UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA APLICADA

Algoritmos para o Máximo Divisor Comum de Polinômios a uma Variável

por

Virgínia Maria Rodrigues

Dissertação submetida como requisito parcial
para a obtenção do grau de
Mestre em Matemática Aplicada

Prof. Vilmar Trevisan
Orientador

Porto Alegre, agosto de 1995.

CIP - CATALOGAÇÃO NA PUBLICAÇÃO

Rodrigues, Virgínia Maria

Algoritmos para o Máximo Divisor Comum de Polinômios a uma Variável / Virgínia Maria Rodrigues.—Porto Alegre: CPGMA da UFRGS, 1995.

63 p.: il.

Dissertação (mestrado)—Universidade Federal do Rio Grande do Sul, Instituto de Matemática, Curso de Pós-Graduação em Matemática Aplicada, Porto Alegre, 1995. Orientador: Vilmar Trevisan

Dissertação: Computação Algébrica, Álgebra Computacional

16409

DISSRET./MAT
R969A

MAT
1996/142547-2
1996/07/31
7665

Para ti, mãe.

AGRADECIMENTOS

Agradeço especialmente ao meu orientador, Prof. Vilmar Trevisan, pela orientação paciente e incentivante. Sem os seus merecidos "puxões de orelha" provavelmente este trabalho ainda estaria inacabado.

Gostaria de agradecer também ao CNPq pelas bolsas de mestrado e iniciação científica. Com o auxílio deste órgão tive a felicidade de estudar com o Prof. Miguel Ferrero, a quem devo grande parte de minha formação em Álgebra.

À Ramona, secretária do CPGMap, quero agradecer e parabenizar pela sua simpatia e dedicação.

Tenho o prazer de registrar meus agradecimentos aos amigos Paulo Ricardo, Alvino, Rogério e Claus, que me deram o privilégio de tê-los como colegas durante este curso.

Por mais que eu diga, sempre será insuficiente para mostrar o quanto sou grata à minha família e aos meus amigos, que com seu carinho e incentivo me fazem lembrar que "a maior felicidade que existe é a silenciosa certeza de que vale a pena viver" (A.K.).

RESUMO

Nesta dissertação apresentamos os principais algoritmos para o cálculo do Máximo Divisor Comum de polinômios a uma variável: os Algoritmos Euclidianos e os Algoritmos Modulares. Obtemos uma nova cota superior para os coeficientes do M.D.C., bem como demonstramos os resultados necessários para a obtenção da cota atualmente utilizada pelos Algoritmos Modulares. Além disso, apresentamos uma classe de polinômios para os quais a nova cota é menor que a anterior.

ABSTRACT

In this thesis we present the main algorithms for computing the Greatest Common Divisor of two univariate polynomials: the Euclidean Algorithms and the Modular Algorithms. We obtain a new upper bound for the coefficients of the G.C.D., as well we prove the results that are necessary for obtaining the bound that has been used by the Modular Algorithms. Besides, we present a class of polynomials for which the new bound is smaller than the previos one.

SUMÁRIO

RESUMO v

ABSTRACT vi

1 INTRODUÇÃO 1

1.1 Computação Algébrica 1

1.2 O Máximo Divisor Comum Polinomial 2

1.3 Descrição do Problema e Organização do Trabalho 3

1.4 Preliminares 4

1.4.1 Existência e Unicidade do M.D.C. 4

1.4.2 Conteúdo e Parte Primitiva de um Polinômio 7

1.4.3 Resultante 10

1.4.4 Teorema Chinês dos Restos 12

2 ALGORITMOS EUCLIDIANOS 13

2.1 Algoritmos para a Divisão de Polinômios 13

2.2 Algoritmos para o M.D.C. de Polinômios sobre um Corpo . . 19

2.3 Algoritmos para o M.D.C. de Polinômios sobre um Domínio Fatorial 24

3 ALGORITMOS MODULARES 30

3.1 Métodos Modulares 30

3.2 Escolhendo os Números Primos 32

3.3 Calculando o M.D.C. 34

3.3.1 Primeira Solução 35

3.3.2 Uma Segunda Solução 38

3.3.3 Terceira Solução 40

4 COTAS SUPERIORES PARA OS COEFICIENTES DO M.D.C. 43

4.1 Uma Cota Superior para os Coeficientes 43

4.2 Uma Nova Cota Superior para os Coeficientes 48

4.3 Comparando as Cotas 52

4.3.1 Exemplos 55

5 CONCLUSÃO 59

5.1 Algoritmo Final 60

BIBLIOGRAFIA 62

1 INTRODUÇÃO

Neste capítulo inicial faremos a colocação do problema do cálculo do Máximo Divisor Comum de polinômios a uma variável e apresentaremos uma descrição do desenvolvimento deste problema ao longo desta dissertação. Alguns resultados básicos que serão úteis no desenrolar deste trabalho também serão apresentados aqui.

1.1 Computação Algébrica

A *Computação Algébrica* é um campo de investigação científica que pode ser considerado um ramo tanto da Matemática quanto da Ciência da Computação, e cuja principal característica é a habilidade de criar, analisar e implementar algoritmos para objetos matemáticos não numéricos.

Dentro do amplo campo da Computação Algébrica, a área de Álgebra Computacional tem importância especial. Esta pode ser considerada como sendo a projeção da primeira sobre o estudo de questões algébricas, ou seja, a construção de soluções algorítmico-simbólicas para problemas que envolvam estruturas algébricas.

Nas últimas décadas foram obtidos importantes sucessos nesta área, tais como algoritmos para a integração de funções, para a fatoração de polinômios e para a solução de equações diferenciais, entre outros exemplos. Ao mesmo tempo, poderosíssimos *Sistemas de Computação Algébrica* foram desenvolvidos e aperfeiçoados e estão à disposição da comunidade científica para auxiliar na manipulação algébrica de expressões, bem como para fornecer meios para a implementação de algoritmos. Exemplos de tais sistemas incluem MACSYMA, MAPLE, DERIVE, MATHEMATICA e REDUCE.

1.2 O Máximo Divisor Comum Polinomial

Os polinômios, que conforme D. E. Knuth são o primeiro passo depois dos números, têm importância fundamental na área de Computação Algébrica, especialmente na Álgebra Computacional.

Em geral, estruturas algébricas, por mais complicadas que sejam, podem ser representadas através de polinômios. Portanto, conhecê-los e operar com eles de modo eficiente é de fundamental interesse quando está em jogo a eficiência de algoritmos para resolver problemas relevantes dentro das estruturas algébricas. Sem uma boa aritmética polinomial, um sistema de Computação Algébrica, como os que citamos anteriormente, seria muito ineficiente, pois grande parte das operações destes sistemas são baseadas em operações com polinômios, como a simplificação e a fatoração.

Durante a última década houve grandes avanços no poder e eficiência dos sistemas de Computação Algébrica. O preço dos computadores que suportam tais sistemas têm diminuído, tornando-os disponíveis a um maior número de pessoas. Quando um usuário de um destes sistemas digita um comando como `MDC(f,g)`, ele espera não só obter uma resposta, como espera obtê-la rapidamente. Desta forma, a eficiência é uma grande motivação para se estudar algoritmos para o Máximo Divisor Comum de polinômios.

Nosso maior objetivo, neste trabalho, é estabelecer algoritmos para o problema do cálculo do Máximo Divisor Comum de polinômios a uma variável que sejam úteis na prática.

1.3 Descrição do Problema e Organização do Trabalho

Definição 1.3.1 *Sejam f e g dois polinômios com coeficientes em um domínio fatorial D. Um Máximo Divisor Comum de f e g é um polinômio de máximo grau que divide f e g, ou seja, dizemos que $d(x) \in D[x]$ é um Máximo Divisor Comum de $f(x)$ e $g(x)$ se:*

i) $d(x)|f(x)$ *e* $d(x)|g(x)$;

ii) $\forall\, d' \in D[x],\ d'|f(x)$ *e* $d'|g(x) \rightarrow d'|d(x)$.

Na seção 1.4 deste capítulo mostraremos a existência e a unicidade, a menos de multiplicação por elementos invertíveis, do Máximo Divisor Comum de polinômios com coeficientes em um domínio fatorial. Por esta razão, consideraremos a noção de M.D.C. somente em domínios fatoriais e poderemos falar no M.D.C. de dois polinômios f e g que indicaremos por $MDC(f,g)$.

No capítulo 2 desta dissertação apresentaremos os primeiros algoritmos para o cálculo do M.D.C., chamados de Algoritmos Euclidianos, os quais baseiam-se na aplicação de um algoritmo para a divisão de polinômios, analogamente ao que é feito para o cálculo do M.D.C. de números inteiros utilizando o Algoritmo da Divisão de Euclides.

Na busca de uma solução eficiente para o cálculo do M.D.C. de polinômios, principalmente para aqueles com coeficientes inteiros (os mais freqüentes na prática da Álgebra Computacional), constata-se que os Algoritmos Euclidianos têm várias deficiências, como mostraremos no capítulo 2. Todavia, este é um exemplo de problema em que a comunidade científica alcançou um grande sucesso. Uma família de métodos (ditos Modulares) foi criada para a resolução de inúmeros problemas algébricos, incluindo o cálculo eficiente do M.D.C. de polinômios com coeficientes inteiros.

No capítulo 3 teremos oportunidade de mostrar como os Métodos Modulares podem ser utilizados para o cálculo do Máximo Divisor Comum de dois polinômios em $\mathbb{Z}[x]$. Algoritmos mais eficientes que os Euclidianos serão apresentados.

Como observaremos, para que os Métodos Modulares possam ser utilizados com sucesso no cálculo do M.D.C., é necessário que se conheça, de antemão, uma estimativa para o tamanho dos coeficientes do Máximo Divisor Comum que queremos calcular.

No capítulo 4 trataremos da obtenção de cotas superiores para os coeficientes do M.D.C. polinomial. Apresentaremos um resultado de Mignotte [14] de 1974, que é a cota mais utilizada pelos Algoritmos Modulares. Introduziremos ainda uma nova cota superior, obtida durante o desenvolvimento deste trabalho, que é vantajosa em relação à cota de Mignotte para grande parte dos polinômios. Faremos comparações entre as duas cotas e obteremos uma classe de polinômios para os quais a nossa nova cota é, garantidamente, melhor que a anterior.

Finalmente, no capítulo 5 faremos uma conclusão deste trabalho, a qual incluirá uma apreciação das contribuições apresentadas nesta dissertação.

1.4 Preliminares

Nesta seção apresentaremos alguns resultados básicos de Álgebra que serão utilizados direta ou indiretamente durante esta dissertação.

1.4.1 Existência e Unicidade do M.D.C.

Definição 1.4.1 *Seja R um anel comutativo com unidade e seja $a \in R$. Dizemos que:*

(i) *Um elemento $b \in R$ é um divisor de a (em R) se existe $c \in R$ tal que $a = bc$. Dizemos também que b divide a, ou que a é múltiplo de b, e escrevemos $b|a$;*

(ii) *a é invertível (em R) se existe $b \in R$ tal que $ab = 1$;*

(iii) *a e $b \in R$ são associados (em R) se existe $u \in R$, u invertível em R, tal que $a = ub$;*

(iv) *a é irredutível (em R) se a não é invertível em R, $a \neq 0$ e sempre que $a = bc$, com b e c em R, então b ou c é invertível em R.*

Definição 1.4.2 *Sejam $a_1, \ldots, a_n \in R$. Dizemos que $d \in R$ é um Máximo Divisor Comum de $a_1, \ldots, a_n$ se:*

i) $d|a_1, \ldots, d|a_n$;

ii) $\forall\, d' \in R,\ d'|a_1, \ldots, d'|a_n \rightarrow d'|d$.

Proposição 1.4.3 *Seja D um domínio de integridade e sejam $a_1, \ldots, a_n \in D$. Se d e d' são Máximos Divisores Comuns de $a_1, \ldots, a_n$ então d e d' são associados.*

Demonstração: Como d' é um M.D.C. de $a_1, \ldots, a_n$, temos que $d'|a_1, \ldots, d'|a_n$. Conseqüentemente, $d'|d$. Analogamente obtemos que $d|d'$. Portanto, existem $u, v \in D$ tais que $d' = ud$ e $d = vd'$. Logo, $d' = uvd'$ e, por tratar-se de um domínio de integridade, $uv = 1$. Portanto, u e v são invertíveis e d e d' são associados. □

Por esta proposição, num domínio de integridade temos unicidade do M.D.C. a menos de multiplicação por elementos invertíveis, e, portanto, podemos falar do M.D.C. dos elementos $a_1, \ldots, a_n$ que indicaremos por $MDC(a_1, \ldots, a_n)$. Entretanto, num domínio qualquer não podemos garantir a existência do M.D.C., que será obtida ao trabalharmos em um *domínio fatorial* (proposição 1.4.5).

Definição 1.4.4 *Um domínio de integridade D é um domínio de fatoração única ou domínio fatorial se:*

i) todo elemento não nulo de D é invertível ou pode ser escrito como produto de um número finito de elementos irredutíveis de D;

ii) a decomposição na parte i) é única a menos da ordem dos fatores irredutíveis e a menos de elementos invertíveis.

Proposição 1.4.5 *Seja D um domínio fatorial e sejam $a \neq 0$, $b \neq 0 \in D$. Então, existe $d \in D$ tal que $d = MDC(a, b)$.*

Demonstração: Como D é um domínio fatorial, existem $p_1, \ldots, p_t$ irredutíveis distintos e $q_1, \ldots, q_s$ irredutíveis distintos tais que

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_t^{\alpha_t} \text{ e } b = q_1^{\beta_1} \cdot \ldots \cdot q_s^{\beta_s},$$

com $\alpha_i, \beta_j \in \mathbb{N}^*$, $i = 1, \ldots, t$, $j = 1, \ldots, s$. Podemos reescrever a decomposição de a e b (completando com expoentes nulos quando necessário), de maneira que

$$a = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r} \text{ e } b = q_1^{\beta_1} \cdot \ldots \cdot q_r^{\beta_r}, \text{ onde } p_i = q_i, \ i = 1, \ldots, r.$$

Seja $d = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$, onde $\gamma_i = \min\{\alpha_i, \beta_i\}$, $i = 1, \ldots, r$. Temos que:

(i) $a = (p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}) \cdot (p_1^{\alpha_1 - \gamma_1} \cdot \ldots \cdot p_r^{\alpha_r - \gamma_r}) = d \cdot (p_1^{\alpha_1 - \gamma_1} \cdot \ldots \cdot p_r^{\alpha_r - \gamma_r})$ e
$b = (p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}) \cdot (p_1^{\beta_1 - \gamma_1} \cdot \ldots \cdot p_r^{\beta_r - \gamma_r}) = d \cdot (p_1^{\beta_1 - \gamma_1} \cdot \ldots \cdot p_r^{\beta_r - \gamma_r})$.
Logo, $d|a$ e $d|b$.

(ii) Seja $d' \in D$ tal que $d'|a$ e $d'|b$. Então, $d' = p_1^{\gamma_1'} \cdot \ldots \cdot p_r^{\gamma_r'}$, onde $\gamma_i' \leq \alpha_i$ e $\gamma_i' \leq \beta_i$, $i = 1, \ldots, r$. Conseqüentemente, $\gamma_i' \leq \min\{\alpha_i, \beta_i\} = \gamma_i$, $i = 1, \ldots, r$, e, portanto, $d'|d$.

