Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Campus de Rio Claro

Explorando o universo dos Números Primos

Rafael Américo de Oliveira

Dissertação apresentada ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional-PROFMAT como requisito parcial para a obtenção do grau de Mestre

Orientador
Prof. Dr. Jamil Viana Pereira

2015

512.7 Oliveira, Rafael Américo de
O48e Explorando o universo do números primos / Rafael Américo de Oliveira. - Rio Claro, 2015
61 f. : il.

Dissertação (mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas
Orientador: Jamil Viana Pereira

1. Teoria dos números. 2. Teorema de Euclides. 3. Testes de Primalidade. I. Título.

Ficha Catalográfica elaborada pela STATI - Biblioteca da UNESP
Campus de Rio Claro/SP

TERMO DE APROVAÇÃO

Rafael Américo de Oliveira

Explorando o universo dos Números Primos

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação Mestrado Profissional em Matemática Universitária do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Prof. Dr. Jamil Viana Pereira
Orientador

Prof. Dr. Sergio Henrique Monari Soares
ICMC- USP

Prof. Dr. Rawlilson de Oliveira Araujo
IGCE - UNESP

Rio Claro, 19 de Junho de 2015

Aos meus pais Aparecido e Glicéria.
À minha sobrinha Maria Vitória.
À minha esposa Luciana.
À minha filha Rafaela, na esperança de que ela se sinta encantada com os números.

Agradecimentos

A Deus, que nas horas mais difícieis concedeu forças que permitiram a conclusão deste trabalho.

Aos meus pais Aparecido e Glicéria pelo apoio, incentivo e dedicação que contribuiram para que eu pudesse buscar os caminhos da realização e felicidade.

À minha esposa Luciana pelo apoio e por abdicar dos finais de semana e feriados.

À Sociedade Brasileira de Matemática pela excelente iniciativa de conceber o PROFMAT, um programa fantástico que realmente contribui para a formação profissional do professor brasileiro.

À CAPES (Coordenação de Aperfeiçoamento de Pessoal de Nível Superior), pela bolsa de estudos concedida, que foi fundamental para a conclusão deste trabalho.

Ao Departamento de Matemática da Unesp de Rio Claro, pela iniciativa desafiadora de promover o PROFMAT no campus de Rio Claro.

Aos meus colegas professores (turma 2012), por oferecerem apoio nos momentos de tensão e propiciarem momentos de alegria durante as aulas.

Aos meus companheiros de viagem, pelas grandes aventuras na SP-191.

À Prof.ª Suzi coordenadora do PROFMAT em 2012, pela maneira acolhedora com que sempre tratou os alunos.

Ao Prof. Dr. Jamil Viana Pereira, por me orientar durante a elaboração deste trabalho com esclarecimentos, correções e sugestões, e por demonstrar compreensão e paciência.

O único lugar onde o sucesso vem antes do trabalho é no dicionário.

Albert Einstein.

Resumo

O objetivo deste trabalho é apresentar um estudo sobre números primos. Trataremos de assuntos clássicos da Teoria dos Números: Congruências, O pequeno Teorema de Fermat, o Teorema de Wilson , a função φ de Euler e o Teorema de Euler. Utilizando estes resultados passaremos a investigar testes de primalidade, números primos especiais e funções que geram números primos.

Palavras-chave: Teoria dos números, Teorema de Euclides, Testes de Primalidade.

Abstract

The aim of this work is a study of prime numbers. We will work with classical subjects of Number Theory, such as, Congruences, The little Fermat's Theorem, the Wilson's Theorem, the Euler's φ function and the Euler's Theorem. Using these results we will investigate primality tests, special prime numbers and functions defining prime numbers.

Keywords: Theory of numbers , Euclid's Theorem , Primality Test.

Sumário

Introdução

Neste trabalho abordaremos conceitos e resultados relativos aos números primos, um conceito de grande relevância para a Matemática, em especial para a Teoria dos Números. Tais números sempre atraíram a atenção de grandes matemáticos e a curiosidade de entusiastas. Um importante resultado, que ratifica a importância dos números primos, é o Teorema Fundamental da Aritmética, que diz: *"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"*.[1]. Vários estudiosos como Euclides, Pitágoras, Fermat, Euler, Legendre e Gauss concentraram esforços na busca de resolução de problemas envolvendo números primos. São problemas que lidam com as seguintes questões [2]:

- Quantos números primos existem?
- Como reconhecer se um número natural é primo?
- Como os números primos estão distribuídos?
- Existem funções que geram números primos?

Estas questões serviram de motivação para este trabalho, e incentivaram a leitura de outros livros e artigos científicos que tratam das mesmas.

Para obter uma resposta para a primeira questão, abordaremos o Teorema de Euclides, apresentado por Euclides na obra *Os Elementos* por volta de 300 a.C, comprovando que a quantidade de números primos é infinita.

No decorrer desta dissertação, estudaremos resultados importantes na Teoria dos Números como: O pequeno Teorema de Fermat, o Teorema de Wilson , a função φ de Euler e o Teorema de Euler ([1], [2], [3], [4]), que nos fornecerão embasamento teórico para o desenvolvimento de temas mais avançados e para a busca de conclusões a respeito de nossas questões envolvendo os números primos.

Ribenboim [2], também inspirou o estudo de alguns Testes de Primalidade, que serão desenvolvidos no capítulo 2 e fornecerão critérios para investigar se um número é

primo. Estes testes apresentam algumas dificuldades, que serão oportunamente apontadas, pois requerem uma gama de cálculos e a ocorrência de certas condições.

No capítulo 3, obteremos algumas estimativas sobre a distribuição dos números primos, em especial será possível examinar determinadas aproximações da função $\pi(x)$ ("a função que conta os números primos").[5]. O capítulo 4 será dedicado ao estudo de números primos que se apresentam de um modo específico: Os Primos de Fermat, Os Primos de Sophie Germain, Os Primos de Mersenne, Primos Gêmeos e Primos Trigêmeos ([1], [2], [3],[5], [6]). Os números Primos de Mersenne estão diretamente ligados a busca por números primos com uma grande quantidade de dígitos. Atualmente, através de algoritmos específicos e super-computadores, estudiosos tentam encontrar números primos de Merssene cada vez maiores.

Uma das questões de grande interesse entre os pesquisadores interessados em números primos será abordada no Capítulo 5, e consiste em investigar a questão: *Existe uma fórmula ou função que gere números primos?*. Em um primeiro momento somos levados a pensar que não existe uma fórmula ou função que nos forneça os números primos. Entretanto, no Capítulo 5, apresentaremos dois resultados: o primeiro deles devido a W.H MILLS [7], que exibiu uma fórmula que fornece números primos e o segundo devido a E. M. WRIGHT [8], um pouco mais preciso que o primeiro, oferecendo uma fórmula que fornece números primos. Porém, esta fórmula depende de uma constante irracional ω cujas aproximações podem gerar erros encontrando números que não são primos. Ademais, estas fórmulas lidam com números grandes, o que prejudica a sua aplicabilidade. Por último abordaremos uma função de duas variáveis que nos fornece números primos, mas que também envolve cálculos com números grandes. Pelo exposto podemos confirmar que, de fato, existem fórmulas que fornecem números primos, mas sua aplicabilidade fica restrita a alguns poucos valores devido a complexidade de cálculos envolvidos, deste modo torna-se um desafio encontrar uma expressão relativamente simples que forneça números primos, e somente esses.

1 Conceitos introdutórios e resultados preleminares

Neste capítulo definiremos o conceito de divisibilidade entre dois números inteiros e demonstraremos algumas propriedades elementares. Dentre estes, enunciaremos e demonstraremos o resultado conhecido como Teorema de Eudoxius, que será necessário na demonstração do Algoritmo da Divisão de Euclides. Discorreremos também sobre o máximo divisor comum entre dois números inteiros e números relativamente primos.

1.1 Divisibilidade

Definição 1.1. *Se a e b são inteiros, dizemos que a divide b, denotando por $a \mid b$, quando existir um inteiro c tal que $b = ac$.*

Proposição 1.2. *Se a, b e c são inteiros, $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$, então existem inteiros k_1 e k_2 de modo que $b = k_1 a$ e $c = k_2 b$. Assim, $c = k_2 k_1 a$, isto é, $a \mid c$. ■

Proposição 1.3. *Se a, b, c, m e n são inteiros, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração: Se $c \mid a$ e $c \mid b$, então existem inteiros k_1 e k_2 tais que $a = k_1 c$ e $b = k_2 c$. Multiplicando-se estas duas equações respectivamente por m e n teremos $ma = mk_1 c$ e $nb = nk_2 c$. Somando-se membro a membro obtemos $ma + nb = (mk_1 + nk_2)c$, o que nos diz que $c \mid (ma + nb)$. ■

Teorema 1.4 (Eudoxius)**.** *Dados a e b inteiros com $b \neq 0$, então a é múltiplo de b ou se encontra entre dois múltiplos consecutivos de b, isto é, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro n tal que, para $b > 0$*

$$nb \leqslant a < (n+1)b,$$

e para $b < 0$

$$nb \leqslant a < (n-1)b.$$

Demonstração: Para nossa demonstração vamos considerar $a > 0$ e $b > 0$ (os casos em que $a < 0$ ou $b < 0$ podem ser demonstrados de maneira análoga). Deste modo, temos duas possibilidades

i. Se $a = nb$, para algum $n \in \mathbb{Z}$ não há o que provar e o resultado segue;

ii. Se $a \neq nb \ \forall \ n \in \mathbb{Z}$, existe um menor inteiro k que satisfaz a condição: $a < kb$.

Afirmamos que

$$(k-1)b < a.$$

De fato, pois, caso $a < (k-1)b$ teríamos uma contradição uma vez que $a < kb$ e k é o menor inteiro em que isto ocorre. Deste modo, devemos ter que $(k-1)b < a$ e então $(k-1)b < a < kb$. Tomando $n = k-1$ obtemos

$$nb \leqslant a < (n+1)b.$$

Como queríamos. ■

Exemplo 1.5. Para $a = 13$ e $b = 4$, devemos tomar $n = 3$

$$3.4 \leqslant 13 < 4.4$$

Para $a = -13$ e $b = 4$, escolhemos $n = -4$

$$-4.4 \leqslant -13 < -3.4$$

Para $a = 35$ e $b = -3$, tomamos $n = -11$

$$-11.(-3) \leqslant 35 < (-12).(-3)$$

Abordaremos agora o Algoritmo da Divisão de Euclides, objeto de estudo do Teorema a seguir.

Teorema 1.6 (Algoritmo da Divisão de Euclides)**.** *Dados dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que*

$$a = qb + r, \quad com \quad 0 \leqslant r < b \quad (r = 0 \Leftrightarrow b \mid a)$$

Demonstração: Pelo Teorema de Eudoxius, como $b > 0$, existe q satisfazendo

$$qb \leqslant a < (q+1)b,$$

o que implica $0 \leqslant a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando

$$a = q_1 b + r_1 \quad \text{com} \quad 0 \leqslant r_1 < b.$$

Temos $(qb + r) - (q_1 b + r_1) = 0$, isto é $b(q - q_1) = r_1 - r$, o que implica $b|(r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $| r_1 - r | < b$ e, portanto, como $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$ o que nos permite concluir que $r = r_1$. Logo $q_1 b = qb$ e daí $q_1 = q$, uma vez que $b \neq 0$. ■

1.2 Máximo divisor comum

Definição 1.7 (Máximo Divisor Comum)**.** *O máximo divisor comum entre dois inteiros a e b (a ou b diferente de zero), denotado por (a, b), é o maior inteiro que divide a e b.*

Teorema 1.8. *Seja d o máximo divisor comum entre a e b, então existem inteiros m e n tais que $d = ma + nb$.*

Demonstração: Seja B o conjunto de todas as combinações lineares $ma + nb$ onde m e n são inteiros. Este conjunto contém, claramente, números negativos, positivos e também o zero. Vamos escolher m_0 e n_0 tais que $c = m_0a + n_0b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c \mid a$ e que $c \mid b$. Como as demontrações são análogas, mostraremos apenas que $c \mid a$. Suponhamos por contradição que $c \nmid a$. Pelo Teorema 1.6, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(m_0a + n_0b) = (1 - qm_0)a + (-qn_0)b$. Isto mostra que $r \in B$, pois $(1 - qm_0)$ e $(-qn_0)$ são inteiros, o que é uma contradição, visto que $0 < r < c$ e c é o menor elemento positivo de B. Logo $c \mid a$ e de forma análoga se prova que $c \mid b$.
Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$ e, portanto, $c = m_0a + n_0b = m_0k_1d + n_0k_2d = d(m_0k_1 + n_0k_2)$, ou seja, $d \mid c$ e então $d \leq c$ (visto que c e d são números positivos) e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = c = m_0a + n_0b$. ■

Teorema 1.9. *O máximo divisor comum d entre a e b é o divisor positivo de a e b que é divisível por todo divisor comum.*

Demonstração: Pelo Teorema 1.8 existem inteiros m e n tais que $d = ma + nb$. Por outro lado se d_1 é um divisor comum de a e b existem inteiros k_1 e k_2 tal que $a = k_1d_1$ e $b = k_2d_1$ e então $ma = mk_1d_1$ e $nb = nk_2d_1$, e então $d = ma + nb = mk_1d_1 + nk_2d_1 = (mk_1 + nk_2)d_1$, donde concluímos que $d_1 \mid d$. ■

1.3 Números relativamente primos

Definição 1.10. *Os inteiros a e b são relativamente primos (ou primos entre si) quando $(a, b) = 1$.*

Teorema 1.11. *Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração: Como $(a, b) = 1$, então pelo Teorema 1.8, existem inteiros m e n tais que $ma + nb = 1$. Multiplicando-se ambos os lados desta igualdade por c obtemos: $mac + nbc = c$. Como $a \mid ac$ e, por hipótese, $a \mid bc$ temos pela Proposição 1.3 que $a \mid c$. ■

Teorema 1.12. *Se a e b são inteiros e $a = qb + r$, onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração: Da relação $a = qb + r$ podemos afirmar que todo divisor de b e r é um divisor de a (pela Proposição 1.3). De outro modo $r = a - qb$, nos informa que todo divisor de a e b é um divisor de r. Logo o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r, o que nos assegura o resultado $(a, b) = (b, r)$. ■

1.4 Números Primos

Os números primos sempre intrigaram estudiosos como Pitágoras, Euclides, Fermat, Euller, Merssene etc. Para investigar resultados sofisticados inerentes a tais números trataremos, neste capítulo, de definir com rigor o conceito de número primo e também apresentaremos três questões interessantes que provocam uma reflexão sobre a importância do tema. Preocupamo-nos em demonstrar o Teorema de Euclides, que elucida a questão sobre a quantidade de números primos existentes.

