ISSN 2359-4799
Volume 6 / Número 4 / Ano 2020 – p. 242-256
DOI: 10.36524/ric.v6i4.854

REVISTA ifes ciência

NÚMEROS PRIMOS: RELAÇÃO HISTÓRICA E ALGUMAS CURIOSIDADES

PRIME NUMBERS: RELATIONSHIP HISTORY AND SOME CURIOSITIES

[1]Carlos Costa dos Reis.
[2]Valmecir Bayer.

[1]Universidade Federal do Espirito Santo. E-mail: carlos.ufes81@gmail.com.
[2]Universidade Federal do Espirito Santo. E-mail: bayervalmecir@gmail.com.

Artigo submetido em 28/09/2020, aceito em 08/10/2020 e publicado em 28/12/2010.

Resumo: Este trabalho traz um texto com um olhar sobre a história dos números primos e várias curiosidades em que se observa o seu uso no cotidiano e na natureza. Pode auxiliar no suporte para professores e alunos dos ensinos fundamental e médio ou mesmo no aprimoramento para turmas que se preparam para as olimpíadas de matemática. A sequência dos temas faz uma explanação histórica sobre os números primos, um resumo da teoria básica e, por fim, fragmentos e artigos sobre curiosidades no mundo inteiro a respeito dos números primos.

Palavras-chave: números primos; história; curiosidades.

Abstract: This work brings a text with a look at the history of prime numbers and several curiosities in which its use in everyday life and in nature is observed. It can assist in the support for teachers and students of elementary and high school or even in the improvement for classes that are preparing for the math Olympics. The sequence of themes provides a historical explanation of prime numbers, a summary of basic theory and, finally, fragments and articles on curiosities around the world about prime numbers.

Keywords: prime numbers; history; curiosities.

1 INTRODUÇÃO

Este trabalho expõe 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 vários trabalhos e artigos sobre números primos, porém pouco divulgados. Nos livros didáticos aparecem apenas a teoria e muitos exercícios, quase sempre mecânicos, que não exigem muito do aluno. Quando falamos em exigência, queremos dizer: pensar e sentir-se atraído pelo assunto a ponto de buscar aprofundar mais, levando-o a fazer uso no seu cotidiano.

Trabalhando o conteúdo em sala de aula e ampliando o conhecimento sobre múltiplos e divisores, um aluno do sexto ano do ensino fundamental (antiga 5ª série)

trouxe a seguinte afirmação: "*Todo número quadrado perfeito de primo possui apenas três divisores naturais*". A maturidade da afirmação desse aluno é o fator motivador para buscar formas de levar outros alunos a entrarem no mundo da Matemática com mesmo prazer que este tem demonstrado durante o processo de aprendizagem.

Seguindo essas diretrizes, o Ministério da Educação, por meio dos Parâmetros Curriculares Nacionais de Matemática, destaca a importância desse momento com o aluno e incentiva a continuidade deste trabalho 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], PCN,1997, 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 descontextualizados, 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], PCN,1997, 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 didáticos, 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 ao desenvolvimento teórico, fazendo o aluno enxergar a Matemática por completo, não como livros de teorias maçantes que calejam a relação professor × aluno, fator esse 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], PCN,1997, 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], PCN,1997 p. 30 - 31).

Por fim, esperamos com este trabalho didático 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.

2 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 matemáticos gregos antigos. Os matemáticos da escola de Pitágoras (500 a 300 a.C.) estavam interessados nos números pelas suas propriedades numerológicas e místicas. Por definição, número primo "p" é aquele que é diferente de 1 e possui dois, e somente dois divisores naturais: o 1 e o próprio p. Os demais números diferentes de 1 são chamados compostos. Entendiam a ideia de primalidade, e revelavam interesse em números perfeitos e amigáveis (um número natural n 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 $1 + 2 + 4 + 7 + 14 = 28$).

