UNIVERSIDADE FEDERAL DO CARIRI - UFCA

CENTRO DE CIÊNCIAS E TECNOLOGIA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

FRANCISCO DO CARMO SILVA

Falsos Primos e o Método de Fatoração de Fermat

JUAZEIRO DO NORTE - 2018

FRANCISCO DO CARMO SILVA

Dissertação de Mestrado:

Falsos Primos e o Método de Fatoração de Fermat

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional - PROFMAT do Centro e Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Paulo César Cavalcante de Oliveira

JUAZEIRO DO NORTE - 2018

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Cariri
Sistema de Bibliotecas

S578f Silva, Francisco do Carmo.
Falsos primos e método de fatoração de Fermat/ Francisco do Carmo Silva. – 2018.
47 f.: il.; color.; enc. ; 30 cm.

Dissertação (Mestrado) – Universidade Federal do Cariri, Centro de Ciências e Tecnologia – Programa de Pós-graduação em Matemática em Rede Nacional, Juazeiro do Norte, 2018.
Área de Concentração: Ensino de Matemática.

Orientação: Prof. Dr. Paulo César Cavalcante de Oliveira.

1. Aritmética. 2. Números primos. 3. Números pseudoprimos. I. Título.

. CDD 510

Bibliotecário: João Bosco Dumont do Nascimento – CRB 3/1355

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO CARIRI
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Falsos Primos e o Método de Fatoração de Fermat

Francisco do Carmo Silva

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional – PROFMAT do Centro de Ciências e Tecnologia da Universidade Federal do Cariri, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática

Aprovada em 25 de abril de 2018.

Banca Examinadora

Prof. Dr. Paulo César Cavalcante de Oliveira - URCA
Orientador

Profa. Dra. Clarice Dias de Albuquerque - UFCA

Prof. Dr. Flávio França Cruz – URCA

Minha Família.

Agradecimentos

Agradeço a Deus por ter me dado oportunidade e coragem para enfrentar esse curso e as longas viagens durante o curso.

A minha mãe Margarida do Carmo Silva, por sempre acreditar em mim.

Aos professores do curso por todas as suas contribuições e, em especial, ao Professor Dr. Paulo César, por sua paciência e dedicação em me encorajar e auxiliar na finalização deste texto.

Agradeço ao colégio de Ensino Médio Dr. João Ribeiro Ramos em nome da atual diretora Professora Mestre Sandra Maria Chaves pela compreensão de minha ausênsia no período do mestrado.

Ao meus amigos José dos Santos Melo e ao Professor Mestre Antônio Luiz Sampaio pelo encorajamento constante para que eu terminasse o mestrado.

Aos colegas da turma de mestrado, pelas reflexões, críticas e sugestões.

Agradeço a CAPES pelo apoio financeiro.

"*E talvez a posteridade me agradeça por ter mostrado que os antigos não sabiam tudo.* ".

P.Fermat

Resumo

Os números desempenham papel fundamental na criptografia RSA e têm muita aplicação no ensino básico. Isto explica bem por que estamos sempre motivados a encontrar primos cada vez maiores. Então nessa busca constante de primos, o presente trabalho tem por objetivo estudar as consequências do Pequeno Teorema de Fermat, que foi formulado pelo Françês Pierre de Fermat. Esse teorema tem implicações espantosas, pois com ele é possivel dizer com certeza se um dado número n é composto sem explicitar seus fatores. No entanto, existem números compostos que satisfazem ao Pequeno Teorema de Fermat, e que não são primos, são os "Falsos Primos"que serão chamados de pseudoprimos. Apresentaremos ainda, um método de fatoração devido a Fermat, esse método representou uma melhoria real em relação ao crivo de Eratóstenes na tentativa de encontrar primos.

Palavras-chave: Aritmética; Números Primos; Números Pseudoprimos.

Abstract

The odd numbers play a key role in RSA encryption and have a lot of application in elementary education. This explains why we are always motivated to find bigger odd numbers. Then in this constant search of primes, the present work aims to study the consequences of the Little Theorem of Fermat, which was formulated by the French Pierre de Fermat. This theorem has amazing implications, since with it it is possible to say with certainty if a given number n is composed without making explicit its factors. However, there are compound numbers that satisfy Fermat's Small Theorem, and which are not prime ones, are "False Odds"that will be called pseudoprimes. We will also present a method of factorization due to Fermat, this method represented an improvement real relation to the Eratosthenes sieve in an attempt to find odd numbers.

Keywords : arithmetic;primary numbers;numbers pseudoprimes.

Lista de Tabelas

Sumário

Capítulo 1

INTRODUÇÃO

Pierre de Fermat foi um francês que viveu no século XVII em Toulose na França. Era advogado por profissão e mantinha como hobby a Matemática. Tanto que é considerado por muitos como o príncipe dos amadores.

Foram muitas suas contribuições à Matemática, dentre elas a criação da Geometria Analítica, contribuiu com a Teoria da Probabilidade. Mas sem dúvida, sua paixão foi a Teoria dos Números, trazendo esta de volta do reino do misticismo e das superstições. De posse do livro de Diofanto de Alexandria, Fermat fez várias anotações, uma delas deixou matemáticos do mundo inteiro ocupados por mais de 350 anos. Uma dizia, "Tenho uma solução realmente maravilhosa desse teorema, mas as margens deste livro é muito estreita para contê-la". Referindo-se ao que ficou conhecido por último teorema de Fermat, no qual afirma não haver solução, exceto a trivial, para equação $x^n + y^n = z^n$ para todo $n \in \mathbb{N}$, tal afirmação foi demonstrado apenas em 1994 pelo matemático britânico Andrew J. Wiles que dedicou 7 anos de sua vida a solução do problema. O fato é que há rumores de que Fermat havia blefado, pois muita matemática foi desenvolvida para solução do mesmo. Quem sabe ele não tinha mesmo a solução?

Pierre de Fermat mantinha correspondência com vários matemáticos de sua época, dentre eles, estão Pascal, Mersenne, Descartes, e tudo que sabemos hoje sobre Fermat, é graças ao seu filho mais velho Clément Samuel que passou cinco anos reunindo cartas e anotações de seu pai e ter publicado à comunidade matemática. Fermat deixou 48 anotações. Coube ao matemático suíço Leonhard Euler, quase 100 anos após a morte de Fermat, recriar e demonstrar. Euler de fato demonstrou todos, exceto um, que como foi dito, trata-se do Último Teorema de Fermat.

Dentre todas as observações feitas por Fermat, vamos tratar neste trabalho de três valiosas perólas para a teoria dos números. Em uma correspondencia destinada a Bernhard Frénicle de Bessy(1605-1675), Fermat afirma que se p é um número primo e a um inteiro qualquer não divisível por p, então p divide $a^{p-1} - 1$. Esta afirmação ficou conhecido como o Pequeno Teorema de Fermat e demonstrado posteriormente por Leonard Euler.

O Pequeno Teorema de Fermat revelou-se como um teste de não primalidade, isto é, dado um inteiro n ímpar, ele detecta facilmente se este número é composto sem precisar fatorar. Caso n seja composto, ele não fornece nenhum fator de sua fatoração. É claro que se n é um número primo, o Pequeno Teorema de Fermat é satisfeito por todo inteiro a qualquer não divisível por n. Mas será que todo n que satisfaz ao Pequeno Teorema Fermat, tem -se necessariamente que n é primo? Muitos matemáticos acreditava que sim. Porém o número 341 divide $2^{340} - 1$, mas $314 = 11 \cdot 31$ é composto. Assim, uma recíproca pura e simples do Pequeno Teorema de Fermat não verdadeira. Então o número n composto que satisfaz ao pequeno teorema de Fermat é chamado de " falsos primos", conhecidos por pseudoprimos, por satisfazer propriedades esperadas de ser encontrada somente em números primos.

Uma outra observação que chamou bastante atenção dos matemáticos, foi que Fermat conjecturou que $F_n = 2^{2^n} + 1$ é primo para todo $n \in \mathbb{N}$. De fato, para $n = 0, 1, 2, 3$ e 4 isso acontece, mas para $n = 5$, F_n ele é composto. Vale ressaltar que os números da forma $F_n = 2^{2^n} + 1$ ou é primo de Fermat ou pseudoprimo de Fermat como veremos adiante. A importância dessa conjectura, é que temos uma outra forma de provar que os números primos estão em quantidade infinita.

Fermat descreveu uma técnica para a fatoração de grandes números, conhecido por "Fatoração de Femat". Dado n ímpar, a fatoração de Fermat consiste na busca de x e y tais que $n = x^2 - y^2$, caso encontremos x e y, teremos $x + y$ e $x - y$ como fatores de n, visto que $n = x^2 - y^2 = (x + y)(x - y)$.

Este trabalho, foi dividido em 5 partes, e é destinado a professores do ensino médio e alunos de olimpíadas de matemática que queiram aprofundar seus conhecimentos em Teoria dos Números.

No capítulo 2, apresentamos fundamentos básicos para entendimentos deste trabalho, tais como indução finita, divisibilidade, algoritmo da divisão euclidiana, máximo divisor comum, definição de número primo e sua propriedades, bem como o Teorema Fundamental

da Aritmética. E finalizando este capítulo, mostramos uns tipos especiais de primos como, os primos gêmeos, primos de Sophie Germain, os primos de Mersenne e os primos de Fermat.

No capítulo 3, apresentamos a técnica milenar de encontrar números primos, o crivo de Eratóstenes e em seguida um método de fatoração de números grandes bem mais ingênuo que o crivo de Eratóstenes criado por Pierre de Fermat.

O capítulo 4, é dedicado a aritmética dos restos, especificamente estudaremos congruências módulo m bem como suas propriedades e aplicações na divisibilidade. Enunciaremos e demonstramos o Pequeno Teorema de Fermat. Finalizamos este capítulo com raízes primitivas e resíduos quadráticos.

E, por fim, o capítulo 5 é dedicado aos números pseudoprimos. Veremos os pseudoprimos de base 2, pseudoprimos de base a, os pseudoprimos de Euler, os Pseudoprimos fortes e os números de Carmichael.

Capítulo 2

FUNDAMENTOS

Neste capítulo será apresentado vários resultados básicos de extrema importância para entendimento do trabalho.

