UNIVERSIDADE FEDERAL DO TRIANGULO MINEIRO - UFTM

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Dissertação de Mestrado

Geogebra como Ferramenta Auxiliar no Processo de Aprendizagem de Números Primos na Educação Básica

Yale de Ângelis Lopes

Uberaba - Minas Gerais

Dezembro de 2017

Geogebra como Ferramenta Auxiliar no Processo de Aprendizagem de Números Primos na Educação Básica

Yale de Ângelis Lopes

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFTM como requisito parcial para obtenção do título de Mestre em Matemática.

Orientadora: Dr. Osmar Aléssio

Uberaba - Minas Gerais

Dezembro de 2017

Catalogação na fonte: Biblioteca da Universidade Federal do Triângulo Mineiro

Lopes, Yale de Ângelis
L856g Geogebra como ferramenta auxiliar no processo de aprendizagem de números primos na educação básica / Yale de Ângelis Lopes. -- 2017.
79 f. : il., fig.

Dissertação (Mestrado Profissional em Matemática em Rede Nacional) -- Universidade Federal do Triângulo Mineiro, Uberaba, MG, 2017
Orientador: Prof. Dr. Osmar Aléssio

1. Matemática - Estudo e ensino. 2. Números primos. 3. Aprendizagem. 4. Criptografia. 5. Crivo. 6. Geogebra.I. Aléssio, Osmar. II. Universidade Federal do Triângulo Mineiro. III. Título.

CDU 51(07)

Yale de Ângelis Lopes

Geogebra como Ferramenta Auxiliar no Processo de Aprendizagem de Números Primos na Educação Básica

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional-PROFMAT, da Universidade Federal do Triângulo Mineiro, como parte das atividades para obtenção do título de Mestre em Matemática.

15 de 12 2017.

Banca Examinadora

Prof. Dr. Osmar Aléssio
Orientador
Unviversidade Federal do Triângulo Mineiro -UFTM

Prof. Dr. Leandro Cruvinel Lemes
Unviversidade Federal do Triângulo Mineiro -UFTM

Profa. Ma. Raquel Oliveira Bodart
Instituto Federal de Educação, Ciência e Tecnologia do Triângulo Mineiro -IFTM

Aos meus pais, Dário e Ruth, e ao meu irmão, Ícaro.
Aos meu colegas professores de matemática.

Agradecimentos

Aos meus pais, Dário e Ruth, por todo amor, força e educação que me deram durante toda minha vida.

Ao meu irmão e melhor amigo, Ícaro, por todo carinho e apoio.

Ao meu orientador, Osmar Aléssio, por toda atenção, suporte e paciência, fundamentais para a conclusão deste trabalho.

Aos meus colegas de Profmat, em vista de todos momentos difíceis e de descontração que compratilhamos.

A todos professores do Profmat, por cada contribuição dada para nossa formação.

Aos meus amigos, em especial, ao Breno, por estar sempre presente, no momentos mais alegres e também nos mais difíceis.

Ao Rafael Ottoboni, Coordenador Local do Profmat, e a Fernanda, responsável pela Secretaria do Profmat, por todo pronto surpote dado quando solicitado.

"A Matemática apresenta invenções tão sutis
que poderão servir não só para satisfazer os
curiosos como, também para auxiliar as artes
e poupar trabalho aos homens"
- René Descartes

Resumo

A presente dissertação busca enriquecer e incentivar a aprendizagem de números primos por alunos do Ensino Médio. Para tanto, modelamos a técnica de Criptografia RSA e o Crivo de Eratóstenes utilizando a aplicação GeoGebra para servir de material didático auxiliar no processo de ensino-aprendizagem de números primos. Iniciamos esse trabalho com uma apresentação dos PCNEM (principal documento orientador do currículo do Ensino Médio) e também de alguns trabalhos realizados com afinidade com o tema desta dissertação. Alguns conceitos mais básicos de Teoria dos Números, também são apresentados, pois são necessários para compreensão da técnica RSA. Neste trabalho não só mostramos como nossas construções no GeoGebra funcionam, como também como elas foram elaboradas e pensadas.

Palavras-chave: Números Primos, Aprendizagem, Criptografia, Crivo, Geogebra.

Abstract

The present dissertation seeks to enrich and encourage the learning of prime numbers by high school students. In order to do so, we model the technique of RSA Cryptography and the Sieve of Eratosthenes using the GeoGebra application to serve as an auxiliary didactic material in the teaching-learning process of prime numbers. We started this paper with a presentation of the PCNEM (main guiding document of the High School curriculum) and also some papers with affinity with the theme of this dissertation. Some basic concepts of Number Theory are also presented once they are necessary for understanding the RSA technique. In this paper we not only show how our constructions in GeoGebra work, but also how they were thought and elaborated.

Keywords: Prime Numbers, Learning, Cryptography, Sieve, GeoGebra.

Sumário

Lista de ilustrações

INTRODUÇÃO

A Matemática sempre causou fascínio no homem. Sua capacidade de descrever o universo por meio de estruturas lógicas ajudou a desmistificar certos fenômenos que eram tidos com algo divino.

Os números primos são um dos temas que mais despertou interesse em muitos estudiosos, desde as civilizações mais antigas, devido suas características e propriedades singulares. O seu estudo é dotado de uma trajetória fascinante, que passa pela descoberta da infinitude dos números primos, pelo Teorema Fundamental da Aritmética - que nos diz que todo número inteiro positivo maior que 1 ou é primo ou pode ser escrito como composição única de fatores primos, exceto da ordem de seus fatores -, pela busca de uma fórmula (funções, algoritmos) capaz de encontrar todos números primos, bem como, a disposição dos mesmos no conjunto dos números inteiros. Sendo assim, é inegável, a importância dos números primos na Matemática e em especial na esfera que corresponde à Teoria dos Números.

Acreditamos que seu ensino na educação básica, desde que em um ambiente enriquecido com historicidade, contextualização e interdisciplinariedade, colabora para uma aprendizagem significativa do aluno, isto é, permite desenvolver competências e aptidões que o ajudarão não só a continuar e desejar continuar com seus estudos, se aperfeiçoando, como também, a compreender e refletir criticamente sobre os fenômenos físicos, naturais, econômicos e sócio-culturais do mundo e sobre sua capacidade de intervir nos mesmos, além de fornecer as ferramentas necessárias para a atividade profissional.

As crianças e adolescentes, de hoje em dia, estão imersos em uma sociedade cujas dimensões da tecnologia e da informação estão muito arraigadas a suas raízes. Vivemos na era dos *smartphones* e seus incomensuráveis aplicativos de diversas utilidades, dos sites de busca e pesquisa, sites de compartilhamento de vídeos, das redes sociais, das lojas virtuais, e etc... todos eles com um apelo social, econômico e emocional muito grande sobre nós. Dessa forma é natural que esses aspectos façam parte da identidade dos alunos de hoje em dia.

Pensar em um ensino distanciado e desconectado desse mundo, não só desestimula o interesse dos alunos a aprender certos conhecimentos, como também, inibe a criação e desenvolvimento de competências que só poderiam ser criadas com a interação da ciência com a tecnologia. Não podemos desconsiderar as potencialidades que os instrumentos tecnológicos podem proporcionar a educação, nem podemos subutilizá-los, isto é, limitar seu potencial utilizando-os apenas para dar um ar contemporâneo e inovador a uma prática tradicional.

Os números primos tem uma aplicação de alta relevância nos dias de hoje, que consiste na segurança da informação. O modelo de Criptografia RSA utiliza suas propriedades em

seu método de criptografar informações. Esse modelo de criptografia assimétrica é o mais utilizado em aplicações comerciais atualmente (COUTINHO, 2009), dado a complexidade computacional exigida para poder quebrar seu processo de codificação.

Tendo em vista esse panorama, nós nos propusemos a modelar a técnica de Criptografia RSA através da aplicação GeoGebra, para que diante da ferramenta construída possamos não só tornar a aprendizagem de números primos mais motivadora como também mais significativa para o aluno, em especial, do Ensino Médio, associando teoria e prática, com recursos tecnológicos que nos são disponíveis. Aproveitando a plataforma do GeoGebra, decidimos construir, também, um modelo do Crivo de Eratóstenes, uma vez que aprendizagem dessa simples técnica pelos alunos pode os ajudar encontrar números primos, bem como, servir como um teste de primalidade, o que pode ser determinante na solução de algum problema.

Dessa forma, a presente dissertação possui como objetivo geral: enriquecer e incentivar a aprendizagem de números primos por alunos do Ensino Médio;

São seus objetivos específicos: contextualizar o ensino de números primos para os alunos do Ensino Médio; modelar a técnica de Criptografia RSA e o Crivo de Eratóstenes na plataforma do Geogebra; incentivar o uso de tecnologias no processo educativo, desde que tal utilização seja significativa para a aprendizagem do educando; motivar outros educadores a desenvolver e criar novas ferramentas e materiais a partir de instrumentos tecnológicos que possam ser introduzidos no ambiente escolar;

A escolha pelo *software* GeoGebra se deu, especificamente, por ser uma aplicação de livre acesso a todos e por ser objeto de trabalho e de projetos de diversos professores de matemática, podendo assim ser um ambiente familiar para alguns alunos. Fora o fato que o GeoGebra não só está disponível para computadores (Windows, macOS, Linux) mas também como aplicativo para Android e iPad, além der possível utilizar suas ferramentas *online* em seu próprio *site*.

Acreditamos ser importante, primeiramente, mostrar como o Ensino Médio é visto e encarado atualmente pelos especialistas da educação, quais são as competências, habilidades e conhecimentos que esse nível de ensino busca desenvolver no aluno, e que papel terá esse aluno em nossa sociedade. Para isso apresentamos alguns entendimentos, perspectivas, filosofias e diretrizes que os PCNEM (Parâmetros Curriculares Nacionais do Ensino Médio) possuem sobre o processo de ensino-aprendizagem no Ensino Médio, em especial na Matemática, uma vez que tal documento seja a principal referência na estruturação curricular do ensino atualmente.

Apresentamos, também, um capítulo com alguns conceitos básicos de Teoria dos Números, porém necessários para compreender e justificar o modelo de Criptografia RSA. Com o mesmo intuito, exibimos alguns conceitos básicos de criptografia em sentido mais amplo.

Após explicarmos o método RSA, declaramos algumas estruturas, ferramentas e

comandos utilizados no GeoGebra, juntamente, com suas respectivas funções e definições. Eles são fundamentais para compreensão da modelagem do Método RSA e do Crivo de Eratóstenes.

Ainda nessa dissertação, apresentamos como funciona cada uma das construções (modelos) feitas no GeoGebra, assim como, a maneira com a qual as elaboramos. Acreditamos que compartilhar as estratégias utilizadas na construção do material pode contribuir não só para o aperfeiçoamento do mesmo, como também, pode servir como base e inspiração para outros trabalhos de natureza semelhante ou não. Somente unidos, compartilhando experiências e estratégias de ensino, cooperando na produção de materiais e desenvolvimento de projetos, que os professores poderão transformar a aprendizagem em sala de aula mais rica e incentivadora, especialmente em Matemática, pois precisamos superar aquelas juízos e concepções errôneas pré-estabelecidos por muitos alunos em relação a natureza dessa ciência.

1 Revisão de Literatura

1.1 Parâmetros Curriculares Nacionais Ensino Médio

1.1.1 Bases Legais

Os Parâmetros Curriculares Nacionais Ensino Médio (FILHO; MAIA, 2000) enaltecem, na formação do aluno, a aquisição de conhecimentos básicos, a preparação científica, a competência de manipular as distintas tecnologias relativas às áreas de atuação.

Esse movimento veio no sentido contrário à concepção anterior de Ensino Médio que era pautado na especialização para o mercado de trabalho. Essa concepção era reflexo do panorama econômico sob o qual o país vivia nas décadas de 60 e 70, que era o de desenvolvimento industrial. Dessa forma, a política educacional daquela época priorizou, como diretrizes do Ensino Médio, a formação de especialistas capazes de manipular as maquinarias ou de dirigir os processos de produção. Esse caráter de profissionalização do Ensino Médio também tinha por objetivo aliviar a pressão da demanda por Ensino Superior (FILHO; MAIA, 2000).

A necessidade de rever o propósito do Ensino Médio se deu basicamente por dois fatores. O primeiro é a ruptura tecnológica característica da revolução técnico-industrial. Nos anos 90, a grande quantidade de informações geradas pelas novas tecnologias, exigiu a criação de novos parâmetros para formação do cidadão. O segundo fator foi a substancial demanda por um ensino que atendesse as novas exigências do mundo de trabalho.

De acordo com os PCNEM (FILHO; MAIA, 2000), o Ensino Médio foi o que mais cresceu no Brasil, considerando a partir de 1980. Para se ter uma idéia, mais de 90% das matrículas realizadas no período entre 1988 e 1997 pertenceram ao Ensino Médio. De 1996 a 1997, as matrículas feitas nesse nível de ensino cresceram 11,6%.

Segundo os PCNEM (FILHO; MAIA, 2000):

> Pensar um novo currículo para o Ensino Médio coloca em presença estes dois fatores: **as mudanças estruturais que decorrem da chamada "revolução do conhecimento", alterando o modo de organização do trabalho e as relações sociais; e a expansão crescente da rede pública, que deverá atender a padrões de qualidade que se coadunem com as exigências desta sociedade.**

Para os PCNEM (FILHO; MAIA, 2000) o ensino brasileiro era descontextualizado, compartimentalizado e baseado no acúmulo de informações. Em contrapartida, sua proposta visa dar significado ao conhecimento escolar, por meio da contextualização; evitar a compartimentalização, através da interdisciplinaridade; e estimular o raciocínio e capacidade de aprender. Dessa maneira propõe-se uma formação geral, ao invés de uma

formação específica; além de buscar o desenvolvimento de competências de pesquisa, como a busca, seleção e análise de informações e também promover a capacidade de aprender, criar, formular, no lugar da simples memorização.

Os PCNEM andam em consonância com os princípios estabelecidos pela Lei de Diretrizes e Bases da educação nacional (LBD - Lei 9.394/96). Somente com essa lei, o Ensino Médio passou a ser considerado como Educação Básica. Aqui cabe uma observação, pois a Constituição de 1988 prenunciava tal concepção, quando, garantia que era dever do estado "a progressiva extensão da obrigatoriedade e gratuidade ao ensino médio"no inciso II do Art. 208. Com a Emenda Constitucional 14/96, contudo, tal inciso passou a ter a seguinte redação: "a progressiva universalização do ensino médio gratuito". Sendo assim, a Constituição confere a esse nível de ensino estatuto de direito de todo cidadão, apesar de não mais conferir sua obrigatoriedade (FILHO; MAIA, 2000). Fato esse que passou a ser garantido com a LBD quando a mesma no inciso I de seu Art. 21 diz "Educação Básica, formada pela educação infantil, ensino fundamental e ensino médio".

Com isso, o Ensino Médio passa a fazer parte do processo educacional que a Nação entende como básica para o exercício da cidadania.

A LBD apud (FILHO; MAIA, 2000) ressalta em seu Art. 36 que o ensino médio é a etapa final da educação básica. Segundo os PCNEM (FILHO; MAIA, 2000) isso não somente busca garantir a consolidação e aprofundamento dos conhecimentos adquiridos no Ensino Fundamental como também aprimorar o educando como pessoa humana; permitir a sequência dos estudos; garantir a preparação básica para o trabalho e cidadania; dotar o aluno de ferramentas que o permitam continuar aprendendo.

Visto isso, os PCNEM (FILHO; MAIA, 2000) destacam as finalidades as quais a LBD estabelece para esse nível de ensino:

- a formação da pessoa, de maneira a desenvolver valores e competências necessárias à integração de seu projeto individual ao projeto da sociedade em que se situa;
- o aprimoramento do educando como pessoa humana, incluindo a formação ética e o desenvolvimento da autonomia intelectual e do pensamento crítico;
- a preparação e orientação básica para a sua integração ao mundo do trabalho, com as competências que garantam seu aprimoramento profissional e permitam acompanhar as mudanças que caracterizam a produção no nosso tempo;
- o desenvolvimento das competências para continuar aprendendo, de forma autônoma e crítica, em níveis mais complexos de estudos.

Finalidades essas bem diversas daquelas estabelecidas pela referência legal anterior, a Lei 5.692/71: preparar para o prosseguimento de estudos e habilitar para o exercício de uma profissão técnica.

Nas sociedades tradicionais, a estabilidade educacional era garantida pelo seu estável quadro político, produtivo e social. A profissionalização demandava disciplina, obediência e respeito às regras estabelecidas no ambiente de trabalho. Eram essas as condições necessárias para inclusão social. Nessa perspectiva, a educação era o instrumento de "conformação"do futuro profissional ao mercado de trabalho. Contudo, diante do desenvolvimento tecnológico e social, tais exigências perderam sua relevância.

Essa nova sociedade, decorrente da revolução tecnológica e seus desdobramentos na produção e na esfera da informação, é caracterizada por constantes mudanças, que levam a rápidas rupturas. O conhecimento nesse novo panorama é constantemente superado e com isso exigem-se uma atualização contínua e também novos parâmetros para a formação do cidadão. A escola, portanto, ao manter uma postura tradicionalista e distanciada das mudanças sociais, acabará se marginalizando.

Os PCNEM ressaltam que, na medida que o desenvolvimento das competências cognitivas e culturais necessárias para o pleno desenvolvimento humano coincidir com o que se espera no processo produtivo, o papel da educação recoloca-se como elemento de desenvolvimento social. No entanto, isso não garante uma homogeneização das oportunidades sociais. Uma vez que, é possível afirmar que o crescimento econômico, pautado nos avanços tecnológicos, como a informatização e a robótica, não necessariamente gera mais empregos, pois o mesmo concorre para diminuição da quantidade de horas trabalhadas e, principalmente, para a diminuição de oportunidades de trabalho não qualificado.

Mesmo com esse quadro desafiador de constante mudança, de novas formas de socialização e processos de produção e novas definições de identidade social e individual, os PCNEM (FILHO; MAIA, 2000) acreditam que a educação surge como um ideal necessário indispensável ao homem na sua construção da paz, da liberdade e da justiça social.

O Relatório da Comissão Internacional sobre Educação para o século XXI, da UNESCO, apud (FILHO; MAIA, 2000) vê a educação "como uma via que conduz a um desenvolvimento mais harmonioso, mais autêntico, de modo a fazer recuar a pobreza, a exclusão social, as incompreensões, as opressões e as guerras".

Sendo assim, segundo os PCNEM (FILHO; MAIA, 2000), urgiu a necessidade de uma reforma curricular que abrangesse conteúdos e estratégias que possibilitassem o individuo realizar os três domínios da ação humana: a vida em sociedade, a atividade produtiva e a experiência subjetiva.

Com esse intuito, prerrogativas apontadas pela UNESCO como eixos estruturais da educação na sociedade contemporânea, incorporam-se como diretrizes gerais e orientadoras dessa nova proposta curricular. São elas:

- Aprender a conhecer: Se baseia na concepção de uma educação geral, mas que permita o aprofundamento em determinada área de conhecimento. A expansão dos saberes que permitem a compreensão da complexidade do mundo colabora para

o desenvolvimento da curiosidade intelectual, estimula o senso crítico e permite o entendimento do real. Essa premissa fornece o alicerce para continuar aprendendo, o que é chave para uma educação permanente.

- Aprender a fazer: Privilegia a aplicação da teoria na prática, bem como busca evidenciar a relação da ciência com tecnologia, tudo isso sob um contexto social. O desenvolvimento de habilidades e o estímulo para o surgimento de novas são fundamentais na sociedade contemporânea em vista do seu dinamismo.

- Aprender a viver: É reconhecer que o individuo vive em uma sociedade, logo tem que aprender a viver em conjunto, de forma a ser capaz de realizar projetos em comum com o próximo ou saber lidar de forma inteligente com conflitos inevitáveis.

- Aprender a ser: Reside na capacitação do indivíduo para que este seja capaz de construir pensamentos autônomos e críticos e de formular seus próprios juízos de valor, para que ele, assim, possa tomar suas próprias decisões frente às diferentes situações que irão surgir. Essa premissa enaltece a liberdade de pensamento, discernimento, sentimento e imaginação, buscando desenvolver os talentos do indivíduo e permitindo, na medida do possível, que ele seja dono do seu próprio destino.

A LBD apud (FILHO; MAIA, 2000) determina que os currículos da Educação Básica sejam construídos com uma Base Nacional Comum que deve ser complementada com aspectos regionais e locais da sociedade, da cultura, da economia e da demanda.

Os PCNEM (FILHO; MAIA, 2000) ressaltam que a Base Nacional Comum possui duas dimensões. Uma corresponde na preparação para a continuação dos estudos, de tal forma que o objetivo do processo de aprendizagem siga na direção da construção de competências e habilidades básicas, e distanciando da acumulação de esquemas resolutivos pré-estabelecidos. A outra se baseia na preparação para a atividade produtiva, isto é, esta dimensão indica que o conteúdo visto em sala de aula seja, também, um instrumento para a solução de um problema real, que ele seja capaz de ser aplicado no planejamento, gestão ou produção de um bem.

A LBD em seu Art.26 determina a obrigatoriedade, nessa Base Nacional Comum, "o estudo da língua portuguesa e da matemática, o conhecimento do mundo físico e natural e da realidade social e política, especialmente do Brasil; O ensino da arte [...] de forma a promover o desenvolvimento cultural dos alunos; A educação física, integrada à proposta pedagógica da escola [...]; A história do Brasil [...]".

Contudo, conforme diz os PCNEM (FILHO; MAIA, 2000), a LBD ao destacar as diretrizes curriculares para o Ensino Médio, ela o faz de forma orgânica, ou seja, ela busca superar a segmentação das disciplinas, revitalizando, assim, a integração e articulação dos conhecimentos, num processo constante de interdisciplinaridade e transdisciplinaridade.

Pode-se observar essa organicidade quando o inciso I do Art.36 dessa lei determina que o currículo do Ensino Médio "destacará a educação tecnológica básica, a compreensão do significado da ciência, das letras e das artes; o processo histórico de transformação da sociedade e da cultura; a língua portuguesa como instrumento de comunicação, acesso ao conhecimento e exercício da cidadania".

Sob essa perspectiva, a Base Nacional Curricular foi organizada por áreas de conhecimento, a saber:

- Linguagens, Códigos e suas Tecnologias:

  A aprendizagem nessa área dará prioridade para a Língua Portuguesa, como língua materna geradora de significação e integradora da organização do mundo e da própria interioridade; o domínio de língua(s) estrangeira(s) como forma de ampliação de possibilidades de acesso a outras pessoas e a outras culturas e informações; o uso da informática como meio de informação, comunicação e resolução de problemas, a ser utilizada no conjunto das atividades profissionais, lúdicas, de aprendizagem e de gestão pessoal; as Artes, incluindo-se a literatura, como expressão criadora e geradora de significação de uma linguagem e do uso que se faz dos seus elementos e de suas regras em outras linguagens; as atividades físicas e desportivas como domínio do corpo e como forma de expressão e comunicação.

