding number.

Referências Bibliográficas

[1] Kosniowski, C., *A First Course in Algebraic Topology*. Cambridge University Press, 1980.

[2] Fulton, W., *Algebraic Topology. A first course*. Springer Verlag, 1995.

Invariantes para Nós

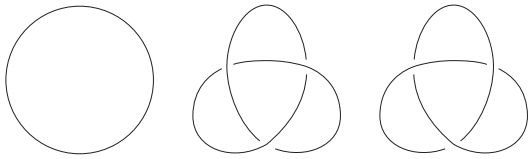
Erika Capelato*
Orientador(a): Profa. Dra. Alice Kimie Miwa Libardi

Resumo: Neste trabalho apresentamos dois invariantes para a classificação de Nós: o grupo fundamental do Nó e o número de coloridos de um Nó.

Palavras-chave: Nós, equivalência de Nós, invariantes.

1 Introdução

A teoria de Nós é um ramo importante dentro da Topologia. Intuitivamente um Nó pode ser pensado como um pedaço de elástico fino cujas extremidades são coladas, como por exemplo um círculo, também chamado de Nó trivial (figura 1.1(a)), um trevo direito (figura 1.1(b)) ou um trevo esquerdo (figura 1.1(c)).



(a) (b) (c)

Figura 1.1: (a) Nó trivial, (b) Trevo direito, (c) Trevo esquerdo.

Suponha que você está caminhando sobre o Nó e como ele é homeomorfo a S^1, você vai verificar que qualquer que seja o Nó, o caminho percorrido tem a propriedade de ser um caminho contínuo e fechado. Assim, um Nó é mais interessante se for visto do lado de fora. Formalmente um Nó é um subespaço do $\mathbb{R}^3$ homeomorfo a S^1.

Uma preocupação que toda teoria em Matemática tem é com a classificação. Ela é feita em geral usando-se relações de equivalência sobre os objetos. No nosso caso a classificação dos Nós será feita usando-se duas definições de equivalências.

*Bolsista PIBIC-CNPq

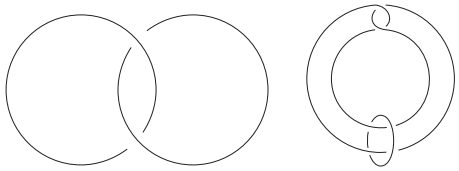
Observe que não é possível obter um trevo direito a partir de um trevo esquerdo através de deformações que podemos fazer com um pedaço de elástico sem cortar e colar de novo.

Mas a reflexão nos dá um homeomorfismo entre o trevo direito e o trevo esquerdo. Isto sugere uma nova definição de equivalência sobre o conjunto dos Nós.

Um invariante pode ser um número, um grupo ou uma propriedade que se associa a um determinado objeto satisfazendo a seguinte condição: *Objetos equivalentes têm os respectivos invariantes iguais.*

Desta forma só podemos garantir que se os invariantes são diferentes então os Nós não são equivalentes.

Se considerarmos vários Nós juntos obtemos os enlaçamentos, tais como o enlaçamento de Hopf (figura 1.2(a)), de Whitehead (figura 1.2(b)) e os anéis de Borromeo (figura 1.3).



(a) (b)

Figura 1.2: Enlaçamentos: (a) de Hopf, (b) de Whitehead.

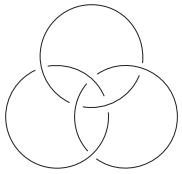


Figura 1.3: Anéis de Borromeo.

O estudo de enlaçamentos é uma importante linha de pesquisa em Topologia, porém não os consideraremos neste trabalho.

2 Definições e resultados

Neste capítulo serão apresentados definições e resultados necessários ao desenvolvimento do trabalho.

Definição 1. Um Nó K é um subespaço do $\mathbb{R}^3$ homeomorfo a S^1, ou seja existe um homeomorfismo $f : S^1 \to K \subset \mathbb{R}^3$.

Definição 2. Dois Nós K_1 e K_2 são similares se existe um homeomorfismo $h : \mathbb{R}^3 \to \mathbb{R}^3$ tal que $h(K_1) = K_2$.

Vamos apresentar uma maneira geométrica de como uma base induz uma orientação no espaço, necessária para a próxima definição.

Dada uma base $E = \{\vec{e_1}, \vec{e_2}, \vec{e_3}\}$ no espaço, seja β um plano contendo os representantes dos vetores $\vec{e_1}$ e $\vec{e_2}$ da base e seja O um ponto de β. A reta que passa por O e dá a direção do vetor $\vec{e_1}$, divide o plano em duas regiões. Esse plano por sua vez divide o espaço em duas regiões, a que contém o ponto $O+\vec{e_3}$ e a que não o contém. Colocamos a mão direita com os dedos abertos no sentido do vetor $\vec{e_1}$ de modo que a palma da mão esteja voltada para a região do plano que contém o ponto $O + \vec{e_2}$ e giramos de $\vec{e_1}$ para $\vec{e_2}$, nesta região. Assumimos que o ponto $O + \vec{e_3}$ está na região do espaço indicado pelo polegar.

Se considerarmos uma outra base $F = \{\vec{f_1}, \vec{f_2}, \vec{f_3}\}$ para o espaço e procedermos de modo análogo ao que foi feito para a base $E = \{\vec{e_1}, \vec{e_2}, \vec{e_3}\}$ dizemos que E e F possuem a mesma orientação se o ponto $O + \vec{f_3}$ também está na região indicada pelo polegar; caso contrário, dizemos que E e F têm orientações opostas. Em geral convenciona-se que uma base é positiva se o ponto $O + \vec{e_3}$ está na região do plano indicada pelo polegar. Caso contrário dizemos que ela é negativa.

Definição 3. Dois Nós K_1 e K_2 são equivalentes se existe um homeomorfismo $h : \mathbb{R}^3 \to \mathbb{R}^3$ que preserva a orientação e tal que $h(K_1) = K_2$.

A figura 1.4 mostra que o trevo direito não é equivalente ao trevo esquerdo.

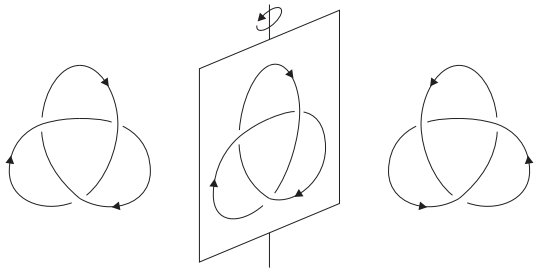


Figura 1.4: Não equivalência dos trevos direito e esquerdo.

As relações das definições 2 e 3 são de equivalência.

Definição 4. Um ponto $x \in \mathbb{R}^2$ é um ponto de cruzamento de um Nó se $p^{-1} \cap K$ consiste de dois ou mais pontos, onde $p : \mathbb{R}^3 \to \mathbb{R}^2$ é a aplicação projeção. Se $p^{-1} \cap K$ consiste de dois pontos, $x \in \mathbb{R}^2$ é um ponto duplo.

Definição 5. Sejam K um Nó e $\hat{K}$ a projeção de K. Esta projeção é chamada projeção regular ou diagrama regular se:

(i) $\hat{K}$ tem um número finito de interseções e

(ii) se Q é um ponto de interseção de $\hat{K}$, então Q é um ponto duplo.

