APLICAÇÕES DO PEQUENO TEOREMA DE FERMAT

APPLICATIONS OF THE FERMAT'S LITTLE THEOREM

Vanessa de Freitas Travello¹; Luana Beatriz Cardoso¹; Juliano Ferreira Lima¹; Thiago Mariano Viana¹; Antonio Carlos Tamarozzi².

Universidade Federal de Mato Grosso do Sul – UFMS, Três Lagoas. MS. e-mail: vanessatravello@gmail.com. ¹Bolsista do Grupo PET MATEMÁTICA – Matemática/CPTL/UFMS. ²Tutor do Grupo PET MATEMÁTICA – Matemática/CPTL/UFMS

RESUMO - O Pequeno Teorema de Fermat é um resultado de impacto para a divisibilidade na Teoria dos Números. O tema foi inserido como parte de um projeto de iniciação científica desenvolvida pelos autores como uma das atividades do grupo PET/Matemática da UFMS/Campus de Três Lagoas. O desenvolvimento do projeto foi realizado através de levantamento bibliográfico, estudo teórico do assunto, discussões e apresentações de seminários com a orientação do tutor e elaboração do relatório final. O trabalho propiciou contato com algumas das técnicas comumente utilizadas em problemas introdutórios da teoria dos números, mais especificamente a análise de congruências. Como aplicações foram estabelecidas diversas congruências importantes, algumas delas de impacto para o desenvolvimento da Teoria dos Números. O estudo pode ser estendido a resultados com a função de Euler, em consequência pode ser apresentado o funcionamento do método criptográfico RSA que, constitui uma aplicação extremamente poderosa desta teoria Matemática.

Palavras-chave - Teste de Primalidade, Criptografia, Teoria dos números.

ABSTRACT - Fermat's Little Theorem is a result of impact for divisibility in Number Theory. The theme was inserted as part of a research project developed by the authors as one of the activities of the group PET/Math UFMS/CPTL. The development project was conducted through a literature review, theoretical study of the subject, discussions and seminar presentations with guidance from the tutor and preparing the final report. The work led to contact with some of the techniques commonly used in introductory problems of number theory, specifically the analysis of congruences. As applications several important congruences, some impact to the development of the Theory of Numbers were established. The study was extended to results with the Euler function, therefore the operation of the RSA cryptographic method that is an extremely powerful Maths application of this theory can be displayed.

Keywords - Primality test, Cryptography, number theory.

1 INTRODUÇÃO

Pierre de Fermat não era um matemático de fato, prestava serviço como juiz e dedicava-se à Matemática em suas horas de lazer. Assim foi considerado um matemático amador e conhecido como o “Príncipe dos Amadores”. A influência de Fermat na matemática foi limitada pela não publicação de seus trabalhos e descobertas. Assim como outros matemáticos, suas pesquisas eram conhecidas através de cartas e anotações enviadas a amigos e também matemáticos.

Fermat estudou diversas áreas da matemática, mas foi graças aos seus estudos em Teoria dos Números que ele ficou famoso. Foi o primeiro a descobrir e enunciar o Pequeno Teorema de Fermat, apesar de que a demonstração de tal teorema ter sido dada por Euler.

Este trabalho tem como objetivo o aprimoramento das teorias algébricas com base em congruência e suas aplicações. A execução deste trabalho como método de investigação científica, propiciou a inserção dos alunos do PET (Programa de Educação Tutorial) envolvidos na pesquisa Matemática, através do desenvolvimento de ferramentas introdutórias para a teoria dos números e, em consequência, a ramos importantes da Matemática.

2 METODOLOGIA

O trabalho é resultado de uma pesquisa teórica, desenvolvido através de discussões do tema com o orientador e apresentações de seminários como parte das atividades do programa PET - Matemática no estudo de Introdução à Teoria dos números.

O trabalho incluiu uma etapa de leitura e resoluções de exercícios, desenvolvimento das atividades propostas e um relatório dissertativo dos resultados obtidos. O estudo e as atividades desenvolvidas foram avaliados através da apresentação de seminários de discussões.

3 RESULTADOS

O resultado de Pierre de Fermat, conhecido como Pequeno Teorema de Fermat, pode ser assim enunciado:

3.1 TEOREMA DE FERMAT - Dados a e p inteiros com p primo, então

$$a^p \equiv a \pmod{p} \Leftrightarrow p|(a^p - a), \forall a \in \mathbb{Z}.$$

Para a demonstração desse teorema utilizamos o lema: Seja p um número primo. Os números da forma $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p .