2.1 Indução Finita

Nesta seção vamos enunciar o princípio da indução finita seguida de uma aplicação. O leitor interessado na demonstração, deverá consultar [7]

Teorema 2.1 (Princípio da Indução Finita)**.** *Seja $P(n)$ a proposição que queremos provar. Para que $P(n)$ seja verdadeira para todo n natural, basta que :*
(i) $P(1)$ seja verdadeira;
(ii) Se $P(k)$ for verdadeira para algum número natural k, então $P(k+1)$ também seja verdadeira.

Exemplo 1. Vejamos como usar esse método para mostrar a validade, para todo natural n, da fórmula

$$1 + 2 + 3 + \cdots (2n - 1) = n^2.$$

Observe que $P(1)$ é verdadeira, já que a fórmula é verificada para $n = 1$. Suponha agora que, para algum n natural, $P(n$ seja verdadeira, ou seja, que

$$1 + 2 + 3 + \cdots (2n - 1) = n^2.$$

Queremos prova que $P(n+1)$ é verdadeira. Somando $2n+1$, que é o próximo ímpar após $2n - 1$, a ambos os lados da igualdade acima, obtemos a igualdade também verdadeira:

$$1 + 2 + 3 + \cdots (2n - 1) + 2n + 1 = n^2 + 2n + 1 = (n + 1)^2.$$

Isso mostra que $P(n+1)$ é verdadeira, toda vez que $P(n)$ é verdadeira. Pelo teorema,a fórmula é válida para todo natural n. $\Diamond$

2.2 Divisibilidade

Definição 1. *Se a e b são inteiros, dizemos que a divide b denotando por $a|b$, se existir um inteiro c tal que $b = ac$. Se a não divide b escrevemos $a \nmid b$*

Exemplo 2. Assim por exemplo, observe que 3 divide 27, logo escrevemos $3|27$, e que 5 não divide 13, denotamos por $5 \nmid 13$ $\Diamond$

A divisibilidade dos números inteiros goza das seguintes propriedades.

Proposição 2.2. *Dados $a, b, c \in \mathbb{Z}$ tem-se:*

i) $1|a$, $a|a$ e $a|0$;

ii) se $a|b$ e $b|c$, então $a|c$;

iii) se $a|b$ e $a|c$, então para todo $x, y \in \mathbb{Z}$ tem-se que $a|(xb + yc)$;

iv) se $a|(b + c)$, então $a|b \iff a|c$.

Demonstração.

i) Isto decorre das igualdades $a = a \cdot 1$, $a = 1 \cdot a$ e $0 = 0 \cdot a$.

ii) Como $a|b$ e $b|c$, existem inteiros k_1 e k_2 tais que $b = k_1 a$ e $c = k_2 b$. Substituindo o valor de b na equação $c = k_2 b$ teremos $c = k_2 k_1 a$, o que implica $a|c$.

iii) Como $a|b$ e $a|c$, existem inteiros f e g tais que $b = fa$ e $c = ga$.
Logo, $xb + yc = x(fa) + y(ga) = (xf + yg)a$, o que mostra que $a|(xb + yc)$.

iv) Deixaremos a prova deste item para o leitor. Interessados consultar [7]. $\square$

Exemplo 3. A fim de ilustrar a Proposição 2.2, tomando $a = 7$, $b = 21$ e $c = 63$, observe que
(i)É fato que $1|7$, $7|7$ e $7|0$;
(ii)vemos sem dificuldades que $7|21$ e $21|63$, então $7|63$;
(iii) Por (ii),$7|21$ e $21|63$, então para todo $x, y \in \mathbb{Z}$ tem-se que $7|(21x + 63y) \iff 7|21(x + 3y)$;
(iv) É claro que $7|(21 + 63)$, pois $7|21$ e $21|63$. $\Diamond$

2.3 Divisão Euclidiana

Antes de enunciar o teorema da divisão euclidiana, vamos definir dois conceitos básicos que será utilizado na demonstração do mesmo.

Definição 2. *Para todo $x \in \mathbb{R}$, definimos piso ou parte inteira $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k < x \leq k+1$.*

Exemplo 4. $\lfloor 2 \rfloor = 2$; $\lfloor 3,7 \rfloor = 3$; $\left\lfloor \sqrt{2} \right\rfloor = 1$; $\lfloor -\pi \rfloor = -4$. ◊

Definição 3. *Para todo $x \in \mathbb{R}$, definimos o teto $\lceil x \rceil$ de x como o único $k \in \mathbb{Z}$ tal que $k-1 < x \leq k$.*

Exemplo 5. $\lceil \sqrt{2} \rceil = 2$; $\lceil -\pi \rceil = -3$; $\lceil 7 \rceil = 7$. ◊

Teorema 2.3 (Divisão Euclidiana)**.** *Dado $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ com*

$$a = bq + r \text{ com } 0 \leq r <\mid b \mid \quad (r = 0 \Longleftrightarrow b|a)$$

(q é chamado de quociente e r de resto da divisão de a por b).

Demonstração. Vamos mostrar a existência de q e r satisfazendo as duas condições acima: basta tomar

$$q = \begin{cases} \lfloor \frac{a}{b} \rfloor, & \text{se} \quad b > 0 \\ \lceil \frac{a}{b} \rceil, & \text{se} \quad b < 0 \end{cases} \quad \text{e} \quad r = a - bq \text{ em ambos casos}$$

É fácil verificar que $o \leq r <\mid b \mid$ a partir das definições das funções piso e teto. Por outro lado, se $a = bq_1 + r_1 = bq_2 + r_2$ com $0 \leq r_1, r_2 <\mid b \mid$, então temos que $r_2 - r_1 = b(q_1 - q_2)$, é um múltiplo de b com $\mid r_2 - r_1 \mid <\mid b \mid$, portanto $r_2 - r_1 = 0$ e assim $q_1 = q_2$ também, o que prova a unicidade.

□

2.4 Máximo Divisor Comum-MDC

Definição 4. *O Máximo Divisor Comum de dois números inteiros a e b, é o maior inteiro positivo que é divisor de a e b ao mesmo tempo. Vamos denotá-lo por (a, b).*

Exemplo 6. O máximo divisor comum de 8 e 10 é 2, pois os divisores positivos de 8 são $\{1, 2, 4, 8\}$ e os divisores positivos de 10 são $\{1, 2, 5, 10\}$. Portanto podemos representar por $(8, 10) = 2$. ◊

Teorema 2.4. *Seja d o máximo divisor comum de a e b, então existem inteiros n_0 e m_0 tais que $d = n_0a + m_0b$.*

Demonstração. Seja B o conjunto de todas as combinações lineares $\{na + mb\}$ onde n e m são inteiros. Este conjunto contém claramente, números negativos, positivos e também o zero. Vamos escolher n_0 e m_0 tais que $c = n_0a + m_0b$ seja o menor inteiro positivo pertencente ao conjunto B. Vamos provar que $c|a$ e $c|b$. Como as demonstrações são similares, mostraremos apenas que $c|a$. A prova é por contradição. Suponhamos que $c \nmid a$. Neste caso, pelo teorema 2.4, existem q e r tais que $a = qc + r$ com $0 < r < c$. Portanto $r = a - qc = a - q(n_0a + m_0b) = (1 - qn_0) + (-qm_0)$. Isto mostra que $r \in \mathbb{B}$, pois $(1 - qn_0)$ e $(-qm_0)$ são inteiros, o que é uma contradição, uma vez que $0 < r < c$ e c é o menor elemento positivo de B. Logo $c|a$ e de forma análoga se prova que $c|b$.
Como d é um divisor comum de a e b, existem inteiros k_1 e k_2 tais que $a = k_1d$ e $b = k_2d$, portanto, $c = n_0a+m_0b = n_0k_1d+m_0k_2d = d(n_0k_1+m_0k_2)$ o que implica $d|c$. Logo $d \leq c$ ambos positivose e como $d < c$ não é possível, uma vez que d é o máximo divisor comum, concluímos que $d = n_0a + m_0b$. □

Definição 5. *Os inteiros a e b são relativamente primos quando $(a, b) = 1$.*

Proposição 2.5. *Se $(a, b) = 1$ e $a|bc$, então $a|c$.*

Demonstração. Como $\text{mdc}(a, b) = 1$, existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1 \Longrightarrow a \cdot cx + (bc) \cdot y = c$ Do fato de a dividir cada termo do lado esquerdo, temos que $a|c$. □

Proposição 2.6. *Sejam $a, b, c \in \mathbb{N}$ e suponhamos que $(a, b) = 1$. Se $a|c$ e $b|c$, então $ab|c$.*

Demonstração. Se $a|c$, então existe $t \in \mathbb{N}$ tal que $c = at$, mas $b|c$ e Como $(a, b) = 1$, isto implica que b tem que dividir t. Assim teremos que $t = bk$, para algum inteiro k. Portanto $c = at = a(bk) = (ab)k$ logo ab divide c. □

Exemplo 7. 7|42 e 3|42 e como (3,7)=1, então $7 \cdot 3|42$. ◊

2.5 Número Primo

Visto o conceito de divisibilidade, estamos preparados para definirmos o conceito de número primo, objeto de estudo deste trabalho.

Definição 6. *Um número inteiro n maior do que 1 que só possui como divisores positivos n e 1 é chamado de número primo. Se n não é primo dizemos que n é composto.*

Proposição 2.7. *Dados dois números primos p e q e um número inteiro a qualquer, valem as seguintes afirmativas.*

i) Se $p|\, q$, então $p = q$.

ii) Se $p \nmid a$, então $(p, a) = 1$.

Demonstração. i) De fato, como $p|q$ e sendo q primo, tem-se que $p = 1$ ou $p = q$. Sendo p primo, tem-se que p é maior que 1, o que acarreta $p = q$.
ii) Se $(p, a) = d$, então $d|p$ e $d|a$. Portanto $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid a$ e, consequentemente, $d = 1$. □

Proposição 2.8 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Se $p|ab$, então existe $e \in \mathbb{Z}$ tal que $ab = pe$. Supondo que $p \nmid a$, então $(p, a) = 1$, pois p é primo e, segue pelo teorema 2.2 que existem $m, n \in \mathbb{Z}$ tais que $mp + na = 1$. Multiplicando a equação acima por b, temos $b = mpb + nab$. Substituindo ab por pe, teremos $b = mpb + npe = p(mb + ne)$ e, portanto $p|b$. □

Exemplo 8. $7|(31 \cdot 42)$, logo $7|42$ uma vez que $(7, 31) = 1$. ◊

2.6 Teorema Fundamental da Aritmética

Teorema 2.9 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Se $n = 2$, o resultado é obviamente verificado. Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos, então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, \cdots p_r$ e $q_1, \cdots, q_s$ tais que $n_1 = p_1 \cdots p_r$ e $n_2 = q_1 \cdots q_s$. Portanto, $n = p_1 \cdots p_r q_1 \cdots q_s$.