  Na atual perspectiva, marcada pelo dinamismo da informação, refletir sobre a linguagem e seus sistemas, mais que necessidade, é garantia de inclusão social, fundamental para cidadania do indivíduo.

- Ciências da Natureza, Matemática e suas Tecnologias:

  A aprendizagem nessa área deve garantir formas de apropriação e construção de sistemas de pensamentos mais abstratos e resinificados, num processo cumulativo de saber e ruptura de consensos e pressupostos metodológicos. Nela deve residir a compreensão e a utilização dos conhecimentos científicos necessários para entender o funcionamento do mundo, bem como ser capaz de planejar, tomar e avaliar decisões de intervenção na realidade;

- Ciências Humanas e suas Tecnologias:

  O ensino nesta área deve propiciar que o aluno compreenda a sociedade como construção humana, num processo contínuo e dotado de historicidade; compreenda também os processos de sociabilidade humana em um contexto coletivo, definindo assim a noção de espaços públicos e privados; construa a si próprio como um agente social cujas ações intervêm na sociedade; avalie o impacto das tecnologias na estruturação e desenvolvimento das sociedades, bem como apropriar se daquelas oriundas do conhecimento desta área.

Essa organização por áreas de conhecimento, ressalta os PCNEM (2000), não desconsidera ou esvazia os conteúdos, mas sim seleciona e integra aqueles com maior relevância para o desenvolvimento pessoal e para uma maior inserção do indivíduo na sociedade. Tal concepção de currículo não descarta o ensino de conteúdos específicos, mas os considera como parte de um todo com várias dimensões interconectadas. Ela tem como fundamento a reunião daqueles conhecimentos que compartilham um mesmo objeto, e por consequência, que se comunicam mais facilmente, permitindo assim a construção de um processo educativo interdisciplinar, uma vez que reconhece-se que a produção do conhecimento é situada sócio, cultural, econômica e politicamente, num espaço e num tempo.

A interdisciplinariedade utiliza dos diversos conhecimentos para tratar um problema concreto sob diferentes perspectivas, evidenciando interconexões dos mesmos por meio de relações de complementaridade, convergência e divergência. Ela, portanto, não tem como pretensão formar novas disciplinas ou saberes, seu caráter é meramente instrumental, (FILHO; MAIA, 2000).

Outro aspecto importante para o currículo escolar é a contextualização. Segundo os PCNEM (FILHO; MAIA, 2000), a aprendizagem significativa se concretiza quando o aluno se identifica nos conteúdos programáticos. Também afirmam que todo o conhecimento é socialmente comprometido e que não há como um conhecimento ser aprendido e reinventado se não estabelecer conexões com as preocupações que as pessoas têm.

A contextualização busca construir no aprendiz a capacidade de compreender e intervir na realidade, numa perspectiva autônoma e desaliante. Para que isso se materialize, ela não deve se restringir apenas na aplicação do contexto mais imediato, muito menos em questões do senso comum.

O distanciamento entre os conteúdos do currículo e as experiências dos educandos, pode levar ao esquecimento ou também na incapacidade de aplicação dos mesmos por desconhecer a relação deles com a realidade. Essa desconexão da programação curricular com a realidade pode levar também ao desinteresse, desmotivação e até mesmo a evasão escolar.

Além de atribuir significado à aprendizagem através da interdisciplinaridade e da contextualização, essa proposta curricular busca incorporar as inovações tecnológicas no processo educativo. Tal inclusão, não somente almeja a preparação para o mundo do trabalho, mas a construção de um cidadão em sentido amplo.

A presença do termo "Tecnologias"na nomenclatura das áreas de conhecimento indicam claramente que se intenta promover competências e habilidades que possibilitem intervir e julgar situações práticas.

Partindo da premissa que não há tecnologia sem uma fundamentação científica, ao mesmo tempo que, instrumentos tecnológicos podem proporcionar a construção de um novo conhecimento científico, tal inserção se justifica e torna-se pertinente.

1.1.2 Matemática - Ciências Naturais, Matemática e suas Tecnologias

A Matemática, por sua universalidade de quantificação e expressão, ocupa uma posição ímpar na aprendizagem do aluno. Sua capacidade de codificar, ordenar, quantificar e interpretar variáveis é insubstituível em qualquer atividade contemporânea. Não o suficiente, os instrumentos matemáticos são extremamente importantes para uma abstração mais elaborada.

Seu ensino no Ensino Médio possui um valor formativo, que corrobora para a estruturação do pensamento e do raciocínio dedutivo, e também um valor instrumental, pois dota o indivíduo de ferramentas que serão necessárias em diversos aspectos da vida cotidiana.

Esta ciência, sob sua perspectiva formativa, contribui para o desenvolvimento de processos de pensamento e aquisição de atitudes, que ultrapassam as fronteiras da própria Matemática, isto é, ela é capaz de desenvolver no aluno a habilidade de resolver problemas reais, com confiança e desprendimento, gerando hábitos de investigação, proporcionando a construção de uma visão ampla e científica da realidade, permitindo a identificação da beleza e harmonia, incentivando a criatividade e o desenvolvimento de outras cruciais competências.

Já sob seu caráter instrumental, a Matemática deve ser encarada como um conjunto de técnicas e estratégias que podem ser tanto aproveitadas em outras áreas do conhecimento, como também, na esfera profissional.

Dessa forma, busca-se que o aluno enxergue a Matemática como linguagem de comunicação de ideias, isto é, um conjunto organizado de códigos e regras capazes de modelar e interpretar a realidade.

No entanto, a Matemática não pode ser resumida apenas pelos seus valores formativos e instrumentais, ela também deve ser compreendida como ciência, isto é, dotada de características estruturais específicas. Segundo os PCNEM (FILHO; MAIA; PEREIRA, 2000), "é importante que o aluno perceba que as definições, demonstrações e encadeamentos conceituais e lógicos têm a função de construir novos conceitos e estruturas a partir de outros e que servem para validar intuições e dar sentido às técnicas aplicadas".

Os PCNEM (FILHO; MAIA; PEREIRA, 2000) afirmam que, quando pensamos na relação das tecnologias com a Matemática, não podemos nos limitar apenas no uso dos instrumentos da informática ou de calculadoras, uma vez que o impacto da tecnologia na vida cotidiana exige mais que a simples interação com máquinas. A velocidade com que o conhecimento surge e se renova atualmente, dado a produção tecnológica, exige que o indivíduo permaneça em um estado de constante aprendizagem. Ne sentido, cabe a Matemática em conjunto com as demais áreas de conhecimento, fornecer informações e instrumentos que permitam o aluno a continuar aprendendo, pois saber aprender é condição básica para o aperfeiçoamento ao longo da vida e necessária para a cidadania.

O desenvolvimento de valores, habilidades e atitudes em relação ao conhecimento

matemático é de fundamental importância, pois são eles que permitem ou impossibilitam a aprendizagem. Somente dessa maneira que preconceitos e concepções distorcidas que os alunos têm em relação a Matemática podem ser superados e não mais constituírem um obstáculo para sua aprendizagem. Sendo assim, trabalhar os fundamentos matemáticos de forma contextualizada e interdisciplinar torna-se necessário para a construção desses valores.

Assim, os PCNEM (FILHO; MAIA; PEREIRA, 2000) estabelecem os seguintes objetivos que devem orientar o ensino de Matemática para uma aprendizagem real e significativa para os alunos:

- compreender os conceitos, procedimentos e estratégias matemáticas que permitam a ele desenvolver estudos posteriores e adquirir uma formação científica geral;
- aplicar seus conhecimentos matemáticos a situações diversas, utilizando-os na interpretação da ciência, na atividade tecnológica e nas atividades cotidianas;
- analisar e valorizar informações provenientes de diferentes fontes, utilizando ferramentas matemáticas para formar uma opinião própria que lhe permita expressar-se criticamente sobre problemas da Matemática, das outras áreas do conhecimento e da atualidade;
- desenvolver as capacidades de raciocínio e resolução de problemas, de comunicação, bem como o espírito crítico e criativo;
- utilizar com confiança procedimentos de resolução de problemas para desenvolver a compreensão dos conceitos matemáticos;
- expressar-se oral, escrita e graficamente em situações matemáticas e valorizar a precisão da linguagem e as demonstrações em Matemática;
- estabelecer conexões entre diferentes temas matemáticos e entre esses temas e o conhecimento de outras áreas do currículo;
- reconhecer representações equivalentes de um mesmo conceito, relacionando procedimentos associados às diferentes representações;
- promover a realização pessoal mediante o sentimento de segurança em relação às suas capacidades matemáticas, o desenvolvimento de atitudes de autonomia e cooperação.

1.2 Trabalhos Relacionados

Na dissertação (SOUZA, 2013) o autor apresenta a criptografia, que é estudada desde a antiguidade e suas técnicas hoje consistem basicamente em conceitos matemáticos. Os

números inteiros prestam um papel importante na criptografia de chave pública RSA, onde são apresentados alguns conceitos importantes, propriedades e resultados desse conjunto, destacando as relações com os números primos, a função de Euler e a operação módulo, conhecida como problema do logaritmo discreto. Apresenta os fundamentos da Criptografia de Chave Pública RSA, em que a base é a cifra assimétrica, mostrando a garantia da privacidade e assinatura das mensagens. Finaliza-se com a ideia do protocolo de criptografia RSA, a construção de um sistema de correios eletrônico, cuja essência é o método para estabelecer uma criptografia de chave pública RSA, baseada no conceito apresentado por Diffie e Hellman.

Na dissertação (NETO, 2015), o autor apresenta três modos de criptografar uma mensagem, são esses: Cifra de César, Cifra Afim e Cifra de Hill. Todas essas cifras são desenvolvidas apenas com matemática básica, ensinadas até o segundo ano do ensino médio. Com o principal objetivo de instigar a curiosidade do aluno em Matemática, o autor desenvolveu um recurso digital de aprendizagem em que o aluno poderá criptografar qualquer mensagem desejada nas três cifras já citadas.

Já (MORIMOTO, 2014) após trazer uma interessante fundamentação em Teoria dos Números passando por divisibilidade, máximo e mínimo divisor comum, congruências, números primos e Pequeno Teorema de Fermat, o autor apresenta algumas definições de números especiais como os primos gêmeos, os pseudo-primos, os números de Carmichael e de Fermat, os primos de Mersenne e de Sophie Germain. Ele também expõe alguns testes de primalidade como o de Fermat, de Euller, de Miller-Rabin, de Lucas-Lehmer e o AKS. O autor também menciona alguns avanços realizados recentemente envolvendo números primos. Finaliza apresentando algumas atividades que podem ser utilizadas em sala de aula que podem contribuir no ensino de propriedades dos números primos, que segundo o autor constituí em um tema rico a ser explorado no ensino de Matemática. A primeira atividade se chama Caça aos Primos. Essa atividade constituí em apresentar um quadro com números de 1 a 50, e dividir a turma em dois grupos. Os dois grupos terão que escolher números da tabela até que não reste nenhum. Eles deverão encontrar os divisores de cada número escolhido e em seguida somá-los, ganha a equipe que obtiver o menor número. O objetivo dessa atividade, de acordo com autor, é descobrir as estratégia utilizadas pelos alunos para obter a menor pontuação e com isso verificar se eles buscam escolher os números primos para poder vencer. A segunda atividade, chamada de Cálculo Mental, consiste em apresentar um quadro (8x8) com números que variam de 0 a 180. Por meio de três dados os alunos deverão utilizando as quatro operações básicas formar uma expressão que corresponda a uma casa desse quadro, tal casa será risca e os alunos ganharam o número de pontos referente a tal casa e das casas adjacentes. Vence a equipe que após todo o quadro riscado obtiver mais pontos. O objetivo de tal atividade, segundo o autor, é estimular o raciocínio dos alunos na busca de diferentes expressões para completar toda a tabela. Ele espera que os alunos notem a importância do uso da multiplicação

na formação dessas expressões e portanto busque encontrar os divisores dos números da tabela a fim de achar as expressões corretas. A terceira atividade seria apresentar um vídeo sobre a história dos primos.

A dissertação de (MELO, 2014), por sua vez, apresenta inicialmente uma trajetória histórica envolvendo estudos dos números primos. Assim como a de (MORIMOTO, 2014), mas não de forma tão detalhada, sua dissertação apresenta uma fundamentação teórica sobre Teoria dos Números, focada em números primos. Em seguida, expõe como o método de Criptografia RSA funciona, bem como, o princípio matemático que o sustenta, além de dar uma noção sobre a complexidade computacional de se quebrar tal método. O autor conclui enaltecendo a importância de se trabalhar os números primos sob a perspectiva de três vertentes: uma histórica, uma teórica e outra prática (contextualizada).

Na dissertação de (CARVALHO, 2015), se vê uma breve passagem histórica sobre os números primos. O autor também apresenta alguns conceitos mais fundamentais da Teoria de Números como divisibilidade, congruência, divisão euclidiana, O Teorema Fundamental da Aritmética, O Pequeno Teorema de Fermat e finaliza seu apanhado teórico caracterizando os números primos por meio do Teorema de Wilson. O autor segue seu trabalho trazendo um breve histórico sobre Criptografia, iniciando com Cifra de César e chegando no modelo criptográfico RSA. Ele também traz alguns polinômios (de uma variável) que retornam valores primos para uma sequência (limitada) de números inteiros e um polinômio com duas variáveis que gera também todos (e somente) os números primos. Algumas curiosidades também são exibidas envolvendo números primos, como o ciclo de vida de algumas espécies de cigarras, a conjectura de Goldbach, os primos de Sophie Germain, os números de Mersenne e os de Fermat. Finaliza seu trabalho apresentando algumas questões (maioria delas retiradas de Olimpíadas de Matemática) que envolve conceitos e propriedades relativas a números primos que podem ser propostos para alunos do ensino fundamental ou médio.

Para (MACHADO, 2015), na perspectiva atual de nossa educação, o ensino de números primos tem seu caráter formativo limitado em vista da falta de sistematização do estudo de seus conceitos e aplicações. Com o intuito de mudar esse quadro, o autor propôs uma sequência didática que foi apresentada para alunos do Colégio Militar de Manaus envolvendo alguns temas discorridos em sua dissertação: uma apresentação histórica sobre os números primos; nova abordagem de encarar o conjunto dos números naturais, isto é, dividindo-o em primos e compostos; princípio da boa ordenação; divisibilidade; congruência; MDC e MMC, Teorema Fundamental da Aritmética; a infinitude e distribuição dos primos; algumas aplicações; testes de primalidade e fórmulas que geram primos. O autor ressalta que as aulas ministradas foram bem recebidas pelos alunos, e que elas despertaram interesse deles sobre o tema e também acredita que a forma com que elas foram planejadas contribuem para formação dos alunos.

Um trabalho muito interessante sobre o ensino de números primos no Ensino Funda-

mental foi realizado por (FARIAS, 2016). Além de uma perspectiva histórica e teórica sobre números primos, sua dissertação também conta com uma análise feita sobre os conhecimentos que alunos do ensino fundamental (de duas escolas do estado Pernambuco e de duas escolas do Estado de Alagoas) tem em relação aos números primos, que para tal foi realizado um questionário que foi aplicado a esse público. O autor constatou que o desempenho dos alunos sobre esse tema foi insuficiente. Ele também analisou alguns livros didáticos do ensino fundamental e percebeu que nos mesmos o tema não recebe grande preocupação em relação a sua conceituação. O tema é abordado praticamente da mesma maneira nos livros, apresentando-se a definição, o Crivo de Eratóstenes, o método de divisões sucessivas, alguns exercícios e finalizando com o MDC e MMC. Segundo o autor, os livros não exploram historicidade inerente aos números primos e nem utilizam jogos para incentivar seu aprendizado. O autor propõe duas sequências didáticas sobre números primos, uma para ser apresentada no sexto ano do Ensino Fundamental e outra para o nono ano. Ele também apresenta diversos jogos e atividades que utilizam conceitos relativos a números primos que podem ser aplicados no Ensino Fundamental. De acordo com o autor, tais atividades podem estimular no alunos a concentração, a criatividade e a habilidade para resolver problemas, além de construir uma atitude positiva no processo de aprendizagem de Matemática.

Nesses e em alguns outros trabalhos aqui não citados se observou a necessidade de uma maior sistematização no ensino de números primos, principalmente em relação a sua contextualização histórica (dado seu teor apelativo), suas propriedades e características e suas aplicações no mundo real.

Sabemos da importância de se estabelecer uma conexão entre o objeto de estudo e o estudante. Sem ela o ensino torna sem importância, levando ao desinteresse e a não aprendizagem. Por essa razão tantos trabalhos, levantam as questões históricas e as situações práticas como instrumentos necessários ao processo educativo.

É comum encontrar na maioria desses trabalhos, quando se fala em aplicações dos números primos, o modelo de criptografia RSA. Normalmente, explica-se como o modelo funciona bem como o princípio matemático que o sustenta.

Como se trata de um modelo mais arrojado de criptografia, acreditamos que apenas apresentá-lo ou citá-lo como uma técnica que utiliza propriedades de números primos para sua eficácia, não acrescentará tanto para a formação do aluno. Por isso, pensamos em modelar tal técnica para que o aluno tomasse uma postura mais ativa no processo de ensino-aprendizagem, pois de tal forma ele poderá interagir com o modelo e ver por si só que o modelo funciona para diversos exemplos, além de perceber a importância que os primos detêm nessa técnica.

Diferente de (NETO, 2015) que modelou as Cifras de César, Cifra Afim e Cifra de Hill em uma página de *internet*, decidimos modelar a técnica RSA no GeoGebra, pois não encontramos nada semelhante feito até então. A razão da escolha de tal aplicação, se

deu, como já mencionamos na introdução, pelo fato do GeoGebra ser um *software* livre e também por ser uma ferramenta muito utilizada por diversos professores de matemática em seus materiais didáticos.

Aproveitamos também essa plataforma para modelar o Crivo de Eratóstenes, pois este constitui uma técnica muito simples e prática para alunos da Educação Básica de se determinar números primos.

2 Conceitos Básicos

2.1 Teoria dos Números

Para compreendermos o modelo de criptografia RSA precisamos conhecer alguns conceitos e propriedades (básicas) que são inerentes à Teoria dos Números, como divisibilidade, congruências e aritmética módulo m. Para tanto nos baseamos em (MARTINEZ et al., 2015) e (MARTINEZ; MOREIRA; SALDANHA, 2012) com algumas ligeiras adaptações.

2.1.1 Divisibilidade

Dados dois inteiros, d e a, com $d \neq 0$, dizemos que d divide a e denotamos $d|a$, caso existir um inteiro q tal que a é igual ao produto de d e q. Nessas condições dizemos também que a é múltiplo de d (ou também que d é divisor de a), caso contrário, d não divide a e por conseguinte a não é múltiplo de d, denotando-se $d \nmid a$.

Em seguida apresentamos algumas propriedades importantes de divisibilidade:

Lema 2.1.1. *Sejam $a, b, d \in \mathbb{Z}$*

1. *Se $d|a$ e $d|b$, então $d|ax + by$ para quaisquer coeficientes $x, y \in \mathbb{Z}$.*
2. *Se $d|a$, então $a = 0$ ou $|d| \leq |a|$.*
3. *Se $d|a$ e $a|b$ então $d|b$ (Transitividade).*

Demonstração:

1. Se $d|a$ e $d|b$, então temos que $a = q_1 d$ e $b = q_2 d$ com $q_1, q_2 \in \mathbb{Z}$. Assim temos, $ax + by = (q_1 d)x + (q_2 d)y = d(q_1 x + q_2 y)$, como $q_1 x + q_2 y \in \mathbb{Z}$, logo $d|ax + by$.
2. Se $d|a$ então existe um $q \in \mathbb{Z}$ tal que $a = qd$. Se $q = 0$ então $a = 0$, caso contrário $|q| \geq 1$ e portanto $|a| = |q||d| \geq |d|$.
3. Se $d|a$ e $a|b$ então sabemos que $a = q_1 d$ e $b = q_2 a$, com $q_1, q_2 \in \mathbb{Z}$. Assim temos, $b = q_2 a = q_2(q_1 d) = (q_2 q_1)d$, onde $q_2 q_1$ é um número inteiro, logo $d|b$.

Um inteiro d é divisor comum de dois outros inteiros a e b, quando d divide tanto o primeiro quanto o segundo. Dizemos que d é o máximo divisor comum (mdc) de a e b quando d for divisor tanto de a quanto de b e se c for divisor de a e b então c divide d. Denotamos o mdc de dois números da seguinte forma:

$$d = mdc(a, b)$$

Seja m um natural múltiplo de a e b, isto é, tanto a quanto b são divisores de m. Dessa forma, dizemos que m é um múltiplo comum desses dois números. Definimos m como sendo o mínimo múltiplo comum (mmc) de dois números, a e b, quando m for múltiplo comum desses dois números, e se n for também um múltiplo comum desses mesmos números, então m é divisor de n. Denotamos o mmc de dois números da seguinte maneira:

$$m = mmc(a, b)$$

Para calcularmos o mdc e o mmc de dois números naturais de forma eficiente utilizaremos o *algoritmo de Euclides*, que pode ser descrito da seguinte forma: dados a, $b \in \mathbb{Z}$ com $b \neq 0$ então, existem q, $r \in \mathbb{Z}$ com $a = bq + r$ e $0 \leq r < |b|$.

Tais q e r são chamados de quociente e resto (respectivamente) da divisão de a por b. Eles são unicamente determinados (veja a seguir) pelas condições mencionadas anteriormente. Antes de mostramos sua existência e unicidade, apresentaremos a definição de parte inteira (floor) e teto.

Definição 2.1.1. *Seja $x \in \mathbb{R}$, definimos a parte inteira $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$, tal que $k \leq x < k + 1$, isto é, o menor inteiro menor ou igual à x.*

Definição 2.1.2. *Seja $x \in \mathbb{R}$, definimos o teto $\lceil x \rceil$ de x como sendo o único $k \in \mathbb{Z}$, tal que $k - 1 < x \leq k$, isto é, o maior inteiro maior ou igual à x.*

Para mostrar a existência de q e r, basta tomar: $q = \lfloor a/b \rfloor$ se $b > 0$ ou $\lceil a/b \rceil$ se $b < 0$ e $r = a - bq$. Usando as definições de parte inteira e teto não é difícil mostrar que $0 \leq r < |b|$. Agora, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 < |b|$ então segue que $r_2 - r_1 = b(q_2 - q_1)$, isto é, $r_2 - r_1$ é múltiplo de b. Mas sabemos que do Lema 2.1.1 (item 2 mais especificamente) que ou $r_2 - r_1 = 0$ ou $|r_2 - r_1| \geq |b|$, o que não pode acontecer, pois $0 \leq r_1, r_2 < |b|$. Logo, $r_2 - r_1 = 0$ e portanto $r_2 = r_1$ e $q_2 = q_1$, o que prova unicidade.

