UNIVERSIDADE ESTADUAL DO CEARÁ

PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA

CENTRO DE CIÊNCIAS E TECNOLOGIA

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

JOSÉ CARLOS DE SALES FARIAS

ALGORITMOS MATEMÁTICOS NA EDUCAÇÃO BÁSICA

FORTALEZA – CEARÁ
2015

JOSÉ CARLOS DE SALES FARIAS

ALGORITMOS MATEMÁTICOS NA EDUCAÇÃO BÁSICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.

Orientador: Prof. Dr. Alberto Flávio Alves Aguiar

FORTALEZA – CEARÁ
2015

Dados Internacionais de Catalogação na Publicação

Universidade Estadual do Ceará

Sistema de Bibliotecas

Farias, José Carlos de Sales.
Algoritmos matemáticos na educação básica [recurso eletrônico] / José Carlos de Sales Farias. - 2015.
1 CD-ROM: il.; 4 ¾ pol.

CD-ROM contendo o arquivo no formato PDF do trabalho acadêmico com 91 folhas, acondicionado em caixa de DVD Slim (19 x 14 cm x 7 mm).

Dissertação (mestrado profissional) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Mestrado Profissional em Matemática em Rede Nacional, Fortaleza, 2015.
Área de concentração: Matemática.
Orientação: Prof. Dr. Alberto Flávio Alves Aguiar.

1. Algoritmos. 2. Tecnologia. 3. Ensino da Matemática. 4. Conhecimento matemático. I. Título.

JOSÉ CARLOS DE SALES FARIAS

ALGORITMOS MATEMÁTICOS NA EDUCAÇÃO BÁSICA

Dissertação apresentada ao curso de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial para obtenção do titulo de Mestre em Matemática.
Área de Concentração: Matemática.

Aprovada em: 18 de novembro de 2015.

BANCA EXAMINADORA

Prof. Dr. Alberto Flávio Alves Aguiar (Orientador)
Universidade Estadual do Ceará – UECE

Prof. Dr. João Montenegro de Miranda
Universidade Estadual do Ceará – UECE

Prof. Dr. José Othon Dantas Lopes
Universidade Federal do Ceará – UFC

Ao meu filho Hugo e esposa Marcela por tudo o que eles representam.

AGRADECIMENTOS

Agradeço primeiramente a Deus, por iluminar meus caminhos e permitir mais essa conquista em minha vida.

A minha esposa Marcela e ao meu filho Hugo pelo apoio e paciência que tiveram ao longo dessa jornada.

Aos meus pais, José Farias e Maria Eunice que desde o início de minha vida sempre tiveram ao meu lado dando força para vencer todas as dificuldades.

Aos meus colegas de trabalho: Helder, Franzé, Marquinhos e Tereza, por compreenderem a necessidade de algumas ausências na escola.

Ao meu orientador Prof. Alberto Flávio por ter sido sempre muito atencioso e pelas oportunas contribuições acrescentadas ao trabalho.

Aos colegas do curso PROFMAT por estarmos sempre juntos compartilhando as angústias e vitórias.

Aos professores do PROFMAT – UECE pelo comprometimento e dedicação para com todos nós alunos.

Ao empenho do professor coordenador Guilhermy Ellery que não mediu esforços para o sucesso de todos que fazem o PROFMAT – UECE.

Ao apoio financeiro da CAPES que possibilitou um melhor êxito na realização das atividades do curso.

E por fim a todos os idealizadores do PROFMAT, um programa que proporciona ao professor de matemática um progresso na sua vida acadêmica e, por conseguinte uma melhoria no ensino de matemática do país.

"Se as pessoas não acham a Matemática simples é só porque ainda não perceberam o quanto a vida é complicada"

(John von Neumann)

RESUMO

Este trabalho aborda alguns algoritmos matemáticos estudados principalmente na Educação Básica, enfatizando sua criação e desenvolvimento ao longo da história, dando destaque ainda sua importância para o conhecimento matemático no mundo atual. Observa-se com os resultados das avaliações externas que um grande número de educandos ao concluir o Ensino Médio não têm o conhecimento matemático condizente com esta etapa de ensino. Para que o ensino da Matemática confira ao aluno uma compreensão sólida e significativa é necessário um melhor entendimento dos algoritmos matemáticos aos quais ele foi exposto, fazendo sempre que possível uma conexão da Matemática com o avanço da tecnologia que está onipresente em nosso cotidiano. Portanto, realizamos uma pesquisa bibliográfica com enfoque em algoritmos matemáticos amplamente utilizados no ensino Fundamental e Médio bem como sua importância no cotidiano.

Palavras chave: Algoritmos, Tecnologia, Ensino da Matemática, Conhecimento matemático.

ABSTRACT

This thesis addresses some mathematical algorithms largely studied in the Basic Education System, emphasizing their development throughout the centuries and highlighting the importance of the mathematical knowledge in the modern world. It is observed from the results of external assessments that a large number of students does not have the mathematical proficiency that they should have gotten in Secondary Education as they conclude this level of their studies. In order that the Mathematics teaching grants the students a more appropriate and meaningful understanding it is required a better understanding of the Mathematics embedded in the algorithms which they were exposed making, wherever possible, a connection with the advancement of technology that is ubiquitous in our daily lives. Therefore, we conducted a bibliographical search focused on mathematical algorithms frequently used in Primary and Secondary schools, as well as their presence and importance around all of us.

Key words: Algorithms, Technology, Teaching of Mathematics, Mathematical Knowledge

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1. INTRODUÇÃO

A importância da matemática está visivelmente destacada no trecho abaixo da coletânea de artigos publicados pelo MEC em 2004 “Explorando o ensino da Matemática”:

> A matemática está presente na vida cotidiana de todo cidadão, por vezes de forma explícita e por vezes de forma sutil. No momento em que abrimos os olhos pela manhã e olhamos a hora no despertador, estamos “lendo” na linguagem matemática, exercitando nossa abstração e utilizando conhecimentos matemáticos que a humanidade levou séculos para construir. ([10], p. 3)

As pessoas convivem diariamente com a linguagem matemática, seja no simples ato de verificar a hora ou em situações que exigem conhecimentos mais “profundos”. Por exemplo, decidir qual investimento de um capital é mais vantajoso diante das inúmeras possibilidades e prazos, analisar os diversos financiamentos na compra de um bem, desenvolver um algoritmo computacional para solução de um problema, enfim, vivemos cercados por situações que levam ao uso de recursos e a raciocínios matemáticos. Por exemplo, quando fazemos uma viagem de avião ou mesmo a simples consulta do GPS do celular para escolher a melhor rota a tomar, sem que percebamos, estamos fazendo uso de vasto conhecimento matemático para realizar estas tarefas.

Conforme CHEVALLARD, BOSCH e GÁSCON (2001):

> A matemática está presente em várias situações do cotidiano de todos nós. Ela é necessária para resolver muitos problemas, grandes ou pequenos, que surgem nessas situações. Sendo assim, cada sujeito precisa de uma educação matemática básica, que lhe possibilite “viver bem e ajudar os outros a viver bem” ([8], p. 35).

É imprescindível que o ensino da Matemática nas escolas seja feito de forma eficiente e eficaz, proporcionando ao aluno uma aprendizagem satisfatória em cada série do currículo. Contudo, é possível verificar em dados de avaliações externas como PISA e ENEM que os alunos já apresentam deficiências no aprendizado da Matemática na Educação Básica.

O PISA (Programa Internacional de Avaliação de Alunos) busca medir o conhecimento e a habilidade em leitura, matemática e ciências de estudantes com 15 anos de idade, tanto de países membros da OCDE (Organização para Cooperação e Desenvolvimento Econômico) como de países parceiros. [23]

Figuram entre os países membros da OCDE: Alemanha, Grécia, Chile, Coreia do Sul, México, Holanda e Polônia. Países como Argentina, Brasil, China, Peru, Qatar e Sérvia aparecem como parceiros e também fazem parte da avaliação. A avaliação já foi aplicada nos anos de 2000, 2003, 2006, 2009 e 2012.

Figura 1 - Tabela: Ranking de Matemática do PISA 2012

Economias	Média
1º - Xangai-China	613
2º - Cingapura	573
3º - Hong Kong-China	561
4º - Taiwan (Taipei-China)	560
5º - Coreia do Sul	554
6º - Macau-China	538
7º - Japão	536
8º - Liechtenstein	535
9º - Suíça	531
10º - Holanda	523
Média da OCDE	**494**
56º - Costa Rica	407
57º - Albânia	394
58º - Brasil	**391**
59º - Argentina	388
60º - Tunísia	388
65º - Peru	368

Fonte: OCDE

Dados da OCDE em relação ao PISA mostram que, 2 em cada 3 alunos brasileiros de 15 anos não conseguem interpretar situações que exigem apenas deduções diretas da informação dada, não são capazes de entender percentuais, frações ou gráficos.

No Exame Nacional do Ensino Médio (ENEM) de 2014 os concluintes do ensino médio tiveram uma queda de 7,3% no desempenho da prova de Matemática em relação a 2013, segundo informação divulgada pelo Ministério da Educação (MEC).

Diante desses resultados faz-se necessário uma atenção maior para o ensino de Matemática em nosso País, programas como o PROFMAT (Programa em Matemática de Mestrado Profissional em Rede Nacional) visam contribuir para melhorar esses resultados.

Analisando os PCNs com ênfase na Matemática pode-se destacar que:

> Em seu papel formativo, a Matemática contribui para o desenvolvimento de processos de pensamento e a aquisição de atitudes cuja utilidade e alcance transcendem o âmbito da própria Matemática, podendo formar no aluno a capacidade de resolver problemas genuínos..... proporcionando... o desenvolvimento da criatividade e de outras capacidades pessoais ([5], p.40)

Hoje, muitos esperam que os professores de Matemática assumam a missão de tornar prazerosa a aprendizagem desta “significativa disciplina” deixando para trás alguns “tabus”, como “a Matemática não é para todos”, “é o bicho papão”, enfim, promovam um ensino motivador que estimule nos alunos um firme interesse na resolução de problemas, na

descoberta do quanto é fascinante o conhecimento matemático e sua abrangente utilidade nas mais diversas áreas do conhecimento.

A revista “Cálculo Matemática Para Todos” na sua edição 47 (dezembro/2014) traz uma reportagem de Danielle Ferreira e Dubles Sônego, “A reputação da Matemática: exemplo de fracasso” enfatizando a importância do ensino da Matemática na Educação Básica.

Para Luiz Márcio Imenes, autor de livros didáticos da Editora Moderna, a culpa recai na Matemática Escolar. “A escola costuma desfigurar o conhecimento não só da Matemática, como também de outras áreas” ([11], p. 38).

Muitos alunos dominam alguns conhecimentos matemáticos que são vivenciados no cotidiano de cada um, seja na efetivação de uma compra, no jogo de estratégia, enfim são diversas situações em que a Matemática se faz presente e que em muitos casos eles dominam muito bem esse conhecimento e conseguem solucionar os problemas, mas durante as aulas de matemática esse domínio deixa de existir muitas vezes porque não é exigido do aluno um raciocínio mais criativo fazendo um elo com situações práticas de seu cotidiano**.** A Matemática muitas vezes é tratada mecanicamente como algo onde o aluno tenha apenas que decorar as regras e manipular os símbolos tirando toda a essência da curiosidade e das ideias inovadoras que a Matemática permite fluir na mente humana.

Na mesma reportagem citada acima se destaca um trecho:

> A Matemática é inútil. Muita gente tem essa impressão, mas se colocasse um selinho com os dizeres “Esta coisa contém Matemática” em tudo o que é feito ou construído com a ajuda de bastante Matemática, haveria um selinho desses em todo computador, todo carro, todo telefone, todo avião, todo semáforo, todo filme de cinema... Porém, porque ela pertence aos bastidores, ninguém a vê. ([11], p. 39)

Na tentativa de despertar no aluno o prazer em estudar Matemática deve-se buscar ferramentas que lhe permitam compreender melhor e guardar os conceitos matemáticos. Portanto, o objetivo deste trabalho é apresentar uma destas ferramentas: alguns algoritmos matemáticos, dando destaque aos usados na Educação Básica, isto é, aqueles usados nas operações básicas (adição, subtração, multiplicação e divisão), na extração de raízes, no cálculo do MMC e MDC, na resolução de equações do 2º grau, na identificação dos números primos, etc. Enfim, bem enfocar o uso desses e de alguns outros algoritmos, não deixando de lado a análise de sua evolução histórica.

A apresentação desses algoritmos unicamente na sua forma final faz com que o aprendizado seja feito de forma mecânica, o aluno tem apenas que “decorar” os passos do algoritmo para conseguir chegar ao resultado final. Porém ao ser contextualizado torna

possível ao aluno compreender o porquê das operações realizadas e o papel que elas desempenham. Espera-se assim fazendo que seu interesse e curiosidade se robusteçam e até mesmo venha a contribuir para o crescimento de sua criatividade. Entretanto, o desempenho vergonhoso não tem como causa única falhas envolvendo o professor da matéria e daí o desinteresse dos alunos. É um problema decorrente de muitas causas. Só pra citar algumas: violência ambiental e doméstica, má gerência escolar, pobreza etc. Não se chegará a uma solução otimizando apenas um desses parâmetros. A solução só começará a surgir quando forem levados em conta todos esses parâmetros. Atesta isto o estudo realizado pelo Instituto Nacional de Estudos e Pesquisa Anísio Teixeira (INEP) reforçando a tese de que a eficácia do professor, além de ser influenciada pelo perfil dos alunos, é afetada também pelas condições das escolas em que trabalha. Outro estudo realizado pelo Dr. José Francisco Soares, da universidade Federal de Minas Gerais (UFMG), com base na análise de informações do banco de dados do INEP mostra que a sociedade, a organização das escolas e os sistemas de ensino têm impacto no desempenho dos alunos da Educação Básica.

Segundo Soares, a aprendizagem não está restrita apenas a escola. Fatores como a família, a igreja, os clubes e a própria estrutura escolar tanto na parte de ensino quanto na parte de gestão fazem a diferença no desempenho dos alunos da Educação Básica. [29]

Entre os grandes entraves da Educação Básica estão a permanência e o ineficiente aprendizado do aluno na escola, levando muitos, de tão desestimulados, a desistirem. São vários os fatores que levam à desistência do aluno, e entre eles estão necessidades financeiras da família, envolvimento com drogas, etc e, finalmente, o método de ensino empregado na Matemática. Assim, a maioria dos alunos que consegue concluir o Ensino Médio apresenta um aprendizado que está aquém do que consta no seu certificado de conclusão, tendo destaque a Matemática, como mencionam os últimos resultados nos exames PISA e ENEM acima referidos. Portanto, a reapresentação de alguns algoritmos matemáticos utilizados na Educação Básica visa oferecer mais um recurso aos professores desta disciplina, na esperança que eles passem dar uma maior atenção ao conhecimento apresentado sob esta forma nas suas aulas diárias, apostando que seus alunos irão mostrar um maior interesse e uma melhor compreensão resultando em um aprendizado mais robusto e permanente.

No Capítulo 1 deste trabalho abordamos a origem do termo “algoritmo”, seu conteúdo histórico, bem como seu conceito matemático e também sua ampla aplicação em outras áreas do conhecimento.

No Capítulo 2 são apresentados os algoritmos matemáticos mais usados na Educação Básica: como seja o da multiplicação, da divisão, do cálculo do MMC e do MDC,

da resolução das equações do 2º grau e o algoritmo para identificação dos números primos. Quando possível também é abordada a história da origem do algoritmo.

No Capítulo 3 discute-se a importância dos algoritmos relacionados à vida atual, principalmente, com o surgimento, aprimoramento e disseminação do uso dos computadores no nosso cotidiano e na capacidade de processamento dos *smartphones*, que tantas transformações vêm acarretando no nosso comportamento, nos valores das pessoas e na maneira como lidamos com as informações.

2. ABORDAGEM HISTÓRICA E CONCEITUAL DO TERMO ALGORITMO

Mesmo sem perceber, os algoritmos são usados rotineiramente no nosso dia-a-dia e nas mais diversas situações quando realizamos ações individuais ou coletivas. Ao cumprir uma tarefa normalmente seguimos regras. Destarte, o uso de algoritmos tem importância na nossa vida, embora na maioria das vezes sua execução passe despercebida, pois de tanto usá-los o fazemos automaticamente. Aqui ficaremos restritos principalmente aos algoritmos usados na aritmética elementar com algumas incursões em outras áreas que exigem um maior conhecimento. Neste Capítulo faremos uma breve exposição da palavra *algoritmos* além de abordar o que ela significa modernamente.

Uma definição informal do que seja um *algoritmo* poderia ser expressa como “um conjunto finito de regras que definem precisamente uma sequencia de operações”. Os cofres mais antigos para serem abertos se fazia necessário que um conjunto de regras fosse executadas de forma sequencial sem nenhum erro. Ao se completar uma determinada regra da sequência pequenos ruídos ou leves estalidos eram ouvidos confirmando que aquela regra tinha sido executada corretamente. Finda a execução da última regra o cofre estava aberto. Para lacrá-lo não era necessário seguir um algoritmo, bastava movimentar as engrenagens de qualquer jeito: pronto, o cofre estava novamente selado. Em fábricas modernas muitos itens para serem fabricados devem seguir regras precisas até o final. Findo o processo a produção do item está concluída. Noutras situações um determinado item a ser produzido é composto por diversas partes que devem ser montadas obedecendo a uma rigorosa sequência. Estes são exemplos de algoritmos que a bem da verdade deixam de serem percebidos como tais.

Hoje vivemos num processo acelerado de “algoritmização” da vida. É difícil se achar um campo de atividade ou de lazer que não esteja sujeito a “algoritmização”, isso vem tomando impulso a partir da Revolução Industrial da segunda metade do século XVIII e nos últimos 50 anos com o nascimento da Era da Informatização. Como chegamos a este ponto e como “a idade do algoritmo” impacta e molda as pessoas desde a sua criatividade e até seus relacionamentos? (até mesmo os que são classificados como românticos).

*Algoritmo*s são muito eficientes em nos dar respostas, mas a verdadeira pergunta é saber se eles estão nos dando a resposta que estamos procurando. Há 350 anos René Descartes dizia: “penso logo existo”. Hoje o parafraseamos dizendo: “quantifico (meço), logo existo”. Nessa direção os serviços nacionais que procuram acompanhar a disseminação de epidemias e sua velocidade, usam a internet para avaliar as mensagens que as pessoas trocam entre si e a partir delas seguir em tempo real a disseminação ou abrandamento da epidemia. Ao

acessarmos apenas alguns *sites*, algoritmos de análise de dados em larga escala procuram traçar nosso perfil e a partir dele saber ou nos sugerir o que estamos procurando.

É recente o uso de equipes de pesquisadores regiamente pagos para elaborar ou aperfeiçoar algoritmos que interessam a governos e grandes conglomerados financeiros em quase todas as áreas de nossa existência. Os conhecimentos matemáticos empregados na coleta e formalização destes dados de tão sofisticados só estão ao acesso de pessoas altamente treinadas e de grande capacidade intelectual.

Em um sentido mais restrito, são algoritmos todos os programas de computadores, inclusive aqueles programas que não executam cálculos numéricos. Todavia, um programa só pode ser considerado um algoritmo se ele chega a um final – para. Nestas situações existe uma consciência que algoritmos estão sendo executados. Mas ao somarmos dois números ou até mesmo quando comparamos dois inteiros para decidir qual deles é o maior estamos lidando com algoritmos embora não percebamos este fato. Estes processos são rotineiramente executados de forma automática.

É comum professores da Educação Básica reclamarem das dificuldades que seus alunos encontram ao se depararem com um problema que tenham de desenvolver um raciocínio matemático para chegar à sua solução, a raiz desta dificuldade é devida principalmente a incapacidade dos alunos no domínio das técnicas usadas nas operações (adição, subtração, multiplicação e divisão) básicas da aritmética. O entendimento e domínio desses algoritmos são de fundamental importância para o êxito na solução de problemas relacionados à Educação Matemática. Como surgiu este termo algoritmo? Qual sua importância para a Matemática?

2.1 SURGIMENTO DO TERMO ALGORITMO

Iniciaremos com uma abordagem das raízes históricas do sistema decimal. Pesquisas sobre como evoluiu o conhecimento matemático revelam que este evoluiu lentamente. Achados arqueológicos na África sugerem que o homem que habitava aquela região já sabia contar, bem antes do surgimento de qualquer civilização.

Com o advento da agricultura no Crescente Fértil talvez devido às necessidades da sociedade, novos conhecimentos e técnicas foram surgindo. Era preciso plantar na época certa e por isso os corpos celestes passaram a ser observados para marcar e compreender a passagem do tempo. Era preciso registrar o que era observado e daí surgiu a escrita não apenas para anotar as necessidades cotidianas mas também para guardar o que iam

observando. Destas observações foram surgindo pequenas descobertas que eram aplicadas para o bem de todos. A população era em sua esmagadora maioria analfabeta. Este conhecimento ficava restrito aos governantes e sacerdotes. Tudo era empírico, obtido experimentalmente. Se surgia algo que podia ser expresso através de uma fórmula ou equação isso não era feito. Seria um tipo primitivo de algoritmo, semelhante ao algoritmo que era usado para cortar uma pedra e poli-la a fim de ser usada em alguma construção.

Estes conhecimentos apesar de serem pouco divulgados, foram pouco a pouco se espalhando pelo mundo conhecido da época. Assim, povos que habitavam ilhas rochosas no atual Mar Egeu (os gregos minóicos) desenvolveram técnicas de navegação e passaram a controlar o comércio dos bens produzidos entre os diversos povos do Mediterrâneo. Muitas destas mercadorias antes de chegarem aos navios eram transportadas nas costas de camelos. Entrepostos controlados por esses navegadores foram para o continente à medida que a economia se desenvolvia. Eles não transportavam apenas mercadorias, transportavam também conhecimentos e técnicas.

Os gregos que iam de Creta para o continente se tornando uma sociedade mais próspera e afluente podiam desfrutar de um certo ócio que usavam para se divertir e aprofundar o conhecimento que acompanhava as atividades econômicas. Então, em algum momento no quinto século a.C. os gregos começaram a tentar provar resultados que eram do conhecimento dos povos babilônico e egípcio. Antecede esta época a descoberta do alfabeto fonético muito mais simples e fácil de ser usado quando comparado aos alfabetos pictóricos usados no Crescente Fértil e no Egito. Esta nova técnica de registrar palavras incentivou o comércio e motivou as pessoas a tentarem aprender a escrever. Até então a escrita só estava ao alcance de especialistas que eram treinados durante anos e anos: os escribas. Eles eram escolhidos a dedo pela classe sacerdotal que exercia um enorme poder tanto civil como religioso, pois era a guardiã dos conhecimentos acumulados. Logo apareceram pessoas escrevendo para serem lidas por outros e foi o início da literatura. Outros registravam os seus pensamentos e as discussões que mantinham com outros homens interessados em responder questões que afetavam a vida de todos. Estes ficaram conhecidos como filósofos. Eles também procuravam resolver problemas e enigmas da época — exerciam o papel de cientistas, sem o saber. Fato curioso, a palavra *cientista* foi cunhada na Inglaterra em 1834 quando foi registrada pela primeira vez em inglês. [6]

A escrita grega não era apropriada para registrar conhecimentos matemáticos, apenas a linguagem cotidiana. Até para registrar um número lançavam mão das letras; assim, alfa também podia significar um; beta, dois etc. Devido a estas razões o grego foi se

espalhando pelo Mediterrâneo onde viviam colônias gregas (entrepostos, às vezes) e pouco a pouco se tornou a primeira língua amplamente disseminada, isto é, a primeira língua internacional. Em Alexandria, no Egito, foi erigida uma biblioteca que visava reunir todo o conhecimento já adquirido pela humanidade. Eram ministrados cursos para alunos que lá acorriam não na língua egípcia e sim, em grego. Ficou conhecida como o Museu de Alexandria. Aliás, nenhum alfabeto é apropriado para registrar o conhecimento matemático. Os símbolos usados atualmente para registrar os conhecimentos matemáticos foram (e ainda estão) surgindo lentamente, tendo havido uma aceleração na sua invenção e uso a partir do século XVII.

