UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO (UFRRJ)
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL (PROFMAT)

DISSERTAÇÃO

NÚMEROS PRIMOS E CRIPTOGRAFIA: DA RELAÇÃO COM A EDUCAÇÃO AO SISTEMA RSA

KELLY CRISTINA SANTOS ALEXANDRE DE LIMA DAINEZE

2013

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL (PROFMAT)

NÚMEROS PRIMOS E CRIPTOGRAFIA: DA RELAÇÃO COM A EDUCAÇÃO AO SISTEMA RSA

KELLY CRISTINA SANTOS ALEXANDRE DE LIMA DAINEZE

Sob a Orientação do Professor
Douglas Monsôres de Melo Santos

Dissertação submetida como requisito parcial para obtenção do grau de **Mestre em Matemática,** no Programa de Mestrado Profissional em Matemática em Rede Nacional.

Seropédica, RJ
Abril/2013

UNIVERSIDADE FEDERAL RURAL DO RIO DE JANEIRO
INSTITUTO DE CIÊNCIAS EXATAS
CURSO DE PÓS-GRADUAÇÃO EM MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL – PROFMAT

KELLY CRISTINA SANTOS ALEXANDRE DE LIMA DAINEZE

Dissertação submetida como requisito parcial para obtenção do grau de **Mestre**, no curso de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, área de Concentração em Matemática.

DISSERTAÇÃO APROVADA EM 15/04/2013

Douglas Monsôres de Melo Santos

Prof. Dr. Douglas Monsôres de Melo Santos – UFRRJ
(Orientador)

André Luiz Martins Pereira

Prof. Dr. André Luiz Martins Pereira – UFRRJ

Edilaine Ervilha Nobili

Profa. Dra. Edilaine Ervilha Nobili – UFF

Ao triângulo que sustenta minha vida: Julia (minha pequena), Diogo (meu amor) e Vânia (a melhor mãe do mundo)...

AGRADECIMENTOS

A Deus, que me permitiu chegar tão longe e me amparou em todos os momentos difíceis.

À minha preciosa filha Julia, que mesmo tão pequena, foi o incentivo para concluir este trabalho. E ao meu amado esposo Diogo, que sempre está ao meu lado, me apoiando, me ajudando, me encorajando. Obrigada por terem compreendido a minha ausência em muitos momentos.

À minha mãe Vania, que mesmo depois de ter criado a filha, assistiu aulas de matemática comigo, logo após o nascimento da minha pequena, para que eu não perdesse aulas e pudesse amamentar.

À minha sogra (segunda mãe) Marly, por cuidar de tudo para que eu pudesse estudar.

Ao meu pai Joel, que lutou muito para propiciar a formação que alcancei.

Ao meu orientador Douglas: pela paciência, pela força, pela ajuda. E, também, a sua esposa, por abrir as portas de sua casa para que pudéssemos discutir o trabalho nos fins de semana.

Aos colegas de curso pela amizade, pelo carinho, pelas risadas, por fazer nossos sábados mais divertidos e, é claro, pela troca de experiências e conhecimentos. Em especial, ao nosso representante, Jorge, que manteve este grupo unido e perseverante.

Aos colegas professores por acreditarem que conseguiríamos.

Aos amigos e familiares, que nestes dois anos, desculparam o meu sumiço.

E a todos aqueles, que com suas orações e pensamentos, estavam torcendo para o meu sucesso.

"Nunca será um verdadeiro matemático aquele
que não for um pouco de poeta".
(Karl Weierstrass)

RESUMO

Este trabalho visa estabelecer uma discussão sobre os conceitos envolvendo criptografia, através de sua aplicação dos números primos, e as possíveis relações com a educação. O critério utilizado para optar por este ou aquele sistema criptográfico foi subjetivo; muitos sistemas não foram abordados, mesmo contendo relações intrínsecas com a temática. A necessidade de troca de informações sigilosas instigou o surgimento da arte de codificar mensagens; a rede virtual e seus milhões de usuários apontou a necessidade de um sistema utilizando chave pública e, ao mesmo tempo, seguro. O RSA veio para suprir as necessidades de uma sociedade que, cada vez mais, realiza suas transações bancárias, comerciais e sociais via web. Uma questão que carece ser pensada diz respeito à maneira como os conteúdos da chamada Teoria dos Números têm sido apresentados e trabalhados na escola. Algo que é tradicionalmente consagrado como enfadonho e sem sentido. A arte da criptografia traz consigo temas relevantes para se pensar nos conceitos matemáticos, propiciando um ensino por Resolução de Problemas. Os caminhos percorridos, a partir daí, propiciam experiências significativas para o sujeito, numa educação emancipatória, como propuseram Adorno e Rancière. As atividades sugeridas a partir de diferentes sistemas de codificação pretendem instigar os educandos e os educadores a repensar as diferentes possibilidades de um problema, suscitando a sensibilidade do pensar e de buscar maneiras para resolver e não repetir os mecanismos de um algoritmo matemático, para que o ato educativo perpasse as circunstâncias complexas que se apresentam na atualidade.

Palavras-chave: Criptografia. Números Primos. RSA.

ABSTRACT

This study aims to provide a discussion of the concepts involving encryption, through its application of prime numbers, and possible links with education. The criterion used to choose one or other cryptographic system was subjective, many systems have not been addressed, even containing intrinsic relations with the theme. The necessity to exchange confidential information urged the rise of art to encode messages, the virtual network and its millions of users identified the need for a system using public key and at the same time, safe. RSA came to supply the needs of a society that increasingly conducts its banking, commercial and social web. One issue which needs to be thought concerning the way how the contents of the called Number Theory have been presented and learned at school. Something that is traditionally consecrated as boring and meaningless. The art of cryptography brings relevant topics to think about mathematical concepts, providing an education for Troubleshooting. The paths taken, thereafter, provide meaningful experiences for the subject, in emancipatory education, as suggested by Adorno and Rancière. Suggested activities from different coding systems intend to instigate students and educators to reconsider the different possibilities of a problem, raising the sensitivity of thinking and find ways to solve and not repeat the mechanisms of a mathematical algorithm, so that the educational act passes by the complex circumstances that present themselves today.

Keywords: Cryptography. Prime Numbers. RSA.

LISTA DE TABELAS

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

1.1 Apresentação

Os Números Primos são parte importante da chamada Teoria dos Números; a eles estão agregados grandes problemas matemáticos que percorrem séculos. A Criptografia é um estudo de métodos, cada vez mais sofisticados, para enviar mensagens secretas.

Este trabalho consiste em um estudo sobre os números primos, trazendo teoremas e resultados importantes a eles relacionados e questionando a maneira como são apresentados na escola. Os diferentes métodos de codificar uma mensagem também fazem parte desse trabalho, onde se propõe um ensino pela resolução de problemas. Apresenta-se, inclusive, a relação entre as duas temáticas, resultando no sistema RSA.

Os números têm um papel significativo na Matemática e na História da Matemática, eles têm também grande importância na Matemática escolar nos anos iniciais, principalmente os números naturais. Questões envolvendo os números primos se colocam a todo tempo na Matemática: o que é um número primo? Quantos primos existem? Como testar a primalidade de um número?

Dessa teia de reflexões que surgem sobre a temática resultou este texto, que tem como proposta metodológica a pesquisa bibliográfica sobre a Teoria dos Números e Criptografia e o diálogo entre estes conhecimentos e as aulas de Matemática. Pretendeu-se apresentar uma síntese dos conceitos envolvendo números primos, pensar como tem se dado o ensino dos números primos na educação básica, compreender o sistema de criptografia RSA como uma aplicação dos números primos e criar atividades de criptografia para serem realizadas na sala de aula.

Este trabalho pretende contribuir para uma reflexão sobre as transformações necessárias no modo como as atividades são apresentadas aos alunos, abordando questões relacionadas ao ensino de números primos e de problemas envolvendo a criptografia. Estas discussões trazem ao debate as dificuldades na qualidade da educação matemática, já mostradas pelos resultados dos diferentes sistemas de avaliações, ou seja, aulas que estimulem a reflexão, a crítica e o aprendizado mais amplo do aluno.

1.2 Organização da Dissertação

Para melhor compreender o presente se fez necessário conhecer as peculiaridades do passado. Assim, o segundo capítulo deste trabalho, *Os Números Naturais e os Números Primos*, traz uma retrospectiva histórica de como surgiram os números e a evolução nos estudos teóricos sobre números primos; traz, ainda, um compêndio sobre resultados importantes envolvendo estes números e uma discussão sobre o lugar que os números primos ocupam na matemática escolar de hoje.

Também se faz necessário compreender como se originou a Criptografia. *Teoria dos Números e Criptografia* apresenta como diversos momentos e movimentos influenciaram e desenvolveram esta área: as cifras da Antiguidade, a cifra de César, dos Templários, até o método RSA. Um breve histórico dos sistemas de codificação mostra que a segurança de um método depende do quão difícil é quebra-lo; a análises de frequência permite codificar

rapidamente determinadas cifras. Assim, este mesmo capítulo traz aspectos particulares do RSA, explicando seu funcionamento e o porquê de sua segurança, baseada na impossibilidade de se fatorar primos muito grandes.

Em *Educação Matemática como formação para o Pensar*, são apresentadas as reflexões dos teóricos Rancière e Adorno, sobre aspectos que, contemplados no ensino de matemática, podem servir para auxiliar um processo de ensino-aprendizagem que ao invés de focar conteúdos, vise resolução de problemas, processos históricos, troca de experiências, resultando em uma educação que forma cidadãos críticos e emancipados.

Atividades envolvendo cifras antigas e sistema Braille, relacionado criptografia com funções e matrizes e apresentando aos alunos da Educação Básica o sistema RSA são tratadas em *Criptografia na Escola*. Uma experiência com "criptografia intuitiva" feita em uma turma da rede municipal de ensino do Rio de Janeiro aparece neste capítulo.

A revisão das raízes conteudistas da escola depende de uma revolução conceitual e metodológica capaz de integrar educação e ensino, desenvolvimento e aprendizagem. Este trabalho se propõe a situar historicamente a criptografia, verificando como se relaciona com a Teoria dos Números e repensando em novas práticas para a sala de aula, onde diferentes conteúdos são interligados.

CAPÍTULO 2 - OS NÚMEROS NATURAIS E OS NÚMEROS PRIMOS

O conceito de número desenvolveu-se antes da escrita, de modo que, não é possível precisar como e quando isso aconteceu. A representação dos números que utilizamos hoje foi encontrada em colunas de pedras na Índia que datam de 250 a.C. Os números primos foram estudados pelos antigos matemáticos gregos que eliminavam o 1 do conjunto dos primos porque não o consideravam como número. Eratóstenes (276 a.C. – 196 a.C.) nascido em Cirene, cidade grega ao norte da África, que escreveu sobre matemática, astronomia, geografia, história e fez críticas literárias, desenvolveu o primeiro método sistemático para verificar se um número é primo e muitos outros matemáticos desenvolveram teoremas relacionados a estes números tão enigmáticos.

2.1 A História dos Números

Os processos de contagem são muito antigos. As primeiras formas de contagem associavam a quantidade de objetos com os dedos das mãos, dos pés, pedras. As técnicas primitivas de contagem possibilitaram ao homem praticar a aritmética mesmo sem saber o que é o número. O homem primitivo sabia somente o que representava 'muitos':

> No pastoreio, o pastor, usava várias formas para controlar o seu rebanho. Pela manhã, ele soltava os seus carneiros e analisava ao final da tarde, se algum tinha sido roubado, fugido, se perdido do rebanho ou se havia sido acrescentado um novo carneiro. Assim eles tinham a correspondência um a um, onde cada carneiro correspondia a uma pedrinha que era armazenada em um saco. No caso das pedrinhas, cada animal que saia para o pasto de manhã correspondia a uma pedra que era guardada em um saco de couro. No final do dia, quando os animais voltavam do pasto, era feita a correspondência inversa, onde, para cada animal que retornava, era retirada uma pedra do saco. Se no final do dia sobrasse alguma pedra, é porque faltava algum dos animais e se algum fosse acrescentado ao rebanho (no caso de nascimento de algum carneiro), era só acrescentar mais uma pedra ao saco. (GONGORA, 2005).

Com a necessidade de contar grandes quantidades, surgiu a representação destas contagens por símbolos. Os primeiros sistemas de numeração, em sua maioria, tinham por regra formar os numerais pela repetição de símbolos básicos e pela soma de seus valores. De acordo com Ifrah (2005), a região do planeta onde aconteceu o desenvolvimento do uso dos números está nas proximidades das margens do mediterrâneo e no Oriente Médio, onde se localizavam as civilizações dos sumérios, babilônios, egípcios, gregos, romanos, hebreus e hindus.

A ideia de base para um sistema de numeração (ou contagem) surgiu da necessidade de efetuar contagens mais extensas e elaboradas. O zero só foi inserido tempos depois e o sistema posicional estabeleceu o que hoje conhecemos como valor absoluto e valor relativo de um número.

Devido à grande importância na composição dos números inteiros, os números primos sempre foram objeto de estudo entre matemáticos. É possível que as primeiras descobertas sobre estes instigantes números tenham sido feitas pela Escola Pitagórica, que já entendia a ideia de primalidade e começava o estudo dos números perfeitos e dos números amigáveis.

Sautoy (2007, p.13) escreveu que "os primos são as pérolas que adornam a vastidão infinita do universo de números que os matemáticos exploraram ao longo dos séculos". Já em 300 a. C., Euclides trouxe muitos resultados importantes sobre números primos que já tinham sido provados por diferentes estudiosos. No livro IX aparece a prova de que existem infinitos

números primos (Proposição 20: Existem mais números primos que qualquer quantidade dada de números primos) e uma demonstração parcial do Teorema Fundamental da Aritmética (Proposição 14: Se um número é o menor que é medido por números primos, então ele não é medido por nenhum outro primo exceto aqueles que o mediam desde o princípio). Pode-se dizer que os números primos são as partículas que formam os demais números.

Segundo Gundlach, (1992, p. 49), Euclides deu uma das primeiras contribuições significativas à teoria dos números primos ao provar que o conjunto destes números é infinito; aliás, a demonstração desse fato é a primeira demonstração por redução ao absurdo que se tem notícia. O Crivo de Eratóstenes, apresentado em 200 a.C., é um dos primeiros algoritmos para calcular números primos. Fermat, no início do século XVII, provou que todo o número primo da forma 4n+1 pode ser escrito de um só modo como soma de dois quadrados e provou o que é hoje conhecido como Pequeno Teorema de Fermat (cf. Teorema 1.2.3).

Euler tem uma grande importância na Teoria dos Números Primos, pois desdobrou o Pequeno Teorema de Fermat e introduziu a função-fi de Euler. Legendre e Gauss fizeram cálculos sobre a densidade dos números primos e chegaram à conjectura de que para um número natural n grande a densidade de números primos perto desse mesmo n é semelhante a $1/\log n$, conhecida como o Teorema dos Números Primos.

Os números primos suscitam uma série de questões interessantes e, por isso, aparecem em vários problemas ilustres ainda sem solução. Um deles é a chamada hipótese de Riemann (cf. def. 1.2.3), um dos sete problemas do milênio, considerado atualmente o mais importante problema da Matemática Pura. Um outro, é a Conjectura de Goldbach (cf. def. 1.2.2).

