2013: Trabalho de Conclusão de Curso do Mestrado Profissional em Matemática - PROFMAT
Universidade Federal de São João del-Rei - UFSJ
Sociedade Brasileira de Matemática - SBM

LIMITAÇÃO DE QUALQUER FATOR PRIMO DE UM NÚMERO PERFEITO ÍMPAR

Jaqueline Vieira Lopes [1]
Jorge Andrés Julca Avila[2]

Resumo: Este trabalho analisa alguns resultados principais da Aritmética, como Teorema Fundamental da Aritmética, congruência, número de Mersenne, números perfeitos. Em particular, estuda os hipotéticos números perfeitos ímpares e suas estimativas a priori, como o caso do Teorema de Euler. Apresenta a demonstração de um teorema que encontra limitantes superiores de qualquer fator primo de um número perfeito ímpar, segundo Acquaah [1].

Palavras-chave: Teoria dos Números. Números primos. Números perfeitos. Número perfeitos ímpares. Limitantes dos fatores primos.

1 Introdução

Desde a antiguidade os números tem sido motivo de pesquisa e estudo, sendo classificados por suas características comuns, por exemplo: os números pares, os primos, os amigáveis, os perfeitos, dentre outros.
Os números perfeitos são definidos como os números cuja soma de seus divisores é igual ao dobro do número. Estes números despertam interesses de muitos matemáticos, desde os pitagóricos. Até a Idade Média se conhecia 5 desses números: 6, 28, 496, 8128 e 33550336. Posteriormente, Euclides e Euler contribuíram com um importante teorema que fornece números perfeitos pares, a cada vez que se encontra um novo primo de Mersenne, surge um novo número perfeito par. Pesquisadores do mundo inteiro estão à procura desses novos números, seja para receberem prêmios, para contribuírem com o crescimento da Aritmética, para teste de hardware, para segurança de dados na internet, ou o fato de serem imortalizados na Matemática. Mas, existem problemas abertos, como é o caso da infinitude dos números perfeitos pares. O último primo de Mersenne foi descoberto em 25 de janeiro de 2013, conhecido como o "*48 primo de Mersenne*" e é dado por $2^{57\,885\,161} - 1$ com 17 425 170 algarismos, é claro que, isso só é possível devido ao uso de supercomputadores, GIMPS [2].

Atualmente, um dos problemas mais famosos da Teoria dos Números é se existe algum número perfeito ímpar. Ninguém até o momento conseguiu demonstrar a não existência, mas também

[1]Aluna de Mestrado Profissional em Matemática, Turma 2011
Instituição: Universidade Federal de São João del-Rei - UFSJ
E-mail: jaquelineprofmat@yahoo.com.br
[2]Orientador do Trabalho de Conclusão de Curso
Departamento de Matemática e Estatística - DEMAT, UFSJ
E-mail: avila_jaj@ufsj.edu.br

não conseguiu encontrar um número ímpar que satisfaça a condição de ser perfeito. Isso tudo motiva os estudiosos e amantes da Matemática, o que a torna uma ciência atual e em constante desenvolvimento.

Assumindo a existência dos números perfeitos ímpares, são consideradas estimativas a priori, isto é, as condições necessárias para estes números serem encontrados. Temos alguns resultados importantes a respeito, como:

- Segundo Ochem e Rao (2012) o número perfeito ímpar deve ser maior que 10^{1500}. Também, o total de fatores primos de sua decomposição (incluindo a multiplicidade) deve ser no mínimo 101.
- Nielsen (2006) ressaltou que este número deve ter no mínimo 9 fatores primos diferentes.

Este trabalho acompanha de perto e expande os detalhes de [1] referente à busca de limitantes superiores de qualquer fator primo, do tão procurado número perfeito ímpar. Primeiro consideramos o estudo de resultados preliminares que foram abordados nas aulas da disciplina de Aritmética do mestrado profissional em Matemática - PROFMAT. Logo, entramos com informações de teoremas importantes sobre os números perfeitos ímpares, para que finalmente, possa ser enunciado e provado o teorema principal deste trabalho, referente aos limitantes superiores de todos os fatores primos da decomposição deste número perfeito ímpar.