Conhecendo os divisores de pares de números encontramos a definição para os *Números amigáveis*: são pares de números onde um deles é a soma dos divisores do outro. Por exemplo, os divisores de 220 são $1, 2, 4, 5, 10, 11, 20, 22, 44, 55$ e 110, cuja soma é 284. Por outro lado, os divisores de 284 são $1, 2, 4, 71$ e 142 e a soma deles é 220. Fermat descobriu também o par 17.296 e 18.416.

Quando *Os Elementos* de Euclides apareceram (cerca de 300 a.C.), muitos 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.

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* –. 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 um largo período de tempo de interregno, na *História dos Números Primos*, a chamada *Idade Negra*. O desenvolvimento seguinte na História dos números primos nos é fornecido por *Pierre de Fermat*, no início do século XVII, provando uma especulação conjecturada por *Albert Girard*, onde estabelece que todo número primo da forma $4n + 1$ pode ser escrito de um só modo, como soma de dois quadrados de números inteiros, além disso criou/provou as seguintes metodologias: qualquer número inteiro positivo pode ser escrito como soma de quatro quadrados, um novo método para fatorar números primos grandes e o *Pequeno Teorema de Fermat* (para distinguir do denominado *Grande Teorema de Fermat*): se p for um número primo, então para qualquer número inteiro a:

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

Tal teorema prova, em parte, a chamada *Hipótese Chinesa*, de cerca de 2000 anos antes, que um inteiro n é primo, se e somente se o número $2^n - 2$ é divisível por n. A recíproca deste teorema é falsa; vê-se facilmente, por 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, no tocante a determinação de números primos, ainda hoje utilizados em larga escala em computação. Fermat manteve correspondência com outros matemáticos do seu tempo, em particular com o monge *Marin Mersenne*. Numa das suas cartas a Mersenne, ele conjecturou que os números da forma:

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

seriam primos. Estes números também são denominados *números de Fermat*. Somente

cerca de 100 anos depois, 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 atenção, devido ao fato que, caso n não seja primo, estes números são compostos, classicamente, chamados de *números de Mersenne* M^n, referenciando o estudo dedicado por este matemático. 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} (número de 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, sendo o maior deles o número $M^{3021377}$, com 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, pois 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*, provada posteriormente por *Johann Carl Friedrich Gauss*.

Ademais, 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*. Mostrou, não apenas que 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.

Na teoria, a soma dos n primeiros 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, 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 específica 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.

Considerando o estudo sobre a densidade dos números primos, *Legendre (Adrien-Marie Legendre)* e *Gauss* fizeram extensos cálculos. Gauss (um prodígio do cálculo) disse a um amigo que, quando tinha 15 minutos de folga, ocupava-se contando os números primos num alcance de 1000 números. Estima-se que, até o fim da sua vida, Gauss tenha contado todos os números primos até três milhões.

No desbravamento dos números primos, Legendre e Gauss chegaram à conclusão que, para n suficientemente grande, a densidade de números primos até de n é aproximadamente $\frac{1}{\log n}$. Legendre deu uma estimativa para a 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,

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

e previu que a densidade de números primos era igual a $\frac{1}{\log n}$. Hoje, isto é conhecido 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 Riemann* que foram capazes de relacionar o problema com algo próximo à chamada *Hipótese de Riemann* que é uma conjectura sobre os zeros no plano complexo de uma função chamada *função ζ (zeta) de Riemann*.

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 Riemann.

Ainda há muitas questões por desvendar (algumas delas que datam de centenas de anos atrás) relacionadas com números primos. (Fonte: [08])

3 TEORIA DOS NÚMEROS

O conjunto dos números naturais é representado pela letra maiúscula $\mathbb{N}$ e estes números são representados, utilizando os algarismos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, também conhecidos como algarismos indo-arábicos. Conhecendo um pouco a história sobre eles, sabe-se que no século VII, os árabes invadiram a Índia, difundindo o seu sistema numérico.

Embora o zero não seja um número natural, no sentido que tenha sido proveniente de contagens naturais de objetos, iremos considerá-lo como um número natural, pois é conveniente do ponto de vista algébrico. 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 os naturais iniciados com o número zero e escreveremos este conjunto como:

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

As reticências (três pontos) indicam a infinitude do conjunto $\mathbb{N}$. Excluindo o zero do conjunto dos números naturais, o conjunto resultante será representado por:

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

A Aritmética é a área da Matemática que estuda os conjuntos numéricos e as suas operações básicas, desenvolvendo propriedades fundamentais para a construção dos números e o seu uso. No conjunto dos números naturais observamos a presença de dois tipos de números: primos e compostos.

