UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

Mestrado Profissional em Matemática em Rede Nacional – PROFMAT

CARLOS COSTA DOS REIS

OFICINA DE ARITMÉTICA: O USO DOS NÚMEROS PRIMOS NA RESOLUÇÃO DE PROBLEMAS E ALGUMAS CURIOSIDADES

VITÓRIA/ES

2014

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

Centro de Ciências Exatas

Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT

"Oficina de Aritmética: O Uso dos Números Primos na Resolução de Problemas e Algumas Curiosidades"

Carlos Costa dos Reis

Defesa de Dissertação de Mestrado Profissional submetida ao Programa de Pós-Graduação em Matemática em Rede Nacional da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 14/04/2014 por:

Valmecir Antonio dos Santos Bayer
Orientador - UFES

Moacir Rosado Filho
Examinador Interno - UFES

Silas Fantin
Examinador Externo - UNIRIO

Dados Internacionais de Catalogação-na-publicação (CIP)

(Biblioteca Central da Universidade Federal do Espírito Santo, ES, Brasil)

Reis, Carlos Costa dos, 1981-

R375o Oficina de aritmética : o uso dos números primos na resolução de problemas e algumas curiosidades / Carlos Costa dos Reis. – 2014.

74 f. : il.

Orientador: Valmecir Antonio dos Santos Bayer.

Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Aritmética - Estudo e ensino. 2. Números primos. 3. Solução de problemas. I. Bayer, Valmecir Antonio dos Santos. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

DEDICATÓRIA

Dedico este trabalho à minha esposa Giselle que tanto me motivou e ajudou na organização dos trabalhos e pela compreensão quanto às minhas horas dedicadas aos estudos, aos meus pais Laurindo e Valdeci, aos meus irmãos Clovis e Cláudia por toda a dedicação da vida em família e meus sogros Vandir e Maria Cimar pela motivação e preocupação quanto aos altos e baixos no meu caminho até mais essa vitória.

Agradecimentos

Agradeço a Deus pelos dons da ciência e da sabedoria, pela oportunidade de poder estudar e complementar minha graduação com este curso de mestrado. Agradeço também ao professor e orientador Valmecir Antonio dos Santos Bayer, pela dedicação e atenção dispensada sempre que solicitado, demonstrando sempre boa vontade em ensinar e orientar nas dúvidas em relação à elaboração deste trabalho, aos professores Moacir Rosado Filho, Etereldes Gonçalves Junior e Fábio Júlio da Silva Valentin pelas produtivas aulas que ministraram contribuindo para minha formação e idealização desse trabalho e ao professor Florêncio Ferreira Guimarães Filho que, como coordenador regional, desempenhou muito bem seu papel de motivador e orientador nas demandas de todos os mestrandos.

Resumo

Este projeto traz uma proposta de oficina didática para professores e alunos dos ensinos fundamental e médio trabalharem, nas aulas ou mesmo no aprimoramento para turmas que se preparam para as olimpíadas de matemática, técnicas de resolução de problemas envolvendo números primos. A sequência dos capítulos expõe a teoria básica, breve argumentação sobre resolução de problemas, problemas diversos sobre números primos e suas resoluções e, por fim, artigos sobre curiosidades no mundo inteiro a respeito dos números primos.

Palavras – Chave: oficina de aritmética; números primos; resolução de problemas; curiosidades.

Abstract

This project presents a didactic workshop proposal for primary and high school teachers and students to work with problem-solving techniques involving prime numbers in class, or even for the improvement of groups which are preparing themselves for Mathematics Olympiads. The chapters sequence exposes the basic theory, a brief argumentation about problem solving, many issues concerning prime numbers and its resolutions, and lastly, articles on prime numbers worldwide curiosities.

Key-words: arithmetic workshop; Prime Numbers; Problems resolutions; Curiosities.

Sumário

01. Introdução

Este trabalho vem expor um contexto técnico, prático e histórico sobre o uso dos números primos. Pesquisando sobre o assunto verificamos que, além de muito interessante no que diz respeito aos conhecimentos teóricos e suas curiosidades, existem poucos trabalhos ou artigos sobre números primos. Nos livros didáticos aparecem a teoria e muitos exercícios, quase sempre mecânicos, que não exigem muito do aluno. Quando falamos em exigência, queremos dizer: pensar e se sentir atraído pelo assunto a ponto de buscar se aprofundar mais e o levando a fazer uso no seu cotidiano.

Leciono a disciplina de Matemática para turmas de Ensino Fundamental e Médio há aproximadamente oito anos e sempre complementei meu trabalho com atividades extras para melhorar o desempenho das turmas em sala de aula ou mesmo motivar os alunos a participar das olimpíadas. Nos últimos anos, vivenciando momentos ricos e curiosos em sala de aula, decidi buscar um aprofundamento sobre o assunto *Números Primos*. Trabalhando este conteúdo e ampliando o conhecimento sobre múltiplos e divisores, fui abordado por um aluno do sexto ano do ensino fundamental (antiga 5ª série) com a seguinte afirmação: "*Professor, todo número quadrado perfeito possui apenas três divisores naturais*". Fiquei admirado com a maturidade da afirmação desse aluno e motivado a buscar formas de levar outros alunos a entrarem no mundo da Matemática com o mesmo prazer que este aluno tem demonstrado durante o processo de aprendizagem.

O Ministério da Educação, por meio dos Parâmetros Curriculares Nacionais de Matemática, destaca esse momento com meu aluno e incentiva a continuidade desta oficina de aritmética ao dizer que

> [...] as necessidades cotidianas fazem com que os alunos desenvolvam uma inteligência essencialmente prática, que permite reconhecer problemas, buscar e selecionar informações, tomar decisões e, portanto, desenvolver uma ampla capacidade para lidar com a atividade matemática. Quando essa capacidade é potencializada pela Escola, a aprendizagem apresenta melhor resultado. ([02], p. 29)

e, completa:

> [...] um conhecimento só é pleno se for mobilizado em situações diferentes daquelas que serviram para lhe dar origem. Para que sejam transferíveis a novas situações e generalizados, os conhecimentos devem ser descontex-tualizados, para serem contextualizados novamente em outras situações.

> Mesmo no ensino fundamental, espera-se que o conhecimento aprendido não fique indissoluvelmente vinculado a um contexto concreto e único, mas que possa ser generalizado, transferido a outros contextos. ([02], p. 30).

Nesse processo de pesquisa e aprofundamento observamos melhor as histórias e curiosidades sobre os números primos. Relações do nosso cotidiano que aparecem pouco nos canais de informação, numa intensidade menor ainda nos livros didático, mas que no processo de planejamento de aula do professor se torna uma área muito rica para se explorar. Visando tornar a aula atrativa e motivadora o professor pode agregar história e curiosidades aos desenvolvimentos teóricos fazendo o aluno enxergar a Matemática por completo, não apenas como livros de teorias maçantes que calejam a relação professor x aluno. Assim como é destacado nas páginas do PCN de Matemática:

> [...] O conhecimento da história dos conceitos matemáticos precisa fazer parte da formação dos professores para que tenham elementos que lhes permitam mostrar aos alunos a Matemática como ciência que não trata de verdades eternas, infalíveis e imutáveis, mas como ciência dinâmica, sempre aberta à incorporação de novos conhecimentos. ([02], p.30).

> [...] Numa perspectiva de trabalho em que se considere a criança como protagonista da construção de sua aprendizagem, o papel do professor ganha novas dimensões. Uma faceta desse papel é a de organizador da aprendizagem; para desempenhá-la, além de conhecer as condições socioculturais, expectativas e competência cognitiva dos alunos, precisará escolher o(s) problema(s) que possibilita(m) a construção de conceitos/procedimentos e alimentar o processo de resolução, sempre tendo em vista os objetivos a que se propõe atingir. ([02], p. 30 - 31).

Por fim, esperamos com esta oficina didática proporcionar opções para o desenvolvimento da Matemática de uma forma lúdica e participativa, sem perder, porém, o prazer em aprofundar-se nos conhecimentos teóricos a partir das curiosidades que os números primos trazem ao nosso cotidiano.

1.1 – Justificativa

Observando trabalhos, oficinas e grupos de estudos para turmas olímpicas, é perceptível uma grande carência no estudo e na demonstração de aplicabilidade dos números primos na resolução dos problemas voltados para turmas do ensino fundamental II. Sabemos do uso dos números primos em algumas áreas da tecnologia e segurança (criptografia, senhas, códigos, etc.), mas, paralelo a isso não é de fácil acesso um estudo, ainda que mais superficial, sobre o assunto de forma a motivar os alunos ao aprofundamento e novas descobertas sobre o tema.

Este trabalho traz uma oportunidade a professores, alunos, leitores e curiosos de conhecer teoria, problemas e métodos de resolução, com uma linguagem simples, porém com uma abordagem ampla no que diz respeito a aplicações da teoria na resolução dos problemas propostos nos livros didáticos, materiais para concursos ou mesmo em grupos de estudos para a preparação de alunos para as olimpíadas. A essência desse trabalho não é alimentar ainda mais as competições olímpicas e sim estimular o estudo da Matemática com as aplicações e curiosidades sobre os números primos.

Alguém já ouviu falar sobre a mística que tem sobre os números dos jogadores de futebol, em especial o time galático do Real Madri (Espanha) há dez anos? Com certeza a mídia futebolística nunca falou em uma transmissão de um jogo de futebol que os galáticos tinham nas costas números primos como identificação dentro de campo. Mais ainda, pouco se sabe sobre as culturas de cigarras que espantam populações em algumas regiões dos Estados Unidos aparecendo, sincronizadamente, em intervalos de 13 ou 17 anos. As relações dos números primos com a teoria musical, entre outras situações muito curiosas no nosso dia a dia, merecem destaque. É esse o papel deste projeto, ampliar a cultura e o conhecimento matemático, mostrando as problemáticas das teorias e as aplicações e curiosidades da vida real.

1.2 – Objetivos

1.2.1 – Objetivos Gerais

Conhecer a Matemática em seus usos, como uma das linguagens humanas, explorando suas estruturas e seus raciocínios. Oportunizar aos alunos e leitores o desenvolvimento de estratégias (selecionar, organizar, relacionar dados e informações representados de diferentes formas) para resolver problemas e a apresentação de uma literatura voltada para a Matemática e suas pesquisas, desenvolvendo hábitos de leitura e de estudo.

1.2.2 – Objetivos Específicos

- Oportunizar um momento de aprofundamento de estudos sobre aritmética;
- Identificar algumas lacunas no processo de aprendizagem dos estudantes do ensino fundamental no que diz respeito ao ensino da Matemática;
- Desenvolver o raciocínio lógico e a busca por métodos e procedimentos nas resoluções de problemas;
- Incentivar o estudo da aritmética e suas aplicações;
- Conhecer e fazer uso das literaturas disponíveis sobre a Matemática;

02. Um Pouco de História

“Podemos em especial nas ciências matemáticas, observar a ordem, a simetria e a restrição; e estas são as formas superiores do belo.” Aristóteles, Metafísica.

Os números primos, e as suas propriedades, foram estudados extensivamente pela primeira vez pelos antigos matemáticos Gregos. Os matemáticos da escola de Pitágoras (500 a 300 a.C.) estavam interessados nos números pelas suas propriedades numerológicas e místicas. Entendiam a ideia de primalidade, e revelavam interesse em números perfeitos e amigáveis (um número n natural é perfeito se ele for igual a soma dos seus divisores próprios, isto é, dos divisores positivos menores que n, por exemplo, o número *6* tem como divisores naturais *1, 2, 3* e *1 + 2 + 3 = 6*, *28* tem como divisores naturais *1, 2, 4, 7, 14* e *1 + 2 + 4 + 7 + 14 = 28*). Um par de números amigáveis é, por exemplo, *220* e *284*, e são tais que, os divisores naturais de um somam-se ao do outro e vice-versa.

Quando *Os Elementos* de Euclides apareceram (cerca de 300 a.C.) já muitos dos resultados importantes sobre números primos tinham sido provados. No livro IX de *Os Elementos*, Euclides prova que existem infinitos números primos. Esta é uma das primeiras demonstrações conhecidas a usar o método da contradição, com vista à obtenção de um resultado.

A demonstração de Euclides:

Suponhamos que a sucessão $p_1, p_2, ..., p_r$ dos r números primos seja finita. Façamos $P = p_1 \cdot p_2 \cdot ... \cdot p_r + 1$ e seja p um número primo que divide P. Esse número não pode ser igual a qualquer um dos números $p_1, p_2, ..., p_r$, porque então ele divide a diferença $P - p_1 \cdot p_2 \cdot ... \cdot p_r = 1$. O que é impossível. Assim p é um número primo que não pertence a sucessão e por consequência $p_1, p_2, ..., p_r$ não pode formar o conjunto de todos os primos.

Euclides nos dá também, uma demonstração do Teorema Fundamental da Aritmética – qualquer inteiro pode ser escrito como produto de números primos em essencialmente uma única maneira – Ele também mostrou que se um número da forma $2^n - 1$ é primo, então o número desta forma é um número perfeito.

O matemático *Leonard Euler* (1747) mostrou que todos os números pares perfeitos são desta forma. Não é conhecido até hoje nenhum número perfeito ímpar. Em 200 a.C. o grego *Eratóstenes* apresentou um algoritmo para calcular números primos, o *Crivo de Eratóstenes*. Segue-se depois um largo período de tempo de interregno, na *História dos Números Primos*, durante a chamada *Idade Negra*. O desenvolvimento seguinte na História dos números primos nos é fornecido por *Pierre de Fermat* no início do século XVII. Este provou uma especulação conjecturada por *Albert Girard*, estabelece que todo número primo da forma $4n+1$ pode ser escrito de um só modo como soma de dois quadrados de números inteiros, foi capaz de nos mostrar que qualquer número inteiro positivo pode ser escrito como soma de quatro quadrados. Criou um novo método para fatorar números primos grandes. Também provou o que é hoje conhecido como *Pequeno Teorema de Fermat* (para distinguir do denominado *Grande Teorema de Fermat*). Seja n um número primo então para qualquer número inteiro a, tem-se que:

$$a^p \equiv a \bmod p.$$

Tal teorema prova em parte, o que foi chamado de *Hipótese Chinesa*, que data de cerca de 2000 anos antes, e que diz que um inteiro n é primo, se e somente se o número $2^n - 2$ é divisível por n. A outra metade deste teorema é falsa; vê-se facilmente com o exemplo que $2^{341} - 2$ é divisível por 341, e $341 = 31 \times 11$.

O Pequeno Teorema de Fermat é a base de muitos resultados da *Teoria dos Números*, e de métodos conceituados com vista a determinação de números primos, que ainda hoje são utilizados em larga escala, em computação. Fermat manteve correspondência com outros matemáticos do seu tempo, e em particular com o monge *Marin Mersenne*. Numa das suas cartas a Mersenne, ele conjecturou que os números da forma

$$F^n = 2^{2^n} + 1 \ ,$$

denominados *números de Fermat*, seriam primos. Somente cerca de 100 anos depois é que Euler demonstra que tal conjectura falha: $2^{32} + 1 = 4294967297$ é divisível por 641 e, portanto não é primo. Os números da forma $2^n - 1$ também atraíram a atenção, devido ao fato que, caso n não seja primo, estes números são compostos. Estes são classicamente chamados de *números de Mersenne* M^n, devido ao estudo que este matemático lhe dedicou. Naturalmente nem todos os números da forma $2^n - 1$, com n primo, são primos.

