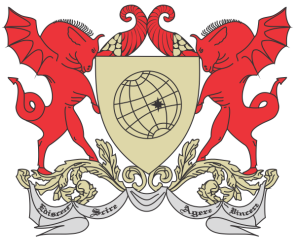
Universidade Federal de Viçosa
Trabalho de Conclusão de Curso



Lucas Mendes Viana

Equações Diofantinas

Florestal
Minas Gerais – Brasil
2022

Lucas Mendes Viana

EQUAÇÕES DIOFANTINAS

Trabalho de Conclusão de Curso apresentado à Universidade Federal de Viçosa, como parte das exigências do Curso de Licenciatura em Matemática, para obter o diploma de Licenciado em Matemática.

Florestal
Minas Gerais – Brasil
2022

Ata de defesa de monografia

Aos 17 dias do mês de novembro de 2022, reuniu-se via videoconferência no Google Meet, a banca composta por Luís Felipe Gonçalves Fonseca (IEF), Danielle Franco Nicolau (IEF) e Luiz Gustavo Perona Araújo (Cefet- MG, Belo Horizonte, Campus Nova Gameleira), para avaliar o Trabalho de Conclusão de Curso do licenciando em matemática **LUCAS MENDES VIANA, matrícula 3368. O título do trabalho de conclusão de curso é "EQUAÇÕES DIOFANTINAS ".** Após apresentação pelo licenciando, o trabalho de conclusão de curso foi aprovado com as devidas correções, sendo feita a comunicação da aprovação. Em seguida, eu, Luís Felipe Gonçalves Fonseca, orientador do estudante, lavrei a presente ata que, se estiver de acordo, deverá ser assinada pelos membros da banca.

_____

Danielle Franco Nicolau – Primeiro Membro

_____

Luís Felipe Gonçalves Fonseca - Orientador

_____

Luiz Gustavo Perona Araújo- Segundo Membro

Agradecimentos

Agradeço a todos os meus familiares, em especial a minha avó por me incentivar desde o primeiro dia, e ao meu irmão por toda ajuda durante o curso. Agradeço também aos meus professores, mais uma vez queria destacar o Prof. Dr. Luís Felipe Gonçalves Fonseca, que me orientou durante grande parte dos meus estudos e sempre me incentivou a querer estudar mais e mais, ao Prof. Dr. Alexandre Alvarenga Rocha pelo convite a participar do projeto Desafios da Matemática ao qual devo bastante apreço pelo trabalho feito com carinho, e ao Prof. Dr. Luiz Gustavo Perona por me orientar academicamente durante o curso. Quero agradecer aos meus colegas de estudo, mais uma vez destacando alguns amigos que fiz durante a caminhada, Augusto Meireles, Dhavy Alexwander, Larissa Ribeiro, Aysla Bianca e Ana Carolina Santos Martins. Quero agradecer também a professora Anna Maria Amaral Costa que me deu espaço em sua sala de aula para que pudesse aprender a lecionar e que com o passar do tempo se tornou uma grande amiga. E finalmente agradeço ao apoio incondicional da minha namorada Maria Eduarda Gomes Silva, que sempre me ajudou.

Resumo

VIANA, Lucas Mendes, Lic., Universidade Federal de Viçosa, novembro de 2022. **Equações Diofantinas**. Orientador: Luís Felipe Gonçalves Fonseca.

Neste trabalho, veremos alguns tipos de equações diofantinas, tais como, as congruências de grau 2, as ternas pitagóricas. Também apresentaremos alguns teoremas como o Teorema de Lagrange e alguns casos do Último Teorema de Fermat. Primeiramente, estudaremos as congruências de grau 2($ax^2 + bx + c \equiv 0 \pmod{p}$) sendo p primo tal que $p \nmid a$, o símbolo de Legendre e as suas propriedades. Terminando os estudos sobre as congruências, provaremos o Teorema da Reciprocidade Quadrática de Gauss. Posteriormente veremos as ternas pitagóricas. Apresentaremos o problema de Waring e forneceremos uma prova para o Teorema de Lagrange. Este teorema diz que todo número natural n pode ser escrito como a soma de quatro quadrados. Concluiremos, vendo dois casos do último Teorema de Fermat ($x^n + y^n = z^n$), os casos $n = 3$ e $n = 4$.

Abstract

VIANA, Lucas Mendes, Universidade Federal de Viçosa, November, 2022. **Diophantine equations**. Adviser: Luís Felipe Gonçalves Fonseca.

In this paper, we will see some types of Diophantine equations, such as the congruences of grade 2, the Pythagorean triples. We will also present some theorems such as Lagrange's Theorem and some cases of Fermat's Last Theorem. First we'll study at grade 2 congruences ($ax^2 + bx + c \equiv 0 \pmod{p}$),where p is prime such that $p \nmid a$, the Legendre symbol and its properties. Finishing the studies on the congruences, we will prove Gauss's Quadratic Reciprocity Theorem. Later we will see the Pythagorean temples. We will present the Waring problem and provide proof for the Lagrange Theorem. This theorem says that any natural number n can be written as the sum of four squares. We will conclude by looking at two cases of Fermat's Last Theorem ($x^n + y^n = z^n$), the cases $n = 3$ and $n = 4$.

Sumário

1

Introdução

É inegável que os países do mediterrâneo foram o berço de grandes matemáticos da história. Nomes como Tales, Pitágoras, Arquimedes e Euclides estão presentes até hoje na vida de qualquer estudante ou entusiasta da matemática. Suas obras são relevantes e primordiais para o estudo de várias áreas da matemática. Muitos avanços que tivemos foram, direta ou indiretamente, ligados aos estudos destes matemáticos.

Neste material, estudaremos as equações diofantinas, que são equações que ganham esse nome por serem equações que, nos seus primórdios, foram estudadas por Diofanto.

Diofanto nasceu em Alexandria, por volta do séc. III d. C. Durante sua vida estudou várias áreas da matemática, sendo um dos primeiros matemáticos a introduzir símbolos no estudo da álgebra, assim ajudando a evoluir os estudos matemáticos daquela época.

Entrando um pouco mais nas equações diofantinas, em especial as lineares, estas são equações da forma:

$$ax + by = c,$$

em que a, b e c são números inteiros assim como as soluções x e y caso existam. Equações desta forma, assim como suas variantes, damos o nome de equações diofantinas. São estas equações que estudaremos neste material, começando com os princípios básicos da aritmética e posteriormente aprofundando nestas equações.

Avançando o trabalho, estudaremos as ternas pitagóricas, que são soluções (a, b, c), sendo todos termos inteiros, da equação $a^2 + b^2 = c^2$. Estas ternas recebem este nome pelo fato de estarem relacionadas com famoso Teorema de Pitágoras. Em nossos estudos veremos como são formadas estas soluções.

Posteriormente veremos o Problema de Waring: para todo positivo k existe um número $s(k)$ tal que todo inteiro positivo pode ser escrito como a soma $s(k)$ potências a^k de inteiros positivos? E veremos o Teorema de Lagrange sobre este problema que fornece uma resposta positiva para o Problema de Waring para $s = 4$ para $k = 2$. A prova do problema de Warring foi dada pelo matemático David Hilbert em 1909.

Por fim, veremos os casos $n = 3$ e $n = 4$ para o Último Teorema de Fermat. Este

teorema afirma que não existem inteiros positivos x, y e z tais que

$$x^n + y^n = z^n,$$

sendo n um natural maior ou igual a 3 qualquer. Embora Fermat não tenha o provado de fato, o que aconteceu somente 350 anos depois, ele afirmava que havia uma prova, utilizando aritmética simples que até hoje não foi encontrada.

2

Conceitos Iniciais

Este primeiro capítulo é baseado em alguns capítulos do livro [5]. Primeiramente, veremos o conjunto dos números inteiros assim como suas operações e algumas propriedades. O conjunto dos números inteiros é dado por:

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

A soma destes números (notação : $a + b$) terá as seguintes propriedades, que aqui serão apenas enunciadas. Sejam a, b, c números inteiros. Temos:

- Associativa

  $a + (b + c) = (a + b) + c$;

- Elemento Neutro

  Existe $0 \in \mathbb{Z}$ tal que: $a + 0 = 0 + a = a$;

- Inverso Aditivo

  Existe $d \in \mathbb{Z}$ tal que: $a + d = d + a = 0$;

- Comutativa

  $a + b = b + a$.

Além da soma, existe neste conjunto a multiplicação (notação : ab ou $a \cdot b$). Como para a soma, iremos apenas enunciar as propriedades desta operação. Sejam a, b, c inteiros. Temos:

- Associativa

  $a(bc) = (ab)c$;

- Elemento Neutro

  Existe $1 \in \mathbb{Z}$ tal que: $1 \cdot a = a \cdot 1 = a$;

- Cancelativa

  Para $a \neq 0$, se $ab = bc$, então $b = c$;

- Comutativa

  $ab = ba$;

- Distributiva

  $a(b + c) = ab + ac$.