Provaremos agora a unicidade da escrita. Suponha que $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i's e os q_j's são números primos. Como, digamos p_1 divide $q_1, \cdots, q_s$, segue pelo Lema de Euclides que p_1 divide algum q_j. Logo, $p_1 = q_j$ para algum j, que após reordenamento de $q_1, \cdots q_s$ podemos supor que seja q_1. Portanto, $p_2 \cdots p_r = q_2 \cdots q_s$. Como $p_2 \cdots p_r < n$, a hipótese de indução acarreta que $r = s$ e $p_i = q_j$. □

Teorema 2.10 (Euclides)**.** *O conjunto dos números primos é infinito.*

Demonstração. Vamos supor que o conjunto dos primos seja finito. Seja pois, $p_1, p_2, ..., p_n$, a lista de todos os primos. Consideramos o número $R = p_1 \cdot p_2 \cdots p_n + 1$. É claro que R não é divisível por nenhum dos p_i de nossa lista e que R é maior do que qualquer p_i. Mas pelo Teorema 2.9, ou R é primo ou possui algum fator primo e isto implica na existência de um primo que não pertence à nossa lista. Portanto o conjunto dos números primos não pode ser finito. □

2.7 Tipos de Primos

Outro problema, cuja solução desde há muito era procurada pelos matemáticos é a determinação de fórmulas geradoras de números primos. Todas às tentativas foram frustadas, pois as fórmulas apresentadas por alguns matemáticos não geravam somentes primos, mas também números compostos. Mas o crédito deve ser dado aos que tentaram, por isso recebem o nome de primos especiais.

2.7.1 Primos gêmeos

Nesta subseção iremos estudar os primos gêmeos.

Definição 7 (Primos Gêmeos)**.** *Se p e $p+2$ são números primos, então eles são chamados de primos gêmeos.*

Os menores pares de primos gêmeos são $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$. Observamos que a diferença entre eles é de duas unidades. Os primos gêmeos foram caracterizados por Clement em 1949, da seguinte maneira:

Se $n \geq 2$. Os inteiros n e $n + 2$ são ambos primos se, e somente se,

$$4[(n-1)! + 1] + n \equiv 0 \, (mod \, n \, (n+2)) \, .$$

Ao leitor interessado na demonstração deste resultado, indicamos [9]. Um problema em aberto é decidir se existe uma infinidade de pares de primos gêmeos.

2.7.2 Primos de Sophie Germain

Um número primo p é dito *primo de Sophie Germain*, se $2p + 1$ é também um número primo. Assim, por exemplo 2 é primo de Sophie, pois $2 \cdot 2 + 1 = 5$ é primo, mas 13 não é primo de Sophie, pois $2 \cdot 13 + 1 = 27$ que é um número composto.

Este resultado foi considerado, em primeiro lugar, por Sophie Germain, que demonstrou o bonito teorema:

Se p é um primo de Sophie Germain, então não existem inteiros x , y e z, diferentes de zero e não múltiplo de p , tais que $x^p + y^p = z^p$.

Em outras palavras, o " primeiro caso do Último Teorema de Fermat"é verdadeiro para todo expoente primo de Sophie Germain.

Conjectura-se a existência de uma infinidade de primos de Sophie Germain, porém sua demonstração será tão difícil quanto à da existência de uma infinidade de primos gêmeos.

p	2	3	5	11	23	29	41	53	83	89
2p+1	5	7	11	23	47	59	83	107	167	179

Tabela 2.1: Os primos de Sophie Germain entre 1 e 100

2.7.3 Primos de Mersenne

Marin Mersenne foi um matemático Françês que viveu no século XVI. Mersenne mantinha correspondência com Fermat, Descartes, Pascal, entre outros. Seu papel principal com esse círculo de amizades foi o de divulgar os conhecimentos matemáticos de sua época. Influenciado por Fermat, Mersenne passou a estudar os números da forma $2^p - 1$, com p primo. E portanto, os números estudados por Mersenne que são primos, são conhecidos por Primos de Mersenne em sua homenagem.

Proposição 2.11. *Sejam a e n números naturais maiores do que* 1. *Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração. Como $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ e o fator da direita é maior do que 1, pois $(a > 1)$, concluímos que $a - 1$ deve ser igual a 1 uma vez que $a^n - 1$ é primo. Portanto a deve ser igual a 2. Por outro lado, se n não for primo então $n = rs, r > 1$ e $s > 1$. Disto concluímos que

$$2^n - 1 = 2^{rs} - 1 = (2^r)^s - 1 = (2^r - 1)((2^r)^{(s-1)} + (2^r)^{(s-2)} + \cdots + 2^r + 1) \,,$$

o que contradiz o fato de $2^{rs} - 1$ ser primo, o que implica que n deve ser primo. □

Definição 8. *Os números de Mersenne são da forma $M_p = 2^p - 1$, onde p é um número primo.*

Desde o tempo de Mersenne, era sabido que certos números de Mersenne são primos e que outros são compostos. Por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ e $M_7 = 127$ são primos, enquanto $M_{11} = 23 \cdot 89 = 2047$ é composto.

Em 1640, Mersenne afirmou que M_q é primo para $q = 13, 17, 19, 31, 67, 127$ e 257; estava ele enganado em relação a 67 e 257; também não incluíra $61, 89$ e 107 (entre os números inferiores a 257) que também fornecem números de Mersenne primos. Sua afirmação era extraordinária, em face da grandeza dos números envolvidos.

Em relação aos números de Mersenne, o problema que se apresenta naturalmente, é saber se são primos ou compostos e, neste último caso, determinar seus fatores primos.

2.7.4 Primos de Fermat

Esta subseção relaciona-se com os números de Fermat, que são da forma $F_n = 2^{2^n} + 1$ em homenagem a Pierre de Fermat.

Proposição 2.12. *Sejam a e n números naturais maiores do 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 do que 2, o que contraria o fato de ser primo. Se n tivesse um divisor primo p diferente de 2, teríamos $n = n'p$ com $n' \in \mathbb{N}$. E portanto, $a^{n'} + 1$ dividiria $(a^{n'})^p + 1 = a^n + 1$, contradizendo o fato de esse último número ser primo. Isto implica que n é da forma 2^m. □

Definição 9. *Os números de Fermat são números da forma $F_n = 2^{2^n} + 1$, $n = 0, 1, 2, 3, ...$*

Em 1640, Fermat escreveu em uma de suas cartas a Mersenne que achava que esses números eram todos primos. De fato ,$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$ são primos, mas não se sabe se havia algum outro motivo para que Fermat achasse que todos os números dessa forma fossem primos.

A demonstração de que o sexto número de Fermat não é primo foi dado por Leonhard Euler em 1732. Contradizendo assim a afirmação de Fermat. Portanto, os números de Fermat primos são chamados primos de Fermat. Até hoje, não se sabe se existem outros primos de Fermat além dos primeiros. Conjecturou-se que os primos de Fermat são em número finito. O teorema seguinte nos fornece uma segunda prova da infinitude dos números primos.

Teorema 2.13. *Quaisquer dois números de Fermat distintos F_n e F_m são relativamente primos.*

Demonstração. Para provarmos este resultado vamos mostrar, primeiramente, que a seguinte relação se verifica.

$$F_0F_1 \cdots F_{n-1} = F_n - 2 \, .$$

A prova será feita por indução. Como o caso $n = 1$ se verifica, isto é, $F_0 = F_1 - 2$, vamos supor a validade para n e mostrar que a mesma relação também vale para $n + 1$. Temos que

$$\begin{aligned} F_0F_1 \cdots F_{n-1}F_n &= (F_0F_1 \cdots F_{n-1})F_n \\ &= (F_{n-2})F_n \\ &= ((2^{2^n} + 1 - 2)(2^{2^n} + 1) \\ &= (2^{2^{n+1}} - 1) \\ &= (2^{2^{n+1}} + 1 - 2) \\ &= F_{n+1} - 2 \, . \end{aligned}$$

Supondo $n < m$ temos, pela relação acima, que $F_0F_1 \cdots F_n \cdots F_{m-1} = F_m - 2$. O que implica que $F_m - F_0F_1 \cdots F_n \cdots F_{m-1} = 2$. Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é ímpar d não pode ser 2 e, portanto $(F_n, F_m) = 1$. □

Deste fato podemos concluir que existem infinitos números primos, pois o conjunto dos números de Fermat é infinito e não possuem fatores primos em comum.

Capítulo 3

FATORAÇÃO DE FERMAT

3.1 Crivo de Eratóstenes

O método mais antigo para encontrar primos é o famoso crivo do grego Eratóstenes, que viveu por volta de 230 antes de Cristo. Este crivo permite determinar todos os primos menores que um inteiro n dado.

Exemplo 9. Vamos determinar todo os números primos menores que 40. Para isso, escrevemos todos os números naturais de 2 a 40. Riscam-se, de modo sistemático, todos os números compostos da tabela. Começando pelo os múltiplos de 2 acima de 2, já que nenhum deles é primo. O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3, pois esses não são primos. O terceiro número não riscado é 5, que é primo. Risque todos os múltiplos de 5 maiores que 5, pois estes não são primos. Observe que nesta estapa já podemos parar, pois o próximo número não riscado é o 7, que é primo. E todos os múltiplos de 7 maiores que 7 já foram riscados.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~

Portanto, os primos entre 2 e 40 são todos aqueles que não foram riscados no processo acima, isto é 2 , 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 e 37. ◊

Por se tratar de um importante teste de primalidade, o teorema descrito abaixo justifica bem o crivo de Eratóstenes.

Teorema 3.1. *Se n não é primo, então n possui necessariamente um fator primo menor ou igual a $\sqrt{n}$.*

Demonstração. Seja, portanto, n um número composto e $f > 1$ seu menor fator, então, existe um inteiro positivo a tal que $n = f \cdot a$. Como f é o menor fator, logo $f \leq a$. Por outro lado, $a = \frac{n}{f}$, daí $f \leq \frac{n}{f}$, disto segue que $f^2 \leq n$ e portanto, $f \leq \sqrt{n}$. □

Em outras palavras, este teorema mostra que, dado n inteiro qualquer, saber se este é primo, basta dividir n por todos os números primos menores ou iguais a $\sqrt{n}$.