2 Preliminares

Definiremos os conceitos básicos da aritmética e enunciaremos teoremas e/ou proposições importantes que são necessários para a demonstração do teorema principal.

Definição 2.1 (Divisibilidade) *Sejam $a, b \in \mathbb{N}$, com $a \neq 0$. Se $\exists k \in \mathbb{N}$, tal que, $b = ka$, dizemos que a divide b,ou, a é um divisor de b ou, ainda, b é múltiplo de a, denotado por $a|b$.*

Quando não existe nenhum natural k, tal que, $b = ka$, escreve-se $a \nmid b$, (a não divide b).

Observação: Algumas propriedades muito úteis da divisibilidade podem ser encontradas em Hefez (2011, p. 31).

Notação: Denote o conjunto de todos os números naturais, sem o 0, por

$$\mathbb{N}^* = \{1, 2, 3, 4, 5, ...\}$$

Definição 2.2 (Máximo Divisor Comum) *Sejam $a, b \in \mathbb{N}$, onde, $a \neq 0$ ou $b \neq 0$. Diremos que $c \in \mathbb{N}^*$ é o máximo divisor comum de a e b, se $c|a$, $c|b$ e c é divisível por todo divisor comum de a e b, denotado $(a, b) = c$*

Definição 2.3 (Número Primo) *Um número natural p, $p > 1$, é chamado primo quando possui somente 2 divisores positivos, sendo eles 1 e p.*

Se $n \in \mathbb{N}$, $n > 1$, não é primo, então é composto.

Definição 2.4 (Números Primos entre si) *Sejam $a, b \in \mathbb{N}$. Dizemos que a e b são números primos entre si, ou coprimos, se $(a, b) = 1$.*

Proposição 2.1 *Dado $a \in \mathbb{N}$ e $b, c \in \mathbb{N}^*$. Então,*

$$b|a \ \ e \ \ c|a \Longleftrightarrow \frac{bc}{(b,c)}|a \tag{1}$$

A demonstração pode ser encontrada em Hefez (2011, p. 61).

Teorema 2.1 (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.*

A demonstração deste teorema pode ser encontrada em Santos (2009, p. 9).

Corolário 2.1 *Dado $n \in \mathbb{N}$, $n > 1$, existem números primos $p_1, ..., p_r$ e $\alpha_1, ..., \alpha_r \in \mathbb{N}$, univocamente determinados, tais que,*

$$n = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \tag{2}$$

Com os p_i, $i = 1, \ldots, r$, satisfazendo $p_1 < \ldots < p_r$.

Esta maneira de se escrever um número natural n é denominada: *Decomposição em fatores primos de n.*
Demonstração: É consequência imediata do Teorema Fundamental da Aritmética. □

Proposição 2.2 *Um número natural $n > 1$, é quadrado perfeito se, e somente se, na decomposição de seus fatores primos os expoentes de cada fator é par. Além disso, o expoente de cada fator primo é par se, e somente se, n possui quantidade de divisores ímpar.*

A seguir enunciaremos um resultado que se deve a Euclides, o qual, foi provado em sua obra: *Os Elementos.*

Teorema 2.2 (Euclides) *Existem infinitos números primos.*

Demonstração: Suponha que a sequência de números primos seja finita, $(p_1, p_2, \ldots, p_r)$. Considere o número natural R, $R = p_1 p_2 \cdots p_r + 1$. R não é divisível por nenhum p_i dessa sequência, pois R não divide 1. Como R é maior do que qualquer p_i e pelo Teorema 2.1, ou R é primo ou possui algum fator primo que não pertence a esta sequência de primos. Portanto, a sequência de números primos não pode ser finita. □

Notação:

(a) Denote o conjunto de todos os números primos por: $\# = \{2, 3, 5, 7, 11, 13, ...\}$

(b) Denote o conjunto de todos os números primos, exceto o 2, por: $\#^* = \{3, 5, 7, ...\}$

Definição 2.5 *Seja $p \in \#$ e $n, u \in \mathbb{N}$. Dizemos que $p^u \parallel n$ se $p^u | n$ e $p^{u+1} \nmid n$.*

Observação: $p \parallel n$ lê-se: p duas barras n.