Com o colapso do império grego depois da morte de Alexandre, o grego continuou com sua influência, agora dividindo com o latim que foi a segunda língua internacional. Mesmo depois do colapso do império romano no século V d. C., estas duas línguas continuam faladas e escritas pelos povos europeus. Símbolos foram sendo inventados pouco a pouco durante os séculos vindouros. Quando Euclides escreveu *Os Elementos* certamente não foi ele quem descobriu todo aquele conhecimento e sim, seus predecessores. Na sua maior parte ele apenas sistematizou o conhecimento existente contribuindo pessoalmente com uma fração própria impossível de ser quantificada, pois ele não deixou isso registrado. Ele foi o primeiro grande sistematizador desse conhecimento que brotava em lugares diversos do planeta e em épocas também distintas.

O conhecimento matemático, como não poderia deixar de ser, está intimamente ligado ao estágio de desenvolvimento da sociedade. Uma parte desse conhecimento vai pouco a pouco se difundindo nesta sociedade ao ponto de ser usado por ela sem que seja percebido, principalmente naqueles lugares que apresentam um desenvolvimento econômico e cultural mais alto. A utilização da Matemática vem aumentando em todas as sociedades humanas à medida que alcançam níveis mais altos de conhecimentos e de recursos econômicos. Nos estágios iniciais são usados apenas conhecimentos básicos de geometria e operações aritméticas.

Os avanços não ocorrem de forma contínua; havia períodos de estagnação que duravam séculos. Então, despertava como de um sono letárgico e punha-se novamente a caminhar, às vezes, em uma região diferente. Um exemplo foi o sono da Matemática na Europa a partir do século V d.C durando até o século XIV. Enquanto isso na Índia ela dava saltos espetaculares nos séculos V-VII e estes conhecimentos transbordaram para os povos vizinhos, o mundo árabe. O que aconteceu na Índia neste período foi tão extraordinário ao ponto de nada que lhe seja equivalente aparecer no cenário mundial nos próximos 1000 anos.

No século VII d.C., quando foi instituído o califado em Bagdá, o aprendizado das culturas adjacentes foi sendo absorvido pela nova e expansiva cultura Árabe. Ao conquistar um território os Árabes tinham pouco a contribuir intelectualmente, eles costumavam adquirir o modo de escrita, particularmente a notação dos numerais dos hindus. Em meados do século VIII foram chamados a Bagdá estudiosos da Síria e Mesopotâmia para contribuir com os seus conhecimentos científicos.

Foi durante o califado de al-Mamum, que os Árabes se entregaram totalmente a sua paixão em traduzir para o árabe o que havia de valor nas culturas vizinhas. Al-Mamum criou em Bagdá um estabelecimento que veio a chamar-se "Casa da Sabedoria", comparável ao antigo Museu de Alexandria, entre seus mestres havia um matemático e astrônomo chamado Mohammed ibu-Musa al-Khowarizmi, cujo nome, como o de Euclides, iria tornar-se familiar na Europa Ocidental. ([4], p.166).

Graças aos trabalhos do matemático al-Khowarizmi, o uso dos numerais hindus rapidamente expandiu-se por todo o mundo Árabe. Um dos primeiros tradutores do trabalho de al-Khowarizmi foi Adelard de Bath que por volta do ano de 1120**,** produziu um texto em latim cujas primeiras palavras eram *Dixit Algorism* ...(Assim disse o Algorismo...) e que passou a ser conhecido simplesmente por algorismo.. Esse termo, e vários outros vocábulos originados de autores diferentes, finalmente se difundiram através das línguas europeias até ao ponto do processo de fazer aritmética com os numerais hindus ser chamado apenas por *algarismo*, e isso nos deu o termo *algoritmo*. ([12], p.33).

Entre as obras de al-Khowarizmi destaca-se uma de tradução latina com o título *De numero hindorum* (Sobre a Arte Hindu de Calcular). Nessa obra baseada numa tradução de Brahmagupta, al-Khowarizmi deu uma exposição tão completa dos numerais hindus que provavelmente foi o responsável pela impressão muito difundida mas falsa de que nosso sistema de numeração é de origem Árabe.([4], p.74).

A expansão dos numerais hindus deu-se rapidamente por todo mundo Árabe e através do comercio e guerras entre árabes e europeus alcançou também o vasto território europeu.

Os numerais romanos não saíram de cena assim da noite para o dia, séculos transcorreram para que o sistema numérico dos hindus fosse ganhando cada vez mais aceitação. O entendimento do zero não era nada fácil já que em algumas situações ele representava a ausência de valores, enquanto em outras, dependendo de sua posição, adquiria valores distintos. Aos poucos as pessoas foram compreendendo a maneira de representar e calcular à moda hindu devido a sua praticidade de realizar operações aritméticas seja para

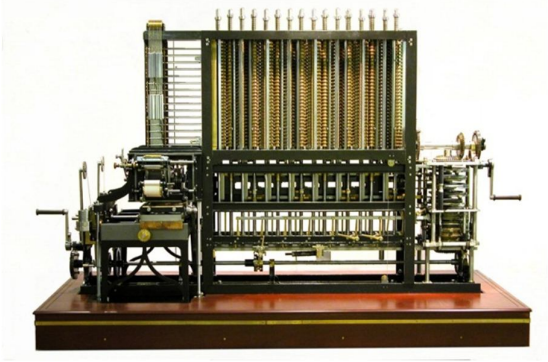
representar estes números seja para operar com eles, levando o sistema romano de representar números e de realizar operações aritméticas com o ábaco chinês fosse caindo em desuso.

Por volta de 1375 o uso dos numerais hindus firmou-se na Europa. Eles começaram a aparecer em muitos documentos diferentes, embora ainda existisse uma grande resistência para a adoção dos novos números. ([12], p.42).

Percebemos que o método de calcular fez com que a representação dos números que utilizamos hoje fosse aceita. Com o crescimento da economia europeia a maneira de se fazer cálculos precisava ser agilizada. Surgiu então a *régua de cálculo* um instrumento inventado pelo pároco inglês William Oughtred em 1622. E isso não foi o fim de tudo como logo veremos.

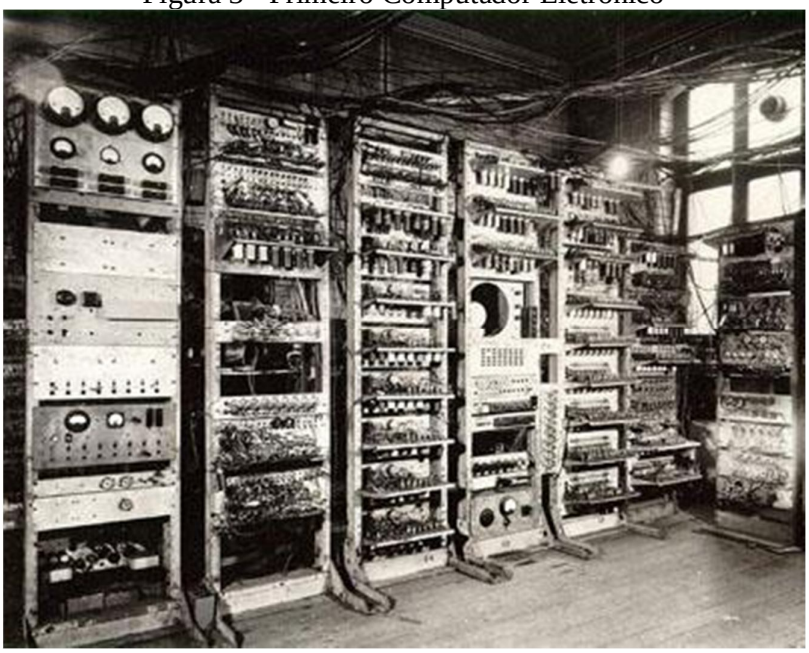
Foi nas antigas civilizações da China, do Egito e da Babilônia onde foram dados os primeiros passos no desenvolvimento de ferramentas que permitissem realizar cálculos aritméticos de maneira mais rápida e com mais eficiência do que os feitos através dos recursos mentais do interessado. Indivíduos tidos por prodígios na realização de cálculos mentais sempre foram raros. Fazer contas mentalmente sempre esteve fora do alcance da maioria, salvo quando se tratava de algo bastante simples. Daí a procura pelo desenvolvimento de ferramentas fáceis de usar, que permitisse realizar cálculos aritméticos sem grande esforço mental (não se está afirmando que os computadores surgiram nesta época), mas sim as primeiras ideias que acabaram por resultar em calculadoras primitivas e sempre mais sofisticadas, a Máquina Analítica de Babbage (movida a vapor) por volta do ano de 1834 e cem anos depois o primeiro computador eletrônico no final da Segunda Guerra Mundial (movidade a eletricidade).

Figura 2 - Máquina Analítica de Babbage



Fonte: http://pnld.moderna.com.br/2012/10/19/a-origem-do-computador/, acesso em 27/07/15.

Figura 3 - Primeiro Computador Eletrônico



Fonte: http://www.din.uem.br/museu/virtualhtml/1946_mm.htm, Acesso em 27/07/15.

Atualmente o uso dos computadores está onipresente no cotidiano das pessoas, seja na sala de aula, no trabalho ou no lazer, na medicina, no auxílio ao desenvolvimento de novas tecnologias, nos transportes, nas atividades culturais etc, Contudo, para que o computador execute as tarefas que tanto facilitam, agilizam e tornam mais precisas as nossas vidas faz-se necessário o emprego maciço de muitos ramos da Matemática, pois são os algoritmos que possibilitam as máquinas fornecerem respostas e agilizarem às demandas solicitadas. Estes processos envolvem cada vez mais pessoas especializadas, resultando em uma aceleração de todos os processos do cotidiano em um ritmo cada vez mais acelerado.

Um algoritmo é um procedimento eficaz, um modo de fazer uma coisa em um número finito de passos discretos que se estende a uma miríade de atividades humanas. A Matemática tem contribuído significativamente, desde a antiguidade, com algoritmos que extrapolam os seus domínios e abarcam outras áreas de atividade de nosso dia-a-dia.

Para David Berlinski (2002), autor do livro *O Advento do Algoritmo*, "o algoritmo é a ideia que rege o mundo". Sem seu uso disseminado, o mundo atual ainda estaria no mesmo estágio do mundo do século XIX e anteriores. Relógios ultra precisos permitiram o uso disseminado do GPS, o desenvolvimento de protocolos (*http*) que deram origem a internet, daí resultando a democratização dos conhecimentos, as mensagens instantâneas, as transações bancárias *on line*, a conquista espacial.

Estes avanços ocorreram e ainda estão a ocorrer com aceleração crescente em todas as áreas do nosso mundo. Muitos de tão disseminados já passam despercebidos pelo homem comum que nem suspeita do que está ocorrendo para que ele tenha acesso a este mundo maravilhoso. Tudo isso só se tornou possível devido ao avanço colossal do conhecimento matemático. Nenhuma ciência contribuiu tanto para moldar e mudar o mundo atual. E o processo continua. Ninguém pode prever o que virá logo em seguida.

Os algoritmos que movem as máquinas operatrizes nas indústrias, muitas vezes substituindo a mão humana com uma eficiência, precisão e ausência de erros, bem como as máquinas controladoras e computadores, todas obedecem a algoritmos que são advindos de descobertas matemáticas, algumas datando de séculos passados, como por exemplo, os *quarternions* usados na aviação e nos jogos de ação em computadores ou os *octônios* que estão entre as ferramentas utilizadas na Teoria da Super-simetria. Previsões meteorológicas só se tornaram possíveis implementando entre outros conhecimentos as Equações de Navier-Stokes que datam dos meados do século XIX.

Todavia, ensinar algoritmos apenas para obter uma resposta, deixando de lado o entendimento das operações que estão nas entrelinhas de cada passo, é tirar do aluno a oportunidade de aprimorar seu entendimento e contribuir para o avanço da Matemática, além de lhe proporcionar uma visão mais ampla e profunda de sua beleza intrínseca.

Mesmo no nível mais elementar, o professor ao ensinar o algoritmo da adição dando ênfase apenas ao resultado final, ele deixa de explorar muito do nosso sistema de numeração, como os agrupamentos de dez em dez, as ordens, enfim o aluno perde a oportunidade de compreender mais profundamente e apreciar a beleza do sistema decimal.

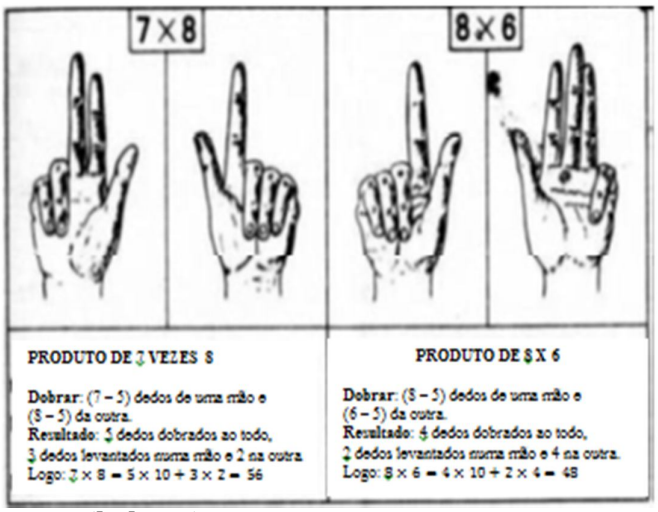
3 ALGORITMOS MATEMÁTICOS

3.1 ALGORITMOS DA MULTIPLICAÇÃO NO EGITO ANTIGO

A operação aritmética mais comum no Egito era adição, enquanto as operações de multiplicação e divisão eram efetuadas na época de Ahmes (aprox.. 1650 anos a.C) por sucessivas “duplações” seguidas da soma de algumas destas duplicações, como logo mais veremos exemplificado. A operação de “multiplicação”, na verdade, sugere o processo egípcio. ([4], p.11)

Os algoritmos ensinados hoje nas escolas para efetuar os cálculos das quatro operações passaram por modificações ao longo do tempo, mas guardam muito do que era usado neste passado remoto. O que se perdeu foi a essência do cálculo, tudo ficou mais automatizado com o surgimento das novas tecnologias. O homem primitivo (e ainda as crianças pequenas hoje) fazia suas contas com o auxílio de seus dedos, que certamente contribuiu para o surgimento do sistema decimal dada a familiaridade adquirida ao longo de incontáveis séculos dessa prática.

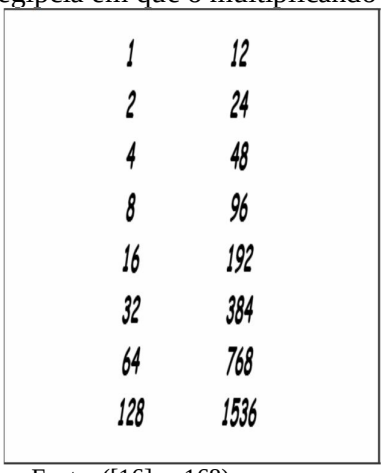
Figura 4 - Multiplicação utilizando os dedos das mãos



Fonte: ([16], p.95)

Conforme Boyer citado acima a multiplicação realizada pelos egípcios, por volta de 2000 a.C. era baseada nas potências de base 2. Para multiplicar 128 por 12 escreviam com algarismos hieroglíficos 1 e 12 e procediam duplicando ambos os números até que o número 128 aparecesse. (Figura 5). O número 1536 constitui o resultado da multiplicação.

Figura 5 - Multiplicação egípcia em que o multiplicando é uma potência de base 2



1	12
2	24
4	48
8	96
16	192
32	384
64	768
128	1536

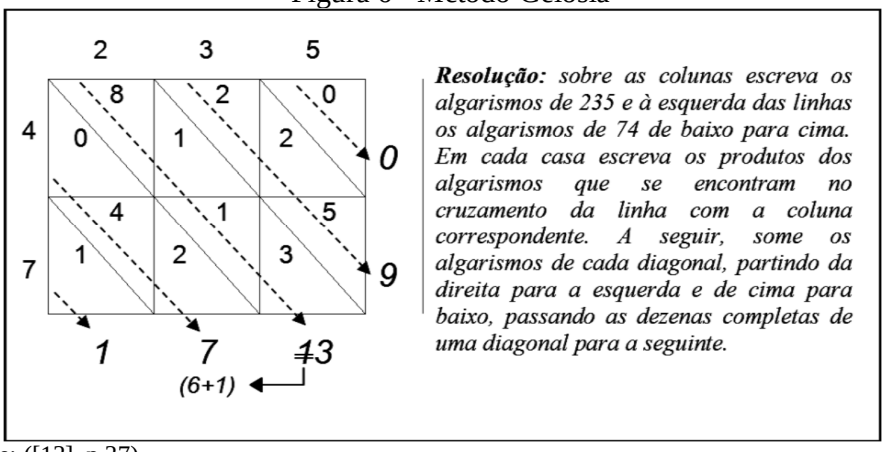
Fonte: ([16], p.168)

A medida que os sistemas de numeração foram evoluindo os métodos para cálculos aritméticos também foram se modificando, principalmente com o surgimento do zero que foi tão importante para facilitar e até viabilizar muitos cálculos que para a época eram impossíveis de serem realizados sem a sua invenção.

A descoberta do zero criou a Aritmética como ela é hoje concebida, ensinada e utilizada, e o mesmo se pode dizer em relação à notação, que acabou por introduzir uma nova etapa na história da Álgebra. ([12], p.53)

Os hindus a partir do século VI utilizavam para multiplicar, um método denominado de *gelosia*. Para multiplicar 235 por 74 desenha-se um quadro de três colunas e duas linhas formando seis novos quadros divididos por diagonais do canto superior esquerdo ao canto inferior direito formando 12 casas (Figura 6).

Figura 6 - Método Gelosia



Fonte: ([13], p.37)

Os algarismos do exterior do quadro formam o produto de 235 por 74 fazendo a leitura da esquerda para a direita e de baixo para cima.

235 x 74 = 17390

Uma forma de multiplicar muito usada no passado e, ainda hoje utilizada é a multiplicação por decomposição, que muitas vezes facilita o cálculo, principalmente o cálculo mental. Por exemplo, na multiplicação de 32 por 45 teremos:

32 x 45 = (30+2) x (40+5)

32 x 45 = (30 x 40) + (30 x 5) + (2 x 40) + (2 x 5)

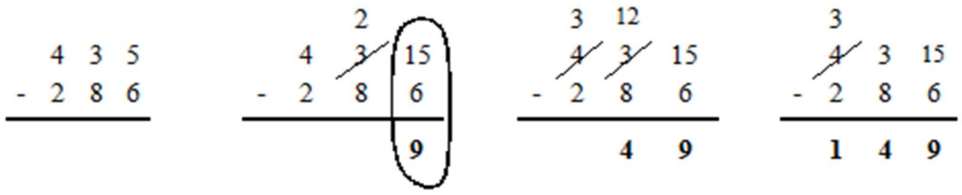
32 x 45 = 1200 + 150 + 80 + 10

32 x 45 = 1440

3.2 ALGORITMOS DA SUBTRAÇÃO

O registro de subtrações foi encontrado no uso de pedras e outros objetos. Em certa aldeia africana, eram utilizados anéis para controlar o número de moças solteiras: “Quando atingia a idade exigida, cada uma confiava um pequeno anel metálico à “casamenteira” da aldeia, [...]. Depois pouco antes da cerimônia, cada futura esposa recuperava seu anel”.([16], p.192).

O algoritmo para subtração mais utilizado nas salas de aulas é habitualmente designado por algoritmo de decomposição em que se recorre alternadamente às ações matemáticas: separar e reagrupar. Vejamos um exemplo:



Este método requer uma compreensão das características do sistema de numeração decimal, a noção de valor posicional e agrupamentos na base 10. Consiste na decomposição do minuendo fazendo o reagrupamento sempre que um ou mais algarismo do minuendo for menor que o algarismo do subtraendo. No exemplo acima temos o cálculo da diferença entre os números 435 e 286. Como o valor relativo do algarismo 5 é menor que o 6, reagrupamos o minuendo transformando 1 dezena em 10 unidades, desta forma ficamos com 15 unidades que subtraindo as 6 unidades temos como resto 9 unidades , seguindo o mesmo raciocínio reagrupando as dezenas e centenas conclui-se a subtração. O uso atual desta técnica certamente deve-se ao fato de ser mais concretizável pelas crianças.

Outro método ainda hoje usado por alguns professores de Matemática é o método da compensação que consiste em adicionar quantidades iguais no minuendo e no subtraendo, ou seja, numa subtração se adicionarmos o mesmo número ao minuendo e ao subtraendo a diferença não se altera. Conforme ilustrado no exemplo abaixo.

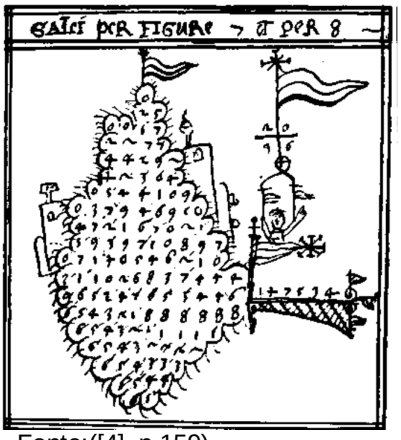
4 3 5	4 3 10+5	4 10+3 15	4 13 15
- 2 8 6	- 2 1+8 6	- 1+2 9 6	- 3 9 6
	9	**4 9**	**1 4 9**

3.3 ALGORITMOS DA DIVISÃO

Sobre métodos de divisão, Boyer (1974) afirma que:

> [...] os árabes (e através deles os europeus mais tarde) parecem ter adotado a maior parte de seus métodos aritméticos da Índia, e por isso é provável que o esquema de divisão conhecido como o "método de riscar" ou "método de galeão" (por sua semelhança com um navio) também tenha tido origem na Índia. ([4], p.158).

Figura 7 - Divisão em galeão, século XVI



Fonte:([4], p.159)

Segue abaixo os passos da divisão de 65782 por 426 usando o *método galeão*:

1. Escreva o divisor à esquerda do dividendo, como se mostra abaixo. Obtenha, da maneira habitual, o primeiro algarismo do quociente (657 : 426), que é 1, e escreva-o à direita do dividendo.

426 | 65782 | 1

2. Escreva o produto de 1 x 426, que é 426, abaixo de 657.

- Faça mentalmente 6 – 4 = 2. Risque o 6 e o 4 e escreva 2 acima do 6.

- Faça mentalmente 5 – 2 = 3. Risque o 5 e o 2 e escreva o 3 acima do 5.

- Faça mentalmente 7 – 6 = 1. Risque o 7 e o 6 e escreva o 1 acima do 7.

$$\begin{array}{cccccccccc} & & & & 2 & 3 & 1 & & & \\ 4 & 2 & 6 & | & \cancel{6} & \cancel{5} & \cancel{7} & 8 & 2 & | \ 1 \\ & & & & \cancel{4} & \cancel{2} & \cancel{6} & & & \end{array}$$

3. O dividendo resultante do passo 2 é 23182, que são os algarismos não riscados, lidos de cima para baixo, na coluna do meio. Obtenha o próximo algarismo do quociente (2318 : 426) que resulta em 5.

- Escreva o produto de 5 x 426, que é 2130, colocando o zero abaixo do 8, o 3 abaixo do 6, o 1 abaixo do 2 e o 2 abaixo do 4.

- Faça mentalmente 2 – 2 = 0. Risque o 2 e o 2, não é necessário escrever o zero acima do 2.

- Faça mentalmente 3 – 1 = 2. Risque o 3, o 1 e escreva o 2 acima do 3.

- Como não podemos subtrair 1 de 3, risque o 2 e escreva o 1 acima do 2 e faça mentalmente 11 – 3 = 8. Risque o 1 e o 3 e escreva o 8 acima do 1.

