Universidade Federal Rural de Pernambuco
Departamento de Matemática
Mestrado Profissional em Matemática

Fatoração no Ensino Médio

PEDRO JOSÉ ALVINO PEREIRA DOS SANTOS

Orientador

Bárbara Costa da Silva

Recife-PE

Agosto de 2014

Universidade Federal Rural de Pernambuco
Departamento de Matemática
Mestrado Profissional em Matemática

Fatoração no Ensino Médio

Um algoritmo matricial para o Crivo de Erathóstenes

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do Título de Mestre em Matemática.

PEDRO JOSÉ ALVINO PEREIRA DOS SANTOS

Recife-PE

Agosto de 2014

Banca examinadora:

Profa. Dra. Bárbara Costa da Silva (Orientador)

Prof. Dr. Thiago Dias Oliveira Silva

Prof. Dr. Rodrigo Gondin Neves

Prof. Dr. Eudes Naziazeno Galvão

A Francisco e Rodrigo.

Canção do Tamoio

Gonçalves Dias

I

Não chores, meu filho;
Não chores, que a vida
É luta renhida:
Viver é lutar.
A vida é combate,
Que os fracos abate,
Que os fortes, os bravos
Só pode exaltar.

II

Um dia vivemos!
E o homem que é forte
Não teme da morte;
Só teme fugir;
No arco que entesa
Tem certa uma presa,
Quer seja tapuia,
Condor ou tapir.

III

O forte, o cobarde
Seus feitos inveja
De o ver na peleja
Garboso e feroz;
E os tímidos velhos
Nos graves concelhos,
Curvadas as frontes,
Escutam-lhe a voz!

IV

Domina, se vive;
Se morre, descansa
Dos seus na lembrança,
Na voz do porvir.
Não cures da vida!
Sê bravo, sê forte!
Não fujas da morte,
Que a morte há de vir!

V

E pois que és meu filho,
Meus brios reveste;
Tamoio nasceste,
Valente serás.
Sê duro guerreiro,
Robusto, fragueiro,
Brasão dos tamoios
Na guerra e na paz.

VI

Teu grito de guerra
Retumbe aos ouvidos
D'imigos transidos
Por vil comoção;
E tremam d'ouvi-lo
Pior que o sibilo
Das setas ligeiras,
Pior que o trovão.

VII

E a mãe nessas tabas,
Querendo calados
Os filhos criados
Na lei do terror;
Teu nome lhes diga,
Que a gente inimiga
Talvez não escute
Sem pranto, sem dor!

VIII

Porém se a fortuna,
Traindo teus passos,
Te arroja nos laços
Do inimigo falaz!
Na última hora
Teus feitos memora,
Tranqüilo nos gestos,
Impávido, audaz.

IX

E cai como o tronco
Do raio tocado,
Partido, rojado
Por larga extensão;
Assim morre o forte!
No passo da morte
Triunfa, conquista
Mais alto brasão.

X

As armas ensaia,
Penetra na vida:
Pesada ou querida,
Viver é lutar.
Se o duro combate
Os fracos abate,
Aos fortes, aos bravos,
Só pode exaltar..

Agradecer é quase sempre tarefa que parece mais fácil de ser feita antes de ser iniciada. Parte de mim se sente tentada a declinar de tal faina. De outra feita, minha gratidão é imensa, assim como o desejo visceral de externá-la. Mas, se, por um lado, o elogio generalizado é inverdade que insulta o mérito, por outro, não é bom deixar de externar o justo agradecimento; nem que seja por esquecer!

Se tentasse agradecer formalmente, como manda o figurino; leria antes os agradecimentos de alguma dissertação já publicada, faria as alterações nominais convenientes e, após imperceptíveis ajustes aqui ou acolá, apresentaria ao leitor essa insípida peça a ser lida pela diagonal, quando não de todo ignorada. Tenho medo da mesmice!

Eu não creio que me esqueceria de expor minha gratidão a Bárbara Costa, minha bondosa orientadora com sua **quase** *infindável paciência e compreensão. Nem tampouco olvidaria a SBM, ou ao IMPA. Temo porém a idéia de esquecer de enfaticamente destacar Thiago DK, nosso bom professor de Álgebra Linear e companheiro de conversas sobre coisas afins (ou não). E se, no corre-corre do processo de confecção destas linhas, a lembrança de algum outro professor ou colega me escapasse?*

Dessa forma, para não esquecer de ninguém, nem tampouco exaltar algo imerecido; desejo, humilde e fervorosamente, agradecer com sinceridade a Deus, Yaweh Kiklos, clemente e misericordioso; por Cícero e Anita, por Francisco e Rodrigo, pelos estudantes que me ensinaram a amar essa profissão honrada, pela Matemática e por TUDO.

Muito obrigado, muito obrigado, muito obrigado.

Em tempo:

Obrigado Tetsuo, obrigado Sérgio, obrigado Fábio, obrigado todo mundo... Muito obrigado!

RESUMO

Alguns dos problemas mais interessantes e atrativos da Matemática do Ensino Médio remetem o estudante direta ou indiretamente ao tema da fatoração. Ocorre, no entanto, que as técnicas de fatoração disponíveis no Ensino Médio quase que invariavelmente são reduzidas a um único algoritmo, com – no máximo – uma ou outra variação superficial. Tal algoritmo – em tempo: testar sistematicamente as possíveis divisibilidades do número em questão pelos números primos menores que sua raiz quadrada; embora de fácil explicação, torna-se lento e enfadonho para números gerais com mais de três dígitos, e quase inútil para valores muito maiores.

Nesse trabalho, buscaremos investigar o problema da fatoração através do Crivo de Erathóstenes e apresentaremos uma abordagem matricial para o mesmo. Com isso, sem nos afastarmos dos conceitos nem do nível do Ensino Médio, mostramos uma abordagem alternativa e algoritmicamente mais simples e eficiente para o problema da fatoração.

Palavras-chave: *Fatoração, crivo de Erathóstenes, primalidade.*

Abstract

Some of the most interesting and appealing problems of High School Mathematics lead the students directly or indirectly to the subject of factorization . It occurs, however, that the techniques of factorization almost invariably reduced to a single algorithm, with no more than one or another superficial variation. Such algorithm - in time: to systematically test possible divisions of the number in question by prime numbers which are smaller than its square root; although this technique may be easy to be explained, it becomes slow and tiresome for general numbers with more than three digits, and almost useless for much larger values.

This study investigated the problem of factorization by the Sieve of Erathostenes and presented a matrix approach for it. Therewith, to conduct this study it was taken into consideration the students school level and the theories. It is presented an alternative approach, algorithmically simpler and more efficient to the problem of factorization.

Key-words : Factorization, Sieve of Eratosthenes, prime numbers

Lista de Tabelas

Sumário

Introdução

0.1 Uma opção didática:

Nosso objetivo é apresentar uma sugestão didática para a investigação do tema da Fatoração no Ensino Básico; que trás – por outro enfoque – o da decisão sobre a Primalidade de um Natural, também sob a ótica do Ensino Médio.

Para tanto, por uma questão de coerência, visto almejar-se que um estudante do Ensino Médio possa transitar sem muitos empecilhos por essas páginas; buscamos adotar uma linguagem e formalismo apropriados para esse público.

Com essa meta em foco, tentamos evitar – sempre que pudemos; ou conseguimos – as demonstrações e abordagens que extrapolassem a área de abrangência conceitual do Ensino Médio. É ululante que tal faina nem sempre é simples, ou mesmo factível. Algumas vezes, o distanciamento desse objetivo primário se deve as peculiaridades de um ou outro tema, que impõem o imprescindível formalismo, que traz verdade, mérito e confiança ao que se diz, sem negligenciar é claro a didática, os exemplos e argumentações empíricas, que dão sentido ao dito. Nas outras situações do texto, para as quais o formalismo e o rigor parecem ser um tanto exagerados ou fora de propósito: è culpa do autor mesmo!

No Capitulo I o problema da fatoração é abordado bem como são exploradas algumas técnicas para resolvê-lo.

No No Capitulo II investigamos a construção de alguns dos algoritmos clássicos de fatoração, exibindo o Crivo de Erathóstenes com mais ênfase.

No Capitulo III reapresentamos o Crivo sob uma ótica matricial, construindo o conceito

de símbolo e suas implicações.

No Capítulo IV finalizamos investigando a estrutura algébrica das matrizes A_n, S_n e C_n; usando-as para resolver problemas de fatoração. Nessa etapa, certo formalismo além do Ensino Médio se fará imprescindível para a generalização dos algoritmos.

Em tempo: Os números que se pretendem usar como exemplos não ultrapassam os cinco dígitos decimais, posto que, em situações práticas de sala de aula, quase nunca se encontra algo palpável que justifique a extrapolação dessa faixa.

Capítulo 1

Fatoração no Ensino Fundamental

1.1 O Conceito de Fatoração no Ensino Básico:

É prática comum de boa parte dos professores de matemática dos Primeiros Ciclos do Ensino Fundamental aproximar-se do tema de divisibilidade via exemplos específicos e "generalizações" intuitivas. Assim, por essa abordagem, afirma-se que

2x3 = 6 então 2 e 3 são divisores de 6

Tal procedimento – normalmente explicado por uma alegada incompetência dos estudantes com o formalismo matemático, havendo inclusive aqueles que defendem sua supressão nessa etapa – quando isolado de outras abordagens paralelas, deixa de lado importantes conclusões sobre o tema que poderiam servir de base para as investigações futuras nos campos da Fatoração Inteira bem como na construção de Algoritmos de Divisibilidade.

Adiante, frequentemente no segundo quartil do 6º ano, os estudantes revisitam a Divisibilidade, ainda com pouco ou mesmo nenhum formalismo, introduzindo ali os temas de Mínimo Múltiplo Comum e Máximo Divisor Comum. Esses importantíssimos conceitos infelizmente servem quase que somente para explicar quando muito um algoritmo para a adição de frações heterogêneas.

Um pouco depois, mais especificamente em meados do 8º ano, o tema retorna em sua versão meramente algébrica; deixando os estudantes – salvo em raras e excepcionalmente notáveis situações didáticas – com a chata tarefa de tentar memorizar os algoritmos que se lhes impõem pela goela abaixo.

Por outro lado, em que pese – do ponto de vista didático – a natural e às vezes imperiosa necessidade de abordar inicialmente um conceito a partir de situações e/ou problemas relacionados a noções já conhecidas ou em processo de construção por parte do estudante, sem dar demasiada ênfase às fórmulas e ao formalismo potencialmente associados ao tema em estudo; há que se considerar a existência de alguns exageros ao se tomar essa postura como metodologia si ne qua non para a investigação generalizada de temas matemáticos. Às vezes simplesmente não há condições de contextualizar um tema a priori. Outras vezes, a busca por essa contextualização é tão laboriosa quanto a própria exploração formal do conceito. No bojo dessa discussão – Formalização X Contextualização – o Problema da Fatoração Natural no Ensino Básico se mostra um exemplo emblemático, pois, sendo comum que os conceitos de

multiplicidade natural sejam abordados nessa fase quase que exclusivamente para a obtenção de um algoritmo para a adição de frações heterogêneas; dá-se também certo direcionamento algorítmico para a execução de fatorações específicas com tão pouco espaço para generalizações que é realmente comum vermos a maioria de nossos estudantes do ensino médio se utilizando de procedimentos aritméticos tão lentos que por vezes chegam a tirar a atenção do problema maior que é investigado. Citando uma particular, mas infelizmente pouco rara situação: quando um estudante mediano se propõe a fatorar, por exemplo, N = 2700, é quase certo encontrarmos seus cálculos – mesmo no Ensino Médio – mais ou menos como abaixo

2700	*2*
1350	*2*
675	*3*
225	*3*
75	*3*
25	*5*
5	*5*
	5

Daí é dito que $2700 = 2^2.3^3.5^2$, *e se vai adiante, quase sempre sem ressaltar que* $2700 = 100.27 = (2.5)^2.3^3 = 2^2.3^3.5^2$. *Isso, por si só, já seria horrível; mas, o pior fica para quando – em algumas das vezes que se chama atenção para o segundo processo – se percebe que parte enorme dos estudantes se põem a questionar sobre a validade desse método, havendo inclusive aqueles que, não obstante reconheçam a verdade do resultado, categorizem esse procedimento como um algoritmo alternativo, um "bizú"; acintosamente pondo de lado as propriedades comutativa e associativa da multiplicação nos Naturais.*

É verdade que essa situação quase sempre pode ser resolvida de maneira simples com alguns argumentos aritméticos e outro tanto de exercícios sugestivos. O núcleo dessa discussão é outro: Qual a dose certa de formalismo a aplicar na investigação matemática no ensino básico?

