UNIVERSIDADE FEDERAL DE SANTA CATARINA

DEPARTAMENTO DE MATEMÁTICA

André Walter

Divisibilidade e Congruência Modular

Florianópolis

2019

André Walter

Divisibilidade e Congruência Modular

Dissertação submetida ao Programa de Mestrado Profissional em Matemática em Rede Nacional- PROFMAT para a obtenção do Grau de Mestre em Matemática.

Orientadora: Profª. Drª. Maria Inez Cardoso Gonçalves.

Florianópolis

2019

Divisibilidade e Aritmética Modular

por

André Walter

Esta Dissertação foi julgada aprovada para obtenção do Título de "Mestre em Matemática", e aprovada em sua forma final pelo Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal de Santa Catarina.

_____

Profª. Drª. Maria Inez Cardoso Gonçalves (UFSC)
Coordenadora do Curso

Banca Examinadora:

_____

Profª. Drª. Maria Inez Cardoso Gonçalves
Orientadora – UFSC

_____

Prof. Dr. Danilo Royer.
UFSC

_____

Prof. Dr. Eduardo Tengan.
UFSC

_____

Prof. Dr. Eliezer Batista.
UFSC

Florianópolis, 18 de abril de 2019.

Se, porém, algum de vós necessita de sabedoria, peça-a a Deus, que a todos dá liberalmente e nada lhes impropera; e ser-lhe-á concedida.
Tiago 1:5.

AGRADECIMENTOS

Agradeço especialmente a Deus por ter me dado forças para chegar até aqui.

Agradeço à minha mãe, Vera Lucia que sempre me deu apoio para concluir o Mestrado.

A minha irmã Daniela, que emprestou o notebook para poder digitar essa dissertação.

Aos meus grandes amigos, Gustavo Alexandre Albano Carli e Anderson de Oliveira que desde a graduação se mostram grandes amigos.

Agradeço aos meus amigos Waldir de Souza, Giselle Martins, Ezequiel Onedi Debortoli e Luiz Arthur Dornelles Júnior por todos os momentos de descontração, estudos e aflições que passamos ao longo do curso.

Agradeço a professora e orientadora Maria Inez Cardoso Gonçalves por toda paciência que teve ao dirigir meus estudos e por toda contribuição.

RESUMO

Esta dissertação tem o intuito de abordar os tópicos mais elementares da Teoria dos Números, a Divisibilidade e a Congruência. Estes dois assuntos são ferramentas interessantes e poderosas na resolução de diversos problemas, que no decorrer do trabalho são apresentados. Por exemplo, as Equações Diofantinas Lineares e não Lineares. No último capítulo temos alguns problemas de vestibulares que envolvem os tópicos abordados nos capítulos anteriores.

Palavras-chave: Divisibilidade. Congruência. Equações Diofantinas.

ABSTRACT

This dissertation aims to address the most basic topics of Number Theory, Divisibility and Congruence. These two subjects are interesting and powerful tools in the resolution of several problems, which are presented in the course of the work, for example the Linear and Nonlinear Diophantine Equations. In the last chapter we have some entrance exam problems that involve the topics discussed in the previous chapters.

Keywords: Divisibility. Congruence. Diophantine Equations.

LISTA DE FIGURAS

Sumário

INTRODUÇÃO

A Teoria dos Números é um ramo da Matemática que se destina em grande parte ao estudo dos números inteiros. Segundo Terence Tao "A teoria dos números poderá não ser divina, mas há à sua volta uma aura de misticismo".

Neste trabalho, iremos considerar alguns resultados da Teoria dos Números, objetivando empregá-los na resolução de alguns problemas que envolvem divisibilidade, congruências e equações Diofantinas lineares e não lineares. Por isto, organizamos o trabalho na seguinte forma:

No Capítulo 1, apresentamos alguns resultados preliminares que serão usados ao longo do texto. Entre os quais destacamos aqueles relacionados à divisibilidade, sendo o Algoritmo da Divisão sua parte principal. Apresentamos também o conceito de máximo divisor comum entre dois inteiros, abordamos os números primos, dentre outras

definições importantes, e um resultado de extrema importância para a Matemática: o Teorema Fundamental da Aritmética. São apresentados exemplos para mostrar a aplicação desses assuntos na resolução de problemas.

Segundo a Proposta Curricular de Santa Catarina, publicada em 1º de agosto de 2008, o assunto de divisibilidade é apresentado no ensino fundamental no sexto ano. Devido à maturidade dos discentes o assunto é visto de uma forma mais superficial e depois não é mais visto no ensino regular. Esse assunto é riquíssimo, e deveria ser revisto no ensino médio de uma forma mais rigorosa e ampla.

No Capítulo 2, destacamos alguns conceitos e resultados de congruências. Aproveitamos esse capítulo para apresentar os Teoremas de Fermat e de Euler, que são dois Teoremas clássicos da Teoria das Congruências, bem como mostrar algumas aplicações desses e de outros resultados tão

relevantes. Esse tópico não está presente na Proposta Curricular de Santa Catarina de forma explicita, mas o professor tem a liberdade de cátedra de apresentar esse assunto de maneira bem natural e intuitiva aos discentes no momento que estiver trabalhando o assunto divisibilidade.

A aritmética modular é a aritmética dos fenômenos cíclicos, está presente na periodicidade dos dias da semana, no relógio entre outras aplicações do dia a dia do aluno. No Capítulo 3, destacamos algumas aplicações de divisibilidade e da aritmética modular na resolução de equações Diofantinas lineares e não lineares. Uma equação Diofantina é toda equação em várias variáveis com coeficientes inteiros. Por exemplo, $4x - 3y = 12$, $2^x = 1 + 3^y$ e $x^4 + 131 = 3y^4$, como veremos no decorrer do trabalho.

Esse tipo de problema foi abordado pelo matemático grego Diofanto em seu tratado Aritmética, escrito por volta de 250 d.C. Por este

motivo as equações deste tipo são chamadas de Diofantinas.

O estudo das Equações Diofantinas está longe de ser um assunto que se esgotou. Existem pesquisadores no Mundo inteiro que se dedicam a resolver estas equações. Por exemplo, no Brasil temos o professor Diego Marques, da Universidade de Brasília, na área de Teoria dos Números com ênfase em Equações Diofantinas e Teoria Transcendente dos Números, e o professor Hemar Teixeira Godinho, da Universidade de Brasília, que também é da área da Teoria dos Números com ênfase em Equações Diofantinas e Teoria Aditiva dos Números.

Por fim, no Capítulo 4, com o objetivo de destacar ainda mais a relevância dos tópicos apresentados neste trabalho na resolução de problemas, apresentamos uma coletânea de problemas de vestibulares, os quais são resolvidos usando-se os capítulos anteriores.

1 DIVISIBILIDADE

Este capítulo tem o intuito de apresentar vários resultados básicos, de extrema importância para a Teoria dos Números. Dentre eles destacamos o Teorema Fundamental de Aritmética e o Teorema de Bachet-Bézout.

Antes de iniciarmos este capítulo faremos uma pausa para fixar algumas notações que serão usadas ao longo deste trabalho.

Conjunto dos Números Naturais $\mathbb{N}$.

$\mathbb{N} = \{1,2,3, \dots\}$.

Conjunto dos Números Inteiros $\mathbb{Z}$.

$\mathbb{Z} = \{-3, -2, -1, 0, 1, 2 \dots\}$.

No conjunto dos números inteiros distinguimos dois subconjuntos:

Conjunto dos Números Inteiros não Negativos $\mathbb{Z}_+$.

$\mathbb{Z}_+ = \{0, 1, 2, 3, 4, \dots\} = \mathbb{N}$.

Conjunto dos Números Inteiros Não Negativos excluindo o zero $\mathbb{Z}_+^*$.

$\mathbb{Z}_+^* = \{1, 2, 3, 4, \ldots\}$.

Iniciamos esse capítulo, apresentando o princípio da Indução Finita, o qual será usado em diversas demonstrações ao longo do trabalho

1.1. PRINCÍPIO DE INDUÇÃO FINITA

Teorema 1. Princípio da Indução Finita.

Se $P(n)$ é uma proposição relativa ao número natural n, tal que

(i) $P(1)$ seja verdadeira;

(ii) Para todo $n \in \mathbb{N}$, se $P(n)$ é verdade, então $P(n+1)$ também é verdade.

Então $P(n)$ é verdadeira para todo número natural n.

Observação 1: O item (ii) do Teorema 1 é chamado de hipótese de indução.

Observação 2: A demonstração deste Teorema pode ser vista em [2] pág.15.

O exemplo a seguir foi extraído de [7], pág.8.

Exemplo 2. Usando o princípio da indução finita, mostre que para todo número natural $n \geq 1$, temos que:

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Demonstração:

Para $n = 1$, temos

$$1^2 = \frac{1(1+1)(2.1+1)}{6}.$$

Hipótese de Indução: Suponha que para $n = k$ o resultado seja verdadeiro, ou seja,

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}. \qquad (1)$$

Temos que provar que para $n = k + 1$, o resultado também é válido, ou seja, que

$$1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}.$$

Somando $(k+1)^2$ em ambos os lados de *(1),* vamos obter

$$1^2 + \cdots + k^2 + (k+1)^2 = \frac{k(k+1)(2k+1)}{6} + (k+1)^2.$$

Desenvolvendo o lado direito da expressão acima vamos obter

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2 =$$

$$= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} =$$

$$= \frac{(k+1)[(2k+1)k + 6(k+1)]}{6} =$$

$$= \frac{(k+1)(k+2)(2k+3)}{6}.$$

Portanto pelo Princípio de Indução Finita temos que

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

■

O exemplo a seguir foi extraído de [7], pág.8

Exemplo 3. Demonstre que $n^3 - n$ é múltiplo de 6 para $n \geq 1$ natural.

Demonstração:

Para $n = 1$, temos

$1^3 - 1 = 0$

Hipótese de indução: Suponha que para $n = k$ o resultado seja verdadeiro, ou seja

$k^3 - k = 6u, u \in \mathbb{N}.$

Temos que provar que para $n = k + 1$, o resultado é válido, ou seja, que $(k+1)^3 - (k+1)$ é múltiplo de 6. Para tanto, observe que para todo $k \in \mathbb{Z}$:

$$(k+1)^3 - (k+1) = k^3 + 3k^2 + 3k + 1 - k - 1 =$$

$$= k^3 + 3k^2 + 2k = \underbrace{k^3 - k}_{H.I} + k + 3k^2 + 2k =$$

$$= \underbrace{k^3 - k}_{H.I} + 3k^2 + 3k = \underbrace{k^3 - k}_{H.I} + 3k(k+1).$$

Como pela hipótese de indução $k^3 - k$ é múltiplo de 6 e como $k(k+1)$ é múltiplo de 2, temos que $3k(k+1)$ é múltiplo de 6. Assim, $k^3 - k + 3k(k+1)$ é múltiplo de 6.

Logo pelo Princípio de indução Finita temos que $n^3 - n$ é múltiplo de 6 para $n \geq 1$ natural.