2.2 Resultados sobre Números Primos

A pergunta que se faz necessária é: afinal, o que é um número primo? Dizemos que um natural *p* maior que 1 é dito primo quando é impossível escrever *p* como o produto de dois números naturais *a* e *b* com $a > 1$ e $b > 1$. Consequentemente, os únicos divisores naturais de um número primo são a unidade e ele próprio.

Uma das primeiras questões interessantes que se pode notar sobre números primos é a falta de regularidade na distribuição de sua sequência, podemos ter primos muito próximos, mais afastados e outros muito distantes dentro de um intervalo, como 2 e 3 (que são consecutivos) ou 577 e 587 (que distam dez unidades, sem nenhum primo entre eles). Outro ponto curioso é a existência de intervalos, tão grande quanto quisermos, onde não existem números primos, os chamados "desertos" de números primos. Para encontrarmos estes "desertos" basta tomarmos um número natural *n* suficientemente grande e considerarmos os números $n! + 2, n! + 3, \ldots, n! + n$. O intervalo $[n! + 2, n! + n]$ possui apenas números compostos e quanto maior o *n* escolhido, maior o intervalo.

Antes de descrevermos como estes números estão sendo abordados na escola, estabeleceremos alguns resultados que serão usados para entender os mistérios que envolvem estes números e, também, para explicar como o código RSA (um sistema criptográfico que utiliza números primos) funciona. As demonstrações desses resultados são baseadas naquelas encontradas em Hefez (2006) e em Coutinho (2005).

O primeiro resultado será utilizado na demonstração do teorema fundamental da aritmética.

Proposição 2.2.1 (Lema de Euclides): *Sejam* $a, b, p, \in \mathbb{N}$*, com p primo. Se* $p|a.b$*, então* $p|a$ *ou* $p|b$*.*

Demonstração: É suficiente provar que se $p|a.b$ e $p \nmid a$ então $p|b$. Suponhamos que p não divide a, daí $mdc(a,p) = 1$. Pelo Algoritmo de Euclides estendido, existem $m, n \in \mathbb{N}$ tais que

$$a.m + p.n = 1$$

e

$$(a.b).m + p.(b.n) = b$$

Como $p|a.b$ (pela hipótese) e $p|p$, então $p|b$. ■

Teorema 2.2.1 (Teorema Fundamental da Aritmética): *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos*.

Demonstração: Usaremos o Segundo Princípio da Indução para demonstrarmos o teorema.

(Existência) Se $n = 2$ verifica-se que o resultado é valido, pois 2 é primo. Suponhamos a afirmação verdadeira para todo k tal que $2 \leq k < n$ e provemos que vale para n. Se n é primo, então a afirmação é valida. Seja n um numero natural composto, daí existem $n_1, n_2 \in \mathbb{N}$, tais que $n = n_1.n_2$, então $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, existem primos $p_1, p_2, \ldots, p_r, q_1, q_2, \ldots, q_s$ tais que $n_1 = p_1.p_2.\ldots.p_r$ e $n_2 = q_1.q_2.\ldots.q_s$. Logo, $n = p_1.p_2.\ldots.p_r.q_1.q_2.\ldots.q_s$, ou seja, n é produto de números primos.

(Unicidade) Seja $n = r_1.r_2, \ldots, r_i = s_1, s_2, \ldots, s_j$, com $r_1.r_2, \ldots, r_i, s_1, s_2, \ldots, s_j$ primos. Então $r_1|s_1.s_2 \ldots s_j$, daí, pela proposição 1.2.1, $r_1|s_m$, para algum $1 \leq m \leq j$. Podemos supor, sem perda de generalidade que $m = 1$. Como r_1 e s_1 são primos, $r_1 = s_1$. Cancelando r_1e s_1 na igualdade $r_1.r_2, \ldots.r_i = s_1.s_2.\ldots.s_j$, segue que $r_2 \ldots r_i = s_2 \ldots s_j$. Repetindo esse procedimento, temos que $i = j$ e os r_k e s_m são iguais, aos pares. ■

Teorema 2.2.2: *Existem Infinitos Números Primos.*

Demonstração: Suponha, por absurdo, que exista um número finito de primos $p_1, p_2, \ldots, p_r$.

Tomemos o numero natural $n = p_1, p_2, \ldots, p_r + 1$. Pelo Teorema Fundamental da Aritmética, n possui, ao menos, um fator primo p, que deve ser algum p_i, com $1 \leq i \leq r$. $p_i|p_1 . p_2 \ldots p_r$ e $p_i|n$, logo $p_i|1$, o que é absurdo, pois 1 não tem divisores maiores que ele mesmo. Logo, existem infinitos primos. ■

Método 2.2.1 (Crivo de Eratóstenes):

Utilizado para encontrar os números primos ou determinar se um número é primo, baseia-se na eliminação dos múltiplos dos primos anteriores ao número que se deseja caracterizar como primo ou não. Para simplificar o método, basta eliminar os múltiplos dos números primos cujo quadrado não supere o número que desejamos testar a primalidade, com base no seguinte resultado.

Proposição 2.2.2: *Se um número natural $n > 1$ não é divisível por nenhum número primo p tal que $p^2 \leq n$, então ele é primo.*

Demonstração: Suponha, para um absurdo, que n não seja divisível por nenhum primo p, com $p^2 \leq n$. Seja q o menor primo que divide n, então $n = q.k$ e $q < k$. Daí, $q^2 = q.q \leq q.k = n \Longrightarrow q^2 \leq n$, o que é absurdo, pois n é divisível por um primo q tal que $q^2 \leq n$. Logo, n é primo. ■

Como exemplo, vamos utilizar o Crivo de Eratóstenes para determinar todos os números primos menores que 197. Construímos uma tabela contendo todos os números naturais de 2 a 197. Começando pelo primeiro número (o número 2), descartamos da tabela todos os múltiplos de 2 que são maiores que 2. Após fazer esse descarte, o próximo número da lista após o 2 (o número 3, no caso) será primo. Repetimos o processo removendo da tabela os múltiplos de 3 que são maiores que 3. Procedemos dessa forma até realizar todas as remoções possíveis. Os números que não foram descartados da tabela são os primos menores ou iguais a 197. Note que, pela Proposição 2.2.2, caso desejássemos apenas saber se 197 é primo, seria necessário eliminar apenas os múltiplos dos números primos ≤ 13, pois o quadrado do primo 17 supera 197.

	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~~	~~171~~	~~172~~	173	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	179	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~	191	~~192~~	193	~~194~~	~~195~~
~~196~~	197													

Lema 2.2.1: Seja p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.

Demonstração: Se $i = 1$, temos que $\binom{p}{1} = p$ e p/p. Tomemos então $1 < i < p$. Como $\binom{p}{i} = \frac{p!}{i!(p-i)!} = \frac{p.(p-1)\ldots(p+1-i).(p-i)}{i!(p-i)!} = \frac{p.(p-1).\ \ldots\ .(p+1-i)}{i!}$

Temos que $i!/p(p-1)\ldots(p+1-i)$. Mas, o máximo divisor comum entre $i!$ e p é 1; daí $i!\,|(p-1)\ldots(p+1-i)$. Logo, $\binom{p}{i} = p.n$, onde $n = \frac{(p-1).\ \ldots.(p+1-i)}{i!}$, e $p|\binom{p}{i}$. ■

Teorema 2.2.3 (Pequeno Teorema de Fermat): *Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{N}$.*

Demonstração: Utilizemos o principio da indução sobre a. Para $a = 1$ temos $a^p - a = 0$, daí $p|0$, que é verdade.

Suponha que o resultado é valido para a e provemos para $a + 1$. Temos:

$$(a+1)^p - (a+1) = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1 - (a+1)$$

$$= \quad a^p - a + \binom{p}{i}a^{p-1} + \binom{p}{2}a^{p-2} + \binom{p}{p-1}a$$

Pela hipótese de indução, $p/a^p - a$ e pelo lema acima $p/\binom{p}{i}$, $0 < i < p-1$, daí $p/(a+1)^p - (a+1)$. ■

Corolário: *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração: Temos pelo Pequeno Teorema de Fermat que $p|a^p - a$, então $p|a(a^{p-1} - 1)$. Pela hipótese $p \nmid a$, então $p|a^{p-1} - 1$. ■

Conjectura de Goldbach: *Todo número inteiro par maior que 2 pode ser representado como a soma de dois números primos.*

A Conjectura de Goldbach foi pela primeira vez enunciada numa carta que Christian Goldbach enviou a Eüler no dia 7 de Julho de 1742. Até hoje, diversos matemáticos tentam demonstrá-la, mas apenas conseguiu-se verificar sua validade para números da ordem de 10 elevado a 14. (CABETTE et al, 2008)

Hipótese de Riemann: Em 1859, Bernhard Riemann, entregou à Academia das Ciências de Berli um relatório (de apenas oito páginas) que tinha por título *Sobre o número de números primos que não excedem uma grandeza dada*. É ali que surge a hipótese de Riemann, que é provavelmente o mais famoso problema em aberto da Matemática.

A Hipótese de Riemann busca entender o comportamento dos números primos, através da função zeta, uma função proposta por Euler

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{\substack{p \geq 2, \\ p\ primo}}^{\infty} \frac{p^s}{p^s - 1}$$

Riemman trabalhou na função Zeta como uma função de uma variável complexa z. Neste caso, se $Re(z) \geq 1$, a função não possui zeros; se $Re(z) \leq 0$, ela possui os zeros triviais $-2, -4, -6, \ldots$ e se $0 < Re(z) < 1$, existem infinitos zeros não triviais. Segundo a hipótese de Riemann, todos os zeros não triviais estariam sobre a reta $Re(z) = \frac{1}{2}$. A demonstração da hipótese de Riemann poderia revelar a maneira como os primos se distribuem (veja ALVITES, 2012).

Definição 2.2.2 (Função φ de Euler): *A função φ de Euler de um natural n é definida como o número de naturais menores ou iguais a n que são relativamente primos com n, ou seja,*

$$\varphi(n) \coloneqq \#\{1 \leq m \leq n / mdc(m,n) = 1\}.$$

Quando n é primo, $\varphi(n) = n - 1$.

Proposição 2.2.3: *Sejam $a, b \in \mathbb{N}$, primos e distintos. Então $\varphi(ab) = \varphi(a)\varphi(b)$.*

Demonstração: Temos que $\varphi(p) = (p-1)$ e $\varphi(q) = (q-1)$, pois p e q são primos. Faça, sem perda de generalidade, $p < q$. Considere o conjunto dos naturais que vão de 1 até $p.q$ e dele vamos descartar todos os números que são divisíveis por p e os que são divisíveis por q.

Os números divisíveis por p são: $p.1, p.2, \dots, p.q$. E os divisíveis por q são: $q.1, q.2, \dots, p.q$. Observe que $p.q$ aparece nos dois conjuntos, então devemos repor um elemento.

Daí:

$$\varphi(p.q) = p.q - p - q + 1 = p(q-1) - (q-1) = (p-1)(q-1) = \varphi(p)\varphi(q).$$

■

Observação 2.2.1: A Proposição 2.2.3 é válida, mais geralmente, para dois números naturais a e b que sejam primos entre si. Para a demonstração dessa versão mais geral, veja Hefez (2006, p.132, Prop.10.1.3).

Definição 2.2.3: Congruência módulo *m*

Seja m um natural diferente de zero, os naturais a e b são congruentes módulo m ($a \equiv b \mod m$) *se os restos da divisão euclidiana por m são iguais.*

Teorema 2.2.4 (Euler): *Se n é um inteiro positivo e a é um inteiro tal que $mdc(a,n) = 1$, então $a^{\varphi(n)} \equiv 1 \mod n$.*

Demonstração: Temos que todo inteiro b que é primo com n tem um inverso módulo n. De fato, pelo Algoritmo de Euclides Estendido, se $mdc(b,n) = 1$, então existem inteiros s e t tais que $sb + tn = 1$; assim, $1 - sb = tn \equiv 0 \mod n$, ou seja, $sb \equiv 1 \mod n$, como queríamos.

Sejam $1 = a_1 < a_2 < \cdots < a_{\varphi(n)} \leq n-1$ os $\varphi(n)$ inteiros entre 1 e n que tem mdc 1 com n. Pelo Teorema Fundamental da Aritmética, $mdc(a_1.a_2 \dots a_{\varphi(n)}, n) = 1$. Daí, $a_1.a_2 \dots a_{\varphi(n)}$ tem inverso módulo n, que denotaremos por α.

Seja agora a um inteiro qualquer com $mdc(a,n) = 1$. Para cada $i = 1, 2, \dots, \varphi(n)$, temos que $mdc(a.a_i, n) = 1$. Segue que $a.a_i \equiv a_j \mod n$ para algum j. Além disso, se $a.a_r \equiv a.a_s \mod n$, multiplicando ambos os lados da congruência pelo inverso de a módulo n, temos que $a_r \equiv a_s \mod n$, o que só é possível para $a_r = a_s$. Podemos concluir que cada inteiro do conjunto $\{a.a_1, \dots, a.a_{\varphi(n)}\}$ é congruente a um único inteiro do conjunto $\{a_1, \dots, a_{\varphi(n)}\}$.

Portanto, pela propriedade multiplicativa das congruências:

$$[(a.a_1).\dots.(a.a_{\varphi(n)})] \equiv a_1 \dots a_{\varphi(n)} \mod n$$

Assim, $[a^{\varphi(n)}.(a_1 \dots a_{\varphi(n)})] \equiv a_1 \dots a_{\varphi(n)} \mod n$. Multiplicando os dois lados da congruência por α, obtemos $a^{\varphi(n)} \equiv 1 \mod n$. ■

2.3. Ensino de Matemática - onde foram parar os Números Primos?

A preocupação com o ensino da matemática é histórica. Na Grécia antiga a matemática era ensinada na escola pitagórica, como um conhecimento necessário para a formação dos filósofos e dos futuros governantes. Com Platão ocorre à implantação definitiva da disciplina matemática, estendida até ao nível das crianças.

Um recorte da história do ensino no Brasil mostra que a matemática inicialmente foi considerada como uma área do conhecimento de pouco valor pelos padres da companhia de Jesus no período colonial. A partir da república, com os novos padrões do mundo do capital, passa a ser, como componente curricular, uma das principais referências para o conhecimento.

D'Ambrosio (2008, p. 43) afirma que, ainda no período da colônia, pode ser evidenciada, a necessidade de conhecimentos matemáticos para:

> A fundação de cidades, na costa e no interior, exigiu a construção de grandes igrejas e edifícios públicos, a urbanização e o traçado de estradas, a construção de pontes, e outras tantas atividades que revelam consideráveis conhecimentos matemáticos. [...] Desde os primeiros tempos da colônia, a construção de fortes era prioridade. Nessa perspectiva, o ensino de matemática consistiria basicamente em transladar, de alguma forma, parte dos saberes canonizados do campo filosófico ao mundo profano dos estudantes.

Essas necessidades emergentes deram à matemática um status inexistente, até então, na colônia. Valente (1999) apresenta que o ensino da matemática no Brasil se deu para a preparação militar, com aulas de artilharia e fortificações e para atender a essa necessidade foram contratados professores estrangeiros para desenvolver atividades. Mesmo com essa necessidade tão explícita, pouco foi realizado para ampliar a abrangência dos estudos em matemática, pela precariedade material e pelas medidas de controle emitidas pela coroa portuguesa durante o período colonial. No período das aulas régias o desinteresse pelas aulas de matemática foi tão intenso, que se instituiu, por meio de edital, penalidades aos alunos que não alcançassem o rendimento esperado ou não comparecesse às aulas (MIORIM, 1998). Com a proclamação da república em 1889, organizou-se a educação brasileira aos moldes da escola francesa, onde a matemática foi considerada como uma das principais e essenciais disciplinas do currículo. A partir da Reforma Campos, a matemática nasce como disciplina escolar, unificando os ramos da matemática representados pela aritmética, álgebra e geometria que, até então, eram tidas como disciplinas independentes.