Os números primos tem grande importância nessa teoria. Por definição, número primo “p” é aquele que é diferente de 1 e possui dois, e somente dois divisores naturais: o 1 e o próprio p. Os demais números diferentes de 1 são chamados compostos. O Teorema Fundamental da Aritmética (ou Teorema da Fatoração Única) nos diz que todo número composto pode ser decomposto, de modo único, a menos da ordem dos fatores, como um produto de números primos.

Utilizando o Teorema Fundamental da Aritmética, podemos calcular o Máximo Divisor Comum (MDC) e o Mínimo Múltiplo Comum (MMC) de um conjunto finito de números naturais. Essas aplicações e algumas curiosidades são os temas fundamentais deste trabalho.

Faz-se necessário ressaltar que o número 1 (um) não é primo nem composto e o número 2 (dois) é o único número natural par e primo. O estudo da fatoração em números primos é muito importante para diversas áreas da Matemática, como por exemplo, para a potenciação e a radiciação.

3.1 O QUE SIGNIFICA FATORAR?

Quando aprendemos multiplicar (nas primeiras séries do Ensino Fundamental), também aprendemos o conceito de fator. Fatorar um número significa encontrar uma multiplicação de números que resulte o número dado.

Exemplos:
Uma possível fatoração para o número *4* pode ser 2×2. Assim, $4 = 2 \times 2$. Da mesma forma,

$$9 = 3 \times 3$$
$$32 = 16 \times 2$$
$$90 = 15 \times 3 \times 2$$

Todos estes são exemplos de fatoração, mas daremos especial atenção à fatoração em números primos. Fatorar um número em fatores primos é encontrar uma multiplicação de primos que resulte o número dado. Nos dois últimos exemplos acima, as fatorações não são em primos, uma vez que *16* e *15* são números compostos. Então, aquelas decomposições são apenas fatorações.

Há um algoritmo prático, que aprendemos nas primeiras séries do Ensino Fundamental II, para fatorar um determinado número em fatores primos. Primeiramente, escrevemos o número a fatorar com uma barra vertical ao lado direito, em seguida efetuamos divisões sucessivas desse número por números primos dispostos do lado esquerdo da barra, como no exemplo a seguir:

18	2
9	3
3	3
1	

3.2 CRITÉRIOS DE DIVISIBILIDADE

Para facilitar a fatoração é conveniente utilizar os critérios básicos de divisibilidade por $2, 3, 4, 5, 6, 7, 8$ *e* 9. Esses critérios estão listados a seguir e algumas ideias de demonstrações e justificativas estão indicadas nas referências deste trabalho.

- Por *2*: Um número é divisível por *2* se ele for par;

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

- Por 4: Um número é divisível por 4 se os dois últimos algarismos formarem um número divisível por 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 7: Devemos multiplicar por 2 o último algarismo do número. Subtrair este valor do número inicial sem o último algarismo, se o resultado for divisível por 7, então o número inicial também será.

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

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

3.3 CÁLCULO DO MDC E MMC

Duas das aplicações importantes do Teorema da Fatoração Única são os cálculos do MDC (Máximo Divisor Comum) e do MMC (Mínimo Múltiplo Comum). É interessante observar que, utilizando as mesmas fatorações dos números podemos obter, simultaneamente, o MDC e o MMC. Vejamos um exemplo no qual foi feita a fatoração simultânea dos números 12 e 42.

12 ,42	**2 (Divisor Comum)**
6 ,21	2
3 ,21	**3 (Divisor Comum)**
1 , 7	7
1 , 1	

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 MDC. 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 fatoração simultânea, o valor 6 é obtido realizando a multiplicação dos divisores comuns, ou seja, $MDC\,(12,42) = 2 \times 3 = 6$. Assim, podemos encontrar o MDC de dois ou mais números naturais fazendo o produto dos fatores comuns na decomposição simultânea desses números.