Por exemplo, $2^{11} - 1 = 2047 = 23 \times 89$ é composto. No entanto isto só foi descoberto por volta de 1536. Por muitos anos os números M^n de Mersenne, com n primo, forneceram os maiores números primos conhecidos. O número M^{19} é primo e isto foi provado por *Pietro Antonio Cataldi* em 1588 e este foi o maior número primo conhecido por cerca de 200 anos, até que *François E. A. Lucas* mostrou que M^{127} (que é um número que tem 39 dígitos) é primo, Este número foi o recordista até a era dos computadores eletrônicos. Em 1952 foram descobertos os números de Mersenne, M^{521}, M^{607}, M^{1279}, M^{2203}, M^{2281} por *Raphael M. Robinson* com a ajuda de um primitivo computador eletrônico (LLT/SWAC) e isto estabelece o início da era eletrônica. Até a presente data é conhecido um total de 37 números primos de Mersenne. O maior deles é o número $M^{3021377}$ que tem 909526 dígitos. O trabalho de Euler tem também um grande impacto na Teoria dos Números em geral e na Teoria dos Números Primos em particular. Ele estende o Pequeno Teorema de Fermat e introduz a *função* φ *(de Euler)*. Como mencionado, Euler fatorou o quinto número de Fermat: $2^{32} + 1$ e descobriu 60 pares de números amigáveis. Além disso, conjecturou (mas não provou) a *Lei da Reciprocidade Quadrática*, que foi provada posteriormente por *Johann Carl Friedrich Gauss*. Euler foi o primeiro a perceber que a Teoria dos Números pode ser estudada usando as ferramentas da Análise, introduzindo desta forma a *Teoria Analítica dos Números*. Ele mostrou que, não só a conhecida série harmônica

$$\sum_{n=1}^{\infty} \frac{1}{n}$$

é divergente, mas que a série harmônica com n primo

$$\sum_{n=primo} \frac{1}{n}$$

também é divergente. A soma dos primeiros *n* termos da série harmônica ordinária cresce logaritmicamente, enquanto a outra série (considerando apenas os primos) diverge ainda mais lentamente sendo assintoticamente comparável a $\log(\log(n))$. Isto significa que somando os inversos de todos os números primos já conhecidos, temos que, mesmo utilizando o mais poderoso dos computadores modernos, obtemos o valor dessa soma em torno de 4, apesar da série ser divergente.

À primeira vista, os números primos parecem não obedecer a uma regra especifica de aparecimento. Por exemplo, em relação aos 100 primeiros números imediatamente antes de 10.000.000 existem apenas nove números primos, enquanto nos 100 números que se seguem existem apenas dois números primos. No entanto, numa maior escala, a distribuição de números primos parece ser mais regular. *Legendre (Adrien-Marie Legendre)* e *Gauss* fizeram extensos cálculos sobre a densidade dos números primos. Gauss (que era um prodígio do cálculo) disse a um amigo que sempre que tinha 15 minutos de folga, os ocupava contando os números primos num alcance de 1000 números. No fim da sua vida estimou-se que Gauss tinha contado todos os números primos até três milhões. Legendre e Gauss chegaram a conclusão que, para *n* suficientemente grande, a densidade de números primos próximo de *n* se é aproximadamente $\frac{1}{\log n}$. Legendre deu uma estimativa para quantidade $\pi(n)$ dos números primos até *n*:

$$\pi(n) \approx \frac{n}{\log(n)}$$

enquanto Gauss estimou este mesmo número em termos da integral logarítmica

$$\pi(n) = \int_2^n \frac{1}{\log t} dt .$$

A conjectura que previa que a densidade de números primos é igual a $\frac{1}{\log n}$ é hoje conhecida como *Teorema dos Números Primos*. Tentativas de prová-la continuaram pelo século XIX com progressos notáveis pelo matemático russo *Pafnuty Lvovich Chebyshev* e pelo matemático alemão *Georg Friedrich Bernhard Rieman* que foram capazes de relacionar o problema com algo próximo à chamada *Hipótese de Rieman* que é uma conjectura sobre os zeros no plano complexo de uma função chamada *função ζ (zeta) de Rieman*. Na verdade, usando métodos poderosos da Análise Complexa, o Teorema dos Números Primos foi primeiramente (1896) demonstrado, independentemente, por dois matemáticos franceses, *Jacques Hadamard* e *Charles-Jean de La Vallée Poussin*, quando estavam interessados no estudo da função zeta de Rieman.

Ainda há muitas questões por desvendar (algumas delas que datam de centenas de anos atrás) relacionadas com números primos. (Veja [07]).

03. Desenvolvimento

Será descrita agora uma proposta pedagógica para a aplicação da oficina de aritmética em escolas ou grupos de estudos.

Indicação dos procedimentos metodológicos e técnicos:

Esta oficina foi aplicada numa escola pública estadual com duas turmas de 30 alunos do segundo ano do Ensino Médio como projeto piloto para o desenvolvimento deste trabalho. Obtivemos uma excelente aceitação da direção da escola e uma participação produtiva dos alunos. Nesse sentido, seguem minhas sugestões para aqueles que tiverem acesso e oportunidade de conhecer este trabalho.

Sugerimos formar grupos de estudos onde os alunos podem ser previamente selecionados segundo critérios do professor ou da Escola para desenvolver a oficina. Observamos que é importante adequar a oficina à realidade de cada escola ou grupo de alunos. Este trabalho é apenas uma sugestão didática.

Público Alvo: Alunos matriculados nos ensinos Fundamental ou Médio.

Alunos por turma: Máximo de vinte alunos.

Número de aulas: Dez encontros de noventa minutos
(1h30min. por encontro = 15 horas por semestre)

Serão apresentadas aulas teóricas para um nivelamento prévio na formação dos alunos quanto aos conteúdos necessários. Em paralelo, será desenvolvida uma bateria de exercícios onde constarão problemas relacionados ao uso dos números primos e suas curiosidades.

Os alunos serão avaliados por desenvolvimento de competências e habilidades na produção das atividades, não havendo uma ‘nota’ individual, mas sim um parecer sobre cada atividade desenvolvida.

04. O Projeto Piloto

Foi formado um grupo de estudos na Escola Estadual de Ensino Fundamental e Médio Arnulpho Mattos – Vitória - ES, onde os alunos foram previamente selecionados segundo critérios da própria Escola, para desenvolver a oficina. Segundo as condições da Escola, trabalhamos com alunos matriculados no Ensino Médio, numa oficina de 10 encontros de sessenta minutos cada. (Foi necessário adequar a oficina com os horários e o tempo de cada aula na escola).

Foram apresentadas aulas teóricas e expositivas para um nivelamento prévio na formação dos alunos quanto aos conteúdos necessários. Em paralelo foi desenvolvida uma bateria de quinze exercícios onde trabalhei problemas relacionados ao uso dos números primos no cotidiano e suas curiosidades. Algumas das atividades produzidas estão anexadas ao projeto final como amostra para novos estudos e oficinas a serem desenvolvidas. Num segundo momento, trazemos alguns comentários sobre as atividades produzidas na oficina como uma forma de explicitar os possíveis resultados que se pode alcançar com este tipo de atividade/projeto e que serviu de complemento na motivação para desenvolver o projeto do trabalho de dissertação de Mestrado do curso de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT/UFES.

A seguir trazemos uma sequência didática, nos moldes que foram aplicados no projeto piloto, como sugestão de aplicação da oficina. Trata-se de dez encontros preparados com uma proposta pedagógica, de forma a facilitar o trabalho do professor/aplicador no desenvolvimento de aulas, possibilitando a ele usar os recursos disponíveis em sua instituição (data-show, laboratório de informática, etc...) de forma a permitir um melhor aprendizado dos alunos participantes.

05. Encontro 01 – Os Números Naturais

Relembremos algumas dicas trabalhadas no material utilizado no PROFMAT/UFES para ajudar na resolução de problemas em Matemática.

(D1) – Ler com cuidado o enunciado do problema e utilizar todas as informações disponíveis.

(D2) – Resolver casos particulares ou casos mais simples de problemas similares, para adquirir familiaridade com o problema.

(D3) – Mudar a representação do problema, transformando-o em um problema equivalente.

(D4) – Usar a imaginação, pesquisando caminhos alternativos.

Além dessas dicas, acrescentamos mais algumas outras:

(D5) – Reúna todos os fatos que você conhece e que estejam relacionados com o problema; em seguida, selecione alguns deles que você ache que possam servir para resolver o problema.

(D6) – Se o problema permitir encontre um invariante. Isto é, uma quantidade ou propriedade que não muda e que possa ser usada para resolver seu problema.

(D7) – Se for possível e conveniente, comece de trás para frente, iniciando na situação final onde você deseja chegar e, a partir de argumentos válidos, tente chegar na situação inicial.

(D8) – Antes de avançar demais, verifique o trabalho já desenvolvido, conferindo se você cometeu algum erro. Isso lhe poupará tempo.

Claramente, nenhuma dessas dicas faria sentido se lida isoladamente e desconectada de um problema específico. Além disso, nenhuma delas é universal, permitindo-lhe tornar-se um grande resolvedor de problemas. Na verdade, resolver problemas é algo que só se aprende fazendo. Porém, adotar estratégias como as que listamos acima pode ajudá-lo a ganhar tempo.

5.1 – Teoria dos Números

O conjunto dos números naturais é representado pela letra maiúscula *N* e estes números são representados utilizando os algarismos *0, 1, 2, 3, 4, 5, 6, 7, 8, 9,* que também são conhecidos como algarismos indo-arábicos. No século VII, os árabes invadiram a Índia, difundindo o seu sistema numérico. Embora o zero não seja um número natural no sentido de que tenha sido proveniente de objetos de contagens naturais, iremos considerá-lo como um número natural uma vez que ele tem as mesmas propriedades algébricas que os números naturais. Na verdade, o zero foi criado pelos hindus na montagem do sistema posicional de numeração para suprir a deficiência de algo nulo.

Na sequência, consideraremos que os naturais têm início com o número zero e escreveremos este conjunto como:

$$N = \{0, 1, 2, 3, 4, 5, 6 \ldots\}$$

As reticências (três pontos) indicam que este conjunto não termina. *N* é um *conjunto infinito*.

Excluindo o zero do conjunto dos números naturais, o conjunto resultante será representado por:

$$N^* = \{1, 2, 3, 4, 5, 6 \ldots\}$$

No conjunto dos números naturais observamos a presença de dois tipos de números: números primos e números compostos. A Aritmética é a área da Matemática que estuda os conjuntos numéricos e as operações básicas desenvolvendo propriedades que fundamentam a construção dos números, suas propriedades e o seu uso. Os números primos tem grande importância nessa construção. Por definição, número primo é aquele que possui dois, e somente dois divisores naturais. Nessas condições, construímos os outros números, chamados compostos, como produto de números primos, ou seja, podemos fazer sua decomposição em fatores primos. Podemos determinar quantos e quais são os divisores de qualquer número natural conhecendo os fatores primos da sua decomposição. Relacionamos grandezas conhecendo seus múltiplos e divisores, usamos o cálculo do MDC (Máximo Divisor Comum) e do MMC (Mínimo Múltiplo Comum) a partir da decomposição em fatores primos para relacionar grandezas. Essas aplicações e algumas curiosidades são os fatores fundamentais deste trabalho. Assim, criamos várias propriedades e dispositivos para desenvolver ferramentas aritméticas junto às operações matemáticas, como por exemplo, determinar quantos e quais são os divisores de um número natural através da sua decomposição em fatores primos.

Faz necessário ressaltar que o número 1 (um) não é primo nem composto e que o número 2 (dois) é o único número natural par e primo.

O estudo da fatoração em números primos é muito importante para diversas partes da Matemática, mas principalmente para potenciação e radiciação. Por isso colocamos todos estes tópicos juntos.

O que significa fatorar?

Quando aprendemos multiplicar (nas primeiras séries do Ensino Fundamental), também aprendemos o que é um fator. Fatorar um número nada mais é do que encontrar uma multiplicação de números que resulte o número dado. Exemplos:

Uma fatoração para o número 4 pode ser $2 \cdot 2$. Assim, $4 = 2 \cdot 2$. Da mesma forma,

$9 = 3 \cdot 3$

$32 = 16 \cdot 2$

$90 = 15 \cdot 3 \cdot 2$

Todos estes são exemplos de fatoração. Mas o que nos interessa é a fatoração em números primos. Fatorar em números primos é achar uma multiplicação de números primos que resulta no número que se deseja fatorar. Veja que os dois últimos exemplos acima, não são fatorações em números primos, uma vez que 16 e 15 não são números primos. Então aquela é apenas uma fatoração, e não “fatoração em números primos”. Para fatorar um determinado número em fatores primos, utilizamos um método que foi ensinado a vocês nas primeiras séries da Escola. Começamos escrevendo o número a fatorar com uma barra vertical ao lado: Por isso não vamos entrar em muitos detalhes.

Veja os exemplos abaixo:

$$
\begin{array}{r|l}
81 & 3 \\
27 & 3 \\
9 & 3 \\
3 & 3 \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
126 & 2 \\
63 & 3 \\
21 & 3 \\
7 & 7 \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
147 & 3 \\
49 & 7 \\
7 & 7 \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
1365 & 3 \\
455 & 5 \\
91 & 7 \\
13 & 13 \\
1 &
\end{array}
$$

Com isso achamos a fatoração em primos destes números:

Número	Fatoração em Primos	Potências
81	$3 \,.\, 3 \,.\, 3 \,.\, 3$	3^{4}
126	$2 \,.\, 3 \,.\, 3 \,.\, 7$	$2 \,.\, 3^{2} \,.\, 7$
147	$3 \,.\, 7 \,.\, 7$	$3 \,.\, 7^{2}$
1365	$3 \,.\, 5 \,.\, 7 \,.\, 13$	

(Veja [03])

06. Encontro 02 – Divisibilidade

Para facilitar a fatoração vamos relembrar os critérios de divisibilidade por *2, 3, 4, 5, 6, 8 e 9.* (Veja [04])

- Por *2*: Um número é divisível por *2* se ele for par; (Segue uma sugestão de demonstração para estimular os alunos a desenvolverem um raciocínio algébrico).

Demonstração: Dado um número qualquer $a\mathrm{bcd...ef}$ (onde $a, \mathrm{b, c, d, ..., e, f}$ são algarismos) então, se 2 divide $a\mathrm{bcd...ef}$ temos que

$$a\mathrm{bcd...ef} = a10^{n} + \mathrm{b}10^{\mathrm{n-1}}...\mathrm{e}10^{1} + \mathrm{f} = 10(a10^{n-1} + \mathrm{b}10^{\mathrm{n-2}}...\mathrm{e}) + \mathrm{f}$$

Assim $\mathrm{f} = a\mathrm{bcd...ef} - 10(a10^{n-1} + \mathrm{b}10^{\mathrm{n-2}}...\mathrm{e})$ que é divisível por 2

- Por *3*: Um número é divisível por *3* se a soma dos seus algarismos resultar em um múltiplo de *3*;

- Por *4*: Um número é divisível por *4* se os dois últimos algarismos formarem um número múltiplo de *4*;

- Por *5*: Um número é divisível por *5* se terminar em zero ou *5*;

- Por *6*: Um número é divisível por *6* se for divisível por *2* e *3* ao mesmo tempo;

- Por *8*: Um número é divisível por *8* se os três últimos algarismos formarem um número múltiplo de *8*;

- Por *9*: Um número é divisível por *9* se a soma dos seus algarismos resultar em um múltiplo de *9*;

Exemplos para fixação: Faça a decomposição dos números seguintes em fatores primos, usando o processo das fatorações sucessivas.

a) $28 = 4 \cdot 7 = 2^2 \cdot 7$

b) $18 = 2 \cdot 9 = 2 \cdot 3^2$

c) $45 = 3^2 \cdot 5$

d) $100 = 2^2 . 5^2$

e) Qual é o número natural cuja fatoração completa é $3 . 5^3$?