Definição 1.13. *Um número inteiro p $(p > 1)$ possuindo somente dois divisores positivos: p e 1 é chamado número primo.*

De acordo com a definição anterior [1], os primeiros números primos são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23...$$

Um número diferente de 0 e 1 que não é primo é chamado de **número composto**.

1.5 Questões interessantes

Perguntas interessantes a respeito dos números primos foram formuladas ao longo de toda a existência da humanidade. São indagações do tipo:

- *Quantos números primos existem?*
  A resposta a esta questão será dada na seção 1.6.

- *Como é a busca pelo maior número primo ?*
  Esta questão será discutida seção 4.3

- *Existem funções que geram números primos?*
  No capítulo 5 trataremos essa questão.

1.6 O Teorema de Euclides

O Teorema a seguir foi demonstrado por Euclides na obra Os Elementos (por volta de 300 A.C) e responde a primeira pergunta da seção anterior.

Teorema 1.14. *(Euclides). A quantidade de números primos é infinita.*

Demonstração: Suponha que $p_1 = 2 < p_2 = 3 < p_3 = 5 < \cdots < p_r$ são todos os primos. Seja $p = p_1p_2\cdots p_r + 1$ e seja p^* um número primo divisor de p (A existência de p^* é uma consequência do Teorema Fundamental da Aritmética [1]). Nessas condições, p^* não pode ser nenhum dos números $p_1, \cdots, p_r$, pois caso contrário dividiria a diferença $p - p_1p_2\cdots p_r = 1$ o que é impossível.
Conclui-se então que p^* é algum outro primo e $p_1, p_2\cdots, p_r$ não são todos os primos. ■

Vamos agora investigar a distribuição dos números primos. É interessante observar que a quantidade de números primos nos primeiros cinco blocos de 1000 números são:

$$168, 135, 127, 120, 119,$$

e nos últimos cinco blocos entre 1000 e 10.000.000 são

$$62, 58, 67, 64, 53.$$

Observando a distribuição de números primos em detalhes verifica-se tratar de uma distribuição extremamente irregular. Uma característica interessante sobre a disposição dos números primos é que há longos blocos de números compostos. Por exemplo, o número primo 370.261 é precedido por 111 números compostos.

Observação 1.15. Vamos verificar que estes longos blocos devem realmente ocorrer. Suponha que

$$2, 3, 5, ..., p$$

são os primos menores que p. Dessa forma todos os números menores que p são divisiveis por um desses primos, então se

$$2 \cdot 3 \cdot 5 \cdot ... \cdot p = q$$

todos os $p - 1$ números

$$q + 2, q + 3, q + 4, \cdots, q + p$$

são compostos.
Para exemplificar o raciocínio desenvolvido acima, vamos considerar todos os números primos até 11.

$$2, 3, 5, 7, 11.$$

Então

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310.$$

Deste modo todos os dez números

$$2312, 2313, ..., 2321.$$

são compostos.
Assim, dado um número primo p é possível determinar um intervalo fechado de números inteiros de comprimento $p - 2$ contendo exatamente $p - 1$ números compostos.

2 Como reconhecer se um número é primo: Os testes de primalidade

Dado um número natural $n > 1$ como afirmar, sem sombra de dúvidas, que tal número é primo. Para números "pequenos" talvez esta tarefa não seja muito difícil visto que efetuando-se divisões sucessivas é possível chegar a conclusões sobre os divisores do número em questão. Entretanto, para números "grandes" esta tarefa não parece ser tão simples como, por exemplo, o número 67891. Um teste (um procedimento, um cálculo, um algoritmo ou programa de computador) que permite decidir se um dado número é primo é chamado de teste de primalidade. Neste capítulo trataremos de um caso particular dos testes de primalidade: os testes de primalidade baseados em congruências. Para tanto exploramos os conceitos de congruência entre dois números naturais e suas principais propriedades, ordem de um elemento, função φ de Euler, Sistema Completo e Sistema Reduzido de Resíduos e o importante Teorema de Euler.

2.1 Congruência

Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são *congruentes* módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \ mod \ m.$$

Por exemplo, $85 \equiv 16 \ mod \ 3$, já que os restos da divisão de 85 e 16 por 3 são iguais a 1.

Quando a relação $a \equiv b \ mod \ m$ for falsa, diremos que a e b não são congruentes, ou que são incongruentes módulo m.

Uma maneira mais simples de verificar se dois números são congruentes é dada pela seguinte proposição.

Proposição 2.1. *Tem-se que $a \equiv b \ mod \ m$ se, e somente se, $m \mid a - b$.*

Demonstração: Se $a \equiv b \ mod \ m$, então existem inteiros k_1, k_2 e r tais que $a = k_1 m + r$ e $b = k_2 m + r$, logo $a - b = m(k_1 - k_2)$ e consequentemente $m \mid a - b$.

Reciprocamente, assumimos que $m \mid a-b$. Pela divisão euclidiana, temos que $a = k_1m + r_1$ e $b = k_2m + r_2$ com $0 \leq r_1 < m$ e $0 \leq r_2 < m$, logo $a - b = m(k_1 - k_2) + (r_1 - r_2)$. Como $m \mid m(k_1 - k_2)$, segue que $m \mid (r_1 - r_2)$, logo $r_1 = r_2$ pois $\mid r_1 - r_2 \mid < m$. Portanto, $a \equiv b \ mod \ m$. ■

Proposição 2.2. *Se a, b, c e m são inteiros tais que $a + c \equiv b + c \ mod \ m$ então $a \equiv b \ mod \ m$*

Demonstração: Por hipótese temos que

$$m \mid (a+c) - (b+c) \Rightarrow m \mid a + c - b - c \Rightarrow m \mid a - b \Rightarrow a \equiv b \ mod \ m$$

■

Teorema 2.3. *Se a, b, c e m são inteiros e $ac \equiv bc \ mod \ m$, então $a \equiv b \ mod \ \frac{m}{d}$, onde $d = (c, m)$.*

Demonstração: Por hipótese, existe $k \in \mathbb{Z}$ tal que $c(a-b) = km$. Se dividirmos os dois membros por d, teremos

$$\left(\frac{c}{d}\right)(a-b) = k\left(\frac{m}{d}\right)$$

Logo,

$$\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a-b)$$

Como $\left(\frac{m}{d}, \frac{c}{d}\right) = 1$, então pelo Teorema 1.11 temos

$$\left(\frac{m}{d}\right) \mid (a-b),$$

isto é,

$$a \equiv b \ mod \ \frac{m}{d}$$

■

2.2 O Pequeno Teorema de Fermat

Teorema 2.4 (Pequeno Teorema de Fermat)**.** *Se p é um número primo e a é um inteiro, então $a^p \equiv a \ mod \ p$. Em particular, se $p \nmid a$, então $a^{p-1} \equiv 1 \ mod \ p$.*

Demonstração: Vamos realizar a demonstração por indução sobre a. Para $a = 1$ tem-se claramente que $a^p \equiv a \ mod \ p$, visto que $a^p = a$ para todo primo p. Vamos assumir que o Teorema seja válido para um certo número inteiro a, isto é, que $a^p \equiv a \ mod \ p$ e mostraremos que o Teorema é válido para $a + 1$. Pelo Teorema Binomial temos $(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \ldots + \binom{p}{p-1}a + 1$, notamos que se $1 \leq k \leq p-1$ então o coeficiente binomial $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ é um múltiplo de p, desta forma : $(a+1)^p \equiv a^p + 1 \equiv a + 1 \ mod \ p$

o que completa a prova por indução.
Por último se $a^p \equiv a \; mod \; p$ pela Proposição 2.1 temos que $p \mid a^p - a$ ou seja $p \mid a(a^{p-1}-1)$. Assim se $p \nmid a$ concluímos que $(p, a) = 1$ e pela Proposição 1.11 temos que $p \mid (a^{p-1}-1)$, utilizando a Proposição 2.1 novamente concluímos que $a^{p-1} \equiv 1 \; mod \; p$. ■

Exemplo 2.5. Determine o resto da divisão de 5^{63} por 29.
Sendo 29 um número primo temos pelo Pequeno Teorema de Fermat que $5^{29} \equiv 5 \; mod \; 29$. Então

$$\begin{aligned} 5^{29} &\equiv 5 \; mod \; 29 \Leftrightarrow \\ 5^{30} &\equiv 25 \; mod \; 29 \Leftrightarrow \\ 5^{60} &\equiv 625 \; mod \; 29 \Leftrightarrow \\ 5^{60} &\equiv 16 \; mod \; 29 \Leftrightarrow \\ 5^3 \cdot 5^{60} &\equiv 5^3 \cdot 16 \; mod \; 29 \Leftrightarrow \\ 5^{63} &\equiv 2000 \; mod \; 29 \Leftrightarrow \\ 5^{63} &\equiv 28 \; mod \; 29 \end{aligned}$$

A última equação nos diz que o resto da divisão de 5^{63} por 29 é igual a 28.

A recíproca do Pequeno Teorema de Fermat: A recíproca do Pequeno Teorema de Fermat é falsa, isto é, não é verdade que se

$$a^{m-1} \equiv 1 \; mod \; m$$

para todo número a tal que $(a, m) = 1$, então m é primo. De fato, escolhendo $m = 561 = 3.11.17$. Se $3 \nmid a$, $11 \nmid a$ e $17 \nmid a$, temos

$$a^2 \equiv 1 \; mod \; 3, \quad a^{10} \equiv 1 \; mod \; 11, \quad a^{16} \equiv 1 \; mod \; 17$$

Entretanto $2 \mid 560$, $10 \mid 560$ e $16 \mid 560$ e então

$$a^{560} \equiv 1 \; mod \; 3, \quad a^{560} \equiv 1 \; mod \; 11, \quad a^{560} \equiv 1 \; mod \; 17$$

Estas últimas congruências garantem que $a^{560} \equiv 1 \; mod \; (3.11.17)$, ou seja: $a^{560} \equiv 1 \; mod \; 561$ e claramente 561 é um número composto. Com este raciocínio mostramos não ser válida a recíproca do Pequeno Teorema de Fermat.
Se

$$a^{m-1} \equiv 1 \; mod \; m$$

é válida para um certo inteiro a e um número composto m nós dizemos que m é um *pseudo-primo* de base a. Se m é um pseudo-primo de base a tal que $(a, m) = 1$, m é chamado de *número de Carmichael*. Não se sabe se existe uma infinidade de números de Carmichael, nem se existe uma infinidade de compostos m tais que $2^m \equiv 2 \; mod \; m$

e $3^m \equiv 3 \ mod \ m$, entretanto o resultado demostrado a seguir mostra que existem infinitos psudos-primos sob certa condição.

Teorema 2.6. *Para cada inteiro $a > 1$ existem infinitos pseudos-primos de base a.*

Demonstração: Seja p um primo ímpar que não divide $a(a^2-1)$. Considere

$$m = \frac{a^{2p}-1}{a^2-1} = \frac{(a^p-1).(a^p+1)}{(a-1).(a+1)} = \left(\frac{a^p-1}{a-1}\right)\cdot\left(\frac{a^p+1}{a+1}\right)$$

Claramente m é um número composto, vamos mostrar que m é um pseudo-primo de base a, ou seja, vamos mostrar que é válida a seguinte relação

$$a^{m-1} \equiv 1 \ mod \ m.$$

Note que

$$(a^2-1).(m-1) = a^{2p} - a^2 = (a^p-a).(a^p+a) = a.(a^{p-1}-1).(a^p+a)$$

Como a e a^p são ambos pares ou ambos ímpares temos que $2 \mid a^p + a$. E ainda $a^{p-1} - 1$ é divisível por p (pelo Pequeno Teorema de Fermat) e por (a^2-1). Por hipótese p foi escolhido de modo que $p \nmid a^2 - 1$, assim concluímos que $p(a^2-1) \mid a^{p-1} - 1$. E então

$$2p \mid a(a^p+a)(a^{p-1}-1) = (a^2-1)(m-1).$$

Deste modo concluí-se que

$$2p \mid m-1.$$

Desta última relação podemos afirmar que existe $k \in \mathbb{R}$ tal que $m - 1 = 2pk$, daí

$$a^{2p} = 1 + m(a^2-1) \equiv 1 \ mod \ m.$$

E então de $a^{2p} \equiv 1 \ mod \ m$ podemos concluir que

$$a^{2pk} \equiv 1 \ mod \ m,$$

Obtendo então que

$$a^{m-1} = a^{2pk} \equiv 1 \ mod \ m$$

Isto é

$$a^{m-1} \equiv 1 \ mod \ m$$

Como nós temos um diferente valor de m para cada primo ímpar que não divide $a(a^2-1)$, o teorema está provado. ■

2.3 A divisibilidade de $2^{p-1}-1$ por p^2

Dado um número primo p vamos examinar a possibilidade de ocorrência de uma condição específica para congruências envolvendo os números $p-1$ e p^2.
Pelo pequeno Teorema e Fermat temos que

$$2^{p-1}-1 \equiv 0 \ mod\ p, \quad \text{se} \quad p>2.$$

É possível que exista um número primo de modo que

$$2^{p-1}-1 \equiv 0 \ mod\ p^2.$$

Para ilustrar a questão observe que

- Para $p=3$ temos $p-1=2$ e $p^2=9$ e então

$$2^{p-1}-1=3 \equiv 3 \ mod\ 9.$$

- Para $p=5$ temos $p-1=4$ e $p^2=25$ e então

$$2^{p-1}-1=15 \equiv 15 \ mod\ 25.$$

- Para $p=7$ temos $p-1=6$ e $p^2=49$ e então

$$2^{p-1}-1=63 \equiv 14 \ mod\ 49.$$

- Para $p=11$ temos $p-1=10$ e $p^2=121$ e então

$$2^{p-1}-1=1023 \equiv 55 \ mod\ 121.$$

- Para $p=13$ temos $p-1=12$ e $p^2=169$ e então

$$2^{p-1}-1=4095 \equiv 39 \ mod\ 169.$$

$$\vdots$$

- Para $p=373$ temos $p-1=372$ e $p^2=139.129$ e então

$$2^{p-1}-1=2^{372}-1 \equiv 76.092 \ mod\ 139.129.$$

De acordo [3], no desenvolvimento da teoria para a resolução do *"Último Teorema de Fermat"* uma questão importante é determinar os números primos para os quais

$$2^{p-1}-1 \equiv 0 \ mod\ p^2.$$

Este fato pode ocorrer, contudo muito raramente, conforme sugere o próximo exemplo.

