Universidade Estadual de Santa Cruz
Departamento de Ciências Exatas e da Terra
Mestrado Profissional em Matemática

Dissertação de mestrado
por

Cediglês lima dos santos

OS NÚMEROS PRIMOS

Orientador: **Prof. Dr. Sérgio Mota Alves**

Ilhéus, 22 de fevereiro de 2014.

Cediglês Lima dos Santos

OS NÚMEROS PRIMOS

Ilhéus
2014

Cediglês Lima dos Santos

OS NÚMEROS PRIMOS

Trabalho de conclusão de curso apresentado ao Curso de Pós-graduação stricto sensu nível mestrado profissional em matemática do departamento de ciências exatas e da terra-DCTE da Universidade Estadual de Santa Cruz-UESC , como requisito para obtenção do título de mestre profissional em matemática.

Orientador: Prof. Dr Sérgio Mota Alves

Universidade Estadual de Santa Cruz
Departamento de Ciências Exatas e da Terra

Ilhéus
2014

CEDIGLÊS LIMA DOS SANTOS

OS NÚMEROS PRIMOS

Trabalho de conclusão de curso apresentado ao Curso de Pós-graduação stricto sensu nível mestrado profissional em matemática do departamento de ciências exatas e da terra-DCTE da Universidade Estadual de Santa Cruz-UESC , como requisito para obtenção do título de mestre profissional em matemática.

Aprovad em Ilhéus._____de_____de 2014.

COMISSÃO EXAMINADORA

Prof. Dr. Sérgio Mota Alves
Universidade Estadual de Santa Cruz-UESC
Orientador

Prof. Dr. Vinicius Augusto Takahashi Arakawa
Universidade Estadual de Santa Cruz-UESC
Co-orientador

Prof. Dr. Fabíolo Moraes Amaral

DEDICATÓRIA

À minha família, em especial, pelo apoio dado, pelo incentivo, dedicação e amor.

AGRADECIMENTOS

A Deus, maior razão da minha existência, agradeço pela oportunidade dada em minha vida de alcançar as minhas metas.

A todos meus colegas de trabalho que de maneira direta ou indireta me incentivaram na caminhada, inclusive os diretores, vice-diretores e coordenadores que flexibilizaram os horários para que eu pudesse fazer este curso.

A todos os colegas de curso e grandes companheiros que fiz durante esses dois anos, em especial os amigos: Emanoel José Cancela, Flávio Oliveira Ribeiro e Jackson Reis por ter participação especial nessa caminhada

Aos meus pais e família, que sempre incentivam-me em toda a minha caminhada acadêmica, valorizando-me sempre.

A todos os Professores destes 4 semestres pelo auxílio e carinho nesse percurso.

Em especial ao meu orientador Prof. Dr Sérgio Mota, pela paciência, colaboração, entusiasmo com o programa e acima de tudo a vontade de ver cada aluno do profmat com o título de mestre.

RESUMO

Este texto relata sobre um dos maiores fascínios matemáticos de todos os tempos, os números primos. Aqui escrevo sobre principais teóricos, fatos históricos, aplicações e outros fatos importantes que considero relevante para o ensino e aprendizagem dos números primos, pois de fato sabe-se da importância destes na teoria dos números e, além disso, o teorema fundamental da aritmética nos afirma que todo número inteiro natural maior que um, se escreve de modo único como produto de números primos. O texto mostra que os números primos são o alicerce no qual se apóia a aritmética, enfatizando que a idéia de número primo é das mais simples, mas também das mais ricas em resultados e aplicações, tanto na própria Matemática como nas ciências e Tecnologia. A principal razão de sua enorme importância reside no fato de que eles funcionam como uma espécie de tijolos com os quais podemos construir, por meio de multiplicação, qualquer outro número natural (exceto os casos triviais n=0 e n=1).

A finalidade do texto não é a pesquisa para encontrar novos números primos, a essência do estudo é tentar explicar a organização desses números e como eles se apresentam, e aborda-lós de forma simples e especial como numa espécie de revista super interessante sobre primos, imaginando que depois da leitura desse trabalho um aluno do ensino básico, seja capaz de ter argumentos para responder perguntas do tipo:

-Quantos são os números primos?

-Como são produzidos?

-Como reconhecer um número primo?

-Pra que servem os números primos?

Existem algumas boas respostas para estas perguntas e algumas outras nos textos abaixo, então agora é só ter paciência e ler todo o conteúdo dissertado.

ABSTRACT

This paper reports on one of the greatest mathematicians of all time fascinations , the prime numbers . Here I write about major theoretical , historical facts , applications and other important facts they consider relevant to the teaching and learning of primes , for indeed we know the importance of these in number theory and, moreover , the fundamental theorem of arithmetic in states that all natural integer greater than one, is written in a unique way as a product of prime numbers. The text shows that the prime numbers are the foundation on which rests the arithmetic , emphasizing that the idea of premier number is the simplest but also the most rich in results and applications both in mathematics itself as the sciences and technology . The main reason of its huge importance lies in the fact that they act as a sort of bricks with which we can build through multiplication, any natural number (except the trivial cases n = 0 and n = 1) .

The purpose of the text is not to find new primes , the essence of the study is to try to explain the organization of these numbers and how they arise, and address them in a simple and special way as a kind of super interesting magazine about cousins imagining that after reading this work a student of basic education , be able to have arguments to answer questions like :

- How many prime numbers ?
- How are they produced ?
- How to recognize a prime number ?
- serving prime numbers ?

There are some good answers to these questions and a few others in the texts below , so now it's just be patient and read the entire contents lectured .

Sumário

Capítulo 1

INTRODUÇÃO

1.1 Justificativa do Tema

Baseando-me no fato de que a maioria dos nossos alunos e as vezes alguns de nós professores termos dificuldades em trabalhar de modo sistemático com este assunto é que estou desenvolvendo este trabalho, ele servirá como fonte de pesquisa sobre fatos históricos e aplicações dos números primos. Justifico este trabalho e sua abordagem no fato de que existem poucas literaturas voltadas ao ensinoo básico que tratam o assunto de modo amplo, aqui escrevo sobre principais teóricos, fatos históricos, aplicações e outros fatos importantes que considero relevante para o ensino e aprendizagem dos números primos.

1.2 Estudo dos números primos

Logo abaixo são apresentadas umas respostas atraentes para as perguntas sobre o estudo dos números primos. Estas respostas foram retiradas da Página dos Números Primos na Internet, página que que leva o nome de página projeto do Instituto de Ciências e Matemática da Faculdade de Ciências da Universidade de Lisboa.