Podemos verificar que **0** (o elemento neutro aditivo) e **1** (elemento neutro multiplicativo) são únicos. Um subconjunto notável de $\mathbb{Z}$ é o conjunto dos números naturais $\mathbb{N} = \{0, 1, 2, 3,...\}$.

Vamos a mais algumas propriedades sobre o conjunto dos números inteiros, e que, através delas, iremos construir a ideia de ordem do conjunto. A relação "menor ou igual", denotada por $\leq$ tem as seguintes propriedades:

- Propriedade reflexiva: Para todo inteiro a tem-se que $a \leq a$.
- Propriedade anti-simétrica: Dados dois inteiros a e b, se $a \leq b$ e $b \leq a$, então $a = b$.
- Propriedade transitiva: Para toda terna de números inteiros a, b e c, tem-se que, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Por serem válidas as propriedades acima, temos que a relação "menor ou igual"é uma relação de ordem. No caso particular quando temos $a \leq b$ e $a \neq b$ iremos usar o símbolo $a < b$, como "a é menor que b". Além disso podemos usar os símbolos $a \geq b$ e $a > b$, quando queremos dizer que $b \leq a$ e $b < a$ respectivamente. Feitas estas distinções podemos falar de mais algumas propriedades desta relação.

- Tricotomia: Dados dois inteiros quaisquer a e b tem-se que ou $a < b$ ou $a = b$ ou $a > b$.
- Para toda terna, a, b, c de inteiros, se $a \leq b$, então $a + c \leq b + c$.
- Para toda terna, a, b, c de inteiros, se $a \leq b$ e $0 \leq c$, então $ac \leq bc$.

Definição 1: Seja A um subconjunto de $\mathbb{Z}$. Diz-se que A é **limitado inferiormente** se existe algum inteiro k tal que, para todo $a \in A$, tem-se que $k \leq a$. Definiremos como mínimo de A o elemento $a_0 \in A$ tal que, para todo $a \in A$ temos que $a_0 \leq a$. Note que se há um mínimo de A ele é único.

De forma análoga podemos definir o que seria um **limitado superiormente** e máximo de um conjunto. Usaremos a notação $min\ A$ e $max\ A$ para indicar o mínimo e o máximo respectivamente, quando eles existirem. Vamos ver uma importante propriedade dos conjuntos de números inteiros.

Princípio da Boa Ordem*: Todo conjunto não-vazio de inteiros limitado inferiormente tem mínimo.*

De forma análoga podemos dizer que se um conjunto é limitado superiormente possui máximo . Existem ainda várias outras propriedades e teoremas a respeito deste conjunto, porém neste material enunciaremos apenas estas. Dito isto vamos para a definição de divisibilidade.

2.1 Divisibilidade

Definição 2: Sejam a e b números inteiros. Dizemos que b **divide** a (ou que b é um **divisor** de a) se existe um numero inteiro c tal que $bc = a$. Denotaremos por $b|a$.

A negativa notaremos por $b \nmid a$. Assim como a soma e a multiplicação, a divisibilidade possui algumas propriedades. Deixamos a sua verificação a cargo do leitor em [5]. Vejamos algumas destas propriedades.

Teorema 1: São algumas propriedades da divisibilidade:

1. (Reflexiva) $a \mid a, \ \forall a \in \mathbb{Z}$.
2. (Transitiva) Para todos $a, b, c \in \mathbb{Z}$ se $a \mid b$ e $b \mid c$, então $a \mid c$.
3. Para todos $a, b, c \in \mathbb{Z}$ se $a \mid b$ e $a \mid c$ então $a \mid bx + cy, \forall x, y \in \mathbb{Z}$.

A seguir veremos o Algorítimo da Divisão.

Teorema 2: Algoritmo da Divisão.
Sejam a, b inteiros, com $b \neq 0$. Então, existem q e r inteiros e únicos tais que

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

A prova deste teorema se encontra na pág. 50 em [5].

Exemplo 1: Sejam a = 23 e b = 3, utilize o Algoritmo da Divisão para determinar q e r tais que $23 = 3q + r$ com $0 \leq r < 3$.

Como o Algoritmo da Divisão diz que existem q e r inteiros tais que

$$a = bq + r \quad e \quad 0 \leq r <\mid b \mid .$$

Podemos utilizá-lo para definirmos como

$$23 = 3 \cdot 7 + 2 \quad e \quad 0 \leq 2 < 3,$$

o que satisfaz o Algoritmo da Divisão.

Definição 3: Os números **q** e **r** determinados no teorema anterior são denominados **q** quociente e **r** resto da divisão de a por b.

No exemplo anterior o quociente $q = 7$ e o resto $r = 2$.

Exemplo 2: O quadrado de qualquer número inteiro é da forma $3k$ ou $3k + 1$ sendo $k \in \mathbb{Z}$.

De fato, se a é um inteiro, então ele é da forma $3m$, $3m + 1$ ou $3m + 2$. Sendo assim, ou $a^2 = (3m)^2 = 3(3m^2)$, ou $a^2 = (3m + 1)^2 = 3(3m^2 + 2m) + 1$, ou $a^2 = (3m + 2)^2 = 3(3m^2 + 4m + 1) + 1$. Logo a^2 ou é $3k$ ou $3k + 1$.

2.2 MDC e MMC

Damos o nome **divisor** de a a todos os números b inteiros tais que $b \mid a$. Definiremos o máximo divisor entre dois números inteiros não simultaneamente nulos da seguinte forma.

Definição 4: Chama-se de **máximo divisor comum** de a e b o maior divisor de seus divisores comuns positivos, ou seja,

$$mdc(a,b) = max\ D^+\ (a,b);$$

em que $D^+(a,b)$ denota o conjuntos de divisores positivos de a e b.

Note que o conjunto $D^+(a,b)$ é sempre não vazio já que 1 pertence a esse conjunto. Além disso, esse conjunto é limitado superiormente por $|a|$ e $|b|$. Portanto, pelo princípio da boa ordenação, $D^+(a,b)$ tem um máximo . Vejamos agora uma condição necessária e suficiente para que um número seja o mdc de um par de inteiros.

Teorema 3: Sejam a, b inteiros. Um inteiro positivo d é o máximo divisor comum de a e b, se e somente se, verificam-se:

1. $d \mid a$ e $d \mid b$.
2. Se $d' \mid a$ e $d' \mid b$, então $d' \mid d$.

A prova deste teorema pode ser encontrada na pág. 67 em [5].

O cálculo do mdc para números pequenos pode ser fácil, porém quando tratamos de números muito grandes podemos ter certa dificuldade para determinarmos este mdc. O teorema abaixo auxilia nestes casos.

Teorema 4: Sejam a, b e $n \in \mathbb{Z}$. Se existe $mdc(a, b - na)$, então existe $mdc(a, b)$ e $mdc(a, b) = mdc(a, b - na)$.

Demonstração: Provaremos que $D^+(a,b) = D^+(a, b - na)$. Seja d um inteiro tal que $d \mid b$ e $d \mid -na$. Logo $d \mid b - na$. Portanto $d \in D^+(a,b - na)$. Reciprocamente, seja $d \in D^+(a,b - na)$. Temos $d \mid a$, $d \mid na$ e $d \mid b - na$. Segue então que $d \mid b$.

■

Com este teorema, podemos calcular de forma mais simples o mdc de certos inteiros.

Exemplo 3: Calcularemos agora o mdc de 1128 e 336.

Inicialmente, note que, pelo algorítimo da divisão,

$$1128 = 3 \cdot 336 + 120$$

Logo, $mdc(1128, 336) = mdc(336{,}1128 - 3 \cdot 336) = mdc(336{,}120) = mdc(120{,}336)$. Na mesma linha de raciocínio feita para 1128 e 336, temos

$$\begin{aligned} 336 &= 2 \cdot 120 + 96, \\ 120 &= 1 \cdot 96 + 24. \\ 96 &= 4 \cdot 24. \end{aligned}$$

Daí segue que

$$mdc(120{,}336) = mdc(120{,}96) = mdc(96{,}120) = mdc(96{,}24) = 24.$$

Portanto mdc(1128,336) = 24.

Há muitas aplicações de mdc. Em particular, propriedades interessantes quando o mdc é 1.

Teorema 5: (Teorema de Euclides) Sejam a, b, c inteiros tais que $a \mid bc$. Se $mdc(a{,}b) = 1$, então $a \mid c$.

A prova deste teorema pode ser encontrada na pág. 68 em [5].

