UNIVERSIDADE DO ESTADO DA BAHIA – UNEB

DEPARTAMENTO DE CIÊNCIAS HUMANAS CAMPUS VI

IVELTON SOARES PINTO

TEMOTEO MARQUES DE SOUZA

NÚMEROS PRIMOS:

Curiosidades e Aplicações

Caetité – Bahia
2004

UNIVERSIDADE DO ESTADO DA BAHIA – UNEB

DEPARTAMENTO DE CIÊNCIAS HUMANAS CAMPUS VI

IVELTON SOARES PINTO

TEMOTEO MARQUES DE SOUZA

NÚMEROS PRIMOS:

Curiosidades e Aplicações

Monografia apresentada à Universidade do Estado da Bahia Campus VI, como parte dos requisitos necessários à obtenção do grau de Licenciado em Ciências com Habilitação em Matemática.

Orientador: Prof. Adson Demétrio Silva Amparo

Caetité – Bahia
2004

UNIVERSIDADE DO ESTADO DA BAHIA – UNEB

DEPARTAMENTO DE CIÊNCIAS HUMANAS CAMPUS VI

Ivelton Soares Pinto

Temoteo Marques de Souza

NÚMEROS PRIMOS:

CURIOSIDADES E APLICAÇÕES.

Monografia apresentada à Universidade do Estado da Bahia Campus VI, como parte dos requisitos necessários à obtenção do grau de Licenciado em Ciências com Habilitação em Matemática.

Nota: _____

Aprovado em _____ de _____

BANCA EXAMINADORA

Professora: Magda Souza Braga David
Universidade do Estado da Bahia
Professora Especialista

Professor: Adson Demétrio Silva Amparo
Universidade do Estado da Bahia
Professor Especialista

Professor: _____
Universidade do Estado da Bahia
_____

DEDICATÓRIA

A DEUS por ter nos auxiliado nos problemas externos ao meio acadêmico, permitindo que nós canalizássemos nossas energias na conclusão deste trabalho.

Aos nossos familiares, incentivadores perpétuos dos nossos estudos.

A CLAUDIANA, minha esposa, pelo incentivo, compreensão e paciência por ter-lhe privado muitas vezes da minha companhia devido à necessidade de dedicação aos estudos. (Ivelton Soares Pinto)

AGRADECIMENTOS

Ao nosso orientador, PROFESSOR ADSON DEMÉTRIO SILVA AMPARO, pela sua atenção e tempo destinados tanto a nós quanto a este trabalho.

A TODOS OS PROFESSORES da UNEB-Campus VI, em especial aos do Colegiado de Matemática.

A TODOS OS SERVIDORES da UNEB-Campus VI.

AOS COLEGAS DE VÁRIAS TURMAS, dos quais guardaremos lembranças, mesmo daqueles que se dispersaram devido à dinâmica da Universidade ou aos imponderáveis da vida.

AOS COLEGAS DAS INDÚSTRIAS NUCLEARES DO BRASIL / UNIDADE DE CAETITÉ que colaboraram me substituindo ou flexibilizando meu horário de expediente, devido à necessidade dos meus estudos. (Ivelton Soares Pinto)

À PROFESSORA NÚBIA MARIA DE BRITO, Coordenadora do Colegiado de Geografia desta Universidade, com a qual eu trabalho, pela colaboração e compreensão, flexibilizando meu horário de trabalho devido à necessidade dos meus estudos. (Temoteo Marques de Souza)

E AOS CIDADÃOS DO ESTADO DA BAHIA que diretamente ou indiretamente contribuem para a manutenção desta valorosa Instituição de Ensino.

RESUMO

Aprender mais sobre os primos e pesquisar material recente sobre o tema foi o propósito deste trabalho. Na parte inicial da pesquisa, a história, os principais conceitos e as noções fundamentais são abordadas. Definição de número primo e composto, os primos como “tijolos” da construção numérica pela multiplicação, interdisciplinaridade (primos x elementos químicos), álgebra x geometria, divisores, MDC e MMC.
Em seguida, começou-se uma parte mais técnica com algumas demonstrações simples sobre a infinidade dos números primos. A participação dos computadores no estudo dos números primos e na caça dos primos especiais. Os primos de Fermat, de Sophie Germain e Mersenne. A relação dos primos de Mersenne com os números perfeitos. Como os primos inspiraram a formação de várias redes mundiais de investigação científica, algumas de elevado espírito humanitário. Uma série de primos que abalou a indústria eletroeletrônica.
A parte final ficou reservada para as aplicações, áreas em que os primos aparecem e o envolvimento dos primos em pendengas judiciais.
Trata-se de um trabalho que buscou trazer na medida do possível fatos do nosso dia-a-dia relacionados com os números primos e que não tem espaço nos livros didáticos, embora tenham ganhado muita importância nos últimos anos por conta do avanço computacional e do incremento das comunicações. Seu valor pedagógico sustenta-se na concepção de ser conveniente para a boa prática educacional recorrer a situações que despertem o interesse e a curiosidade dos alunos.

Palavras-chave: Primos, fatoração, Fermat, Sophie, Mersenne, criptografia, astronomia, química, educação, biologia.

ABSTRACT

Learn more about the prime numbers and search in newest material concerning the topic were the purposes on this schoolwork. The first part of the research, the History, the leading concepts and fundamental notions are mentioned. Definitions of prime numbers and compounded numbers, prime number as “bricks” in the number building using the multipication, interdisciplinity (primes vs. Chemical elements), Algebra vs. Geometry, divisors, MDC and MMC (Portuguese Math Terms).
Afterwards, the technical part is begun with some simple demonstration about a great deal of prime numbers. The participation of computers in the study of prime numbers and in the searching for special prime numbers. Fermat’s prime numbers, and Sophie’s and Mersenne’s ones with the perfect numbers. How the prime numbers had orientated the formation of several worldwide nets for scientific investigation; some of them with great humanitarian spriit. A contiunation of primes that affected the Electroeletronics.
The final part is reserved for the their applying, areas in which the primes appear and the involvement of them in judicial quarrels.
That’s a work that tried as possible to focus day-after-day facts related with prime numbers and that doesn’t have the correct space in the school books, however they had got much importance in those last years because of computer’s advance and communication development. Its pedagogical value maintains itself in the conception of being convenient for the good upbringing practice using situations that watch the students’ interest and curiosity.

Wordkey: Cousins, factor, Fermat, Sophie, Mersenne, cryptography, astronomy, chemistry, education, biology.

SUMÁRIO

1. INTRODUÇÃO

A notícia divulgada no início do ano de 2002 em jornais e revistas especializadas de que uma descoberta matemática relacionada a números primos poderia ameaçar a criptografia foi o impulso inicial para a confecção desta monografia. Já tínhamos lido sobre criptografia e sabíamos da sua importância para a proteção das informações, o que despertou o nosso interesse sobre o alcance desta descoberta, e na medida que a pesquisa se desenvolvia outros movimentos em torno dos números primos apareciam, envolvendo desde matemáticos e técnicos de computação profissionais até usuários de computadores domésticos. Este material é o resultado de uma extração seletiva que visa enriquecer o estudo da aritmética e da álgebra, em especial a Teoria dos Números, através de trabalhos recentes sobre os primos.

O número é a entidade mais importante da Matemática estando na origem de diversos ramos desta ciência. Entre os seres vivos, o homem é um dos poucos que possui senso numérico. Por isso, desde os primórdios da raça humana os números já estavam presentes, tendo surgido para auxiliar o homem a controlar quantidades a partir do contraste entre pouco e muito, resultando na criação dos primeiros sistemas de contagem. Juntamente com a linguagem, a escrita e outras habilidades, o número está no conjunto das criações humanas em que se baseou o desenvolvimento das nossas sociedades.

Neste trabalho, falaremos sobre números, mas de um tipo especial: os números primos. A motivação inicial para a produção desta monografia, conforme já mencionado, foi um assunto muito em pauta atualmente, que é a questão da segurança da informação. Excetuando-se os especialistas em segurança eletrônica

de dados, a grande maioria das pessoas não sabe que a inviolabilidade dos seus dados pessoais depende em parte destes números. Os primos, um conhecimento sem aplicação desde as civilizações mais antigas, são a base dos códigos de segurança de informação para computadores. Como estamos vivendo, segundo alguns historiadores e sociólogos na “Era da Informação” pode-se depreender sua importância para a nossa vida diária, embora não apareçam de forma explícita. A propósito, podemos citar a frase do matemático Nicolai Lobachevsky (1793-1856):

> Não há ramo da Matemática, por abstrato que seja, que não possa um dia vir a ser aplicado nos fenômenos do mundo real.

Além desta importante aplicação, consta deste trabalho material compatível para os níveis fundamental, médio e superior, visando estender o estudo dos números primos, mostrando as áreas em que surgem e sua utilidade. O conteúdo aqui sugerido difere do que é normalmente apresentado aos alunos: exercícios que exploram pouco suas propriedades, assim como não se procura relacionar o tema com fatos ou fenômenos do mundo real.

Os primos são apresentados pela primeira vez aos alunos na 5ª série e depois são quase esquecidos. No nível médio, apesar do aluno estar mais amadurecido para a Matemática, eles não reaparecem, embora pudessem ajudar na fixação do conteúdo específico, assim como devido ao fascínio que exercem por conta das curiosidades e mistérios que os envolvem, despertar no aluno o gosto por problemas da Teoria dos Números. Cabe ressaltar, que os números primos tem ganhado importância por causa das aplicações na criptografia, deixando de ser uma mera curiosidade.

Fazem parte do ensino fundamental, entre outras, as noções de Máximo Divisor Comum (MDC), Mínimo Múltiplo Comum (MMC), Números primos e Fatoração, que compõem uma parcela significativa da Teoria dos Números. No caso

específico dos números primos, pretende-se mostrar a relevância destes através da abordagem de temas atuais onde aparecem e sua conexão com outras áreas do conhecimento. Com isso, visamos a contextualização e a interdisciplinaridade, ambas importantes para que o aluno veja a matemática como uma aliada na vida prática e sua relação com outras disciplinas. Neste sentido, busca-se que o aluno perceba que os números e a álgebra formam um sistema de códigos ligados especialmente a diversas aplicações.

Na pesquisa serão apresentados fatos interessantes que podem ser trazidos para dentro da sala de aula pelo professor, auxiliando numa das tarefas mais desafiadoras para os educadores atualmente, que é a busca de exemplos motivadores para atrair a atenção dos alunos, contemporâneos de uma sociedade cada vez mais tecnológica. É consenso que os professores devem buscar uma educação para a cidadania. Desta forma, um papel de destaque está reservado para o conhecimento matemático, já que ele é a “porta de entrada” para o mundo tecnológico. Segundo Ubiratan D’Ambrosio (1996):

> A educação para a cidadania, que é um dos grandes objetivos da educação de hoje, exige uma apreciação do conhecimento moderno, impregnado de ciência e tecnologia. (p. 87)

Os números primos são um exemplo para os alunos, de como podemos a partir de uma definição antiga e relativamente simples, construir uma teoria que foi sendo enriquecida ao longo do tempo de outros conhecimentos, culminando no seu aproveitamento em aplicações tecnológicas de última geração.

Tendo como foco principal os alunos dos níveis Fundamental e Médio, esta monografia é uma proposta para ampliar a visão sobre estes números, que gradativamente estão ocupando um espaço cada vez maior na área das Ciências Exatas, além de enriquecer o conteúdo sobre este tema, já que se avolumam as

pesquisas sobre os Números Primos confirmando a tendência de torná-los uma área de destaque dentro da Teoria dos Números.

2. REFERENCIAL TEÓRICO

A fundamentação teórica que norteou a produção desta monografia, pensando de forma mais abrangente inicialmente, é no papel que a educação escolar deve exercer no tocante ao preparo do aluno para o exercício de sua cidadania, procurando na medida do possível acompanhar as mudanças sociais, políticas, culturais e tecnológicas. Em outras palavras, temos que preparar o aluno para a vida, o que exige do professor ampliação do seu conhecimento e atualização constante, além de uma boa cultura geral, na medida que atua como mediador na aproximação com a realidade. Segundo Neidson Rodrigues (1981):

> Quando não se coloca o centro da gravidade do ato educativo na educação do educando para a vida, lança-se a vida para fora do ato educativo. (Prefácio / p.5)

Vivemos dentro de uma sociedade moderna cuja organização é influenciada pelo conhecimento científico. Para exemplificar, basta vermos as mudanças de relações a nível global que a indústria eletroeletrônica provocou nos últimos trinta anos. As Ciências Exatas, sem dúvida foram as responsáveis por elas. A Física, através da descoberta de novos materiais, aliada a algoritmos matemáticos sofisticados provocaram uma revolução na área das Telecomunicações e da Informática. Por isso, cabem principalmente aos professores de Ciências, dentre os quais, os de Matemática, mostrar como isso é produzido destacando as idéias que motivaram as pesquisas para o domínio da tecnologia. Dentro desta visão, Neidson Rodrigues escreve (1981):

> ... é necessário, pois, iniciarmos as crianças nessa forma de produzir o mundo. Não se deve crer que se formarão pequenos cientistas, pequenos químicos, pequenos “Issacs Newtons”. Mesmo que a escola não disponha de laboratório bem montado, as operações científicas e o controle da razão no confronto com os fatos do mundo pode ser executado. (p. 73).

Sabemos que nem sempre é possível confrontar o estudo de um assunto com fatos do dia-a-dia. Porém, a contextualização é importante, pois visa provocar a curiosidade e motivação do aluno. Muito embora, a aplicação seja um dos componentes da estrutura didática da aula, há alguns anos atrás, não seria possível para o professor mostrar exemplos de aplicação dos números primos. No entanto, a situação mudou devido à rapidez com que esta área se desenvolveu dentro da Álgebra, permitindo ao professor dentro da sua prática escolar ilustrar melhor este tema. Em sintonia com Libâneo (1994):

> O objetivo da aplicação é estabelecer vínculo do conhecimento com a vida de modo a suscitar independência de pensamento e atitude crítica e criativa expressando a sua compreensão da prática social. Ou seja, a função pedagógica-didática da aplicação é a de avançar da teoria à prática, é colocar os conhecimentos disponíveis a serviço da interpretação e análise da realidade. (p. 189).