1.2 A Tábua de Testes para os Divisores Naturais de um Número Natural:

Logo após a abordagem inicial dos temas de multiplicação e divisão, normalmente nos últimos ciclos do Ensino Fundamental, surgem os problemas envolvendo implicitamente o conceito empírico de divisibilidade. Uma aproximação interessante se dá ao explorar problemas de contagem, tais como: De quantas maneiras se podem formar equipes numa sala com 16 alunos? Com 20? E com 24?

O Algoritmo da Divisão de Euclides nos mostra que cada maneira de formar uma equipe está relacionada com o fato do resto da divisão do número de alunos pela possível quantidade de alunos por equipe ser sempre 0. A quantidade de vezes em que tal fenômeno ocorre será a quantidade de maneiras de se formar equipes. Explora-se e se enfatiza aqui que, obviamente, em cada caso, junto com a quantidade de alunos por equipe, tem-se também a quantidade de equipes a se formar na sala!

A partir dessas situações-problema pode ser perfeitamente apresentada, não sem alguma observação e reflexão sobre outros casos particulares, a definição que segue

Definição 1.1. *Considere $a, b \in \mathbb{N}$. Caso exista $n \in \mathbb{N}$, de modo que $a \cdot n = b$, dizemos que*

1. *b é um múltiplo natural de a, e*
2. *a é divisor natural de b, ou a divide b, ou, simbolicamente $a \mid b$*

Em contrapartida, dados $a, b \in \mathbb{N}$, caso não exista $n \in \mathbb{N}$, de modo que $a \cdot n = b$, dizemos que $a \nmid b$, i.e. a não divide b.

Para simplificar, haja vista que esses conceitos são aplicados apenas em naturais, dizemos somente múltiplo e divisor; e omitimos, subentendendo-o, o adjetivo natural.

Voltando ao problema inicial, vê-se que contar quantas equipes podem ser feitas equivale também a contar quantos são os divisores do número D, de alunos da sala. Para tanto, e para a investigação dos conceitos vindouros, construiremos dois conjuntos úteis. A saber

Definição 1.2. *Considerando $k \in \mathbb{N}$,denotaremos*

1. $d(k) = \{d \in \mathbb{N}; d \mid k\}$, *como o conjunto dos divisores de k, e*

2. $d'(k) = d(k) \setminus \{1, k\}$, *como o conjunto dos divisores não triviais de k*

Tendo em mente o Algoritmo de Euclides, e buscando simplesmente organizar as tentativas de obter d(D), construímos uma Tábua de Testes para os seus possíveis divisores; onde são explicitados, para cada possível d, divisor de D, seus respectivos quocientes (q) e restos (r). Assim, por exemplo, para obter os divisores de $D = 20$, atentando que nessa etapa sabemos apenas que $d \leq D$, temos, em princípio,

Tabela 1.1: Tábua dos possíveis divisores de 20

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
q																				
r																				

Calculando diretamente q e r, para cada d, obtemos

Tabela 1.2: Tábua de teste para os divisores de 20

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
q	20	10	6	4	4	3	2	2	2	2	1	1	1	1	1	1	1	1	1	1
r	0	0	2	4	0	2	6	4	2	0	9	8	7	6	5	4	3	2	1	0

De onde observamos imediatamente os divisores de $D = 20$, sempre que $r = 0$. Daí: $d(20) = \{1, 2, 4, 5, 10, 20\}$.

Mas, com um pouco mais de atenção, percebemos ainda outras coisas.

Alguns anos de experiência no ensino de Matemática ensinaram a esse autor que, dispondo de um bom planejamento, com paciência, persistência e confiança, depois de mais alguns exemplos e exercícios e, se deixados à vontade para argumentar e testar suas hipóteses, muitos estudantes chegam à belíssimas reflexões sobre a Matemática; uma dessas é a conclusão de que essa Tábua de Testes, depois de algum burilamento, fica, de fato, muitíssimo reduzida.

Senão, vejamos:

Quase sempre os estudantes percebem que, quando $d = 1$, tem-se imediatamente que $r = 0$ e $q = 20$. Mas, isso é dizer que $20 = 1.20$ – um fato já conhecido e esperado; de fato, como $D = 1.D$, dizemos que 1 e D são os Divisores Triviais de D. Isso contudo significa que 20 também é um divisor de 20, tornando assim desnecessária, por redundância, a sua inclusão na Tábua, na linha dos divisores; ou seja: buscamos d'(20). Além disso, como não existe nenhum divisor entre 1 e 2, também não existirá um divisor entre 10 e 20; o que nos permite exclui-los também da Tábua. Caso análogo se dá entre 4 e 5.

Poderíamos chegar a dizer que, por força desses argumentos, está tabela poderia ser reduzida pela metade. Normalmente, nesse ponto da aula, já há alguns alunos que propõem exatamente isso. Ao final dessa mesma aula, com mais alguns argumentos e exercícios, os estudantes chegam a construção de uma nova Tábua, que terá bem menos colunas que essa suposta metade da original.

Em verdade, basta testar somente quando $d \leq q$; e, no caso extremo $d = q$, temos simplesmente $D = d^2$. Essas observações, colocadas sob os rigores da organização algébrica, permitem enunciar – e demonstrar – nossas próximas proposições:

Proposição 1.1. *Seja $N \in \mathbb{N}$*

Se $\exists\, d_1, d_2 \in \mathbb{N}; N = d_1.d_2$,com $d_1 \leq d_2$,

então $d_1 \leq \sqrt{N} \leq d_2$, ocorrendo a igualdade quando $d_1 = d_2$.

Demonstração: *Considerando que a raiz quadrada é uma função crescente, segue diretamente da observação de que $d_1.d_1 \leq d_1.d_2 \leq d_2.d_2$* ■

Proposição 1.2. *Seja $N \in \mathbb{N}$*

Se $\exists\, d_1, d_2, q_1, q_2 \in \mathbb{N}; N = d_1.q_1 = d_2.q_2$,com $d_1 \leq d_2$,

então $\exists\, d \in d(N); d_1 \leq d \leq d_2 \Longleftrightarrow \exists\, q \in d(N); q_2 \leq q \leq q_1$.

Demonstração: *Observe inicialmente que*

$$d \in d(N) \Rightarrow \exists q \in \mathbb{N}; N = d.q \Rightarrow q \in d(N)$$

Por outro lado, o conceito de ordem nos naturais diz também que

$$d_1 \leq d \leq d_2 \Leftrightarrow \exists k_1, k_2 \in \mathbb{N}; d = d_1 + k_1 = d_2 - k_2$$

Daí segue que a sequência de equivalências

$$N = d_1.q_1 = d.q = d_2.q_2$$
$$\Updownarrow$$
$$d_1.q_1 = (d_1 + k_1).q = (d_2 - k_2).q = d_2.q_2$$
$$\Updownarrow$$
$$[d_1.(q_1 - q) = k_1.q] \wedge [d_2.(q - q_2) = k_2.q]$$
$$\Downarrow$$
$$(0 \leq q_1 - q) \wedge (0 \leq q - q_2)$$
$$\Updownarrow$$
$$q_2 \leq q \leq q_1$$

■

A recíproca segue diretamente das unicidades de quociente e divisor afirmadas pelo Algoritmo da Divisão de Euclides.

Ocorre também que, ainda da observação da Tábua de testes para os Divisores de 20, pode-se perceber – ou chamar a atenção do estudante – que $3 \nmid 20$*, e que, sendo assim, um outro múltiplo de 3 não poderia ser divisor de 20. Isso se evidencia na Tábua nos casos em que* $d = 6, 9, 12, 15$ *e 18. No entanto as proposições 1.1 e 1.2 já apresentam de antemão outros motivos – bem mais fortes – para excluirmos esses divisores. Como estamos explorando o problema, a exclusão direta desses possíveis divisores poderia – caso não se tome a cautela necessária – deixar ocultos outros importantes resultados. Uma idéia para investigar esses outros pormenores está em construir Tábuas de Testes de Divisores para números um pouco maiores.*

Tome-se, para observar particularmente algumas dessas relações entre os divisores de um número natural, $D = 370$*.*

Como $\sqrt{370} < 20$*, a proposição 01 nos garante que* $d < 20$*, e assim construímos uma*

versão mais compacta da Tábua de Testes para os Divisores de 370,

Tabela 1.3: Tábua de testes para os divisores de 370

d	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
q	370	185	123	92	74	61	52	46	41	37	33	30	28	26	24	23	21	20	19
r	0	0	1	2	0	4	6	2	1	0	7	10	6	6	10	2	13	10	9

Veja ainda que $(3 \nmid 370)$ *e* $6(\nmid 370)$*; e o mesmo se repete para* $d = 9, 12, 15$ *e* 18*; ou seja: os múltiplos de 3. Vê-se também a mesma situação quando* $d = 4$*, e quando* $d = 7$*.*

Buscamos naturalmente uma regularidade entre esses dados. Felizmente é deveras fácil, além de intuitivo, concluir uma generalização para o que observamos nessa Tábua. Temos assim o resultado que segue.

Proposição 1.3. *Se* $(a \nmid N)$*,e* $(a \mid b)$*, então* $(b \nmid N)$*.*

Demonstração:

Segue diretamente da definição de divisor.

■

Esta proposição nos permite dizer que, uma vez que se tenha um candidato a divisor que não o seja, podemos excluir da Tábua todos os seus múltiplos. Isso torna possível mais uma otimização em nosso algoritmo, posto que necessitamos atentar apenas para a primeira vez em que um candidato não é divisor do número estudado; deixando, por exclusão, de testar seus múltiplos. Dessa forma, ainda no caso $D = 370$*, nossa Tábua de Testes ficaria assim:*

Tabela 1.4: Tábua de testes para os divisores de 370

d	1	2	3	4	5	7	10	11	13	17	19
q	370	85	123	92	74	52	37	33	28	21	19
r	0	0	1	2	0	6	0	7	6	13	9

Bem menor, e mais simples, que a Tábua inicial essa versão pode ainda receber uma pequena otimização: A exclusão dos divisores triviais (1) e (370).

Tabela 1.5: Tábua de testes para os divisores de 370

d	2	3	4	5	7	10	11	13	17	19
q	85	123	92	74	52	37	33	28	21	19
r	0	1	2	0	6	0	7	6	13	9

Assim, finalmente, para o caso $D = 370$, teríamos:

Dessa forma, $D'(370) = \{2, 5, 10, 37, 74, 185\}$

Chegaríamos ao fim de nossas aulas sobre o tema da divisibilidade com essa Tábua, e a utilizaríamos como um Algoritmo para a Obtenção dos Divisores Naturais de um Número Natural. As próximas abordagens visariam o estudo de Números Primos e Algoritmos de Fatoração.

1.3 Uma Pequena Observação Aritmética:

No que se refere aos processos operatórios – ou as contas propriamente ditas – há um certo resultado que , embora não sendo menos simples, pede ao estudante mediano um tantinho mais de "paquera" para se deixar ver.