Exemplo 2.7. Existe um número primo p para o qual

$$2^{p-1}-1 \equiv 0 \ mod\ p^2.$$

De fato isto é válido quando $p = 1093$, conforme os cálculos a seguir.
Se $p = 1093$, então $p^2 = 1194649$ e deste modo

$$3^7 = 2187 = 2p+1 \Rightarrow$$

$$3^{14} = (2p+1)^2 = 4p^2+4p+1 \equiv 4p+1 \ mod\ p^2.$$

E ainda

$$2^{14} = 16384 = 15p-11 \Rightarrow$$

$$2^{28} = (15p-11)^2 = 225p^2-330p+121 \equiv -330p+121 \ mod\ p^2.$$

Daí

$$3^2.2^{28} \equiv -2970p+1089 = -2969p-4 \equiv -1876p-4 \ mod\ p^{2\cdot}$$

Dividindo esta última expressão por 2^2 chegamos a

$$3^2.2^{26} \equiv -469p-1 \ mod\ p^2.$$

Asim, temos

$$3^{14}.2^{182} = (3^2.2^{26})^7 \equiv (-469p-1)^7 \ mod\ p^2.$$

Agora, utilizando o Teorema Binomial

$$\begin{aligned}(-469p-1)^7 &= -\left(\sum_{k=0}^{7}\binom{n}{k}(469p)^{n-k}(1)^{n-k}\right)\\ &\equiv -\left(\binom{7}{6}(469p)^1(1)^6+\binom{7}{7}(469p)^0(1)^7\right) \ mod\ p^2.\end{aligned}$$

Como

$$-\left(\binom{7}{6}(469p)^1(1)^6+\binom{7}{7}(469p)^0(1)^7\right) = -(7.(469p)+1) = -(3283p+1) \equiv -(4p+1)\ mod\, p^2,$$

e

$$-3^{14} \equiv -(4p+1) \ mod\ p^2,$$

então

$$(-469p-1)^7 \equiv -3^{14} \ mod \ p^2.$$

Daí,

$$3^{14}2^{182} \equiv -3^{14} \ mod \ p^2,$$

isto é

$$2^{182} \equiv -1 \ mod \ p^2.$$

Elevando a 6 esta última congruência obtemos

$$2^{1092} \equiv 1 \ mod \ p^2.$$

Como queríamos.

2.4 A Ordem de um elemento

Definição 2.8. *Suponha que $a, m \in \mathbb{N}^*$, com $m > 1$ e $(a, m) = 1$, definimos a* ***ordem de a*** *com relação a m como sendo o menor expoente natural h para o qual $a^h \equiv 1 \ mod \ m$, neste caso escrevemos: $h = ord_m(a)$.*

Observação 2.9. A existência de um número h tal que $a^h \equiv 1 \ mod \ m$ quando $(a, m) = 1$ é uma consequência imediata Teorema de Euler que será abordado na seção 2.7.

Exemplo 2.10. A ordem de 2 módulo 7 é 3, pois

$$\begin{aligned} 2^1 &\equiv 2 \ mod \ 7 \\ 2^2 &\equiv 4 \ mod \ 7 \\ 2^3 &\equiv 1 \ mod \ 7 \end{aligned}$$

Exemplo 2.11. A ordem de 5 módulo 18 é 6, pois

$$\begin{aligned} 5^1 &\equiv 5 \ mod \ 18 \\ 5^2 &\equiv 7 \ mod \ 18 \\ 5^3 &\equiv 17 \ mod \ 18 \\ 5^4 &\equiv 13 \ mod \ 18 \\ 5^5 &\equiv 11 \ mod \ 18 \\ 5^6 &\equiv 1 \ mod \ 18 \end{aligned}$$

2.5 A função φ de Euler

Definição 2.12. *Para cada $n > 1$, seja $\varphi(n)$ a quantidade de números inteiros a, $1 \leq a < n$, tais que $(a, n) = 1$. Isto define uma importante função*

$$\varphi : \mathbb{N}^* \to \mathbb{N},$$

chamada função φ de Euler.

Pela definição anterior, temos que

$$\varphi(n) \leq n - 1.$$

Além do mais $\varphi(n) = n - 1$ se, e somente se, n é um número primo. Os resultados a seguir serão úteis para determinarmos uma expressão para $\varphi(n)$.

Proposição 2.13. *Se p é um número primo e r, um número natural, então tem-se*

$$\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right).$$

Demonstração: Pela definição de $\varphi(n)$ sabemos que $\varphi(p^r)$ é o número de inteiros positivos não superiores a p^r e relativamente primos com p^r. Mas os únicos números não primos com p^r e menores do que ou iguais a p^r são aqueles divisiveis por p. Como os múltiplos de p não superiores a p^r são, em número, p^{r-1}, o resultado segue. ■

Exemplo 2.14. Observe

$$\varphi(9) = \varphi(3^2) = 3^2 - 3 = 9 - 3 = 6.$$

$$\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 125 - 25 = 100.$$

2.6 Sistema completo e sitema reduzido de resíduos

Definição 2.15. *O conjunto dos inteiros $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo m se*

(i) $r_i \not\equiv r_j \bmod m$, para $i \neq j$;

(ii) Para todo inteiro n existe um inteiro r_i tal que $n \equiv r_i \bmod m$.

Exemplo 2.16. O conjunto $\{0, 1, 2, \cdots, m-1\}$ é um sistema completo de resíduos módulo m.

Teorema 2.17. *Se $r_1, r_2, ..., r_m$ é um sistema completo de resíduos módulo m e a e b são interios com $(a, m) = 1$, então*

$$ar_1 + b, ar_2 + b, ..., ar_m + b,$$

também é um sistema completo de resíduos módulo m.

Demonstração: Vamos mostrar que quaisquer dois inteiros do conjunto $ar_1 + b, ar_2 + b, ..., ar_m + b$, são incongruentes módulo m. Para isto vamos supor que $ar_i + b \equiv ar_j + b \ mod \ m$. Logo, pela Proposição 2.2, temos $ar_i \equiv ar_j \ mod \ m$. Mas, como $(a, m) = 1$, o Teorema 2.3 nos diz que $r_i \equiv r_j \ mod \ m$. O fato de que $r_i \equiv r_j \ mod \ m$ implica $i = j$, uma vez que $r_1, r_2, ..., r_m$ formam um sistema completo de resíduos módulo m. Deste modo $ar_1 + b, ar_2 + b, ..., ar_m + b$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. ■

Exemplo 2.18. O conjunto $\{12, 25, 74, 111, 148, 281, 546, 991, 1052, 1125, 1354, 1547\}$ é um sistema completo de resíduos módulo 12. Como $(5, 12) = 1$ para qualquer $b \in \mathbb{Z}$ o conjunto

$\{5 \cdot 12 + b, 5 \cdot 25 + b, 5 \cdot 74 + b, 5 \cdot 111 + b, 5 \cdot 148 + b, 5 \cdot 281 + b, 5 \cdot 546 + b, 5 \cdot 991 + b,$
$5 \cdot 1052 + b, 5 \cdot 1125 + b, 5 \cdot 1354 + b, 5 \cdot 1547 + b\}$,

também é um sistema completo de resíduos módulo 12.
Por exemplo, se $b = 3$ teríamos

$$\{63, 128, 373, 558, 743, 1408, 2733, 4958, 5263, 5628, 6773, 7738\}.$$

Definição 2.19. *O conjunto dos inteiros $\{r_1, r_2, \cdots, r_j\}$ é um sistema reduzido de resíduos módulo m se*

(i) $(r_i, m) = 1$, *para todo* $i = 1, \cdots, j$;

(ii) $r_i \not\equiv r_j \ mod \ m$, *para* $i \neq j$;

(iii) Para todo inteiro n tal que $(n, m) = 1$ existe um inteiro r_i tal que $n \equiv r_i \ mod \ m$.

Pode-se obter um sistema reduzido de resíduos módulo m a partir de um sistema completo de resíduos módulo m, bastando para isso eleminar no sistema completo de resíduos todos os elementos que não são primos com m.

Observação: Um sistema reduzido de resíduos módulo m possui exatamente $\varphi(m)$ elementos, pois se a é um elemento qualquer de um sistema reduzido de resíduos módulo m por definição temos que $(a, m) = 1$, ou seja, todo elemento de um sistema reduzido de resíduos módulo m é primo com m, ademais se $b < m$ é tal que $(b, m) = 1$ e b não pertence ao sistema reduzido de resíduos módulo m existe um elemento c que pertence ao sistema reduzido de resíduos módulo m tal que $b \equiv c \ mod \ m$ e pelo fato que quaisquer dois elementos de um sistema reduzido de resíduos módulo m são incongruentes podemos assegurar que este representante é único. Desta forma podemos concluir que os elementos que são primos com m petencem ao sistema reduzido de resíduos ou possui um único representante em tal sistema, ou seja, a quantidade de elementos em um sistema reduzido de resíduos coincide com o valor de $\varphi(m)$ uma vez que $\varphi(m)$ nos revela a quantidade de números que são primos com m.

Exemplo 2.20. O conjunto $A = \{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, como os números $0, 2, 4$ e 6 não são primos com 8 temos que o conjunto $B = \{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8 e ainda $\varphi(8) = 4$ que é justamente a quantidade de elementos do conjunto B.

Proposição 2.21. *Seja* $\{r_1, \cdots, r_{\varphi(m)}\}$ *um sistema reduzido de resíduos módulo* m *e seja* $a \in \mathbb{N}$ *tal que* $(a, m) = 1$. *Então* $\{ar_1, \cdots, ar_{\varphi(m)}\}$ *é um sistema reduzido de resíduos módulo* m.

Demonstração: Seja $\{a_1, \cdots, a_m\}$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos $\{r_1, \cdots, r_{\varphi(m)}\}$. Do fato de que $(a_i, m) = 1$ se, e somente se, $(aa_i, m) = 1$, o resultado segue. ■

Teorema 2.22. *A função* φ *de Euler é multiplicativa, isto é* $\varphi(mn) = \varphi(m)\varphi(n)$ *quando* $(m, n) = 1$.

Demonstração: Vamos dispor os números de 1 até mn da seguinte forma

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \cdots & (n-1)m+3 \\ & & & \vdots & \\ m & 2m & 3m & \cdots & nm. \end{array}$$

Mostraremos que a a quantidade de números primos com $m{\cdot}n$ no conjunto $\{1, 2, 3..., m \cdot n\}$ é igual a $\varphi(m)\varphi(n)$. Para tal analisaremos a tabela acima: se em uma tinha r, onde estão os termos $r, m + r, 2m + r, \cdots, (n-1)m + r$, tivermos $(m, r) = d > 1$, então nenhum termo nesta linha será primo com mn, uma vez que estes termos, sendo da forma $km{+}r$, $0 \leq k \leq n-1$, são todos divisiveis por d que é o máximo divisor comum de m e r. Logo, para encontrar os inteiros desta tabela que são primos com mn, devemos olhar na linha r somente se $(m, r) = 1$. Sabemos que $\varphi(m)$ nos revela a quantidade de elementos que são primos com m, deste modo na primeira coluna onde estão os elementos $\{1, 2, ..., m\}$ há exatamente $\varphi(m)$ elementos que são primos com m. Ou seja há $\varphi(m)$ linhas cujo primeiro elemento é primo com m. Agora em cada uma dessas linhas vamos procurar descobrir quantos são os elementos primos com n. O conjunto $\{1, 2, ..., n-1\}$ é um sistema completo de resíduos módulo n e como $(m, n) = 1$ o Teorema 2.17 garante que o conjunto $\{r, m + r, 2m + r, \cdots, (n-1)m + r\}$ também é um sistema completo de resíduos módulo n. Logo cada uma destas linhas possui $\varphi(n)$ elementos primos com n e, como eles são primos com m, eles são primos com mn. Esta contagem mostra que há $\varphi(m)\varphi(n)$ elementos que são primos com $m \cdot n$, o que nos permite concluir que $\varphi(mn) = \varphi(m)\varphi(n)$. ■

Finalmente o próximo resultado nos mostra como calcular $\varphi(n)$.

Teorema 2.23. *Se $n = {p_1}^{r_1}\cdots{p_k}^{r_k}$ é a decomposição de n em fatores primos, então*

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Demonstração: Pela Proposição 2.13 temos

$$\varphi(p_i^{r_i}) = p_i^{r_i} - p_i^{r_i-1} = p_i^{r_i}\left(1-\frac{1}{p_i}\right).$$

Portanto, o Teorema 2.22 nos garante que

$$\begin{aligned}\varphi({p_1}^{r_1}\cdots{p_k}^{r_k}) &= p_1^{r_1}\left(1-\frac{1}{p_1}\right)p_2^{r_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{r_k}\left(1-\frac{1}{p_k}\right)\\ &= {p_1}^{r_1}{p_2}^{r_2}\cdots{p_k}^{r_k}\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

■

A fórmula do Teorema 2.23 pode ser reescrita da seguinte maneira:

$$\varphi({p_1}^{r_1}\cdots{p_k}^{r_k}) = {p_1}^{r_1-1}\cdots{p_k}^{r_k-1}(p_1-1)\cdots(p_k-1).$$

2.7 O Teorema de Euler

Nesta seção vamos abordar um importante resultado envolvendo a função φ de Euler.

Teorema 2.24 (**Euler**). *Sejam $m, a \in \mathbb{N}$ com $m > 1$ e $(a, m) = 1$. Então*

$$a^{\varphi(m)} \equiv 1 \ mod\ m.$$

Demonstração: Seja $\{r_1, \cdots, r_{\varphi(m)}\}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição 2.21, $\{ar_1, \cdots, ar_{\varphi(m)}\}$ formam um sistema reduzido de resíduos módulo m. Portanto,

$$a^{\varphi(m)} r_1 \cdot r_2\cdots r_{\varphi(m)} = ar_1 \cdot ar_2\cdots ar_{\varphi(m)} \equiv r_1 \cdot r_2\cdots r_{\varphi(m)} \ mod\ m.$$

Como $(r_1 \cdot r_2\cdots r_{\varphi(m)}, m) = 1$, é válida a lei do cancelamento com relação à multiplicação e então

$$a^{\varphi(m)} \equiv 1 \ mod\ m.$$

■

Uma consequência imediata do Teorema de Euler é que se $a, m \in \mathbb{N}$ com $(a, m) = 1$ então $ord_m(a) \mid \varphi(m)$.

Exemplo 2.25. Vamos utilizar o Teorema de Euler e obter o resto da divisão de 5^{60} por 26.

Inicialmente temos que

$$\varphi(26) = \varphi(2.13) = \varphi(2).\varphi(13) = 2^0(2-1)13^0(13-1) = 1.12 = 12.$$

Como $(5, 26) = 1$, então o Teorema de Euler nos garante que

$$5^{12} \equiv 1 \ mod\ 26.$$

Logo,

$$5^{12} \equiv 1 \ mod\ 26 \Rightarrow 5^{5.12} \equiv 1 \ mod\ 26.$$

Portanto, 1 é o resto da divisão de 5^{60} por 26.

2.8 Testes de primalidade baseados em congruências

Nesta seção abordaremos testes de primalidade baseados em congruências. Estes testes estão presentes em [2]. Inicialmente apresentaremos a recíproca do Pequeno Teorema de Fermat, descoberto por Lucas em 1876.