Quando o mdc de um par de números é 1, damos uma relação nominal a estes números.

Definição 5: Dois inteiros a e b dizem-se relativamente primos se $mdc(a, b) = 1$.

Quando dois números inteiros são relativamente primos, teremos alguns fatos que podemos provar sobre eles, por exemplo o teorema abaixo.

Teorema 6: Sejam a, b primos relativos, seja c um outro inteiro tal que $a \mid c$ e $b \mid c$, então $ab \mid c$.

Demonstração: Por hipótese, $mdc(a{,}b) = 1$. Além disso, existem x e y tais que $c = ax = by$. Visto $b \mid ax$ e $mdc(a{,}b) = 1$, segue do Teorema de Euclides que $b \mid x$. Consequentemente, existe $x' \in \mathbb{Z}$ tal que $x = bx'$. Dessa forma, $c = abx'$ e, portanto, $ab \mid c$.

■

O nome **múltiplo** de a é dado a todos os números inteiros n tais que $n = ak$, com k inteiro. Definiremos agora a relação de menor múltiplo entre dois números inteiros.

Definição 6: Chama-se de **mínimo múltiplo comum** de dois inteiros a e b o menor de seus múltiplos positivos comuns, ou seja,

$$mmc(a, b) = min\ M^+\ (a, b),$$

em que $M^+(a{,}b)$ denota o conjunto dos múltiplos comuns positivos de a e b.

Note que o conjunto $M^+(a,b)$ é sempre não vazio já que ab pertence a esse conjunto. Além disso, esse conjunto é limitado inferiormente por 0, por exemplo. Portanto, pelo princípio da boa ordenação, $M^+(a,b)$ tem um mínimo.

Lema 6.1: Sejam a e b inteiros. Então o $mmc(a,b)$ divide todo múltiplo comum de a e b.

Teorema 7: Sejam a, b inteiros. Um inteiro positivo m é o mínimo múltiplo comum de ae b, se e somente se, verifica :

1. $a \mid m$ e $b \mid m$.
2. Se $a \mid m'$ e $b \mid m'$, então $m \mid m'$.

Tanto a demonstração do lema quanto do teorema podem ser encontradas nas páginas 75 e 76 em [5]. E agora, por fim, iremos ver a relação entre o mdc e o mmc de dois números a e b.

Teorema 8: Sejam a, binteiros, $d = mdc(a,b)$ e $m = mmc(a,b)$. Então

$$md = \mid ab \mid .$$

A demonstração deste teorema pode ser encontrada na página 76 em [5].

Exemplo 4: Determinar inteiros positivos ae b, tais que $ab = 9900$ e $mmc(a,b) = 330$.

Inicialmente, note que $mdc(a,b) = \dfrac{ab}{mmc(a,b)}$ e, portanto, $mdc(a,b) = \dfrac{9900}{330} = 30$. Assim, existem inteiros c e d tais que $a = 30c$ e $b = 30d$. Visto que $ab = 9900$, segue que $ab = (30c)(30d) = 900cd = 9900$, logo $cd = 11$. Temos dois casos a se considerar:

$$c = 1, d = 11 \text{ (Caso 1)},$$

$$c = 11, d = 1 \text{ (Caso 2)}.$$

No primeiro caso temos que $a = 30$ e $b = 330$(note que o mmc(30,330) = 330).Já no segundo caso temos que $a = 330$ e $b = 30$.

Teorema 9: (Teorema de Bézout) Sejam a, b inteiros e $d = mdc(a,b)$. Então existem inteiros r e s tais que $d = ra + sb$.

A demonstração deste teorema pode ser encontrada na pág. 65 em [5].

Definição 7: Um inteiro $p > 1$ diz-se primo se tem exatamente dois divisores positivos, 1 e ele mesmo.

Teorema 10: (Teorema Fundamental da Aritmética) Seja a um inteiro diferente de 0, 1, -1. Então, existem primos positivos $p_1 < p_2 < ... < p_r$ e inteiros positivos n_1,n_2, ..., n_r, tais que $a = Ep_1^{n_1} \cdots p_r^{n_r}$, em que $E = \pm 1$, conforme a seja positivo ou negativo. Além disso, esta decomposição é única.

A prova deste teorema pode ser encontrada a partir da página 81 em [5].

É conhecido que o conjunto de números primos é infinito. De fato, suponha por absurdo que este conjunto seja finito $P = \{p_1, ..., p_n\}$. Considere o número inteiro positivo $a = p_1 \cdots p_n + 1$. Seja q um divisor primo de a. Necessariamente, $q \mid p_1 \cdots p_n$ pois $q \in P$. Ora, isso implica que $q \mid 1$. Tal fato é um absurdo, pois q é um inteiro maior que 1. Assim o conjunto P dos números primos é infinito.

2.3 Equações Diofantinas Lineares e Congruências

Agora iremos conhecer e estudar as equações que são a inspiração para este trabalho, as equações diofantinas. Começaremos com o caso linear. Uma equação diofantina linear é uma equação da forma

$$ax + by = c$$

com a, b,c inteiros e a e b ambos não nulos. Uma das primeiras perguntas que nós podemos fazer é se estas equações terão solução, ou seja, existem x e y inteiros tais que

$$ax + by = c,$$

outra pergunta está relacionada com a unicidade. Podemos perceber que, algumas destas equações não admitem solução, um exemplo é $4x + 6y = 5$ que, se tivesse solução, como $2|(4x + 6y)$ 2 dividiria também 5, o que não ocorre. Todavia algumas equações diofantinas possuem soluções, como é o caso de $x + y = 1$, cuja solução $x = 1$ e $y = 0$ é correta. Assim é natural perguntarmos quando terão solução e é isto que veremos no próximo teorema.

Lema 10.1: Sejam $a, b,$, e d inteiros tais que $mdc(a,b) = d$. Logo os conjuntos $A = \{ax + by | x, y \in \mathbb{Z}\}$ e $B = \{dz | z \in \mathbb{Z}\}$ são iguais.

Demonstração: Pelo Teorema de Bézout(Teorema 9) temos que $d \in A$ pois $d = ax_1 + by_1$ e por consequência $dz \in A$ pois $dz = z(ax_1 + by_1) = ax_1z + by_1z$. Logo B esta contido em A.

Note que $A \cap \mathbb{N}^* \neq \emptyset$, pois $a \cdot a + b \cdot b = a^2 + b^2 \in A$. Disto, pelo Princípio da Boa Ordem, o conjunto A possui um mínimo, seja esse mínimo d'. Logo $d' = ax_2 + by_2$, e como $d \mid a$ e $d \mid b$, $d \mid d'$, e pelo fato de d' ser o mínimo $d = d'$. Note que todo elemento de A é múltiplo de d, seja $m = ax_3 + by_3$ um elemento de A, pelo Algorítimo da Divisão existem q e r tais que

$$\frac{m}{d} = dq + r \text{ com } 0 \leq r < d.$$

Note que $m - dq = r$, ou seja, $ax_3 + by_3 - dq = r$. Novamente como $d \mid a$ e $d \mid b$, $d \mid ax_3 + by_3 - dq$, dai $d \mid r$ o que implica que $r = 0$, ou seja $m = dq$ com $q \in \mathbb{Z}^*$. Dai temos que A esta contido em B.

Como B contido em A e A contido em B, logo $A = B$.

■

Teorema 11: Sejam a, b, e c inteiros e $d = mdc(a, b)$. A equação $ax + by = c$ terá solução se, e somente se, d | c.

DEMONSTRAÇÃO: Se $c \in \{ax + by | x, y \in \mathbb{Z}\}$ então pelo Lema anterior temos que c é múltiplo de d e portando $d \mid c$.

■

Agora que já sabemos determinar se uma equação diofantina linear possui solução, vejamos como resolver este tipo de equação.

Teorema 12: Sejam a, b e c inteiros tais que $d \mid c$, sendo $d = mdc(a, b)$. Seja (x_0,y_0) uma solução da equação diofantina linear $ax + by = c$. Toda outra solução é da forma

$$x = x_0 + \frac{b}{d} \cdot t, \ y = y_0 - \frac{a}{d} \cdot t, \quad \text{com } t \in \mathbb{Z}.$$

E reciprocamente, para todo $t \in \mathbb{Z}$ os valores de x e y dados pelas fórmulas acima são soluções da equação.