É o seguinte: Tendo as propriedades comutativa e associativa em mente, quando se torna a observar a Tábua de Divisores para D = 370, vê-se imediatamente que 370 = (10).(37). Ocorre também que 10 = (2).(5). Logo, pela aplicação direta das propriedades citadas, conclui-se que 370 = (37).(2.5) = (37.2).(5) = (37.5).(2).

Em síntese: 370 = 1 . 370 = 2 . 185 = 5 . 74 = 10 . 37

Infelizmente, as propriedades operacionais da multiplicação, como também da adição, embora muito enfatizada nos Ciclos Iniciais do Ensino Fundamental, é em geral pouco usada pelos profissionais do ensino de matemática dos Ciclos Finais na construção e compreensão de algoritmos de Aritmética. Sobre os motivos dessa postura – na opinião deste autor – pode-se apenas conjecturar. O certo é que muitos algoritmos – como os de fatoração, determinação de MMC e MDC, apenas para citar alguns dentre os que são mais pertinentes a esta dissertação – afastam-se de tal maneira da natureza tautológica da Matemática que se tornam para os estudantes meros procedimentos mnemônicos. Outra consequência – também deveras lamentável – é que, tornadas invisíveis, essas proposições deixam de fornecer ao estudante pistas ou ideias para a resolução de problemas.

Nesse caso particular, a observação dessas propriedades conduzem o estudante automaticamente aos divisores de 370. Com um tanto mais de paciência, persistência e planejamento, passando pela investigação desse 'estranho' número (37) – que possui apenas os divisores triviais – pode-se chegar ao belíssimo Teorema Fundamental da Aritmética e a seus não menos notáveis corolários. Esse é o objetivo da próxima secção.

Capítulo 2

Algoritmos de fatoração

2.1 Os Números Primos:

A partir de exercícios de determinação de divisores de um natural, mesmo ainda sem chegar formalmente a qualquer algoritmo de fatoração, os estudantes geralmente percebem um resultado simples e direto oriundo da própria definição de divisor de um número natural. Qual seja: que os divisores de um divisor de N também são divisores de N.

Simbolicamente: $[d \mid N] \Rightarrow [d \mid (k.N)], \forall k \in \mathbb{N}^*$.

Tal assertiva, embora óbvia, dá a um algoritmo de obtenção de divisores uma velocidade extra muito bem vinda. Tomando a mesma situação prática: Fatorar 370.

Veja que como 370 = 2.185, a nossa tábua de divisores de 370 poderia ser reduzida a tábua dos divisores de 185, pois, além desses, restariam apenas os produtos deles por 2. Em síntese: Se $d \mid 185$, *então* $(2d) \mid 370$.

Generalizando, tem-se

Proposição 2.1. $[d \mid N] \Leftrightarrow [d \mid (k.N)], \forall k \in \mathbb{N}^*$

Demonstração:

$(\Rightarrow)$:

Sejam $N, k \in \mathbb{N}$

$$d \mid N \Leftrightarrow \exists q \in \mathbb{N}; N = d.q \Rightarrow k.N = k.d.q \Leftrightarrow (kd)|(kN)$$

$(\Leftarrow)$:

De forma análoga, segue diretamente da definição de divisor.

■

Logo de início, os benefícios trazidos pela proposição 2.1 são bem recebidos em sala pelos estudantes. Mas, a alegria dura apenas até alguém observar que existem números que tem poucos divisores. Em sala, para investigar as possíveis relações entre um número e a quantidade

de divisores não triviais dele, podemos iniciar com uma tabela simples de duas linhas, onde $|d'(N)|$ *é a quantidade de divisores não triviais de N*

Assim, temos

Tabela 2.1: Quantidade de divisores não-triviais de N

N	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\mid d'(N) \mid$	0	0	0	1	0	2	0	2	1	2	0	4	0	2	0	3	0	4	0	4

Esta tábua apresenta alguns números com a peculiar característica de não possuir outros divisores além dos triviais. Eliminando o caso óbvio da unidade (1); haja vista que, nos naturais, pode-se escrever 1 apenas produto dele por si; i.e.: $1 = 1.1$*; aos outros números com esse interessante atributo dá-se o nome de Número Primo. Em tempo: Quando um número admite algum divisor além dos triviais, dizemos que ele é Composto. Daí, segue que para qualquer número natural* $N, 1 < N$*, vale a assertiva: Se não é primo, ele é composto; e vice-versa.*

Consideraremos ainda o conjunto $\mathbb{P} = \{p \in \mathbb{N} \backslash 0, 1; \mid d'(p) \mid = 0\}$ *dos números primos.*

Veja que as tabelas anteriores sugerem fortemente que uma vez conhecidos os divisores primos de um número é possível acessar todos os outros. Isso é bem razoável se considerarmos que – não tendo um número primo divisores – se tomarmos, por exemplo, dois deles, p_1 *e* p_2*, o conjunto* $d'(N)$ *dos divisores naturais não-triviais do número* $N = p_1.p_2$ *seria necessariamente* $\{p_1, p_2\}$*. Ao se considerar uma quantidade pouco maior de primos, muitos estudantes levantam sozinhos a conjectura de que, de fato, os divisores de um produto de primos deve ser produto de uma combinação deles. Essa conjectura é verdadeira, e mais: Se N é um produto de primos, então esses primos são únicos; ou seja: A fatoração em primos é única.*

A natureza da próxima asserção, o merecidamente chamado Teorema Fundamental da Aritmética, afirma exatamente isso. Um resultado usado sem reservas desde os antigos gregos e babilônios, mas, até onde nos informa a História, somente demonstrado com rigor por Gauss, no final do sec. XVIII.

Teorema 2.1 (Teorema Fundamental da Aritmética)**.** *Dado $N \in \mathbb{N}\backslash 0,1$, tem-se, exclusivamente, que: N é primo, ou N é produto único, a menos de permutação, de um número finito de primos.*

ou,

$$\exists!\ q_1, q_2, \ldots, q_m \in \mathbb{P}, e\ \alpha_1, \alpha_2, \ldots, \alpha_m \in \mathbb{N}; N = \prod_{k=1}^{m} (q_k)^{\alpha_k}$$

Demonstração:

Usando a segunda forma do Princípio de Indução vemos que:

O resultado se verifica imediatamente para $n = 2$.

Considere agora o resultado verdadeiro para todo número natural menor do que k e vamos provar que vale para k. Suponhamos, para dispensar a análise do caso óbvio em que k é primo, que k seja composto. $\exists k_1, k_2 \in \mathbb{N}; k = k_1.k_2, com 1 < k_1 \leq k_2 < k$. Pela hipótese de indução, temos que existem únicos números primos que fatoram k_1 e k_2.

Daí segue que os divisores primos de cada k_i serão necessariamente, pela própria característica de serem primos, os únicos divisores primos de k.

■

Uma pergunta inicial bem razoável, posto que ser primo é uma característica muito particular, é: A quantidade de Números Primos é finita?

Tal questionamento é deveras pertinente, e muito natural, quer seja nos ciclos finais do Ensino Fundamental ou no Ensino Médio. Num primeiro momento, alguém poderia achar maravilhoso que todos os números naturais pudessem ter seus divisores gerados por um conjunto finito de outros números; afinal esse fenômeno parece ocorrer em outras áreas do conhecimento. Aparentemente coisa parecida acontece na Química, no caso dos elementos químicos; ou na literatura, quando se percebe que um livro enorme é feito com a disposição de apenas 27 letras. O estendal de exemplos poderia continuar, mas é o bastante.

Voltando ao caso em estudo; iniciamos uma aproximação do problema buscando observar como os números primos se distribuem no Conjunto dos Naturais. Para tanto, construímos

uma simples Tábua de Distribuição de Freqüência sobre as quantidades de números primos existentes em intervalos de mesmo comprimento. A própria confecção dessa tabela se torna, por si só, um bom exercício para a determinação de primos.

A partir do conjunto $\mathbb{P}$, de todos os números primos, e dos naturais a e b, definimos $P[a;b] = \{x \in \mathbb{P}; a \leq x \leq b\}$, e $\mid P[a;b] \mid$ sua cardinalidade. Daí segue a tabela:

Tabela 2.2: Quantidade de divisores não-triviais de N

n	0	10	20	30	40	50	60	70	80	90	100	110	120	130	140
$\mid P[n;n+10] \mid$	4	4	2	2	3	2	2	3	2	1	4	1	1	3	1

Aparentemente – observando apenas os dados e resultados que se dispõem até aqui – a densidade de primos sobre os naturais diminui quando n cresce; vemos que essa diminuição se dá – também aparentemente – de forma irregular. Tomando $n > 200$ vemos alguns desses intervalos livres de primos. Quando se aumenta n aumenta-se também a quantidade de intervalos desse tipo. Daí – e notando também que não parece ser clara a existência de alguma regularidade na distribuição desses primos – é quase fácil sermos tentados a levantar a conjectura de que a quantidade de primos é finita.

Euclides nos deixou uma bela demonstração de que tal não ocorre. A quantidade de números primos é de fato infinita! Esse é o enunciado da próxima assertiva.

Proposição 2.2. $\nexists\, n \in \mathbb{N}; |\mathbb{P}| = n$

Demonstração:

Suponha, por absurdo, que $\mathbb{P} = \{p_1, p_2, p_3, \ldots, p_n\}$, e considere o problema da fatoração do $N = p_1.p_2.p_3.\ldots.p_n + 1$. Veja que obviamente $N \notin \mathbb{P} = \{p_1, p_2, p_3, \ldots, p_n\}$, pela própria construção de N e de $\mathbb{P}$; i.e.: N não é primo. Por outro lado, o Teorema Fundamental da Aritmética garante que ou N é primo ou N é necessariamente produto de elementos de $\mathbb{P}$. Posto isso, deve existir, em $\mathbb{P}$, um divisor de N. É justamente a suposta existência desse divisor que produz o absurdo. Senão vejamos:

$$[N - p_1.p_2.p_3.\ldots.p_n = 1] \Leftrightarrow \exists p_t \in \mathbb{P}; p_t.(\frac{N}{p_t} - (p_1.p_2.p_3.\ldots.p_n)/p_t) = 1 \Leftrightarrow p_t|1 \rightarrow\leftarrow$$

■

Ocorre muitas vezes - e aqui é um exemplo - que pode ser a pergunta em si, e as tentativas de respondê-la, que levam a outros resultados significativos. Na construção da Tabela 2.2, por exemplo, faz-se necessário decidir quais números de cada intervalo são primos. Para resolver esse problema, por hora, cabe-nos apenas analisar caso a caso os números de cada intervalo. Para tal, valemo-nos – em uma primeira abordagem – do algoritmo já conhecido das Tábuas de Divisores.