Teorema 2.26 (Primeiro Teste de Lucas)**.** *Seja $N > 1$. Assuma que exista um inteiro $a > 1$ tal que*

(i) $a^{N-1} \equiv 1 \ mod\ N$;

(ii) $a^m \not\equiv 1 \ mod\ N$, *para* $m = 1, 2, \cdots, N-2$.

Então N é primo.

Demonstração: É suficiente mostrar que para cada inteiro m, $1 \leq m < N$, é primo com N, isto é que $\varphi(N) = N - 1$. Para este propósito é suficiente mostrar que existe a, $1 \leq a < N$, $mdc(a, N) = 1$, de modo que a ordem de a $(mod\ N)$ é $N - 1$. Isto está implicito exatamente nas hipóteses. ■

Em 1891, Lucas apresentou o seguinte teste:

Teorema 2.27 (Segundo Teste de Lucas)**.** *Seja $N > 1$. Assuma que exista um inteiro $a > 1$ tal que*

(i) $a^{N-1} \equiv 1 \ mod\ N$;

(ii) $a^m \not\equiv 1 \ mod\ N$, *para qualquer divisor m de $N-1$* $(m < N-1)$.

Então N é primo.

Demonstração: Certamente temos que $(a, N) = 1$. Se d é a ordem de a $(mod\ N)$ então $d \mid (N-1)$ e $d \mid \varphi(N)$. Como $a^d \equiv 1\ mod\ N$, e d é um divisor de $N-1$ devemos ter:

(i) $d = N - 1$;

(ii) $N - 1 \mid \varphi(N)$.

Porém

$$\varphi(N) = N.\prod_{p|N}\left(1 - \frac{1}{p}\right) < N - 1,$$

se N é composto. Logo N deve ser um número primo, como desejávamos. ■

Em 1967, Brillhart e Selfridge tornaram o teste de Lucas mais flexível:

Teorema 2.28. *Seja $N > 1$. Assuma que para cada fator primo q de $N-1$ exista um inteiro $a = a(q) > 1$ tal que*

(i) $a^{N-1} \equiv 1\ mod\ N$.

(ii) $a^{\left(\frac{N-1}{q}\right)} \not\equiv 1\ mod\ N$;

Então N é primo.

Antes de realizarmos a demonstração deste resultado vamos tecer alguns esclarecimentos a respeito dos testes apresentados até o presente momento. Inicialmente é necessário obsevar que este último teste requer a necessidade de conhecer todos o fatores primos de $N-1$, entretanto, exige que menos congruências sejam satisfeitas quando comparado aos testes de Lucas.
Em uma análise mais aprofundada, podemos notar que, afinal, para verificar que $a^{N-1} \equiv 1\ mod\ N$ é necessário em particular obter o resíduo de a^n módulo N (para cada $n \leq N-1$, e desta forma o Primeiro Critério de Lucas poderia ter sido usado. O ponto é que existe um algoritmo rápido para encontrar a potência a^n, e consequentemente $a^n \equiv 1\ mod\ N$ sem computar todas as potências precedentes. Ele é executado da seguinte forma: Escreva o expoente n na base 2

$$n = n_0 2^k + n_1 2^{k-1} + n_2 2^{k-2} + \cdots + n_{k-1} 2 + n_k 2^0,$$

onde cada n_i é igual a 0 ou 1, e $n_0 = 1$.
Fazemos

$$s_0 = n_0 = 1,$$

e se s_j foi calculado, calculamos s_{j+1} do seguinte modo

$$s_{j+1} = 2s_j + n_{j+1}.$$

Seja

$$r_j = a^{s_j}.$$

Assim

$$r_{j+1} = a^{s_{j+1}} = a^{2s_j+n_{j+1}} = a^{2s_j}.a^{n_{j+1}}$$

Deste modo

$$r_{j+1} = {r_j}^2.a^{n_{j+1}}.$$

Então temos

$$r_{j+1} = \begin{cases} {r_j}^2 & \text{quando } n_{j+1} = 0 \\ a.{r_j}^2 & \text{quando } n_{j+1} = 1. \end{cases}$$

Note que $r_k = a^n$ então é somente necessário executar $2k$ operações, um quadrado ou uma multiplicação por a.
No cálculo de $a^n \equiv 1 \; mod \; N$, então isto é mais fácil ainda, visto que em cada etapa r_j está sendo substituído por seu resíduo módulo N. Agora, k é igual a

$$\left[\frac{\log n}{\log 2}\right],$$

onde $[x]$ representa o maior inteiro menor do que ou igual a x.
De fato, pois se k é o maior expoente inteiro para o qual $2^k \leq n < 2^{k+1}$ então

$$k \log 2 \leq \log n < (k+1) \log 2,$$

ou seja

$$k \leq \frac{\log n}{\log 2} < k + 1$$

Esta última desigualdade é satisfeita sempre que

$$k = \left[\frac{\log n}{\log 2}\right].$$

Assim, se $n = N - 1$, então somente

$$2\left[\frac{\log(N-1)}{\log 2}\right]$$

operações serão necessárias para encontrar $a^{N-1} \equiv 1 \; mod \; N$ e não há necessidade de se calcular todas as potências $a^n \equiv 1 \; mod \; N$. Agora vamos proceder a **demonstração do teste de Brillhart e Selfridge - Teorema 2.28**.

Demonstração: A prova é por contradição. Devemos mostrar que $\varphi(N) = N - 1$, e como $\varphi(N) \leq N - 1$, é suficiente mostrar que $N - 1$ divide $\varphi(N)$. Vamos supor que $N - 1 \nmid \varphi(N)$, desta forma existe um primo q e um $r \geq 1$ tal que q^r divide $N - 1$; porém $q^r \nmid \varphi(N)$. Seja $a = a(q)$ e seja e a ordem de a $(mod \; N)$. Desta forma e divide $N - 1$ e não divide $\left(\frac{N-1}{q}\right)$, assim q^r divide e. Como $a^{\varphi(N)} \equiv 1 \; mod \; N$ temos $e \mid \varphi(N)$, assim $q^r \mid \varphi(N)$, o que é uma contradição, assim concluímos a prova. ■

Exemplo 2.29. Vamos utilizar o algoritmo descrito anteriormente para obter o resíduo de 2^{6960} módulo 6961.

Neste caso temos $a = 2$ e $N = 6961$. O número de operações necessárias é

$$2\left[\frac{\log(6960)}{\log 2}\right] = 2\left[12,7648...\right] = 2 \cdot 12 = 24.$$

Inicialmente vamos escrever o número 6960 na base 2

$$(6960)_{10} = (1101100110000)_2 .$$

Colocamos

$$s_0 = n_0 = 1.$$

Fazendo

$$s_{j+1} = 2s_j + n_{j+1}.$$

Temos

$$s_1 = 2s_0 + n_1 = 2 \cdot 1 + 1 = 3$$

$$s_2 = 2s_1 + n_2 = 2 \cdot 3 + 0 = 6$$

$$s_3 = 2s_2 + n_3 = 2 \cdot 6 + 1 = 13$$

$$s_4 = 2s_3 + n_4 = 2 \cdot 13 + 1 = 27$$

$$s_5 = 2s_4 + n_5 = 2 \cdot 27 + 0 = 54$$

$$s_6 = 2s_5 + n_6 = 2 \cdot 54 + 0 = 108$$

$$s_7 = 2s_6 + n_7 = 2 \cdot 108 + 1 = 217$$

$$s_8 = 2s_7 + n_8 = 2 \cdot 217 + 1 = 435$$

$$s_9 = 2s_8 + n_9 = 2 \cdot 435 + 0 = 870$$

$$s_{10} = 2s_9 + n_10 = 2 \cdot 870 + 0 = 1740$$

$$s_{11} = 2s_{10} + n_{11} = 2 \cdot 1740 + 0 = 3480$$

$$s_{12} = 2s_{11} + n_{12} = 2 \cdot 3480 + 0 = 6960$$

Lembrando que $r_j = a^{s_j}$ e $r_{j+1} = {r_j}^2 \cdot a^{n_{j+1}}$ temos

$$r_0 = 2^{s_0} = 2^1 = 2$$

$$r_1 = r_0^2 \cdot 2^{n_1} = 2^2 \cdot 2^1 = 4 \cdot 2 = 8 \equiv\ 8\ mod\ 6961$$

$$r_2 = r_1^2 \cdot 2^{n_2} = 8^2 \cdot 2^0 = 64 \cdot 1 = 64 \equiv\ 64\ mod\ 6961$$

$$r_3 = r_2^2 \cdot 2^{n_3} = 64^2 \cdot 2^1 = 4096 \cdot 2 = 8192 \equiv\ 1231\ mod\ 6961$$

$$r_4 = r_3^2 \cdot 2^{n_4} = 1231^2 \cdot 2^1 = 1515361 \cdot 2 = 3030722 \equiv\ 2687\ mod\ 6961$$

$$r_5 = r_4^2 \cdot 2^{n_5} = 2687^2 \cdot 2^0 = 7219969 \cdot 1 = 7219969 \equiv\ 1412\ mod\ 6961$$

$$r_6 = r_5^2 \cdot 2^{n_6} = 1412^2 \cdot 2^0 = 1993744 \cdot 1 = 1993744 \equiv\ 2898\ mod\ 6961$$

$$r_7 = r_6^2 \cdot 2^{n_7} = 2898^2 \cdot 2^1 = 8398404 \cdot 2 = 16796808 \equiv\ 6876\ mod\ 6961$$

$$r_8 = r_7^2 \cdot 2^{n_8} = 6876^2 \cdot 2^1 = 47279376 \cdot 2 = 94558752 \equiv\ 528\ mod\ 6961$$

$$r_9 = r_8^2 \cdot 2^{n_9} = 528^2 \cdot 2^0 = 278784 \cdot 1 = 278784 \equiv\ 344\ mod\ 6961$$

$$r_{10} = r_9^2 \cdot 2^{n_{10}} = 344^2 \cdot 2^0 = 118336 \cdot 1 = 118336 \equiv\ 6960\ mod\ 6961$$

$$r_{11} = r_{10}^2 \cdot 2^{n_{11}} = 6960^2 \cdot 2^0 = 48441600 \cdot 1 = 48441600 \equiv\ 1\ mod\ 6961$$

$$r_{12} = r_{11}^2 \cdot 2^{n_{12}} = 1^2 \cdot 2^0 = 1 \cdot 1 = 1 \equiv\ 1\ mod\ 6961$$

Como $r_{12} = 2^{s_{12}} = 2^{6960}$, conclímos que

$$2^{6960} \equiv\ 1\ mod\ 6961.$$

Relacionando os cálculos envolvidos no desenvolvimento do algoritmo podemos determinar outros resíduos, por exemplo, $r_5 = 2^{s_5}$ o que nos permite concluir que $2^{54} \equiv 1412\ mod\ 6961$.

Vamos apresentar agora um teste de primalidade que permite testar a primalidade de um número N, quando escrito de certa maneira (este teste pode ser encontrado em [3]).

Teorema 2.30. *Se $p > 2$, $h < p$, $N = hp + 1$ ou $hp^2 + 1$ e*

(i) $2^{N-1} \equiv 1\ mod\ N$;

(ii) $2^h \not\equiv 1\ mod\ N$.

Então N é primo.

Demonstração: Nós escrevemos $N = hp^b + 1$, onde $b = 1$ ou $b = 2$, e vamos supor d como sendo a ordem de 2 $(mod\ N)$ então $d \nmid h$ e $d \mid N - 1$ isto é $d \mid hp^b$ e assim $d \mid p^b$ o que assegura que $d \mid p$ e $d \mid p^2$ donde concluímos que $p \mid d$.
Porém

$$d \mid \varphi(N),$$

e então

$$p \mid \varphi(N).$$

Se

$$N = p_1^{\alpha_1}.\cdots.p_k^{\alpha_k}$$

nos temos

$$\varphi(N) = p_1^{\alpha_1 - 1}.\cdots.p_k^{\alpha_{k-1}}(p_1 - 1).\cdots.(p_k - 1),$$

e como $p \nmid N$ então p deve dividir pelo menos um dos fatores $(p_1-1), (p_2-1), \cdots, (p_k-1)$. Então N possui um fator primo P tal que

$$P \equiv\ 1\ mod\ p.$$

Para P primo e $m \geq 1$ podemos escrever N da seguinte maneira

$$N = Pm. \tag{2.1}$$

Como

(i) $N \equiv 1 \ mod \ p$;

(ii) $P \equiv 1 \ mod \ p$.

Chegamos à seguinte conclusão

$$Pm \equiv m \ mod \ p \Rightarrow N \equiv m \ mod \ p \Rightarrow m \equiv 1 \ mod \ p.$$

Se $m > 1$, podemos encontrar u e v, $1 \leq u \leq v$ de modo que

$$\begin{cases} P = up + 1 \\ m = vp + 1 \end{cases}$$

Desta forma

$$N = (up + 1)(vp + 1),$$

e ainda

$$N = hp^b + 1 \Leftrightarrow$$

$$(up + 1)(vp + 1) = hp^b + 1 \Leftrightarrow$$

$$uvp^2 + up + vp + 1 = hp^b + 1 \Leftrightarrow$$

$$hp^{b-1} = uvp + u + v.$$

Se $b = 1$ temos

$$h = uvp + u + v,$$

e então

$$p \leq uvp < h < p,$$

o que é uma **contradição**.
Se $b = 2$ temos:
De $hp = uvp + u + v$ concluímos que

$$p \mid (u + v),$$

de modo que

$$(u + v) \geq p.$$

Como $v \geq u$ temos que $2v \geq u + v$.
Assim

$$2v \geq u + v \geq p \Rightarrow$$

$$v \geq \frac{p}{2}.$$

E também

$$hp = uvp + u + v \geq uvp + p = p(uv + 1) \Rightarrow$$

$$h \geq uv + 1.$$

Como $uv + 1 \geq uv$ obtemos a seguinte desigualdade

$$h \geq uv.$$

Deste modo

$$uv < h < p \Rightarrow$$

$$uv \leq p - 2.$$

Desta última desigualdade concluímos que

$$u \leq \frac{p-2}{v} \leq \frac{2(p-2)}{p} = 2 - \frac{4}{p}.$$

Ou seja

$$u < 2.$$

Então $u = 1$ e como $u + v \geq p$ temos que

$$v \geq p - 1,$$

esta última desigualdade nos permite concluir que

$$uv \geq p - 1,$$

o que é uma **contradição**, pois $uv \leq p - 2$.
Logo 2.1 só é possível quando $m = 1$ e $n = P$, ou seja, N é um número primo, como desejávamos. ■

Exemplo 2.31. Vamos mostrar que o número 911 é um número primo.