Um dos invariantes para Nós é o grupo fundamental do seu complementar $\mathbb{R}^3 - K$, chamado grupo fundamental do Nó. Faremos a seguir uma breve exposição sobre o grupo fundamental de um espaço topológico X.

Definição 6. Sejam X um espaço topológico e $x \in X$. Um caminho $f : I = [0,1] \to X$ é fechado com ponto base x se $f(0) = f(1) = x$.

Sejam f e g dois caminhos fechados com ponto base x. Dizemos que f e g são equivalentes se existe uma função $F : I \times I \to X$ tal que $F(t,0) = f(t)$ e $F(t,1) = g(t)$, $t \in I$; $F(0,s) = f(0)$ e $F(1,s) = f(1)$, $s \in I$.

Denotamos por $[f]$ a classe de equivalência de um caminho fechado f e

definimos o produto de classes de equivalência por $[f][g] = [f * g]$, onde

$$(f * g)(t) = \begin{cases} f(2t) & 0 \leq t \leq 1/2 \\ g(2t-1) & 1/2 \leq t \leq 1 \end{cases}.$$

O conjunto das classes de equivalências de caminhos fechados com ponto base x é denotado por $\Pi(X, x)$. Com a operação definida acima o conjunto satisfaz os axiomas para um grupo e é chamado grupo fundamental de X com ponto base x.

O grupo fundamental do Nó é o grupo fundamental do seu complementar, $\Pi(\mathbb{R}^3 - K)$.

O próximo resultado mostra uma importante propriedade envolvendo o grupo fundamental.

Teorema 7. *Se $f : X \to Y$ é um homeomorfismo entre os espaços topológicos X e Y então $f_* : \Pi(X, p) \to \Pi(Y, f(p))$ é um isomorfismo, para cada ponto p em X.*

Prova: Seja $f_* : \Pi(X, p) \to \Pi(Y, f(p))$ definida por $f_*[g] = [fg]$, onde $[g] \in \Pi(X, p)$. Mostremos que f_* é um homomorfismo.

Dados $[h], [g] \in \Pi(X, p)$,

$$f_*([h][g]) = f_*[h * g] = [f(h * g)] = [fh * fg] = [fh][fg] = f_*[h]f_*[g].$$

Mostremos agora que f_* é bijetora.

Como f é um homeomorfismo existe f^{-1}. Sejam f_* induzida pela f e f_*^{-1} induzida por f^{-1}.

Seja $[g]$ qualquer classe de caminho fechado em $\Pi(X, p)$. Então $f_*^{-1}f_*[g] = (f^{-1}f)_*[g] = I_*[g]$ e $f_*f_*^{-1}[g] = (ff^{-1})_*[g] = I_*[g]$. Portanto, o teorema está demonstrado. ∎

Definição 8. Um Nó K é desnodado se existe um homeomorfismo $h : \mathbb{R}^3 \to \mathbb{R}^3$ tal que $h(K)$ é o círculo $\{(x, y, 0) \in \mathbb{R}^3; x^2 + y^2 = 1\}$ em $\mathbb{R}^2 \subset \mathbb{R}^3$.

3 Dois invariantes para Nós

3.1 O Grupo Fundamental $\Pi(\mathbb{R}^3 - K)$ do Nó

O primeiro invariante que usaremos para classificar os Nós é dado pelo grupo fundamental do Nó, $\Pi(\mathbb{R}^3 - K)$.

Suponha que são dados dois Nós K_1 e K_2 e que os grupos $\Pi(\mathbb{R}^3 - K_1)$ e $\Pi(\mathbb{R}^3 - K_2)$ não são isomorfos. Pelo teorema 7, $\mathbb{R}^3 - K_1$ e $\mathbb{R}^3 - K_2$ não são homeomorfos.

Mas se K_1 e K_2 são Nós equivalentes, então existe um homeomorfismo conforme a definição 3 e esta aplicação restrita a $\mathbb{R}^3 - K$ nos dá um homeomorfismo de $\mathbb{R}^3 - K_1$ sobre $\mathbb{R}^3 - K_2$, o que implica que seus respectivos grupos fundamentais são isomorfos.

Se um Nó é desnodado então seu grupo $\Pi(\mathbb{R}^3 - K)$ é isomorfo a $\mathbb{Z}$.

3.2 O número de coloridos de um Nó

Outro invariante é obtido associando-se um número para cada diagrama regular de Nós. Este número é o mesmo para diagramas diferentes do mesmo Nó e é obtido da seguinte maneira.

Suponha que $\hat{K}$ seja a projeção regular do Nó K tendo n pontos de cruzamento $P_1, P_2, \ldots, P_n$. Como cada P_i é a projeção dos pontos P_i' e P_i'' de K (figura 1.5), podemos por meio desses pontos dividi-lo em segmentos (ou curvas poligonais). A cada um desses segmentos podemos associar uma das três cores, vermelho, azul ou verde, de modo que satisfaçam:

1. Se A_l e A_k são como na figura 1.5 eles têm a mesma cor e

2. A_k (ou A_l), A_r e A_s ou todos têm a mesma cor associada ou cada um tem uma cor diferente associada a ele.

Se não há cruzamento onde exatamente duas cores chegam juntas dizemos que é um colorido próprio.

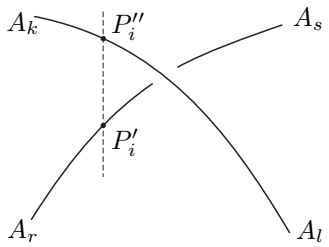


Figura 1.5

Não exigiremos portanto, que os invariantes distinguam todos os Nós não equivalentes, pois para alguns pares de Nós distintos, os valores dos invariantes podem coincidir.

Teorema 9. *O número de coloridos próprios diferentes de um diagrama de Nós é um invariante de Nós.*

Prova: Considere todas as possíveis transformações no cruzamento que podem ocorrer na deformação dos diagramas de Nós da figura 1.6.

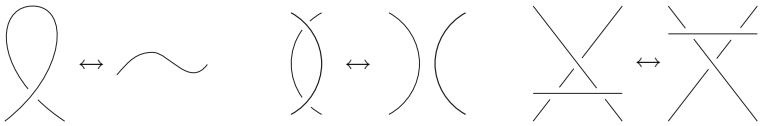


Figura 1.6

Suponha que um colorido próprio de um diagrama é dado e o diagrama é submetido a uma das transformações mostradas na figura 1.6. Vamos deixar o colorido do Nó como era, fora do lugar onde houve a transformação. Então as extremidades dos arcos mostradas nas figuras são coloridas. Devemos mostrar que este colorido pode ser estendido a um colorido próprio da parte do diagrama onde houve as mudanças.

Quando todas as extremidades estão pintadas de uma única cor não há problemas: há um único colorido.

Nos casos mostrados na figura 1.7, a extensão exigida do colorido onde houve

a mudança também é única.

Portanto, as transformações não mudam o número de coloridos e o teorema está provado. ■

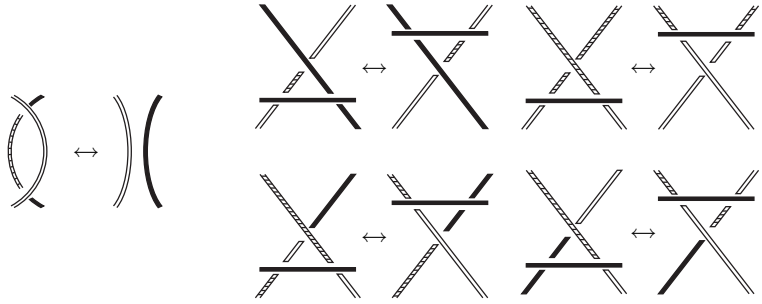


Figura 1.7

Exemplo 10. O trevo não pode ser desnodado.