Continuando a pensar em termos de educação escolar e no âmbito das teorias do conhecimento, encontramos um elo com as idéias de Piaget, cujos conceitos epistemológicos consistem considerar que o conhecimento só é possível quando o Sujeito e o Objeto interagem. Neste sentido, Marcus Vinicius da Cunha (2000) escreve:

> O Objeto exerce pressão perturbadora sobre o Sujeito, contribuindo para fornece-lhe motivação interna e criar envolvimento pessoal com o Objeto. Em segundo lugar, temos a atividade do Sujeito, que se traduz em atividades de busca, desvendamento, pesquisa, enfim ação sobre o Objeto a ser conhecido. (p. 74).

Transportando essa concepção para dentro da sala de aula, temos que mostrar ao aluno a relevância daquilo que vai ser ensinado, deixando de lado inicialmente, o rigor e a formalização matemática, para que o aluno se posicione de modo ativo diante da matéria que está sendo iniciada. A dupla Márcia Regina F. De Brito e Maria Helena C. Castro Gonçalez (2001) escrevendo sobre atitudes positivas em relação à aprendizagem matemática afirmam:

> Cabe aos professores propiciar situações motivadoras, desafiadoras e interessantes de ensino, nos quais o aluno possa interagir com o objeto de

> estudo e, acima de tudo, possa construir significativamente o conhecimento, chegando às abstrações mais complexas. Provavelmente, experiências pedagógicas desse tipo permitirão o desenvolvimento de atitudes positivas com relação à matemática. (p.223).

Percebemos com clareza uma tendência mundial da educação matemática caminhar cada vez mais para dentro da vida das pessoas, sendo uma ferramenta fundamental para que as pessoas ocupem o seu espaço no mundo. Por conta da rapidez do surgimento de novas tecnologias, entendemos ser necessário que o professor vá mais além, dando acesso a novas formas de pensar, apresentando novas informações e mostrando possibilidades. Qualquer que seja o público alvo, ele sempre estará ávido por novidades que tenham relação com o seu interesse pessoal. Certamente, no nível individual será impossível atender a todos, contudo, acreditamos ser esta uma opção pedagógica bastante eficaz para motivar o aluno em seu processo de aprendizagem, aumentando as chances de uma postura favorável em relação à disciplina.

3. PESQUISA

Em conformidade com a nossa proposta, isto é, de apresentar matérias recentes e compatíveis sobre os números primos para os alunos do nível fundamental e médio, realizamos uma pesquisa que podemos dizer que é uma combinação da bibliográfica com a documental, procurando principalmente por coisas modernas que possam interessar ao aluno, sem contudo deixar de abordar fatos do passado que contribuíram para a evolução do conhecimento sobre estes números. Seguindo nesta linha, nos preocupamos mais com as definições e aplicações, reservando demonstrações somente para aquilo que for estritamente necessário, já que o objetivo não foi escrever um texto formal sobre a aritmética dos inteiros, mas sim levantar material que possa ser aproveitado dentro da sala de aula. Nesta parte inicial, apresentamos um resumo histórico, vindo na seqüência as principais definições que se relacionam com os números primos.

Os primos são estudados pelos aritméticos desde as civilizações mais antigas. Entretanto, é na Grécia que identificaremos a Teoria dos Números tal como a estudamos hoje. Entre os problemas da Teoria dos Números abordados pelos gregos estão: O cálculo do MDC entre dois números, a determinação dos números primos menores que um dado inteiro e a demonstração de que há infinitos números primos.

Estes problemas constam do mais famoso texto herdado dos Gregos, *Os Elementos* escrito pelo matemático Euclides, que viveu em Alexandria por volta de 300 a.C. Outro matemático grego que tem seu nome vinculado aos números primos é Eratóstenes (276 a 194 a.C), responsável pela criação do Crivo que leva o seu nome, um método de localização de números primos que toda criança tem contato

quando estuda pela primeira vez este tópico da matemática. Neste estágio, já é possível que o estudante faça a seguinte pergunta: Por que o nome *primo* para os números primos?

Certamente os estudantes acharão, assim como a maioria das pessoas, que a palavra primo tem analogia com alguma forma de parentesco. Porém, esta hipótese é falsa, já que a palavra primo dentro deste contexto, refere-se à idéia de primeiro, estando sua origem na concepção numérica dos pitagóricos.

A noção de número primo foi introduzida por Pitágoras em 530 a.C. A Escola Pitagórica dava grande importância ao número um (1), que era chamada de unidade (em grego: monad). Os demais números naturais (2, 3, 4, 5, 6, etc.) eram considerados como múltiplos da unidade (gerados por ela), e por isso recebiam a denominação número (em grego: arithmói). Na Escola Pitagórica existiam dois tipos de números:

1. Os **protói arithmói** (números primos ou primários):

   Aqueles que não podiam ser gerados, via multiplicação, por outro número. Por exemplo: 2, 3, 5, 7, 11, ...

2. Os **deuterói arithmói** (números secundários):

   Aqueles que podiam ser gerados por outro número. Por exemplo: 6 = 2 x 3, 8 = 2 x 4, etc.

Desta forma, os matemáticos gregos dividiam os números inteiros naturais em três classes:

1. A **monad** (unidade, 1).
2. Os **protói arithmói** (números primos) ou **asynthetói aritmói** (números não compostos): 2, 3, 5, 7, 11, etc.
3. Os **deuterói arithmói** (números compostos): 4, 6, 8, 10, 12, 14, etc.

É importante registrar que os escritos de Pitágoras perderam-se ao longo do tempo, tendo as suas idéias registro em fragmentos de textos escritos várias gerações depois dele. Contudo, estes fragmentos são unânimes em afirmar que Pitágoras iniciou o estudo dos números primos.

O mais antigo texto de matemática que chegou completo ao nosso tempo e que desenvolve o estudo dos números primos é o Elementos de Euclides. Como Euclides seguia a Escola Pitagórica, ele num dos livros que tratam da Teoria dos Números, define número primo de forma compatível com as idéias pitagóricas:

> *Protós arithmói estin monadi mone metroymenos.*
> (Tradução)
> Número primo é todo aquele que só pode ser medido através da unidade.

Acima vimos a documentação grega. Agora, iremos falar do surgimento da denominação latina primus.

O livro do grego Nikomachos (100 d.C), Arithmetiké, é depois de *Elementos*, o mais antigo livro da Teoria dos Números que chegou até nossos dias. Este livro foi a base do primeiro livro sobre a Teoria dos Números escrito em latim: De Institutione Arithmetica, do romano Boethius (500 d.C). Neste livro é que aparece, pela primeira vez, a denominação **numerus primus** como tradução da tradicional *Protós arithmói* preservada de Euclides por Nikomachos.

O livro de Boethius foi durante seiscentos anos, a única fonte de estudos da Teoria dos Números na idade Média. Em 1200 iniciou o renascimento científico e matemático do Mundo Cristão, com o afluxo das obras árabes e a tradução das obras gregas. Nesta época, surge um dos mais influentes livros da Matemática: o *Líber Abacci*, de Fibonacci. Como ele tinha estudado entre os muçulmanos do Norte da África, preferiu adotar ***primus*** ao invés do incomposto preferido pelos árabes, consagrando desta forma em definitivo a denominação número primo em toda a Europa.

4. DEFINIÇÃO DE NÚMERO PRIMO

Falamos sobre a origem do nome primo para os números primos e das idéias que motivaram a sua adoção. Consoante com a idéia inicial, chegamos à definição atual e mais freqüentemente encontrada nos livros voltados para o ensino fundamental e médio; aquela que afirma que **número primo é todo número natural (ou inteiro) maior do que 1 e que é divisível apenas por si próprio e pelo 1**. Da definição, podemos ensaiar uma pequena seqüência de números primos:

(2, 3, 5, 7, 11, 13, 17, 19, 23,...)

Facilmente observamos, que com exceção do 2 (único par primo), todos os demais primos são ímpares. Também, podemos concluir que terminando em cinco (5) existe apenas um único primo, que é o próprio 5 , já que os demais são todos múltiplos de 5, sendo por isso, chamados de números não-primos ou compostos, cuja definição vem em seguida.

5. DEFINIÇÃO DE NÚMERO COMPOSTO OU NÃO-PRIMO

É todo número inteiro maior que 1 obtido pelo produto de números primos. Neste caso, ele pode ser decomposto num produto de fatores primos, que em outras palavras significa dizer que ele é fatorável em números primos, como por exemplo:

21 = 3 x 7 , 36 = 2 x 2 x 3 x 3 , 70 = 2 x 5 x 7

Pelo seu caráter básico, essa propriedade é conhecida como o **Teorema Fundamental da Aritmética (TFA)**, cujo enunciado afirma **que todo inteiro diferente de 0, 1 e –1 pode ser expresso como produto de números primos, de forma única, a menos da ordem dos fatores.**

Observando os nossos exemplos, vemos que não podemos mais continuar com a fatoração, de onde concluímos que a sua decomposição chegou no limite. Neste ponto temos condições de responder uma das perguntas que mais freqüentemente aparece: **Por que o número 1 não é primo?**

Para esta questão existem inúmeras respostas cada uma mais técnica do que a outra. A primeira resposta é imediata se recorrermos para a definição: **número primo é todo número inteiro maior do que 1 e que é divisível apenas por si próprio e pelo 1**. Claramente temos que o **1** está excluído, porém a força da definição não responde plenamente ao “Por que ?”.

A segunda resposta pode ser creditada ao Teorema Fundamental da Aritmética: **que todo inteiro diferente de 0, 1 e –1 pode ser expresso como produto de números primos, de forma única, a menos da ordem dos fatores**. A chave da resposta está na expressão **“de forma única”,** pois se o **1** fosse considerado primo não teríamos a unicidade, já que haveria infinitas fatorações para um dado número. Por exemplo:

12 = 2 x 2 x 3, mas,

12 = 1 x 2 x 2 x 3 como também,

12 = 1 x 1 x 2 x 2 x 3 ou ainda,

12 = 1 x 1 x 1 x 2 x 2 x 3.

Enfim, poderíamos continuar indefinidamente com esta construção o que nos levaria a ter infinitas fatorações, contrariando desta forma o Teorema.

Como dissemos, existem outras respostas mais técnicas, mas por requererem um maior aprofundamento na Teoria dos Números e não fazerem parte do programa do ensino fundamental e médio não serão aqui abordadas.

Retornando a nossa propriedade garantida pelo Teorema Fundamental da Aritmética da decomposição em fatores primos de um número composto, é possível pensar nos números primos como os “tijolos” da construção numérica pela multiplicação, desempenhando um papel parecido com o dos elementos na Química, que iremos explorar para propor uma atividade interdisciplinar.

A atividade inicia-se criando uma tabela que associa um primo matemático (um número primo) a um primo químico (o elemento químico). O objetivo é chegar ao número composto correspondente à substância composta, de preferência de uso cotidiano, cuja fórmula química é fornecida. Pode-se também inverter o objetivo, fornecendo o número composto, sendo descoberta a fórmula da substância através da sua fatoração e usando um pouco de raciocínio dedutivo.

TABELA

NÚMERO PRIMO	ELEMENTO QUÍMICO
2	O (OXIGÊNIO)
3	H (HIDROGÊNIO)
5	S (ENXOFRE)

7	Na (SÓDIO)
11	Cl (CLORO)
13	Ca (CÁLCIO)
17	F (FLÚOR)
19	C (CARBONO)

Número composto: **1976**

Fatoração: **2 x 2 x 2 x 13 x 19**

Substância composta: **O + O + O + Ca + C**

3 átomos de oxigênio

1 átomo de cálcio

1 átomo de carbono

Fórmula da substância: O_3CaC => **$CaCO_3$** (Carbonato de Cálcio)

Uso cotidiano: Mármores

Número composto: **18**

Fatoração: **2 x 3 x 3**

Substância composta: **O + H + H**

1 átomo de oxigênio

2 átomos de hidrogênio

Fórmula da substância: OH2 => **H_2O** (Água)

Uso cotidiano: Solvente universal

Número composto: **77**

Fatoração: **7 x 11**

Substância composta: **Na + Cl**

1 átomo de sódio

1 átomo de cloro

Fórmula da substância: NaCl => **NaCl** (Cloreto de Sódio)

Uso cotidiano: Sal de cozinha

Número composto: **1040**

Fatoração: **2 x 2 x 2 x 2 x 5 x 13**

Substância composta: **O + O + O + O + S + Ca**

4 átomos de oxigênio

1 átomo de enxofre

1 átomo de cálcio

Fórmula da substância: O_4SCa => **$CaSO_4$** (Sulfato de Cálcio)

Uso cotidiano: Giz escolar

Número composto: **119**

Fatoração: **7 x 17**

Substância composta**: Na + F**

1 átomo de sódio

1 átomo de flúor

Fórmula da substância: NaF => **NaF** (Fluoreto de Sódio)

Uso cotidiano: Anticárie

Podemos perceber que é possível formar várias tabelas de acordo com as substâncias compostas que desejamos trabalhar, fazendo com que os seus

elementos tenham correspondência com determinados primos, que produzirão através da sua multiplicação números compostos convenientes para a descoberta das fórmulas desejadas.

Uma outra atividade que pode ser proposta é a montagem de uma ***Rede de Divisores***, onde é possível representar os divisores naturais de determinados números através de figuras geométricas. Estas figuras poderão ser **lineares**, **planas** ou **espaciais**, as quais nos mostram uma relação importante existente entre a álgebra e a geometria.

Para obter a rede de divisores o exercício deve ser desenvolvido da seguinte maneira:

a) Decompor o número em fatores primos;

b) Obter a quantidade de divisores naturais do número;

c) Escrever o conjunto dos divisores naturais do número;

d) Construir a rede de divisores naturais desse número, Lembrando que:

- A rede é linear quando temos, na forma decomposta, o mesmo número primo como base;
- A rede é plana quando temos, na forma decomposta, dois números primos distintos como base;
- A rede é espacial quando temos, na forma decomposta, três ou mais números primos distintos como base.