Por outro lado, o MMC será obtido ao multiplicar todos os divisores da fatoração simultânea. Sendo assim,

$$MMC(12,42) = 2 \times 2 \times 3 \times 7 = 2^2 \times 3 \times 7 = 84$$

.

Evidenciamos na Matemática um espaço para uma disciplina especial chamada “Resolução de Problemas”. Essa teoria básica sobre Números Primos nos permite desenvolver uma quantidade enorme de problemas práticos e usuais em nosso cotidiano. Neste sentido, destacamos agora algumas curiosidades que extrapolam o uso e a importância dos Números Primos em nosso cotidiano e na natureza. (Fonte: [04], [07], [09], [10])

4 CURIOSIDADES

Destacamos algumas curiosidades em que os números primos são protagonistas. A mídia, os canais de informação e os livros didáticos não fornecem o devido destaque e importância observados nessas histórias reais do nosso cotidiano. Assim, com o uso desse material, podemos, de forma lúdica, conhecer um pouco mais da aplicabilidade desses números no dia a dia e na natureza.

4.1 PRIMOS GALÁTICOS

Elemento fundamental na composição e desenvolvimento dos esportes, os números são usados para identificar os competidores/jogadores, enumerar ou mesmo nomear táticas e regras, além de quantificar o resultado final para vencedores e perdedores. Nesse sentido, os números trazem curiosidades impressionantes num dos meios mais competitivos e lucrativos do esporte: o Futebol.

Destaca DU SAUTOY em “Os mistérios dos números, uma viagem pelos grandes enigmas da matemática” uma curiosa história sobre o time galáctico do Real Madrid (Espanha) na temporada 2003/2004. Contratado junto ao Manchester United (Inglaterra), muito se especulou qual seria o número utilizado por David Beckham para compor a constelação das estrelas madrilenhas. Tanto no time inglês quanto em sua seleção vinha jogando com a camisa 7.

Porém, Raul era o dono dessa camisa no Real Madrid e não parecia estar disposto a ceder o número para o "menininho glamoroso" da Inglaterra.

O número escolhido foi o "primo" 23. Muitas teorias foram levantadas sobre o motivo para tal escolha e a mais natural tem ligação com o mercado internacional. O Real Madrid queria expandir sua marca no mercado americano e, segundo essa teoria, associou o futebol (soccer para os americanos) a um dos esportes mais praticados e lucrativos nos EUA, o basquetebol. Uma pesquisa identificou que Michael Jordan era o nome mais famoso na época e usou em toda sua carreira o número 23 no Chicago Bulls. Era esperado que associar a camisa do David Beckham à estrela americana tornaria efetiva e lucrativa essa magia dos números.

Essa mística sobre os números primos e o Real Madrid não para na camisa do Beckham. Como destaca DU SAUTOY em seu livro: "...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". Como destacado anteriormente, o número 1 não é primo, assim, evidenciamos o fato de o goleiro do Real Madrid, mesmo fazendo parte da constelação de jogadores madrilenhos, usar a camisa 1.

Místico ou não, a associação entre futebol e os números primos é uma forma muito curiosa e estimulante de observar os números e toda a matemática como parte essencial do nosso cotidiano. (Fonte: [05] DU SAUTOY, 2013, p.10-13)

4.2 CIGARRAS USAM NÚMERO PRIMO PARA SOBREVIVER

Uma das seis espécies existentes de cigarras Magicicada

No ano de 2014, após passarem *17* anos no subsolo, alimentando-se de raízes, bilhões de cigarras emergiram do chão nos Estados Unidos prontas para acasalar. No céu americano, nuvens de até *1,5* milhões de indivíduos por acre se formaram e, mesmo que inofensiva, a *Magicicada sp* 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. Essa prática fez parte do ritual de acasalamento que durou cerca de seis semanas. Após depositar os seus ovos (até seiscentos por indivíduo), a fêmea adulta morre. Os filhotes voltaram a repetir o processo de se enterrarem no solo, onde ficarão até 2031.