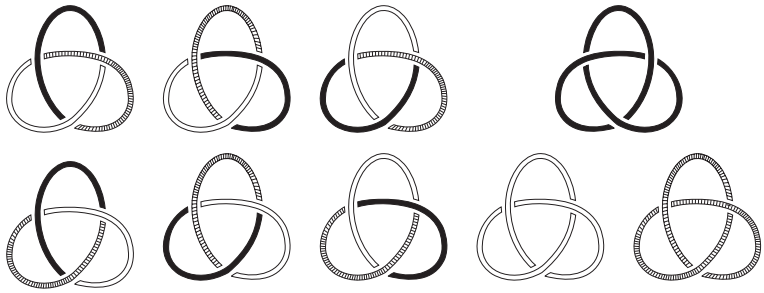


Figura 1.8

De fato, a figura 1.8 mostra que o número total de coloridos próprios do trevo usando três cores é seis. O primeiro arco pode ser pintado usando qualquer uma das três cores, o segundo usando qualquer uma das duas que restaram e o terceiro arco tem a cor determinada.

Além desses, temos três coloridos únicos que ao todo somam nove coloridos próprios. Como o círculo tem três coloridos próprios não há deformação do

trevo no Nó desnodado.

Agradecimentos: Agradeço à Alice Kimie Miwa Libardi pela orientação e ao Thiago de Melo pela arte gráfica.

Abstract: In this work we introduce two invariants to classifying knots: the fundamental group of the knot and the coloring number of a knot.

Keywords: Knot, knots equivalence, invariants.

Referências Bibliográficas

[1] Crowell, R.H., Fox, R.H., *Introduction to Knot Theory*. Editorial Board, First Edition, 1963.

[2] Farmer, W.D., Stanford, B.T., *Knots and surfaces: A guide to discovering Mathematics*. Mathematical World, vol. 6. American Mathematical Society, 1995.

[3] Kosniowski, C., *A First Course in Algebraic Topology*. Cambridge University Press, NY, 1980.

[4] Murasugy, K., *Knot theory and its applications*. Mirkhäuser, Boston-Basel-Berlin, 1996.

[5] Prasolov, V.V., *Intuitive Topology*. Mathematical World.Volume 4, 1995.

Esquema Criptográfico de Curvas Elípticas Simples

Fabio Antonio Araújo de Campos*

Orientador(a): Prof. Dr. Henrique Lazari

Resumo: Neste trabalho apresentamos alguns aspectos da teoria de criptografia sobre curvas elípticas em nível introdutório para fins educacionais. Para ilustrar o processo da codificação de algumas seqüências simples é apresentado um programa em Fortran.

Palavras-chave: Criptografia, curvas elípticas.

1 Introdução

Nosso interesse é apresentar de um modo prático e simples o método de criptografia sobre curvas elípticas. Não apresentaremos aqui todos os tópicos associados a curvas elípticas e tão pouco, chegaremos perto de cobrir parte dos comentários significativos sobre criptografia nestas curvas. Porém usaremos um exemplo simples de curvas elípticas, para com ele chegar ao que muitas vezes não é exposto nos textos sobre o assunto. Primeiramente iremos falar rapidamente sobre curvas elípticas, particularmente curvas elípticas sobre corpos finitos. Depois falaremos sobre a álgebra das curvas elípticas e sua utilização para a criptografia. Finalmente falaremos de criptografia utilizando o protocolo de chave pública e chave privada de Diffie-Hellmam [1] e para isso utilizaremos um exemplo de curva elíptica bem simples e a implementaremos em Fortran PowerStation 4.0, pelo fato desta linguagem ainda ser muito usada nos nossos cursos de graduação.

*Estagiário de I.C.

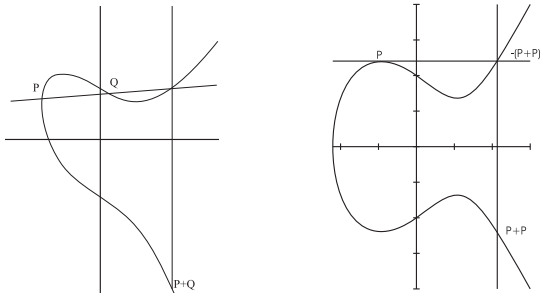
2 Curvas Elípticas

Para um corpo $\mathbb{F}$, uma curva elíptica $E(\mathbb{F})$ é o gráfico de uma equação da forma

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

em que as variáveis x, y e os coeficientes a, b, c, d, e estão todos em $\mathbb{F}$.

O fato interessante para nós em curvas elípticas é que a muitas delas podemos atribuir uma estrutura de grupo, que está associada a uma operação que denotaremos pelo símbolo $+$. Dados os pontos $P, Q \in E(\mathbb{F})$, traçaremos uma reta r ligando estes pontos. Então pelo terceiro ponto onde r intercepta a curva, traçaremos uma reta l vertical. O segundo ponto onde esta reta l interceptar a curva será o ponto $P + Q$ (figura 1.1(a)).



(a) (b)

Figura 1.1: (a) $y^2 + xy = x^3 + 1$, (b) $y^2 = x^3 - 4x + 5$.

Se quisermos somar P consigo mesmo basta tomarmos a reta tangente t passando por P. Então, pelo segundo ponto onde t interceptar a curva, traçaremos uma reta vertical v e chamaremos de $P + P$ ao segundo ponto em que v interceptar a curva (figura 1.1(b)).

Dada uma curva elíptica, se uma reta vertical interceptar a curva em dois pontos P_1 e P_2, então teremos $P_1 = -P_2$, porém se a reta interceptar a curva em apenas um ponto P, diremos que $P = -P$. Para entender o que queremos dizer com esta última afirmação, basta pensar no caso do número 1 em $\mathbb{Z}_2$.

Assim, verifica-se que a reta que une P a Q interceptará a curva novamente em $-(P+Q)$ e a reta tangente a curva pelo ponto P irá interceptar a curva novamente em $-(P+P)$.

Observe que se traçarmos uma reta vertical que intercepte a curva em dois pontos, esta reta não interceptará a curva em um terceiro ponto. A este fato associaremos o conceito de ponto no infinito, que denotaremos por $\mathcal{O}$, ou seja, dado $P \in E(\mathbb{F})$ teremos que $P - P = \mathcal{O}$.

Uma curva elíptica $E(\mathbb{F})$, associada com a operação $+$, pode representar um grupo cujos elementos consistem de pares (x, y) que satisfazem a equação que define a curva E, junto com o ponto no infinito $\mathcal{O}$. Mais tarde, definiremos as operações deste grupo para o corpo $\mathbb{F}_{2^m}$.

3 Criptografia sobre Curvas Elípticas

Geralmente as curvas elípticas definidas pela equação acima, são curvas sobre os números reais ou outros corpos infinitos, logo são geralmente curvas contínuas por partes. Porém, em criptografia, estaremos interessados em curvas elípticas sobre corpos finitos, o que muda muito o traço da curva, pois agora nossa curva será um conjunto discreto de pontos.