Exemplo 1: Construir a rede de divisores naturais do número 32.

Decompondo o número 32 em fatores primos, temos:

$32 = 2 \times 2 \times 2 \times 2 \times 2 \Rightarrow 32 = 2^5$

Para obter o número de divisores naturais de 32, devemos somar **1** a cada expoente na forma decomposta. Portanto, o número de divisores naturais de 32 é **6**.

O conjunto de divisores é {1, 2, 4, 8, 16, 32}.

A rede destes divisores é linear pois a base é a mesma (2).

Para construir a rede, usaremos o símbolo $\longrightarrow$ que significa “é divisor de”. Sendo assim, obtemos:

“rede linear”

Exemplo 2: Construir a rede de divisores naturais do número 24.

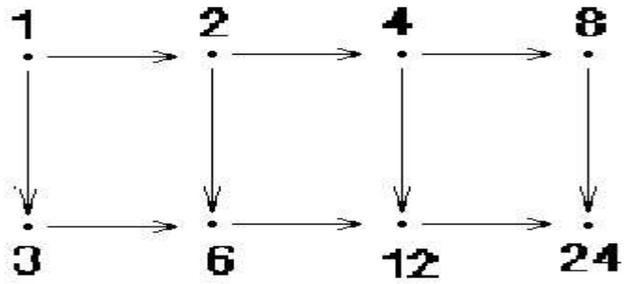
$24 = 2 \times 2 \times 2 \times 3 = 2^3 \times 3^1$

Números de divisores = $(3 + 1) \times (1 + 1) = 4 \times 2 =$ **8**

Conjunto dos divisores é {1, 2, 3, 4, 6, 8, 12, 24}.

A rede dos divisores, neste caso, será plana, pois temos duas bases distintas (2 e 3) na forma decomposta.

Sendo assim, temos:



“rede plana”

Exemplo 3 : Construir a rede de divisores naturais do número 30.

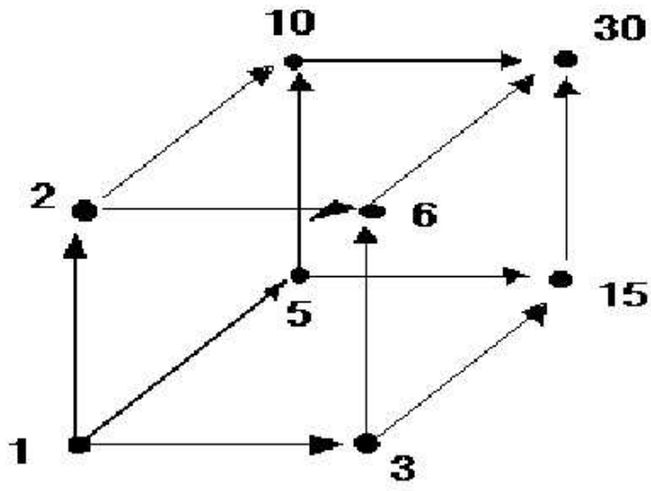
$30 = 2 \times 3 \times 5 = 2^1 \times 3^1 \times 5^1$

Número de divisores = (1 + 1) x (1 + 1) x (1 + 1) = 2 x 2 x 2 = 8

Conjunto de divisores = {1, 2, 3, 5, 6, 10, 15, 30}.

A rede de divisores é espacial, pois temos três bases distintas (2, 3 e 5) na forma decomposta.

Sendo assim, temos:



“rede espacial”

6. CÁLCULO DO MDC E DO MMC ATRAVÉS DA FATORAÇÃO EM PRIMOS

Logo após o ensino da fatoração são introduzidas as definições de MDC (máximo divisor comum) e MMC (mínimo múltiplo comum). Dados os números naturais **a** e **b**, seu MDC é o maior divisor que divide tanto **a** quanto **b**. O MMC é o menor múltiplo simultâneo de **a** e **b.** O número 1 é divisor de qualquer número, e se **a** e **b** não admitem outro divisor comum, além do 1, dizemos que o MDC (a, b) = 1, e que **a** e **b** neste caso são primos entre si.

Se os números **a** e **b** estão decompostos em fatores primos, é fácil achar o MDC e o MMC.

Como exemplo, tomemos os números **36** e **150**.

36 = 2 x 2 x 3 x 3 = $\mathbf{2^2 \times 3^2}$

150 = 2 x 3 x 5 x 5 = $\mathbf{2 \times 3 \times 5^2}$

Qualquer divisor comum tem que ter o **2** e o **3** como fatores primos. O maior deles é 2 x 3 = 6, então MDC (36,150) = 6. Por isso, a regra diz que o MDC é o produto dos fatores primos comuns, elevados ao menor expoente.

O mínimo múltiplo comum (MMC), como o próprio nome diz, é um múltiplo de 36 e 150, logo tem que conter pelo menos todos os fatores primos de 36 e 150 elevados a maior potência com que aparecem, então MMC (36,150) = $\mathbf{2^2 \times 3^2 \times 5^2}$ = 900.

No caso do MDC, principalmente quando se tratar de números grandes é mais eficiente usar o algoritmo de Euclides, baseado em divisões sucessivas, já que nem sempre é fácil fatorar um número grande. Por exemplo: 1128 e 336. Aplicando o algoritmo de Euclides temos:

	3	2	1	4
1128	336	**120**	**96**	**24**
120	**96**	**24**	0	

MDC (1128,336) = **24**

Um outro método é o que fornece ao mesmo tempo, o MMC e o MDC.

1128	336	2
564	168	2
282	84	2
141	42	3
47	14	

MDC = 2 x 2 x 2 x 3 = **24**
MMC = 24 x 47 x 14 = **15.792**

Nesta disposição, um número primo comparece na coluna da direita somente quando divide ambos os números à sua esquerda. As divisões terminam quando isto não for mais possível, o que significa que encontramos dois números primos entre si nas colunas da esquerda. O MDC é o produto dos primos que estão na coluna da direita e o MMC é o produto do MDC pelos números primos entre si que ficaram na última linha à esquerda.

A justificativa do método é que na coluna da direita achamos só os primos que dividem ambos os números, logo são os fatores primos do MDC, como conseqüência o MDC será o produto destes fatores. Quanto ao MMC, temos que observar que os números da última linha são primos entre si, não tendo em comum nenhum fator primo. Sendo assim, qualquer múltiplo de 1128 terá que conter os fatores 24 e 47, assim como qualquer múltiplo de 336 conterá os fatores 24 e 14.

Logo, o menor de todos os múltiplos comuns é originário do produto 24 x 47 x 14 = 15.792.

O processo e a sua justificativa são conseqüência de uma importante relação entre o MDC e o MMC de dois números **a** e **b** :

$$\mathrm{MMC}(a,b)\times \mathrm{MDC}(a,b) = a\times b$$

A inclusão deste assunto neste trabalho é por conta do cálculo do MDC e do MMC ser uma aplicação dos números primos, sendo ambos bastante utilizados nas operações envolvendo frações ordinárias, assim como na resolução de problemas elementares.

7. INFINIDADE: Uma qualidade do conjunto dos primos

Há cerca de 2300 anos, na proposição 20 do livro IX dos seus *Elementos*, Euclides apresentou uma demonstração de que a quantidade de números primos é inesgotável. A argumentação de Euclides é bastante simples. Supondo que exista um número finito de primos, sendo **P** o maior deles. Agora, peguemos o número **N** = 2 x 3 x 5 x 7 x 11 x ..... x **P + 1**, que é o produto de todos os primos existentes, acrescido de uma unidade. Esse número **N**, ou é primo ou composto. Se for primo, encontramos um **N**, primo, maior que **P**. Se for composto, pelo Teorema Fundamental da Aritmética, **N** será fatorado por um primo diferente de 2, 3, 5, ..., **P**, pois ao ser dividido por qualquer um destes deixa resto **1**. Em qualquer caso, teremos encontrado um novo número primo, contradizendo a nossa hipótese inicial.

A demonstração de Euclides é a mais simples de todas as conhecidas sobre este resultado. Sua vantagem em relação as demais é a sua simplicidade, pois requer apenas o domínio do Teorema Fundamental da Aritmética.

Atualmente, com o recurso de programas podemos explorar os números **N** e descobrir uma curiosidade sobre eles quando são fatorados. Calculando os números **N** temos: $N_2 = 2 + 1$, $N_3 = 2 \times 3 + 1$, $N_5 = 2 \times 3 \times 5 + 1$, $N_7 = 2 \times 3 \times 5 \times 7 + 1$, etc. A tabela abaixo fornece até N_{37} e sua fatoração em primos quando N_P é composto.

$N_P = 2 \times 3 \times 5 \times ..... \times P + 1$	PRIMOS GERADOS
$N_2 =$ **3**	3
$N_3 =$ **7**	7
$N_5 =$ **31**	31
$N_7 =$ **211**	211

N_{11} = **2311**	2311
N_{13} = 30031= 59 X 509	59, 509
N_{17} = 510511 = 19 X 97 X 277	19, 97, 277
N_{19} = 9699691 = 347 X 27953	347, 27953
N_{23} = 223092871	317, 703763
N_{29} = 6469693231	331, 571, 34231
N_{31} = **200560490131**	200560490131
N_{37} = 7420738134811	181, 60611, 676421

Na primeira coluna, os números primos estão em negrito, os outros são compostos. No entanto, ao fatorarmos os compostos obtemos novos primos em relação aos obtidos nas linhas anteriores.

A lista completa dos números primos p < 100.000 tais que N_P é primo é: p = 2 , 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029 e 42209 que é o recorde atual obtido em 1999 pelo matemático C. Caldwell, possuindo este primo o total de 18.241 algarismos.

Uma outra demonstração é a que o matemático Kummer fez em 1878. Esta demonstração é considerada uma “semi-demonstração” por ser considerada uma variante da de Euclides. Entre as demonstrações pesquisadas, no total de 15 (quinze), esta se destaca pela sua simplicidade. A argumentação de Kummer é a seguinte:

Suponhamos que exista um número (n) finito de primos, então podemos escrever p1 < p2 < p3 < ..... < p_n, tome N = p_1 x p_2 x p_3 x p_4 x …… x p_n, que é obviamente maior que 2. O inteiro N – 1 sendo o produto de fatores primos, teria

então um fator primo p_i, que dividiria também N, então p_i dividiria 1 = N – (N –1), o que é absurdo.

Não é objetivo deste trabalho mostrar todas demonstrações, mas vale a pena citar mais uma devida a Euler pois ela constitui a base de desenvolvimentos muito importantes. Esta demonstração requer conhecimento das séries geométrica e harmônica e um pouco de análise. A essência da sua argumentação está no estabelecimento de uma expressão infinita formada com os números primos.

Se p é um número primo qualquer, então $\left(\frac{1}{p}\right) < 1$. Então, a soma da série geométrica de razão $\frac{1}{p}$ e o primeiro termo 1 é dada por $\sum_{k=0}^{\infty} \frac{1}{p^k} = \frac{1}{1-\left(\frac{1}{p}\right)}$ da mesma forma, se q é outro número primo, então $\sum_{k=0}^{\infty} \frac{1}{q^k} = \frac{1}{1-\left(\frac{1}{q}\right)}$.

Multiplicando, membro a membro essas duas igualdades temos:

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+.....+\frac{1}{p^k}\right)\times\left(1+\frac{1}{q}+\frac{1}{q^2}+.....+\frac{1}{q^k}\right) = \frac{1}{1-\left(\frac{1}{p}\right)}\times\frac{1}{1-\left(\frac{1}{q}\right)}$$

O primeiro membro é a soma dos inversos de todos os inteiros naturais da forma $p^h q^k$ (com h ≥ 0, k ≥ 0) , cada um sendo contado uma e uma só vez, porque a expressão de cada número natural, como produto de números primos é única. Esta idéia está na base da demonstração de Euler.

Suponhamos que p_1, p_2, ...,p_r formam o conjunto dos números primos. Para cada i = 1, 2, ..., r temos:

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = \frac{1}{1-\left(\frac{1}{p_i}\right)}.$$

Multiplicando membro a membro essas **r** igualdades, temos:

$$\prod_{i=1}^{r}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^{\,k}}\right)=\prod_{i=1}^{r}\frac{1}{1-\frac{1}{p_i}}$$

O primeiro membro depois de efetuadas todas as operações, é a soma dos inversos de todos os números naturais, cada um contado uma só vez, como resulta do TFA que estabelece a unicidade da decomposição em fatores primos de qualquer número composto.

Sabemos que a série $\sum_{n=1}^{\infty}\frac{1}{n}$ é divergente.

Assim, o primeiro lado da igualdade será infinito, enquanto que outro lado será finito, o que é um absurdo.

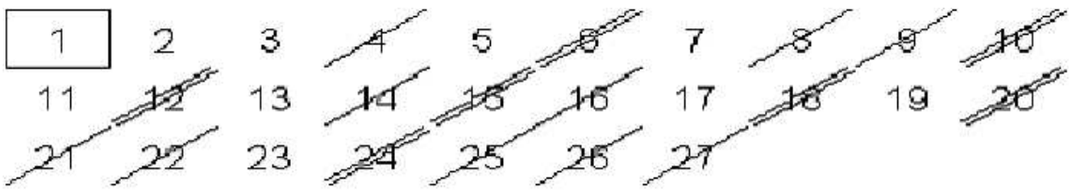
Esta idéia permitiu a Euler em 1737 demonstrar que a soma dos inversos dos números primos é divergente, isto é $\sum\frac{1}{p}=\infty$.

8. MÉTODOS DE LOCALIZAÇÃO DE PRIMOS

O Crivo de Eratóstenes é o mais antigo método para achar primos, sem envolver fórmula específica. Eratóstenes foi diretor da famosa biblioteca de Alexandria e viveu entre 276 a 194 AC. Apesar de seu vasto conhecimento em muitas áreas, foi ele por exemplo, que mediu o raio da Terra, comparando os comprimentos das sombras de dois mastros ao meio-dia em Alexandria e Syene, um tempo em que ainda poucos acreditavam que a Terra fosse realmente redonda, os contemporâneos de Eratóstenes julgavam que ele não havia chegado à perfeição em nenhuma área, por isso o chamavam de “Beta” (β segunda letra do alfabeto grego). Diante desta classificação que atribuíam a Eratóstenes ficamos a imaginar o nível dos matemáticos da Grécia Antiga.