Por (i) e (ii) obtemos que $d = MDC(a, b)$. □

Para o anel de polinômios a uma variável sobre um domínio fatorial, obteremos a existência do M.D.C. como conseqüência da proposição anterior e do teorema 1.4.6.

Teorema 1.4.6 (Gauss) *Seja D um domínio fatorial. Então $D[x]$ é um domínio fatorial.*

Demonstração: A demonstração deste teorema pode ser vista com detalhes em [8]. Nela os autores utilizam as noções de polinômio primitivo e conteúdo de um polinômio que apresentaremos na próxima seção. □

1.4.2 Conteúdo e Parte Primitiva de um Polinômio

Definição 1.4.7 *Seja $f(x) = \sum_{i=0}^{\alpha} a_i x^i \in D[x]$, onde D é um domínio fatorial. O conteúdo de f é o $MDC(a_0, \ldots, a_\alpha)$ e será indicado por $c(f)$. Dizemos que f é primitivo em $D[x]$ se o conteúdo de f é 1.*

Pela proposição 1.4.3, o conteúdo de cada polinômio com coeficientes em um domínio fatorial é único a menos de multiplicação por invertíveis. Conseqüentemente:

1) Se $f \in D[x]$, D um domínio fatorial, então podemos escrever $f = c(f) \cdot f_1(x)$, com $f_1(x)$ primitivo em $D[x]$;

2) Esta representação é única a menos de multiplicação por um invertível.

Assim, podemos escrever qualquer polinômio não nulo f como

$$f = c(f) \cdot pp(f),$$

onde $pp(f)$ é um polinômio primitivo chamado de *parte primitiva* de f.

Lema 1.4.8 (Lema de Gauss) *O produto de polinômios primitivos sobre um domínio fatorial é primitivo.*

Demonstração: Seja D um domínio fatorial e sejam $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ e $g(x) = \sum_{i=0}^{\beta} b_i x^i$ polinômios primitivos em $D[x]$. Se $f \cdot g$ não é primitivo, então existe um irredutível $p \in D$ que divide todos os coeficientes de $f \cdot g$. Como f e g são primitivos, existe um primeiro índice j tal que p não divide a_j e um primeiro índice k tal que p não divide b_k. Por outro lado, p divide o coeficiente de x^{j+k} em $f \cdot g$ que é

$$c_{j+k} = a_0 b_{j+k} + \ldots + a_j b_k + \ldots + a_{j+k} b_0$$

(onde $a_i = 0$, $\forall i \geq \alpha$, e $b_i = 0$, $\forall i \geq \beta$). Como p divide $a_0, \ldots, a_j$, divide $b_0, \ldots, b_k$ e divide c_{j+k}, temos que p divide $a_j b_k$. Porém, isto contradiz a hipótese de que p é um irredutível que não divide a_j nem divide b_k. Logo, $f \cdot g$ é primitivo. □

Corolário 1.4.9 *Sejam f e $g \in D[x]$, onde D é um domínio fatorial. Então,*

$$c(f \cdot g) = c(f)c(g),$$

$$pp(f \cdot g) = pp(f)pp(g),$$

a menos de multiplicação por invertíveis.

Demonstração: Seja $d = c(f)$ e $d' = c(g)$. Temos que $f = d\ pp(f)$ e $g = d'\ pp(g)$. Logo, $f \cdot g = dd'\ pp(f)pp(g)$ e, portanto,

$$c(f \cdot g) = c(dd'\ pp(f)pp(g)) = dd'\ c(pp(f)pp(g)).$$

Pelo lema de Gauss (lema 1.4.8), $c(pp(f)pp(g)) = 1$. Logo, $c(f \cdot g) = dd' = c(f)c(g)$ e, portanto, $pp(f \cdot g) = pp(f)pp(g)$, a menos de multiplicação por invertíveis. □

Lema 1.4.10 *Sejam f e $g \in D[x]$, onde D é um domínio fatorial. Então,*

$$c(MDC(f,g)) = MDC(c(f), c(g)),$$

$$pp(MDC(f,g)) = MDC(pp(f), pp(g)),$$

a menos de multiplicação por invertíveis.

Demonstração: Seja $h = MDC(f,g)$.

(i) $h|f$ e $h|g \Rightarrow f = h \cdot q_1$ e $g = h \cdot q_2$, $q_1, q_2 \in D[x]$. Pelo corolário 1.4.9, $c(f) = c(h)c(q_1)$, $c(g) = c(h)c(q_2)$, $pp(f) = pp(h)pp(q_1)$ e $pp(g) = pp(h)pp(q_2)$, a menos de multiplicação por invertíveis. Logo, $c(h)|c(f)$, $c(h)|c(g)$, $pp(h)|pp(f)$ e $pp(h)|pp(g)$, e isto implica que $c(h)|MDC(c(f), c(g))$ e $pp(h)|MDC(pp(f), pp(g))$.

(ii) Seja $d \in D$ tal que $d|c(f)$ e $d|c(g)$. Então, existem $m, n \in D$ tais que $c(f) = d \cdot m$ e $c(g) = d \cdot n$. Logo, $f = dm\ pp(f)$ e $g = dn\ pp(g)$. Conseqüentemente, $h = MDC(f,g) = d \cdot MDC(m\ pp(f), n\ pp(g))$ e, portanto, $c(h) = d \cdot c(MDC(m\ pp(f), n\ pp(g)))$. Logo, $d|c(h)$.

(ii)′ Seja $d'(x) \in D[x]$ tal que $d'(x)|pp(f)$ e $d'(x)|pp(g)$. Então, $d'(x)$ é primitivo e existem $m(x), n(x) \in D[x]$ tais que $pp(f) = d'(x) \cdot m(x)$ e $pp(g) = d'(x) \cdot n(x)$. Logo, $f = c(f)d'(x)m(x)$ e $g = c(g)d'(x)n(x)$. Conseqüentemente, $h = MDC(f,g) = d'(x) \cdot MDC(c(f)m(x), c(g)n(x))$ e, portanto, $pp(h) = pp(d') \cdot pp(MDC(c(f)m(x), c(g)n(x))) = d'(x) \cdot pp(MDC(c(f)m(x), c(g)n(x)))$. Logo, $d'(x)|pp(h)$.

Por (i) e (ii)′ concluímos que $pp(h) = MDC(pp(f), pp(g))$. □

Definição 1.4.11 *Seja $f \in D[x]$. O coeficiente líder de f é o coeficiente do termo de maior grau de f e será indicado por $l(f)$. Dizemos que f é mônico se $l(f) = 1$.*

1.4.3 Resultante

Definição 1.4.12 *Seja D um domínio e sejam $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ e $g(x) = \sum_{i=0}^{\beta} b_i x^i$, onde $a_\alpha, b_\beta \neq 0$, dois polinômios em $D[x]$ de graus ≥ 1. A resultante de f e g, indicada por $Res(f,g)$ é o determinante da matriz*

$$\begin{pmatrix}
a_\alpha & a_{\alpha-1} & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 \\
0 & a_\alpha & a_{\alpha-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \dots \\
0 & \dots & 0 & a_\alpha & a_{\alpha-1} & \dots & \dots & \dots & \dots \\
b_\beta & b_{\beta-1} & \dots & b_1 & b_0 & 0 & 0 & \dots & 0 \\
0 & b_\beta & b_{\beta-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\
\vdots & \ddots & \ddots & \ddots & \dots & \ddots & \ddots & \ddots & \dots \\
0 & \dots & 0 & b_\beta & b_{\beta-1} & \dots & \dots & \dots & \dots
\end{pmatrix}$$

sendo que existem β linhas de a_i e α linhas de b_i.

Teorema 1.4.13 *Seja D um domínio e sejam $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ e $g(x) = \sum_{i=0}^{\beta} b_i x^i$, onde $a_\alpha, b_\beta \neq 0$, dois polinômios em $D[x]$ de graus ≥ 1. Então, são equivalentes:*

i) $Res(f,g) = 0$;

ii) Existem polinômios não nulos f_1 e $f_2 \in D[x]$, de graus menores que α e β, respectivamente, tais que $f_1(x)g(x) = g_1(x)f(x)$;

Se D é um domínio fatorial, estas condições são equivalentes a:

iii) f e g possuem um fator comum em $D[x]$ de grau ≥ 1.

Demonstração: Encontrar polinômios não nulos $f_1(x) = \sum_{i=0}^{\alpha-1} c_i x^i$ e $g_1(x) = \sum_{i=0}^{\beta-1} d_i x^i$ em $D[x]$ tais que $f_1(x)g(x) = g_1(x)f(x)$ é equivalente a encontrar uma solução não trivial do seguinte sistema homogêneo de $\alpha + \beta$ equações nas incógnitas $d_{\beta-1}, d_{\beta-2}, \ldots, d_0, c_{\alpha-1}, c_{\alpha-2}, \ldots, c_0$:

$$\begin{cases} a_\alpha d_{\beta-1} - b_\beta c_{\alpha-1} = 0 \\ a_{\alpha-1} d_{\beta-1} + a_\alpha d_{\beta-2} - b_{\beta-1} c_{\alpha-1} - b_\beta c_{\alpha-2} = 0 \\ \ldots \\ a_0 d_0 - b_0 c_0 = 0 \end{cases}$$

Existe uma solução não trivial deste sistema se e somente se o determinante da matriz dos coeficientes é nulo. Observa-se que o $Res(f, g)$ é o determinante da transposta da matriz dos coeficientes deste sistema, a menos de multiplicação por -1 das linhas envolvendo b_i. Conseqüentemente, $i)$ e $ii)$ são equivalentes.
Suponhamos que f e g satisfazem $iii)$. Então, $\exists\ p(x) \in D[x]$ de grau ≥ 1 tal que:

$$f(x) = p(x)f_1(x), \text{ com } f_1(x) \in D[x], \text{ grau de } f_1 < \alpha \text{ e}$$

$$g(x) = p(x)g_1(x), \text{ com } g_1(x) \in D[x], \text{ grau de } g_1 < \beta.$$

Logo, $f_1(x)g(x) = f_1(x)p(x)g_1(x) = f(x)g_1(x)$. Conseqüentemente, $iii) \Rightarrow ii)$.
Suponhamos que existem $f_1(x), g_1(x) \in D[x]$ que satisfazem $ii)$. Sendo $D[x]$ um domínio fatorial, todos os fatores irredutíveis de grau ≥ 1 de f aparecem no produto $f_1(x)g(x)$. Nem todos eles podem aparecer em f_1, pois, por hipótese, f_1 tem grau menor que f. Assim, pelo menos um dos fatores irredutíveis de grau ≥ 1 de f aparece em g. Conseqüentemente, $ii) \Rightarrow iii)$ e, portanto, são equivalentes. □

Corolário 1.4.14 *O resultante de dois polinômios não nulos com coeficientes em um domínio fatorial é zero se e somente se eles possuem um fator comum de grau* ≥ 1.

Demonstração: Segue imediatamente do teorema 1.4.13. □

1.4.4 Teorema Chinês dos Restos

Apresentaremos uma versão para números inteiros do teorema Chinês dos Restos. Uma generalização para domínios Euclidianos pode ser vista em [12].

Teorema 1.4.15 (Teorema Chinês dos Restos) *Sejam m e n dois inteiros relativamente primos, ou seja, $MDC(m,n) = 1$. Então, $\forall\ a, b \in \mathbb{Z}$, $\exists\ c \in \mathbb{Z}$ tal que $x \equiv a \bmod m$ e $x \equiv b \bmod n$ se e somente se $x \equiv c \bmod mn$.*

Demonstração: Como $MDC(m,n) = 1$ e $\mathbb{Z}$ é um domínio principal, existem α e $\beta \in \mathbb{Z}$ tais que $1 = \alpha m + \beta n$. Seja $c = a + (b-a)\alpha m$. Suponhamos que $x \equiv c \bmod mn$. Então, $x \equiv c \bmod m$ e, como $c \equiv a \bmod m$, obtemos que $x \equiv a \bmod m$. Além disso, $c = a + (b-a)\alpha m = a + (b-a)(1-\beta n)$. Logo, $c \equiv a + (b-a) \bmod n \equiv b \bmod n$, e, portanto, $x \equiv c \bmod mn$ implica $x \equiv b \bmod n$.
Reciprocamente, suponhamos que $x \equiv a \bmod m$ e $x \equiv b \bmod n$. Visto que $c \equiv a \bmod m$ e $c \equiv b \bmod n$, temos que $x \equiv c \bmod m$ e $x \equiv c \bmod n$. Logo, como m e n são relativamente primos, $x \equiv c \bmod mn$. □

2 ALGORITMOS EUCLIDIANOS

Neste capítulo apresentaremos algoritmos para o cálculo do Máximo Divisor Comum de polinômios a uma variável com coeficientes em um domínio fatorial.

Os algoritmos que descreveremos baseiam-se na aplicação de um algoritmo para a divisão de polinômios sobre um domínio fatorial, uma extensão do Algoritmo da Divisão de Euclides para polinômios sobre um corpo.

Também apresentaremos algoritmos específicos para o caso particular de polinômios sobre um corpo, os quais utilizam o próprio Algoritmo da Divisão de Euclides.

2.1 Algoritmos para a Divisão de Polinômios

Para calcularmos o Máximo Divisor Comum de polinômios com coeficientes em um domínio fatorial D, necessitamos de um algoritmo para a divisão de polinômios em $D[x]$.

Se o domínio fatorial for, em particular, um corpo K, o teorema 2.1.1 mostrará que é possível dividir polinômios em $K[x]$, ou seja, que $K[x]$ é um domínio euclidiano.

Teorema 2.1.1 *Seja K um corpo e seja $K[x]$ o domínio dos polinômios numa variável sobre K. Seja $\partial : K[x]\backslash\{0\} \to \mathbb{N}$ a função grau. Então,*

$$\forall f(x), g(x) \in K[x],\ g(x) \neq 0,\ \textit{existem únicos}\ q(x), r(x) \in K[x]\ \textit{tais que}$$

$$f(x) = q(x) \cdot g(x) + r(x),\ \textit{com}\ r(x) = 0\ \textit{ou}\ \partial r(x) < \partial g(x). \tag{2.1}$$

Demonstração: Sejam $f = \sum_{i=0}^{\alpha} a_i x^i$ e $g = \sum_{i=0}^{\beta} b_i x^i \in K[x]$, onde $b_\beta \neq 0$.

Existência:

Se $f(x) = 0$ ou se $\partial f(x) = \alpha < \beta = \partial g(x)$, basta tomar $q(x) = 0$ e $r(x) = f(x)$.

Se $\partial f(x) \geq \partial g(x)$, consideremos o polinômio $f_1(x)$ definido por:

$$\begin{aligned} f_1(x) &= f(x) - \frac{a_\alpha}{b_\beta} x^{\alpha-\beta} g(x) = \\ &= \left(a_{\alpha-1} - \frac{a_\alpha b_{\beta-1}}{b_\beta}\right) x^{\alpha-1} + \ldots + \left(a_{\alpha-\beta} - \frac{a_\alpha b_0}{b_\beta}\right) x^{\alpha-\beta}. \end{aligned}$$

Assim,

$$f(x) = \frac{a_\alpha}{b_\beta} x^{\alpha-\beta} g(x) + f_1(x) \quad \text{e} \quad \partial f_1(x) < \partial f(x).$$

Então, por indução sobre $\partial f(x) = \alpha$, temos que $\exists\ q_1(x),\ r_1(x) \in K[x]$ tais que

$$f_1(x) = q_1(x) \cdot g(x) + r_1(x), \text{ com } r_1(x) = 0 \text{ ou } \partial r_1(x) < \partial g(x).$$

Conseqüentemente,

$$f(x) = \left(\frac{a_\alpha}{b_\beta} x^{\alpha-\beta} + q_1(x)\right) g(x) + r_1(x),$$

e, portanto, basta tomar $q(x) = \frac{a_\alpha}{b_\beta} x^{\alpha-\beta} + q_1(x)$ e $r(x) = r_1(x)$.