Sistemas criptográficos geralmente estão baseados em problemas matemáticos de tratamento difícil, ou seja, problemas que em condições ideais podem se tornar praticamente insolúveis, porém em criptografia isto não significa que sejam impossíveis de se resolver, mas apenas que o problema pode ser computacionalmente inviável. Na Segunda Guerra Mundial, a máquina Enigma, fabricada pelos alemães, era na época um sofisticado sistema criptográfico e muito difícil de ser quebrado (de ser decifrado), porém hoje este tipo de sistema não resistiria por muito tempo ao ataque de um computador pessoal moderno.

A criptografia sobre curvas elípticas baseia-se no problema do log discreto, que consiste em: dados dois pontos $P, Q \in (E(\mathbb{F}), +)$, encontrar o número n tal

que $nQ = P$, ou seja,

$$\underbrace{Q + Q + \cdots + Q}_{n \text{ vezes}} = P.$$

O problema do log discreto possui este nome porque, se estivéssemos trabalhando com a multiplicação usual, o problema se resumiria em achar o número n tal que $Q^n = P$, ou seja, achar o valor de $\log_Q P$.

Porém já existe um algoritmo eficiente para solucionar o problema do log discreto para uma classe de curvas, chamadas curvas anômalas. Para evitar tais curvas costuma-se utilizar uma certa classe de equações de curvas elípticas que caracterizam as operações sobre dois tipos de curvas, onde uma delas é considerada sobre corpos de característica dois e a outra sobre corpos de ordem prima, e estas curvas são chamadas Formas Normais. Para uma curva sobre um corpo de característica dois, segundo [2] as formas normais são dadas por:

1. (Formas Normais) $y^2 + xy = x^3 + cx^2 + e$, onde $e \neq 0$.
2. (Inversa) $(x, x + y)$.
3. (Operações do grupo) Dois pontos na curva são calculados de acordo com que eles se apresentam.
   (a) Se $P = -Q$, então $P + Q = \mathcal{O}$.
   (b) Se $P = Q$ então $2P = (x'', y'')$, onde $x'' = x^2 + \frac{e}{x^2}$ e $y'' = x''(x^2 + y)x^{-1} + x^2 + x''$.
   (c) Se $P \neq Q$ então $P + Q = (x'', y'')$, onde $x'' = m^2 + m + c + x + x'$, $y'' = m(x + x'') + y + x''$ e $m = \frac{(y'+y)}{(x'+x)}$.

4 Criptografia de Chave Pública

Segundo [1], um protocolo de chave pública e chave privada obedece às seguintes condições. Considere a letra K para denotar as chaves e a letra M para denotar a mensagem, onde E e D são transformações de cifragem e decifragem respectivamente.

1. Para todo $K \in \mathbf{K}$, E_K é a inversa de D_K.

2. Para todo $K \in \mathbf{K}$ e $M \in \mathbf{M}$, o algoritmo E_K e D_K é facilmente calculado.

3. Para quase todo $K \in \mathbf{K}$, é inviável calcular D_K de E_K.

4. Para todo $K \in \mathbf{K}$, é fácil o cálculo de E_K e D_K.

Pelo protocolo de chave pública e chave privada, um usuário P terá duas chaves relacionadas com ele, uma chave pública P_b e uma chave privada P_v, tal que

$$P_b = P_v G \tag{1.1}$$

onde G é um ponto da curva de ordem n, tal que n é um número primo grande que divide a ordem do grupo $(E(\mathbb{F}_q), +)$. Além disso, a chave privada deve ser escolhida no intervalo $[0, n-1]$. O item (2) acima diz que o par E_K e D_K estão em função de G, P_b e P_v.

Observe que E_K e D_K não devem ser transformações lineares, pois não estaríamos observando o item (3) acima. A natureza da operação $+$ que definimos em $E(\mathbb{F})$ indica um tipo especial de transformações como nossas candidatas. Se estivéssemos trabalhando com a operação usual de soma, estas transformações corresponderiam às translações.

Por (1.1), temos

$$P_b = P_v G \Rightarrow P_b - P_v G = \mathcal{O}.$$

Considere uma variável X que representará a nossa mensagem. Somando X em ambos os lados da expressão anterior temos

$$P_b - P_v G + X = X.$$

Note que à esquerda temos uma transformação aplicada a X, que resultará no próprio X, ou seja, esta expressão será equivalente à transformação identidade. Então, decompondo esta transformação em duas outras, obtemos

$$\begin{aligned} E_K(X) &= X + P_b, \\ D_K(Y) &= Y - P_v G. \end{aligned}$$

Mas note que um intruso poderia obter a mensagem X sem conhecer a chave secreta do destinatário P_v, bastando aplicar o elemento oposto de P_b à mensagem (uma vez que P_b é pública).

Porém, observe que para qualquer número inteiro λ, se o multiplicarmos em ambos os lados da expressão (1.1), teremos

$$\lambda P_b = \lambda P_v G \Rightarrow \lambda P_b - \lambda P_v G = \mathcal{O} \Rightarrow \lambda P_b - \lambda P_v G + X = X.$$

A expressão acima nos diz que o remetente pode escolher valores de λ aleatoriamente, dificultando assim o trabalho do interceptor da mensagem e eliminando o problema citado anteriormente. Porém isso não modificará em nada o trabalho do destinatário da mensagem, pois ele não precisará saber os valores de λ para decifrar a mensagem, no entanto sua chave secreta será essencial.

Então, tomaremos como candidatas às transformações de cifragem e decifragem, as transformações

$$\begin{aligned} E_{K\lambda}(X) &= (\lambda G, X + \lambda P_b), \\ D_K(Y, Z) &= Z - YP_v. \end{aligned}$$

Notemos que

$$D_K(E_{K\lambda}(X)) = D_K(\lambda G, X + \lambda P_b) = X + \lambda P_b - \lambda G P_v = X + \lambda P_b - \lambda P_b = X,$$

logo D_K é a inversa de $E_{K\lambda}$.

Mostramos como obter transformações de cifragem e decifragem relacionadas com um certo destinatário. O caso geral é análogo, pois se considerarmos um grupo de pessoas $x_1, x_2, \ldots, x_n$, que querem se comunicar utilizando o sistema de criptografia sobre curvas elípticas, elas devem seguir os seguintes passos.

1. Selecionar uma curva elíptica sobre $\mathbb{F}_q$ (onde de preferência, q deve ser primo ou potência de dois).

2. Escolher um ponto G de ordem n no grupo formado pelos pontos da curva elíptica, onde n é um número primo grande que divide a ordem do grupo.

3. Cada pessoa deve escolher um par de chaves P_{bi} e P_{vi} que serão as chaves pública e privada respectivamente, para $i = 1, 2, \ldots, n$, onde $P_{bi} = P_{vi}G$.

5 Como utilizar a rotina `Cifra`

A rotina `Cifra` foi feita com o propósito de servir como um exemplo simples de implementação em software, da teoria de criptografia sobre curvas elípticas. Esta rotina foi implementada em Fortran PowerStation 4.0, pelo fato desta linguagem ainda ser muito usada em nossos cursos de graduação.