O algoritmo de Euclides segue da aplicação reiterada do seguinte lema:

Lema 2.1.2. *(Euclides) Se $a = bq + r$, então $mdc(a, b) = mdc(b, r)$*

Demonstração:

Seja $d_1 = mdc(a, b)$, dessa forma temos que $d_1|a$ e $d_1|b$, em particular, $d_1|a - bq$ (propriedade de divisibilidade), isto é, $d|r$. Seja $d_2 = mdc(b, r)$, logo $d_2|b$ e $d_2|r$, em particular, $d_2|bq + r$, ou seja, $d_2|a$. Mas se d_1 divide r e b, então quer dizer que $d_1|d_2$ (pois d_2 é $mdc(b, r)$). Por outro lado se d_2 divide a e b, então $d_2|d_1$. Dessa forma, temos que $d_1 = d_2$.

Como os restos da aplicação sucessiva do algoritmo de Euclidades formam uma sequência estritamente decrescente, temos que o algoritmo cessa quando atinge resto 0.

Teorema 2.1.1. *Sejam $a, b \in [Z]$. Então existem $x, y \in [Z]$ com*

$$ax + by = mdc(a, b)$$

. Portanto se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$ então $c|mdc(a,b)$.

Demonstração:

O caso $a = b = 0$ é trivial ($x = y = 0$). Nos demais casos, considere o conjunto de todas as combinações $\mathbb{Z}$-lineares de a e b:

$$I(a,b) = \{ax + by : x, y \in \mathbb{Z}\}.$$

Seja $d = ax_0 + bx_0$ o menor elemento positivo de $I(a,b)$ Afirma-se que d divide todos os elementos de $I(a,b)$. Veja que, dado $m = ax + by \in I(a,b)$, e sejam $q, r \in \mathbb{Z}$ o quociente e o resto na divisão euclidiana de m por d, de modo que $m = dq + r$ e $0 \leq r < d$. Assim temos,

$$r = m - dq = a(x - qx_0) + b(y - qy_0) \in I(a,b).$$

Mas como $r < d$ e d é o menor elemento positivo de $I(a,b)$, segue que r = 0 e, portanto, d | m. Em particular, como $a, b \in I(a,b)$ temos que $d|a$ e $d|b$, logo $d \leq mdc(a,b)$. Veja ainda que se $c|a$ e $c|b$, então $c|ax_0 + by_0 \iff c|d$. Pegando $c = mdc(a,b)$ temos que $mdc(a,b)|d$ o que, juntamente com a desigualdade $d \leq mdc(a,b)$, mostra que $d = mdc(a,b)$.

Proposição 2.1.1. *Se $mdc(a,b) = 1$ e $a|bc$, então $a|c$.*

Demonstração:

Como $mdc(a,b) = 1$, existem $x, y \in \mathbb{Z}$ tais que

$$ax + bx = 1 \Longrightarrow a(cx) + (bc)y = c.$$

Como a divide ambos os termos do lado esquerdo, temos que $a|c$.

Chamamos de número primo, aquele natural p diferente do número 1, tal que seus únicos divisores sejam 1 e ele mesmo. Por outro lado, um número $n > 1$ é composto quando admite outros divisores além de 1 e n. Note que, se p é primo e $p \nmid a$, então $mdc(p,a) = 1$.

Corolário 2.1.1. *Seja p um número primo e sejam $a_1, ..., a_m$ inteiros. Se $p|a_1 \cdots a_m$, então $p|a_i$ para algum i, $1 \leq i \leq m$.*

Para demonstrar esse último corolário, basta utilizar a proposição anterior e aplicar indução em m.

A seguir apresentaremos um lema que sintetiza algumas propriedades importantes do mdc:

Lema 2.1.3. *Temos*

1. *Se p é primo, então $mdc(a,p)$ é 1 ou p.*
2. *Se k é um inteiro, então $mdc(a,b) = mdc(a - kb, b)$.*

3. *Se $a|c$, então $mdc(a,b)|mdc(c,b)$.*

4. *Se $mdc(a,b)=1$, então $mdc(ac,b)=mdc(c,b)$.*

Demonstração:

1. É fácil ver, pois p só pode ser divido por 1 ou por ele mesmo.

2. Veja que este item é o mesmo que o Lema de Euclides apresentado anteriormente.

3. Seja $d_1 = mdc(a,b)$ e $d_2 = mdc(c,b)$. Por hipótese temos que $a|c$, mas como $d_1|a$ então $d_1|c$, mas sabemos que $d_1|b$, logo d_1 é divisor comum de b e c e, portanto, $d_1|d_2$.

4. É fácil notar que $mdc(c,b)$ divide tanto ac e b, logo $mdc(c,b)|mdc(ac,b)$. Agora veja que podemos escrever $ax+by=1$ com $x,y\in\mathbb{Z}$, pois como vimos antes $mdc(a,b)=1$. Assim, $mdc(ac,b)$ divide $(ac)x+b(cy)=c$ e também divide b, logo divide $mdc(c,b)$, ou seja, $mdc(ac,b)=mdc(b,c)$.

A seguinte proposição nos mostra uma relação entre o mdc e o mmc de dois números naturais.

Proposição 2.1.2. *Sejam a e b dois números naturais, então $mdc(a,b)\cdot mmc(a,b)=a\cdot b$*

Demonstração:

Seja d = mdc(a,b), ou seja, $a=a_1d$ e $b=b_1d$ com $a_1,b_1\in\mathbb{Z}$. É fácil observar que $mdc(a_1,b_1)=1$. Podemos escrever $mmc(a,b)=al$ para algum $l\in\mathbb{Z}$. Dessa forma temos $b|mmc(a,b)\iff b_1d|a_1dl\iff b_1|a_1l$. Como $mdc(a_1,b_1)=1$, isto implica que $b_1|l$ pela proposição 2.1.1. Pela definição de mínimo múltiplo comum, temos que l deve ser o menor número divisível por b_1, desta forma conclui-se que $l=b_1$ e portanto $mmc(a,b)=b_1a$. Logo $mdc(a,b)\cdot mmc(a,b)=d\cdot b_1a=a\cdot b$.

O seguinte teorema carateriza todo número natural com base em seus "constituintes"primos.

Teorema 2.1.2. *(Teorema Fundamental da Aritmética) Seja $n\geq 2$ um número natural. Podemos escrever n de uma única forma como um produto $n=p_1\cdots p_m$ onde $m\geq 1$ é um natural e $p_1\leq\cdots\leq p_m$ são primos.*

Demonstração:

A existência da fatoração de n em primos pode ser mostrada pelo segundo princípio de indução. Se n é primo não há o que provar. Agora, se n é composto podemos escrever $n=ab$, $a,b\in\mathbb{N}$, $1<a<n$, $1<b<n$. Por hipótese de indução, a e b se decompõem como produto de primos. Agrupando as fatorações de a e b (e reordenando os fatores) obtemos uma fatoração de n. Para mostrar a unicidade, suponha por absurdo que n possui duas fatorações distintas

$$n=p_1\cdots p_m=q_1\cdots q_{m'}$$

com $p_1 \leq \cdots \leq p_{m'}$, $q_1 \leq \cdots \leq q_{m'}$ e que n é mínimo com tal propriedade. Como $p_1 | q_1 \cdots q_{m'}$ temos que $p_1 | q_i$ para algum valor de i por 2.1.1. Logo, como q_i é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, pela minimalidade de n, donde $m = m'$ e $p_i = q_i$ para todo i, o que contradiz o fato de n ter duas fatorações.

A seguir veremos um teorema que afirma a infinitude dos primos:

Teorema 2.1.3. *(Euclides) Existem infinitos primos*

Demonstração:

Por absurdo, suponha que $p_1, p_2, \cdots, p_m$ fossem todos os primos. O número $N = p_1 p_2 \cdots p_m + 1 > 1$ não seria divisível por nenhum primo p_i (observe pois, que 1 só pode ser divisível por ele mesmo), o que contradiz o Teorema Fundamental de Aritmética.

2.1.2 Congruência

Veremos agora o conceito de congruência,assim como suas propriedades mais básicas.

Tomando $a, b, n \in \mathbb{Z}$. Dizemos que a é *congruente* a b *módulo* n, e denotamos

$$a \equiv b (mod\ n)$$

se $n | a - b$, isto é, se a e b, na divisão por n, deixam o mesmo resto.

Proposição 2.1.3. *Para quaisquer $a, b, c, d, n \in \mathbb{Z}$ temos:*

1. *(Reflexividade) $a \equiv a (mod\ n)$;*
2. *(Simetria) se $a \equiv b (mod\ n)$, então $b \equiv a (mod\ n)$;*
3. *(Transitividade) se $a \equiv b (mod\ n)$ e $b \equiv c (mod\ n)$, então $a \equiv c (mod\ n)$;*
4. *Podemos somar e subtrair "membro a membro":*

$$\begin{cases} a \equiv b (mod\ n) \\ c \equiv d (mod\ n) \end{cases} \implies \begin{cases} a + c \equiv b + d (mod\ n) \\ a - c \equiv b - d (mod\ n) \end{cases}$$

   Em particular, se $a \equiv b (mod\ n)$, então $ka \equiv kb (mod\ n)$ para to $k \in \mathbb{Z}$.

5. *Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b (mod\ n) \\ c \equiv d (mod\ n) \end{cases} \implies ac \equiv bd (mod\ n)$$

   Particularmente, se $a \equiv b (mod\ n)$, então $a^k \equiv b^k (mod\ n)$ para todo $k \in \mathbb{Z}$

6. *(Cancelamento) Se mdc(c,n) = 1, então*

$$ac \equiv bc(mod\ n) \iff a \equiv b(mod\ n)$$

.

Demonstração:

1. Observe que $n|a - a = 0$ (sai direto da definição).
2. Veja que, $n|a - b \Longrightarrow n| - (a - b) \iff n|b - a$.
3. Se $n|a - b$ e $n|b - c \Longrightarrow n|(a - b) + (b - c) \iff n|a - c$.
4. Se $n|a-b$ e $n|c-d \Longrightarrow n|(a-b)+(c-d) \iff n|(a+c)-(b+d), n|(a-b)-(c-d) \iff n|(a - c) - (b - d)$.
5. Se $n|a - b$ e $n|c - d \Longrightarrow n|(a - b)c + (c - d)b \iff n|ac - bd$.
6. Temos que $n|ac - bc \iff n|c(a - b) \iff n|a - b$ uma vez que $mdc(c, n) = 1$.

Proposição 2.1.4. *Seja p um número primo, então toda combinação* $\begin{pmatrix} p \\ n \end{pmatrix}$, *com* $0 < n < p$ *e* $n \in \mathbb{N}^*$, *é divisível por p.*

Demonstração:
Sabemos que,

$$\begin{pmatrix} p \\ n \end{pmatrix} = \frac{p!}{(p-n)!n!} = \frac{p(p-1)!}{(p-n)!n!}.$$

Também sabemos que $\begin{pmatrix} p \\ n \end{pmatrix} \in \mathbb{Z}$, isto é, (p-n)!n! | p!. Contudo como $n < p$, temos que o $mdc(p, (p - n)!) = 1$ e $mdc(p, n!) = 1$, ou também que $mdc(p, (p - n)!n!) = 1$. Dessa forma pela proposição 2.1.1, $(p - n)!n!|(p - 1)!$, isto é, $\begin{pmatrix} p \\ n \end{pmatrix}$ sempre terá p como um seus fatores, portanto, $p|\begin{pmatrix} p \\ n \end{pmatrix}$.

Teorema 2.1.4. *(Pequeno Teorema de Fermat) Seja a um inteiro positivo e p um primo, então*

$$a^p \equiv a(mod\ p)$$

Em particular, se $p \nmid a$, *então*

$$a^{p-1} \equiv 1(mod\ p)$$

Demonstração:

Para demonstrar o teorema anterior utilizaremos o princípio de indução sobre a. Sabemos que p é primo. Note que, para $p = 2$ temos $a^2 \equiv a(mod\ 2) \iff 2|a(a-1)$ o que é verdade, pois é fácil ver que $a(a-1)$ é par. Para $p > 2$ a afirmação é verdadeira para $a = 0$ e $a = 1$. Pela hipótese de indução, temos que $a^p \equiv a(mod\ p)$. Assim queremos provar que a afirmativa vale para $a + 1$, isto é, $(a+1)^p \equiv a + 1(mod\ p)$. Sendo assim, temos

$$(a+1)^p \equiv a^p + \begin{pmatrix} p \\ 1 \end{pmatrix} a^{p-1} + \cdots + \begin{pmatrix} p \\ p-1 \end{pmatrix} a + 1(mod\ p) \equiv a^p + 1(mod\ p) \equiv a + 1(mod\ p).$$

Logo pelo princípio de indução $a^p \equiv a(mod\ p)$, para todo a inteiro positivo. Para provar a segunda parte, sabendo que $p \nmid a$, basta aplicar a proposição 2.1.1.

3 Criptografia RSA

Os conceitos e princípios apresentados nas seções seguintes podem ser encontrados mais detalhadamente em (VIANA, 2017) e (COUTINHO, 2009).

3.1 Criptografia

A criptografia é um conjunto de técnicas e princípios que visam, essencialmente, transformar determinada informação ou conjunto de dados, a fim de ocultar seu verdadeiro significado. Isto é, a criptografia busca tornar informação ilegível para aqueles que não são seus destinatários, de forma que apenas a pessoa alvo daquela informação seja capaz de entender a mensagem.

No passado, a cifragem era aplicada na troca de mensagens, em especial em questões ligadas à guerra, para evitar que o inimigo de quem às emitisse pudesse compreender seu conteúdo e, por assim dizer, utilizá-lo em benefício próprio, o que poderia gerar consequências catastróficas para aqueles que emitissem a mensagem. Ela também era usada para proteger segredos diplomáticos e até amorosos.

Com o passar dos anos, a criptografia foi se tornando cada vez mais importante no que se refere à segurança da informação, principalmente com o avanço da tecnologia da informação. Até pouco tempo, quando a tecnologia ainda não fazia muita parte de nosso dia à dia, as informações e grande parte dos processos organizacionais eram registrados basicamente no papel, sendo armazenados em armários ou cofres protegidos por cadeados ou senhas. Hoje em dia, esse panorama, em grande parte, se modificou, pois as informações são processadas e armazenadas em ambientes digitais, o que originou uma forte dependência entre os sistemas de informação e as organizações. Com a chegada da internet, as informações navegam em meios públicos, podendo ser interceptadas por qualquer pessoa. Não é difícil de imaginar os gigantescos prejuízos para uma instituição caso houvesse uma falha na segurança desses dados.

Vale ressaltar, que o objetivo da criptografia não é impedir que certa informação ou dado sejam interceptados, mas sim de dificultar a compreensão do dado capturado, ou seja, garantir a confidencialidade de seu conteúdo. A seguir, veremos alguns conceitos relacionados a esta técnica.

3.2 Criptografia Simétrica

Os algoritmos que utilizam a criptografia simétrica caracterizam-se essencialmente pela utilização de uma mesma chave criptográfica tanto para codificar quanto descodificar uma

informação. Devido à esta razão que esse tipo criptografia recebeu o nome "simétrica".

Chave criptográfica é o termo utilizado para definir um conjunto de caracteres, que juntamente com o algoritmo de criptografia irão definir o processo de cifragem e decifragem da mensagem.

Sendo mais preciso, esse método se materializa quando, o emissor da mensagem codifica uma mensagem utilizando algum algoritmo de criptografia e uma determinada chave. O receptor da mensagem para transformá-la em sua forma de origem, utiliza aquele algoritmo e aplica a mesma chave usada pelo emissor. Sem a chave, não é possível decifrar a mensagem. Vale ressaltar, que o nível de segurança depende tanto do algoritmo, assim como do tamanho da chave escolhida, isto é, do total de bits que ela possui.

Um dos pontos positivos desse modelo é exatamente esse, o de ser fácil de se implementar. Outra vantagem seria a velocidade deste processo em contrapartida da criptografia assimétrica (que veremos logo a seguir), de tal maneira que uma grande quantidade de dados seja encriptada em um menor tempo.

Os aspectos negativos desse modelo estão ligados à criação e compartilhamento das chaves. Uma chave muito simples não impedirá que um algoritmo de força bruta a quebre. Um algoritmo de força bruta utiliza inúmeras combinações de caracteres na tentativa de uma delas ser compatível com a chave do algoritmo. Deve-se tomar cuidado também com a forma de compartilhar as chaves entre os interessados na informação, para que elas não caiam em mãos erradas. Para efetuar a distribuição das chaves deve-se utilizar um *canal seguro*, ou seja, um canal de comunicação que permita a transmissão de dados sem que corra o risco de interceptação ou adulteração.

3.3 Criptografia Assimétrica

A criptografia assimétrica também é conhecida como criptografia de chave pública. Ela se caracteriza por contar com o uso de duas chaves ao invés de uma, como na criptografia simétrica. Uma é denominada chave privada, que é aquela que deverá ser mantida em segredo. Já a outra é a chave pública que é distribuída para outros usuários. Nesse modelo, o que for cifrado pela chave privada só poderá ser decifrado pela chave pública e contrário também se aplica, ou seja, o que for codificado pela chave pública apenas poderá ser descodificado pela chave privada.

A grande vantagem desse método está na impossibilidade (computacional) de uma chave privada ser determinada a partir de sua chave pública correspondente. Dessa forma, a chave pública pode ser divulgada sem comprometer a segurança do método. Por essa razão que esse método, diferentemente de algoritmos de chave simétrica, não precisam de um canal seguro para a troca de chaves entre as partes.

Dada sua complexidade computacional, a encriptação assimétrica é geralmente utilizada para transferir uma chave simétrica pela qual a mensagem será criptografada. Talvez esse

seja seu maior aspecto negativo, pois esse método não é o mais recomendado para codificar uma grande quantidades de dado, pois é um método "computacionalmente exaustivo".

Em fim, a seguir, apresentaremos os aspectos mais gerais do método criptografia RSA, que é o modelo assimétrico mais utilizado em aplicações comerciais atualmente.

3.4 Criptografia RSA

Este modelo foi criado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, época em que trabalhavam no Massachussets Institute of Technology (M.I.T). Note que a sigla RSA corresponde às inicias dos sobrenomes dos criadores do método.

Suponha que queiramos codificar a seguinte mensagem utilizando o modelo RSA:

PENSO LOGO EXISTO

O modelo exige que trabalhemos com números inteiros. Desta maneira, precisamos de converter as letras do alfabeto em números inteiros antes de começarmos o processo de codificação. Para isso utilizaremos o seguinte quadro para realizar a conversão:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Para o espaço entre as letras usaremos o número 99. Dessa forma, nossa mensagem após a conversão ficaria na seguinte forma:

25142328249921241624991433182829 24

Vale ressaltar que, todos os caracteres ao serem convertidos devem todos ter o mesmo número de algarismos entre si para evitar que haja ambiguidades. Por exemplo, se começássemos nossa conversão a partir do número um, teríamos $A = 1$, $B = 2$, $C = 3$ e assim por diante. Dessa forma, na hora da desconversão não saberíamos se 12 seria AB ou L, que é a décima segunda letra do alfabeto.

Nosso próximo passo será escolher dois primos distintos, p e q, que serão nossos parâmetros do sistema RSA, isto é, a partir deles que obteremos nossa chave pública e nossa chave secreta. Feito isso, obtemos um número n que é o produto dos dois primos.

Em seguida, quebraremos em blocos nossa mensagem já convertida, respeitando duas regras. A primeira é que cada bloco tem que ser um número menor que n. A segunda

regra é que o primeiro algarismo de cada bloco não pode ser zero (pois caso contrário traria mais uma vez ambiguidades, como 021 e 21). Suponha que nossos primos escolhidos são $p = 17$ e $q = 23$. Com isso, nosso n valeria 391. Uma forma de quebrar nossa mensagem, respeitando as regras, seria então da seguinte maneira:

251-42-328-249-92-124-162-49-91-43-318-282-92-4

Esse procedimento de quebra se faz necessário, pois dessa forma torna a decodificação por contagem de frequência basicamente impossível. Veja que da forma que quebramos nossa mensagem, nenhum dos blocos correspondem a uma unidade linguística, seja ela uma letra ou uma palavra.

O passo seguinte corresponde à codificação dos blocos que será aplicado a cada um separadamente. Uma vez os blocos codificados, os mesmos não poderão ser reagrupados, pois isso tornaria a decodificação impossível de se realizar.

Mas antes de seguir a diante, apresentaremos a *função phi de Euller* $\phi(n)$. Seja $n = p_1^{k_1} \cdots p_r^{k_r}$, onde p_j são os fatores primos (distintos) de n, então:

$$\phi(n) = (p_1 - 1){p_1}^{k_1 - 1} \cdots (p_r - 1){p_r}^{k_r - 1}$$

Como nosso $n = pq$, nossa função de phi de Euller pode ser escrita da seguinte forma:

$$\phi(n) = (p - 1)(q - 1)$$

Lembrando que nosso $n = 391$ temos, $\phi(391) = (16) \cdot (22) = 352$.

Seja b um bloco pertencente ao conjunto de blocos que formam a minha mensagem. Devemos agora escolher um inteiro positivo d, tal que o $mdc(d, \phi(n)) = 1$. Agora, C(b) será a função que codificará cada bloco. Ela será dada por:

$$C(b) \equiv b^d (mod\ n).$$

Escolhendo $d = 3$ (observe que mdc(3,352)=1), temos:

$C(b) \equiv b^d (mod\ 391)$
$C(251) \equiv 251^3 (mod\ 391) \equiv 38$
$C(42) \equiv 42^3 (mod\ 391) \equiv 189$
$C(328) \equiv 328^3 (mod\ 391) \equiv 193$
$C(249) \equiv 249^3 (mod\ 391) \equiv 5$
$C(92) \equiv 92^3 (mod\ 391) \equiv 207$
$C(124) \equiv 124^3 (mod\ 391) \equiv 108$
$C(162) \equiv 162^3 (mod\ 391) \equiv 185$
$C(49) \equiv 49^3 (mod\ 391) \equiv 349$
$C(91) \equiv 91^3 (mod\ 391) \equiv 114$
$C(43) \equiv 43^3 (mod\ 391) \equiv 134$
$C(318) \equiv 318^3 (mod\ 391) \equiv 28$
$C(282) \equiv 282^3 (mod\ 391) \equiv 354$
$C(92) \equiv 92^3 (mod\ 391) \equiv 207$
$C(4) \equiv 4^3 (mod\ 391) \equiv 64$

Dessa forma, nossa mensagem codificada apresentaria a seguinte sequência:

38-189-193-5-207-108-185-349-114-134-28-354-207-64

Agora com a mensagem codificada, queremos uma função que a descodifique, isto é, um processo que a deixe em sua forma original. Essa função será representada por D(c), onde $c \in C(b)$. Ela será dada por:

$$D(c) \equiv c^e (mod\ n),$$

onde e é o inverso de d módulo $\phi(n)$, isto é:

$$ed \equiv 1 (mod\ \phi(n))$$

Achando o e podemos realizar o processo de desencriptação da nossa mensagem. Sendo assim temos,

$$e \cdot 3 \equiv 1 (mod\ 352).$$

Para resolvermos essa equação modular basta tomar $e = 235$. Veja que,

$$235 \cdot 3 \equiv 705 \equiv 1 (mod\ 352),$$

pois $705 = 352 \cdot 2 + 1$.