Ao todo, existem seis espécies do gênero Magicicada, três delas com ciclos de *17* anos. 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 são deixadas para trás e os americanos podem se preparar para usar suas pás para limpar mais do que apenas folhas de jardim. (Fonte: [05] DU SAUTOY, 2013; [06])

4.3 CONJECTURA DE GOLDBACH

Harald Andrés Helfgott

O peruano Harald Andrés Helfgott (foto) resolveu um problema com números primos que estava sem solução há quase 300 anos. A chamada "conjectura fraca" enviada em carta por Christian Goldbach para Leonhard Euler, 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. Helfgott desvendou a teoria fraca derivada da "versão forte", no qual todo número par maior que 2 é a soma de dois primos.. Helfgott não aborda a conjectura forte no estudo. (Fonte: [01])

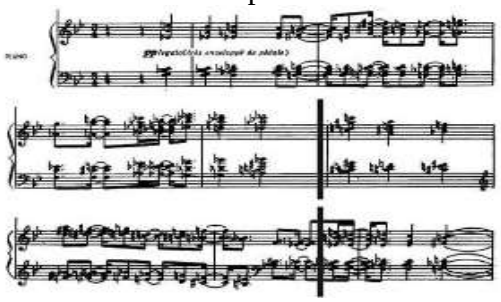
4.4 COMO OS PRIMOS *17* E *29* SÃO A CHAVE PARA O FIM DOS TEMPOS?

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. Messiaen decidiu formar um quarteto com os três músicos e 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 $\frac{2}{3}$. O efeito da escolha dos números primos *17* e *29* é que as sequências rítmicas e de acordes não se repetiam até a nota 17×29 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 número 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.

Figura 1: ‘Liturgia de cristal’, de Messiaen, do Quarteto para o fim dos tempos.



Fonte: Messiaen (1994).

O primeiro traço vertical indica onde termina a primeira sequência rítmica de *17* notas, O segundo traço vertical indica o timbre da sequência harmônica de *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 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. (Fragmento: [05] DU SAUTOY,2013,p.17-19)

4.5 CRIPTOGRAfiA

Existem muitos estudos e curiosidades sobre criptografia evidenciando a importância que esse tema possui nos dias atuais. Dentre esses, destacamos o que Coutinho (COUTINHO 2016) desenvolveu em material teórico para a OBMEP (Olimpíada Brasileira de Matemática para Escolas Públicas).

A priori, temos a expressão cryptos, que vem do grego e significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que só seu destinatário legítimo consiga interpretá-la. É a arte dos "códigos secretos". Um dos códigos secretos mais simples consiste em substituir uma letra do alfabeto pela seguinte. Por exemplo, a mensagem AMO A OBMEP seria codificada como

BNPBPCNFQ.

Um código semelhante a este foi usado, por exemplo, pelo ditador romano Júlio César para comunicar-se com as legiões romanas em combate pela Europa. Este parece ser o primeiro exemplo de um código secreto de que se tem notícia.

Vejamos como codificar uma mensagem simples. Códigos como o de César padecem de um grande problema: são muito fáceis de "quebrar". Quebrar um código significa ser capaz de ler a mensagem, mesmo não sendo seu destinatário legítimo. Na verdade, qualquer código que envolva substituir cada letra sistematicamente por outro símbolo qualquer sofre do mesmo problema. Isto ocorre porque a frequência média com que cada letra aparece em um texto de uma dada língua é mais ou menos constante. Por exemplo, a frequência média de cada letra na língua portuguesa é dada na tabela 1, a seguir.

Tabela 1: Frequência das letras no Português

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

Fonte: Elaborada pelos autores.

Assim, apenas contando a frequência de cada símbolo no texto, podemos descobrir a que letra correspondem os símbolos mais frequentes. Isto geralmente é suficiente para quebrar o código e ler toda a mensagem. Observe, entretanto, que este método para quebrar o código só funciona bem se a mensagem for longa. É fácil escrever uma mensagem curta cuja contagem de frequência seja totalmente diferente da contagem de frequência média do português. Por exemplo, em "Zuza zoou da Zezé" a letra mais frequente é o Z que aparece 5 vezes em um texto de 14 letras. Como 5/14 = 0, 35... a porcentagem do Z no texto acima é de cerca de 35%; muito acima dos usuais 0, 47%. Já o A aparece uma só vez, o que dá uma porcentagem de

cerca de 7%; portanto, abaixo dos 14% usuais.