Primeiramente tomamos a equação $y^2 + xy = x^3 + 1$ e a partir desta equação calculamos os pontos da curva elíptica sobre o corpo finito $\mathbb{F}_4$. Adicionando a este conjunto o ponto $\mathcal{O}$, obtemos assim o grupo

$$E(\mathbb{F}_4) = (\mathcal{O}, (0,1), (1,0), (1,1), (\alpha, 0), (\alpha+1, 0), (\alpha, \alpha), (\alpha+1, \alpha+1)).$$

Estes pontos foram obtidos das equações das formas normais, para corpos do tipo $\mathbb{F}_{2^m}$, [2]. Porém, para implementar os pontos do grupo $E(\mathbb{F}_4)$ em Fortran, interpretamos cada ponto como um vetor, ou seja, como cada coordenada em $\mathbb{F}_4$ corresponde a duas coordenadas em $\mathbb{F}_2$, logo teremos 4 bits para cada ponto da curva.

$$\begin{aligned} (0,1) &= 0010 & \qquad (1,0) &= 1000 \\ (1,1) &= 1010 & \qquad (\alpha,0) &= 0100 \\ (\alpha+1,0) &= 1100 & \qquad (\alpha,\alpha) &= 0101 \\ (\alpha+1,\alpha+1) &= 1111 \end{aligned}$$

Observe que neste método os pontos da curva é que são cifrados, logo dada uma mensagem temos que mapeá-la em pontos da curva elíptica e depois cifra-los. Em nosso exemplo, temos uma curva elíptica com sete pontos. Então para ilustrar, mapearemos a mensagem 'NÃO ATAQUE'. Assim tomaremos

N = 1111	A = 0010
O = 1100	T = 1010
Q = 1000	U = 0101
E = 0100	

Note que 4 bits não são suficientes para representar o alfabeto inteiro, pois só conseguiríamos representar no máximo 16 letras do alfabeto com 4 bits. Porém, como nosso interesse aqui é apenas ilustrar de uma forma didática a criptografia sobre curvas elípticas, utilizaremos 4 bits para representar as letras acima.

Para implementar este método utilizamos o protocolo de chave pública e chave privada de Diffie-Hellman. Supondo que iremos enviar a mensagem para um usuário X, temos que conhecer a sua chave pública, que denotaremos por P_X, e o gerador do grupo com o qual foram geradas as chaves P_X e n_X, onde n_X é a chave privada de X. No nosso exemplo iremos tomar $P_X = 1100$ e o gerador do grupo $G = 0100$.

Por exemplo, se quisermos cifrar a letra N utilizando o método descrito, temos que primeiro escolher um valor para λ, que na rotina será dado aleatoriamente. Tomando $\lambda = 3$ e lembrando que a letra N está associada com o ponto 1111 da curva e considerando $P_X = 1100$ com $n_X = 5$, podemos calcular o valor da transformação E_K no ponto 1111 através das equações das formas normais para corpos de característica 2,

$$\begin{aligned} \lambda G &= 3(0100) = 1111, \\ \lambda P_X &= 3(1100) = 0101, \\ X + \lambda P_X &= 1111 + 0101 = 1000. \end{aligned}$$

Logo a letra N será cifrada como 11111000.

Quando o destinatário da mensagem receber a seqüência de números, ele tomará os quatro primeiros números da seqüência e o somará 5 vezes, pois 5 é

a chave privada do destinatário. Então

$$YP_v = (1111)5 = 0100 \quad \text{e} \quad -YP_v = 0100,$$

logo $X = 1000 + 0100 = 1111$, que é justamente a nossa letra N inicial.

6 Executando a rotina `Cifra`

Quando executarmos a rotina `Cifra` aparecerá a mensagem *'Digite a chave pública do destinatário'*, então supondo-a conhecida deveremos digitar a chave pública do destinatário. Em nosso exemplo, temos a opção de quatro possíveis destinatários representados pelas possíveis chaves públicas $(\alpha, 0)$, (α, α), $(\alpha + 1, 0)$ e $(\alpha+1, \alpha+1)$. Tomaremos em particular a chave $(\alpha+1, 0)$, logo digitaremos o vetor 1100.

Observe que o vetor deve ser digitado em uma mesma linha, considerando um espaço entre as colunas.

Em seguida aparecerá a mensagem *'Digite o número de letras da mensagem'*. Deveremos então digitar o número de letras que a nossa mensagem terá, porém como nossa intenção é dar um exemplo simples, não devemos digitar uma mensagem muito grande, até mesmo porque a mensagem deverá conter somente o número de letras mapeadas acima.

Finalmente aparecerá a mensagem *'Digite um caracter'*. Agora basta digitar a mensagem desejada, porém cada letra da mensagem deve vir entre apóstrofo e a cada letra digitada deveremos teclar 'enter'. Os dígitos binários assim obtidos, representam o caracter cifrado.

Uma vantagem desta rotina é que podemos digitar cinco vezes um dado caracter, que ele será cifrado de maneira diferente em cada uma das cinco vezes, evitando assim a detecção de alguma espécie de padrão.