Unicidade:

Suponhamos que existam $q_1(x),\ r_1(x),\ q_2(x),\ r_2(x) \in K[x]$ tais que

$$f(x) = q_1(x) \cdot g(x) + r_1(x) = q_2(x) \cdot g(x) + r_2(x),$$

onde $r_i(x) = 0$ ou $\partial r_i(x) < \partial g(x),\ i = 1,\ 2$.

Assim,

$$[q_1(x) - q_2(x)] \cdot g(x) = r_2(x) - r_1(x).$$

Se $q_1(x) \neq q_2(x)$, como $b_\beta \neq 0$ e K não possui divisores de zero, teremos que:

$$\partial(r_2(x) - r_1(x)) = \partial([q_1(x) - q_2(x)] \cdot g(x)) = \partial(q_1(x) - q_2(x)) + \partial g(x).$$

Logo, $\partial(r_2(x) - r_1(x)) > \partial g(x)$, o que é absurdo, pois

$$\partial(r_2(x) - r_1(x)) \leq \max\{\partial r_1(x), \partial r_2(x)\} < \partial g(x).$$

Portanto, $q_1(x) = q_2(x)$ e daí segue que

$$r_1(x) = f(x) - q_1(x) \cdot g(x) = f(x) - q_2(x) \cdot g(x) = r_2(x). \quad \square$$

Para obter os polinômios $q(x)$ e $r(x)$ que satisfazem a equação (2.1), podemos utilizar o Algoritmo 2.1 que generaliza o processo usual da divisão de polinômios .

Algoritmo 2.1 (Algoritmo da Divisão de Euclides) *Dados dois polinômios com coeficientes em um corpo,* $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ *e* $g(x) = \sum_{i=0}^{\beta} b_i x^i$, *onde* $b_\beta \neq 0$ *e* $\alpha \geq \beta \geq 0$, *este algoritmo encontra os polinômios* $q(x) = \sum_{i=0}^{\alpha-\beta} q_i x^i$ *e* $r(x) = \sum_{i=0}^{\beta-1} r_i x^i$ *tais que*

$$f(x) = q(x) \cdot g(x) + r(x), \quad \textit{onde } r(x) = 0 \textit{ ou } \partial r(x) < \partial g(x).$$

1. **Para** $k = \alpha - \beta,\ \alpha - \beta - 1,\ \ldots,\ 0,$

   faça

   1.1. $q_k \leftarrow \dfrac{a_{\beta+k}}{b_\beta}$;

   1.2. **Para** $i = \beta + k - 1,\ \beta + k - 2,\ \ldots,\ k,$

   faça $a_i \leftarrow a_i - q_k b_{i-k}$;

2. *O algoritmo termina com* $r_i \leftarrow a_i,\ \forall\ 0 \leq i \leq \beta - 1.$

Exemplo 2.1 Escrevendo apenas os coeficientes na divisão dos polinômios

$$\begin{aligned} f(x) &= x^8 + x^6 + 8x^4 + 8x^3 + 8x^2 + 2x + 6 \quad e \\ g(x) &= 3x^6 + 5x^4 + 7x^2 + 2x + 10 \quad \in \mathbb{Z}_{11}[x], \end{aligned}$$

obtemos:

1	0	1	0	8	8	8	2	6	|	3	0	5	0	7	2	10
1	0	9	0	6	8	7				4	0	1				
	0	3	0	2	0	1	2	6								
		3	0	5	0	7	2	10								
			0	8	0	5	0	7								

Portanto,

$$f(x) = (4x^2 + 1)g(x) + (8x^4 + 5x^2 + 7) \bmod 11.$$

Se o domínio fatorial D não for um corpo, pelo teorema 2.1.2 obteremos a existência e unicidade de uma "pseudo-divisão" de polinômios em $D[x]$.

Teorema 2.1.2 *Seja D um domínio fatorial e seja $D[x]$ o domínio dos polinômios numa variável sobre D. Seja $\partial : D[x]\backslash\{0\} \to \mathbb{N}$ a função grau. Então,*

$$\forall f(x), g(x) \in D[x],\ g(x) \neq 0,\ \textit{existem únicos } q(x), r(x) \in D[x] \textit{ tais que}$$

$$l(g)^{\partial f - \partial g + 1} f(x) = q(x) \cdot g(x) + r(x),\ \textit{com } r(x) = 0 \textit{ ou } \partial r(x) < \partial g(x). \qquad (2.2)$$

Demonstração: Sejam $f = \sum_{i=0}^{\alpha} a_i x^i$ e $g = \sum_{i=0}^{\beta} b_i x^i \in D[x]$, onde $b_\beta \neq 0$.

Existência:

Se $f(x) = 0$ ou $\partial f(x) = \alpha < \beta = \partial g(x)$, basta tomar $q(x) = 0$ e $r(x) = b_\beta^{\alpha - \beta + 1} f(x)$.

Se $\partial f(x) = \partial g(x)$, basta tomar $q(x) = a_\alpha$ e $r(x) = b_\beta f(x) - a_\alpha g(x)$, pois teremos

$$q(x) \cdot g(x) + r(x) = a_\alpha g(x) + (b_\beta f(x) - a_\alpha g(x)) = b_\beta f(x) = l(g)^{\alpha-\beta+1} f(x)$$

e, ou $\partial f(x) = \partial g(x) = 0$ e, portanto,

$$r(x) = b_\beta a_\alpha - a_\alpha b_\beta = 0,$$

ou $\partial f(x) = \partial g(x) \geq 1$ e

$$r(x) = (b_\beta a_{\alpha-1} - a_\alpha b_{\beta-1})x^{\alpha-1} + \cdots + (b_\beta a_0 - a_\alpha b_0).$$

Logo, $\partial r(x) \leq \alpha - 1 = \beta - 1 < \partial g(x)$.
Se $\partial f(x) > \partial g(x)$, consideremos o polinômio $f_1(x)$ definido por:

$$f_1(x) = b_\beta f(x) - a_\alpha x^{\alpha-\beta} g(x).$$

Temos que $\partial f_1(x) \leq \alpha - 1$ e, portanto, $\partial f_1(x) - \partial g(x) \leq \alpha - 1 - \beta < \alpha - \beta$.
Então, por indução sobre $\partial f(x) - \partial g(x) = \alpha - \beta$, $\exists\ q_1(x),\ r_1(x) \in D[x]$ tais que

$$b_\beta^{(\alpha-1)-\beta+1} f_1(x) = q_1(x) \cdot g(x) + r_1(x), \text{ com } r_1(x) = 0 \text{ ou } \partial r_1(x) < \partial g(x).$$

Logo,

$$b_\beta^{\alpha-\beta}(b_\beta f(x) - a_\alpha x^{\alpha-\beta} g(x)) = q_1(x) \cdot g(x) + r_1(x).$$

Conseqüentemente,

$$b_\beta^{\alpha-\beta+1} f(x) = (a_\alpha b_\beta^{\alpha-\beta} x^{\alpha-\beta} + q_1(x)) \cdot g(x) + r_1(x)$$

e, portanto, basta tomar $q(x) = a_\alpha b_\beta^{\alpha-\beta} x^{\alpha-\beta} + q_1(x)$ e $r(x) = r_1(x)$.

Unicidade:

Análoga à demonstração da unicidade no teorema 2.1.1. □

Para calcular os polinômios $q(x)$ e $r(x)$ que satisfazem a equação (2.2), podemos utilizar o Algoritmo 2.2.

Este algoritmo baseia-se na constatação de que o Algoritmo 2.1 requer divisão apenas por b_β, o coeficiente líder de $g(x)$, e que esta divisão é realizada $\alpha-\beta+1$ vezes (passo 1.1). Assim, se $f(x)$ e $g(x)$ têm coeficientes inteiros, os denominadores que aparecem em $q(x)$ e $r(x)$, ao aplicarmos o Algoritmo 2.1, são divisores de $b_\beta^{\alpha-\beta+1}$. Conseqüentemente, se multiplicarmos $f(x)$ por $b_\beta^{\alpha-\beta+1}$ saberemos que no passo 1.1 todos os quocientes poderão ser calculados em $\mathbb{Z}$.

Algoritmo 2.2 (Pseudo-Divisão de Polinômios) *Dados dois polinômios com coeficientes em um corpo,* $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ *e* $g(x) = \sum_{i=0}^{\beta} b_i x^i$, *onde* $b_\beta \neq 0$ *e* $\alpha \geq \beta \geq 0$, *este algoritmo encontra os polinômios* $q(x) = \sum_{i=0}^{\alpha-\beta} q_i x^i$ *e* $r(x) = \sum_{i=0}^{\beta-1} r_i x^i$ *tais que*

$$l(g)^{\alpha-\beta+1} f(x) = q(x) \cdot g(x) + r(x), \text{ onde } r(x) = 0 \text{ ou } \partial r(x) < \partial g(x).$$

1. $f(x) \leftarrow b_\beta^{\alpha-\beta+1} f(x)$
2. *Aplique o Algoritmo 2.1 para os polinômios* $f(x)$ *e* $g(x)$.

Exemplo 2.2 Escrevendo apenas os coeficientes na divisão dos polinômios

$$\begin{aligned} f(x) &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 \quad e \\ g(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21 \quad \in \mathbb{Z}[x], \end{aligned}$$

obtemos:

1	0	1	0	-3	-3	8	2	-5		3	0	5	0	-4	-9	21
27	0	27	0	-81	-81	216	54	-135		9	0	-6				
27	0	45	0	-36	-81	189										
	0	-18	0	-45	0	27	54	-135								
		-18	0	-30	0	24	54	-126								
			0	-15	0	3	0	-9								

Logo,

$$27f(x) = (9x^2 - 6)g(x) + (-15x^4 + 3x^2 - 9).$$

2.2 Algoritmos para o M.D.C. de Polinômios sobre um Corpo

Nesta seção apresentaremos algoritmos para o Máximo Divisor Comum de polinômios que, em particular, possuem coeficientes em um corpo.

Os algoritmos que descreveremos a seguir baseiam-se no lema 2.2.1.

Lema 2.2.1 *Sejam $f(x)$, $g(x) \in K[x]$, onde K é um corpo.*
Se $g(x) = 0$, então $MDC(f,g) = f$. Caso contrário, $MDC(f,g) = MDC(g,r)$, onde r é dado pela equação (2.1).

Demonstração:
1º caso: $g(x) = 0$. Temos que:

(i) $f|f$ e $f|g$, pois $f = 1 \cdot f$ e $g = 0 = 0 \cdot f$.

(ii) Qualquer $h' \in K[x]$ que divide f e g, divide f.

Logo, por (i) e (ii) concluímos que $MDC(f,g) = f$.

2º caso: $g(x) \neq 0$. Seja $h = MDC(f,g)$. Então,

(i) $h|f$ e $h|g \Rightarrow h|f$ e $h|qg \Rightarrow h|(f - qg) \Rightarrow h|r$.
Logo, $h|g$ e $h|r$.

(ii) Seja $h' \in K[x]$ tal que $h'|g$ e $h'|r$. Então, $h'|qg$ e $h'|r \Rightarrow h'|(qg+r) \Rightarrow h'|f$. Logo, como h' também divide g, temos que $h'|MDC(f,g) = h$ e, conseqüentemente, $h'|h$.

Por (i) e (ii) concluímos que $MDC(f,g) = h = MDC(g,r)$. □

Algoritmo 2.3 (Algoritmo de Euclides) *Dados dois polinômios f e g com coeficientes em um corpo, este algoritmo calcula o M.D.C. de f e g utilizando o Algoritmo da Divisão de Euclides.*

1. **Se** $g = 0$,
então
1.1. $h \leftarrow f$;
1.2. **vá para** *8;*

2. *Calcule $r(x)$ utilizando o Algoritmo 2.1;*

3. **Se** $r(x) = 0$,
então
3.1. $h \leftarrow g$;
3.2. **vá para** *8;*

4. **Se** $\partial r(x) = 0$,
então
4.1. $h \leftarrow 1$;

4.2. **vá para** *8;*

5. $f \leftarrow g$;

6. $g \leftarrow r$;

7. **vá para** *2;*

8. *O algoritmo termina com h como o M.D.C. procurado.*

Segundo Knuth [11], este processo de cálculo do M.D.C. via sucessivas aplicações do Algoritmo da Divisão de Euclides foi utilizado pela primeira vez por Simon Stevin em 1585.

Exemplo 2.3 Considerando os polinômios $f(x)$ e $g(x)$ do exemplo 2.2, ao aplicarmos o Algoritmo 2.3 obtemos os seguintes coeficientes:

$f(x)$	$g(x)$	$r(x)$
$1,0,1,0,-3,-3,8,2,-5$	$3,0,5,0,-4,-9,21$	$-\frac{5}{9},0,\frac{1}{9},0,-\frac{1}{3}$
$3,0,5,0,-4,-9,21$	$-\frac{5}{9},0,\frac{1}{9},0,-\frac{1}{3}$	$-\frac{117}{25},-9,\frac{441}{25}$
$-\frac{5}{9},0,\frac{1}{9},0,-\frac{1}{3}$	$-\frac{117}{25},-9,\frac{441}{25}$	$\frac{233150}{19773},-\frac{102500}{6591}$
$-\frac{117}{25},-9,\frac{441}{25}$	$\frac{233150}{19773},-\frac{102500}{6591}$	$-\frac{1288744821}{543589225}$

Logo, $MDC(f,g) = 1$.

Como podemos observar pelo exemplo 2.3, mesmo que f e g sejam polinômios com coeficientes inteiros e pequenos, o Algoritmo 2.3 pode produzir coeficientes intermediários não inteiros e grandes. Além disso, cálculos com coeficientes racionais envolvem cálculos de M.D.C. de inteiros, uma operação que se torna cara à medida que os coeficientes crescem.

Podemos melhorar o Algoritmo 2.3 tornando f e g mônicos antes de aplicarmos o Algoritmo da Divisão, pois assim eliminaremos os fatores que tornam

os coeficientes mais complicados que o necessário. A validade do Algoritmo 2.4, no qual implementaremos esta modificação, é dada pelo lema 2.2.2.

Lema 2.2.2 *Sejam $f(x)$, $g(x) \in K[x]$, onde K é um corpo. Então,*

$$MDC(f,g) = MDC\left(\frac{f}{l(f)}, \frac{g}{l(g)}\right).$$

Demonstração: Seja $h = MDC(f,g)$.

Então, $h|f$ e $h|g$. Como num corpo qualquer elemento não nulo é invertível, temos que $h|\frac{1}{l(f)}f$ e $h|\frac{1}{l(g)}g$.

Seja $h' \in K[x]$ tal que $h'|\frac{f}{l(f)}$ e $h'|\frac{g}{l(g)}$. Então, $h'|l(f)\frac{f}{l(f)}$ e $h'|l(g)\frac{g}{l(g)}$, ou seja, $h'|f$ e $h'|g$. Conseqüentemente, $h'|MDC(f,g) = h$.