Em posse de e, podemos neste momento utilizar nossa função de decodificação D(c), para retornar nossa mensagem à forma que ela era inicialmente. Sendo assim se aplicarmos nossa função D(c), na nossa função codificada, a saber,

38-189-193-5-207-108-185-349-114-134-28-354-207-64

obteremos o seguinte:

$D(c) \equiv c^e (mod\ 391)$
$D(38) \equiv 38^{235} (mod\ 391) \equiv 251$
$D(189) \equiv 189^{235} (mod\ 391) \equiv 42$
$D(193) \equiv 193^{235} (mod\ 391) \equiv 328$
$D(5) \equiv 5^{235} (mod\ 391) \equiv 249$
$D(207) \equiv 207^{235} (mod\ 391) \equiv 92$
$D(108) \equiv 108^{235} (mod\ 391) \equiv 124$
$D(185) \equiv 185^{235} (mod\ 391) \equiv 162$
$D(349) \equiv 349^{235} (mod\ 391) \equiv 49$
$D(114) \equiv 114^{235} (mod\ 391) \equiv 91$
$D(134) \equiv 134^{235} (mod\ 391) \equiv 43$
$D(28) \equiv 28^{235} (mod\ 391) \equiv 318$
$D(354) \equiv 354^{235} (mod\ 391) \equiv 282$
$D(207) \equiv 207^{235} (mod\ 391) \equiv 92$
$D(64) \equiv 64^{235} (mod\ 391) \equiv 4$

Dessa forma, obtemos uma nova sequência:

251-42-328-249-92-124-162-49-91-43-318-282-92-4

.

Note que a sequência acima é igual à nossa mensagem antes da encriptação, ou seja, nossa decodificação foi bem sucedida. Agora basta reagrupar os blocos e converter os números (usando nossa tabela de conversão) para retornar à nossa mensagem original:

$$PENSOLOGOEXISTO.$$

Uma dúvida fica no ar: será que esse método de encriptação e desencriptação, sempre, será bem sucedido? A seguir mostraremos que sim.

Mostrar que o método de criptografia RSA sempre funciona, é o mesmo que mostrar em linguagem matemática, que $D(C(b)) = b$, isto é, uma função identidade. Mas mostrar que, $D(C(b)) = b$ é o mesmo que provar que $D(C(b)) \equiv b(mod\ n)$. Observe que, como $D(C(b))$ e b estão no intervalo 1 e $(n-1)$ a congruência vale se, e somente se, a igualdade

for satisfeita. Note a relevância de termos escolhidos b (isto é, os blocos) menor que n. Assim temos,

$$D(C(b)) \equiv b^{de}(mod\ n).$$

Queremos então, para ser claro, mostrar que

$$b^{de} \equiv b(mod\ n)$$

No entanto, dizer que $ed \equiv 1(mod\ \phi(n))$ é o mesmo que $ed = 1 + k\phi(n)$, com $k \in \mathbb{Z}$. Note que $k > 0$, pois $e, d > 2$ e $\phi(n) > 0$. Desse jeito, podemos substituir ed por $1 + k\phi(n)$ na nossa equação modular anterior, ficando com

$$b^d e \equiv b^{1+k\phi(n)} \equiv b(b^{k\phi(n)}) \equiv b(b^{k(p-1)(q-1)})(mod\ n)$$

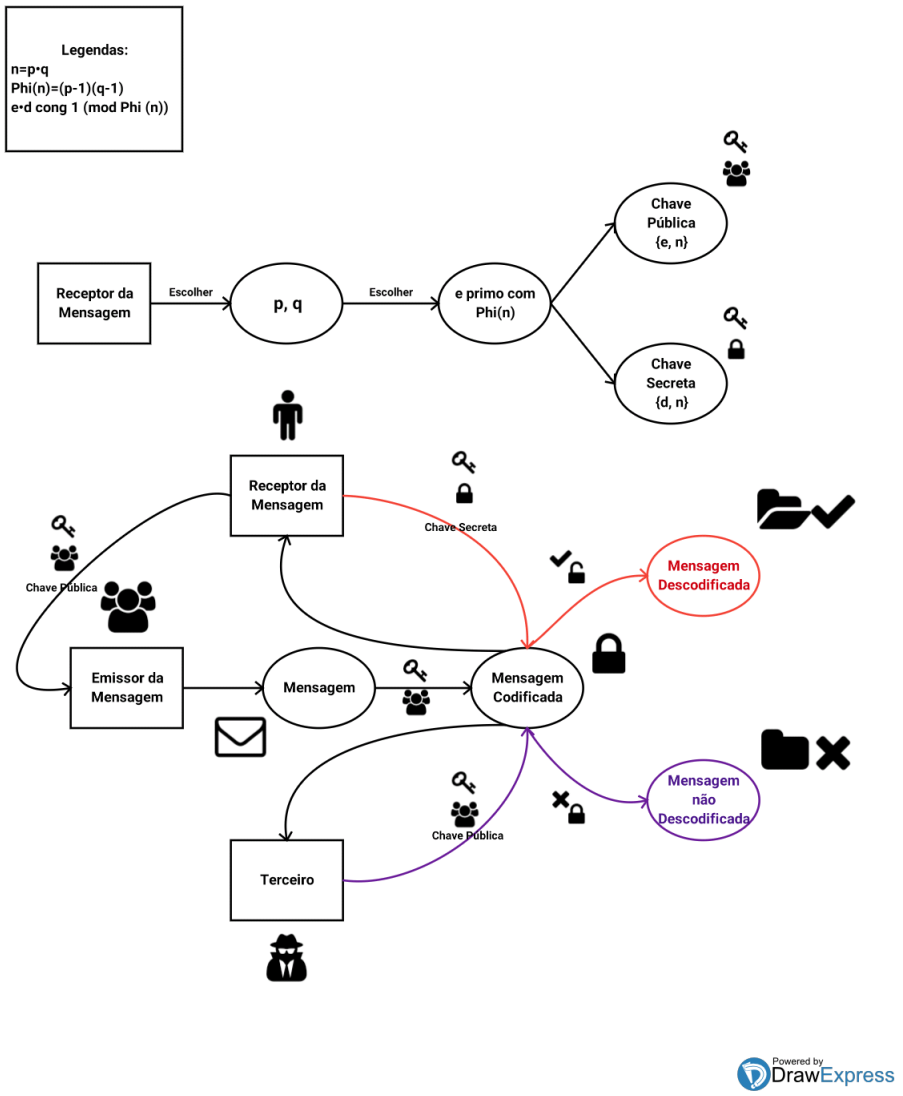
Vejamos, primeiramente, se conseguimos provar que $b^{de} \equiv b(mod\ p)$. Observe que se $p \not| b$, então pelo pequeno teorema de Fermat, temos que $b^{p-1} \equiv 1(mod\ p)$, logo $b^{de} \equiv b(mod\ p)$. Agora se $p|b$, então $b \equiv 0(mod\ p)$, ou seja, $b^{de} \equiv 0^{de} \equiv 0 \equiv b(mod\ p)$. Portanto, demonstramos que, realmente, $b^{de} \equiv b(mod\ p)$, e de forma análoga podemos provar que $b^{de} \equiv b(mod\ q)$. Mas como p e q, são primos distintos (isto é, mdc(p,q)=1) e como vimos que tanto p quanto q divide $(b^{de} - b)$, temos por conseguinte que n divide $(b^{de} - b)$, em outras palavras, $b^{de} \equiv b(mod\ n)$.

Note que, o par (d, n) é a nossa chave de codificação, também conhecida como chave pública. Em contrapartida, o par (e, n) é chave de desencriptação, nossa chave secreta. Na verdade para desencriptar a informação basta apenas conhecer e.

Dessa forma, utilizando o modelo de criptografia RSA, uma empresa ou indivíduo que queira preservar a informação daqueles que lhe enviam informações deve fornecer uma chave pública, (n, d), a eles para que eles possam encriptar suas informações. Em posse da chave secreta (n, e) somente o destinátario da mensagem pode descodificar a mensagem e ler seu conteúdo. Lembramos que essas chaves são obtidas pela escolha inicial do par de primos distintos.

Veja a seguinte figura:

Figura 1 – Diagrama RSA



Fonte: Do Autor, 2017.

Vejamos a seguinte situação: Imagine que uma empresa, que comercialize produtos pela internet, utilize o modelo de encriptação RSA para proteger as informações trocadas (via rede) por ela e seus clientes. O cliente para efetuar uma compra de um produto desta empresa utiliza seu cartão de crédito. Isto é, o cliente precisa declarar ao site da empresa certas informações (pessoais e de seu cartão de crédito) para que o crédito seja autorizado e a compra devidamente efetuada. Mas qualquer pessoa de posse dessas informações poderia utilizar o cartão de crédito daquele cliente. É nesse momento, que nosso modelo RSA entra em ação, pois o site da empresa diz ao computador do cliente como ele deverá codificar aqueles dados, isto é, o site envia a chave de encriptação (chave pública) para o cliente, como vimos, o par (n, d). Agora, mesmo que no processo de transferência a mensagem seja interceptada por um terceiro, este não será capaz de decifrá-la detendo apenas a chave pública, pois ela é a chave de encriptação e não a chave de desencriptação

(lembre-se esse modelo é assimétrico), isto é, a chave privada (que sabemos que é (n, e)) que é mantida em segredo pela empresa. Então, para decifrar a mensagem esse terceiro mal intencionado precisaria basicamente de saber quem são p e q. Mas isso não seria fácil de se descobrir? Uma vez que bastaria ele fatorar n.

Mas uma coisa que ainda não dissemos é que uma chave segura de RSA é gerada a partir de números primos de cerca de 100 algarismos cada, de forma que n, por ser o produto desses primos,teria cerca de 200 algarismos. Apesar da idéia parecer simples, na prática, é inviável, pois trata-se de uma limitação tecnológica, uma vez que não há computadores rápidos o bastante, nem mesmo algoritmos bons o suficiente, que permitam fatorar um número inteiro de tamanho astronômico que não tenha fatores relativamente pequenos (COUTINHO, 2009).

No próximo capítulo, veremos como será feita a modelagem desta técnica de criptografia utilizando apenas o software Geogebra.

4 Modelagem do RSA no Geogebra

A seção asseguir foi elaborada com base em informações obtidas em (GEOGEBRA,) e (GEOGEBRA, 2017).

4.1 Geogebra

O Geogebra é um software interativo de geometria, álgebra, estatística e cálculo, desenvolvido para ensino-aprendizagem de matemática e ciências desde a educação básica até a faculdade. Ele está disponível em diversas plataformas como: Windows, macOS, Linux, Android e iPad. Ele também pode ser utilizado no proprio navegador da internet.

Foi desenvolvido por Markus Hohenwarter em 2001 incialmente como parte de sua Tese de Mestrado na Universidade de Salzburg. Hoje ele conta com a ajuda de diversos desenvolvedores de código aberto e tradutores ao redor do mundo.

Com essa ferramenta pode-se fazer construções com pontos, vetores, segmentos, linhas, poligonos, cônicas, inequações e funções. Todas elas podem ser modificadas dinamicamente, isto é, elementos podem ser inseridos e modificados diretamente pelo mouse, ao toque, ou mesmo pela barra de entrada. O Geogebra nos permite também usar variáveis para números, vetores e pontos além de encontrar derivadas e intregais de funções dadas e possui outras diversas funções utéis.

Dentre suas principais funções podemos destacar:

1. Ambiente geométrico interativo (2D e 3D);
2. Planilha eletônica;
3. CAS (*computer algebra sumosstem* é um software matemático capaz de manipular expressões matemáticas de um jeito similar aos tradicionais cálculos feitos à mão por matemáticos e cientistas);
4. Ferramentas de estatística e de cálculo;
5. Programação;
6. Além de posssuir um vasto número de materiais interativos de ensino-aprendizagem em GeoGebraMaterials.

Asseguir, veremos algumas funções, comandos e estruturas utilizadas para construir o modelo RSA na plataforma do GeoGebra.

4.1.0.1 Comando, funções e estruturas do Geogebra

Na *Janela de Álgebra*, você pode diretamente inserir expressões algébricas usando a *Barra de Entrada* (localizada na parte inferior da janela do Geogebra). Após clicar em na tecla Enter sua expressão aparece na Janela de Álgebra enquanto sua representação gráfica aparece automáticamente na *Janela de Visualização*. A Janela de Visualização sempre exibe a representação gráfica de objetos criados no GeoGebra.

A Janela CAS (Computer Algebra System) permite que você utilize cálculos simbólicos. Por exemplo, se você colocar no campo de entrada dessa janela a expresão `(a+b)^2` sem ter atribuído valores para a e b obteremos $a^2 + 2ab + b^2$. Para atribuirmos valores nessa janela devemos utilizar `":="`. Por exemplo, para atribuirmos o valor 2 a letra a devemos prosseguir do seguinte jeito: `a:=2`. O símbolo "="é usado para definir equações nessa janela. As estruturas desta janela se comunicam com as demais janelas (Janela de Álgebra, Janela de Visualizção, etc.).

Para criarmos uma constante $a = 1$, por exemplo, basta inserirmos $a = 1$ na Barra de Entrada e apertar Enter. Já para criarmos a função $f(x) = x^2$, devemos inserir no Campo de Entrada `f(x)=x^2` e em seguida clicar em Enter.

Um *Controle Deslizante* é uma ferramenta que nos permite criar uma váriavel, onde podemos determinar o seu intervalo (isto é, seu valor mínimo e máximo) e também o incremento utilizado em sua variação. Em suas propriedades (para acessá-las, basta clicar em sua estrutura e selecionar propriedades), podemos escolher animar essa ferramenta, bem como a velocidade e a modalidade do movimento.

Para criar um *Botão* você primeiro deve ir no botão de criar um controle deslizante e clicar numa setinha apontada para baixo. Ao fazer isso aparecerá a opção para criar um botão. Você pode programá-lo para criar, alterar estruturas quando clicado. Por exemplo, esse ferramenta pode ser é utilizada para dar início à uma animação, ou até mesmo fazer aparecer ou ocultar certas estruturas na Janela de Visualização.

Assim como fizemos para achar a ferramenta Botão, o mesmo será necessário para criar um *Campo de Entrada* na Janela de Visualização. Você vai atrelar um objeto à esse campo de entrada, seja uma váriavel, uma lista (vetor) ou um texto. Ao digitar nesse campo você estará atribuindo, àquele objeto atrelado a ele, aquilo que você escrever dentro dele (podendo alterar a natureza do objeto).

Uma lista (vetor) pode ser criada de maneira fácil utilizando apenas a Barra de Entrada. Já na Barra de Entrada, digite o nome que você queira dar a sua lista e iguale aos elementos que a compõe separando os por vírgulas. Por exempo, `lista1={1,2,3,4,5}`.

Asseguir apresentaremos alguns comandos que utilizamos para modelar o RSA no GeoGebra:

1. `Sequência[<Expressão>,<Váriavel>,<Valor Inicial>,<Valor Final>]`.
   Com esse comando você gera uma lista de elementos, que obedecerão a lei de formação

colocada no primeiro campo. No segundo campo você irá denfinir quem é a variável da lei de formação da sequência. No terceiro e quarto, você definirá qual valor que a variável irá começar e terminar, respectivamente. O incremento utilizado nesse comando é sempre 1.

2. `Dimensão[<Objeto>]`
   Esse comando retorna a dimensão do objeto. Seja a `lista1={1,5,7}`, fazendo `Dimensão[lista1]` obteremos o número 3.

3. `Se[<Condição>,<Então>,<Senão>]`
   Esse comando retornar o valor ou executa a ação colocada no segundo campo caso a condição colocada no primeiro campo seja satisfeita, caso contrário, retorna o valor ou executa a ação colocada no terceiro campo.

4. `ÉInteiro[<Número>]`
   Esse comando retorna *true* (verdadeiro) se o número testado for inteiro, do contrário retorna *false* (falso).

5. `IniciarAnimação[<Controle Deslizante ou Ponto>,<true or false>]`
   Esse comando inicia a animação de um ponto ou controle deslizante caso a afirmação colocada no segundo campo seja verdadeira e ele para a animação desses objetos caso a afirmalção seja falsa.

6. `TextoParaUnicode[<Texto>]`
   Cada caracter possui um inteiro correspondente no GeoGebra. Ao utilizarmos esse comando, transformamos um texto em uma lista, de mesmo número de caracteres, composta pelo número associado a cada caracter utilizado no texto, respeitando a mesma ordem.

7. `UnicodeParaTexto[<Lista de Inteiros>]`
   Esse comando faz exatamento o oposto do comando anterior.

8. `Elemento[<Lista>,<Posição do Elemento>]`
   Esse código retorna o número que está em determinada posição (segundo campo) de uma lista (primeiro campo).

9. `Resto[<Número Dividendo>,<Número Divisor>]`
   Retorna o resto da divisão do número situado no primeiro campo pelo número do segundo campo.

10. `MDC[<Número>,<Número>]`
    Retorna o valor do mdc entre os dois números selecionados.

11. `" "`
    Dá qualidade de texto a variavél declarada. Exemplo, se você definir `texto1="Olá"`, você irá criar um texto na Janela de Visualização dizendo *Olá*.

12. `!`
    Negação da afirmação seguinte. Exemplo, se temos `a!=0`, quer dizer que a é diferente de 0.

13. `floor(<x>)`
    Retorna o maior inteiro menor ou igual a número inserido.

14. `ParteDaLista[ <Lista>,<Posição Inicial>,<Posição Final>]`
    Particiona uma lista, de modo que o número inserido no segundo campo de entrada corresponde a posição inicial da partição e o número do último campo de entrada corresponde à final. Portanto esse comando nos retorna um pedaço da lista (isto é, outra lista).

15. `ElementosÚnicos[<Lista>]`
    Esse comando retira todos os elementos repetidos da lista, isto é, gera uma nova lista a partir de uma outra com apenas elementos únicos.

16. `PróximoPrimo[<Número>]`
    Retorna o menor primo maior que o número selecionado.

17. `PrimoAnterior[<Número>]`
    Retorna o maior primo menor que o número selecionado.

18. `FatoresPrimos[<Número>]`
    Lista os fatores primos de um número. Por exemplo, FatoresPrimos[20]={2,2,5}.

19. `Frequência[<Lista>]`
    Gera uma outra lista com a frequência de seus elementos. Por exemplo, Frequência[{2,2,5}]={2,1}.

20. `Produto[<Lista>]`
    Retorna o produto dos elementos pertencentes a uma lista. Por exemplo, Produto[{2,2,5}]=20.

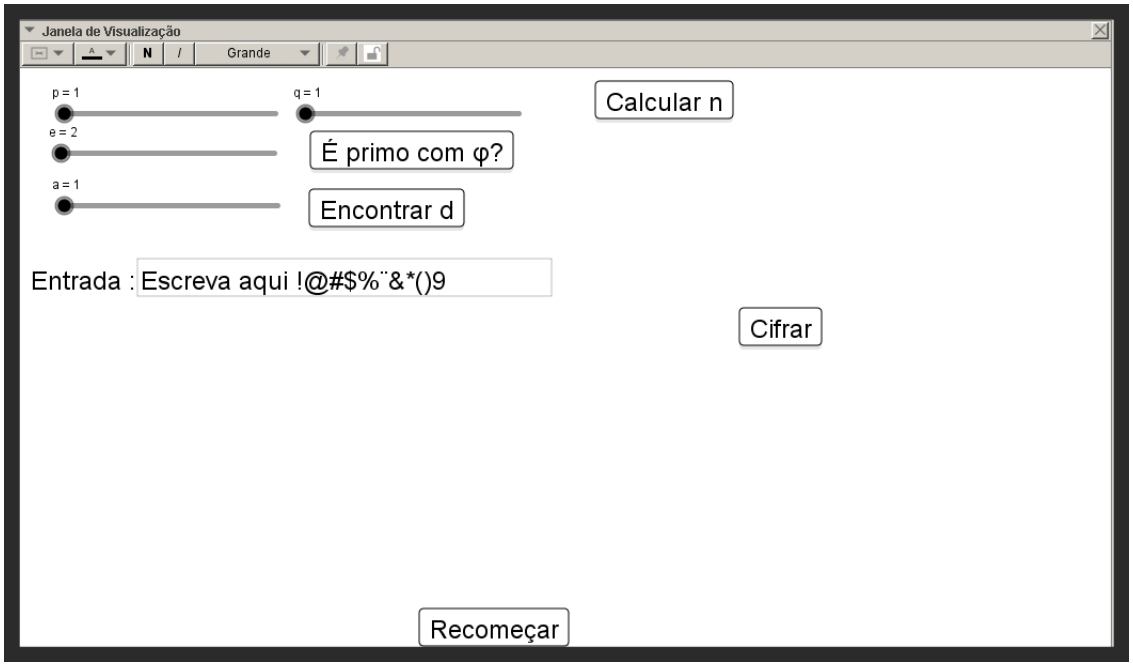
Apresentaremos na próxima seção como operar o modelo de criptografia RSA adaptado no Geogebra, em seguida mostraremos como foi pensado e construido.

4.2 Modelo RSA no GeoGebra

A modelagem da técnica RSA realizada neste trabalho pode ser encontrada em: <https://ggbm.at/MVERRUUZ>.

A figura seguinte mostra como é a estrutura inicial do nosso modelo RSA.