Demonstração do teorema - Vamos provar o resultado por indução sobre a , com $a \geq 0$. O resultado vale claramente para $a = 0$, pois $p|0$.

Supondo o resultado válido para a , iremos prova-lo para $a + 1$. Pela formula do binômio de Newton,

$$(a + 1)^p - (a + 1) = a^p - a + \binom{p}{1}a^{p-1} + \dots + \binom{p}{p-1}a.$$

Pelo lema apresentado acima e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p . Que é o que queríamos provar.

Notação: utilizaremos (a, p) para designar o máximo divisor comum entre os números inteiros a e p .

Pode-se mostrar que a recíproca do Pequeno Teorema de Fermat não é valida. De fato, considerando $p = 561$ e $a \in \mathbb{N}$ 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

$$3|(a^{280})^2 - 1; 11|(a^{56})^{10} - 1; \\ 17|(a^{35})^{16} - 1.$$

Segue-se daí que 561 divide $a^{560} - 1$, para todo a tal que $(a, 561) = 1$, Mas 561 não é primo.

O Pequeno Teorema de Fermat adquire outro formato que pode ser assim descrito:

3.2 TEOREMA DE FERMAT (SEGUNDA VERSÃO) - Dados $a \in \mathbb{Z}$ e p um primo que não divide a , tem-se,

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração - Pelo Pequeno Teorema de Fermat 3.1 temos que

$$p|a^p - a \Rightarrow p|a(a^{p-1} - 1),$$

e como $(a, p) = 1$, segue-se imediatamente, que p divide $a^{p-1} - 1$.

■

Observação: Temos como consequência desse teorema o teste de não primalidade, que é dado por: Seja $m \in \mathbb{Z}$ com $m > 1$, se existir um $a \in \mathbb{N}$ com $(a, m) = 1$ tal que se $m \nmid a^{m-1} - 1$, então m não é primo.

Antes de apresentar as aplicações do teorema de Fermat, serão apresentadas duas proposições importantes de congruência e divisibilidade de números primos.

A proposição seguinte é um resultado clássico que caracteriza os números primos.

3.3 PROPOSIÇÃO – Sejam a, b e $p \in \mathbb{Z}$, com p primo. Se $p|ab$ então $p|a$ ou $p|b$.

Demonstração - Se $p|ab$, então existe e tal que $ab = pe$. Vamos supor que $p \nmid a$ então $(a, p) = 1$ Assim, existe $m, n \in \mathbb{Z}$ tais que

$$an + pm = 1.$$

Multiplicando b em ambos os lados da igualdade acima, temos que

$$b = abn + pbm,$$

substituindo ba por pe nesta última igualdade, temos que

$$b = pen + pbm = p(en + bm)$$

e portanto $p|b$.

De forma análoga suponhamos que $p \nmid b$ e chegamos que $p|a$.

Portanto $p|a$ ou $p|b$.

■

A proposição seguinte tem consequências importantes para este trabalho:

3.4 PROPOSIÇÃO - Dado $a, b, c \in \mathbb{Z}$, com b e c não ambos nulos, temos que $b|a$ e $c|a$ equivale que $\frac{bc}{(b,c)}|a$.

Demonstração - temos que $b|a$ e $c|a$ implica que $a = bn = cm$, com $m, n \in \mathbb{Z}$. Logo

$$n \frac{b}{(b,c)} = m \frac{c}{(b,c)},$$

como $\left(\frac{b}{(b,c)}, \frac{c}{(b,c)}\right) = 1$ segue que $\frac{b}{(b,c)}|m$, o que implica que

$$c \frac{b}{(b,c)} = cm$$

como $cm = a$, o resultado segue.

Observação: Um caso particular da proposição 3.4 é o seguinte resultado: dados $a, b, c \in \mathbb{Z}$, com b e c primos entre si, tais que $b|a$ e $c|a$. Então $bc|a$.

Com o trabalho de pesquisa, exploramos algumas aplicações do Pequeno

Teorema de Fermat, para melhor entendimento do conceito dado.

1. Seja p primo maior que 2, provaremos que

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} = -1 \pmod{p}$$

Prova:

Vamos analisar a congruência de cada uma das parcelas do primeiro membro.

$p \nmid 1 \Rightarrow p|1^{p-1} - 1$, assim temos que $1 \equiv 1 \pmod{p}$.

$p \nmid 2 \Rightarrow p|2^{p-1} - 1$, assim temos que $2^{p-1} \equiv 1 \pmod{p}$.