DEMONSTRAÇÃO: De fato, se dados $x = x_0 + \frac{b}{d}\ t$, $y = y_0 - \frac{a}{d}\ t$, sendo x_0 e y_0 soluções, temos que (x,y) são soluções também, visto que

$$ax + by = a\left(x_0 + \frac{b}{d}\ t\right) + b\left(y_0 - \frac{a}{d}\ t\right) = ax_0 + \frac{ab}{d}\ t + by_0 - \frac{ab}{d}\ t = ax_0 + by_0 = c.$$

Agora basta mostrar que dada uma solução (x', y'), existe t inteiro tal que $x' = x_0 + \frac{b}{d}\ t$ e $y' = y_0 - \frac{a}{d}\ t$. Como (x', y') é solução, temos

$$ax' + by' = c = ax_0 + by_0$$

, onde $a(x' - x_0) = b(y' - y_0)$. Seja a' e b' inteiros tais que $a = da'$ e $b = db'$ daí temos que $mdc(a',b') = \frac{d}{d} = 1$. Daí podemos dividir $a(x' - x_0) = b(y' - y_0)$ por d e teremos $a'(x' - x_0) = b'(y' - y_0)$.

Em particular teremos que $b' \mid a'(x' - x_0)$. Como o $mdc(a',b' = 1)$, $b' \mid (x' - x_0)$, daí existe um inteiro t tal que $x' - x_0 = b't$, ou seja,

$$x' = x + \frac{b}{d}\ t.$$

Ainda do fato que $x' - x_0 = b't$ temos que $a'(x' - x_0) = b'(y' - y_0)$ implica que $a'b' = b'(y' - y_0)$, daí $a't = y' - y_0$, Logo

$$y' = y_0 - \frac{a}{d}\ t$$

■

Exemplo 5: Vamos encontrar as soluções de $56x + 72y = 40$.

Observe que $mdc(56, 72) = 8$ e que $8 \mid 40$, logo existe solução. Note que,

$$72 = 56 \cdot 1 + 16,$$
$$56 = 16 \cdot 3 + 8,$$
$$8 = 8 \cdot 2.$$

Com base no Teorema 4, temos $mdc(72,56) = mdc(56,16) = mdc(16,8) = 8$.

Por outro lado, note que

$$8 = 56 - 16 \cdot 3$$
$$8 = 56 - (72 - 56) \cdot 3$$
$$8 = 4 \cdot 56 - 3 \cdot 72.$$

Assim, $40 = 20 \cdot 56 - 15 \cdot 72$.

Isto mostra que $(20, -15)$ é uma solução da equação diofantina linear $56x + 72y = 40$. Já a solução geral é da forma

$$\begin{cases} x = 20 + 72/8t = 20 + 9t \\ y = -15 - 56/8t = -15 - 8t, \quad t \in \mathbb{Z}. \end{cases}$$

Como pudemos perceber até aqui, a relação divide é de grande importância em $\mathbb{Z}$. Podemos aplicá-la em diversos momentos. A definição que trazemos a seguir é uma aplicação dessa relação muito útil para o estudo dos números inteiros.

Definição 8: Seja $m \neq 0$ um dado inteiro. Dois inteiros a e b são ditos congruentes módulo m (notação: $a \equiv b \pmod{m}$) se m divide $a - b$.

A título de exemplo temos $17 \equiv 5 \mod 3$ e $80 \equiv 3 \mod 7$. Seguem abaixo algumas propriedades das congruências.

Teorema 13: Seja $m > 0$ um inteiro. Sejam a, b, c, d inteiros quaisquer . Então valem as seguintes propriedades

1. (Reflexiva) $a \equiv a \pmod{m}$.
2. (Simétrica) Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$.
3. (Transitiva) Se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$.
4. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$.
5. Se $a \equiv b \pmod{m}$, então $a + c \equiv b + c \pmod{m}$.
6. Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $ac \equiv bd \pmod{m}$.
7. Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo n inteiro positivo.
8. Se $a + c \equiv b + c \pmod{m}$, então $a \equiv b \pmod{m}$.

Demonstração : Os itens (1) e (2) são de demonstração direta e ficam a cargo do leitor.

Para o item (3), se $a \equiv b \pmod{m}$, então $m \mid (a-b)$ e se $b \equiv c \pmod{m}$ temos que $m \mid (b-c)$. Teremos então $m \mid (a-b)+(b-c)$ o que implica que $m \mid (a-c)$, logo $a \equiv c \pmod{m}$. O item (4) é análogo ao item (3), e o item (5) decorre do item (4) haja vista que pelo item (1) $c \equiv c \pmod{m}$. Já o item (6), se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então existem q_1, q_2 tais que

$$a - b = mq_1 \text{ e } c - d = mq_2 \text{ o que implica } ac = (b + mq_1)(d + mq_2).$$

Logo $ac = bd + m(bq_2 + bq_1 + q_1q_2m)$, daí $m \mid ac - bd$ e, por consequência, $ac \equiv bd \pmod{m}$. O item (7) decorre do item (6) e por fim, o item (8) vem do fato que se $m \mid (a+c)-(b+c)$ então $m \mid a-b$ e, portanto, $a \equiv b \pmod{m}$.

■

Uma outra maneira de pensar em a, b congruentes módulo m é analisando seus restos na divisão por m. É fácil ver que dizer que $a \equiv b \mod m$ é equivalente a a e b deixarem o mesmo resto na divisão por m.

Há muitas aplicações de congruências, muitos são os problemas que são solucionados a partir delas. Vejamos no exemplo abaixo, uma de suas utilidades.

Exemplo 6: Verificaremos agora, por indução matemática, que $10^n \equiv 4 \pmod{6}$ para todo $n \in \mathbb{N}^*$.

Com efeito, para $n = 1$, temos $10 \equiv 4 \pmod{6}$, pois $6 \mid 10-4$. Agora admita que $10^n \equiv 4 \pmod{6}$. Multiplicando por 10 temos $10 \cdot 10^n \equiv 10 \cdot 4 \equiv 40 \equiv 4 \pmod{6}$, pois $6 \mid 40-4$. Ou seja, verificamos que $10^{n+1} \equiv 4 \pmod{6}$. Por indução matemática, segue que $10^n \equiv 4 \pmod{6}$ para todo $n \in \mathbb{N}^*$ o conjunto dos números naturais sem o zero.

2.4 Teoremas essenciais

Nesta seção, veremos alguns teoremas utilizados de forma recorrente neste trabalho. Por não ser o foco, algumas demonstrações serão omitidas, vejamos primeiramente o Pequeno Teorema de Fermat.

Teorema 14: (Pequeno Teorema de Fermat).
Sejam p um primo e a um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \pmod{p}$.

O leitor pode encontrar esta prova nas págs. 126 e 127 em [5].

Corolário 14.1: Sejam p um primo e a um inteiro arbitrário. Então $a^p \equiv a \pmod{p}$.

Demonstração: Suponha inicialmente que $p \mid a$. Temos assim $p \mid a^p - a$. Suponha agora que $p \nmid a$. Ora, nesta situação $p \mid a^{p-1} - 1$ pelo Pequeno Teorema de Fermat. Daí segue que $p \mid a^p - a$.

■

Exemplo 7: Seja a um inteiro arbitrário. Prove que os algarismos da casa das unidades de a e de a^5 são iguais, ou seja, $a^5 \equiv a \pmod{10}$.

Pelo Pequeno Teorema de Fermat temos que $a^5 \equiv a \pmod{5}$, ou seja, $5 \mid (a^5 - a)$. Por outro lado temos que $2 \mid (a^5 - a)$, já que ambos serão pares ou ambos serão ímpares. E, como $mdc(2, 5) = 1$, temos que $10 \mid (a^5 - a)$. Pelo teorema 6.

Logo $a^5 \equiv a \pmod{10}$.

Definição 9: A função $\phi : \mathbb{N}^* \to \mathbb{N}$, definida por:

$$\begin{cases} \phi(1) = 1 \\ \phi(n) = \text{quantidades de elementos relativamente primos com } n \text{ menores que } n, \end{cases}$$

é dita função ϕ de Euler.

Exemplo 8: Vamos encontrar o $\phi(24)$

Para calcular $\phi(24)$ precisamos encontrar os números, menores que 24, que são relativamente primos com ele. Com efeito, note que os números relativamente primos com 24 na lista {1, 2, 3, ..., 24 } é constituída por {1, 5, 7, 11, 13, 17, 19, 23}.

Portanto $\phi(24) = 8$.

Como forma de generalização do Pequeno Teorema de Fermat, Euler publicou em 1747 o teorema a seguir.

Teorema 15: (Teorema de Euler) Sejam a e n relativamente primos, com $n \geq 1$. Então, $a^{\phi(n)} \equiv 1 \pmod{n}$.

Note que se p é um primo, então $\phi(p) = p - 1$, logo podemos ver que o Pequeno Teorema de Fermat é um caso particular do Teorema de Euler. A demonstração deste teorema pode ser encontrada nas págs. 129 e 130 em [5].

Exemplo 9: O Teorema de Euler nos auxilia no cálculo de congruências. Como exemplo vamos calcular o resto de 5^{10} por 24.