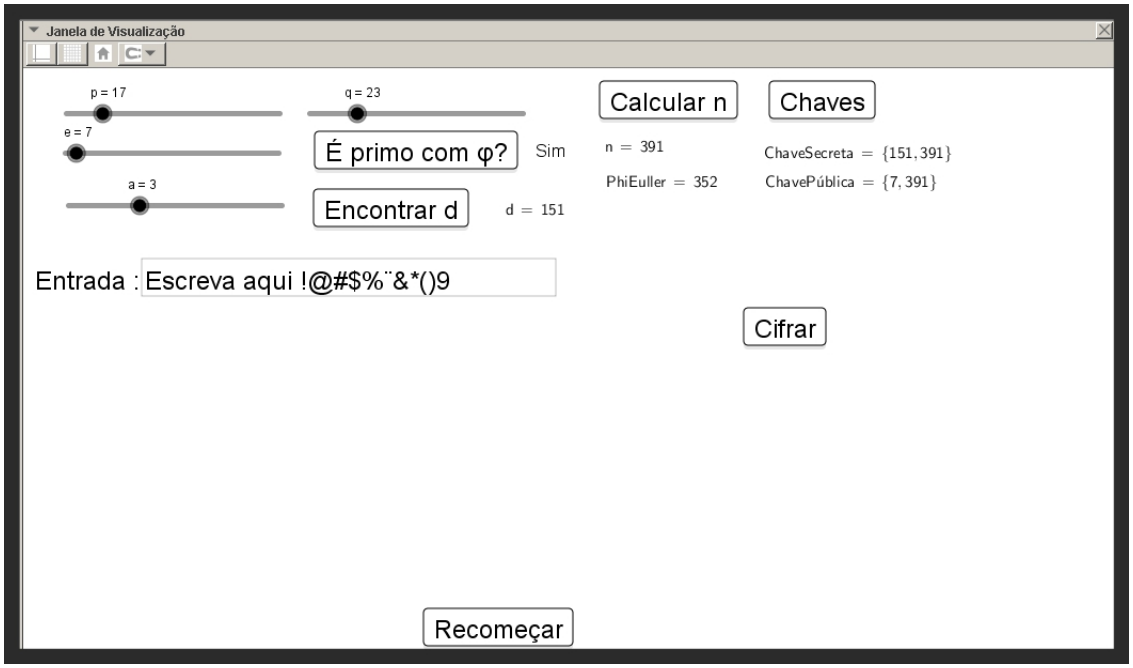
Figura 2 – Tela inicial



Fonte: Do Autor, 2017.

A primeira coisa que queremos fazer é criar nossas chaves de encriptação e desencriptação. Para alcançar tal objetivo, devemos, primeiramente, escolher p e q primos distintos. Sendo assim, por meio dos controles deslizantes p e q, escolhemos, a nosso gosto, os primos que darão origem às nossas chaves. Após a escolha deles, utilizaremos o botão *Calcular* n para calcular o nosso n e também $\phi(n)$ (representado na figura por PhiEuller). Tendo em mãos o valor $\phi(n)$, devemos escolher e de tal modo que $mdc(e, \phi(n)) = 1$, ele será parte da nossa chave privada. Podemos verificar se nosso e escolhido é primo com $\phi(n)$, usando o botão *É primo com* ϕ*?*. Uma vez escolhido e temos que achar d de tal forma que $ed \equiv 1(mod\phi(n))$, isto é, o inverso multiplicativo de e módulo $\phi(n)$. Assim, basta clicar no botão *Encontrar d*. Esse botão irá nos retornar o d que estávamos procurando. Ele fará parte da nossa chave pública. Em seguida, clicamos no botão *Chaves* para deixar claro quem são nossas chaves. A seguinte figura ilustra o resultado dos procedimentos que abacamos de mencionar.

Figura 3 – Criando Chaves de codificação e descodificação

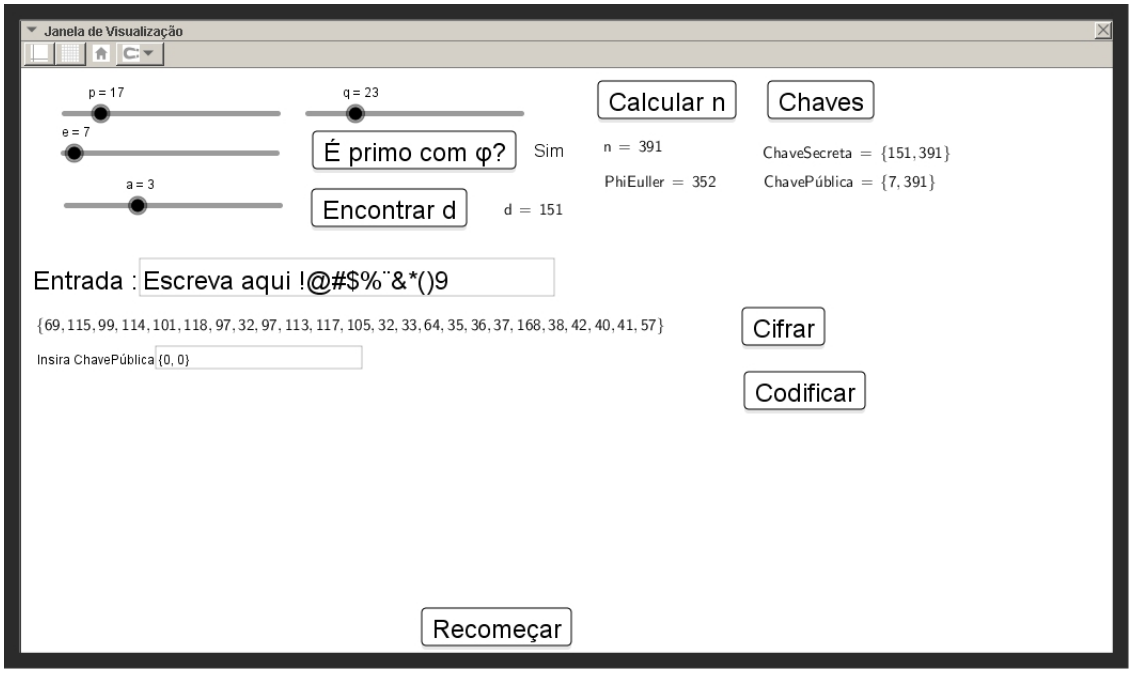


Fonte: Do Autor, 2017.

Veja na imagem anterior que escolhemos os primos $p = 17$ e $q = 23$. Como nosso $\phi(n) = 352$, escolhemos $e = 7$ (note que o mdc entre esses números vale um). Tendo escolhido $e = 7$, determinamos nosso $d = 151$ (verifique que o produto desses números é congruente à 1 módulo $\phi(n) = 352$). Assim, nossas chaves pública e secreta são respectivamente, 7,391 e 151,391.

Agora queremos verificar se, realmente nossas chaves funcionam para encriptar e desencriptar nossa mensagem. No *campo de entrada* da Janela de Visualização chamado de *Entrada* você pode escrever a mensagem que quizer para testar o modelo. A etapa seguinte consiste em converter cada caracter da nossa mensagem para um número inteiro. Para realizar tal procedimento basta clicar no botão *Cifrar* (aqui usamos a palavra cifrar no sentido de converter a mensagem para números inteiros). Feito isso, aparecerá um vetor de números inteiros embaixo da mensagem. Usaremos nossa mensagem padrão `Escreva aqui !@#$%&*()9` para mostrar que o GeoGebra além de letras também converte outros caracteres especiais e até números. Veja como ficaria na figura asseguir:

Figura 4 – Conversão da mensagem para inteiros

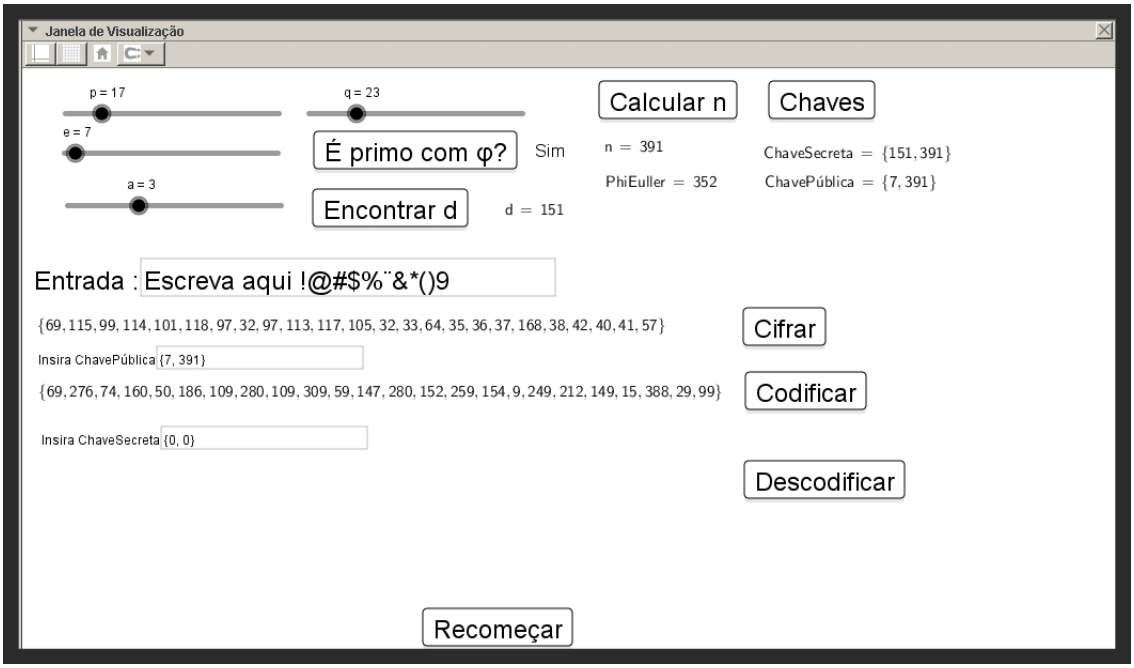


Fonte: Do Autor, 2017.

Gostaria de fazer uma pequena observação, neste momento, pois nosso modelo sempre irá converter um mesmo caracter sempre da mesma forma, isto é, para um mesmo número inteiro. Dessa forma não temos liberdade para escolhermos como será feita a conversão, pois, para realizá-la, utilizamos um comando próprio do GeoGebra (a saber `TextoParaUnicode[]`).

Note também na imagem anterior, que surgiu um novo campo de entrada chamado de *Inserir Chave Pública*, logo abaixo do vetor encontrado. Nele devemos inserir nossa chave pública que sabemos é o par $7, 391$. Em seguida clicamos no botão *Codificar*, ele nos retornará (logo abaixo do campo de entrada anterior) um outro vetor já encriptado. A figura, a seguir, mostra o resultado do procedimento que acabamos de realizar.

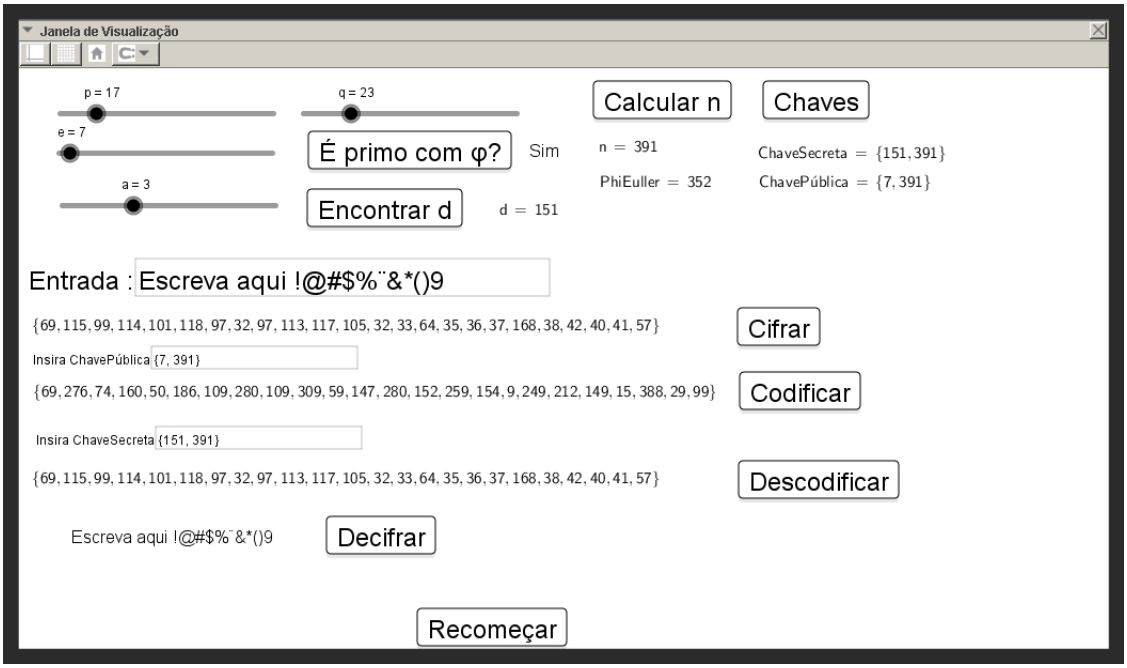
Figura 5 – Codificação da mensagem



Fonte: Do Autor, 2017.

Observe que, novamente, surgiu um novo campo de entrada denominado *Inserir Chave Secreta*. Assim procedemos da mesma forma que anteriormente: inserimos a chave secreta (que corresponde a $151, 391$) no novo campo de entrada e prontamente podemos clicar em *Descodificar*. Isso nos dará um novo vetor, que, se você reparar, será igual àquele nosso primeiro vetor, ou seja, fomos bem sucedidos no nosso processo de descodificação. Agora para finalizar você pode clicar em *Descifrar*, pois assim converteremos todos os números do nosso vetor para linguagem de texto. Veja na próxima figura:

Figura 6 – Descodificação da mensagem



Fonte: Do Autor, 2017.

Para utilizarmos o modelo novamente, desde o início, basta clicarmos no botão *Recomeçar*.

Algumas observações:

1. Você pode ter notado que, no nosso modelo, nós não separamos nossa mensagem em blocos, fato esse devido a complexidade do procedimento uma vez que ele deve respeitar as seguintes regras: o número de cada bloco tem que ser menor que n, e também o primeiro algarismo de cada bloco não pode ser 0. Dados os recursos que o GeoGebra nos oferece, não conseguimos encontrar uma maneira de programar esse procedimento. Com isso na prática nossa construção do modelo RSA no Geogebra não seria tão segura, pois se tratando de uma mensagem de tamanho considerável o método poderia ser quebrado por contagem de frequência, sem necessidade de descobrir a chave secreta.

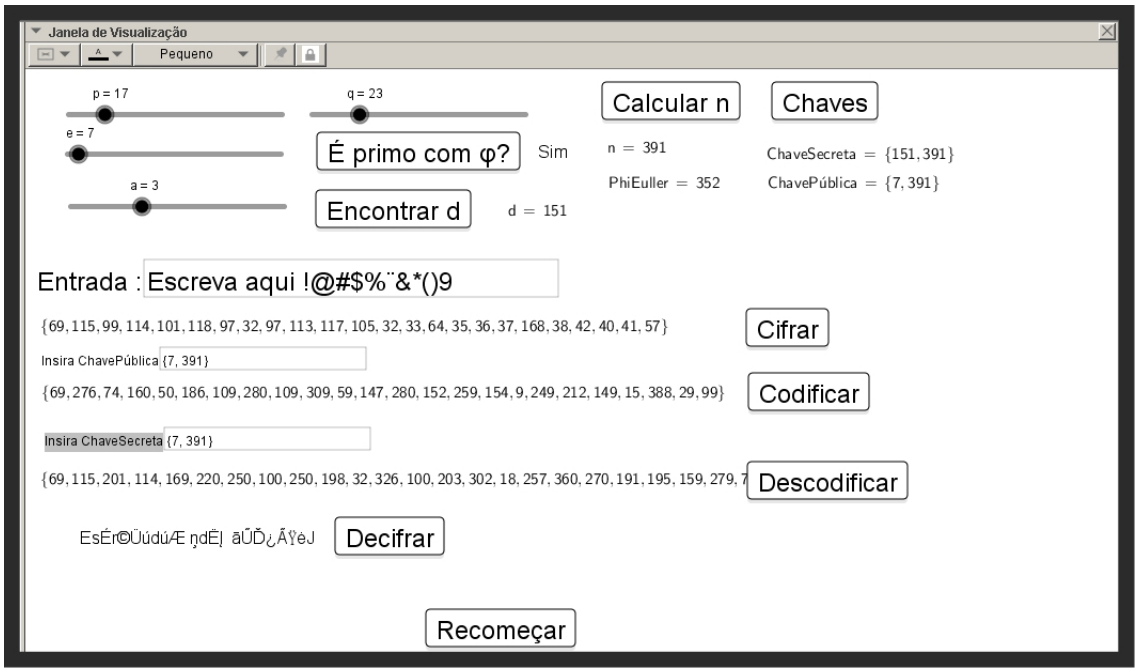
2. Lembre-se que utilizamos um comando do Geogebra para converter nossa mensagem para inteiros. Isso pode nos levar a alguns problemas. Veja que a letra s é convertida pelo GeoGebra no número 115, isso quer dizer que se escolhermos os primos $p = 7$ e $q = 11$ (ou seja, $n = 77$), após o processo de codificação e descodificação de tal elemento, obteremos um número menor que $n = 77$, ou seja, após o processo de "desconversão"obteremos um caracter diferente de s, a saber, o símbolo *&*. Não chegamos a testar todos os caracteres existentes, porém se tomarmos p e q tal que n seja maior que 300 não haverá esse tipo de problema para os caracteres presentes

num teclado de computador convensional. Ao apresentar esse modelo em sala de aula temos que explicar tal peculiariades. Podemos, ao utilizar essa construção em sala de aula, exigir que os alunos utilizem primos maiores que 15, e depois instigar eles a utilizar primos menores, explicando o porquê o método não retorna o resultado esperado. Acima de tudo temos que explicar que o número de caracteres (distintos) não pode ser maior que n, por isso devemos ter cuidado com a escolha de nossos primos.

3. Vale lembrar também que o número de algarismos de cada bloco no modelo RSA tem que ser o mesmo, para previnirmos ambiguidades. Contudo como não separamos em blocos e nem agrupamos todos os números em um só, não corremos esse risco.

4. Com esse material podemos mostrar para o aluno que mesmo um terceiro que tenha interceptado a mensagem e em posse (apenas) da chave pública ele não seria capaz de decifrar a mensagem, uma vez que sabemos que apenas com a chave secreta pode-se decodificar a mensagem encriptada, lembre-se que trata-se de um modelo de encriptação assimétrico. Veja a imagem a seguir:

Figura 7 – Erro ao se utilizar uma chave diferente da secreta



Fonte: Do Autor, 2017.

A seguir veremos como foi construido o modelo RSA utilizando as ferramentas do GeoGebra

4.3 Construindo o RSA no GeoGebra

Em primeiro lugar, criamos os controles deslizantes p e q. Depois configuramos eles para variar, cada um, de 1 até 100, com incremento de uma unidade. Criados p e q, definimos `n=p*q`. Definimos *PhiEuller* do seguinte jeito:

`PhiEuller=Produto(L_4)`,

onde

`L_1=FatoresPrimos(n)`,

`L_2=Frequência(L_1)`,

`L_3=ElementosÚnicos(L_1)` e

```
L_4=Sequência((Elemento(L_3, k) - 1)

        (Elemento(L_3, k)^(Elemento(L_2, k) - 1)), k, 1, Dim2).
```

Note que tal modelagem corresponde justamente a $\phi(n)$, como vimos em 3.4.

Os números n e *PhiEuller* não estarão visíveis na Janela de Visualização, para mudarmos isso, devemos clicar neles e arrastá-los da Janela Álgebra para a Janela de Visualização. Criamos também uma constante $CN = 1$ (logo você entenderá o porquê de sua criação). Em seguida criamos o botão *Calcular n*. Na programação de seu botão, adicionamos na aba *Ao Clicar* o seguinte código CN=1. Isto significa, que toda vez que clicarmos no botão *Calcular n*, teremos $CN = 1$. Posteriormente, clicamos em n com o botão direito do mouse para acessarmos suas propriedades. Na aba *Avançado*, colocamos, no campo de entrada *Condição para Exibir Objeto(s)*, `CN==1`. Desta forma n só aparecerá na Janela de Visualização quando $CN = 1$. Faremos exatamente o mesmo para `PhiEuller`.

Podemos, neste momento, criar o controle deslizante e configurando-o da mesma forma que fizemos para p e q. Em seguida, criamos `b=MDC[e,PhiEuller]` e `v=2`. Criamos, em seguida, os textos *Sim* e *Não*. Na *Condição para Exibir Objeto(s)* desses textos colocaremos para o primeiro `v==1` e para o segundo `v==0`. Logo após isso, criaremos o botão *É primo com ϕ?* de tal forma que na aba *Ao Clicar* de sua programação colocaremos `v=Se[b==1,1,0]`. Sempre que clicarmos nesse botão, se e e *PhiEuller* forem primos entre si ($b = 1$), então $v = 1$ e portanto a mensagem *Sim* irá aparecer, caso contrário ($b \neq 1$), $v = 0$ e a mensagem irá que aparecer será *Não*. Note que as duas mensagens nunca vão aparecer ao mesmo tempo.

Agora queremos achar d. Para isso, sabemos que $ed \equiv 1(mod\phi(n))$ o que vale dizer que $d = \frac{1+a\phi(n)}{e}$ para algum $a \in \mathbb{Z}$. Definiremos nosso d com essa última expressão e

colocaremos em sua *Condição para Exibir Objeto(s)* `ÉInteiro[d]`. Posteriormente, criamos um controle deslizante a variando de 1 até e com um incremento de uma unidade. Você pode estar se perguntando, porque variar a até e? A resposta é simples, pois se $a = e$, temos $\frac{1+e\phi(n)}{e} = \frac{1}{e} + \phi(n)$ e nós sabemos que existe um $d < \phi(n) < \frac{1}{e} + \phi(n)$, com $d \in \mathbb{Z}$ que satisfaz $ed \equiv 1(mod\phi(n))$. Logo se variarmos a até e garantiremos encontrar tal d. Após criarmos o botão *Encontrar d* colocaremos em sua programação na aba *Ao Clicar* os seguintes comandos `IniciarAnimação[a, !ÉInteiro[d]]`, $w = 1$ e $finD = 1$. Voltando para o controle deslizante a colocaremos em sua programação `Se[w==1,IniciarAnimação[a, !ÉInteiro[d']]]`, onde $d' = \frac{1+(a+1)\phi(n)}{e}$.Bom explicaremos, a seguir, o que acontece quando clicamos no botão *Encontrar d*: se d não é inteiro, ele inicia a animação do controle deslizante a, além disse coloca $w = 1$, mas se $w = 1$, então o controle deslizante a vai parar sua animação quando d' for inteiro. Mas o que realmente acontece e que a animação verifica quando d' é inteiro mas ela só para no valor seguinte de a quando d' já não é mais inteiro, mas por "sorte"meu d nesse momento é inteiro, pois nosso $d(a) = d'(a-1)$. Assim se meu d é inteiro então ele irá aparecer na Janela de Visualização (pois essa é a condição que colocamos para que ele aparecesse).