- Faça mentalmente 8 – 0 = 8. Risque o 8 e o zero e escreva o 8 acima do 8.

$$\begin{array}{cccccccccc} & & & & & 1 & & & & \\ & & & & & \cancel{2} & 8 & & & \\ & & & & \cancel{2} & \cancel{3} & \cancel{1} & 8 & & \\ 4 & 2 & 6 & | & \cancel{6} & \cancel{5} & \cancel{7} & \cancel{8} & 2 & | \ 1 \ 5 \\ & & & & \cancel{4} & \cancel{2} & \cancel{6} & \cancel{0} & & \\ & & & & \cancel{2} & \cancel{1} & \cancel{3} & & & \end{array}$$

4. O dividendo resultante do passo 3 é 1882, que são os algarismos não riscados, lidos de cima para baixo, na coluna do meio. Obtenha o próximo algarismo do quociente (1882 : 426), que é 4.

- Escreva o produto de 4 x 426, que é 1704, colocando o 4 abaixo do 2, o zero abaixo do zero, o 7 abaixo do 3 e o 1 abaixo do 1.

- Faça mentalmente 1 – 1 = 0. Risque o 1 e o 1, não é necessário escrever o zero acima do 1.

- Faça mentalmente 8 – 7 = 1. Risque o 8 e o 7, escreva o 1 acima do 8.

- Faça mentalmente 8 – 8 = 0. Risque o 8 e o zero. Escreva o 8 acima do 8.

- Como não podemos subtrair 2 de 4, risque o 8 e escreva o 7 acima do 8 e faça mentalmente 12 – 4 = 8. Risque o 2 e o 4, escreva o 8 acima do 2.

$$
\begin{array}{cccc|cccccc|ccc}
 & & & & & \cancel{1} & 1 & 7 & & & & & \\
 & & & & & \cancel{2} & \cancel{8} & \cancel{8} & & & & & \\
 & & & & \cancel{2} & \cancel{3} & \cancel{1} & \cancel{8} & 8 & & & & \\
4 & 2 & 6 & | & \cancel{6} & \cancel{5} & \cancel{7} & \cancel{8} & \cancel{2} & | & 1 & 5 & 4 \\
 & & & & \cancel{4} & \cancel{2} & \cancel{6} & \cancel{0} & \cancel{4} & & & & \\
 & & & & \cancel{2} & \cancel{1} & \cancel{3} & \cancel{0} & & & & & \\
 & & & & & \cancel{1} & \cancel{7} & & & & & &
\end{array}
$$

5. O quociente é 154 e o resto é 178.

No Egito o algoritmo da divisão, assim como a multiplicação era efetuado por sucessivas duplicações seguidas de somas de algumas destas duplicações, baseado no fato de que todo número pode ser representado por uma soma de potências de base 2.([4], p.11)

Para dividir 3420 por 75, dobramos o divisor sucessivamente, conforme o quadro abaixo:

75 x 2 = 150
150 x 2 = 300
300 x 2 = 600
600 x 2 = 1200
1200 x 2 = 2400

O dobro de 2400 ultrapassa 3420, então:

3420 = 2400 + 600 + 300 + 75 + 45
3420 = (75 x 32) + (75 x 8) + (75 x 4) + (75 x 1) + 45
3420 = 75 x (32 + 8 + 4 + 1) + 45
3420 = 75 x 45 + 45
Logo o quociente é 45 e o resto também é 45

O algoritmo da divisão é considerado por muitos alunos e professores de Matemática da Educação Básica como sendo um dos mais difíceis, Mandarino (2005) afirma que:

> O algoritmo da divisão é, sem dúvida, o mais difícil e o mais complexo dentre os algoritmos das quatro operações, pois envolve, além do sistema de numeração, dos fatos básicos e do conceito de operação, a utilização das outras operações (adição, subtração e multiplicação) e a propriedade distributiva da divisão em relação à adição ([17], p. 157).

3.4 ALGORITMOS PARA O CÁLCULO DE RAÍZES

Outra operação bastante usada na Matemática básica e que deixa muitos alunos intrigados sobre o seu método de cálculo é a extração de raízes.

René Descartes, filósofo e matemático do século XVII, considerado por muitos como o “pai da Matemática moderna”, destaca a extração de raízes, em especial as raízes quadradas, uma operação especial na aritmética, ao lado das quatro operações básicas (adição, subtração, multiplicação e divisão), em seu livro “*La Géométrie*”, afirma que:

“(...) toda a aritmética é apenas composta por quatro ou cinco operações, que são: a adição, a subtração, a multiplicação, a divisão e a extração das raízes, que pode ser entendida como uma espécie de divisão (...)”

O cálculo da raiz quadrada nos dias atuais é uma banalidade, bastando para tanto ter acesso a uma calculadora simples que, de tão disseminada, está ao alcance de praticamente todas as pessoas. Este é um fato recente. No início dos anos setenta, a calculadora HP-35, (assim batizada devido as suas 35 teclas, além da tecla de liga/desliga) e vendida na época por US$400 que, atualizados, seriam hoje US$1.500 levando em conta uma inflação média de 3% ao ano. Em 1978 seu preço tinha despencado para US$15 atuais, isto é, custava 100 vezes mais há apenas 5 anos! Mesmo com tamanho preço vendeu em três anos mais de 300.000 unidades. Foi a primeira calculadora portátil digital (pesava menos de 250 g) a calcular logaritmos, exponenciais e as funções trigonométricas. Hoje, uma calculadora HP gráfica, sensível ao toque, programável custa apenas US$150. Ela é capaz de fazer todo tipo de cálculo numérico, financeiro e estatístico além de integrar, derivar, resolver equações diferenciais, etc.

A primeira calculadora semi-portátil (pesava pouco mais de 700 g) foi lançada pela Sharp em 1971, batizada por Sharp EL-8 ao preço de US$345 nos EUA. (custaria hoje aproximadamente US$1.230). Só fazia as quatro operações — nada de raiz quadrada!

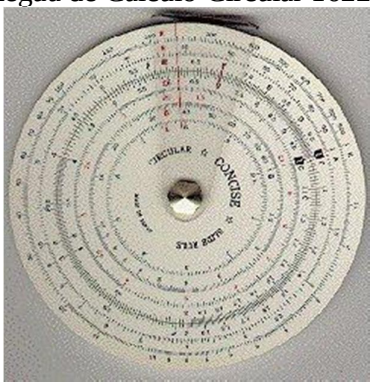
Figura 8 - Calculadora Sharp EL-8

Fonte: https://en.wikipedia.org/wiki/Sharp_EL-8 Acesso em 19/09/2015

Este ano marca o transcurso dos 400 anos desde que Napier publicou (em 1614) sua famosa tabela dos logaritmos, na qual ele empregou 20 anos de trabalho árduo. Os logaritmos, que ele escreveu conseguiram libertar os matemáticos do “tedioso dispêndio de tempo” e dos “erros traiçoeiros” presentes nas “multiplicações, divisões, extração de raízes quadradas, cúbicas de números grandes”. Em 1617, um ano após a morte de Napier, Briggs publicou uma nova tabela de logs de todos os números inteiros de 1 a 1000 com oito casas decimais e agora, na base 10 (a base usada por Napier era $(1 - 10^{-7})$. Realmente, os cálculos eram difíceis, tediosos de serem feitos, além de sujeitos a muitos erros. Fazia-se pois necessário a invenção de dispositivos mecânicos que os agilizassem e não cometessem erros no caminho. Foram surgindo então muitos dispositivos e entre eles as réguas de cálculo.

Note-se que Oughtred foi o bispo anglicano e matemático inglês que inventou a primeira régua de cálculo em 1622 que consistia em duas escalas justapostas lado a lado que, quando movimentadas corretamente permitiam que multiplicações e divisões fossem realizadas.

Figura 9 - Régua de Cálculo Circular 1622



Fonte: http://www.din.uem.br/museu/virtualhtml/600_regua.htm, acesso em 27/07/15.

Estes dispositivos reinaram por mais de 300 anos até que as calculadoras eletrônicas, devido a sua facilidade de uso, os substituíssem.

Entre os dispositivos mais notáveis se destaca a calculadora portável conhecida por Curta — a única calculadora mecânica de bolso já produzida. Era capaz de fazer as quatro operações, extrair raízes quadradas e cúbicas, cálculos estatísticos, etc. A primeira vista parecia um moedor de pimenta.

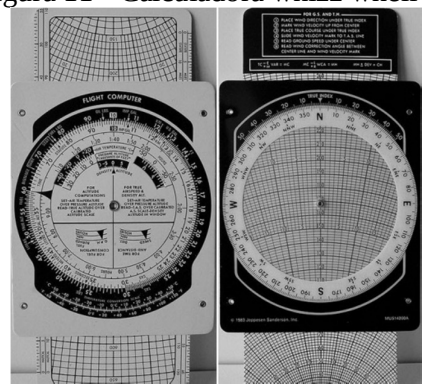
Figura 10 - Calculadora mecânica de bolso

Fonte: http://www.vcalc.net/cu.htm acesso em 19/09/2015

Sua invenção encerra uma história singular, Curt Herzstark, seu inventor, um engenheiro austríaco, filho de pai judeu, projetou seu protótipo enquanto era prisioneiro no campo de Buchenwald. As autoridades do campo aceitaram poupá-lo da morte devido a sua fama de engenheiro genial, permitindo que ele trabalhasse no projeto. Caso tivesse êxito não seria morto e ganharia um certificado de ariano. Foi libertado pelos aliados no final da II Guerra Mundial, levando no bolso de um casaco seu projeto quase concluído. Buscou então alguém que pudesse financia-lo. Essa pessoa foi o príncipe de Liechtenstein e a produção de sua calculadora teve início em 1948. Foram produzidas cerca de 150 mil calculadoras em duas versões. Deixou de ser produzida no início dos anos 70 e seu inventor, que residia em Liechtenstein, morreu aos 86 anos em 1988. A Curta tinha 600 peças e fornecia respostas precisas.

Não é inteiramente verdadeiro que as calculadoras eletrônicas baniram completamente as réguas de cálculo. Ainda existe uma usada por pilotos de avião. É conhecida como *whizz whell*, e calcula velocidade, distância, tempo, consumo de combustível, densidade do ar, etc. Tem formato circular. É usado nos cálculos de planejamento do voo quando ainda em terra. Nos pequenos aviões que não dispõem de recursos eletrônicos ela não pode faltar sendo, portanto necessário que os pilotos saibam como usa-las. Nos grandes aviões elas também estão por lá, caso o sistema de cálculo a bordo entre em pane.

Figura 11 - Calculadora whizz whell



Fonte: (www.en.wikipedia.org/wiki/E6B)

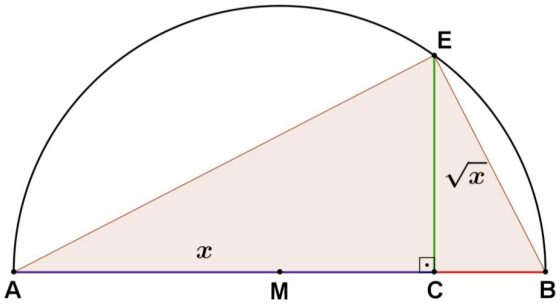
Entretanto, para que estes dispositivos pudessem processar os cálculos, os algoritmos já deviam ser conhecidos. Vejamos alguns deles. Existem vários algoritmos para extração de raízes quadradas.

Descartes apresenta um método geométrico para o cálculo da raiz quadrada usando régua e compasso, descrevemos os passos da seguinte forma:

1. Seja *x* o número que se deseja calcular sua raiz quadrada
2. Construa um segmento unitário BC acrescentando na sua extremidade o segmento de medida *x*, AC.
3. Determine o ponto médio M, do segmento AB.
4. Trace a circunferência que tem centro no ponto M e a medida do raio é dado pelo segmento MB.
5. Trace uma perpendicular ao segmento AB pelo ponto C, que toca a circunferência no ponto E, obtendo assim o segmento CE.

   A medida do segmento CE representa a raiz quadrada de *x*.

Figura 12 - Esboço do esquema para encontrar a raiz quadrada



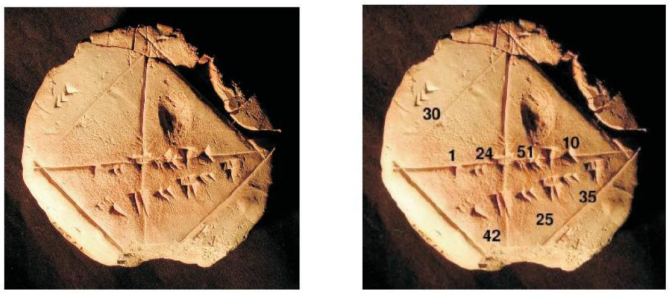
Fonte: ([28], p.2)

Demonstração: Conforme a (Figura 12) o ângulo AEB está inscrito em um semicírculo, logo é um ângulo reto. Portanto os ângulos AEC e CEB são complementares, assim também como os ângulos AEC e EAC, CEB e EBC, logo $EAC = CEB$, $EBC = AEC$ (têm o mesmo complemento) e $\Delta ACE \sim \Delta ECB$ (caso de semelhança AA). Podemos concluir que $\frac{AC}{CE} = \frac{EC}{BC}$ ou $AC \times BC = (EC^2)$, como $AC = x$, $BC = 1$, temos que $EC = \sqrt{x}$.

■

Na Mesopotâmia alguns séculos a.C. os mesopotâmios já faziam aproximações de raízes quadradas de números que não eram quadrados perfeitos. Inscrições relativas as raízes quadradas foram encontradas em pequenas tábuas de argila, como na tábua YBC7289 da coleção da Universidade de Yale (*Yale Babylonian Collection*)

Figura 13 - Tábula YBC 7289



Fonte: http://www.bibnum.education.fr, acesso em 17. abr. 2015.

Como o sistema de numeração dos Mesopotâmios era sexagesimal, ou seja, de base 60, então nesta tábua está inscrito um quadrado com lado 30 e no seu interior estão os dois números:

$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}$ e $42 + \frac{25}{60} + \frac{35}{60^2}$, Como

$$30 \times \left(1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}\right) = 42 + \frac{25}{60} + \frac{35}{60^2}$$

Concluímos que $1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}$ é uma aproximação da diagonal de um quadrado de lado 1.

Sabemos que a medida da diagonal de um quadrado de lado 1 é $\sqrt{2}$ e

$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} \approx 1{,}4142129663$, portanto os Mesopotâmios já faziam aproximações para $\sqrt{2}$.

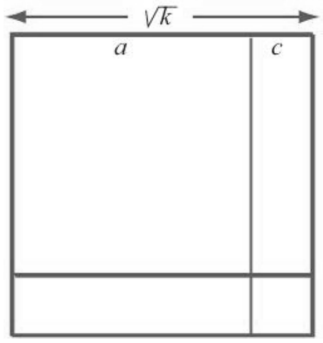
O algoritmo que os Mesopotâmios usavam para obter esta aproximação não é conhecido, porém o historiador Victor Katz propôs uma explicação plausível, baseando-se em

inscrições que figuram em algumas tábuas, afirmando que trata de um método para o qual existe alguma evidência textual (KATZ apud [15],p.3)

3.4.1 Algoritmo mesopotâmico para o cálculo do valor de $\sqrt{k}$

O cálculo de $\sqrt{k}$ pode ser interpretado como encontrar a medida do lado de um quadrado que tem área *k*. O que supõe-se que os mesopotâmios faziam era tentar colocar no interior deste quadrado o maior quadrado possível cujo lado seja um valor conhecido, já que eles possuíam numerosas tábuas contendo números elevados ao quadrado.

Figura 14 - Algoritmo mesopotâmico para calcular o valor de √k



Fonte: ([28], p.11)

Chamando de a o lado do quadrado conhecido e c o comprimento do segmento que falta para obter $\sqrt{k}$, conforme a (Figura 14), temos que $a + c = \sqrt{k}$.

Devemos determinar um valor a' mais próximo de $\sqrt{k}$, que é o mesmo que encontrar um valor bem próximo de c, que pode ser feito analisando a região em forma de << L >> invertido ao redor do quadrado de lado a, região que era chamada pelos antigos gregos de *gnómon*, uma analogia ao relógio de sol ou ainda com um esquadro.

A área do *gnómon* é dada por $k - a^2$, área do quadrado de lado $\sqrt{k}$ menos a área do quadrado de lado a, observemos também que a área deste *gnómon* é $2ac + c^2$, pois é composto por dois retângulos de lados a e c mais um quadrado de lado c, logo,

$$2ac + c^2 = k - a^2$$

Fazendo c bastante pequeno, podemos desprezar c^2, pois a área do quadrado menor será próxima a zero, obtendo a aproximação:

$$2ac' \approx k - a^2$$

$$c' \approx \frac{k - a^2}{2a}$$

Portanto, uma boa aproximação para $\sqrt{k}$ (em relação ao valor inicial a) é obtida tomando para a aproximação de $a + c$ o valor:

$$a' = a + \frac{k - a^2}{2a}$$

$$a' = a + \frac{k - a^2}{2a} = \frac{a^2 + k}{2a}$$

■

Observemos que para $c' = \frac{k-a^2}{2a}$ a aproximação $c' \approx c$ é uma aproximação por excesso $(c' > c)$, pois a expressão $2ac'(\approx)k - a^2$, informa que dois retângulos de lados a e c' têm a mesma área do *gnómon*, fazendo com que o valor de c' seja superior ao valor de c, então $a' = a + c'$, resulta numa aproximação por excesso $(a' > \sqrt{k})$, que também pode ser verificado elevando ao quadrado cada um dos membros da desigualdade.

Como $a' = \frac{a^2+k}{2a}$, então, $a'^2 - k = \frac{a^4+2a^2k+k^2-4a^2k}{4a^2} = \frac{(a^2-k)^2}{4a^2}$, portanto, $a'^2 - k > 0$, pois o numerador e o denominador $\frac{(a^2-k)^2}{4a^2}$, são estritamente positivos.

Este algoritmo pode ser reescrito, obtendo uma fórmula de aproximação bastante conhecida na Matemática. Fazendo $b = k - a^2$, que é a diferença entre as áreas dos quadrados de lados $\sqrt{k}$ e a, ou seja, área do *gnómon*. Obtemos:

k = *área do quadrado de lado* a *mais área do gnómon*, então:

$$\sqrt{k} = a + c$$

$$\sqrt{k} \approx a + \frac{k - a^2}{2a}$$

$$\sqrt{a^2 + b} \approx a + \frac{b}{2a}$$

■

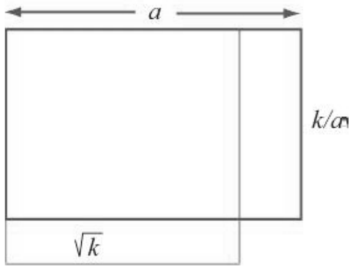
Podemos também fazer outra simplificação na fórmula mesopotâmica obtendo assim uma nova interpretação geométrica para o cálculo de $\sqrt{k}$.(cf.[15], p.5) Fazendo,

$$a + \frac{k - a^2}{2a} = \frac{1}{2}(a + \frac{k}{a})$$

Obtemos a média aritmética dos números a e $\frac{k}{a}$, então a determinação do quadrado com área k pode ser obtido substituindo este quadrado por um retângulo de lados a e $\frac{k}{a}$,

também com área *k*, este retângulo representa uma aproximação do quadrado com a mesma área.

Figura 15 - Algoritmo mesopotâmico para calcular o valor de √k



Fonte: ([28], p.15)

A média aritmética, $a' = \frac{1}{2}(a + \frac{k}{a})$ dos dois lados desse retângulo, *a'*, representa uma melhor aproximação do lado do quadrado, conforme ilustrado na figura acima, tem-se por um lado $a' < a$, (pois a média está situada entre os valores a e $\frac{k}{a}$, com $\frac{k}{a} < a$) e por outro lado, conforme já foi visto, *a'* é sempre maior do que $\sqrt{k}$. Portanto $\sqrt{k} < a' < a$, sendo que a aproximação *a'* é a mais próxima de $\sqrt{k}$ do que *a*.

Este método também pode ser reinterpretado relacionando a média geométrica e a média aritmética, ou seja, a aproximação da raiz quadrada de um número *k*, conforme a (Figura 15), pode ser dada pela média geométrica dos números $a\ e\ \frac{k}{a}$, através da média aritmética destes números.

Pode-se também envolver a média harmônica, agora considerando um novo retângulo também de área *k*, mas com lados, $a' e\ \frac{k}{a'}$. Fazendo $a' > \sqrt{k}$ temos que:

$\frac{k}{a'} < \sqrt{k} < a'$, esta desigualdade decorre de $a' . \frac{k}{a'} = k$, a raiz quadrada do produto de dois fatores, está situada entre esses fatores. Assim, obtemos:

$$\frac{k}{a'} = \frac{k}{\frac{1}{2}(a + \frac{k}{a})} = \frac{2(a\frac{k}{a})}{a + \frac{k}{a}}$$

Sendo esta última expressão a média harmônica dos números $a\ e\ \frac{k}{a}$.

Desigualdades MH-MG-MA

Dados dois números reais não negativos u e v, tem-se que:

$$\frac{2uv}{u + v} \leq \sqrt{uv} \leq \frac{1}{2}(u + v)$$

Aplicando esta desigualdade no caso estudado, temos:

$$\frac{2(a\frac{k}{a})}{a+\frac{k}{a}} \leq \sqrt{a\frac{k}{a}} \leq \frac{1}{2}(a+\frac{k}{a}) \rightarrow \frac{k}{a'} \leq \sqrt{k} \leq a'$$

Ocorrendo a igualdade quando $a = \frac{k}{a}$

Portanto, não apenas o lado a', do novo retângulo de aproximação é superior a $\sqrt{k}$, mas o seu outro lado $\frac{k}{a'}$ é inferior a $\sqrt{k}$, como a' é a média aritmética entre $\frac{k}{a'}$ e a, o ponto a' situa-se precisamente no meio do intervalo, separando estes dois pontos. O valor procurado, $\sqrt{k}$, encontra-se na metade esquerda deste intervalo. O mesmo acontece nas etapas de aproximações seguintes.

Este método de aproximar a raiz quadrada é por vezes chamado de *método da média aritmética-harmônica*. ([15],p.8)

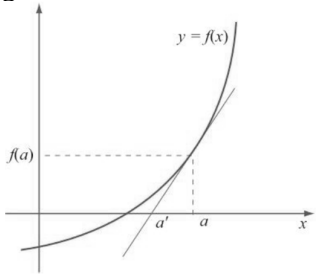
3.4.2 O método de Newton-Raphson

Este método foi introduzido por Isaac Newton em cerca de 1670 e em 1690 simplificado pelo seu colega Joseph Raphson nas fórmulas iterativas que se usam hoje em dia. (cf.[15], p.15)

Algebricamente $\sqrt{k}$ é a solução da equação $x^2 - k = 0$. O algoritmo de Newton-Raphson centra-se na procura dos zeros da função f, tal que $f(x) = x^2 - k$, ou seja, determinar os valores da variável x que são raízes da equação $f(x) = 0$, porém envolve conhecimento de derivadas, tópico estudado em cálculo diferencial.

Seja $f(x) = x^2 - k$. Este algoritmo consiste em tomar um valor arbitrário a, bem próximo da raiz procurada, (esse valor existe, pois $k > 0$ e a função f é contínua e derivável) e em seguida tomar como aproximação desta raiz o ponto a' resultante da intersecção com o eixo x da tangente à curva no ponto $f(a)$.

Figura 16 – Método de Newton - Raphson



Fonte: ([15], p.16)

Sendo que o declive desta tangente se exprime, através da função derivada *f*, na forma:

$$f'(a) = \frac{f(a)}{a - a'}, então\ a' = a - \frac{f(a)}{f'(a)}$$

Portanto a ideia é proceder por aproximações sucessivas, obtendo assim uma sucessão de valores $a_1, a_2, a_3, ...$, que se aproximam cada vez mais do zero da função *f*.