É notadamente fácil detectar os primeiros primos. As dificuldades parecem surgir quando o número N a ser testado começa a ficar grande. Aparentemente a quantidade de operações aritméticas necessárias é bem maior. Para investigar essa relação entre N e a quantidade de operações para decidir sobre sua primalidade, partindo da já construída Tábua para $N = 370$*, tomamos o caso particular de* $N = 371$*. Em sala, propomos o problema: O número 371 é primo ?*

Inicialmente verifica-se que $2 \nmid 371$*. Daí, pela proposição 1.3, segue diretamente que* $4 \nmid 371$, $6 \nmid 371$, $8 \nmid 371$*, etc. Analogamente excluímos os múltiplos de 3. Como não é necessário testar* $d = 4$*, avançamos e vemos que* $5 \nmid 371$*, e excluímos seus múltiplos. Ignorando o também já desprezado* $d = 6$*, e observando que* $7 \mid 371$*, damos por respondida a pergunta inicial: Não, 371 não é primo, pois é um múltiplo de 7.*

A pergunta está respondida, mas na busca de algo além dela pode-se atentar para o fato de que quando se pergunta se certo número natural N é primo ou composto não há, em princípio, interesse algum em conhecer seus divisores não triviais. Deseja-se saber tão somente se ele os possui ou não! No caso específico, $N = 371$*, veja que foi necessário testar – como candidatos a divisores de N – apenas os primos menores que* $\sqrt{371}$*; no caso: 2, 3, 5, 7, 11, 13, 17 e 19. O algoritmo parou em* $d = 7$*, a quarta tentativa.*

Generalizando: A partir do conjunto $\mathbb{P}$*, de todos os números primos, e de um número real N, denotamos* $P_N = \{x \in \mathbb{P}; x < N\}$*, o conjunto dos primos menores que N, afirmamos:*

Proposição 2.3. *Dado* $p \in \mathbb{N}$*,*

$$(p \in \mathbb{P}) \Leftrightarrow (d \nmid p, \forall d \in P_{\sqrt{N}})$$

Demonstração: *Segue da generalização direta dos argumentos já mostrados.* ■

Os argumentos que validam essa assertiva geram diretamente - para números com até três dígitos decimais - um algoritmo eficiente, embora pouco prático, para decidir se um número é primo. Chamaremos esse algoritmo de Algoritmo Primário, e, a seguir, apresentamos duas versões dele; uma de fato bem grosseira e uma segunda algo melhorada.

2.2 O Algoritmo Primário:

Dado um número natural N, deseja-se saber se ele é possível determinar sua primalidade, e , caso afirmativo, decidir se ele primo ou não.

Nossa idéia inicial consiste em as possíveis divisibilidades de N por todos os primos menores que $\sqrt{N}$*. Lançamos não de uma tábua indexando uma lista inicial de números primos e, a partir dela, definimos os limites de nosso algoritmo bem como sua estrutura. Senão, vejamos*

Algoritmo Primário(1ª versão):

Inicializações: Lista $P_k = p_1, p_2, p_3, \ldots, p_m, i := 1.$

Passo I: Receber N

Passo II: Testar

$$\begin{cases} Se \sqrt{N} > p_m, retornar: \text{ ' Não é possível fatorar N. ' }, \boxdot \\ Senão, n := \lfloor \sqrt{N} \rfloor \end{cases}$$

Passo III: Testar

$$\begin{cases} Se\ p_i > n, retornar: \text{ ' O algoritmo está encerrado ' }, \boxdot \\ Senão, \end{cases}$$

Passo IV: Testar

$$\begin{cases} Se\ p \mid n, retornar: \text{ ' N é divisível por } p_i', \boxdot \\ Senão, retornar: \text{ ' N não é divisível por } p_i\text{'} \end{cases}$$

Passo V: $i := i + 1$*, ir para Passo III*

A seguir observamos, a partir de dois exemplos, a aplicação dessa versão do Algoritmo Primário; onde tentaremos também investigar suas vantagens e limitações.

Exemplo 2.1. *Fatorar 871*

Inicialização: Considere $P_{100} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, ..., 83, 89, 97\}$

1. $N := 871$
2. $n := 29, e\ p_m = 29$
3. *871 não é divisível por 2*
4. *871 não é divisível por 3*
5. *871 não é divisível por 5*
6. *871 não é divisível por 7*
7. *871 não é divisível por 11*
8. *871 é divisível por 13*
9. *871 não é divisível por 17*
10. *871 não é divisível por 19*
11. *871 não é divisível por 23*
12. *871 não é divisível por 29,*
13. *O Algoritmo está encerrado!,* $\boxdot$

O Algoritmo Primário nos diz que 871 é divisível por 13 e 67; ou, mais apropriadamente, que 13 e 67 são os divisores primos de 871.

Exemplo 2.2. *Fatorar 2737*

Inicialização: Considere $P_{100} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, ..., 83, 89, 97\}$

1. *2737 não é divisível por 2*
2. *2737 não é divisível por 3*
3. *2737 não é divisível por 5*
4. *2737 é divisível por 7*
5. *2737 não é divisível por 11*
6. *2737 não é divisível por 13*
7. *2737 é divisível por 17*
8. *2737 não é divisível por 19*
9. *2737 é divisível por 23*
10. *2737 não é divisível por 29*
11. *2737 não é divisível por 31*
12. *2737 não é divisível por 37*
13. *2737 não é divisível por 41*
14. *2737 não é divisível por 43*
15. *2737 não é divisível por 47*
16. *O Algoritmo está encerrado!,*

O Algoritmo Primário nos diz que 7,17 e 23 são os divisores primos de 2737.

Veja que, no exemplo 2.1, se tivéssemos percebido que 67 era primo, poderíamos ter dado o algoritmo por encerrado no 8ª etapa da execução do Algoritmo. Nesse caso, bastaria uma simples pergunta ($67 \in P_{100}$ (?))*, já que 67 é um elemento de nossa lista inicial de primos.*

Se não o fosse, seria outro problema; mas, de uma forma ou de outra, é uma vantagem sabê-lo. Já no exemplo 2.2, vemos uma situação conhecida: A 6ª etapa no informa que 2737 = 7.391; e disso – e do Teorema Fundamental da Aritmética – se deduz que não nos seria necessário continuar com a fatoração de 2737. Bastar-nos-ia fatorar 391 para finalizá-la!

Há ainda o caso de N ser primo, estando ou não em nossa lista inicial. Seria interessante poder explicitar a conclusão desse resultado. Declará-lo formalmente. Isso sem contar com um caso um pouco mais delicado: o da divisibilidade por uma potência de primo. Veja que, em se aplicando direta e simplesmente essa primeira versão do algoritmo, que testa apenas os divisores primos de um número, algum estudante em um momento de pouca atenção, ao observar que $871 = 13.67$ *e que* $2737 = 7.17.23$*, poderia erroneamente inferir que esse algoritmo dá mesmo a fatoração de N. De fato, tal situação didática não é incomum em sala, quando nessa etapa inicial das investigações sobre esse tema. No entanto, esse mal-entendido quase sempre é resolvido quando se atenta para o fato de que, se tal afirmação fosse verdade, chegaríamos à bizarra conclusão de que, por exemplo,* $216 = 2.3$*, haja vista que 2 e 3 são os únicos primos pelos quais 216 é divisível.*

É claro que o parágrafo anterior poderia ser entendido como mero estendal de percepções das limitações ou mesmo dos erros do algoritmo em questão. Isso não seria um equívoco, mas, quando se considera o campo de investigação que é uma sala de aula do Ensino Básico, percebemos sim que esses pontos e exemplos evidenciados representam alguns dos deslizes mais frequentes por parte dos estudantes. É necessário pensar sobre um problema se o objetivo da abordagem for resolvê-lo.

Vejamos agora uma versão mais burilada desse algoritmo. Em síntese, adicionamos um contador "d", cujo objetivo é verificar, e informar, se N é primo; e podemos também oferecer certa velocidade ao algoritmo, substituindo N, sempre que encontrarmos um seu divisor, pelo quociente de N por por esse divisor. Assim,temos,

Algoritmo Primário(2ª versão):

Inicializações: Lista $P_k = \{p_1, p_2, p_3, \ldots, p_m\}, i := 1, d := 0.$

Passo I: Receber N

Passo II: Testar

$$\begin{cases} Se N \in P_k, retornar: \text{'N é um número primo.'}, \boxdot \\ Senão, \end{cases}$$

Passo III: Testar

$$\begin{cases} Se \sqrt{N} > p_m, retornar: \text{' Não é possível fatorar N. '}, \boxdot \\ Senão,\ n := \lfloor \sqrt{N} \rfloor \end{cases}$$

Passo IV: Testar

$$\begin{cases} Se\ p_i > n, retornar: \text{ ' O algoritmo está encerrado ', ir para Passo VI }, \\ Senão, \end{cases}$$

Passo V: Testar

$$\begin{cases} Se\ p_i \mid n, retornar: \text{' N é divisível por } p_i\text{'}, N := \frac{N}{p_i}, d := d + 1, \text{ ir para Passo III }, \\ Senão, retornar: \text{ ' N não é divisível por } p_i \text{ '}, i := i + 1, \text{ ir para Passo IV }, \end{cases}$$

Passo VI: Testar

$$\begin{cases} Se\ d = 0, retornar: \text{' N é um número primo '}, \boxdot \\ Senão, \boxdot \end{cases}$$

Mesmo após essas, e até ainda outras otimizações, o Algoritmo Primário continua apresentando duas sérias limitações operacionais. A primeira se refere a necessidade de uma lista inicial de primos para efetivamente processar o algoritmo. A segunda, bem mais complicada e difícil de contornar, diz respeito ao tamanho do procedimento em si; à quantidade de cálculos necessários à finalização do algoritmo. Se N for muito grande, essa quantidade de cálculos se torna um número proibitivo.

Podemos, por outro lado, à guisa de simplicidade didática, apresentar apenas a Tábua de Restos para os supostos divisores primos da lista inicial, até $\sqrt{N}$*. Isso pode ser feito em um editor de tabelas como o Excel ou o Lotus 123. Um programa realmente simples do ponto de vista didático. Assim, no Exemplo 1 teríamos*

Tabela 2.3: Tábua de testes para os divisores de 871 (Simplificada)

d	2	3	5	7	11	13	17	19	23	29
r	1	1	1	3	2	0	4	16	20	1

O algoritmo continuaria sendo executado da mesma forma; até, talvez, um pouco mais lentamente, considerando a inexistência aqui de um teste que "freie" o algoritmo. O estudante ganharia na visualização dos resultados.

2.3 O Crivo De Erathóstenes:

Erathóstenes abordou o problema da primalidade de uma maneira não convencional, centrando sua atenção na fácil tarefa de determinar múltiplos de alguns números em vez de possíveis divisores de outros, coisa quase sempre bem mais complicada. Investigaremos seu Algoritmo – o Crivo de Erathóstenes – a partir de algumas conclusões já conhecidas.

Senão vejamos:

Decidir se certo número natural N é primo ou não geralmente remete o estudante a uma Tábua de Divisores, onde a linha/coluna de divisores é composta apenas pelos primos menores – ou iguais – que $\sqrt{N}$*. Já vimos esse algoritmo!*

Determinar qual o primeiro primo maior que certo natural N é um problema um tanto mais delicado, haja vista que testar – usando Tábuas de Divisores – a primalidade dos naturais maiores que N pode ser uma tarefa algo demorada. A aparente irregularidade da distribuição dos primos apresenta também uma dificuldade extra: Não se sabe, a priori, se o próximo primo maior que N está próximo de N. A Tábua de Restos se mostra uma ferramenta útil para abordar esse problema e outros similares a ele; tais como encontrar os k primeiros primos maiores que N, ou analogamente como encontrar os k últimos primos menores que N. Se o N e o k não forem demasiado grandes, a Tábua de Restos é uma boa opção como estratégia de resolução do problema.

É interessante quando se percebe que encontrar – por exemplo – os 10 primeiros primos maiores que 300 é faina que demanda um esforço bem menor que o esperado sem a Tábua de Restos. Já se viu que tal melhoria vem quando se nota a irrelevância de explicitar os quocientes das divisões de 300 pelos hipotéticos divisores, posto que os restos se devem apenas a um resto fixo – o de 300, no caso – e a k. Em outros termos: Aparentemente quando o problema se complicou – ou pareceu ter se complicado, o algoritmo para resolvê-lo ficou mais simples.

Erathóstenes se aproximou desse problema para investigar aquele, o primeiro: o da determinação da primalidade de um número natural; e o fez de uma maneira didaticamente belíssima. Ele não usou truques ou artifícios além dos razoáveis para o nível do próprio problema; muito pelo contrário, a construção de seu algoritmo leva em conta tão somente a óbvia definição de número primo e suas conseqüências imediatas. Para estudantes do Ensino Básico,

e provavelmente para todo investigador do problema, a engenhosidade de seu Crivo salta aos olhos, quer seja pela simplicidade no trato com os elementos manipulados, quer seja pela amplitude de sua solução: O Crivo não diz apenas se determinado número é primo ou não; ele delimita, isso sim, as fronteiras de um intervalo onde existem primos, explicitando-os diretamente.