1.2.1 Tradição

Euclides foi provavelmente o primeiro a definir a primalidade dos números no seu livro *Os Elementos*, aproximadamente 300 a.C. O seu objetivo era caracterizar os números perfeitos pares (um número perfeito, é um número cujo resultado da soma dos seus divisores naturais é ele mesmo; por exemplo o número 6 tem como divisores 1, 2, 3 e 1+2+3=6, 28 tem como divisores 1, 2, 4, 7, 14 e 1+2+4+7+14=28) . No entanto apercebeu-se de que os números perfeitos pares (não existem até há data números perfeitos ímpares.) eram todos proximamente relacionados com os números primos da forma $2^n - 1$ para algum número primo p (agora chamados de números de Mersenne). Portanto a procura deste tipo de jóias começou perto de 300 a.C.. Grandes números primos (especialmente desta última forma) foram então estudados (segundo ordem cronológica) por Cataldi, Descartes, Fermat, Mersenne, Frenicle, Leibniz, Euler, Landry, Lucas, Catalan, Sylvester, Cunningham, Pepin, Putnam e Lehmer (para nomear alguns). Como podemos então resistir ao encantamento de nos juntarmos a tal ilustre grupo? Muita da teoria dos números elementar foi desenvolvida enquanto se decidia como se tratar de grandes números, como caracterizar os seus fatores e descobrir de entre os quais, os que eram números primos. Em pouco tempo, a tradição pela procura de grandes números primos tem sido frutuita. É uma tradição bem merecida de ser continuada.

1.2.2 Pelos produtos que advém da procura

Ter sido a primeira nação a pôr o Homem na Lua foi de grande valor político para os EUA, mas o que foi talvez mais valorizado para a sociedade foram os produtos que daí advieram e que melhoraram a nossa vida. Produtos esses como as tecnologias, os materiais, (que foram desenvolvidos pelo Homem, e para o Homem, e que são itens comuns aos nossos dias), e o e o melhoramento das infra-estruturas educacionais (que levaram muitos homens e mulheres a vidas produtivas como engenheiros e cientistas). O mesmo é verdade quando se buscam números primos recordistas, que deixaram como legado alguns dos maiores teoremas da teoria elementar dos números primos, tais como o

pequeno teorema de Fermat, e a reciprocidade quadrática. Mais recentemente a busca de tais primos é ainda usada por professores para motivarem os seus alunos na pesquisa matemática e talvez para os de mover a futuras carreiras nas áreas de ciências e engenharias. E estes são apenas alguns dos produtos que advém desta pesquisa.

1.2.3 As pessoas colecionam itens raros e bonitos

Os números primos de Mersenne, que são nos dias de hoje os maiores números primos conhecidos, são raros e belos. Desde que Euclides iniciou a pesquisa e o estudo de números primos cerca de 300 a.C., que apenas 36 destes números primos foram descobertos. Apenas 36 em toda a História da Humanidade - Isso é raríssimo! Mas são igualmente belos. A Matemática, como todas as ciências, tem uma noção definida do belo. Quais são as qualidades do belo na matemática? Procuram-se demonstrações simples, concisas e claras, e se possível que combinem conceitos iguais anteriores, ou que ensinem algo de novo. Por exemplo, os números primos de Mersenne são de uma única forma possível de números primos $2^n - 1$, a demonstração da sua primalidade é elegante e simples. Os números primos de Mersenne são belos e possuem aplicações surpreendentes.

1.2.4 Pela glória

Porque é que os atletas tentam correr mais rápido do que qualquer outra pessoa, salta mais alto, atirar um peso mais longe? É porque utilizam as técnicas do lançamento no seu trabalho? O mais provável é que seja pelo desejo de competir (e ganhar). Este desejo de competir não é sempre direcionado para outros Humanos. Os escaladores de montanhas podem "ver"uma montanha como um desafio. Certos escaladores de montanhas não resistem a certas montanhas. Olhe então para o incrível tamanho dos números primos recordistas! Aqueles que os encontraram são como os atletas na sua corrida para a vitória. São como os escaladores de montanhas, no sentido em que escalaram montanhas mais altas. As suas maiores contribuições para a Hu-

manidade não é meramente pragmática, é pela curiosidade e pelo espírito do Homem. Se perdermos o desejo do "fazer ainda melhor", estaremos de alguns modos ainda completos?

1.2.5 Para testar hardware

Este tem sido historicamente utilizado como um argumento para a evolução computacional em geral, logo é mais uma motivação para uma companhia do que para apenas um único indivíduo. Desde o princípio da computação eletrônica, que programas com o intuito de encontrar grandes números primos têm sido utilizados como teste para hardware. Por exemplo, rotinas de software do projeto GIMPS foram utilizadas pela Intel para testar os chips de Pentium II e Pentium Pro antes de serem lançados no mercado. Logo uma grande quantidade de leitores de uma página de internet são "diretamente"os beneficiários dessa mesma pesquisa. O famoso bug do Pentium foi descoberto por Nicely quando tentava calcular a constante dos números primos gêmeos. Porque é que programas para encontrar números primos são utilizados desta maneira? Estão diretamente relacionados com o CPU de um computador. São relativamente pequenos, fornecem uma resposta fácil de verificar como sendo verdadeira (quando se computa um número primo conhecido, devem fornecer uma resposta verdadeira após efetuarem os requeridos bilhões de cálculos). Podem ser facilmente "corridos"ao mesmo tempo em que outras tarefas "mais importantes", e são fáceis de parar e de recomeçar.

1.2.6 Para saber mais sobre a sua distribuição

Apesar da Matemática não ser uma ciência experimental, freqüentemente se procuram exemplos para testar conjecturas. Com o evoluir do tamanho dos números, evolui, de certo modo, o nosso conhecimento sobre a distribuição dos mesmos. O Teorema dos números primos foi descoberto através do simples "olhar"para tabelas de números primos e verificar a sua distribuição. No entanto esta pequena especificação não é a única da lista das razões, por exemplo, muitas pessoas podem sentir-se motivadas pela pesquisa de números primos simplesmente, ou devido à necessidade de publicar algo. Muitos outros indivíduos sentem-se aborrecidos por verificarem que os seus computadores estão a desperdiçar capacidade. Provavelmente estes argumentos não o convencerão. Se tal acontecer, lembre-se apenas de que os olhos podem não

ver, os que os ouvidos poderão ouvir, mas que isso não reduz o valor do som. Existem sempre melodias que ultrapassam os nossos

1.3 Um pouco de história

Os números primos são conhecidos pela humanidade há muito tempo. No papiro Rhindi, por exemplo, há indícios de que o antigo povo egípcio já possuía algum conhecimento sobre esse tipo de números. No entanto, os registros mais antigos de um estudo explícito sobre números primos são devido aos gregos. Os Elementos de Euclides (cerca de 300 A.C), contém teoremas importantes sobre números primos, incluindo a demonstração de sua infinitude, o teorema fundamental da aritmética de Euclides também mostrou como construir um número perfeito a partir de um primo de Mersenne. Ao grego Eratóstenes, atribui-se um método simples para o cálculo de números primos, conhecido atualmente como crivo de Eratóstenes. Por outro lado, nos tempos atuais, os grandes números primos são encontrados por computadores, através de testes de primalidade mais sofisticados, como por exemplo, o teste de primalidade AKS.