Observação: A derivada $f'(a)$ é a inclinação da reta tangente ao gráfico da função no ponto a. Se o ponto a está localizado nos pontos de inflexão, máximos ou mínimos, a derivada da função tende a zero e é por esse motivo que o Método de Newton-Raphson não converge se $f'(a)$ tende a zero.

Aplicando a relação que exprime a' na função $f(x) = x^2 - k$ obtem-se

$$a' = a - \frac{a^2 - k}{2a} = \frac{1}{2}(a + \frac{k}{a})$$

Isso nos traz de volta à fórmula mesopotâmica já estudada.

Exemplo: Aproximar √3 pelo Método de Newton-Raphson, com precisão de $\varepsilon = 1 \times 10^{-4}$. O erro $E = |(a_n)^2 - k|$.

Como queremos encontrar uma aproximação para √3, fazemos:

$$x = \sqrt{3}$$

$$x^2 = 3$$

Logo:

$$f(x) = x^2 - 3$$

$$f'(x) = 2x$$

A raiz quadrada de 3 está situada entre 1 e 2. Desta forma, tomaremos como uma aproximação inicial $a_0 = 1{,}5$. Então:

$$a_1 = a_0 - \frac{f(a_0)}{f'(a_0)}$$

$$a_1 = 1{,}5 - \frac{f(1{,}5)}{f'(1{,}5)}$$

$$a_1 = 1{,}5 - \frac{-0{,}75}{3}$$

$$a_1 = 1{,}75$$

Como $E = |1{,}75^2 - 3| > 10^{-4}$, continuamos as iterações:

$$a_2 = a_1 - \frac{f(a_1)}{f'(a_1)}$$

$$a_2 = 1{,}75 - \frac{f(1{,}75)}{f'(1{,}75)}$$

$$a_2 = 1{,}75 - \frac{0{,}0625}{3{,}5}$$

$$a_2 = 1{,}732142857$$

Como $E = |1{,}732142857^2 - 3| > 10^{-4}$, continuamos as iterações:

$$a_3 = a_2 - \frac{f(a_2)}{f'(a_2)}$$

$$a_3 = 1{,}732142857 - \frac{f(1{,}732142857)}{f'(1{,}732142857)}$$

$$a_3 = 1{,}732142857 - \frac{0{,}000318877056}{3{,}464285714}$$

$$a_3 = 1{,}73205081$$

Como $E = |1{,}73205081^2 - 3|$ menor que 10^{-4} paramos as iterações e tomamos a_3 como um valor aproximado da $\sqrt{3}$.

3.5 ALGORITMOS PARA RESOLUÇÃO DA EQUAÇÃO DO 2º GRAU

Vimos que o método de Newton-Raphson para extração de raízes quadradas utiliza a equação $x^2 - k = 0$, analisaremos agora como se deu a história das equações desse tipo.

3.5.1 Método Egípcio

Os mais importantes documentos deixados pelos egípcios até hoje conhecidos que comprovam o conhecimento matemático que utilizavam naquela época (4000 a.C à 30 a. C),

foram os Papiros de Kahun, de Berlim, de Moscou e o Papiro Rhind, descobertos no século XIX em escavações no Egito.

> O papiro matemático de Rhind é uma cópia de um trabalho ainda mais antigo. Foi copiado por um escriba (escriturário egípcio) chamado Ahmes em escrita hierática, por volta de 1650 a.C, e por esse motivo também é referenciado por Papiro de Ahmes. O papiro foi adquirido por Alexander Henry Rhind em Luxor, Egito, em 1858. O museu britânico incorporou-o ao seu patrimônio em 1865, após a morte de Rhind, permanecendo em seu acervo até os dias atuais. [9]

No Papiro de Berlim foi encontrada a resolução de uma equação escrita hoje na forma $x^2 + y^2 = k$, k um número positivo, pelo **método da falsa posição** desenvolvido pelos egípcios para resolver equações do 1º grau.

> Os problemas egípcios descritos até agora são de tipo digamos, aritmético, mas há outros que merecem a designação de algébricos. Não se referem a objetos concretos específicos, como pães e cerveja, nem exigem operações entre números conhecidos. Em vez disso, pedem o que equivale a soluções de equações lineares, da forma ou, onde são conhecidos e *x* é desconhecido. A incógnita é chamada de "*aha*". O Prob. 24, por exemplo, pede o valor de *aha*, e as operações indicadas à esquerda do sinal de igualdade são efetuadas sobre esse número suposto. O resultado é então comparado com o resultado que se pretende, e usando proporções chega-se à resposta correta. No problema 24 o valor tentado para a incógnita é 7, de modo que $x + \frac{1}{7}x$ é 8 em vez de 19 como se queria. Como $8\left(2 + \frac{1}{4} + \frac{1}{8}\right) = 19$, deve-se multiplicar 7 por $2 + \frac{1}{2} + \frac{1}{8}$ para obter a resposta: Ahmes achou $16 + \frac{1}{2} + \frac{1}{8}$. Então conferiu a resposta mostrando que se a $16 + \frac{1}{2} + \frac{1}{8}$ somarmos um sétimo disto (que é $2 + \frac{1}{2} + \frac{1}{8}$) de fato obteremos 19. Aqui notamos outro passo significativo no desenvolvimento da Matemática, pois a verificação é um exemplo simples de prova. ([4], p.12).

Exemplo de um problema retirado do Papiro de Berlim

A soma das áreas de dois quadrados é 100 unidades. O triplo do lado de um deles é o quádruplo do lado do outro. Encontre os lados desse quadrado.

Na simbologia atual representamos algebricamente o problema da seguinte forma:

$x^2 + y^2 = 100$ (1) $\qquad\qquad$ $y = \frac{4}{3}x$ (2)

Usando o algoritmo da falsa posição procedemos da seguinte forma:

1. Tome $x = 3$, então, $y = 4$
2. Assim, $3^2 + 4^2 = 25, mas\ (25 \neq 100)$
3. Para obter a soma 100, basta multiplicar ambos os membros por 4,

4. $x^2 = 4.3^2; y^2 = 4.4^2$
5. $x^2 + y^2 = 36 + 64 = 100$ *e* $4x = 4.6 = 24; 3y = 3.8 = 24$.
6. Os lados são 6 *e* 8. (Papiro de Berlim)

3.5.2 Método Babilônico

Já os babilônios enunciavam a equação e sua resolução através de palavras, a solução era apresentada como uma "receita matemática" registrada num tijolo de argila. O primeiro registro de problemas envolvendo equações do 2º grau pelos babilônios data de 1700 a.C. Segue um exemplo de como o problema era resolvido.

Exemplo: Qual o lado de um quadrado em que a área menos o lado dá 870?

(Na forma atual: $x^2 - x = 870$; onde *x* representa o lado do quadrado).

Pela "receita" dos babilônios segue:

Tome a metade de *1 (coeficiente de x)* e multiplique por ela mesma *(0,5 .0,5 = 0,25)*. Some o resultado a *870 (termo independente)*. Obtém-se um quadrado ($\sqrt{870{,}25} = 29{,}5$), cujo lado somado à metade de *1 vai dar 30*, o lado do quadrado procurado.

Há cerca de 2000 a.C. escritos achados revelam que os sábios Babilônios sabiam resolver problemas que pediam para achar dois números cujo seu produto, soma ou diferença eram dados. Portanto os Babilônios podiam resolver sistemas de equações com duas variáveis:

$$x + y = p$$
$$xy = q$$

Ou seja, tinham conhecimento da resolução da *equação quadrática* $\boldsymbol{x^2 + q = px}$

Pela análise do problema citado acima (cf [4], p.24) segue abaixo os passos que os Babilônios usavam para resolver *equação quadrática* $\boldsymbol{x^2 + q = px}$

1. Tomar a metade de p:

$$\frac{p}{2} = \frac{x + y}{2}$$

2. Elevar ambos os membros ao quadrado:

$$(\frac{p}{2})^2 = (\frac{x + y}{2})^2$$

3. Subtrair q do resultado obtido:

$$(\frac{p}{2})^2 - q = \left(\frac{x+y}{2}\right)^2 - xy$$

$$(\frac{p}{2})^2 - q = \left(\frac{x-y}{2}\right)^2$$

4. Tomar a raiz quadrada do resultado obtido:

$$\sqrt{(\frac{p}{2})^2 - q} = \frac{x-y}{2}$$

5. Somar a metade de p ao resultado:

$$\frac{p}{2} + \sqrt{(\frac{p}{2})^2 - q} = \frac{x-y}{2} + \frac{x+y}{2}$$

$$\frac{p}{2} + \sqrt{(\frac{p}{2})^2 - q} = x$$

O resultado obtido (x) é um dos números desejados o outro é a diferença deste para p, portanto:

$$p - x = (x+y) - x = y$$

Os números procurados são:

$$\frac{p}{2} + \sqrt{(\frac{p}{2})^2 - q} = \frac{p + \sqrt{p^2 - 4q}}{2}$$

E

$$p - (\frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}) = \frac{p - \sqrt{p^2 - 4q}}{2}$$

Que está de acordo com as formulas que hoje utilizamos para resolver a *equação quadrática* $\boldsymbol{x^2 + q = px}$.

Os Babilônios não conheciam os números negativos, estes números ainda não tinham sido incluídos em sua aritmética.

> "Até os tempos modernos não havia ideia de resolver uma equação quadrática da forma $x^2 + px + q = 0$, onde p e q são positivos, pois a equação não tem raiz positiva. Por isso as equações quadráticas na antiguidade e na Idade Média, e mesmo no começo do período moderno, foram classificadas em três tipos 1) $x^2 + px = 0$, 2) $x^2 = px + q$ e 3) $x^2 = px + q$. Todos esse tipos são encontrados em textos do período Babilônio antigo, de uns 4000 anos atrás."([4], p. 23)

3.5.3 Solução apresentada pelos gregos

Os matemáticos gregos desenvolveram um tratamento geométrico para muitos problemas matemáticos, talvez pela dificuldade que tinham com os números racionais e irracionais, pela falta de praticidade do sistema de numeração grego, que usava seu alfabeto ou mesmo por uma afeição natural que tinham pela geometria.

Em "Os Elementos" de Euclides encontram-se algumas proposições que tratam da solução de equações do 2º grau geometricamente.

O livro II apresenta na proposição 11:

"Dividir um segmento de reta dada de maneira que o retângulo determinado pelo todo e por uma das partes tenha área igual à do quadrado sobre a outra parte"

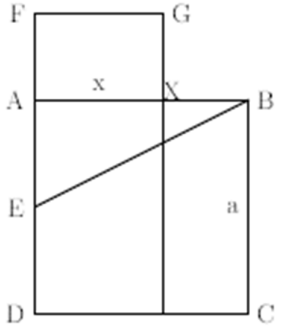
Seja $AB = a$ o segmento dado, o objetivo é encontrar um ponto por X neste segmento de modo que $(AB).(XB) = (AX)^2$, ou seja, dado um segmento de reta AB, deve-se determinar um ponto X nesse segmento tal que o retângulo de lados AB e XB tenha a mesma área do quadrado de lado AX

Ou ainda se $AB = a$ e $AX = x$ temos:

$$a(a - x) = x^2 \Leftrightarrow x^2 + ax = a^2$$

Portanto, esta proposição traz uma abordagem geométrica para resolução da equação de 2º grau do tipo $x^2 + ax = a^2$.

Figura 17 – Resolução de Euclides para equação de 2º grau do tipo $x^2 + ax = a^2$.



Fonte: Revista Eletrônica de Matemática (REMat, n.2 – 2010, p.5)

Segue abaixo os passos da solução de Euclides, de forma simplificada e na notação atual.

1. Construir o quadrado $ABCD$ sobre o segmento AB;
2. Tomar o ponto médio, E, de AD;

3. Tomar F sobre o prolongamento de DA de maneira que $EF=EB$
4. Construir o quadrado sobre o lado AF
5. O vértice X desse quadrado, pertencente ao segmento AB é a solução do problema.

   Vejamos:

$AE = \frac{1}{2}AD = \frac{1}{2}a$. Portanto, no triangulo ABE tem-se $EB = \sqrt{a^2 + (\frac{a}{2})^2} = \frac{a\sqrt{5}}{2}$.

Portanto, $x = AX = AF = EF - EA = EB - EA = \frac{a\sqrt{5}}{2} - \frac{a}{2} = \frac{a(-1+\sqrt{5})}{2}$ é a raiz positiva de $x^2 + ax = a^2$, denominado número áureo, que é a medida do segmento AX. ([22], p.5)

Euclides contribui significativamente não apenas para resolução de equações do 2º grau, ele deixou um grande legado para a Matemática em suas obras. Ainda em "Os Elementos" podemos destacar o livro VI com algumas proposições que apresentam a resolução geral das equações do 2º grau de forma geométrica.

3.5.4 Solução apresentada pelos hindus

Dentre os matemáticos hindus destacam-se Aryabhata (476-550), Brahmagupta (séc. VII d.C.), Sridhara (séc. XI d.C.) e Bhaskara (1114-1185) que aperfeiçoaram os métodos de resolução das equações de 2º grau desenvolvidos pelos babilônios e gregos.

Segue abaixo a solução dada por Brahmagupta para solução das equações do tipo: $ax^2 + bx = d$, ([7], p.14)

1. A soma é multiplicada pelo coeficiente do quadrado, você adiciona o quadrado da metade do coeficiente da incógnita;

$$x^2 = a.d + \left(\frac{b}{2}\right)^2$$

2. Em seguida extrai a raiz quadrada

$$x = \sqrt{a.d + (\frac{b}{2})^2}$$

3. A metade do coeficiente da incógnita é subtraída;

$$x = \sqrt{a.d + (\frac{b}{2})^2} - \frac{b}{2}$$

4. Divide pelo coeficiente do quadrado

$$x = \frac{\sqrt{a.d + (\frac{b}{2})^2} - \frac{b}{2}}{a}$$

5. Portanto a equação final;

$$x = \frac{\sqrt{4a.d + b^2} - b}{2a}$$

Bhaskara foi outro matemático hindu que deu contribuições significativas para a resolução da equação de 2º grau. Ele costumava chamar a Álgebra de a arte dos raciocínios perfeitos. Resolveu equações do tipo $ax^2 + bx = c$, utilizando o método de completar quadrados.

Vejamos um exemplo de um problema da época de Bhaskara; a oitava parte de um bando de macacos, elevada ao quadrado, brinca em um bosque. Além disso, 12 macacos podem ser vistos sobre uma colina. Qual o total de macacos? ([7], p.15)

$$(\frac{x}{8})^2 + 12 = x$$

$$\frac{x^2}{64} + 12 = x$$

As soluções são: $x_1 = 48 \; e \; x_2 = 16$

O matemático hindu S'ridhara (?850-950? d.C.) foi quem primeiro enunciou a regra hindu que originou a fórmula atual para a resolução de equações de 2º grau. Aqui no Brasil ela é conhecida como "Fórmula de Bhaskara".

"É por unidades iguais a quatro vezes o número de quadrados que é preciso multiplicar os dois membros; e é a quantidade igual ao quadrado do número primitivo de quantidades desconhecidas simples que é preciso adicionar" ([26], p.240)

Seja a equação $ax^2 + bx = c$

1. Multiplicando ambos os membros por $4a$, obtemos:

$$4a^2x^2 + 4abx = 4ac$$

2. Somando a ambos os membros o quadrado do coeficiente da quantidade desconhecida:

$$4a^2x^2 + 4abx + b^2 = 4ac + b^2 \Leftrightarrow (2ax + b)^2 = b^2 + 4ac$$

3. Extraindo a raiz quadrada temos

$$2ax + b = \sqrt{b^2 + 4ac}$$

Chegando a uma equação do primeiro grau, cuja solução já era conhecida.

Observemos que a raiz negativa não era considerada.

3.5.5 Solução apresentada pelos árabes

No califado al-Mamum foi fundada em Bagdad uma academia de ciência chamada "Casa da Sabedoria" comparada ao antigo museu de Alexandria, o trabalho inicial desta comunidade consistia em estudar obras da antiguidade e traduzi-las para o árabe. Segundo (Boyer p.165), sob o comando dos califas – Al-Mansur, Harum al-Rachid e al-Mamum durante a segunda metade do oitavo século, devido ao ambiente favorável para o estudo da Matemática e da Astronomia, Bagdad tornou-se um centro de atração para profissionais destas duas áreas de conhecimento, reunindo ainda numerosos tradutores vindos de diferentes cidades do mundo.

Com a criação da Casa da Sabedoria surgiram as bases para o desenvolvimento da álgebra. Entre os que mais contribuíram destaca-se Al-Khowarizmi, considerado por muitos como o "Pai da álgebra" ([2], p.45)

> O matemático árabe de maior importância foi Mohamed-ibu-Musa Al-Khowarizmi (780-850 d.C), que foi membro da "Casa da Sabedoria", e o responsável pelo apogeu das atividades islâmicas nas ciências exatas. Realizou estudos também em outras áreas como, geografia, astronomia, aritmética e também introdutor de métodos hindu no mundo islâmico, o que mostra sua ligação com os indianos. ([7], p.16)

Foi Al-Khowarizmi quem introduziu equações para resolver problemas, sendo aceitas somente as de coeficientes e soluções positivas. Escreveu, entre 813 e 833 sua principal obra *Al Kitab al-muhtasar fi hisab al-jabar wa al-mukabala,* cuja tradução é *Breve tratado sobre o cálculo [para o processo] de restauração e comparação.*

Al-Khowarizmi estudou seis tipos de equações:

Equações simples

1º tipo: quadrados iguais a raízes, $ax^2 = bx$

2º tipo: quadrados iguais a números, $ax^2 = c$

3º tipo: raízes iguais a números, $ax = b$

Equações combinadas

4º tipo: raízes e quadrados iguais a números, $x^2 + px = q$

5 º tipo: quadrados e números iguais a raízes, $x^2 + q = px$

6º tipo: raízes e números iguais a quadrados, $px + q = x^2$

Análise de Al-Khowarizmi para equações do 2º grau:([2], p.50)

1º TIPO: quadrados iguais a raízes, $ax^2 = bx$

Vejamos um exemplo: Um quadrado é igual a cinco das suas raízes. A raiz do quadrado é 5 e 25 constitui o próprio quadrado, que é evidente igual a 5 vezes a sua raiz.

Outro exemplo: Um terço de um quadrado é igual a quatro vezes a raiz. A raiz do quadrado é 12, e 144 é o número que corresponde ao próprio quadrado.

Representado os exemplos na simbologia atual temos:

$$x^2 = 5x \Leftrightarrow x = 5 \Leftrightarrow x^2 = 25$$

$$\frac{x^2}{3} = 4x \Leftrightarrow x^2 = 12x \Leftrightarrow x = 12 \Leftrightarrow x^2 = 144$$

Caso Geral: $ax^2 = bx \Leftrightarrow x^2 = \frac{b}{a}x \Leftrightarrow x = \frac{b}{a} \Leftrightarrow x^2 = (\frac{b}{a})^2$

Notemos que a solução nula era ignorada.

2º TIPO: quadrados iguais a números, $ax^2 = c$

Exemplos:

Um quadrado é igual a 9. O número 9 dá a área de um quadrado, daí que o número 3 seja a raiz.

Cinco quadrados são equivalentes a 80. Daí que um quadrado corresponda a uma quinta parte do número 80, que é evidentemente 16.

A metade de um quadrado é equivalente a 18. O quadrado inteiro vale, portanto 36.

Na simbologia atual:

$$x^2 = 9 \Leftrightarrow x = 3$$

$$5x^2 = 80 \Leftrightarrow x^2 = \frac{80}{5} \Leftrightarrow x^2 = 16$$

$$\frac{1}{2}x^2 = 18 \Leftrightarrow x^2 = 36 \Leftrightarrow x = 6$$

Caso Geral: $ax^2 = c \Leftrightarrow x^2 = \frac{c}{a} \Leftrightarrow x = \sqrt{\frac{c}{a}}$

Notemos que a raiz negativa não era considerada.

3º TIPO: raízes iguais a números, $ax = b$

Exemplos:

Uma raiz é igual a 3. Daí que o número 9 seja o quadrado dessa raiz.

Quatro raízes iguais a 20. Então a raiz desse quadrado será igual a 5.

A metade de uma raiz é igual a 10. A raiz inteira é portanto igual a 20, daí que, é evidente que 400 represente o quadrado.

Na simbologia atual:

$$x = 3 \Leftrightarrow x^2 = 9$$

$$4x = 20 \Leftrightarrow x = 5 \Leftrightarrow x^2 = 25$$

$$\frac{1}{2}x = 10 \Leftrightarrow x = 20 \Leftrightarrow x^2 = 400$$

Caso geral: $ax = b \Leftrightarrow x = \frac{b}{a} \Leftrightarrow x^2 = (\frac{b}{a})^2$

Uma vez que nas equações do 1º tipo, a solução nula era ignorada, as equações do 3º tipo têm uma resolução equivalente às do 1º tipo.

Vejamos agora os algoritmos usados por Al-Khowarizmi para os três tipos de equações combinadas.

4º TIPO: raízes e quadrados iguais a números, $x^2 + bx = c$

> Quando os tesouros e as raízes são iguais a um número, é como quando tu dizes: um tesouro e dez das suas raízes são iguais a trinta e *nove* dinheiros. O seu significado é que ao teu bem, se lhe juntares o equivalente a dez das suas raízes, atinge trinta e nove. O processo [de resolução] consiste em dividir as raízes por dois, que é cinco neste problema. Multiplica-lo por si próprio que dá vinte e cinco. Junta o que obtiveste aos trinta e nove. Isso dará sessenta e quatro. Tomas então a sua raiz quadrada que é oito e retiras-lhe a metade [do número] das raízes *que* são cinco. Resta três que é a raiz do bem que tu procuras e o bem é nove. ([2] p. 55)

Este problema reduz-se à resolução da equação $x^2 + 10x = 39$.

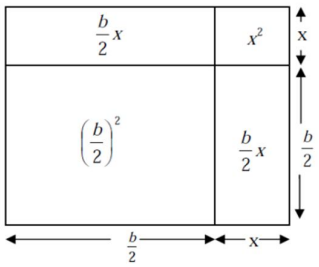
O algoritmo usado por Al-Khowarizmi foi $x = \sqrt{(\frac{10}{2})^2 + 39} - \frac{10}{2} = 3$ que no caso geral corresponde a $x = \sqrt{(\frac{b}{c})^2 + c} - \frac{b}{2}$

A justificativa geométrica dada por Al-Khowarizmi decorre exatamente com a que está representada no livro II, dos Elementos de Euclides, no entanto ele não é mencionado pelo autor árabe. ([19]. p,18)

Considere um quadrado de lado *x*, com área igual a x^2. Some dois retângulos, tendo cada um deles os lados $\frac{b}{2}$ e *x*. A área dos retângulos somada a área do quadrado menor é igual a $x^2 + 10x$. Assim o quadrado menor terá lado 5 e área 25.

Ao completar o quadrado de lado x, obtemos um quadrado maior com área expressa por $x^2 + 2(5x) + 25$. Somando as áreas dos quadrados, temos $39 + 25 = 64$, então $x^2 + 10x + 25 = 64$. Portanto o lado do quadrado maior será $(x + 5)^2 = 64 \Leftrightarrow x = 3$

Figura 18 - Demonstração de Al-Khowarizmi



Fonte: ([19], p.18)

5 º TIPO: quadrados e números iguais a raízes, $x^2 + q = px$

> Quando os quadrados e os números são iguais às raízes é como quando tu dizes: Um quadrado e vinte e um em número é igual a dez das suas raízes. Isto vale também para o teu bem, que é tal que se lhe juntares vinte e um dinheiros, a soma que daí resulta é igual a dez raízes desse bem. O método de resolução consiste no seguinte:
>
> Toma metade das raízes, isto é cinco. Multiplica-as por elas próprias, dá vinte e cinco. Retira-lhe os vinte e um que é o que nós dissemos que está junto do quadrado, restará quatro. Toma a sua raiz que é dois. Retira [esse valor] ã metade das raízes que são cinco. Restam três. Isso é a raiz do quadrado que tu procuras e o quadrado é nove.
>
> Se tu quiseres, junta a raiz (de quatro) à metade das raízes. Isso dá sete que é [também] a raiz do quadrado que tu procuras, e o quadrado é quarenta e nove. ([2], p.58)

Na linguagem atual o problema consiste na resolução da equação $x^2 + 21 = 10x$.