Atualmente, a matemática está presente na escola desde a Educação Infantil. Já nos primeiros anos de escolarização nos vemos diante de atividades de "arme e efetue", "contagem" ou "exercícios" sem significados e distantes da realidade. A matemática apresentada na escola soa vazia, pouco ou quase nenhum espaço tem-se para o pensar. O pensar com liberdade, este pensar que é encontrar, desencontrar e reencontrar.

A matemática é vista por muitos como um conteúdo pronto, acabado e incontestável. Para estes, fazer matemática é o mesmo que resolver listas de exercícios em que fórmulas são aplicadas, sem nenhum sentido. Todos os alunos aprendem a memorizar e repetir operações, tabuadas e contas consagradas ou não. Constatando ser esse o caminho mais curto, tranquilo e "seguro" os alunos vão "passando" pela escola sem que realmente façam uso do que a educação se propõe a fornecer. Uma vez iniciado esse processo de "faz-de-conta", esse ciclo se perpetua pelo ensino fundamental, médio e, em algumas vezes, vergonhosamente no ambiente acadêmico. Mas ora, se a escola tem como um de seus objetivos formar cidadãos críticos e participativos, como é possível a essa instituição imputar aversão ao importante requisito de crítica e participação social que é o pensar? Como afirma Freire (1980),

> [...] o educador ou a educadora crítica, exigente, coerente, no exercício de sua reflexão sobre a prática educativa ou no exercício da própria prática, sempre a entende em sua totalidade. Não centra a prática educativa, por exemplo, nem no educando, nem no educador, nem no conteúdo, nem nos métodos, mas a compreende nas relações de seus vários componentes, no uso coerente por parte do educador ou da educadora dos materiais, dos métodos, das técnicas. (p. 110)

Todos os professores de matemática enfrentam, anualmente, a tarefa de começar as aulas para um público novo. Quando é necessário começar do zero, o desafio é ainda maior. Isto porque se sabe que é preciso estar preparado para enfrentar algumas perguntas que inevitavelmente chegarão: "o que é matemática?", "para que serve?", "o que fazem os matemáticos?".

Segundo Resende (2007), o número primo é um conceito fundamental na Teoria Elementar dos Números. Desde a década de 1990, estudos e pesquisas vem sendo realizados com questões relacionadas ao ensino e à aprendizagem da Álgebra, tanto nos Ensinos Fundamental e Médio, como no Ensino Superior, apontando para a relevância de se definir o papel da Aritmética no ensino da matemática, no que diz respeito a Teoria Elementar dos Números. Machado et al. (2005) afirmam que ela tem um potencial formador que vem sendo negligenciado em todos os níveis de escolarização e apontam alguns objetivos para seu ensino:

> […] auxiliar a reconhecer e compensar limitações de estudantes em seu entendimento conceitual da aritmética dos números inteiros; criar oportunidades, através da abordagem de tópicos como decomposição em primos e divisibilidade, para propor problemas fecundos que desenvolvam a compreensão conceitual da matemática; instigar as habilidades de estudantes para generalizar e fazer conjecturas e para encontrar maneiras de justificar essas conjecturas; promover o desenvolvimento de estratégias de prova indutivas e dedutivas. (MACHADO; MARANHÃO; COELHO, 2005, p. 2).

Sobre a aprendizagem dos números primos, as investigações vêm mostrando que ela não se completa nos anos iniciais do Ensino Fundamental; a Teoria dos Números Primos tem um papel central na Matemática e na História da Matemática, e que é pouco enfatizada nos currículos. Moreira (2004, p. 85) afirma "que a aritmética dos naturais é um tema complexo, cuja apreensão, em níveis considerados satisfatórios, não se esgota no processo que se desenvolve ao longo das séries iniciais".

O primeiro contato que o aluno tem com o conteúdo de números primos é a definição errada dada pelo professor do primeiro segmento do ensino fundamental: o número que só é divisível por 1 e por ele mesmo, além disso, o único número par que é primo é o 2. Daí passa-se a exercícios de teste de primalidade a partir de divisões exaustivas, onde testa-se quais números são primos; devido ao método primitivo, geralmente, contenta-se em conhecer os primos compreendidos entre 1 e 30 ou ainda recomenda-se que os alunos devem tentar memorizar números primos, pelo menos os números primos abaixo do 50 ou do 100.

Esta poderia ser uma apresentação inocente, se não trouxesse precipitações já em sua definição; o fato do número 2 ser o único par que é primo é uma consequência e não uma definição. Além disso, não se faz relação com o conteúdo já aprendido, qual seja, paridade de um número – a esta altura os alunos já sabem (ou deveriam saber?) que um número par é múltiplo de 2 e assim, todo número par (exceto o 2) já apresenta um divisor diferente de um e dele mesmo. Sem contar que, existem autores que dizem que "um número natural é primo se for divisível apenas por 1 e por ele mesmo". Seguindo a ideia dessa frase, 1 seria considerado primo!

Já no início do segundo segmento do ensino fundamental, apresentamos a fatoração de um número em fatores primos, para uso no cálculo do Mínimo Múltiplo Comum (MMC) e Máximo Divisor Comum (MDC). Em uma "versão escolarizada" do Teorema Fundamental da Aritmética, os alunos utilizam a técnica da fatoração para resolver problemas que envolvem estes conteúdos, como o abaixo, que emprega o MDC:

Três peças de tecido medem respectivamente, 180m, 252m e 324m. Pretende-se dividir em retalhos de igual comprimento. Qual deverá ser esse comprimento de modo que o número de retalhos seja o menor possível? Em quantos pedaços as peças serão divididas?

Primeiro é preciso calcular o MDC entre 180, 252 e 324, fatorando os números simultaneamente:

180	252	324	2
90	126	162	2
45	63	81	3
15	21	27	3
5	7	9	36

A fatoração produz como resultado o comprimento do tecido, 36 metros, e quantos pedaços serão obtidos: 5 da primeira peça, 7 da segunda e 9 da última.

O problema é que esta maneira de calcular o MDC entre os números não faz nenhuma relação com o que o aluno fazia até então (listar os múltiplos ou divisores dos números e comparar), nem mesmo fazem referência aos critérios de divisibilidade, que em alguns casos são estudados depois, ou nem chegam a ser conhecido pelos educandos. A ideia de que a meta principal da escola não é o ensino dos conteúdos disciplinares, mas sim o desenvolvimento das competências, está atualmente no centro das atenções. É preciso apresentar o conteúdo de modo que os alunos possam fazer descobertas significativas para o seu aprendizado.

CAPÍTULO 3 - TEORIA DOS NÚMEROS E CRIPTOGRAFIA

O uso da criptografia já se fazia presente no sistema egípcio de escrita hieroglífica; em diferentes épocas e lugares, sistemas para ocultar de terceiros certas informações compartilhadas e importantes, foram criados. Na Palestina foram usadas as cifras hebraicas. Júlio César usava um cifrário para comunicar seus planos de batalha aos generais de seu exército. Hoje contamos com sofisticados sistemas criptográficos que utilizam a matemática dos números primos para que possamos estar seguros em nossas transações bancárias e troca de informações pela rede virtual.

3.1 O Caminho da Criptografia

A palavra criptografia deriva do grego, onde *cryptos* significa oculto, secreto, escondido e *grapho* significa escrita, grafia. A criptografia pode ser entendida como o estudo de métodos para transformar uma mensagem em algo incompreensível para todos (codificação), exceto para o destinatário da mensagem que a tornará legível (decodificação).

Os hebreus, desde a Antiguidade, tinham interesse em ocultar informações. Para tal utilizavam, pelo menos, três tipos de cifras *atbash*, *albam* e *atbah*, que consistiam em substituir umas letras pelas outras. Na cifra *atbash*, a primeira letra do alfabeto é substituída pela última, a segunda letra pela penúltima e assim sucessivamente. Na cifra *albam*, a substituição é feita da seguinte maneira: a primeira letra é substituída pela que ocupa 14ª posição, a segunda letra pela que ocupa a 15ª, até a 13ª letra ser substituída pela 26ª, de modo que o sistema fica da seguinte maneira:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M

A cifra *atbah* tinham a seguinte substituição:

A	B	C	D	J	K	L	M	E	S	T	U	V
I	H	G	F	R	Q	P	O	N	Z	Y	X	W

Os espartanos usavam o *scytale* ou *bastão de Licurgo* para transmitir mensagens confidenciais. Trata-se de uma cifra de transposição onde era enrolada uma tira de couro ou papiro num cilindro, escrevia-se uma mensagem no sentido do seu comprimento, em seguida desenrolava-se a tira e era transportada até o destinatário, que por sua vez enrolava a tira num bastão de igual diâmetro e decodificava a mensagem.

A cifra de Políbio data de 200 a.C e consiste no uso da tabela abaixo em que cada letra passa a ter como representação duas outras, duplicando a extensão da mensagem original:

	A	B	C	D	E
A	A	B	C	D	E
B	F	G	H	I/J	K
C	L	M	N	O	P
D	Q	R	S	T	U
E	V	W	X	Y	Z

Há ainda uma outra versão desta mesma cifra em que as letras A, B, C, D, E utilizadas para codificar as mensagens são trocadas pelos números 0, 1, 2, 3 e 4; desta forma, a mensagem poderia ser enviada por meio escrito ou utilizando as mãos ao segurar tochas de fogo (dois grupos de 5) representando os números e transmitindo a mensagem letra a letra (FIARRESGA,2010).

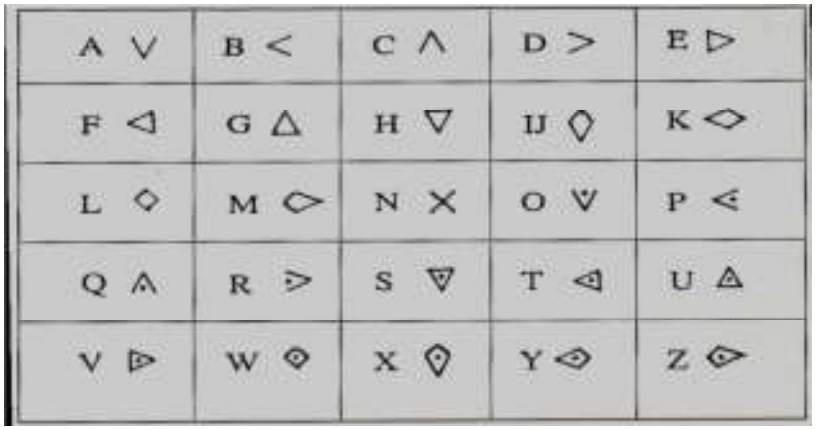
O famoso Julio César (por volta de 60 a.C.) usava um cifrário para comunicar seus planos de batalha aos generais de seu exército. Suetônio, escritor romano que viveu no início da era cristã (69 d.C.), em *Vida dos Doze Césares*, conta que Júlio César usava na sua correspondência particular um código de substituição no qual transladava as letras do alfabeto três casas adiante. Após um tempo, a denominação de Código de César passou a designar qualquer cifra na qual cada letra da mensagem seja substituída por outra deslocada um número fixo de posições.

As cifras utilizadas durante muito tempo eram cifras monoalfabéticas, por isso em 855 d.C., no livro "Um Manuscrito sobre a Decifração de Mensagens Criptográficas" (al-Kindi), é descrito um método para decifrar mensagens, utilizando a análise de frequências. Quando contamos a frequência com que as letras aparecem em um texto longo (figura 1), em qualquer idioma, descobrimos uma frequência relativa; a partir deste fato, foi possível decifrar diversas mensagens e "quebrar" vários códigos monoalfabéticos; isto ocorre porque, geralmente, as letras mais frequentes no texto cifrado representam as letras mais comuns do idioma mesmo que não siga a mesma ordem. Um texto cifrado em nosso idioma deverá conter mais cifras que representem as letras A, E, O, que são as mais frequentes em português, podendo acontecer da cifra da letra E se repetir mais vezes que a da letra A e, mesmo assim, reduzir as possibilidades de decodificação.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Fonte: COUTINHO, 2012. Aritmética I, material de disciplina.
Figura 1- Análise da frequência de letras em português

Os Templários utilizaram a criptografia para comunicação e para codificar letras de câmbio e outros documentos financeiros e comerciais. A cifra (figura 2) foi retirada da Cruz das Oito Beatitudes, que era o emblema da Ordem dos Templários e se utilizava de símbolos, não apenas de permutações de letras.



Fonte: FIARRESGA, 2012. Criptografia e Matemática, p.11
Figura 2 – Cifra utilizada pelos Templários

Em 1411, surgem as primeiras cifras homofônicas. Para dificultar a análise de frequências, são introduzidos os homófonos e os nulos. Os primeiros consistiam de símbolos diferentes para representar a mesma letra e os últimos eram colocados aleatoriamente ao longo do texto cifrado para confundir qualquer um que fizesse uma análise de frequências do texto. Em uma cifra de substituição homofônica, cada letra é substituída por uma variedade de símbolos, proporcional à frequência da letra. Por exemplo, a letra A corresponde a 14% de todas as letras que aparecem num texto em português, daí, deve-se criar 14 símbolos para representa-lo e a cada vez que a letra A aparecer no texto original, substituímos por um dos 14 símbolos criados. Desta forma, a frequência dos símbolos fica mais equilibrada no texto cifrado, diminuindo a possibilidade da mensagem ser decodificada por alguém a quem a mensagem não se destina.

O primeiro sistema polialfabético conhecido surge em 1466, o disco de cifra era constituído por dois discos concêntricos, divididos em vinte e quatro setores. No disco maior, que era fixo, se escrevia cada uma das letras do alfabeto (exceto H, J, K, U, W e Y) e os algarismos 1, 2, 3 e 4. O disco menor, móvel, continha de forma aleatória as letras do alfabeto. Para cifrar uma mensagem com o disco de cifra escolhe-se uma letra chave e uma palavra-chave, de forma que se tem uma cifra polialfabética, onde o número de alfabetos de cifra utilizados depende da quantidade de letras da palavra-chave escolhida. O disco de cifras do século XV inspirou outros: em 1795, o então secretário de estado norte americano Thomas Jefferson criou uma máquina de codificação (figura 3) que consistia de 25 discos de madeira os quais giram em torno de um eixo comum. Para torna-los individuais, em cada disco de madeira as 26 letras do alfabeto foram gravadas de forma aleatória.

Fonte: Cipher Machines. Disponível em:< http://ciphermachines.com/jefferson>. Acesso em 5 mar 2013.
Figura 3 – Disco de Cifras criado por Thomas Jefferson

Em 1563, Della Porta utilizou onze alfabetos distintos para criar uma cifra. No século XVI, o filósofo inglês Francis Bacon criou um código, utilizando apenas as letras A e B, em

que cada letra é substituída por uma combinação com cinco itens; tal codificação pode servir para escrever cada uma das letras em código binário, bastando substituir A e B por 0 e 1.