O melhor sinônimo para crivo é peneira. Os garimpeiros a utilizam para separar da mistura de areia e pedras comuns às valiosas pedras preciosas. De forma análoga, o crivo de Eratóstenes separa da mistura com os números compostos, os preciosos primos.

O objetivo do crivo é determinar todos os primos menores que um certo número dado N > 0. Para ver como funciona vamos aplicá-lo para N=27. Em primeiro lugar, escrevemos os números em ordem, colocando o 1 numa caixa para mostrar que se trata da unidade.



Em seguida riscamos de dois em dois a partir do 2 (todos os pares a partir do 2 são riscados). Na seqüência procuramos o menor elemento, maior que 2, que não

tenha sido riscado; que é o 3. Riscamos todos os múltiplos de 3 maiores que 3. Na seqüência procuramos o menor elemento, maior que 3, que não tenha sido riscado, que é o 5. E assim por diante, até chegar a N.

Neste pequeno exemplo (N é pequeno) já podemos destacar dois fatos interessantes. De imediato, alguns números são riscados mais de uma vez. O outro, é que todos os números compostos já tinham sido riscados após riscarmos todos os múltiplos de 5, não havendo necessidade de procurarmos os múltiplos de 7, 11 e 13.

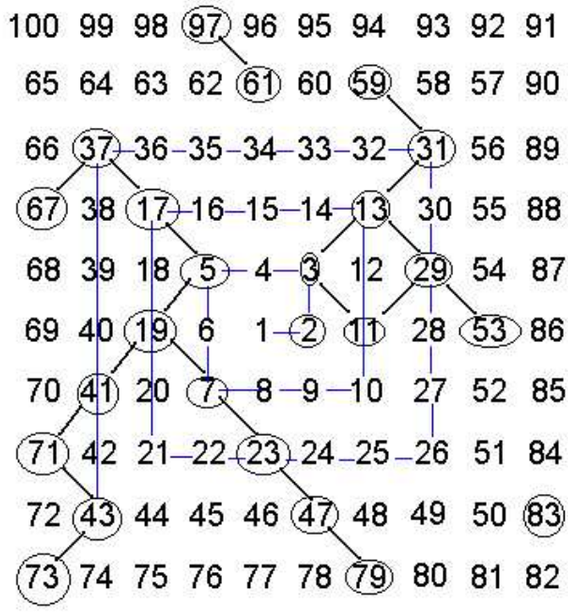
O primeiro fato é justificado por ao considerar um dado **p** primo, todos os seus produtos por números menores do que **p** já foram cortados e o primeiro que ainda não foi será igual a p x p = p^2 . No nosso exemplo, para p = 3, poderíamos ter começado a riscar a partir do **9** ao invés do **6** (já tinha sido riscado por ser múltiplo de 2). Uma outra argumentação para este fato é a propriedade da comutatividade da multiplicação, pois 6 = 2 x 3, mas 6 = 3 x 2, assim como 15 = 3 x 5 e 15 = 5 x 3.

O segundo fato indica que podemos parar de riscar antes de chegar a **N**. O motivo é devido ao seguinte: Se d > 0 é um divisor próprio de um inteiro composto **m**, temos que m = dc, em que c > 1.

Se $d > \sqrt{m}$ e $c > \sqrt{m}$, teríamos que $m = dc > \sqrt{m}\sqrt{m} = m$, uma contradição. Assim, podemos afirmar que todo número composto **m** tem um divisor primo menor ou igual a $\sqrt{m}$. Então, se pegarmos um **m** inteiro da lista, temos m ≤ N. Se **m** for composto, então terá um fator menor ou igual a $\sqrt{m}$. Mas $\sqrt{m} \leq \sqrt{N}$, logo qualquer número composto da lista tem um fator menor ou igual a $\sqrt{N}$. Por isso não precisamos riscar números de **p** em **p** quando $p > \sqrt{N}$. Em nosso exemplo $\sqrt{27} \approx 5{,}2$ comprovando porque todos os compostos já tinham sido riscados por ser $7 > \sqrt{27}$.

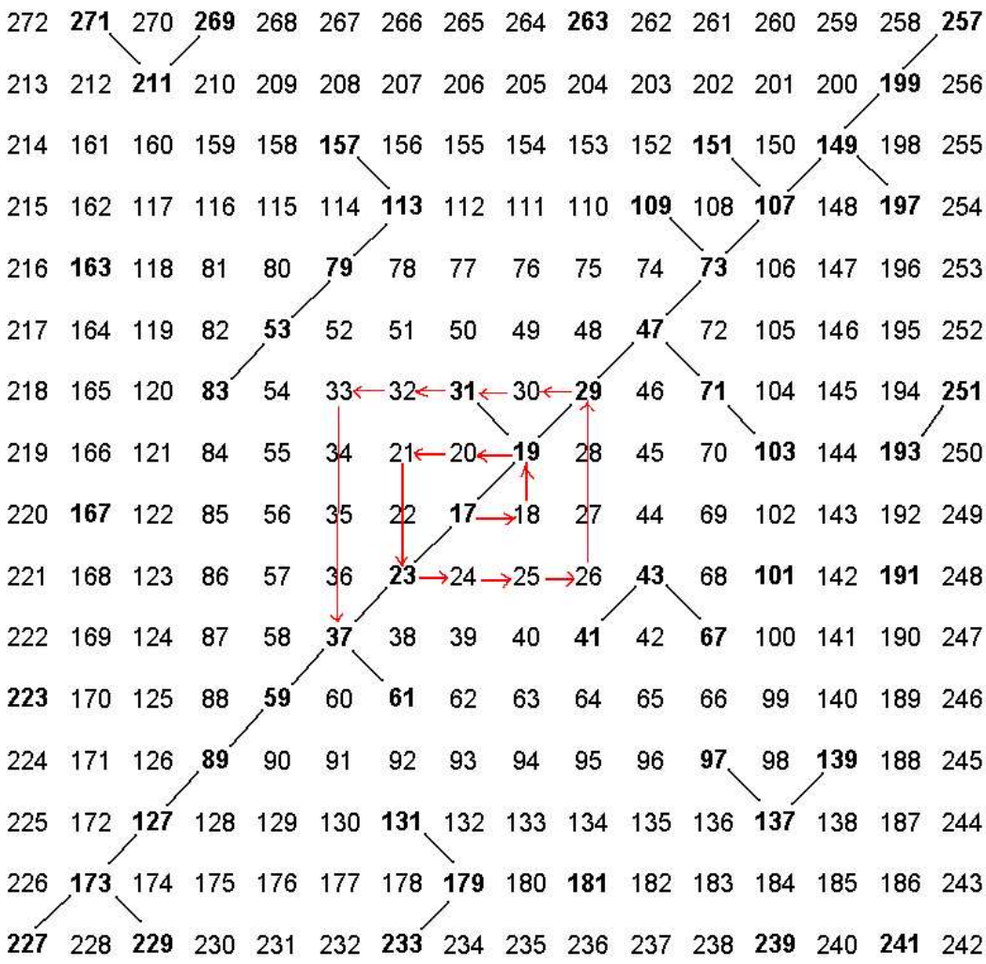
Atualmente os computadores com algoritmos sofisticados e processadores cada vez mais velozes criam tabelas de números primos. Todavia, antes do advento da computação as tabelas eram construídas manualmente usando o crivo de Eratóstenes, como foi o caso da tabela publicada em 1914 por Derick Norman Lehemer que continha os números primos menores do que 10 milhões.

Desde Euclides, os matemáticos tentam encontrar padrões nos números primos, o que acaba acontecendo até por acaso. Em 1983, o matemático Stanilaw Ulam ao rabiscar números inteiros consecutivos, começando por **1**, numa espécie de espiral quadrada no sentido anti-horário, observou uma preferência dos números primos pelas diagonais.



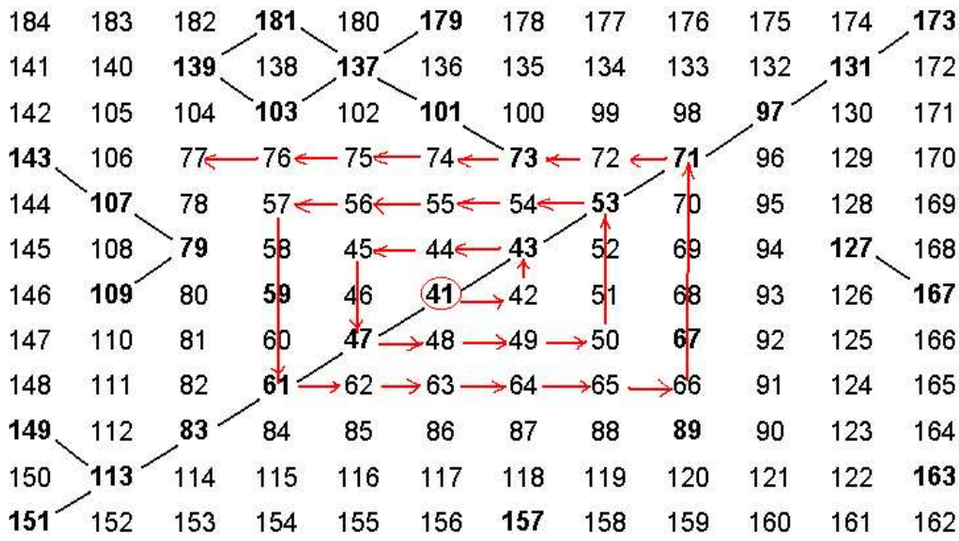
Em um teste realizado pelo computador Maniac II do laboratório de Los Alamos (EUA), programado para imprimir uma espiral quadrada de todos os números inteiros até 10 milhões, os primos continuaram a mostrar sua preferência pelas diagonais.

Se colocarmos o **17** no centro da espiral e acrescentarmos os inteiros até **272**, vamos observar que uma das diagonais principais é toda ela composta de números primos.



Vamos colocar agora o **41** no centro da espiral e acrescentarmos os inteiros até **184.** Vamos observar também que em uma das diagonais principais só aparecem números primos.

(*a aspiral foi colocada na folha seguinte por ser grande e não caber nesta folha*)



Na realidade, o que existe por trás desta disposição são as fórmulas polinomiais que Euler já tinha descoberto no século XVIII. No caso da espiral de centro **"17"**, o polinômio é $n^2 + n + 17$ que gera primos para $0 \leq n \leq 15$. Para n=16 $P(n) = 289 = 17^2$ (composto).

Os valores de P(n) são os que aparecem na diagonal principal.

O mesmo acontece para a espiral de centro "41". O polinômio é $n^2 + n + 41$ que gera primos para $0 \leq n \leq 39$. Para n=40, $P(n) = 1681 = 41^2$ (composto).

O computador Maniac II mostrou que o polinômio $n^2 + n + 41$ para números abaixo de 10 milhões gera primos 47,5 % das vezes. Um número bastante respeitável tendo em vista a simplicidade da "fórmula".

Para os polinômios do tipo $x^2 + x + q$ o melhor resultado possível é o $x^2 + x + 41$.

No caso dos polinômios cúbicos o recordista é $2x^3 – 489x^2 + 39847x – 1084553$ que assume 267 valores primos para P(x) para $0 \leq x \leq 500$ (53,4 %).

Na verdade, não existe polinômio de uma variável apenas em qualquer grau de coeficientes inteiros que gere somente números primos. Isso é garantido pelo

Teorema “Não existe nenhum polinômio f(x) não constante, com coeficientes inteiros, tal que f(x) seja primo, para todo inteiro positivo n”.

É importante registrar que o teorema citado é sobre polinômios de mesma variável. Em 1971, Matiyasevic produziu um polinômio em várias variáveis com coeficientes inteiros, cujos valores percorrem todos os primos positivos e inteiros negativos. Como curiosidade, este polinômio tinha grau 37 e 24 variáveis. Mais tarde outros polinômios foram obtidos, mas à medida que o grau diminuía as variáveis aumentavam. O recorde é um polinômio de grau 5 mas com 42 variáveis obtido em 1976 por Jones, Sato, Wada e Wiens.

9. UMA FÓRMULA PARA OS NÚMEROS PRIMOS

No item anterior foi mostrada a existência de polinômios que geram números primos, mas são de alta complexidade. No entanto, existe uma fórmula simples que gera todos os primos e somente esses. Ela consta de um artigo da Profª. Renate Watanabe (IME/USP), que por sua vez foi extraída do livro Mathematical Gems II de R. Horisberg, The Mathematical Association of América, 1976.

A fórmula é a seguinte: Sejam **a** e **b** números naturais, $b \neq 0$ e $c = A(B+1) - (B!+1)$, $F(a,b) = \frac{(b-1)}{2} \times \left(\left| c^2 - 1 \right| - \left(c^2 - 1 \right) \right) + 2$.

Fazendo alguns testes obtemos:

a= 1 e b = 1 $\rightarrow$ F (1,1) = 2 (primo)

a = 1 e b = 1 $\rightarrow$ F (1,1) = 2 (primo)

a = 1 e b = 2 $\rightarrow$ F (1,2) = 3 (primo)

a = 1 e b = 3 $\rightarrow$ F (1,3) = 2 (primo)

a = 1 e b = 4 $\rightarrow$ F (1,4) = 2 (primo)

a = 5 e b = 4 $\rightarrow$ F (5,4) = 5 (primo)

a = 6 e b = 5 $\rightarrow$ F (6,4) = 2 (primo)

a = 103 e b = 6 $\rightarrow$ F (103,6) = 7 (primo)

a = 329891 e b = 10 $\rightarrow$ F (329891,10) = 11 (primo)

a = 36846277 e b = 12 $\rightarrow$ F (36846277,12) = 13 (primo)

Como podemos constatar, embora seja simples, ela não é nada prática, pois envolve cálculos com números muito grandes. Imagine o tamanho do natural **a** quando atingirmos o primo 89! Além do mais, a fórmula tem uma preferência muito grande pelo primo 2. Outra dificuldade é obter os pares ordenados que geram os primos diferentes de 2.