Portanto, $h = MDC\left(\frac{f}{l(f)}, \frac{g}{l(g)}\right)$. □

Algoritmo 2.4 *Dados dois polinômios não nulos f e g com coeficientes em um corpo, este algoritmo calcula o M.D.C. de f e g tornando os polinômios mônicos em cada etapa e utilizando o Algoritmo da Divisão de Euclides.*

1. $f \leftarrow \frac{f}{l(f)}$;
2. $g \leftarrow \frac{g}{l(g)}$;
3. *Calcule $r(x)$ utilizando o Algoritmo 2.1;*
4. **Se** $r(x) = 0$,
   então
   4.1. $h \leftarrow g$;
   4.2. **vá para** *9;*
5. **Se** $\partial r(x) = 0$,
   então
   5.1. $h \leftarrow 1$;

5.2. **vá para** *9;*

6. $f \leftarrow g$;

7. $g \leftarrow \frac{r}{l(r)}$;

8. **vá para** *3;*

9. *O algoritmo termina com h como o M.D.C. procurado.*

Exemplo 2.4 Considerando os polinômios $f(x)$ e $g(x)$ do exemplo 2.2 (também utilizados no exemplo 2.3), ao aplicarmos o Algoritmo 2.3 obtemos:

$f(x)$	$g(x)$
$1, 0, 1, 0, -3, -3, 8, 2, -5$	$1, 0, \frac{5}{3}, 0, -\frac{4}{3}, -3, 7$
$1, 0, \frac{5}{3}, 0, -\frac{4}{3}, -3, 7$	$1, 0, -\frac{1}{5}, 0, \frac{3}{5}$
$1, 0, -\frac{1}{5}, 0, \frac{3}{5}$	$1, \frac{25}{13}, -\frac{49}{13}$
$1, \frac{25}{13}, -\frac{49}{13}$	$1, -\frac{6150}{4663}$
$1, -\frac{6150}{4663}$	1

Ao aplicarmos o Algoritmo 2.4, apesar dos coeficientes intermediários não serem tão grandes como os obtidos através do Algoritmo 2.3, ainda teremos o problema de utilizar aritmética racional e, conseqüentemente, ter que avaliar um grande número de M.D.C.s de números inteiros.

Na próxima seção apresentaremos algoritmos para o M.D.C. nos quais os coeficientes intermediários pertencem ao mesmo domínio dos polinômios iniciais. Assim, se estivermos procurando o M.D.C. de polinômios em $\mathbb{Z}[x]$, todos os coeficientes intermediários serão números inteiros.

2.3 Algoritmos para o M.D.C. de Polinômios sobre um Domínio Fatorial

Nesta seção apresentaremos algoritmos para o cálculo do M.D.C. de polinômios sobre um domínio fatorial, os quais tem como "ferramenta" principal o algoritmo que permite dividir estes polinômios: o Algoritmo da Pseudo-Divisão.

Podemos estender o Algoritmo 2.3 para um algoritmo que calcule o M.D.C. de polinômios com coeficientes sobre um domínio fatorial, utilizando o Algoritmo 2.2 ao invés do Algoritmo de Euclides. Além disso, analogamente ao que fizemos no Algoritmo 2.4, podemos tornar os polinômios primitivos antes de aplicarmos o Algoritmo da Pseudo-Divisão, obtendo coeficientes intermediários menos complicados.

Se estendermos o Algoritmo 2.3 sem tornar os polinômios primitivos em cada etapa, teremos, em geral, crescimento exponencial dos coeficientes, como poderemos observar no exemplo 2.5.

Exemplo 2.5 Sejam f e g os polinômios do exemplo 2.2. Ao aplicarmos o Algoritmo 2.3 utilizando o Algoritmo da Pseudo-Divisão no passo 2, obtemos a seguinte seqüência de restos:

$$-15x^4 + 3x^2 - 9,$$

$$15795x^2 + 30375x - 59535,$$

$$1254542875143750x - 1654608338437500$$

e

$$1259333879550074310093115199218750 0.$$

A validade do Algoritmo 2.5, no qual utilizaremos o Algoritmo da Pseudo-Divisão e retiraremos os fatores comuns dos coeficientes dos polinômios em cada etapa, é dada pelos lemas 2.3.1 e 2.3.2.

Lema 2.3.1 *Sejam $f(x)$, $g(x) \in D[x]$, onde D é um domínio fatorial. Então,*

$$MDC(f,g) = MDC(c(f),c(g)) \cdot MDC(pp(f),pp(g)).$$

Demonstração: Seja $h = MDC(f,g)$. Temos que $h = c(h)pp(h)$. Pelo corolário 1.4.10, $c(h) = a \cdot MDC(c(f),c(g))$ e $pp(h) = b \cdot MDC(pp(f),pp(g))$, onde a e b são invertíveis. Conseqüentemente, $h = a \cdot b \cdot MDC(c(f),c(g)) \cdot MDC(pp(f),pp(g))$. Como o produto de invertíveis é um invertível, $h = MDC(c(f),c(g)) \cdot MDC(pp(f),pp(g))$. □

Lema 2.3.2 *Sejam $f(x)$, $g(x) \in D[x]$ polinômios primitivos de graus α e β, respectivamente, tais que $\alpha \geq \beta$.*
Se $g(x) = 0$, então $MDC(f,g) = f$. Caso contrário, $MDC(f,g) = MDC(g,r) = MDC(g,pp(r))$, onde r é dado pela equação (2.2).

Demonstração:
1º caso: $g(x) = 0$.
Análogo à demonstração do 1º caso no lema 2.2.1.

2º caso: $g(x) \neq 0$. Seja $h = MDC(f,g)$.

(*i*) $h|f$ e $h|g \Rightarrow h|(l(g)^{\alpha-\beta+1}f)$ e $h|qg \Rightarrow h|(l(g)^{\alpha-\beta+1}f - qg) \Rightarrow h|r$. Logo, $h|g$ e $h|r$.

(*ii*) Seja $h' \in K[x]$ tal que $h'|g$ e $h'|r$. Então, $h'|qg$ e $h'|r \Rightarrow h'|(qg+r) \Rightarrow h'|(l(g)^{\alpha-\beta+1}f)$. Como g é primitivo e h' divide g, temos que h' é primitivo e, conseqüentemente, $h'|f$. Logo, $h'|MDC(f,g) = h$.

Por (i) e (ii) concluímos que $MDC(f,g) = h = MDC(g,r)$.
Além disso, como g é primitivo, $MDC(g,r) = MDC(g, pp(r))$.
Portanto,

$$MDC(f,g) = MDC(g,r) = MDC(g, pp(r)). \ \square$$

Algoritmo 2.5 *Dados dois polinômios não nulos f e g com coeficientes em um domínio fatorial, este algoritmo calcula o M.D.C. de f e g tornando os polinômios primitivos em cada etapa e utilizando o Algoritmo da Pseudo-Divisão.*

1. $d \leftarrow MDC(c(f), c(g))$;

2. $f \leftarrow pp(f)$;

3. $g \leftarrow pp(g)$;

4. *Calcule $r(x)$ utilizando o Algoritmo 2.2;*

5. **Se** $r(x) = 0$,
então vá para *10;*

6. **Se** $\partial r(x) = 0$,
então

6.1. $g \leftarrow 1$;

6.2. **vá para** *10;*

7. $f \leftarrow g$;

8. $g \leftarrow pp(r)$;

9. **vá para** *4;*

10. *O algoritmo termina com $d \cdot g(x)$ como o M.D.C. procurado.*

Exemplo 2.6 Para os polinômios

$$\begin{aligned} f(x) &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 \quad e \\ g(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21 \quad \in \mathbb{Z}[x], \end{aligned}$$

dos exemplos anteriores, utilizando o algoritmo 2.5 para calcular seu M.D.C., obtemos:

$f(x)$	$g(x)$	$r(x)$
$1, 0, 1, 0, -3, -3, 8, 2, -5$	$3, 0, 5, 0, -4, -9, 21$	$-15, 0, 3, 0, -9$
$3, 0, 5, 0, -4, -9, 21$	$5, 0, -1, 0, 3$	$-585, -1125, 2205$
$5, 0, -1, 0, 3$	$13, 25, -49$	$-233150, 307500$
$13, 25, -49$	$4663, -6150$	143193869

O Algoritmo 2.5, além da vantagem de poder ser aplicado para polinômios sobre um domínio fatorial que não seja um corpo, é mais rápido que os algoritmos apresentados na seção anterior, visto que, no caso dos polinômios terem coeficientes inteiros, trabalha-se em todas as etapas com números inteiros, evitando o problema de aumento no custo ao utilizar-se aritmética racional. Entretanto, para eliminar os fatores comuns dos restos e obter coeficientes menores, temos que calcular M.D.C.s de números inteiros em cada etapa, exatamente o que estamos tentando evitar ao não utilizar aritmética racional.

Felizmente, é possível evitar o cálculo da parte primitiva de cada $r(x)$ no passo 8 do Algoritmo 2.5 e manter os coeficientes com um tamanho razoável, bastando dividir cada resto por um elemento do domínio que prova-se ser um divisor de seus coeficientes. Este algoritmo, chamado de Algoritmo Sub-Resultante, foi descoberto por George E. Collins e aperfeiçoado por W. S. Brown e J. F. Traub.

Para uma demonstração da validade do Algoritmo Sub-Resultante, veja [11].

Algoritmo 2.6 (Algoritmo Sub-Resultante) *Dados dois polinômios não nulos f e g com coeficientes em um domínio fatorial, este algoritmo calcula o M.D.C. de f e g utilizando o Algoritmo da Pseudo-Divisão de Polinômios, necessitando de um número menor de cálculos de M.D.C.s de coeficientes.*

1. $d \leftarrow MDC(c(f), c(g))$;
2. $f \leftarrow pp(f)$;
3. $g \leftarrow pp(g)$;
4. $a \leftarrow b \leftarrow 1$;
5. $k \leftarrow \partial f(x) - \partial g(x)$;
6. *Calcule $r(x)$ utilizando o Algoritmo 2.2;*
7. **Se** $r(x) = 0$,
   então vá para *14;*
8. **Se** $\partial r(x) = 0$,
   então
   - 8.1. $g \leftarrow 1$;
   - 8.2. **vá para** *14;*
9. $f \leftarrow g$;
10. $g \leftarrow \dfrac{r(x)}{ab^k}$;
11. $a \leftarrow l(f)$;
12. $b \leftarrow b^{1-k}a^k$;
13. **vá para** *5;*
14. *O algoritmo termina com $d \cdot pp(g)$ como o M.D.C. procurado.*

Exemplo 2.7 Ao aplicarmos o Algoritmo 2.6 para os polinômios $f(x)$ e $g(x)$ dos exemplos anteriores obtemos:

$f(x)$	$g(x)$	a	b
$1,0,1,0,-3,-3,8,2,-5$	$3,0,5,0,-4,-9,21$	1	1
$3,0,5,0,-4,-9,21$	$-15,0,3,0,-9$	3	9
$-15,0,3,0,-9$	$65,125,-245$	-15	25
$65,125,-245$	$-9326,12300$	65	169

Apesar de termos crescimento linear dos coeficientes intermediários, o Algoritmo Sub-Resultante é o melhor de todos os algoritmos baseados no Algoritmo da Divisão de Euclides estendido para polinômios com coeficientes em um domínio fatorial, os chamados Algoritmos Euclidianos.

Podemos conseguir algoritmos melhores que os Euclidianos para o cálculo do M.D.C. utilizando *métodos modulares* que descreveremos no próximo capítulo.

Como na prática geralmente trabalha-se com polinômios com coeficientes no domínio fatorial dos inteiros, a partir do próximo capítulo trabalharemos com polinômios com coeficientes em $\mathbb{Z}$ ao invés de polinômios sobre um domínio fatorial genérico D.

3 ALGORITMOS MODULARES

Os algoritmos para o cálculo do Máximo Divisor Comum de polinômios baseados no Algoritmo da Divisão de Euclides, estudados no capítulo anterior, podem ter um custo computacional extremamente grande devido ao crescimento das expressões intermediárias. Como observamos no capítulo 2, no melhor algoritmo deste tipo, o Algoritmo Sub-Resultante, ainda há crescimento linear dos coeficientes intermediários.

Neste capítulo veremos que é possível obter algoritmos para o M.D.C. mais eficientes que os Euclidianos: os algoritmos que utilizam métodos modulares.

3.1 Métodos Modulares

A idéia principal dos métodos modulares é calcular o M.D.C. de dois polinômios com coeficientes inteiros em um outro domínio e, através de homomorfismos, recuperar a resposta do problema original.

Estes métodos baseiam-se no seguinte diagrama:

$$\begin{array}{ccc} f, g \in \mathbb{Z}[x] & & h = MDC(f,g) \in \mathbb{Z}[x] \\ \downarrow & & \uparrow \\ f_p, g_p \in \mathbb{Z}_p[x] & \longrightarrow & \bar{h} = MDC(f_p, g_p) \in \mathbb{Z}_p[x] \end{array}$$

Ou seja, dados dois polinômios com coeficientes inteiros, calcula-se o Máximo Divisor Comum dos seus polinômios correspondentes em $\mathbb{Z}_p[x]$, onde p é um número primo (na prática trabalha-se com vários números primos pequenos), e então obtém-se o M.D.C. em $\mathbb{Z}[x]$ conforme descreveremos na seção 3.3.

Os Algoritmos Modulares possuem a vantagem de não haver possibilidade de crescimento dos coeficientes intermediários na determinação do M.D.C.

em $\mathbb{Z}_p[x]$, pois o tamanho de todos os coeficientes fica limitado por p. Entretanto, surgem os seguintes problemas:

Problema 1: Os coeficientes do M.D.C. em $\mathbb{Z}_p[x]$ podem ser muito pequenos, isto é, menores que os coeficientes do M.D.C. procurado;

Problema 2: O grau do M.D.C. em $\mathbb{Z}_p[x]$ pode ser diferente do grau do M.D.C. em $\mathbb{Z}[x]$.

O Problema 1 é evitado através da obtenção de uma cota superior para os coeficientes do Máximo Divisor Comum que se deseja calcular, ou seja, calcula-se um número M maior que o módulo de todos os coeficientes do M.D.C.:

$$M \geq \|h\|_\infty = \max_i |c_i|, \qquad \text{onde } h = \sum_{i=0}^{n} c_i x^i = MDC(f,g).$$

Trabalha-se então em $\mathbb{Z}_p[x]$, onde p é um número primo maior que $2M$ (na prática trabalha-se com vários primos cujo produto é maior que $2M$), de maneira que os coeficientes ficam entre $-M$ e M.

Nos métodos modulares fica portanto evidente a importância do cálculo da cota M. No capítulo 4 apresentaremos duas cotas superiores distintas para os coeficientes do Máximo Divisor Comum.

O Problema 2 também pode ser contornado, como veremos na seção 3.2, onde introduziremos alguns resultados que garantem e explicam a eficiência destes métodos.

3.2 Escolhendo os Números Primos

Sejam $f(x) = \sum_{i=0}^{\alpha} a_i x^i$ e $g(x) = \sum_{i=0}^{\beta} b_i x^i$ polinômios com coeficientes inteiros e seja p um número primo. Denotaremos por $f_p(x)$ o polinômio $f(x)$ mod p e $g_p(x)$ o polinômio $g(x)$ mod $p \in \mathbb{Z}_p[x]$.