Podemos utilizar o Teorema 2.28. Seja $N = 911$, então $N - 1 = 910 = 2 \cdot 5 \cdot 7 \cdot 13$. Realizamos os seguintes cálculos

A. Para o fator primo $q = 2$ escolhemos $a = 7$ e verificamos que

$$7^{910} \equiv 1 \ mod\ 911$$

$$7^{\frac{910}{2}} = 7^{455} \equiv -1 \ mod\ 911 \not\equiv 1 \ mod\ 911.$$

B. Para o fator primo $q = 5$ escolhemos $a = 3$ e verificamos que

$$3^{910} \equiv 1 \ mod\ 911$$

$$3^{\frac{910}{5}} = 3^{182} \equiv 482 \ mod\ 911 \not\equiv 1 \ mod\ 911.$$

C. Para o fator primo $q = 7$ escolhemos $a = 2$ e verificamos que

$$2^{910} \equiv 1 \ mod\ 911$$

$$2^{\frac{910}{7}} = 2^{130} \equiv 568 \ mod\ 911 \not\equiv 1 \ mod\ 911.$$

D. Para o fator primo $q = 13$ escolhemos $a = 2$ e verificamos que

$$2^{910} \equiv 1 \ mod\ 911$$

$$2^{\frac{910}{13}} = 2^{70} \equiv 570 \ mod\ 911 \not\equiv 1 \ mod\ 911.$$

Desta maneira o Teorema 2.28 nos garante que o número 911 é um número primo.

Exemplo 2.32. Vamos mostrar que o número 67891 é um número primo.

Novamente utilizamos o Teorema 2.28. Seja $N = 67891$, então $N - 1 = 67890 = 2 \cdot 3 \cdot 5 \cdot 31 \cdot 73$.
Realizamos os seguintes cálculos:

A. Para o fator primo $q = 2$ escolhemos $a = 2$ e verificamos que

$$2^{67890} \equiv 1 \ mod\ 67891$$

$$2^{\frac{67890}{2}} = 2^{33945} \equiv -1 \ mod\ 67891 \not\equiv 1 \ mod\ 67891.$$

B. Para o fator primo $q = 3$ escolhemos $a = 7$ e verificamos que

$$7^{67890} \equiv 1 \ mod\ 67891$$

$$7^{\frac{67890}{3}} = 7^{22630} \equiv 6908 \ mod\ 67891 \not\equiv 1 \ mod\ 67891.$$

C. Para o fator primo $q = 5$ escolhemos $a = 11$ e verificamos que

$$11^{67890} \equiv 1 \ mod\ 67891$$

$$11^{\frac{67890}{5}} = 7^{13578} \equiv 37301 \ mod\ 67891 \not\equiv 1 \ mod\ 67891.$$

D. Para o fator primo $q = 31$ escolhemos $a = 3$ e verificamos que

$$3^{67890} \equiv 1 \ mod\ 67891$$

$$3^{\frac{67890}{31}} = 3^{2190} \equiv 60178 \ mod\ 67891 \not\equiv 1 \ mod\ 67891.$$

E. Para o fator primo $q = 73$ escolhemos $a = 5$ e verificamos que

$$5^{67890} \equiv 1 \ mod\ 67891$$

$$5^{\frac{67890}{73}} = 5^{930} \equiv 62741 \ mod\ 67891 \not\equiv 1 \ mod\ 67891.$$

Desta maneira o Teoreman 2.28 nos garante que o número 67891 é um número primo.

Exemplo 2.33. Vamos mostrar que o número 11299 é um número primo.

Podemos aplicar o Teorema 2.30, da seguinte maneira

$$N = 11299 = 42 \cdot 269 + 1.$$

Escolhemos $h = 42$ e $p = 269$, deste modo

$$2^{N-1} = 2^{11298} \equiv 1 \ mod \ 11299$$

$$2^{42} \equiv 606 \ mod \ 11299 \not\equiv 1 \ mod \ 11299.$$

Desta forma o Teorema 2.30 nos garante que o número 11299 é um número primo.

3 Algumas estimativas sobre a distribuição dos Números Primos

Neste capítulo centraremos nossos estudos em dois resultados centrais sobre a distribuição dos números primos o Teorema de Chebyshev e o Teorema dos Números Primos, o primeiro deles nos informa que é possível obter uma aproximação da função $\pi(x)$ para determinadas constantes apropriadas já o segundo mostra uma aproximação da função $\pi(x)$ quando x tende ao infinito. Os resultados que serão abordados e discutidos neste capítulo podem ser encontados em [5].

3.1 O Teorema de Chebyshev

Proposição 3.1 (Fatores do Fatorial)**.** *Seja p um número primo. Então a maior potência de p que divide $n!$ é p^α onde*

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

onde $\left[\frac{a}{b}\right]$ representa o quociente da divisão euclidiana de a por b.

Observe que a soma acima é finita pois os termos $\left[\frac{n}{p^i}\right]$ são eventualmente zero.

Demonstração: No produto $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot n$, apenas os múltiplos de p contribuem com um fator p. Há $\left[\frac{n}{p}\right]$ de tais múltiplos entre 1 e n. Destes os que são múltiplos de p^2 contribuem com um fator p extra e há $\left[\frac{n}{p^2}\right]$ tais fatores. Dentre estes últimos, os que sáo múltiplos de p^3 contribuem com mais um fator primo e assim por diante, resultando na fórmula acima. ■

Exemplo 3.2. Determine com quantos zero termina 1000!.

Solução: O problema se resume em determinar qual a maior potência de 10 que divide 1000! e como há mais fatores 2 do que 5 em 1000! o expoente desta potência coincide com o da maior potência de 5 que divide 1000!, ou seja

$$\left[\frac{1000}{5}\right]+\left[\frac{1000}{5^2}\right]+\left[\frac{1000}{5^3}\right]+\left[\frac{1000}{5^3}\right]=200+40+8+1=249$$

Assim, 1000! termina com 249 zeros.

Lema 3.3. *Sejam n um número natural, p um número primo e θ_p o inteiro tal que $p^{\theta_p}<2n<p^{\theta_p+1}$.Então o expoente da maior potência de p que divide $\binom{2n}{n}$ é menor ou igual a θ_p. Em particular, se $p>\sqrt{2n}$ então o expoente desta máxima potência de p é menor do que ou igual a 1. Além disso, se $\frac{2}{3}n<p<n$ então p não divide $\binom{2n}{n}$.*

Demonstração: Sejam α e β os expoentes das duas maiores potências de p que dividem $(2n)!$ e $n!$ respectivamente.Sabemos da proposição 3.1 que

$$\alpha=\left[\frac{2n}{p}\right]+\left[\frac{2n}{p^2}\right]+\left[\frac{2n}{p^3}\right]+\cdots \quad \text{e} \quad \beta=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots$$

Portanto o expoente da máxima potência de p que divide $\binom{2n}{n}=\frac{(2n)!}{n!n!}$ é

$$\alpha-2\beta=\sum_{i=1}^{\theta_p}\left[\frac{2n}{p^i}\right]-2\left[\frac{n}{p^i}\right].$$

Mas como

$$\frac{2n}{p^i}-1<\left[\frac{2n}{p^i}\right]\leq\frac{2n}{p^i} \qquad \text{e} \qquad -2\frac{n}{p^i}\leq-2\left[\frac{n}{p^i}\right]<-2\left(\frac{n}{p^i}-1\right),$$

temos que

$$-1<\left[\frac{2n}{p^i}\right]-2\left[\frac{n}{p^i}\right]<2.$$

Deste modo a expressão

$$\left[\frac{2n}{p^i}\right]-2\left[\frac{n}{p^i}\right],$$

só pode assumir valores 1 e 0. Portanto concluímos que

$$\alpha-2\beta\leq\sum_{i=1}^{\theta_p}1=\theta_p.$$

Agora se $\frac{2}{3}n<p<n$ então $1<\frac{n}{p}<\frac{3}{2}$ e $2<\frac{2n}{p}<3$, razão pela qual $\alpha=2$ e $\beta=1$ e então $\alpha-2\beta=0$. ■

Vamos agora apresentar um importante resultado conhecido como Teorema de Chebyshev.

Teorema 3.4. *(Chebyshev). Seja $\pi(x)$ a quantidade de primos menores do que ou iguais a x. Existem constantes c e C tais que*

$$c\frac{x}{\log x}<\pi(x)<C\frac{x}{\log x},$$

para todo $x>2$.

Demonstração: Observemos inicialmente que $\binom{2n}{n} = \frac{2n!}{n!n!}$ é múltiplo de todos os primos p que satisfazem $n < p < 2n$. Como

$$\binom{2n}{n} < \sum_{k=0}^{2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre n e $2n$ é menor que 2^{2n}. Como há $\pi(2n) - \pi(n)$ primos comos esses seque que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que n). Deste modo podemos obter a seguinte desigualdade

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log 2}.$$

Esta última desigualdade nos sugere que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}.$$

De fato, isto é verificado diretamente para $k < 5$ para $k \geq 5$ vamos utilizar a indução sobre k.

Vamos supor que

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k},$$

seja válido para algum k, $k \geq 5$.

Agora observemos as implicações abaixo

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n} \Rightarrow$$

$$\pi(2n) < \pi(n) + \frac{2n \log 2}{\log n} \Rightarrow$$

$$\pi(2^{k+2}) < \pi(2^{k+1}) + \frac{2^{k+2} \log 2}{\log 2^{k+1}} \Rightarrow$$

$$\pi(2^{k+2}) < \pi(2^{k+1}) + \frac{2^{k+2} \log 2}{(k+1) \log 2} \Rightarrow$$

$$\pi(2^{k+2}) < \pi(2^{k+1}) + \frac{2^{k+2}}{k+1}.$$

Agora utilizando a nossa hipótese de indução temos

$$\pi(2^{k+2}) < \pi(2^{k+1}) + \frac{2^{k+2}}{k+1} \leq \frac{5 \cdot 2^k}{k} + \frac{2^{k+2}}{k+1}. \tag{3.1}$$

Para todo $k \geq 5$, temos que

$$\frac{3 \cdot 2^{k+1}}{k+1} - \frac{5 \cdot 2^k}{k} \geq 0,$$

isto é

$$\frac{3 \cdot 2^{k+1}}{k+1} \geq \frac{5 \cdot 2^k}{k}.$$

Voltando na equação (3.1) temos

$$\pi(2^{k+2}) < \pi(2^{k+1}) + \frac{2^{k+2}}{k+1} \leq \frac{5\cdot 2^k}{k} + \frac{2^{k+2}}{k+1} \Rightarrow$$

$$\pi(2^{k+2}) < \frac{5\cdot 2^k}{k} + \frac{2^{k+2}}{k+1} \leq \frac{3\cdot 2^{k+1}}{k+1} + \frac{2\cdot 2^{k+1}}{k+1} \Rightarrow$$

$$\pi(2^{k+2}) \leq \frac{3\cdot 2^{k+1}}{k+1} + \frac{2\cdot 2^{k+1}}{k+1} = \frac{5\cdot 2^{k+1}}{k+1}.$$

Deste modo o Princípio da Indução finita nos garante que

$$\pi(2^{k+1}) \leq \frac{5\cdot 2^k}{k}.$$

Agora se $2^k < x \leq 2^{k+1}$, então usando o fato de que $f(x) = \frac{x\log 2}{\log x}$ é uma função crescente para $x \geq e$ temos

$$2^k < x \Rightarrow$$

$$\frac{2^k \log 2}{k\log 2} < \frac{x\log 2}{\log x} \Rightarrow$$

$$\frac{2^k}{k} < \frac{x\log 2}{\log x}.$$

Então

$$\pi(x) \leq \frac{5\cdot 2^k}{k} \leq \frac{5x\log 2}{\log x} = 5\log 2\frac{x}{\log x}.$$

Assim escolhendo, por exemplo, $C = 6\log 2$ temos que $\pi(x) < C\frac{x}{\log x}$. Vamos agora provar a outra desigualdade. Se $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ é a decomposiccão em fatores primos de $\binom{2n}{n}$ então pelo Lema 3.3 temos $p^{\alpha_p} \leq 2n \Leftrightarrow \alpha_p \log p \leq \log 2n$ e portanto

$$\log\binom{2n}{n} = \sum_{p<2n} \alpha_p \log p \leq \pi(2n)\log(2n).$$

donde

$$\pi(2n) \geq \frac{\log\binom{2n}{n}}{\log(2n)} \geq \frac{n\log 2}{\log 2n},$$

pois

$$\binom{2n}{n} = \frac{2n}{n}\cdot\frac{2n-1}{n-1}\cdots\frac{n+1}{1} \geq 2^n,$$

assim

$$\pi(x) \geq \frac{x\log 2}{2\log x},$$

para todo x par, o que implica na mesma estimativa para todo x inteiro, pois $\pi(2k-1) = \pi(2k)$. Desta maneira escolhendo, por exemplo, $c = \frac{\log 2}{3}$ temos que $\pi(x) > c\frac{x}{\log x}$. ■

Exemplo 3.5. Utilize o Teorema de Chebyshev e encontre uma estimativa para $\pi(20000)$.

Resolução: Pelo visto anteriormente temos $c = \frac{\log 2}{3} \approx 0,1$ e $C = 6\log 2 \approx 1,8$. Isto é

$$0,1 \cdot \frac{x}{\log x} < \pi(x) < 1,8 \cdot \frac{x}{\log x}.$$

Para $x = 20000$ obtemos

$$0,1 \cdot \frac{20000}{\log 20000} < \pi(20000) < 1,8 \cdot \frac{20000}{\log 20000} \Rightarrow$$
$$465 < \pi(20000) < 8370.$$

Exemplo 3.6. Qual a quantidade mínima de números primos no conjunto

$$A = \{1, 2, 3, 4, \cdots, 1000000\}?$$

Resolução: Para responder a esta questão é suficente determinar um limite inferior para $\pi(1000000)$. Pelo Teorema de Chebyshev temos

$$\pi(x) > 0,1 \cdot \frac{x}{\log x} \Rightarrow$$
$$\pi(1000000) > 0,1 \cdot \frac{1000000}{\log 1000000} \Rightarrow$$
$$\pi(1000000) > 16666.$$

Deste modo, podemos afirmar que o conjunto A possui pelo menos 16667 números primos.

As constantes c e C do Teorema de Chebyshev tem sido aperfeiçoadas ao longo dos anos.

3.2 O Teorema dos Números Primos

O Teorema de Chebyshev, demonstrado na seção anterior nos mostrou que $\pi(x)$ está entre $c\frac{x}{\log x}$ e $C\frac{x}{\log x}$ para duas constantes $c < C$. Na verdade há um resultado mais preciso e sofisticado:

Teorema 3.7. *(Teorema dos Números Primos).*

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$$

Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauss, mas a demosntração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independente). Não faremos a demosntração deste Teorema, pois foge do objetivo deste trabalho, as demostrações elementares conhecidas são todas bastantes difíceis.