Pelo Teorema de Euler que $5^{\phi(24)} \equiv 1 \pmod{24}$. Com base no exemplo anterior, $\phi(24) = 8$. Deste modo $5^8 \equiv 1 \pmod{24}$. Consequentemente, $5^8 \cdot 5^2 \equiv 1 \cdot 5^2 = 25 \equiv 1 \pmod{24}$. Isto mostra que o resto da divisão de 5^{10} por 24 é 1.

Teorema 16: (Teorema de Wilson).

Seja p um primo. Então $(p - 1)! + 1 \equiv 0 \pmod{p}$.

O leitor pode encontrar a prova deste teorema nas págs. 132 e 133 de [5].

Exemplo 10: Vamos calcular o resto da divisão de 15! por 17.

De acordo com o Teorema de Wilson, $16! \equiv -1 \pmod{17}$. Haja vista que $16 \equiv -1 \pmod{17}$, segue que $-1 \cdot 15! \equiv -1 \pmod{17}$. Assim $15! \equiv 1 \pmod{17}$ e, portanto, o resto da divisão de 15! por 17 é 1.

2.5 Congruências lineares

Nesta seção, veremos brevemente as congruências lineares, que são congruências da forma $aX \equiv b \pmod{m}$, em que a, b, m são coeficientes inteiros dados com m positivo. Vejamos de forma mais formal a definição .

Definição 10: Sejam a, b, m inteiros com $m > 0$. A equação $aX \equiv b \pmod{m}$ é chamada congruência linear.

Naturalmente poderíamos nos perguntar se tais congruências possuem solução, se sim, como determiná-las. O próximo teorema esclarece algumas destas dúvidas.

Teorema 17: Sejam a, b, m inteiros com $m > 0$. A congruência $aX \equiv b \pmod{m}$ tem solução se , e somente se, $d = mdc(a, m)$ divide b.

A prova deste teorema pode ser encontrada a partir da pág. 112 em [5]. Sabendo agora como identificar congruências que possuem solução, será que podemos determinar uma forma de encontrar tais soluções? Vejamos o próximo teorema.

Teorema 18: Sejam a e m inteiros, $d = mdc(a, m)$ e b um múltiplo de d. Escrevendo $d = ra + sm$ com r, s inteiros e $b = b_1 d$, a congruência $aX \equiv b \pmod{m}$ tem d soluções não congruentes, duas a duas, módulo m, a saber:

$$x_0 = rb_1,\ x_1 = rb_1 + \frac{m}{d},\ x_2 = rb_1 + \frac{2}{d}m, \cdots,\ x_{d-1} = rb_1 + \frac{d-1}{d}m.$$

Toda outra solução é congruente a uma dessas, módulo m.

E deste teorema decorre o corolário abaixo.

Corolário 18.1: Se a e m são inteiros relativamente primos, a congruência $aX \equiv b \pmod{m}$ tem sempre solução. Escrevendo $1 = ra + sm$, temos que $x = rb$ é uma solução e é única módulo m.

A prova, tanto do teorema quanto do corolário seguem das páginas 112,113 e 114 em [5].

Exemplo 11: Vamos encontrar a solução da congruência $-3X \equiv 18 \pmod{15}$

Note que $mdc(-3, 15) = 3$. Podemos escrever $3 = 4(-3) + 1 \cdot 15$, ou seja, temos que $r = 4$. Também podemos calcular $b_1 = 18/3 = 6$. Daí concluímos que $x_0 = rb_1 = 4 \cdot 6 = 24$ é uma solução. Calculando $x_1 = rb_1 + \frac{m}{d} = 24 + \frac{15}{3} = 24 + 5 = 29$ e $x_2 = rb_1 + \frac{2m}{d} = 24 + \frac{30}{3} = 24 + 10 = 34$, que também são soluções da congruência. Pelo Teorema 18, estas são as únicas soluções haja vista que todas outras serão congruentes a uma destas módulo 15.

Definição 11: Sejam a, m inteiros com $m > 1$. Diz-se que a é invertível módulo m quando existe um inteiro b tal que $ab \equiv 1 \pmod{m}$

Note que os números 2 e 5 são invertíveis módulo 7, pois $2 \cdot 4 \equiv 1 \mod 7$ e $5 \cdot 3 \equiv 1 \mod 7$. O número 3, por sua vez, não é invertível módulo 6.

3

Congruência de grau 2

Este capítulo foi baseado no livro [4]. Como vimos anteriormente, existem congruências simples, como é o caso da congruência do tipo $ax + b \equiv 0 \pmod{m}$. Mas será que este é o único tipo de congruência que podemos ter? A resposta é não. Assim como nas equações que podem ter graus maiores que 1, as congruências também não se limitam apenas ao primeiro grau. Nesta parte, estudaremos as congruências de grau 2, e veremos uma prova para o Teorema da Reciprocidade Quadrática de Gauss.

Figura 3.1: Carl Friedrich Gauss.
Fonte: (https://bityli.com/FdnGM6) acessado em 10/06/2021.

Carl Friedrich Gauss foi um grande matemático alemão do seculo XIX, nascido no ano de 1977. Aos 19 anos, ele conseguiu provar algo surpreendente. Ele provou que polígonos regulares de lados primos podem ser construídos com régua e compasso se, e somente se, tais primos são da forma $2^{2^n} + 1$. A história conta que ele começou quando descobriu, ainda com 19 anos, que um polígono regular de 17 lados podia ser construído com régua e compasso. Seu orgulho foi tão grande, que pediu para gravarem em sua lápide um polígono de 17 lados, o que não ocorreu. Porém este

símbolo pode ser encontrado na base de sua estátua em Brunswick, cidade natal do matemático.

Definição 12: Sejam $p > 2$ um primo e a,b,$c \in \mathbb{Z}$ tais que $p \nmid a$ e $a \neq 0$. A congruência

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

é dita **congruência de grau 2 módulo** p.

É fácil ver que $ax^2 + bx + c \equiv 0 \pmod{p}$ é equivalente a $4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}$, que por sua vez, também é equivalente a $(2ax+b)^2 - b^2 + 4ac \equiv 0 \pmod{p}$. E isso só ocorre, se, e somente se, $(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$.

Definição 13: Diz-se que $d \in \mathbb{Z}$ é um resíduo quadrático módulo p primo, quando a congruência

$$X^2 \equiv d \pmod{p}$$

tiver solução.

Existem exatamente $(p + 1)/2$ resíduos quadráticos módulo p, com p primo, são eles :

$$0^2, 1^2, 2^2, 3^2, ... \left(\frac{p-1}{2}\right)^2 \mod p.$$

Tendo em vista que para todo $x \in \mathbb{Z}$, $x \equiv \pm i \mod p$ para algum i tal que $0 \leq i \leq (p-1)/2$, segue que x^2 é congruente a algum dos números da lista acima.

Exemplo 12: Vamos encontrar os resíduos quadráticos módulo 7.

Há 7 restos possíveis na divisão por 7, 0, 1, 2, 3, 4, 5, 6. Assim os resíduos módulo 7 são: $0^2 = 0$, $1^2 = 1$, $2^2 = 4$, $3^2 = 2$, $4^2 = 2$, $5^2 = 4$, $6^2 = 1$. Note que bastava olhar para 0^2, 1^2, 2^2 e 3^2 , uma vez que 4=-3, 5=-2 e 6=1 módulo 7.

Afirmamos que os elementos do conjunto $\{0^2, 1^2, \cdots, (\frac{p-1}{2})^2\}$ são dois a dois não congruentes módulo p. De fato, considere $i, j \in \{0, 1, 2, \cdots, \frac{p-1}{2}\}$ e suponha que $i^2 \equiv j^2 \pmod{p}$. Temos assim $p \mid (i + j)(i - j)$. Logo $p \mid i + j$ ou $p \mid i - j$. Tendo em mente que $i, j \in \{0, 1, 2, \cdots, \frac{p-1}{2}\}$, a única maneira de $p \mid i + j$ ou $p \mid i - j$ é com $p \mid i - j$, sendo assim $i = j$.

3.1 Símbolo de Legendre

Vejamos a definição do símbolo de Legendre. Ela irá nos auxiliar no decorrer de nossos estudos.

Definição 14: Sejam $p > 2$ um primo e a um inteiro qualquer. Definiremos o **símbolo**

de Legendre como:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{se } p \nmid a \text{ e } a \text{ é um resíduo quadrático} \\ 0 & \text{se } p \mid a \\ -1 & \text{caso contrário} \end{cases}$$

Assim, para sabermos se a é resíduo quadrático módulo p (primo maior que 2) basta calcularmos o símbolo de Legendre $\left(\frac{a}{p}\right)$. Para nos auxiliar neste trabalho temos o critério de Euler.