1.3.1 Euclides e Eratóstenes

Quando Euclides de Alexandria publicou Os Elementos, cerca de 300 a.C., já haviam sido provados vários resultados importantes sobre números primos. A demonstração de que existem infinitos números primos aparece no livro IX de Os Elementos e é uma das primeiras provas conhecidas que se utiliza a demonstração por redução ao absurdo. Euclides também forneceu a prova para o Teorema Fundamental da Aritmética. Aliás, os livros VII, VIII e IX de Os Elementos são quase que exclusivamente dedicados à Teoria dos Números, área da Matemática que estuda os número inteiros e suas propriedades. Cerca de 200 a.C. o grego Eratóstenes de Cirene (aprox. 276 – 194 a.C.) desenvolveu um algoritmo para calcular números primos, conhecido como Crivo de Eratóstenes. Este algoritmo ainda é a forma mais eficiente de achar todos os números primos não muito grandes. Ele consiste em dispor os números naturais até um determinado valor e eliminar desta lista os múltiplos dos números primos já conhecidos

1.3.2 Fermat e Mersenne

O mais famoso teorema de Pierre Fermat(1601-1665) é conhecido como o Último Teorema de Fermat: O último Teorema afirma que se n é um inteiro maior do que 2, a equação $x^n + y^n = z^n$ não admite solução x, y e z no conjunto dos números inteiros maiores do que 1.Foi um matemático e cientista francês, Seu pai,Dominique de Fermat, era um rico mercador de peles e lhe propiciou uma educação privilegiada, inicialmente no mosteiro franciscano de Grandselve e depois na Universidade de Toulouse. Ingressou no serviço público em 1631. Em 1652 ele foi promovido para Juiz Supremo na Corte Criminal Soberana do Parlamento de Toulouse, todavia esta promoção se deu em ocorrência da chegada da praga, que levou a vida de grande parte da população da Europa. Neste mesmo ano Fermat também adoeceu e chegou-se a afirmar que ele havia morrido, entretanto ele se recuperou e permaneceu vivo por mais de uma década. Sua morte, de fato, deu-se a 12 de Janeiro de 1665, em Castres. Em razão de seu cargo, Fermat não podia ter muitos amigos para não ser acusado de favoritismo em seus julgamentos, também em razão da tumultuada fase que passava a França de então, com o Cardeal Richelieu sendo primeiro-ministro. Ao se investigar a produção matemática de Fermat, percebe-se facilmente a característica amadora predominante em seus trabalhos. Na verdade, com pouquíssimas exceções, ele não publicou nada em vida e nem fez qualquer exposição sistemática de suas descobertas e de seus métodos, tinha as questões da matemática mais como desafios a serem resolvidos. Considerado o Príncipe dos amadores, Pierre de Fermat nunca teve formalmente a matemática como a principal atividade de sua vida. Jurista e magistrado por profissão, dedicava à Matemática apenas suas horas de lazer e, mesmo assim, foi considerado por Pascal o maior matemático de seu tempo. Contudo, seu grande gênio matemático perpassou várias gerações, fazendo com que várias mentes se debruçassem com respeito sob o seu legado, que era composto por contribuições nas mais diversas áreas das matemáticas, as principais: cálculo geométrico e infinitesimal; teoria dos números; e teoria da probabilidade. Entre os estudiosos com os quais mantinha contato postal, estão: Sir Kenelm Digby, John Wallis, Nicholas Hensius, além de

Blaise Pascal, Assendi, Roberval, Beaugrand e o padre Marin Mersenne. O interesse desperto em Fermat pela Matemática, possivelmente, deu-se com a leitura de uma tradução latina, feita por Claude Gaspar Bachet de Méziriac, de Aritmética de Diophante, um texto sobrevivente da famosa Biblioteca de Alexandria, queimada pelos árabes no ano 646 d.C., e que compilava cerca de dois mil anos de conhecimentos matemáticos. A matemática do século XVII estava ainda se recuperando da Idade das Trevas, portanto não é de se admirar o caráter amador dos trabalhos de Fermat. No entanto, se ele era um amador, então era o melhor deles, devido à precisão e à importância de seus estudos, que, diga-se ainda, estavam sendo realizados longe de Paris, o único centro que abrigava grandes matemáticos, mas até então ainda não prestigiados estudiosos da Matemática, como Pascal, Gassendi, Mersenne, entre outros. O padre Marin Mersenne teve um papel importante na história da matemática francesa do século XVII e também foi uma das poucas amizades de Fermat. Todavia, é interessante observar mais de perto o desenvolvimento da Matemática nesta época. Diferentemente da famosa escola pitagórica, os franceses não tinham o costume de trocar com os colegas os avanços recentes de suas pesquisas, devido à influência dos cosistas do século XVI, italianos que utilizavam símbolos para representar quantidades desconhecidas. Mersenne tinha o costume, desagradável para seus contemporâneos matemáticos, de divulgar os trabalhos dos pesquisadores. Em suas viagens pela França e por países estrangeiros, acabou conhecendo Fermat e trocando com ele várias correspondências. No entanto, mesmo com a insistência do padre, Fermat não publicou nada.

Contam os historiadores que, em 1637, Fermat afirmou que tinha uma prova para a proposição que ficou conhecida com o Último Teorema de Fermat. Ele escreveu sua afirmação nas margens do livro de Diofanto, Arithmeticae, uma versão feita por Claude Gaspar Bachet (1581–1683). Ele afirmou: "Tenho uma prova maravilhosa para esta proposição, mas a margem é muito pequena para cabê-la". Muitos matemáticos tentaram, sem sucesso, uma prova: Euler, Gauss, Dirichlet, Legendre, Lamé, Kummer, Dedekind etc.

Em setembro de 1994, o matemático Andrew Wiles, de Princeton, e seu estudante Richard Taylor concluíram uma prova usando fatos sobre curvas

elípticas.

Em uma carta enviada a Mersenne, Fermat afirma ter descoberto uma fórmula para achar números primos: para todo n $\in$ N,$f_n = 2^{2^n} + 1$ é primo. Embora não tivesse conseguido provar este resultado, a fórmula funcionava para n = 0, 1, 2, 3 e 4. Os números da forma $2^{2^n} + 1$, ficaram conhecidos como números de Fermat, mas mais de 100 anos depois Euler provou que $f_5 = 2^{2^5} = 2^{32} + 1$= 4.294.967.297 é divisível por 641 e portanto composto.Os números da forma $M_n = 2^n - 1$ são conhecidos como números de Mersenne. Os números de Mersenne estão diretamente ligados aos números perfeitos, aqueles cuja soma dos seus divisores é igual a duas vezes o próprio número. Já na época de Euclides sabia-se que, se $2^n - 1$ é primo, então$2^{n-1}(2^n - 1)$ é perfeito. Sabe-se hoje que todos os números perfeitos pares são deste tipo, mas não se sabe se existem números perfeitos ímpares. Marin Mersenne (1.588 – 1.648) sabia que, se n é composto, então M_n também será composto. Mas se n é primo, M_n nem sempre é primo 2^{11} - 1 = 2.047 = 23 x 89 é composto). Em 1.644 Mersenne afirmou (sem provar) que Mn era primo para n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 e 257 e composto para os outros primos menores que 257. Como na época só havia tábuas de números primos e técnicas para verificar atéM_{19}, Mersenne jamais soube se estava certo. O primeiro erro da lista foi descoberto em 1.886, por Pervusian e Seelhof:M_{61} era primo. Além de M_{61}, também são primos M_{89} e M_{107} e os números M_{67} e M_{257} são compostos. Os resultados foram obtidos pelo chamado Teste de Lucas. Usando seu teste, Lucas (1.842 – 1.891) demonstrou em 1.876 que M_{127} era primo e este número ficou sendo o maior número primo conhecido até 1.952. Em 1.952 começava a era da computação. Robinson conseguiu mostrar que M_{521} ,M_{607}, M_{1279}, M_{2203} e M_{2281} são primos, por meio de computadores. Até hoje foram descobertos 48 números primos de Mersenne. Até o presente momento, o maior primo de Mersenne conhecido é $M_{57885161}$, descoberto em 25 de janeiro de 2013 e que possui no sistema decimal 17425170 dígitos. Um número de Mersenne com mais de 17 milhões de algarismos em sua representação decimal, e foi descoberto pelo Great Internet Mersenne Prime Search. Este além de ser o maior primo de Mersenne também é o maior primo já calculado.