Solução: Sabemos que $5^3 = 125$, logo, $3 . 5^3 = 375$.

f) $2^2.7.11$ é a decomposição em fatores primos de que número?

Solução: Sabemos que $2^2 = 4$, logo, $2^2 . 7 . 11 = 4 . 77 = 308$.

g) Que número decomposto em fatores primos é igual a $2^3.5.7^2$?

Solução: Sabemos que $2^3 = 8$ e que $7^2 = 49$, logo, $2^3 . 5 . 7^2 = 8 . 5 . 49 = 1960$.

h) Nas turmas de sextos anos de uma escola há *198* alunos, e nos sétimos anos há *189* alunos. Para realizar um trabalho comunitário, os alunos serão organizados em grupos do maior tamanho possível, todos com o mesmo número de alunos e sem que se misturem alunos de anos diferentes.

i) Qual é o número máximo de alunos que pode haver em cada grupo?

Solução: Sabemos que $198 = 2 . 3^2 . 11$ e $189 = 3^3 . 7$, logo, o número de alunos em cada grupo será o maior divisor comum aos dois números, nesse caso, 3^2. Portanto, o número máximo de alunos em cada grupo será *9*.

j) Nesse caso, quantos grupos serão formados em cada ano?

Solução: Serão formados $198 : 9 = 22$ grupos de sextos anos e $189 : 9 = 21$ grupos de sétimos anos.

07. Encontro 03 – MDC e MMC

Um dos pontos importantes da fatoração, encontra-se no cálculo do M.D.C (Máximo Divisor Comum) e do M.M.C (Mínimo Múltiplo Comum). Entretanto, devemos tomar cuidado quanto à obtenção desses valores, pois utilizaremos o mesmo procedimento de fatoração, ou seja, a mesma fatoração de dois ou mais números nos oferece o valor do M.D.C e do M.M.C. Sendo assim, devemos compreender e diferenciar o modo pelo qual se obtém cada um desses valores, através da fatoração simultânea.

Vejamos um exemplo no qual foi feita a fatoração simultânea:

$$\begin{array}{r|l} 12\ ,\ 42 & \mathbf{2}\ \textbf{(Divisor Comum)} \\ 6\ ,\ 21 & 2 \\ 3\ ,\ 21 & \mathbf{3}\ \textbf{(Divisor Comum)} \\ 1\ ,\ 7 & 7 \\ \hline 1\ ,\ 1 & \end{array}$$

Note que na fatoração foram destacados os números que dividiram simultaneamente os números *12* e *42*. Isto é um passo importante para conseguirmos determinar o M.D.C. Se fossemos listar os divisores de cada um dos números, teríamos a seguinte situação:

$$D(12) = \{2,3,4,\mathbf{6},12\}$$

$$D(42) = \{2,3,\mathbf{6},7,21,42\}$$

Note que o maior dos divisores comuns entre os números *12* e *42* é o número *6*. Observando a nossa fatoração simultânea, este valor *6* é obtido realizando a multiplicação dos divisores comuns, ou seja, M.D.C $(12,42) = 2 . 3 = 6$. Assim, podemos encontrar o M.D.C de dois ou mais números naturais fazendo o produto dos fatores comuns na decomposição simultânea desses números. Por outro lado, o M.M.C será obtido de uma maneira diferente. Por se tratar dos múltiplos, deveremos multiplicar todos os divisores da fatoração. Sendo assim, o M.M.C $(12,42)= 2 . 2 . 3 . 7 = 2^2 . 3 . 7 = 84$. Deste modo, podemos encontrar o M.M.C de dois ou mais números naturais fazendo o produto de todos fatores na decomposição simultânea desses números.

7.1 – Problemas de Aplicação

Problema 7.1 – Num painel de propaganda, três luminosos se acendem em intervalos regulares: o primeiro a cada *12* segundos, o segundo a cada *18* segundos e o terceiro a cada *30* segundos. Se, em dado instante, os três se acenderem ao mesmo tempo, os luminosos voltarão a se acender, simultaneamente, depois de quanto tempo?

Solução: Os luminosos irão acender juntos nos múltiplos comuns de *12*, *18* e *30*. Assim, a primeira vez que isso acontecerá será o M.M.C *(12, 18, 30)*. Fatorando simultaneamente estes números, teremos:

$$
\begin{array}{r|l}
12, 18, 30 & 2 \\
6, 9, 15 & 2 \\
3, 9, 15 & 3 \\
1, 3, 5 & 3 \\
1, 1, 5 & 5 \\
\hline
1, 1, 1 & 2^2 \cdot 3^2 \cdot 5 = 180
\end{array}
$$

Logo, o M.M.C *(12, 18, 30) = 180* e, portanto, os luminosos irão acender simultaneamente após 180 minutos ou 3 horas.

Problema 7.2 – Dois depósitos têm respectivamente, *1350* e *4356* litros de capacidade. Para encher cada um desses depósitos usou-se uma mesma vasilha, um número exato de vezes. Qual a maior capacidade que pode ter a vasilha?

Solução: A maior capacidade dessa vasilha é o maior divisor comum de *1350* e *4356*, isto é, precisamos calcular o M.D.C *(1350, 4356)*. Assim, fatorando simultaneamente estes números, teremos:

1350 , 4356	***2* (Divisor Comum)**
675 , 2178	*2*
675 , 1089	***3* (Divisor Comum)**
225 , 363	***3* (Divisor Comum)**
75 , 121	*3*
25 , 121	*5*
5 , 121	*5*
1, 121	*11*
1, 11	*11*
1, 1	

A capacidade da vasilha é dada pelo M.D.C $(1350, 4356) = 2 \,.\, 3^2 = 18$ litros

Problema 7.3 – Sabendo que x e y são números primos distintos calcule o M.D.C de $5.x.y^5$, $15.x^3.y$ e $17.x^5.y^3$.

Solução: Sabemos que x e y são primos entre si (Chamamos de números primos entre si um conjunto de dois ou mais números naturais cujo único divisor comum a todos eles seja o número 1), observamos que na decomposição dos números $5.x.y^5$, $15.x^3.y$, $17.x^5.y^3$ só comparece, como fatores comuns a todos os termos, o produto $x.y$, assim, o M.D.C de $5.x.y^5$, $15.x^3.y$, $17.x^5.y^3$ é igual a $x.y$.

Problema 7.4 – Um país lançou em 02/01/2014 os satélites artificiais *A, B* e *C* com as tarefas de fiscalizar o desmatamento em áreas de preservação, as nascentes dos rios e a pesca predatória no Oceano Atlântico. No dia 03/01/2014 podia-se observá-los alinhados, cada um em uma órbita circular diferente, tendo como referência a Terra. Se os satélites *A, B* e *C* levam, respectivamente, *6, 10* e *9* dias para darem uma volta completa em torno da Terra, então calcule em que dia ocorrerá o próximo alinhamento.

Solução: O alinhamento dos satélites ocorre nos múltiplos de *6, 9* e *10*, ou seja, o próximo alinhamento ocorrerá no M.M.C *(6,9,10)*. Fatorando simultaneamente esses valores, teremos:

$$\begin{array}{c|l}
6 , 9 , 10 & 2 \\
3 , 9 , 5 & 3 \\
1 , 3 , 5 & 3 \\
1 , 1 , 5 & 5 \\
\hline
1 , 1 , 1 & 2 \,.\, 3^2 \,.\, 5 = 90
\end{array}$$

Portanto, o alinhamento dos satélites ocorrerá em *90* dias, isto é, dia 03/04/2014.

08. Encontro 4 – Atividades de Aprofundamento e Curiosidade 1

Obs.: Aqui o professor pode usar sua criatividade ou se adequar à realidade da sua turma preparando esse material em slides para projeção para a turma ou mesmo preparar uma lista para cada aluno e deixar um tempo para que eles tentem desenvolver a atividade. Durante esse tempo o professor pode ser um mediador de ideias, estimulando os alunos a compartilhar os pensamentos e desenvolver conjuntamente as habilidades e competências necessárias para produzir um material satisfatório.

Disponho aqui uma lista de problemas e sugestões de solução para cada um deles.

Problema 8.1 – Usando a decomposição simultânea em fatores primos dos números *507* e *1287*, calcular o M.D.C*(507,1287)* e o M.M.C*(507,1287).*

Solução: Fazendo a decomposição em fatores primos, teremos:

507 , 1287	***3*** **(Divisor Comum)**
169 , 429	*3*
169 , 143	*11*
169 , 13	***13*** **(Divisor Comum)**
13 , 1	*13*
1 , 1	

Assim, M.D.C$(507,1287) = 3 . 13 = 39$ e M.M.C$(507,1287) = 3^2 . 11 . 13^2 = 16731$.

Problema 8.2 – Ao longo de um dia, um supermercado fez vários anúncios dos produtos *A*, *B* e *C*, todos eles com o mesmo tempo de duração. Os tempos totais de aparição dos produtos *A*, *B* e *C* foram, respectivamente, iguais a *90s, 108s* e *144s*. Se os três produtos apareceram em tempos iguais e a duração de cada anúncio, em segundos, foi a maior possível, então, a soma do número de aparições dos três produtos, nesse dia, foi igual a:

Solução: Precisamos calcular a quantidade de aparições de cada produto que é o maior divisor comum dos tempos 90s, 108s e 144s. Assim, calculamos o M.D.C(90, 108, 144) usando a decomposição simultânea.

90 , 108 , 144	***2* (Múltiplo comum)**
45 , 54 , 72	*2*
45 , 27 , 36	*2*
45 , 27 , 18	*2*
45 , 27 , 9	***3* (Múltiplo comum)**
15 , 9 , 3	***3* (Múltiplo comum)**
5 , 3 , 1	*3*
5 , 1, 1	*5*
1, 1, 1	M.D.C*(90, 108, 144)* $= 2 \cdot 3^2 = 18$

O produto *A* apareceu cinco vezes, pois, *18 . 5 = 90;*

O produto *B* apareceu seis vezes, pois, *18 . 6 = 108;*

O produto *C* apareceu oito vezes, pois, *18 . 8 = 144.*

Assim, o total de aparições dos três produtos é igual a *5 + 6 + 8 = 19* vezes.

Problema 8.3 – Uma indústria de tecidos fabrica retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas: *156* centímetros e *234* centímetros. O gerente de produção ao ser informado das medidas deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?

Solução: O funcionário deve cortar as peças de tecidos em pedaços cujo tamanho seja o M.D.C *(156, 324).* Assim, fatoramos simultaneamente:

156 , 234	***2* (Divisor Comum)**
78 , 117	*2*
39 , 117	***3* (Divisor Comum)**
13 , 39	*3*
13 , 13	***13* (Divisor Comum)**
1 , 1	

Portanto, o funcionário pode cortar as peças em tamanhos iguais a

M.D.C *(156, 324) = 2 . 3 . 13 = 78 cm* cada pedaço.

Problema 8.4 – Numa aventura pelo deserto, o sábio e "grande matemático" Malba Tahan foi consultado sobre o seguinte enigma: "Quantos números de dois algarismos não são primos nem múltiplos de *2, 3,* ou *5*?" Ajudando ao grande sábio, qual é a resposta do enigma?

Solução: Os números de dois algarismos variam de *10* a *99*, nesse intervalo procuramos os números que não são primos nem múltiplos de *2, 3, 5.* Uma maneira é escrever todos os números e eliminar aqueles que não satisfazem a hipótese. Por outro lado, como é um intervalo de números pequenos e conhecidos, fica fácil identificar que os números que não são primos nem múltiplos de *2, 3* e *5* devem ser alguns múltiplos de sete com outros primos diferentes de *2, 3* e *5.* Assim:

$$7 \,.\, 7 = 49$$

$$7 \,.\, 11 = 77$$

$$7 \,.\, 13 = 91$$

Portanto a resposta do enigma é: "Três números de dois algarismos: *49, 77* e *91*."

8.1 – Curiosidade 1 – Primos e o Real Madrid

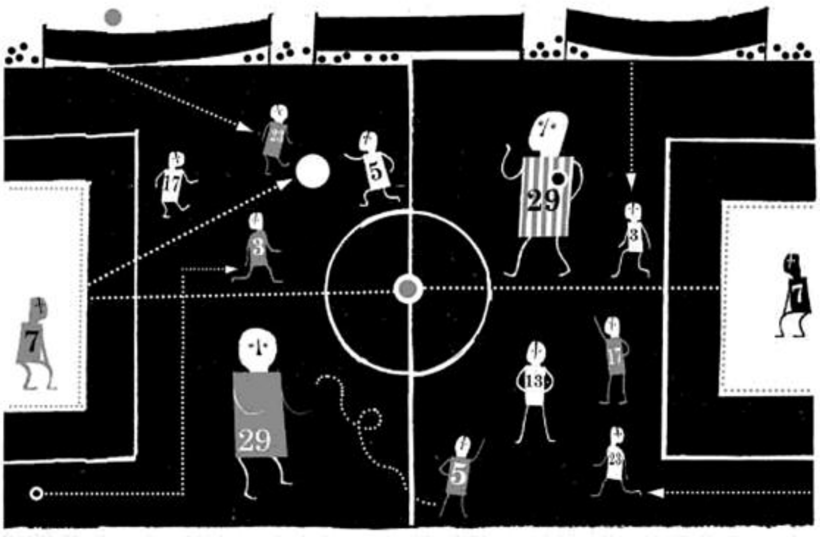
Por que Beckham escolheu a camisa *23*?

Quando David Beckham foi para o Real Madrid, em 2003, houve muita especulação acerca do motivo que o teria levado a escolher a camisa numero *23*. Foi uma opção estranha, pensaram muitos, uma vez que ele vinha jogando com o número *7* pelo Manchester United e pela seleção inglesa. O problema era que no Real Madrid a camisa *7* já era usada por Raúl, e o espanhol não estava disposto a abrir mão dela para o menininho glamouroso da Inglaterra.

Muitas teorias diferentes foram apresentadas para explicar a escolha de Beckham e, a mais popular era a "teoria Michael Jordan". O Real Madrid queria entrar no mercado dos Estados Unidos e vender muitas réplicas da camisa para a enorme população norte-americana. Mas o futebol (ou soccer, como é lá conhecido) não é um jogo popular nos Estados Unidos. Os americanos gostam de basquete e basebol, jogos que terminam com contagens de *100 x 98* e nos quais há, invariavelmente, um vencedor. Eles não conseguem ver sentido num jogo que dura *90* minutos e pode terminar em *0 x 0*, sem ninguém marcar gol nem ganhar.