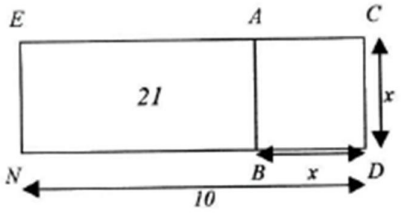
O algoritmo usado para resolver esta equação foi: $x = \frac{10}{2} - \sqrt{\left(\frac{10}{2}\right)^2 - 21} = 3 \Rightarrow x^2 = 9$, no caso geral temos: $x = \frac{p}{2} - \sqrt{\left(\frac{p}{2}\right)^2 - q}$.

Notemos que esta equação tem duas soluções positivas. Para obter a outra solução deve-se alterar a última operação para uma adição, portanto teremos o valor da segunda solução: $x = \frac{10}{2} + \sqrt{\left(\frac{10}{2}\right)^2 - 21} = 7 \Rightarrow x^2 = 49$. No caso geral corresponde a $x = \frac{p}{2} + \sqrt{\left(\frac{p}{2}\right)^2 - q}$.

Demonstração geométrica:

Al Khowarizmi representa a área do quadrado (x^2) por uma superfície quadrada com lado desconhecido. Em seguida, e sobre um dos lados do quadrado constrói um retângulo de área igual a 21. Pelas condições do problema $(x^2 + 21 = 10x)$, conclui-se que o comprimento desse retângulo tomado com o lado do quadrado inicial vale 10. Vejamos como fica a figura.

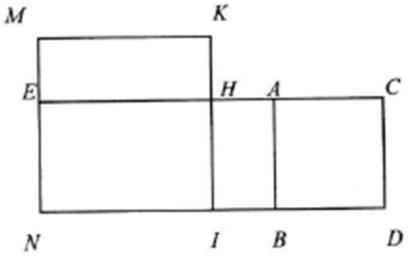
Figura 19 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.59)

Em seguida, Al Khowarizmi divide o segmento EC ao meio no ponto H, e constrói um quadrado sobre esse lado (o lado desse quadrado corresponde a metade do número de raízes).

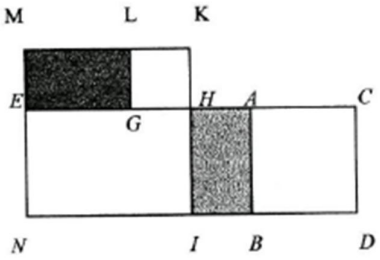
Figura 20 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.59)

Para concluir, constrói-se no canto superior direito de *NK* um quadrado sobre o lado *KH*, obtendo a figura:

Figura 21 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.59)

Demonstração:

Por construção temos que a área da figura AD é x^2, EB é 21. E pela equação $x^2 + 21 = 10x$ temos que a área de ED é $10x$ e, portanto o segmento $ND\ mede\ 10$. Como I é o ponto médio de $ND\ e\ NK$ é um quadrado, temos que a área de NK vale $\left(\frac{10}{2}\right)^2 = 5^2 = 25$.

Como por construção $MK = KI\ e\ KL = KH$, conclui-se que $ML = HI$. E como $EG = HI = AC\ e\ EH = HC, temos\ que\ LG = GH = HA$, portanto conclui-se que as áreas $MG\ e\ IA$ são iguais e:

$$área\ de\ GK = área\ de\ KN - (área\ de\ NH + área\ de\ MG)$$

$$área\ de\ GK = área\ de\ KN - (área\ de\ NH + área\ de\ IA)$$

$$área\ de\ GK = área\ de\ KN - área\ de\ EB$$

$$área\ de\ GK = 25 - 21 = 4$$

Então, podemos concluir que $HG = 2$. E como $HG = HA$ temos que:

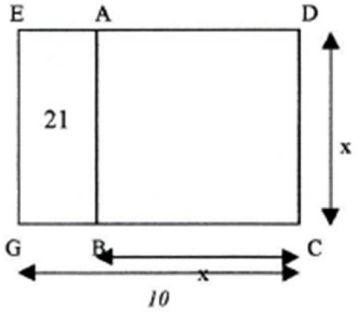
$x = CA = HC - HA = 5 - 2 = 3$. ■

Em relação a segunda solução da equação não foi encontrada qualquer demonstração nos manuscritos árabes de Al Khowarizmi que estão guardados em Oxford. Ela aparece na obra de um contemporâneo de Al Khowarizmi chamado Ibn Turk.

Demonstração em linguagem e simbologia atual:

De modo análogo ao caso anterior representa-se a área do quadrado por (x^2); constrói-se uma superfície quadrada seguida de um retângulo de área 21 em que um dos lados é o quadrado desenhado anteriormente (desta vez o retângulo será menor que o quadrado) tal que, o lado do retângulo juntamente com lado do quadrado mede 10 e a área da figura completa tem área $10x$.

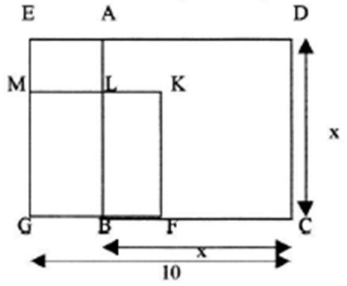
Figura 22 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.62)

Em seguida divide-se o segmento *CG* ao meio no ponto *F* e constrói-se um quadrado sobre o lado *GF*.

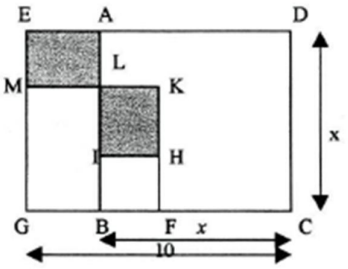
Figura 23 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.62)

Para terminar constrói-se um quadrado sobre *BF*, obtendo-se assim a figura pretendida:

Figura 24 - Demonstração de Al Khowarizmi para equações do tipo $x^2 + q = px$



Fonte: ([2], p.62)

Demonstração:

Por construção temos que a área de AC é x^2 e a de EB é 21. Temos também que *CG* é igual a 10 e com *F* é o ponto médio de *CG*, então, $GF = FC = 5$, logo a área de *GK* é igual $5^2 = 25$.

As superfícies *HL* e *LE* são iguais, pois por construção temos que:

$$KM = KF \; e \; FH = HI = KL, logo \; HK = LM \; e$$

$$AL = AB - BL, mas \; AB = BC \; e \; BL = FK = FC, então:$$

$AL = BC - FC = KL$, portanto como $HK = LM \; e \; AL = LK$ concluímos que *HL* e *LE* têm a mesma área e assim temos que:

$$área \; de \; IF = área \; de \; GK - (área \; de \; BM + área \; de \; HL)$$

$$área \; de \; IF = área \; de \; GK - (área \; de \; BM + área \; de \; LE)$$

$$área \; de \; IF = área \; de \; GK - área \; de \; EB)$$

$$área \; de \; IF = 25 - 21 = 4$$

Portanto, concluímos que $BF = 2$, logo, $x = CB = CF + FB = 5 + 2 = 7$. ■

6º TIPO: raízes e números iguais a quadrados, $px + q = x^2$

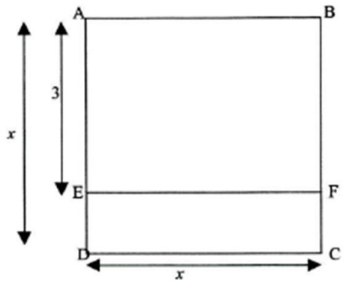
> Para equações deste tipo, propomos o seguinte: 3 raízes e 4 números são iguais a um quadrado. (...) Divide-se por 2 o número das raízes; obtém-se $1\,1/2$; multiplicamos de seguida esse número por ele próprio, faz $2\,1/4$. A esse número junta-se 4, faz $6\,1/4$. Extrai-se a raiz quadrada desse número; obtém-se $2\,1/2$. Junta-se essa raiz a metade do número das raízes, isto é $1\,1/2$, obtém-se 4, que corresponde à raiz do quadrado. O quadrado no seu conjunto vale 16. ([2], p.64)

O problema é expresso pela equação $3x + 4 = x^2$, que é do tipo $px + q = x^2$. O algoritmo apresentado foi $x = \sqrt{(\frac{3}{2})^2 + 4} + \frac{3}{2} = 4 \Longrightarrow x^2 = 16$, que no caso geral corresponde a $x = \sqrt{(\frac{p}{2})^2 + q} + \frac{p}{2}$

Demonstração:

Al Khowarizmi representa o quadrado (x^2), por uma superfície quadrada de lado desconhecido (x). Em seguida, divide esse quadrado em duas partes conforme a figura abaixo:

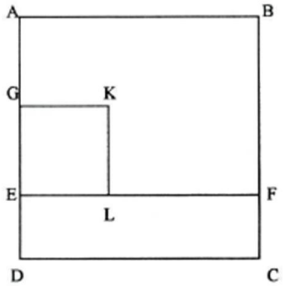
Figura 25 - Demonstração de Al Khowarizmi para equações do tipo $px + q = x^2$



Fonte: ([2], p.65)

Portanto temos que a área de EB vale $3x$ e pelas condições do problema conclui-se que a área de EC mede 4. Em seguida Al Khowarizmi divide o segmento AE ao meio no ponto G e faz um quadrado sobre o lado GE, vejamos:

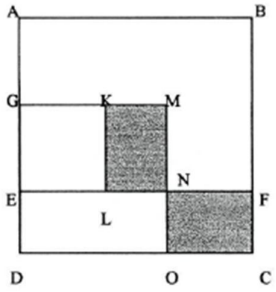
Figura 26 - Demonstração de Al Khowarizmi para equações do tipo $px + q = x^2$



Fonte: ([2], p.65)

Para obter a figura desejada constrói-se um outro quadrado (GO), sobre o lado GD.

Figura 27 - Demonstração de Al Khowarizmi para equações do tipo $px + q = x^2$



Fonte: ([2], p.65)

Demonstração na linguagem e simbologia atual:

Por hipótese e por construção temos que AC vale x^2, AF vale $3x$ e, consequentemente EC vale 4. Temos também que o segmento AE mede 3.

Como AC é um quadrado, vem que $AD = DC$. Como DM também é um quadrado, vem que $GD = DO$. Daí se conclui que $OC = AG$. Mas $AG = GE$ e $GE = KL$, portanto $OC = KL$. Como GO é um quadrado, vem que $GM = MO$. Como GL também é um quadrado, vem que $GK = GE$, que por sua vez é igual a MN, daí se tira que $KM = NO$.

Como as superfícies $KN\ e\ NC$ têm os mesmos comprimentos, são iguais. Então:

$$\text{área de } DM = \text{área de } GL + (\text{área de } DN + \text{área de } NK)$$
$$= \text{área de } GL + (\text{área de } DN + \text{área de } NC)$$
$$= \text{área de } GL + \text{área de } EC$$
$$= 2\,{}^{1}\!/_{4} + 4$$
$$= 6\,{}^{1}\!/_{4}$$

Então, $GD = 2\,{}^{1}\!/_{2} \rightarrow x = AD = AG + GD = 1\,{}^{1}\!/_{2} + 2\,{}^{1}\!/_{2} = 4$. ■

3.5.6 Solução apresentada pelos europeus a partir do séc. XVI

Foi a partir do século XII que o conhecimento matemático europeu iniciou seu desenvolvimento, destacando-se Leonardo de Pisa (1175-1250) mais conhecido por Fibonacci. Entre seus muitos escritos destaca-se a obra *Liber Abaci* (1202) que continha muita informação aritmética e algébrica do mundo de então. Nesta obra introduziu o sistema de numeração hindu-arábico. Discutiu também a base dez e o zero. Didático, ainda se preocupa

com o entendimento de seus leitores, proporcionando a solução de muitos problemas comuns a comerciantes, banqueiros e agiotas através de exemplos resolvidos em detalhes.

Fibonacci destacou em seu trabalho as três equações da obra de Al Khowarizmi $ax^2 + bx = c$, $bx + c = ax^2$, $ax^2 + c = bx$, mostrou as mesmas justificativas geométricas, mas discutiu outros exemplos próprios que o levaram utilizar números negativos e irracionais e também o zero como raiz da equação, tópicos que os árabes tinham deixado de fora.

Na obra *Liber Abaci* aparece o exemplo:

$$\left(1 + \frac{3}{4}x\right)\left(1 + \frac{2}{3}x\right) = 73$$

Na segunda metade do século XV, com a invenção da imprensa na Alemanha os estudos científicos passaram a ser cada vez mais produtivos devidos principalmente pelas traduções das obras gregas e árabes para o latim e sua divulgação impressa. Outra consequência dos livros impressos, que eram cada vez mais numerosos, foi o forte incentivo para que as pessoas aprendessem a ler, principalmente nas regiões onde os Protestantes eram mais numerosos. Isso facilitou a divulgação dos conhecimentos. Uma outra consequência menos mencionada foi o desenvolvimento de óculos para perto (presbiopia), pois até então não se percebia que a visão estava deficiente uma vez que ela não era tão solicitada a enxergar de perto. Isso fomentou o desenvolvimento acelerado da ótica e no final do século XVI apareceu o primeiro microscópio na Holanda. Dez anos depois, Galileu desenvolveu o primeiro telescópio (uma luneta, com aumento de 30 vezes). Com ela ele pode observar quatro dos satélites de Júpiter que giravam em torno deste planeta. Divulgou este conhecimento e fortaleceu o modelo solar de Copérnico, publicado em meados do século XV. Neste período histórico destaca-se o matemático francês François Viète (1540-1603) que entre as suas contribuições à álgebra figura a introdução sistemática das primeiras notações algébricas: adotou vogais para as incógnitas e consoantes para as grandezas conhecidas, Viète também contribuiu na resolução de equações quadráticas, cúbicas e quárticas.

O Método de Viète para resolução de equações do 2º grau: (cf [1], p.19)

Seja $ax^2 + bx + c = 0, \ com\ a \neq 0$.

Fazendo $x = u + v$, onde u e v são incógnitas auxiliares, substituindo na equação acima obtemos:

$$a(u + v)^2 + b(u + v) + c = 0$$

$$a(u^2 + 2uv + v^2) + b(u + v) + c = 0 \Leftrightarrow av^2 + (2au + b)v + au^2 + bu + c = 0$$

Fazendo $u = \frac{-b}{2a}$, Viète transforma numa equação incompleta do 2º grau:

$$av^2 + a(\frac{-b}{2a})^2 + b(\frac{-b}{2a}) + c = 0$$

Efetuando as operações obtém-se:

$$v^2 = \frac{b^2 - 4ac}{4a^2}$$

Se $b^2 - 4ac \geq 0$ então $v = \frac{\pm\sqrt{b^2-4ac}}{2a}$, portanto

$x = u + v = -\frac{b}{2a} \pm \frac{\sqrt{b^2-4ac}}{2a} = \frac{-b\pm\sqrt{b^2-4ac}}{2a}$,

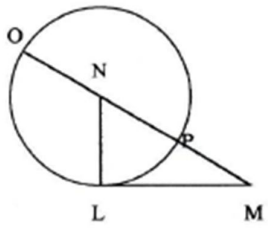
Hoje chamada fórmula de Bháskara.

René Descartes (1596-1650) também contribuiu para o estudo da resolução de equações do 2º grau. Segundo Boyer ([4], p.248), no terceiro volume (*La Geomètre)* da obra *O Discurso do Método,* Descartes solucionou geometricamente a equação do tipo $x^2 = bx + c^2$, com b e c positivos.

Método de Descartes para equações do tipo $\boldsymbol{z^2 = az + bb}$

> Constrói-se o triângulo NLM tal que LM seja igual a b, a raiz quadrada da quantidade conhecida bb e o [lado] LN seja $a/2$, a metade da outra quantidade conhecida, que está multiplicada por z que se supõe ser a linha desconhecida. Depois, prolonga-se MN, a base desse triângulo, até O, de modo que NO seja igual a NL; toda a linha OM é z, a linha procurada. Ela exprime-se desta forma:
> $z = \frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}$. (Descartes; Apud [2], p.104)

Figura 28 - Método de Descartes para equações do tipo $z^2 = az + bb$



Fonte: ([2], p.104)

Demonstração:

Por construção tem-se que $LM = b$ e que $LN = \frac{a}{2}$. Pela proposição III-36 dos Elementos de Euclides temos que $MP \times MO = (ML)^2$. Portanto

$$MP \times MO = (ML)^2$$
$$\Leftrightarrow (MO - a) \times MO = bb$$
$$\Leftrightarrow (MO)^2 - a \times MO = bb$$
$$\Leftrightarrow (MO)^2 = a \times MO + bb$$

Nesta última igualdade concluímos que MO satisfaz a equação $\boldsymbol{z^2 = az + bb}$, sendo, portanto solução da equação.

Para deduzirmos a expressão algébrica da solução $z = \frac{1}{2}a + \sqrt{\frac{1}{4}aa + bb}$, basta aplicarmos o Teorema de Pitágoras ao triângulo MNL. A solução obtém-se acrescentando à hipotenusa do triângulo MNL o raio da circunferência.

Outro matemático que contribuiu para a resolução de equações do 2º grau foi o britânico Colin MacLaurin, que nasceu na Escócia no ano de 1698 e faleceu no ano de 1746. Boyer ([4] p.315) classificou MacLaurin de "o mais importante matemático britânico da geração posterior a Newton".

A demonstração algébrica mais ensinada hoje em dia aos alunos do Ensino Básico é baseada na resolução que MacLaurin apresentou no seu livro *Álgebra*, publicado em 1748.

Vejamos tal resolução:

> Transportam-se todos os termos que contêm a incógnita para um membro da equação e todos os termos conhecidos para o outro.
> Se o quadrado da incógnita está multiplicado por alguma quantidade, dividem-se todos os termos da equação por essa quantidade.
> Forma-se o quadrado da metade da quantidade que multiplica a incógnita simples, juntando-se ambos os membros da equação e, nesse momento, um membro da equação será um quadrado perfeito.
> Tira-se a raiz quadrada de ambos os membros, e um membro será sempre a incógnita com a metade da quantidade que multiplica a incógnita simples, de modo que se transpusermos essa metade, teremos o valor da incógnita. ([2], p.108)

Exemplo: $x^2 + bx = c$

Juntamos o quadrado de $\frac{b}{2}$: $\rightarrow x^2 + bx + \frac{b^2}{4} = c + \frac{b^2}{4}$

Extraímos a raiz: $\rightarrow x + \frac{b}{2} = \pm\sqrt{c + \frac{b^2}{4}}$

Transpomos $\frac{b}{2}$: $\rightarrow x = \pm\sqrt{c + \frac{b^2}{4}} - \frac{b}{2}$

Como o lado de todo quadrado é expresso por um número positivo, então a raiz quadrada de uma quantidade negativa é imaginária, razão pela qual existem equações do 2º grau sem solução nos reais.

Vejamos um exemplo:

$$x^2 - bx = -3b^2$$

Juntamos o quadrado de $\frac{b}{2}$: $\rightarrow x^2 - bx + \frac{b^2}{4} = -3b^2 + \frac{b^2}{4} = -\frac{11a^2}{4}$

Extraímos a raiz: $\rightarrow x - \frac{b}{2} = \pm\sqrt{-\frac{11b^2}{4}} \Leftrightarrow x = \frac{b}{2} \pm \sqrt{-\frac{11b^2}{4}}$

Neste exemplo os dois valores de x são imaginários ou impossíveis nos reais, pois não podemos aceitar a raiz quadrada de $-\frac{11b^2}{4}$. (Cassinet, *Apud*.[2], p.110)

3.6 ALGORITMOS PARA O CÁLCULO DO MDC (Máximo Divisor Comum) E MMC (Mínimo Múltiplo Comum)

Problemas que envolvam o cálculo do máximo divisor comum entre dois números inteiros e a determinação dos números primos menores que um inteiro dado já era objeto de estudo das civilizações mais antigas, em os Elementos, escrito por Euclides por volta de 300 a.C esses problemas já eram tratados. Além de outros matemáticos destacaram-se na resolução destes problemas o matemático francês Pierre de Fermat (1601 – 1665), o Último Teorema de Fermat publicado pelo seu filho Clément-Samuel tem um enunciado extremamente simples, *"Não existe nenhum conjunto de inteiros positivos x, y, z e n com n maior que 2 que satisfaz a equação* $x^n + y^n = z^n$*"*, o matemático suíço Leonard Euler (1707 – 1783) sucessor de Fermat, desenvolveu algumas de suas ideias e refutou algumas de suas conjecturas e o matemático alemão Carl Friedrich Gauss (1777 – 1855) que com sua obra *Disquisitiones Arithmeticae*, publicada em 1801, teve início o desenvolvimento sistemático da teoria dos números.

O método para o cálculo do MDC e MMC é estudado logo no Ensino Fundamental da Educação Básica no conteúdo de divisibilidade dos números naturais, mas pouco explorado no Ensino Médio. Estes conteúdos têm muitas aplicações práticas, isto é, presentes no cotidiano dos alunos. Consideremos, por exemplo, o seguinte problema:

Um terreno retangular de 221m por 117m será cercado. Em toda a volta desse cercado, serão plantadas árvores igualmente espaçadas. Qual o maior espaço possível entre as árvores? (Subentendendo que uma árvore deve ser plantada em cada canto do terreno e que o espaço entre as árvores deve ter um número inteiro de metros, então é um problema de MDC que obtemos como resultado 13m).

Atualmente é um conhecimento utilizado nas mais diversas áreas, destacando-se os números primos na área da informática.

Entendendo como um conteúdo que deve ser mais explorado e aprofundado na Educação Básica, segue abaixo os tópicos relacionando alguns conceitos deste ramo da Matemática.

Definição (Divisibilidade): Dizemos que um inteiro não nulo a divide um inteiro b, representado por $a \mid b$ quando existe um inteiro c, tal que $b = a \cdot c$. Também podemos dizer:

- a é divisor de b
- a é fator de b
- b é múltiplo de a
- b é divisível por a, no caso em que $a \neq 0$.
- $c = \frac{b}{a}$ é o quociente de b por a..

Observação: Quando a não divide b, escrevemos $a \nmid b$.

Exemplo: $5 \mid 10$, pois $10 = 5 \cdot 2$, porém $5 \nmid 12$, pois não existe um inteiro c tal que $12 = 5 \cdot c$.

A partir da definição segue algumas propriedades básicas em relação a divisibilidade.

Proposição 2.1: Sejam a, b e c números inteiros. Então,

i. $\boldsymbol{1 \mid a}$, $\boldsymbol{a \mid a}$ e $\boldsymbol{a \mid 0}$;

ii. Se $\boldsymbol{a \mid b}$ e $\boldsymbol{b \mid c}$, então, $\boldsymbol{a \mid c}$;

iii. Se $\boldsymbol{a \mid b}$ e $\boldsymbol{a \mid c}$ então $\boldsymbol{a \mid b + c}$ e $\boldsymbol{a \mid b - c}$;

iv. Se a e b são positivos e $\boldsymbol{a \mid b}$, então $\boldsymbol{a \leq b}$;

v. Se $\boldsymbol{a \mid b}$ e $\boldsymbol{b \mid a}$, então $\boldsymbol{a = b}$ ou $\boldsymbol{a = -b}$;

vi. Se $\boldsymbol{a \mid b}$, então $\boldsymbol{a \mid b \cdot d}$ para qualquer inteiro d;

vii. Se $\boldsymbol{a \mid b}$, então $\boldsymbol{a \cdot d \mid b \cdot d}$ para qualquer inteiro d.