Lema 3.2.1 *Se p não divide o coeficiente líder do $MDC(f,g)$, então o grau do $MDC(f_p,g_p)$ é maior ou igual ao grau do $MDC(f,g)$.*

Demonstração: Sejam $h(x) = MDC(f(x),g(x))$ e $h_p(x) = h(x)$ mod $p \in \mathbb{Z}_p[x]$. Temos que h/f e, como homomorfismos preservam múltiplos, segue que h_p/f_p. Analogamente, h_p/g_p. Logo, $h_p/MDC(f_p,g_p)$. Portanto, o grau do $MDC(f_p,g_p)$ é maior ou igual ao grau de h_p. Como p não divide o coeficiente líder de h, temos que o grau de h_p é igual ao grau de h e obtemos a desigualdade procurada. □

Na prática o lema anterior não resolve o problema de obtermos o grau correto do M.D.C. ao trabalharmos módulo p, já que para utilizá-lo precisaríamos conhecer de antemão o coeficiente líder do M.D.C. que queremos calcular. Além disso, o lema só garante a desigualdade.

Porém, como conseqüência do lema obteremos o corolário 3.2.2 que poderá ser utilizado na prática com mais facilidade.

Corolário 3.2.2 *Se p não divide simultaneamente os coeficientes líderes de f e g, então o grau do $MDC(f_p,g_p)$ é maior ou igual ao grau do $MDC(f,g)$.*

Demonstração: Visto que o M.D.C. de f e g divide os dois polinômios, o seu coeficiente líder terá que dividir os coeficientes líderes dos dois polinômios. Como por hipótese p não divide o coeficiente líder de f ou não divide o coeficiente líder de g, obtemos que p não divide o coeficiente líder do M.D.C. de f e g. Assim, pelo lema 3.2.1, o grau do $MDC(f_p,g_p)$ é maior ou igual ao grau do $MDC(f,g)$. □

Trabalhando com um número primo p que satisfaça as hipóteses do corolário 3.2.2 poderemos garantir que o M.D.C. em $\mathbb{Z}_p[x]$ não terá grau menor que o M.D.C. em $\mathbb{Z}[x]$. Porém, ainda existirá a possibilidade de que o grau do M.D.C. em $\mathbb{Z}_p[x]$ seja estritamente maior que o grau do M.D.C. em $\mathbb{Z}[x]$. Por exemplo, considerando os polinômios

$$\begin{aligned} f(x) &= x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5; \\ g(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21, \end{aligned}$$

citados em [6], obtemos que $MDC(f_2, g_2) = x + 1$, enquanto que $MDC(f, g) = 1$. Trabalhando com p=5 e com os polinômios

$$\begin{aligned} r(x) &= x^3 + 5x - 1; \\ s(x) &= x - 1, \end{aligned}$$

obtemos que $MDC(r_5, s_5) = x - 1$, enquanto que $MDC(r, s) = 1$.

Entretanto, conforme mostraremos no corolário 3.2.4, somente para um número finito de primos p existe a possibilidade de que o grau do M.D.C. módulo p seja maior que o grau do M.D.C. sobre os inteiros.

Lema 3.2.3 *Seja $h = MDC(f, g)$. Se p não divide simultaneamente os coeficientes líderes de f e g, e não divide $Res(f/h, g/h)$, então $MDC(f_p, g_p) = h_p$.*

Demonstração: Como p não divide o coeficiente líder de h (conforme observamos na demonstração do corolário anterior), obtemos que h_p é não nulo. Assim, considerando os quocientes f_p/h_p e g_p/h_p, temos que:

$$MDC(f_p, g_p) = h_p MDC(f_p/h_p, g_p/h_p). \tag{3.1}$$

Por outro lado, como p não divide $Res(f/h, g/h)$, obtemos que $Res(f/h, g/h)_p$ é não nulo. Visto que o resultante é um determinante e $det(M_p) = (det(M))_p$, onde M representa uma matriz, obtemos que $Res(f_p/h_p, g_p/h_p) = Res(f/h, g/h)_p \neq 0$. Pelo corolário 1.4.14, concluímos que f_p/h_p e g_p/h_p não têm nenhum fator em comum e, conseqüentemente, $MDC(f_p/h_p, g_p/h_p) = 1$. Substituindo este resultado em (3.1) o lema fica demonstrado. □

Corolário 3.2.4 *Existe somente um número finito de números primos p tais que o M.D.C. em $\mathbb{Z}[x]$ não tem o mesmo grau do M.D.C. em $\mathbb{Z}_p[x]$.*

Demonstração: Se p é um número primo p tal que o grau do M.D.C. em $\mathbb{Z}[x]$ é diferente do grau do M.D.C. em $\mathbb{Z}_p[x]$, então p não satisfaz as hipóteses do lema 3.2.3, ou seja, p divide simultaneamente os coeficientes líderes de f e g, e divide o $Res(f/h, g/h)$. Como f/h e g/h são relativamente primos (pois $h = MDC(f, g)$), pelo corolário 1.4.14 obtemos que o $Res(f/h, g/h)$ é diferente de zero e, portanto, tem um número finito de divisores. □

Como conseqüência do corolário 3.2.4, temos que sempre é possível obter um número primo p tal que o grau do M.D.C. em $\mathbb{Z}_p[x]$ seja o mesmo do M.D.C. em $\mathbb{Z}[x]$, o que garante que os algoritmos modulares que apresentaremos na próxima seção terminarão após um número finito de passos.

3.3 Calculando o M.D.C.

Nesta seção apresentaremos três algoritmos para o cálculo do Máximo Divisor Comum de polinômios, baseados em métodos modulares. A eficiência destes algoritmos, embora possa parecer surpreendente, está atestada pelas suas implementações nos sistemas de Computação Algébrica.

Lembremos que para que os métodos modulares possam ser utilizados, é necessário que o Problema 1 e Problema 2 da seção 3.1 sejam resolvidos. Os algoritmos que apresentaremos a seguir diferem pela técnica de resolução do Problema 1. A solução do Problema 2, ou seja, a garantia de que o grau do M.D.C. modular seja o mesmo do M.D.C procurado, é obtida nos três algoritmos através de tentativas, processo cuja validade está garantida pelo corolário do lema 3.2.3.

Com o objetivo de evitar o Problema 1, os algoritmos modulares requerem que seja previamente conhecida uma cota superior para os coeficientes do M.D.C. No capítulo 4, discutiremos detalhadamente a obtenção de duas cotas superiores distintas (corolários 4.1.6 e 4.2.5). Como ambas são razoavelmente simples de serem implementadas, sugerimos que para a aplicação destes algoritmos as duas sejam calculadas, escolhendo-se a menor delas.

3.3.1 Primeira Solução

Nesta primeira resolução do M.D.C. via métodos modulares, a garantia de que os coeficientes do M.D.C módulo p sejam do tamanho correto (Problema 1), é obtida escolhendo-se p maior que $2M$, a cota para os coeficientes.

Sejam f e g dois polinômios com coeficientes inteiros para os quais busca-se

$$h(x) = MDC(f(x), g(x)) = \sum_{i=0}^{n} c_i x^i,$$

e seja

$$M \geq \|h\|_\infty = \max_i |c_i|.$$

Se escolhermos p satisfazendo

$$p \geq 2M,$$

poderemos garantir que os coeficientes do MDC obtido módulo p têm o tamanho correto.

Algoritmo 3.1 *Dados dois polinômios não nulos f e g com coeficientes inteiros, este algoritmo calcula o M.D.C. de f e g utilizando redução módulo um número primo p.*

1. *$M \leftarrow$ cota superior para os coeficientes do$MDC(f,g)$;*
2. *$p \leftarrow$ número primo maior que $2M$;*
3. **Se** *p não divide o coeficiente líder de f ou não divide o coeficiente líder de g,*
   então $\bar{h} \leftarrow MDC(f_p, g_p)$,
   senão vá para *2;*
4. **Se** *$\bar{h}$ divide f e divide g,*
   então $h \leftarrow \bar{h}$,
   senão vá para *2;*
5. *O algoritmo termina com h como o M.D.C. procurado.*

Observações:

1.Neste algoritmo escolhemos um número primo p maior que os coeficientes do M.D.C. de f e g para evitar o Problema 1. Não é necessário, entretanto, escolher p maior que os coeficientes intermediários que podem ser maiores que os coeficientes "finais" do M.D.C. (veja o exemplo 2.5).

2. Para calcular o M.D.C. de f_p e g_p no passo 3, pode-se utilizar o Algoritmo de Euclides para polinômios sobre um corpo (Algoritmo 2.3) ou um de seus derivados, apresentados no capítulo 2.

3. O passo 4 baseia-se no seguinte resultado:

Lema 3.3.1 *Sejam f e g polinômios e seja $\bar{h}$ o M.D.C. de f_p e g_p, onde p é um número primo que não divide simultaneamente os coeficientes líderes de f e g. Se $\bar{h}$ divide f e divide g, então ele é o M.D.C. de f e g.*

Demonstração: Pelo corolário 3.2.2, o grau de $\bar{h}$ é maior ou igual ao grau do M.D.C. de f e g. Por outro lado, como $\bar{h}$ divide f e divide g, ele divide o M.D.C. de f e g e, portanto, seu grau é menor ou igual ao grau do M.D.C. de f e g. Conseqüentemente, pela unicidade do M.D.C. concluímos que $\bar{h}$ é o M.D.C. de f e g. □

4. Se no passo 4 $\bar{h}$ não divide f ou não divide g, isto significa que $\bar{h}$ tem grau maior do que h. Pelo lema 3.2.3, isso é equivalente a dizer que p divide $\text{Res}(f/h, g/h)$. Como existe somente um número finito de primos p que satisfazem essa condição , segue que o algoritmo termina com sucesso após um número finito de passos.

Exemplo 3.1 Sejam

$$\begin{aligned} f(x) &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 \quad e \\ g(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21 \quad \in \mathbb{Z}[x]. \end{aligned}$$

Ao calcularmos uma cota superior M para os coeficientes do M.D.C. de f e g, obtivemos $M = 99.3579$ utilizando o corolário 4.1.6, e $M = 510.219$ pelo corolário 4.2.5. Assim,

1. $M \leftarrow 99.3579$

2. $p \leftarrow 199$

3. $\bar{h} \leftarrow 1$

4. $h \leftarrow 1$.

No passo 3 aplicamos o Algoritmo 2.3 para calcular o $MDC(f_{199}, g_{199})$, obtendo os seguintes coeficientes:

$f(x)$	$g(x)$	$r(x)$
$1,0,1,0,-3,-3,8,2,-5$	3,0,5,0,-4,-9,21	-89,0,-22,0,66
3,0,5,0,-4,-9,21	-89,0,-22,0,66	59,-9,54
-89,0,-22,0,66	59,-9,54	-84,74
59,-9,54	-84,74	30
-84,74	30	0

Ao aplicarmos o Algoritmo 3.1, é possível que tenhamos que trabalhar com um número primo grande, o que possibilitará que os coeficientes intermediários no cálculo do M.D.C módulo p também sejam grandes, ocasionando lentidão nos cálculos. Uma solução para este problema será apresentada no Algoritmo 3.2.

3.3.2 Uma Segunda Solução

No algoritmo abaixo, utilizam-se vários números primos pequenos (ao invés de um único número primo como no Algoritmo 3.1) e o Teorema Chinês dos Restos (teorema 1.4.15) para obter-se o M.D.C. de polinômios em $\mathbb{Z}[x]$ através de imagens homomórficas. Esta idéia, devida a W. S. Brown e G. E. Collins, foi descrita detalhadamente por Brown em [5].

Algoritmo 3.2 *Dados dois polinômios não nulos f e g com coeficientes inteiros, este algoritmo calcula o M.D.C. de f e g utilizando redução módulo números primos pequenos e o Teorema Chinês dos Restos.*

1. $M \leftarrow$ *cota superior para os coeficientes do* $MDC(f,g)$;
2. $N \leftarrow MDC$(*coef. líder de* f, *coef. líder de* g);
3. $p \leftarrow$ *número primo que não divide* N;
4. $\bar{h} \leftarrow MDC(f_p, g_p)$;
5. **Se** *o grau de* $\bar{h}$ *for zero,*
   então

5.1. $h \leftarrow 1$;

5.2. **vá para** *11;*

6. $prodprim \leftarrow p$;

7. $result \leftarrow \bar{h}$;

8. **Enquanto** $prodprim \leq 2M$

faça

8.1. $p \leftarrow$ *número primo que não divide* N;

8.2. $\bar{h} \leftarrow MDC(f_p, g_p)$;

8.3. **Se** *o grau de* $\bar{h}$ *for menor que o grau de result,*

então vá para *5;*

8.4. **Se** *o grau de* $\bar{h}$ *for igual ao grau de result,*

então

8.4.1. $result \leftarrow$ *Teorema Chinês dos Restos aplicado a cada coeficiente dos polinômios result* (mod *prodprim*) *e* $\bar{h}$ (mod p);

8.4.2. $prodprim \leftarrow prodprim \times p$;

9. **Se** *result divide f e divide g,*

então

9.1. $h \leftarrow result$;

9.2. **vá para** *11;*

10. **Vá para** *3;*

11. *O algoritmo termina com h como o M.D.C. procurado.*

Observações:

1. O passo 8.3 testa se o M.D.C. módulo o novo primo obtido em 8.1 tem grau menor que os M.D.C. anteriores. Em caso afirmativo conclui-se que os M.D.C. anteriores devem ser desprezados pois vieram de más reduções, ou seja, $MDC(f_p, g_p) \neq MDC(f, g)_p$.

2. O passo 9 só será executado se todos os M.D.C. calculados vierem de más reduções, uma possibilidade remota.

3. Se o primeiro primo calculado no passo 3 for de boa redução, nenhum dos desvios será executado durante a aplicação do algoritmo.

Freqüentemente, as cotas superiores para os coeficientes do M.D.C. são muito pessimistas (veja as tabelas 4.1 e 4.2 do capítulo 4), sendo possível que já tenhamos encontrado os coeficientes corretos antes de atingirmos $2M$. Considerando esta possibilidade, numa tentativa de melhorar o Algoritmo 3.2 apresentaremos o Algoritmo 3.3, no qual testaremos se já foi obtido um divisor dos polinômios e, portanto, o seu M.D.C., sempre que os coeficientes não se alterarem após aplicarmos o Teorema Chinês dos Restos.