Para se obter o primo **p**, fazemos F(a,b) para $a = \frac{(p-1)!+1}{p}$ e $b = (p-1)$.

Assim foi obtido o 13, fazendo $a = \frac{(13-1)!+1}{3} = 36.846.277$ e $b = 13-1 = 12$.

A demonstração da fórmula é baseada no Teorema de Wilson que afirma que **p** é primo, se e somente se, p ≠ 1 e p é um divisor de (p-1)**!** + 1.

Aqui cabe uma observação a respeito do Teorema de Wilson. Ele é um dos mais simples que testam a primaridade de um número, mas foi abandonado devido ao fatorial (p-1)**!** , porque não se conhece ainda uma maneira de se calcular rapidamente o fatorial de um número.

<u>F (a,b) é sempre primo:</u>

O número **c** é inteiro => c^2 é inteiro.

Para $c^2 \geq 1$ (o que normalmente ocorre e daí vem o aparecimento constante do primo 2).

$F(a,b) = \frac{(b-1)}{2} \times (c^2 - 1 - c^2 + 1) + 2 = 0 + 2 = 2$ (primo).

Para $c^2 = 0 \rightarrow F(a,b) = \left(\frac{(b-1)}{2}\right) \times 2 + 2 = b + 1.$

Neste caso, sendo c = 0 temos a(b+1) = b**!** + 1 , o que implica que b + 1 é um divisor de b**!** + 1, logo pelo teorema de Wilson (b + 1) é um número primo.

F(a,b) fornece todos os números primos:

Seja p um número primo. Pelo Teorema de Wilson:

$\frac{((p-1)!+1)}{p}$ é um número natural e podemos calcular $F\left(\left[\frac{(p-1)!+1}{p}\right], p-1\right)$.

O valor de c é $c = \frac{((p-1)!+1)}{p} \times p - ((p-1)!+1) = 0$.

Logo segue $F\left(\left[\frac{(p-1)!+1}{p}\right], p-1\right) = (p-1)+1 = p$.

10. TIPOS DE PRIMOS

Existem números primos que possuem nomes especiais. A maioria deles leva o nome de seus descobridores e seguem um modelo para obtê-los. Estas formas foram conseqüência da tentativa de vários matemáticos de se obter uma fórmula, em que se enquadrassem todos os primos, mas como não geravam todos, os primos decorrentes dela acabavam sendo batizados com um nome específico.

10.1. Primos de Fermat

Em 1640, Fermat mostrou que os números $F_n = 2^{2^n} + 1$ são primos para n = 0, 1, 2, 3 e 4, e conjecturou que todo número desta forma é primo, ficando assim conhecidos como os Números de Fermat. Em 1739, cerca de 100 anos mais tarde, Euler demonstrou que a conjectura de Fermat era falsa ao provar que $F_5 = 2^{32} + 1$ ($32 = 2^5$) é divisível por 641. Ainda não se conhece nenhum outro primo de Fermat além dos cinco primeiros (3, 5,17, 257 e 65537), como também não se sabe se o número de primos de Fermat é, ou não infinito. Para os números de Fermat com n ≥ 9, não existe fatoração completa, mas são conhecidas as fatorações de F_6 (em 1880), F_7 (em 1971) e F_8 (em 1981).

Os números de Fermat aparecem também na Geometria, através de um resultado obtido por Gauss em 1796 com apenas 19 anos de idade. Gauss provou que um polígono regular de **n** lados é construtível, com régua e compasso, se e somente se, **n** é um número natural da forma $n = 2^k \times p_1 \times p_2 \ldots \times x \ldots p_r$, com k ≥ 0, e cada p_i primo de Fermat, isto é, $p_i = 2^{2^{m_i}} + 1$, com $m_i \geq 0$, e p_1, p_2, ..., p_r são primos de Fermat distintos. Com isso, é muito provável que só existam 5 polígonos de lados

ímpares construtíveis com régua e compasso, pois até o momento só são conhecidos 5 primos de Fermat.

Gauss tinha tanto orgulho de sua descoberta, e não era para menos, pois resolveu um problema de 2000 anos, que o pedestal de sua estátua em Gottingen tem o formato de um polígono regular de 17 lados. O mais fantástico desta história é o fato que os números primos ajudaram a resolver um problema de construção geométrica que desafiava os matemáticos desde a antiguidade.

10.2. Primos de Mersenne

Os primos de Mersenne tem relação com os números perfeitos. Um número se diz perfeito, se a soma dos seus divisores próprios é igual a si mesmo. Por exemplo, 6 é perfeito, pois d(6) = 1 + 2 + 3 = 6, como também 28 é perfeito, pois d(28) = 1 + 2 + 4 + 7 + 14 = 28. Os números perfeitos já eram conhecidos pelos gregos, que além do 6 e do 28, tinham conhecimento do 496 e 8128. Dezessete séculos mais tarde foi descoberto o 5º número perfeito: 33.550.336. Sempre que se descobre um primo da forma $2^n - 1$ pode-se gerar um número perfeito par multiplicando-o por 2^{n-1}. Os números $m_q = 2^q - 1$ (com **q** primo) são chamados números de Mersenne (Marin Mersenne, 1588 – 1648). $m_q = 2^q - 1$

Euclides, no livro IX do *Elementos*, demonstrou que qualquer número da forma $2^{n-1} \times (2^n - 1)$ é par perfeito, se e somente se, $2^n - 1$ for primo.

Demonstração:

Seja d(N) a função que fornece a soma dos divisores de um inteiro N. Se N for primo d(N) = N + 1.

Se p é primo e n qualquer inteiro positivo, então:

$d(p^n) = \frac{p^{n+1} - 1}{p - 1}$ (Soma de uma PG de razão **p**).

Se N for composto temos $N = p^n q^m$..... e teremos $d(N) = d(p^n.q^m.....) = d(p^n) x d(q^m)$....., ou seja a função d(N) é multiplicativa.

Exemplo: $d(60) = d(2^2 \times 3 \times 5) = d(2^2) \times d(3) \times d(5) = 168$

De fato, d(60) = 1 + 2 + 3 + 4 + 5 + 6 + 7 + 10 + 12 + 15 + 20 + 30 + 60 = 168

No caso de números perfeitos d(N) = 2N, a conclusão é imediata, pois se N é perfeito, a soma de seus divisores é N, então d(N) = N + N = 2N.

(=>) Se $2^n - 1$ é primo, então $2^{n-1} (2^n - 1)$ é par perfeito.

$N = 2^{n-1}(2^n - 1)$, então $d(N) = d(2^{n-1}) (2^n - 1 + 1) = (2^n - 1) 2^n = (2^n - 1) 2^{n-1} \times 2 = 2N$ => N é perfeito.

(<=) N é par perfeito então $N = 2^{k-1} \times ak \geq 2$

$d(N) = d(2^{k-1} \times a) = d(2^{k-1}) \times d(a) = (2^k - 1) \times d(a)$

mas N é perfeito, então $d(N) = 2N = 2^k \times a$

$2^k \times a = (2^k - 1) \times d(a)$ => $2^k - 1$ divide a => $a = (2^k - 1) \times c$

$2^k (2^k - 1) \times c = (2^k - 1) \times d(a)$ => $2^k \times c = d(a)$

a e c são divisores de a, sabemos que:

$2^k \times c = d(a) \geq a + c = 2^k \times c$ => $d(a) = a + c$

Isto significa que **a** é primo, pois só tem 2 divisores: o 1(um) e $2^k - 1$. Logo, $2^k - 1$ é um primo.

A demonstração é válida somente para os números perfeitos pares, pois os perfeitos ímpares até hoje não foram encontrados. A existência de um número perfeito ímpar é um dos mais antigos problemas matemáticos ainda sem solução. Caso eles existam o limite inferior é 10^{300}, ou seja, é um número de grandeza cósmica, resultado obtido em 1993 pelos matemáticos Brent, Cohen e Te Riele. O

mais provável é que eles não existam mesmo, embora nada de concreto tenha sido obtido até o momento.

O maior primo conhecido é um primo de Mersenne: $\mathbf{2^{24.036.583} - 1}$, um gigante com mais de sete milhões de dígitos. Esse número foi achado em maio de 2004 pelo norte-americano Josh Findle. O número é conseqüência do Projeto **GIMPS** (Great Internet Mersenne Prime Search) um conjunto de mais 200 mil micros colaboradores, que juntos atingem velocidade comparável ao do TERASCALE, o mais poderoso supercomputador do mundo, que custa 45 milhões de dólares. O computador de Findley gastou 14 dias analisando o número. Depois, dois membros independentes do GIMPS verificaram a descoberta na França e na Alemanha. A corrida pela obtenção de primos ainda maiores continua, existindo prêmios para quem os descobrir. A Eletronic Frontier Foudation (Fundação Fronteira Eletrônica), dos Estados Unidos, prometeu dar US$ 100 mil para quem descobrir um número primo com 10 milhões de dígitos e prêmios maiores para números com 100 milhões de dígitos e com 1 bilhão de dígitos. Este prêmio acaba atingindo dois objetivos, estimula a pesquisa matemática, ao mesmo tempo em que testa o comportamento do software e hardware no campo novo da computação distribuída.

Os primos de Mersenne em pouco tempo revolucionaram a computação. Hoje em dia existem dezenas de projetos de computação distribuída por todo o mundo com finalidades diversas, baseados no modelo do pioneiro GIMPS. Qualquer pessoa, sem qualquer formação científica, sem distinção de raça, religião ou localização, através do seu computador doméstico, pode participar de forma decisiva para o progresso de uma investigação científica. Existem inúmeros, tais como: AIDS, Mal de Alzheimer, clima global, descoberta de vida extraterrestre, vacina contra gripe, Robótica, Problemas de matemática, Estrutura tridimensional das proteínas

mapeadas pelo projeto Genoma, drogas contra a leucemia, drogas contra o bacilo do Antraz, etc. A maioria destes projetos são causas nobres de apelo humanitário que visam melhorar a condição de vida do homem.

Decorridos mais de trezentos e cinqüenta anos após a sua morte, o padre Mersenne e as suas conjecturas sobre os números primos motivaram a criação do projeto GIMPS, que serviu como inspiração para a criação de outros similares de perspectivas bastante promissoras para a humanidade.

10.3. Primos de Sophie Germain

$2p+1$

No início do século XIX o Último Teorema de Fermat era o mais famoso problema da teoria dos números. Muitos matemáticos, inclusive Euler, tinham fracassado ao tentar demonstrá-lo gerando um certo desânimo. Todavia, uma descoberta de Sophie fez com que os matemáticos retomassem a busca pela demonstração. O teorema enunciado por Sophie diz que **"**se p é um primo de modo que 2p + 1 também seja primo, então não existem inteiros x, y e z, diferentes de zero e não múltiplos de p, tais que $x^p + y^p = z^p$". Os números p tal que 2p + 1 é primo são conhecidos como os primos de Sophie Germain. Esse resultado causou um choque no estudo do Último Teorema de Fermat e era superior aos obtidos pelos matemáticos da época.

O choque não foi apenas matemático, mas social também, pois Sophie teve que adotar um pseudônimo masculino – Antoine August Le Blanc – para ser aceita pelos matemáticos. Naquela época a sociedade era patriarcal, preconceituosa e discriminava as mulheres que mostravam talento em alguma área, principalmente na de exatas. Dentre todos os países europeus, a França era o mais reticente na

aceitação de mulheres instruídas, pois os franceses achavam a matemática inadequada para as mulheres, já que ela estaria além de sua capacidade mental. A única mulher que conseguiu durante os séculos XVIII e XIX furar este bloqueio intelectual e se tornar uma grande teórica dos números foi Sophie Germain. Durante muito tempo Sophie Germain se correspondeu com Gauss usando o pseudônimo masculino. Porém, em 1807 ela revelou sua identidade e Gauss, ao invés de ficar zangado escreveu-lhe uma carta encantadora. Outro grande matemático da época que a apoiou foi Lagrange que se tornou seu amigo e mentor.

O maior primo de Sophie Germain conhecido foi obtido em 2003, $2540041185 \times 2^{114729} - 1$ que possui 34.547 algarismos. Acredita-se que os primos de Sophie sejam infinitos, mas a demonstração será tão difícil quanto a de mostrar que os primos gêmeos são infinitos.

10.4. Primos Gêmeos

Primos gêmeos são os números primos tais que dado um primo p, p + 2 também será primo. Os primos gêmeos formam pares, como por exemplo (3, 5), (5, 7), (11, 13), (17, 19), (71, 73), (1.000.000.000.061, 1.000.000.000.063), (10.006.427, 10.006.429), (824.633.702.441, 824.633.702.443). Os matemáticos acreditam que o seu número seja infinito, mas ninguém até agora conseguiu provar. A um nível mais profundo, ninguém encontrou uma forma fácil de prever a que distância de um número primo estará o próximo.

Em 1919, o matemático norueguês Viggo Brun demonstrou um resultado curioso: a soma dos inversos dos primos gêmeos é finita. Mas deste resultado não se conclui nada, pois podemos ter um número infinito e a série convergir.

O valor dessa soma é conhecido como a constante de Brun. O resultado mais recente sobre esta constante é de 1998 obtida por Nicely, ou seja:

$$\sum\left(\frac{1}{p}+\frac{1}{p+2}\right)=\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+.....=1{,}902160518\,23$$

Os primos gêmeos ajudaram a derrubar um gigante da eletrônica industrial. Em 1993, Thomas Nicely professor de matemática de uma instituição privada em Lynchberry, tentando melhorar o cálculo da soma de Brun através da utilização de cinco computadores 486 e um Pentium, obteve resultados diferentes nas duas máquinas. O resultado do 486 estava de acordo com os resultados publicados, mas o do Pentium, não. Após inúmeras verificações se conseguiu localizar o problema. O Pentium que a Intel garantia dar 19 casas decimais corretas em cálculos matemáticos, dava apenas 9, um erro 10^{10} vezes superior ao anunciado. Nicely então comunicou o fato a Intel, mas é ignorado, o que o leva a pedir ajuda a outros matemáticos. No entanto, a notícia se espalha pela internet e o bug é confirmado por dezenas de pessoas.