De acordo com [5] em 1994 M. Deléglise e Rivat, usando o algoritmo de Lagarias, Miller e Odlyzko computaram $\pi(10^{18}) = 24739954287740860$, quebrando o recorde anterior (1985): $\pi(4 \cdot 10^{16}) = 1075292778793150$. Deste modo, para valores suficientemente grandes, o Teorema dos Números Primos nos diz que

$$\pi(x) \approx \frac{x}{\ln x}.$$

3.3 Aplicações do Teorema dos Números Primos

Os exemplos que serão expostos a seguir nos mostrará a utilidade do Teorema dos Números Primos para estimar a quantidade de números primos que satisfazem determinada condição.

Exemplo 3.8. Utilize o Teorema dos Números Primos e encontre uma estimativa para $\pi(10^{100})$.

Resolução: De acordo com o Teorema dos Números Primos temos

$$\pi(10^{100}) \approx \frac{10^{100}}{\ln 10^{100}} = \frac{10^{100}}{100\ln 10} = \left(\frac{1}{100}\right)\cdot\left(\frac{10^{100}}{\ln 10}\right) = \frac{0,01\cdot 10^{100}}{\ln 10} = \left(\frac{0,01}{\ln 10}\right)\cdot\left(10^{100}\right) \approx$$

$$0,00434\cdot 10^{100} = 4,34\cdot 10^{97}.$$

Ou seja,

$$\pi(10^{100}) \approx 4,34\cdot 10^{97}.$$

Exemplo 3.9. Quantos números primos com 20 dígitos existem?

Resolução: Desejamos obter o valor de $\pi(10^{20}) - \pi(10^{19})$. Vamos aplicar o Teorema dos Números Primos

$$\pi(10^{20})-\pi(10^{19}) \approx \frac{10^{20}}{\ln 10^{20}}-\frac{10^{19}}{\ln 10^{19}} = \frac{10^{20}}{20\ln 10}-\frac{10^{19}}{19\ln 10} = \left(\frac{1}{20}\right)\cdot\left(\frac{10^{20}}{\ln 10}\right)-\left(\frac{1}{19}\right)\cdot\left(\frac{10^{19}}{\ln 10}\right) \approx$$

$$\frac{0,05\cdot 10^{20}}{\ln 10}-\frac{0,0526\cdot 10^{19}}{\ln 10} = \frac{0,5\cdot 10^{19}}{\ln 10}-\frac{0,0526\cdot 10^{19}}{\ln 10} = \frac{0,4474\cdot 10^{19}}{\ln 10} = \left(\frac{0,4474}{\ln 10}\right)\cdot\left(10^{19}\right) \approx$$

$$0,1943\cdot 10^{19} = 1,943\cdot 10^{18}.$$

Ou seja, há aproximadamente $1,943\cdot 10^{18}$ números primos com 20 dígitos.

Exemplo 3.10. Seja $A = \{n \mid n \text{ possui exatamente 150 dígitos}\}$. Escolhido ao acaso um elemento do conjunto A qual é a probabilidade de que seja um número primo?

Resolução: Inicialmente vamos estimar a quantidade de números primos no conjunto A

$$\pi(10^{150})-\pi(10^{149}) \approx \frac{10^{150}}{\ln 10^{150}}-\frac{10^{149}}{\ln 10^{149}} = \frac{10^{150}}{150\ln 10}-\frac{10^{149}}{149\ln 10} = \left(\frac{1}{150}\right)\cdot\left(\frac{10^{150}}{\ln 10}\right)-\left(\frac{1}{149}\right)\cdot\left(\frac{10^{149}}{\ln 10}\right) \approx$$

$$\frac{0,0067\cdot 10^{200}}{\ln 10}-\frac{0,0067\cdot 10^{149}}{\ln 10} = \frac{0,067\cdot 10^{149}}{\ln 10}-\frac{0,0067\cdot 10^{149}}{\ln 10} = \frac{0,0603\cdot 10^{149}}{\ln 10} = \left(\frac{0,0603}{\ln 10}\right)\cdot\left(10^{149}\right) \approx$$

$$0,0261\cdot 10^{149} = 2,61\cdot 10^{147}.$$

O conjunto A possui aproximadamente $2,61\cdot 10^{147}$ números primos.

A quantidade de números com 150 dígitos é dada por

$$10^{150} - 10^{149} = 10 \cdot 10^{149} - 10^{149} = 9 \cdot 10^{149}$$

Isto é, o conjunto A possui $9 \cdot 10^{149}$ elementos.
Finalmente, ao escolher um número ao acaso no conjunto A a probabilidade de que seja primo é dada por

$$\frac{2,61 \cdot 10^{147}}{9 \cdot 10^{149}} = \left(\frac{2,61}{9}\right) \cdot \left(\frac{10^{147}}{10^{149}.}\right) = 0,29 \cdot 10^{-2} = 0,29\%.$$

4 Números Primos especiais

Neste capítulo, estudaremos propriedades de certos números primos que possuem formas especiais.

4.1 Os Primos de Fermat

Nesta seção estudaremos números conhecidos como números de Fermat em homenagem a Pierre de Fermat (1601-1665), jurista francês e matemático. Após Euclides e Erastótenes, Fermat é considerado o primeiro matemático a contribuir para o desenvolvimento da Teoria dos Números do ponto de vista teórico. Muitos dos resultados e problemas deixados por Fermat motivaram o extraordinário avanço da Matemática.

Proposição 4.1. *Sejam a e n números naturais maiores que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.*

Demonstração: Suponhamos que $a^n + 1$ seja primo, onde $a > 1$ e $n > 1$. Logo, a tem que ser par, pois caso contrário, $a^n + 1$ seria par e maior que dois, o que contraria o fato de ser primo.
Se n tivesse um divisor primo p diferente de 2, teríamos $n = kp$ com $k \in \mathbb{N}$. Como $a + b$ divide $a^{2n+1} + b^{2n+1}$ sempre que $a, b, n \in \mathbb{N}$ e $a + b \neq 0$ teríamos que $a^k + 1$ dividiria $(a^k)^p + 1 = a^n + 1$, contradizendo o fato desse último número ser primo. Logo n não possui um fator primo diferente de 2, ou seja n é da forma 2^m. ■

Definição 4.2. *Seja n um número natural. Um número da forma*

$$F_n = 2^{2^n} + 1,$$

é chamado número de Fermat.

Em 1640, Fermat afirmou que achava que esses números eram todos primos, baseado no fato de que $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65537$ são todos primos.
Em 1732, Leonhard Euler mostrou que

$$F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417,$$

ou seja, composto, desmentindo assim a afirmação de Fermat. A dificuldade em verificar a primalidade dos números de Fermat se deve ao fato de que os números F_n aumentam muito rapidamente, sendo necessário testes de primalidade específicos para os números de Fermat. Pepin apresentou em 1877 um teste de primalidade específico para os números de Fermat. Apresentaremos o teste de Pepin, antes, porém, apresentaremos algumas definições necessárias.

Definição 4.3. *Quando a congruência* $X^2 \equiv a \ mod \ m$ *possui alguma solução, diz-se que* a *é* ***resíduo quadrático, módulo m****; caso contrário, diz-se que* a ***é não resíduo quadrático, módulo m****.*

Exemplo 4.4. Como $6^2 \equiv 4 \ mod \ 8$, 4 é um resíduo quadrático módulo 8.

Exemplo 4.5. A congruência $X^2 \equiv 2 \ mod \ 3$, não possui nenhuma solução, isto é, 2 é não resíduo quadrático módulo 3.

Definição 4.6. *Se* p *é um número primo ímpar, define-se o* ***símbolo de Legendre*** *de* a *módulo* p *como sendo*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } a \text{ é um resíduo quadrático módulo } p; \\ -1 & \text{se } a \text{ é não resíduo quadrático módulo } p. \end{cases}$$

Exemplo 4.7. De acordo com a definição anterior, temos

$$\left(\frac{4}{7}\right) = 1, \text{ pois } 5^2 \equiv 4 \ mod \ 7$$

$$\left(\frac{2}{5}\right) = -1, \text{ pois } X^2 \equiv 2 \ mod \ 5 \text{ não possui solução.}$$

Teorema 4.8 (Teste de Pepin)**.** *Seja* $F_n = 2^{2^n} + 1$ *(com* $n \geqslant 2$*) e* $k \geqslant 2$*. Então as seguintes afirmações são equivalentes*

i. F_n *é primo e* $\left(\frac{k}{F_n}\right) = -1$*;*

ii. $k^{\frac{F_n-1}{2}} \equiv -1 \ mod \ F_n$*.*

A demonstração do teste de Pepin pode ser encontrada em [2]. Possíveis valores de k são $k = 3$, $k = 5$, ou $k = 10$. Assim, escolhendo $k = 3$ podemos simplificar o teste de Pepin

$$F_n \text{ é primo} \Leftrightarrow 3^{\frac{F_n-1}{2}} \equiv -1 \ mod \ F_n.$$

O teste de Pepin é de fácil aplicação. Contudo, caso F_n seja um número composto, o teste não revela qualquer fator de F_n.
Luccas usou isto para mostrar que

$$F_6 = 2^{2^6} + 1 = 2^{64} + 1 = 18446744073709551617,$$

é composto e em 1880, aos 82 anos, Landry mostrou que

$$F_6 = 274177 \cdot 67280421310721.$$

Landry nunca descreveu como ele conseguiu fatorar F_6 (para mais informaçõs consulte [2]).
A fatorização de F_7 foi primeiramente realizada por Morrison e Brillhart (1970, publicada em 1975), e F_8 por Bent e Pollard (1981). Apenas dois outros números de Fermat foram completamente fatorados: F_9 e F_{11}.

4.2 Primos de Sophie Germain

Marie-Sophie Germain (1776-1831) foi uma matemática francesa que dedicou seus estudos a números primos que satisfazem uma condição específica e deste modo conseguiu provar o chamado primeiro caso do Último Teorema de Fermat para estes números primos específicos.

Definição 4.9. *Os primos p para os quais $2p+1$ é primo são chamados de primos de Sophie Germain.*

Exemplo 4.10. O número 3 é um primo de Sophie Germain, pois: 3 e $2 \cdot 3 + 1 = 7$ são primos.

Exemplo 4.11. O número 5 é um primo de Sophie Germain, pois: 5 e $2 \cdot 5 + 1 = 11$ são primos.

O resultado a seguir é devido à Sophie Germain e prova o chamado primeiro caso do Último Teorema de Fermat (demonstrado completamente por Wiles e Taylor).

Proposição 4.12. *(Sophie Germain). Se $p > 2$ é um primo de Sophie Germain, então não existem inteiros x, y e z com $mdc(x, y, z) = 1$ e $p \nmid xyz$ tais que $x^p + y^p = z^p$.*

A demonstração deste resultado pode ser encontrada em [5].

Observação 4.13. A proposição anterior requer que $mdc(x, y, z) = 1$, pois caso $mdc(x, y, z) \neq 1$ é possível encontrar soluções que talvez não sejam interessantes, como por exemplo: $x = -2$, $y = 2$ e $z = 0$ é uma solução da equação

$$x^3 + y^3 = z^3.$$

Exemplo 4.14. Como o número 3 é um primo de Sophie Germain a equação $x^3+y^3 = z^3$ não possui soluções inteiras x, y e z tais que $3 \nmid xyz$ e $mdc(x, y, z) = 1$.

4.3 Os Primos de Mersenne

Marin de Mersenne foi um matemático e padre francês que dedicou estudos a números que podem se escritos da forma $2^n - 1$. Mersenne acreditava que estes números eram primos sempre que n eram primos e por essa razão os números da forma $2^n - 1$ que são primos são chamados primos de mersenne. Aqui examinaremos algumas particularidades referentes aos primos de mersenne.

Definição 4.15. *Os números de Mersenne são números da forma*

$$M_p = 2^p - 1,$$

onde p é um número primo.

Um número de Mersenne que é primo é chamado de *Primos de Mersenne*. A proposição a seguir nos mostra que $2^p - 1$ só tem chance de ser primo quando p for primo.

Proposição 4.16. *Se $2^n - 1$ é primo então n é primo.*

Demonstração: Vamos supor que n não é primo. Temos que $n = ab$ com $a, b \geq 2$. Como $2^a - 1$ divide $(2^a)^b - 1 = 2^n - 1$, segue que $2^n - 1$ não é primo, o que é uma contradição. Logo n deve ser primo. ■

A busca por números primos cada vez maiores

De acordo com [5], em abril de 2010, os nove maiores primos conhecidos são da forma $M_p = 2^p - 1$ para $p = 43112609$, 42643801, 37156667, 32582627, 30402457, 25964951, 24036583, 20996011. Estes são os únicos primos conhecidos com mais de 4000000 de dígitos. Talvez um dos resultados mais triviais sobre os números de Mersenne seja devido a Hudalricus Regis que em 1536 msotrou que $2^p - 1$ não precisa ser primo sempre que p for primo: $2^{11} - 1 = 2047 = 23 \cdot 89$. Os maiores números primos conhecidos atualmente são primos de Mersenne. Atualmente (dezembro/2014) o mais recente Primo de Mersenne descoberto é o 48º que corresponde a $M_{57.885.161}$, um número com 17.425.171 dígitos. Mas a procura por Primos de Mersenne não é uma tarefa das mais faceis, ela envolve calculos complexos e muito recurso computacional, desde 1996 existe o projeto **GIMPS**-Great Internet Mersenne Prime Search, que através do site *www.mersenne.org.br* concentra pessoas e seus computadores com um objetivo comum: descobrir novos Primos de Merssene.

4.4 Primos Gêmeos e Primos Trigêmeos

Primos Gêmeos - Ao observar atentamente a distribuição de números primos notamos a indefinida persistência de pares de primos que diferem por duas unidades,

como por exemplo: $(3,5)$, $(5,7)$, $(11,13)$, $(41,43)$, $(107,109)$, $(239,241)$, entre outros. Pares de primos como estes são chamados de **primos gêmeos**.

Primos Gêmeos foram caracterizados por Clement (veja [2]) em 1949, conforme o resultado:

Proposição 4.17. *Seja $n \geq 2$. Os inteiros n, $n+2$ formam um par de primos gêmeos se, e somente se,*

$$4\left[(n-1)!+1\right]+n \;\equiv\; 0 \;mod\; \left[n\cdot(n+2)\right].$$

A demonstraąão desta última proposição pode ser encontrada em [2].
De um modo geral a caracterização dada por Clement não possui uma aplicação prática para a determinação de primos gêmeos.
De acordo com [2], Sergusov (1971) e Leavitt e Mullin (1981) provaram o seguinte fato: *"Um número natural n é um produto de primos gêmeos, isto é $n = p\cdot q$ onde (p,q) é um par de primos gêmeos, se, e somente se $\varphi(n)\cdot\sigma(n) = (n-3)\cdot(n+1)$.*
Onde

i. $\varphi(n)$ é a função φ de Euler;

ii. $\sigma(n)$ denota a soma de todos os divisores de n.

Este último resultado também é de dificil aplicação pois $\varphi(n)$ e $\sigma(n)$ são determinados a partir da fatoração de n.
Vários estudos tentam verificar se os primos gemêos são em número finito ou infinito.