3.3.3 Terceira Solução

Algoritmo 3.3 *Dados dois polinômios não nulos f e g com coeficientes inteiros, estealgoritmo calcula o M.D.C. de f e g utilizando redução módulo números primos pequenos e o Teorema Chinês dos Restos, testando se o M.D.C. já foi obtido antes de atingir-se o dobro da cota superior para os coeficientes.*

1. $M \leftarrow$ *cota superior para os coeficientes do* $MDC(f,g)$;

2. $N \leftarrow MDC$(*coef. líder de* f, *coef. líder de* g);

3. $p \leftarrow$ *número primo que não divide* N;

4. $\bar{h} \leftarrow MDC(f_p, g_p)$;

5. **Se** *o grau de* $\bar{h}$ *for zero,*

então

5.1. $h \leftarrow 1$;

5.2. **vá para** *11;*

6. $prodprim \leftarrow p$;

7. $result \leftarrow \bar{h}$;

8. **Enquanto** $prodprim \leq 2M$

faça

8.1. $p \leftarrow$ *número primo que não divide* N;

8.2. $\bar{h} \leftarrow MDC(f_p, g_p)$;

8.3. **Se** *o grau de* $\bar{h}$ *for menor que o grau de result,*
então vá para *5;*

8.4. **Se** *o grau de* $\bar{h}$ *for igual ao grau de result,*
então

8.4.1. *anterior* $\leftarrow$ *result;*

8.4.2. *result* $\leftarrow$ *Teorema Chinês dos Restos aplicado a cada coeficiente dos polinômios result* (mod *prodprim*) *e* $\bar{h}$ (mod p);

8.4.3. **Se** *result* = *anterior e result divide f e divide g,*
então

8.4.3.1. $h \leftarrow$ *result;*

8.4.3.2. **vá para** *11;*

8.4.4. *prodprim* $\leftarrow$ *prodprim* $\times$ p ;

9. **Se** *result divide f e divide g,*
então

9.1. $h \leftarrow$ *result;*

9.2. **vá para** *11;*

10. **Vá para** *3;*

11. *O algoritmo termina com h como o M.D.C. procurado.*

Observação: Testar em cada etapa se já encontramos o M.D.C. é uma operação que pode ter um custo muito grande. Por esta razão, no passo 8.4.3 este teste é realizado apenas quando os coeficientes não se alteram após a aplicação do Teorema Chinês dos Restos, visto que, neste caso, é maior a possibilidade de que já tenhamos encontrado os coeficientes corretos.

A obtenção de uma cota superior que não se distancie demasiadamente dos coeficientes verdadeiros é um ponto crucial para os Algoritmos Modulares, pois

poderemos obter o M.D.C. através do Algoritmo 3.2 mais rapidamente e sem a necessidade de realizar os dispendiosos testes implementados no Algoritmo 3.3.

No próximo capítulo trataremos desse problema, inclusive introduzindo uma nova cota para o M.D.C. que, na maioria dos casos, é melhor que a cota atualmente utilizada, ou seja, fica mais próxima dos coeficientes para a maior parte dos polinômios.

Uma alternativa em relação à utilização do Teorema Chinês dos Restos para a obtenção do M.D.C. módulo "$prodprim \times p$" nos Algoritmos 3.2 e 3.3, é, conforme sugerido por J. Moses e D. Y. Y. Yun em [18], a utilização do lema de Hensel para passarmos da solução módulo p para a solução módulo p^k, com k suficientemente grande. Entretanto, este método, conhecido por p-ádico, só é válido diretamente quando $MDC\left(\bar{h}, \frac{f_p}{\bar{h}}\right) = 1$ ou $MDC\left(\bar{h}, \frac{g_p}{\bar{h}}\right) = 1$, onde $\bar{h} = MDC(f_p, g_p)$. Esta é uma das razões pelas quais este método não é utilizado na prática.

4 COTAS SUPERIORES PARA OS COEFICIENTES DO M.D.C.

Os Algoritmos Modulares mais eficientes para o cálculo do Máximo Divisor Comum de polinômios, apresentados no capítulo anterior, requerem que seja onhecida uma cota superior para os coeficientes do M.D.C. que se deseja calcular.

Neste capítulo apresentaremos a nova cota superior, que obtivemos utilizando a norma com pesos introduzida em Beauzamy *et al* [1], e a cota utilizada atualmente, devida a Mignotte [14], obtida como conseqüência da desigualdade de Landau. Na seção 4.3 faremos uma comparação entre as cotas.

4.1 Uma Cota Superior para os Coeficientes

A cota superior para os coeficientes do Máximo Divisor Comum de polinômios que apresentaremos nesta seção é obtida aplicando-se a desigualdade de Landau-Mignotte para o M.D.C. de dois polinômios. Apresentaremos detalhadamente a obtenção desta cota, utilizando resultados que, embora estejam disponíveis na literatura, não estão compilados de modo simples como faremos aqui.

Definição 4.1.1 (Norma Euclidiana) *Seja* $h = \sum_{i=0}^{n} c_i x^i$ *um polinômio com coeficientes complexos. A Norma Euclidiana de* h *é definida por*

$$\|h\| = \sqrt{\sum_{i=0}^{n} |c_i|^2}.$$

Definição 4.1.2 (Medida de Mahler) *Seja* $h = \sum_{i=0}^{n} c_i x^i$ *um polinômio com coeficientes complexos e sejam* $z_1, \ldots, z_n$ *as suas raízes. A Medida de Mahler de* h *é*

definida por

$$M(h) = |c_n| \prod_{i=1}^{n} \max\{1, |z_i|\}.$$

A medida de Mahler também pode ser escrita na forma

$$M(h) = |c_n| \prod_{|z_i|>1} |z_i|.$$

O lema que enunciaremos a seguir será necessário para obtermos a desigualdade de Landau.

Lema 4.1.3 *Seja h um polinômio com coeficientes complexos e seja z um número complexo não nulo. Então,*

$$\|(x+z)h(x)\| = \|(\bar{z}x+1)h(x)\|.$$

Demonstração: Seja $h(x) = \sum_{i=0}^{n} c_i x^i$. Então,

$(x+z)h(x) = (x+z)\sum_{i=0}^{n} c_i x^i = \sum_{i=0}^{n+1}(c_{i-1} + c_i z)x^i$, onde $c_{-1} = c_{n+1} = 0$.

Logo,

$$\begin{aligned}
\|(x+z)h(x)\|^2 &= \sum_{i=0}^{n+1} |c_{i-1} + c_i z|^2 = \sum_{i=0}^{n+1}(c_{i-1} + c_i z)\overline{(c_{i-1} + c_i z)} = \\
&= (|c_0|^2|z|^2) + (|c_0|^2 + z c_1 \bar{c}_0 + \bar{z}\bar{c}_1 c_0 + |c_1|^2|z|^2) + \ldots + \\
&+ (|c_{n-1}|^2 + z c_n \bar{c}_{n-1} + \bar{z}\bar{c}_n c_{n-1} + |c_n|^2|z|^2) + (|c_n|^2) = \\
&= (1+|z|^2)\left(\sum_{i=0}^{n} |c_i|^2\right) + \sum_{i=0}^{n}(z c_i \bar{c}_{i-1} + \bar{z}\bar{c}_i c_{i-1}), \text{ onde } c_{-1} = 0.
\end{aligned}$$

Além disso,

$(\bar{z}x+1)h(x) = (\bar{z}x+1)\sum_{i=0}^{n} c_i x^i = \sum_{i=0}^{n+1}(c_{i-1}\bar{z} + c_i)x^i$, onde $c_{-1} = c_{n+1} = 0$.

Logo,

$$\begin{aligned}
\|(\bar{z}x+1)h(x)\|^2 &= \sum_{i=0}^{n+1} |c_{i-1}z + c_i|^2 = \sum_{i=0}^{n+1} (c_{i-1}\bar{z}+c_i)\overline{(c_{i-1}\bar{z}+c_i)} = \\
&= (|c_0|^2) + (|c_0|^2|z|^2 + zc_1\bar{c}_0 + \bar{z}\bar{c}_1c_0 + |c_1|^2) + \ldots + \\
&+ (|c_{n-1}|^2|z|^2 + zc_n\bar{c}_{n-1} + \bar{z}\bar{c}_nc_{n-1} + |c_n|^2) + (|c_n|^2|z|^2) = \\
&= (1+|z|^2)\left(\sum_{i=0}^{n-1} |c_i|^2\right) + \sum_{i=0}^{n} (zc_i\bar{c}_{i-1} + \bar{z}\bar{c}_ic_{i-1}), \text{ onde } c_{-1} = 0.
\end{aligned}$$

Conseqüentemente,

$\|(x+z)h(x)\|^2 = \|(\bar{z}x+1)h(x)\|^2$ e o lema fica demonstrado. □

Teorema 4.1.4 (Desigualdade de Landau) *Seja* $h(x) = \sum_{i=0}^{n} c_i x^i$, *onde* $c_n \neq 0$, *um polinômio com coeficientes complexos, e sejam* $z_1, \ldots, z_n$ *as suas raízes. Então,*

$$M(h) \leq \|h\|.$$

Demonstração: Sejam $z_1, \ldots, z_k$ as raízes de h fora do círculo unitário, isto é $|z_i| > 1$, $i = 1, \ldots, k$. Então, $M(h) = |c_n||z_1 \ldots z_k|$. Seja

$$f(x) = c_n \prod_{j=1}^{k} (\bar{z}_j x - 1) \prod_{j=k+1}^{n} (x - z_j) = \sum_{j=1}^{n} b_j x^j.$$

Aplicando o lema 4.1.3 em cada um dos k fatores $\bar{z}_j x - 1$ de f, obtemos que

$$\begin{aligned}
\|f(x)\| &= |c_n| \, \| \prod_{j=1}^{k} (\bar{z}_j x - 1) \prod_{j=k+1}^{n} (x - z_j)\| = \\
&= |c_n| \, \| \prod_{j=1}^{k} (-\bar{z}_j x + 1) \prod_{j=k+1}^{n} (x - z_j)\| = \\
&= |c_n| \, \| \prod_{j=1}^{k} (x - z_j) \prod_{j=k+1}^{n} (x - z_j)\| = \\
&= |c_n| \, \| \prod_{j=1}^{n} (x - z_j)\| = \|h(x)\|.
\end{aligned}$$

Além disso, temos que

$$\|f\|^2 \geq |b_n|^2 = |c_n \bar{z}_1 \dots \bar{z}_k|^2 = |c_n|^2 |z_1 \dots z_k|^2 = M(h)^2.$$

Conseqüentemente, $M(h) \leq \|f\| = \|h\|$ e o teorema fica demonstrado. □

Teorema 4.1.5 (Desigualdade de Landau-Mignotte) *Seja* $h = \sum_{i=0}^{n} c_i x^i$ *um divisor do polinômio* $f = \sum_{i=0}^{\alpha} a_i x^i$ *(onde* a_i *e* c_i *são inteiros). Então,*

$$\sum_{i=0}^{n} |c_i| \leq 2^n \left|\frac{c_n}{a_\alpha}\right| \sqrt{\sum_{i=0}^{\alpha} |a_i|^2} = 2^n \left|\frac{c_n}{a_\alpha}\right| \|f\|. \tag{4.1}$$

Demonstração: Sejam $z_1, \dots, z_n$ as raízes de h ordenadas de maneira que $z_1, \dots, z_k$ sejam as raízes fora do círculo unitário. Cada coeficiente c_i de h é, a menos de sinal, soma de $\binom{n}{i}$ parcelas, sendo cada uma delas um produto de $n-i$ raízes; ou seja, cada parcela é da forma $c_n z_{j_1} \dots z_{j_i}$, onde $\{j_1, \dots, j_i\}$ é um subconjunto de $\{1, \dots, n\}$ com cardinalidade $n - i$. Conseqüentemente,

$$|c_i| \leq |c_n| \binom{n}{i} |z_1 \dots z_k|.$$

Como $\sum_{i=0}^{n} \binom{n}{i} = 2^n$, segue que

$$\sum_{i=0}^{n} |c_i| \leq 2^n |c_n| |z_1 \dots z_k| = 2^n M(h).$$

Por outro lado, como as raízes de h também são raízes de f, obtemos que

$$\frac{M(h)}{|c_n|} = \prod_{i=1}^{n} \max\{1, |z_i|\} \leq \prod_{i=1}^{\alpha} \max\{1, |z_i'|\} = \frac{M(f)}{|a_\alpha|},$$

onde $z'_1, \ldots, z'_\alpha$ são as raízes de f. Logo,

$$M(h) \leq \left|\frac{c_n}{a_\alpha}\right| M(f).$$

Além disso, pela desigualdade de Landau (teorema 4.1.4),

$$M(f) \leq \|f\|.$$

Assim,

$$\sum_{i=0}^{n} |c_i| \leq 2^n M(h) \leq 2^n \left|\frac{c_n}{a_\alpha}\right| \|f\|. \quad \square$$

Corolário 4.1.6 (Cota de Landau-Mignotte) *Todo coeficiente do M.D.C. de* $f = \sum_{i=0}^{\alpha} a_i x^i$ *e* $g = \sum_{i=0}^{\beta} b_i x^i$ *(onde* a_i *e* b_i *são inteiros) é limitado por*

$$2^{\min\{\alpha,\beta\}} MDC(a_\alpha, b_\beta) \min\left\{ \frac{1}{|a_\alpha|}\sqrt{\sum_{i=0}^{\alpha} |a_i|^2},\ \frac{1}{|b_\beta|}\sqrt{\sum_{i=0}^{\beta} |b_i|^2} \right\}. \tag{4.2}$$

Demonstração: Seja $h = \sum_{i=0}^{n} c_i x^i$ o $MDC(f,g)$. Então, h é um divisor de f e g com grau menor ou igual ao grau de cada um dos polinômios. Além disso, o coeficiente líder de h divide o coeficiente líder de f e o coeficiente líder de g. Conseqüentemente,

$$\sum_{i=0}^{n} |c_i| \leq 2^n \left|\frac{c_n}{a_\alpha}\right| \sqrt{\sum_{i=0}^{\alpha} |a_i|^2} \leq 2^{\min\{\alpha,\beta\}} MDC(a_\alpha, b_\beta) \frac{1}{|a_\alpha|}\sqrt{\sum_{i=0}^{\alpha} |a_i|^2}$$

e

$$\sum_{i=0}^{n} |c_i| \leq 2^n \left|\frac{c_n}{b_\beta}\right| \sqrt{\sum_{i=0}^{\beta} |b_i|^2} \leq 2^{\min\{\alpha,\beta\}} MDC(a_\alpha, b_\beta) \frac{1}{|b_\beta|}\sqrt{\sum_{i=0}^{\beta} |b_i|^2}.$$

Assim,

$$\sum_{i=0}^{n} |c_i| \leq 2^{\min\{\alpha,\beta\}} MDC(a_\alpha, b_\beta) \min\left\{ \frac{1}{|a_\alpha|}\sqrt{\sum_{i=0}^{\alpha} |a_i|^2},\ \frac{1}{|b_\beta|}\sqrt{\sum_{i=0}^{\beta} |b_i|^2} \right\},$$

e obtemos a cota procurada. □

A cota de Landau-Mignotte 4.2 é a cota mais utilizada nos algoritmos modulares para o cálculo do M. D. C. polinomial implementados nos sistemas de Computação Algébrica. O resultado que apresentaremos na próxima seção é melhor que este resultado de 1974 para a maioria dos polinômios.

4.2 Uma Nova Cota Superior para os Coeficientes

Nesta seção aplicaremos um resultado apresentado por Beauzamy em [2] para obter uma nova cota superior para os coeficientes do M.D.C. de dois polinômios.

Em seu trabalho Beauzamy utilizou a norma com pesos que havia sido introduzida por E. Bombieri em Beauzamy *et al* [1], ao invés da norma euclidiana.

Definição 4.2.1 *Seja* $f = \sum_{i=0}^{\alpha} a_i x^i$ *um polinômio com coeficientes complexos. A norma com pesos de* f *é definida por*

$$[f]_2 = \left(\sum_{i=0}^{\alpha} \frac{|a_i|^2}{\binom{\alpha}{i}} \right)^{1/2}.$$

É fácil ver que a norma com pesos introduzida por Bombieri satisfaz

$$[f]_2 \leq \|f\|.$$

Teorema 4.2.2 *Sejam p e q polinômios com coeficientes complexos de graus m e n, respectivamente. Então:*

$$[pq]_2 \geq \sqrt{\frac{m!n!}{(m+n)!}}[p]_2[q]_2. \tag{4.3}$$

Este resultado é o melhor possível.