1.3.3 Euler e Gauss

Após Fermat e Mersenne, um século se passou e Leonhard Euler (1.707 – 1.783) trouxe novos avanços à Teoria dos Números. Ele estendeu o Pequeno Teorema de Fermat e demonstrou uma afirmação mais geral, que ficou conhecida como função j de Euler. A função j(n) é definida como o número de naturais menores que n que são primos com n. Como mencionado anteriormente, ele fatorou o quinto número de Fermat e achou 60 pares de números amigos.

Existem quantos números primos menores que um número dado? Esta pergunta vem perseguindo os matemáticos desde quando Euclides provou que existem infinitos números primos, há 2.300 anos atrás. A distribuição dos primos ao longo dos inteiros pode parecer "localmente" irregular, por exemplo, de 9.999.900 à 10.000.000 existem 9 primos enquanto que de 10.000.000 à 10.000.100 existem apenas 2. Mas em grandes escalas, ela se torna bastante regular. Se x é um número real positivo, definimos p(x) como sendo a quantidade de números primos menor ou igual a x. Achar uma boa aproximação para a função p(x) é um dos problemas mais importantes da Teoria dos Números. Karl Friedrich Gauss (1.777 – 1.855) foi o primeiro matemático a fazer alguns avanços neste sentido

Capítulo 2

Números Primos

Neste capítulo estudaremos os conceitos dos números primos, um dos mais importantes de toda matemática.Os números primos , desempenham um papel importantíssimo e é associado a muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações.

2.1 Definição:

Um número natural maior do que 1 e que só é divisível por 1 e por se próprio é chamado de número primo.

2.2 Teorema Fundamental da Aritmética

Todo número natural maior do que 1 ou é primo ou se escreve de modo único ,a menos da ordem dos fatores, como um produto de números primos. Um número maior do que 1 e que não é primo será chamado de composto.Portanto, se um número n é composto, existirá um divisor n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq$ n . Portanto, existirá um número natural n_2 tal que n = $n_1.n_2$, com 1< n_1 < n e, 1< n_1 < n Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto os números 4, 6, 8, 10 e 12 são compostos. Utilizaremos o princípio de indução finita para demonstrar o teorema fundamental da arit-

mética. Demonstração: Se n = 2, o resultado é obvio (uma vez que dois é primo). Suponhamos o resultado válido para todo número menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar.Suponhamos então que n seja composto.Logo existem n_1 e n_2 tais que n = $n_1.n_2$, com 1< n_1< n e 1< n_2 < n.Pela hipótese de indução, temos que existem números primos p_1,..., n_r e g_1,..., g_s tais que $n_1 = p_1...p_r$ e $n_2 = g_1...g_s$ e portanto n = $p_1...p_r.q_1...q_s$., que também é um produto de números primos.

Exemplo1

Baseando-se no conceito de decomposição, fatore em primos o número inteiro 120.

Solução: O número dado se decompõe como produto de primos do seguinte modo:

120 = 2.2.2.3.5, portanto 120 = 2^3.3.5, com 2 < 3 < 5.

Exemplo 2

Baseando-se no conceito de decomposição, fatore em primos o número inteiro 4.667.544.

Solução:O número dado se decompõe como produto de primos da seguinte maneira: 4667544 = 2.2.2.3.3.3.3.7.7.7.7, portanto 4.667.544 = $2^3.3^4.7^4$, com 2< 3 < 7.

Exemplo 3:Baseando-se nos conceitos acima Escreva cada um dos números 360, 540 e 700, de forma única, como produto de primos.

Solução:

- 360 = 2.2.2.3.3.5. = $2^3.3^2.5$
- 3540 = 2.2.3.3.3..5 = $2^2.3^3.5$
- 3700 = 2.2.5.5.7 =$2^2.5^2.7$

2.2.1 Teorema decorrente do teorema fundamental da aritmética

Dado um número natural n > 1, existem primos p_1< ... < p_r e $\propto_1$, ..., $\propto_1$ ∈ N,univocamente como determinados tais que n = $p_1^{\propto_1}$... $p_r^{\propto_r}$. Quando

estivermos lidando com a decomposição em fatores primos de dois, ou mais, números naturais, usaremos o recurso de acrescentar fatores da forma $p^0(= 1)$, onde p é um número primo qualquer.Assim, dados n ∈ N com n > 1 e m > 1 quaisquer podemos escrever : n =$p_1^{\propto_1}$... $p_r^{\propto_r}$ e m = $p_1^{\emptyset_1}$... $p_r^{\emptyset_r}$, usando o mesmo conjunto de primos p_1,..., p_r, desde que permitamos que os expoentes $\propto_1$, ..., $\propto_1$,$\emptyset_1$, ..., $\emptyset_r$ variem em função de N*. Observe que um número natural m > 1, escrito na forma m = $p_1^{\emptyset_1}$... $p_r^{\emptyset_r}$,como no teorema acima é um quadrado perfeito se, e somente se, cada expoente ,$\emptyset_i$ é par.

Denotando-se por d(m) o número de divisores do número natural m, segue, por uma contagem fácil, que se m = $p_1^{\emptyset_1}$... $p_r^{\emptyset_r}$, p_1< ... < p_r são primos e $\emptyset_1$, ..., $\emptyset_r$ naturais, então d(m) = ($\emptyset_1$+ 1) ($\emptyset_2$ + 1)... ($\emptyset_r$ + 1). Decorre imediatamente deste teorema que um número natural m = $p_1^{\emptyset_1}$... $p_r^{\emptyset_r}$ possui uma quantidade ímpar de divisores se, e somente se, é um quadrado perfeito

. *Exemplo 4*

Quantos são os divisores positivos de 540?