Primos Trigêmeos -Uma terna de números primos da forma $(p, p+2, p+4)$ são chamados de **primos trigêmeos**. Vamos mostrar que $(3,5,7)$ é a única terna de primos trigêmeos. De fato, se $(n, n+2, n+4)$ é uma terna de trigêmeos então o número n pode ser escrito da seguinte forma: $3k+i,\ i = 0,1,2$. Assim, se n, $n+2$ e $n+4$ são primos, um dos três números é igual a 3 por ser divisivel por 3. Portanto a única possibilidade é $n = 3$, $n+2 = 5$ e $n+4 = 7$.

5 Existem funções que geram os Números Primos?

Vamos investigar a possibilidade de existir uma fórmula ou função que nos forneça números primos e somente esses. Na busca em determinar uma função que gera primos nos esbarramos em situações do tipo: (a) encontrar uma relação que seja relativamente simples de manusear; (b) uma fórmula nos fornece somente números primos (temos que ter a garantia de que os números gerados são, de fato, primos). Por exemplo a função $f: \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2n^2 - 1$ fornece números primos para $n \in \{1, 2, 3, 4\}$, entretanto, $f(5) = 49 = 7.7$, logo esta expressão não atende ao que desejamos. Para vislumbrar possíveis soluções para o problema recorreremos a importantes artigos científicos e utilizaremos um importante resultado conhecido como *Teorema de Wilson* que será útil para o desenvolvimento do tema e que será apresentado na próxima seção.

5.1 O Teorema de Wilson

Nesta seção vamos abordar um importante resultado relativo aos números primos, antes, porém vamos demonstrar um Lema que nos auxiliará na demonstração do Teorema de Wilson.

Lema 5.1. *Seja p um número primo e a um número inteiro. Se $a^2 \equiv 1 \ mod\ p$ então tem-se $a \equiv 1 \ mod\ p$ ou $a \equiv -1 \ mod\ p$.*

Demonstração: A condição $a^2 \equiv 1 \ mod\ p$ significa que p divide $a^2 - 1 = (a+1)(a-1)$. Como p é primo, deve dividir pelo menos um dos fatores deste produto, isto é, tem-se que: $a \equiv 1 \ mod\ p$ ou $a \equiv -1 \ mod\ p$. ■

Teorema 5.2 (Teorema de Wilson)**.** *Se p é um número primo, então*

$$(p-1)! \equiv -1 \ mod\ p.$$

Demonstração: Suponhamos p primo. Para todo $a \in \{2, ..., p-2\}$ tem-se que $(a, p) = 1$, razão pela qual a congruência $ax \equiv 1 \ mod\ p$ possui uma única solução módulo p (em [1] encontramos o seguinte resultado: *"Dados $a,\ c,\ m \in \mathbb{N}^*$ tais que $m > 1$ e $(a, m) = 1$,*

então a congruência $ax \equiv\ c\ mod\ m$ *possui uma única solução módulo* m"). Assim dado $a \in \{2, ..., p-2\}$ existe $x \in \{0, 1, 2, ..., p-1\}$ tal que $ax \equiv\ 1\ mod\ p$. Certamente x não pode ser 0 nem 1. E x não pode ser $p-1$ pois neste caso $a(p-1) \equiv\ 1\ mod\ p$, isto é $a \equiv\ -1\ mod\ p$, o que não pode ocorrer pois $a \in \{2, ..., p-2\}$. Logo $b \in \{2, ..., p-2\}$. Note-se também que não se pode ter $x = a$ pois nesse caso $a^2 \equiv\ 1\ mod\ p$ e pelo Lema anterior teríamos $a \equiv\ 1\ mod\ p$ ou $a \equiv\ -1\ mod\ p$, o que é impossível pois $a \in \{2, ..., p-2\}$. As considerações feitas até agora permitem concluir que para cada $a \in \{2, ..., p-2\}$, existe $x \neq a$ no mesmo conjunto tal que $ax \equiv\ 1\ mod\ p$. Desta forma podemos agrupar os números $2, 3, ..., p-2$ em $\frac{p-3}{2}$ pares cujo produto seja congruente a 1 módulo p. Multiplicando estas congruências membro a membro teremos

$$2 \cdot 3 \cdot \cdots (p-2) \equiv\ 1\ mod\ p$$

e, portanto,

$$2 \cdot 3 \cdot \cdots (p-2)(p-1) \equiv\ p-1\ mod\ p$$

e como

$$p-1 \equiv\ -1\ mod\ p$$

temos

$$(p-1)! \equiv\ -1\ mod\ p.$$

■

A recíproca do Teorema de Wilson também é verdadeira.

Teorema 5.3. *Se* n *é um inteiro tal que* $(n-1)! \equiv\ -1\ mod\ n$*, então* n *é primo.*

Demonstração: A prova é por contradição. Vamos supor que $(n-1)! \equiv\ -1\ mod\ n$, isto é, $n \mid ((n-1)! + 1)$ e que n não seja primo, ou seja $n = rs$ com $1 < r < n$ e $1 < s < n$. Podemos considerar que r é tal que $1 < r \leq n-1$ e como $(n-1)! = 1 \cdot 2 \cdot ... \cdot r \cdot ... \cdot (n-1)$ temos que $r \mid (n-1)!$. Temos ainda que $r \mid n$ razão pela qual $r \mid ((n-1)! + 1)$. Como $r \mid (n-1)!$ e $r \mid ((n-1)! + 1)$, r divide a diferença $(n-1)! + 1 - (n-1)! = 1$, o que é um absurdo uma vez que $r > 1$. Logo, um n satisfazendo $(n-1)! \equiv\ -1\ mod\ n$ deve ser primo. ■

5.2 Obtendo uma fórmula que gera os Números Primos numa certa ordem

Desejamos encontrar uma função $f : \mathbb{N} \to \mathbb{N}$ tal que

$$\forall n \quad f(n) = p_n \ \text{ onde } \ p_n \text{ é o n-ésimo número primo.}$$

Consideremos o número $N = (n-1)! + 1$.
Temos duas possibilidades

i. N é divisível por n;

ii. N não é divisível por n.

O item i. ocorre se e somente se n for primo conforme o Teorema de Wilson (Teorema 5.2)

$$N = (n-1)! + 1 \equiv 0 \ mod \ n.$$

Consideremos agora a função F dada por

$$F(j) = \begin{cases} 1 & \text{se } j = 1 \\ \left[\cos^2\left(\frac{\pi((j-1)!+1)}{j}\right)\right] & \text{se } j \neq 1, \text{ onde } [x] \text{ denota a parte inteira de x.} \end{cases}$$

Agora observe que
Se j é um número primo o Teorema de Wilson nos garante que

$$(j-1)! + 1 = kj, \ k \in \mathbb{Z}.$$

e então

$$F(j) = \left[\cos^2\left(\frac{\pi((j-1)!+1)}{j}\right)\right] = \left[\cos^2\left(\frac{\pi kj}{j}\right)\right] = [\cos^2(\pi k)] = 1.$$

Agora se j é um número composto temos

$$F(j) = 0, \quad \text{pois} \quad 0 \leq \cos^2\left(\frac{\pi((j-1)!+1)}{j}\right) < 1.$$

Deste modo com os racíocinios detalhados acima podemos obter uma lei mais simples para a função F

$$F(j) = \begin{cases} 1 & \text{se } j = 1 \ \text{ ou } j \text{ é primo} \\ 0 & \text{caso contrário} \end{cases}$$

Com essas características cada vez que $F(j) = 1$ e $j \neq 1$ então j é um número primo. Ainda mais, a soma dos $F(j)$ para todos o j pertencente a um certo intervalo nos permite contar a quantidade de números primos dentro deste intervalo e isto pode ser feito com o auxílio da seguinte fórmula

$$\sum_{j=1}^{m} F(j) = 1 + \pi(m).$$

A funcão π é a funcão que conta os números primos.
WILLIANS (1964) citado por [2] apresentou, para o problema em questão, a seguinte fórmula

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\sqrt[n]{\frac{n}{1+\pi(m)}} \right], \text{ onde } [x] \text{ denota a parte inteira de x.}$$

Esta fórmula fornece o n-ésimo número primo, entretanto, ocorrem somas muito complicadas além do fato de que para encontrar um número primo devemos contar quantos sáo os números primos a 2^n, como por exemplo

$$29 = p_{10} = 1 + \sum_{m=1}^{1024} \left[\sqrt[10]{\frac{10}{1+\pi(m)}} \right]$$

Deste modo a fórmula apresentada por WILLIANS é de difícil aplicação.
Apresentaremos uma outra fórmula, antes, porém, vamos definir uma importante função aritmética.

Definição 5.4. *A função μ de Möbius é definida por*

- $\mu(1) = 1$;
- $\mu(n) = (-1)^r$ *para* $n = p_1{}^{a_1} p_2{}^{a_2} \ldots p_r{}^{a_r}$ *e* $a_1 = a_2 = \ldots = a_r = 1$;
- $\mu(n) = 0$ *caso contrário.*

Esta definição nos diz, portanto, que $\mu(n) = 0$ sempre que n for divisível pelo quadrado de algum número primo.

Exemplo 5.5.

A. $\mu(2) = \mu(2^1) = (-1)^1 = -1$.

B. $\mu(8) = 0$

C. $\mu(65) = \mu(5 \cdot 13) = (-1)^2 = 1$.

D. $\mu(100) = 0$.

E. $\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1$.

GANDHI (1971), citado por [2] apresentou a seguinte fórmula que permite obter o n-ésimo número primo p_n

$$p_n = \left[1 + \frac{1}{\ln 2} \left(-\frac{1}{2} + \sum_{d|P} \frac{\mu(d)}{2^d - 1} \right) \right],$$

onde

- $P = p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1}$
- μ é a função de *Möbius*
- $[x]$ denota a parte inteira de x
- $d \mid P$ significa d divide P

Novamente temos uma fórmula de dificil aplicação, pois o número P possui muitos divisores e se desejássemos calcular, por exemplo, p_{20} seria necessário determinar $\mu(d)$ para muitíssimos valores d o que torna a fómula de GANDHI impraticável.

5.3 Obtendo uma fórmula que gera Números Primos aleatórios

Vamos concentrar nossos estudos em dois importantes artigos científicos. O primeiro deles é de autoria de W. H .MILLS [7], e o segundo de autoria de E. M WRIGHT [8]. Vamos encontrar uma função $f : \mathbb{N} \to \mathbb{N}$ tal que

$$\forall \quad n \quad f(n) \text{ é primo e se } n \neq m \text{ então } f(n) \neq f(m).$$

W.H. MILLS provou que existe um número real A tal que, para todo valor inteiro positivo x, o número

$$\left[A^{3^x}\right], \text{ onde } [x] \text{ denota a parte inteira de x.}$$

é um número primo. Mais tarde E.M. WRIGHT apresentou uma fórmula em que dado um número inteiro, digamos 10, o resultado obtido a partir desta fórmula é um número primo, mas não o décimo. Se é dado o número 11, teremos um outro número primo e assim por diante. O resultado de E.M. WRIGHT é baseado no resultado de W.H. MILLS e diz que o número

$$f(n) = \left[2^{2^{2^{\cdot^{\cdot^{2^{\omega}}}}}}\right].$$

é **primo**. Onde

- $[x]$ denota a parte inteira de x
- $2^{2^{2^{\cdot^{\cdot^{2^{\omega}}}}}}$ representa n etapas de expoentes
- A escolha de ω não é única, um possível valor é $\omega = 1,9287800$.

Utilizando o software Maple, vamos aplicar a fórmula de E.M. WRIGHT para $\omega = 1,9287800...$

- Para $n = 1$ temos

$$f(1) = \left[2^{1,9287800}\right] = [3,807331001] = 3.$$

- Para $n = 2$ temos

$$f(2) = \left[2^{2^{1,9287800}}\right] = \left[2^{3,807331001}\right] = [13,99976787] = 13.$$

- Para $n = 3$ temos

$$f(3) = \left[2^{2^{2^{1,9287800}}}\right] = \left[2^{2^{3,807331001}}\right] = \left[2^{13,99976787}\right] = [16.381,36402] = 16.381.$$

- Para $n = 4$ temos

$$f(4) = \left[2^{2^{2^{1,9287800}}}\right] = \left[2^{2^{2^{3,807331001}}}\right] = \left[2^{2^{13,99976787}}\right] = \left[2^{16.381,36402}\right] = \left[1,913991085 \cdot 10^{4931}\right] = ...$$

Como se pode obsrvar para $n = 4$ obtemos um número com mais de 4900 dígitos. Deste modo a fórmula proposta por E.M. WRIGHT é muito complicada e de pouca aplicabilidade, além disso há na fórmula o número ω cuja existência foi demostrada e o cálculo feito, mas com certa aproximação, o que pode resultar em erros nos levando a obter um número que não é primo.

5.4 Uma função de duas variáveis que gera números primos

HONSBERGER [9] apresenta em sua obra uma função de duas variáveis que fornece números primos, e que será objeto de estudo nesta seção.
Sejam x e y números naturais, $y \neq 0$ e $a = x(y+1) - (y!+1)$ a fórmula a seguir fornece todos os números primos e somente esses

$$f(x,y) = \left(\frac{y-1}{2}\right)\left(|\, a^2 - 1 \,| - (a^2 - 1)\right) + 2.$$

Demonstraremos este fato em duas partes:

A. Vamos provar que $f(x,y)$ é sempre um número primo
O número a é sempre um número inteiro e, portanto, a^2 é inteiro. Há dois casos para considerar: $a^2 \geq 1$ e $a^2 = 0$.

- Se $a^2 \geq 1 \Rightarrow |\, a^2 - 1 \,| = a^2 - 1$ e então $f(x,y) = 2$.
- Se $a^2 = 0 \Rightarrow f(x,y) = \left(\frac{y-1}{2}\right)(|\, -1 \,| - (-1)) + 2 = \left(\frac{y-1}{2}\right)(1+1) + 2 = y - 1 + 2 = y + 1$
  Como $a^2 = 0$ temos que $a = 0$ e então

$$x(y+1) - (y!+1) = 0 \Rightarrow (y!+1) = x(y+1) \Rightarrow y! \equiv -1 \ mod\ y+1.$$

E deste modo o Teorema 5.3, para $n = y + 1$, nos garante que $y + 1$ é um número primo.
Os dois casos acima provam que $f(x,y)$ é sempre um número primo.

B. Vamos provar que $f(x,y)$ fornece **todos** os números primos
Seja p um número primo. De acordo com o Teorema de Wilson, $\frac{(p-1)!+1}{p}$ é um número natural e então podemos calcular $f\left(\frac{(p-1)!+1}{p}, p-1\right)$. O valor de a é

$$a = \left(\frac{(p-1)!+1}{p}\right) \cdot p - ((p-1)!+1) = 0.$$

Segue-se que

$$f\left(\frac{(p-1)!+1}{p}, p-1\right) = p - 1 + 1 = p.$$

Esta fórmula apresenta cálculos com números muito grandes deixando a sua aplicação um tanto complexa.