Foi o matemático alemão, Gottfried Wilhelm Von Leibniz, quem inventou a máquina de calcular e descreveu o sistema binário. Já Gilbert Sandford Vernam, utilizando uma chave aleatória, inventou uma máquina de cifragem polialfabética. Ao final da Primeira Guerra Mundial, em 1918, o exército alemão inventou e usou a cifra ADFGVX, que era simultaneamente de substituição (semelhante à cifra de Políbio) e transposição (escolhia-se uma palavra-chave e escrevia-se a mensagem que já estava cifrada, em seguida ordenavam-se as letras da palavra-chave por ordem alfabética). As mensagens eram transmitidas em Código Morse.

Em 1929 surge um texto codificado através de uma operação de matrizes. Após a Primeira Guerra Mundial, cria-se a máquina Enigma (figura 4), devido ao elevado número de chaves utilizadas e à sua complexidade foi empregada para fins militares pelos alemães.

Fonte: Redes. Disponível em: <http://phantomsys.blogspot.com.br/2012/03/criptografia.html>. Acesso em 05 mar 2013.
Figura 4 – Máquina Enigma

Em meados do século XX, o computador trouxe consigo um problema para a criptografia: como as empresas poderiam trocar mensagens com um grande número de informações de forma segura e eficiente? Além disso, a necessidade da troca de chave entre emissor e destinatário tornava a tarefa vulnerável (a chave poderia ser interceptada) e impossibilitava o envio de mensagens codificadas a quem não tivesse conhecimento da chave.

Até o final do século XX, as chaves criptográficas eram funções injetivas, que permitam a sua decodificação através da sua função inversa; ou seja, letras distintas resultavam em símbolos distintos e para decodificar bastava usar o processo inverso daquele feito na codificação. Em 1976, Whitfied Diffie e Martin Hellman encontraram uma forma de poder haver uma troca segura de chaves, sem as pessoas se encontrarem, através da aritmética modular e da cifra assimétrica. A ideia era usar uma chave para codificar a mensagem e outra para decodificar. Foram Ronald Rivest, Adi Shamir, e Leonard Adleman que, em Abril de 1977, criaram a cifra assimétrica RSA. As funções de codificação e de decodificação utilizadas neste sistema são unidirecionais, ou seja, uma função computacionalmente viável de se calcular f(x) dado x e computacionalmente inviável determinar x tal que f(x) = y dado y.

Depois desta, outras cifras assimétricas foram criadas: em 1984, Taher ELGamal cria uma baseado no Problema do Logaritmo Discreto; em 1986, Miller introduz na criptografia as curvas elípticas; os anos 90 trouxeram os estudos dos computadores quânticos e criptografia quântica.

3.2 O Método RSA

O RSA é um método criptográfico assimétrico muito usado em aplicações comerciais. De modo geral, para codificar uma mensagem usando o RSA é preciso obter dois primos grandes e para decifrar seria necessário fatorar o produto destes primos. Neste método quem tem a chave de codificação não tem necessariamente a chave de decodificação.

Apresentaremos agora o modo como o método funciona. Em primeiro lugar, cada letra do alfabeto deve estar associada a um valor numérico, além de uma numeração específica para o espaço entre palavras. Esta associação é feita de acordo com a escolha de quem deseja criptografar a mensagem, tomando-se o cuidado de associar cada letra a um número que tem sempre a mesma quantidade de algarismos, para que não haja um agrupamento errado. Computacionalmente utilizamos a tabela ASCII[1]. É necessário escolher dois números primos p e q (com $p \neq q$) que serão usados para obter as chaves de codificação e decodificação; uma parte é obtida pela multiplicação dos primos p e q ($n = p.q$).

Outra parte da chave de codificação é obtida pela função φ de Euler de n. Temos:

$$\varphi(n) = \varphi(p.q) = \varphi(p)\varphi(q) = (p-1)(q-1), \text{ pois, } mdc(p,q) = 1.$$

Ao calcularmos $\varphi(n)$ devemos procurar o número e, tal que, $mdc\big(e, \varphi(n)\big) = 1$. Desta forma, a chave será o par (n, e). Obtida a chave, passa-se à codificação da mensagem, através de sistema de congruências. Para tal, dividimos a mensagem numérica, gerando uma sequência que é quebrada em blocos de diferentes tamanhos, que representam inteiros m no intervalo $(0, n)$. Então cada bloco A é codificado.

Para cada bloco, usa-se a congruência:

$$A^e \equiv R \ \ mod\, n,$$

Após a codificação destes blocos não poderemos mais agrupá-los, para que possamos decifrar os dados. Para a decodificação dos dados, determina-se d tal que $ed \equiv 1(mod\ \varphi(n))$, ou seja, d é o inverso multiplicativo de e módulo $\varphi(n)$; e fazemos para cada bloco codificado R, $R^d \equiv B\ mod\, n$. O usuário do sistema RSA publica a chave de codificação (e, n) e mantém em segredo a chave de decodificação (d, n).

Observemos que todo o processo de codificação usa a Teoria dos Números para criar a chave e que a multiplicação de dois primos grandes é facilmente calculada (com o auxílio dos computadores), mas que dado o produto de dois primos grandes obter a fatoração do produto não é tarefa simples. Para decodificar a mensagem é necessário saber quais são os números primos p e q tais que $n = pq$. A segurança do RSA é baseada na impossibilidade de se fatorar um número grande rapidamente (Tabela 1). E precisamos da fatoração de n para calcular $\varphi(n)$.

Talvez, uma pergunta intrigante seja: se é tão difícil fatorar um número grande, como encontrar primos enormes para gerar minha chave de codificação? A resposta é que existe uma diferença considerável entre detectar se um número é primo e fatorá-lo. Testes como o de Monte Carlo (veja BERNSTEIN, 2002) identificam a primalidade de um número com milhões de casas decimais em tempo muito rápido, sem a necessidade de usar fatoração. Há também testes de primalidade determinísticos como o AKS, um pequeno algoritmo de 14 linhas onde é possível identificar a primalidade de um número em tempo polinomial (veja BRAGA, 2002 e COUTINHO, 2004).

[1] Na tabela ASCII (American Standard Code for Information Interchange) cada caracter é representado por um código de 8 bits (um byte), ou seja, combinações numéricas de 0s e 1s, com oito algarismos.

nº de algarismos de n	Tempo necessário para "quebrar" o RSA
50	3,9 horas
75	104 dias
100	74 anos
200	3,8 x 10^7 séculos
300	4,9 x 10^{13} séculos
500	4,2 x 10^{23} séculos

Tabela 1 – Tempo para quebrar o RSA. Adaptada de: Criptografia e a importância das suas aplicações. RPM 12.

Suponha, para fins de exemplo, que queremos codificar a mensagem SOU MÃE DA JULIA utilizando o sistema RSA. Primeiro, associamos cada letra do alfabeto um número natural:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

O espaço será associado ao número 37. Observe que só usamos números naturais com 2 dígitos: 11, 12, ..., 37. Se tivéssemos escolhido valores de 1 a 27 não saberíamos se 25 corresponde à letra Y ou à sílaba BE. Nossa mensagem numérica será

29253137231115371411372031221911

Agora, escolhemos dois números primos distintos. Usaremos os números 5 e 11, para facilitar os cálculos (observando que na aplicação real, escolhemos primos muito grandes), temos $p = 5$ e $q = 11$, daí $n = 5.11 = 55$ e $\varphi(n) = 4.10 = 40$ e podemos tomar $e = 3$.

A próxima etapa é dividir a sequencia acima em blocos com números menores que 55 (valor de n), obtemos, por exemplo:

29 – 2 - 53 – 13 – 7 – 23 – 1- 1- 1-53 - 7 - 20 – 3 – 12 – 21 – 9 – 11

Aplicamos a cada bloco a congruência $A^3 \equiv R\ (mod 55)$. Desta forma, temos:

- $29^3 \equiv 24(mod 55)$.
- $2^3 \equiv 8(mod 55)$.
- $53^3 \equiv 47(mod 55)$.
- $13^3 \equiv 52\ (mod 55)$.
- $7^3 \equiv 13(mod 55)$.
- $23^3 \equiv 12\ (mod 55)$.
- $1^3 \equiv 1\ (mod 55)$.
- $20^3 \equiv 25(mod 55)$.
- $3^3 \equiv 27(mod 55)$.
- $12^3 \equiv 23(mod 55)$.
- $21^3 \equiv 21(mod 55)$.
- $9^3 \equiv 14\ (mod 55)$.
- $11^3 \equiv 16(mod 55)$.

Nossa mensagem será:

24 – 8 – 47 – 52 – 13 – 12 – 1- 1- 1- 47 – 13 - 25 – 27 – 23 – 21 – 14 – 16

Para encontrarmos o valor d, podemos utilizar o Algoritmo Euclidiano Estendido, onde teremos $1 = 27.3 - 40.2$, e a chave privada será $(55,27)$. Dizemos que o RSA é um criptossistema cujo alfabeto de entrada é o alfabeto binário, e provaremos agora que o sistema funciona.

Teorema 3.2.1. *A decodificação do RSA funciona*.

Queremos provar que ao codificar um bloco da mensagem, poderemos decodifica-lo depois voltando ao bloco original.

Demonstração: Seja R, o bloco codificado, queremos provar que $R^d \equiv A \; mod \; n$. Como $A^e \equiv R \; mod \; n$, então, basta provar que $A^{e.d} \equiv A \; mod \; n$.

Temos que $e.d \equiv 1 \; mod \; \varphi(n)$, então $\exists k \in \mathbb{Z}$ tal que $e.d = 1 + k.\varphi(n)$. Logo, $A^{e.d} \equiv A^{1+k.\varphi(n)} \equiv \left(A^{\varphi(n)}\right)^k . A \; mod \; n$.

Se $mdc\ (A, n) = 1$, podemos usar o Teorema de Euler:

$$A^{e.d} \equiv \left(A^{\varphi(n)}\right)^k . A \ \equiv A \; mod \; n$$

Se $mdc\ (A, n) = p$, temos: $A^{e.d} \equiv \left(A^{(p-1)}\right)^{k.(q-1)} . A \ \; mod \; p$. Se $mdc(A, p) = 1$, pelo Teorema de Fermat, $A^{e.d} \equiv A \ \; mod \; p$; caso contrário, temos que $p|A$ e, portanto, $A^{e.d} \equiv 0 \equiv A \; mod \; p$. Prosseguindo, de modo análogo, quando $mdc\ (A, n) = q$, obtemos $A^{e.d} \equiv A \; mod \; q$.

Portanto, como $n = p.q$,

$$\begin{cases} A^{ed} \equiv A \; mod \; p \\ A^{ed} \equiv A \; mod \; q \end{cases}$$

$$A^{ed} - A = kpq$$

$$A^{ed} \equiv A \; mod \; pq$$

$$A^{e.d} \equiv A \; mod \; n$$

■

Para que o sistema RSA possa manter-se seguro é necessário que os números p e q não estejam próximos um do outro, senão, ambos os primos estarão próximos de $\sqrt{n}$ e daí, é possível mostrar que n pode ser fatorado facilmente, através de um algoritmo devido a Fermat. Para mais detalhes, veja Coutinho (2005, Seções 2.4 e 2.5).

Os métodos de fatoração existentes ainda não dão conta de fatorar números inteiros tão grandes quanto os utilizados nos RSA, por isso, este sistema criptográfico é muito utilizado e seguro.

CAPÍTULO 4 - EDUCAÇÃO MATEMÁTICA COMO FORMAÇÃO PARA O PENSAR

Neste capítulo serão abordadas as teorias sobre as quais as atividades propostas ao final desse trabalho foram pensadas, ações que não visam a aplicação de exercícios sobre determinados conteúdos, mas que se utilizam de conhecimentos matemáticos para criptografar mensagens. Trouxemos as contribuições feitas por Jacques Rancière a partir de sua defesa da igualdade das inteligências, quando recupera e experiência de Jacotot, no início do século XIX, e as contribuições de Theodor Adorno sobre a relação educação-emancipação, fazendo um contraponto com os resultados dos alunos nas avaliações em escalas nacionais. Depois são discutidas as ideias de Polya sobre a aprendizagem por Resolução de Problemas, também presente nos Parâmetros Curriculares Nacionais, que reforça ainda a História da Matemática como ferramenta de ensino-aprendizagem.

4.1 A troca de experiências: por um ensino emancipatório

A ideia de que a educação por si conduzirá o aprendiz a um existir atravessado pelo pensamento está ultrapassada. O exercício do pensamento é algo que ninguém pode fazer por nós: ensinar matemática não pode significar mais que organizar e dispor atentamente os elementos que supomos contribuir para a iniciação do pensar.

Viver a experiência do pensamento nos exercícios de matemática é experimentar uma desconstrução do tempo-espaço que conhecemos na escola. Para Ranciére, a igualdade necessária para a emancipação não é possível nos moldes de uma escola como a que temos, com práticas pedagogizadas, com seus fins predeterminados, que subordina uma inteligência a outra inteligência. Nesses termos, a igualdade é um fim a ser alcançado pela escola, enquanto para o autor, a igualdade deve ser um princípio, invertendo completamente a lógica defendida pelo discurso hegemônico.

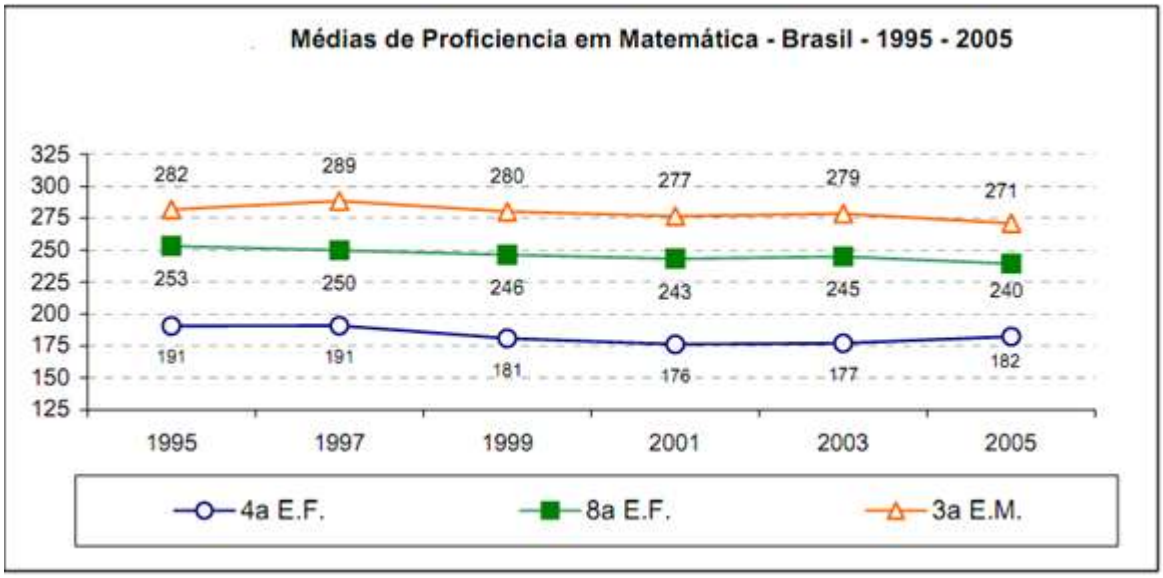
Não é possível, oferecer uma grade curricular com disciplinas desarticuladas que não visam a uma ligação efetiva entre teoria e prática, e aspirar a um perfil de aluno capaz de questionar sua ação, propor soluções e experimentá-las.