4.5.1 CÓDIGOS EM BLOCO

Por sorte, existe uma maneira simples de tornar inviável a aplicação de uma contagem de frequência. Para isso, subdividimos a mensagem em blocos de várias letras e embaralhamos estes blocos. Por isso este processo de criptografar uma mensagem é conhecido como código de bloco. Por exemplo, considere a mensagem

$$AMO\ A\ OBMEP$$

Para codificá-la seguiremos os seguintes passos:

• eliminamos os espaços e completamos a mensagem com um A no final, caso tenha uma quantidade ímpar de letras;

• subdividimos a mensagem em blocos de duas letras;

• refletimos cada bloco;

• permutamos os blocos trocando o primeiro com o último, o terceiro com a antepenúltimo, e assim por diante, mas deixando os outros como estão.

Aplicando isto, passo a passo, à mensagem acima, obtemos primeiro

$$AMOAOBMEPA$$

Depois

$$AM - OA - OB - ME - PA$$

em seguida

$$MA - AO - BO - EM - AP$$

e, finalmente,

$$AP - AO - BO - EM - MA$$

que nos dá como mensagem codificada

$$APAOBOEMMA.$$

Apesar de códigos como este serem melhores que o código de César, eles apresentam uma grande desvantagem quando se trata de aplicações comerciais da criptografia. Por exemplo, digamos que faremos uma compra via web usando nosso computador, em uma loja em que nunca compramos antes. Para isso acessamos a página da loja, escolhemos os produtos que desejamos e, quando estamos prontos para comprar, escolhemos “ir para o caixa”. O pagamento será feito usando o cartão de crédito. Para isso, precisamos informar a loja sobre os dados do cartão: geralmente o número e a data de vencimento. Mas isto significa que qualquer outra pessoa que tenha estes dados pode fazer compras em nosso nome. Para evitar este problema, as informações sobre o cartão são codificadas pelo computador antes de serem enviadas.

Note, contudo, que o nosso computador não pode usar um código qualquer para codificar estas informações, porque a loja precisa lê-las e, para isso, tem que saber como decodificar a mensagem. Na prática o que ocorre é que o nosso computador comunica-se com o da loja, que lhe informa como deve ser feito o processo de codificação. Isto é, nosso computador codifica as informações do cartão de crédito usando um processo de codificação que é enviado pela loja. Infelizmente os códigos de blocos não se prestam a este tipo de aplicação porque o computador da loja usa a linha telefônica (ou de banda larga) à qual nosso computador está interligado para enviar o processo de codificação a ser utilizado. Como é fácil pôr uma escuta na linha, uma outra pessoa pode facilmente descobrir como nosso computador vai codificar as informações sigilosas que serão enviadas à loja. Usando a mesma escuta é fácil interceptar também as mensagens que contêm os dados do cartão. Mas isto basta porque, se sabemos como foi feito o embaralhamento dos blocos, podemos facilmente desfazê-lo e ler os dados do cartão! A única maneira de contornar este

problema é ter acesso ao que é conhecido como um canal seguro: uma maneira secreta de fazer a informação sobre o processo de codificação chegar até o computador do usuário da loja. Talvez a loja pudesse mandar, pelo correio registrado, um cartão especial com os dados a serem usados para a codificação. O problema é que isto tornaria a transação lenta, já que seria necessário esperar dias pela chegada do cartão – nesse meio tempo nós talvez preferíssemos escolher uma loja real, mesmo que fosse longe de casa. E ainda há outro problema, mais sério. Se o nosso computador for invadido por um "hacker", o processo de codificação será descoberto e qualquer mensagem enviada com ele poderá ser lida.