Prova:

i. Basta fazer $a = 1 \cdot a$, $a = a \cdot 1$ *e* $0 = a \cdot 0$;

ii. Se $a|b$ *e* $b|c$, então existem q_1 e q_2 inteiros, tais que $b = a \cdot q_1$ e
$c = b \cdot q_2$. Segue daí que $c = (a \cdot q_1) \cdot q_2 = a \cdot (q_1 \cdot q_2)$, com $q_1 \cdot q_2$ inteiro.

iii. Já que $a|b$ e $a|c$, então existem r_1e r_2 inteiros, de modo que $b = a \cdot r_1$ e $c = a \cdot r_2$. Isso acarreta em $b + c = ar_1 + ar_2 = a(r_1 + r_2)$ com $r_1 + r_2$ inteiro. Portanto, $a|b + c$. De maneira análoga provamos que $a|b - c$.

iv. Se $a, b > 0$ e $a|b$, então existe q inteiro tal que $b = a \cdot q$, com $q \geq 1$. Multiplicando essa ultima desigualdade por $a > o$, tem-se
$b = a \cdot q \geq a > 0$.

v. Uma vez que $a|b$ e $b|a$, tem-se $|a|\ divide\ |b|\ e\ |b|\ divide\ |a|$. De acordo com item anterior, $|a| \leq |b|\ e\ |b| \leq |a|$, isso implica em $|a| = |b|$. Logo, $a = b$ ou $a = -b$.

vi. Como $a|b$, deve existir q_3 inteiro, tal que $b = a \cdot q_3$. Portanto, $b \cdot d = (a \cdot q_3)d = a(q_3 \cdot d)$. Logo, $a|b \cdot d$

vii. Se $a|b$, então existe q inteiro, de modo que $b = a \cdot q$. Logo, $b \cdot d = (a \cdot q)d = (a \cdot d)q$, para q inteiro. Portanto, $a \cdot d|b \cdot d$. ■

3.6.1 Algoritmo da Divisão Euclidiana

Sejam a e b inteiros (únicos), com $b \neq 0$. Existem inteiros q e r, únicos, tais que $a = bq + r$, com $0 \leq r < |b|$. Tais inteiros q e r são chamados, respectivamente, o quociente e o resto da divisão de a por b.

Prova: Suponhamos inicialmente, $b > 0$ e q o maior inteiro tal que $b \cdot q \leq a$. Assim temos que $bq \leq a < b(q + 1)$, de modo que $0 \leq a - bq < b = |b|$, logo, basta definir, $r = a - bq$.

Se $b < 0$, então $-b > 0$, portanto existem inteiros q e r tais que $a = (-b)q + r$, com $0 \leq r < -b = |b|$, acarretando em $a = b(-q) + r$, concluindo então a primeira parte.

Para provarmos a unicidade de q e r, admitamos que existem inteiros q_1 e r_1, tal que $a = b_1 q_1 + r_1$, com $0 \leq r_1 < |b_1|$. Dessa forma, temos $(bq + r) - (bq_1 + r_1) = 0$, o que implica em $b(q - q_1) = r_1 - r$, portanto $|b|divide|r_1 - r|$. Como $0 \leq r_1 < |b_1|$ e $0 \leq r < |b|$, então $|r_1 - r| < |b|$, portanto, como $|b|divide|r_1 - r|$, temos que $r_1 - r = 0$, o que acarreta em $r = r_1$. Logo, $bq_1 = bq \Longrightarrow q_1 = q$, pois $b \neq 0$. ■

3.6.2 Máximo Divisor Comum (MDC)

Definição: Sejam a e b inteiros, (a ou b diferente de zero). O *Máximo Divisor Comum* de a e b, representado por $mdc(a,b)$, é o maior dentre os divisores positivos comuns de a e b. Portanto, se $mdc(a, b) = d$, então, d é um inteiro que satisfaz as seguintes condições:

(i) $d > 0$

(ii) $d|a\ e\ d|b$

(iii) Se $k \in \mathbb{Z}$ é tal que $k|a\ e\ k|b$, então $k|d$. (Estas três condições são tomadas por muitos autores como a definição do MDC).

Proposição 2.2: Sejam a e b inteiros positivos.

i. Se b é divisor de a, então $mdc(a,b) = b$;

ii. Se $a = bq + c$, com $c \neq 0$, então o conjunto dos divisores comuns dos números b e c é igual ao conjunto dos divisores comuns de a e b. Em particular, $mdc(a,b) = mdc(b,c)$

Prova:

i. Todo divisor comum de a e b é um divisor de b. Como b é divisor de a, tem-se que todo divisor de b é também divisor de a, ou seja, um divisor comum de a e b. Portanto, o conjunto dos divisores comuns dos inteiros a e b é igual ao conjunto dos divisores de b. Como o maior divisor de b é ele mesmo, tem-se $mdc(a,b) = b$.

ii. Usando os itens iii e vi da proposição 2.1, tem-se que todo divisor comum de a e b também divide c, consequentemente, é um divisor comum de b e c. Pelo mesmo motivo todo divisor comum de b e c também divide a, consequentemente, é um divisor comum de a e b. Logo os divisores comuns de a e b são os mesmos que os divisores comuns de b e c. Em particular, também coincidem os maiores divisores comuns, ou seja, $mdc(a,b) = mdc(b,c)$.

Para o cálculo do *mdc* de dois números inteiros Euclides escreveu no início do livro VII de "Os elementos" duas proposições hoje conhecida como "o algoritmo de Euclides"

> Dados dois números diferentes, subtrai-se o menor a do maior b repetidamente até que se obtenha um resto r_1 menor do que o menor número; então subtrai-se repetidamente esse resto r_1 de a até resultar um resto $r_2 < r_1$; então subtrai-se repetidamente r_2 de r_1; e assim por diante. Finalmente o processo leva a um resto r_n que mede r_{n-1}, portanto todos os restos precedentes, bem como a e b; este número r_n será o máximo divisor comum de a e b.([4], p.84)

3.6.3 Algoritmo de Euclides

Há cerca de 2000 anos atrás, Euclides, um dos maiores matemáticos da Grécia, criou um algoritmo bastante simples e eficiente para determinar o máximo divisor comum de dois números inteiros e que ainda hoje é considerado como um dos algoritmos iniciais mais eficientes e mais conhecidos no mundo.

Sejam a e b números inteiros positivos. Aplica-se sucessivamente a divisão euclidiana para obter a seguinte sequência de igualdades:

Passo *1*: $a = bq_1 + r_1 \qquad 0 < r_1 < b$

Passo *2*: $b = r_1 q_2 + r_2$ $\quad 0 < r_2 < r_1$

Passo *3*: $r_1 = r_2 q_3 + r_3$ $\quad 0 < r_3 < r_2$

$\vdots \qquad \vdots \qquad \vdots$

Passo *j*: $r_{j-2} = r_{j-1} q_j + r_j$ $\quad 0 < r_j < r_{j-1}$

Passo *j+1*: $r_{j-1} = r_j q_{j+1} + 0$

Observação: A execução do algoritmo para após certo número finito de passos, pois, desde que r_1, r_2,... são inteiros para os quais $b > r_1 > r_2 > \cdots$, se a sequência de restos não acabasse, em algum momento teríamos um resto negativo, o que é um absurdo, portanto deve existir um menor natural j tal que r_j é o último resto não nulo no processo de divisão acima. ([20], p.24)

Para demonstrarmos o Algoritmo de Euclides usaremos o resultado do lema seguinte.

Lema: Sejam a, b inteiros positivos e $t \in \mathbb{Z}$. Então $mdc(a, b) = mdc(a, b + at)$ e $mdc(a, b) = mdc(a + bt, b)$.

Demonstração: Vamos provar que $mdc(a, b) = mdc(a, b + at)$.

Seja $d = mdc(a, b)$ e $d' = mdc(a, a + bt)$. Temos que

$$d = mdc(a, b) \Longrightarrow d|a, d|at \text{ e } d|b \Rightarrow d|a \text{ e } d|b + at$$

Logo, d é um divisor comum de a e $b + at$ e como d' é o maior divisor comum, temos então $d' \geq d$. Analisemos o $mdc(a, b + at)$:

$$d'|a \text{ e } d'|b + at \Rightarrow d'|a, d'|at \text{ e } d'|b + at \Rightarrow d'|a \text{ e } d'|b + at - at \Rightarrow d'|a \text{ e } d'|b$$

Assim, d' é um divisor comum de a e b e como d é o maior divisor comum, temos $d \geq d'$. Mas já provamos que $d' \geq d$, portanto $d = d'$, como queríamos. A outra identidade se demonstra de forma análoga.

Agora usando esse lema demonstraremos o resultado do Algoritmo de Euclides. Vejamos: $mdc(a, b) = mdc(a - q_1 b, b) = mdc(r_1, b) \Longrightarrow mdc(a, b) = mdc(b, r_1)$

$$mdc(b, r_1) = mdc(b - r_1 q_2, r_1) = mdc(r_2, r_1) \Rightarrow mdc(b, r_1) = mdc(r_2, r_1)$$

Fazendo isso sucessivamente: $mdc(a, b) = mdc(b, r_1) = mdc(r_2, r_1) = \cdots = mdc(r_{j-1}, r_j) = mdc(q_j r_j, r_j) = r_j$, assim temos que $mdc(a, b) = r_j$, como queríamos provar. ■

Exemplo: Utilize o algoritmo de Euclides para mostrar que o *mdc* de 140 e 648 é igual a 16.

$$648 = 140 \cdot 4 + 88$$

$$140 = 88 \cdot 1 + 52$$

$$88 = 52 \cdot 1 + 36$$

$$52 = 36 \cdot 1 + 16$$

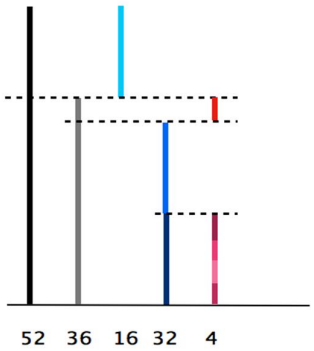
$$36 = 16 \cdot 2 + 4$$

$$16 = 4 \cdot 4 + 0$$

Portanto, $mdc(140, 640) = 4$.

Outro exemplo está na figura abaixo, mostrando que $mdc(52,36) = 4$.

Figura 29 - Algoritmo de Euclides



Fonte: http://mathforum.org/mathimages/index.php/Euclidean_Algorithm

Explicação: Use o número inteiro menor dos dois, 36, para dividir o maior, 52. Use o resto desta divisão, 16, para dividir 36. Obtém-se o resto 4. Agora dividir o último divisor, 16, por 4 e verifica-se que eles dividem exatamente. Portanto, 4 é o maior divisor comum. Para cada dois inteiros é possível determinar o *mdc*, repetindo este mesmo processo até atingir o resto 0 (nulo).

3.6.4 Mínimo Múltiplo Comum (MMC)

Definição: Dados inteiros não nulos *a* e *b*. O *Mínimo Múltiplo Comum* de *a* e *b*, denotado por *mmc(a, b)*, é o menor dentre todos os múltiplos positivos comuns de *a* e *b*.

Exemplo: *mmc(8,12) = 24*, pois, $m(8) = \{8, 16, \mathbf{24}, 32, 40, \dots\}$ *e* $m(12) = \{12, \mathbf{24}, 48, \dots\}$;

Números Primos

Um inteiro $p > 1$ é *primo* se seus únicos divisores positivos forem *1* e *p*. Um inteiro $a > 1$ que não é primo é dito *composto*.

Primos menores que 50: *2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47*.

Lema de Euclides: Todo inteiro $n > 1$ pode ser expresso como o produto de um número finito de primos, não necessariamente distintos.

Prova: Façamos a prova por indução sobre n. se $n = 2$, nada há a fazer uma (vez que 2 é primo). Suponha, agora, que todo inteiro n tal que $2 \leq n < m$ pode ser escrito como o produto de um número finito de primos; provemos que este é também o caso para m: se m for primo, nada há a fazer. Senão, existem inteiros a e b tais que $m = ab$, com $1 < a, b < m$. Pela hipótese de indução, a e b podem ser escritos como produtos de números finitos de primos, digamos $a = p_1, \ldots, p_k$, $b = q_1, \ldots, q_l$, com $k, l > 1$ e $p_1, \ldots, p_k, q_1, \ldots, q_l$ primos. Logo, $m = ab = p_1 \ldots p_k q_1 \ldots q_k$, também o produto de um número finito de primos. ■

Proposição 2.3: Se $p|a \cdot b$, p primo, então $p|a$ ou $p|b$.

Prova: Se $p|a$, então nada há a fazer. Caso $p \nmid a$, tem-se $mdc(p, a) = 1$, pois p é primo. Portanto, pela Relação de Bézout, existem x e y inteiros tal que $px + ay = 1$. Multiplicando essa igualdade por b obtemos, $pbx + aby = b$. Como $p|pbx$ e $p|paby$, temos que $p|pbx + aby = b$. ■

Usando a proposição anterior e indução temos o seguinte resultado:

***Corolário*:** Seja p um número primo e sejam $a_1, \cdots, a_n \in \mathbb{N}$, tal que $p|a_1 a_2 \cdots a_n$ então existe $1 \leq i \leq n$ tal que $p|a_i$. Em particular, se $a_1, \cdots, a_n$ forem todos primos, então existe $1 \leq i \leq n$ tal que $p = a_i$.

(Teorema Fundamental da Aritmética): Todo inteiro $n > 1$ pode ser escrito como o produto de potências de primos distintos: Ademais, tal decomposição de n é única no seguinte sentido: $se\ n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k} = {q_1}^{\beta_1} \cdots {q_l}^{\beta_l}$, onde $p_1 < \cdots < p_k$ e $q_1 < \cdots < q_l$ são números primos e $\alpha_i, \beta_j \geq 1$ são inteiros, então $k = l$ e, para $1 \leq i \leq k$, $p_i = q_i$ e $\alpha_i = \beta_i$.

Prova: A parte da existência foi estabelecida pelo Lema de Euclides.

Para a unicidade, suponhamos que o inteiro $n > 1$ admite duas decomposições como no enunciado. $p_1|n$, temos que $p_1|{q_1}^{\beta_1} \cdots {q_l}^{\beta_l}$, e o corolário anterior a existência de $1 \leq j \leq l$, tal que $p_1 = q_j$. Por outro lado, como $q_1|n$, temos que $q_1|{p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k}$ e, novamente pelo corolário anterior, existe $1 \leq i \leq k$ tal que $q_1 = p_1$ e daí,

$$n = {p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k} = {q_1}^{\beta_1} \cdots {q_l}^{\beta_l}.$$

Provemos que $\alpha_1 = \beta_1$. Se $\alpha_1 < \beta_1$, então ${p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k} = {p_1}^{\beta_1 - \alpha_1} {q_2}^{\beta_2} \cdots {q_l}^{\beta_l}$, de maneira que $p_1|{q_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$. Argumentando como acima, existe $2 \leq i \leq k$ tal que $p_1 = p_i$, o que é um absurdo. Analogamente, não pode ser $\alpha_1 < \beta_1$. Logo, $\alpha_1 = \beta_1$ e segue que,

$${p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k} = {q_2}^{\beta_2} \cdots {q_l}^{\beta_l}.$$

Repetindo o argumento acima várias vezes, concluímos sucessivamente que $p_2 = q_2$ e $\alpha_2 = \beta_2$, $p_3 = q_3$ e $\alpha_3 = \beta_3$, $\cdots$ Ao final se $k < l$, obteremos $1 = q_{k+1}^{\beta_{k+1}} \cdots q_l^{\beta_l}$, o

que é um absurdo; se $k > l$, obtemos também de forma análoga um absurdo. Logo $k = l$ e nada mais há a fazer. ■

Lema: Sejam $a = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ e $d = {p_1}^{\beta_1} \cdot {p_2}^{\beta_2} \cdots {p_k}^{\beta_k}$ inteiros positivos, onde $p_1 \cdots p_k$ são primos e $\alpha_k, \beta_k \geq 0, 1 \leq i \leq k$. Então $d|a$ se, e somente se, $\beta_k \leq \alpha_k, 1 \leq i \leq k$.

Prova. Primeiro, mostraremos que, se $d|a$ então $\beta_k \leq \alpha_k, 1 \leq i \leq k$. Se $d|a$, então existe um número c tal que $a = dc$.

Escrevendo $c = {p_1}^{\gamma_1} \cdots {p_k}^{\gamma_k}$, tem-se:

$${p_1}^{\alpha_1} \cdots {p_k}^{\alpha_k} = {p_1}^{\beta_1} \cdots {p_k}^{\beta_k} \cdot {p_1}^{\gamma_1} \cdots {p_k}^{\gamma_k} = {p_1}^{\beta_1+\gamma_1} \cdots {p_1}^{\beta_k+\gamma_k}$$

Pela unicidade do teorema fundamental da aritmética, vê-se que $\alpha_k = \beta_k + \gamma_k$.

Segue daí que $\alpha_k \geq \beta_k, 1 \leq i \leq k$. Portanto, concluímos a primeira parte.

Agora devemos mostrar que, se $\beta_k \leq \alpha_k, 1 \leq i \leq k$, então $d|a$.

Seja $\beta_k \leq \alpha_k, 1 \leq i \leq k$. Fazendo $\gamma_k = \alpha_k - \beta_k$, obtemos:

$$a = {p_1}^{\beta_1+\gamma_1} \cdots {p_1}^{\beta_k+\gamma_k} = {p_1}^{\beta_1} \cdots {p_k}^{\beta_k} \cdot {p_1}^{\gamma_1} \cdots {p_k}^{\gamma_k} = d \cdot {p_1}^{\gamma_1} \cdots {p_k}^{\gamma_k}.$$

Logo, $d|a$. ■

No Teorema seguinte usaremos a notação $min\{a, b\}$, para representar o elemento $x \in \{a, b\}$ tal que $x \leq a \; e \; x \leq b$. O $max\{a, b\}$ é o elemento $y \in \{a, b\}$, tal que $y \geq a \; e \; y \geq b$.

Exemplos:

- $min\{4,6\} = 4$
- $max\{8,10\} = 10$
- $min\{7,7\} = 7$

Teorema: Se $a = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ e $b = {p_1}^{\beta_1} \cdot {p_2}^{\beta_2} \cdots {p_k}^{\beta_k}$ nas condições do lema anterior, então:

$mdc(a, b) = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}}$ e $mmc(a, b) = \prod_{i=1}^{k} p_i^{\max\{\alpha_i, \beta_i\}}$.

Prova. Façamos a prova para o *mdc* (a prova para o *mmc* é análoga).

Como o $\min\{\alpha_i, \beta_i\} \leq \alpha_i, \beta_i$ para todo i, temos que o número $d = \prod_{i=1}^{k} p_i^{\min\{\alpha_i, \beta_i\}}$ divide ambos a e b. Seja agora, d' um divisor positivo qualquer de a e b. Então a decomposição em primos de d' é da forma $d' = {p_1}^{\gamma_1} \cdots {p_k}^{\gamma_k}$ com $\gamma_i \geq 0$ para todo i. Mas, $d'|a$ implica $\gamma_i \leq \alpha_i$ e $d'|b$ implica $\gamma_i \leq \beta_i$. Assim, para todo i, temos que $\gamma_i \leq \min\{\alpha_i, \beta_i\}$, de modo que $d'|d$. Logo, $d = mdc(a, b)$. ■

Exemplo: Calcule o *mdc* e o mmc de 1800 e 210, usando a decomposição desses números em fatores primos.

$$1800 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^0$$

$$210 = 2 \cdot 3 \cdot 5 \cdot 7$$

Então, $mdc(1800,210) = 2 \cdot 3 \cdot 5 \cdot 7^0 = 30$

e $mmc(1800,210) = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7 = 12600$

Vejamos mais alguns exemplos práticos de aplicação do *mdc* e *mmc* para solução de problemas presentes no cotidiano das pessoas:

- Samantha tem dois pedaços de tecido. Uma das peças mede 72 centímetros de largura e a outra 90 centímetros de largura. Ela deseja cortar as duas peças em tiras de mesma largura com a maior medida possível. Qual a largura ela deve cortar as tiras?

Este problema pode ser resolvido usando o máximo divisor comum, porque estamos cortando ou "dividindo" as tiras de pano em pedaços menores de 72 e 90 (fator comum) e estamos olhando para os mais amplos possíveis.

- Rubens faz exercícios a cada 12 dias e Isabel a cada 8 dias. Rubens e Isabel fizeram exercícios hoje. Quantos dias irão transcorrer até que eles novamente façam exercícios juntos?

Este problema pode ser resolvido usando mínimo múltiplo comum, porque estamos tentando descobrir quanto mais cedo (menos) tempo será com a continuidade nos intervalos dos exercícios (múltiplo) irá acontecer ao mesmo tempo (comum).

Vários outros exemplos de problemas do cotidiano envolvendo estes dois assuntos (*mdc* e *mmc*) podem ser apresentados, segue mais alguns métodos que buscam facilitar o cálculo do *mdc e do mmc.*

3.6.5 Outro método para cálculo do mdc e mmc ([20], p.36)

Uma variação do método (algoritmo) acima simplifica os cálculos e fornece, ao mesmo tempo, o *mmc* e o *mdc* dos números, Exemplificamos calculando o *mmc* e o *mdc* dos mesmos números 1800 e 210.

Figura 30 - Cálculo do MMC e MDC

1800	210	|	2
900	105	|	3
300	35	|	5
60	7		

Fonte: Elaborado pelo autor

Novamente temos:

$mdc(1800,210) = 2 \cdot 3 \cdot 5 = 30$ e $mmc(1800,210) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 60 = 12600$

Neste algoritmo um número primo comparece na coluna da direita apenas quando divide ambos os números à sua esquerda, na mesma linha. As divisões terminam quando isso não for mais possível, o que significa que os dois números encontrados nas duas colunas da esquerda são primos entre si.

O *mdc* é o produto dos números que estão na coluna da direita e o *mmc* é o produto deste *mdc* pelo dos números primos entre si que restaram na última linha à esquerda.

Justificativa: Colocando na coluna da direita, só os primos que dividem ambos os números da esquerda, estamos certamente relacionando fatores primos do *mdc*. Levando o processo até chegarmos a dois números primos entre si, teremos esgotado os fatores primos do *mdc*. Portanto, o produto $2 \cdot 3 \cdot 5 = 30$ dos primos da coluna da direita é o *mdc* dos números 1800 *e* 210.

Por outro lado, devido à maneira como se chegou aos números primos entre si, *60* e *7*, tem-se que $1800 = 30 \cdot 60$ e $210 = 30 \cdot 7$, então qualquer múltiplo de 1800 deve conter os fatores *30* e *60* e qualquer múltiplo de *210* deve conter os fatores *30* e *7*; assim, o menor de todos os múltiplos comuns é aquele que se obtém do produto dos fatores *30*, *60* e *7*.

Observações:

1) Os argumentos acima podem ser generalizados para quaisquer dois números inteiros positivos *a* e *b*.
2) Este método também se aplica para o cálculo do *mdc* e do *mmc* de mais do que dois números.
3) A justificativa exposta acima traz uma relação importante entre o *mdc*, o *mmc* e o produto de dois números, que é bastante utilizada:

$$mmc(a,b) = \frac{a \times b}{mdc(a,b)}$$

3.6.6 Método geométrico para o cálculo do mmc e mdc de dois números inteiros positivos. ([14], p.86-88)

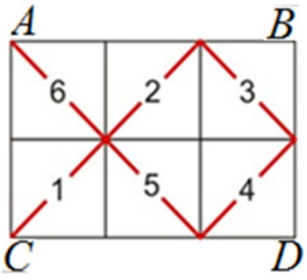
Segue mais um algoritmo para calcular o *mmc e mdc* de dois números naturais *m* e *n* sem efetuar operações utilizando apenas contagem:

Cálculo do mmc: (O método)

1) Considere um retângulo *ABCD* de lados *m* e *n*. O retângulo deve ser subdividido em quadrados unitários.
2) Partindo de um dos vértices do retângulo, trace as diagonais dos quadrados unitários observando a seguinte ordem:
   i. Trace a diagonal do quadrado que tem o vértice coincidente com o vértice escolhido do retângulo.
   ii. Trace a partir do vértice no qual parou as diagonais dos quadrados que têm um ângulo oposto pelo vértice com o quadrado anterior, ou na ausência deste trace a diagonal do quadrado ao lado e a partir do vértice de onde parou.
   iii. As diagonais dos quadrados unitários devem ser traçadas até que se chegue a um dos outros vértices do retângulo *ABCD*.
   iv. O número de quadrados unitários que tiveram suas diagonais traçadas é o *mmc* de *m* e *n*.