Exemplo 2.1 Sejam $p = 3$, $n = 45$ e $u = 2$. Então, temos que $3^2|45$ e $3^3 \nmid 45$. Assim, $3^2 \parallel 45$.

Notação: Seja $n \in \mathbb{N}^*$. A soma dos divisores de n é denotada por $\sigma(n)$.

Proposição 2.3 *$\sigma(n)$ é uma função multiplicativa, isto é, se $(n, m) = 1$, então $\sigma(nm) = \sigma(n)\sigma(m)$.*

Proposição 2.4 *Seja $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $r \geqslant 1$, onde os $p_i \in \#$ e são diferentes. Então,*

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1} \tag{3}$$

Demonstração: Utilizando o Corolário 2.1, temos que $p_i \neq p_j$, $i \neq j$. Então,

$$\begin{aligned} \sigma(n) &= \sigma(p_1^{\alpha_1} \cdots p_r^{\alpha_r}) = \sigma(p_1^{\alpha_1}) \cdots \sigma(p_r^{\alpha_r}) = \prod_{i=1}^{r} \sigma(p_i^{\alpha_i}) \\ &= \prod_{i=1}^{r} (1 + p_i + ... + p_i^{\alpha_i}) = \prod_{i=1}^{r} \frac{p^{\alpha_{i+1}} - 1}{p_i - 1} \end{aligned}$$

Assim, concluímos a prova. □

Definição 2.6 (Número Perfeito) *Dizemos que $n \in \mathbb{N}^*$ é um número perfeito se $\sigma(n) = 2n$.*

Note que nenhum número primo é perfeito, pois $\sigma(p) = p + 1$. Na Tabela 1 apresentamos alguns números perfeitos.

Tabela 1: Alguns números perfeitos.

Número perfeito
6
28
496
8128
33550336
8589869056
137438691328
2305843008139952128
2658455991569831744654692615953842176
191561942608236107294793378084303638130997321548169216
13164036458569648337239753460458722910223472318386943117783728128
⋮

Definição 2.7 (Número de Mersenne) *Os números de Mersenne são da forma, $M_p = 2^p - 1$, com p primo.*

Os números de Mersenne que são primos são chamados *primos de Mersenne*. Por exemplo, $M_{11} = 2047$ é um número de Mersenne que não é primo, pois $2047 = 23 \times 89$.

Teorema 2.3 (Euclides-Euler) *Um número natural n é um número perfeito par se, e somente se, $n = 2^{p-1}(2^p - 1)$, onde $2^p - 1$ é um primo de Mersenne.*

Uma prova do Teorema 2.3 encontra-se em Hefez (2011, p. 102).

Observação: Se M é um primo de Mersenne e n um número perfeito. Então

$$n = \frac{M(M+1)}{2}$$

A seguir definiremos a congruência modular (aritmética com os restos da divisão euclidiana). Uma ferramenta matemática introduzida por Gauss que serviu de base para o desenvolvimento da Teoria dos Números.

Definição 2.8 (a congruente com b módulo m) *Sejam $a, b \in \mathbb{N}$ e $m \in \mathbb{N}^*$. Diremos que a e b são congruentes módulo m, quando os restos das divisões euclidianas a por m e b por m forem iguais. Denotamos por $a \equiv b \bmod m$.*

Proposição 2.5 *Sejam $a, b \in \mathbb{N}$, $a \geq b$. Tem-se $a \equiv b \bmod m$ se, e somente se, $m|(a-b)$.*

Uma demonstração da Proposição 2.5 é encontrada em Hefez (2011, p. 111).