Hoje em dia, o Brasil consegue matricular quase todas as crianças (97%) no ensino fundamental. No entanto, os resultados das avaliações da aprendizagem de matemática no Brasil mostram que a melhoria, identificada no campo das pesquisas teóricas e aplicada em Matemática, não alcançou as atividades escolares. A matemática não é a única matéria em que os jovens se deparam com dificuldades, mas é a matéria em que são maiores as limitações dos alunos. Os dados do Saeb (Sistema Nacional de Avaliação da Educação Básica) mostram, alarmantemente, que o desempenho dos alunos está diminuindo: as informações identificam 13 pontos a menos no desempenho dos alunos do último ano do Ensino Fundamental em um período de apenas 10 anos (figura 5).

Isto significa que os alunos do 9º ano do Ensino Fundamental (antiga 8ª série) não são capazes de identificar a localização de números inteiros na reta numérica ou resolver problemas utilizando divisão com resto diferente de zero ou, ainda, resolver equações do 1° grau com uma incógnita. Já os alunos do 5º ano do Ensino Fundamental (antiga 4ª série) não adquiriram habilidades consideradas básicas, tais como: ler informações e dados apresentados em tabela, identificar a localização/movimentação de objeto em mapas (desenhado em malha quadriculada), identificar a divisão como a operação que resolve uma dada situação-problema.

O caso não é diferente no 3° ano do Ensino Médio. Identificar em um gráfico de função o comportamento de crescimento/decrescimento, resolver problemas com uma equação de primeiro grau que requeira manipulação algébrica ou calcular o volume de sólidos

simples (como o cubo) são problemas que eles não conseguem solucionar. Esses alunos estão em um nível de conhecimento esperado para quem ingressa no Ensino Médio.



Fonte: Inep

Figura 5 – Médias de Proficiência em matemática – Brasil – 1995 – 2005

Tal realidade leva as seguintes indagações: o que ocorre com aqueles para os quais a matemática é algo alheio e que acabam de entrar em contato com ela? É possível ensinar, é possível transmitir ou contagiar este interesse em problematizar? Em última instância, é possível ensinar o desejo de fazer matemática?

Há um senso-comum que atribui à construção do pensamento um papel secundário nos Ensinos Fundamental e Médio, como se não fosse importante à formação do educando. Trocar experiências com as crianças provoca a ação de pôr em movimento o que estava parado. O professor deve incentivar a troca entre os alunos como forma de aprendizagem, respeitando o pensamento e a produção de todos e, assim, desenvolver um trabalho livre do preconceito de que Matemática é um conhecimento direcionado apenas para poucos.

Nesse sentido, a educação teria mais do que uma dimensão adaptativa; Costa (2005, p. 61) nos auxilia nessa compreensão, afirmando que:

> A educação para a adaptação, como já destacado por Adorno (1995), tem a função de preparar os homens para se orientarem no mundo. Ou seja, a questão da adaptação é importante e a educação deve tê-la como meta, mas deve ir além dela, no sentido da emancipação.

Pensar em escola democrática possibilita a reflexão sobre a escola que se tem e a escola que se almeja. Sabe-se que a primeira é segregadora, ou seja, não dá conta de atender à diversidade humana, educa para a homogeneização, uma vez que desconsidera as diferenças e hierarquiza os indivíduos. A sociedade começa a se mobilizar pela mudança e reorientação da escola que não se contenta mais em reproduzir a lógica da marginalização, demasiadamente evidente na sociedade intolerante.

Encontramos em Ranciére (2002) um caminho para pensar na temporalidade das experiências de aprendizado a partir do que o autor trata como *forma-escola*. Escola aqui não como um lugar ou uma função definida por uma finalidade social, mas escola como ócio. Ranciére traz os sentidos da *scholé* grega, não como um lugar de transmissão de saberes com objetivo de preparar as crianças para as atividades a serem realizadas numa vida adulta, senão como um lugar fora das demandas dos trabalhos, um lugar onde se aprende por aprender, um

lugar de igualdade por excelência. Onde uma habilidade não pode se destacar da outra, ao contrário do que mostra a figura 6.

Fonte: Filosofia Hoje. Disponível em: < http://www.filosofiahoje.com/2012/09/o-nosso-sistema-educacional-em-uma.html >. Acesso em 03 abr 2013.

Figura 6 – A "igualdade" da educação

No pensamento de Adorno, está presente a ideia de que democratizar significa formar indivíduos com autonomia. Sem a constituição das subjetividades, o que temos é a massificação, ou seja, alguns poucos indivíduos pensam por uma maioria, e se impõe o que os primeiros exigem, independente das necessidades da totalidade dos indivíduos. Sobre a educação, Adorno (1995, p. 141) acrescenta que "Eu diria que atualmente a educação tem muito mais a declarar acerca do comportamento no mundo do que intermediar para nós alguns modelos ideais preestabelecidos".

A questão do ensino de matemática pode ser compreendida como um problema filosófico tentando superar a contraposição produção-reprodução que condena a didática da matemática a não ser mais que um conjunto de técnicas facilitadoras da compreensão de alguns conteúdos. Discutir a relação que mantêm entre si os saberes matemáticos canonizados e os realmente ensinados é um caminho possível para compreender as dificuldades encontradas no processo ensinar/aprender matemática.

Tem-se, por um lado, o universo dos matemáticos e investigadores profissionais em questões da área e, por outro, o dos leigos e aprendizes, os estudantes. Os professores ocupam o lugar da mediação entre os dois mundos e sua função é tentar aproximar ou transformar os segundos nos primeiros. O problema é ensinar e aprender uma disciplina que carrega tantos preconceitos e estereótipos como a matemática.

A questão que se apresenta é que qualquer um poderia colocar determinados tipos de perguntas e tentar, em alguma medida, respondê-las. Claro que o grau de profundidade, de enquadramento teórico ou de erudição será diferente ao de um especialista. Porém não as tornam menos próprias, ao contrário, permitem e potencializam o pensar, é uma atitude produtora e criadora, não meramente uma reprodução ou repetição do que há. Desta forma, transmitir ideias já elaboradas não significa, obviamente, ensinar a pensar.

O hábito de pensar vem do prazer da descoberta, se nossas experiências com a prática são verdadeiramente prazerosas, elas nos fazem significado e gostamos de repeti-las, transformando-as em um hábito. Se nos trazem momentos ruins, se tornam verdadeiros martírios.

Notemos que o fim da educação não é ativar o pensamento, fazer com que usemos a razão, mas, sim, proporcionar as condições para que estejamos livres para usar e expandir o pensamento. Assim, embora a educação não possa esperar que todos façam uso de suas

próprias potências do pensamento todo o tempo e, por esse motivo, impõe laços de obediência, a ela tampouco convém impedir que os educandos pensem por si só.

4.2 Resolvendo problemas da Matemática

Atualmente, tem-se buscado, sem sucesso, uma aprendizagem em Matemática pelo caminho da reprodução de procedimentos e da acumulação de informações; subestimando a capacidade dos alunos, sem reconhecer que resolvem problemas, lançando mão de seus conhecimentos sobre o assunto e buscando estabelecer relações entre o já conhecido e o novo. A questão da resolução problemas na sala de aula foi abordada pela primeira vez de modo consistente por Polya, em 1995.

Através da resolução de problemas, inserida num ambiente propício e favorável, o aluno verifica a validade dos conceitos matemáticos, realiza conjecturas, relaciona os conceitos, generaliza, estimula os procedimentos num contexto significativo, toma uma atitude reflexiva e desenvolve a capacidade de raciocínio e o pensamento matemático.

Um problema matemático é toda situação requerendo a descoberta de informações desconhecidas para a pessoa que tenta solucioná-lo, ou seja, é preciso inventar estratégias e criar ideias. Kantowski (1997) considera que um problema é uma situação com que uma pessoa se depara e para a realização da qual não tem um procedimento ou algoritmo que conduza à solução; o que é problema para um indivíduo poderá ser exercício para outro ou ainda uma frustração para um terceiro.

Polya (1995), sugere quatro etapas de resolução de problemas:

- 1ª etapa: Compreender o problema – consiste em identificar qual é a incógnita do problema, verificar quais são os dados e quais são as condições, levantar hipóteses;
- 2ª etapa: Construção de uma estratégia de resolução - encontrar as conexões entre o que temos (dados) e o que queremos (incógnita);
- 3ª etapa: Execução da estratégia - utilizar os algoritmos para solucionar o problema;
- 4ª etapa: Revisando a solução - verificação dos resultados e dos argumentos utilizados.

Somente após estudar e compreender com alguma profundidade os problemas matemáticos e desafios trazidos pelos professores é que os alunos começam a construir possíveis soluções. Mas o processo não termina aí. Os professores devem coletar as produções de seus alunos e abrir espaço para a discussão, para então intervir.

O papel do professor consiste em apoiar os alunos, com vista ao desenvolvimento progressivo da autonomia destes e à construção da competência de resolução de problemas, questionando e fornecendo-lhes sugestões. A compreensão dos princípios científicos deve estar associada a problemas que o aluno se propõe a solucionar. Para isso, é interessante que o professor apresente situações reais ou simuladas nas quais o aluno possa aplicar esses princípios. É preciso experenciar para perceber o saber matemático como algo prazeroso na formação do cidadão.

O desafio de ensinar (e de aprender) deve ser visto a cada dia como algo novo: um recomeçar, uma escalada a um ponto mais alto que ainda não se alcançou, uma troca de papéis – o mestre que sempre ensina, de repente é também aprendiz; não há conhecimento absoluto, pois tudo está em constante transformação.

Segundo os Parâmetros Curriculares Nacionais (PCNs) para terceiro e quarto ciclos do Ensino Fundamental, o exercício da indução e da dedução em Matemática reveste-se de importância no desenvolvimento da capacidade de resolver problemas, o que assegura um papel de relevo ao aprendizado dessa ciência em todos os níveis de ensino. Smullyan (2000), em seu livro *Alice no País dos Enigmas*, traz circunstâncias em que um problema é uma situação que demanda a realização de uma sequência de ações ou operações para obter um resultado. O enigma a seguir, a título de exemplificação, é a terceira historia do segundo

capitulo, intitulado *Quem roubou as tortas?*. As duas primeiras historias fazem referencia as tentativas frustradas da Rainha de Copas de preparar saborosas tortas, a pedido do rei. A cada tentativa, percebia-se que algum dos ingredientes havia sido roubado. Uma terceira tentativa de fazer as tortas compõe a terceira historia:

> –Bem, aqui está sua farinha –disse o Rei, satisfeito –, de modo que agora você pode fazer as tortas.
>
> - Fazer as tortas sem pimenta? –perguntou a Rainha.
>
> - Pimenta! –exclamou o Rei, incrédulo. Quer dizer que você usa pimenta em suas tortas?
>
> - Não muita – respondeu a Rainha.
>
> - E suponho que ela tenha sido roubada!
>
> - É claro! –disse a Rainha. Encontre a pimenta e, quando descobrir quem a roubou, corte-lhe...
>
> - Vamos, vamos! –disse o Rei.
>
> Bem, a pimenta tinha que ser encontrada, é claro. Agora, como todos vocês sabem, as pessoas que roubam pimenta nunca dizem a verdade.
>
> (...)
>
> Então, continuando a historia, o suspeito mais obvio era a cozinheira da duquesa. No juramento ela fez apenas uma declaração: – Eu sei quem roubou a pimenta!
>
> Supondo que a pessoa que roubou a pimenta sempre mente, a cozinheira é culpada ou inocente?
>
> PORTANTO QUEM ROUBOU A PIMENTA? Bem os suspeitos seguintes do Rei foram a Lebre de Março, o Chapeleiro Louco e o Leirão. Os soldados foram mandados as casas deles, mas nenhuma pimenta foi encontrada. Mesmo assim, eles poderiam estar escondendo-a em algum lugar, de modo que foram detidos, com base nos princípios gerais.
>
> No julgamento, a Lebre afirmou que o Chapeleiro era inocente e o Chapeleiro afirmou que o Leirão era inocente. O Leirão resmungou uma declaração qualquer enquanto dormia, mas ela não foi registrada.
>
> Como se constatou, nenhum inocente fizera uma afirmação falsa, e (como estamos lembrando) as pessoas que roubam pimenta nunca fazem afirmações verdadeiras. Além disso, a pimenta foi roubada por apenas uma criatura. Qual dos três é o culpado, se é que foi um deles?
>
> Então quem roubou a pimenta? –ora, ora, esse é realmente um caso difícil! –disse o Rei.
>
> Os suspeitos seguintes, curiosamente, foram o Grifo, a Falsa Tartaruga e a Lagosta. No julgamento, o Grifo afirmou que a Falsa Tartaruga era inocente, e a Falsa Tartaruga disse que a Lagosta era culpada.
>
> Mas uma vez, nenhum inocente mentiu e nenhum culpado disse a verdade.
>
> Quem roubou a pimenta? (Smullyan, 2000, p.21-23)

Neste problema, o "resolvedor" deverá pensar em uma série de pensamentos lógicos encadeados que levam à conclusão de quem roubou a pimenta: a Lagosta. Na resolução, fará uso de uma importante ferramenta matemática, qual seja a demonstração por redução ao absurdo, pois deve considerar cada personagem culpado para que possa provar sua inocência, a partir da análise dos dados e hipóteses.

O conhecimento matemático ganha significado quando os alunos têm situações desafiadoras para resolver e trabalham para desenvolver estratégias de resolução. Ou seja, a solução não está disponível de início, mas é possível construí-la. Resolver um problema não se resume em compreender o que foi proposto e em dar respostas aplicando procedimentos adequados. Aprender a dar uma resposta correta, que tenha sentido, pode ser suficiente para que ela seja aceita e até seja convincente, mas não é garantia de apropriação do conhecimento envolvido.

4.3 História da Matemática nos Parâmetros Curriculares Nacionais: Uma Relação com o Ensinar e o Aprender

No texto de introdução dos Parâmetros Curriculares Nacionais de Matemática dos ciclos finais do Ensino Fundamental, lançado no final dos anos noventa, a matemática aparece como um forte filtro social na seleção dos alunos que vão concluir, ou não, o Ensino Fundamental ou o Ensino Médio. A matemática, então, é apresentada sob a marca de uma crise que se estende a todos os níveis da educação, como numa aflição generalizada. Segundo os PCNs de Matemática para o Ensino Fundamental (1997), "a História da Matemática pode oferecer uma importante contribuição ao processo de ensino e aprendizagem dessa área do conhecimento". Conhecer como se deu a construção de determinado conceito matemático pode ser um aliado útil na hora de resolver determinadas questões e situações que se lançam ao aluno.

Entender uma questão, muitas vezes, depende de saber a historia da ideia. A História da Matemática pode oferecer uma importante contribuição ao processo de ensino e aprendizagem dessa área do conhecimento. Ao abordar-se a História da Matemática não se deve focar na reprodução dos textos escritos, com a finalidade de perpetuar a historia de uns, deixando no anonimato outros sujeitos que construíram o cotidiano das relações socioculturais, econômicas e políticas. No processo pedagógico é importante que o professor possibilite ao aluno o entendimento de que as sociedades nem sempre adotam o mesmo modo de resolução de um problema, como também há mudanças significativas nas técnicas de cálculo e que estas foram elaboradas, ao longo das eras históricas, de acordo com as necessidades da humanidade.

Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor cria condições para que o aluno desenvolva atitudes e valores mais favoráveis diante desse conhecimento. Além disso, conceitos abordados em conexão com sua história constituem veículos de informação cultural, sociológica e antropológica de grande valor formativo.