Listamos abaixo o programa em Fortran que executa o algoritmo da rotina `Cifra`.

```
c 234567
  Program Cifra
c Este programa cifra letras digitadas no teclado
c atraves de eq. de curvas elipticas
c Fabio Campos-mat
  character s,x,veja,car,car1,v,v1,msoma
  integer n,na,na8,i,xa,a,t,index
  dimension g(1,4),pr(1,4),veja(1,8),xa(1,4),m(15,1,8),p(15,1,4)
c
  mat(8,4),s1(1,4),car(8,1),mat1(8,4),x(15),car1(8,1),msoma(9,9),
  cv(1,9),v1(9,1),hhmat(8,4),a(0:9),pri(4,4)
  open(1,file='hmat1.dat',status='old')
  open(2,file='hcar1.dat',status='old')
  open(3,file='fabio.dat',status='old')
  open(4,file='hmat.dat',status='old')
  open(5,file='hsoma.dat',status='old')
  open(6,file='hhmat.dat',status='unknown')
  open(7,file='g1.dat',status='unknown')
  open(8,file='g2.dat',status='unknown')
  open(9,file='g3.dat',status='unknown')
  open(10,file='g4.dat',status='unknown')
  open(11,file='g5.dat',status='unknown')
  open(12,file='g6.dat',status='unknown')
  open(13,file='g7.dat',status='unknown')
  open(14,file='g8.dat',status='unknown')
  open(15,file='p1.dat',status='unknown')
  open(16,file='p2.dat',status='unknown')
  open(17,file='p3.dat',status='unknown')
  open(18,file='p4.dat',status='unknown')
  open(19,file='p5.dat',status='unknown')
  open(20,file='p6.dat',status='unknown')
  open(21,file='p7.dat',status='unknown')
  open(22,file='p8.dat',status='unknown')
  open(23,file='hcar.dat',status='unknown')
  open(24,file='pri.dat',status='unknown')
  open(25,file='pri1.dat',status='unknown')
  open(26,file='pri2.dat',status='unknown')
  open(27,file='pri3.dat',status='unknown')
  open(28,file='pri4.dat',status='unknown')
  open(29,file='gerador.dat',status='unknown')
  do k=1,4
     read(24,*) (pri(k,j),j=1,4)
  end do
  do k=1,8
     read(1,*) (mat1(k,j),j=1,4)
  end do
```

```
read(2,*) (car1(k,1),k=1,8)
do k=1,8
   read(3,*) car(k,1)
end do
read(23,*) (veja(1,l),l=1,8)
do l=1,8
   read(4,*) (mat(l,f),f=1,4)
end do
do k=1,9
   read(5,*) (msoma(k,j),j=1,9)
end do
read(5,*) (v(1,j),j=1,9)
do j=1,9
   read(5,*) v1(j,1)
end do
do j=1,8
   read(6,*) (hhmat(j,k),k=1,4)
end do
read(29,*) (g(1,j),j=1,4)
write(*,*)'Digite a chave publica do destinatario'
read(*,*) (pr(1,j),j=1,4)
write(*,*)'Digite o numero de letras da mensagem'
read(*,*) n
do i=1,n
   write(*,*)'Digite um caracter'
   read(*,*) x(i)
   call rand(index,a)
   na=a(index)
   do l=1,8
      if (x(i).eq.veja(1,l))then
         do t=1,4
          xa(1,t)=hhmat(l,t)
         end do
         call mod8(na,na8)
         do t=1,4
          if ((pr(1,1).eq.pri(t,1)).and.(pr(1,2).eq.pri(t,2)).and.
           c(pr(1,3).eq.pri(t,3)).and.(pr(1,4).eq.pri(t,4)))then
           read(24+t,*) (p(i,1,j),j=1,4)
          end if
         end do
         do k=1,16
          if (na8.eq.k)then
           read(k+6,*) (m(i,1,j),j=1,4)
           read(k+14,*) (p(i,1,j),j=1,4)
           goto 20
          end if
```

```
            end do
20          call soma(i,xa,p,mat1,car1,v,v1,msoma,car,mat,s)
            do t=1,8
             do j=1,4
              if (s.eq.car(t,1))then
              s1(1,j)=mat(t,j)
              m(i,1,4+j)= s1(1,j)
              end if
             end do
            end do
         end if
      end do
      write(*,*) (m(i,1,k),k=1,8)
   end do
   close(1)
   close(2)
   close(3)
   close(4)
   close(5)
   close(6)
   close(7)
   close(8)
   close(9)
   close(10)
   close(11)
   close(12)
   close(13)
   close(14)
   close(15)
   close(16)
   close(17)
   close(18)
   close(19)
   close(20)
   close(21)
   close(22)
   close(23)
   end
c  ****************************
   subroutine soma(i,xa,p,mat1,car1,v,v1,msoma,car,mat,s)
   character car2,car4,car,car1,s,msoma,v,v1
   integer i,xa
   dimension mat(8,4),xa(1,4),car(8,1),car1(8,1),mat1(8,4),
   cmsoma(9,9),v(1,9),v1(9,1),p(15,1,4)
   do k=1,8
      do j=1,4
```

```
         if ((xa(1,1).eq.mat(k,1)).and.(xa(1,2).eq.mat(k,2))
            c.and.(xa(1,3).eq.mat(k,3)).and.(xa(1,4).eq.mat(k,4)))then
            car2=car(k,1)
         end if
         if((p(i,1,1).eq.mat1(k,1)).and.(p(i,1,2).eq.mat1(k,2))
          c.and.(p(i,1,3).eq.mat1(k,3)).and.(p(i,1,4).eq.mat1(k,4)))then
          car4=car1(k,1)
         end if
      end do
   end do
   do k=1,9
      do j=1,9
         if ((car2.eq.v(1,k)).and.(car4.eq.v1(j,1)))then
            s=msoma(j,k)
         end if
      end do
   end do
   return
   end
c  ****************************
   subroutine mod8(na,na8)
   integer na,na8
   if (na.lt.8)then
      na8=na
      else
      do i=1,na
        if ((na-8*i).lt.8)then
          na8=na-8*i
          if (na8.eq.0)then
            na8=8
          end if
          goto 30
        end if
      end do
   end if
30 return
   end
c  ***************************
   subroutine rand(index,a)
   implicit none
   integer a(0:9),i,index
   integer count(1)
   real x
   a=0
   call system_clock(count(1))
   call random_seed(put=count)
```

```
   do 10 i=1,1000
      call random_number(x)
      index=int(x*100.)
      a(index)=a(index)+1
10 continue
   return
   end
```

O algoritmo acima foi feito com a intenção de servir como um exemplo simples de implementação em software da teoria de criptografia sobre curvas elípticas, por esta razão ele tem algumas peculiaridades. Note que apesar de usarmos uma curva sobre um corpo de característica dois, não implementamos as fórmulas das Formas Normais para corpos de característica dois para operar os pontos da curva no algoritmo. Ao invés disso, criamos um arquivo chamado `hmat` e nele colocamos uma tabela com todos os possíveis cálculos dos pontos da curva, ou seja, quando a rotina opera dois pontos do grupo ela percorre as linhas e as colunas da tabela para obter o valor desejado.

Note que, como nossa curva tem apenas 7 pontos, bastou realizar 64 operações para obter a tabela do grupo, porém este procedimento em uma implementação real se mostra inviável. Neste caso seria interessante implementar as fórmulas das Formas Normais, pois não iríamos mais precisar de um arquivo com uma tabela gigantesca.

A subrotina `soma` tem como objetivo operar os pontos solicitados pelo programa principal e depois devolvê-los. Já a subrotina `mod8` tem como objetivo, dado um número x, achar y tal que $x \equiv y \mod 8$ e a subrotina `rand` gera números aleatórios para o programa principal.

Abstract: In this paper we present some aspects of the theory of the elliptic curve cryptography in an introductory level for educational purposes. In order to illustrate the codification process of some simple sequences a fortran program is provided.

Keywords: Cryptography, elliptic curves.

Referências Bibliográficas

[1] Diffie, W., Hellman, M.E., *New Directions in Cryptography*, IEEE Transactions on information Theory, 1976.

[2] Leaning, J.S., *Algebra and Complexity Theory in Cryptography*, U.S. Patent and trademark Office - September, 2000.

[3] Moreno, D.E., Pereira, F.D., Chiaramonte, R.B., *Criptografia em Software e Hardware*, Novatec. São Paulo, 2005.

Códigos Cíclicos

Jussara Rodrigues Ciappina*
Orientador(a): Prof. Dr. Henrique Lazari

Resumo: Neste trabalho apresentamos um introdução às extensões de corpos e à teoria dos corpos finitos, o fundamento algébrico básico à teoria dos códigos corretores de erros lineares, especialmente os códigos cíclicos.

Palavras-chave: Corpo finito, código cíclico.

1 Introdução

Seja F_q um corpo finito contendo q elementos ($q \geq 2$). Representaremos os vetores de F_q^n por $(x_0, \ldots, x_{n-1})$.

Um subespaço vetorial $C \subset F_q^n$ é chamado de **código cíclico** se, para todo $c = (c_0, \ldots, c_{n-1}) \in C$, o vetor $(c_{n-1}, c_0, \ldots, c_{n-2})$ pertence a C.

Equivalentemente, o código linear C é um código cíclico se, dada a aplicação permutação de coordenadas

$$T : F_q^n \to F_q^n$$

definida por

$$T((c_0, c_1, \ldots, c_{n-1})) = (c_{n-1}, c_0, \ldots, c_{n-2}),$$

temos que $T(c) \in C$ para todo $c \in C$, ou seja, $T(C) \subset C$.