Exemplo 10. Vamos verificar se 53 é um número primo ou composto. Os número primos menores que $\sqrt{53}$ são 2,3,5,e 7. É fácil ver que 53 não é divisível por nenhum destes números, logo 53 é um número primo. ◊

Apesar deste método ser simples, infelizmente é ineficiente para grandes números, pois exige uma quantidade enorme de divisões.

3.2 Método de Fatoração de Fermat

Em um fragmento de uma carta, escrito ao padre Marin Mersenne em 1643, Fermat descreveu uma técnica para a fatoração de grandes números. Isso representou a primeira melhoria real em relação ao método clássico de tentar encontrar um fator de n dividindo por todos os primos que não excedam $\sqrt{n}$.

3.3 Fatoração

A fatoração de Fermat consiste na busca de fatores de um inteiro ímpar n, visto que se n é par, então 2 é um de seus fatores.

Portanto, fatorar n é equivalente a obter solução x e y da equação

$$n = x^2 - y^2 \ .$$

Se n é a diferença de dois quadrados, então é evidente que n pode ser fatorado como

$$n = x^2 - y^2 = (x + y)(x - y) \ .$$

Logo $x - y$ e $x + y$ são fatores de n.

O caso mais fácil do algoritmo de Fermat ocorre quando n é um quadrado perfeito; isto é, quando existe algum inteiro k tal que $n = k^2$. Neste caso temos que k é fator de n. Além disso, na notação acima $x = k$ e $y = 0$.

Observe que se $y > 0$ então $x = \sqrt{n + y^2} > \sqrt{n}$. Isto sugere que a solução começa com a busca de possíveis x e y que satisfaçam a equação $n = x^2 - y^2$, que é equivalente a equação $x^2 - n = y^2$. Primeiro, determinando o menor número inteiro para o qual $k^2 \geq n$. Agora sucessivamente para os números $k^2 - n, (k+1)^2 - n, (k+2)^2 - n, (k+3)^2 - n, \ldots$, até um valor de $m \geq \sqrt{n}$ para o qual $m^2 - n$ é um quadrado ou quando $x = \left(\frac{n+1}{2}\right)$ donde finalmente chegamos a igualdade

$$\left(\frac{n+1}{2}\right)^2 - n = \left(\frac{n-1}{2}\right)^2 .$$

A representação de n correspondente a fatoração trivial de $n = n \cdot 1$. Se este ponto for alcançado sem que haja uma diferença de quadrados descoberta anteriormente, n não possui outros fatores além de n e 1, caso em que é primo.

Fermat usou o procedimento que acabamos de descrever ao fator $2027651281 = 44021 \cdot 46061$. Em apenas 11 passos, em comparação com 4850 divisões pelos primos ímpares até 44021. Este foi provavelmente um caso favorável apresentado por ele para mostrar a principal virtude de seu método, pois não exige que se conheça todos os primos menores do que $\sqrt{n}$ a fim de encontrar fatores de n.

Exemplo 11. Para ilustrar a aplicação do método de Fermat, vamos fatorar o número inteiro $n = 119143$.

De uma tabela de quadrados, encontramos que $345^2 < 119143 < 346^2$. Assim basta considerar o valor de $k^2 - 119143$ para k no intervalo $346 < k < \left(\frac{119143+1}{2}\right) = 59572$. O cálculo começa da seguinte forma:

$$\begin{aligned}
346^2 - 119143 &= 573; \\
347^2 - 119143 &= 1266; \\
348^2 - 119143 &= 1961; \\
349^2 - 119143 &= 2658; \\
350^2 - 119143 &= 3357; \\
351^2 - 119143 &= 4058; \\
352^2 - 119143 &= 4761 = 69^2. ,
\end{aligned}$$

Esta última linha exibe a fatoração

$$119143 = 352^2 - 69^2 = (352 + 69) \cdot (352 - 69) = 421 \cdot 283.$$

Os dois fatores em si mesmo são primos. Em apenas sete passos obtivemos a principal fatoração do número 119143. ◊

Claro que nem sempre isso ocorre, pois pode demorar muitos passos antes de uma diferença se tornar um quadrado. Ao examinar a diferença $k^2 - n$ como possível quadrado, muitos valores podem ser imediatamente excluídos por inspeção dos dígitos finais. Sabemos, por exemplo que um quadrado deve terminar em um dos seis dígitos 0, 1,4,5,6,9. Isso nos permite excluir todos os valores no exemplo acima, salvo para 1266, 1961 e 4761. Calculando os quadrados dos inteiros de 0 a 99 módulo 100, verifica-se, que para um quadrado, os dois últimos dígitos são limitados para as seguintes 23 possibilidades

00	21	41	64	89
01	24	44	69	96
04	25	49	76	
09	29	56	81	
16	36	61	84	

O número inteiro 1266 pode ser eliminado da consideração. Desta maneira, uma vez que 61 está entre os dois últimos dígitos permitidos em um quadrado, é necessário apenas observar os números 1961 e 4761. O primeiro não é um quadrado, mas $4761 = 69^2$.

O método de Fermat é efeciente quando os dois fatores de n são quase da mesma magnitude, pois neste caso, um quadrado adequado aparecerá rapidamente como veremos a seguir.

Exemplo 12. Ilustremos mais uma vez fatorando o número $n = 23449$. O quadrado mais pequeno que excede n é 154^2, de modo que a sequência $k^2 - n$ comece. Temos

$$\begin{aligned} 154^2 - 23449 &= 267 \\ 155^2 - 23449 &= 576 = 24^2 \,, \end{aligned}$$

consequentemente, a fatoração de $23449 = (155+24) \cdot (155-24) = 179 \cdot 131$. Verifiquemos que os dois fatores de 23449 são primos. Para isso devemos efetuar a divisão por todos os p primos menores que $\sqrt{179} = 13$, ou seja, devemos dividir 179 por todos os números

primos menores ou iguais a 13 e da mesma forma o número 131 que devemos dividir por todos os números primos menores ou iguais a $\sqrt{131}$. Ao fazer as divisões, percebemos que de fato os números 179 e 131 são números primos. $\Diamond$

3.4 Demonstração do algoritmo de Fermat

Antes de fazermos a demonstração do algoritmo de Fermat, vamos escrever x e y em função de a e b.

Suponhamos n ímpar que pode ser fatorado na forma $n = a \cdot b$ com $a \leq b$. Queremos obter inteiros positivos x e y tais que $n = x^2 - y^2$. Ou seja:

$$n = a \cdot b = (x - y)(x + y) = x^2 - y^2 \ .$$

Como $x - y \leq x + y$, isto sugere que tomemos $a = x - y$ e $b = x + y$. Resolvendo este sistema, obtemos

$$x = \tfrac{b+a}{2} \text{ e } y = \tfrac{b-a}{2} \ .$$

De fato, expandindo os produtos notáveis, verificamos facilmente que

$$x^2 - y^2 = \left(\frac{b+a}{2}\right)^2 - \left(\frac{b-a}{2}\right)^2 = a \cdot b = n \ .$$

Observe que x e y são inteiros positivos, e n é ímpar por hipótese, mas a e b são fatores de n, logo a e b são ímpares. Portanto $b + a$ e $b - a$ são pares e, consequentemente, $\frac{b+a}{2}$ e $\frac{b-a}{2}$ são inteiros.

se n é primo, então só podemos ter $a = 1$ e $b = n$. Com isto, o único valor possível de x para n primo é $\frac{n+1}{2}$

Vamos mostrar agora que se n é composto, o algoritmo pára antes de chegar a $\frac{n+1}{2}$. De fato, se n é um quadrado, temos que $a = b$ e o algoritmo pára. Podemos supor que n é composto e não é um quadrado perfeito, isto é, que $1 < a < b < n$, então devemos mostrar que existe $x > \lfloor \sqrt{n} \rfloor$ tal que $\sqrt{x^2 - n}$ é um inteiro, com $x < \frac{n+1}{2}$. Veremos que neste caso, o algoritmo vai parar se forem satisfeitas as desigualdades

$$\lfloor \sqrt{n} \rfloor \leq \frac{a+b}{2} < \frac{n+1}{2}$$

Veja que a desigualdade da direita nos diz que $a + b < n + 1$, substituindo $n = a \cdot b$, teremos $a + b < a \cdot b + 1$. subtraindo $b + 1$ de ambos os lados,fica $a - 1 < b(a - 1)$, como $a > 1$, podemos dividir a desigualdade por $a - 1$, donde teremos que $1 < b$. Repare que $1 < b$ é equivalente a a desingualde original $1 < a < b < n$. Como $1 < a < b$ vale por hipótese, provamos que $\frac{a+b}{2} < \frac{n+1}{2}$.

Considere agora a desigualdade da esquerda, ou seja, queremos mostrar que $\lfloor\sqrt{n}\rfloor \leq \frac{a+b}{2}$. Observe que $\lfloor\sqrt{n}\rfloor \leq \sqrt{n}$, basta verificar que $\sqrt{n} \leq \frac{a+b}{2}$. Esta desigualdade é verdadeira se, e somente se, $n \leq \left(\frac{b+a}{2}\right)^2$ é verdadeira, mas por $x^2 - n = y^2$,

$$\left(\frac{b+a}{2}\right)^2 - n = \left(\frac{b-a}{2}\right)^2 .$$

Que é sempre um número positivo e, portanto $\left(\frac{b+a}{2}\right)^2 - n \geq 0$, o que mostra que $\sqrt{n} \leq \frac{a+b}{2}$.

Por fim, sabemos que a variável x é inicializada com o valor $\lfloor\sqrt{n}\rfloor$ e, que vai sendo incrementada de uma unidade a cada laço. Assim $\lfloor\sqrt{n}\rfloor \leq \frac{a+b}{2} < \frac{n+1}{2}$ nos garante que se, n for composto, chegaremos a $\frac{a+b}{2}$ antes de chegar a $\frac{n+1}{2}$ tendo determinado os fatores de n.

Capítulo 4

O PEQUENO TEOREMA DE FERMAT

Vamos iniciar este capítulo com uma indispensável abordagem acerca de congruência, que foi desenvolvida por Gauss e hoje é uma poderosa ferramenta na divisibilidade.