Berlinghoff e Gouvêa (2010) discutem como a história da matemática se relaciona com o ensinar-aprender tal disciplina na escola:

> Então, qual é uma boa maneira de usar a história da matemática na sala de aula? A primeira resposta que vem à mente provavelmente é "contar histórias" – episódios históricos ou, mais comumente, informação biográfica. (...) Uma maneira de usar história é fornecer uma visão mais ampla. É muito comum que os estudantes pensem na matemática da escola como uma coleção arbitrária de pedaços de informação. Mas não é assim que a matemática é criada. (...) A história, muitas vezes, ajuda fornecendo contexto. A matemática, afinal, é um produto cultural. É criada por pessoas em um momento e lugar dados e frequentemente é afetada por esse contexto. Saber mais sobre isso ajuda a entender como a matemática se ajusta a outras atividades humanas (p. 1 e 3)

Em muitas situações, o recurso à História da Matemática pode esclarecer ideias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas a alguns porquês e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento. Numa educação que visa à autonomia do pensamento.

CAPÍTULO 5 - CRIPTOGRAFIA NA ESCOLA

A matemática na escola pode, e deve, ser uma experiência significativa, do tipo que possibilita novos aprendizados. A lei da sala de aula como o lugar onde se impõe a cultura do silêncio, o silêncio do exercício, no que diz respeito a fazer e não discutir as soluções, a ler e não entender nada, a refletir e não encontrar respostas, nem formular perguntas, é incabível numa perspectiva de Educação emancipadora.

As atividades a seguir são pautadas nas ideias de que é possível e preciso resolver e criar problemas. A criptografia pode ser utilizada para isso, ajudando o aluno a desenvolver um raciocínio lógico.

Os problemas matemáticos não precisam ser obrigatórios para serem resolvidos, eles precisam ser bem recomendados e bem apresentados. Talvez, a propaganda ainda seja a alma do negócio. Com efeito, muitas vezes, um conhecimento não precisa ser explicado, precisa ser sentido: "antes de ser o ato do pedagogo, a explicação é o mito da pedagogia" (RANCIÈRE, 2002, p.20). É a falta de densidade, de materialidade, de concreção, de significação para os outros, que faz da prática matemática um caos educativo:

> "Quantos estudantes, por exemplo, se tornaram insensíveis às ideias e quantos perdem o ímpeto por aprender, devido ao modo por que experimentam o ato de aprender? [...] Quantos acabam por associar o processo de aprendizagem com algo de enfadonho e tedioso?" (DEWEY, 1979, p.15).

Segundo Rancière (2002), pode-se ensinar qualquer coisa mesmo sendo ignorante no assunto, mas é preciso emancipar o aluno, ou seja, permitir que use sua própria inteligência. O que é realmente importante é que os alunos aprendam a aprender. Não é necessário ter explicações para haver aprendizagem. Ao contrário, a palavra do mestre emudece a matéria dada, pois condiciona o aprendiz à explicação. Os alunos podem aprender através da pesquisa e desta maneira, não é preciso saber o conteúdo, mas sim, como aprendê-lo.

Precisamos primeiro entender porque ensinamos matemática em nossas escolas e o verdadeiro papel deste conhecimento na formação do aluno; mais do que um item necessário em atividades práticas que envolvem questões quantitativas ou no desenvolvimento do raciocínio lógico, a matemática é importante porque foi (e ainda é) a base da construção de inúmeros conhecimentos, seja na própria invenção da escrita, na organização do tempo histórico, na representação dos territórios geográficos, seja no desenvolvimento de teorias e conceitos dentro do próprio universo dos números.

Neste capítulo, serão apresentadas sugestões de atividades que envolvem a criptografia. Essas atividades farão uso dos números primos e outros conceitos matemáticos que os estudantes aprendem em sua jornada escolar. Somente a primeira atividade foi aplicada durante a pesquisa. Os demais, são problemas que vão dos mais simples aos mais elaborados (que envolvem conteúdos de anos finais do Ensino Médio). Considerando-se que a educação quando usa o pensar como instrumento deve lembrar que a matemática, bem como as demais disciplinas, caracteriza-se pela construção de sentidos:

> "Quem sabe conseguíssemos ver poeticamente o aprender e o ensinar. Estar em estado de poesia nos levaria a perceber a dimensão poética da matemática, da história, da biologia, das ciências como um todo. Preocupar-nos-íamos não apenas com o ensinar, mas com o 'deixar aprender' antecipado por Heidegger" (LEAL, 2004, p. 29).

5.1 A criptografia intuitiva

A primeira noção de criptografia parece ser natural aos nossos jovens, eles criam um código para escrever mensagens em seus diários e/ou para trocarem mensagens entre si. Geralmente, estes códigos costumam serem símbolos que representam letras. O docente pode utilizar esta ideia para introduzir a noção de criptografia e seus elementos, assim como a necessidade de um código seguro para evitar a decodificação.

A atividade a seguir foi aplicada em uma turma de 6º ano do Ensino Fundamental da rede pública municipal do Rio de Janeiro, na escola municipal Prefeito Juarez Antunes, situado em Bangu, zona oeste. A turma é composta por 42 alunos, com faixa etária de 11 a 13 anos. A organização da atividade não encontrou problemas, pois a sala de aula é estruturada de maneira que as carteiras estejam agrupadas de dois em dois, além de não ter sido necessário recursos materiais ou tecnológicos, apenas lápis/caneta e papel.

Inicialmente foi proposto que os alunos criassem códigos em duplas para as 26 letras do nosso alfabeto e os dez algarismos, alguns utilizaram símbolos diversos aleatórios (figuras 7 e 8), outros utilizaram figuram relacionadas a letras, onde cada símbolo tinha como inicial do nome a letra correspondente (figura 9) e outros associaram a cada letra, números, em um processo próximo as primeiras criptografias (figura 10).

Figura 7 – Criptografia aleatória do Grupo 1

Figura 8 – Criptografia aleatória do Grupo 7

Figura 9 – Criptografia relacionada do Grupo 5

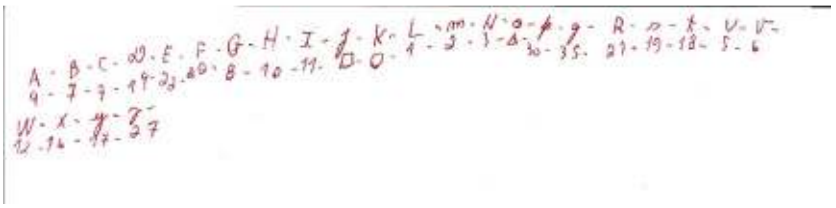


Figura 10 – Criptografia aleatória do Grupo 2

O objetivo desta atividade foi apresentar a criptografia aos alunos e tentar responder, ainda que parcialmente, a grande indagação de nossos educandos (para que serve a matemática?). Em seguida, cada dupla, escreveu uma mensagem usando seu código e depois trocou com outra para que tentassem quebrar o código. No decorrer da atividade, eles perceberam que quanto mais aleatório era o código criado, mais difícil se tornava a sua leitura e quanto maior a mensagem escrita, mais símbolos eles conseguiam associar às letras e números, em uma noção intuitiva da análise de frequência das letras nas palavras da Língua Portuguesa.

Ao fim, concluíram que se eu não possuo a chave de decodificação, não consigo ler a mensagem ou, até conseguiria, se conseguisse saber como o código foi pensado. Abaixo, as mensagens escritas com base nos códigos anteriores (figura 11).

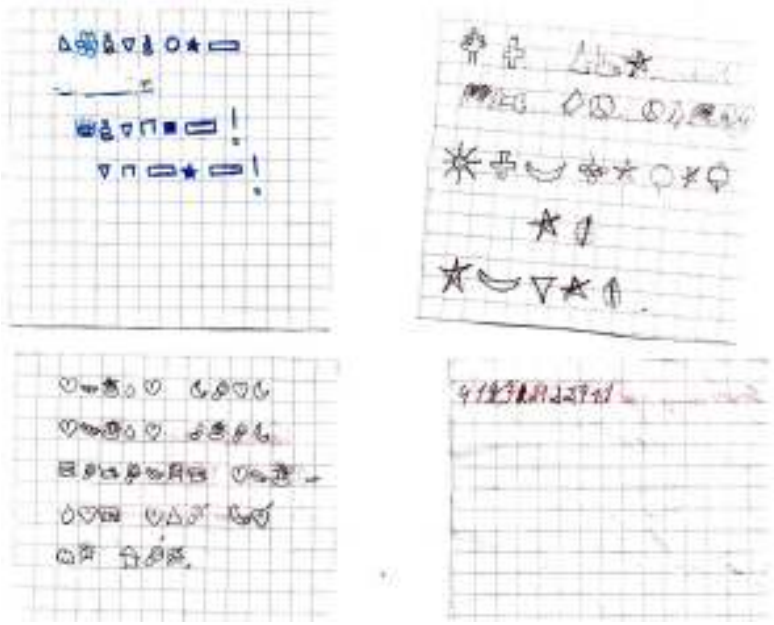


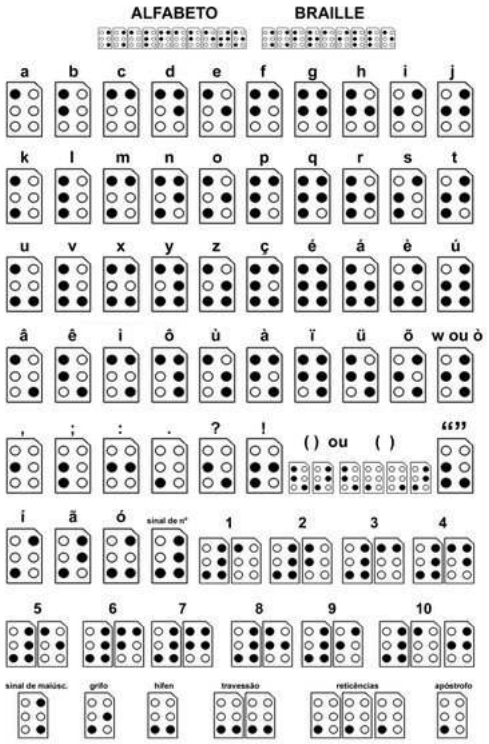
Figura 11 – Mensagens codificadas

5.2 Criptografando com a Escrita Braille

O objetivo desta atividade é tentar compreender como é possível relacionar diferentes representações de uma mesma ideia, como os números e as letras, para tanto faremos um estudo da escrita Braille, utilizada pelos deficientes visuais, compreendendo-a como uma maneira de criptografar uma mensagem/texto.

O Sistema Braille é formado pelo arranjo de seis pontos em relevo, dispostos em duas colunas de três pontos. Os seis pontos formam o que se convencionou chamar "cela Braille". Para facilitar sua identificação, os pontos são numerados da seguinte forma, do alto para baixo: coluna da esquerda, pontos 1, 2, 3, coluna da direita, pontos 4, 5, 6. As diferentes

disposições desses seis pontos permitem a formação de 63 combinações, ou símbolos Braille (figura 12).



Fonte: Projeto Nova Visão. Disponível em:< http://projetonovavisao.spaceblog.com.br/1231591/O-QUE-E-O-METODO-BRAILLE/>. Acesso em 25 mar 2013
Figura 12 – Sistema Braille

As dez primeiras letras do alfabeto (a –j) são formadas pelas diversas combinações possíveis dos quatro pontos superiores (1, 2, 4, 5); as dez letras seguintes são as combinações das dez primeiras letras, acrescidas do ponto 3, e formam a segunda linha de sinais. A terceira linha é formada pelo acréscimo dos pontos 3 e 6 às combinações da primeira linha. Os mesmos sinais da primeira linha, na mesma ordem, assumem características de valores numéricos 1-0, quando precedidas do sinal do número (formado pelos pontos 3456).

A escrita Braille é um código que possibilita a comunicação entre as pessoas que conhecem seu funcionamento; como atividade a ser realizada com a turma propõe-se que seja apresentado aos alunos o sistema Braille, além de um exercício de aprendizado de criptografia, tal atividade terá um caráter conscientizador, possibilitando que os alunos compreendam a importância de se criar recursos para os portadores de necessidades especiais. Pode-se criar textos em Braille que envolvam conceitos matemáticos e trabalhar com comunicações deste tipo.

Deve-se iniciar a atividade com a apresentação de um texto em Braille, utilizando o esquema da figura 12. Algumas embalagens descartáveis (figuras 13, 14 e 15) possuem a inscrição em Braille, é interessante levá-las para a sala de aula e pedir que os alunos decifrem. Esta atividade servirá para os alunos compreenderem o conceito de criptografar uma mensagem, qual seja, escrever um texto em que apenas as pessoas que conhecem a maneira como é feito pode ler.

Fonte: Revista Época
Figura 13- Embalagem de cosmético com escrita Braille

Fonte: Conselho Regional de Farmácia do Paraná. Disponível em: < http://www.crf-pr.org.br/site/noticia/visualizar/id/3891/?Anvisa_quer_receita_para_remedio_tarja_vermelha.html>. Acesso em 25 mar 2013.
Figura 14- Embalagem de remédio com escrita Braille

Fonte: Portal do Professor
Figura 15- Embalagem de bala com escrita Braille

Quando os alunos estiverem familiarizados com o sistema Braille, pode-se "escrever" textos; para tanto, uma alternativa é recortar fichas retangulares e perfurar os círculos marcados em preto com um furador de papel, depois, eles trocam as mensagens. Esta é uma noção que pode ser também apresentada através do Código Morse (figura 16), visualmente (com pontos e traços) ou auditivamente (com batidas curtas e longas).

Símbolo	Código	Símbolo	Código
A	·–	W	·––
B	–···	X	–··–
C	–·–·	Y	–·––
D	–··	Z	––··
E	·	1	·––––
F	··–·	2	··–––
G	––·	3	···––
H	····	4	····–
I	··	5	·····
J	·–––	6	–····
K	–·–	7	––···
L	·–··	8	–––··
M	––	9	––––·
N	–·	0	–––––
O	–––	ponto final	·–·–·–
P	·––·	vírgula	––··––
Q	––·–	ponto de interrogação	··––··
R	·–·	dois pontos	–––···
S	···	ponto e vírgula	–·–·–·
T	–	hífen	–····–
U	··–	barra	–··–·
V	···–	aspas	·–··–·

,

Fonte: O Livro dos Códigos, p. 80.
Figura 16 – Código Morse

5.3 A cifra de César

Pensamos, normalmente, a criptografia inserida na informática, pensamos a informática antes da criptografia. Pensamos até mesmo que a criptografia foi inventada para a era digital. Escrever mensagens cifradas, utilizando os métodos que deram origem à criptografia é um importante fator de ensino-aprendizagem de algo que tornou possível trocar as informações da maneira que fazemos hoje, que já guiou exércitos e escondeu frases românticas de adolescentes; por não poder expressar seu amor publicamente, os jovens apaixonados da Inglaterra vitoriana começaram a trocar mensagens codificadas através dos jornais, em colunas dedicadas às mensagens dos leitores. Essas colunas ficaram conhecidas como "colunas de óbito" (SINGH, 2003).