Eis o Algoritmo de Erathóstenes:

Primeiramente lista-se a seqüência dos primeiros números naturais até um limite K explicitado. Para o estudo de um caso particular, tomaremos K = 170.

Assim, temos uma primeira lista de naturais; todos eles, a priori, sendo candidatos a primos.

Tabela 2.4: (Lista dos números naturais não nulos menores que 171)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68
69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85
86	87	88	89	90	91	92	93	94	95	96	97	98	99	100	101	102
103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119
120	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136
137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153
154	155	156	157	158	159	160	161	162	163	164	165	166	167	168	169	170

Agora observe que, pela definição, se p é primo, então $p > 1$. Daí, de nossa lista, retiramos o seu primeiro elemento (1). Vê-se também que o primeiro número dessa nova lista – o 2 – satisfaz perfeitamente a definição de primo; aliás, a excessaõ de si próprio, ele não pode ser múltiplo de nenhum outro número além de 1, pois é o primeiro depois dele. Assim, 2 é primo!

Por outro lado, todo múltiplo de 2, justamente por ser múltiplo de algum número, é composto. Logo não é primo. Podemos assim excluir também da lista todos os múltiplos de 2; restando apenas

Tabela 2.5: (Lista dos números naturais menores que 171, primos ou livres de multiplicidade por 2), ou (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2 \notin d'(n)\}$)

	2	3		5		7		9		11		13		15		17
	19		21		23		25		27		29		31		33	
35		37		39		41		43		45		47		49		51
	53		55		57		59		61		63		65		67	
69		71		73		75		77		79		81		83		85
	87		89		91		93		95		97		99		101	
103		105		107		109		111		113		115		117		119
	121		123		125		127		129		131		133		135	
137		139		141		143		145		147		149		151		153
	155		157		159		161		163		165		167		169	

Note de novo que o primeiro número maior que 2 que restou nessa lista é 3. Como, por construção da lista, $2 \nmid 3$*; e observando também que, por exclusão, 2 é o único número do qual 3 poderia ser múltiplo; resta que 3 é primo; e podemos excluir da lista – pelos mesmos argumentos apresentados para os múltiplos de 2 – todos os múltiplos de 3; restando*

Tabela 2.6: (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2,3 \notin d'(n)\}$)

	2	3		5		7				11		13				17
	19				23		25				29		31			
35		37				41		43				47		49		
	53		55				59		61				65		67	
		71		73				77		79				83		85
			89		91				95		97				101	
103				107		109				113		115				119
	121				125		127				131		133			
137		139				143		145				149		151		
	155		157				161		163				167		169	

Analogamente, 5 só poderia ser múltiplo de algum primo menor que ele. Ora, tais primos são justamente os já explicitados na lista, 2 e 3; cujos múltiplos foram excluídos da seqüência original. Como o 5 não foi excluído, não é composto; logo é primo, e, ato contínuo, deve-se retirar da lista seus múltiplos.

Assim,

Tabela 2.7: (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2,3,5 \notin d'(n)\}$)

	2	3		5		7				11		13				17
	19				23						29		31			
		37				41		43				47		49		
	53						59		61						67	
		71		73				77		79				83		
			89		91						97				101	
103				107		109				113						119
	121						127				131		133			
137		139				143						149		151		
			157				161		163				167		169	

O próximo "sobrevivente" do Crivo é 7, que, por construção, não é composto. Segue que 7 é primo e o próximo passo seria a natural exclusão de seus múltiplos. Mas, antes de fazê-lo, já é possível observar um fato importante: Nessa etapa do algoritmo, pode-se garantir a primalidade não apenas de 7 – o próximo primeiro não excluído da lista, mas também de 11, bem como de 13, 17, 19, 23, 29, 31, 37, 41, 43 e de 47.

A afirmação é forte, mas de simples verificação.

Senão vejamos: Quando se vai excluir os múltiplos de 7 da lista percebe-se que alguns deles já foram excluídos antecipadamente; quais sejam: 14, pois $2 \mid 14$*; 21, pois* $3 \mid 21$*; 28, pois* $2 \mid 28$*, e* $4 \mid 28$*; 35, pois* $5 \mid 35$*; e 42, pois* $2 \mid 42$*. Ou seja, começar-se-á a exclusão a partir de* $7^2 = 49$*. Nota-se também que nenhum dos números menores que 49 que ainda figuram na lista são compostos, pois caso algum deles fosse múltiplo de um número, deveria ser forçosamente também de 2, 3 ou 5, cujos múltiplos já foram excluídos da lista. Resta que todos são primos.*

É possível observar que situação análoga ocorreu também para a exclusão dos múltiplos

de 3 e 5. Acontece que, enquanto os números são pequenos, pode não ser tão fácil perceber alguns detalhes.

Continuando com o algoritmo, afirma-se que 7 é primo, bem como todos os listados menores que 49, e excluímos seus múltiplos, bastando buscá-los a partir de 49.

Temos então a nova lista

Tabela 2.8: (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2,3,5,7 \notin d'(n)\}$)

	2	3		5		7				11		13				17
	19				23						29		31			
		37				41		43				47				
	53						59		61						67	
		71		73						79				83		
			89								97				101	
103				107		109				113						
	121						127				131					
137		139				143						149		151		
			157						163				167		169	

Na próxima etapa, afirma-se que 11 é primo, bem como todos os listados menores que 121, e excluímos seus múltiplos, bastando buscá-los a partir de 121. Assim

Tabela 2.9: (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2,3,5,7,11 \notin d'(n)\}$)

	2	3		5		7				11		13				17
	19				23						29		31			
		37				41		43				47				
	53						59		61						67	
		71		73						79				83		
			89								97				101	
103				107		109				113						
	0						127				131					
137		139										149		151		
			157						163				167		169	

Finalmente, conclui-se que todos os listados menores menores que 169 são primos, restando excluir apenas o próprio 169, haja vista que os seus outros múltiplos são maiores que 170, o K limitador definido no início.

Daí, segue a explicita lista dos Números Naturais Primos Menores que K = 170.

Tabela 2.10: (Lista $L = \{n \in N_{171} \setminus \{0,1\}; 2,3,5,7,11,13 \notin d'(n)\}$)

	2	3		5		7				11		13				17
	19				23						29		31			
		37				41		43				47				
	53						59		61						67	
		71		73						79				83		
			89								97				101	
103				107		109				113						
	0						127				131					
137		139										149		151		
			157						163				167			

2.4 O Algoritmo de Fermat:

Fermat investigou o problema da fatoração por um ângulo no mínimo inusitado. Para fatorar um número natural N, ele não procurou fatores primos em N; o que , em primeira análise, poderia se assemelhar a uma estupidez tremenda, haja vista que o Algoritmo primário foi construído a partir de um burilamento do processo de teste de divisores. Verificou-se que os melhores candidatos eram justamente os primos. Como pensar em testar agora para um divisor qualquer? Parece de fato um retrocesso.

Parece mesmo, mas a astuta abordagem de Fermat mostra que isso é apenas aparência. Em verdade, seu algoritmo se torna lento apenas para números com fatoração em primos com características muito particulares. Quais sejam: $N = p.q$, com p,q primos e distantes um do outro. Já se verá o porque disso.

Fermat parte do fato óbvio de que, eliminando o caso trivialíssimo de quando N é um número par, qualquer dupla de divisores de N deve constar de dois números ímpares. Sendo assim, $N = p.q$, com $p < q$. Nesses termos, $\exists\, d \in \mathbb{N}; q = p + d$

Por outro lado,

$$2 \nmid N = p.q \Rightarrow (2 \nmid p) \wedge (2 \nmid q) \Rightarrow \exists\, m, n \in \mathbb{N}; (p = 2.m + 1) \wedge (q = 2.n + 1)$$

Veja então que

$$d = q - p = (2n + 1) - (2m + 1) = 2.(n - m)$$

Tome então $\beta = \dfrac{d}{2}$ *e veja que*

$$p + \beta = 2m + 1 + n - m = m + n + 1 = \tfrac{1}{2}.(2m + 2n + 2) = \tfrac{p+q}{2} = q - \beta = M$$

Assim, $N = p.q = (M - \beta).(M + \beta) = M^2 - \beta^2; e\, M^2 = N + \beta^2.$

Testando valores para a distância média β de p e q, encontra-se uma fatoração para N, quando o segundo termo for um quadrado perfeito. Tal fatoração, é óbvio, não é necessariamente prima, mas depende dos fatores primos de N. Em certas situações – quando os números são relativamente pequenos – é relativamente fácil gerar, com alguns ajustes, a fatoração completa do número N.Isso é garantido pelo Teorema Fundamental da Aritmética.

Uma versão simples do algoritmo propriamente dito é mostrada a seguir, e pode ser implementada também em um Editor de Planilhas como o Lotus 123, MS Excel ou equivalente.

Algoritmo de Fermat:

Inicializações: $i := 0, d := 0$.

Passo I: Receber N

Passo II: Testar

$$\begin{cases} Sei \leq \frac{N}{2}, M := \sqrt{N + i^2} \\ Senão,\ retornar:\ '\ O\ algoritmo\ está\ encerrado.'\ , irparaPassoV \end{cases}$$

Passo III: Testar

$$\begin{cases} SeM \in \mathbb{N}, retornar:\ '\ Uma\ fatoração\ de\ N\ é\ N = (\ M\ -\ i\ ).(\ M\ +\ i\ )'\ , d := d + 1 \\ Senão, \end{cases}$$

Passo IV:

$i := i + 1$, *ir para Passo II*

Passo V: Testar

$$\begin{cases} Se\ p_i \mid n, retornar:\ '\ N\ é\ divisível\ por\ p_i\ ', N := \frac{N}{p_i}, d := d + 1, irparaPasso\,III \\ Senão,\ retornar:\ '\ N\ não\ é\ divisível\ por\ p_i\ ',\ ir\ paraPasso\,IV \end{cases}$$

Passo VI: Testar

$$\begin{cases} Se\ d = 0, retornar:\ '\ N\ é\ um\ número\ primo\ ', \boxdot \\ Senão, \boxdot \end{cases}$$

Vejamos num caso particular a aplicação desse algoritmo.

Exemplo 2.3. *Fatorar N = 1833.*

Optaremos pela apresentação tabular dos testes para a distância entre os divisores de N. A tabela abaixo é parte de uma maior, gerada com o Excel.

Tabela 2.11: Tábua de testes para os divisores de 871 (Simplificada)

i	1	2	3	4	5	6	7	8	9	10	11	12
M	42,825	42,86	42,919	43	43,105	43,232	43,382	43,555	43,749	43,966	44,204	44,463

Vemos que, quando $i = 4, M = 1833 + 16 = 1849 = 432$. *Daí, segue uma fatoração de* $N = (43 - 4).(43 + 4) = 39.47$. *Fatorando* $39 = 3.13$, *obtemos* $N = 3.13.47$. *A grande vantagem desse algoritmo está em prescindir de uma lista inicial de valores armazenada. Isso, segundo algum parecer, pode ser considerado pouco, pois os estudantes já poderiam dispor de uma tábua de primos ao iniciar uma fatoração. Algoritmicamente porém é bom poder resolver um problema sem a necessidade de um bloco de informações preliminares.*

A desvantagem – enorme! – não se vê nesse exemplo. É que, como não estamos testando os divisores primos, de fato não precisamos de uma lista deles, mas, por outro lado, a quantidade de testes pode ser muito maior que no Algoritmo Primário.