Solução:Pelo que vimos anteriormente, a decomposição de 540 em fatores primos é: 540 = $2^2.3^3.5$ e todo divisor positivo de 540 é da forma d(m) = ($\emptyset_1$+ 1) ($\emptyset_2$ + 1)...($\emptyset_r$ + 1).Onde: $\emptyset_1$ ∈ 0, 1, 2, $\emptyset_2$ ∈ 0, 1, 2, 3 e $\emptyset_1$ ∈ 0 ,1. Desse modo, usando o Princípio Multiplicativo, a quantidade de divisores positivos de 540 é igual a (2 + 1).(3 + 1).(1 + 1) = 24. A fatoração de números naturais em primos revela toda a estrutura multiplicativa desses números, permitindo, entre outras coisas, determinar facilmente o mdc e mmc de um conjunto de números, como veremos logo abaixo.

2.2.2 Teorema

. Sejam a = $p_1^{\propto_1}$... $p_r^{\propto_r}$ e b = $p_1^{\emptyset_1}$... $p_r^{\emptyset_r}$, pondo γ_i = min($\propto_i$, $\emptyset_i$) e δ_i = máx($\propto_i$, $\emptyset_i$),com i = 1, 2,..., n,tem-se que (a,b) = ($p_1^{\gamma_1}$... $p_r^{\gamma_r}$) e [a,b] = ($p_1^{\delta_1}$... $p_r^{\delta_r}$), onde: (a,b) é o máximo divisor comum (mdc) entre a e b, quando existe o mdc e [a,b] é o mínimo múltiplo comum [mmc] entre a e b, quando existe o mmc.

DEMONSTRAÇÃO: É óbvio, pelo teorema 2.1.3 que $p_1^{\gamma_1}$... $p_r^{\gamma_r}$ é um divisor

comum de a e b. Seja c = $p_1^{\xi_1}$... $p_r^{\xi_r}$, onde $\xi_i \leqslant \min(\propto_i, \emptyset_i)$ e portanto, c $|(p_1^{\delta_1}$... $p_r^{\delta_r})$. Do mesmo modo, prova-se acerca do mmc. Podemos usar a decomposição de um número inteiro maior do que 1 como produto de números primos para encontrar o Máximo Divisor Comum de dois inteiros positivos. A título de ilustração, consideremos os números 1890 e 360 e suas decomposições em fatores primos $1890 = 2.3^3.5.7$ e $360 = 2^3.3^2.5$ Observamos que os fatores primos comuns na decomposição dos dois números são 2 , 3 e 5. Para encontrar o MDC(1890, 360), basta agora multiplicar os fatores primos comuns elevados aos menores expoentes, isto é, MDC(1890, 360) = $2.3^2.5$ = 90. De um modo geral, se MDC(m, n) = d, então, na decomposição de d em fatores primos comparecem os fatores primos comuns aos números inteiros m e n. Como d é o maior divisor comum a m e n, então, cada fator primo comum comparece com o menor expoente.Analisando de um modo mais sofisticado uma solução de uma questão deste tipo como a do exemplo abaixo, poderiamos escrever:
Use o Teorema Fundamental da Aritmética para calcular o MDC e o MMC dos números: 68 e 120. Solução :Decompondo ambos os números dados, obtemos: $68 = 2^2.17$ e $120 = 2^3.3.5$. Como ,já sabemos que o (a,b) = ($p_1^{\gamma_1}$... $p_r^{\gamma_r}$) e $\gamma_i = \min(\propto_i, \emptyset_i)$, e que $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, com os respectivos $\gamma_1 = 2$, $\gamma_2 = 0$, $\gamma_i = 0$ e $\gamma_4 = 0$, teremos que o MDC(68, 120) $=2^2.3^0.5^0.7^0 = 4$, do mesmo modo como já sabemos que [a,b] = ($p_1^{\delta_1}$... $p_r^{\delta_r}$) e δ_i = máx($\propto_i$, $\emptyset_i$), obtemos que o MMC(68,120) = $2^3.3.5.17 = 2040$

2.3 Distribuição dos Números Primos

Quantos serão os números primos? Essa pergunta foi respondida por Euclides no livro IX dos elementos, onde pela primeira vez se registra o uso de uma demonstração por absurdo em matemática. Essa prova é considerada um das pérolas da matemática.

2.3.1 Teorema. Existem infinitos primos

DEMONSTRAÇÃO: Suponha que exista apenas um número finito de primos p_1,..., p_r. Considere o número natural n = p_1... p_r + 1. E pelo teorema do item 2.1.2 esse número n possui um fator primo p que, portanto, deve ser um dos p_1,..., p_r, e consequentemente, divide o produto p_1... p_r. Mas isto implica que p divide 1, o que é absurdo.

2.3.2 Proposição

. Seja n $\in$ N, com n $>$ 2. Se n é composto, então n admite pelo menos um fator primo p $\leqslant\sqrt{}$n.

DEMONSTRAÇÃO:Como n é composto então existem a e b tais que n = ab, onde 1 $<$ a $<$ n e 1 $<$ b $<$ n. Supondo a $\leq$ b temos $a^2 \leq$ ab = n, isto é, a $\leqslant\sqrt{}$n. Pela proposição anterior existe p primo tal que p |a. Como p|a e a | n, então p |n e temos também que p $\leqslant$ a $\sqrt{}$n . Logo, n possui um divisor primo p $\leqslant\sqrt{}$n

Observação:

1. A proposição anterior fornece um processo que permite reconhecer se um dado natural n $>$ 1 é primo ou composto. Basta dividir n sucessivamente pelos primos menores do que $\sqrt{}$n , se a divisão for exata para algum primo menor do que $\sqrt{}$n, então ele é composto, caso contrário ele é primo.

Observações:

É conveniente então termos a nossa disposição uma lista de primos. Várias tabelas de números primos, até certo limite, já foram calculadas. O cálculo destas tabelas baseia-se num algoritmo ou crivo, desenvolvido por Eratosthenes (276-194 A.C.), que consiste no seguinte:

2.3.3 Crivo de Eratosthenes

Escrevem-se na ordem natural todos os números naturais a partir de 2 até n e, em seguida, eliminam-se todos os inteiros compostos que são múltiplos dos

primos p tais que p $\sqrt{}$n isto é, 2p, 3p, 4p,...., até n.Os números que sobrarem na tabela são todos os primos entre 2 e n. Exemplo. Construa a tabela de todos os primos menores do que 100.