4.1 Congruências

Definição 10. *Seja $m > 1$ um número natural. Diremos que dois números inteiros a e b são congruentes módulo m, e escreve-se $a \equiv b\,(mod\, m)$ quando $m|a-b$, ou seja, existe $q \in \mathbb{Z}$ tal que $a - b = mq$. Caso $m \nmid a - b$, dizemos que a e b são incongruentes módulo m, escrevemos $a \not\equiv b\,(mod\, m)$.*

Exemplo 13. Observe que $31 \equiv 7\,(mod\, 3)$, pois $3|(31-7) = 24$. Mas, $25 \not\equiv 12\,(mod\, 3)$, pois $3 \nmid (25-12) = 13$ $\Diamond$

A proposição abaixo decorre, imediatamente da definição de congruência.

Proposição 4.1. *Seja $m \in \mathbb{N}$. Para todo a, b, $c \in \mathbb{Z}$, tem-se que*

i) $a \equiv a\,(mod\, m)$;

ii) se $a \equiv b\,(mod\, m)$, então $b \equiv a\,(mod\, m)$;

iii) se $a \equiv b\,(mod\, m)$ e $b \equiv c\,(mod\, m)$, então $a \equiv c\,(mod\, m)$.

Demonstração. (i) se $a \equiv a\,(mod\, m)$, então $m|(a-a)$, mas pela proposiçao 2.2, $m|0$.
(ii) se $a \equiv b\,(mod\, m)$, então existe $k \in \mathbb{Z}$ tal que $a - b = km$, isto implica que $b - a =$

$(-k)m$, o que equivale a $b \equiv a\,(mod\,m)$.
(iii) se $a \equiv b\,(mod\,m)$ e $b \equiv c\,(mod\,m)$, então $m|(a-b)$ e $m|(b-c)$. Pela proposição 2.2, $m|(a-b)+(b-c) = a-c$, o que mostra que $a \equiv c\,(mod\,m)$. □

Perceba que a congruência módulo m é uma relação de equivalência. E, mais que isso, podemos dizer que se a e b são congruentes módulo m, então o resto da divisão de a e de b por m são iguais.Por outro lado, dados a e m, $m > 0$ do algoritmo euclidiano existem q e r tais que $a = mq + r$, com $0 \leq r < m$, donde podemos escrever $a - r = mq$, logo é cômodo usar a notação $a \equiv r\,(mod\,m)$, onde r é o resto da divisão de a por m.

Exemplo 14. Como o resto da divisão de 25 por 7 é 4, podemos escrever $25 \equiv 4\,(mod\,7)$. De fato $7|25-4$. ◊

Definição 11. *Sistema completo de resíduos módulo m é todo conjunto de números inteiros cujos restos pela divisão por m são os números $0, 1, 2, 3, 4..., m-1$, sem repetições e numa ordem qualquer.*

Portanto, um sistema completo de resíduos módulo m possui m elementos. Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m.

Exemplo 15. O conjunto $A = \{0, 1, 2, 3, 4, 5, 6\}$ é um sistema completo de resíduo módulo 7, pois representa todos os possíveis restos da divisão de um inteiro n qualquer por 7. ◊

Exemplo 16. $\{0, 1, 2, ..., m-1\}$ é um sistema completo de resíduo módulo m. ◊

Definição 12 (Função Fi de Euler)**.** *Dado o conjunto $\{0, 1, 2, ..., m-1\}$, um sistema de resíduo módulo m, à quantidade de números naturais desse conjunto que são primos com m é definido como a função "fi"de Euler, e representado por $\phi(m)$.*

Em particular, se m é primo, então $\phi(m) = m - 1$.

Exemplo 17. Observe que $\{0, 1, 2, ..., 9\}$ é sistema de resíduo módulo 10, e os números $1, 3, 7$ e 9 são primos com 10, logo $\phi(10) = 4$. ◊

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 4.2. *Seja $a, b, c, d, m, \in \mathbb{Z}$, com $m > 1$, tem-se*

i) se $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, então $a + c \equiv b + d\,(mod\,m)$;

ii) se $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, então $ac \equiv bd\,(mod\,m)$.

Demonstração. Suponhamos que $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$. Logo, temos que $m|b-a$ e $m|d-c$.
(i) Basta observar que $m|(b-a)+(d-c)$ e, portanto, $m|(b+d)-(a+c)$, o que mostra $a + c \equiv b + d\,(mod\,m)$.
(ii)Note que $bd - ac = d(b-a) + a(d-c)$, logo concluímos que $m|bd - ac$. □

Corolário 4.3. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b\,(mod\,m)$, então tem-se que $a^n \equiv b^n\,(mod\,m)$*

Demonstração. A prova será feita por indução. Para $n = 1$, tem se que $a^1 \equiv b^1\,(mod\,m)$, o que é verdade. Suporemos que $a^n \equiv b^n\,(mod\,m)$, ou seja, que $m|a^n - b^n$, queremos mostrar que o mesmo é válido para $n + 1$. De fato, observe que

$$a^{n+1} - b^{n+1} = aa^n - bb^n = aa^n - ba^n + ba^n - bb^n = a^n(a-b) + b(a^n - b^n)$$

Como $m|a - b$ e por hipótese $m|a^n - b^n$, segue que $m|a^{n+1} - b^{n+1}$, e portanto $a^n \equiv b^n\,(mod\,m)$ para todo $n \in \mathbb{N}$. □

Proposição 4.4. *Se $(c, n) = 1$, então $ac \equiv bc\,(mod\,n) \iff a \equiv b\,(mod\,n)$.*

Demonstração. Temos que $n|ac - bc \iff n|(a-b)c$ como $\text{mdc}(c, n) = 1$, pela proposição (2.3) $n|a - b$. O que mostra que $a \equiv b\,(mod\,n)$.

□

Exemplo 18. Vamos determinar o resto da divisão de 3^{45} por 10. Note inicialmente que

$$3^2 \equiv -1(mod\,10)$$

pelo corolário 4.3, temos que

$$(3^2)^{22} \equiv (-1)^{22}(mod\,10)$$

$$3^{44} \equiv 1(mod\,10),$$

Por outro lado, como $3 \equiv 3(mod\,10)$ segue da proposição 4.2(ii) que

$$3^{44} \cdot 3 \equiv 1 \cdot 3(mod\,10)$$

$$3^{45} \equiv 3(mod\,10).$$

E, portanto o resto da divisão de 3^{45} por 10 é 3. $\Diamond$

Exemplo 19. Utilizando as propriedades de congruências, vamos mostrar que 641 divide o sexto número de Fermat, ou seja, F_5.
De fato,

$$2^{16} = (256)^2 = 65536 \equiv 154\,(\mathrm{mod}\,641).$$

Logo,

$$2^{32} \equiv (154)^2 \equiv 23716 \equiv 640 \equiv -1\,(\mathrm{mod}\,641).$$

Daí, temos que

$$2^{2^5} + 1 \equiv 0\,(\mathrm{mod}\,641),$$

o que implica que $641|F_5$. $\Diamond$

Exemplo 20. Mostremos que o número de Mersenne $M_{83} = 2^{83} - 1$ não é primo, apesar de 83 ser primo. De fato, temos que

$$\begin{aligned} 2^8 &= 256 \equiv 89\,(\mathrm{mod}\,167) \\ 2^{16} &\equiv 89^2 = 7921 \equiv 72\,(\mathrm{mod}\,167) \\ 2^{32} &\equiv 72^2 = 5184 \equiv 7\,(\mathrm{mod}\,167) \\ 2^{64} &\equiv 7^2 = 49\,(\mathrm{mod}\,167)\ . \end{aligned}$$

Daí, segue que $2^{83} = 2^{64}2^{16}2^3 \equiv 49 \cdot 72 \cdot 8 \equiv 1\,(\mathrm{mod}\,167)$, o que implica que $2^{83} - 1$ é divisível por 167. $\Diamond$

Proposição 4.5. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, tem-se que $a^{2n} \equiv b^{2n}\,(mod\,(a+b))$.*

Demonstração. Novamente usaremos indução sobre n.
A afirmação é verdadeira para $n = 1$, pois claramente $a+b$ divide $a^2 - b^2 = (a+b)(a-b)$.
Supomos, agora, que $a + b|a^{2n} - b^{2n}$. Observe agora que

$$a^{2(n+1)} - b^{2(n+1)} = a^2a^{2n} - b^2b^{2n} + b^2a^{2n} - b^2a^{2n} = (a^2 - b^2)a^{2n} + b^2(a^{2n} - b^{2n}).$$

Como $a+b|a^2-b^2$ e, por hipótese, $a+b|a^{2n}-b^{2n}$, decorre das igualdades acima e da proposição 2.1(iii) que $a+b|a^{2(n+1)}-b^{2(n+1)}$, ou seja, $a^{2(n+1)} \equiv b^{2(n+1)}(mod\,(a+b))$ para todo $n \in \mathbb{N}$. □

Exemplo 21. Mostraremos que a congruência $9^{2n} \equiv 2^{4n}\,(mod\,13)$ é verdadeira para todo $n \in \mathbb{N}$.
Inicialmente observe que 13=9+4 e $2^{4n} = 4^{2n}$, e pela proposição anterior,
$9^{2n} \equiv 4^{2n}\,(mod\,(9+4))$. ◊

Proposição 4.6. *Seja $n \in \mathbb{N}$ um número ímpar, então $(n-1)^{(n-1)} \equiv 1(mod\,n)$.*

Demonstração. Como n é ímpar, então $n-1$ é par e por sua vez $n-1=2k$, para algum $k \in \mathbb{N}$. Portanto

$$(n-1)^{(n-1)} \equiv 1(mod\,n)$$
$$(2k)^{2k} \equiv 1(mod\,(2k+1))$$

E,portanto pela proposição (4.4) a congruência acima é sempre verdadeira. □

Com a notação de congruência, o Pequeno Teorema de Fermat enuncia-se como se segue.

4.2 O Pequeno Teorema de Fermat

Teorema 4.7 (O Pequeno Teorema de Fermat)**.** *Se p é um número primo e $p \nmid a$, então $a^{p-1} \equiv 1\,(mod\,p)$.*

Demonstração. Como $p \nmid a$ e, p é primo, então $(a,p)=1$. Considere agora a sequência $(a,\ 2a,\ 3a,\ ...,(p-1)a)$. Analisemos alguns fatos sobre esta sequência.

Fato 1: *Esta é uma sequência de $p-1$ múltiplos de a na qual não há múltiplo de p.*

De fato, seja $k \in \{1;\ 2;\ 3;\ ,...,p-1\}$. Suponha que exista k tal que ka seja um múltiplo de p, logo $p|ka$.