Capítulo 3

Algoritmo Matricial para o Crivo de Erathóstenes

3.1 Uma Otimização para o Crivo de Erathóstenes:

Considere a seguinte afirmação:

Proposição 3.1. *Dados $d, n \in \mathbb{N}$; temos que*

Se $d \mid n$,

Então $d \mid (n + k.d), \forall k \in \mathbb{N}$.

A proposição 3.1, embora óbvia e de imediata verificação, fornece ao Crivo de Erathóstenes uma velocidade operacional extra e muito interessante. É que distribuindo os números da lista inicial em um número par de linhas – ou colunas - vê-se que, uma vez determinado um múltiplo de 2, os seus vizinhos de linha – ou coluna, conforme o caso – serão todos também pares. O mesmo se dá, de forma análoga, se tomássemos um número múltiplo de 3 de linhas/colunas: ao se determinar um múltiplo de 3, os seus vizinhos de linha – ou coluna, conforme o caso – serão todos também múltiplos de 3. O mesmo argumento se estende naturalmente para os múltiplos de quaisquer números dados.

A próxima idéia é natural. E se os números da lista inicial forem organizados em um número múltiplo de 2 e 3 de linhas – ou colunas? Um múltiplo de 6, no caso. Posto isso, nenhum óbice se põe à generalização dessa idéia para um múltiplo de 5, 7, 11 ou qualquer produto de primos.

Antes de dar prosseguimento, introduziremos uma definição que nos será útil a partir de agora. A de Primordial de um número primo.

Definição 3.1. *Considerando $p_1, p_2, p_3, ..., p_n$ os n'ésimos primeiros números naturais primos denomina-se $\alpha_n = \prod_{i=1}^{n}(p_i)$ o primordial de p_n.*

Considere $\alpha_3 = 2.3.5 = 30$. Veja que para qualquer múltiplo k de 2, 3 ou 5 valerá, pela proposição 12, a assertiva de que o número $T = k + \alpha_3$ gozará da mesma multiplicidade. Claro está que se pode fazer a generalização dessa verdade para qualquer α_n, mas, por ora, somente à guisa de exemplificação, tomaremos o caso particular de α_3 e usaremos a proposição 3.1 para buscar introduzir uma otimização no Crivo de Erathóstenes.

Posto isso, iniciaremos o processo de refazer o Crivo de Erathóstenes – a partir dos mesmos argumentos de antes – apenas com a pequena alteração de organizar a lista inicial de números em – digamos – α_3 linhas.

Escrevemos então a lista de todos os números naturais menores até 540

Tabela 3.1: (Lista L_1, do naturais menores que 540)

1	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2	32	62	92	122	152	182	212	242	272	302	332	362	392	422	452	482	512
3	33	63	93	123	153	183	213	243	273	303	333	363	393	423	453	483	513
4	34	64	94	124	154	184	214	244	274	304	334	364	394	424	454	484	514
5	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
6	36	66	96	126	156	186	216	246	276	306	336	366	396	426	456	486	516
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
8	38	68	98	128	158	188	218	248	278	308	338	368	398	428	458	488	518
9	39	69	99	129	159	189	219	249	279	309	339	369	399	429	459	489	519
10	40	70	100	130	160	190	220	250	280	310	340	370	400	430	460	490	520
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
12	42	72	102	132	162	192	222	252	282	312	342	372	402	432	462	492	522
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
14	44	74	104	134	164	194	224	254	284	314	344	374	404	434	464	494	524
15	45	75	105	135	165	195	225	255	285	315	345	375	405	435	465	495	525
16	46	76	106	136	166	196	226	256	286	316	346	376	406	436	466	496	526
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
18	48	78	108	138	168	198	228	258	288	318	348	378	408	438	468	498	528
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
20	50	80	110	140	170	200	230	260	290	320	350	380	410	440	470	500	530
21	51	81	111	141	171	201	231	261	291	321	351	381	411	441	471	501	531
22	52	82	112	142	172	202	232	262	292	322	352	382	412	442	472	502	532
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
24	54	84	114	144	174	204	234	264	294	324	354	384	414	444	474	504	534
25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505	535
26	56	86	116	146	176	206	236	266	296	326	356	386	416	446	476	506	536
27	57	87	117	147	177	207	237	267	297	327	357	387	417	447	477	507	537
28	58	88	118	148	178	208	238	268	298	328	358	388	418	448	478	508	538
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539
30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480	510	540

Seguindo os argumentos já expostos anteriormente, excluiremos, desta lista de possíveis primos, o número 1, por definição; deixaremos o número 2, por antítese primo e eliminaremos também os múltiplos de 2, por natural exclusão.

Ocorre justamente que ao iniciar a eliminação desses múltiplos de 2, nada de real interesse parece acontecer enquanto os números excluídos são menores que A_3. Quando, porem, passamos de A_3, percebemos que os novos excluídos se encontram todos nas mesmas linhas dos antigos. Considerando a proposição 3.1, isso não trás novidade, mas para o estudante é algo digno de nota. De fato, é esta observação que gera a construção da conjectura e demonstração da proposição 3.1.

Assim, a lista L_2 seria

h

Tabela 3.2: (Lista $L_2 = \{n \in N_{540} \setminus \{0,1\}; 2 \notin d'(n)\}$)

	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2																	
3	33	63	93	123	153	183	213	243	273	303	333	363	393	423	453	483	513
5	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
9	39	69	99	129	159	189	219	249	279	309	339	369	399	429	459	489	519
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
15	45	75	105	135	165	195	225	255	285	315	345	375	405	435	465	495	525
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
21	51	81	111	141	171	201	231	261	291	321	351	381	411	441	471	501	531
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505	535
27	57	87	117	147	177	207	237	267	297	327	357	387	417	447	477	507	537
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539

h

Tabela 3.3: (Lista $L_2 = \{n \in N_{540} \setminus \{0,1\}; 2 \notin d'(n))$

	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2																	
3	33	63	93	123	153	183	213	243	273	303	333	363	393	423	453	483	513
5	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
9	39	69	99	129	159	189	219	249	279	309	339	369	399	429	459	489	519
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
15	45	75	105	135	165	195	225	255	285	315	345	375	405	435	465	495	525
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
21	51	81	111	141	171	201	231	261	291	321	351	381	411	441	471	501	531
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505	535
27	57	87	117	147	177	207	237	267	297	327	357	387	417	447	477	507	537
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539

Pode-se então, de maneira natural, simplesmente excluir não apenas os números mas as próprias linhas.

Uma outra escrita – mais concisa – para L2 seria

Continuando o processo, analogamente quando da exclusão dos pares, 3 é primo e excluímos seus múltiplos, deixando L_3

Tabela 3.4: (Lista $L_3 = \{n \in N_{540} \setminus \{0,1\}; 2,3 \notin d'(n))$

	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2																	
3																	
5	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505	535
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539

Compactando-a, temos

Tabela 3.5: (Lista $L_3 = \{n \in N_{540} \setminus \{0,1\}; 2,3 \notin d'(n)\}$

	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2																	
3																	
5	35	65	95	125	155	185	215	245	275	305	335	365	395	425	455	485	515
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
25	55	85	115	145	175	205	235	265	295	325	355	385	415	445	475	505	535
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539

Finalmente, usando os mesmos artifícios para 5, temos L_4.

Tabela 3.6: (Lista $L_4 = \{n \in N_{540} \setminus \{0,1\}; 2,3,5 \notin d'(n)\}$

	31	61	91	121	151	181	211	241	271	301	331	361	391	421	451	481	511
2																	
3																	
5																	
7	37	67	97	127	157	187	217	247	277	307	337	367	397	427	457	487	517
11	41	71	101	131	161	191	221	251	281	311	341	371	401	431	461	491	521
13	43	73	103	133	163	193	223	253	283	313	343	373	403	433	463	493	523
17	47	77	107	137	167	197	227	257	287	317	347	377	407	437	467	497	527
19	49	79	109	139	169	199	229	259	289	319	349	379	409	439	469	499	529
23	53	83	113	143	173	203	233	263	293	323	353	383	413	443	473	503	533
29	59	89	119	149	179	209	239	269	299	329	359	389	419	449	479	509	539

Nessa altura do algoritmo já podemos concluir que todos da lista L_4, anteriores a $49 = 7_2$, são primos. Desses, 7 é o primeiro. Excluindo displicentemente seus múltiplos teríamos L_5 de maneira direta, mas, por outro lado, novamente durante o processo de exclusão, pode ficar evidente um novo fato: Não se precisa excluir nenhum dos números de L_4 menores que 49, posto que os múltipos 7 anteriores a este já passaram pelo crivo de 2, 3 e 5. Disso já se sabia! Acontece, entretanto, por outro lado, que também os múltiplos de 7 com divisores entre 7 e 11 pelos mesmos motivos já se foram; o mesmo ocorrendo para todos os divisíveis por algum múltiplo de 2, 3, ou 5. Todos eles, pelo processo de construção de L_4, já foram eliminados.

Resta assim, visando o processo de exclusão, atentar somente para os múltiplos de 7 divisíveis pelos elementos de L_4.

Dessa forma, construímos L_5 enfatizando – como primos – em L_4 os seus elementos menores que 49 e eliminando dela os números $7.7 = 49, 7.11 = 77, 7.13 = 91, 7.17 = 119$, e assim por diante, até, pela limitação da lista, $7.77 = 539$.

Tabela 3.7: (Lista $L_5 = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7 \notin d'(n)\}$

	31	61		121	151	181	211	241	271		331	361	391	421	451	481	
2																	
3																	
5																	
7	37	67	97	127	157	187		247	277	307	337	367	397		457	487	517
11	41	71	101	131		191	221	251	281	311	341		401	431	461	491	521
13	43	73	103		163	193	223	253	283	313		373	403	433	463	493	523
17	47		107	137	167	197	227	257		317	347	377	407	437	467		527
19		79	109	139	169	199	229		289	319	349	379	409	439		499	529
23	53	83	113	143	173		233	263	293	323	353	383		443	473	503	533
29	59	89		149	179	209	239	269	299		359	389	419	449	479	509	

Analogamente, construímos L_6 explicitando – como primos – os números de L_5 menores que 121 e excluindo dela os elementos $11.11 = 121, 11.13 = 143$, *até, pela limitação da lista,* $11.47 = 517$.

Tabela 3.8: (Lista $L_6 = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7,11 \notin d'(n))$

	31	61			151	181	211	241	271		331	361	391	421		481	
2																	
3																	
5																	
7	37	67	97	127	157			247	277	307	337	367	397		457	487	
11	41	71	101	131		191	221	251	281	311			401	431	461	491	
13	43	73	103		163	193	223		283	313		373	403	433	463	493	523
17	47		107	137	167	197	227	257		317	347	377		437	467		527
19		79	109	139	169	199	229		289		349	379	409	439		499	529
23	53	83	113		173		233	263	293	323	353	383		443		503	533
29	59	89		149	179		239	269	299		359	389	419	449	479	509	

De maneira similar, enfatizando os $t \in L6; t < 169$ *e de L6 eliminando* $13.13 = 169, 13.17 = 221, ..., 13.41 = 533$*, construímos* L_7.