Segundo essa teoria, o Real Madrid fizera sua pesquisa e descobrira que o jogador de basquete mais popular do mundo era decididamente Michael Jordan, o mais prolífico cestinha do Chicago Bulls. Jordan vestiu a camisa *23* durante toda sua carreira. Tudo que o Real Madrid precisava era pôr *23* nas costas de uma camisa de futebol, cruzar os dedos e esperar que a ligação com Jordan fizesse valer sua magia, e eles conseguiriam irromper no mercado americano. Outros consideraram isso cínico demais, mas sugeriram uma teoria ainda mais sinistra. Júlio César foi assassinado com *23* punhaladas nas costas. Seria a escolha de Beckham para o número em suas costas um mau presságio? Outros achavam que talvez a escolha estivesse relacionada ao amor de Beckham por Guerra nas Estrelas (a princesa Leia estava aprisionada no bloco de detenção *AA23*, no primeiro filme da série). Ou seria o jogador um membro secreto dos discordianistas, moderno culto que venera o caos e tem uma obsessão cabalística pelo número *23*?

Mas assim que vi o número de Beckham, ocorreu-me imediatamente uma solução mais matemática. O *23* é um número primo. Um número primo é um número divisível apenas por ele mesmo e por *1*. Os números *17* e *23* são primos porque não podem ser escritos como dois números menores multiplicados entre si, ao passo que *15* não é primo porque $15 = 3 \times 5$. Números primos são os números mais importantes da matemática porque todos os outros números inteiros são formados multiplicando-se números primos entre si. Tome por exemplo, o número *105* que, claramente é divisível por *5*. Então podemos escrever *105 = 5 x 21*. O número *5* é primo, um número indivisível. O número *21* não é: podemos escrever *21 = 3 x 7*. Logo, *105* pode ser escrito como *3 x 5 x 7*, mas esse é o máximo onde podemos chegar. Podemos fazer isso com qualquer número inteiro, uma vez que todo número inteiro ou é primo e indivisível ou não é primo e pode ser decomposto em números menores indivisíveis.



Os primos são os blocos construtivos de todos os números inteiros. Assim como as moléculas são compostas de átomos como hidrogênio e oxigênio, ou sódio e cloro, os números inteiros são produtos de primos. No mundo da matemática, os números *2, 3* e *5* são como hidrogênio, hélio e lítio. É isto que os torna os números mais importantes em matemática. Mas eram, obviamente, importantes também para o Real Madrid. Quando passei a examinar um pouco mais de perto o time de futebol do Real Madrid, comecei a desconfiar que talvez eles tivessem um matemático no banco. Na época da transferência de Beckham para lá, uma análise mais detalhada revelaria que todos os 'galácticos', jogadores-chave do Real Madrid, atuavam com camisas assinaladas com números primos: Roberto Carlos (o bloco construtivo da defesa), número *3*; Zidane (o coração do meio-campo), número *5*; Raúl e Ronaldo (os alicerces da artilharia do Real Madri), *7* e *11*. Assim, talvez fosse inevitável que Beckham tivesse um número primo, um número ao qual ele ficou muito ligado. Quando foi para o LA Galaxy insistiu em levar consigo seu número primo, na tentativa de cortejar o público americano com um belo jogo.

Isso soa totalmente irracional vindo de um matemático, uma pessoa que deveria ser um pensador analítico e lógico. No entanto, eu também jogo com uma camisa de número primo no meu time de futebol, o Recreativo Hackney, de modo que senti alguma conexão com o homem da camisa *23*. Meu time da Liga Dominical não é tão grande como o Real Madrid e não tínhamos uma camisa *23*, de modo que escolhi a *17*, número primo bastante simpático — como veremos adiante. Mas, na primeira temporada, nosso time não se saiu particularmente bem. Jogamos na Superliga Dominical de Londres, na 2ª divisão, e acabamos na lanterna. Felizmente, essa é a divisão mais baixa em Londres, então o único caminho era para cima. Mas como poderíamos melhorar nossa posição na Liga? Talvez o Real Madrid soubesse de algo — haveria alguma vantagem psicológica em se jogar com uma camisa de número primo? Talvez houvesse jogadores demais no time com números não primos, como *8*, *10* ou *15*. Na temporada seguinte, persuadi o time a mudar o jogo de camisas, e todos jogamos com números primos: *2, 3, 5, 7, ...* a sequência toda até o *43*. Isso nos transformou. Fomos promovidos à 1ª divisão, onde, depressa, aprendemos que os primos duram apenas uma temporada. Fomos relegados de volta à 2ª divisão, e agora estamos em busca de uma nova teoria matemática para incrementar nossas chances.

O goleiro do Real Madrid deveria usar a camisa número 1?

Se os jogadores-chave do Real Madrid vestem números primos, então que camisa o goleiro deveria usar? Ou, falando matematicamente, o número *1* é primo? Bem, sim e não. (Este é exatamente o tipo de pergunta matemática que todo mundo adora, e ambas as respostas estão certas). Duzentos anos atrás, as tabelas de números primos incluíam o número *1* como primeiro primo. Afinal, ele não é divisível, pois o único número inteiro positivo pelo qual ele se divide é ele próprio. Mas hoje dizemos que *1* não é primo porque a coisa mais importante nos primos é que eles são blocos construtivos de números inteiros. Se eu multiplico um número por um primo, obtenho um número novo. Embora *1* não seja divisível, se eu multiplico qualquer número por *1*, obtenho o número com o qual comecei, e nessa base excluímos o *1* da lista de primos, e começamos com o *2*.

Claro que o Real Madrid não foi o primeiro a descobrir o poder dos primos. Mas que cultura chegou lá antes? Os gregos antigos? Os chineses? Os egípcios? Acabou-se descobrindo que os matemáticos foram batidos na descoberta dos primos por um pequeno e estranho inseto. (Veja [05])

09. Encontro 05 – Atividades de Aprofundamento e Curiosidade 2

Problema 9.1 - Tenho *693* amigos em minha rede social, e nela publiquei a frase de Pitágoras: “A Matemática é o alfabeto com o qual DEUS escreveu o universo”. O número de amigos que curtiram minha frase tem dois dígitos iguais e é divisor de *693*. A soma desses dois dígitos é um número de dois dígitos que somados resultam um número primo. Quantos curtiram minha frase?

Solução: Uma estratégia para resolver esse problema é determinar os divisores do número *693*, para isso vamos usar a sua fatoração em números primos.

		1
693	*3*	*3*
231	*3*	*9*
77	*7*	*7, 21, 63*
11	*11*	*11, 33, 99, 77, 231, 693*
1		

onde o conjunto {*1, 3, 7, 9, 11, 21, 33, 63, 77, 99, 231, 693*} é formado pelos divisores de *693*. Dentre esses números aquele que satisfaz as hipóteses do problema é *77*, pois,

$7 + 7 = 14$ e $1 + 4 = 5$

que é primo. Portanto, *77* amigos curtiram minha frase.

Problema 9.2 - Achar todos os pares de números primos p e q, tais que $p - q = 3$.

Solução: Uma diferença entre dois números resulta em um número ímpar se apenas um deles for par, como p e q são primos, necessariamente, $q = 2$ e $p = 5$. Solução única.

Problema 9.3 - Achar o menor inteiro positivo pelo qual se deve dividir *3720* para se obter um quadrado perfeito.

Solução: Um número é quadrado perfeito se, na sua fatoração em números primos, todos os fatores assumirem expoente par (Equivalentemente, um número é quadrado perfeito quando é o quadrado de um número inteiro maior do que 1). Assim, vamos analisar a fatoração do número *3720*.

$$
\begin{array}{r|l}
3720 & 2 \\
1860 & 2 \\
930 & 2 \\
465 & 3 \\
155 & 5 \\
31 & 31 \\
\hline
1 & 2^3 \,.\, 3 \,.\, 5 \,.\, 31
\end{array}
$$

Assim, o menor número que divida $2^3 \,.\, 3 \,.\, 5 \,.\, 31$ resultando em um quadrado perfeito será

$2 \,.\, 3 \,.\, 5 \,.\, 31 = 930$.

9.1 Curiosidade 2 – Cigarras Exóticas

Bilhões de cigarras emergem nos Estados Unidos após 17 anos no solo

(National Geographic - 10/05/2013)

Uma das seis espécies existentes de cigarras Magicicada

Elas estão de volta. Após passar *17* anos no subsolo, alimentando-se de raízes, bilhões de **cigarras** devem emergir do chão nos **Estados Unidos** prontas para acasalar. No céu americano, nuvens de até *1,5* milhões de indivíduos por acre podem se formar - e ainda que a ***Magicicada sp*** seja inofensiva, ela não é nada silenciosa. Famosas por seu canto, o intenso ruído emitido por estes insetos pode atingir *100* decibéis, uma altura equivalente ao som de um cortador de grama ou furadeira. A prática faz parte de um **ritual de acasalamento** que dura de duas a seis semanas. Após depositar os seus ovos (até seiscentos por indivíduo), a fêmea adulta morre. Estes filhotes eclodirão em poucos dias e logo devem se enterrar no solo, onde ficarão até **2031**. Ao todo, existem seis espécies do gênero **Magicicada**, três delas com ciclos de *17* anos. As cigarras que nasceram em *1996* já começam a emergir nos Estados Unidos e são esperadas até o fim de maio em *14* estados da costa leste. Os insetos deste gênero possuem olhos vermelhos e um curioso mecanismo genético que os faz sair do solo quando o mesmo atinge a temperatura de *18°C*. Os cientistas acreditam que o longo período de isolamento (curiosamente em números primos - *17* ou *13* anos, no caso das três outras espécies de Magicicada) ajuda a evitar predadores.

Ao fim do processo, bilhões de cascas vazias serão deixadas para trás e até o começo deste verão, no hemisfério Norte, os americanos podem se preparar para usar suas pás para limpar mais do que apenas folhas de jardim.

Cigarra usa número primo para sobreviver

Salvador Nogueira (Folha de S.Paulo - 15/06/2004 - 06h47)

O ataque das cigarras - como tem sido chamada a emergência sincronizada de algumas espécies do inseto, num ciclo exato de *17* anos - pode ser resultado não do acaso, mas sim de uma forte pressão seletiva. É o que sugere um estudo de pesquisadores brasileiros, que aponta uma solução para o mistério que tem encantado os americanos nas últimas semanas. A pesquisa faz uso das possibilidades de simular em computador o processo de evolução por seleção natural - área de estudo chamada genericamente de "vida digital". A ideia é criar uma espécie de videogame em que criaturas são simuladas por programas. Elas se reproduzem e sobrevivem como coisas vivas, de acordo com a maior ou menor adaptação.

No caso das cigarras, os pesquisadores conceberam um modelo que mostrasse como poderia emergir o estranho padrão desses insetos. Muitas espécies de cigarra têm períodos diferentes de amadurecimento, com ciclos vitais de duração variada, enquanto as larvas ficam sob a terra. Mas sete espécies do gênero Magicicada têm uma característica adicional: elas são sincronizadas, ou seja, saem do chão todas ao mesmo tempo, para cerca de duas semanas de canto ensurdecedor, acasalamento e postura de ovos. Para esses grupos sincronizados, é curioso notar que os ciclos normalmente acontecem em *13* ou *17* anos. São números primos, ou seja, divisíveis apenas por si mesmos e por um. É difícil acreditar que a natureza tenha escolhido aleatoriamente esses números para as cigarras. Apostando nisso, o grupo encabeçado por Paulo Campos, da Universidade Federal Rural de Pernambuco, e composto por Viviane de Oliveira, Ronaldo Giro e Douglas Galvão, da Unicamp, decidiu verificar se a seleção natural poderia ter algo a ver com a coisa.

Números Primos Altos

"Queríamos descobrir se ciclos de vida em números primos significavam alguma vantagem seletiva para os indivíduos que os desenvolvem", afirma Campos. "No início não sabíamos como começar a abordar o problema, mas logo surgiu a ideia de modelar isso utilizando um autômato celular estocástico - nesse modelo, as cigarras e os predadores evoluem no computador, no estilo dos trabalhos de vida digital." A estratégia deu certo. Ao longo das gerações simuladas, eles perceberam que as cigarras começavam a sobreviver mais conforme seus ciclos de vida se aproximavam desses números primos altos. Eram números que evitavam ao máximo o confronto com seus predadores naturais (pássaros, por exemplo), que por sua vez estariam lá todo o tempo. Mais ainda, a estratégia só funcionava se a espécie estivesse toda sincronizada - todas as cigarras precisavam sair do chão ao mesmo tempo. "Essa sincronização é extremamente relevante", diz Campos. "Porque, quando saem todas juntas, uma fração delas é comida pelo predador, mas o restante sobrevive, porque o predador já está saciado. Isso é, de fato, uma estratégia." Agora, se a ideia é tão boa, por que mais espécies não acabaram adotando esse modo de vida? É um dos mistérios que ainda vão permanecer. "Não se sabe por que outras espécies não evoluíram para esse estado. Possivelmente por não poderem suportar longos períodos de hibernação (sua estrutura física não possibilita isso) ou porque elas nunca estiveram ameaçadas de extinção em qualquer momento de sua existência", diz Campos. A ameaça de aniquilação, de fato, é notória por sua capacidade de incentivar a emergência de soluções criativas para a sobrevivência dos indivíduos e da espécie.

A pesquisa brasileira oferece uma resposta realista ao problema. Outras simulações já haviam obtido sucesso no passado, mas tratavam os predadores de forma totalmente irregular, atribuindo também a eles ciclos de incubação próprios. "Não foi provada a existência de predadores que se comportem dessa maneira. Existem, sim, predadores como pássaros, que estão lá o tempo todo. Eles não têm tempo de incubação." O estudo de Campos e seus colegas supera essa dificuldade, mas será muito difícil confirmar de outra maneira se ele é realmente a resposta para o problema. "Realizar experimentos com sistemas ecológicos é uma coisa bastante complexa. Primeiro porque a escala evolutiva não é curta - ou seja, é necessário deixar o sistema evoluir por séculos para obter um resultado preciso e confiável. Segundo, você tem de eliminar todas as fontes de perturbação do sistema, o que é muito difícil", diz o pesquisador. "Por isso é tão complicado reconstruir nossa história evolutiva de uma forma unívoca e precisa."

A pesquisa foi submetida para publicação no periódico científico "Physical Review Letters". (Veja [08])

10. Encontro 06 – Atividades de Aprofundamento e Curiosidade 3

Problema 10.1 – Três vendedores encontraram-se num certo dia na cidade de Vitória - ES e jantaram juntos. O primeiro vendedor visita esta cidade a cada seis dias, o segundo a cada oito dias e o terceiro a cada cinco dias. Estes três vendedores marcaram de jantar juntos novamente no próximo encontro, quantos dias depois esse jantar ocorrerá?

Solução: Os vendedores se encontram em quantidades de dias múltiplas de 5, 6 e 8. Assim, o próximo encontro será o M.M.C$(5, 6, 8)$, que calculamos usando a decomposição simultânea.

$$\begin{array}{r|l} 5\ ,\ 6\ ,\ 8 & 2 \\ 5\ ,\ 3\ ,\ 4 & 2 \\ 5\ ,\ 3\ ,\ 2 & 2 \\ 5\ ,\ 3\ ,\ 1 & 3 \\ 5\ ,\ 1\ ,\ 1 & 5 \\ \hline 1,\ 1,\ 1 & 2^3\ .\ 3\ .\ 5 \end{array}$$

M.M.C$(5, 6, 8) = 2^3\ .\ 3\ .\ 5 = 120$

Portanto, os vendedores jantarão juntos após 120 dias.