Observe que $k \in \{1;\ 2;\ 3;\ ,...,p-1\}$ e p é maior que todo os elementos do conjunto, isto implica que $p \nmid k$ e conclui-se que $p|a$, um absurdo, pois $(a,p)=1$.

Fato 2: *Nesta sequência, não há dois números congruentes módulo p.*

Com efeito, seja $k_1 \neq k_2$ com k_1 e $k_2 \in \{1;\, 2;\, 3;, ..., p-1\}$ Suponha por absurdo que existem dois números congruentes módulo p, então $ak_1 \equiv ak_2 \,(\mathrm{mod}\, p)$, mas $(a, p) = 1$ e portanto $k_1 \equiv k_2 \,(mod\ p)$ implica $k_1 = k_2$ o que é uma contradição. Assim fica mostrado o fato 2.

Cada um dos números da sequência $(a,\, 2a,\, 3a, ..., (p-1)a)$ é congruente a $(1,\, 2,\, 3, ..., p-1)$, pois são sistemas completo de restos módulo p. Multiplicando estas duas sequências, teremos

$$\begin{aligned} a \cdot 2a \cdot 3a \cdots (p-1)a &\equiv 1 \cdot 2 \cdots (p-1) \,(\mathrm{mod}\, p) \\ a^{p-1}(p-1)! &\equiv (p-1)! \,(\mathrm{mod}\, p)\ , \end{aligned}$$

como $(p, (p-1)!) = 1$, podemos cancelar $(p-1)!$ nos dois membros, donde finalmente temos

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)\ ,$$

como queríamos demonstrar. . □

Corolário 4.8. *Considere p um primo e a um inteiro qualquer. Então :*

$$a^p \equiv a \,(mod p)\ .$$

Demonstração. Se $p|a$, então é claro que $a^p \equiv a \,(\mathrm{mod}\, p)$. Suponhamos que $p \nmid a$. Do Pequeno Teorema de Fermat temos, $a^{p-1} \equiv 1 \,(\mathrm{mod}\, p)$, então $a \cdot a^{p-1} \equiv a \cdot 1 \,(\mathrm{mod}\, p)$, e portanto, $a^p \equiv a \,(\mathrm{mod}\, p)$. □

Exemplo 22. Para ilustrar o Corolário 4.8, calculemos o resto da divisão por 7 do número $1^7 + 2^7 + 3^7 + \cdots + 100^7$. Pelo Corolário do Pequeno Teorema de Fermat, $a^7 \equiv a \,(mod\, 7)$ para todo $a \in \mathbb{Z}$, logo

$$1^7 + 2^7 + \cdots + 100^7 \equiv 1 + 2 + \cdots + 100 \equiv \frac{100 \cdot 101}{2} \equiv 3 \,(\mathrm{mod}\, 7)\ .$$

Portanto o resto procurado é 3. ◊

Exemplo 23. Ilustremos o Teorema 4.7 calculando o resto da divisão por 17 do número

$$S = 1^{16} + 2^{16} + 3^{16} + \cdots + 85^{16}\ .$$

Pelo Pequeno Teorema de Fermat,

$$a^{16} \equiv \begin{cases} 1, & \text{se} \quad 17 \text{ não divide } a \\ 0, & \text{se} \quad 17 \text{ divide } a \end{cases} \,(\mathrm{mod}\, 17)\ .$$

Como $85 = 17 \cdot 5$, então de 1 a 85 há 5 múltiplos de 17 e $85 - 5 = 80$ não múltiplos de 17 (i.e, primos com 17), logo $S \equiv 80 \cdot 1 \equiv 12\,(mod\,17)$. Portanto, o resto da divisão de S por 17 é 12. ◊

Veremos agora algumas consequências do Pequeno Teorema de Fermat.

4.3 Raízes Primitivas

Dado $a \in \mathbb{Z}$, o Pequeno Teorema de Fermat afirma que se p é primo, então $p|a^{p-1} - 1$, porém pode acontecer de existir um menor valor inteiro k para o qual $p|a^k - 1$. Isso pode facilitar a verificação de uma determinada propriedade como veremos no próximo capítulo.

Definição 13. *O menor inteiro positivo k para o qual $a^k \equiv 1(mod\,m)$, onde $(a, m) = 1$, é chamado de "ordem de a módulo m", e será denotado por $ord_m a$.*

Assim, $2^3 \equiv 1(\mathrm{mod}\,7) \Rightarrow ord_7 2 = 3$, pois 3 é o menor expoente para o qual a congruência é válida. ◊

Definição 14. *Se $ord_m a = \phi(m)$, dizemos que a é uma raiz primitiva módulo m.*

Exemplo 24. *Para calcular $ord_{10}3$ computamos módulo 10 as potências 3, 3^2,3^3, etc.*

$$\begin{aligned} 3 &\equiv 3(mod\,10)\,, \\ 3^2 &\equiv 9(mod\,10)\,, \\ 3^3 &\equiv 7(mod\,10)\,, \\ 3^4 &\equiv 1(mod\,10)\,. \end{aligned}$$

Assim $ord_{10}3 = 4$ e como $\phi(10) = 4$, Segue que 3 é uma raiz primitiva módulo 10. ◊

4.4 Resíduos Quadráticos

Nesta seção, estamos interessados em saber, caso exista, solução para a congruência

$$x^2 \equiv a\,(\mathrm{mod}\,p)$$

Teorema 4.9. *Para p um primo ímpar e a um inteiro não divisível por p, a congruência*

$$x^2 \equiv a\,(mod\,p)$$

caso tenha solução, tem exatamente duas soluções incongruentes módulo p.

Demonstração. Caso esta congruência tenha solução x_1, claramente $-x_1$ também será solução, uma vez que $(-x_1)^2 = x_1^2 \equiv a\,(mod\,p)$. Devemos mostrar que estas soluções x_1 e $-x_1$ são incongruentes módulo p. Se $x_1 \equiv -x_1\,(mod\,p)$, então teríamos $2x_1 \equiv 0\,(mod\,p)$ e, como p é ímpar e $p \nmid x_1$ (pois $p|(x_1^2 - a)$ e $p \nmid a$), isto é impossível. Precisamos mostrar que só existem duas soluções incongruentes. Seja y uma solução de $x^2 \equiv a\,(mod\,p)$ i,e., $y^2 \equiv a\,(mod\,p)$. Como x_1 é solução temos $x_1^2 \equiv y^2 \equiv a\,(mod\,p)$ e, portanto, $x_1^2 - y^2 = (x_1+y)(x_1-y) \equiv 0\,(mod\,p)$. Logo, $p|(x_1+y)$ ou $p|(x_1-y)$, o que implica $y \equiv -x_1\,(mod\,p)$ ou $y \equiv x_1\,(mod\,p)$. Com isto mostramos que, caso exista uma solução, existem exatamente duas soluções incongruentes.

□

Definição 15. *Sejam a e m inteiros com $(a, m) = 1$. Dizemos que a é um resíduo quadrático módulo m se a congruência $x^2 \equiv a\,(mod\,p)$ tiver solução. Caso $x^2 \equiv a\,(mod\,p)$ não tenha solução, dizemos que a não é resíduo quadrático módulo m.*

Por exemplo, como $3^2 \equiv 1\,(\mathrm{mod}\,8)$, então 1 é resíduo quadrático módulo 8.

Exemplo 25. Ilustremos o Teorema 4.4, considerando o múmero primo 13, calculemos então todos os números que são resíduos quadráticos módulo 13.

Para isto é suficiente considerarmos os quadrados dos números $1, 2, 3, \ldots, 12$. Observe que estes números formam um sistema reduzido de resíduos módulo 13. Temos

$$\begin{aligned}
1^2 &\equiv 1\,(\mathrm{mod}\,13)\,,\\
2^2 &\equiv 4\,(\mathrm{mod}\,13)\,,\\
3^2 &\equiv 9\,(\mathrm{mod}\,13)\,,\\
4^2 &\equiv 3\,(\mathrm{mod}\,13)\,,\\
5^2 &\equiv 1\,(\mathrm{mod}\,13)\,,\\
6^2 &\equiv 10\,(\mathrm{mod}\,13)\,,\\
7^2 &\equiv 10\,(\mathrm{mod}\,13)\,,\\
8^2 &\equiv 12\,(\mathrm{mod}\,13)\,,\\
9^2 &\equiv 3\,(\mathrm{mod}\,13)\,,\\
10^2 &\equiv 9\,(\mathrm{mod}\,13)\,,\\
11^2 &\equiv 4\,(\mathrm{mod}\,13)\,,\\
12^2 &\equiv 1\,(\mathrm{mod}\,13)\,.
\end{aligned}$$

Na coluna da esquerda temos os quadrados dos números de 1 até 12 e na coluna da direita apenas os números 1,3,4,9,10 e 12. Estes são todos os resíduos quadráticos módulo 13. ◊

A definição abaixo é extremamente conveniente para lidarmos com resíduos quadráticos.

Definição 16. *Para p um primo ímpar e a um inteiro não-divisível por p, definimos Símbolo de Legendre $\left(\frac{a}{p}\right)$ por*

$$\left(\frac{a}{p}\right) \equiv \begin{cases} 1, & \textit{se } a \textit{ é um resíduo quadrático de } p\,. \\ -1, & \textit{se } a \textit{ não é um resíduo quadrático de } p\,. \end{cases}$$

Exemplo 26. Como as congruências $x^2 \equiv 1 \pmod 7, x^2 \equiv 2 \pmod 7$ e $x^2 \equiv 4 \pmod 7$ possuem soluções, temos que

$$\left(\frac{1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{4}{p}\right) = 1\,,$$

por outro lado,

$$\left(\frac{3}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{6}{p}\right) = -1\,.$$

Uma vez que as congruências $x^2 \equiv 3 \pmod 7, x^2 \equiv 5 \pmod 7$ e $x^2 \equiv 6 \pmod 7$ não possuem soluções. ◊

Teorema 4.10 (Critério de Euler)**.** *Se p for um primo ímpar e a um inteiro não-divisível por p, então*

$$\left(\frac{a}{p}\right) \equiv a^{(\frac{p-1}{2})}\,(mod p)\,.$$

O leitor interessado na demonstração pode consultar [10].