Criaremos o botão *Chaves* cuja a condição para ele aparecer também será `ÉInteiro[d]`. Colocaremos em sua programação o seguinte código $keys = 1$, de forma que toda vez que for clicado ele fará $keys = 1$. Duas listas também serão construídas, são elas: `Chave Pública={d,n}` e `Chave Secreta={e,n}`. Em *Condição para Exibir Objeto(s)* de ambas as listas colocaremos `keys==1`, assim quando clicarmos em *Chaves* fará com que essas duas listas aparecam e nos mostre quem são nossas chaves de encriptação e desencriptação.

A próxima etapa consiste em criarmos um campo de entrada na Janela de Visualização, no nosso caso, o chamamos de *Entrada:*. Essa estrutura nós permitirá escrever nossa mensagem secreta. O texto que escrevermos nela estará atrelado a uma variável de texto, nosso caso *texto2*.

Asseguir iremos realizar a conversão dos caracteres de nossa mensagem para inteiros. Utilizamos, para tal, o seguinte comando

`MsgCifrada:=TextoParaUnicode[texto2]`,

que foi inserido na Janela CAS. Dessa forma criamos um vetor com todos os caracteres da mensagem convertidos para inteiros. Como condição para essa lista aparecer, colocamos `Cif==1`. Por essa razão criamos o botão *Cifrar* que em sua programação foi inserido o código `Cif=1`. Logo, sempre que clicarmos nele, a lista aparecerá.

Em seguida, construímos outro campo de entrada chamado *Insira Chave Pública* atrelado à váriavel *CP*. É neste campo que devemos inserir nossa chave pública (d,n) para podermos encriptar nossa frase secreta. Ele irá aparecer quando `Cif=1`.

Um dado importante para construção dos vetores de codificação e decodificação é o número de caracteres que nossa mensagem possui. Como o vetor *MsgCifrada* possui o mesmo número de elementos que nossa mensagem, utilizamos o seguinte comando para salvar esse número, `Dim=Dimensão[MsgCifrada]`, onde *Dim* é o nome da váriavel que será responsável por guardar esse tamanho do vetor.

Para construir o vetor que representa nossa mensagem encriptada utilizamos o seguinte comando:

`Sequência[Resto[Elemento[MsgCifrada,k]^Elemento[CP,1],Elemento[CP,2]], k,1,Dim,1]`.

O que ele faz é muito simples, ele determina o resto de cada elemento do vetor *MsgCifrada* elevado a *Elemento[CP,1]* quando divido por *Elemento[CP,1]*, lembrando que $CP = d, n$, nossa chave pública. Note que ele é o nosso algoritmo de encriptação. Como condição para ele aparecer, colocamos `Cod==1`. Para isso criamos o botão *Codificar*, que quando clicado fará `Cod=1`. Tal botão só aparecerá quando `Cif=1`.

Construímos mais um campo de entrada, *Inserir Chave Secreta*. Esse agora será o lugar para inserirmos nossa chave secreta, e, n. Ele também só aparecerá quando `Cod=1` e está vinculado à variável *CS*.

Por outro lado, afim de construir o vetor que será nosso algoritmo de desencriptção, usamos o seguinte código

`Sequência[Resto[Elemento[MsgCodificada,k]^Elemento[CS,1],Elemento[CS,2]], k,1,Dim,1]`.

Observe a semelhança dele com o anterior. É fácil ver que, ele retorna o resto da divisão euclidiana de cada elemento de *MsgCodificada* elevado a *Elemento[CS,1]* por *Elemento[CS,2]*, recordando que $CS = e, n$, nossa chave secreta. Colocamos como condição para esse vetor aparecer, `DCod==1`. Fizemos outro botão, *Descodificar*, que terá o papel de justamente fazer nosso vetor descodificado fique visível, isto é, colocamos em sua programação `DCod=1`. Esse botão tornará-se visível quando `Cod=1`.

Agora para convertermos os valores do vetor desencriptado para a linguagem de texto, criamos um texto com o código

`MsgDescifrada=UnicodeParaTexto[MsgDescodificada]`.

Essa mensagem de texto só aparecerá quando `DCif==1`, cujo responsável para tal acontecimento será o botão *Decifrar* que só aparecerá se `DCod=1`.

Por fim temos o botão *Recomeçar* que possui os seguintes comandos em sua programação:

1. Cif=0 $\longrightarrow$ Esconde o vetor *MsgCifrada*, o campo de entrada *Inserir Chave Pública* e o botão *Codificar*

2. Cod=0 $\longrightarrow$ Esconde o vetor *MsgCodificada*, o campo de entrada *Inserir Chave Secreta* e o botão *Descodificar*
3. DCod=0 $\longrightarrow$ Esconde o vetor *MsgDescodificada* e o botão *Decifrar*.
4. DCif=0 $\longrightarrow$ Esconde o texto *MsgDecifrada*
5. v=2 $\longrightarrow$ Esconde tanto o texto *Sim* quanto *Não*
6. w=0 $\longrightarrow$ Não permite que o controle deslizante a entre em animação.
7. CP=0,0 $\longrightarrow$ Deixa o valor do campo de entrada *Inserir Chave Pública* igual a 0,0.
8. CS=0,0 $\longrightarrow$ Deixa o valor do campo de entrada *Inserir Chave Secreta* igual a 0,0.
9. keys=0 $\longrightarrow$ Esconde as chaves pública e secreta.
10. p=1 $\longrightarrow$ Atribui a p o valor 1.
11. q=1 $\longrightarrow$ Atribui a q o valor 1.
12. e=2 $\longrightarrow$ Atribui a e o valor 2 (não pode ser nesse caso 1, pois se o fosse, a deixaria de ser um controle deslizante).
13. a=1 $\longrightarrow$ Atribui a a o valor 1.
14. CN=0 $\longrightarrow$ Esconde n e $PhiEuller$.
15. PhiEuller=0 $\longrightarrow$ Atribui a $PhiEuller$ o valor 0.
16. L_4= $\longrightarrow$ Transforma L_4 em uma lista vazia.
17. L_3= $\longrightarrow$ Transforma L_3 em uma lista vazia.
18. L_2= $\longrightarrow$ Transforma L_2 em uma lista vazia.
19. L_1= $\longrightarrow$ Transforma L_1 em uma lista vazia.

Vale ressaltar que os três vetores criados, *MsgCifrada*, *MsgCodificada* e *MsgDescodificada* foram criados na Janela CAS, pois acreditamos que a Janela Álgebra exige mais memória do que a Janela CAS. Nós observamos que, quando usamos a função `Resto[<Número>,<Número>]`, cujo primeiro número constitui um valor muito alto, na Janela Álgebra, ela retorna valor indefinido, o que já não acontece com a Janela CAS.

4.4 Aplicação do Modelo RSA em Sala de Aula

Aqui lembramos que o público alvo deste trabalho são alunos do Ensino Médio, pois acreditamos que eles, a esse tempo, já terão a maturidade e os conhecimentos necessários para compreender como esse modelo de criptografia funciona.

Tendo em vista a concepção de contextualização como uma metodologia enriquecedora e motivadora do ensino, acreditamos que a apresentação do modelo de criptografia RSA em sala de aula deve seguir a recaptulação de definições e conceitos como os de números primos, de fatoração, de MDC e MMC, e também do resto da divisão entre dois números inteiros.

Apenas dessa maneira tal contextualização se tornará significativa, pois permitirá o aluno a conectar os saberes apreendidos em sala de aula com suas utilidades no mundo real, deixando, assim, a aprendizagem mais interessante e consolidando tal conhecimento.

Devemos presumir que alguns alunos não saibam o que se entende por criptografia, logo faz-se necessário a introdução de seus conceitos mais básicos (como fizemos nesta dissertação) para que essa contextualização seja mais completa e efetiva.

A exposição do método pode ser feito na lousa, enquanto para os alunos interagirem com o modelo do RSA feito no GeoGebra precisará da disponibilidade do laboratório de informática da escola.

Asseguir utilizaremos o exemplo visto na seção 3.4 com uma línguagem mais acessível aos alunos para mostrar como o método funciona.

Assim queremos criptografar a seguinte frase:

`PENSO LOGO EXISTO`

Escolhemos, aqui, dois números primos, p=17 e q=23, e dizemos que serão fundamentais para a codificação da mensagem.

Em seguida apresentamos nossa tabela de conversão que transformará nossos caracteres em números naturais.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Aqui faremos a observação que essa tabela de conversão fica a critério do codificador, ou seja, você pode atribuir quaisquer valores ao seu conjunto de caracteres, desde que cada um tenha valor diferente e o mesmo número de algarismos. Acrescentamos, também, que os espaços serão representados pelo número 99.

Fazendo a conversão, obteremos o seguinte número:

$$25142328249921241624991433182829 24$$

Em seguida quebraremos esse número em blocos, explicando a razão para tal, isto é, para impossibilitar que a mensagem seja decifrada por contagem de frequência, bem como o que se entende por isso.

Devemos explicar para os alunos quais são os critérios para essa divisão em blocos, a saber, o valor de cada bloco não pode ser superior a n, onde $n = pq$, e nenhum dos blocos podem iniciar com o algarismo 0.

A organização em blocos será realizada da mesma forma que fizemos na seção 3.4. Logo:

251-42-328-249-92-124-162-49-91-43-318-282-92-4

Agora para iniciar efetivamente o processo de cripografia devemos escolher um número e que seja primo com $(p-1)(q-1)$. Novamente optamos por $e = 3$. Sendo assim, podemos dizer aos alunos que o método para criptografar consiste em pegar o valor de cada bloco, elevar ele a $e = 3$, e encontrar o resto desse número obtido pela divisão dele por $n = 391$. O valor de cada bloco deverá ser substituido pelos respectivos restos encontrados. Realizando essa sequência de ações no vetor anterior, obteremos o seguinte:

38-189-193-5-207-108-185-349-114-134-28-354-207-64

Dessa forma, nossa mensagem encontra-se criptografada. Queremos, neste momento, descriptografá-la. Para isso devemos, primeiro, encontrar um d tal que o resto da divisão de ed por $(p-1)(q-1)$ seja igual a 1. Como neste caso $e = 3$ e $(p-1)(q-1) = 16 * 22 = 352$, temos que $d = 235$. Assim de forma análoga ao processo de codificação da mensagem seguimos com a descodificação, para ser mais claro, pegamos os valores atualizados de cada bloco, elevamos eles a $d = 235$, e a partir desse processo encontramos o resto da divisão deles por $n = 391$. Com isso obteremos os seguintes valores:

251-42-328-249-92-124-162-49-91-43-318-282-92-4

Nesse instante, podemos pedir os alunos para comparar os números dos blocos antes do processo de codificação com os obtidos após a descodificação. Eles observarão que os dois serão os mesmos e portanto o método de criptografia RSA funciona. Basta, agora, para finalizar eliminar a organização em blocos e usar a tabela de conversão para retornar a mensagem original.

Algumas observações devem ser feitas aos alunos. A primeira é que a Chave Secreta neste caso consiste no par e, n e a Chave Pública no par d, n. Vale lembrar que não importa qual é qual, pois o que se deve levar em consideração é que o que for encriptado por uma só pode ser descodificado pela outra e vice-versa. O que define qual delas é a secreta e qual é a pública é decisão de colocar uma delas em absoluto sigilo. Outra observação importante é que a segurança do método reside na escolha dos primos p e q que permanece oculta, pois conhecendo eles a informação encriptada poderia ser desvendada. No entanto, esse primos são escolhidos de tal forma que cada um deles possua ao menos 100 algarismos, impossibilitando, dessa maneira, a fatoração de n que é informação dada, pois faz parte da chave pública. Como já dito, não existe, ainda, capacidade computacional ou algoritmo realmente eficaz capaz de fatorar um inteiro n (cujos os fatores não são relativamente pequenos) de tal ordem em tempo hábil.

A seguir apresentamos um passo a passo para para facilitar o entendimento do modelo RSA pelos alunos:

1. Determinando as chaves pública e privada.

   a) Seja $n = pq$. Escolha p e q, primos distintos;

   b) Escolha e, de tal forma que ele seja primo com $(p-1)(q-1)$, isto é,

   $$mdc(e, (p-1)(q-1)) = 1;$$

   c) Encontre d, tal que, o resto da divisão de $e \cdot d$ por $(p-1)(q-1)$ seja igual a 1.

   d) Feito os passos anteriores você terá encontrado suas chaves. Sua chave pública corresponde ao par $\{d, n\}$. Agora sua chave secreta corresponde ao par $\{e, n\}$.

2. Encriptando uma mensagem.

   a) Escolha uma mensagem.

   b) Converta seus caracteres para valores naturais. Para isso, utilize a tabela de conversão.

   c) Organize o número obtido (mensagem convertida) em blocos.

   d) Pegue o valor de cada bloco e eleve a d-ésima potência. Agora substitua os valores de cada bloco pelos valores encontrados.

   e) Com os valores dos blocos atualizados, descubra seus respectivos restos quando divididos por n. Atualize novamente os valores dos blocos por esses que você acabara de encontrar.

   f) Com isso sua mensagem agora está encriptada. Veja que nos dois itens anteriores você utilizou a chave pública ($\{d, n\}$) para encriptar a mensagem.

3. Desencriptando uma mensagem.

    a) Pegue os valores atualizados de cada bloco eleve-os a e-ésima potência. Atualize os valores dos blocos para esses encontrados.

    b) Com os valores dos blocos atualizados, descubra seus respectivos restos quando divididos por n. Atualize novamente os valores dos blocos por esses que você acabara de encontrar. Perceba que os valores dos blocos nesse momento equivalem aqueles que você obteve ao converter os caracteres de sua mensagem para números naturais.

    c) Veja que, nos dois itens anteriores, você utilizou a chave secreta ($\{e, n\}$) para descodificar a mensagem encriptada.

    d) Para voltar a mensagem à sua forma original disfaça os blocos e utilizando a tabela de conversão transforme os números naturais em caracteres.

Afim de ilustrar melhor esse modelo de criptografia para os alunos na vida cotidiana, podemos citar a situação apresentada no final do capítulo anterior, isto é, o exemplo da empresa que quer comercializar produtos pela internet.

Sabendo, agora, os alunos, como funciona o método, apresentamos, asseguir, um roteiro que auxilie os alunos interagir com a modelagem do RSA feita no GeoGebra.

1. Digite no campo de entrada a mensagem a qual você quer codificar.

2. Escolha p e q primos distintos, cujo seu produto seja maior que 300.

3. Aperte o botão "Calcular n".

4. Escolha e de forma que ele seja primo com "PhiEuller". Obs: Você pode verificar tal fato clicando no botão "É primo com Φ ?".

5. Encontre d. Obs: Tente encontrá-lo primeiro antes de clicar no botão "Encontrar d". Você sabe que d deve ser tal que $e * d$ divido por $PhiEuller = (p-1)(q-1)$ deve obter resto 1.

6. Você agora já sabe quais são as chaves de codificação e descodificação, no entanto, clique no botão "Chaves"para definirmos qual delas será a pública e qual será a privada.

7. Clique no botão "Cifrar". Note que cada caracter da mensagem foi transformado em um número inteiro pré-estabelecido pelo GeoGebra. Essa conversão é sempre constante, isto é, sempre um mesmo caracter será levado ao mesmo valor.

8. Insira a Chave Pública em seu respectivo campo de entrada, em seguida, clique no botão "Codificar".

9. Insira a Chave Secreta em seu respectivo campo de entrada, em seguida, Clique no botão "Descodificar".

10. Clique no botão "Decifrar"e confira se corresponde a mensagem inicial.

11. Clique no botão "Recomeçar"e repita todos os itens anteriores utilizando primos diferentes dos escolhidos em sua primeira vez.

12. Em seu caderno, agora, você irá realizar todo o processo de Criptografia RSA. Escolha uma palavra com mais de 5 letras, dois números primos distintos, e com eles codifique a palavra e depois descodifique a mensagem codificada e veja se o resultado é a palavra escolhida inicialmente. Utilize a calculadora do computador para efetuar os cálculos. Por fim utilize esse exemplo na ferramenta construída no GeoGebra para efeito de comparação.

13. Refaça os itens de 1 a 10, inserindo no campo de entrada da Chave Secreta sua Chave Pública e no campo de entrada Chave Pública sua Chave Secreta. Observe o resultado e tire conclusões.

14. Refaça os itens de 1 a 10, inserindo no campo de entrada da Chave Secreta, valores diferentes daquele que você deveria colocar. Observe o resultado e tire conclusões.

15. Refaça os itens de 1 a 10, tomando p e/ou q não primos. Tire conclusões.

16. Refaça os itens de 1 a 10, sem observar o critério que o produto de p e q seja maior 300. Utilize p e q menores que 12. O método funcionou? Tente explicar o porquê.

17. Refaça os itens de 1 a 10, escolhendo $p = q$.

18. Refaça os itens de 1 a 10, escolhendo e de forma que ele não seja com primo com $PhiEuller$.

O décimo segundo item do roteiro busca que o aluno não só compreenda que a metodologia RSA não se dá através de mágica, mas sim que existe todo conjunto lógico de cálculos que fazem o método funcionar e que usamos o computador apenas por sua capacidade de calcular que viabiliza o uso dessa técnica de criptografia. Com esse item também o professor terá a oportunidade de ensinar os alunos algumas novas funções das calculadoras cientificas que serão importantes para a vida do aluno. Talvez a maior dificuldade para os alunos nesse item seja encontrar d em função de e e $PhiEuller$, contudo cabe o professor ajudá-los nesse momento.

O item 13 do roteiro reforça a idéia de que o que for encriptado por uma chave pública só pode ser descodificado por sua respectiva chave secreta, e que o inverso também é verdadeiro.

Os items 14 ao 18, são bem relevantes, pois mostrarão ao aluno que essa técnica de criptografia só funcionará se tomarmos p e q primos distintos, se os valores a serem codificados forem menor do que n e se e for primo com $PhiEuller$. Além disso, observar que apenas com a Chave Secreta que se poderá descriptografar a mensagem encriptada (pela Chave Pública).

5 Crivo de Eratóstenes

O presente capítulo foi escrito com base nas informações encontradas em (COUTINHO, 2009).

Eratóstenes de Cirene (276 a.C. - 194 a.C.) foi um matemático, astrônomo, geógrafo, gramático, bibliotecário e poeta da Grécia Antiga. Nasceu em Cirene, e morreu em Alexandria. Apesar de sua profiência em diversos ramos de conhecimento, seus contemporâneos julgavam que ele não havia alcançado a perfeição em nenhum. Razão essa, pela qual era chamado de "Beta", uma alusão a segunda letra do alfabeto grego. Ele é mais conhecido por ter calculado a circunferência da Terra e também pelo Crivo de Eratóstenes, que ainda constitui uma importante ferramenta na teoria dos números. O crivo é citado na obra *Aritmética* de Nicômaco, publicada por volta de 100 d.C., que segundo ele, trata-se de um método para obter números primos, fazendo analogia à uma peneira, uma vez que pegamos os números ímpares misturados e separamos os primos (ou indecomponíveis) dos compostos (ou secundários). É fácil de entender o emprego da palavra *ímpares* da oração anterior, pois com excessão do número 2 todos os primos são ímpares.

O crivo é uma simples técnica de encontrar todos os primos até um inteiro positivo n dado previamente. O uma variante do método (mas sem perder sua essência) consiste, em primeiro lugar, escrevermos uma lista de todos os números naturais até n. Tomando $n = 100$, temos:

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Em primeiro lugar, eliminaremos o número 1, pois sabemos que ele não é primo (aliás nem composto). Partindo do 2 crivaremos todos os demais números saltando de 2 em 2, com isso todos os múltiplos de 2 da tabela serão cortados da tabela com exceção do próprio 2. Veja asseguir:

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

Assim, eliminamos todos os pares da tabela exceto o 2. O próximo número não riscado é 3. Assim partindo do 3 cortaremos todos os outros números menores que n saltando de 3 em 3, eleminando, dessa forma, todos os múltiplos de 3.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

O próximo número não riscado é 5. Seguindo o mesmo raciocínio, iniciando no 5 cortaremos todos os demais os números de 5 em 5. Observe asseguir:

~~1~~	2	3	~~4~~	~~5~~	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Como 7 é próximo número não crivado, procederemos da mesma forma que das vezes anteriores.

~~1~~	2	3	~~4~~	~~5~~	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Observe que, se fizermos o mesmo procedimento partindo de 11 não eliminaríamos mais nenhum elemento da tabela, o mesmo vale para o 13 e o restante dos números na tabela. Como riscamos todos os números compostos da tabela, aqueles que não foram riscados são todos os primos até 100. São eles:

2	3	5	7	11
13	17	19	23	29
31	37	41	43	47
53	59	61	67	71
73	79	83	89	97

Por meio desse exemplo, pode-se observar alguns aspectos do crivo. Veja que, a partir de um dado momento, continuar fazendo o procedimento seria redundante, pois estaríamos riscando números já riscados. Outro aspecto é que, há alguns casos que um mesmo número é riscado mais de uma vez. Por exemplo, o número 30 é riscado três vezes, pois ele é múltiplo de $2, 3$ e 5.

Podemos dar uma explicação para nossa primeira observação. Seja m um inteiro da lista. Logo $m \leq n$. Veja que se m é composto, então $m = m_1 * m_2$. Seja $m_1 \leq m_2$. Dessa forma, temos ${m_1}^2 \leq m \iff m_1 \leq \sqrt{m}$, o que significa que existe um fator de m menor que $\sqrt{m}$. Dessa forma, temos $m_1 \leq \sqrt{m} \leq \sqrt{n}$, o que quer dizer que todo número composto da lista tem um fator menor ou igual a $\sqrt{n}$, logo não precisamos realizar o método para números maiores que $\sqrt{n}$, pois já teremos cortado todos os números compostos fazendo o procedimento até $\sqrt{n}$. No nosso exemplo, utilizamos $n = 100$, então bastava realizar o procedimento até 7, pois ele é o maior primo menor que 10.

Com relação a segunda observação, não há como evitar totalmente que alguns números sejam riscados mais de uma vez. No entanto, é possível melhorar o método para evitar alguns casos. Suponhamos que queremos riscar os números de p em p para algum primo p. É fácil ver que, os múltiplos de p que são múltiplos de primos menores que p já foram cortados da tabela. Ou seja, números da forma kp com $k \in \mathbb{Z}^+$, onde $k < p$, já terão

sido riscados, o que nos leva a concluir que podemos começar a crivar de p em p a partir de p^2. Por exemplo, no caso anterior onde $n = 100$, para crivar de 7 em 7 poderíamos começar a partir do 49 (7^2), pois todos os múltiplos de 7 menores que 49 já foram cortados anteriormente (com exceção do 7 é claro).

