Universidade Federal de Minas Gerais

Instituto de Ciências Exatas

Departamento de Matemática

Sávio Ribas

Orientador:

Fabio Enrique Brochero Martinez

Infinitos números de Carmichael

Apoio: CAPES

Belo Horizonte - MG

Abril - 2013

UNIVERSIDADE FEDERAL DE MINAS GERAIS
INSTITUTO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA

SÁVIO RIBAS

INFINITOS NÚMEROS DE CARMICHAEL

Dissertação de mestrado apresentada como parte dos requisitos para obtenção do título de Mestre pelo Departamento de Matemática do Instituto de Ciências Exatas da Universidade Federal de Minas Gerais.

Orientador: Fabio E. Brochero Martinez.

BELO HORIZONTE - MG
ABRIL - 2013

Agradecimentos

- Agradeço primeiramente a Deus.
- Aos meus pais, Antonio e Rovia, pelo oportunidade que me deram de vir estudar em Belo Horizonte, por sempre me incentivar e ensinar o que era melhor para mim.
- Ao meu irmão e à minha cunhada, Sabir e Tiene, pelo incentivo que sempre me deram.
- À minha namorada, Karine, pela força, companheirismo e compreensão.
- À minha tia Lili, por todos os ensinamentos e por me fazer gostar de Matemática.
- Ao meu avô, Vicente, aos meus tios, primos e demais membros familiares.
- Ao meu orientador, Fabio, por todos os ensinamentos, pela paciência e pela enorme boa vontade. Está sendo muito proveitoso trabalhar contigo.
- À toda equipe do PICME pela oportunidade. Em especial, à Sylvie, Mário Jorge e Remy, pela força e pelas dicas.
- Aos demais professores e funcionários do Departamento de Matemática.
- Aos meus amigos de Ouro Preto, Mariana e Belo Horizonte: Flávia, Michele, Marcus, Vitor, Lucas Assis, Saulo, Tulio, Luana, Vladimir, Alice, Daniel, Paim, Remer, Natália, Dani, Jéssica, Vinícius, Luis Felipe, Danilo, Carol, Pedros (Daldegan e Franklin), Lilian, Letícia, Pablo, Luccas, a todos os outros moradores e ex-moradores da minha república, entre outros.

Resumo

O objetivo desse trabalho é mostrar que existem infinitos números de Carmichael. Com isso, os números de Carmichael são de certa forma os piores números para se testar a primalidade utilizando o Pequeno Teorema de Fermat. Assim, o Pequeno Teorema de Fermat pode ser (e é) usado como um bom teste de não primalidade, mas nunca pode ser usado como um teste de primalidade. Nossa principal referência foi o artigo *There are infinitely many Carmichael numbers* ([1], de W. R. Alford, A. Granville e C. Pomerance) e para cumprir nosso objetivo foram estudados diversos tópicos em várias áreas da Matemática, como as estimativas assintóticas de Mertens, teoria de grupos e caráteres, a função de Carmichael, a constante de Davenport, a desigualdade de Brun-Titchmarsh (que nos levou a estudar a teoria de Fourier e o grande crivo), o Teorema dos Números Primos em Progressão Aritmética em hipóteses mais gerais e algumas estimativas acerca dos zeros das L-séries de Dirichlet.

Abstract

The goal of this work is to show that there are infinitely many Carmichael numbers. Hence, the Carmichael numbers are in some way the worst numbers for testing primality using Fermat's Little Theorem. Thus, Fermat's Little Theorem can be (and is) used as a good test of non-primality, but it never can be used as a primality test. Our main reference was the paper *There are infinitely many Carmichael numbers* ([1], W. R. Alford, A. Granville and C. Pomerance) and to fulfill our goal we studied many topics in various areas of Mathematics, such as Mertens' asymptotic estimates, group theory and characters, Carmichael's function, Davenport's constant, Brun-Titchmarsh inequality (which led us to study the Fourier's theory and the large sieve), Prime Number Theorem in Arithmetic Progression in more general hypotheses and some estimates about the zeros of Dirichlet L-series.

Sumário

Introdução

No final do século XX, a necessidade de determinar se um número $n \in \mathbb{N}$ é primo de forma computacionalmente eficiente se tornou um problema prático fundamental. Tal necessidade surgiu a partir da invenção dos sistemas criptográficos assimétricos baseados no fato de que não é conhecido no momento nenhum algoritmo eficiente e genérico para fatorar números que tenham apenas fatores primos grandes.

O sistema criptográfico desse tipo mais conhecido e usado é o RSA, que é um sistema inventado pelos professores Ronald Rivest, Adi Shamir e Leonar Adleman, do MIT. Esse método consiste em uma chave pública (n, a) e uma chave privada (p, q, b), onde $n = pq$ com p e q primos gigantes, a é um inteiro tal que $1 < a < n$ escolhido de forma a ser relativamente primo com $\varphi(n) = (p-1)(q-1)$ (onde φ é a função de Euler) e $b \equiv a^{-1} \pmod{\varphi(n)}$. É claro que se conhecemos algum dos três números da chave privada então os outros dois são facilmente calculáveis computacionalmente, isto é, tal cálculo é de complexidade polinomial com respeito ao tamanho da entrada.