Capítulo 5

PSEUDOPRIMOS

Para motivar este capítulo, suponha um número $a \in \mathbb{N}$, tal que $1 < a < 7$ e $n = 7$ primo. Logo, pelo Pequeno Teorema de Fermat sabemos que $a^{p-1} \equiv 1(\text{mod}p)$, daí temos que:

$$\begin{aligned} 2^{7-1} &= 2^6 = 64 \equiv 1(\text{mod}\,7) \\ 3^{7-1} &= 3^6 = 729 \equiv 1(\text{mod}\,7) \\ 4^{7-1} &= 4^6 = 4.096 \equiv 1(\text{mod}\,7) \\ 5^{7-1} &= 5^6 = 15.625 \equiv 1(\text{mod}\,7) \\ 6^{7-1} &= 6^6 = 46.656 \equiv 1(\text{mod}\,7)\ . \end{aligned}$$

Será que a recíproca do Pequeno Teorema de Fermat é verdadeira? Ou seja, dado um inteiro n , a condição $a^{n-1} \equiv 1(\text{mod}\,n)$ para todo $a \in \mathbb{N}$ tal que $(a, n) = 1$, acarreta,necessariamente, que n é primo? Leibniz, matemático alemão, acreditava que sim e até usava como um eficiente teste de primalidade. Porém, em 1819, Sarrus mostrou que $2^{340} \equiv 1(\text{mod}\,341)$. Para Leibniz 341 seria um número primo. Infelizmente para a surpresa de Leibniz, e claro para nossa, a recíproca do Pequeno Teorema de Fermat não é verdadeira, pois $341 = 11 \cdot 31$ é composto. Estes "falsos primos"são conhecidos como pseudoprimos.

Note portanto que o Pequeno Teorema de Fermat fornece-nos um teste de não primalidade. Com efeito, dado $n \in \mathbb{N}$ com $n > 1$, se existir algum $a \in \mathbb{N}$, com $(a, n) = 1$ tal que

$$a^{n-1} \not\equiv 1(\text{mod}n)\ ,$$

então n não é primo. Isto nos dá uma maneira indireta de verificar se um número é composto sem precisar determinar seus fatores. Na prática só precisamos considerar os

inteiros a no intervalo $1 < a < n-1$. Uma vez que a congruência $a^{n-1} \equiv 1(mod\, n)$ é sempre verificada quando $a = 0, 1, n-1$.

Exemplo 27. Observe que, se 314 fosse de fato primo, pelo Pequeno Teorema de Fermat, ele teria que ser verificado para todo $a \in \mathbb{N}$ tal que $1 < a < 340$, mas $3^{340} \equiv 56(mod 341)$. Quando isso, acontece, dizemos que 3 é testemunha de 341 é composto. $\Diamond$

5.1 Pseudoprimos na base a

Os antigos chineses acreditavam que, se um número natural n satisfaz a congruência

$$2^n \equiv 2(\mathrm{mod}\, n)\ ,$$

então n é necessariamente primo. De fato, esse resultado é válido para $n \leq 340$, mas, como vimos acima, falha para $n = 341$.

Definição 17. *Seja n um inteiro positivo ímpar e composto. Se existir um inteiro a tal que $1 < a < n-1$ e $a^{n-1} \equiv 1\,(mod\, n)$, dizemos que n é um pseudoprimo na base a.*

Observação: Historicamente, a definição de pseudoprimo era somente um número natural n que satisfaz a congruência $2^n \equiv 2(\mathrm{mod}\, n)$, com o avanço dos estudos sobre pseudoprimos é que surgiram outros tipos de pseudoprimos. Doravante, sempre nos referiremos a pseudoprimo na base 2 apenas como pseudoprimo.

Exemplo 28. Mostraremos que 91 é um pseudoprimo na base 3. Como 91 é pseudoprimo, ele é composto. de fato, $91 = 7 \cdot 13$. Observe que a $ord_{13}3 = 3$, isto é,

$$3^3 \equiv 1(mod\, 13)$$
$$(3^3)^{30} \equiv 1^{30}(mod\, 13)$$
$$3^{90} \equiv 1(mod\, 13)$$

Por outro lado, temos que 7 é primo e $(3, 7) = 1$, pelo Pequeno Teorema de Fermat,

$$3^6 \equiv 1(mod\, 7)$$
$$(3^6)^{15} \equiv 1^{15}(mod\, 7)$$
$$3^{90} \equiv 1(mod\, 7)$$

Portanto como $(7, 13) = 1$, pela proposição 2.5, isto implica que $3^{90} \equiv 1(mod\, 91)$ $\Diamond$

A tabela abaixo indica alguns pseudoprimos com suas respectivas bases.

Bases	menores pseudoprimos
2	$341 = 11 \cdot 31$
3	$91 = 7 \cdot 13$
5	$217 = 7 \cdot 31$
7	$25 = 5 \cdot 5$
2,3	$1105 = 5 \cdot 13 \cdot 17$
2,5	$561 = 3 \cdot 11 \cdot 17$
2,7	$561 = 3 \cdot 11 \cdot 17$
3,5	$1541 = 23 \cdot 67$
3,7	$703 = 19 \cdot 37$
5,7	$561 = 3 \cdot 11 \cdot 17$
2,3,5	$1729 = 7 \cdot 13 \cdot 19$
2,3,7	$1105 = 5 \cdot 13 \cdot 17$
2,5,7	$561 = 3 \cdot 11 \cdot 17$
3,5,7	$29341 = 13 \cdot 37 \cdot 61$
2,3,5,7	$29341 = 13 \cdot 37 \cdot 61$

Tabela 5.1: Menores números pseudoprimos para várias bases

Teorema 5.1. *Se n é pseudoprimo e $n' = 2^n - 1$, então n' é também pseudoprimo.*

Demonstração. Mostraremos inicialmente que n' é composto. De fato, se $n = a \cdot b$, com $1 < a, b < n$ então:

$$n' = 2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)((2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1) \, .$$

Agora, sendo n pseudoprimo, temos que $n|2^n - 2$, i. e., $2^n - 2 = rn$, para algum $r \in \mathbb{N}$. Temos então

$$\begin{aligned} 2^{n'-1} - 1 &= 2^{rn} - 1 = (2^n - 1)((2^n)^{r-1} + (2^n)^{r-2} + \cdots + 2^n + 1) \\ &= n'((2^n)^{r-1} + (2^n)^{r-2} + \cdots + 2^n + 1) \, , \end{aligned}$$

logo, $n' = 2^n - 1$ divide $2^{n'-1} - 1$. □

Esse teorema mostra que sempre é possível gerar um novo pseudoprimo, desta forma vemos que existe uma infinidade de números pseudoprimos.

Um outro método para gerar uma infinidade de pseudoprimos é o seguinte: *Sejam* $k \geq 5$ *um número ímpar qualquer,* p *um fator primo de* $2^k - 1$ *e* q *um fator primo de* $2^k + 1$. *Então* pq *é um número pseudoprimo.*

Podemos ver, por exemplo, que tomando $k = 5$, temos $2^5 - 1 = 31$ e sua fatoração é $1 \cdot 31$ com fator p primo igual a 31 e $2^5 + 1 = 33$ e, sua fatoração é $3 \cdot 11$ com fator q primo igual a 11. Multiplicando $11 \cdot 31 = 341$, e como já vimos antes, 341 é um pseudoprimo. Vejamos agora algumas curiosidades a respeito desse assunto:

- Entre 1 e 10^9 existem 5597 pseudoprimos.
- Existem números compostos pares n que satisfazem a congruência $2^n \equiv 2(\mathrm{mod} n)$, são os chamados *pseudoprimos pares* e estão em quantidade infinita. O menor deles é $n = 2 \cdot 73 \cdot 1103 = 161038$.
- Existe uma infinidade de números primos p tais que $2^{p-1} \equiv 1(\mathrm{mod} p^2)$? Sim, existem pseudoprimos que são quadrados, mas não se sabe se são infinitos. Os menores exemplos são 1093^2 e 3511^2.
- Sendo dado $a \geq 2$, existe uma infinidade de números primos p, tais que $a^{p-1} \equiv 1(\mathrm{mod} p^2)$? (problema em aberto!) A tabela abaixo mostra alguns resultados para $p \leq 37$ encontrado por Jacobi.

$3^{10} \equiv 1 \,(\mathrm{mod}\, 11^2)$
$9^{10} \equiv 1 \,(\mathrm{mod}\, 11^2)$
$14^{28} \equiv 1 \,(\mathrm{mod}\, 29^2)$
$18^{36} \equiv 1 \,(\mathrm{mod}\, 37^2)$

Tabela 5.2: Jacobi

5.2 Pseudoprimos de Euler na base a

Até aqui estudamos as congruências ligadas diretamente ao Pequeno Teorema de Fermat. No entanto, existem outras congruências que são satisfeitas por números primos, que

ao considerá-las aparecem outros tipos de números compostos como os pseudoprimos de Euler na base a.

Definição 18. *Um número composto ímpar n, tal que $mdc(a,n)=1$ que satisfaz o critério de Euler abaixo, é chamado de pseudoprimo de Euler na base a.*

$$\left(\frac{a}{n}\right) \equiv a^{\frac{(n-1)}{2}} (mod n).$$

Exemplo 29. Exemplifiquemos mostrando que 25 é um pseudoprimo de Euler na base 7. De fato, como 7 não é resíduo quadrático módulo 25, então $\left(\frac{7}{25}\right) = -1$, logo podemos concluir que

$$-1 = \left(\frac{7}{25}\right) \equiv 7^{\frac{25-1}{2}} = 7^{12} \equiv -1 \,(\mathrm{mod}\, 25)\ .$$

Logo, 25 é um pseudoprimo de Euler na base 7. ◊

Duas considerações são pertinentes a esta seção. A primeira é que seja natural perceber que todo pseudoprimos de Euler na base a é um pseudoprimo de base a, isto nos levar a concluir que os pseudoprimos de Euler estão em quatidade infinita e que entre 1 e 10^9 existem 2939 pseudoprimos de Euler e a segunda consideração é que dado um inteiro composto n, este só poderá ser pseudoprimo de Euler na base a para no máximo $\frac{1}{2} \cdot \phi(n)$ de base $a, 1 < a < n$, com $(a,n) = 1$.

5.3 Pseudoprimos Fortes na base a

A defnição que veremos a seguir, é graças ao teste de primalidade de Miller-Rabin.[1]

Definição 19. *Seja n um número inteiro e composto ímpar, seja ainda $n-1 = 2^s \cdot d$ com d ímpar e $s \geq 1$, seja a tal que $1 < a < n$ e $(a,n) = 1$. Diz-se que n é um pseudoprimo forte na base a quando, ou $a^d \equiv 1(mod n)$, ou então $a^{2^r d} \equiv -1(mod n)$ para algum inteiro r, $1 \leq r < s$.*

É claro que se n é primo ímpar, então satisfaz a definição 19 para todo a tal que $1 < a < n$ e $(a,n) = 1$.