2 3 4 5 6 7 8 9 10

11 12 13 14 15 16 17 18 19 20

21 22 23 24 25 26 27 28 29 30

31 32 33 34 35 36 37 38 39 40

41 42 43 44 45 46 47 48 49 50

51 52 53 54 55 56 57 58 59 60

61 62 63 64 65 66 67 68 69 70

71 72 73 74 75 76 77 78 79 80

81 82 83 84 85 86 87 88 89 90

91 92 93 94 95 96 97 98 99 100

Observações:

1. O número 1 não é primo nem composto.

2. Se a $\in$ Z, a $>$ 0, então ou a é primo, ou a é composto, ou a = 1.

3. O número 2 é o único natural par que é primo.

4. De acordo com a definição acima, para decidir se um dado número n é primo é necessário verificar a divisibilidade dele por todos os números naturais menores que ele, o que fica extremamente trabalhoso a medida que avançamos na seqüência dos números naturais. Os resultados acima nos garantem que é suficiente testar a divisibilidade de n pelos primos menores que a sua raiz quadrada. Uma questão muito importante que se coloca é de como os números primos se distribuem dentro dos números reais. Em particular, qual pode ser a distância entre dois primos consecutivos? Qual é sua freqüência? Olhando para a tabela acima, nota-se que há vários pares de números primos que diferem de duas unidades. São eles: (3,5), (5,7), (11,13), (17,19), (41,43), (59,61), (71,73). Pares de números primos com esta propriedade são chamados de primos gêmeos. Até o presente momento, ainda não se sabe se existem infinitos pares de números gêmeos. Portanto, respondendo à primeira pergunta é que não existe nenhum padrão que descreva o quanto dois primos consecutivos estão longe um do outro. Respondendo à segunda pergunta, é necessário formalizar o conceito de freqüência de primos, que é

a mesma coisa que probabilidade de primos. Denotemos por $\Pi(x)$, a quantidade de números primos menores ou iguais a x. Portanto, a probabilidade de que um elemento do conjunto 1, 2,..., x seja primo é dada por $\frac{\Pi(x)}{x}$. Este quociente é uma função bastante complexa, o que se gostaria de fazer é achar uma função de comportamento bem conhecido que se aproxima do quociente acima para n suficientemente grande. Legendre e Gauss, analisando tabelas, chegaram a conclusão de que este quociente tem a ver com $\frac{1}{lnx}$. Por Volta de 1900, J. Hadamard e Ch. De La Valleè-Poussin, independentemente, provaram o profundo resultado, chamado de Teorema do Números Primos.Em 1949, A.Selberg simplificou substancialmente a prova do Teorema do Números Primos, merecendo por seu trabalho a Medalha Fields (maior distinção dada a um indivíduo por sua contribuição à matemática). A distribuição de números primos ainda é algo bastante misterioso e a ela estão associados muitos problemas em aberto. Uma outra curiosidade matemática, ainda em aberto é a famosa conjectura de Goldbach, este que formulou a Euler em 1742 a conjectura que afirma que todo número natural par maior do que 3 pode ser escrito como soma de dois números primos. O matemático russo Ivan Vinogradov, em 1973, demonstrou o difícil teorema que garante que todo número natural ímpar, suficientemente grande, pode ser escrito como soma de, no máximo, três primos. Finalmente, não podemos de deixar de mencionar o mais importante problema em aberto em Teoria dos Números: a hipótese de Riemann, que se provado revelará muitos dos mistérios dos números primos e deixará o seu realizador num destacado lugar entre os imortais da matemática.

2.4 Pequeno Teorema de Fermat

Depois de alguns séculos sem qualquer descoberta importante, surge Pierre de Fermat (1.601 – 1.665) no início do século XVII. Ele provou o que ficou conhecido como o *Pequeno Teorema de Fermat*, que afirma que se p é um número primo, então para todo número inteiro a é válido que p $|a^p$ – a . Este resultado já era conhecido para o caso particular a = 2 cerca de 2.000 anos antes e era conhecido como a Hipótese Chinesa. Ela afirmava também que a recíproca era verdadeira. Além de generalizar para qualquer valor inteiro de a, Fermat mostrou que a recíproca é falsa (2341 – 2 é divisível por 341, embora 341 = 31 x 11 não seja primo). O Pequeno Teorema de Fermat é a base de muitos outros trabalhos na Teoria dos Números e ainda hoje é utilizado em testes de primalidade. Numa carta para Bernard Frenicle de Bessy (1605–1675), datada de 18 de outubro de 1640, Pierre de Fermat (1601 – 1665) deu sua versão do que hoje conhecemos como *Pequeno Teorema de Fermat*. Ele descobriu algo surpreendente e que foi usado para a criação do sistema RSA. Fermat descobriu que se você, por exemplo, calcular as potências de 2 em uma calculadora comum e verificar o resto na divisão por 7, estes restos têm um padrão:
Fermat, ainda viu que este padrão se mantinha se ele substituísse 7 por qualquer número primo, enunciando o seguinte:

2.4.1 Teorema 3

. (Pequeno Teorema de Fermat). Dado um número primo p, tem-se que p$|a^p$, para todo a ∈ N.
DEMONSTRAÇÃO: Vamos provar o resultado por indução sobre a. O resultado é óbvio para a = 1, pois p| 0.
Suponha o resultado válido para a, iremos prová-lo para a + 1. Pela fórmula do binômio de Newton $(a+1)^p$ – (a + 1) = a^p – a + $C_{p,1}.a^p - 1 + C_{p,2}.a^{p-2}$ + ... + $C_{p,p-1}$.a e como pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, logo o resultado é válido.
Corolário. Se p é primo e se a é um número natural não divisível por p,

então p| a^{p-1}– 1.

DEMONSTRAÇÃO: Como , pelo Pequeno Teorema de Fermat, p|$a(a^{p-1}$ – 1) e como (a, p) = 1, segue-se, imediatamente, que p|a^{p-1} – 1 . Este corolário também é chamado de *Pequeno Teorema de Fermat.*

O Pequeno Teorema de Fermat nos fornece um teste de não primalidade. De fato, dado m ∈ N, Com m > 1, se existir algum a ∈ N, com (a, m) = 1, tal que m ∤a^{m-1} – 1, então m não é primo.

2.4.2 *EXEMPLOS DE APLICAÇÃO*

(solução de alguns exercícios do livro elementos de aritmética de Abramo Hefez)

a) Mostre que, para todo n ∈ N,é natural o número $\frac{3}{5}\ n^5 + \frac{2}{3}\ n^3 + \frac{11}{15}\ n$

Solução: adicionando $\frac{3}{5}$ n + $\frac{2}{3}$ n e subtraindo $\frac{3}{5}$ n + $\frac{2}{3}$ n ao número $\frac{3}{5}\ n^5$ + $\frac{2}{3}\ n^3$ + $\frac{11}{15}$, obtemos $\frac{3}{5}\ n^5$ - $\frac{3}{5}$ n + $\frac{2}{3}\ n^3$ - $\frac{2}{3}$ n + $\frac{11}{15}$ n + $\frac{3}{5}$ n + $\frac{2}{3}$ n + $\frac{11}{15}$ n = $\frac{3}{5}\ (n^5 - n) + \frac{2}{3}\ (n^3 - n) + \frac{30}{15}$ n= $\frac{3}{5}\ (n^5 - n) + \frac{2}{3}\ (n^3 - n)$ + 2n, mas pelo *Pequeno Teorema de Fermat* 5|(n^5 – n) e 3|n^3- n, portanto $\frac{3}{5}\ n^5$ + $\frac{2}{3}\ n^3 + \frac{11}{15}$ n. = $\frac{3}{5}\ (n^5 - n) + \frac{2}{3}\ (n^3 - n)$ + 2n é natural para todo n.