Exemplo 5.6. Observe alguns valores da função f obtidos com o auxílio do software Maple.

A. $f(1,1) = f(45,18) = f(6754,97) = f(44,145) = f(1527,14) = f(37,172) = 2$.

B. $f(1,2) = 3$.

C. $f(5,4) = 5$.

D. $f(103,6) = 7$.

E. $f(329891,10) = 11$.

F. $f(36846277,12) = 13$.

No exemplo anterior usamos uma *"receita"* para determinar os pares (x,y). A *"receita"* é a seguinte: para se determinar o número primo p, basta calcular $f(x,y)$ para

$$x = \frac{(p-1)!+1}{p} \quad \text{e} \quad y = p-1.$$

Deste modo para obter o número primo 71 devemos escolher

$$x = \frac{(71-1)!+1}{71} = \frac{70!+1}{71} \quad \text{e} \quad y = 71-1 = 70.$$

6 Conclusão

Através dos tópicos abordados neste trabalho foi possível uma melhor compreensão dos números primos. Ao explorar algumas questões relativas aos números primos fomos conduzidos a uma variedade de resultados de extrema importância na Teoria dos Números que ampliaram o nosso conhecimento em Matemática. Também foi salutar no desenvolvimento do trabalho a utlização da linguagem LaTeX que se apresentou como um modo eficaz e incrivelmente estético para a elaboração de trabalhos acadêmicos. Conforme tudo o que foi estudado e encontrado nas respectivas bibliografias concluímos que os números primos continuarão sendo um tópico de extrema importância na Matemática, em especial para a Teoria dos Números.

A Aplicações no Ensino Médio

A.1 Números Primos e o máximo divisor comum entre dois números naturais

Neste plano de aula deseja-se apresentar ao estudante do ensino médio aplicações envolvendo os números primos e o máximo divisor comum entre dois números naturais.

1. **Tema:** Números primos e máximo divisor comum entre dois números naturais.
2. **Objetivos Gerais:** Deseja-se que o estudante adquira habilidades que possibilite a resolução de questões envolvendo números primos e o máximo divisor comum entre dois números naturais.
3. **Objetivos Específicos:** Pretende-se que o estudante ao final dos estudos seja capaz de: compreender o conceito de máximo divisor comum entre dois números naturais, calcular o máximo divisor comum entre dois números naturais e resolver situações problema que envolvam o máximo divisor comum entre dois números naturais.
4. **Conteúdo:** Números primos e máximo divisor comum.
5. **Metodologia:** Aula expositiva que contemple o conteúdo mencionado, resolução de exemplos a fim de fixar a teoria desenvolvida, sugestão de exercícios visando aplicar os conceitos e resultados trabalhados, correção de exercícios e esclarecimento de eventuais dúvidas.
6. **Bibliografia Recomendada:** HEFEZ, A. *Elementos de Aritmética*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.

A.1.1 Desenvolvimento

Inicialmente, vamos definir o máximo divisor comum entre dois números naturais.

Definição A.1 (Máximo Divisor Comum)**.** *O máximo divisor comum entre dois naturais a e b (a ou b diferente de zero), denotado por (a, b), é o maior inteiro que divide a e b.*

Exemplo A.2. Temos que $(18, 12) = 6$, visto que 6 é o maior número que divide 18 e 12.

Para calcular o máximo divisor comum entre dois números naturais há um processo prático e muito eficiente, que será detalhado a seguir.

Dados dois números naturais a e b para obter (a, b) procedemos da seguinte forma:

i. Decompomos a e b em fatores primos;

ii. Após realizadas as decomposições em fatores primos, escolhemos os fatores primos comuns com seus menores expoentes;

iii. Efetue produto dos fatores primos comuns com seus menores expoentes.

De um modo geral: **"O máximo divisor comum é igual ao produto dos fatores primos comuns tomados com seus menores expoentes".**

Observação A.3. O processo descrito anteriormente pode ser extendido para três ou mais números.

Exemplo A.4. Calcule $(72, 90)$.

Resolução: Vamos efetuar as decomposições em fatores primos

$$72 = 2^3 \cdot 3^2 \qquad 90 = 2 \cdot 3^2 \cdot 5.$$

Os fatores primos comuns são: 2 e 3. Para o fator 2 o menor expoente é 1 e para o fator 3 escolhemos expoente 2 (comum nas duas decomposições), deste modo

$$(72, 90) = 2^1 \cdot 3^2 = 2 \cdot 9 = 18$$

Exemplo A.5. Calcule $(2000, 2400)$.

Resolução: Vamos efetuar as decomposições em fatores primos

$$2000 = 2^4 \cdot 5^3 \qquad 2400 = 2^5 \cdot 3 \cdot 5^2.$$

Os fatores primos comuns são: 2 e 5. Para o fator 2 o menor expoente é 4 e para o fator 5 o menor expoente é 2, deste modo

$$(2000, 2400) = 2^4 \cdot 5^2 = 16 \cdot 25 = 400$$

Exemplo A.6. Um tanque tem 210 litros e outro tanque tem 475 litros. Qual seria a capacidade máxima, em litros, de um balde (totalmente cheio) que pudesse completar o volume dos dois tanques?

Resolução: A capacidade do balde deve ser suficiente para completar os dois tanques, então a capacidade do balde deve ser um divisor comum de 210 e 475, como a capacidade deve ser a máxima possível concluímos que a capacidade do balde deve ser igual ao $(210, 475)$. Como

$$210 = 2 \cdot 3 \cdot 5 \cdot 7 \qquad 475 = 5^2 \cdot 19.$$

Temos

$$(210, 475) = 5.$$

Resposta: O balde deve ter uma capacidade de 5 litros.

Exemplo A.7. Um marceneiro dispõe de três ripas de madeira que medem 60 cm, 80 cm e 100 cm de comprimento, respectivamente. Ele deseja cortá-las em pedaços iguais de maior comprimento possível. Qual é a medida procurada?

Resolução: Como os pedaços devem tem o mesmo comprimento sendo este o máximo possível, o comprimento desejado é equivalente ao $(60, 80, 100)$. Como

$$60 = 2^2 \cdot 3 \cdot 5 \qquad 80 = 2^4 \cdot 5 \qquad 100 = 2^2 \cdot 5^2.$$

Temos

$$(60, 80, 100) = 2^2 \cdot 5 = 4 \cdot 5 = 20.$$

Resposta: A medida procurada é 20 cm.

A.2 Tópico preparatório para olimpíadas de Matemática

Neste plano de aula deseja-se apresentar ao estudante do ensino médio o conceito de congruência entre dois números inteiros bem como suas principais propriedades. Este tópico geralmente não está presente no currículo do ensino médio, entretanto, é de fundamental importância para o aluno que deseja participar da Olimpíada Brasileira de Matemática promovida pela Sociedade Brasileira de Matemática (SBM) e para os alunos que desejam se aprofundar na disciplina de Matemática. Deste modo será possível que o aluno utilize as congruências e suas propriedades para resolver questões sofisticadas como, por exemplo, as questões de matemática olímpica. Assim o aluno é estimulado e encorajado a estudar matemática.

1. **Tema:** Aritmética dos Restos
2. **Objetivos Gerais:** Deseja-se que o estudante adquira habilidades que possibilite a resolução de questões avançadas relacionadas com a aritmética dos restos.

3. **Objetivos Específicos:** Pretende-se que o estudante ao final dos estudos seja capaz de compreender o conceito de congruência entre dois números inteiros e utilizar as principais propriedades para resolver problemas avançados.

4. **Conteúdo:** Resto de uma divisão, congruência entre dois inteiros e suas principais propriedades.

5. **Metodologia:** Aula expositiva que contemple o conteúdo mencionado, resolução de exemplos a fim de fixar a teoria desenvolvida, sugestão de exercícios visando aplicar os conceitos e resultados trabalhados, correção de exercícios e esclarecimento de eventuais dúvidas.

6. **Bibliografia Recomendada:**

[1] SANTOS, J.P.D.O. *Introdução à Teoria dos Números.* 1. ed. Rio de Janeiro: Impa 2007.

[2] HEFEZ, A. *Elementos de Aritmética.* 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.

A.2.1 Desenvolvimento

Vamos, inicialmente, definir o conceito de congruência entre dois números inteiros.

Definição A.8. *Seja m um número natural diferente de zero. Diremos que dois números naturais a e b são congruentes módulo m se os restos de sua divisão por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se:*

$$a \equiv b \; mod \; m$$

Por exemplo, $256 \equiv 130 \; mod \; 7$, pois 256 quando dividido por 7 deixa resto 4 e 130 quando dividido por 7 também deixa resto 4.

Três Propriedades Importantes: Se a, b, c, m e n são inteiros, $m > 0$ e $n > 0$, as seguintes propriedades são válidas (as demonstrações podem ser encontradas na bibliografia recomendada).

P_1. Se $a \equiv b \; mod \; m$ e $b \equiv c \; mod \; m$ então $a \equiv c \; mod \; m$.

P_2. Se $a \equiv b \; mod \; m$ então $a \cdot c \equiv b \cdot c \; mod \; m$.

P_3. Se $a \equiv b \; mod \; m$ então $a^n \equiv b^n \; mod \; m$.

Exemplo A.9. Determine o resto da divisão de 41^{65} por 7.

Resolução: Inicialmente observamos que

$$41 \equiv 6 \; mod \; 7$$

Utilizando a propriedade $\mathbf{P_3}$ na congruência acima obtemos que $41^5 \equiv 6^5 \ mod\ 7$ e como $6^5 = 7776 \equiv 6 \ mod\ 7$, a propriedade $\mathbf{P_1}$ nos permite dizer que $41^5 \equiv 6 \ mod\ 7$, aplicando $\mathbf{P_3}$ obtemos que $41^{10} \equiv 36 \ mod\ 7$, e como $36 \equiv 1 \ mod\ 7$ a propriedade $\mathbf{P_1}$ permite concluir que $41^{10} \equiv 1 \ mod\ 7$, aplicando a propriedade $\mathbf{P_3}$ nesta última desigualdade chegamos à $41^{60} \equiv 1 \ mod\ 7$. Agora utilizando $\mathbf{P_2}$ temos

$$41^{65} = 41^5 \cdot 41^{60} \equiv 41^5 \cdot 1 \ mod\ 7 \Rightarrow 41^{65} \equiv 41^5 \ mod\ 7$$

Como $41^5 \equiv 6 \ mod\ 7$, a propriedade $\mathbf{P_1}$ nos permite concluir que

$$41^{65} \equiv 6 \ mod\ 7$$

Ou seja, o resto da divisão de 41^{65} por 7 é igual a 6.

Exemplo A.10. Determine o algarismo das unidades do número 7^{999999}.

Resolução: Determinar o algarismos das unidades de um número é equivalente a determinar o resto de sua divisão por 10. Deste modo vamos determinar o resto da divisão de 7^{999999} por 10. Observe que

$$999999 = 999996 + 3 = 4 \cdot 249999 + 3$$

Agora verifique a sequência de implicações

$$7^4 = 2401 \equiv 1 \ mod\ 10 \Rightarrow 7^{4 \cdot 249999} \equiv 1^{249999} \ mod\ 10 \Rightarrow 7^{999996} \equiv 1 \ mod\ 10 \Rightarrow$$

$$7^3 \cdot 7^{999996} \equiv 7^3 \cdot 1 \ mod\ 10 \Rightarrow 7^{999999} \equiv 7^3 \ mod\ 10$$

Como $7^3 = 343 \equiv 3 \ mod\ 10$, temos que $7^{999999} \equiv 3 \ mod\ 10$, isto é, o algarismo das unidades do número 7^{999999} é igual a 3.

Exemplo A.11. Detrmine o algarismo das centenas do número 14^{82}.

Resolução: Para resolver a questão vamos determinar o resto da divisão de 14^{82} por 1000, o algarismo da centena deste resto coincide com o algarismo da centena de 14^{82}. Obesrve

$$14^5 = 537824 \equiv 824 \ mod\ 1000 \Rightarrow 14^{10} \equiv 824^2 \ mod\ 1000 \Rightarrow$$

$$14^{10} \equiv 678976 \ mod\ 1000 \Rightarrow 14^{10} \equiv 976 \ mod\ 1000 \Rightarrow$$

$$14^{20} \equiv 976^2 \ mod\ 1000 \Rightarrow 14^{20} \equiv 952576 \ mod\ 1000 \Rightarrow 14^{20} \equiv 576 \ mod\ 1000 \Rightarrow$$

$$14^{40} \equiv 576^2 \ mod\ 1000 \Rightarrow 14^{40} \equiv 331776 \ mod\ 1000 \Rightarrow 14^{40} \equiv 776 \ mod\ 1000 \Rightarrow$$

$$14^{80} \equiv 776^2 \ mod\ 1000 \Rightarrow 14^{80} \equiv 602176 \ mod\ 1000 \Rightarrow 14^{80} \equiv 176 \ mod\ 1000 \Rightarrow$$

$$14^{80} \equiv 176 \ mod\ 1000 \Rightarrow 14^2 \cdot 14^{80} \equiv 14^2 \cdot 176 \ mod\ 1000 \Rightarrow 14^{82} \equiv 196 \cdot 176 \ mod\ 1000 \Rightarrow$$

$$14^{82} \equiv 34496 \ mod\ 1000 \Rightarrow 14^{82} \equiv 496 \ mod\ 1000$$

Deste modo o resto da divisão de 14^{82} por 1000 é 496 razão pela qual o algarismo das centenas do número 14^{82} é 4.

Referências

[1] HEFEZ, A. *Elementos de Aritmética*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2011.

[2] RIBENBOIM, P. *The New Book of Prime Number Records*. 3. ed. New York: Springer Verlag, 1996.

[3] HARDY, G. H.; WRIGHT, E. M. *An Introduction to the Theory Of Numbers*. 5. ed. New York: Oxford University Press, 1979.

[4] SANTOS, J. P. D. O. *Introdução à Teoria dos Números*. 1. ed. Rio de Janeiro: Impa, 2007.

[5] MARTINEZ, F. E. B. et al. *Teoria dos Números: Um Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro*. 3. ed. Rio de Janeiro: Impa, 2013.

[6] GIMPS. *Great Internet Mersenne Prime Search*. nov. 2014. Disponível em: <http://www.mersenne.org/>.

[7] MILLS, W. A prime-representing function. *American Mathematical Society*, v. 53, p. 604, 1947.

[8] WRIGHT, E. M. A prime-representing function. *The American Mathematical Monthly*, v. 58, p. 616–618, 1951.

[9] HONSBERGER, R. *Mathematical Gems II*. 1. ed. United States of America: The Mathematical Association of America, 1976.

[10] WATANABE, R. G. Uma fórmula para os números primos. *Revista do Professor de Matemática*, v. 37, p. 19–21, 1998.