[1] É um teste probabilístico da primalidade de um dado número n. Se um número n não passar pelo teste, n com certeza é um número composto (ou seja, não-primo). Se o número passar no teste, ele é primo, com uma probabilidade $P(n \in \mathbb{P}) \geq 0,75$, sendo que $\mathbb{P}$ denomina o conjunto de todos números primos.

Exemplo 30. Vamos ilustrar mostrando que M_{11} um número de Mersenne composto é um pseudoprimo forte na base 2. Seja $n = M_{11} = 2^{11} - 1 = 2047$, portanto $2047 - 1 = 2046 = 2 \cdot 1023 = 2^s \cdot d$, donde podemos concluir que $d = 1023$ e $s = 1$. Vemos sem dificuldade que $2^{11} \equiv 1 \,(\mathrm{mod}\, 2047) \Longrightarrow (2^{11})^{93} \equiv 1^{93} (\mathrm{mod}\, 2047) \Longrightarrow 2^{1023} \equiv 1 \,(\mathrm{mod}\, 2047)$. $\Diamond$

Este exemplo nos motiva as proposições seguintes.

Proposição 5.2. *Seja n um inteiro composto ímpar. Se n for um pseudoprimo, então $2^n - 1$ é um pseudoprimo forte na base 2.*

Demonstração. Queremos mostrar que, escrevendo $(2^n - 1) - 1 = 2^s \cdot d$, teremos, ou $2^d \equiv 1(\mathrm{mod}(2^n - 1))$, ou $2^{2^r \cdot d} \equiv -1(\mathrm{mod}(2^n - 1))$, para algum $1 \leq r < s$.

Observe que $(2^n - 1) - 1 = 2^n - 2 = 2(2^{n-1} - 1)$. Assim, devemos ter

$$2^{2^{n-1}-1} \equiv 1(\mathrm{mod}(2^n - 1)) \quad \text{ou} \quad 2^{2(2^{n-1}-1)} \equiv -1(\mathrm{mod}(2^n - 1)) \,.$$

Agora, como n é um pseudoprimo ímpar, temos que $2^{n-1} \equiv 1(\mathrm{mod} n)$. Logo, $2^{n-1} - 1 = nt$, para algum t inteiro. Temos então,

$$2^{2^{n-1}-1} - 1 = 2^{nt} - 1 = (2^n - 1)((2^n)^{t-1} + (2^n)^{t-2} + \cdots + 2^n + 1) \,,$$

portanto, $2^n - 1$ é um pseudoprimo forte na base 2. $\square$

Assim, devido a existência de uma infinidade de pseudoprimo na base 2, existem outros tantos pseudoprimos fortes na base 2. De fato, entre 1 e 10^9, existem 1282 pseudoprimos fortes.

Proposição 5.3. *Se o número de Mersenne $M_p = 2^p - 1$ é composto, em que p é primo, então M_p é um pseudoprimo.*

Demonstração. Como M_p é composto, temos que $p > 2$. Assim, pelo corolário do Pequeno Teorema de Fermat segue que $2^p \equiv 2(\mathrm{mod} p)$. Logo, $2^p - 2 = pr$, para algum r inteiro. Observe que

$$2^{M_p-1} - 1 = 2^{2^p-2} - 1 = 2^{pr} - 1 = (2^p)^r - 1 = (2^p - 1)((2^p)^{r-1} + (2^p)^{r-2} + \cdots + 2^p + 1) \,,$$

portanto, M_p é um pseudoprimo, pois $M_p | 2^{M_p-1} - 1$. $\square$

Proposição 5.4. *Todo número de Fermat ou é primo ou é pseudoprimo.*

Demonstração. Um número de Fermat é da forma $F_n = 2^{2^n} + 1$, onde $n \geq 0$. Se F_n é primo, então $(F_n, 2) = 1$. Logo, pelo Pequeno Teorema de Fermat, tem-se

$$2^{F_n - 1} \equiv 1 (\mathrm{mod} F_n).$$

Suponhamos F_n composto. Temos que $n+1 \leq 2^n$ para $n \geq 1$, logo $2^{n+1} | 2^{2^n}$. Observe que

$$2^{F_n - 1} - 1 = 2^{2^{2^n}} - 1 = 2^{2^{n+1} \cdot k} - 1 = (2^{2^{n+1}} - 1)((2^{2^{n+1}})^{k-1} + (2^{2^{n+1}})^{k-2} + \cdots + 2^{2^{n+1}} + 1).$$

Logo, $2^{2^{n+1}} - 1$ divide $2^{F_n - 1} - 1$. Mas, F_n divide $2^{2^{n+1}} - 1$. Concluímos que F_n composto, também satisfaz ao Pequeno Teorema de Fermat, e portanto F_n é um pseudoprimo . □

5.4 Os números de Carmichael

Definição 20. *Os números de Carmichael ou pseudoprimos absolutos são os números compostos n tais que*

$$a^{n-1} \equiv 1 \, (mod n) \, ,$$

para todo $a, 1 < a < n - 1$, onde a é primo com n.

Exemplo 31. Verifiquemos por exemplo que 561 é um número de Carmichael. Seja $a \in \mathbb{N}$ tal que $(a, 3) = (a, 11) = (a, 17) = 1$. Note que essa condição é equivalente a $(a, 561) = 1$, pois $3 \cdot 11 \cdot 17 = 561$. Por outro lado

$$(a^{280}, 3) = (a^{56}, 11) = (a^{35}, 17) = 1$$

e, portanto, pelo Pequeno Teorema de Fermat, 3 divide $(a^{280})^2 - 1 = a^{560} - 1$, 11 divide $(a^{56})^{10-}1 = a^{560} - 1$ e 17 divide $(a^{35})^{16} - 1 = a^{560} - 1$. Segue daí que 561 divide $a^{561} - 1$, para todo a tal que $(a, 561) = 1$, sem que 561 seja primo. ◊

vale ressaltar que o números de Carmichael estão em quantidade infinita. De fato, entre 1 e 10^9 existem 646 pseudoprimos absolutos. Determinado pelo Carmichael, a tabela abaixo ilustra os menores pseudoprimo absolutos.

$561 = 3 \cdot 11 \cdot 17$	$15841 = 7 \cdot 31 \cdot 73$	$101101 = 7 \cdot 11 \cdot 13 \cdot 101$
$1105 = 5 \cdot 13 \cdot 17$	$29341 = 13 \cdot 37 \cdot 61$	$115921 = 13 \cdot 37 \cdot 241$
$1729 = 7 \cdot 13 \cdot 19$	$41041 = 7 \cdot 11 \cdot 13 \cdot 41$	$126217 = 7 \cdot 13 \cdot 19 \cdot 73$
$2465 = 5 \cdot 17 \cdot 29$	$46657 = 13 \cdot 37 \cdot 97$	$162401 = 17 \cdot 41 \cdot 233$
$2821 = 7 \cdot 13 \cdot 31$	$52633 = 7 \cdot 73 \cdot 103$	$172081 = 7 \cdot 13 \cdot 31 \cdot 61$
$6601 = 7 \cdot 23 \cdot 41$	$62745 = 3 \cdot 5 \cdot 47 \cdot 89$	$188461 = 7 \cdot 13 \cdot 19 \cdot 109$
$8911 = 7 \cdot 19 \cdot 67$	$63973 = 7 \cdot 13 \cdot 19 \cdot 37$	$252601 = 41 \cdot 61 \cdot 101$
$10585 = 5 \cdot 29 \cdot 73$	$75361 = 11 \cdot 13 \cdot 17 \cdot 31$	

Tabela 5.3: Menores números de Carmichael

CONCLUSÃO

Este trabalho possibilita mostrar aos professores e alunos de olimpíadas de matemática a existência de "falsos primos", mostrando assim que os números de Fermat e Mersenne compostos são pseudoprimos. Por não ser nosso objeto de estudo, não comentamos nada sobre Criptografia, mas este os números primos têm uma forte aplicação no sistema de Criptografia RSA, pois a segurança desse sistema depende da escolha de um número n que é produto de dois números primos eventualmentes grandes. Para a escolha desses primos, o Pequeno Teorema de Fermat se mostra como um teste de não primalidade, no entanto ele pode ser inconclusivo mesmo quando todas as condições do P.T.F são sastisfeitas para que o número n dado seja primo, pois podemos estar diante de um pseudoprimo absoluto, que são os números de Carmichael. Por outro lado, o método de fatoração de Fermat, se apresenta como um teste de primalidade uma vez que n primo tem por fatoração $n \cdot 1$. O método de fatoração de Fermat exerce forte influência na escolha dos primos que serão utilizados na Criptogria, pois caso os números escolhido sejam grande, mas próximos um do outro, o método de Fermat irá detectar facilmente.

Referências Bibliográficas

[1] Alencar, E. F., *Teoria Elementar dos Números*, São Paulo, Nobel, 1981.

[2] Burton, D. M., *Teoria Elementar dos Números*, LTC, 7ª. ed., Rio de Janeiro, 2016.

[3] Clement, P.A., *Congruences for sets of premiums*, American Math. Monthly, 59 (1949), 23 - 25.

[4] Coutinho, S.C, *Números Inteiros e Criptografia RSA*, LTC, 2ª. ed., Rio de Janeiro, IMPA, 2014.

[5] Courant, Richard e Robbins, Herbert, *O que é matemática?*.Rio de Janeiro: Ciência Moderna Ltda., 2000.

[6] Filho, Clésio S., *Números Pseudoprimos*. Macapá, 2014, 97p.

[7] Hefez, A., *Aritmética* .1ª. ed. 2ª. reimp. Rio de Janeiro: SBM, 2014. (Coleção PROFMAT)

[8] Moreira, Carlos Gustavo Tamm de Araújo., *Tópicos de Teoria dos Números* . 1ª.ed.Rio de Janeiro: SBM, 2012. (Coleção PROFMAT,02)

[9] Ribenboim, P., *Números primos - Velhos Mistérios e Novos Recordes* .1ª ed.- Rio de Janeiro: IMPA, 2012. 328p.

[10] Santos, J. P. de Oliveira, *Introdução à Teoria dos Números*, Coleção Matemática Universitária, Rio de Janeiro, IMPA, 2006.

[11] Singh, Simon, *O último Teorema de Fermat*, 17ª ed.- Rio de Janeiro: Record, 2010.