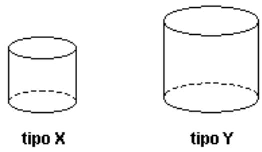
Problema 10.2 – Se o mínimo múltiplo comum entre os números 6 e k é maior do que 31 e menor do que 41, então qual deve ser o valor do número k?

Solução: Dado que o

$$31 < \text{M.MC}(6, k) < 41$$

e fazendo alguns cálculos percebemos que, como o único múltiplo de seis entre 31 e 41 é 36 e o M.M.C de 6 com qualquer outro número menor que 31 resulta em números maiores ou menores do que aqueles que estão nesse intervalo, o valor de k deve ser igual a 36.

Problema 10.3 – Uma empresa de construção dispõe de *117* blocos de tipo *X* e *145* blocos de tipo *Y*. Esses blocos têm as seguintes características: todos são cilindros retos, o bloco *X* tem *120* cm de altura e o bloco *Y* tem *150 cm* de altura. A empresa foi contratada para edificar colunas, sob as seguintes condições: cada coluna deve ser construída sobrepondo blocos de um mesmo tipo e todas elas devem ter a mesma altura. Com o material disponível, qual será o número máximo de colunas que podem ser construídas?



Solução: Para determinar o número máximo de colunas que podem ser construídas precisamos calcular quantos blocos de cada tipo, *X* e *Y*, são necessários em cada coluna, sabendo que todas as colunas tem o mesmo número de blocos. Para tanto, basta calcular o M.M.C*(120, 150)*. Assim:

$$
\begin{array}{r|l}
120,\ 150 & 2 \\
60,\ 75 & 2 \\
30,\ 75 & 2 \\
15,\ 75 & 3 \\
5,\ 25 & 5 \\
1,\ 5 & 5 \\
\hline
1,\ 1 & \text{M.M.C}(120, 150) = 2^3 \cdot 3 \cdot 5^2 = 600
\end{array}
$$

Para cada coluna do tipo *X* são necessárias *5* peças, pois, *5 . 120 = 600* e para cada coluna do tipo *Y* são necessárias *4* peças, pois, *4 . 150 = 600*. Como a empresa possui *117* blocos do tipo *X* ela poderá fazer *23* colunas desse tipo, sobrando duas peças. Para os blocos do tipo *Y*, com *145* peças, ela poderá fazer *36* colunas, sobrando uma peça. Portanto a empresa poderá fazer um total de *23 + 36 = 59* colunas.

Problema 10.4 – Conjectura de Goldbach: todo inteiro par maior que cinco pode ser expresso como uma soma de dois primos ímpares. Dê cinco exemplos de números que satisfazem a **Conjectura de Goldbach.** (Utilize números primos distintos)

Solução: Utilizando primos distintos teremos:

$8 = 3 + 5$ $10 = 3 + 7$ $12 = 5 + 7$ $14 = 3 + 11$ $16 = 5 + 11$

10.1 – Curiosidade 3 – Conjectura de Goldbach

Matemático peruano resolve problema de 3 séculos sobre números primos

24/05/201315h38 > Atualizada 24/05/2013 22h18

Harald Andrés Helfgott (foto) conseguiu resolver um problema com números primos - aqueles que só são divisíveis por eles mesmos e por um - que estava sem solução há quase 300 anos. O matemático desvendou a "conjectura fraca" de Goldbach, descrita em 1794, em que todo número ímpar maior do que 5 pode ser decomposto na soma de até três números primos. A teoria deriva da "versão forte", no qual todo número par maior que 2 é a soma de dois primos (Segundo CNRS/ENS).

O peruano Harald Andrés Helfgott conseguiu resolver um problema matemático sem solução por 271 anos. A chamada "conjectura fraca" proposta por Christian Goldbach, em 1742 , diz que cada número ímpar maior do que cinco pode ser expresso como uma soma de três números primos, mas ninguém tinha conseguido provar isto. Os números primos são aqueles que só são divisíveis por eles mesmos e por um.

"Nós expressamos em uma linha de texto uma verdade que não tinha sido demonstrada por mais de 270 anos (sobre o problema matemático)", disse Helfgott, em entrevista à Rádio Filarmonia.

O especialista lembrou que o problema havia sido descrito por Godfrey Harold Hardy em seu discurso de 1921 como um dos mais difíceis problemas não resolvidos da matemática. Há ainda a conjectura forte, que diz que todo número par maior que *2* é a soma de dois primos. Como o nome indica, a versão fraca seria confirmada se a versão forte fosse verdadeira: para representar um número ímpar como uma soma de três números primos seria suficiente subtrair *3* dele e aplicar a versão forte para o número par resultante. Por exemplo, *34* é a soma de *11* com *23*. Para chegar em *37*, bastaria somar *11*, *23* e *3*.

A conjectura forte não é abordada no estudo. Seu trabalho faz parte de uma longa linha de artigos que usam uma técnica chamada de "método do círculo de Hardy-Littlewood-Vinogradov". A ideia geral é transformar uma questão sobre números, neste caso, os primos, em integrais em círculos usando técnicas originalmente provenientes da análise de planos complexos.

Helfgott é pesquisador do Centro Nacional para Investigação Científica (CNRS) em Paris e seu estudo está disponível nos arquivos da Universidade de Cornell e ainda necessita revisão. (Veja [10])

11. Encontro 07 – Atividades de Aprofundamento e Curiosidade 4

Problema 11.1 – Priscila, Ana e Gabriela, colocadas em uma roda, se divertem com o seguinte jogo: uma delas escolhe um número inteiro e o diz em voz alta; a que está a sua esquerda divide esse número por seu maior divisor primo e fala o resultado em voz alta, e assim sucessivamente. Ganhará aquela que disser em voz alta o número *1*, momento em que o jogo termina. Ana escolheu um número inteiro maior do que *50* e menor do que *100* e ganhou. Priscila escolheu o inteiro imediatamente superior ao escolhido por Ana e também ganhou. Sabe-se que o número que Ana escolheu não é um múltiplo de *3*. Qual é ele?

Solução: Para que uma delas diga um número e ganhe, tem de falar um número composto por uma quantidade de fatores primos divisível por três (porque são três pessoas no jogo!). Os números maiores do que *50* e menores do que *100*, formados por uma quantidade de fatores primos divisível por três são:

$2 \cdot 2 \cdot 13 = 52$

$3 \cdot 3 \cdot 7 = 63$

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$

$2 \cdot 3 \cdot 11 = 66$

$2 \cdot 2 \cdot 17 = 68$

$2 \cdot 5 \cdot 7 = 70$

$3 \cdot 5 \cdot 5 = 75$

$2 \cdot 2 \cdot 19 = 76$

$2 \cdot 3 \cdot 13 = 78$

$2 \cdot 2 \cdot 23 = 92$

$2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 96$

$2 \cdot 7 \cdot 7 = 98$

$3 \cdot 3 \cdot 11 = 99$

Priscila escolheu o número imediatamente superior ao que Ana escolheu e também ganhou. Existem somente três pares de números nessas condições: “*63* e *64*”, “*75* e *76*” e “*98* e *99*”. Logo, o número que Ana escolheu pertence ao conjunto {*63*, *75*, *98*}. Como *63* e *75* são múltiplos de *3*, a resposta é *98*.

Problema 11.2 –Seja *N* o menor inteiro pelo qual se deve multiplicar *2520* para que o resultado seja o quadrado de um número natural. Calcule a soma dos algarismos de *N*.

Solução: Um número é quadrado perfeito se, na sua fatoração em números primos, todos os fatores assumirem expoente par. Assim, vamos analisar a fatoração do número *2520*.

$$\begin{array}{r|l} 2520 & 2 \\ 1260 & 2 \\ 630 & 2 \\ 315 & 3 \\ 105 & 3 \\ 35 & 5 \\ 7 & 7 \\ \hline 1 & 2^3 \,.\, 3^2 \,.\, 5 \,.\, 7 \end{array}$$

Assim, o menor número que devemos multiplicar $2^3 \,.\, 3^2 \,.\, 5 \,.\, 7$ resultando em um quadrado perfeito será $N = 2 \,.\, 5 \,.\, 7 = 70$. Assim, a soma dos algarismos de *N* será igual a $7 + 0 = 7$.

Problema 11.3 – Um professor inventou uma brincadeira para os seus alunos descobrirem os três números inteiros positivos que ele pensou. Primeiro o professor faz as seguintes afirmações sobre esses números: O produto dos três números é igual a *1105*; Nenhum dos números possuem *3* algarismos; A soma dos algarismos do maior número é igual ao dobro da soma dos algarismos do número do meio.

E, logo em seguida, um aluno tenta descobrir os números que ele pensou. Após ouvir o professor, uma aluna descobriu quais foram os números que ele pensou e falou que a diferença entre o maior e o menor número. Calcule essa diferença.

Solução: Precisamos descobrir os números que o professor pensou, para tanto vamos fatorar em primos o número *1105*.

$$\begin{array}{r|l} 1105 & 5 \\ 221 & 13 \\ 17 & 17 \\ \hline 1 & 5 \,.\, 13 \,.\, 17 \end{array}$$

Como a fatoração em primos de um número composto é única, os números que obedecem às hipóteses do problema e que o professor pensou foram *5, 13* e *17*. Assim, a diferença entre o maior número e o menor número é $17 - 5 = 12$.

11.1 – Curiosidade 4

Como os primos *17* e *29* são a chave para o fim dos tempos?

Durante a Segunda Guerra Mundial, o compositor francês Olivier Messiaen foi encarcerado como prisioneiro de guerra em Stalag VIII-A, onde havia um clarinetista, um violoncelista e um violinista entre seus colegas de prisão. Decidiu compor um quarteto com os três músicos, ele próprio ao piano. O resultado foi uma das grandes obras musicais do século XX: Quarteto para o fim dos tempos. Ele foi executado pela primeira vez para os detentos e oficiais da prisão dentro de Stalag VIII-A, com Messiaen tocando um vacilante piano de armário que encontrara no campo.

No primeiro movimento, chamado “Liturgia de cristal”, Messiaen quis produzir uma sensação de tempo interminável, e os primos *17* e *29* revelaram-se a chave. Enquanto o violino e a clarineta intercambiavam temas representando canto de pássaros, o violoncelo e o piano forneciam a estrutura rítmica. Na partitura do piano há uma sequência rítmica de *17* notas que se repete muitas e muitas vezes, e a sequência de acordes tocada por cima desse ritmo é formada por *29* acordes. Assim, quando o ritmo de *17* notas começa pela segunda vez, a sequência de acordes está chegando apenas a *2/3*. O efeito da escolha dos números primos *17* e *29* é que as sequências rítmicas e de acordes não se repetiam até a nota *17x29* da peça.

Essa música em contínua mudança cria a sensação de tempo interminável que Messiaen teve a perspicácia de estabelecer — e ele usa o mesmo truque que as cigarras com seus predadores. Pense nas cigarras como o ritmo e nos predadores como os acordes. Os diferentes primos *17* e *29* mantêm as sequências fora de sincronia, de modo que a peça termina antes que você ouça a música se repetir.

Messiaen não foi o único compositor a utilizar números primos. Alban Berg também recorreu a um numero primo como assinatura de sua música. Assim como David Beckham, Berg usava o número *23* — na verdade, era obcecado por ele. Por exemplo, em Lyric Suite, sequências de *23* barras compõem a estrutura da peça. Mas imersa dentro da peça há a representação de um caso amoroso que Berg tinha com uma rica mulher casada. Sua amante era simbolizada por uma sequência de *10* barras que ele emaranhava com sua própria assinatura *23*, usando a combinação de Matemática e música para dar vida ao romance.

‘Liturgia de cristal’, de Messiaen, do Quarteto para o fim dos tempos. O primeiro traço vertical indica onde termina a primeira sequência rítmica de *17* notas, O segundo traço vertical indica o timbre da sequência harmônica dc *29* notas.

Da mesma maneira que Messiaen empregou os primos no Quarteto para o fim dos tempos, a matemática recentemente foi usada para criar uma peça que, embora não seja atemporal, não se repetirá por mil anos. Para marcar a virada do novo milênio, Jem Finer, membro fundador da banda The Pogues, decidiu criar uma instalação musical no East End de Londres que se repetiria pela primeira vez na virada do próximo milênio, em *3000*. Ela se chama, apropriadamente, Longplayer.

Finer começou com uma peça de música criada com taças e sinos tibetanos de diversos tamanhos. A fonte musical original tem *20* minutos e *20* segundos de duração, e, utilizando alguma matemática similar aos truques empregados por Messiaen, ele a expandiu para uma peça com duração de mil anos. São tocadas simultaneamente seis cópias da fonte musical original, mas em diferentes velocidades. Além disso, de *20* em *20* segundos, cada trilha é reiniciada a uma distância determinada da reprodução original, embora a alteração das trilhas seja diferente. E na decisão de quanto alterar cada trilha que se usa a matemática, para garantir que as trilhas não se alinhem perfeitamente de novo antes de mil anos.

Não apenas os músicos são obcecados por primos. Esses números parecem entrar em sintonia com praticantes de muitas espécies de artes. O autor Mark Haddon só usava números primos nos capítulos de seu best-seller O estranho caso do cachorro morto. O narrador da história é um menino com síndrome de Asperger chamado Christopher, que gosta do mundo matemático porque pode entender como ele se comportará — a lógica desse mundo significa que ele não tem surpresas. As interações humanas, porém, são repletas de incertezas e mudanças ilógicas que Christopher não consegue suportar. Como ele próprio explica: “Eu gosto de números primos... Acho que os números primos são como a vida. São muito lógicos, mas a gente nunca consegue entender as regras, mesmo que se passe a vida toda pensando nelas.”

Os números primos têm até uma participação no cinema. No filme de suspense futurista Cubo, sete personagens são aprisionados num labirinto de salas que se assemelha a um complexo cubo de Rubik — o cubo mágico. Cada sala no labirinto tem forma de cubo, com seis portas levando a outras salas do labirinto, O filme começa quando os personagens acordam e se descobrem dentro do labirinto. Eles não têm ideia de como chegaram lá, mas precisam encontrar uma saída. O problema é que algumas das salas são armadilhas. Os personagens precisam descobrir algum meio de saber se uma sala é segura antes de entrar nela, pois toda uma série de mortes horrorosas os aguarda, inclusive ser incinerado, coberto de ácido ou fatiado em minúsculos cubos — como percebem depois que um deles é morto.

Uma das personagens, Joan, é matemática e de repente vê que os números na entrada de cada sala encerram a chave para revelar se há uma armadilha. Parece que se algum dos números na entrada é primo a sala contém uma armadilha. “Que lindo cérebro”, declara o líder do grupo diante desse modelo de dedução matemática. Acontece que eles também precisam tomar cuidado com potências primas, mas isso se mostra além da capacidade da sagaz Joan. Eles passam a depender de outro integrante, um autista savant, o único que sai com vida do labirinto de números primos.