Teorema 19: (Critério de Euler) Sejam $p > 2$ um primo e a um inteiro qualquer tal que $mdc(a, p) = 1$. Então:

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

DEMOSTRAÇÃO: Para $a \equiv 0 \pmod{p}$ o resultado é valido, então podemos supor $p \nmid a$. Sabemos, pelo Pequeno Teorema de Fermat, que $a^{p-1} \equiv 1 \pmod{p}$, em que

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}$$

o que ocorre se, e somente se, $p \mid a^{\frac{p-1}{2}} - 1$ ou $p \mid a^{\frac{p-1}{2}} + 1$. Isto por sua vez só acontece se $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Agora devemos mostrar que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ se, e somente se, a é um resíduo quadrático módulo p. Primeiramente verificaremos que se $x^2 \equiv a \pmod{p}$ não tem solução, então $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Com efeito, seja $r \in \{1, 2, ..., p-1\}$. A congruência linear $rx \equiv a \pmod{p}$ possui solução única módulo p. Seja $r' \in \{1, 2, ..., p-1\}$ tal que $rr' \equiv a \pmod{p}$. Haja vista que $x^2 \equiv a \pmod{p}$ não possui solução, temos que $r \neq r'$. Agrupando os elementos de $\{1, 2, ..., p-1\}$ aos pares de tal modo que o produto de dois elementos de cada par seja igual a a, temos pelo Teorema de Wilson que,

$$-1 \equiv (p-1)! \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Agora, provaremos que se $x^2 \equiv a \pmod{p}$ tem solução, então $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. Inicialmente, note que se $x_1, x_2 \in \{1, 2, ..., p-1\}$ e $x_1 \equiv x_2 \equiv a \pmod{p}$, então $p \mid x_1^2 - x_2^2$, ou seja, $p \mid (x_1 + x_2)(x_1 - x_2)$. Logo, $p \mid x_1 + x_2$ ou $p \mid x_1 - x_2$. No primeiro caso, $x_1 = p - x_2$; no segundo caso, $x_1 = x_2$. Para finalizar mostraremos que existem apenas duas soluções distintas em $\{1, 2, ..., p-1\}$ para $x^2 \equiv a \pmod{p}$, provaremos que $x_2 \not\equiv p - x_2 \pmod{p}$. De fato, se assim não fosse, teríamos $x_2 \equiv p - x_2 \pmod{p}$ e, consequentemente, $p \mid 2x_2$. Ora, mas isto é um absurdo, o número p é primo maior do que 2 e $x_2 \in \{1, 2, ..., p-1\}$. Cientes de que existem (apenas) duas soluções em $\{1, 2, ..., p-1\}$ para $x^2 \equiv a \pmod{p}$, considere r e $r' = p - r$ estas soluções. Note que $rr' \equiv r(p-r) \equiv rp - r^2 \equiv -r^2 \equiv -a \pmod{p}$. Os elementos de $\{1, 2, ..., p-1\} - \{r, r'\}$ se agrupam em pares distintos s e s' tais que $ss' \equiv a$

(mod p). Pelo Teorema de Wilson temos que

$$-1 \equiv (p-1)! \equiv -a(a)^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p},$$

com isso, mostramos que $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

■

Corolário 19.1: O símbolo de Legendre possui as seguintes propriedades:

1. Se $a \equiv b \pmod{p}$ e $mdc(a,p) = mdc(b,p) = 1$,então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2. $\left(\frac{a^2}{p}\right) = 1$ se $p \nmid a$.
3. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.
4. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, se $mdc(a,p) = mdc(b,p) = 1$.

Demonstração: Os itens 1 e 2 seguem imediatamente da definição, e o item 3 segue do Critério de Euler. De fato, $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ implica que $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, já que $p > 2$. Provaremos agora o item 4.

Aplicando o Critério de Euler, temos que $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$.

■

Dando prosseguimento aos estudos, vejamos agora o Lema de Gauss.

Lema 19.1: (Lema de Gauss)
Sejam $p > 2$ um primo e $a \in \mathbb{Z},$ com $a > 0,$ tais que $mdc(a,p) = 1$. Seja s o número de elementos do conjunto

$$\{a, 2a, 3a, ..., \tfrac{p-1}{2} \cdot a\}$$

tais que seu resto, na divisão por p, é maior do que $\frac{p-1}{2}$. Então

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Demonstração: Inicialmente, note que o conjunto A= $\{\pm 1, \pm 2, ..., \pm\frac{p-1}{2}\}$ tem $p-1$ elementos, os elementos são dois a dois não congruentes módulo p e, além disso, todos eles são invertíveis módulo p.

Para cada $j = 1, ..., \frac{p-1}{2}$, podemos escrever $a \cdot j \equiv \epsilon_j m_j \pmod{p}$ com $\epsilon_j \in \{-1, 1\}$ e $m_j \in \{1, ..., \frac{p-1}{2}\}$. Por um raciocínio de rotina, pode-se verificar que se $i \neq j$, com $i, j \in \{1,...,\frac{p-1}{2}\}$, então $m_i \neq m_j$. Deste fato segue que $\{m_1, ..., m_{\frac{p-1}{2}}\} = \{1, ..., \frac{p-1}{2}\}$.

Multiplicando as congruências $a \cdot j \equiv \epsilon_j m_j \pmod{p}$, temos

$$(a\cdot 1)\cdot(a\cdot 2)\cdots(a\cdot\frac{p-1}{2})\equiv \epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}}\cdot m_1m_2\cdots m_{\frac{p-1}{2}} \pmod p.$$

Isto é

$$a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\equiv \epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!$$

À luz da invertibilidade de $(\frac{p-1}{2})!\pmod p$, segue que

$$a^{\frac{p-1}{2}}\equiv \epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}} \pmod p.$$

Pelo o Critério de Euler, temos

$$\left(\frac{a}{p}\right)\equiv \epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}} \pmod p.$$

Visto que $\left(\frac{a}{p}\right), \epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}}\in\{-1,1\}$, concluímos que

$$\left(\frac{a}{p}\right)=\epsilon_1\cdot\epsilon_2\cdots\epsilon_{\frac{p-1}{2}}=(-1)^s,$$

sendo s o número de elementos em $\epsilon_1,...,\epsilon_{\frac{p-1}{2}}$ iguais a $a-1$, isto é, o número de elementos do conjunto $\{a,2a,...,\frac{p-1}{2}a\}$ tais que, seu resto, na divisão por p, é maior que 1.

■

No teorema abaixo, para $a\in[0,\infty)$, denotaremos por $\lfloor a\rfloor$ como a parte inteira de a. Enfim o Teorema da Reciprocidade Quadrática.

Teorema 20: Reciprocidade Quadrática

1. Sejam p e q primos ímpares distintos .Então :

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

2. Seja p um primo ímpar. Então

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=\begin{cases}1 & \text{se } p\equiv\pm1 \pmod 8\\ -1 & \text{se } p\equiv\pm3 \pmod 8\end{cases}.$$

DEMOSTRAÇÃO: Recorreremos ao Lema de Gauss para provarmos o item 2. Se $p\equiv 1 \pmod 4$, ou seja, $p=4k+1$, temos $\frac{p-1}{2}=2k$. Então seja $1\le 2j\le\frac{p-1}{2}$ para $j\le k$ e $\frac{p-1}{2}<2j\le p-1$ para $k+1\le j\le 2k$.Note que há k elementos em $\{k+1,...,2k\}$.

Temos:

$$\left(\frac{2}{p}\right) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 8 \\ -1, & \text{se } p \equiv 5 \pmod 8 \end{cases}.$$

Se $p \equiv 3 \pmod 4$, digamos $p = 4k+3$, temos $(p-1)/2 = 2k+1$. Com $1 \leq j \leq k$ temos $1 \leq 2j \leq \frac{p-1}{2}$. Para $k+1 \leq j \leq 2k+1$, há k elementos em $\{k+1,...,2k\}$, temos $\frac{p-1}{2} < 2j \leq p-1$, em que

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod 8 \\ 1, & \text{se } p \equiv 7 \pmod 8 \end{cases}.$$

Por fim, note que $\frac{p^2-1}{8}$ é um numero inteiro par quando $p \equiv \pm 1 \mod 8$. E $\frac{p^2-1}{8}$ é um número ímpar quando $p \equiv \pm 3 \mod 8$. Para provar o item 1 da Lei da Reciprocidade Quadrática, vamos mostrar que

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \tag{1}$$

e que

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor} \quad \text{e} \quad \left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor}. \tag{2}$$

O somatório $\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor$ é uma contagem de pontos de coordenadas inteiras no interior de um retângulo de vértices $(0,0), (p/2,0), (0,q/2), (p/2,q/2)$, acima da reta $y = \frac{q}{p}x$.