■

1.2 DIVISIBILIDADE

Nesta seção veremos um dos tópicos mais básicos da Teoria dos Números, a divisibilidade. O qual será fundamental para o próximo capítulo.

Definição 4. Dados a e b pertencentes ao conjunto dos números inteiros com $a \neq 0$, dizemos a divide b ou que b é divisível por a, se o quociente b/a é um inteiro, ou seja, se existir um número inteiro m, tal que $b = ma$.

Quando a divide b usaremos a notação $a|b$, e quando a não divide b, usaremos a notação $a \nmid b$.

O próximo resultado será usado exaustivamente para resolvermos as equações Diofantinas não lineares no desenvolver do trabalho.

Proposição 5. Sejam a, b, c e d inteiros. Temos que:

(i) Se $d|a$ e $d|b$, então $d|(ax + by)$ para qualquer x e $y \in \mathbb{Z}$.

(ii) Se $d|a$, então $a = 0$ ou $|d| \leq |a|$.

(iii) Se $a|b$ e $b|c$, então $a|c$.

***Demonstração*:**

(i) Por hipótese temos que $d|a$ e $d|b$, então $a = dm_1$ e $b = dm_2$ com m_1 e $m_2 \in \mathbb{Z}$. Logo, substituindo $a = dm_1$ e $b = dm_2$ em $ax + by$, teremos que $ax + by = dm_1x + dm_2y = d(m_1x + m_2y)$ como $(m_1x + m_2y) \in \mathbb{Z}$, pela definição 1.1 temos que $d|ax + by$.

(ii) Suponha que $d|a$.

Se $a = 0$, nada a fazer, pois $d|0$, para todo $d \in \mathbb{Z}$.

Se $a \neq 0$, temos que $a = dv$ com $v \in \mathbb{Z}^*$, assim $|v| \geq 1$ e, portanto $|a| = |d||v| \geq |d|$.

(iii) Por hipótese temos que $a|b$ e $b|c$, então $b = an_1$ e $c = bn_2$ com n_1e $n_2 \in \mathbb{Z}$.

Assim,

$c = bn_2 = (an_1)n_2 = a(n_1n_2)$, e como $n_1n_2 \in \mathbb{Z}$ temos que $a|c$.

■

Exemplo 6. Encontre todo os inteiros positivos n tais que $(2n-1)|(n^3-1)$.

***Solução*:** Iremos utilizar repetidas vezes o item (i) da proposição 5 para reduzir o grau de (n^3-1).

Assuma que $(2n-1)|(n^3-1)$. Temos que

$(2n-1)|(2n-1)$, logo

$$(2n-1)|2.(n^3-1) - n^2.(2n-1),$$

ou seja,

$$(2n-1)|(n^2-2).$$

Assim, como $(2n-1)|(n^2-2)$ e $(2n-1)|(2n-1)$, temos que

$$(2n-1)|2.(n^2-2)-n.(2n-1),$$

ou seja,

$$(2n-1)|(n-4).$$

Usando o mesmo raciocínio, temos que

$$(2n-1)|((-2).(n-4)+1.(2n-1)),$$

ou seja,

$$(2n-1)|7.$$

Podemos utilizar a Proposição 5 item (ii) para obter os possíveis valores de n.

Se $(2n-1)|7$, então $2n-1 \leq 7 \Leftrightarrow n \leq 4$. Como n é um inteiro positivo, temos apenas 4 possibilidades,

$n = 1, 2, 3$ ou 4.

Para os valores de $n = 3$ e $n = 2$ o enunciado do problema não é satisfeito, apenas $n = 1\, e\, n = 4$ são soluções.

Para o próximo exemplo iremos apresentar três soluções. O exemplo a seguir foi extraído de [9], pág.58.

Exemplo 7. Demonstrar que a soma $S_n = n^3 + 3n^2 + 5n + 3$ é divisível por 3 para qualquer valor inteiro positivo de n.

Iremos apresentar três soluções para esse exemplo.

Solução 1:

Como $S_n = n^3 + 3n^2 + 5n + 3 =$

$$= 3(n^2 + n + 1) + n^3 + 2n,$$

nosso objetivo agora é provar que $n^3 + 2n$ é múltiplo de 3.

Todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $3\mathrm{k}$, $3\mathrm{k} + 1$, ou $3\mathrm{k} + 2$, onde $k \in \mathbb{Z}$.

Vamos analisar os três casos:

Se $n = 3k$, então

$n^3 + 2n = 27k^3 + 2.(3k) = 3(9k^3 + 2k)$,

ou seja, $n^3 + 2n$ é múltiplo de 3.

Se $n = 3k + 1$, então

$n^3 + 2n = (3k + 1)^3 + 2(3k + 1)$

$= 27k^3 + 9k^2 + 9k + 1 + 6k + 2$

$= 3(9k^3 + 3k^2 + 5k + 1)$, que também é múltiplo de 3.

Finalmente, se $n = 3k + 2$, então

$n^3 + 2n = (3k + 2)^3 + 2(3k + 2) =$

$= (3k + 2)(9k^2 + 12k + 6) =$

$= 3(3k + 2)(3k^2 + 4k + 2)$, que também é múltiplo de 3.

■

Solução 2:

Antes de darmos continuidade à solução, vamos enunciar e demonstrar um Lema, o qual será fundamental para a resolução do exemplo 1.5.

***Lema*:** O produto de três inteiros positivos consecutivos é múltiplo de 3.

***Demonstração*:** Considere $n, n+1$ e $n+2$ três inteiros positivos consecutivos. Queremos provar que $n(n+1)(n+2)$ é um múltiplo de 3.

Vamos utilizar o Princípio de Indução Finita.

Para $n = 1$, temos que

$1.(1+1)(1+2) = 6$, ou seja, $P(1)$ é verdadeira.

Hipótese de Indução: Agora suponha que para $n = k$, seja verdadeira, ou seja, que

$k(k+1)(k+2) = k^3 + 3k^2 + 2k$ é múltiplo de 3.

Queremos provar que para $n = k+1$ também teremos um múltiplo de 3, ou seja, que

$(k+1)(k+2)(k+3) = k^3 + 3k^2 + 2k +$
$3(2k^2 + 3k + 2)$ também é múltiplo de 3.

Mas, pela Hipótese de Indução $k^3 + 3k^2 + 2k$ é múltiplo de 3. Logo, $(k+1)(k+2)(k+3)$ também é múltiplo e 3.

Portanto para $n = k + 1$ é também verdadeira.

Pelo Princípio da Indução Finita, temos que o produto de três inteiros positivos consecutivos é múltiplo de 3. ■

Retomando ao exemplo 1.5, temos que

$S_n = n^3 + 3n^2 + 5n + 3$

$= n(n^2 + 3n + 2) + 3n + 3$

$= n(n+1)(n+2) + 3(n+1)$, pelo Lema anterior, $n(n+1)(n+2)$ é múltiplo de 3, logo

$S_n = n^3 + 3n^2 + 5n + 3$ é múltiplo de 3 para todo inteiro positivo n. ■

Solução 3:

Vamos utilizar o Princípio de Indução Finita.

Para $n = 1$, temos $S_n = 12$.

Hipótese de Indução: Suponha que $S_k = k^3 + 3k^2 + 5k + 3$ seja múltiplo de 3.

Temos que provar que para $n = k + 1$, o resultado é válido, ou seja, que

$S_{k+1} = (k+1)^3 + 3(k+1)^2 + 5(k+1) + 3$ é múltiplo de 3.

De fato, como

$$S_{k+1} = (k+1)^3 + 3(k+1)^2 + 5(k+1) + 3$$

$$= \underbrace{k^3 + 3k^2 + 5k + 3}_{hipotese\ de\ indução} + 3(k^2 + 3k + 3).$$

Temos que S_{k+1} também é múltiplo de 3. Portanto, usando o Princípio de Indução Finita, temos que $S_n = n^3 + 3n^2 + 5n + 3$ é múltiplo de 3 para todo n inteiro positivo. \■

O exemplo a seguir foi extraído de [8], pág.29.

Exemplo 8. Provar que não existe $n \in \mathbb{N}$ tal que $7|(4n^2 - 3)$.

Demonstração: Suponha que exista $n \in \mathbb{N}$ tal que $7|(4n^2 - 3)$.

Pela Proposição 5, item (i), como $7|(4n^2 - 3)$ e $7|7$, temos que $7|[2.(4n^2 - 3) - (n^2 + 1).7]$, ou seja, $7|(n^2 + 1)$.

Para que $7|(n^2 + 1)$, o resto da divisão de n^2 por 7 deve ser 6. Mas, podemos escrever n da seguinte maneira:

$$n = 7k + r, \text{ onde } k \in \mathbb{Z} \text{ e } 0 \leq r \leq 6.$$

A seguir, iremos analisando os 7 casos possíveis para os valores do resto.

1º caso: $r = 0$.

Neste caso $n = 7k$, o que implica que

$$n^2 = 49k^2 = 7.(7k^2).$$

2º caso: $r = 1$.

Portanto $n = 7k + 1$, o que implica que

$n^2 = 49k^2 + 14k + 1 = 7.(7k^2 + 2k) + 1.$

3º caso: $r = 2$.

Assim, $n = 7k + 2$, logo

$n^2 = 49k^2 + 28k + 4 = 7.(7k^2 + 4k) + 2.$

4º caso: $r = 3$.

$n = 7k + 3$, logo

$n^2 = 49k^2 + 42k + 9 = 7.(7k^2 + 6k + 1) + 2.$

5º caso: $r = 4$.

$n = 7k + 4$, então

$n^2 = 49k^2 + 56k + 16 = 7.(7k^2 + 8k + 2) + 2.$

6º caso: $r = 5$.

$n = 7k + 5$, ou seja:

$n^2 = 49k^2 + 70k + 2 = 7.(7k^2 + 10k + 3) + 4.$

7º caso: $r = 6$.

Assim, $n = 7k + 6$, o que implica que:

$$n^2 = 49k^2 + 84k + 36 = 7.(7k^2 + 12k + 5) + 1.$$

Portanto os possíveis restos na divisão de n^2 por 7 são $1, 2$, e 4. Logo a suposição da existência de $n \in \mathbb{N}$ tal que $7|(4n^2 - 3)$ é um absurdo.

Logo, não existe $n \in \mathbb{N}$ tal que $7|(4n^2 - 3)$.

■

Os próximos dois exemplos podem ser encontrados em, pág.51 e 52, respectivamente.

Exemplo 9. Mostre que para todo $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$,

$$(a - b)|(a^n - b^n).$$

Demonstração:

Para $n = 1$, temos que $(a - b)|(a - b)$.

Hipótese de Indução: Suponha que para $n = k$

$$(a - b)|(a^k - b^k).$$

Temos que provar que para $n = k + 1$,

$$(a - b)|(a^{k+1} - b^{k+1}).$$

Iremos reescrever $a^{k+1} - b^{k+1}$ de maneira que possamos aplicar a hipótese de indução.