Como as cigarras descobriram, saber matemática é a chave para a sobrevivência neste mundo. Qualquer professor com dificuldade em motivar sua turma de matemática poderia achar nas sangrentas mortes de Cubo uma grande peça de propaganda para fazer seus alunos aprenderem os números primos. (Veja [05])

12. Encontro 8 – Atividades de Aprofundamento e Curiosidade 5

Problema 12.1 – (CESPE - Carteiro Correios 2011) Em um bairro onde as casas foram todas construídas de acordo com um projeto padrão, os lotes têm *12* metros de frente. Em cada lote a caixa de correspondências fica sempre na mesma posição e os postes de iluminação pública são espaçados de *50* metros. O carteiro que entrega correspondências nesse bairro percebeu que a caixa de correspondências da primeira casa de uma rua bastante longa fica exatamente atrás de um poste de iluminação. Nesse caso, caminhando nessa rua e desconsiderando os possíveis espaços entre dois lotes vizinhos, até que encontre a próxima caixa de correspondências atrás do poste de iluminação, o carteiro deverá percorrer uma distância igual a quantos metros?

Solução: Note que queremos conhecer quando um múltiplo de *12* coincidirá com um múltiplo de *50*, ou seja, o mínimo múltiplo comum, popular mmc.

$$
\begin{array}{r|l}
50,\ 12 & 2 \\
25,\ \ 6 & 2 \\
25,\ \ 3 & 3 \\
25,\ \ 1 & 5 \\
5,\ \ 1 & 5 \\
\hline
1,\ \ 1 &
\end{array}
\qquad 2^2.3.5^2 = 300
$$

Portanto, o carteiro deverá percorrer uma distância igual a *300* metros para encontrar outra caixa de correios atrás de um poste.

Problema 12.2 – Uma gráfica está imprimindo dois tipos de livros: *A* e *B*. O tempo necessário para que um livro *A* seja impresso é *50* minutos, e para que um livro *B* seja impresso é *90* minutos. Sabendo-se que as máquinas que imprimem os livros trabalham continuamente, sem parar, e que, certo dia, às *7* horas da manhã, um livro *A* e um *B* ficaram prontos ao mesmo tempo, pode-se afirmar que isso irá ocorrer novamente em que horário?

Solução: O livro *A* é impresso em: *90 min, 180 min, 270 min...*, ou seja, todos os múltiplos de *90*. O livro *B* é impresso em: *50 min, 100 min, 150 min...*, ou seja, todos os múltiplos de *50*. Precisamos achar o menor desses múltiplos, de modo que sejam iguais, ou seja, o mmc deles.

$$\begin{array}{r|l} 50,\ 90 & 2 \\ 25,\ 45 & 3 \\ 25,\ 15 & 3 \\ 25,\ \ 5 & 5 \\ 5,\ \ 1 & 5 \\ \hline 1,\ \ 1 & \end{array} \qquad 2 \cdot 3^2 \cdot 5^2 = 450$$

Temos então que após *450* minutos os livros ficaram prontos ao mesmo tempo, e que *450* minutos correspondem a *7* horas e *30* minutos, ou seja

7 horas + *7* horas e *30* minutos = *14* horas e *30* minutos

Problema 12.3 – O piso de uma sala retangular, medindo $3{,}52\ m \times 4{,}16\ m$ será revestido com ladrilhos quadrados, de mesma dimensão, inteiros, de forma que não fique espaço vazio entre ladrilhos vizinhos. Os ladrilhos serão escolhidos de modo que tenham a maior dimensão possível. Na situação apresentada, qual deve ser a medida do lado do ladrilho?

Solução: Como as respostas estão em *cm*, vamos considerar a medida da área da sala em cm^2, a saber: *352cm x 416cm.* Note que estamos querendo revestir com ladrilhos quadrados iguais de modo que não fiquem espaços vazios e que sejam os maiores possíveis. Não é difícil observar que na verdade estamos querendo achar o maior divisor comum, o popular M.D.C.

$$\begin{array}{r|l} 416,\ 352 & \mathbf{2} \\ 208,\ 176 & \mathbf{2} \\ 104,\ \ 88 & \mathbf{2} \\ 52,\ \ 44 & \mathbf{2} \\ 26,\ \ 22 & \mathbf{2} \\ 13,\ 11 & 11 \\ 13,\ \ 1 & 13 \\ \hline 1,\ \ 1 & \end{array}$$

Os fatores primos em comum são $2^5 = 32$. Assim, o lado do ladrilho deve medir *32 cm.*

Problema 12.4 – Uma empresa de logística é composta de três áreas: administrativa, operacional e vendedores. A área administrativa é composta de *30* funcionários, a operacional de *48* e a de vendedores com *36* pessoas. Ao final do ano, a empresa realiza uma integração entre as três áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários com o maior número possível. Determine quantos funcionários devem participar de cada equipe e o número possível de equipes.

Solução: Precisamos encontrar o maior divisor comum entre *48, 36* e *30*. Assim, vamos calcular o MDC*(48, 36, 30)* fatorando simultaneamente.

$$\begin{array}{r|l}
48,\ 36,\ 30 & \mathbf{2} \\
24,\ 18,\ 15 & 2 \\
12,\ 9,\ 15 & 2 \\
6,\ 9,\ 15 & 2 \\
3,\ 9,\ 15 & \mathbf{3} \\
1,\ 3,\ 5 & 3 \\
1,\ 1,\ 5 & 5 \\
\hline
1,\ 1,\ 1 &
\end{array}$$

Logo, o número de participantes em cada equipe é MDC $(30, 36, 48) = 2 \cdot 3 = 6$.

Determinando o número total de equipes:

$48 + 36 + 30 = 114 \rightarrow 114 : 6 = 19$ equipes

O número de equipes será igual a *19*, com *6* participantes cada uma.

Problema 12.5 – Determine todos os números inteiros positivos n tais que n, $n + 2$ e $n + 4$ sejam primos.

Solução: O número n não pode ser par uma vez que, se $n = 2k$ então teríamos,
$n + 2 = 2k + 2 = 2(k + 1)$ par e, portanto, não seria primo. Assim, n, $n + 2$ e $n + 4$ são três ímpares consecutivos. Ora, $n = 3$, $n + 2 = 5$ e $n + 4 = 7$ são três primos ímpares consecutivos. Para $n > 3$, temos $n = 3k$ ou $n = 3k + 1$ ou $n = 3k + 2$, com $k > 1$.
Se $n = 3k$ então n não seria primo, pois seria múltiplo de 3.
Se $n = 3k + 1$ então $n + 2 = 3k + 1 + 2 = 3k + 3 = 3(k + 1)$ e teríamos que $n + 2$ não seria primo por ser múltiplo de 3. Se $n = 3k + 2$, $n + 4 = 3k + 2 + 4 = 3.(k + 2)$ então teríamos que $n + 4$ não seria primo por ser múltiplo de 3.
Portanto, o único valor de n para que n, $n + 2$ e $n + 4$ sejam primos é 3 e temos então que apenas 3 inteiros satisfazem a hipótese do problema: 3, 5 e 7.

13.1 – Curiosidade 5

Criptografia RSA

O mais conhecido dos métodos de criptografia de chave pública é o RSA. Este código foi inventado em 1977 por R. L. Rivest, A. Shamir e L. Adleman, que na época trabalhavam no Massachussets Institute of Technology (M.I.T.), uma das melhores universidades americanas. As letras RSA correspondem às iniciais dos inventores do código. Há vários outros códigos de chave pública, mas o RSA continua sendo o mais usado em aplicações comerciais.

O Método RSA

A descrição completa do funcionamento do RSA é justamente o tema desta apostila. Para entender como funciona precisaremos estudar várias ideias e técnicas novas de matemática. Nesta seção explicaremos apenas o suficiente sobre o RSA para que você entenda como
é possível um problema ser "fácil de fazer e difícil de desfazer". Isto também nos ajudará a identificar os problemas matemáticos que precisaremos abordar para poder discutir os detalhes do funcionamento do RSA. Digamos que você vai criar uma implementação do RSA para uma determinada loja, que vai usá-lo na codificação de dados de clientes em compras pela internet. Para começar, você precisa escolher dois números primos distintos e multiplicá-los, obtendo um número inteiro n. A loja manterá secreta a informação sobre quais são os primos escolhidos, porque é isto que é necessário para decodificar as mensagens enviadas usando a versão do RSA que você está construindo. Já n vai ser enviado para o computador de qualquer pessoa que compre nessa loja pela web, porque é dele que o computador do usuário necessita para codificar os dados sobre o do cartão de crédito e enviá-los ao computador da loja. Portanto, no caso do RSA, o problema "fácil de fazer e difícil de desfazer" é simplesmente multiplicar dois primos.
Já consigo imaginar você pensando:
Só isso? Mas para desfazer o problema basta fatorar o número e achar os primos!

É verdade, mas há um detalhe que esqueci de contar: estes números primos serão muito, muito grandes. Na prática uma chave segura de RSA é gerada a partir de números primos de cerca de 100 algarismos cada, de forma que n, que é o produto destes primos, terá cerca de 200 algarismos. Acontece que, como veremos na página 29, podem ser necessários zilhões de anos para fatorar um número deste tamanho e achar seus fatores primos – mesmo se usarmos os mais poderosos computadores existentes atualmente.

Resumindo: ² para implementar o RSA escolhemos dois primos distintos muito grandes p e q e calculamos o produto n = p ¢ q; ² para codificar uma mensagem usamos n; para decodificar uma mensagem usamos p e q;

- n pode ser tornado público;
- p e q precisam ser mantidos em segredo;
- quebrar o RSA consiste em fatorar n, que leva muito tempo se n for grande.

Teoria de Números

O que vimos acima sugere que os principais problemas matemáticos relacionados ao RSA são: como achar números primos e como fatorar um número. A área da matemática a que estes problemas pertencem é conhecida como teoria de números e tem por objetivo geral o estudo das propriedades dos números inteiros. Entre os problemas que teremos que estudar para podermos descrever completamente o RSA também estão:

- como calcular os restos da divisão de uma potência por um número dado;
- como achar um número que deixa restos especificados quando dividido por uma série de números dados;
- como estabelecer critérios de divisibilidade por números primos.

Há muitos outros problemas que são parte da teoria dos números, mas dos quais não trataremos aqui, entre eles:

1. Calcular o máximo divisor comum entre dois números dados;
2. Determinar todos os inteiros a, b e c que satisfazem $a^2 + b^2 = c^2$;
3. Mostrar que se três inteiros a, b e c satisfazem $a^n + b^n = c^n$, onde $n > 2$ é um inteiro positivo, então a, b ou c têm que ser iguais a zero;
4. Provar que $2^{2n} + 1$ é composto se $n > 4$;
5. Provar que todo número par é soma de dois primos ímpares;
6. Determinar todos os inteiros consecutivos que são potências de números inteiros.

Os problemas acima têm grau de dificuldade muito variável. A solução de alguns deles é conhecida desde a antiguidade, como é o caso de (1) e (2). Na verdade, é bem provável que você saiba resolver (1) usando o método descrito por Euclides em seu livro Elementos escrito por volta de 300 a.C.; já (2) está relacionado ao Teorema de Pitágoras o que talvez baste para lembrar-lhe de algumas soluções possíveis. Todas as outras questões são muito mais difíceis. Para começar temos (3), que é muito parecida com (2), exceto pelo fato do expoente n ter que ser pelo menos 3. Este problema tem uma história muito interessante. Em algum momento entre 1621 e 1636 o francês Pierre de Fermat, magistrado da corte de Toulouse, adquiriu uma cópia da recém-publicada tradução latina da Aritmética escrita pelo matemático grego Diofanto mais de mil anos antes. Fermat, que era um matemático amador, leu o texto de Diofanto, fazendo várias anotações na margem do texto. Em uma dessas anotações ele afirmou ter uma demonstração do fato enunciado em (3) mas, segundo ele, o espaço disponível na margem do livro não seria suficiente para conter seu argumento. É improvável que a demonstração de Fermat estivesse correta, já que o resultado permaneceu sem demonstração até 1995. Como este foi o último resultado enunciado por Fermat a ser demonstrado, tornou-se conhecido como o Último Teorema de Fermat. Para complicar, os métodos usados por A. Wiles em sua prova de (3) são extremamente sofisticados e sequer existiam há 50 anos atrás. A questão (4) é outra que está ligada ao nome de Fermat. Na verdade, o número

$$F(N) = 2^{2n} + 1$$

é conhecido como o n-ésimo número de Fermat porque, em uma de suas cartas a um outro matemático, Fermat propôs que F(n) seria sempre primo, qualquer que fosse o valor de n. De fato, calculando F(n) para n de 0 a 4 obtemos os números listados na tabela 2.

n	F(n)
0	3
1	5
2	17
3	257
4	65537

Tabela 2: Números de Fermat primos

que são todos primos. Aparentemente, foi nessa tabela que Fermat baseou-se para fazer a sua afirmação. Infelizmente, generalizar a partir de alguns casos é sempre uma prática perigosa em matemática e, neste caso, Fermat deu-se realmente mal. Nenhum número primo da forma

F(n) é conhecido quando n > 4, daí o problema enunciado em (4), que ninguém até hoje sabe como resolver. A questão (5) é conhecida como Conjectura de Goldbach, em homenagem a Christian Goldbach, um outro matemático amador, que viveu na mesma época que Euler, com quem trocava frequentes cartas sobre matemática. Embora se saiba que todo número par com menos de 18 algarismos seja mesmo a soma de dois primos ímpares, ninguém até hoje conseguiu provar o enunciado de Goldbach. Apesar disso, alguns resultados parciais são conhecidos. Um dos mais recentes foi a demonstração descoberta em 2002 por Roger Heath-Brown e Jan-Christoph Schlage-Puchta de que todo número par muito grande pode ser escrito como a soma de dois primos ímpares e exatamente 13 potências de 2. Se você tentar descobrir duas potências de inteiros pequenos, que sejam consecutivas, vai logo dar de cara com 8 e 9, que são iguais a 23 e 32, respectivamente. Por mais que procure, não encontrará outros exemplos. Em vista disso, o matemático belga Eugène Charles Catalan propôs em 1844 que essas duas potências seriam as únicas soluções do problema (5). Isto é correto, como foi provado pelo matemático romeno Preda Mihailescu em 2002. Talvez você tenha percebido que, embora os enunciados das cinco questões acima sejam muito fáceis de entender, resolvê-las pode ser muito difícil: o Último Teorema de Fermat levou mais de 300 anos para ser provado e o problema proposto por Catalan levou 158 anos. Sem falar da conjectura de Goldbach e do problema relativo aos números de Fermat, que até hoje ninguém sabe resolver.

Histórico

Encaminhar uma mensagem de forma segura é uma preocupação que remonta aos primeiros estrategistas que se têm notícia, na Grécia Antiga. Houve época em que soldados tinham mensagens escritas em seu couro cabeludo como estratégia para transpassar uma informação pelas linhas inimigas, bastando chegar ao seu destino e ter sua cabeça raspada. Com o passar dos anos, a evolução da Matemática e a criatividade humana em desenvolver novos mecanismos fez com que a arte cifrar mensagens grande destaque nas decisões políticas, com influência direta nos acontecimentos históricos. Na Segunda Guerra Mundial, a Alemanha dispunha de um intrincado sistema de informações criptografadas. A base de todo esse sistema era uma máquina eletromecânica conhecida como **enigma**, capaz de gerar mensagens criptografadas com enorme facilidade. A preocupação com a guarda das informações é a base da **Criptografia** , essencial para o tráfego de informações, especialmente nos dias atuais.