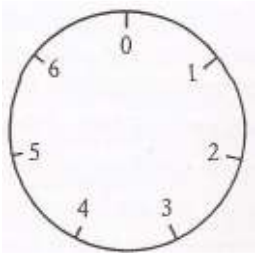
Como experiência de pensamento com outros, essas atividades entram na escola para dar espaço à criação, para gerar tempo de pensamento que suspende o não-pensar em prol da atividade livre. A Cifra de Cesar consiste em deslocar as letras do alfabeto em três posições:

> "Discutivelmente, o esquema de criptografia mais antigo é a Cifra de Cesar, que recebeu esse nome em homenagem a Júlio Cesar, que usou este esquema para proteger importantes mensagens militares (todas as mensagens de César eram escritas em Latim, naturalmente, o que as tornava incompreensíveis para a maioria das pessoas). A Cifra de Cesar é uma maneira simples de confundir uma mensagem escrita em linguagem que forma palavras a partir de um alfabeto. (GOODRICH, 2004. Pag. 112)"

Na Cifra de César, para dificultar a decodificação, caso a mensagem seja interceptada por um inimigo, é comum remover os espaços entre as letras no texto cifrado. Importante ressaltar, que ao inserir atividades com a Cifra de César (assim, como nas atividades dos itens anteriores e do próximo) não estamos fazendo, propriamente, o ensino de uma matemática formal, de algum conteúdo pré-estabelecido nos currículos escolares, e, sim, um exercício prático de raciocínio e matemática criptográfica em situação educativa.

Nesta atividade, é interessante que o aluno faça outros deslocamentos para codificar uma mensagem, assim vai compreender o funcionamento da Régua de Saint'Cyr e do Quadrado de Vigenère (que serão descritos na seção 5.4), pois, o sistema de encriptação de uma cifra de César serve frequentemente de base ou é incorporado como parte de esquemas mais complexos (como a cifra de Vigenère) e continua tendo aplicações, como no sistema ROT13[2].

Para aqueles que não acreditam que uma atividade possa ter finalidade em si mesma, a Cifra de Cesar também pode ser representada usando aritmética modular. Não é preciso utilizar a representação que conhecemos. A ideia é trabalhar com os restos; para tal, podemos utilizar a "aritmética dos relógios", onde os possíveis restos da divisão por um número são dispostos como no mostrador do relógio (figura 17) ou utilizar a divisão euclidiana.



Fonte: O Livro dos Códigos, p. 288.
Figura 17 – Relógio do módulo 7

O primeiro passo é transformar as letras em números, de acordo com o esquema: $A = 1, B = 2, C = 3, D = 4, \dots, X = 24, Y = 25,\ Z = 26$, termos também a representação do espaço, que será o número zero. Tomemos, $\gamma = texto\ cifrado,\ \delta = deslocamento, \rho = texto\ simples$, temos $\gamma \equiv \rho + \delta\ (mod\ 27)$.

Como exemplo, considere um deslocamento de cinco letras e o texto QUERO APRENDER A CRIPTOGRAFAR COM VOCÊ, temos $\delta = 5$:

- Para criptografar Q, $\rho = 17$, daí $\gamma \equiv 22\ (mod\ 27)$, como 22 é a letra V, temos a cifra da primeira letra.
- Para criptografar U, $\rho = 21$, daí $\gamma \equiv 26\ (mod\ 27)$, daí temos a letra Z.
- Para criptografar E, $\rho = 5$, daí $\gamma \equiv 10\ (mod\ 27)$, daí temos a letra J.
- Para criptografar R, $\rho = 18$, daí $\gamma \equiv 23\ (mod\ 27)$, daí temos a letra W.
- Para criptografar O, $\rho = 15$, daí $\gamma \equiv 20\ (mod\ 27)$, daí temos a letra T.

A primeira palavra do nosso texto será VZJWT. O espaço também será deslocado, temos $\rho = 0$, daí $\gamma \equiv 5\ (mod\ 27)$, daí temos a letra E. Continuando este processo, teremos:

VZJWTEFUWJSIJWEFEHWNUYTLWFKFWEHTRE

Observemos que na palavra VOCÊ:

[2] ROT13(ROTATE BY 13 PLACES) é um sistema de substituição, aplicado na língua inglesa, parecido com a Cifra de César, com um deslocamento de 13 posições.

- Para criptografar V, $\rho = 22$, daí $\gamma \equiv 27\ (mod\ 27)$, como $27 \equiv 0\ (mod\ 27)$ e 0 representa espaço, temos a cifra de V.

Terminando a cifragem temos nossa mensagem final :

VZJWTEFUWJSIJWEFEHWNUYTLWFKFWEHTRETHJ.

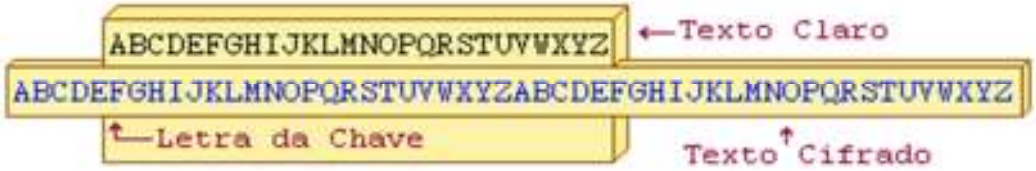
Se o objetivo é decifrar uma mensagem basta fazer $\rho \equiv \gamma - \delta\ (mod\ 27)$. Considere a mensagem criptografada: IWXYHEV; sabendo que utilizamos um deslocamento $\delta = 4$, vamos decodificar a mensagem:

- Para decifrar I, $\gamma = 9$, daí $\rho \equiv 9 - 4(mod\ 27)$ e $\rho = 5$, daí temos a letra E.
- Para decifrar W, $\gamma = 23$, daí $\rho \equiv 23 - 4(mod\ 27)$ e $\rho = 19$, daí temos a letra S.
- Para decifrar X, $\gamma = 24$, daí $\rho \equiv 24 - 4(mod\ 27)$ e $\rho = 20$, daí temos a letra T.
- Para decifrar Y, $\gamma = 25$, daí $\rho \equiv 25 - 4(mod\ 27)$ e $\rho = 21$, daí temos a letra U.
- Para decifrar H, $\gamma = 8$, daí $\rho \equiv 8 - 4(mod\ 27)$ e $\rho = 4$, daí temos a letra D.
- Para decifrar E, $\gamma = 5$, daí $\rho \equiv 5 - 4(mod\ 27)$ e $\rho = 1$, daí temos a letra A.
- Para decifrar V, $\gamma = 22$, daí $\rho \equiv 22 - 4(mod\ 27)$ e $\rho = 18$, daí temos a letra R.

A mensagem que recebemos foi ESTUDAR.

5.4 Aparatos de Criptografar

A régua de Saint'Cyr é composta por uma tira longa de papel ou cartolina, denominada "stator" ou parte fixa, que contém um alfabeto ordenado clássico, e por uma segunda tira, móvel e mais comprida que a primeira, contendo dois alfabetos sucessivos. Tradicionalmente, o alfabeto claro (mensagem original) é colocado na parte fixa (figura 18).



Fonte: Códigos Secretos. Disponível em:<>. Acesso em 15 mar 2013.
Figura 18 – Régua de Saint'Cyr

Este tipo de régua permite fazer substituições monoalfabéticas, basta deslocar a parte móvel o número de letras correspondente ao deslocamento desejado. Para cifrar o texto, troca-se a letra da parte fixa pela letra que lhe corresponder na parte móvel, utilizando para tanto a palavra chave de codificação. Por exemplo: Para cifrar a frase OS NÚMEROS PRIMOS SÃO FUNDAMENTAIS NA CRIPTOGRAFIA com a palavra-chave REGUA; primeiro desloca-se à parte móvel para alinhar o R com o A da parte fixa, a seguir, procura-se a letra O na parte fixa e substitui-se pelo F. Para trocar a segunda letra posiciona-se a parte móvel da régua de modo que o E fique alinhado com o A da parte fixa, depois se localiza o S no alfabeto claro e troca-se pelo W. Desloca-se novamente a parte móvel para alinhar o G com o A da parte fixa e se substitui o N por T, e assim sucessivamente. Nossa mensagem resultará em

FWTAMVVUMPRMSISKEUZUEHGGEEXGCSEEILIGZUARRJOU.

O mesmo procedimento utilizado para codificar uma mensagem pela régua de Saint'Cyr é empregado na Cifra de Vigenère, que utiliza 26 alfabetos cifrados diferentes para codificar uma mensagem. Para tanto usamos o Quadrado de Vigenère (figura 19) composto pelo alfabeto escrito em sua ordem usual, seguido de 26 alfabetos cifrados, cada alfabeto com deslocamento de uma casa à frente no mesmo alfabeto, seguindo o princípio do Código de César. Na linha superior estão disponíveis as letras do texto puro. Através de uma chave a ser utilizada, encontra-se a primeira letra da chave na coluna vertical esquerda e a letra desta intersecção é a letra correspondente, criptografada.

Utilizando a Cifra de Vigenère, após um período longo de trabalho acaba tornando-se comum a existência de erros devido à dificuldade de visualização das letras. Neste sentido, a Régua de Saint'Cyr é mais prática, ou ainda, o disco de Cifras pode ser menos enfadonho.

Apresentar estes métodos criptográficos iniciais é uma maneira de anunciar o conceito de criptografia, assim como de trabalhar o raciocínio através da codificação/decodificação de mensagens.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	P	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Figura19 – Quadro de Vigenère

5.5 Criptografando com Funções Invertíveis

As atividades propostas nessa seção e na seção 5.6 foram inspiradas nas ideias de Tamarozzi (2001)

Podemos criptografar uma mensagem utilizando uma função, onde a mensagem enviada ao receptor será uma sequência de números; para isto associamos a cada letra do alfabeto um número, como na Tabela 2:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
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

Tabela 2- Valor numérico de cada letra utilizada na criptografia para função

A seguir, escolhemos uma função cifradora, que pode ser uma função afim ou exponencial ou logarítmica. A mensagem a ser transmitida ao receptor deve ser a sequência numérica obtida pela imagem da função. Quando o receptor receber a mensagem ele deverá calcular a imagem de f^{-1}.

Vamos utilizar a função afim $f(x) = 2x + 3$ e queremos decodificar a mensagem EU ESTUDO MATEMÁTICA. Temos:

- $E = 5$, então $f(5) = 2.5 + 3 = 13$
- $U = 21$, então $f(21) = 2.21 + 3 = 45$
- $S = 19$, então $f(19) = 2.19 + 3 = 41$
- $T = 20$, então $f(20) = 2.20 + 3 = 43$
- $D = 4$, então $f(4) = 2.4 + 3 = 11$
- $O = 15$, então $f(15) = 2.15 + 3 = 33$

Assim, continuando a codificar as letras, teremos a mensagem 13 45 13 41 43 45 11 33 29 5 43 13 29 5 43 21 9 5. Quem receber a mensagem precisa da função inversa $f^{-1}(x) = \frac{x-3}{2}$; esta será a nossa chave de decodificação.

Um aspecto interessante é supor que o receptor tenha perdido a chave ou que a mensagem tenha sido interceptada; se o intruso souber que a mensagem foi codificada utilizando-se uma função inversa, fica fácil quebrar o código, já que seriam necessárias apenas duas associações corretas para determinar a lei da função, o que pode ser feito através da análise de frequências.

É possível escolher, também, uma função exponencial, levando-se em consideração que, para este tipo de função, os cálculos ficam cada vez maiores e mais complicados, podendo-se fazer uso da calculadora. Consideremos a função $f(x) = 2^x$ e a mensagem CRIPTOGRAFIA temos:

- $C = 3$, então $f(3) = 2^3 = 8$;
- $R = 18$, então $f(18) = 2^{18} = 262144$;
- $I = 9$, então $f(9) = 2^9 = 512$;
- $P = 16$, então $f(16) = 2^{16} = 65536$;
- $T = 20$, então $f(20) = 2^{20} = 1048576$;
- $O = 15$, então $f(15) = 2^{15} = 32768$;
- $G = 7$, então $f(7) = 2^7 = 128$;
- $A = 1$, então $f(1) = 2^1 = 2$;
- $F = 6$, então $f(6) = 2^6 = 64$;

Nossa mensagem fica: 8 262144 512 65536 1048576 32768 128 2 64. Observemos que mesmo uma mensagem pequena gerou números grandes e que para decodifica-la precisamos trabalhar com a inversa da função exponencial, que é a função logarítmica. Se quisermos decodificar nossa mensagem teremos:

$x = \log_2 8 = 3$	$x = \log_2 262144 = 18$	$x = \log_2 512 = 9$
$x = \log_2 65536 = 16$	$x = \log_2 1048576 = 20$	$x = \log_2 32768 = 15$
$x = \log_2 128 = 7$	$x = \log_2 2 = 1$	$x = \log_2 64 = 6$

Esta é uma atividade que possibilita o trabalho com funções e reforça o conceito de inversa de funções (principalmente de que a inversa da função exponencial é a função logarítmica).

5.6 Criptografando com Matrizes

No que diz respeito ao processo de ensino-aprendizagem de matrizes, podemos dizer que este se caracteriza pela repetição de exercícios pouco motivadores para os alunos. Segundo Sanches (2002, p.6) o ensino de matrizes apresenta-se em "total descompasso com os avanços tecnológicos".

Uma maneira de codificar mensagens utiliza-se de matrizes. Para tal é preciso escolher uma matriz codificadora, de ordem n, invertível, pois a inversa será a matriz decodificadora.

Seja a matriz $A = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix}$, a matriz codificadora. Utilizaremos a associação de letras da tabela 2 para escrever minha mensagem. Quero criptografar SOU MENINA, minha matriz a ser criptografada é $\begin{bmatrix} 19 & 15 & 21 & 13 & 5 \\ 14 & 9 & 14 & 1 & 1 \end{bmatrix}$; como temos um número ímpar de letras, vamos repetir a última letra. A minha matriz mensagem a ser enviada será:

$$B = A.M = \begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 19 & 15 & 21 & 13 & 5 \\ 14 & 9 & 14 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 47 & 33 & 49 & 15 & 7 \\ 71 & 54 & 77 & 40 & 16 \end{bmatrix}$$

Que equivale a sequência numérica: 47 33 49 15 7 71 54 77 40 16. Para ler a mensagem recebida, devemos encontrar a matriz inversa de A e calcular $A^{-1}.B$.

Supondo que tenhamos recebido a mensagem criptografada $\begin{bmatrix} 38 & 31 & 54 & 26 & 31 \\ 34 & 18 & 57 & 63 & 18 \end{bmatrix}$ onde foi utilizada a matriz A acima. Temos que $A^{-1} = \begin{bmatrix} -1/5 & 2/5 \\ 3/5 & -1/5 \end{bmatrix}$, daí,

$$A^{-1}B = \begin{bmatrix} 6 & 1 & 12 & 20 & 1 \\ 16 & 15 & 21 & 3 & 15 \end{bmatrix}.$$

Então, nossa mensagem é: FALTA POUCO.

5.7 Criptografando com Computadores

Nesta atividade, o objetivo é mostrar para os alunos como funciona a criptografia utilizada nas transações bancárias ou compras pela internet. Para tal utilizaremos primos bem pequenos, que possibilitem o cálculo e facilitem o entendimento. Nossa intenção não é falar de conceitos avançados da matemática ou de toda teoria dos números, mas mostrar porque e

como utilizamos um sistema criptográfico usando números primos, ou seja, discutir o porquê do RSA estar se mostrando tão seguro.