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

Assim, $(a - b)|(a - b)$ e, pela hipótese de indução temos que $(a - b)|(a^k - b^k)$, logo $(a - b)|(a^{k+1} - b^{k+1})$.

Portanto pelo Princípio de Indução Finita temos que $(a - b)|(a^{k+1} - b^{k+1})$.

■

Exemplo 10. Mostre que para todo $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$,

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

Demonstração:

Para $n = 1$, temos $(a + b)|(a^2 - b^2)$.

Hipótese de Indução: Suponha que

$$(a + b)|(a^{2k} - b^{2k}).$$

Temos que provar que para $n = k + 1$,

$$(a + b)|(a^{2(k+1)} - b^{2(k+1)}).$$

Reescrevendo $a^{2(k+1)} - b^{2(k+1)}$, vamos obter

$$\begin{aligned} a^{2(k+1)} - b^{2(k+1)} &= a^{2k}a^2 - b^{2k}b^2 + b^{2k}a^2 - b^{2k}a^2 \\ &= a^2\left(\underbrace{a^{2k} - b^{2k}}_{HI}\right) + b^{2k}(a^2 - b^2). \end{aligned}$$

Portanto $a^{2(k+1)} - b^{2(k+1)}$ é múltiplo de $(a + b)$.

Logo, pelo Princípio de Indução Finita temos que $(a + b)|(a^{2n} + b^{2n})$. ■

Exemplo 11. Mostrar que se para algum $n \in \mathbb{N}$, $m|(35n + 26)$ e $m|(7n + 3)$ e $m > 1$, então $m = 11$.

Solução: Iremos aplicar a Proposição 5, item (i)

Como $m|(35n + 26)$ e $m|(7n + 3)$, temos que

$$m|[(35n + 26) - 5(7n + 3)],$$

ou seja, $m|11$.

Como $m > 1$, temos então que $m = 11$.

■

O Teorema a seguir apareceu no livro VII dos "Elementos" de Euclides, escrito por volta do ano 300 a.C.

Teorema 12. Divisão Euclidiana

Sejam a e b dois números inteiros com $b \neq 0$. Então, existem dois únicos inteiros q e r tais que

$$a = bq + r, \text{ com } 0 \leq r < |b|.$$

Observação: Sua demonstração pode ser consultada na página 18 de [7].

Teorema 13. (Teorema dos Restos) Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:

(i) b_1 + b_2 deixa o mesmo resto que r_1 + r_2 na divisão por a,

(ii) $b_1 b_2$ deixa o mesmo resto que $r_1 r_2$ na divisão por a.

Demonstração:

(i) Temos por hipótese, que existem q_1 *e* $q_2 \in \mathbb{Z}$ tais que $b_1 = aq_1 + r_1, b_2 = aq_2 + r_2$ e $r_1 + r_2 = aq + r$, logo:

$$b_1 + b_2 = a\,(q_1 + q_2 + q) + r.$$

Como $0 < r < |a|$, temos que $b_1 + b_2$ deixa resto r quando dividido por a.

(ii) Por hipótese, existem q_1 *e* $q_2 \in \mathbb{Z}$ tais que $b_1 = aq_1 + r_1$, $b_2 = aq_2 + r_2$ e $r_1 . r_2 = aq_3 + r_3$, logo:

$$b_1 . b_2 = a\,(aq_1q_2 + q_1r_2 + r_1q_2 + q_3) + r_3.$$

Como $0 < r_3 < |a|$, temos que o resto da divisão de $b_1 b_2$ por a é r. ■

1.3 MÁXIMO DIVISOR COMUM

Definição 14. Sejam $a, b \in \mathbb{Z}$, com pelo menos um deles diferente de zero. O máximo divisor comum de a e b, denotado por (a, b), é um inteiro positivo d tal que:

(i) $d|a$ e $d|b$;

(ii) se $c \in \mathbb{Z}$ é tal que $c|a$ e $c|b$, então $c|d$.

Se o $(a, b) = 1$, então dizemos que a e b são primos entre si ou que são relativamente primos.

Convencionamos que $(0,0) = 0$.

Teorema 15. Se a e b são inteiros e $a = qb + r$ onde q e r são inteiros, então $(a, b) = (b, r)$.

Observação: A demonstração do Teorema acima pode ser encontrada em [7], página 19.

O próximo resultado fornece uma maneira de determinar o máximo divisor comum sem precisar fatorar os números. Geralmente os livros didáticos do ensino fundamental não trazem esse resultado.

Lema 16. (Lema de Euclides) Sejam $a, b\ e\ n \in Z$, então: $(a, b) = (a, b - na)$

Demonstração: Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, temos que $b = b - na + na$. Portanto, d é um divisor comum de a e b. Suponha agora que c c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c|d$. Com isso temos que $d = (a, b)$.

■

O resultado abaixo possui um papel relevante na teoria de Equações Diofantinas Lineares, sua demonstração pode ser consultada na página 108 de [11].

Teorema 17. (Bachet-Bézout): Seja d o máximo divisor comum de a e b. Então existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.

Observação 1: O máximo divisor comum é o menor valor positivo dentre todas as combinações lineares do tipo $d = ax_0 + by_0$.

Os exemplos abaixo mostram uma maneira bastante eficiente de determinar o máximo divisor comum sem precisar encontrar a fatoração em números primos, o que é interessante especialmente quando tratamos de números "grandes".

Exemplo 18. Encontrar o Máximo Divisor Comum do seguinte par de números:

$$1268 \text{ e } 948$$

Soluções: Será aplicado o Lema de Euclides para encontrar o máximo divisor comum.

$(1268, 948) =$

$= (1268 - 948, 948) =$

$= (320, 948) =$

$= (320, 948 - 2(320)) =$

$= (320, 308) =$

$= (320 - 308, 308) =$

$= (12, 308) =$

$= \big(12, 308 - 25(12)\big) =$

$= (12, 8) =$

$= (12 - 8, 8) =$

$= (4, 8) =$

$= (4, 8 - 2(4)) =$

$= (4, 0) = 4.$

Exemplo 19. Seja $a \in \mathbb{Z} - \{-1\}$.

a) Se $m \in \mathbb{N}$, mostre que

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

***Solução*:**

$$\frac{a^{2m} - 1}{a + 1} = a^{2m-1} - a^{2m-2} + a^{2m-3} - \cdots + a^3 +$$

$$-a^2 + a - 1 =$$

$$= (a^{2m-1} + 1) - (a^{2m-2} - 1) + (a^{2m-3} + 1) -$$

$\ldots + (a^3 + 1) - (a^2 - 1) + (a + 1) - 2m + 1 - 1$

$= (a + 1)q - 2m$, onde $q \in \mathbb{Z}$.

Pelo Lema de Euclides temos que:

$\big((a + 1)q - 2m, a + 1\big) = (2m, a + 1)$.

b) Seja $m \in \mathbb{N} \cup \{0\}$. Mostre que

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

Solução:

$$\frac{a^{2m+1} + 1}{a + 1} = a^{2m} - a^{2m-1} + a^{2m-2} - \cdots + a^2$$

$-a + 1 =$

$= (a^{2m} - 1) - (a^{2m-1} + 1) + (a^{2m-2} - 1) - \cdots$

$+(a^2 - 1) - (a + 1) + 2m + 1 =$

$= (a + 1)q + 2m + 1.$

Pelo Lema de Euclides temos que:

$\big((a + 1)q + 2m + 1, a + 1\big) = (2m + 1, a + 1)$.

O exemplo a seguir foi extraído de [2], pág.93.

Exemplo 20. Calcule:

$a)\ \left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right).$

$b)\ \left(\frac{2^{40}+1}{2^8+1}, 2^8+1\right).$

***Soluções*:** a) Inicialmente iremos fazer $3^5 = a$. Então

$$\left(\frac{3^{40}-1}{3^5-1}, 3^5-1\right) = \left(\frac{a^8-1}{a-1}, a-1\right).$$

Reescrevendo a expressão $\frac{a^8-1}{a-1}$, temos

$$\frac{a^8-1}{a-1} = a^7+a^6+a^5+a^4+a^3+a^2+a+1.$$

$$a^7+a^6+a^5+a^4+a^3+a^2+a+1 =$$

$$(a^7-1)+(a^6-1)+(a^5-1)+(a^4-1)+$$

$$+(a^3-1)+(a^2-1)+(a-1)+8.$$

Pelo Exemplo 9,

$(a-b)|(a^n-b^n)$ para todo $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$.

Assim,

$$(a^7-1)+(a^6-1)+(a^5-1)+(a^4-1)+$$

$$+(a^3-1)+(a^2-1)+(a-1)+8=$$

$$(a-1).k+8, \quad k \in \mathbb{Z}.$$

Pelo Lema de Euclides temos que

$$\big((a-1)k+8, a-1\big) = (8, a-1) = (8, 242)$$

$$= (8, 242-30.8) = (8, 2) = 2.$$

b) Fazendo $2^8 = a$, então

$$\left(\frac{2^{40}+1}{2^8+1}, 2^8+1\right) = \left(\frac{a^5+1}{a+1}, a+1\right).$$

Reescrevendo a expressão $\frac{a^5+1}{a+1}$, temos

$$\frac{a^5+1}{a+1} = (a^4-a^3+a^2-a+1).$$

$$a^4-a^3+a^2-a+1=$$

$$=(a^4-1)-(a^3+1)+(a^2-1)-(a+1)+5$$

$= (a + 1)n + 5, n \in \mathbb{Z}.$

Agora iremos aplicar o Lema de Euclides para encontrar o máximo divisor comum

$$\big((a + 1)n + 5, a + 1\big) = (5, a + 1) = (5, 257)$$

$$= (5, 2) = 1.$$

Exemplo 21. Para $n \in \mathbb{N}$, prove que

$$(21n + 4,14n + 3) = 1.$$

Solução: Pelo Lema de Euclides temos que:

$$\begin{aligned}(21n + 4,14n + 3) = \\ &= (21n + 4 - 14n - 3,14n + 3) \\ &= (7n + 1,14n + 3) \\ &= (7n + 1,14n + 3 - 14n - 2) = \\ &= (7n + 1, 1) = 1.\end{aligned}$$

O exemplo a seguir foi extraído de [8], pág.31.

Exemplo 22. Encontrar o menor inteiro positivo da forma $36x + 54y$ onde x e y são inteiros.

Solução: Pelo Teorema de Bachet-Bézout, sabemos que o menor valor inteiro positivo da forma $ax + by$ é dado por (a, b). Assim, basta encontrar (36,54).

Pelo Lema de Euclides temos $(36{,}54) = (36{,}18) = (0{,}18) = 18$. Logo, o menor valor da expressão é 18.

1.4 NÚMEROS PRIMOS E COMPOSTOS

"2, 3, 5, 7, 11, 13, ... Esses são os primos, os números indivisíveis que são os blocos de construção de todos os outros números – o hidrogênio e o oxigênio do mundo da matemática."

[Sautoy 2013, pág.13].

Definição 23. Um número inteiro positivo maior que um é dito um número primo, se possuir exatamente dois divisores positivos, ele mesmo e 1.