O algoritmo RSA

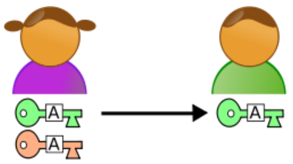
Um dos algoritmos mais seguros de encriptação de informações atuais originou-se dos estudos de Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, um trio de Matemáticos brilhantes que mudaram a história da Criptografia. O princípio do algoritmo é construir chaves públicas e privadas utilizando números primos. Uma **chave** é uma informação restrita que controla toda a operação dos algoritmos de criptografia. No processo de codificação uma chave é quem dita a transformação do texto puro (original) em um texto criptografado.

Chave Privada: É uma informação pessoal que permanece em posse da pessoa - não publicável.

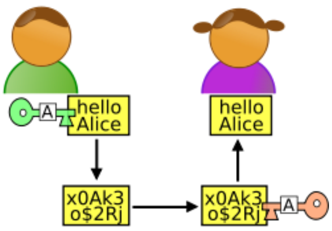
Chave Pública: Informação associada a uma pessoa que é distribuída a todos.

Uma analogia amplamente conhecida no meio acadêmico é a transmissão de mensagens entre Alice e Bob. Alice e Bob são personagens fictícios que precisam trocar mensagens seguras sem interceptação. O algoritmo RSA permite essa troca segura de mensagens pela utilização de chaves públicas e privadas: Alice cria seu par de chaves (uma pública e outra privada) e envia sua chave pública para todos, inclusive Bob; Bob escreve sua mensagem para Alice. Após escrita, Bob faz a cifragem do texto final com a chave pública de Alice, gerando um texto criptografado; Alice recebe o texto criptografado de Bob e faz a decifragem utilizando a sua chave privada. O procedimento é realizado com sucesso porque **somente a chave privada de Alice** é capaz de decifrar um texto criptografado com a sua chave pública. É importante destacar que se aplicarmos a chave pública de Alice sobre o texto criptografado não teremos a mensagem original de Bob. Dessa forma, mesmo que a mensagem seja interceptada é impossível decifrá-la sem a chave privada de Alice.

As figuras a seguir ilustram bem a dinâmica de uso de chaves públicas e privadas.



Alice envia sua chave pública para todos, inclusive Bob.



Bob cifra a mensagem com a chave pública de Alice e a envia.

Alice, por sua vez, recebe o texto criptografado e o decifra utilizando sua chave privada.

Funcionamento

Conforme mencionado, o algoritmo RSA é baseado na construção de chaves públicas e privadas utilizando números primos. Inicialmente devem ser escolhidos dois números primos quaisquer ***P*** e ***Q***. Quanto maior o número escolhido mais seguro será o algoritmo. A título de exemplificação, serão escolhidos números primos pequenos, para permitir um acompanhamento de todo o processo de cifragem e decifragem. $P = 17$ $Q = 11$

A seguir são calculados dois novos números ***N*** e ***Z*** de acordo com os números ***P*** e ***Q*** escolhidos:

$N = P * Q$ $Z = (P - 1) * (Q - 1)$

No caso obtêm-se como resultado:

$N = 17 * 11 = 187$ $Z = 16 * 10 = 160$

Agora define-se um número *D* que tenha a propriedade de ser ***relativamente primo com Z***. Pode-se escolher qualquer número que satisfaça essa propriedade. Nesse exemplo, visando simplificação dos cálculos, opta-se pela escolha: $D = 7$

De posse desses números começa o processo de criação das chaves públicas e privadas. É necessário encontrar um número ***E*** que satisfaça a seguinte propriedade: $(E * D) \bmod Z = 1$

Se forem feitos os testes com *1, 2, 3...* teremos:

$E = 1 => (1 * 7) \bmod 160 = 7$	$E = 2 => (2 * 7) \bmod 160 = 14$
$E = 3 => (3 * 7) \bmod 160 = 21$	$E = 23 => (23 * 7) \bmod 160 = 1$
$E = 183 => (183 * 7) \bmod 160 = 1$	$E = 343 => (343 * 7) \bmod 160 = 1$
$E = 503 => (503 * 7) \bmod 160 = 1$	

Logo até o momento os números *23, 183, 343, 503* satisfazem a propriedade indicada. Para efeito de simplificação de cálculos, será tomado como referência:

$E = 23$.

Com esse processo definem-se as chaves de encriptação e desencriptação. Para encriptar: utilizar ***E*** e ***N*** - esse par de números será utilizado como chave **pública**. Para desencriptar: utilizar ***D*** e ***N*** - esse par de números utilizado como chave **privada**.

As equações são:

$$\text{TEXTO CRIPTOGRAFADO} = (\text{TEXTO ORIGINAL})^{E} \bmod N$$

$$\text{TEXTO ORIGINAL} = (\text{TEXTO CRIPTOGRAFADO})^{D} \bmod N$$

Caso prático para o exemplo

Seja a necessidade de se encaminhar uma mensagem bem curta de forma criptografada, como o número ***4*** por exemplo, tendo por base as chaves aqui estabelecidas.

Para codificar:

$$\text{TEXTO ORIGINAL} = 4$$

$$\text{TEXTO CRIPTOGRAFADO} = (4^{23}) \bmod 187$$

$$\text{TEXTO CRIPTOGRAFADO} = 70.368.744.177.664 \bmod 187$$

$$\text{TEXTO CRIPTOGRAFADO} = 64$$

Para decodificar:

TEXTO RECEBIDO = 64

TEXTO ORIGINAL = (64^7) *mod 187*

TEXTO ORIGINAL = 4.398.046.511.104 mod 187

TEXTO ORIGINAL = 4

A questão das escolhas dos números primos envolvidos é fundamental para o algoritmo. Por essa razão escolhem-se números primos gigantescos para garantir que a chave seja inquebrável. Assim como o exemplo apresentado, existem outras combinações que podem ser feitas rapidamente para confirmação, sem que se exija uma aplicação especial para os cálculos envolvidos. (Veja [12])

P	***Q***	***D***	***E***
11	*17*	*7*	*23*
5	*7*	*11*	*35*
3	*13*	*7*	*31*
3	*13*	*7*	*7*
3	*5*	*17*	*9*

13. Encontro 9 – Atividades de Aprofundamento 6

Problema 13.1 – Mostrar que se $n^2 + 2$ é primo então 3 é um divisor de n.

Solução: Todo número inteiro é da forma $3k$, $3k + 1$ e $3k + 2$. Se n é da forma $3k + 1$, teremos:

$$n^2 + 2 = (3k + 1)^2 + 2 = (3k)^2 + 6k + 1 + 2 = 3.(k^2 + 2k + 1)$$

Então, para números da forma $(3k + 1)$, $n^2 + 2$ é composto e tem 3 como um de seus divisores. Se n é da forma $3k + 2$, teremos:

$$n^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 4 + 2 = 3.(3k^2 + 4k + 2)$$

Assim, para números da forma $(3k + 2)$, $n^2 + 2$ não é primo e possui 3 como um de seus divisores. Assim, números da forma $n^2 + 2$ só poderão ser primos se n for da forma $3k$, que é divisível por 3.

Problema 13.2 – Se $p > 5$ é um primo, então $p^2 + 2$ é composto.

Solução: Todo número inteiro pode ser representado por uma das formas $3k$, $3k + 1$ ou $3k + 2$. Para $p = 3k$, p não é primo. Portanto, se p é primo e maior ou igual a 5, p é da forma $3k + 1$ ou $3k + 2$, com $k > 1$.

Se $p = 3k + 1$, temos

$$p^2 + 2 = (3k + 1)^2 + 2 = 9k^2 + 6k + 1 + 2 = 9k^2 + 6k + 3 = 3.(9k^2 + 6k + 1)$$

é múltiplo de 3, maior que 3 pois $k > 1$.

Se $p = 3k + 2$, temos

$$p^2 + 2 = (3k + 2)^2 + 2 = 9k^2 + 12k + 4 + 2 = 9k^2 + 12k + 6 = 3.(3k^2 + 4k + 2)$$

é múltiplo de 3, maior que 3, pois $k > 1$.

Assim, qualquer que seja $p > 5$, com p primo, $p^2 + 2$ é composto.

Problema 13.3 – Mostrar, por meio de um contra exemplo que a seguinte informação é falsa: Todo número quadrado perfeito possui apenas três divisores naturais.

Solução: De fato, considere o número 36 que é um quadrado perfeito. Usando a decomposição em fatores primos podemos determinar todos os divisores de *36*.

		1
36	*2*	*2*
18	*2*	*4*
9	*3*	*3, 6, 12*
3	*3*	*9, 18, 36*
1		

Logo, verificamos que o número 36 possui como divisores {*1, 2, 3, 4, 6, 9, 12, 18, 36*} Portanto mais de três divisores naturais.

Problema 13.4 – Partindo da ideia do problema anterior prove que todo número primo elevado ao quadrado possui apenas três divisores naturais.

Solução: De fato, dado que um número p é primo, então possui como divisores naturais apenas o número um e o próprio p. Considere o número p^2 que pode ser escrito na forma $p^2 = p \,.\, p$ que possui como divisores naturais o número 1, p e o próprio p^2. Portanto, três divisores naturais.

14. Encontro 10 – Atividades de Aprofundamento 7

Problema 14.1 – Demonstre que o número $\underbrace{1000...001}_{2012 \to zeros}$ é composto.

Solução: Para termos uma ideia da prova deste fato, vamos provar que o número 1001 é composto. Ora, temos que 1001 = 11 . 91. Do mesmo modo, 100001 = 11 . 9091 e que 10000001 = 11 . 909091. Assim, depois dessa análise inicial, fica bem claro que nosso candidato para divisor do número pedido é o 11; Podemos verificar sem maiores dificuldades que

$$\underbrace{1000...001}_{2012 \to zeros} = 11.\underbrace{90.90....90}_{1005 \to vezes}.91$$

Problema 14.2 – Encontre números primos *p, q, r* para os quais $p + q^2 + r^3 = 200$. Diga todas as possibilidades.

Solução: Vamos fazer um estudo das potências maiores para as potências menores, isto é, quais os valores que *q* e *r* podem assumir para que q^2 e r^3 satisfaçam a soma $p + q^2 + r^3 = 200$. Usando essa estratégia, verificamos que *r* deve assumir números primos menores que *7* pois $7^3 = 243 > 200$; Analogamente, *q* deve assumir números primos menores que *17*, pois $17^2 = 289 > 200$; Assim

- Caso $q = 13$ temos $13^2 = 169$; $r = 2$ temos $2^3 = 8$; $p = 23$ e, logo o terno *(23, 13, 2)* é uma possibilidade.

- Caso $q = 11$ temos $11^2 = 121$; $r = 2$ temos $2^3 = 8$; $p = 71$ e, logo o terno *(71, 11, 2)* é uma possibilidade.

- Caso $q = 2$ temos $2^2 = 4$; $r = 5$ temos $5^3 = 125$; $p = 71$ e, logo o terno *(71, 2, 5)* é uma possibilidade.

Portanto, esses são os ternos que satisfazem a soma $p + q^2 + r^3 = 200$: *(23, 13, 2), (71, 11, 2)* e *(71, 2, 5)*.

Problema 14.3 – Mostrar que todo inteiro da forma $n^4 + 4$, com $n > 1$ é composto.

Solução: Considere a expressão $(n^2+2)^2 - 4n^2 = n^4 - 4$. Assim,

$(n^2 + 2 - 2n)\,(n^2 + 2 + 2n) = n^4 + 2n^2 + 2n^3 + 2n^2 + 4 + 4n – 2n^3 – 4n – 4n^2 = n^4 - 4$

$(n^2 + 2)^2 - 4n^2 => (n^2 + 2 - 2n)\,(n^2 + 2 + 2n)$ nesse ponto chegamos a um produto de dois números, com $n > 1$ (dado) caracterizando um composto.

Problema 14.4 – Os números naturais $p = 2^{31} - 1$ e $q = 2^{61} - 1$ são primos. Então, quantos e quais são os divisores de $2.p.q$?

Solução: Dado que p e q são primos o produto $2.p.q$ terá como divisores $\{1, 2, p, q\}$

Problema 14.5 – Prove que se n é ímpar então $n^2 - 1$ é divisível por 8.

Solução:. Como n é ímpar, temos que $n = 2q + 1$ para algum $q \in$ Z. Assim,

$n^2 - 1 = (2q + 1)^2 - 1 = 4q^2 + 4q + 1 - 1 = 4q^2 + 4q = 4q(q + 1)$:

Como q e $q + 1$ são consecutivos, um deles tem que ser par. Logo, $n^2 - 1$ é divisível por 8.

Problema 14.6 – Um robô possui dois botões, permitindo que a cada momento ele suba a degraus ou desça b degraus de uma escada com infinitos degraus. Sabendo que o robô está no início da escada, pergunta-se:

(a) Se $a = 12$ e $b = 3$, é possível que o robô visite todos os degraus após uma sucessão desses movimentos?

Solução: Se apertamos o botão de subir x vezes e o de descer y vezes, o robô irá subir ou descer $12x - 3b$ degraus. Note que esse número é sempre múltiplo de 3, não sendo possível para o robô com uma sequência desses movimentos atingir um degrau com número que não é divisível por 3.

(b) Mostre que se a e b são primos entre si, o robô consegue visitar todos os degraus.

Solução: Como a e b são primos entre si, pelo Teorema de Bezout-Bachet, é possível encontrar x e y de modo que $ax - by = 1$. Assim, o robô pode sair do nível inicial e ir para o degrau 1 apertando-se x vezes o botão de subir e em seguida apertando-se y vezes o botão de descer. Repetindo esse procedimento, o robô pode atingir qualquer degrau.

Teorema de Bezout-Bachet: Dados inteiros *a* e *b*, não ambos nulos, existem inteiros *m* e *n* tais que *am* + *bn* = mdc(*a, b*).

Demonstração:

Vamos definir o conjunto $B = \{ma + nb; m, n \in Z\}$. Seja $c = ma + nb$ o menor elemento de B. Basta mostrar que c divide a e b. Suponha por contradição que c não divide a, então existe q e r naturais, tais que $a = q.c + r$ com $0 < r < c$, assim

$$r = a - q.c$$
$$r = a - q.(ma + nb)$$
$$r = (1 - qm)a + (-qn)b$$

$\Rightarrow r \in B$ Pois c é o menor elemento de B. Assim c divide a e, de forma análoga, c divide b.

Como d = mdc(a, b) então d divide a e b, desse modo existem $k_1, k_2 \in N$ tais que

$$a = k_1 d$$
$$b = k_2 d$$
$$\Rightarrow c = ma + nb = mk_1 d + nk_2 d$$
$$\Rightarrow c = (mk_1 + nk_2)d$$

Então d divide c e, portanto $d \leq c$ (ambos positivos)

Mas como d < c não é possível uma vez que d = mdc(a, b) então $d = ma + nb$.