Exemplo 2.2 Sejam $a = 47,\ b = 23$ e $m = 6$. Como $47 = 6 \times 7 + 5$ e $23 = 6 \times 3 + 5$, dizemos que $47 \equiv 23 \bmod 6$. Por outro lado, $6|24$ ou, equivalentemente, $6|(47-23)$, como indica a Proposição 2.5.

Proposição 2.6 *Seja m um número natural. Então,*

(a) *se m é ímpar $\implies m^2 \equiv 1 \bmod 4$*

(b) *se m é par $\implies m^2 \equiv 0 \bmod 4$*

Demonstração: Como m é natural, temos que $m \equiv r \bmod 4$, com $r \in \mathbb{N}$ e $r \leq m$, logo $m^2 \equiv r^2 \bmod 4$. Como $m - r = 4k,\ k \in \mathbb{N},$ e r é o resto da divisão por 4, podemos assumir $r = \{0, 1, 2, 3\}$. Então $m = 4k + r \iff m^2 = (4k+r)^2 \iff m^2 = 4(4k + 2kr) + r^2$. Logo, $m^2 \equiv r^2 \bmod 4$. Assim,

$$\begin{aligned} m^2 &\equiv 0^2 \bmod 4 \equiv 0 \bmod 4 \\ m^2 &\equiv 1^2 \bmod 4 \equiv 1 \bmod 4 \\ m^2 &\equiv 2^2 \bmod 4 \equiv 0 \bmod 4 \\ m^2 &\equiv 3^2 \bmod 4 \equiv 1 \bmod 4 \end{aligned}$$

Note que se m é ímpar então m^2 é congruente com 1 módulo 4, e se m é par então m^2 é divisível por 4. Assim, provamos (a) e (b), respectivamente. □

Proposição 2.7 *Seja $p \in \#^*$, então, para qualquer potência $\alpha \in \mathbb{N}$*

$$\sigma(p^\alpha) < \frac{3}{2}p^\alpha \tag{4}$$

Demonstração: Como $\sigma(p^\alpha) = 1 + p + ... + p^\alpha$, então

$$\begin{aligned} \frac{\sigma(p^\alpha)}{p^\alpha} &= \frac{1}{p^\alpha}\left(1 + p + ... + p^\alpha\right) = \left(\frac{1}{p}\right)^\alpha + \left(\frac{1}{p}\right)^{\alpha-1} + ... + 1 = \frac{1 - \left(\frac{1}{p}\right)^{\alpha+1}}{1 - \frac{1}{p}} \\ &= \frac{\frac{p^{\alpha+1}-1}{p^{\alpha+1}}}{\frac{p-1}{p}} = \frac{p^{\alpha+1}-1}{p^{\alpha+1}}\frac{p}{p-1} < \frac{p}{p-1} = \frac{1}{1-\frac{1}{p}} \end{aligned}$$

Como $p \geq 3$, então, $1 - \frac{1}{p} \geq \frac{2}{3}$. Assim, $\frac{1}{1-\frac{1}{p}} \leq \frac{3}{2}$. Logo, $\frac{\sigma(p^\alpha)}{p^\alpha} < \frac{3}{2}$, ou seja, $\sigma(p^\alpha) < \frac{3}{2}p^\alpha$. $\square$

Exemplo 2.3 Seja $p = 7$ e $\alpha = 2$. Então, $\sigma(7^2) = 57 < \frac{3}{2}7^2 = 73,5$.

3 Números Perfeitos Ímpares

Apesar de até o momento não se tenha conhecimento da existência de um número perfeito ímpar, isso não implica que não possamos obter estimativas a priori desse número. A partir de agora analisaremos resultados desse hipotético número, o qual denotaremos por x.