Se $n > 1$ não é primo dizemos que n é composto.

Observação: O número 1 não é nem primo e nem composto, por convenção.

Teorema 24. Se $a|(b.c)$ e $(a,b)=1$, então $a|c$.

***Demonstração*:** Como $(a,b)=1$ pelo Teorema 17, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = 1$. Multiplicando ambos os lados desta igualdade por c, temos:

$c = x_0(ac) + y_0(bc)$. Como $a|ac$ e, por hipótese $a|(b.c)$, então, $bc = ak$, para algum $k \in \mathbb{Z}$. Assim, c pode ser escrito como: $c = a(cx_0 + y_0k)$, o que implica que $a|c$.

■

Proposição 25. Um número inteiro positivo é primo se, e somente se, satisfaz a seguinte propriedade:

Se $p|ab$, então $p|a$ ou $p|b$. *(1)*

onde a e b são inteiros.

***Demonstração**:* Suponha primeiramente que p é primo e que $p \nmid b$, logo $(p,b)=1$. Então, pelo Teorema 24 temos que $p|a$.

Reciprocamente, suponhamos que a propriedade *(1)* é válida e além disso vamos supor por absurdo que p não é um número primo. Então,

$p = u.v$, com $1 < u < p, 1 < v < p$. *(2)*

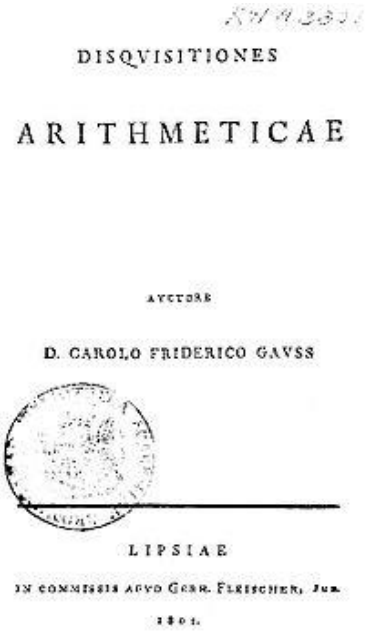
De *(2)* segue que $p|u$ ou $p|v$; consequentemente

$p \leq u$, ou $p \leq v$, contradizendo *(2).*

Logo, temos que p é um número primo.

■

O próximo Teorema é um resultado muito relevante para a matemática. A sua publicação apareceu no livro "Os Elementos" de Euclides, mas a sua demonstração completa e correta foi dada por Carl Friedrich Gauss e publicada na sua obra Disquisitiones Arithmeticae em 1801.



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, JUN.

1801.

FIGURA 1 PÁGINA TÍTULO DA PRIMEIRA EDIÇÃO

Teorema 26.

(Teorema Fundamental da Aritmética): Todo número inteiro maior que 1 pode ser representado de maneira única (a menos de ordem) como um produto de fatores primos.

Observação: Sua demonstração pode ser consultada na página 25 de [7].

Os quatro exemplos a seguir utilizam os resultados apresentados na secção 1.4.

Exemplo 27. Mostre que além de $2 = 1^3 + 1$ nenhum número da forma $n^3 + 1$ é primo.

Solução: Vamos provar que $n^3 + 1$ é um número composto para todo $n > 1$.

Como $n^3 + 1 = (n + 1)(n^2 - n + 1)$, então se $n > 1$ temos que $(n + 1)$ é maior ou igual a 2 e

$n^2 - n + 1$ é igual a 1 somente para os valores de $n = 0\ e\ n = 1$.

Logo, para todo $n > 1$, $n^3 + 1$ é sempre um número composto.

Exemplo 28. Mostrar que 3 é o único número primo p, tal que $p, p + 2$ e $p + 4$ são todos primos.

Solução: Se p for da forma $3k$, então $p = 3$.

Para $p = 3$, teremos a sequência 3, 5 e 7, os quais são números primos.

Se p for da forma $3k + 1$, teremos a sequência $3k + 1$, $3k + 3$ e $3k + 5$.

Note que $3k + 3$ é um número composto, pois $3|3k + 3$.

Logo, p não pode ser da forma $3k + 1$.

Se p for da forma $3k + 2$, teremos $3k + 2$,$3k + 4$ e $3k + 6$.

Mas, $3k + 6$ é um número composto, pois $3|3k + 6$.

Assim, $p = 3$ é o único número primo p tal que p, $p + 2$ e $p + 4$ são todos primos.

■

Exemplo 29. Mostrar que para $n \in \mathbb{N} - \{1\}$ os números $n^4 + 4$ e $n^4 + n^2 + 1$ são, ambos compostos.

Solução: Iremos fatorar as expressões $n^4 + 4$ e $n^4 + n^2 + 1$. Para tanto, necessitamos da Identidade de *Sophie Germain* para fatorar a expressão $n^4 + 4$.

Identidade de *Sophie Germain:* Dados $a, b \in \mathbb{R}$, vale a igualdade:

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab).$$

Logo a fatoração de $n^4 + 4$ será

$$n^4 + 4 = (n^2 + 2n + 2)(n^2 - 2n + 2).$$

Temos que,

$n^2 + 2n + 2 = (n + 1)^2 + 1 > 1$ e que

$n^2 - 2n + 2 = (n - 1)^2 + 1 > 1.$

Portanto temos que $n^4 + 4$ é composto.

A seguir iremos fatorar a expressão $n^4 + n^2 + 1$.

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

Como $n > 1$, temos que

$$n^2 - n + 1 = n(n-1) + 1 > 1.$$

e $n^2 + n + 1 > 1$, logo, $n^4 + n^2 + 1$ é composto.

■

O exemplo a seguir foi extraído de [4], pág.7.

Exemplo 30. Sejam a e n inteiros, com $a > 1$. Mostre que:

(i) Se $a^n + 1$ é primo, então n é uma potência de 2.

(ii) Se $n > 1$ e $a^n - 1$ é primo, então n é primo e $a = 2$.

***Solução**:*

(i) Suponha por absurdo que n não seja uma potência de 2. Podemos escrever $n = 2^c.u$, onde $u \geq 0$ impar e $c \geq 0$.

$$(a^{2^c})^u + 1 = (a^{2^c} + 1)(a^{(u-1)2^c} - a^{(u-2)2^c} + \cdots + 1).$$

Logo $(a^{2^c})^u + 1$ é um número composto.

Chegamos a uma contradição. Portanto n é uma potência de 2.

(ii) Fatorando a expressão $a^n - 1$, obtemos

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

Como o fator $a^{n-1} + a^{n-2} + \cdots + a + 1 > 1$ e $a^n - 1$ é um número primo, temos que $(a - 1) = 1$. Logo, $a = 2$.

Se n não for um número primo, então n é da forma $n = uv$, onde u e v são maiores que 1. Fatorando $2^{uv} - 1$, vamos obter

$$2^{uv} - 1 = (2^u - 1)(2^{u(v-1)} + 2^{u(v-2)} + \cdots + 2^u + 1).$$

As duas parcelas da fatoração são maiores que 1 e isso contradiz a hipótese de ser um número primo. Portanto n é um número primo

■

Curiosidades: Os primos da forma do item (i) são denominados **Primos de Fermat** e os números primos da forma que aparecem no item (ii) são chamados de **Primos de Mersenne**.

2. CONGRUÊNCIA

Carl Friedrich Gauss foi responsável por introduzir o conceito, e a notação de congruência na Teoria dos Números na sua obra "Disquisitiones Arithmeticae".

FIGURA 2 CARL FRIEDRICH GAUSS

Euler, em 1750 já tinha introduzido o conceito de congruência, mas essa obra só foi publicada em 1849.

A Teoria de Congruência Modular permeia a Teoria dos Números em diversos assuntos.

Definição 31. Sejam a, b e m inteiros, com $m > 1$. Dizemos que a é congruente a b, módulo m, se

$m|(a - b)$ e neste caso usamos a notação

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

Podemos dizer de forma equivalente que a e b deixam o mesmo resto na divisão por m.

De fato, se a deixar resto r_1 por m podemos escrever que $a = mq_1 + r_1$, $0 \leq r_1 < m$ e $q_1 \in \mathbb{Z}$.

De forma análogo se b deixar resto r_2 por m podemos escrever que $b = mq_2 + r_2$, $0 \leq r_2 < m$ e $q_2 \in \mathbb{Z}$.

Fazendo $(a-b)$ temos $mq_1 + r_1 - mq_2 - r_2 = m(q_1 - q_2) + (r_1 - r_2)$. Note que o resto da divisão de $(a-b)$ por m é $(r_1 - r_2) = 0$.

Logo o resto da divisão de a e b por m são iguais.

Se $m \nmid (a-b)$ dizemos que a é incongruente a b modulo m e usamos a notação $a \not\equiv b\ (mod\ m)$.

Proposição 32. Dados inteiros a, b, c e m, sendo $m > 1$, temos:

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

(ii) (Simetria)$a \equiv b\ (mod\ m) \Longrightarrow b \equiv a(mod\ m\ )$,

(iii) (Transitividade) $a \equiv b\ (mod\ m)$ e

$b \equiv c\ (mod\ m) \Longrightarrow a \equiv c\ (mod\ m)$.

Demonstração:

(i) Como $m|0$, então $m|(a-a)$, o que implica

$a \equiv a\ (mod\ m)$.

(ii) Se $m \mid (b - a)$, então $m \mid (a - b)$, pois $a - b = -(b - a)$.

(iii) Se $m \mid (b - a)$ e $m \mid (c - b)$, então $m \mid (c - a)$, pois $c - a = (c - b) + (b - a)$.

■

Proposição 33. Se $a, b, c,$ e m *s* ão inteiros, com $m > 1$, tais que $a \equiv b \ (mod\ m)$, então

$(i)\ (a + c) \equiv (b + c)\ (mod\ m)$;

$(ii)\ (a - c) \equiv (b - c)\ (mod\ m)$;

$(iii)\ ac \equiv bc\ (mod\ m)$;

Demonstração: (i) Por hipótese temos que $m \mid (a - b)$. Logo, existe um $q \in \mathbb{Z}$ tal que $(a - b) = (a + c) - (b + c) = m.q$. Logo $(a + c) \equiv (b + c)\ (mod\ m)$.

(ii) Por hipótese temos que $m \mid (a - b)$. Logo, existe um $q \in \mathbb{Z}$ tal que $(a - b) = (a - c) - (b - c) = m.q$. Portanto $(a - c) \equiv (b - c)\ (mod\ m)$.

(iii) Por hipótese temos que $m|(a-b)$, logo, existe um $q \in \mathbb{Z}$, tal que $a-b=m.q$.

Multiplicando por c a última equação em ambos os membros iremos obter $(ca-cb)=mcq$ o que implica que $m|(ac-cb)$ e, portanto $ac \equiv bc\ (mod\ m)$. ■

Proposição 34. Sejam $a,b,c,d,m,n \in \mathbb{Z}$, com $m,n>1$.