15. Experiência como o Projeto Piloto.

O projeto foi aplicado entre os meses de setembro e novembro de 2013, com um encontro semanal de 60 minutos, como citado anteriormente, com duas turmas do segundo ano do ensino médio da Escola de Ensino Fundamental e Médio Arnulpho Matos situado no Bairro República – Vitória. Participaram como colaboradores o Professor Filipe Pinel Bermudes e seus alunos, que por motivos éticos não faremos constar os seus nomes. Havendo a necessidade de adaptar o projeto às condições da escola, trabalhamos cinco aulas em cada turma de forma que nas primeiras aulas foram apresentados os conteúdos básicos para um nivelamento prévio onde constatamos uma dificuldade muito grande da maioria dos alunos, num primeiro momento, em relembrar o conteúdo e num segundo momento em fazer leitura e interpretação dos problemas propostos. Em algumas aulas, um pequeno número de alunos deixou de participar das aulas, porém a grande maioria dos alunos teve uma participação proveitosa, fazendo a escrita da teoria apresentada e se empenhando na resolução dos problemas.

Durante o processo de resolução, os alunos discutiram ideias sobre os caminhos a seguir, a lógica de algumas situações trabalhadas tanto da teoria quanto dos problemas propostos e souberam organizar com qualidade as respostas desenvolvidas (Anexo 1). Queremos valorizar o esforço e a participação dos alunos que, mesmo deixando algumas questões em branco ou incompletas, se esforçaram e tentaram produzir o máximo possível. Para motivá-los, essa foi uma frase que procurei falar sempre com eles: “Produzir o máximo possível” independentemente de estar correta ou não a linha de raciocínio, pois queria extrair deles o máximo possível de conhecimento e aplicação (anexos 2 e 3). Nesse sentido é importante ressaltar que algumas estratégias eram erradas ou equivocadas. O aluno iniciava bem, tomava a decisão de qual caminho seguir, mas ao chegar à conclusão para finalizar o problema cometia alguns erros que julgo preocupante para a faixa etária e a série que o mesmo se encontra (Anexos 3 e 4).

Paralelo às atividades, apresentamos aos alunos também algumas das curiosidades listadas no corpo deste projeto, tentando mostrar de uma maneira lúdica as áreas do cotidiano em que encontramos matemática, em especial os números primos. Como esperado a reação foi a mesma em ambas as turmas. Inicialmente ficaram espantados e admirados pela forma com que passavam a encontrar a Matemática no dia a dia deles ou até mesmo na mídia que em geral não é tão divulgada. Eles começaram a perceber que nos mesmos meios de comunicação que aparecem noticiários, esporte, política, etc, também comparece a Matemática da sala de aula que até então só conheciam lá.

Finalizando a oficina, obtive uma motivação importante ao ouvir as palavras da diretora da escola e do Professor Filipe Bermudes de satisfação e o quanto fora importante a aplicação da oficina e como seria importante que projetos como este fossem sempre aplicados nas escolas durante o ano letivo, em relação ao valor dessa oficina para resgatar conhecimentos passados, trabalhar nos alunos o desenvolvimento de estratégias para a resolução de problemas, cálculo mental, dando uma excelente oportunidade para os alunos crescerem e aprimorarem seus conhecimentos matemáticos, oportunizando a quebra das barreiras criadas ao se estudar matemática no ensino básico.

16. Considerações Finais

Faz-se necessário ressaltar que nos dias atuais, pelas experiências vivenciadas e pelos depoimentos dos colegas de trabalhos em todas as oportunidades (Escolas), uma tarefa muito grande para nós professores é apresentar a Matemática de uma maneira mais dinâmica de forma que os alunos passem a tomar gosto de estudar, se concentrem na busca pelas melhores estratégias de solução e consigam evoluir. Em outras palavras, fazer com que os alunos pensem. Em linhas gerais, oportunizar isso, ou motivar essa iniciativa é muito prazeroso, é a idealização e realização dos sonhos didáticos e pedagógicos que muitos professores têm, porém, pela realidade das estruturas de trabalho e do sistema, ficam impedidos de realizá-los.

Como minha motivação principal foi uma afirmação "madura" de um aluno com dez anos de idade, trabalhar este projeto é vencer os desafios das novas tecnologias que tanto chamam a atenção dos alunos. É muito mais prazeroso para alguns, "perder" tempo com celulares tecnológicos, jogos de computadores e aparelhos sofisticados do que dispensar horas em um problema matemático que para alguns deles não vão levar a lugar algum (Perguntas constantes nas salas de aula: Para que serve isso? Onde vou usar isso na minha vida? Entre outras). Mas a esperança ainda sobrevive, pois temos alunos que sentem prazer em aproveitar horas do seu dia em pesquisar e resolver problemas matemáticos, conhecer e se aprofundar em teorias que podem não fazer sentido hoje, pela idade que eles têm, mas que fará sentido um dia, quando mais maduros, tomarem a decisão sobre que caminho seguir. Pensar na resolução de problemas vai muito além de somente aprender cálculos matemáticos, é parte da preparação para a vida, assim como foi exposto nas curiosidades desse projeto, observamos que em todas as áreas da nossa vida encontramos fatos e situações curiosas que, se não é possível observar explicitamente a teoria matemática, é pelo menos curioso pelo fato de envolver muitas outras áreas do nosso cotidiano.

A "primalidade" desse trabalho se compara a importância dos números primos na composição dos outros números e de todas as técnicas que construímos a partir deles. Mesmo com algumas decepções, encontramos em alguns exemplos, ainda que poucos, a motivação de continuar a ensinar e ter a maior vitória que é o prazer de ver que ainda temos alunos interessados em aprender Matemática.

17. Anexos

Anexo 1

PROFMAT

SBM
Sociedade Brasileira de Matemática

Mestrado Profissional
em Matemática em Rede Nacional

Dissertação (Mestrado) – Universidade Federal do Espirito Santo

Mestrando: Prof. Carlos Costa dos Reis

Orientador: Prof. Dr. Valmecir Bayer

TEMA - Oficina de Aritmética: o uso dos números primos na resolução de problemas e algumas curiosidades.

Aluno(a):_

1 - Usando a decomposição em fatores primos dos números 507 e 1287 separadamente, calcular o mdc(507,1287) e o mmc(507,1287).

507	3
169	13
13	13
1	$3\cdot13^2$

1287	3
429	3
143	11
13	13
1	$3^2\cdot11\cdot13$

$mmc = 3^2\cdot13^2\cdot11 \rightarrow$ (R: 16621)

$mdc = 3\cdot13 \rightarrow$ (39)

R. ______________________________________

2 - Ao longo de um dia, um supermercado fez vários anúncios dos produtos A, B e C, todos eles com o mesmo tempo de duração. Os tempos totais de aparição dos produtos A, B e C foram, respectivamente, iguais a 90s, 108s e 144s. Se os três produtos apareceram em tempos iguais e a duração de cada anúncio, em segundos, foi a maior possível, então, a soma do número de aparições dos três produtos, nesse dia, foi igual a?

A - 90
B - 108
C - 144

90, 108, 144	2
45, 54, 72	2
45, 27, 36	2
45, 27, 18	2
45, 9, 9	3
5, 3, 3	3
5, 1, 1	5
1, 1, 1	$2^4\cdot3^2\cdot5$

$mdc = 2\cdot3^2 = 2\cdot9 = \boxed{18}$

$90 \div 18 = 5$
$108 \div 18 = 6$
$144 \div 18 = 8$

(19 vezes)

R. ______________________________________

as propagandas aparacerão 19 vezes durante o dia

Anexo 2

3 - Uma indústria de tecidos fabrica retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas: 156 centímetros e 234 centímetros. O gerente de produção ao ser informado das medidas deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?

156	2
78	2
39	3
13	13
1	$2^2 \cdot 3 \cdot 13$

234	2
117	3
39	3
13	13
1	$2 \cdot 3^2 \cdot 13$

mdc = $2 \cdot 3 \cdot 13 = 78$ cm

$156 \div 78 = 2$ partes

$234 \div 72 = 3$ partes

R. O dono poderá corta os dos ~~dois~~ panos em 5 partes de 78 cm.

4 - Numa aventura pelo deserto, o sábio e grande matemático Malba Tahan foi consultado sobre o seguinte enigma: "Quantos números de dois algarismos não são primos nem múltiplos de 2, 3, ou 5?" Ajudando ao grande sábio, qual é a resposta do enigma?

R. ____________________

5 - Tenho 693 amigos em minha rede social, e nela publiquei a frase de Pitágoras: "A Matemática e o alfabeto com o qual DEUS escreveu o universo". O numero de amigos que curtiram minha frase tem dois dígitos iguais e é divisor de 693. A soma desses dois dígitos dá um numero de dois dígitos que somados resultam um numero primo. Quantos curtiram minha frase?

$77 = 7 + 7 = 14 \rightarrow 1 + 4 = 5$

693	3
231	3
77	7
11	11
1	$3^2 \cdot 7 \cdot 11$

R. 77 pessoas curtiram a frase.

Anexo 3

PROFMAT

SBM
Sociedade Brasileira de Matemática

Mestrado Profissional
em Matemática em Rede Nacional

Dissertação (Mestrado) – Universidade Federal do Espirito Santo

Mestrando: Prof. Carlos Costa dos Reis

Orientador: Prof. Dr. Valmecir Bayer

TEMA - Oficina de Aritmética: o uso dos números primos na resolução de problemas e algumas curiosidades.

Aluno(a):

1 – Três vendedores encontraram-se num certo dia na cidade de Medianeira - PR e jantaram juntos. O primeiro vendedor visita esta cidade a cada seis dias, o segundo a cada oito dias e o terceiro a cada cinco dias. Estes três vendedores marcaram de jantar juntos novamente no próximo encontro, quantos dias depois esse jantar ocorrerá?

6, 8, 5 | 2
3, 4, 5 | 2
3, 2, 5 | 2
3, 1, 5 | 3
1, 1, 5 | 5
1, 1, 1 | $2^3 . 3 . 5 = 15 . 2^3 = 8 . 15 = \boxed{120 \text{ dias}}$

15 × 8 = 120

R. ______________________________

2 - Se o mínimo múltiplo comum entre os números 6 e k é maior do que 31 e menor do que 41, então qual deve ser o valor do número k?

36 = mmc 6, k = 41 > x > 31

36, 6 | 2
18, 3 | 2
9, 3 | 3
3, 1 | 3
1, 1 | $2^2 . 3^2$

$2^2 . 3^2 = 4 . 9 = 36$

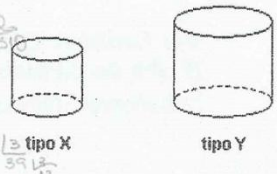
6 | 2
3 | 3
1 | 2.3 = 6×5 = 30
6×6 = 36
6×7 = 42

R. ______________________________

3 - Uma empresa de construção dispõe de 117 blocos de tipo X e 145 blocos de tipo Y. Esses blocos têm as seguintes características: todos são cilindros retos, o bloco X tem 120 cm de altura e o bloco Y tem 150 cm de altura. A empresa foi contratada para edificar colunas, sob as seguintes condições: cada coluna deve ser construída sobrepondo blocos de um mesmo tipo e todas elas devem ter a mesma altura. Com o material disponível, qual será o número máximo de colunas que podem ser construídas?

21750 | 2
1875 | 5
375 | 5
75 | 5
15 | 3
5 | 5
1 | $2 . 3 . 5^4$

14.040 | 2
7020 | 2
3510 | 2
1755 | 5
351 | 3
117 | 3
39 | 3
13 | 13
1 | $2^3 . 5 . 3^3 . 13$



R. ______________________________

mdc ⇒ 2 . 3 . 5 = $\boxed{30 \text{ colunas}}$

Anexo 4

2

3 - Uma indústria de tecidos fabrica retalhos de mesmo comprimento. Após realizarem os cortes necessários, verificou-se que duas peças restantes tinham as seguintes medidas: 156 centímetros e 234 centímetros. O gerente de produção ao ser informado das medidas deu a ordem para que o funcionário cortasse o pano em partes iguais e de maior comprimento possível. Como ele poderá resolver essa situação?

156	2
78	2
39	3
13	13
1	$2^2 . 3 . 13$

↳ 2 partes

234	2
117	3
39	3
13	13
1	$2 . 3^2 . 13$

↳ 3 partes

mdc = $2 . 3 . 13 = 6 . 13 =$ (

R. O dono poderá cortar os dois panos em partes de 78 cm, o primeiro em 2 partes e o segundo em 3 p

4 - Numa aventura pelo deserto, o sábio e grande matemático Malba Tahan foi consultado sobre o seguinte enigma: "Quantos números de dois algarismos não são primos nem múltiplos de 2, 3, ou 5?" Ajudando ao grande sábio, qual é a resposta do enigma?

R.

5 - Tenho 693 amigos em minha rede social, e nela publiquei a frase de Pitágoras: "A Matemática e o alfabeto com o qual DEUS escreveu o universo". O numero de amigos que curtiram minha frase tem dois digitos iguais e é divisor de 693. A soma desses dois digitos dá um numero de dois digitos que somados resultam um numero primo. Quantos curtiram minha frase?

693	3
231	3
77	7
11	11
1	$3^2 . 7 . 11$

$77 = 7 + 7 = 14 = 1 + 4 = 5$

R. 77 pessoas curtiram a frase.

18. Bibliografia

[01] HEFEZ, Abramo. Curso de Álgebra, volume 1, 3ª edição. Associação Instituto Nacional de Matemática Pura e Aplicada, Rio de Janeiro, 2002.

[02] BRASIL/MEC. Parâmetros Curriculares Nacionais do Ensino Médio: orientações educacionais complementares aos Parâmetros Curriculares Nacionais – Ciências da Natureza, Matemática e suas Tecnologias. Brasília: MEC/SEMTEC, 2002.

[03] DANTE, Luiz Roberto. (2008) Tudo é Matemática. 3a ed. 4 vols. São Paulo: Ática.

[04] IEZZI, Gelson; DOLCE, Osvaldo; MACHADO, Antônio dos Santos. Matemática e Realidade. 8ª edição, editora Atual.

[05] DU SAUTOY, Marcus; Os mistérios dos números, uma viagem pelos grandes enigmas da matemática – Rio Zahar, 2013.

[06] OLIVEIRA, Sara; VENTURA, Helena; PAIS, Alexandre. Página dos Números Primos – Projeto da cadeira do ICM do DEFCUL.

[07] <http://www.educ.fc.ul.pt/icm/icm98/icm12/Historia.htm> Acesso em: 07 de setembro de 2013.

[08] <http://www1.folha.uol.com.br/folha/ciencia/ult306u11973.shtml> Acesso em: 07 de setembro de 2013.

[09] <http://ellalves.net.br/textos/conteudo/19/teoria_dos_numeros_exercicios_de_numeros_primos> Acesso em: 07 de setembro de 2013.

[10] <http://noticias.uol.com.br/ciencia/ultimasnoticias/redacao/2013/05/24/matematico-peruano-resolve-problema-de-3-seculos-sobre-numeros-primos.htm> Acesso em: 07 de setembro de 2013.

[11] <http://www.educ.fc.ul.pt/icm/icm98/icm12/Historia.htm> Acesso em: 07 de setembro de 2013.

[12] <http://www.darlen.eti.br/publicacoes/introrsa.html> Acesso em: 13 de Março de 2014.

[13] <http://poti.impa.br/index.php/material> Acesso em: 13 de Março de 2014.