A partir daí, a onda cresce com a notícia chegando nas TVs. A Intel recebe uma chuva de reclamações dos seus clientes, mas ainda continua a não dar satisfações, até que a IBM (outra gigante da eletrônica) anuncia que vai deixar de comercializar PCs com Pentium. A Intel ameaça processá-la, mas a sua credibilidade já estava muito baixa. A cotação das suas ações despencam nas Bolsas de Valores, o que a leva admitir finalmente o erro e propor a substituição de todos os Pentium que tinham o bug.

Passado este episódio, a Intel lança no mercado o Pentium II, III e IV sem bugs, reconquistando a confiança e a posição no mercado para a felicidade dos seus acionistas, que certamente nunca mais querem ouvir falar de primos quanto mais gêmeos.

Os maiores primos gêmeos conhecidos foram obtidos em 2002 cada um contendo 51.090 algarismos: $33218925 \times 2^{169690} \pm 2$.

11. A DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

A principal motivação dos matemáticos na corrida de obtenção de fórmulas ou funções que forneçam todos os números primos, sempre tem o objetivo também de descobrir uma certa regularidade na sua distribuição e com isso poder afirmar a existência de números primos, e até mesmo localizá-los, quando é fornecido um intervalo de números inteiros para investigação.

Primeiro, Legendre, e depois Gauss conjecturaram que o número de primos $\pi(n)$ menores ou igual a um determinado n (natural) podia ser aproximado pela função $\frac{n}{\log n}$, e que essa aproximação seria tento melhor quanto maior fosse n. Essa conjectura iria ser demonstrada quase um século mais tarde por Jacques Hadamard e Charles De La Vallée Poussin que trabalhando de forma independente enunciaram o Teorema dos Números primos:

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\log n}} = 1$$

O aparecimento do log pode ser notado ao se montar uma tabela que consta os valores de n, π (n) e a razão $\frac{n}{\pi(n)}$.

n	π (n)	$\frac{n}{\pi(n)}$
10	4	2,5
100	25	4,0
1000	168	6,0
10000	1.229	8,1
100.000	9.592	10,4
1.000.000	78.498	12,7
10.000.000	664.579	15,0
100.000.000	5.761.455	17,4
1.000.000.000	50.847.534	19,7
10.000.000.000	455.052.512	22,0

Observando a tabela vemos principalmente que a partir de $n = 10^4$ que ao passarmos para a potência seguinte, a razão $\frac{n}{\pi(n)}$ cresce aproximadamente de 2,3. Mas 2,3 é aproximadamente igual ao $\log_e 10 = 2{,}30258...$ e daí, "parece" que até 10^n, 1 em cada $2{,}3\ n = \ln\ 10^n$ é primo . Voltando ao teorema, para N suficientemente grande ($N = 10^n$), temos :

$$\frac{\frac{\pi(N)}{N}}{\frac{}{\ln\ N}} \approx 1 \Rightarrow \frac{\pi(N)}{N} \approx \frac{1}{\ln\ N}$$

Mas $\ln\ N = n\ \ln\ 10 = 2{,}3\ n$. Em outras palavras, podemos pensar que a densidade média dos números primos em um intervalo de 1 até $N = 10^n$ é igual $\frac{1}{\ln\ N} = \frac{1}{2{,}3\ n}$. Disso, o que tiramos concretamente é que à medida que N cresce os números primos vão se tornando mais raros, pois a sua densidade diminui.

É importante frisar que a densidade é *média* , porque existe a possibilidade de ocorrer concentrações de primos em alguns lugares e a ausência deles em outros. A ausência é mais fácil de mostrar sendo estes intervalos denominados de *desertos* de primos. Um exemplo de intervalo que seja um deserto de primos é o (n! + 2, n! + n), pois n! + 2 é divisível por 2, n! + 3 é divisível por 3, ..., n! + n é divisível por n. Neste intervalo existem n – 1 números compostos e consecutivos. Como n é arbitrário, podemos criar um deserto de primos tão grande quanto quisermos. Se escolhermos n = 10, teremos 9 números compostos e consecutivos, se n = 100 teremos 99 números compostos e consecutivos, se n = 1.000.001 teremos 1 milhão de números compostos e consecutivos !

Diante disso, podemos supor que a densidade média dos números primos tende a zero, já que eles vão ficando em média, cada vez mais raros quanto maiores forem e o intervalo entre números primos consecutivos cresça de acordo com o crescimento dos números. Todavia, existe um pequeno detalhe, que são os primos gêmeos, que tudo leva a crer , embora não tenha sido demonstrada, a existência de infinitos pares. Neste caso, o intervalo é pequeno e os números imensos, o que nos mostra mais uma vez o quanto os primos são perseverantes em esconder a regra da sua distribuição, caso ela exista.

Com o avanço computacional foi possível mostrar que a razão $\frac{n}{\ln(n)}$ é uma aproximação simples para $\pi(n)$ por ela não ser muito exata. Sendo assim, tem-se procurado obter funções que melhorem a aproximação para diminuir o erro entre os valores constatados e os estimados pelas funções. Estas funções se utilizam de fórmulas assintóticas que fornecem uma quantidade de números abaixo de um número inteiro n arbitrariamente grande. Quanto maior for o n mais exata se torna a estimativa, ou seja, em outras palavras, o erro relativo diminui e com isso a estimativa e o valor real se tornam “assintoticamente” próximos, isto é, convergem. Atualmente, a função que fornece a melhor aproximação para $\pi(n)$ é a função **R(n)**:

$$R(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k(k+1)} \times \frac{(\log n)^k}{k!} \times \frac{1}{f(z)}$$

Onde **f(z)** representa a famosa função Zeta de Riemann:

$$f(z) = 1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + ...$$

A seguir é apresentada uma tabela que mostra como é boa a aproximação entre $\pi(n)$ e **R**(n).

n	π(n)	R(n)
100.000.000	5.761.455	5.761.552
200.000.000	11.078.937	11.079.090
300.000.000	16.252.325	16.252.355
400.000.000	21.336.326	21.336.185
500.000.000	26.355.867	26.355.517
600.000.000	31.324.703	31.324.622
700.000.000	36.252.931	36.252.719
800.000.000	41.146.179	41.146.248
900.000.000	46.009.215	46.009.949
1.000.000.000	50.847.534	50.847.455
10.000.000.000	455.052.511	455.050.683
100.000.000.000	4.118.054.813	4.118.052.495
1.000.000.000.000	37.607.912.018	37.607.910.542

Como vimos, a função é uma aproximação para $\pi(n)$ já que o surgimento dos primos é irregular não obedecendo a nenhuma lei conhecida. Os pares de primos gêmeos são um exemplo de como será difícil um enquadramento regular. De qualquer forma, alguma ordem tem sido possível colocar no caos. Com o avanço dos métodos computacionais e da necessidade de criação de códigos criptográficos cada vez mais seguros, muitas pesquisas estão em andamento, o que significa que poderemos ter em breve novidades em relação aos números primos.

12. CRIPTOGRAFIA: A APLICAÇÃO MAIS IMPORTANTE DOS PRIMOS

Criptografia é a ciência de esconder o significado de uma mensagem, a palavra tem origem grega (Kripto = escondido, oculto). Ela consiste em codificar informações, usando-se uma chave, antes que sejam transmitidas, e em decodificá-las, após a recepção. O principio básico da criptografia é encontrar uma transformação (função) injetiva f entre um conjunto de mensagens escritas em um determinado alfabeto (letras, números) para um conjunto de mensagens codificadas. Como f é inversível existe a garantia de o processo ser reversível, o que vai possibilitar a revelação das mensagens pelos destinatários. O grande segredo da criptografia está justamente em esconder de maneira eficiente o processo (chave) para a inversão de f. Abaixo temos um diagrama que ajuda a entender a idéia do processo criptográfico:

Aqui podemos dar um exemplo didático acessível para alunos do primeiro ano do ensino médio, se bem que é possível aplicá-lo até em turmas do ensino fundamental já que não é preciso necessariamente o professor utilizar a noção de função.

Para começar criamos uma tabela que relaciona números com letras do nosso alfabeto:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	....
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	....

Agora, escolhemos uma função f que vai receber o valor da letra que queremos transmitir e gerar um outro valor através de f. Ou seja, a imagem de f é que será transmitida. Vamos supor que f seja a função $f(x)=3x+5$, que é também chamada de função cifradora. O emissor vai transmitir a palavra MONOGRAFIA. Então, conforme a tabela acima temos a seguinte correspondência:

M = 13, $\Rightarrow$ f(M) = f (13) = **31**

O = 15, $\Rightarrow$ f(O) = f (15) = **50**

N = 14, $\Rightarrow$ f(N) = f (14) = **47**

O = 15, $\Rightarrow$ f(O) = f (15) = **50**

G = 7, $\Rightarrow$ f(G) = f (7) = **26**

R = 18, $\Rightarrow$ f(R) = f (18) = **59**

A = 1, $\Rightarrow$ f(A) = f (1) = **8**

F = 6, $\Rightarrow$ f(F) = f (6) = **23**

I = 9, $\Rightarrow$ f(I) = f (9) = **32**

A = 1, $\Rightarrow$ f(A) = f (1) = **8**

A palavra M O N O G R A F I A ao passar pela função cifradora será transformada na seqüência de números 31 50 47 50 26 59 8 23 32 8, que é a mensagem que o receptor receberá.

O receptor ao receber a mensagem codificada (seqüência numérica), realizará a operação inversa $f^{-1}(x)=\frac{x-5}{3}$. Por exemplo, o receptor recebeu **8**, $f^{-1}(8)=\frac{8-5}{3}=1=f(1)=f(A)$, logo **8** (destino) = **A** (origem), e assim sucessivamente até recompor totalmente a mensagem original.

Acima demos um exemplo didático visando entender o princípio fundamental da criptografia. Embora seja simples, é possível compreendermos que sem o

conhecimento das chaves f e f^{-1} não é possível descobrir a mensagem que foi trocada entre o emissor e o receptor. É esta dificuldade que vai garantir o sigilo da informação. Neste caso, as nossas chaves eram funções afins que podem ser facilmente descobertas, mas se as chaves fossem matrizes invertíveis a violação ficaria mais difícil, pois achar a inversa de uma matriz mesmo para computadores não é tarefa fácil. No entanto, na realidade esses métodos não são utilizados pois os usuários (receptor/emissor) tem conhecimento prévio das chaves, o que é inconveniente. Por isso, são inviáveis para as transações eletrônicas, onde um único receptor recebe dados de milhares de emissores, como por exemplo: vendas pela internet, operações bancárias, cartões de crédito, etc. Nestes casos mais complexos e de grande demanda, a Teoria dos Números, então esquecida, foi resgatada acabando por fornecer armas poderosas para a proteção destas transações.

Os dados confidenciais na Internet ou nas comunicações bancárias, são transmitidos em cifra pelas redes públicas, sendo codificados na partida e decodificados na chegada. Isso não é novidade. Desde Júlio César (imperador de Roma) que dados militares são transmitidos também desta forma. Um dos episódios mais famosos da 2ª Guerra Mundial foi a quebra pelos Aliados da máquina *Enigma* utilizada pelos nazistas, façanha que contribuiu para o sucesso da invasão da Normandia em 1944.

O sistema clássico de criptografia, em que uma chave secreta é conhecida tanto pelo emissor quanto pelo receptor é muito vulnerável, pois ela tem que ser transmitida de forma independente da mensagem. Em 1976, uma idéia nova surgiu na criptografia: a chave pública. A idéia é a seguinte: no lugar de uma chave secreta, de posse tanto do emissor como do receptor, temos duas chaves. Uma delas sendo pública, disponível para qualquer pessoa, que serve apenas para codificar a

mensagem, mas não para a decodificar, e uma segunda, privada, de posse apenas do receptor, que serve para decodificar a mensagem. O emissor codifica a mensagem com a chave pública e a transmite. O receptor decodifica com a privada. Mesmo que alguém intercepte a mensagem, não saberá qual a chave privada, pois esta não será transmitida a ninguém. Se for impossível reconstruir a chave privada a partir da pública, o código é inviolável.

Esta idéia se concretizou em 1977, através de **R**ivest, **S**hamir e **A**dleman do Instituto Tecnológico de Massachuchets que criaram o algoritmo **RSA**. É o mais utilizado atualmente, possui patente e a exportação de produtos que o utilizam é controlado rigidamente pela área militar do governo americano. Este processo é apenas teoria dos números aplicada, compondo seu eixo central, o algoritmo de fatoração de Euclides, um Teorema de Euler do século XVIII e o pequeno Teorema de Fermat.

Vamos mostrar de uma forma simples como o sistema funciona. Suponhamos que você possua um cartão de crédito de banda VISA e esteja realizando uma compra pela Internet e a central de cartões precise da informação da banda para autorizar a transação. O V é 22ª letra do alfabeto, o I é a 9ª , o S é a 19ª e o A é a 1ª. A chave pública **C**, e o número **N** são disponibilizados para o público pela central dos cartões. Todavia, somente a central tem a chave secreta **S**. Além disso, C, N e S tem que satisfazer as seguintes condições:

a) **N** = p x q p e q números primos;

b) C x **S** – 1 tem que ser divisível pelo produto (p – 1) (q – 1);

c) S e (p – 1) (q – 1) tem que ser primos entre si.

Adotando N = 26, C = 5 e S = 17 verificamos que as condições a, b e c são satisfeitas:

26 = 2 x 13 2 e 13 são primos

5 x 17 – 1 é divisível por 12 = (2 – 1) (13 – 1)

17 e 12 = (2 – 1) (13 – 1) são primos entre si, MDC (17,12) = 1

O usuário tem a chave pública C e N e inicia a transmissão pela letra V que é a 22ª letra do alfabeto, fazendo a seguinte transformação: 22 em "22^{5} mod 26", em outras palavras: achar o resto da divisão de 22^{5} por 26 que é igual a 16, r = 16 => $22^{5} \equiv 16 \pmod{26}$. Portanto, o usuário transmite 16.