(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 $ac \equiv bd\ (mod\ m)$,

(iii) Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então $(a-c) \equiv (b-d)(mod\ m)$,

(iv) Se $a \equiv b\ (mod\ n)$ e $a \equiv b\ (mod\ m)$, com $(n,m)=1$, então $a \equiv b\ (mod\ (n.m))$.

Observação: A demonstração da Proposição 34 será omitida, porém pode ser encontrada na página 120 de [4].

Corolário 35. 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 demonstração do corolário será feita usando Indução Finita.

Para $n = 1$, temos $a \equiv b\ (mod\ m)$ por hipótese.

Hipótese de Indução: Agora suponha que para $n = k$ o resultado seja verdadeiro, ou seja, $a^k \equiv b^k\ (mod\ m\ )$.

Temos que provar que para $n = k + 1$, o resultado é válido, ou seja, que $a^{k+1} \equiv b^{k+1}\ (mod\ m\ )$.

Por hipótese temos que: $a \equiv b\ (mod\ m)$ e pela hipótese de indução que: $a^k \equiv b^k\ (mod\ m\ )$.

Pela Proposição 34. item (ii) e pela transitividade temos que: $a^{k+1} \equiv b^{k+1}\ (mod\ m\ )$. Portanto pelo Princípio de Indução Finita temos a validade do Corolário.

■

Proposição 35. Sejam $a, b, c, m\ \in \mathbb{Z}, com\ m > 1$ e $(m, c) = d$. Então

$$ac \equiv bc\ (mod\ m\ ) \Leftrightarrow a \equiv b\ \left(mod \frac{m}{d}\right).$$

Demonstração: Como $\left(\frac{m}{d}\right)$ e $\left(\frac{c}{d}\right)$ são primos entre si, temos que

$$ac \equiv bc\ (mod\ m\ ) \Leftrightarrow m|(b-a)c \Leftrightarrow \left(\frac{m}{d}\right)|(b-a)\left(\frac{c}{d}\right) \Leftrightarrow \left(\frac{m}{d}\right)|(b-a) \Leftrightarrow a \equiv b\ \left(mod\ \left(\frac{m}{d}\right)\right).$$

■

A próxima Proposição será muito útil para facilitar na resolução de alguns problemas. Os exemplos 58, 59 e 62 do Capítulo 3 são aplicações desse

resultado, sua demonstração pode ser consultada na página 124 de [4].

Proposição 36. Para todo $a \in \mathbb{Z}$ temos que:

(i) $a^2 \equiv 0, 1, 4, 5, 6$ ou 9 $(mod 10)$.

(ii) $a^2 \equiv 0$ ou 1 $(mod 3)$.

(iii) $a^2 \equiv 0$ ou 1 $(mod 4)$.

(iv) $a^2 \equiv 0, 1$ ou 4 $(mod 8)$.

(v) $a^4 \equiv 0$ ou 1 $(mod 16)$.

Pequeno Teorema de Fermat

Pierre de Fermat expressou em carta ao matemático Bernard Frenicle de Bessey que tinha criado um "pequeno Teorema de Fermat", capaz verificar se um número é ou não primo.

A primeira prova do chamado "pequeno Teorema de Fermat" foi dada por Leonhard Euler e levou quase cem anos para ser divulgada. Leonhard Euler publicou em 1736.

FIGURA 3 PIERRE DE FERMAT

O próximo resultado será útil para conseguirmos provar o Pequeno Teorema de Fermat.

Lema 37. Seja p um número primo e a um número inteiro. Então, $(a+1)^p \equiv (a^p+1)\ (mod\ p)$.

***Demonstração*:**

Temos que provar que $p|[(a+1)^p - (a^p+1)]$.

Pelo Teorema Binomial temos que:

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

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

Note que é suficiente provar que

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} \equiv 0 \ (mod\ p).$$

Considere o fator Binomial $\binom{p}{i} = \frac{p!}{i!(p-i)!} \in \mathbb{Z}$

Iremos provar que ele é múltiplo de p.

Temos que $1 \leq i \leq p-1$. Então o denominador $i!$ não possui o fator primo p. Portanto o fator p que está no numerador não será cancelado por nenhum fator do denominador. Logo

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

é múltiplo de p. Consequentemente

$$\sum_{i=1}^{p-1} \binom{p}{i} a^{p-i} \equiv 0 \ (mod\ p).$$

■

Teorema 38. (Pequeno Teorema de Fermat)

Para $a, p \in \mathbb{Z}$, com p primo, temos

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

***Demonstração*:**

Iremos utilizar o Princípio de Indução Finita em $a \in \mathbb{N}$.

Para $a = 1$, temos trivialmente que $1^p \equiv 1 \ (mod\ p)$, pois $p|(1^p - 1)$.

Hipótese de Indução: Suponhamos que para $a = k$ a afirmação seja verdadeira, ou seja,

$$k^p \equiv k \ (mod\ p).$$

Precisamos provar a partir da hipótese de indução e do Lema 37, que para $a = k + 1$,

$$(k+1)^p \equiv (k+1)\ (mod\ p).$$

Usando o Lema 37, temos que $(k+1)^p \equiv (k^p + 1^p)$, ou seja, $(k+1)^p \equiv (k^p+1)\ (mod\ p)$. Como pela hipótese de indução $k^p \equiv k\ (mod\ p)$, obtemos

$$(k+1)^p \equiv (k+1)\ (mod\ p).$$

Logo pelo Princípio de Indução Finita o teorema fica provado para o caso onde a é um numero natural.

Agora vamos provar o caso onde a é um número inteiro negativo e p é ímpar. Então $-a$ é positivo e assim podemos usar o resultado já provado, ou seja,

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

Como p é impar, temos que $(-a)^p = -a^p$, e

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

Multiplicando ambos os membros da congruência por -1, concluímos que $a^p \equiv a\ (mod\ p)$.

Agora só nos resta provar o caso onde $p = 2$.

$a^2 \equiv a\ (mod\ 2) \Leftrightarrow 2|a(a-1)$, que obviamente é verdade.

Assim provando o Pequeno Teorema de Fermat.

■

Teorema de Euler-Fermat

A Função φ de Euler foi introduzido pelo matemático suíço Leonhard Euler (1707-1783). Ela será importantíssima para o Teorema de Euler-Fermat.

Definição 39. Função φ de Euler

A função $\varphi: \mathbb{N}^* \longrightarrow \mathbb{N}^*$ que associa cada $m \in \mathbb{N}^*$ ao número de elementos do conjunto $\{k \in \mathbb{N}^* | 1 \leq k \leq m\ e\ (k,m) = 1\}$ é chamada função φ de Euler.

Exemplos.

$(a)\ \varphi(2) = 1,$

$(b)\ \varphi(6) = 2,$

$(c)\ \varphi(p) = p - 1,$ se p é um número primo.

Teorema 40. Para um número primo p e a um inteiro positivo temos

$$\varphi(p^a) = p^a - p^{a-1}.$$

Demonstração: Procuramos a quantidade de números de 1 até p^a que são relativamente primos com p^a. De 1 até p^a existem p^a números, e devemos retirar a quantidade de múltiplos de p.

Afirmação: O número de múltiplos de p que estão no intervalo de 1 até p^a é p^{a-1}.

De fato, os múltiplos de p são precisamente $p, 2p, 3p, \dots, p^{a-1}.p$.

Logo,

$$\varphi(p^a) = p^a - p^{a-1}.$$

■

Teorema 41 Sejam m e n números naturais tais que $(m, n) = 1$. Então

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

Observação: A demonstração do teorema acima pode ser encontrada na página 172 de [6].

Teorema 42. Seja $m > 1$ e seja $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ a decomposição de m em fatores primos.

Então,

$$\varphi(m) = p_1^{\alpha_1} \dots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_n}\right).$$

Observação: Sua demonstração pode ser consultada na página 73 de [8].

O próximo Teorema torna o Pequeno Teorema de Fermat um caso particular.

Teorema 43. (Teorema de Euler-Fermat)

Sejam $m, a \in \mathbb{Z}$ com $m \geq 1$ e $(a, m) = 1$. Então,

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

Observação: Sua demonstração pode ser consultada na página 43 de [8].

Teorema de Wilson

O matemático Edward Waring publicou em 1770 um tratado sobre Teoria dos Números chamado de *Meditationes Algebricae,* no qual incluía um resultado que lhe fora comunicado por um dos seus alunos, John Wilson, segundo o qual todo número primo p divide o número $(p-1)!+1$.

Este Teorema atribuído ao inglês John Wilson (1741- 1793), mas que foi demonstrado pela primeira vez por Joseph Louis Lagrange $(1730-1813)$.

FIGURA 4 JOHN WILSON

Antes de provarmos o Teorema de Wilson precisamos de dois Lemas auxiliares.

Lema 44. Seja $p > 2$ um inteiro primo. Os únicos elementos do conjunto $R = \{1, 2, 3, \ldots, p-1\}$ que verificam a equação $x^2 \equiv 1\ (mod\ p)$ são 1 e $p - 1$.

Demonstração: Seja $m \in R$ tal que a equação $m^2 \equiv 1\ (mod\ p)$ seja verdadeira, ou de forma equivalente tal que

$$p|(m^2-1) \Leftrightarrow p|[(m-1).(m+1)].$$

Como p é primo, então $p|(m-1)$ ou $p|(m+1)$.

Se $p|(m-1)$ então $m=1$ ou $m-1 \geq p \Leftrightarrow m \geq p+1$. Logo o único valor possível para m é 1.

Se $p|(m+1)$ então $m=-1$ ou $m+1 \geq p \Leftrightarrow m \geq p-1$. Assim, o único valor possível para m é $p-1$.

Portanto, $m=1$ ou $m=p-1$ como queríamos provar. ■

Lema 45. Seja $p>2$ um inteiro primo.

Consideremos o conjunto $R = \{2,\ldots,p-2\}$.

Para cada elemento $c \in R$ existe um único número $a \in R$ tal que $c.a \equiv 1\ (mod\ p)$,com $a \neq c$.

Observação: Sua demonstração pode ser encontrada na página 18 de [10].

Teorema 46. (Teorema de Wilson)

Seja p um número primo. Então

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

Demonstração: Para $p = 2$ e $p = 3$ o resultado é verdadeiro.

De fato, pois para $p = 2$, temos

$$(2-1)! \equiv -1\ (mod\ 2) \Leftrightarrow 2|(2-1)! + 1 \Leftrightarrow 2|2$$

e para $p = 3$, temos

$$(3-1)! \equiv -1\ (mod\ 3) \Leftrightarrow 3|(3-1)! + 1 \Leftrightarrow 3|3.$$

Para $p \geq 5$, consideremos o conjunto

$$A = \{2, 3, 4, \dots, p-2\}.$$

O conjunto A tem $p - 3$ elementos, e pelos Lema 44 e 45 para cada elemento $c \in A$ existe um único um número $a \neq c \in A$ tal que $c.a \equiv 1\ (mod\ p)$

Logo podemos concluir que

$$2.3.4 \dots p-2 \equiv 1\ (mod\ p). \qquad 1.2.1$$

A congruência abaixo é óbvia, mas relevante para a demonstração

$$p-1 \equiv -1\ (mod\ p). \qquad 2.2.1$$

Portanto de *(1.2.1)* e *(2.2.1)* e pela Proposição 34 chegamos em

$$2.3.4. \ldots, .(p-2).(p-1) \equiv -1.1 \ (mod\ p)$$

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

■

Recíproca do Teorema de Wilson

Seja $p \geq 2$ um inteiro. Se $(p-1)! \equiv -1(\ mod\ p)$, então p é primo.