4.5.2 CÓDIGOS DE CHAVE PÚBLICA

As dificuldades que relacionamos acima parecem condenar de maneira irremediável a possibilidade de fazer transações pela web. Afinal, seja qual for o código utilizado, se sabemos como fazer a codificação, basta desfazê-la e decodificamos a mensagem. Ou não?

De fato, isto é basicamente verdade; mas há um porém. Acontece que podemos imaginar um processo que seja fácil de fazer, mas muito difícil de desfazer e, ao utilizá-lo para criptografar uma mensagem, estaríamos garantindo que quem a interceptasse, mesmo sabendo como foi codificada, teria um trabalho enorme em decodificá-la. Abusando um pouco da fantasia, podemos imaginar que o trabalho de desfazer o processo levasse tanto tempo que ninguém conseguisse pô-lo em prática. É claro que quão difícil será desfazer o procedimento depende dos recursos disponíveis a quem interceptou a mensagem.

A lagosta fica presa na gaiola porque, para poder sair, teria que encontrar e passar pela parte estreita do funil, que é um problema complicado demais para uma lagosta, cujo cérebro tem o tamanho aproximado de uma ervilha. Não preciso dizer que uma armadilha desse tipo não funcionaria para pegar um macaco, nem mesmo um passarinho. Muito interessante, mas que problema matemático satisfaz esta condição de ser "fácil de fazer e difícil de desfazer", para que possamos utilizá-lo em criptografia?

4.5.3 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.

Para entender como funciona o método RSA precisaremos estudar várias ideias e técnicas novas de matemática. 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 esquecemos 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 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.

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. (Fonte: [03])

5 CONCLUSÕES

Buscamos nesse trabalho evidenciar a importância do uso dos números primos em várias áreas do nosso cotidiano. Analisando o contexto histórico, observamos brilhantes estudiosos dedicando-se na busca por desvendar as curiosidades e formalidade dos números primos.

No tocante à sala de aula, agrupamos um material que proporciona, segundo a criatividade de cada profissional da educação, transformar o ambiente de aprendizagem mais lúdico e atrativo para o ensino da matemática. Uma vez que a motivação principal deste trabalho foi a afirmação “madura” de um aluno de dez anos de idade, trabalhar este conceito é vencer os desafios das novas tecnologias, transpor as barreiras da natureza e levar para aqueles estudantes mais desejosos a oportunidade de amadurecerem cognitivamente e explorar as mais variadas áreas da vida pela visão dos números.

Enxergar o uso dos números primos fora dos livros didáticos, aplicando-os em áreas como esportes, música, criptografia e, até mesmo, na natureza, nos permite entender o porquê tantos matemáticos se dedicaram e entregam ainda hoje parte da vida em estudos e pesquisas sobre esses números tão curiosos.

6 REFERÊNCIAS

BBC NEWS, Brasil. Disponível em: <https://www.bbc.com/portuguese/noticias/2015/10/151004_matematico_peruano_helfgott_mv. Acesso em: 27 de setembro de 2020.

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.

COUTINHO, Severino. **Criptografia**, Rio de Janeiro, IMPA, 2016. 217 páginas. Disponível em: https://portaldaobmep.impa.br/uploads/material_teorico/83bhrw1mjmgwo.pdf. Acesso em: 25 de Outubro de 2020.

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

Folha Uol, São Paulo. http://www1.folha.uol.com.br/folha/ciencia/ult306u11973.shtml. Acesso em: 07 de setembro de 2013.

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

OLIVEIRA, Sara; VENTURA, Helena; PAIS, Alexandre. P**ágina dos Números Primos** – Projeto da cadeira do ICM do DEFCUL. Disponível em: http://www.educ.fc.ul.pt/icm/icm98/icm12/Historia.htm. Acesso em: 20 de setembro de 2020.

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

POTI, **Polos olímpicos de Treinamento Intensivo**. Disponível em: http://poti.impa.br/index.php/material. Acesso em: 20 de setembro de 2020.

MESSIAEN, Olivier. **Traité de rythme, de couleur et d'ornithologie** (1949-1992). Tome I. Paris: Leduc, 1994.