Tabela 3.9: (Lista $L_7 = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7,11,13 \notin d'(n)\}$

	31	61			151	181	211	241	271		331	361	391	421			
2																	
3																	
5																	
7	37	67	97	127	157				277	307	337	367	397		457	487	
11	41	71	101	131		191		251	281	311			401	431	461	491	
13	43	73	103		163	193	223		283	313		373		433	463	493	523
17	47		107	137	167	197	227	257		317	347			437	467		527
19		79	109	139		199	229		289		349	379	409	439		499	529
23	53	83	113		173		233	263	293	323	353	383		443		503	
29	59	89		149	179		239	269			359	389	419	449	479	509	

E, para L_8, teríamos

Tabela 3.10: (Lista $L_8 = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7,11,13 \notin d'(n)\}$

	31	61			151	181	211	241	271		331	361		421			
2																	
3																	
5																	
7	37	67	97	127	157				277	307	337	367	397		457	487	
11	41	71	101	131		191		251	281	311			401	431	461	491	
13	43	73	103		163	193	223		283	313		373		433	463		523
17	47		107	137	167	197	227	257		317	347			437	467		
19		79	109	139		199	229				349	379	409	439		499	529
23	53	83	113		173		233	263	293		353	383		443		503	
29	59	89		149	179		239	269			359	389	419	449	479	509	

E, finalmente, quando para encontrar L_9 *excluirmos convenientemente* 19.19 *e* 19.23*; e de* L_9 *eliminarmos* 23.23*, teremos a lista* L_{10}*, dos números primos menores que 540, segundo o Crivo de Erathóstenes.*

Tabela 3.11: (Lista $L_{10} = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7,11,13,17,19,23 \notin d'(n)\}$

	31	61			151	181	211	241	271		331			421			
2																	
3																	
5																	
7	37	67	97	127	157				277	307	337	367	397		457	487	
11	41	71	101	131		191		251	281	311			401	431	461	491	
13	43	73	103		163	193	223		283	313		373		433	463		523
17	47		107	137	167	197	227	257		317	347				467		
19		79	109	139		199	229				349	379	409	439		499	
23	53	83	113		173		233	263	293		353	383		443		503	
29	59	89		149	179		239	269			359	389	419	449	479	509	

Capítulo 4

As Matrizes de Erathóstenes

4.1 A Matriz A, de Erathóstenes:

Observe a lista L_10, e veja que – se já considerarmos inicialmente os números 2, 3 e 5 como primos – as linhas 2, 3 e 4 de L_10 podem ser também diretamente suprimidas, deixando então outra lista, a L_11, mais compacta e simples. Ao escrevê-la, percebe-se que em sua primeira coluna restaram apenas os números menores que α_3 e coprimos com ele.

Tabela 4.1: (Lista $L_{11} = \{n \in N_{540} \setminus \{0,1\}; 2,3,5,7,11,13,17,19,23 \notin d'(n)\}$)

	31	61			151	181	211	241	271		331			421			
7	37	67	97	127	157				277	307	337	367	397		457	487	
11	41	71	101	131		191		251	281	311			401	431	461	491	
13	43	73	103		163	193	223		283	313		373		433	463		523
17	47		107	137	167	197	227	257		317	347				467		
19		79	109	139		199	229				349	379	409	439		499	
23	53	83	113		173		233	263	293		353	383		443		503	
29	59	89		149	179		239	269			359	389	419	449	479	509	

Designaremos assim o conjunto $\Omega_3 = \{1,3,7,11,13,17,19,23,29\}$ como o dos resíduos coprimos de α_3. Para maior abrangência, generalizamos esse conceito com a definição que segue.

Definição 4.1. *Sejam p_n o n-ésimo número primo, $\alpha_n = \prod_{i=1}^{n}(p_i)$ o primordial de p_n, e $N_t = \{x \in \mathbb{N}; x < t\}$; denominamos $\Omega_n = \{x \in N_{\alpha_n}; mdc(x, \alpha_n) = 1\}$ o conjunto dos resíduos coprimos de α_n.*

Há duas observações importantes sobre Ω_n; ambas aqui apresentadas como proposições.

Proposição 4.1. *Considerando a função φ de Euler,*

$$\varphi(\alpha_n) = |\Omega_n|$$

Demonstração: *Segue diretamente da definição de $\varphi(\alpha_n)$.* ■

Atente para o fato de que a proposição 3.1 nos permite apresentar uma outra escrita para o conjunto Ω_n, enumerando-o segundo a função de Euler. Assim $\Omega_n = \{r_1, r_2, r_3, \cdots, r_{\varphi(\alpha_n)}\}$

Proposição 4.2. *Ω_n é o conjunto dos menores representantes das classes dos inversíveis mod(α_n)*

Demonstração: *A proposição 4 diz que [u] é inversível mod(k) somente quando mdc(u,k) = 1. Daí, tomando o menor natural u nesses termos, segue imediatamente, pela construção de Ω_n que $u \in \Omega_n$* ■

Observadas essas considerações, e notando a óbvia relação entre as linhas e colunas de L11 e o produto cartesiano $\alpha_3 N_{19} \times \Omega_3$, definimos a Matriz A de Erathóstenes nos seguintes termos.

Definição 4.2. *Dado $t \in \mathbb{N}$, denotamos a matriz $A_n = (a_{ij})_{t\varphi(\alpha_n)}$; onde$a_{ij} = \alpha_n.i + r_j$ como a Matriz A de Erathóstenes de Magnitude n.*

Claro está, pela própria construção de A_n, que seus elementos são justamente os candidatos a primos que são menores que $\alpha_n.t$, para um certo t; quando dos naturais menores que $\alpha_n.t$ retiramos os múltiplos dos primos que figuram na fatoração de α_n. A partir daí se desencadeia o procedimento de exclusão dos múltiplos dos outros primos maiores que p_n, segundo a seqüência de eliminações já vistas na secção anterior. As Ondas.

4.2 A Matriz C, de Erathóstenes:

O objetivo final desse estudo é explicitar quais dos elementos de An são primos e quais são compostos. Definiremos para tanto os conceitos de Onda de Exclusão e Símbolo de Erathóstenes, a partir dos quais serão caracterizados os elementos de A_n, segundo os conceitos de primos ou compostos. De fato, o Símbolo diz um pouco mais. Vejamos.

Definição 4.3. *Considerando A_n como a Matriz de Erathóstenes de Magnitude n, denotaremos por i-ésima Onda de Exclusão em A_n ao processo de eliminação dos múltiplos de p_{n+i}*

pertencentes a A_n. Por eliminar se pode entender descartar – caso há interesse em ver os elementos de A_n como uma lista – um subconjunto de $\mathbb{N}$; ou tornar nulo – quando se observa A_n estritamente como uma matriz.

Definição 4.4. *Considerando A_n como a Matriz de Erathóstenes de Magnitude n, denotaremos por Símbolo Menor de Erathóstenes a função*

$$S : A_n \longrightarrow \mathbb{N}$$
$$a_{ij} \longmapsto (s_{ij} = \begin{cases} 0 & se \quad a_{ij} = 1 \\ 1 & se \quad a_{ij} \ é \ primo \\ l & se \quad p_{l+n-1} = min[d'(a_{ij})] \end{cases}$$

Diremos também que s será o símbolo menor de a, ou simplesmente o símbolo de a e o utilizaremos para construir outro conceito: O de Matriz Simbólica. Nosso objetivo é, dada a matriz A_n, apresentar outra cujos elementos sejam os símbolos dos elementos de A_n. Sua definição é tão natural quanto o conceito.

Definição 4.5. *Considerando A_n como a Matriz de Erathóstenes de Magnitude n, com t colunas, denotaremos por Matriz Simbólica Completa de A_n a matriz*

$$S_n = (s_{ij})_{t\varphi(\alpha_n)}; \ onde s_{ij} = S(s_{ij})$$

A definição de S_n, de fato, é bem simples. È nosso objetivo construir um algoritmo para sua obtenção. Veja que S_n, posta dessa forma, é uma tábua de fatoração direta para os naturais menores que $(t+1).\varphi(n)$ e não divisíveis por nenhum primo menor que $p_(n+1)$. Sua construção direta, numa abordagem simplista, estaria condicionada ao emprego de tábuas de divisores para cada um de seus elementos. Uma aproximação menos ingênua poderia ser a utilização de tábuas de restos. Um avanço indubitavelmente significativo, mas – em se considerando listas maiores – ainda insuficiente.

O Crivo de Erathóstenes, ou mais especificamente, seus argumentos, permitem-nos prescindir dessas tábuas e chegar a S_n de forma indireta. De fato, a partir das Ondas de Exclusão em A_n, construiremos algoritmicamente duas matrizes: A primeira – a crivada – será obtida diretamente pelo efeito das ondas de exclusão em A_n; já para a outra – a simbólica incompleta – usaremos uma recorrência sobre os elementos da anterior. Ao final de cada onda,

esta matriz terá seus elementos associados diretamente os símbolos dos de A_n. Ao final do Crivo, teremos a Matriz Simbólica de A_n. Senão, vejamos:

Definição 4.6. *Considerando A_n como a Matriz de Erathóstenes de Magnitude n, com t colunas, e logo após a (k-1)-ésima Onda de Exclusão em A_n, denotaremos por Matriz Crivada de k-ésima Onda, ou k-ésima Crivada de A_n a matriz*

$$C_n^k = (c_{ij}^k)_{t\varphi(\alpha_n)};\ onde \begin{cases} c_{ij}^0 &= a_{ij} \\ c_{ij}^{t+1} &= \begin{cases} c_{ij}^t, & se \quad p_{t+n+1} \nmid c_{ij}^t \\ 0, & se \quad p_{t+n+1} \mid c_{ij}^t \end{cases} \end{cases}$$

Veja também que tal definição apresenta uma vantagem sobre a primeira, visto que verificar uma divisibilidade é mais simples que o cálculo do mdc. Ocorre ainda que o conceito de onda fica algebricamente implícito na definição por recorrência, além de sugerir – também implicitamente – uma recorrência para determinar S_n. Com efeito, pode-se pensar numa matriz de símbolos para cada C_n^k.

4.3 A Matriz S, de Erathóstenes:

Ótimo seria se pudéssemos, simples e diretamente, definir $S_n^k = (s_{ij}^k)_{t\varphi(\alpha_n)}$*;onde* $s_{ij}^k = S(c_i j)^k$*, como a matriz de símbolos para* C_n^k*. Infelizmente esse intento é mal fadado quando se percebe a dificuldade de calcular* $S(c_i j)^k$ *para alguns elementos de* S_n^k*. Tal contratempo se dá justamente por conta daqueles elementos de* A_n *que, sendo maiores que* $p_{(n+k+1)^2}$*, não foram excluídos pela k-ésima onda, nem pelas anteriores.*

Buscaremos nessa secção construir algoritmicamente a Matriz S_n *a partir da aplicação do Algoritmo de Erathóstenes no caso particular da Matriz* A_3*, e a respectiva construção de* S_3*. Para simplificar nossa notação, levando-se em consideração que todas as matrizes aqui envolvidas apresentam sempre magnitude 3, denotaremos, para esse estudo em particular, simplesmente* $\alpha_3 = \alpha$*,* $A = A_n$*,* $C^k = C_3^k$ *e* $S^k = S_3^k$*.*

Tome-se $t = 17$ *o número de colunas de* S_0 *e acrescente-se a ela, por questões didáticas, uma linha e uma coluna extras; onde se explicitam os valores de i e j e de* a_{ij}*. Ainda à guisa de inicialização consideraremos* $s_{ij}^0 = 1$*,exceto para* $s_{11}^0 = 0$*. Dessa forma temos, como Matriz inicial:*

Tabela 4.2: (Matriz S^0)

	0	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480
1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
23	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Note que, pela construção de A_n, já se tem uma lista inicial dos primos. Denominaremos essa lista de $\theta_{0n} = \{p_1, p_2, \ldots, p_n\}$, e, mesmo antes da primeira onda, é possível apresentar também o conjunto $\theta_{1n} = \{x \in A_n \setminus \{1\};\ x < p_{(n+1)^2}\}$ como uma outra lista mais longa de primos. Isso se deve ao fato de que nenhum dos elementos de θ_{1n} possui divisores não triviais, visto que os únicos possíveis são os elementos de θ_{0n}. Apresentamos a seguir uma definição mais generalizada dessas listas.