b) Ache o resto da divisão de 12^p***-1 por p quando p é primo***

Solução: pelo Pequeno Teorema de Fermat temos que se p é primo, então p| 12^p – 12, portanto temos dois casos a considerar. Caso 1: se p| 12 então o resto da divisão de 12^p-1 por p é zero Caso 2: se p|12, então pelo Pequeno Teorema de Fermat p| 12^{p-1} – 1, portanto existe um q ∈ N, tal que 12^{p-1} – 1

= p.q com 1 < q < p, logo 12^{p-1} = pq + 1, logo o resto da divisão de 12^{p-1} – 1 por p é 1.

c) Se p e q são números primos tais que 5⩽ q ⩽ p, então 24| $p^2 - q^2$

Solução: temos que 24 = 3×8 e já sabemos pelo Pequeno Teorema de Fermat que 3| p^2– 1 e 3| q^2 – 1 e portanto 3 | p^2 – 1 – (q^2 – 1) = p^2 –q^2 .Agora temos que mostrar que 8| p^2 – q^2. Como p e q são primos maiores ou iguais a 5 então eles são ímpares, portanto podem ser escritos na forma p = 2n + 1 e q = 2m + 1. Logo teremos que $p^2 - q^2 = (2n+1)^2$ - $(2m+1)^2$ = $4n^2$+4n+1 – ($4m^2$+4m+1) =$4n^2$- $4m^2$ + 4n – 4m = $4(n^2 \veebar m^2)$ + 4(n – m) = 4(n+m)(n-m)+4(n – m) = 4(n –m)n + m + 1, portanto se n e m tem paridades iguais n – m é par e se n e m tem paridades distintas então n + m + 1 é par, logo $p^2 \veebar q^2$ = 4(n –m)n + m + 1 é múltiplo de 8. Como 3| $p^2 \veebar q^2$ e 8| $p^2 \veebar q^2$ então 24| $p^2 \veebar q^2$, e isto é o queríamos demonstrar.

d) Todo primo da forma 3n + 1 é também da forma 6m + 1

Solução: Seja p-primo tal que p = 3n + 1 para algum n ∈ N. Se n-ímpar então p não é primo, logo necessariamente n-par. Suponhamos n = 2m; m ∈ N, então p = 3n + 1 = 3(2m) + 1 = 6m+ 1

e) Mostre que o único número primo da forma n^3 ***– 1 = 7***

Solução: Seja p primo tal que p = n^3- 1 para algum n ∈ N, então p = (n-1)(n^2+ n+ 1). Se n é ímpar então p é par, isto é absurdo. para o caso n par como p ⩾ 2, então n = 2, 4 ... , 2k com k ∈ N.Se n = 2 ⇒ p = 7, para o caso n ⩾ 4 ⇒ (n- 1) ⩾ 3 e (n^2+ n+ 1) ⩾ 21 logo p = (n- 1)(n^2+ n+ 1) é composto, não é primo. Portanto, p = 2^3- 1 = 7

f) Mostre que entre n e n! existe pelo menos um número primo

Solução : Joseph Louiz f. Bertrand (1822 - 1900) foi um matemático, historiador de ciências e acadêmico francês.Em 1845 lançou a conjetura que

sempre existe ao menos um número primo entre n e $2n-2$ para $\forall$todo n $>$ 3. P. Tchebychev demonstrou essa conjetura, o postulado de Bertrand, em 1850. Pela conjetura de J. Bertrand temos que existe um primo p tal que 3 $<$ n $<$ p $<$ $2(n-1)$.Como $2(n-1)$ $<$ n! segue que existe um primo p tal que 3 $<$ n $<$ p $<$ n! Para o caso n = 3 $\Rightarrow$ 3 $<$ 5 $<$ 3! Portanto, entre n e n! existe pelo menos um número primo.

g) Mostre que se p, p + 2, e p + 4 são primos, então p = 3

Solução: Por hipótese os números p; p+2 e p+4 são primos, suponhamos que p = 2k +1; k $\geqslant$1. Assim temos então que os números p; p + 2 e p + 4 são uma terna de primos ; isto é os números agora terão a forma 2k + 1; 2k + 3; 2k + 5 $\Longleftrightarrow$ 2k + 1; 2(k + 1) + 1; 2(k + 2) + 1; k$\geqslant$ 1, estes são primos, além disso como se pode observar são três números ímpares consecutivos. Sabemos que todo número natural k pode ser escrito como algum elemento do conjunto A = 3n; 3n + 1; 3n + 2; $\forall$ n $\in$ N .
se k = 3n $\Rightarrow$ p = 6n + 1; p + 2 = $3(2n+1)$; p + 4 = 6n + 5.
se k = 3n+1 $\Rightarrow$ p = $3(2n+1)$; p+2 = $3(2n+1)+2$; p+4 = $3(2n+2)+1$.
se k = 3n+2 $\Rightarrow$ p = 3(2n+1)+2; p+2 = 3(2n+2)+1; p+4 = 3(2n+3).
Com qualquer hipótese para n$\geqslant$ 1, um dos números p; p + 2 e p + 4 é composto e múltiplo de três. Quando n = 0 temos p = 3; p + 2 = 5 e p + 4 = 7 .Portanto, p = 3

Capítulo 3

PRIMOS ESPECIAIS

Estudaremos agora algumas propriedades de certos números primos que possuem formas especiais e de certos números que possuem propriedades especiais

3.1 Primos de Fermat e de Mersenne

3.1.1 Primos de Fermat

Os números de Fermat são os números da forma F_nn $= 2^{2^n} + 1$, Fermat achava que esses números eram todos primos.
De fato, $F_1 = 5$; $F_2 = 17$; $F_3 = 257$; $F_4 = 65537$ são primos. Em 1732, Euler mostrou que $F_5 = 2^{2^5} + 1 = 4294967297 = 641 \times 6700417$; portanto, composto, desfazendo assim esta crença de Fermat. Os números de Fermat primos são chamados de primos de Fermat. Até hoje, não se sabe se existem outros primos de Fermat além dos quatro primeiros.

3.1.2 Primos de Mersenne

Os números de Mersenne são os números da forma $M_p = 2^p$ -1, onde p é um número primo.
No intervalo $2 \leqslant p \leqslant 5000$ os números de Mersenne que são primos, cha-

mados de primos de Mersenne, correspondem aos seguintes valores de p: 2; 3; 5; 7; 13; 19; 31; 61; 89; 107; 127; 521; 607; 1279; 2203; 2281; 3217; 4253 e 4423.Até o presente momento, o maior primo de Mersenne conhecido é M57885161, descoberto em 25 de janeiro de 2013 e que possui no sistema decimal 17425170 dígitos. Um número de Mersenne com mais de 17 milhões de algarismos em sua representação decimal, e foi descoberto pelo Great Internet Mersenne Prime Search. Este além de ser o maior primo de Mersenne também é o maior primo já calculado.