Observação: Sua demonstração pode ser consultada na página 240 de [2].

Exemplo 47. Mostre que $47|(2^{23}-1)$.

Solução: Mostrar que $47|(2^{23}-1)$ é equivalente a mostrar que $2^{23} \equiv 1 \ (mod\ 47)$.

Inicialmente observe que $2^7 \equiv -13 \ (mod\ 47)$.

Pelo Corolário 35 podemos elevar em ambos os membros da congruência ao quadrado, obtendo

$$2^{14} \equiv (-13)^2 \equiv -19\ (mod\ 47).$$

Pela Proposição 34 item (ii) concluímos que

$$2^{21} = 2^7.2^{14} \equiv (-13).(-19)\ (mod\ 47).$$

Pela Proposição 33 item (iii) podemos multiplicar por 2^2 em ambos os lados dessa congruência, obtendo

$$2^{23} = 2^2.2^7.2^{14} \equiv (-13).(-19).4$$
$$\equiv 1\ (mod\ 47).$$

Portanto $47|(2^{23} - 1)$.

O exemplo a seguir foi extraído de [3], pág.94.

Exemplo 48. Mostre que $2^{70} + 3^{70}$ é múltiplo de 13.

Solução:

Como $(2,13) = 1$ e 13 é um número primo, então podemos utilizar o Pequeno Teorema de Fermat. Assim temos que

$$2^{12} \equiv 1\ (mod\ 13).$$

Pelo Corolário 35 podemos elevar em ambos os membros da congruência por 5, obtendo

$(2^{12})^5 \equiv 1^5 \ (mod\ 13)$, ou seja,

$2^{60} \equiv 1 \ (mod\ 13)$,

Pela Proposição 33 item (iii) podemos multiplicar por 2^{10} ambos os lados dessa congruência.

$2^{10}.2^{60} \equiv 1.2^{10} \ (mod\ 13)$

Logo $2^{70} \equiv 2^{10} \ (mod\ 13)$

Agora vamos achar o resto da divisão de 3^{70} por 13.

Como $(3{,}13) = 1$ e 13 é um número primo, novamente podemos utilizar o Pequeno Teorema de Fermat, obtendo que

$$3^{12} \equiv 1 \ (mod\ 13).$$

Pelo Corolário 35 podemos elevar em ambos os membros da congruência por 5.

$(3^{12})^5 \equiv 1^5 \ (mod\ 13)$, ou seja, $3^{60} \equiv 1 \ (mod\ 13)$.

Precisamos saber primeiramente o resto da divisão de 3^{10} por 13.

Como $3^2 \equiv -4\ (mod\ 13)$, então $3^{10} = (3^2)^5 \equiv (-4)^5 = -2^{10}\ (mod\ 13)$,

Portanto,

$3^{70} = 3^{10}.3^{60} \equiv 1.3^{10} \equiv -2^{10}\ (mod\ 13)$.

Logo, $2^{70} + 3^{70} \equiv (2^{10}) + (-2^{10}) = 0\ (mod\ 13)$.

Exemplo 49. Mostre que não existe x inteiro tal que $x^5 - 2$ é múltiplo de 41.

Solução:

Suponha que $x^5 \equiv 2\ (mod\ 41)$. Elevando a 8 ambos os lados iremos obter que $x^{40} \equiv 2^8\ (mod\ 41)$.

Como 41 é um número primo e supondo que $(41, x) = 1$, podemos utilizar o Teorema de Euler-Fermat, obtendo

$$x^{40} \equiv 1\ (mod\ 41).$$

Logo, $x^{40} \equiv 2^8 \ (mod\ 41)$ e $x^{40} \equiv 1 \ (mod\ 41)$, o que implica que $1 \equiv 2^8 \ (mod\ 41)$, o que é um absurdo, pois $10 \equiv 2^8 \ (mod\ 41)$.

Assim, não existe x tal que $x^5 - 2$ é múltiplo de 41.

O exemplo a seguir foi extraído de [3], pág.94.

Exemplo 50. Encontre os dois últimos algarismos de 3^{1005} na notação decimal.

Solução:

Para encontrarmos os últimos 2 dígitos de um número precisamos analisar ele módulo 100.

Pelo Teorema de Euler - Fermat temos que

$$3^{\varphi(100)} \equiv 1 \ (mod 100).$$

Pelo Teorema 40, obtemos $\varphi(100) = 40$. Assim,

$$3^{40} \equiv 1 \ (mod\ 100).$$

Pelo Corolário 35 podemos elevar ambos os membros da congruência a potência 25, obtendo que

$(3^{25})^{40} \equiv 1^{25}\ (mod\ 100)$, ou seja, $3^{1000} \equiv 1\ (mod\ 100)$.

Pela Proposição 33 item (iii), podemos multiplicar por 3^5 ambos os membros dessa congruência, $3^5.3^{1000} \equiv 3^5.1 \equiv 43\ (mod\ 100)$.

Portanto, o algarismo das unidades é 3 e o das dezenas é 4.

Exemplo 51. Determine o resto da divisão por 2027 do número

$$S = 1^{2026} + 2^{2026} + 3^{2026} + \cdots + 2016^{2026}.$$

Solução:

Note inicialmente que 2027 é um número primo e que o $(j, 2027) = 1$, para $1 \leq j \leq 2016$.

Iremos aplicar o Pequeno Teorema de Fermat em cada parcela dessa soma.

$1^{2026} \equiv 1\ (mod\ 2027)$

$2^{2026} \equiv 1\ (mod\ 2027)$

$3^{2026} \equiv 1\ (mod\ 2027)$

$\vdots \quad \vdots \quad \vdots \quad \vdots$

$2016^{2026} \equiv 1\ (mod\ 2027).$

Somando todas essas congruências vamos obter o seguinte

$1^{2026} + 2^{2026} + \cdots + 2016^{2026} \equiv 2016\ (mod\ 2027).$

Portanto o resto será 2016.

Exemplo 52. Provar que para p primo

$$(p-1)! \equiv p-1\ \big(mod\ 1+2+3+\cdots+(p-1)\big).$$

Demonstração:

Provar isso é equivalente a mostrar que

$$(p-1)! \equiv p-1\ \left(\frac{p(p-1)}{2}\right).$$

Para $p = 2$ a congruência é válida. Agora temos que $p > 2$ e com isso o fator $\frac{(p-1)}{2}$ é um número inteiro.

Um fato importante para essa solução é que o máximo divisor comum de p e $\frac{(p-1)}{2}$ é 1.

Iremos usar o Lema de Euclides para provar esse fato.

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

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

Pela Proposição 33 item (iv) precisamos mostrar que

$(p-1)! \equiv p-1 \left(mod \left(\frac{(p-1)}{2}\right)\right)$ e que

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

Vamos primeiramente mostrar que

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

Mas a congruência acima é exatamente o Teorema de Wilson, logo é sempre verdadeira para todo $p > 2$.

Agora vamos provar que

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

Note que $\frac{(p-1)}{2} | (p-1)$, logo a congruência acima é válida.

Portanto temos que $(p-1)! \equiv p-1\ \left(\frac{p(p-1)}{2}\right)$ é verdadeira para todo número primo p.

3 APLICAÇÕES DE DIVISIBILIDADE E CONGRUÊNCIA.

A congruência modular é uma ferramenta extremamente útil para a resolução de equações Diofantinas no campo dos números inteiros.

O nome dado a essas equações é uma homenagem ao matemático grego Diofanto de Alexandria.

A equação Diofantina mais famosa é a que ficou conhecida como o "Último Teorema de Fermat". Seu enunciado é o seguinte: A equação $x^n + y^n = z^n$ não possui solução para n inteiro, $n \geq 3$ e xyz não nulo. Gerações inteiras de matemáticos brilhantes tentaram demonstrar tal Teorema. Dentre os grandes matemáticos ao longo dos tempos que tentaram resolver o problema podemos mencionar: Euler, Dirichlet, Legendre, Gabriel Lamé, Sophie Germain, Kummer e mais recentemente, Wagstaff.

Só em 1995 que o matemático Andrew Willes juntamente com a ajuda de Richard Taylor obteve sucesso na demonstração de tal Teorema.

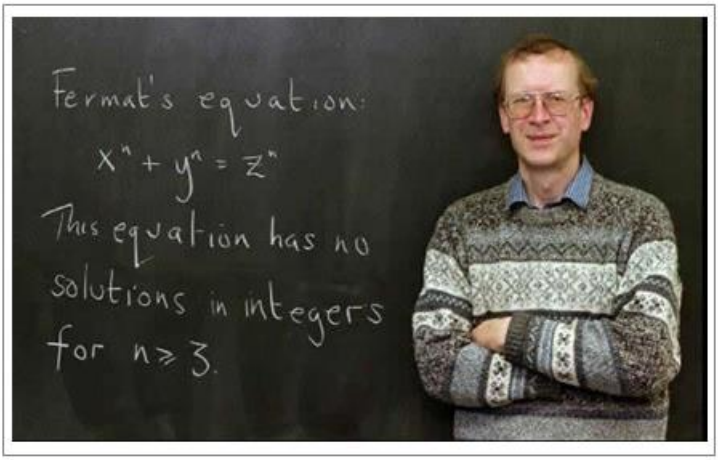


FIGURA 5 ANDREW WILES

3.1 EQUAÇÕES DIOFANTINAS LINEARES

Equações Diofantinas Lineares com duas incógnitas são equações do tipo

$$ax + by = c \qquad (1)$$

Onde $a, b \in \mathbb{Z}$ e a e b não simultaneamente nulos. Uma solução de (1) é, neste caso, um par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ para o qual a igualdade $ax_0 + by_0 = c$ é verdadeira.

Utilizaremos congruência vista no capítulo anterior para resolvermos equações Diofantinas lineares.

O resultado abaixo nos dirá quando uma equação Diofantina tem solução, e ainda nos fornece a "cara" de todas as soluções.

Proposição 53. Sejam a, b e c inteiros não nulos dados. A equação $ax + by = c$ admite soluções $x, y \in \mathbb{Z}$ se, e só se, $(a, b)|c$. Nesse caso, se $d = (a, b)$ e $x = x_0$, $y = y_0$ for uma solução inteira qualquer da equação, então as fórmulas

$$x = x_0 + \frac{b}{d}t \text{ e } y = y_0 - \frac{a}{d}t,$$

onde $t \in \mathbb{Z}$, dão todas as soluções inteiras possíveis.

Observação: Sua demonstração pode ser consultada na página 23 de [4].