Proposição 3.1 *Se $q^r \parallel x$ com $q \in \#^*$, e $r \geq 2$ então*

$$q < (2x)^{\frac{1}{4}} \tag{5}$$

Demonstração: Se $q^r \parallel x$ então $q^r | x$. Por ser x perfeito e, pelo Corolário 2.1,

$$\sigma(x) = 2x = \sigma(p_1^{\alpha_1}) \cdots \sigma(q^r) \cdots \sigma(p_r^{\alpha_r}),$$

logo $q^r | \sigma(x)$. Por outro lado, $\sigma(q^r) | \sigma(x)$ e pela Proposição 2.1, temos que,

$$\frac{q^r\, \sigma\big(q^r\big)}{\big(q^r, \sigma(q^r)\big)} | \sigma(x)$$

Então existe $k \in \mathbb{N}^*$, tal que,

$$\sigma(x) = k \frac{q^r\, \sigma(q^r)}{\big(q^r, \sigma(q^r)\big)}$$

Assim, $q^r \sigma(q^r) | \sigma(x)$, logo $\sigma(x) \geq q^r \sigma(q^r)$. Como $\sigma(q^r) = 1 + q + q^2 + ... + q^r > q^r$, então, $q^r \sigma(q^r) > q^{2r}$. Assim, $\sigma(x) > q^r \sigma(q^r) > q^{2r}$. Como $r \geq 2$, $q^{2r} \geq q^4$, então $\sigma(x) > q^4$, ou seja, $2x > q^4$. Portanto, $q < (2x)^{\frac{1}{4}}$. $\square$

Euler também contribuiu com um importante resultado de um número perfeito ímpar, conforme teorema abaixo.

Teorema 3.1 (Teorema de Euler) *Se x um número perfeito ímpar, então $\exists Q$, $Q \in \#$, $\alpha, m \in \mathbb{N}$, tal que*

$$x = Q^\alpha m^2, \tag{6}$$

onde $Q \equiv 1 \bmod 4$ e $\alpha \equiv 1 \bmod 4$.

Demonstração: Como x é um número natural (maior que 2) podemos decompor nos seguintes fatores primos:

$$x = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

Por ser x perfeito, temos que $2x = \sigma(x)$ e como $(p_i^{r_i}, p_j^{r_j}) = 1$, com $i \neq j$ temos

$$2x = \sigma(x) = \sigma(p_1^{r_1})\sigma(p_2^{r_2}) \cdots \sigma(p_k^{r_k}) \tag{7}$$

Como x é ímpar, exige que somente uns dos fatores de (7) seja par e todos os outros ímpares. O fator par não deve ser divisível por 4, caso contrário exigiria que o x deveria ser par. Sem perda de generalidade, podemos assumir que o primeiro fator $\sigma(p_1^{r_1})$ seja par, e os outros $\sigma(p_i^{r_i})$, $i = 2, ..., k$, ímpares.
Analisemos os i-ésimo fator ímpar:

$$\sigma(p_i^{r_i}) = 1 + p_i + p_i^2 + ... + p_i^{r_i}, \quad i = 2, ..., k \tag{8}$$

Sabemos que

$$1 \equiv 1 \bmod 2, \quad p_i \equiv 1 \bmod 2, \quad p_i^2 \equiv 1 \bmod 2, \ \ldots \ , p_i^{r_i} \equiv 1 \bmod 2 \tag{9}$$

De (9) temos que $\sigma(p_i^{r_i}) \equiv (1 + r_i) \bmod 2$. Como $\sigma(p_i^{r_i})$ é ímpar então r_i tem que ser par, para todo $i = 2, ..., k$. Assim $p_i^{r_i} = p_i^{2s_i}$, com $i = 2, ..., k$. Logo, $p_2^{r_2} \cdots p_k^{r_k} = (p_2^{s_2} \cdots p_k^{s_k})^2 = m^2$. Como $p_i^{s_i}$, $i = 2, ..., k$, é ímpar temos que m^2 é ímpar. Assim pela Proposição 2.6a $m^2 \equiv 1 \bmod 4$. Por outro lado, como x é ímpar, temos que $p_1^{r_1}$ é ímpar e como $\sigma(p_1^{r_1})$ é par, então

$$\sigma(p_1^{r_1}) \equiv 2 \bmod 4 \tag{10}$$

Agora $\sigma(p_1^{r_1}) = 1 + p_1 + ... + p_1^{r_1}$ implica que $p_1 + ... + p_1^{r_1}$ deve ser ímpar, e isto só é verdade se r_1 é ímpar, isto é,