Será construída uma "Tabela de Chaves" (Tabela 3) com os alunos, ou seja, cada aluno publicará sua chave para toda a turma. Os alunos devem seguir o comando do professor e seguir o seguinte passo-a-passo:

- Escolham dois números primos diferentes, que chamaremos de a e b;
- Chamem de n, a multiplicação dos números acima;
- Chamem de m, a multiplicação $(a-1).(b-1)$;
- Encontre o primeiro número primo que não divida m; chame este número de e;
- Divulgue na "Tabela de Chaves" a sua chave pública, que será (n, e).

Aluno 1	Aluno 2	Aluno 3	Aluno 4	Aluno 5	Aluno 6	Aluno 7	Aluno 8
$(55,3)$	$(77,7)$	$(1081,3)$	...	...	...	...	

Tabela 3 – Tabela de Chaves

Neste momento, qualquer aluno já pode enviar mensagens criptografadas ao criador da chave. Suponha que um aluno queira enviar a mensagem BEIJOS para o Aluno 1, cuja chave é $(55,3)$:

- Transforme cada letra da mensagem em um número conforme tabela 4 abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
11	12	13	14	15	16	17	18	19	20	21	22	23
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
24	25	26	27	28	29	30	31	32	33	34	35	36

Tabela 4 - Valor numérico de cada letra utilizada na criptografia RSA

Temos: 12 – 15 – 19 – 20 – 25 – 29.

- Separe os números que formam a mensagem algarismo por algarismo (ou reagrupe-os de modo que sempre formem números menores que n), chame cada algarismo de x (1 – 21 – 5 – 1 – 9 – 20 – 2 – 5 – 2 – 9);
- Cada número codificado será o resto da divisão de x^e por n. Teremos:

$1^3 = 1$, que deixa resto 1 na divisão por 55.	$2^3 = 8$, que deixa resto 8 na divisão por 55.	$5^3 = 125$, que deixa resto 15 na divisão por 55.
$9^3 = 729$, que deixa resto 14 na divisão por 55.	$20^3 = 8000$, que deixa resto 25 na divisão por 55.	$21^3 = 9261$, que deixa resto 21 na divisão por 55.

A mensagem enviada ao Aluno 1 será: 1 – 21 – 15 – 1 – 14 – 25 – 8 – 15 – 8 – 14. Este aluno deseja ler a mensagem que recebeu para tanto precisa encontrar a chave de decodificação:

- Encontrar o número d, que quando multiplicado por e, deixa resto 1 na divisão por m. Para essa etapa, deve-se utilizar o computador, já que o cálculo de d pressupõe o conhecimento do Algoritmo de Euclides Estendido.

O aluno 1 obterá $d = 27$. A chave de decodificação do Aluno 1 é: $(55,27)$.

- Para ler a mensagem deve calcular o resto da divisão de cada número recebido elevado à d, por n e substituir na mensagem.

1^{27}deixa resto 1 na divisão por 55.	8^{27} deixa resto 2 na divisão por 55.	14^{27}deixa resto 9 na divisão por 55.
15^{27}deixa resto 5 na divisão por 55.	21^{27} deixa resto 21 na divisão por 55.	25^{27}deixa resto 20 na divisão por 55.

Observe que os cálculos da etapa acima não podem ser feitos apenas com lápis e papel, é necessário o uso de computação (planilhas eletrônicas ou calculadoras científicas). O Aluno 1 passará a ler a mensagem recebida assim: 1 – 21 – 5 – 1 – 9 – 20 – 2 – 5 – 2 – 9.

- Basta separar os valores obtidos em blocos com dois algarismos e fazer a substituição dos números pelas letras, de acordo com a tabela utilizada para criptografar a mensagem.

O Aluno 1 terá: 12 – 15 – 19 – 20 – 25 – 29. Obtendo a mensagem que lhe foi enviada: BEIJOS. É interessante propor que os outros alunos tentem quebrar a chave do Aluno 1 (por exemplo), para isso é preciso discutir o que é necessário para se achar a chave de decodificação, ou seja, o único valor desconhecido d, é obtido a partir do valor m, que apenas o Aluno 1 sabe qual é. No entanto, se descobrimos quem é a e b, obtemos m. Neste momento, é preciso fatorar n, que é conhecido por todos.

Para que os alunos não saiam com a ideia de que é possível quebrar facilmente o sistema RSA, faz-se necessário pedir que fatorem outros números maiores e informar que não conhecemos algoritmos capazes de encontrar fatores primos grandes rapidamente, mesmo com o auxílio de computadores muito potentes.

O professor pode ainda levar uma mensagem criptografada com o sistema RSA e, distribuindo a chave pública pedir que decodifiquem a mensagem. Suponha que a mensagem seja 304 – 210 – 44 – 297 – 1 criptografada pela chave $(391,3)$. Precisamos primeiro fatorar o número 391, que apesar de não ter fatores primos grandes, já causa um certo trabalho. Obtemos 17 e 23, e podemos saber que $m = 352$. Daí, $d = 352 - 117 = 235$, fazemos:

304^{235} deixa resto 111 na divisão por 391.	210^{235} deixa resto 311 na divisão por 391	44^{235} deixa resto 122 na divisão por 391	297^{235} deixa resto 53 na divisão por 391	1^{235} deixa resto 1 na divisão por 391

Resultando em 111311122531, que agrupados dois a dois ficam: 11 – 13 – 11 – 12 – 25 – 31. Observe que, como escolhemos números primos pequenos, ficou fácil decodificar (mesmo que os cálculos sejam extensos, é fácil obter os resultados na calculadora científica). Substituindo pelas letras correspondentes, temos a mensagem: ACABOU.

CAPÍTULO 6 - CONSIDERAÇÕES FINAIS

Esta pesquisa objetivou investigar como os números primos e outros elementos da chamada Teoria dos Números são abordados na escola e sua aplicabilidade na Criptografia, com o intuito de fazer uma conexão entre a Matemática teórica, ensinada na sala de aula, e a Matemática aplicada, estudando o desenvolvimento dos sistemas criptográficos para uma aplicação direta na sociedade na qual estamos inseridos.

Algoritmos criptográficos servem para ocultar informações sigilosas de qualquer pessoa desautorizada a lê-las. Assim, segurança sempre foi um assunto importante em desenvolvimento de sistemas criptográficos. De acordo com os estudos efetuados, a criptografia não se aplica apenas à informática, estando ela presente desde a Antiguidade, com padrões de criptografia definidos em décadas atrás que são vastamente utilizados.

Acreditando ser possível e necessária a diminuição da distância entre a matemática escolar e a matemática "útil", observou-se a importância da exploração de competências que auxiliem na resolução de problemas. Sabemos que a massificação do ensino brasileiro está feita; agora é preciso que os alunos aprendam a pensar. A criptografia pode ajudar os alunos na sua concentração e persistência perante a resolução de problemas.

O sistema de criptografia RSA depende bastante dos conceitos de Teoria dos Números, a base de cálculo dos algoritmos está vinculada fortemente ao uso de números primos, ao gerar primos aleatoriamente e ao fatorar inteiros grandes. Como não existe uma fórmula para calcular números primos, torna-se inviável calcular dois números primos a partir do resultado de sua multiplicação.

A prova de que este algoritmo é seguro é o uso recorrente na criptografia de hoje, tanto na transmissão via rede mundial de computadores, quanto em transações bancárias. Se alguém conseguir fatorar um número e encontrar os dois números primos que o formam, provavelmente ele recuperaria a informação inicial.

Muitos criptossistemas ficaram de fora deste trabalho e outras abordagens poderiam ter sido feitas. A criptografia tem muitos caminhos que podem ser percorridos e difíceis de serem aqui discutido em toda a sua complexidade. O meu desejo é que as atividades propostas neste trabalho sirvam para formar, como diria Morin, para além das cabeças bem cheias, cabeças bem feitas.

REFERÊNCIAS BIBLIOGRÁFICAS

A HIPÓTESE DE RIEMANN E A INTERNET (I). Disponível em:<http://www.somatematica.com.br/coluna/gisele/15022005.php>. Acesso em 08 abr 2013.

ADORNO, T. W. **Educação e Emancipação**. São Paulo: Paz e Terra, 1995.

ALVITES, J. C. V. **Hipótese de Riemann e física**. Universidade de São Paulo, São Carlos, 2012. Dissertação de Mestrado.

BERLINGHOFF, W. P.; GOUVÊA, F. Q. **A Matemática Através dos Tempos**: um guia fácil e prático para professores e entusiastas. 2 ed. São Paulo: Blucher, 2010.

BERNSTEIN, D. **Deterministic Polynomial:**Time Primality Tests. 2002.

BRAGA, B. R. **Algoritmo AKS**: Primalidade de um número em tempo polinomial. Universidade Federal do Rio de Janeiro, Rio de Janeiro, 2002.

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais**: 3º e 4º ciclos do Ensino Fundamental na Matemática. Brasília: MEC/SEF, 1997.

CABETTE, E. L. S.; NAHUR, M. T. M.; CABETTE, R. E. **Direito e Matemática**: uma abordagem interdisciplinar. Revista Jus Vigilantibus. N 269. Ano II, 2008.

Cipher Machines. Disponível em:< http://ciphermachines.com/jefferson>. Acesso em 5 mar 2013.

COUTINHO, S.C.; Primalidade em tempo polinomial: uma introdução ao algoritmo AKS. Rio de Janeiro, Sociedade Brasileira de Matemática (SBM), Coleção Iniciação Científica, 2004.

COUTINHO, S. **Números Inteiros e Criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2005.

COUTINHO, S. Introdução à Criptografia I. In: **Aritmética I**, material de disciplina do Mestrado Profissional em Matemática em Rede Nacional.

COSTA, V. A. **Formação e Teoria Crítica da Escola de Frankfurt**: trabalho, educação, indivíduo com deficiência. Niterói: EdUFF, 2005.

D'AMBROSIO, U. **Uma história concisa da matemática no Brasil.** Petrópolis: Vozes, 2008.

DEWEY, J. **Experiência e educação**. 3 ed. São Paulo: Nacional, 1979.

EUCLIDES. Os Elementos. Tradução de Irineu Bicudo. São Paulo: Unesp, 2009.

FIARRESGA, V. M. C. **Criptografia e Matemática**. Dissertação (Mestrado em Matemática para Professores). Universidade de Lisboa, 2010.

Filosofia Hoje. Disponível em: < http://www.filosofiahoje.com/2012/09/o-nosso-sistema-educacional-em-uma.html >. Acesso em 03 abr 2013.

FREIRE, P. **Pedagogia do Oprimido**. 8 ed. Rio de Janeiro: Paz & Terra, 1980.

GONGORA, M.; SODRE, U. **A origem dos números**. 2005 Disponível em: <http:// Pessoal.Sercontel.com.br/matemática/fundam/números/números.htm>. Acesso em: 19 set. 2012.

GOODRICH, M. T.; TAMASSIA, Roberto**. Projeto de Algoritmos**. São Paulo: Bookman, 2004.

GUNDLACH, B.H. **Números e Numerais.** Trad. Hygino H. Domingues. São Paulo: Atual, 1992. 77p. (Tópicos de História da matemática para uso em sala de aula).

HEFEZ, A. **Elementos de Aritmética.** Sociedade Brasileira de Matemática, Textos Universitários, 2006.

IFRAH, G. **Os números**: história de uma grande invenção. Tradução de Stella Maria de Freitas Senra. São Paulo: Globo, 2005. 11 ed.

KANTOWSKI, M. G. Algumas Considerações sobre o ensino para a resolução de problemas. In: KRUILK, S.; REYS, R.E. **A resolução de problemas na Matemática Escolar**. São Paulo: Atual, 1997. p. 270 – 282.

LEAL, B. Leituras da Infância na poesia de Manoel de Barros. In: KOHAN, W. (org.) **Lugares da Infância**: Filosofia. Rio de Janeiro: DP&A, 2004. p. 19-30.

MACHADO, S. D. A.; MARANHÃO, M.C.; COELHO, S. P. **Como é utilizado o Teorema Fundamental da Aritmética por atores do Ensino Fundamental**. In: Atas do V CIBEM. Porto, julho de 2005, v.1, p. 1-12.

MIORIM, M. A. **Introdução a História da Matemática.** São Paulo, SP: Atual, 1998.

MOREIRA, P. C. **O conhecimento matemático do professor**: formação na licenciatura e prática docente na escola básica. Tese (Doutorado em Educação). UFMG, Faculdade de Educação. Belo Horizonte, 2004.

POLYA, G. **A arte de resolver problemas**: Um novo aspecto do método matemático. Rio de Janeiro: Interciência, 1995.

Projeto Nova Visão. Disponível em:< http://projetonovavisao.spaceblog.com.br/1231591/O-QUE-E-O-METODO-BRAILLE/>. Acesso em 25 mar 2013

RANCIÈRE, J. **O Mestre Ignorante**: Cinco lições sobre a emancipação intelectual. Belo Horizonte: Autêntica, 2002.

Redes. Disponível em: <http://phantomsys.blogspot.com.br/2012/03/criptografia.html>. Acesso em 05 mar 2013.

RESENDE, M. R. **Re-significando a disciplina Teoria dos Números na formação do professor de Matemática na Licenciatura**. Tese (Doutorado em Educação Matemática). PUC-SP, 2007.

SANCHES, M.H.F. **Efeitos de uma estratégia diferenciada dos conceitos de matrizes.** Dissertação (Mestrado em educação matemática) UNICAMP, São Paulo, 2002.

SAUTOY, M. **A Música dos Números Primos: a história de um problema não resolvido na matemática.** Rio de Janeiro: Jorge Zahar, 2007.

SINGH, S. **O Livro dos Códigos**: A ciência do sigilo – do antigo Egito à criptografia quântica. 9 ed. Rio de Janeiro: Record, 2011.

SMULLYAN**,** R. **Alice no país dos enigmas**: incríveis problemas lógicos no país das maravilhas. Tradução de Vera Ribeiro. Rio de Janeiro: Jorge Zahar Editor, 2000.

TAMAROZZI, A.C. **Codificando e Decifrando Mensagens**. Revista do professor de matemática, volume 45. SBM, 2001. p. 41-47.

TERADA, R. **Criptografia e a importância das suas aplicações**. Revista do Professor de matemática, volume 12. SBM, p. 1-8, 1988.

VALENTE, W. R. **Uma História da Matemática Escolar no Brasil**. São Paulo: Annablume: FAPESPE, 1999.

BIBLIOGRAFIA CONSULTADA

AL-KADI; IBRAHAM, A. **The origins of cryptology**: The Arab Contributions. Cryptologia, vol 16, nº 2, abril de 1992, p. 97 – 126.

BEISSINGER, J.; PLESS, V. **The Cryptoclub**: Using Mathematics to Make and Break Secret Codes. Massachusetts: A K Peters, 2006.

GROENWALD, C. L.; OLGIN, C. A. Educação Matemática e o Tema Criptografia. **Ciencias Basicas en Ingenieria**. UNNE. n 5, ano 3, jul 2011. p. 23 – 36.

IEZZI, G. **Álgebra Moderna**. 3 ed. São Paulo: Atual, 1982.

LEMOS, M. **Criptografia, Números Primos e Algoritmo**. 4 ed. Rio de Janeiro: IMPA, 2010.

LINS, R.C.; GIMENES, J. **Perspectivas em aritmética e Álgebra para o século XXI**. 4 ed. Campinas, SP: Papirus, 1997.

SUETONIO. **A Vida dos Doze Césares**. Coleção A Obra-Prima de Cada Autor. São Paulo: Martin Claret, 2004.