Exemplo 54: Resolva cada uma das seguintes equações Diofantinas:

$a) \ 30x + 17y = 201$

$b) \ 47x + 29y = 1288$

Soluções:

$a)$ A equação tem solução, pois $(30, 17)|201$. Aplicando congruência módulo 17 teremos que:

$30x \equiv 201(mod\ 17) \Leftrightarrow -4x \equiv -3\ (mod\ 17) \Leftrightarrow$

$4x \equiv 3(mod\ 17)$.

Multiplicando essa última congruência por 4 em ambos os membros, teremos

$16x \equiv 12\ (mod\ 17)\ \Leftrightarrow -x \equiv -5\ (mod\ 17) \Leftrightarrow$

$x \equiv 5\ (mod\ 17)$, portanto $x = 17t + 5$. Substituindo $x = 17t + 5$ na equação encontramos $y = -30t - 3$.

Logo a solução geral da equação é

$$S = \{(17t + 5; -30t - 3) | t \in \mathbb{Z}\}.$$

$b)$ A equação tem solução, pois $(47, 29)|1288$. Aplicando congruência módulo 29 teremos que:

$47x \equiv 1288\ (mod\ 29) \Leftrightarrow 18x \equiv 12\ (mod\ 29)$ e $(6{,}29) = 1 \Rightarrow 3x \equiv 2\ (mod\ 29)$.

Multiplicando essa última congruência por 10 teremos

$$30x \equiv 20\ (mod\ 29) \Leftrightarrow x \equiv -9\ (mod\ 29),$$

portanto $x = 29t - 9$. Substituindo $x = 29t - 9$ na equação encontramos $y = -47t + 59$.

Logo a solução geral da equação é

$$S = \{(29t - 9; -47t + 59) | t \in \mathbb{Z}\}.$$

3.2 EQUAÇÕES DIOFANTINAS NÃO LINEARES

Definição 55. Uma equação Diofantina é classificada como não linear se pelo menos um dos seus termos é um termo não linear.

Exemplo:

$a) \ x^2 + y^2 = z^2$

$b) \ 2^x = y^2 + 615$

$c) \ \frac{1}{n} + \frac{1}{m} = \frac{1}{143}$

Exemplo 56. Encontre todos os pares de inteiros positivos (x, y) tais que

$$2^x = 1 + 3^y.$$

***Solução*:** Se $y \geq 1$, então $3^y \equiv 0 \ (mod \ 3)$. Assim

$$2^x \equiv 1 \ (mod \ 3).$$

Por outro lado, $2 \equiv -1 \ (mod \ 3)$ o que implica que

$$(-1)^x \equiv 1 \ (mod 3).$$

Para que a congruência acima seja verdade temos que x é um número par. Caso contrário teríamos que $-1 \equiv 1 (mod \ 3)$, o que claramente é falso.

Escrevendo $x = 2m$, com m um número inteiro positivo e reescrevendo a equação iremos obter o seguinte:

$2^{2m} = 1 + 3^y$, ou seja, $2^{2m} - 1 = 3^y$, ou ainda

$(2^m - 1).(2^m + 1) = 3^y$.

Como $2^m - 1$ e $2^m + 1$ são divisores de uma potência de 3, então $2^m - 1$ e $2^m + 1$ são ambas potências de 3 cuja a diferença entre elas é $2^m + 1 - 2^m + 1$ é igual a 2. Logo $2^m - 1$ é igual a 1 e $2^m + 1$é igual a 3.

Portanto, $m = 1$, o que implica que $x = 2$.

Se $x = 2$, então substituindo na equação $2^x = 1 + 3^y$ iremos encontrar que $y = 1$.

Não podemos esquecer que no início da solução assumimos $y \geq 1$. Vamos analisar o que ocorre com $y = 0$.

Se $y = 0$, iremos obter $2^x = 2 \Rightarrow x = 1$.

Portanto temos dois pares ordenados como soluções da equação Diofantina.

$$S = \{(1,0); (2,1)\}$$

Exemplo 57. Encontre todos os inteiros positivos x e y tais que $3^x - 2^y = 7$.

Solução: Se $y \geq 3$, então $2^y \equiv 0\ (mod\ 8)$. Assim

$$3^x \equiv 7\ (mod\ 8).$$

Por outro lado, $7 \equiv -1\ (mod\ 8)$ o que implica que

$$3^x \equiv -1\ (mod\ 8).$$

Note que $3^2 \equiv 1(mod\ 8)$ e pelo corolário 35 podemos concluir que $3^{2n} \equiv 1(mod\ 8)$.

Multiplicando em ambos os lados por 3 a congruência $3^{2n} \equiv 1(mod\ 8)$ concluímos que $3^{2n+1} \equiv 3\ (mod\ 8)$.

Logo, independentemente da paridade do expoente a congruência $3^x \equiv -1\ (mod\ 8)$ nunca irá ocorrer.

Portanto podemos concluir que para $x \geq 3$ não existe solução nos inteiros positivos.

Agora iremos analisar os casos onde $y = 0,1$ ou 2.

Se $y = 0$ iremos obter $3^x = 8$, a qual não possui solução nos inteiros.

Se $y = 1$ iremos obter $3^x = 9 \Rightarrow x = 2$.

Se $y = 3$ teremos $3^x = 15$, a qual não possui solução nos inteiros.

Portanto a equação $3^x - 2^y = 7$ possui uma única solução no conjunto dos números inteiros positivos.

$$S = \{(2,1)\}$$

4. CONGRUÊNCIA E DIVISIBILIDADE NOS VESTIBULARES.

A finalidade desse capítulo é apresentar algumas questões que apareceram em questões de Divisibilidade e de Equações Diofantinas no Vestibulares.

Essas questões são relativamente comuns nos vestibulares do Instituto Militar de Engenharia e no Colégio Naval.

(IME 2017/2018) Determine todos os números primos p, q e r tais que

$$35p + 11pq + qr = pqr.$$

***Solução*:** Vamos analisar a equação modulo p.

Note que $35p + 11pq$ e pqr são múltiplos de p e portanto são côngruos a zero módulo p. Por esse

motivo temos que $q.r \equiv 0\ (mod\ p)$. Com isso temos que $q = p$ ou $p = r$. Iremos separar em 2 casos.

1ª caso: Fazendo $p = r$, temos

$$35p\ +\ 11pq\ +\ qp\ =\ p^2q.$$

Dividindo e ambos os lados por p iremos obter

$$35 +\ 11q\ +\ q\ =\ pq.$$

$$35 +\ 12q\ =\ pq.$$

$35 = q(-12 +\ p)$. Como q é um número primo temos que $q = 5$ ou $q = 7$.

Se $q = 5$ temos que $r = p = 19$.

Se $q = 7$ temos que $r = p = 17$.

Portanto neste primeiro caso temos duas soluções.

2ª caso: Fazendo $p = q$, então

$$35p\ +\ 11p^2\ +\ pr\ =\ p^2r$$

Dividindo por p em ambos os lados da igualdade iremos obter:

$35 + 11p + r = pr.$

Isolando p na equação obteremos que:

$$p = \frac{35-r}{r-1}.$$

Desta última igualdade temos que

$(r-1)|(35-r) \Rightarrow (r-1)|34.$

Os possíveis valores de r são: 2 e 3.

Se $r = 2$ então $q = p = 33.$

Se $r = 3$ então $q = p = 16.$

Perceba que nos casos onde $r = 2$ e $r = 3$ os valores de q e p não são números primos, logo não constituem triplas (p, q, r) que satisfazem a equação do problema.

Portanto as duas triplas (p, q, r) que são soluções são $(19,5,19)$ e $(17,7,17)$.

(IME 2015/2016) Seja a equação $n^2 - 7m^2 = (5m - 2n)^2 + 49$. Determine todos os pares de inteiros (m, n) que satisfazem a esta equação.

Solução: A estratégia será fatorar a expressão $n^2 - 7m^2 = (5m - 2n)^2 + 49$.

$$n^2 - 7m^2 = (5m - 2n)^2 + 49$$
$$\Leftrightarrow 32m^2 - 20mn + 3n^2 = -49 \Leftrightarrow$$

$$\Leftrightarrow -32m^2 + 20mn - 3n^2 = 49$$
$$\Leftrightarrow -32m^2 + 8mn + 12mn - 3n^3 = 49$$

$$\Leftrightarrow 8m(-4m + n) - 3n(-4m + n) = 49$$
$$\Leftrightarrow (-4m + n)(8m - 3n) = 49.$$

Agora vamos analisar os 6 casos:

1º Caso

$$\begin{cases} -4m + n = 1 \\ 8m - 3n = 49 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(-13, -51)$.

2º Caso

$$\begin{cases} -4m + n = 49 \\ 8m - 3n = 1 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(-37, -99)$.

3º Caso

$$\begin{cases} -4m + n = -1 \\ 8m - 3n = -49 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(13{,}51)$.

4º Caso

$$\begin{cases} -4m + n = -49 \\ 8m - 3n = -1 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(37{,}99)$.

5º Caso

$$\begin{cases} -4m + n = 7 \\ 8m - 3n = 7 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(-7, -21)$.

6º Caso

$$\begin{cases} -4m + n = -7 \\ 8m - 3n = -7 \end{cases}.$$

Este sistema tem como solução o par ordenado

$(7,21)$.

(IME 2011/012) Sejam r e $s \in \mathbb{Z}$ (inteiro). Prove que $(2r + 3s)$ é múltiplo de 17 se e somente se $(9r + 5s)$ é múltiplo de 17.

Solução:

Vamos provar que se $(2r + 3s)$ é múltiplo de 17 então $(9r + 5s)$ é múltiplo de 17.

Por hipótese temos que $17|(2r + 3s) \Rightarrow 17|(-4)(2r + 3s) + 17(r + s) \Rightarrow 17|(9r + 5s)$.

Agora vamos provar que $(9r + 5s)$ é múltiplo de 17 então $(2r + 3s)$ é múltiplo de 17.

Por hipótese temos que $17|(9r + 5s) \Rightarrow 17|(-1).(9r + 5s) + 17(r + s) \Rightarrow 17|4(2r + 3s)$.

Como 17 não divide 4, temos que $17|(2r + 3s)$.

(IME 2009/2010) Seja a equação $p^n + 144 = q^2$, onde n e q são números inteiros positivos e p é um número primo. Determine os possíveis valores de n, p e q.

Solução: $p^n + 144 = q^2 \Leftrightarrow p^n = q^2 - 144$

$p^n + 144 = q^2 \Leftrightarrow p^n = (q - 12)(q + 12)$.

Note que os fatores $(q - 12)$ e $(q + 12)$ são números inteiros positivos e com isso temos que $q > 12$.

Como p é primo temos que os fatores $(q - 12)$ e $(q + 12)$ são potências de p. Logo

$(q - 12)|(q + 12) \Rightarrow (q - 12)|(q + 12) - (q - 12)$

Portanto $(q-12)|24$ e que $q>12$.

Portanto as únicas possibilidades para q são os seguintes

$q=13,14,15,16,18,20,24,36$. Vamos analisar cada uma.

Se $q=13$, então

$p^n=(13-12)(13+12)=25=5^2$.