$$r_1 \equiv 1 \bmod 4$$

Das quatro possibilidades de congruência temos: $p_1 \equiv 0 \bmod 4$, $p_1 \equiv 1 \bmod 4$, $p_1 \equiv 2 \bmod 4$ e $p_1 \equiv 3 \bmod 4$. Como p_1 é ímpar desconsideramos as possibilidades de restos 0 e 2. Suponha $p_1 \equiv 3 \bmod 4$. Assim,

$$\begin{aligned}
1 &\equiv 1 \bmod 4 \\
p_1 &\equiv 3 \bmod 4 \\
p_1^2 &\equiv 3^2 \bmod 4 \equiv 1 \bmod 4 \\
p_1^3 &\equiv 3^3 \bmod 4 \equiv 3 \bmod 4 \\
&\vdots \\
p_1^{r_1} &\equiv 3^{r_1} \bmod 4 \equiv 3 \bmod 4
\end{aligned}$$

Então,

$$\sigma(p_1^{r_1}) = 1 + p_1 + p_1^2 + p_1^3 + ... + p_1^{r_1} \equiv (1 + 3 + 1 + 3 + ... + 3) \bmod 4 \tag{11}$$

Por outro lado,

$$1 + 3 + 1 + 3 + ... + 3 = 1\frac{(r_1 + 1)}{2} + 3\frac{r_1 + 1}{2} = 2(r_1 + 1)$$

Como r_1 é ímpar, podemos escrever $r_1 = 2\varepsilon + 1$. Logo $2(r_1 + 1) = 2(2\varepsilon + 1 + 1) = 4(\varepsilon + 1)$. Logo, de (11), $\sigma(p_1^{r_1}) \equiv 0 \bmod 4$ que é uma contradição com (10). Portanto $p_1 \equiv 1 \bmod 4$ e $\sigma(p_1^{r_1}) = 1 + p_1 + ... + p_1^{r_1} \equiv 1 + 1 + ... + 1 = 1 + r_1 \equiv 2 \bmod 4$. Assim a demonstração termina quando denotamos $p_1 = Q$ e $r_1 = \alpha$. □

4 Teorema Principal

Enfim enunciaremos o Teorema principal devido a Acquaah e Konyagin (2012).

Teorema 4.1 *Se x é um número perfeito ímpar e q qualquer fator primo de x, então*

$$q < (3x)^{1/3} \tag{12}$$

Demonstração: Pelo Teorema 3.1 podemos escrever $x = Q^{\alpha}m^2$, onde $Q \in \#^*, m, \alpha \in \mathbb{N}$ e Q e α são congruentes a 1 módulo 4. Por outro lado, como q é fator primo de x então $q|x$. Agora, suponha que:

i) $q \neq Q$

Então pelo Teorema 3.1 temos que $x = Q^{\alpha}q^2$, o qual implica, que $q^2|x$ e $q^{2+1} \nmid x$, então $q^2 \parallel x$. Pela Proposição 3.1 temos que $q < (2x)^{\frac{1}{4}} < (2x)^{\frac{1}{3}} < (3x)^{\frac{1}{3}}$. Portanto temos $q < (3x)^{\frac{1}{3}}$.

ii) $q = Q$

Sem perda de generalidade assumimos $\alpha = 1$. Por outro lado, como x é perfeito ímpar, $\exists p$, $p \in \#^*$ tal que, para todo a, $a \in \mathbb{N}^*$,

$$p^{2a} \parallel x \tag{13}$$

com $q|\sigma(p^{2a})$. Novamente, do Teorema 3.1 podemos considerar

$$x = q\,(p^a\,v)^2 = q\,p^{2a}v^2 \tag{14}$$

Para encontrar um limitante de q em termos de x consideraremos dois casos:

Caso 1: $p \nmid \sigma(q)$

De $q|\sigma(p^{2a})$ e de $p^{2a}|\sigma(v^2)$ temos $qp^{2a}|\sigma(p^{2a})\sigma(v^2)$ ou, equivalentemente, $qp^{2a}|\sigma(p^{2a}v^2)$. Assim

$$qp^{2a} \leq \sigma(p^{2a}v^2) \tag{15}$$

Por outro lado, por ser x perfeito e satisfazer (14),

$$\begin{aligned} 2x &= \sigma(x) = \sigma(qp^{2a}v^2) = \sigma(q)\sigma(p^{2a})\sigma(v^2) = (q+1)\sigma(p^{2a})\sigma(v^2) \geqslant (q+1)qp^{2a} \\ &= q^2p^{2a} + qp^{2a} > q^2p^{2a} > q^2\frac{2}{3}\sigma(p^{2a}) \geqslant q^2\frac{2}{3}q = \frac{2}{3}q^3 \end{aligned}$$

Logo, $q < (3x)^{\frac{1}{3}}$.

Caso 2: $p|\sigma(q)$

Como $q|\sigma(p^{2a})$ então $\exists u \in \mathbb{N}^*$ tal que,

$$\sigma(p^{2a}) = qu \tag{16}$$

Por outro lado,

$$\sigma(p^{2a}) = 1 + p + ... + p^{2a} \ \equiv \ (1 + 0 + ... + 0) \bmod p \ \equiv \ 1 \bmod p \tag{17}$$

De (16) e (17),

$$qu \equiv 1 \bmod p \tag{18}$$

De $p|\sigma(q)$ temos que $p|(q+1)$. Logo, $q + 1 \equiv 0 \bmod p$ ou, equivalentemente,

$$q \equiv -1 \bmod p \tag{19}$$

De (18) e (19),

$$u \equiv -1 \bmod p \tag{20}$$

Então $p|(u+1)$, isto é, $u + 1 = kp$ para algum $k \in \mathbb{N}^*$. De (16) u é ímpar, então $u + 1 \neq p$. Assim, $kp \neq p$. Então para $k = 2s$, $s \in \mathbb{N}^*$, temos que $2p|(u+1)$. Assim,

$$u \geq 2p - 1 \tag{21}$$

Seja

$$p^b \parallel \sigma(q), \quad b \geq 1 \tag{22}$$

Note que $p^{2a-b} \parallel \sigma(v^2)$. Assim, $b \leq 2a$, e

$$\sigma(v^2) \geq p^{2a-b} \tag{23}$$

Como $b \leq 2a \leq 2a + 1$ temos que $p^b \leq p^{2a+1} \Longrightarrow p^b | p^{2a+1}$. Logo

$$p^{2a+1} \equiv 0 \bmod p^b \tag{24}$$

De (22), $p^b|\sigma(q) \Longrightarrow \sigma(q) \equiv 0 \bmod p^b$ ou, equivalentemente,

$$(p-1)u\sigma(q) \equiv 0 \bmod p^b \tag{25}$$

De (3) temos que $\sigma(p^{2a}) = \frac{p^{2a+1}-1}{p-1}$ ou, equivalentemente, $p^{2a+1} - 1 = (p-1)\sigma(p^{2a})$.
Por (16),

$$p^{2a+1} - 1 = (p-1)uq = (p-1)u\big(\sigma(q) - 1\big) = (p-1)u\sigma(q) - u(p-1) \tag{26}$$

ou,

$$p^{2a+1} = (p-1)u\sigma(q) - u(p-1) + 1 \tag{27}$$

De (24) e (25) temos que

$$0 \equiv -u(p-1) + 1 \bmod p^b \Longleftrightarrow u(p-1) \equiv 1 \bmod p^b$$

Então, $p^b|\big(u(p-1) - 1\big)$. Logo, $p^b \leq (p-1)u - 1 < (p-1)u$. Assim, $(p-1)u > p^b$ ou, $up^{-b} > \frac{1}{p-1}$. Logo,

$$up^{2a-b} > \frac{p^{2a}}{p-1} \tag{28}$$

De (23) temos que $u\sigma(v^2) \geq up^{2a-b}$ e, por (28), temos

$$u\sigma(v^2) > \frac{p^{2a}}{p-1} \tag{29}$$

Por ser x perfeito e usando (14) e (16),

$$2x \;=\; \sigma(x) \;=\; \sigma(qp^{2a}v^2) \;=\; \sigma(q)\sigma(p^{2a})\sigma(v^2) \;=\; (q+1)qu\sigma(v^2) \tag{30}$$