Demonstração: A demonstração deste teorema pode ser encontrada em [2]. Nela Beauzamy utiliza um resultado de Bombieri em [1] para polinômios a várias variáveis para obter a desigualdade 4.3. Ele também mostra em [2] que os polinômios

$$p(z) = 2^{-n/2}(1-z)^n, \quad \text{e} \quad q(z) = 2^{-n/2}(1+z)^n$$

satisfazem a igualdade, fazendo com que o resultado seja o melhor possível. □

Beauzamy aplicou o teorema 4.2.2 para obter uma cota superior para os coeficientes de p ou de q, conhecendo os coeficientes do produto $f = p \cdot q$.

Teorema 4.2.3 (Beauzamy, 1992) *Seja f um polinômio de grau α com coeficientes inteiros, tal que $f(0) \neq 0$, e seja $f = p \cdot q$ uma fatoração de f em $\mathbb{Z}[x]$, onde p e q têm graus m e n, respectivamente. Então, qualquer coeficiente c_i de p satisfaz:*

$$|c_i| \leq \sqrt{\frac{1}{2}\binom{m}{i}\binom{\alpha}{m}}[f]_2 = \sqrt{\frac{\alpha!}{2(\alpha-m)!(m-i)!i!}}[f]_2. \tag{4.4}$$

Demonstração: Pelo teorema 4.2.2, temos que

$$[f]_2{}^2 = [pq]_2{}^2 \geq \frac{m!n!}{(m+n)!}[p]_2{}^2[q]_2{}^2.$$

Logo,

$$[p]_2{}^2 \leq \frac{(m+n)!}{m!n!}\frac{[f]_2{}^2}{[q]_2{}^2}.$$

Como q tem coeficientes inteiros, seus coeficientes têm módulo ≥ 1. Em particular, o primeiro e o último coeficientes de q têm módulo ≥ 1. Portanto, $[q]_2 \geq \sqrt{2}$ e

$$[p]_2{}^2 \leq \frac{(m+n)!}{2m!n!}[f]_2{}^2.$$

Conseqüentemente, cada coeficiente c_i de p satisfaz:

$$|c_i|^2 \leq \binom{m}{i}\frac{(m+n)!}{2m!n!}[f]_2{}^2 = \binom{m}{i}\frac{\alpha!}{2m!(\alpha-m)!}[f]_2{}^2 = \frac{1}{2}\binom{m}{i}\binom{\alpha}{m}[f]_2{}^2.$$

Logo,

$$|c_i| \leq \sqrt{\frac{1}{2}\binom{m}{i}\binom{\alpha}{m}}[f]_2 = \sqrt{\frac{\alpha!}{2(\alpha-m)!(m-i)!i!}}[f]_2. \quad \square$$

Utilizando o teorema 4.2.3 Beauzamy obteve uma cota superior para os coeficientes de um fator qualquer de um polinômio.

Teorema 4.2.4 (Beauzamy, 1992) *Seja f um polinômio de grau α com coeficientes inteiros tal que $f(0) \neq 0$, e seja h um divisor de f em $\mathbb{Z}[x]$. Então, todo coeficiente c_i de h satisfaz:*

$$|c_i| \leq \frac{3^{3/4}}{2\sqrt{\pi}}\frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2. \tag{4.5}$$

Demonstração: Suponhamos que h tenha grau $n \geq 1$. Pelo teorema 4.2.3, temos que

$$|c_i| \leq \sqrt{\frac{\alpha!}{2(\alpha-n)!(n-i)!i!}}[f]_2.$$

Pela Fórmula de Stirling [4, 7]:

$$\begin{aligned}
\alpha! &\sim 2^{\frac{1}{2}}\pi^{\frac{1}{2}}\alpha^{\alpha+\frac{1}{2}}e^{-\alpha} \\
(\alpha-n)! &\sim 2^{\frac{1}{2}}\pi^{\frac{1}{2}}(\alpha-n)^{(\alpha-n)+\frac{1}{2}}e^{n-\alpha} \\
(n-i)! &\sim 2^{\frac{1}{2}}\pi^{\frac{1}{2}}(n-i)^{(n-i)+\frac{1}{2}}e^{i-n} \\
i! &\sim 2^{\frac{1}{2}}\pi^{\frac{1}{2}}i^{i+\frac{1}{2}}e^{-i}
\end{aligned}$$

Logo,

$$|c_i| \leq \sqrt{\frac{\alpha^{\alpha+\frac{1}{2}}}{4\pi(\alpha-n)^{(\alpha-n)+\frac{1}{2}}(n-i)^{(n-i)+\frac{1}{2}}(i)^{(i+\frac{1}{2})}}}[f]_2 \tag{4.6}$$

Por outro lado, observa-se que o denominador em 4.6 é da forma

$$x^{x+1/2}y^{y+1/2}z^{z+1/2}, \quad \text{onde } x+y+z=\alpha \text{ e } x,y,z \in \mathbb{Z}_+^*$$

(podemos assumir que x, y, z são não nulos). Considerando a função $f(x,y,z) = xyz$, e a superfície de nível $g(x,y,z) = \alpha$, onde $g(x,y,z) = x+y+z$, obtemos que

$$\overrightarrow{\text{grad}}\, f(x,y,z) = x^{x+1/2}y^{y+1/2}z^{z+1/2}\left(1+\frac{1}{2x}+lnx,\ 1+\frac{1}{2y}+lny,\ 1+\frac{1}{2z}+lnz\right)$$

e $\overrightarrow{\text{grad}}\, g(x,y,z) = (1,1,1)$. Pela teoria dos Multiplicadores de Lagrange, o mínimo de f ocorre quando $\overrightarrow{\text{grad}}\, f = \lambda \cdot \overrightarrow{\text{grad}}\, g$. Logo, f atinge seu valor mínimo sobre a superfície g num ponto (x,y,z) tal que

$$\frac{1}{2x}+lnx = \frac{1}{2y}+lny = \frac{1}{2z}+lnz. \tag{4.7}$$

Como a função $h(t) = \frac{1}{2t} + lnt$ é estritamente crescente para $t \geq 1$, as equações 4.7 implicam que $x = y = z$. Portanto, o valor mínimo de f sobre a superfície $x+y+z = \alpha$ ocorre no ponto $(\alpha/3, \alpha/3, \alpha/3)$. Conseqüentemente,

$$\frac{\alpha^{\alpha+\frac{1}{2}}}{(\alpha-n)^{(\alpha-n)+\frac{1}{2}}(n-i)^{(n-i)+\frac{1}{2}}(i)^{(i+\frac{1}{2})}} \leq \frac{\alpha^{\alpha+\frac{1}{2}}}{(\frac{\alpha}{3})^{\frac{\alpha}{3}+\frac{1}{2}}(\frac{\alpha}{3})^{\frac{\alpha}{3}+\frac{1}{2}}(\frac{\alpha}{3})^{\frac{\alpha}{3}+\frac{1}{2}}} = \frac{\alpha^{\alpha+\frac{1}{2}}}{(\frac{\alpha}{3})^{\alpha+\frac{3}{2}}} = \frac{3^{\frac{3}{2}}3^{\alpha}}{\alpha}.$$

Assim,

$$|c_i| \leq \sqrt{\frac{3^{3/2}3^{\alpha}}{4\pi\alpha}}[f]_2 = \frac{3^{3/4}}{2\sqrt{\pi}}\frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2. \quad \square$$

No teorema a seguir apresentaremos a nova cota superior para os coeficientes do M.D.C. de dois polinômios que obtivemos utilizando o teorema 4.2.4.

Teorema 4.2.5 *Todo coeficiente do M.D.C. de* $f = \sum_{i=0}^{\alpha} a_i x^i$ *e* $g = \sum_{i=0}^{\beta} b_i x^i$ *(onde* a_i *e* b_i *são inteiros) é limitado por*

$$\frac{3^{3/4}}{2\sqrt{\pi}} \min\left\{ \frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2, \frac{3^{\beta/2}}{\sqrt{\beta}}[g]_2 \right\} \tag{4.8}$$

Demonstração: Seja $h = \sum_{i=0}^{n} c_i x^i$ o $MDC(f,g)$. Então, h é um fator de f e g e qualquer coeficiente c_i de h satisfaz:

$$|c_i| \leq \frac{3^{3/4}}{2\sqrt{\pi}} \frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2 \qquad e \qquad |c_i| \leq \frac{3^{3/4}}{2\sqrt{\pi}} \frac{3^{\beta/2}}{\sqrt{\beta}}[g]_2.$$

Conseqüentemente,

$$|c_i| \leq \frac{3^{3/4}}{2\sqrt{\pi}} \min\left\{ \frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2, \frac{3^{\beta/2}}{\sqrt{\beta}}[g]_2 \right\}. \quad \square$$

Como geralmente $[f]_2$ é muito menor que $\|f\|$ para a maioria dos polinômios, espera-se que a nova cota seja melhor que a de Landau-Mignotte, como teremos oportunidade de mostrar na próxima seção.

4.3 Comparando as Cotas

Nesta seção faremos uma comparação entre a cota de Landau-Mignotte (desigualdade 4.2) e a nova cota superior (desigualdade 4.8).

Sejam $f = \sum_{i=0}^{\alpha} a_i x^i$ e $g = \sum_{i=0}^{\beta} b_i x^i$ polinômios com coeficientes inteiros. Seja

$$\begin{aligned} M_1 &= 2^k MDC(a_\alpha, b_\beta) \min\left\{ \frac{1}{|a_\alpha|}\|f\|, \frac{1}{|b_\beta|}\|g\| \right\} = \\ &= MDC(a_\alpha, b_\beta) \min\left\{ \frac{2^k}{|a_\alpha|}\|f\|, \frac{2^k}{|b_\beta|}\|g\| \right\}, \end{aligned}$$

onde $k = \min\{\alpha, \beta\}$, a cota de Landau-Mignotte para os coeficientes do M.D.C. de f e g, e seja

$$M_2 = \frac{3^{3/4}}{2\sqrt{\pi}} \min\left\{ \frac{3^{\alpha/2}}{\sqrt{\alpha}}[f]_2, \frac{3^{\beta/2}}{\sqrt{\beta}}[g]_2 \right\}$$

a nova cota superior para os coeficientes.

Comparando-se as quantidades envolvidas na determinação de M_1 e M_2, observa-se que:

- $\frac{3^{3/4}}{2\sqrt{\pi}} \simeq 0.643 < 1 \leq MDC(a_\alpha, b_\beta)$. Logo, $\frac{3^{3/4}}{2\sqrt{\pi}} < MDC(a_\alpha, b_\beta)$;
- $[f]_2 \leq \|f\|$ e $[g]_2 \leq \|g\|$, sendo que as desigualdades são estritas se os polinômios tiverem algum coeficiente intermediário não nulo. Ou seja,

$$(\exists i,\ 1 \leq i \leq \alpha - 1,\ \text{tal que } a_i \neq 0) \ \rightarrow\ [f]_2 < \|f\|$$

e

$$(\exists i,\ 1 \leq i \leq \beta - 1,\ \text{tal que } b_i \neq 0) \ \rightarrow\ [g]_2 < \|g\|;$$

- Se os coeficientes líderes de f e g forem pequenos é grande a possibilidade de que tenhamos $\frac{3^{\alpha/2}}{\sqrt{\alpha}} < \frac{2^k}{|a_\alpha|}$ e $\frac{3^{\beta/2}}{\sqrt{\beta}} < \frac{2^k}{|b_\beta|}$ e, conseqüentemente, $M_2 < M_1$, como ilustraremos no corolário 4.3.2.

Proposição 4.3.1 *Se* $|a_\alpha| = |b_\beta| = 1$ *e* $1 < \alpha \leq \beta < \alpha + 2$, *então*

$$\frac{3^{\alpha/2}}{\sqrt{\alpha}} < \frac{2^k}{|a_\alpha|} \quad e \quad \frac{3^{\beta/2}}{\sqrt{\beta}} < \frac{2^k}{|b_\beta|}, \quad \textit{onde } k = \min\{\alpha, \beta\}.$$

Demonstração: Por hipótese temos que α é maior que 1, logo $\frac{3^\alpha}{\alpha} < 3^\alpha < 4^\alpha$. Conseqüentemente,

$$\frac{3^{\alpha/2}}{\sqrt{\alpha}} = \sqrt{\frac{3^\alpha}{\alpha}} < \sqrt{4^\alpha} = 2^\alpha = \frac{2^k}{|a_\alpha|}.$$

Além disso, por hipótese temos também que $\beta = \alpha$ ou $\beta = \alpha + 1$. Portanto,

$$\frac{3^{\beta/2}}{\sqrt{\beta}} = \frac{3^{\alpha/2}}{\sqrt{\alpha}} < 2^{\alpha} = \frac{2^k}{|b_\beta|}$$

ou

$$\frac{3^{\beta/2}}{\sqrt{\beta}} = \frac{3^{(\alpha+1)/2}}{\sqrt{\alpha+1}} \leq \frac{3^{(\alpha+1)/2}}{\sqrt{3}} = 3^{\alpha/2} < 4^{\alpha/2} = 2^{\alpha} = \frac{2^k}{|b_\beta|}. \quad \square$$

Corolário 4.3.2 *Sejam f e g polinômios mônicos cujos graus são maiores que 1 e diferem por no máximo uma unidade. Então, a nova cota superior para os coeficientes de f e g é menor que a cota de Landau-Mignotte.*

Demonstração: Segue imediatamente da proposição 4.3.1 □

É importante observar que as condições do corolário anterior não são muito restritivas, pois é muito freqüente que tenhamos polinômios mônicos e de graus similares ao calcularmos o Máximo Divisor Comum.

Além disso, mesmo que os polinômios f e g tenham graus muito distintos, isto é, que a diferença entre os seus graus seja grande, pelo lema 2.3.2 temos que $MDC(f,g) = MDC(g,r)$, onde r é o resto obtido pela "pseudo-divisão" de f e g. Conseqüentemente, podemos aplicar um dos algoritmos modulares para os polinômios g e r, cujos graus são similares, utilizando a nova cota superior.

Também é importante notar que as hipóteses do corolário 4.3.2 são condições suficientes mas não necessárias para que a nova cota superior seja menor que a cota de Landau-Mignotte. Mesmo trabalhando com polinômios não mônicos ou com graus que diferem em mais de uma unidade obtivemos $M_2 < M_1$ em vários casos, como ilustraremos a seguir.