Pelo Teorema Fundamental da Aritmética temos que $p=5$ e $n=2$.

Logo, $q=13, p=5\ e\ n=2$.

Se $q=14$, então,

$p^n=(14-12)(14+12)=52$.

Se $q=15$, então,

$p^n=(15-12)(15+12)=81=3^4$.

Pelo Teorema Fundamental da Aritmética temos que $p=3$ e $n=4$.

Se $q = 16$, então,

$p^n = (16 - 12)(16 + 12) = 112.$

Se $q = 18$, então,

$p^n = (18 - 12)(18 + 12) = 180.$

Se $q = 20$, então

$p^n = (20 - 12)(20 + 12) = 256 = 2^8.$

Pelo Teorema Fundamental da Aritmética temos que $p = 2\ e\ n = 8$

Logo $q = 20, p = 2\ e\ n = 8$

Se $q = 24$, então,

$$p^n = (24 - 12)(24 + 12) = 432.$$

Se $q = 36$, então

$p^n = (36 - 12)(36 + 12) = 1152.$

Os casos onde $q = 14, 16, 18, 24$ e 36 não constituem soluções

Logo as triplas (p, n, q) que satisfazem a equação diofantina são as seguintes:

$(5,2,13), (3,4,15), (2,8,20).$

(IME 2000/2001) Prove que para algum número inteiro positivo x, os números x e x^5 terminam sempre com o mesmo algarismo (algarismo das unidades).

Solução:

Qualquer número x inteiro pode ser escrito da forma

$x = 10b + c$, onde c é o algarismo das unidades do número x.

Queremos provar que $x^5 = 10m + c$ que, é equivalente a provar que

$x^5 - x$ é múltiplo de 10.

$$x^5 - x = x(x^4 - 1) = x(x^2 - 1)(x^2 + 1)$$
$$= x(x - 1)(x + 1)(x^2 + 1).$$

Já podemos garantir que $(x^5 - x)$ é múltiplo de 2, pois $x(x-1)$ são inteiros consecutivos.

Agora temos que provar que é múltiplo de 5.

Por consequências do Pequeno Teorema de Fermat temos que $x^5 \equiv x\ (mod 5)$.

Logo $x^5 - x$ é múltiplo de 2 e de 5 e com isso é múltiplo de 10.

■

(IME 1999/2000) Considere quatro números inteiros a, b, c e d. Prove que o produto:

$(a-b)\,(c-a)\,(d-a)\,(d-c)\,(d-b)\,(c-b)$
é divisível por 12

Solução:

Vamos primeiramente provar que $(a-b)\,(c-a)\,(d-a)\,(d-c)\,(d-b)\,(c-b)$

é múltiplo de 4 para quais a, b, c e d inteiros.

1ª Caso: (a, b, c e d são números pares)

$$\underbrace{(a-b)}_{par}\ \underbrace{(c-a)}_{par}\ \underbrace{(d-a)}_{par}\ \underbrace{(d-c)}_{par}\ \underbrace{(d-b)}_{par}\ \underbrace{(c-b)}_{par}$$

Esse produto possui 6 números pares assim garantindo que é múltiplo de 4.

2º caso (3 números pares e 1 ímpar)

Suponha sem perda de generalidade que a, b e c são pares e d é ímpar.

$$\underbrace{(a-b)}_{par}\ \underbrace{(c-a)}_{par}\ \underbrace{(d-a)}_{impar}\ \underbrace{(d-c)}_{impar}\ \underbrace{(d-b)}_{impar}\ \underbrace{(c-b)}_{par}$$

Esse produto possui 3 números pares assim garantindo que é múltiplo de 4.

3ª Caso (2 números pares e 2 números impares)

Suponha sem perda de generalidade que a e b são pares e que c e d são impares.

$$\underbrace{(a-b)}_{par}\ \underbrace{(c-a)}_{impar}\ \underbrace{(d-a)}_{impar}\ \underbrace{(d-c)}_{par}\ \underbrace{(d-b)}_{impar}\ \underbrace{(c-b)}_{ímpar}$$

Esse produto possui 2 números pares assim garantindo que é múltiplo de 4.

4ª Caso (1 número par e 3 números impares)

Suponha sem perda de generalidade que a é par e os demais são impares.

$$\underbrace{(a-b)}_{impar}\ \underbrace{(c-a)}_{impar}\ \underbrace{(d-a)}_{impar}\ \underbrace{(d-c)}_{par}\ \underbrace{(d-b)}_{par}\ \underbrace{(c-b)}_{par}$$

Esse produto possui 3 números pares assim garantindo que é múltiplo de 4.

5ª Caso (a, b, c e d são pares)

$$\underbrace{(a-b)}_{par}\ \underbrace{(c-a)}_{par}\ \underbrace{(d-a)}_{par}\ \underbrace{(d-c)}_{par}\ \underbrace{(d-b)}_{par}\ \underbrace{(c-b)}_{par}$$

Esse produto possui 6 números pares assim garantindo que é múltiplo de 4.

Então, em qualquer situação,

$(a-b)\ (c-a)\ (d-a)\ (d-c)\ (d-b)\ (c-b)$
é múltiplo de 4.

Agora temos que garantir que também seja múltiplo de 3.

Qualquer inteiro pode ser escrito de uma dessas maneiras

$n = 3k\ (multiplos\ de\ 3)$,

$n = 3k + 1\ (deixa\ resto\ 1)$

$n = 3k + 2\ (deixa\ resto\ 2)\ ,\ k \in \mathbb{Z}$

Como temos 4 números e três possíveis restos, temos que pelo menos dois deles irão deixar o mesmo resto.

Portanto

$(a - b)\ (c - a)\ (d - a)\ (d - c)\ (d - b)\ (c - b)$
é múltiplo de 3.

■

CONSIDERAÇÕES FINAIS

Fazer esse trabalho foi um aprendizado enorme. Relembrei vários resultados estudados na disciplina de Aritmética.

A Teoria dos Números apresentada é elementar, mas, contudo, é fundamental para a compreensão de assuntos mais complexos.

Os assuntos de divisibilidade e congruência modular nos ajudam a resolver diversos problemas de uma forma muito eficiente. Esses assuntos poderiam enriquecer muito o ensino básico.

Espera - se deste trabalho é que ele auxilie o professor na prática docente no que diz respeito ao desenvolvimento de conteúdos e principalmente

nas resoluções de problemas. Pois acredita-se veemente que essas ideias poderão facilitar o aprendizado dos alunos, em muitas situações e principalmente na hora de ir fazer uma prova de vestibular.

REFERÊNCIAS

[1] ANDREESCU, T. et al. **An Introduction to Diophantine Equations: A Problem-Based Approach**- New York: Birkhäuser Mathematics, 2010.

[2] A. Hefez, **Aritmética**, Coleção PROFMAT, SBM, 2013.

[3] BOAVA, Giuliano. **Divisibilidade e Congruência**. VII Encontro da Olimpíada Regional de Matemática, Florianópolis, 31 de março de 2012. Disponivel em: <http://www.orm.mtm.ufsc.br/arquivos/downloads/congruencia.pdf>. Acesso em: 4 de fevereiro de 2019.

[4] CAMINHA, A, **Teoria dos Números**, Coleção Tópicos de Matemática Elementar, Volume 5, SBM, 2ª ed, 2014.

[5] COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. 2ª ed. Rio de Janeiro: IMPA, 2011.

[6] DOMINGUES, Hygino H. **Fundamentos de aritmética**. São Paulo: Editora UFSC, 2ª ed, 2017.

[7] F.E.B. Martinez, C.G.T. Moreira, N.C Saldanha e E. Tengan, **Teoria dos Números- Um Passeio com Primos e Outros Números Familiares pelo Mundo Inteiro**, Coleção Projeto Euclides, Impa, Segunda Edição, 2011.

[8] J.P.O. Santos, **Introdução à Teoria dos Números**, Coleção Matemática Universitária, Impa, Terceira Edição, 2011.

[9] LIDSKY, V.B; OVSIANIKOV, L.V; TULAIKOV, A.N. **Problemas de Matemática Elementar**.Vestseller,1ºed. Fortaleza-CE,2014.

[10] MAIER, Rudolf (Richard). **TEORIA DOS NÚMEROS**. 2005. Disponível em: <Http://www.mat.unb.br/~maierr/tnotas.pdf>. Acesso em: 4 de fevereiro de 2019.

[11] OLIVEIRA, Krerley Irraciel Martins; FERNÁNDEZ, Adán José Corcho. **Iniciação à Matemática: um curso com problemas e soluções**. 1. ed. Rio de Janeiro: SBM, 2010.

[12] MADEIRA, Renato. **EXERCÍCIOS DE TEORIA DOS NÚMEROS DO IME**. Disponível em: https://drive.google.com/file/d/0B09ggPPZzKsZRm94cEVhWU5qSFk/view. Acesso dia: 08 de fevereiro de 2019.

[13] SAUTOY, du Marcus. **Os Mistérios dos Números. Uma viagem pelos grandes enigmas da matemática (que até hoje ninguém foi capaz de resolver).** Rio de Janeiro: ZAHAR, 2013.

[14] TAO, Terence. **Como Resolver Problemas Matemáticos**, Coleção do Professor de Matemática, 1ª ed. Rio de Janeiro: SBM, 2013

[15] VIANA, M. **"Túnel do tempo: "pequeno teorema de Fermat""**.2017. Disponível em: https://impa.br/page-noticias/tunel-do-tempo-pequeno-teorema-de-fermat/. Acesso dia: 05 de fevereiro de 2019.

[16] <Http://clubes.obmep.org.br/blog/teorema-fundamental-da-aritmetica/>. Acesso dia: 10 de fevereiro de 2019.

[17] WIKIPÉDIA, **DISQUISITIONES ARITHMETICAE**. Disponível em: https://pt.wikipedia.org/wiki/Disquisitiones_Arithmeticae#/media/File:Disqvisitiones-800.jpg. Acesso dia: 12 de fevereiro de 2019.

[18] WIKIPÉDIA, **JONH WILSON**. Disponível em: https://ca.wikipedia.org/wiki/John_Wilson_(matem%C3%A0tic). Acesso dia: 12 de fevereiro de 2019.

[19] WIKIPÉDIA, **CARL FRIEDRICH GAUSS**. Disponível em:https://ca.wikipedia.org/wiki/Carl_Friedrich_Gau%C3%9F.Acesso dia: 13 de fevereiro de 2019.

[20] WIKIPÉDIA, **TESTE DE PRIMALIDADE DE FERMAT**. Disponível em: https://pt.wikipedia.org/wiki/Teste_de_primalidadp_de_Fermat. Acesso dia: 13 de fevereiro de 2019.

[21] G1-GLOBO, **Matemático que solucionou problema de 357 anos recebe o prêmio Abel.** Disponível em: http://g1.globo.com/ciencia-e-saude/noticia/2016/03/matematico-que-solucionou-problema-de-357-anos-recebe-premio-abel.html.

Acesso dia: 13 de fevereiro de 2019.