3.2 Números Perfeitos

Os números como 6 e 28, com a propriedade de serem iguais à metade da soma de seus divisores, tiveram o poder de fascinar os gregos antigos, que os chamaram de números perfeitos. Até a Idade Média, conheciam-se apenas os seguintes números perfeitos: 6; 28; 496; 8128 e 33550336. Atualmente, conhecem-se mais alguns números perfeitos. Um fato curioso é que todos os números perfeitos conhecidos são pares. Não se sabe nada sobre a existência ou não de números perfeitos ímpares.

3.2.1 Teorema

.Denotemos por S(n) a soma de todos os divisores de um número natural n. Tem-se que S(1) = 1 e se $p_1^{\propto_1}.... \ p_r^{\propto_r}$ é a decomposição em fatores primos de n > 1

Então S(n) = $\frac{p_1^{\propto_1+1}-1}{p_1-1}$ ... $\frac{p_r^{\propto_r+1}-1}{p_r-1}$

DEMONSTRAÇÃO: Considere a igualdade

$(p_1^0+p_1^1+...p_1^{\propto_1})...(p_1^0+p_1^1+...p_1^{\propto_1}) = S(n)$ e aplicando a fórmula da soma dos termos de uma progressão geométrica o resultado da soma do lado esquerdo resulta na fórmula acima do teorema dado.

Exemplos: S(3) = $\frac{3^2-1}{3-1}$

S(6)= S(2×3)= $\frac{2^2-1}{2-1} \times \frac{3^2-1}{3-1} = 12$

Lema 2.4.2.2. Seja n ∈ N.Tem-se que S(n) = n + 1 se, e somente se, n é um número primo.

DEMONSTRAÇÃO: Se S(n) = n +1, segue-se que n > 1 e que seus divisores são 1 e n, logo, n é primo.

Reciprocamente, se n é primo segue-se do teorema 2.4.2.1 que S(n) = $\frac{n^2-1}{n-1}$ = n+1.

3.2.2 *Teorema:Euclides-Euler*

Um número natural n é um número perfeito par se, e somente se,
n = $2^{p-1} \times (2^p - 1)$ onde $2^p - 1$ é um primo de Mersenne.

DEMONSTRAÇÃO: Suponha que n = $2^{p-1} \times (2^p - 1)$ onde $2^p - 1$ é um primo de Mersenne.Logo, p > 1, e, conseqüentemente, n é par.Como $2^p - 1$ é ímpar, temos que (2^{p-1},$2^p - 1$) = 1. Logo pela proposição 2.4.2.1, segue que S(n) = S($2^{p-1} \times 2^p - 1$) =
= S $(2^p - 1) \times$ S(2^{p-1}) = $(2^p - 1) \times 2^p$ = 2n .

3.2.3 Exemplo de aplicação

(solução de exercício do livro elementos de aritmética de Abramo Hefez)

a) Mostre que a soma dos inversos dos divisores de um número perfeito par é sempre igual a 2

Solução: Um número é perfeito par se, e somente se a soma de seus divisores é igual ao seu dobro, ou seja S*(n) = 2n e também da forma n = $2^{p-1} \times (2^p - 1)$ onde $2^p - 1$ é um primo de Mersenne.

Seja S*(n) a soma dos inversos dos divisores de n, então
S*(n) = $(\frac{1}{2^0} + \frac{1}{2^1} + \frac{1}{2^2} + \ldots + \frac{1}{2^{p-1}}) \times (1 + \frac{1}{2^p - 1})$

$S^*(n) = \frac{\frac{1}{2^p} - 1}{\frac{1}{2} - 1} \times (\frac{2^p - 1 + 1}{2^p - 1}) \Rightarrow S^*(n) = \frac{1 - \frac{1}{2^p}}{1 - \frac{1}{2}} \times \frac{2^p}{2^p - 1} =$

$= \frac{\frac{2^p - 1}{2^p}}{\frac{1}{2}} \times \frac{2^p}{2^p - 1} = 2 \times \frac{2^p - 1}{2^p} \times \frac{2^p}{2^p - 1} = 2 \Rightarrow S^*(n) = 2$, que é o que queriamos demosntrar.

Capítulo 4

CONSIDERAÇÕES FINAIS

Os números primos sempre foram um grande mistério e fascinaram matemáticos de todas as gerações, então nessa breve escrita em torno de tão maravilhoso tema tentei focar os principais conceitos que são utilizados mesmo que implicitamente por nós professores em sala de aula.
Com demonstrações de alguns teoremas e resolução de alguns exercícios do principal livro utilizado nas nossas aulas do PROFMAT tentei mostrar como os números primos nos ajuda a melhorar nossa prática de sala de aula, pois facilita as idéias e traz várias boas estratégias para atrair a atenção ou mesmo diminuir a dificuldade nos ensino de fatorações, máximo divisor comum(MDC), mínimo múltiplo comum(MMC), número de divisores, produto de divisores, conhecimento de primos em geral e conhecimento de um número perfeito. Como já citei anteriormente este trabalho é apenas uma breve escrita acerca destes fascinantes números, de modo que só foi tratado aqui os conceitos mais básicos de mmc e mdc, além do teorema fundamental e com mais ênfase o pequeno teorema de Fermat, este material poderá posteriormente ser utilizado por estudantes que queiram se aprofundar nesses conceitos já citados, pois é tratado de uma maneira bastante simples e fundamentada em autores com notável respeito nessa área do conhecimento. Durante o desenvolvimento desse trabalho acabei aprendendo coisas incríveis, que certamente serão utilizadas por mim em sala de aula e possivelmente ser-

virão como base para um artigo na área de elementos de aritmética, só para citar uma dessas coisas que achei muito importante, foi a demonstração que não se encontra aqui neste trabalho, mais que consegui fazer de forma bastante convincente, que o produto dos divisores naturais de um número inteiro positivo n é $n^{\frac{d}{2}}$, onde d é o número de divisores de n. Apesar de ter ficado de fora desta escrita por causa da delimitação do tema, não posso deixar de citar que os números primos são de suma importância na decomposição do fatorial, nas congruências e nos testes de primalidade de Euler e Wilson, que são temas presentes nos livros de fundamentos de aritmética.

Referências Bibliográficas

EVES, Howard. Introdução à história da matemática, Campinas, SP,Unicamp, 2004.

HEFEZ, Abramo. Elementos de aritmética. 2.ed.,Rio de Janeiro,SBM, 2011.

HEFEZ, Abramo. Curso de álgebra. Volume 1.,Rio de Janeiro,IMPA, 1993.

LAKATOS, Eva M.; ANDRADE, Marina M. Fundamentos de metodologia científica. São Paulo: Atlas, 1986.

$HTTP://PT.wikipedia.org/wiki/PierredeFermat$

MUNIZ NETO, Antônio Caminha. Tópicos de matemática elementar. 1.ed.Rio de Janeiro,SBM, 2012.

PRESTES, Maria de Luci de Mesquita. A pesquisa e a construção do conhecimento científico: do planejamento aos textos, da escola à academia. 4. ed. São Paulo, Rêspel, 2012.

AZEVEDO, F. V. LaTeX. São Paulo: FEBAB, 2012. Apostila (Curso: Ferramenta para Estruturação de Trabalhos Científicos e Livros)