$p \nmid 3 \Rightarrow p|3^{p-1} - 1$, assim temos que $3^{p-1} \equiv 1 \pmod{p}$.

Assim prosseguindo obtemos similarmente que

$p \nmid (p-1) \Rightarrow p|(p-1)^{p-1} - 1$, ou seja $(p-1)^{p-1} \equiv 1 \pmod{p}$.

Portanto, somando congruências, obtemos que

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} \equiv (p-1)$$

Dado que, $(p-1) \equiv -1 \pmod{p}$, segue por transitividade que

$$1^{p-1} + 2^{p-1} + 3^{p-1} + \dots + (p-1)^{p-1} = -1 \pmod{p}$$

■

2. Encontrar o resto da divisão de $2^{1000000}$ por 17.

Temos que 17 é primo e não divide 2, então pelo Pequeno Teorema de Fermat

$$2^{16} \equiv 1 \pmod{17},$$

mas $100\,000 = (6\,250)(16)$.

Portanto

$$2^{1000\,000} = [(2^{16})^{6250}] \equiv 1^{6250} \pmod{17} \equiv 1 \pmod{17}$$

Assim, temos pelo Pequeno Teorema de Fermat que o resto da divisão de

$$2^{1000\,000} \text{ por } 17 \text{ é } 1.$$

3. Usamos o Teorema para mostrar que $42|a^7 - a$ para todo número inteiro a .

Temos que 42 é divisível por 2, 3 e 7 sendo estes números primos entre si. De acordo com a proposição 3.4, é suficiente verificarmos que cada um deles divide $a^7 - a$. Esta verificação será feita nos itens a), b) e c) que seguem:

a) $a^7 \equiv a \pmod{7}$, por uma aplicação direta do Pequeno teorema de Fermat.

$$b) \quad 3|a^7 - a.$$

Temos

$$\begin{aligned} a^7 - a &= a(a^6 - 1) = a((a^2)^3 - 1) \\ &= a(a^2 - 1)(1 + a^2 + a^4) = (a^3 - a)(1 + a^2 + a^4) \end{aligned}$$

Pelo Pequeno Teorema de Fermat temos que $a^3 \equiv a \pmod{3} \Rightarrow 3|a^3 - a$ o que é suficiente para termos $3|a^7 - a$.

$$c) \quad 2|a^7 - a.$$

O resultado segue da seguinte fatoração

$$\begin{aligned} a^7 - a &= a(a^6 - 1) = \\ &= a(a^2 - 1)(a^4 + a^2 + 1) = \\ &= a(a - 1)(a + 1)(1 + a^2 + a^4) = \\ &= (a^2 - a)(a + 1)(1 + a^2 + a^4) \end{aligned}$$

haja vista que, pelo pequeno teorema de Fermat, temos que $a^2 \equiv a \pmod{2} \Rightarrow 2|a^2 - a$.

4. Mostraremos que, para todo $n \in \mathbb{N}$, é natural o número:

$$\frac{3}{5}n^5 + \frac{2}{3}n^3 + \frac{11}{15}n.$$

Prova: Efetuamos inicialmente a seguinte simplificação da expressão dada:

$$\begin{aligned} &\frac{3}{5}n^5 - \frac{3}{5}n + \frac{3}{5}n + \frac{2}{3}n^3 - \frac{2}{3}n + \frac{2}{3}n + \frac{11}{15}n \\ &= \frac{3}{5}n^5 - \frac{3}{5}n + \frac{2}{3}n^3 - \frac{2}{3}n + \frac{11 + 9 + 10}{15}n \\ &= \frac{3}{5}(n^5 - n) + \frac{2}{3}(n^3 - n) + 2n. (*) \end{aligned}$$

Temos pelo Pequeno Teorema de Fermat que $n^5 - n$ é divisível por 5, ou seja $n^5 \equiv n \pmod{5}$ e $n^3 - n$ é divisível por 3, ou seja $n^3 \equiv n \pmod{3}$. Assim existem $a, b \in \mathbb{N}$, tais que $n^3 - n = 3a$ e $n^5 - n = 5b$, logo substituindo em (*) teremos:

$$\begin{aligned} &\frac{3}{5}n^5 - \frac{3}{5}n + \frac{3}{5}n + \frac{2}{3}n^3 - \frac{2}{3}n + \frac{2}{3}n + \frac{11}{15}n = \\ &= \frac{3}{5}(n^5 - n) + \frac{2}{3}(n^3 - n) + 2n = \\ &= \frac{3}{5}5b + \frac{2}{3}3a + 2n = \\ &= 3a + 2b + 2n, \end{aligned}$$

assim temos que $3a + 2b + 2n$ é um número natural para todo $n \in \mathbb{N}$.