4.3.1 Exemplos

Consideraremos os seguintes polinômios:

$$
\begin{aligned}
f_1(x) &= 45x^4 - 78x^3 + 165x^2 + 64x - 26 \\
f_2(x) &= x^5 + 3x^4 + 2x^3 - 2x^2 - 3x - 1 \\
f_3(x) &= 21525x^5 + 28050x^4 - 20401x^3 - 16122x^2 + 11254x - 1962 \\
f_4(x) &= x^6 + x^5 + 6x^4 - 5x^3 + 2x^2 + 2 \\
f_5(x) &= 904050x^7 + 1479450x^6 - 2336817x^5 - 3403088x^4 + 2021847x^3 \\
&\quad +1477766x^2 - 1006566x + 170694 \\
f_6(x) &= 3x^6 + 5x^4 - 4x^2 - 9x + 21 \\
f_7(x) &= x^6 + 3x^5 + 3x^4 + 2x^3 + 3x^2 + 3x + 1 \\
f_8(x) &= 3x^6 + 5x^4 + 9x^2 + 4x + 8 \\
f_9(x) &= x^8 + x^6 - 3x^4 - 3x^3 + x^2 + 2x - 5 \\
f_{10}(x) &= x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5 \\
f_{11}(x) &= x^8 + x^6 + 10x^4 + 10x^3 + 8x^2 + 2x + 8 \\
f_{12}(x) &= x^8 + 8x^7 + 21x^6 + 21x^5 + 42x^4 + 13x^3 + 12x^2 - 14x + 12 \\
f_{13}(x) &= 9x^9 + 3x^8 + 14x^7 - 16x^6 + 5x^5 - 11x^4 - 3x^3 - 2x^2 - 13x - 13 \\
f_{14}(x) &= x^{15} + 30x^{14} + 5x^{13} + 2x^{12} + 5x + 2 \\
f_{15}(x) &= x^{18} + 9x^{17} + 45x^{16} + 126x^{15} + 189x^{14} + 27x^{13} - 540x^{12} - 1215x^{11} \\
&\quad +1377x^{10} + 15444x^9 + 46899x^8 + 90153x^7 + 133893x^6 + 125388x^5 \\
&\quad +29160x^4 - 32076x^3 + 26244x^2 - 8748x + 2916 \\
f_{16}(x) &= x^{33} + 7x^{32} + 27x^{31} + 76x^{30} + 174x^{29} + 343x^{28} + 603x^{27} + 968x^{26} \\
&\quad +1442x^{25} + 2016x^{24} + 2667x^{23} + 3359x^{22} + 4046x^{21} + 4677x^{20} \\
&\quad +5202x^{19} + 5578x^{18} + 5774x^{17} + 5774x^{16} + 5578x^{15} + 5202x^{14} \\
&\quad +4677x^{13} + 4046x^{12} + 3359x^{11} + 2667x^{10} + 2016x^9 + 1442x^8 \\
&\quad +968x^7 + 603x^6 + 343x^5 + 174x^4 + 76x^3 + 27x^2 + 7x + 1
\end{aligned}
$$

$$
\begin{aligned}
f_{17}(x) &= x^{41} - x^{40} - x^{39} + x^{36} + x^{35} - x^{33} + x^{32} - x^{30} - x^{27} + x^{23} + x^{22} - x^{21} \\
&\quad -x^{20} + x^{19} + x^{18} - x^{14} - x^{11} + x^9 - x^8 + x^6 + x^5 - x^2 - x + 1 \\
a_1(x) &= 78192x^{10} + 20480x^9 + 58368x^8 - 161792x^7 + 198656x^6 + 199680x^5 \\
&\quad -414848x^4 - 4160x^3 + 171816x^2 - 48556x + 469 \\
a_2(x) &= 8192x^{10} + 12288x^9 + 66560x^8 - 22528x^7 - 138240x^6 + 572928x^5 \\
&\quad -90496x^4 - 356032x^3 + 113032x^2 + 23420x - 8179 \\
a_3(x) &= 4096x^{10} + 8192x^9 + 1600x^8 - 20608x^7 + 20032x^6 + 87360x^5 \\
&\quad -105904x^4 + 18544x^3 + 11888x^2 - 3416x + 1 \\
a_4(x) &= 4096x^{10} + 8192x^9 - 3008x^8 - 30848x^7 + 21056x^6 + 146496x^5 \\
&\quad -221360x^4 + 1232x^3 + 144464x^2 - 78488x + 11993 \\
f_{40}(x) &= a_1 \cdot a_2 \cdot a_3 \cdot a_4 \\
g_1(x) &= -100x + 1 \\
g_2(x) &= 3x^2 + 1 \\
g_3(x) &= 10^{10}x^2 + 1 \\
g_4(x) &= -6x^3 + 2 \\
g_5(x) &= 5x^3 + 2 \\
g_6(x) &= -341x^{13} + 80x^{11} - 4x^7 + 3x^2 \\
g_7(x) &= -700x^{36} + 300x^{20} + 1 \\
g_8(x) &= -x^{100} + 1 \\
g_9(x) &= -x^{101} + 1 \\
g_{10}(x) &= x^{200} + 1
\end{aligned}
$$

Os polinômios f_1, f_3, f_5 e f_{15} são exemplos de [3], f_4 é um exemplo de [2], f_6, f_8, f_{10} e f_{11} são exemplos de [11], f_2, f_7 e f_9 são exemplos de [6], f_{12} e f_{14} são exemplos de [14] e f_{13}, f_{16} e f_{17} de [19]. O polinômio f_{40} é o *SIGSAM Problem #7*, que pode ser visto em [21].

Na tabela 4.1 são apresentados polinômios para os quais nossa cota é vantajosa sobre a cota de Landau-Mignotte, o que ocorre na maioria das vezes.

f	g	Cota de Landau-Mignotte	Nova Cota Superior	$MDC(f,g)$
g_8	g_9	1.79273×10^{30}	6.52851×10^{22}	$x-1$
g_8	g_{10}	1.79273×10^{30}	6.52851×10^{22}	1
f_{16}	f_{17}	4.20819×10^{10}	3.18324×10^{7}	f_{16}
a_1	f_{40}	5.78762×10^{8}	4.5577×10^{6}	a_1
a_2	a_4	3.22397×10^{8}	1.96157×10^{6}	1
a_3	a_4	1.45742×10^{8}	540979	1
f_{12}	f_{14}	7927.74	281.99	1
f_{12}	f_{14}	7927.74	281.99	1
f_{11}	f_{15}	4678.57	155.208	1
f_1	f_5	3204.24	286.217	1
f_{13}	f_{14}	1833.73	502.881	1
f_{13}	f_{17}	1833.73	502.881	1
f_{12}	f_{17}	1254.14	281.99	1
f_6	f_{10}	510.219	99.3579	1
f_6	f_9	452.548	95.441	1
f_4	f_5	370.305	21.3622	1
f_8	f_{11}	297.904	64.471	1
f_2	f_7	169.328	11.3408	$(x+1)^4$
f_{12}	g_{10}	362.039	281.99	1

Tabela 4.1: Comparação entre as cotas: $M_1 > M_2$

Na tabela 4.2, na próxima página, são apresentados polinômios em que a cota de Landau-Mignotte é menor que a nova cota 4.8. Note que para que isto aconteça, geralmente é necessário que pelo menos uma das três condições seja satisfeita:

1) O coeficiente líder de um dos polinômios é muito maior que seu grau;

2) A diferença entre os graus dos polinômios é grande;

3) Os coeficientes intermediários dos polinômios são quase todos nulos.

f	g	Cota de Landau-Mignotte	Nova Cota Superior	$MDC(f,g)$
a_1	a_4	118429	1.96157×10^6	1
f_3	f_{16}	67.4214	120077	1
g_6	g_7	8415.28	76817.5	1
f_3	f_{12}	67.4214	281.99	1
g_1	g_8	2.0001	111.383	1
g_4	g_5	8.43274	10.3886	1
g_2	g_3	4	4.31362	1

Tabela 4.2: Comparação entre as cotas: $M_1 < M_2$

Cada um desses três fatores é "ruim" para a nova cota, isto é, estas condições são favoráveis para que a cota de Landau-Mignotte seja menor. De fato, os polinômios $g_1, ..., g_{10}$ foram criados com esse propósito. Entretanto, 1), 2) e 3) não são condições suficientes para que tal aconteça, pois mesmo que as três situações ocorram simultaneamente, a nova cota pode ser menor que a de Landau-Mignotte, como mostra o exemplo a seguir.

Exemplo 4.1 Sejam

$$\begin{aligned} f(x) &= x^3 + 1 \quad e \\ g(x) &= 10^{100}x^{100} + 1 \quad \in \mathbb{Z}[x]. \end{aligned}$$

A cota de Landau-Mignotte para o $MDC(f,g)$ é 8, ao passo que a nova cota é 2.72818.

(Os resultados apresentados nesta seção foram obtidos com a implementação das cotas no MATHEMATICA).

5 CONCLUSÃO

Nosso principal objetivo no desenvolvimento desta dissertação era a apresentação de algoritmos eficientes para o cálculo do Máximo Divisor Comum de polinômios a uma variável. Apresentamos duas classes de algoritmos: os Euclidianos e os Modulares.

Entre os Algoritmos Euclidianos, o Sub-Resultante (Algoritmo 2.6) é o que apresenta menor custo por requerer um número menor de cálculos de M.D.C.s de coeficientes além de evitar o crescimento exponencial das expressões intermediárias.

Os Algoritmos Modulares, conforme observamos no capítulo 3, são mais eficientes que os Euclidianos. Para que estes algoritmos funcionem mais rapidamente é importante que seja conhecida uma cota superior para os coeficientes do M.D.C. que não esteja muito distante dos coeficientes verdadeiros.

Uma das contribuições deste trabalho foi a apresentação e demonstração detalhadas dos resultados necessários para a obtenção da cota superior de Landau-Mignotte.

A principal contribuição desta dissertação foi a obtenção de uma nova cota superior que é menor que a de Landau-Mignotte para grande parte dos polinômios. Inclusive obtivemos uma classe de polinômios para os quais a nova cota é garantidamente menor que a anterior (corolário 4.3.2).

Assim, para o cálculo do M.D.C. de polinômios a uma variável sugerimos a aplicação do Algoritmo 3.2 com uma modificação no 1º passo: se os polinômios satisfazem as hipóteses do corolário 4.3.2, utiliza-se a nova cota; caso contrário, escolhe-se a menor das duas cotas superiores. Esta versão do Algoritmo 3.2 será apresentada na seção 5.1.

Uma extensão do estudo de algoritmos para o M.D.C. de polinômios a uma variável, que desenvolvemos nesta dissertação, é o estudo de algoritmos para o M.D.C. de polinômios a várias variáveis. Podemos obter um algoritmo semelhante ao Algoritmo 3.2 para o cálculo do M.D.C. de dois polinômios a n variáveis. Para mais detalhes veja [6].

5.1 Algoritmo Final

Apresentaremos a seguir o algoritmo que acreditamos ter melhor desempenho que todos os algoritmos apresentados durante esta dissertação. Este algoritmo é baseado no Algoritmo 3.2 e na utilização da nova cota superior nos freqüentes casos em que ela é menor que a cota de Landau-Mignotte.

Algoritmo 5.1 *Dados dois polinômios não nulos f e g com coeficientes inteiros, este algoritmo calcula o M.D.C. de f e g utilizando redução módulo números primos pequenos e o Teorema Chinês dos Restos, escolhendo no 1º passo a menor entre as duas cotas superiores para os coeficientes.*

1. **Se** *f e g são mônicos, de graus maiores que 1 e $|\partial f - \partial g| < 2$,*
   então *$M \leftarrow$ nova cota superior para os coeficientes,*
   senão *$M \leftarrow \min\{$nova cota superior, cota de Landau-Mignotte$\}$;*
2. *$N \leftarrow MDC$(coef. líder de f, coef. líder de g);*
3. *$p \leftarrow$ número primo que não divide N;*
4. *$\bar{h} \leftarrow MDC(f_p, g_p)$;*
5. **Se** *o grau de $\bar{h}$ for zero,*
   então
   5.1. *$h \leftarrow 1$;*
   5.2. **vá para** *11;*
6. *prodprim $\leftarrow p$;*
7. *result $\leftarrow \bar{h}$;*

8. Enquanto $prodprim \leq 2M$

   faça

   8.1. $p \leftarrow$ *número primo que não divide* N;

   8.2. $\bar{h} \leftarrow MDC(f_p, g_p)$;

   8.3. Se *o grau de* $\bar{h}$ *for menor que o grau de result,*

   então vá para *5;*

   8.4. Se *o grau de* $\bar{h}$ *for igual ao grau de result,*

   então

   8.4.1. *result* $\leftarrow$ *Teorema Chinês dos Restos aplicado a cada coeficiente dos polinômios result* (mod *prodprim*) *e* $\bar{h}$ (mod p);

   8.4.2. $prodprim \leftarrow prodprim \times p$;

9. Se *result divide* f *e divide* g,

   então

   9.1. $h \leftarrow result$;

   9.2. vá para *11;*

10. Vá para *3;*

11. *O algoritmo termina com h como o M.D.C. procurado.*

BIBLIOGRAFIA

[1] Beauzamy, B., Bombieri, E., Enflo, P. e Montgomery, H., "Products of Polynomials in Many Variables", Journal of Number Theory, vol. 36, n. 2, 219-245 (1990).

[2] Beauzamy, B., "Products of Polynomials and a Priori Estimates for Coefficients in Polynomial Decompositions: A Sharp Result", Journal of Symbolic Computation, vol. 13, 463-472 (1992).

[3] Beauzamy, B., Trevisan, V. e Wang, P. S., "Polynomial Factorization: Sharp Bounds, Efficient Algorithms", Journal of Symbolic Computation, vol. 15, n. 4, 393-413 (1993).

[4] Bellandi Filho, J., *Funções Especiais*, Editora Papirus, Campinas, 1985.

[5] Brown, W. S., "On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors", Journal of ACM, vol. 18, 478-504 (1971)

[6] Davenport, J. H., Siret Y. e Tournier, E., *Computer Algebra: Systems and Algorithms for Algebraic Computation*, Academic Press, 1988.

[7] Grahan, R. L., Knuth, D. E. e Patashnik, O., *Concrete Mathematics: A Foundation for Computer Science*, Addison-Wesley, 1989.

[8] Garcia, A. e Lequain, Y., *Álgebra: um curso de introdução* , IMPA, 1988.

[9] Herstein, I. N., *Tópicos de Álgebra*, Editora Polígono, São Paulo, 1970.

[10] Jones, A., *Notas de Álgebra*, IME-USP, 1979.

[11] Knuth, D. E., *The Art of Computer Programming*, vol. 2, Addison-Wesley, 1981.

[12] Lauer, M., "Computing by Homomorphic Images", *Computer Algebra-Symbolic and Algebraic Computation*, Computing Supplementum 4, Springer-Verlag, 139-168, 1982.

[13] Lipson, J. D., *Elements of Algebra and Algebraic Computing*, Addison-Wesley, 1981.

[14] Mignotte, M., "An Inequality about Factors of Polynomials", Mathematics of Computation, vol. 28, n. 128, 1153-1157 (1974).

[15] Mignotte, M., "Some Useful Bounds", *Computer Algebra-Symbolic and Algebraic Computation*, Computing Supplementum 4, Springer-Verlag, 259-263, 1982.

[16] Mignotte, M., "An Inequality about Irreducible Factors of Integer Polynomials", Journal of Number Theory, vol. 30, n. 2, 156-166 (1988).

[17] Mignotte, M., *Mathematics for Computer Algebra*, Springer-Verlag, 1992.

[18] Moses, J. e Yun, D. Y. Y., "The EZ-GCD Algorithm", Proceedings of ACM Conference 28, 159-166 (1973).

[19] Trevisan, V., *Univariate Polynomial Factorization*, PhD Dissertation, Kent State University, 1992.

[20] Trevisan, V., *Computação Algébrica e Simbólica*, SBMAC, 1992.

[21] Wang, P. S., "Parallel Univariate Polynomial Factorization on Shared-Memory Multiprocessors", Proceedings of the ISSAC'90, 145-151 (1990).

[22] Wolfram, S., *Mathematica: A System for Doing Mathematics by Computer*, Addison-Wesley, 1988.