Exemplos:

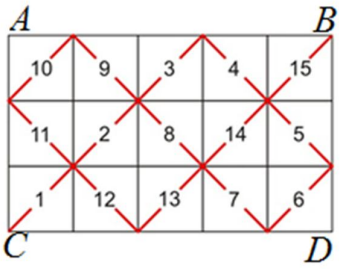
Figura 31 - $mmc(2,3) = 6$



Fonte: Próprio Autor

Observe que 6 quadrados tiveram sua diagonais traçadas.

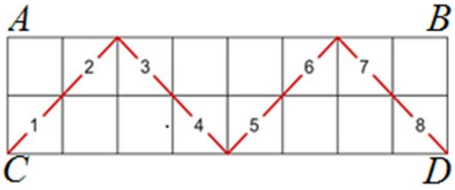
Figura 32 - $mmc(3,5) = 15$



Fonte: Próprio Autor

15 quadrados tiveram suas diagonais traçadas.

Figura 33 - $mmc(2,8) = 8$



Fonte: Próprio Autor

8 quadrados tiveram suas diagonais traçadas.

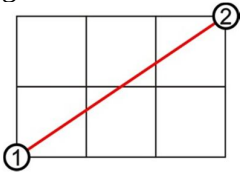
Justificativa: ao partirmos de um vértice do retângulo e chegarmos a um outro vértice desse mesmo retângulo, traçamos diagonais de um número de quadrados que correspondem a um múltiplo tanto de *m* quanto de *n*; parando no primeiro outro vértice do retângulo *ABCD*, estamos determinando o mínimo dentre os múltiplos comuns de *m* e *n*.

Cálculo do mdc: (O método)

1) Considere um retângulo de lados, com medidas inteiras *a* e *b*, dividido em quadradinhos unitários.
2) Trace uma das diagonais do retângulo, marcando-a nos pontos que são vértices de algum quadradinho unitário.
3) Conte em quantas partes esses pontos dividem a diagonal: esse número *d* é o $mdc(a, b)$.

Exemplos:

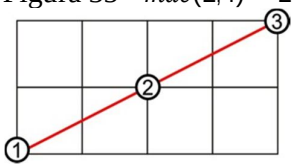
Figura 34 - $mdc(2,3) = 1$



Fonte: Próprio Autor

A diagonal traçada encontra somente dois vértices dos quadradinhos internos, ou seja, essa diagonal foi dividida apenas em 1 parte. Esse número de divisões é equivalente ao *mdc* entre os números 2 e 3.

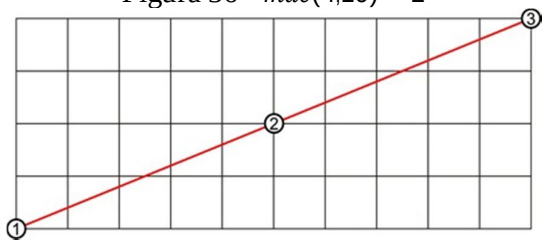
Figura 35 - $mdc(2,4) = 2$



Fonte: Próprio Autor

A diagonal traçada encontra três vértices dos quadradinhos internos, ou seja, essa diagonal foi dividida em 2 partes. Esse número de divisões é equivalente ao *mdc* entre os números 2 e 4.

Figura 36 - $mdc(4,10) = 2$



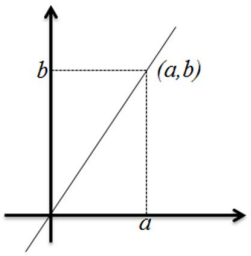
Fonte: Próprio Autor

A diagonal traçada encontra três vértices dos quadradinhos internos, ou seja, essa diagonal foi dividida em 2 partes. Esse número de divisões é equivalente ao *mdc* entre os números 4 e 10.

Justificativa: Se $d = mdc(a, b)$, existem inteiros u e v tais que $a = du$ e $b = dv$, com u e v primos entre si.

Considerando um sistema de eixo ortogonais com a origem num dos vértices do retângulo, como na figura, a equação da reta que contém a diagonal considerada é $y = \frac{b}{a}x$.

Figura 37 - $y = \frac{b}{a}x$



Fonte: Próprio Autor

Logo, pertencem à diagonal os pontos *(0,0); (u,v)* pois

$\frac{b}{a} = \frac{v}{u}; (2u, 2v); \cdots; (du, dv) = (b, a)$, ou seja, $(d + 1)$ pontos de coordenadas inteiras igualmente espaçadas.

Para verificar que são apenas esses os pontos da diagonal com coordenadas inteiras, suponha que *(p,q)* pertença à diagonal e tenha coordenadas inteiras. Então,

$$q = \frac{b}{a}p = \frac{v}{u}p.$$

O que implica $qu = vp$ e sendo $mdc(u, v) = 1$, vem que $q = rv$ e $p = ru$, com $0 \leq r \leq d$. Logo, a diagonal fica dividida em ***d*** pedaços iguais.

3.7 ARITMÉTICA MODULAR

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Será abordado em primeiro lugar este conceito e em seguida algumas aplicações práticas serão descritas.

Dizemos que um número *a* é congruente a outro número *b* módulo *n*, quando a divisão de *a* por *n* restar *b*, que representamos na linguagem simbólica matemática da seguinte forma:

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

Lemos: *a* é côngruo *b* módulo *n*, com $a, b, n \in \mathbb{Z}, n > 1$.

Uma maneira equivalente de dizer isso é afirmar que a diferença $(a - b)$ ou $(b - a)$ é divisível por *n*.

Exemplo: 11 é congruente ao número 2, módulo 9, pois ambos deixam resto 2, ao serem divididos por 9, que representamos por $11 \equiv 2\ (mod\ 9)$.

Foi Gauss que observou que usávamos com muita frequência frases do tipo "*a* dá o mesmo resto que *b* quando divididos por *n*". Foi Gauss então que introduziu uma notação específica para este fato e que denominou de "*congruência*". [27]

A congruência define uma equivalência, pois satisfaz as propriedades:

- Reflexiva: $a \equiv a\ (mod\ n)$
- Simétrica: $a \equiv b\ (mod\ n), então\ b \equiv a\ (mod\ n)$
- Transitiva: $a \equiv b\ (mod\ n)$ e $b \equiv c\ (mod\ n)$, então $a \equiv c\ (mod\ n)$

Outras propriedades importantes da congruência

- Se $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n)$, então $a \pm c \equiv b \pm d\ (mod\ n)$
- Se $a \equiv b\ (mod\ n)$ e $c \equiv d\ (mod\ n)$, então $ac \equiv bd\ (mod\ n)$

- Se $a \equiv b\ (mod\ n)$, então $ac \equiv bc\ (mod\ nc)$
- Se $a \equiv b\ (mod\ n)$, então $a^c \equiv b^c\ (mod\ n)$

Usamos a congruência modular em diversas aplicações, tais como: Critérios de divisibilidade, códigos numéricos de identificação (códigos de barras, em números dos documentos: CPF, CNPJ, RG; criptografia, otimização de redes de computadores, entre outras). Vejamos alguns exemplos dessas aplicações.

- **Códigos de Barras**

O EAN-13 é um dos códigos de barras mais usados no mundo. É constituído de 13 algarismos sendo que o último é o dígito de controle calculado através da congruência módulo 10, sendo os dígitos 1 e 3 os fatores que compõem a base de multiplicação, que vão se repetindo da esquerda para a direita. [27]

Se $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9\ a_{10}\ a_{11}\ a_{12}$ é a sequência formada pelos 12 primeiros dígitos, devemos multiplicá-los nesta ordem, por {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. O dígito que está faltando, representaremos por a_{13} que somado com *S* deve gerar um múltiplo de 10, isto é, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja,

$S + a_{13} \equiv 0\ mod 10$.

Conforme a figura 38 os três primeiros dígitos do código representam o país de registro do produto; os cinco dígitos seguinte identificam o fabricante; os próximos quatro identificam o produto e o último é o dígito de controle.

Figura 38 - Código de barras

Fonte: http://www.devmedia.com.br/artigo-clube-delphi, acesso em 28/07/15

Vejamos um exemplo.

Efetuar os cálculos para a determinação do dígito de controle do código de barras destacado na figura 38.

Código	7	8	9	9	9	9	9	9	1	2	3	4
Base de multiplicação	1	3	1	3	1	3	1	3	1	3	1	3
Produtos	7	24	9	27	9	27	9	27	1	6	3	12

Efetuando os produtos obtemos:

$$7 + 24 + 9 + 27 + 9 + 27 + 9 + 27 + 1 + 6 + 3 + 12 = 161$$

Dividindo 161 por 10, obtemos como quociente 16 e resto 1. Logo, o digito de controle é igual a 9 (10 – 1). Notemos que $161 + 9 = 170$ (múltiplo de 10).

O precursor dos atuais códigos de barra ocorreu no início dos anos 50 nos EE.UU. Procurava-se identificar vagões de trens para transporte de carga afixando dez números em ambos os lados dos vagões, sendo que os quatro primeiros identificavam a companhia dona do vagão e os seis últimos o vagão, cada grupo de números pintado com cores diferentes. A malha ferroviária nos EE. UU. é privada e pertence a dezenas de companhias. Os vagões transitavam em qualquer via, fazendo-se assim necessário a sua identificação e a quem pertencia. O sistema não funcionou a contento e foi abandonado cerca de dez anos depois. Outro setor da economia que precisava com urgência de um sistema de controle eram as redes de supermercados. Tinham necessidade de identificar em cada item comercializado, o fabricante, sua origem, dados do produto, validade, preços, rotatividade e quantidade em estoque. Este último item era crucial, pois tanto um baixo estoque como um alto estoque acarretavam prejuízos financeiros.

No início dos anos 70 um sistema praticamente idêntico ao atual foi usado para identificar chicletes de certo fabricante no estado de Ohio. Logo o sistema ganhou popularidade e foi estendido a tudo quanto era produto vendido em supermercados. Assim, o sistema de controle dos supermercados deu um salto de produtividade além de reduzir a fila de espera dos fregueses que aguardavam nas filas dos caixas. Tudo era muito rápido usando dispositivos a laser capazes de ler o código. Logo os supermercados delegaram aos fornecedores a missão de controlar o estoque de seus produtos em cada supermercado das diversas redes reduzindo os custos destes últimos ainda mais. O sistema se espalhou também pela indústria que passaram a controlar com mais eficiência suas matérias primas, níveis de estoque, preços etc.

O sistema de código de barra evoluiu com diversos aperfeiçoamentos e aumento de sua capacidade de armazenar dados. No Japão, em meados dos anos 90 a indústria automobilística criou um código bidimensional que ficou conhecido como QR code (**Q**uick **R**esponse code). Evidentemente era muito mais potente (cerca de 350 vezes mais), pois tinha

duas dimensões em vez de só uma do código de barras. Todavia, QR codes com mais resolução estão sendo implementados e seu uso se estendendo a muitas áreas onde o código de barra é insuficiente para guardar tanta informação.

- **Cadastro das pessoas físicas na Receita Federal – CPF**

O número do CPF que é constituído de 11 dígitos, sendo um primeiro bloco com nove algarismos e um segundo com mais dois algarismos que são os dígitos de controle ou de verificação. A determinação desses dois últimos dígitos segue um raciocínio análogo ao do código de barras visto no exemplo anterior. Sendo calculados pela congruência módulo 11, tendo como base de multiplicação os algarismos {1, 2, 3, 4, 5, 6, 7, 8, 9} para o primeiro dígito e {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} para o segundo dígito. O décimo dígito que está faltando, representado por a_{10} deve ser tal que subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número S-a_{10} deve ser múltiplo de 11, ou seja,

$S - a_{10} \equiv 0\, mod 11$. Observemos que tal número será o próprio resto da divisão por 11 da soma obtida.

Exemplo:

Suponhamos uma pessoa que tenha os 9 dígitos de seu CPF sendo: 959.903.303, o primeiro dígito de controle é calculado da seguinte maneira:

Código	9	5	9	9	0	3	3	0	3
Base de multiplicação	1	2	3	4	5	6	7	8	9
Produtos	9	10	27	36	0	18	21	0	27

Efetuando os produtos obtemos:

$$9 + 10 + 27 + 36 + 0 + 18 + 21 + 0 + 27 = 148$$

Dividindo 148 por 11, obtemos quociente 3 e resto 5. Portanto, 5 é o primeiro dígito verificador.

Calculamos o segundo da mesma forma:

Código	9	5	9	9	0	3	3	0	3	5
Base de multiplicação	0	1	2	3	4	5	6	7	8	9
Produtos	0	5	18	27	0	15	18	0	24	45

Efetuando os produtos obtemos:

$$0 + 5 + 18 + 27 + 0 + 15 + 18 + 0 + 24 + 45 = 152$$

Dividindo 152 por 11, obtemos quociente 13 e resto 9. Portanto, 9 é o segundo dígito verificador.

- **Em que dia da semana você nasceu?**

Este algoritmo funciona para datas entre 1900 e 2399 (devido a uma particularidade dos anos bissextos terminados em “00”) e utiliza a congruência módulo 7.

1. Calcule quantos anos se passaram desde 1900 até o ano em que você nasceu. Esse valor obtido será representado por A.
2. Calcule quantos anos bissextos existiram após 1900. Que será o quociente da divisão de A por 4. Esse valor será representado por B.
3. Considerando o mês de nascimento, obtenha o número associado a ele na tabela abaixo. Esse número será representado por C.

Figura 39 - Tabela dos meses

Tabela dos meses			
Janeiro	0	Julho	6
Fevereiro	3	Agosto	2
Março	3	Setembro	5
Abril	6	Outubro	0
Maio	1	Novembro	3
Junho	4	Dezembro	5

Fonte:([27].p.13)

4. Considere o dia do nascimento (x). Calcule x – 1, que será representado por D.
5. Some os quatro valores obtidos nas etapas anteriores (A+B+C+D). Divida essa soma por 7 e verifique o o valor do resto da divisão.
6. Procure esse resto na tabela a seguir e terá o dia da semana do nascimento de qualquer pessoa que queira descobrir.

Figura 40 - Dias da semana

SEGUNDA-FEIRA	0	SEXTA-FEIRA	4
TERÇA-FEIRA	1	SÁBADO	5
QUARTA-FEIRA	2	DOMINGO	6
QUINTA-FEIRA	3		

Fonte: ([27]. p.14)

Exemplo:

Suponhamos que uma pessoa tenha nascido em 27 de julho de 1982. Qual foi o dia da semana que representa esta data?

1) (1982 – 1900), portanto, $A = 82$
2) $82 \div 4 = 20$, desconsidera-se o resto, então $B = 20$
3) O mês é julho, então $C = 6$ (Figura 39)

4) $x = 27$ (dia do nascimento), logo $D = 26\ (x - 1)$
5) Somando os quatro valores, obtemos: $82 + 20 + 6 + 26 = 134$, então, dividindo 134 por 7 temos como quociente 19 e o resto 1, logo a dia da semana referente a data acima é terça-feira, conforme figura 40.
   Vejamos o calendário de julho de 1982

Figura 41 - Julho 1982

calendário mensal		ANO 1982				www.jogral.com.br
julho						
Dom	Seg	Ter	Qua	Qui	Sex	Sab
				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

Fonte: http://www.jogral.com.br/calendario-mensal/, acesso em 28/07/15.

Justificativa matemática para o algoritmo: ([27]. p.14 – 15)

- Todos os passos que foram colocados no algoritmo visam determinar o "deslocamento", na sequência de dias da semana, partindo do fato de que o dia 1º de janeiro de 1900 foi uma segunda-feira.
- Cada ano de 365 dias tem o 1º de janeiro "afastado" de uma posição para a direita no ciclo dos dias da semana (segunda, terça, quarta, quinta, sexta sábado, domingo, segunda, terça, etc.) em relação ao dia da semana em que caiu o1º de janeiro do ano anterior, pois 365 dividido por 7 deixa resto 1.
- Quando fazemos a diferença entre o ano de nascimento e o ano 1900, calculamos quantos deslocamentos essa data sofreu em relação a data de 01/01/1900.
- Como 366 deixa resto 2 quando dividido por 7, então quando calculamos a quantidade de anos bissextos no passo 2, ao dividir o resultado do passo 1 por 4, estamos acrescentado ao deslocamento adicional mais uma "casa" no ciclo dos dias da semana para cada ano bissexto considerado.
- No passo 3 acrescentamos os deslocamentos gerados pelo mês e pelo dia da data procurada.
- Janeiro é a referência, portanto não há afastamento em relação a ele próprio. Por isso na tabela da figura 39, este mês está representado pelo número zero.

- Como o mês de janeiro tem 31 dias e 31 deixa resto 3 quando dividido por 7, então esse mês vai “empurrar” o primeiro dia do mês seguinte 3 “casas” para a direita em relação ao primeiro de janeiro daquele ano, por isso o mês de fevereiro está representado pelo número 3.
- Como fevereiro tem 28 dias e 28 deixa resto 0 quando dividido por 7 esse mês não irá acrescentar qualquer “deslocamento” adicional ao mês seguinte. Por isso o mês de março também é representado pelo número 3 na tabela (3+0).
- Como março tem 31 dias e 31 deixa resto 3 quando dividido por 7, esse mês vai “empurrar” os dias do mês seguinte (3+0+3) “casas” para a direita, portanto este mês será representado pelo número 6 na tabela.
- Como abril tem 30 dias e 30 deixa resto 2 quando dividido por 7, esse mês vai “empurrar” os do mês seguinte (3+0+3+2) “casas” para a direita, mas como a semana só tem 7 dias, na congruência módulo 7 o número 8 corresponde ao número 1, pois deixa resto 1 quando dividido por 7, ou seja avançar oito “casas” no ciclo dos dias da semana é o mesmo que avançar apenas uma “casa”. Por isso o mês de maio é representado pelo número 1 na tabela. Seguindo o mesmo raciocínio justificam-se os números que representam os demais meses.
- Os passos anteriores determinaram a quantidade de “casas” em que o primeiro dia do mês da data considerada está adiante, no ciclo dos dias da semana, do dia 1º de janeiro de 1900. Para finalizar precisamos determinar a quantidade de deslocamentos necessários para atingirmos a dia da data procurada.
- Se encontrarmos o dia 1 e queremos o dia x de um determinado mês basta fazer um deslocamento de $(x - 1)$ “casas” para a direita no ciclo dos dias da semana.
- Para finalizar soma – se os quatro valores obtidos nos passos anteriores. O valor dessa soma será congruente módulo 7 ao valor k, esse k é o dia da semana da data procurada representado na tabela da figura 40.

3.8 ALGORITMOS PARA TESTES DE PRIMALIDADE

Hoje, mais do que nunca, o uso de informações é de fundamental importância na vida das pessoas, principalmente com o advento da internet, das transações bancarias e senhas as mais diversas. Estamos cada vez mais imersos nessa tecnologia, seja para enviar uma mensagem para um amigo, guardar informações ou dados em uma nuvem, fazer compras,

efetuar transações bancárias, buscar algum conhecimento na rede, ouvir música, assistir filmes, porém, necessitamos e exigimos que haja segurança nessas transações.

Uma técnica usada para que as informações cheguem ao destinatário de forma segura é a que usa criptografia. Criptografia palavra de origem grega; Cripto (escondido) e Grafia (escrita) consiste em técnicas que fazem com que a informação original seja transformada numa informação que não possa ser entendida por possíveis bisbilhoteiros, de forma que só possa ser conhecida por quem a enviou e pelo seu destinatário. Existem vários algoritmos matemáticos que criptografam uma mensagem, o mais conhecido é o RSA criado por Ronald Rivest, Adi Shamir e Leonard Adleman em 1978. Este algoritmo utiliza o produto de dois números primos para cifrar uma mensagem, caso alguém que não seja o destinatário queira decifrar a mensagem deve descobrir quais são os dois números primos usados.

A decodificação de mensagens que utilizam o RSA traz à tona outro tema que, assim como a criptografia, é bem antigo: a fatoração de um número, ou ainda a descoberta se um número é primo ou composto. O primeiro algoritmo para este fim é o Crivo de Eratóstenes.

3.8.1 Crivo de Eratóstenes

Eratóstenes, foi um matemático grego do século II a.C. um verdadeiro polímata. Além de seu algoritmo de primalidade, outro trabalho notável seu foi conseguir medir a circunferência da Terra com precisão impressionante para a época.

O *crivo* atua como uma peneira que se aplicado aos inteiros positivos ímpares maiores que $n > 2$, pois 2 é o único primo par, retém os números primos, mas deixa passar os compostos.

O algoritmo consiste em escolher um número *n* e montar uma lista com todos os números ímpares *m*, tais que $1 < m \leq n$. Funciona da seguinte maneira:

1º passo: Listamos os números de 3 até *m.*

2º passo: Risca-se todos os números da lista que são múltiplos de 3.

3º passo: Observa-se o menor valor da lista que não está riscado, no caso é o 5. Risca-se todos os múltiplos de 5 maiores que ele mesmo.

E assim por diante até que se tenha usado todos os números menores ou iguais a $\sqrt{n}$. Os números que não foram riscados são todos os primos p com $2 < p \leq n$.

O ponto de parada em $\sqrt{n}$ deve-se ao fato de que estamos riscando os múltiplos de p, ou seja, de p em p e se $p > \sqrt{n}$, então o menor composto que ainda não foi riscado em uma etapa anterior seria $p^2 > n$, que está fora da lista.

Exemplo: Vamos utilizar o Crivo de Eratóstenes para encontrar todos os primos até 100.

Listamos os ímpares de 3 a 99.

	3	5	7	9
11	13	15	17	19
21	23	25	27	29
31	33	35	37	39
41	43	45	47	49
51	53	55	57	59
61	63	65	67	69
71	73	75	77	79
81	83	85	87	89
91	93	95	97	99

Riscamos os múltiplos de 3.

	3	5	7	~~9~~
11	13	~~15~~	17	19
~~21~~	23	25	~~27~~	29
31	~~33~~	35	37	~~39~~
41	43	~~45~~	47	49
~~51~~	53	55	~~57~~	59
61	~~63~~	65	67	~~69~~
71	73	~~75~~	77	79
~~81~~	83	85	~~87~~	89
91	~~93~~	95	97	~~99~~

Procedemos da mesma forma com os múltiplos de 5 e 7

	3	5	7	~~9~~
11	13	~~15~~	17	19
~~21~~	23	~~25~~	~~27~~	29
31	~~33~~	~~35~~	37	~~39~~

41 43 ~~45~~ 47 ~~49~~

~~51~~ 53 ~~55~~ ~~57~~ 59

61 ~~63~~ ~~65~~ 67 ~~69~~

71 73 ~~75~~ ~~77~~ 79

~~81~~ 83 ~~85~~ ~~87~~ 89

~~91~~ ~~93~~ ~~95~~ 97 ~~99~~

Como o próximo primo seria 11 que é maior do que $\sqrt{100} = 10$, encerramos o processo. Portanto, temos todos os primos até 100;
$(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 \text{ e } 97)$.

Para números primos muitos grandes este algoritmo torna-se inviável, então muitos matemáticos estudaram e ainda buscam por algoritmos que obtenham de forma mais rápida este resultado.

3.8.2 Algoritmo de Fermat

Pierre de Fermat foi um matemático francês que viveu no século XVII, deixou importantes contribuições para a matemática, tendo a teoria dos números como sua maior paixão.