Dada uma mensagem M com $1 < M < n$, a mensagem criptografada será um número C tal que $1 < C < n$ e $C \equiv M^a \pmod{n}$. Para decodificar a mensagem basta observar que existe k_1 tal que:

$$C^b \equiv M^{ab} \equiv M^{k_1\varphi(n)+1} \equiv M \pmod{n},$$

onde a igualdade anterior é verdadeira para quase todo valor de M. De fato, ela pode ser falsa no caso que $mdc(M, n) \neq 1$, mas isso acontece com probabilidade $\frac{1}{p} + \frac{1}{q} - \frac{1}{pq}$. Porém, no caso em que $mdc(M, n) > 1$ ainda podemos decodificar a mensagem. Sobraram os seguintes casos: $mdc(M, n) = p, q$ ou n. O último implica que n divide M, o que é um absurdo pois $1 < M < n$. Os outros dois são completamente análogos entre si, de forma que podemos supor sem perda de generalidade que p divide M e $mdc(M, q) = 1$. Sabemos que $b \equiv a^{-1} \pmod{\varphi(n)}$ e $C \equiv M^a \pmod{n}$ implicam $b \equiv a^{-1} \pmod{q-1}$ e $C \equiv M^a \pmod{q}$, respectivamente. Logo, existe k_2 tal que:

$$C^b \equiv M^{ab} \equiv M^{k_2(q-1)+1} \equiv M \pmod{q},$$

assim o Teorema Chinês dos Restos nos diz que M é o único inteiro tal que:

$$\begin{cases} M \equiv 0 \pmod{p} \\ M \equiv C^b \pmod{q} \\ 1 < M < n \end{cases}.$$

Observemos que o método tradicional para determinar se um número n é primo consiste em dividir n por todos os primos menores ou iguais a $\sqrt{n}$. Este método também nos permite determinar seus fatores primos menores ou iguais a $\sqrt{n}$, mas tal método é computacionalmente ruim. De fato, se n tem k algarismos binários, então o tamanho da entrada é k, isto é, $n = O(2^k)$. Por esse método realizaríamos $O(\sqrt{n}) = O(2^{k/2})$ divisões, ou seja, o algoritmo tem tempo exponencial com respeito ao tamanho da entrada.

Podemos usar vários teoremas de Teoria dos Números para testar a não primalidade de um número inteiro positivo grande. Atualmente, a melhor ideia é a de usar o Pequeno Teorema de Fermat.

Teorema 0.0.1 (Pequeno Teorema de Fermat)**.** *Para todo p primo e $a \in \mathbb{Z}$ temos $a^p \equiv a \pmod{p}$.*

Esse mesmo teorema pode ser reescrito da seguinte forma:

Teorema 0.0.2. *Seja n um inteiro positivo. Se existe a inteiro tal que n não divide $a^n - a$ então n não é primo.*

Esta segunda versão do teorema de Fermat apresenta um método para mostrar que um dado n não é primo. O número a é dito *testemunha* da não primalidade de n.

Exemplo 0.0.1. *O número $n = 2^{2^7} + 1$ não é primo, pois:*

$$3^n \equiv 142534992508324304154873225278078075561697 6 \not\equiv 3 \pmod{n},$$

assim 3 é uma testemunha da não primalidade de n.

Ressaltamos que para calcular a potência anterior módulo n não precisamos multiplicar $a \times a \times \cdots \times a$, n vezes (o que daria $O(n)$ operações). Existe um algoritmo linear com respeito ao tamanho da entrada, isto é, fixando $1 < a < n$, para o cálculo de $a^n \pmod{n}$ podemos fazer no máximo $4 \log_2 n$ operações. No exemplo anterior, a quantidade de operações é menor que 1000. De fato, começando do 1, podemos multiplicar por a, elevar ao quadrado, (possivelmente) tomar o resto da divisão por n, (possivelmente) multiplicar por a e novamente tomar o resto da divisão por n. Dessa forma, o número de operações é no máximo 4 vezes o número de dígitos binários de n.

Definição 0.0.1. *Dizemos que n composto é um pseudoprimo na base $a > 1$ se $a^{n-1} \equiv 1 \pmod{n}$.*

Exemplo 0.0.2. *O menor pseudoprimo na base 2 é $341 = 11 \times 31$. De fato, temos $2^{10} \equiv 1 \pmod{11} \implies 2^{340} \equiv 1 \pmod{11}$ e $2^5 \equiv 1 \pmod{31} \implies 2^{340} \equiv 1 \pmod{31}$. Como $mdc(11, 31) = 1$ segue que $2^{340} \equiv 1 \pmod{341}$.*