O somatório $\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor$ é uma contagem de pontos de coordenadas inteiras no interior de um retângulo de vértices $(0,0), (p/2,0), (0,q/2), (p/2,q/2)$, abaixo da reta $y = \frac{q}{p}x$.

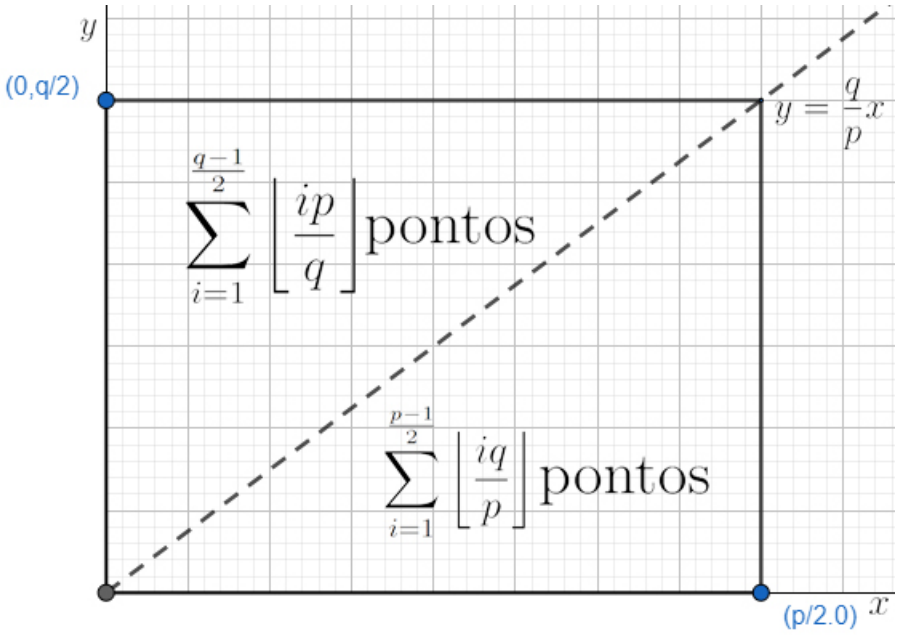


Figura 3.2: Gráfico dos pontos.
Fonte: Feito no GeoGebra inspirado no gráfico da página 93 de [4]

Para mostrar a segunda equação, primeiro item, é suficiente verificar que

$$\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2$$

em que s é como no Lema de Gauss aplicado para $a = q$. Seja r_i o resto da divisão de iq por p, de modo que $iq = \left\lfloor \frac{ip}{q} \right\rfloor p + r_i$. Somando e utilizando a notação da demonstração do Lema de Gauss, obtemos

$$q\sum_{i=1}^{\frac{p-1}{2}} i = p\sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (p - m_i).$$

Tendo em mente p e q são impares módulo 2 temos

$$\sum_{i=1}^{\frac{p-1}{2}} i \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{r_i<p/2} m_i + \sum_{r_i>p/2} (1 + m_i). \pmod 2.$$

Note que $\{m_1, m_2, ..., m_{\frac{p-1}{2}}\}=\{1, 2, ..., \frac{p-1}{2}\}$. Logo

$$\sum_{i=1}^{\frac{p-1}{2}} i \equiv \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor + \sum_{i=1}^{\frac{p-1}{2}} i + \sum_{r_i>p/2} 1. \pmod 2 \text{ se, e somente se, } \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor \equiv s \pmod 2.$$

De modo análogo, verifica-se que $\sum_{i=1}^{\frac{q-1}{2}} \left\lfloor \frac{ip}{q} \right\rfloor \equiv s \mod 2$. em que s é como Lema de Gauss aplicado para $a = p$. A prova esta concluída.

■

4

Ternas Pitagóricas

Este próximo capítulo foi baseado no estudo realizado em [9]. Muito mistério há em volta da figura de Pitágoras. Pelo que se sabe, Pitágoras nasceu na ilha de Samos, na antiga Grécia, em meados de 572 a.C.. É provável que Pitágoras fosse discípulo de Tales, grande filósofo e matemático grego. Depois de passar alguns anos no Egito, Pitágoras foi a uma colônia grega, situada no sul da Itália, e lá fundou a famosa escola pitagórica, um local criado para o estudo da matemática, filosofia, e ciências naturais.

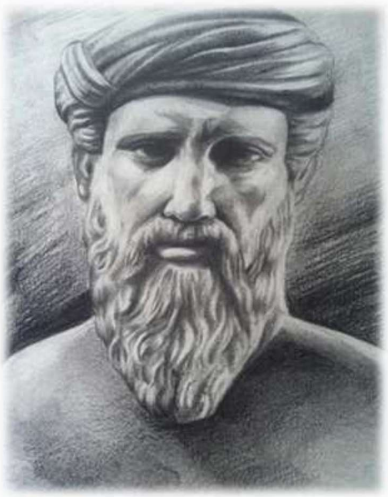


Figura 4.1: Pitágoras
Fonte: https://bityli.com/XFOoGEAx acessado dia 19/10/2022 às 15:30h.

Segundo registros históricos, uma das maiores contribuições da escola pitagórica é o Teorema de Pitágoras, que diz que dado um triangulo retângulo, a soma dos quadrados das medidas dos catetos (lados que formam o angulo reto) é igual ao quadrado da medida da hipotenusa (lado oposto ao angulo reto), ou seja, se c é a medida da hipotenusa, e b e a são as medidas dos catetos, é correto afirmar que

$$c^2 = a^2 + b^2.$$

Definição 15: Sejam a, b e $c \in \mathbb{N}^*$. A terna (a, b, c) é pitagórica se :

$$a^2 + b^2 = c^2.$$

Uma terna pitagórica é dita primitiva se o $mdc(a,b,c) = mdc((a,b),c) = 1$. Dito isto nosso objetivo é encontrar este tipo de terna pitagórica. Podemos supor a,b e c relativamente primos dois a dois, tendo em vista que se existe um p primo tal que $p|mdc(a,b)$ implica que $p|a^2 + b^2$ e, consequentemente, $p|c$. Podemos observar que a e b não podem ser pares ao mesmo tempo no caso em que (a, b, c) é primitiva. Logo podemos supor a ímpar. Além disto observemos que $(2k + 1)^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$ e $(2k)^2 \equiv 0 \pmod 4$, ou seja, quadrados perfeitos são congruentes a 0 ou 1 módulo 4. Portanto b é par , pois se b é ímpar temos $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 4$, o que é impossível. Resumindo temos a par, b ímpar e c ímpar também.

Assim:

$$b^2 = c^2 - a^2 = (c - a)(c + a).$$

Seja $d = mdc(c - a,c + a)$. Então d divide

$$(c - a) + (c + a) = 2c \text{ e } (c + a) - (c - a) = 2a,$$

ou seja, $d|mdc(2a,2c) = 2mdc(a,c) = 2$, pois $mdc(a,c) = 1$. Mas como $c - a$ e $c + a$ são ambos pares, temos $d = 2$ e $mdc\left(\frac{c-a}{2}, \frac{c+a}{2}\right) = 1$. Podemos então dizer que

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

Como $\dfrac{c+a}{2}$ e $\dfrac{c-a}{2}$ são relativamente primos e seu produto é um quadrado perfeito, pelo Teorema Fundamental da Aritmética, segue que cada um destes fatores deve ser o quadrado perfeito de um numero natural. Logo temos,

$$\frac{c+a}{2} = m^2, \qquad \frac{c-a}{2} = n^2, \qquad b = 2mn, \text{ pois } b^2 = (c-a)(c=a) = 4m^2n^2,$$

sendo $mdc(m.n) = 1$.

Em termos de m e n, temos a, b, c como:

$$a = m^2 - n^2, \qquad b = 2mn \qquad c = m^2 + n^2, \text{ com } m > n.$$

E como c e ímpar, a paridade de m é diferente da paridade de n.

Pode-se verificar que se (a, b, c) é uma terna pitagórica, então

$$\left(\frac{a}{mdc(a,b,c)}, \frac{b}{mdc(a,b,c)}, \frac{c}{mdc(a,b,c)}\right)$$

é primitiva.

Exemplo 13: Vamos encontrar todas as ternas primitivas de números (a,b,c) tais

que a^2,b^2, c^2 estão em progressão aritmética.