Fermat criou um algoritmo que nos permite encontrar fatores de um número, principalmente se tivermos $n = ab$, com *a* e *b* relativamente próximos entre si e *n* ímpar.

Proposição: Seja $n \in \mathbb{N}$ ímpar. Existe uma correspondência biunívoca entre os pares (x, y), com $0 \leq y \leq x \leq n = x^2 - y^2$, e (r, s), com $1 \leq s \leq r \leq n = rs$.

Demonstração: sendo $n = x^2 - y^2$, podemos tomar $r = x + y$ e $s = x - y$, de forma que $n = x^2 - y^2 = (x + y) \cdot (x - y) = rs$.

Por outro lado, como *n* é ímpar, e $n = rs$, tanto *r* quanto *s* devem ser ímpares também, o que implica que $\frac{r \pm s}{2}$ é inteiro. Se tomarmos $x = \frac{r+s}{2}$ e $y = \frac{r-s}{2}$, teremos $0 \leq y \leq x \leq n$ e $x^2 - y^2 = \left(\frac{r+s}{2}\right)^2 - \left(\frac{r-s}{2}\right)^2 = \frac{(r^2+2rs+s^2)-(r^2-2rs+s^2)}{4} = \frac{4rs}{4} = rs = n.$ ■

Desta proposição decorrem duas consequências:

Seja $n \in \mathbb{N}$ ímpar

i) Para cada decomposição distinta de n, $n = rs$, existe uma decomposição como diferença de quadrados, $n = x^2 - y^2$.

ii) n é primo $\Leftrightarrow n = \left(\frac{n+1}{2}\right)^2 - \left(\frac{n-1}{2}\right)^2$ é a única decomposição possível de n como diferença de quadrados.

O algoritmo consiste em supormos que $n = x^2 - y^2$, o que pode ser feito, pois n é ímpar e todo número ímpar pode ser escrito como a diferença de dois quadrados. Como $x^2 - y^2 = (x + y) \cdot (x - y)$, temos $a = (x - y)$ e $b = (x + y)$.

Devemos então procurar $[\sqrt{n}]$, a parte inteira de $\sqrt{n}$. Caso $\sqrt{n}$ seja inteiro, sabemos que ele é um dos fatores de n. Caso contrário, acrescentamos uma unidade a $[\sqrt{n}]$e dizemos que $[\sqrt{n}] + 1 = x$ é um candidato a fator de n.

Para sabermos se esse x é mesmo o fator de n, temos que calcular $y = \sqrt{x^2 - n}$, caso y seja inteiro, calculamos a e b a partir desse x e y. Caso contrário, devemos acrescentar outra unidade ao nosso candidato a fator de n e repetir o processo até que encontramos y inteiro ou $x = \frac{n+1}{2}$.

Se o processo se estender até termos $x = \frac{n+1}{2}$, então sabemos que n é primo. ([18], p.47 - 48).

Atualmente com o avanço computacional este algoritmo não está otimizado, mas para a época em que Fermat o desenvolveu era bastante eficiente.

O *Pequeno Teorema de Fermat* também fornece um simples e conveniente teste de primalidade.

***Teorema*:** (Pequeno Teorema de Fermat) Se p é um número primo, então para qualquer inteiro a, vale:

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

O teste de Fermat consiste em tomarmos um número a qualquer e calcularmos $a^{p-1}\ (mod\ p)$, onde p é o número cuja primalidade queremos atestar.

Portanto, há dois possíveis resultados:

1) Caso $a^{p-1} \equiv 1\ (mod\ p)$, então provavelmente p é primo, podendo o teste ser repetido para valores diferentes de a, afim de obter uma probabilidade melhor de que p seja primo
2) Caso $a^{p-1} \not\equiv 1\ (mod\ p)$, confirmamos que p é composto, e assim encerra o teste.

Uma limitação deste teste é que existem números que independente do valor de a escolhido, o teste sempre retorna números primos, apesar dos números serem compostos.

Exemplo: $2^{340} \equiv 1\ (mod\ 341)$ mas $341 = 11.31$, não é primo.

Com os avanços tecnológicos também cresceu a necessidade de proteger dados sigilosos assim como a privacidade das pessoas e com máquinas cada vez mais sofisticadas, rápidas e potentes outros testes de primalidade vão sendo estudados e aperfeiçoados:

- Teste de Primalidade de Euler
- Teste de Primalidade de Miller – Rabin
- Teste de Primalidade de Lucas – Lemer
- Teste de Primalidade AKS

3.8.3 Teste de Primalidade AKS

O teste (algoritmo) de primalidade AKS foi desenvolvido em 2002 pelos indianos Manindra Agrawal; Neeraj Kayal; Nitin Saxena. O teste está fundamentado no pequeno teorema de Fermat e uma de suas variações. É considerado um marco na história dos algoritmos de primalidade, pois se trata do primeiro teste que consegue ao mesmo tempo ser determinístico com um tempo de execução polinomial podendo ser executado em computadores comuns com memória adequada.

O teste está fundamentado na seguinte congruência entre polinômios: Seja a um inteiro e p um natural, $p \geq 2$ e $mdc(a, n) = 1$. Então p é primo se, e somente se,

$(x + a)^p \equiv x^p + a\ (mod\ p)$.

Cada algoritmo vai sendo generalizado e aperfeiçoado dando origem a métodos bastante eficientes para determinar a primalidade de um número. Várias versões do algoritmo AKS começaram a surgir tão logo o artigo de Agrawal, Kayal e Saxena foi postado na web.

A solução de um problema matemático, como na ciência em geral, abre caminhos para outros resultados, como no caso do algoritmo AKS.

4. ALGORITMOS NO COTIDIANO

O texto publicado na edição impressa do jornal Gazeta do Povo em 12 de junho de 2011, “O uso cotidiano do algoritmo”, retrata bem o quanto usamos os algoritmos em nosso dia a dia nas mais diversas atividades.

> Com mais de 500 milhões de usuários, o Facebook é um sucesso global pelos recursos de conectividade entre as pessoas, desenvolvidos a partir de algoritmos. Na medicina o uso de algoritmos é difundido na análise de tomografias radiografias e ressonâncias magnéticas. (...) O próximo passo, garantem os cientistas é criar algoritmos para analisar sintomas e sugerir diagnósticos, Jayme Luiz Szwarcfiter, especialista em algoritmos, prevê que a ferramenta deve encontrar resistência. “os médicos não gostam da ideia, pois pensam que o programa pode substituí-los. Mas o que o software vai fazer é acumular uma série de informações sobre sintomas e, a partir do exame, apontar possíveis doenças.” [30]

Assistimos passivamente como as fórmulas matemáticas participam cada vez mais de nossas atividades corriqueiras.

> O jornalista Ken Schwencke, do Los Angeles Times, estava dormindo quando, às 6h25 do dia 17 de março, um terremoto sacudiu a Costa Oeste dos EUA. Com o susto, correu para o computador e descobriu que Quakebot, um algoritmo que ele criou, já havia escrito um texto sobre o assunto. O jornal deu um furo de reportagem noticiando os detalhes do tremor antes de todos os outros e fez a fama do algoritmo, que se conecta automaticamente com o serviço Geológico dos EUA e escreve pequenas notas com os dados. (Revista Galileu)

Um algoritmo, isto é, o conjunto de regras e operações para fazer cálculos, realizar tarefas ou solucionar problemas, por mais complexo que seja não passa de uma fórmula seguindo regras predefinidas.

A Matemática está em toda a parte, frase pronunciada por quase todos os professores de Matemática. Com o processamento das informações e, por conseguinte o uso de algoritmos computacionais muito conhecimento matemático torna-se ainda mais necessário em nossas ações. Entre os algoritmos mais utilizados está o de pesquisa do Google que, quando bem usado consegue encontrar a informação que estamos buscando. Outros algoritmos são capazes de detectar doenças em recém-nascidos, outros minimizam ou evitam engarrafamentos no trânsito, ainda outros são capazes de negociar ações em bolsa de valores e existem até algoritmos que influenciam relacionamentos íntimos como o ***okcupid***, fazendo perguntas e pelas respostas dadas, estes sites de namoro tentam ajudar a formar casais de namorados entre seus usuários, fornecendo os dados para os algoritmos de compatibilidade que possam existir entre as pessoas cadastradas.

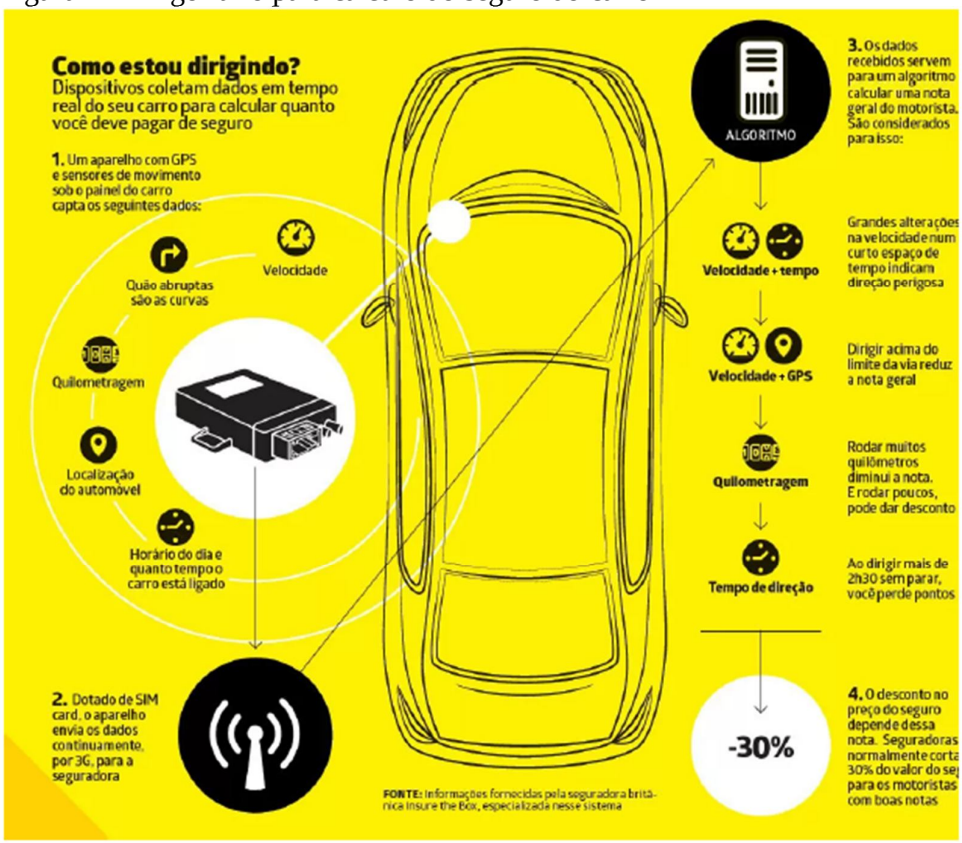
> Para calcular uma porcentagem entre você e outra pessoa, o algoritmo irá levar em consideração nos resultados das perguntas da pesquisa, três aspectos: qual sua

> resposta, qual a resposta que você gostaria que a outra pessoa desse, e o quão importante a questão é para você. No programa de computador, esses valores abstratos são atribuídos à números, que são agrupados em uma porcentagem de combinação. (retirado do BLOG: http://go2web.com.br/pt-br/blog)

Na Fórmula 1 os algoritmos também aceleram. Simon Williams defende que uma escuderia campeã precisa de boas fórmulas matemáticas. Numa corrida é calculado em tempo real fatores como desgaste de pneus, *pit-stops* e estratégias de pilotos; esses dados geram gráficos que dão informações para a equipe sobre melhor momento de parada, qual pneu colocar e qual estratégia usar de acordo com todos os parâmetros embutidos nos cálculos. ([30])

Seguradoras também já usam sensores acoplados nos carros para alimentar fórmulas que interferem no valor do seguro de acordo com o comportamento do condutor. A figura abaixo mostra como funciona.

Figura 42 - Algoritmo para cálculo do seguro do carro



Fonte: http://revistagalileu.globo.com/Revista/noticia/2014/05/como-os-algoritmos-dominaram-o-mundo.html

No mercado financeiro, os *softwares* são programados com algoritmos para obter ganhos em volume a partir de transações pequenas. Sócio fundador da Trade Gráfico, Carlos

Martins afirma que as vantagens que os algoritmos levam sobre os operadores de carne e osso são incontáveis. “O mercado de ações exige disciplina, dedicação e sangue frio. Ao contrário dos humanos, os algoritmos trabalham 24 horas por dia, fazem sempre a mesma coisa, sem fugir de regras, e não têm medo de operar”. Enquanto os corretores humanos costumam comprar algumas ações pela manhã e vender outras à tarde, os programas de computador conseguem operar em uma escala sobre-humana negociando centenas de ações em segundos e obtendo como lucro, centavos, em cada uma. ([30])

Figura 43 - Máquinas de apostar

Fonte: http://revistagalileu.globo.com/Revista/noticia/2014/05/como-os-algoritmos-dominaram-o-mundo.html

Por outro lado, como um algoritmo opera em alta velocidade, caso ocorra um erro, ocasionará danos em proporções bem maiores. Em 2010, o índice da bolsa de Dow Jones despencou 1000 pontos em 20 minutos por conta de um algoritmo. No dia 2 de agosto de 2012, um *bug* na instalação de um *software* resultou na compra desordenada de milhões de ações por preços ruins, essa transação fez, com que a *Knight*, empresa de transações de alta frequência perdesse US$ 440 milhões em 45 minutos. A livraria Bordebook colocou um algoritmo para reajustar automaticamente o preço de um livro sobre moscas na Amazon sempre que a concorrente também reajustasse. Só que a concorrente fez o mesmo. Isso levou a muitíssimos reajustes e o livro chegou a ser oferecido por US$ 23,6 milhões!!

Os algoritmos permitem que máquinas realizem tarefas em escalas maiores e muitas vezes melhores que as realizadas pelos humanos, mas que sem a supervisão da

inteligência humana podem causar grandes transtornos como foi relatado nos casos acima. A Física busca entender as leis que regem o mundo e para expressar este conhecimento a linguagem é sempre a matemática: a Química e a Biologia também fazem amplo uso da Matemática. Praticamente não existe ramo do conhecimento humano que não envolva o uso da Matemática Deve-se então incentivar o seu ensino e aprendizado de forma permanente reavaliando estratégias e métodos de forma continuada.

Por fim, não se pode omitir o mais importante algoritmo, executado trilhões de vezes dia e noite há bilhões de anos: o algoritmo da divisão celular. Ele é mencionado por último não porque não seja importante mas, porque não faz parte da Matemática e sim, da Biologia. Sem ele não estaríamos aqui.

Em 1948 o matemático John von Neumann publicou um trabalho matemático sobre robôs capazes de se auto reproduzir que teve grande impacto no meio científico. O que ele mostrou é basicamente o que veio a ser descoberto no início dos anos cinquenta sobre o código genético por Francis Click e James Watson. É claro que nesta época muito já era conhecido sobre a vida e seus processos. Von Neumann não foi o único matemático a prever a existência de um código (algoritmo) da vida: um outro matemático que se interessou pelo assunto foi George Gamov, também no final dos anos quarenta. Sem dúvida, o algoritmo (código que executa este algoritmo) da vida é mesmo o mais importante entre todos.

6. CONSIDERAÇÕES FINAIS

A partir do século XVII os algoritmos matemáticos tem tido um crescimento vigoroso e cada vez mais intenso. Nos últimos cem anos seu uso se espalhou por quase todos os ramos, principalmente a partir dos anos 80 do século XX devido ao uso de computadores em larga escala, a civilização voltaria à barbárie se seu uso fosse descontinuado. Portanto, no ensino da Matemática deve ser enfatizado o estudos dos algoritmos para que o aprendizado seja cada vez mais satisfatório e coerente com o que é ensinado.

Seu ensino deve ser reforçado a partir da Educação Básica como um recurso para tornar a Matemática melhor compreendida e mais agradável aos alunos. Na Educação Básica é mister mostrar que as operações de soma, diferença, multiplicação e divisão são algoritmos. Isso feito deve-se prosseguir pelos algoritmos para extração de raízes, para o cálculo do MMC, do MDC e testes de primalidade, bem como proporcionar aplicações destes algoritmos na vida prática das pessoas.

Não se teve a pretensão de fazer uma análise mais aprofundada dos algoritmos aqui apresentados, mas sim de trazer ao leitor informações relevantes como outras formas de desenvolver esses algoritmos e de como os matemáticos de antigamente manuseavam esses algoritmos bem como algumas aplicações interessantes em nosso cotidiano e de como são fundamentais para a evolução da tecnologia e de grandes avanços da Ciência.

Aqui foram contemplados apenas alguns poucos algoritmos visto que é um assunto muito vasto.

Aos professores de Matemática, principalmente os que lecionam na Educação Básica espero ter contribuído com informações úteis para suas aulas ou que sirvam de embasamento em sua formação acadêmica e que incentivem a busca de novos conhecimentos.

É importante ressaltar que a Matemática principalmente na Educação Básica necessita de estímulos motivadores para que os educandos tenham uma melhor compreensão do que lhes é ensinado e apresentem consequentemente melhores resultados não só na sua vida de estudante como também na vida profissional. O estudo dos algoritmos aqui apresentados é uma das formas de tornar o aprendizado da Matemática ensinada nas escolas mais atraente e significativo sabendo, entretanto este esforço sozinho não será capaz de reverter o quadro presente sem que os outros parâmetros mencionados no início sejam levados em consideração. Só um esforço bem planejado e continuado (uma política de governo) que abranja os diversos gargalos da escola pública brasileira poderá tirar do fundo do poço o aprendizado da Matemática em nosso País.

REFERÊNCIAS

[1] AMARAL, João Tomas do. **Método de Viéte para resolução de equações do 2ºgrau**. RPM, Revista do Professor de Matemática Nº.13. Julho/1988.

[2] ANDRADE, Bernardino Carneiro. **A evolução histórica da resolução das equações do 2º grau**. Tese (Mestrado) Departamento de Matemática Pura da Faculdade de Ciências da Universidade do Porto. 2000.

[3] BERLINSKI, David, 1942, O advento do algoritmo: a idéia que governa o mundo; tradução Leila de Souza Mendes. São Paulo, Globo, 2002

[4] BOYER,C.B. História da matemática. Trad: Elza F. Gomide. São Paulo, Edgard/Blucher, 1996.

[5] BRASIL. Ministério da Educação. Secretaria de Educação Média e Tecnológica. *Parâmetros Curriculares Nacionais (Ensino Médio)*. Brasília: MEC, 2000.

[6] BRYSON, Bill. Em casa - Uma breve história da vida doméstica, ed. Companhia das letras.

[7] CARVALHO, Silva Beatriz Fagundes. **Resolução de equações de 2º grau: Uma abordagem metodológica**. 2008, Monografia, Centro Universitário Franciscano (UNIFRA), Santa Maria – RS.

[8] CHEVALLAR, Y., BOSCH, M. e GÁSCON, J. Estudar Matemáticas: o elo perdido entre o ensino e a aprendizagem. Porto Alegre: Artmed, 2001.

[9] EVES, Howard. Introdução à história da matemática. 2º ed. UNICAMP, 2002.

[10] Explorando o ensino da Matemática : artigos : volume 1 / seleção e organização Ana Catarina P. Hellmeister...[et al.] ; organização geral Suely Druck. - Brasilia : Ministério da Educação, Secretaria de Educação Básica, 2004. 240 p.

[11] FERREIRA, Danielle e SÔNEGO, Dubes. A reputação da matemática: exemplo de fracasso. **Revista Cálculo**, São Paulo, v.4, n.47, p.38-45, dez./2014.

[12] FONSECA FILHO, Cléuzio. **História da computação [recurso eletrônico]: O Caminho do Pensamento e da Tecnologia** / Cléuzio Fonseca Filho. – Porto Alegre: EDIPUCRS, 2007. 205 p. disponível em http://www.pucrs.br/orgaos/edipucrs

[13] GONÇALVES, Alex Oleandro. **Algoritmos: uma perspectiva de professores de quarta e quinta séries do ensino fundamental**. Dissertação de Mestrado – Programa de Pós-graduação em Educação Matemática. Universidade Federal do Paraná, Paraná, 2010.

[14] GONÇALVES, Otânio Alves, CARDOSO, Mário Lúcio. **Uma interpretação geométrica do MMC.** Coleção explorando o ensino da matemática, Brasília, 2004.

[15] HODGSON, B. **Uma breve história da quinta operação**. Gazeta de Matemática, 2008. Portugal, n. 156, p. 730, 2008. Disponível em: <http://gazeta.spm.pt-/_chagazeta?id=156>. Acesso em: 17 abr. 2015.

[16] IFRAH, Georges. História Universal dos Algarismos: A inteligência dos homens contada pelos números e pelo cálculo. Tomo 2. Rio de Janeiro: Editora Nova Fronteira, 1997.

[17] MANDARINO, Mônica Cerbella Freire. BELFORT, Elizabeth. **Números naturais: conteúdo e forma**. Universidade Federal do Rio de Janeiro, Laboratório de Pesquisa e Desenvolvimento em Ensino de Matemática e Ciências, Rio de Janeiro, 2005.

[18] Morimoto, Ricardo Minoru. **Números Primos: Propriedades, Aplicações e Avanços.** Dissertação(mestrado). Universidade Estadual Paulista, Instituto de Geociências Exatas, Rio Claro - SP, 2014.

[19] NOBRE, Sergio. **História da resolução da equação de 2º grau: Uma Abordagem Pedagógica.** Coleção história da matemática para professores. ed. Sociedade Brasileira de História da Matemática. Rio Claro – SP. Abril 2003

[20] PATERLINI, Roberto Ribeiro. ***Um método para o cálculo do mdc e do mmc.***, Revista do Professor de Matemática (RPM) nº13 p.36 julho/1988

[21] **Pedagógica**. Coleção histórica da Matemática para professores. ed. Sociedade Brasileira de História da Matemática. Rio Claro – SP: Abril 2003.

[22] PEDROSO, Hermes Antônio. **Uma breve história da equação do 2º grau**. Revista Eletrônica de Matemática (REMat). São Paulo, ISSN 2177-5095, n. 2 – 2010. Disponível em <www2.jatai.ufj.br/ojs/index.php/matemática> Acesso em 12 de maio de 2015

[23] PISA: desempenho do Brasil piora em leitura e "empaca" em ciências. Disponível em <http://educacao.uol.com.br/noticias/2013/12/03/pisa-desempenho-do-brasil-piora-em-leitura-e-empaca-em-ciencias.htm> Acessado em 27/02/2015

[24] POLEZZI, Marcelo. ***Como obter o MDC e o MMC sem fazer contas?*** Explorando o ensino da matemática. v.1, Cap.3, p. 87-88. Ministério da Educação. Brasília, 2004

[25] **René Descartes** (1637/1894), La Geométrie. Versão em francês moderno em: Auguste Comte, La géométrie analytique. Paris, Louis Bahl.

[26] ROQUE, T. História da Matemática: uma visão crítica, desfazendo mito s e lendas. Rio de Janeiro. Zahar. 2012.

[27] SÁ, Ilydio Pereira de Sá. **Aritmética Modular e algumas de suas aplicações**. Disponível em http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf, Acesso em 28/07/15.

[28] SILVA, Andreilson Oliveira da. **O Cálculo da Raiz Quadrada Através dos Séculos**. Dissertação de Mestrado – PROFMAT. Universidade Federal de Paraíba, Paraíba, 2013.

[29] SOARES, José Francisco. **Projeto: As evidências do SAEB e avaliações correlatas sobre o impacto das estruturas sociais e da organização das escolas e dos sistemas de ensino no desempenho dos alunos da educação básica**. Disponível em http://portal.inep.gov.br/web/observatorio-da-educacao/ Acesso em 19/09/15.

[30] TAVARES, Osny. O uso cotidiano do algoritmo. Jornal Gazeta do povo, São Paulo, Junho/2011, disponível em www.gazetadopovo.com.br acesso em 09/07/15