Por ser um método simples (mas eficaz) em determinar todos os números primos até um dado n (não muito grande), o Crivo de Eratóstenes, apesar de possuir mais de 2000 anos, ainda possui um valor extremamente importante na aprendizagem dos alunos de hoje em dia.

Ensinar sua técnica da forma como a qual apresentamos nesta dissertação pode ajudar o aluno a determinar se um dado número é primo ou não, podendo, assim, ajudá-lo na solução rápida e eficaz de um problema sem precisar ter que recorrer a tabelas ou a testes de primalidades mais complexos que só fazem sentido em um ambiente computacional.

Apresentaremos agora nosso modelo do Crivo de Eratóstenes utilizando o GeoGebra como plataforma.

5.1 O Crivo no GeoGebra

Vimos que, a técnica do crivo consiste em encontrar todos os primos menores que um dado n. Nossa modelagem do Crivo pode ser encontrada em: <https://ggbm.at/WhW4RveD>

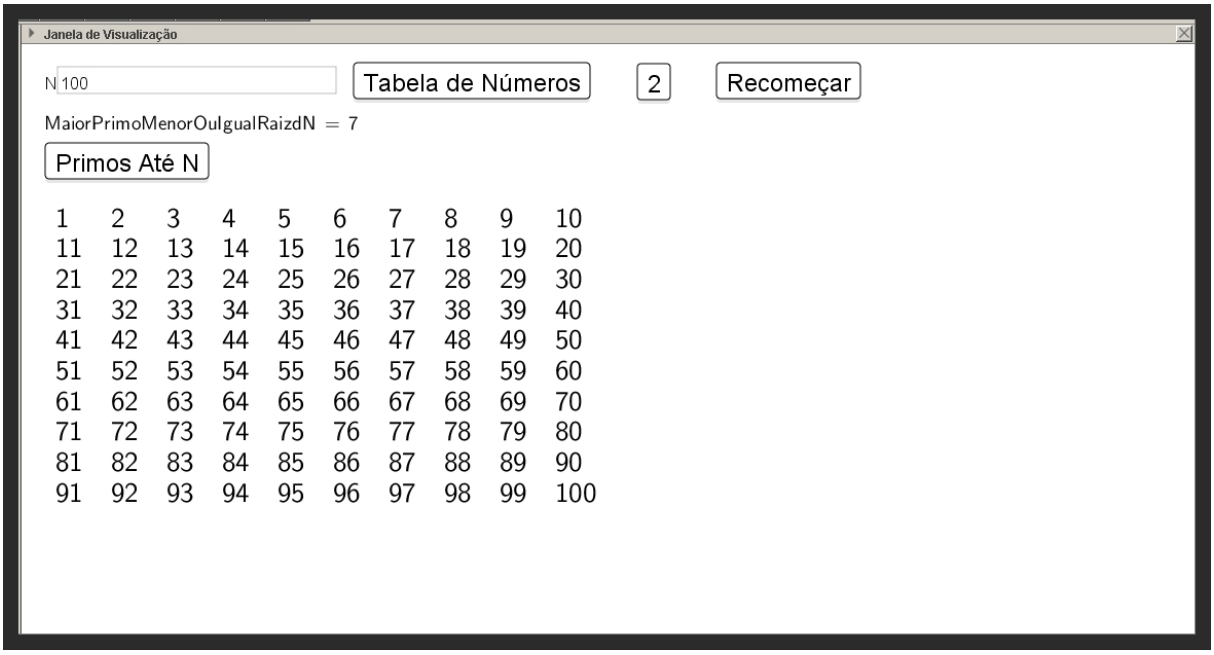
A figura a seguir mostra como é a tela do nosso modelo antes de começarmos a interagir com ele.

Figura 8 – Tela Incial do Crivo no GeoGebra

Fonte: Do Autor, 2017.

Veja que no campo de entrada N está inserido 25, isto é, $N = 25$. Para seguir adiante vamos trocar esse número por 100, para efeito de comparação com o exemplo que utilizamos, anteriormente, para mostrar como o método funciona. Após assinarmos 100 em N, clicaremos no botão *Tabela de Números*. Isso nos retornará uma tabela com os 100 primeiros números naturais e também fará com que o botão 2 apareça. Observe na próxima imagem.

Figura 9 – Botão *Tabela de Números*

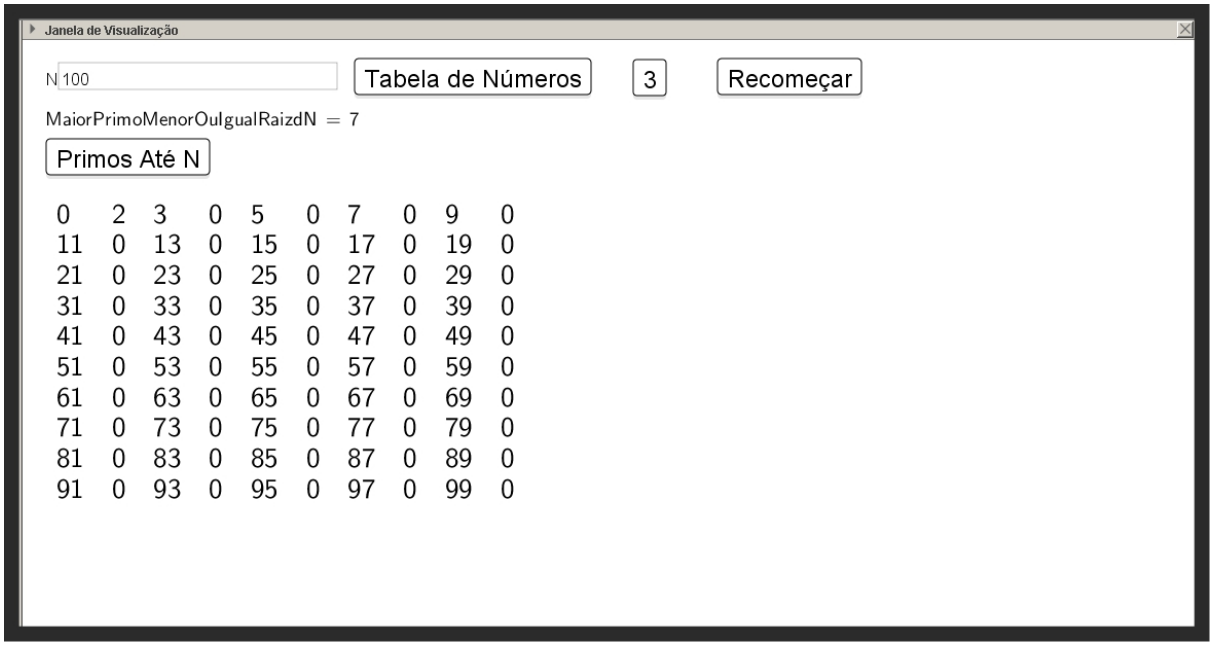


Fonte: Do Autor, 2017.

Talvez você deve ter percebido que temos uma variável chamada *MaiorPrimoMenorOuIgualRaizdN*, que representa, como seu próprio nome sugere, o maior inteiro menor ou igual à $n = \sqrt{N}$. Essa váriavel nos indica, como vimos antes, até qual valor devemos aplicar o método de crivar para que nossa tabela de números contenha apenas primos. Lembre-se que continuar a riscar utilizando primos maiores que $\sqrt{N}$ é totalmente desnecessário, pois já teríamos encontrado todos os primos menores N. Observe que, na tela inicial *MaiorPrimoMenorOuIgualRaizdN=5* e na imagem anterior *MaiorPrimoMenorOuIgualRaizdN=7*. O que faz total sentido, pois $\sqrt{N}$ vale 5 e 10, respectivamente.

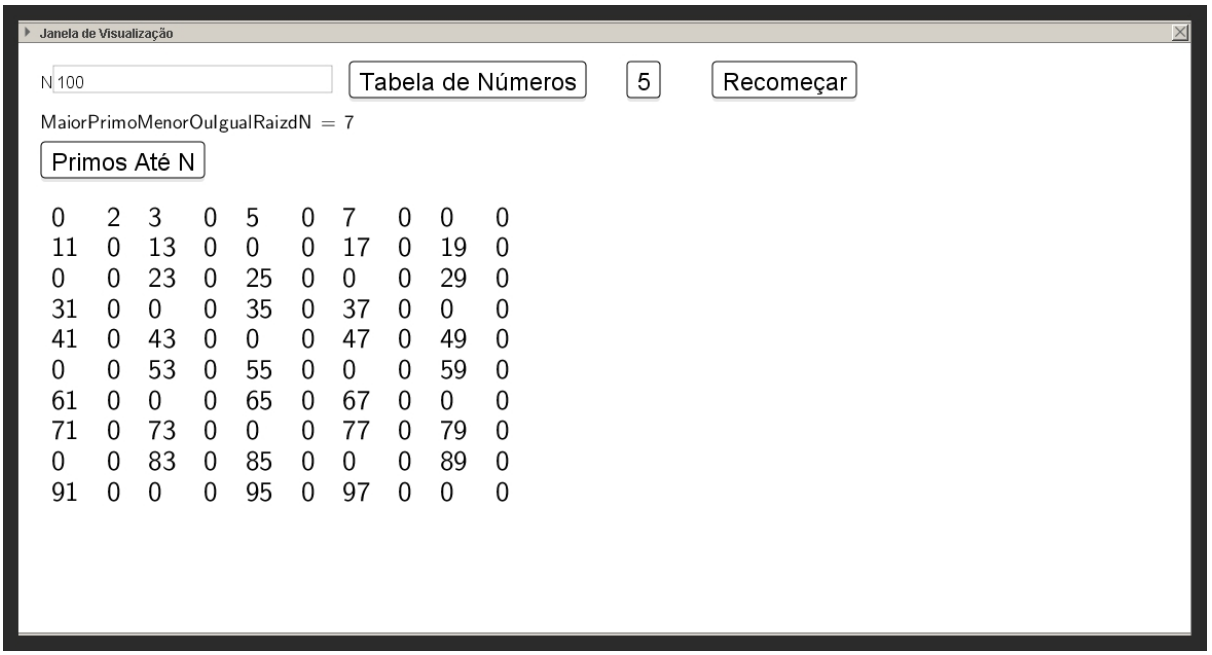
Sabemos assim que devemos prosseguir crivando até o primo 7. O que nos resta a fazer agora é clicar no botão 2, que irá eliminar todos múltiplos de 2 maiores que 2 da nossa tabela, retirando também, como bônus, o número 1. Após termos clicado nesse botão, ele dará lugar ao botão 3, que apertando-o irá retirar todos os múltiplos (menos o prório 3) restantes da tabela. Da mesma forma que antes, ele desaparecerá para dar lugar ao botão 5. Ao clicarmos no botão 5, o botão 7 aparecerá em seu lugar, e todos os números restantes que são divisíveis por 5 também terão desaparecido (a menos do próprio 5). Em fim, clicamos no botão 7 (que dará lugar para o botão 11) e com isso eleminaremos todos os múltiplos de 7 remanescentes das eliminações anteriores, e mais, nossa tabela agora está apenas constituida por números primos. Veja nas imagens asseguir:

Figura 10 – Botão *Primo 2*



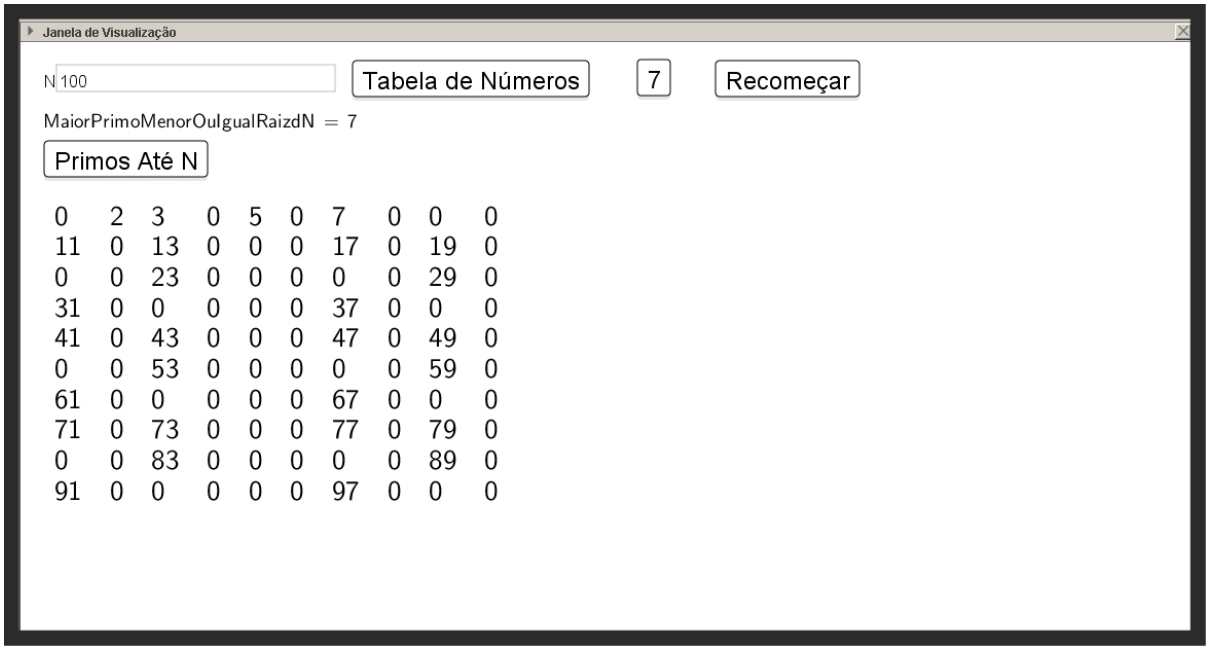
Fonte: Do Autor, 2017.

Figura 11 – Botão *Primo 3*



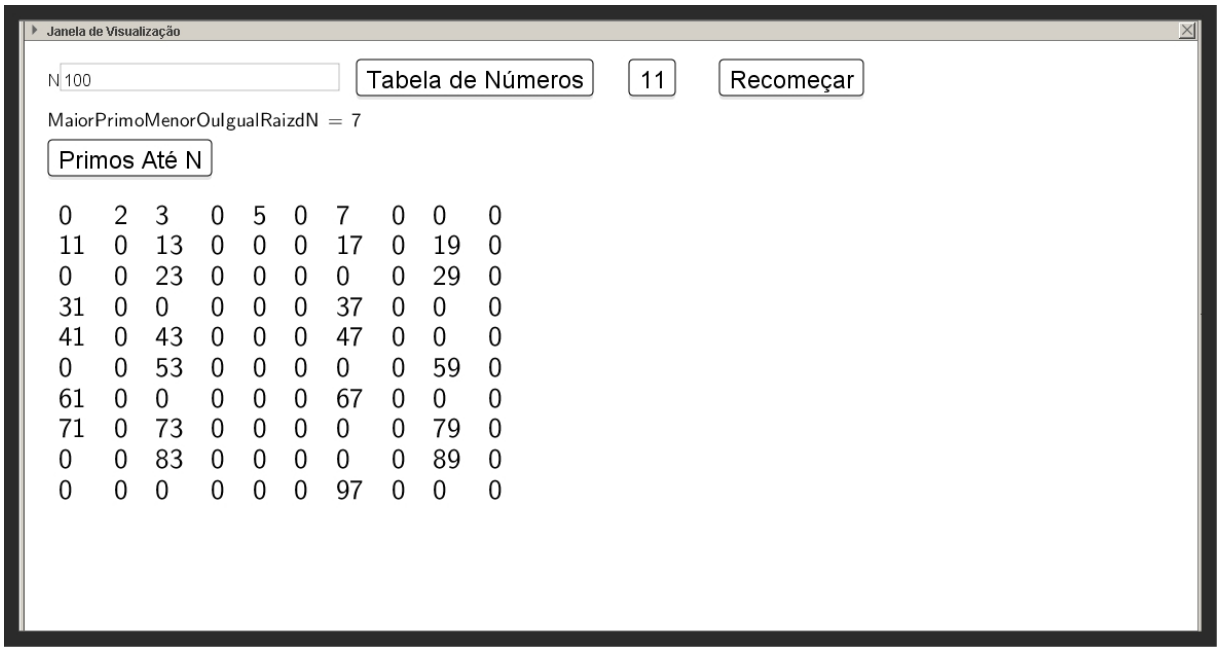
Fonte: Do Autor, 2017.

Figura 12 – Botão *Primo 5*



Fonte: Do Autor, 2017.

Figura 13 – Botão *Primo 7*



Fonte: Do Autor, 2017.

Agora se quisermos, podemos clicar no botão *Primos Até N* para gerar uma lista dos primos menores N, para uma melhor visualização ou para podermos conferir se nosso

modelo retorna realmente os mesmos números. Para voltarmos para tela inicial da nossa construção basta clicar em recomeçar.

Asseguir, apresentaremos um roterio para facilitara interação do aluno com o material construido.

1. No campo de entrada N, digite o número com o qual você quer determinar todos os números primos menores que ele. Obs: Não utilize números maiores que 900, pois o modelo não suporta ir mais longe.

2. Aperte o botão *Tabela de Números*.

3. Aperte nos botões com números primos que irão surgindo até você possuir apenas números primos em sua tabela.

4. Aperte o botão "Recomeçar"para reiniciar o modelo.

Pode ser interessante para os alunos, que na aula expositiva do método, omitir a parte que explica que não faz sentido aplicarmos o método para primos maiores que $\sqrt{n}$. Podemos através do material construido levar o aluno a perceber que após aplicarmos o método algumas vezes, a partir de certo ponto a tabela de números não muda mais, ou seja, todos aqueles números que sobraram nela são primos e portanto faz sentido em pensar qual é o número mínimo de vezes que devemos aplicar o método para que na tabela haja apenas números primos. Após levar o aluno a pensar sobre essa questão, poderíamos, então, explicar que é redundante aplicarmos o método utilizando primos maiores que $\sqrt{n}$. Sendo assim, a príncipio, torna-se interessante ocultarmos a variável "MaiorPrimoMenorOuIgualRaizdN".

Na seção que se segue, mostraremos como utilizamos os recursos do GeoGebra para construir nosso modelo do crivo.

5.2 Construindo o Crivo de Eratóstenes no GeoGebra

Primeiro, criamos um campo de entrada com variável N atrelada à ele. Em seguida, atribuimos

$$n = \sqrt{N}.$$

Criamos também uma variável binária I tal que se n for inteiro, então $I = -1$, caso contrário, $I = 0$.

O próximo passo foi construir a $lista1$. O código utilizado foi:

```
lista1=Sequência[k,k,1,(floor(n+1+I)^2)]
```

A *lista*1 gera valores consecutivos de 1 até `floor(n+1+I)^2`. Note que se n é inteiro então a *lista*1 possui valores que vão de 1 até N, agora se n não é inteiro a *lista*1 possui valores que vão de 1 até o menor quadrado perfeito maior que N. A *lista*2*a* foi criada para eliminar (mais especificamente zerar) os números maiores que N da lista1, que acontece somente quando n não for inteiro. Usei o seguinte código:

```
lista2a=Sequência[Se[Elemento[lista1, k] > N, 0, Elemento[lista1, k]],
k, 1, floor(n + 1 + I)^2]
```

Note que se n for inteiro a *lista*2*a* é igual à *lista*1.

Para transformar a *lista*2*a* em uma matriz quadrada, utilizamos o comando abaixo, criando assim a *lista*2*b* (que é uma matriz):

```
lista2b=Sequência[ParteDaLista[lista2a, floor(n + 1 + I) k + 1,
floor(n + 1 + I) (k + 1)], k, 0, floor(n) + I]
```

Veja que essa comando quebra a *lista*2*a* em n pedaços com n elementos em cada um, caso n seja inteiro e em $floor(n) + 1$ pedaços com $floor(n) + 1$ elementos cada um caso n não seja inteiro. Vale lembrar que, o comando $ParteDaLista[]$ cria uma lista particionando uma outra lista. Quando utilizamos listas como elementos do comando $Sequência[]$ geramos uma matriz no Geogebra, isto é, uma sequência de listas é uma matriz (para ser mais preciso uma lista cujos elementos são listas formam uma matriz). Assim o comando acima nos fornece uma matriz quadrada de ordem $floor(n) + 1 + I$.

Para transformarmos a matriz anterior em uma tabela utilizamos o seguinte código:
`texto5=TabelaDeTexto[lista2b]`

Essa tabela foi configurada para aparecer na posição (0,0). Criamos uma variável c, tal que, se ela for igual a 1 então essa tabela estará aparecendo, caso contrário, ela não aparecerá.

Em seguida, construimos um botão chamado $TabeladeNúmeros$. Em sua programação, temos: $b = 1$ e $c = 1$. Isto é, toda vez que clicarmos neste botão faremos que b e c sejam 1. Sabemos que, se $c = 1$, então a tabela *texto*5 aparecerá.

Neste momento, começamos a criar os botões que aplicarão o crivo de Eratóstenes na matriz *lista*2*b*. Foram criados 25 botões, um para cada primo menor que 100.

A condição para o botão 2 aparacer é $b = 1$, ou seja, quando apertarmos o botão Tabela de Números, o botão 2 aparecerá. Na programação do botão 2, foram inseridos, os seguintes comandos:

```
A2=Sequência[Se[Resto[Elemento[lista2a, k], 2] == 0, 0, Elemento[lista2a, k]],
k, 1, floor(n + 1 + I)^2]
```

```
a2=Sequência[Se[Elemento[lista2a,k]==2,2,0],k,1,floor(n + 1 + I)^2]
```

```
a1=Sequência[Se[Elemento[lista2a,k]==1,-1,0],k,1,floor(n + 1 + I)^2]

listap2=A2+a2+a1

lista4=Sequência[ParteDaLista[listap2, floor(n + 1 + I) k + 1,
floor(n + 1 + I) (k + 1)], k, 0, floor(n) + I]

TabelaPrimos=TabelaDeTexto[lista4]

b=2
c=0
e=1
```

A lista $A2$ do comando acima é a fundamento do método do crivo de Eratóstenes. Ela é um vetor de mesmo tamanho da $lista2a$, isto é, de $floor(n+1+I)^2$, de tal forma que se o elemento correspondente (em termos de posição) da $lista2a$ é divisivel por 2 então ela zera o mesmo, se não o elemento permace igual ao respectivo da $lista2a$. Contudo, nesse processo nós zeramos o elemento 2 também, pois 2 é divisivel por 2, mas 2 é primo e precisamos que ele fique no vetor.