Definimos R_n como sendo o anel das classes residuais em $F_q[X]$ módulo $X^n - 1$, isto é,

$$R_n = \frac{F_q[X]}{\langle X^n - 1 \rangle}.$$

Um elemento de R_n é da forma

$$\overline{f(X)} = \{f(X) + g(X)(X^n - 1) : g(X) \in F_q[X]\}$$

*Bolsista FAPESP – Processo 03/12835-8

e a adição e a multiplicação em R_n são respectivamente definidas por

$$\overline{f_1(X)} + \overline{f_2(X)} = \overline{f_1(X) + f_2(X)},$$

$$\overline{f_1(X)} \cdot \overline{f_2(X)} = \overline{f_1(X) \cdot f_2(X)}.$$

R_n munido da multiplicação por escalares $\lambda \in F_q$, definida por

$$\lambda\overline{f(X)} = \overline{\lambda f(X)}$$

é um F_q-espaço vetorial de dimensão n com base

$$B = \{1, \overline{X}, \ldots, \overline{X^{n-1}}\}$$

e é isomorfo a F_q^n através da transformação linear

$$\Psi : F_q^n \to R_n$$

$$(a_0, \ldots, a_{n-1}) \mapsto \overline{a_0 + a_1X + \cdots + a_{n-1}X^{n-1}}.$$

Então, todo código linear $C \subset F_q^n$ pode ser interpretado como um elemento de R_n através de Ψ.

Denotaremos um corpo arbitrário por K.

Um ideal de $K[X]$ é da forma $I = \langle F(X) \rangle$, onde $F(X) \in K[X]$. Todo ideal de $K[X]$ é principal, logo, um ideal I de $K[X]$ pode ser gerado por vários polinômios $F(X)$. Existe uma relação entre tais polinômios: eles são associados. Assim, se $I \neq 0$, então existe um único polinômio mônico $F(X)$ em I, tal que $I = \langle F(X) \rangle$.

Enunciaremos alguns resultados necessários para os teoremas que são objetos do presente trabalho.

Teorema 1. *Os ideais do anel de classes residuais em K módulo um polinômio $P(X)$, $\dfrac{K[X]}{\langle P(X) \rangle}$, são da forma $I = \langle \overline{F(X)} \rangle$, onde $F(X)$ é um divisor de $P(X)$.*

$$I = \left\{ \overline{H(X)} \cdot \overline{F(X)} : \overline{H(X)} \in \frac{K[X]}{\langle P(X) \rangle} \right\} = \langle \overline{F(X)} \rangle.$$

Com isto, vamos determinar matrizes geradoras e matrizes verificação de paridade de códigos cíclicos em $\frac{K[X]}{\langle P(X)\rangle}$.

Seja $c = (c_0, \ldots, c_{n-1}) \in F_q^n$, temos que

$$T(c) = (c_{n-1}, c_0, \ldots, c_{n-2})$$

e

$$\begin{aligned}\Psi(T(c)) &= \overline{c_{n-1} + c_0X + \cdots + c_{n-2}X^{n-1}} \\ &= \overline{X} \cdot \overline{c_0 + c_1X + \cdots + c_{n-1}X^{n-1}} \\ &= \overline{X} \cdot \Psi(c).\end{aligned}$$

Lema 2. *Seja V um subespaço vetorial de R_n. Então V é um ideal de R_n se, e somente se, V é fechado pela multiplicação por $\overline{X}$.*

Teorema 3. *Um subespaço C de F_q^n é um código cíclico se, e somente se, $\Psi(C)$ é um ideal de R_n.*

Portanto, um código C em F_q é cíclico se, e somente se, $\Psi(C) = \langle\overline{g(X)}\rangle$, onde $g(X) \in F_q[X]$ é um divisor de $X^n - 1$.

Teorema 4. *Seja K um corpo. Existe uma bijeção entre os ideais de $\frac{K[X]}{\langle P(X)\rangle}$ e os divisores mônicos de $P(X)$.*

Prova: Seja A o conjunto dos ideais de $K[X]$ que contém $\langle p\rangle$. Como

$$J \in A \Leftrightarrow \exists f : J = \langle f\rangle \quad \text{e} \quad \langle p\rangle \subseteq J \Leftrightarrow f \mid p,$$

existe uma bijeção entre os elementos de A e os divisores mônicos de p. Seja B o conjunto dos ideais de $\frac{F_q[X]}{\langle p\rangle}$ e seja a função $\Phi : A \to B$.

Se $\langle f\rangle \in A$, $\langle f\rangle \neq \langle p\rangle$, temos que $f \mid p$ e $p \nmid f$.

$$\langle p\rangle \subseteq \langle f\rangle,$$

$\langle p\rangle$ é um subanel de $\langle f\rangle$.

Sejam $g \in \langle f \rangle$ e $\alpha p \in \langle p \rangle$.

$$g\alpha p = \alpha \underbrace{gp}_{\in \langle p \rangle} \in \langle p \rangle.$$

Logo, $\langle p \rangle$ é um ideal de $\langle f \rangle$. Tomemos $\Phi(\langle f \rangle) = \langle \overline{f} \rangle$. Já sabemos que todo ideal de $\dfrac{F_q[X]}{\langle p \rangle}$ é da forma $\langle \overline{f} \rangle$, portanto, Φ é sobrejetora.

Se $\Phi(\langle f \rangle) = \Phi(\langle g \rangle)$ então $f \sim g$, portanto, $\langle f \rangle = \langle g \rangle$ e assim Φ é injetora. ■

Denotaremos por $g(X)$ um divisor de $X^n - 1$ e $h(X) = \dfrac{X^n - 1}{g(X)}$.

Teorema 5. *Seja $I = \langle \overline{g(X)} \rangle$, onde $g(X)$ é um divisor de $X^n - 1$ de grau s. Temos que $B = \{\overline{g(X)}, \overline{Xg(X)}, \overline{X^2 g(X)}, \ldots, \overline{X^{n-s-1} g(X)}\}$ é uma base de I como espaço vetorial sobre F_q.*

Prova: Suponhamos que

$$a_0\overline{g(X)} + a_1\overline{Xg(X)} + \cdots + a_{n-s-1}\overline{X^{n-s-1}g(X)} = \overline{0}.$$

Logo, $\overline{g(X)a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}} = \overline{0}$. Se

$$g(X)(a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}) \neq 0$$

então $\partial(g(X)(a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1})) \leq n-1$. Portanto devemos ter $g(X)(a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}) = 0$. Logo, $a_0 = a_1 = \cdots = a_{n-s-1} = 0$. Segue que B é linearmente independente.

Se $\overline{f(X)} \in I$, temos que $f(X) \equiv d(X)g(X) \mod (X^n - 1)$. Pelo algoritmo da divisão, temos que $d(X) = h(X)c(X) + r(X)$, com $r(X) = a_0 + a_1X + \cdots + a_{n-s-1}X^{n-s-1}$. Logo, $f(X) \equiv d(X)g(X) \equiv c(X)h(X)g(X) + r(X)g(X) \mod (X^n - 1)$ e portanto

$$f(X) \equiv c(X)(X^n - 1) + r(X)g(X) \equiv r(X)g(X) \mod (X^n - 1).$$

Segue que $\overline{f(X)} = a_0\overline{g(X)} + a_1\overline{Xg(X)} + \cdots + a_{n-s-1}\overline{X^{n-s-1}g(X)}$, ou seja, B gera I sobre F_q. ■

Corolário 6. *Seja $g(X) = g_0 + g_1X + \cdots + g_sX^s$ um divisor de $X^n - 1$ de grau s. Se $I = \langle\overline{g(X)}\rangle$ então o código $C = \Psi^{-1}(I)$ tem matriz geradora*

$$G = \begin{pmatrix} \Psi^{-1}(\overline{g(X)}) \\ \Psi^{-1}(\overline{Xg(X)}) \\ \vdots \\ \Psi^{-1}(\overline{X^{n-s-1}g(X)}) \end{pmatrix} = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_s \end{pmatrix}.$$

Dado um polinômio $h(X) = h_0 + h_1X + \cdots + h_tX^t$ que divide $X^n - 1$, o polinômio recíproco de $h(X)$ é $h^*(X) = X^t h(1/X) = h_t + h_{t-1}X + \cdots + h_0X^t$.