5. Podemos verificar que, para todo $n \in \mathbb{N}$, $15 \mid (3n^5 + 5n^3 + 7n)$.

Temos que 15 é divisível por 3 e 5, logo basta provar que $3 \mid (3n^5 + 5n^3 + 7n)$ e $5 \mid (3n^5 + 5n^3 + 7n)$, o que será feito nos itens seguintes:

$$\begin{aligned} \text{a)} \quad 3n^5 + 5n^3 + 7n &= 3n^5 - \\ -3n + 3n + 5n^3 + 7n &= 3n^5 - 3n + \\ +5n^3 + 10n. \end{aligned}$$

Temos claramente que $5n^3 + 10n$ é divisível por 5, sendo o mesmo ocorrendo com $3n^5 - 3n$, de acordo com o Pequeno Teorema de Fermat. Logo segue que $5 \mid (3n^5 + 5n^3 + 7n)$.

$$\begin{aligned} \text{b)} \quad 3n^5 + 5n^3 + 7n &= 3n^5 + \\ +5n^3 - 5n + 5n + 7n &= 3n^5 + 5n^3 - 5n + \\ +12n \end{aligned}$$

Temos que $5n^3 - 5n$ é divisível por 3, porque, $3 \mid n^3 - n$ (pelo pequeno teorema de Fermat). Dado que $3 \mid 3n^5 + 12n$ é imediato, segue que 3 também divide a soma, ou seja,

$$3 \mid 3n^5 + 5n^3 + 7n$$

Uma análise similar mostra que 5 também é um divisor. Logo, pela proposição 3.4 temos que $15 \mid 3n^5 + 5n^3 + 7n$, para qualquer $n \in \mathbb{N}$.

6. Seja $n \in \mathbb{N}$. Mostremos que:

a) Se $5 \nmid n$, $5 \nmid n - 1$, $5 \nmid n + 1$, então $5 \mid n^2 + 1$.

Temos pelo Pequeno Teorema de Fermat que se $5 \nmid n$ então $5 \mid n^4 - 1$, mas

$$\begin{aligned} n^4 - 1 &= (n^2 + 1)(n^2 - 1) = \\ &= (n^2 + 1)(n - 1)(n + 1). \end{aligned}$$

Como sabemos, 5 é primo, $5 \nmid n - 1$ e $5 \nmid n + 1$, segue que $5 \mid n^2 + 1$.

b) Se $7 \nmid n$, $7 \nmid n - 1$, $7 \nmid n^3 + 1$, então $7 \mid n^2 + n + 1$.

Temos pelo Pequeno Teorema de Fermat que se $7 \nmid n$ então $7 \mid n^6 - 1$, mas

$$\begin{aligned} n^6 - 1 &= (n^3 - 1)(n^3 + 1) = \\ &= (n - 1)(n + n^2 + 1)(n^3 + 1). \end{aligned}$$

Como sabemos $7 \nmid n^3 + 1$ e $7 \nmid n - 1$, segue da proposição 3.3 que $7 \mid (n^2 + n + 1)$.

7. Mostraremos que $a^{12} - b^{12}$ é divisível por 13, se a e b são primos com 13. Mostraremos também que $a^{12} - b^{12}$ é divisível por 91, se a e b são primos com 91.

Solução:

a) Sendo $(a, 13) = 1$ e

b)

c) $(b, 13) = 1$, mostremos que $13 \mid a^{12} - b^{12}$. Mas

$$\begin{aligned} a^{12} - b^{12} &= \\ &= a^{12} - 1 + 1 - b^{12} = a^{12} - 1 - b^{12} + 1 \end{aligned}$$

Como $13 \nmid a$ e $13 \nmid b$, segue do Pequeno Teorema de Fermat, $13 \mid a^{12} - 1$ e $13 \mid b^{12} - 1$. Em particular, temos que 13 também divide o oposto, ou seja, $13 \mid 1 - b^{12}$

Portanto

$$13 \mid a^{12} - b^{12}$$

$$d) \quad 91|a^{12} - b^{12}.$$

Temos que 91 é divisível somente por 7 e 13, que são primos entre si. Logo é suficiente mostrarmos que 7 e 13 são divisores de $a^{12} - b^{12}$. Observemos que

$$\begin{aligned} a^{12} - b^{12} &= a^{12} - 1 + 1 - b^{12} = \\ &= (a^{12} - 1) + (1 - b^{12}) = \\ &= (a^6 - 1)(a^6 + 1) + (1 - b^6)(1 + b^6). \end{aligned}$$

Agora basta provarmos que temos a soma de dois produtos divisíveis por 7.