A lista $a2$ é justamente o código que utilizamos para repor o 2 no vetor. Esse código nada mais é que um vetor com o número 2 na posição dois com os demais elementos nulos. A lista $a1$ foi criada para tirar o número 1 de nosso vetor, pois ele não é primo. Assim como na lista $a2$, a lista $a1$ representa um vetor cujo primeiro elemento é 1 e os demais são zero.

Assim somando as três listas mencionadas acima ($A2$, $a2$, $a1$) criamos a $listap2$ que representa um vetor em que se foi crivado (zerado) todos os múltiplos de 2 maiores que 2.

Mas queremos uma matriz e não um vetor (para facilitar a visualização do método), e é isso que a $lista4$ representa. Da mesma forma que construímos a matriz $lista2a$, construímos a $lista4$, ou seja, pegamos a $listap2$ $(A2 + a2 + a2)$ e quebramos ela em $floor(n) + 1 + I$ pedaços com $floor(n) + 1 + I$ elementos cada um. Assim obtemos nossa matriz que com o comando $TabelaDeTexto[lista4]$ criamos uma tabela a partir da $lista4$ que chamamos de $TabelaPrimos$.

Dessa forma, quando apertarmos o botão 2, além de executar esse comando criando todas essas listas e por fim gerando a $TabelaPrimos$, b será 2 (fazendo com que o botão 2 desapareça), c será 0 (escondendo assim a tabela $texto5$, que representa a tabela de todos os números variando de 1 a N)e e será igual à 1.

Essa $TabelaPrimos$, eu a configurei para aparecer quando $e = 1$, ou seja quando eu apertar o botão 2 ela aparecerá na janela de visualização do Geogebra.

A condição do botão 3 aparecer é que $b = 2$. Então assim que eu apertar o botão 2, este sumirá enquanto aquele aparecerá.

O botão "3"como os demais, eu os configurei de maneira análoga ao botão "2". Veja Abaixo:

```
A3=Sequência[Se[Resto[Elemento[listap2, k], 3] == 0, 0, Elemento[lista2a, k]],
k, 1,floor(n + 1 + I)^2]

a3=Sequência[Se[Elemento[lista2a,k]==3,3,0],k,1,floor(n + 1 + I)^2]

listap3=A3+a3

lista4=Sequência[ParteDaLista[listap3, floor(n + 1 + I) k + 1,
floor(n + 1 + I) (k + 1)], k, 0, floor(n) + I]

TabelaPrimos=TabelaDeTexto[lista4]

b=3
```

Você pode notar que assim como no botão 2, $A3$ é uma lista com todos os elementos da $listap2$ (e não da $lista2a$ como foi no caso de $A2$ do botão 2) exceto os múltiplos de 3.

A lista $a3$ é uma lista que possui o elemento 3 na terceira posição e os demais são nulos. Ela é o método de reposição do primo 3 no nosso vetor.

A $listap3$ nos retorna nosso vetor atualizado, isto é, com todos os números da $listap2$ exceto os múltiplos de 3 (diferente do 3, é claro).

Após isso, substituimos em $lista4$, onde estava escrito $lista2p$, por $listap3$, para atualizarmos nossa matriz (lista4) e por conseguinte nossa tabela ($TabelaPrimos$).

No final definimos $b = 3$, que será a condição para o botão 5 aparecer na janela de visualização. Seguimos fazendo o mesmo processo com todos primos até o botão 97. Ou seja, pegamos o vetor em sua forma atualizada e aplicamos na fórmula, gerando um novo vetor que será aplicado na fórmula do primo seguinte, ao final definimos b com uma unidade a mais que a anterior, pois essa será a condição do próximo primo (botão) aparecer.

Vimos na seção anterior que, a função variável $MaiorPrimoMenorOuIgualRaizdN$ é mostrar até qual primo devemos clicar para que o método do crivo tenha se completado, isto é, até qual botão precisamos apertar para termos apenas elementos primos na tabela gerada. Foi utilizado o seguinte código para defini-la:

```
MaiorPrimoMenorOuIgualRaizdN=PrimoAnterior[floor(n + 1)]
```

Para criarmos a lista $PrimosAteN$, nós utilizamos o seguinte comando:

```
PrimosAteN=ElementosÚnicos[Sequência[PróximoPrimo[k],
k,1,PrimoAnterior[PrimoAnterior[N + 1]]]]
```

Para ententermos como esse comando procede analizaremos primeiro o seguinte comando:

```
Sequência[PróximoPrimo[k],k,1,PrimoAnterior[PrimoAnterior[N + 1]]]
```

Cada elemento da sequência anterior representa o menor primo maior que k para cada k entre 1 e o primo anterior do primo anterior de $N + 1$. Por exemplo, se $N = 11$ então *PrimoAnterior[PrimoAnterior[12]]=7*, dessa forma, temos que a sequência anterior retorna {2,3,5,5,7,7,11}. Assim, quando aplicamos o comando *ElementosÚnicos* no nosso exemplo, obtemos {2,3,5,7,11}, que são todos os primos até $N = 11$ (observe que utilizamos na fórmula $N + 1$ justamente para ela funcionar nos casos em que N é primo).

A condição para a lista *PrimosAteN*aparecer na Janela de Visualização é $f == 1$. A função do botão *Primos Até N* é justamente fazer essa lista aprecer na Janela de Visualização. Sua codificação consiste em apenas $f = 1$, ou seja, sempre que apertarmos ele, f será 1 e portanto a lista *PrimosAteN* aparecerá.

O botão *Recomeçar* que é utilizado para deixar a tela limpa e aliviar a memória do algoritmo. Nesse botão temos o seguinte código:

$b = 0$	$c = 0$	$e = 0$	$f = 0$	$N = 25$
$lista4 = \{\}$ $listap97 = \{\}$ $A97 = \{\}$ $a97 = \{\}$	$listap89 = \{\}$ $A89 = \{\}$ $a89 = \{\}$	$listap83 = \{\}$ $A83 = \{\}$ $a83 = \{\}$	$listap79 = \{\}$ $A79 = \{\}$ $a79 = \{\}$	$listap71 = \{\}$ $A71 = \{\}$ $a71 = \{\}$
$listap71 = \{\}$ $A71 = \{\}$ $a71 = \{\}$	$listap67 = \{\}$ $A67 = \{\}$ $a67 = \{\}$	$listap61 = \{\}$ $A61 = \{\}$ $a61 = \{\}$	$listap59 = \{\}$ $A59 = \{\}$ $a59 = \{\}$	$listap53 = \{\}$ $A53 = \{\}$ $a53 = \{\}$
$listap47 = \{\}$ $A47 = \{\}$ $a47 = \{\}$	$listap43 = \{\}$ $A43 = \{\}$ $a43 = \{\}$	$listap41 = \{\}$ $A41 = \{\}$ $a41 = \{\}$	$listap37 = \{\}$ $A37 = \{\}$ $a37 = \{\}$	$listap31 = \{\}$ $A31 = \{\}$ $a31 = \{\}$
$listap29 = \{\}$ $A29 = \{\}$ $a29 = \{\}$	$listap23 = \{\}$ $A23 = \{\}$ $a23 = \{\}$	$listap19 = \{\}$ $A19 = \{\}$ $a19 = \{\}$	$listap17 = \{\}$ $A17 = \{\}$ $a17 = \{\}$	$listap13 = \{\}$ $A13 = \{\}$ $a13 = \{\}$
$listap11 = \{\}$ $A11 = \{\}$ $a11 = \{\}$	$listap7 = \{\}$ $A7 = \{\}$ $a7 = \{\}$	$listap5 = \{\}$ $A5 = \{\}$ $a5 = \{\}$	$listap3 = \{\}$ $A3 = \{\}$ $a3 = \{\}$	$listap2 = \{\}$ $A2 = \{\}$ $a2 = \{\}$ $a1 = \{\}$

Podemos ver que o Botão *Recomeçar* "apaga"todas as listas criadas com exceção, das: lista1, lista2a e lista2b. Na verdade o que acontece é que nós as tornamos vazias.

O motivo para isso é devido justamente a questão de memória. Se eu nao às "apagasse", quando nós mudassemos o valor de N elas seriam todas recalculadas o que algumas vezes levava o programa a travar, ou dar um erro irreversível.

Além das listas serem apagadas, nos definimos $b = 0$ (escondendo assim todos os botões de primos), $c = 0$ (que esconderá nossa tabela inicial, texto5, aquela que contém todos os números naturais de 1 até N), $e = 0$ (escondendo a TabelaPrimos, usada para mostar o processo crivo quando apertamos os botões de primos), $f = 0$ (ocultando a lista $PrimoAteN$) e $N = 25$ (para voltarmos ao nosso N de início).

Cabe ressaltar que, durante a construção do modelo, não conseguimos um método que salvasse todas as informações que precisávamos em uma mesma lista, isto é, aplicar o método do crivo em uma lista e salvar o resultado nela mesma. Por isso, para cada aplicação do crivo, tínhamos que criar novas listas para salvar o resultado obtido, listas estas que dependiam das anteriores para existir e que seriam necessárias para as listas seguintes. Assim, à medida que vamos aplicando a técnica vamos gerando mais e mais listas, o que é previsível que em algum momento sobrecarregasse a capacidade do $software$ calcular e achar as mesmas.

Todas as listas e matrizes foram criadas na Janela CAS. Mas isso não ocorreu desde o príncipio, pois originalmente elas foram criadas na Janela Álgebra. Só que o modelo dava erro para calcular valores próximos de $N = 900$, à medida que íamos crivando. Após mudarmos as listas para o ambiente CAS, observamos um melhora de desempenho, pois fomos bem sucedidos para valores próximos à $N = 1089$.

Nós observamos que o problema consiste, que na busca por mais mémoria (mais espaço), o GeoGebra para salvar um nova lista, e não encontrando espaço, ele apaga uma lista anterior (talvez de modo aleatório), o que leva nosso sistema a colapso, pois nossas listas são dependentes umas das outras.

Veja que a ordem para se apagar as listas é importante nesse caso, pois como já sabemos, as listas de um primo são dependentes das listas dos primos anteriores à ele, o que pode levar a um erro se apagarmos uma lista que determina uma outra. Por isso que o comando apaga as últimas listas criadas primeiro ate chegar nas listas mais antigas (ou criadas a mais tempo).

CONSIDERAÇÕES FINAIS

Com base nos PCNEM (FILHO; MAIA, 2000), vimos nesta dissertação, as competências as quais o Ensino Médio deve desenvolver no aluno para que este seja capaz de se inserir e intervir efetivamente em sua sociedade. Muito mais do que a mera preparação para a atividade produtiva, esse nível de ensino deve contribuir, também, para formação humana do indivíduo, além de fornecer as ferramentas necessárias tanto para a constante aprendizagem, como também, para a continuação dos estudos em níveis mais avançados. Sob essa perspectiva de educação, busca-se uma formação ética, assim como, o desenvolvimento do pensamento autônomo e crítico que são essenciais para a constituição da cidadania.

Observamos também, o papel fundamental que a interdisciplinaridade e a contextualização possuem nesse processo educativo.

A primeira refere-se a questão que o conhecimento não deve ser segmentado, compartimentado, divido em diferentes áreas sem que haja o estabelecimento de suas devidas ligações e conexões. Um objeto de estudo pode ser analisado por diferentes áreas do conhecimento, e utilizar de diversas perspectivas para complementar o estudo de um saber é essencial para a sedimentação de tal conhecimento.

A segunda trata-se da importância de aproximar os conteúdos ministrados dentro da sala de aula com questões reais abrangidas por eles fora dela. Tal relevância se dá em função que, desta forma, o processo de ensino-aprendizagem se torna significativo para aluno, não só despertando um maior interesse em aprender, como também, permitindo o aluno a identificar, utilizar e aplicar seus conhecimentos em seu cotidiano.

A Matemática possui um contribuição de peso nessa busca por uma formação do aluno em sentido mais amplo. Aprendê-la não só muni a pessoa com ferramentas que poderão ser uteis em seu cotidiano e em sua atividade profissional, como também, ajuda no desenvolvimento de uma melhor abstração e na estruturação do pensamento e do raciocínio dedutivo. Com tais ferramentas o individuo é capaz de ler e interpretar a realidade de forma crítica, podendo assim, intervir nela com criatividade.

Com o intuito de tornar a aprendizagem por parte dos alunos (do Ensino Médio) mais significativa, especificamente, sobre números primos, nos propusemos a elaborar um material que pudesse auxiliar e enriquecer seu ensino. Essa proposta consistiu em modelar a técnica de Criptografia RSA e o Crivo de Eratóstenes utilizando a aplicação GeoGebra para que eles pudessem ser utilizados em sala de aula, tanto para, sedimentar seus conceitos quanto para dar sentido a sua aprendizagem.

Lembramos que os números primos possuem um papel chave no modelo de Criptografia RSA para garantir a segurança da informação encriptada. O Crivo de Eratóstenes, por

sua vez, é uma interessante técnica para encontrar números primos até um dado n, que é de simples entendimento e execução. Por essas razões, acreditamos que trabalhando com seus conceitos em sala de aula contribui para os objetivos dessa dissertação.

Apesar de algumas dificuldades principalmente inerentes as limitações do *software* GeoGebra (toda aplicação tem a sua limitação), conseguimos construir o material. Bem verdade, não da forma com que se pensava inicialmente.

Recordamos, também, que o modelo construído simula o processo de Criptografia RSA, a exceção da divisão da informação em blocos. Assim, tomando dois números primos, inicialmente, obtemos a partir deles chaves (uma Pública e uma Privada) que serão utilizadas na codificação e descodificação da mensagem.

A partir de um dado inteiro positivo N, conseguimos determinar quais são os números primos menores que tal número com o nosso modelo do Crivo. Determinando N, geramos uma tabela composta por números de 1 a N que após sucessivas aplicações do método do Crivo tal tabela será composta por números primos e por zeros (que em nosso modelo representa os números da tabela que foram crivados, isto é, que são compostos).

Cabe aqui dizermos alguns aspectos dos modelos criados que podem ser melhorados. Talvez a principal modificação necessária na modelagem RSA feita seria acrescentar um algoritmo para poder dividir a mensagem em blocos. Lembramos que esse processo é necessário para evitar que o método seja quebrado por contagem de frequência. No entanto, devemos lembrar que essa organização em blocos demanda que a conversão de caracteres para inteiros leve a números com o mesmo número de algarismos, o que o observamos que o GeoGebra não faz. Contudo, podemos dar um jeito para que isso ocorra. Antes de dividir a informação em blocos, utilizamos o comando *TextoParaUnicode[mensagem]* e depois adicionamos 100 a cada valor inteiro obtido, dessa maneira, acreditamos que todos os valores possuirão três algarismos. No processo reverso de conversão de números inteiros para caracteres, após a eliminação dos blocos, deveremos subtrair 100 de cada valor obtido e depois utilizar o comando *UnicodeParatexto[vetor]* para retornar a mensagem original.

Ainda sobre a modelagem RSA, podemos apresentar o material de uma outra forma. Ao invés de utilizarmos controles deslizantes para assinar nossos números primos p e q e também nosso número e poderíamos utilizar caixas de entrada. Nossa escolha por controles deslizantes se deu para que os alunos se familiarizassem e interagissem com essa ferramenta do GeoGebra e também pois para mostrar que o método funciona não precisaríamos utilizar primos muito grandes, além de forçar a escolha de números inteiros. Com as caixas de entradas porém você pode oferecer uma maior liberdade de escolha para seus primos e para o inteiro e, pois lembramos que os controles foram construídos variando de 1 a 100 com incremento de uma unidade. Além disso, com as caixas de entrada, será possível determinar o quão grandes poderão ser tomados nossos primos de tal forma que nosso modelo ainda seja capaz de criptografar e descriptografar uma mensagem.

Você também pode criar um novo campo de entrada para o vetor que será descodificado.

Dessa forma, os alunos ao escolherem seus números primos poderão criar chaves públicas e secretas e trocar mensagens secretas que só poderão ser lidas por aqueles que eles quiserem. Por exemplo, suponha que o aluno A queira enviar uma mensagem secreta para o aluno B, o aluno B então pela escolha de seu par de primos criará uma chave pública (o par d,n) e uma secreta (o par e,n). Ele passará a chave pública para quem quiser enviar uma mensagem secreta a ele, no nosso caso o aluno A. Dessa forma, o aluno A pegará a chave pública feita por B e encriptará sua mensagem e enviará para B. O aluno B em posse do vetor encriptado e de sua chave secreta conseguirá ler e entender a mensagem que A o enviou. Da mesma forma, se B quiser enviar uma mensagem secreta para A, A deverá compartilhar sua chave pública com B para que ele seja capaz de encriptar uma mensagem que só será possível desencriptá-la com a chave secreta de A.

Com relação à modelagem de Crivo de Eratóstenes, acreditamos que seu maior defeito é que ele exige muita memória para aplicar seu algoritmo para números não tão pequenos, isso em função da grande quantidade listas criadas em seu processo. Não descobrimos um jeito de trabalhar com uma única lista, isto é, continuar atualizando ela sem que desse algum erro, pois os métodos que utilizávamos nos levava a uma estrutura circular, e portanto a um erro. Deixamos esse desafio para a comunidade. Talvez possa até ser de simples solução, mas com os conhecimentos que temos em relação ao GeoGebra, não fomos capazes de resolver.

Outra melhoria que poderia ser feita seria utilizar um procedimento que aplicasse o método do crivo para todo o primo que se quisesse. Lembre-se que na modelagem, construímos 25 botões, um para cada primo menor que 100, que se apertados eliminarão da tabela todos seus múltiplos. Claro que se não tivéssemos um problema de memória, com esse atual modelo, encontraríamos todos os primos menores que 10201, que é o quadrado do número 101, que por sua vez é primo subsequente do primo 97 que consiste no último botão primo criado. Dessa forma, o método não eliminaria os números cujos fatores fossem primos (ou múltiplos de primos) maiores que 97. Por exemplo, após utilizarmos todos os botões não conseguiríamos riscar da tabela o número $10201 = 101^2$ e nem o número $1071509 = 101 * 103^2$.

Numa sociedade tecnológica e informacional, marcada pela contínua superação e renovação de saberes e competências, o papel do professor no processo educativo do aluno torna-se ainda mais determinante. O professor tem que ser capaz de não só congregar o conteúdo ministrado com outras áreas de conhecimento, como também, de aproximar a realidade do aluno com aquilo que é trabalhado na escola. Dessa forma, o educador precisa ter uma sensibilidade em relação a seus alunos, para que ele consiga identificar as aptidões e conhecimentos já adquiridos por seus alunos, e por conseguinte, adotar estratégias mais eficazes para estimular o desenvolvimento dessas competências como também surgimento de novas, pois elas serão essenciais para que os alunos consigam se inserir em sua sociedade. Contudo, para que isso aconteça, o professor também deverá

estar em um processo contínuo de aperfeiçoamento, isto é, sempre buscando se atualizar.

Ressaltamos a importância do professor na elaboração de novos materiais e projetos que possam ser utilizados com seus alunos. Tal iniciativa não só contribui para formação dos alunos como também para a do professor. A busca por estratégias e conhecimentos para se construir uma ferramenta de ensino engrandece sua prática profissional e também contribui para o desenvolvimento de suas competências.

Assim, acreditamos que as tecnologias podem ser instrumentos de peso na construção desses materiais. Não pelo mero teor apelativo inerente a elas, mas também, pelo caráter formativo e interativo que elas podem adicionar ao processo de ensino, além aproximar a teoria com a realidade.

Lembramos a proposta da presente dissertação foi apresentar um material que pudesse ser introduzido a alunos do Ensino Médio com o intuito de enriquecer e dar maior significado a aprendizagem de números primos, e portanto não constituiu objetivo a aplicação desse material neste momento. Dessa forma, uma oportunidade para projetos futuros seria a aplicação em sala de aula das ferramentas criadas neste trabalho e a sequente análise de suas repercussões.

Referências

CARVALHO, A. P. de. ***Caracterização dos Números Primos e Aplicações no Ensino Básico***. Dissertação (Mestrado) — UFPI/Teresina, 2015.

COUTINHO, S. C. ***Criptografia***. 2009. Online; acessado em 28-Fevereiro-2017. Disponível em: <https://www.passeidireto.com/arquivo/2281703/numeros-inteiros-e-criptografia-rsa---s-c-coutinho>.

FARIAS, D. G. de. ***O Estudo do Ensino de Números Primos na Educação Básica***. Dissertação (Mestrado) — UFAL/Maceió, 2016.

FILHO, R. L. B.; MAIA, E. M. ***Parâmetros Curriculares Nacionais Ensino Médio***. [S.l.], 2000. Online; acessado em 20-Agosto-2017. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/blegais.pdf>.

FILHO, R. L. B.; MAIA, E. M.; PEREIRA, A. R. S. ***Parâmetros Curriculares Nacionais Ensino Médio***. [S.l.], 2000. Online; acessado em 22-Agosto-2017. Disponível em: <http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf>.

GEOGEBRA. ***O que é o GeoGebra?*** Online; acessado em 10-Agosto-2017. Disponível em: <https://www.geogebra.org/about>.

GEOGEBRA. ***Manual***. 2017. Online; acessado em 10-Agosto-2017. Disponível em: <https://wiki.geogebra.org/pt/Manual>.

MACHADO, E. R. ***Números Primos Uma Abordagem Educacional***. Dissertação (Mestrado) — UFAM/Manaus, 2015.

MARTINEZ, F.; MOREIRA, C. G.; SALDANHA, N. ***Tópicos de Teoria dos Números***. 1ª. ed. Rio de Janeiro: SBM, 2012.

MARTINEZ, F. et al. ***Teoria dos Números um passeio com primos e outros números familiares pelo mundo inteiro***. 4ª. ed. Rio de Janeiro: IMPA, 2015.

MELO, R. P. de. ***Números Primos****: História, Tópicos, Criptografia e o Ensino da Matemática*. Dissertação (Mestrado) — UECE/Ceará, 2014.

MORIMOTO, R. M. ***Números Primos****: Propriedades, Aplicações e Avanços*. Dissertação (Mestrado) — UNESP/Rio Claro, 2014.

NETO, A. S. da S. ***Criptografia Online***. Dissertação (Mestrado) — UFTM/Uberaba, 2015.

SOUZA, A. N. L. ***Criptografia de Chave Pública, Criptografia RSA***. Dissertação (Mestrado) — UNESP/Rio Claro, 2013.

VIANA, E. ***Criptografia****: Conceito e aplicações*. 2017. Online; acessado em 15-Março-2017. Disponível em: <https://www.devmedia.com.br/criptografia-conceito-e-aplicacoes-revista-easy-net-magazine-27/26761>.