Teorema 7. *Sejam K um corpo e $F(X), G(X) \in K[X]$ de grau n. Se $G(X)$ divide $F(X)$ então $G^*(X)$ divide $F^*(X)$.*

Prova: Suponhamos $F = UG$. Temos que

$$F^* = X^{\partial F}F(1/X) = X^{\partial U}U(1/X)X^{\partial G}G(1/X) = U^*G^*,$$

logo, G^* divide F^*. ∎

Como $-(X^n - 1) = (X^n - 1)^*$, segue que

$$hq = X^n - 1 \Rightarrow h^*q^* = (X^n - 1)^* = -(X^n - 1).$$

Assim, h^* também é um divisor de $X^n - 1$ e portanto é o polinômio gerador de algum código cíclico que identificaremos adiante.

Teorema 8. *Seja C um código cíclico onde $I = \langle\overline{g(X)}\rangle$, com $g(X)$ um divisor de $X^n - 1$. Então, $C^\perp$ é cíclico e $C^\perp = \Psi^{-1}(J)$, onde $J = \langle\overline{h^*(X)}\rangle$.*

Prova: Sejam

$$g(X) = g_0 + g_1X + \cdots + g_sX^s$$

e

$$h(X) = h_0 + h_1X + \cdots + h_{n-s}X^{n-s} = \frac{X^n - 1}{g(X)}.$$

Como $\partial h = n - s$, temos que $h_{n-s} \neq 0$. Sejam

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_s \end{pmatrix}$$

e

$$H = \begin{pmatrix} h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & h_{n-s} & h_{n-s-1} & \cdots & h_0 \end{pmatrix}.$$

As linhas de H são linearmente independentes (pois $h_{n-s} \neq 0$). Vamos mostrar que $G \cdot H^T = 0$. Seja $a = [a_1\ a_2\ \cdots\ a_n]$ uma linha qualquer de G. A i-ésima linha de G é da forma: $1 \leq i \leq n - s$,

$$a_1 = \cdots = a_{i-1} = 0,$$

$$a_i = g_0, \quad a_{i+1} = g_1, \quad a_{i+2} = g_2, \ldots, a_{i+s} = g_s,$$

$$a_{i+s+1} = a_{i+s+2} = \cdots = a_n = 0.$$

Seja $b = [b_1\ b_2\ \cdots\ b_n]$ uma coluna qualquer de H^T. A j-ésima coluna de H^T é da forma: $1 \leq j \leq s$

$$b_1 = \cdots = b_{j-1} = 0, \quad b_j = h_{n-s}, \quad b_{j+1} = h_{n-s-1},$$

$$b_{j+2} = h_{n-s-2}, \ldots, b_{j+(n-s)} = h_{n-s-(n-s)} = h_0,$$

$$b_{j+(n-s)+1} = b_{j+(n-s)+2} = \cdots = b_n = 0.$$

Temos que $a \cdot b = \sum_{\lambda=1}^{n} (a_\lambda b_\lambda)$ e $G \cdot H^T =$

$$= \begin{pmatrix} g_0 & g_1 & \cdots & g_s & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_s & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_s \end{pmatrix} \cdot \begin{pmatrix} h_{n-s} & 0 & \cdots & 0 \\ h_{n-s-1} & h_{n-s} & \cdots & 0 \\ \vdots & h_{n-s-1} & \cdots & \vdots \\ h_0 & \vdots & \cdots & 0 \\ 0 & h_0 & \cdots & h_{n-s} \\ 0 & 0 & \cdots & h_{n-s-1} \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & \cdots & h_0 \end{pmatrix}.$$

Suponhamos que $i \leq j$. Então, para $\lambda < j$ segue que $a_\lambda b_\lambda = 0$ e para $\lambda = j$ temos que $a_\lambda b_\lambda = g_{j-i} h_{n-s}$.

Como $a_{\lambda+k} b_{\lambda+k} = g_{j-i+k} h_{n-s-k}$, onde $1 \leq k \leq n-s$ e $j-i+k \leq s$, temos que $a \cdot b$ é o coeficiente de $X^{j-i+n-s}$ no produto $g(X)h(X) = X^n - 1$.

Como $0 \leq j-i \leq s-1$, temos que $1 \leq j-i+n-s \leq n-1$, assim concluímos que esse coeficiente é igual a zero. Análogo para $j \leq i$.

Fica então provado que $G \cdot H^t = 0$ e portanto H é uma matriz geradora de $C^\perp$.

Observamos que

$$H = \begin{pmatrix} \Psi^{-1}(\overline{h^*(X)}) \\ \Psi^{-1}(\overline{Xh^*(X)}) \\ \vdots \\ \Psi^{-1}(\overline{X^{s-1}h^*(X)}) \end{pmatrix},$$

portanto, temos que $C^\perp = \Psi^{-1}(J)$, onde $J = \langle \overline{h^*(X)} \rangle$. ∎

Corolário 9. *H é a matriz verificação de paridade do código cíclico $C = \Psi^{-1}(I)$, onde $I = \langle \overline{g(X)} \rangle$.*

Abstract: In this paper we present an introduction to the fields extensions and finite fields, the basic algebraic foundation of the theory of error correction linear codes, specially the cyclic codes.

Keywords: Fields extensions, cyclic codes.

Referências Bibliográficas

[1] Hefez, A., Villela, M.L.T., *Códigos Corretores de Erros*, Rio de Janeiro, IMPA, 2002.

[2] Palazzo Jr., R., Interlando, J.C., Geronimo, J.R., Andrade, A.A., Favareto, O.M., Nóbrega Neto, T.P., *Códigos Corretores sobre Estrutura de Corpos, Anéis e Grupos*, Notas de Aulas, Campinas, FEEC, UNICAMP, 2000.

[3] Lin, S., Costello, D.J., *Error Control Coding: Fundamentals and Applications*, New Jersey, Prentice Hall, 1983.

ISSN 1980-024X

Boletim de Iniciação Científica em Matemática – BICMat

Orientação aos autores

Ao redigir o material a ser divulgado o autor deve observar que o alvo principal é o aluno de graduação, devendo a redação ser clara e objetiva incentivando-o à leitura.

O trabalho deve ser enviado à Comissão Editorial, via e-mail, na linguagem LaTeX, usando a classe `bicmat`. Mais informações sobre a formatação do trabalho podem ser encontradas em `www.rc.unesp.br/igce/matematica/bicmat`, assim como o endereço para o envio do trabalho.

A responsabilidade de cada artigo é exclusiva do autor e respectivo orientador.