A central de posse da chave secreta S = 17 calcula 16^{17} mod 26, que dá 22 ficando ciente que a letra transmitida foi V que é a 22ª letra do alfabeto.

Em resumo, o transmissor codifica o número $\underline{\alpha}$ a ser transmitido em $\underline{\beta}$ através da transformação $\beta \equiv \alpha^{C} \pmod{N}$. O receptor ao receber β calcula $\gamma \equiv \beta^{S} \pmod{N}$. Se N, C e S satisfazem as condições a, b e c então γ = α. Este resultado é garantido pelo Teorema de Fermat e pelo Teorema de Euler.

Fazendo para I, temos que I é a 9ª letra do alfabeto, logo fica assim:

Usuário : α = 9 => $\beta \equiv 95 \pmod{26}$ => β = 3

Central: β = 3 => $\gamma \equiv 3^{17} \pmod{26} = \alpha$

=> $\gamma \equiv 9 \pmod{26} = \alpha$

=> α = 9

Da mesma forma fazemos com o S e o A.

A segurança deste processo poderia ser questionada já que a chave pública e o N são conhecidos. Aquilo que alguém mais interessado pode fazer é fatorar N nos seus fatores p e q, calculando S a partir de C (condição b). Mas nisto é que reside o problema. Os números p e q são apagados no computador, após o cálculo da chave secreta. Fatorar um número é muito mais difícil do que multiplicar. Multiplicar dois números de 100 algarismos é trivial para o computador. No entanto, fatorar um

número de 200 algarismos é difícil até de imaginar. Se os números forem bem escolhidos, seriam necessárias 10^{80} tentativas, número que traduz o número de partículas do Universo !

Atualmente, para importantes transações bancárias N gira em torno de 300 algarismos. Mesmo se colocássemos em rede toda a produção anual mundial de micros, algo em torno de 100 milhões, eles levariam mais de 1.000 anos para quebrar N. Com valores cada vez maiores para p e q, a criptografia baseada no RSA é inviolável. A razão é que o tempo necessário para a multiplicação de dois números cresce de acordo com um polinômio, que é mais devagar, enquanto que o tempo para fatorar um número cresce de forma exponencial. Ainda estamos muito longe de produzir algoritmos de fatoração rápidos capazes de ameaçar a criptografia baseada nos números primos. Esta questão é de tamanha seriedade, que muitas das pesquisas científicas em teoria de números realizada nos Estados Unidos tem que passar pelo crivo do Departamento de Defesa, que decide o que é publicável e o que deve permanecer secreto.

No ano de 2002 três matemáticos indianos descobriram um algoritmo de primaridade, que informa se um dado número é primo ou não. Essa descoberta divulgada pela imprensa (o que despertou o nosso interesse pelos números primos) causou uma preocupação mundial devido os códigos criptográficos utilizarem os números primos. Até então, nenhum dos algoritmos utilizados demorava um tempo polinomial como é o dos indianos. No entanto, a criptografia não depende somente de saber se um número é primo ou não, mas do conhecimento dos fatores primos de números gigantescos, que é um problema quase insolúvel. Daí, podemos compreender a corrida por números primos cada vez maiores. Imagine fatorar um número N que seja o produto de dois primos de Mersenne mantidos em segredo!

13. OUTRAS ÁREAS EM QUE OS PRIMOS APARECEM

13.1. Astronomia (Mensagens ao Espaço)

Os números primos existem em qualquer sistema de numeração. Isso nos faz acreditar na sua universalidade. A chave do filme *Contacto*, baseado no romance de mesmo nome do astrônomo Carl Sagan, no qual extraterrestres chamam a atenção dos terrestres enviando sinais de rádio com número primo de impulsos, é um exemplo de que os números primos não habitam somente as cabeças dos matemáticos.

O homem possui dez dedos, por isso o nosso sistema numérico é baseado em dez algarismos (base decimal). Os computadores usam o sistema binário (base 2) e hexadecimal (base 16). Os Babilônicos tinham um sistema de base 60 (60 segundos em um minuto, 60 minutos em uma hora). Em todos estes sistemas existem também números primos. Se existirem extraterrestres certamente possuem um sistema de numeração, mas quantos dedos possuem, só Deus sabe.

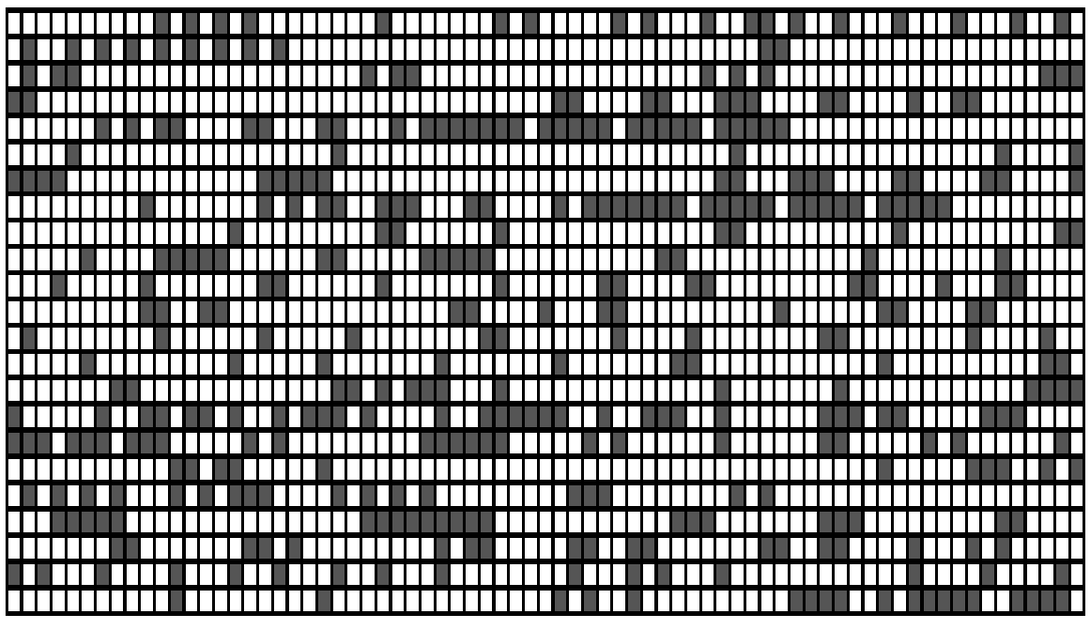
Essa tentativa de estabelecer contato acontece também na vida real. Em 1974 uma mensagem da Terra foi transmitida ao espaço. Uma equipe liderada pelo astrônomo Frank Drake, transmitiu do rádio telescópio de Arecibo (Porto Rico) durante 169 segundos (13^2) a seguinte mensagem no sistema binário:

(*a seqüência foi colocada na folha seguinte por ser grande e não caber nesta folha*)

00000010101010000000000001010000010100000001001000100010001
00101100101010101010101010010010000000000000000000000000000
00000000011000000000000000000011010000000000000000000110100
00000000000000001010100000000000000000011111000000000000000
00000000000000000110000111000110000110001000000000000011001
00001101000110001100001101011111011111011111011111000000000
00000000000000001000000000000000001000000000000000000000000
00000100000000000000001111110000000000001111100000000000000
00000000000110000110000111000110001000000100000000010000011
01000011000111001101011111011111011111011111000000000000000
00000000001000000110000000001000000000001100000000000000001
00000110000000000111111000001100000011111000000000011000000
00000001000000001000000001000001000000110000000100000001100
00110000001000000000110001000011000000000000000011001100000
00000001100010000110000000011000011000000100000001000000 1
00000000100000100000001100000000100010000000011000000001000
10000000001000000010000010000000100000001000000010000000000
00110000000001100000000110000000001000111010110000000000010
00000010000000000000010000011111000000000000100001011101001
01101100000010011100100111111110111000011100000110111000000
00101000001110111001000001110111001000000101000001111110010 00
00010100000110000001000001101100000000000000000000000000000
00000011100000100000000000000111010100010101010101001110000
00000101010100000000000000000010100000000000000111110000000
00000001111111110000000000001110000000111000000000110000000
00001100000001101000000000101100000110011000000011001100001
00010100000101000100001000100100010010001000000001000101000
10000000000001000010000100000000000010000000001000000000000
00100101000000000001111001111101001111000

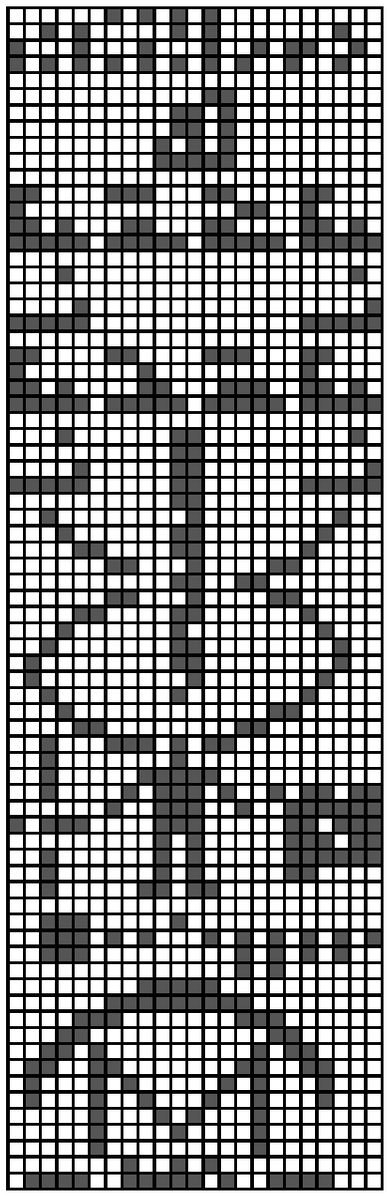
Essa seqüência binária foi transmitida na direção de um conglomerado de 300 mil estrelas, algumas com planetas em órbita. Esta seqüência consistia de 1679 bits (0 ou 1). Mas por que este número? temos uma seqüência contínua de binários. Podemos arrumar estes números em matrizes de diversos tamanhos e tentar formar algo com algum significado. Se a mensagem tivesse, por exemplo, 1000 bits, algumas opções seriam: 10 x 1000, 50 x 20, 25 x 40, etc... Mas, no caso de 1679 só temos duas matrizes possíveis: 23 x 73 ou 73 x 23, sendo que 23 e 73 não podem mais ser fatorados, pois são primos.

Bem, agrupando esses números em 23 linhas com 73 bits, ou seja, uma matriz (23 x 73), ou a sua transposta (73 x 23). Se, representarmos o 1 por um ponto escuro e 0 por um ponto claro, teremos a seguinte figura numa matriz 23 x 73:



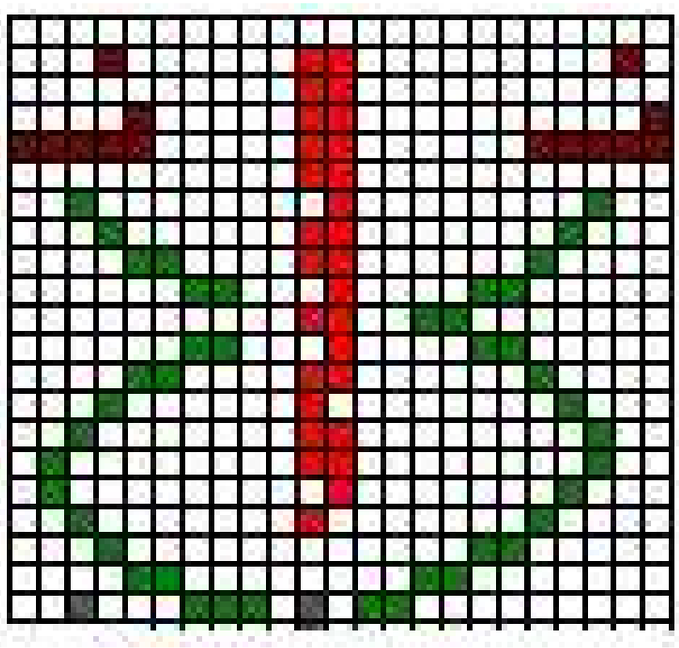
A figura anterior obtida não transmite nenhum significado. Porém, se usarmos a transposta e o 1 permanecendo como um ponto escuro e o 0 como um ponto claro, obteremos a seguinte figura:

(*a figura foi colocada na folha seguinte por ser grande e não caber nesta folha*)

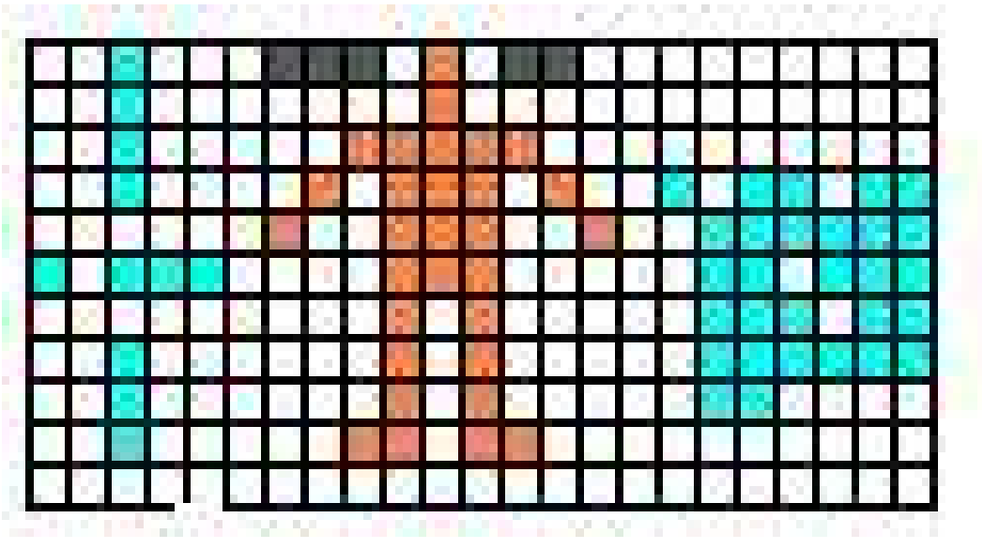


Com exceção da figura de um homem, o resto da figura é de difícil definição. Todavia, o astrônomo Carl Sagan decifrou a mensagem quase toda. Neste trabalho, vamos apresentar o significado de algumas partes da figura.