De (29),

$$2x > (q+1)q\frac{p^{2a}}{p-1} > qq\frac{(p^{2a})}{p-1} \tag{31}$$

Por (4),

$$2x > \frac{q^2}{p-1}\left(\frac{2}{3}\sigma(p^{2a})\right) \tag{32}$$

Pela equação (16) temos

$$2x > \frac{q^2}{p-1}\left(\frac{2}{3}qu\right) = \frac{2}{3}\frac{q^3}{(p-1)}u \tag{33}$$

De (21),

$$2x > \frac{2}{3}\frac{q^3}{p-1}(2p-1) = \frac{q^3}{3}\frac{2(2p-1)}{(p-1)} = \frac{q^3}{3}\frac{(4p-2)}{(p-1)} > \frac{q^3}{3}\frac{(4p-4)}{(p-1)} = \frac{q^3}{3}4 \tag{34}$$

Então,

$$2x > \frac{4}{3}q^3 \Longleftrightarrow x > 2\frac{q^3}{3} > \frac{q^3}{3}$$

Portanto,

$$q < (3x)^{\frac{1}{3}}$$

Desse modo terminamos de demostrar nosso teorema principal. □

5 Considerações Finais

A Teoria dos Números é uma área da Matemática muito promissora, desde 300 a.C. até o momento os estudiosos estão descobrindo grandes resultados e importantes teoremas, que com o apoio dos supercomputadores, cada vez mais acessível em centros de pesquisa, vem sendo provados e verificados a exatidão dos mesmos.
Analisamos nesse trabalho os principais resultados da Aritmética e ampliamos os detalhes do trabalho de Acquaah e Konyagin (2012), referente a "cotas superiores" de todos os fatores primos, que resultam da decomposição em fatores primos, destes curiosos números perfeitos ímpares. Fazendo desse modo, possível que qualquer graduando de Matemática entenda esses resultados e desperte o interesse na procura da existência, ou não, destes números.

Agradecimentos

Primeiramente a Deus pela vida e pela oportunidade de realizar esse curso de suma importância para minha vida profissional e pessoal, "*até aqui me ajudou o Senhor*". A todos que contribuíram para a conclusão desse projeto. Em especial, a toda minha família pais e irmãos, pelo amor, apoio e compreensão. Aos companheiros do curso pelo incentivo e companheirismo. Ao meu orientador Prof. Dr. Jorge Julca Avila, pela disponibilidade, paciência e o aprendizado que me proporcionou. A todos os docentes que lecionaram no PROFMAT 2011-2013, que privilegiaram toda turma com seus conhecimentos. Enfim a toda UFSJ e a Capes.

Referências

[1] ACQUAAH, Peter; KONYAGIN, Sergei. **On prime factors of odd perfect Numbers**. International Jornal of Number Theory, v.8, n.6, 2012.

[2] GIMPS. **Great Internet Mersenne Prime Search**. Disponível em <http://www.mersenne.org>. Acesso em: 26 janeiro de 2013.

[3] HEFEZ, Abramo. **Elementos de Aritmética**. 2ed. Rio de Janeiro: SBM, 2011. 169 p.

[4] NIELSEN, Pace P. **Odd perfect numbers have at least nine distinct prime factors**. Mathematics of Computation, 76, Nº 260, p.2109-2126, 2006.

[5] OCHEM, Pascal; RAO, Michaël. **Odd perfect numbers are greater than** 10^{1500}. Mathematics of Computation, 81, p.1869-1877, 2012.

[6] SANTOS, José Plínio de Oliveira. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2009. 198 p.