Como $(a, 91) = 1$ então $7 \nmid a$, logo temos pelo Pequeno teorema de Fermat que $7|a^6 - 1$. Da mesma forma o somando $(1 - b^6)(1 + b^6)$ é divisível por 7.

Como 7 divide as duas partes da soma, assim $7|a^{12} - b^{12}$ e já temos assegurado que $13|a^{12} - b^{12}$, resulta $91|a^{12} - b^{12}$, como desejado.

8. Provaremos que para todo $n \in \mathbb{Z}$, o número $n^{13} - n$ é divisível por 2, 3, 5, 7, 13 e 273.

Da definição de congruência $n^p \equiv n \pmod{p}$ temos que $p|n^p - n$.

Temos que 273 é divisível por 3, 7 e 13; assim basta mostrarmos que 3, 7 e 13 divide $n^{13} - n$ (proposição 3.4).

$$\begin{aligned} i) \quad 2|n^{13} - n \\ n^{13} - n &= n(n^{12} - 1) \\ &= n(n^6 - 1)(n^6 + 1) \\ &= n(n^6 + 1)(n^3 - 1)(n^3 + 1) \end{aligned}$$

$$= n(n^6 + 1)(n^3 + 1)(n - 1)(n^2 + n + 1).$$

E segue imediatamente o resultado.

$$\begin{aligned} ii) \quad 3|n^{13} - n \\ n^{13} - n &= n(n^{12} - 1) = \\ &= n(n^6 - 1)(n^6 + 1) = \\ &= n(n^6 + 1)(n^2 - 1)(n^4 + n^2 + 1). \end{aligned}$$

Assim pelo Pequeno teorema de Fermat temos que $n^2 \equiv 1 \pmod{3} \Rightarrow 3|n^2 - 1$.

Logo

$$3|n^{13} - n.$$

$$\begin{aligned} iii) \quad 5|n^{13} - n. \\ n^{13} - n &= n(n^{12} - 1) = \\ &= n(n^4 - 1)(n^8 + n^4 + 1). \end{aligned}$$

Assim pelo Pequeno teorema de Fermat temos que $n^4 \equiv 1 \pmod{5} \Rightarrow 5|n^4 - 1$.

Logo

$$5|n^{13} - n.$$

$$\begin{aligned} iv) \quad 7|n^{13} - n. \\ n^{13} - n &= n(n^{12} - 1) = \\ &= n(n^6 - 1)(n^6 + 1). \end{aligned}$$

Assim pelo Pequeno teorema de Fermat temos que $n^6 \equiv 1 \pmod{7} \Rightarrow 7|n^6 - 1$.

Logo

$$7|n^{13} - n.$$

$$v) \quad 13|n^{13} - n.$$

Essa é uma aplicação direta do pequeno teorema de Fermat

$$vi) \quad 273|n^{13} - n$$

Temos 273 é fatorável por 3, 7, e 13. Pela proposição 3.4 e por ii), iv) e v) temos que

$$273 | n^{13} - n.$$

Apresentaremos agora uma pequena introdução ao teorema de Euler, que é uma extensão do teorema apresentado neste trabalho. Necessitamos da definição da função phi de Euler

Definição: Designaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo m , $m \geq 2$, que corresponde à quantidade de números naturais entre 0 e $m-1$ que são primos com m . Pondo $\varphi(1) = 1$, está definida uma importante função $\varphi: \mathbb{N} \rightarrow \mathbb{N}$, conhecida como função phi de Euler.

Observamos que resulta diretamente da definição que para todos $m \geq 2$,

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

3.5 PROPOSIÇÃO - Se $m > 1$, então $\varphi(m) = m - 1$ se, e somente se, m for primo.

Demonstração: De fato, se m é primo então o sistema reduzido modulo m é formado por:

$$1, 2, \dots, m-1 \Rightarrow \varphi(m) = m-1.$$

■

Utilizando a proposição anterior e uma contagem simples, podemos mostrar que, se m é primo, então

$$\varphi(m^k) = m^k - m^{k-1}.$$

3.6 TEOREMA DE EULER-FERMAT – Sejam $m, a \in \mathbb{Z}$, com $m > 1$ e $(a, m) = 1$ então

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

Demonstração: Seja $r_1, r_2, \dots, r_{\varphi(m)}$ um sistema reduzido módulo m , ou seja, $(r_i, m) = 1$, para todo $i = 1, 2, 3, \dots, s$. E como $(a, m) = 1$ então $ar_1, ar_2, \dots, ar_{\varphi(m)}$ forma um sistema reduzido módulo m .