(*a figura foi colocada na folha seguinte por ser grande e não caber nesta folha*)

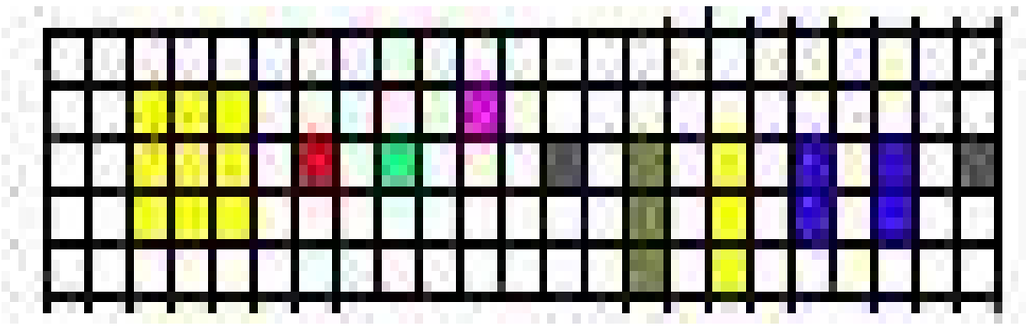


Esta figura representa a estrutura helicoidal do nosso DNA.

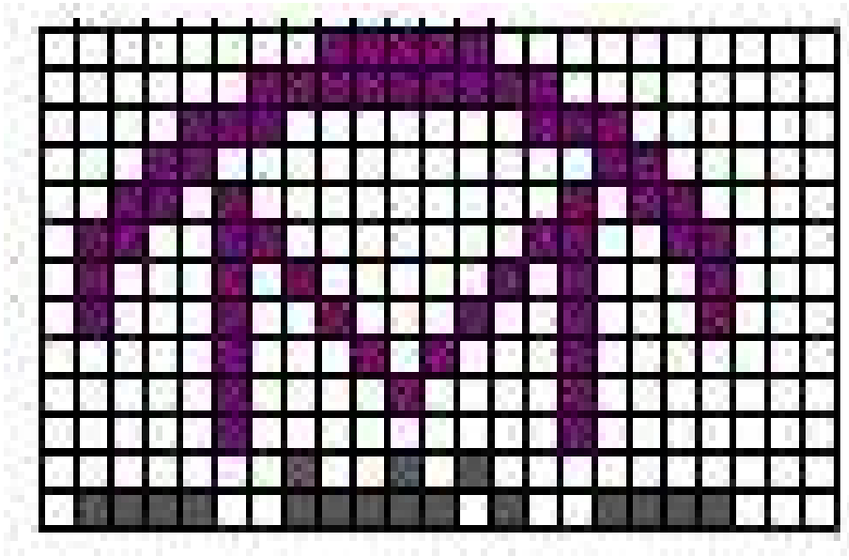


Vindo abaixo da forma estrutural do DNA vem a figura de um ser. Este ser tem relação com a molécula.

(*a figura foi colocada na folha seguinte por ser grande e não caber nesta folha*)



Logo abaixo está uma representação do nosso sistema solar com o terceiro planeta (Terra – cor magenta) mais próxima do ser humano. A figura pretende dar uma idéia dos tamanhos dos corpos celestes do sistema Solar.



No final da mensagem, este diagrama representa a antena de Arecibo utilizada.

Decorridos quase 30 anos do envio desta mensagem, até o momento não sabemos se alguém respondeu ou não, mas o 23 e o 73 continuarão sua viagem tentando encontrar seus respectivos primos, seja qual for a base adotada pelos nossos supostos vizinhos.

13.2. Primos na Biologia

Sabemos da complexa cadeia alimentar existente na natureza, tanto no reino animal como no vegetal. Qualquer organismo para sobreviver necessita de se alimentar de nutrientes para manter seu sistema biológico funcionando. Toda espécie de certa forma depende de outra, sendo comum a adoção do ato predatório para se obter o alimento. Por isso, várias espécies adotam mecanismos de defesa para se protegerem dos predadores. Camuflagem, espinhos ou cascas duras são algumas das armas. A lista é enorme, um exemplo da riqueza de estratégias que a natureza pode produzir.

Um inseto da ordem *Orthoptera* que inclui os grilos e gafanhotos, nos fornece uma surpreendente estratégia para se proteger do seu predador, e assim minimizar o impacto da predação sobre sua população objetivando garantir a continuidade da espécie.

A cigarra periódica é a autora da façanha. Elas emergem em ciclos de 13 e 17 anos, não existindo ciclos de 12, 14, 15, 16 ou 18 anos. A opção pelo 13 e 17 tem duas razões: além de serem números primos, são números que excedem em muito a duração de vida dos seus predadores. Muitos predadores têm ciclos de 2 a 5 anos. Se considerarmos um predador de ciclo de vida igual a 5 anos, e se as cigarras aparecessem de 15 em 15 anos, cada explosão reprodutiva será atingida pelo predador. Porém, ao adotar um número primo alto, como por exemplo, o 17, as cigarrras minimizam o número de coincidências, que neste caso ocorrerá somente a cada 85 anos.

Este exemplo mostra que a luta das criaturas pela sobrevivência não fica restrita a exibição de armas. No caso das cigarras, tendo elas adotado um número

primo para o seu ciclo reprodutivo, fica garantida uma população abundante quando seu ciclo coincidir com a do predador. A adoção deste ciclo (13 ou 17) é resultado de processos de adaptação ao ambiente e ao tipo de predador, mas como elas fazem esta contagem ainda é um mistério.

13.3. Primos em Litígio

O algoritmo DECSS que decodifica discos de DVD é considerado ilegal nos Estados Unidos, podendo sofrer sanções penais quem possuir uma cópia dele. Mantendo esta linha de pensamento, fica proibida a posse do seguinte número primo:

4856507896573978293098418946942861377074420873513579240196520736
8698513401047237446968797439926117510973777701027447528049058831
3840375497099879096539552270117121570259746669932402268345966196
0603485174249773584685188556745702571254749996482194184655710084
1190862597169479707991520048667099759235960613207259737979936188
6063169144735883002453369727818139147979555133999493948828998469
1783610018259789010316019618350343448956870538452085380458424156
5482488933380474758711283395989685223254460840897111977127694120
7958624054716132100500645982017696177180947811362200272344827224
9323259547234688002927776497906148129840428345720146348968547169
0823547378356619721862249694316227166639390554302415647329248552
4899122573946654862714048211713812438821771760298412552446474450
5583462814488335631902725319590439283873764073916891257924055015
6208897871633759991078870849081590975480192857684519885963053238
2349058092032999603234471140776019847163531161713078576084862236
3702835701049612595681846785965333100770179916146744725492728334
8691600064758591746278121269007351830924153010630289329566584366
2000800476778967984382090797619859493646309380586336721469695975
0279687712057249966669805614533820741203159337703099491527469183
5659376210222006812679827344576093802030447912277498091795593838
7121000588766689258448700470772552497060444652127130404321182610
1035911864766629638584950874484973734768614208805294 43

conversão para a base 16 não é fácil, sendo somente possível se for utilizado um programa de computador, tendo em vista o tamanho do número.

Outro exemplo polêmico envolvendo números primos, são as chaves de criptografia pública, que são números especiais com centenas de dígitos obedecendo a certas propriedades. Roger Schlafly, um consultor de computação de Santa Cruz, Califórnia (EUA), conseguiu patentear um número primo de 150 dígitos e depois um de 320, já que eles melhoram a performance das repetidas divisões modulares quando se utiliza o sistema Diffie-Hellman de criptografia pública. Nos Estados Unidos, o patenteamento de algoritmos é proibido desde 1972, mas a decisão da Suprema Corte não define o que é um algoritmo matemático, dando margem a decisões controversas a respeito de registros de patentes de software e algoritmos.

14. CONCLUSÃO

Sendo uma notícia de natureza matemática a propulsora deste trabalho, esta acabou por revelar apenas a ponta do iceberg do assunto sobre os números primos. Foi uma pesquisa estimulante apesar da sua extensão. Curiosidades, recordes e um pouco de misticismo numérico são alguns dos seus ingredientes que a tornaram interessante. Dentro do aspecto técnico, ainda restam muitas questões a serem respondidas que ocuparão por muito tempo os matemáticos.

Em termos didáticos a pesquisa mostrou que os números primos não servem apenas para a obtenção do MDC e MMC a partir da fatoração dos números. É possível trabalhar com eles em outras áreas da matemática mostrando também como surgem em outras áreas de conhecimento, de forma natural ou proposital. Com certeza, a abrangência de aplicações incentiva o aprendizado, principalmente quando trabalhamos com jovens ávidos por informações relacionadas à vida moderna onde o conhecimento tecnológico se faz cada vez mais influente.

Observou-se que os resultados mais interessantes e curiosos foram obtidos graças à utilização do computador, um poderoso aliado quando lidamos com números. A parceria entre a matemática e os microcomputadores para pesquisar os números primos inspirou projetos semelhantes ao GIMPS, o que mostra como idéias de cunho matemático influenciaram a criação de projetos de pesquisa para o bem da humanidade, embora nem sempre seja assim. A criptografia protege a privacidade do cidadão comum, como também daqueles que entram nas redes mundiais para cometer atos ilícitos. Esperamos com isso atingir a capacidade de crítica dos alunos para fazê-los perceber a influência da ciência em suas vidas.

Acreditamos ser este trabalho uma demonstração da interação de várias áreas com os números primos, podendo ter tratamento didático compatível e ilustrar uma aula sobre números primos para motivá-la, atitude adotada por muitos professores antes de entrar numa sala de aula independente da sua disciplina.

15. REFERÊNCIAS BIBLIOGRÁFICAS

BOYER, Carl B.: História da Matemática. São Paulo, Editora Edgard Blucher, 1996.

BRITO, Márcia Regina F. : Psicologia da Educação Matemática, Florianópolis, Editora Insular, 2001.

BUESCU, Jorge: O Mistério do Bilhete de Identidade e outras Histórias
Lisboa, Gradiva Editora, Julho 2002.

CONWAY, John H. e **GUY**, Richard K.: O Livro dos Números. Lisboa, Gradiva Editora e Universidade de Aveiro, 1999.

COUTINHO, S.C: Números Inteiros e Criptografia RSA, Rio de Janeiro, Instituto de Matemática Pura e Aplicada,1997.

CUNHA, Marcus Vinicius da: Psicologia da Educação, São Paulo, DP&A Editora, 2000.

DAVIS, Philip J. e **Hersh**, Reuben: A Experiência Matemática. Rio de Janeiro, Livraria Francisco Alves Editora, 1985.

DOMINGUES, Hygino e **IEZZI**, Gelson: Álgebra Moderna. São Paulo, Atual Editora, 1995.

D'AMBROSIO, Ubiratan: Educação Matemática – Da teoria à Prática. Campinas, Papirus Editora, 1996.

GOULD, Stephen Jay: Darwin e os Grandes Enigmas da Vida, Editora Martin Fontes, 1999.

HEFEZ, Abramo: Curso de Álgebra, Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 1993.

LIBÂNEO, José Carlos: Didática, São Paulo, Editora Cortez, 1994.

MILIES, César Polcino e **COELHO**, Sônia Pitta: Números – Uma Introdução à Matemática. São Paulo, EDUSP , 2001.

RIBENBOIM, Paulo: Números Primos: Mistérios e Recordes, Rio de Janeiro, Instituto de Matemática Pura e Aplicada, 2001.

RODRIGUES, Neidson: Da Mistificação da Escola à Escola Necessária. São Paulo, Cortez Editora, Abril de 1987.

SINGH, Simon: O Último Teorema de Fermat. Rio de Janeiro, Editora Record, 1998.

SINGH, Simon: O Livro dos Códigos. Rio de Janeiro, Editora Record, 2002.

SKOVSMOSE, Ole: Educação Matemática Crítica. Campinas, Papirus Editora, 2001.

TENENBAUM, Gerald e **FRANCE**, Michel Mendès: The Prime Numbers and their Distribution. Student Mathematical Library Volume 6. American Mathematical Society. 2001

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 45 – 1º Quadrimestre 2001.

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 41 – 3º Quadrimestre 1999.

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 47 – 3º Quadrimestre 2001

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 13 – 2º Semestre 1998

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 37 – 2º Quadrimestre 1998

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 11 – 2º Semestre 1987

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 19 – 2º Semestre 1991

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 48 – 1º Quadrimestre 2002

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 49 – 2º Quadrimestre 2002

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 50 – 3º Quadrimestre 2002

Sociedade Brasileira de Matemática. **REVISTA DO PROFESSOR DE MATEMÁTICA** Nº 12 – 1º Semestre de 1998

INTERNET:

Disponível em <http://www.educ.fc.ul.pt/> Acesso em 28/08/04

Disponível em <http://www.cic.unb.br/> Acesso em 28/08/04

Disponível em <http://www.inf.aedb.br/> Acesso em 28/08/04

Disponível em <http://www.revistadolinux.com.br> Acesso em 29/08/04

Disponível em <http://www.fourmilab.ch/goldberg/arecibo> Acesso em 28/08/04

Disponível em <http://www.pr.gov.br> Acesso em 29/08/04

Disponível em <http://www.redes.unb.br> Acesso em 29/08/04

Disponível em <http://www.utm.edu/research/primes> Acesso em 29/08/04

Disponível em <http://www.uerj.br/dinfo> Acesso em 28/08/04

Disponível em <http://www.objetivo.com.br> Acesso em 28/08/04

Disponível em <http://www.athena.ufrgs.br> Acesso em 29/08/04

Disponível em <http://www.mersenne.org> Acesso em 28/08/04