Definição 4.7. *Considerando A_n como a Matriz de Erathóstenes de Magnitude n, e na iminência da k-ésima Onda de Exclusão em A_n, denotaremos por k-ésima Lista Residual de A_n o conjunto $\theta_{kn} = \{x \in C_n^k \setminus \{1\};\ x < p_{(n+1)^2}\}$.*

Observe que as listas residuais resolvem um pequeno problema que poderia surgir na própria concepção do Crivo de Erathóstenes. È que, por definição, para efetivar a k-ésima onda de exclusão necessita-se do (k+n)-ésimo primo. Um investigador pouco atento poderia então questionar: Se, por esse método, encontrar primos depende de ondas de exclusão, que, por sua vez, precisam de primos para ser geradas, então já seria necessário conhecer $\mathbb{P}$ para gerá-lo. Parece um cachorro correndo atrás do próprio rabo.

Não é! De fato, para começar uma lista residual, faz-se necessário sim um subconjunto de $\mathbb{P}$; não o $\mathbb{P}$ completo, mas apenas seus primeiros elementos. Mais especificamente: os n primeiros primos para a geração do α_n, primordial de p_n. A partir daí, os próximos primos, maiores que p_n, serão obtidos não de $\mathbb{P}$, mas de uma lista residual.

Vem então a pergunta: Será que ao tomar elementos de uma dessas listas residuais, podemos ter certeza de estarmos realmente tomando números primos? E ainda mais: Podemos ter certeza de estarmos tomando todos os números primos? Em outras palavras: Será que as Listas Residuais geram $\mathbb{P}$?

A busca de uma resposta nos leva ao estudo de uma afirmação mais simples. Ela é apresentada na forma da próxima proposição.

Proposição 4.3.

$$\theta_{kn} = P_{p_{(n+k)^2}}$$

Demonstração:

Sejam p_{n+k}, o (n+k)- ésimo número primo, e $m \in N_{p_{(n+k)^2}}$.

Por construção,

$$m \in \theta_{kn} \iff m \in C_n^k \setminus \{0,1\} \iff mdc(\alpha_{n+k}, m) = 1 \iff m \in P_{p_{(n+k)^2}}$$

■

A Proposição 10 nos garante que todos os elementos da k-ésima Lista Residual de A_n são todos primos, e além disso, são todos os primos menores que $p_{(n+k)^2}$. Para uma generalização da Proposição 10, considere $\Theta = \bigcup_{i=1}^{\infty} \theta_{in}$, o conjunto de todos os números naturais que são elementos de alguma lista residual. A generalização que se busca é enunciada como o seguinte teorema.

Teorema 4.1.

$$\Theta = \mathbb{P}$$

Demonstração:

Usando diretamente a proposição 10, vemos que
($\Theta \subseteq \mathbb{P}$):

$$p \in \Theta \implies \exists k \in \mathbb{N}; p \in \theta_{kn} = P_{p_{(n+k)^2}} \subseteq \mathbb{P}$$

($\mathbb{P} \subseteq \Theta$):

$$p \in \mathbb{P} \implies \exists k \in \mathbb{N}; p \in P_{p_{(n+k)^2}} = \theta_{kn} \subseteq \Theta$$

■

No presente estudo particular, em conformidade com as notações simplificadas para o primordial de n, e para as matrizes abordadas, consideraremos $\theta_{k3} = \theta_k$.

Para a lista inicial de primos, temos $\theta_0 = \{2, 3, 5, 7, 11, 13, 17, 19, 23\}$ *e, de imediato,* $\theta_1 = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\} = \{x \in A_n;\ x < 49 = 7^2\}$. *Tal assertiva decorre da constatação de que uma vez apresentado o 7 como primeiro primo externo a* θ_0, *por construção de A, todos os elementos de A menores que* $7.7 = 49$, *exceto 2,3 e 5, são livres de divisibilidade por 2,3 e 5. Observe agora que 2,3 e 5 são justamente os primos menores que 7, logo aqueles cujos múltiplos se poderiam apresentar como divisores de algum elemento de* θ_1. *Os elementos de* θ_1 *são todos primos!*

Por outro lado, como já argumentado na secção anterior, quando se aplica a primeira onda de exclusão em C^0, *é desnecessário tentar excluir os múltiplos de 7 que possuam algum divisor externo a A, posto que eles já foram eliminados! Assim, para a construção da matriz S, resta apenas deixar indicados os símbolos de* θ_1 *como 1 e carregar com 2 os múltiplos de 7 cujos divisores se encontram na Matriz* C^0.

É a esse procedimento que denominamos Primeira Onda de Exclusão em S, ou varredura, e o que se segue é a matriz S^1, *dos símbolos de* C^1, *com seus elementos assim definidos:*

$$s_{ij}^1 = \begin{cases} s_{ij}^0, & se \quad 7 \nmid c_{ij}^1 \\ 2, & se \quad 7 \mid c_{ij}^1 \end{cases}$$

Visualmente temos

Tabela 4.3: (Matriz S^1)

	0	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480
1	0	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1
7	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1
11	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1
13	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1
17	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2
19	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1
23	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1
29	1	1	1	2	1	1	1	1	1	1	2	1	1	1	1	1	1

Concluímos também que $\theta_2 = \{x \in C^1;\ x < 121 = 11^2 = (p_5)^2\} = P_{121}$.

Antes de passarmos à segunda onda, vejamos duas considerações.

Primeiro note que, para toda linha de A, a quantidade de colunas entre dois múltiplos de 7 é também um múltiplo de 7. Como a matriz ora investigada é finita, é razoável questionar sua generalização. Esta, de fato ocorre; e é aqui apresentada como nossa próxima proposição.

Proposição 4.4. *Sejam* $p \in \mathbb{P}$, *e* $a_{ij} \in A_n$.

Caso exista $a_{(i+p)j}$, *tem-se que:* $\quad p \mid a_{ij} \iff p \mid a_{(i+p)j}$

Demonstração:

$(\Rightarrow)$:

Segue diretamente da proposição 12 e da construção de A_n.

$(\Leftarrow)$:

$p \mid a_{(i+p)j} \Longrightarrow p \mid (\alpha_n.(i+p) + r_j)$, *pela construção de* A_n

$\Longrightarrow p \mid (\alpha_n.i + r_j)$, *pela proposição 3*

■

Por outro lado, durante a segunda onda, chegaremos ao número $539 = 72.11$, *que deve, por definição, ter o símbolo 2, e já o é assim identificado em* S^1. *Vê-se então que não se pode fazer como na primeira onda e simplesmente atribuir 3 aos símbolos dos múltiplos de 11, pois alguns deles também serão múltiplos de 7, e já foram catalogados como tal.*

Dessa feita, em nosso algoritmo, por coerência para com a definição de símbolo, apenas os elementos de S^1 *com símbolo 1 receberão símbolo 3 em* C^2. *Os demais permanecerão tal como se encontravam em* S^1. *A matriz* S^2 *fica assim definida*

$$S^2 = (s^2_{ij})_{t\varphi(\alpha_n)};\ onde \begin{cases} s^1_{ij}, & se \quad (s^1_{ij} \neq 1) \vee (11 \nmid c^2_{ij}) \\ 3, & se \quad (s^1_{ij} = 1) \wedge (11 \mid c^2_{ij}) \end{cases}$$

Assim, após a segunda onda (a exclusão dos múltiplos de 11, a partir de 121), visualizamos S^2 como a matriz abaixo

Tabela 4.4: (Matriz S^2)

	0	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480
1		1	1	2	3	1	1	1	1	1	2	1	1	1	1	3	1
7	1	1	1	1	1	1	3	2	1	1	1	1	1	1	2	1	1
11	1	1	1	1	1	2	1	1	1	1	1	3	2	1	1	1	1
13	1	1	1	1	2	1	1	1	3	1	1	2	1	1	1	1	1
17	1	1	2	1	1	1	1	1	1	2	1	1	1	3	1	1	2
19	1	2	1	1	1	1	1	1	2	1	3	1	1	1	1	2	1
23	1	1	1	1	3	1	2	1	1	1	1	1	1	2	1	3	1
29	1	1	1	2	1	1	3	1	1	1	2	1	1	1	1	1	1

Sem surpresa alguma, durante a terceira onda, deparamo-nos com a mesma situação da onda anterior. Existem números, acima de 13^2, que já foram excluídos. Pelos mesmos argumentos de antes, a matriz S^3 fica assim definida

$$S^3 = (s^3_{ij})_{t\varphi(\alpha_n)};\ onde \begin{cases} s^3_{ij}, & se \quad (s^2_{ij} \neq 1) \vee (p_6 = 13 \nmid c^3_{ij}) \\ 3, & se \quad (s^2_{ij} = 1) \wedge (p_6 = 13 \mid c^3_{ij}) \end{cases}$$

Daí, a terceira onda fornece

Tabela 4.5: (Matriz S^3)

	0	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480
1		1	1	2	3	1	1	1	1	1	2	1	1	1	1	3	4
7	1	1	1	1	1	1	3	2	4	1	1	1	1	1	2	1	1
11	1	1	1	1	1	2	1	4	1	1	1	3	2	1	1	1	1
13	1	1	1	1	2	1	1	1	3	1	1	2	1	4	1	1	1
17	1	1	2	1	1	1	1	1	1	2	1	1	4	3	1	1	2
19	1	2	1	1	1	4	1	1	2	1	3	1	1	1	1	2	1
23	1	1	1	1	3	1	2	1	1	1	1	1	1	2	1	3	1
29	1	1	1	2	1	1	3	1	1	4	2	1	1	1	1	1	1

Notamos aqui que os argumentos usados para definir as simbólicas até agora sugerem fortemente uma fórmula geral de recorrência para S_n^k. Com efeito, tais considerações podem ser algoritmicamente generalizadas para a definição abaixo.

Definição 4.8. *Considerando C_n^k como a k-ésima Crivada de A_n, com t colunas, denotaremos por Matriz Simbólica C_n^k a matriz*

$$S_n^k = (s_{ij}^k)_{t\varphi(\alpha_n)};\ onde\ s_{ij}^k = \begin{cases} s_{ij}^0 = \begin{cases} 0, & se \quad i = j = 1 \\ 1, & se \quad i \neq 1 \neq j \end{cases} \\ s_{ij}^{t+1} = \begin{cases} s_{ij}^t, & se \quad (s_{ij}^t \neq 1) \vee (p_{l+n+1} \nmid c_{ij}^t) \\ 3, & se \quad (s_{ij}^t = 1) \wedge (p_{l+n+1} \mid c_{ij}^t) \end{cases} \end{cases}$$

Dessa forma, após a 6ª onda de exclusão, finalizamos nosso algoritmo e apresentamos $S = S_3^6$, a Matriz Simbólica de $A = A_3$.

Tabela 4.6: (Matriz S^6)

	0	30	60	90	120	150	180	210	240	270	300	330	360	390	420	450	480
1		1	1	2	3	1	1	1	1	1	2	1	6	5	1	3	4
7	1	1	1	1	1	1	3	2	4	1	1	1	1	1	2	1	1
11	1	1	1	1	1	2	1	4	1	1	1	3	2	1	1	1	1
13	1	1	1	1	2	1	1	1	3	1	1	2	1	4	1	1	5
17	1	1	2	1	1	1	1	1	1	2	1	1	4	3	6	1	2
19	1	2	1	1	1	4	1	1	2	5	3	1	1	1	1	2	1
23	1	1	1	1	3	1	2	1	1	1	5	1	1	2	1	3	1
29	1	1	1	2	1	1	3	1	1	4	2	1	1	1	1	1	1

Referências Bibliográficas

- *HEFEZ, Abramo. Elementos de Aritmética. 2ª Ed. Rio de Janeiro: SBM, 2011.*
- *SANTOS, José Plínio de Oliveira. Introdução a Teoria dos Núumeros. 3ª Ed. Rio de Janeiro: IMPA, 2009.*