Portanto,

$$\begin{aligned} a^{\varphi(m)} r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} &= \\ &= ar_1 \cdot ar_2 \cdot \dots \cdot ar_{\varphi(m)} \equiv \\ &\equiv r_1 \cdot r_2 \cdot \dots \cdot r_{\varphi(m)} \pmod{m}. \end{aligned}$$

Como $(a, m) = 1, \forall i = 1, 2, 3, \dots, \varphi(m)$, Segue que

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

■

Um importante resultado da função de Euler é dado por: Sejam $m, n \in \mathbb{N}$ tais que $(m, n) = 1$, então

$$\varphi(m, n) = \varphi(m) \cdot \varphi(n).$$

Tal resultado não será demonstrado nesse trabalho.

Exemplos

1) Determinemos $\varphi(1024)$

Temos que $1024 = 2^{10}$, assim

$$\varphi(1024) = \varphi(2^{10})$$

Como 2 é primo e usando a consequência da proposição 3.5 teremos

$$\begin{aligned} \varphi(1024) &= \varphi(2^{10}) = \varphi(1024) = 2^{10} - \\ &- 2^9 = 2^9 = 512. \end{aligned}$$

Logo, $\varphi(1024) = 512$.

2) Ache o resto da divisão $34 \mid 3^{100}$.

Temos que

$$\begin{aligned}\varphi(34) &= \varphi(2)\varphi(17) = \\ &= (2-1)(17-1) = 16\end{aligned}$$

Então pelo teorema de Euler-Fermat

$$3^{16} \equiv (1 \bmod 34)$$

Assim

$$\begin{aligned}3^{100} &= (3^{16})^6 3^4 \equiv (1^6) 3^4 \pmod{34} = \\ &= 3^4 = 81 \equiv 13 \pmod{34}\end{aligned}$$

Portanto 13 é o resto da divisão de 3^{100} por 34.

4 DISCUSSÃO

Ao longo do trabalho estudamos congruências e divisibilidade sob a ótica do Pequeno Teorema de Fermat. A partir deste resultado obtemos apresentações de problemas da álgebra básica com maior elegância e precisão, além de possibilitar generalizações importantes.

5 CONSIDERAÇÕES FINAIS

O trabalho propiciou contato com algumas das técnicas comumente utilizadas em problemas introdutórios da teoria dos números, mais especificamente a análise de congruências. Como aplicações foram estabelecidas diversas congruências importantes, algumas delas de impacto para o desenvolvimento da Teoria dos Números.

A continuidade do estudo deste tema pode ser estendido a resultados com a função de Euler que visa generalizar o

Pequeno Teorema de Fermat para quaisquer números inteiros, utilizando, para isso a função φ de Euler, em consequência pode ser apresentado o funcionamento do método criptográfico RSA que, constitui uma aplicação extremamente poderosa desta teoria Matemática.

A sequência didática apresentada neste trabalho teve resultados de impacto motivador para o estudo da Matemática, desenvolvido com alunos do curso de Licenciatura em Matemática.

AGRADECIMENTOS

Os autores agradecem ao programa de Educação Tutorial (PET-MAT), o apoio financeiro.

REFERÊNCIAS

COUTINHO, Severino C., Números Inteiros e Criptografia RSA, Série Computação e Matemática, SBM, 1997.

DOMINGUES, Hygino H., Álgebra moderna, São Paulo: Atual, 2003.

HEFEZ, Abramo. Elementos de Aritmética. 2 ed. Rio de Janeiro, RJ: SBM, 2006. iv, 169. (textos universitários).

MARTINEZ, Fabio Brochero; et al. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro, 2 ed. Rio de Janeiro: IMPA, 2011

SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números. Rio de Janeiro, Instituto de Matemática Pura e Aplicada, CNPq, 1998.

SCHEINERMAN, Edward R. Matemática discreta: uma introdução. Tradução da 2. Ed. Norte americana. São Paulo: Cengage learning, 2011