A diferença de dois termos consecutivos é constante numa progressão aritmética, logo vamos dizer que a terna seja (a,b,c), assim:

$$b^2 - a^2 = c^2 - b^2,$$

ou seja, $a^2 + c^2 = 2b^2$, e disto temos que a e c têm a mesma paridade. Assim tomando $r = \frac{c+a}{2}$, $s = \frac{c-a}{2}$, temos $c = r + s$ e $a = r - s$. Note que $mdc(\frac{c+a}{2}, \frac{c-a}{2}) = 1$. Substituindo, temos:

$$2b^2 = a^2+c^2 = (r-s)^2+(r+s)^2 = [r^2-2rs+c^2]+[r^2+2rs+c^2] = 2r^2+2s^2 = 2(r^2+s^2).$$

Isto é,

$$b^2 = r^2 + s^2.$$

Logo existem m e n inteiros para terna (r, s, b) tais que

$$r = m^2 - n^2 \qquad s = 2mn \qquad b = m^2 + n^2,$$

com $m > n$, $mdc(m,n) = 1$.

Ou seja temos

$$a = |m^2-n^2-2mn| \quad b = m^2+n^2 \quad c = m^2-n^2+2mn \text{ com } m > n \text{ e } mdc(m,n) = 1$$

Assim determinamos todas as ternas primitivas que satisfazem a condição.

Exemplo 14: Vamos resolver em inteiros positivos a equação

$$x^{-2} + y^{-2} = z^{-2}$$

Fazendo uma manipulação simples, podemos concluir que a equação acima é equivalente a

$$x^2 + y^2 = \left(\frac{xy}{z}\right)^2.$$

O que nos diz que x^2+y^2 é um quadrado perfeito. Seja $t = \frac{xy}{z}$. Temos então $x^2+y^2 = t^2$ para algum inteiro positivo t. Seja $d = mdc(x, y, t)$. Então $x = ad, y = bd, t = cd$, em que $a, b, c \in \mathbb{N}^*$, com $mdc(a, b, c) = 1$. Então temos que $z = \frac{abd}{c}$ e

$$a^2 + b^2 = c^2.$$

Usando o fato que $c \mid abd$ e $mdc(a, b, c) = 1$, deduzimos que $c|d$,ou seja , $d = kc, k \in \mathbb{N}^*$. Daí

$$x = ad = kac, \quad y = bd = kbc, \quad t = cd = kc^2, \quad z = kab.$$

Utilizando o resultado geral das ternas pitagóricas primitivas (a, b, c), $a = m^2-n^2, b =$

$2mn, c = m^2 + n^2$, temos

$$x = k(m^4 - n^4),\ y = 2kmn(m^2 + n^2),\ z = 2kmn(m^2 - n^2)$$

sendo que $k, m, n \in \mathbb{N}^*$ e $m > n$ e $mdc(m,n) = 1$.

4.1 Método Geométrico

Usando ferramentas de geometria analítica, iremos resolver alguns problemas envolvendo ternas pitagóricas e algumas variações.

Exemplo 15: Determine todas as soluções inteiras da equação $a^2 + 2b^2 = 11c^2$.

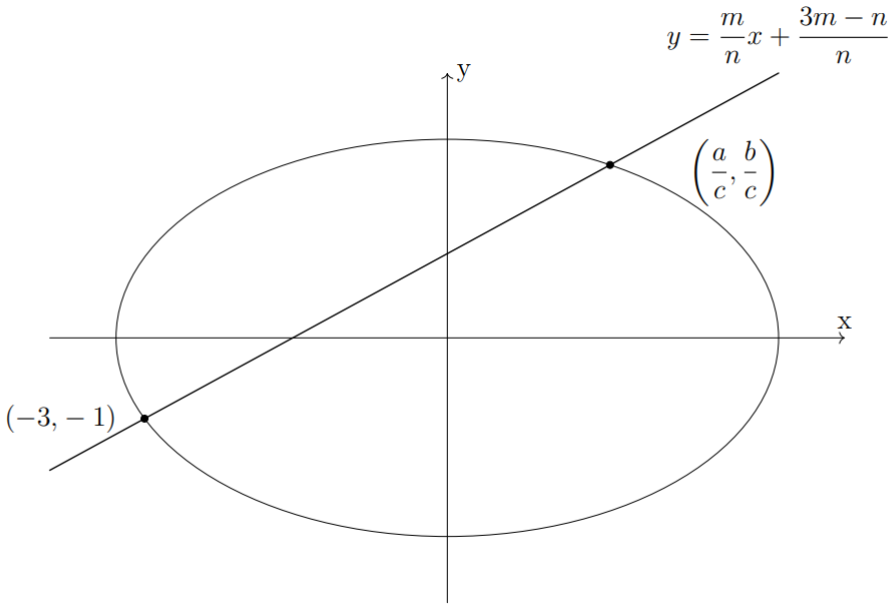


Figura 4.2: Interseção da reta com a elipse
Fonte: Autor, baseada na figura da pag. 122 do texto [9].

Divida a equação por c^2. Teremos

$$\left(\frac{a}{c}\right)^2 + 2\left(\frac{b}{c}\right)^2 = 11$$

Sejam $x = \frac{a}{c}$ e $y = \frac{b}{c}$. Temos $x^2 + 2y^2 = 11$, que geometricamente falando, representa uma elipse centrada na origem do plano cartesiano. Vejamos os pontos da elipse (3,1),(3,-1), (-3,1), (-3,-1) e o ponto $(\frac{a}{c}, \frac{b}{c})$. Seja então a reta que passa pelos pontos (-3,-1) e $(\frac{a}{c}, \frac{b}{c})$. Denotaremos a inclinação desta reta por $\frac{m}{n}$. Então a equação da reta será:

$$y = \frac{m}{n}(x + 3) - 1 = \frac{m}{n}x + \frac{3m - n}{n}.$$

Os pontos de interseção entre a reta e a elipse são dados pelas raízes da equação $11 = x^2 + 2(\frac{m}{n}x + \frac{3m-n}{n})^2$. Resolvendo esta equação temos:

$$11 = \frac{n^2+2m^2}{n^2}x^2 + 4x\frac{m(3m-n)}{n^2} + 2\frac{9m^2-6mn+n^2}{n^2}.$$

Multiplicando a equação de cima por $\dfrac{n^2}{n^2+2m^2}$

$$x^2 + 4\frac{m(3m-n)x}{n^2+2m} - 3\frac{3n^2+4mn-6m^2}{n^2+2m^2} = 0,$$

sendo que $2\cdot\frac{9m^2-6mn+n^2}{n^2} - 11 = -3\cdot\frac{3n^2+4mn-6m^2}{n^2}$. E como o ponto $(-3,-1)$ pertence tanto a reta quanto a elipse, temos que $x=-3$ é solução da equação. Além disso, temos que o coeficiente independente de uma equação quadrática, com o coeficiente líder igual a 1, é o produto das raízes. Portanto, a outra raiz é

$$\frac{a}{c} = x = \frac{3n^2+4mn-6m^2}{n^2+2m^2}.$$

E assim, substituindo $\frac{a}{c}$ em $y = \frac{m}{n}x + \frac{3m-n}{n}$, temos:

$$\frac{b}{c} = \frac{m}{n}\left(\frac{3n^2+4mn-6m^2}{n^2+2m^2}\right) + \frac{3m-n}{n} = \frac{2m^2+6mn-n^2}{n^2+2m^2}.$$

E como $\frac{a}{c} = \frac{3n^2+4mn-6m^2}{n^2+2m^2}$ e $\frac{b}{c} = \frac{2m^2+6mn-n^2}{n^2+2m^2}$, então existirá um k inteiro tal que:

$$a = \frac{k}{d}(3n^2+4mn-6m^2), \quad b = \frac{k}{d}(2m^2+6mn-n^2), \quad c = \frac{k}{d}(n^2+2m^2)$$

em que $d = mdc(3n^2+4mn-6m^2, 2m^2+6mn-n^2)$.

4.2 Método Aritmético Modular

Como vimos anteriormente, podemos usar outras áreas da matemática para nos ajudar. Vejamos como podemos utilizar a aritmética modular para resolver certos problemas.

Exemplo 16: A equação $x^2 = 3y^2 + 8$ não possui solução em inteiros x e y.

Analisemos esta equação, estrategicamente, módulo 3.

$$x^2 \equiv 3y^2 + 8 \pmod 3 \text{ implica que } x^2 \equiv 0 + 2 \pmod 3$$

o que implica em $x^2 \equiv 2 \pmod 3$.

Vejamos então se isto é possível. Se $x \equiv 1 \pmod 3$, então $x^2 \equiv 1 \pmod 3$, e se $x \equiv 2 \pmod 3$, então $x^2 \equiv 4 \equiv 1 \pmod 3$ e é obvio que se $x \equiv 0 \pmod 3$, x^2 também o será. Logo é impossível que aconteça o caso $x^2 \equiv 2 \pmod 3$. A equação diofantina não possui solução.

Exemplo 17: Não existe solução em inteiros positivos x, y, z com $z > 1$ para a equação

$$(x+1)^2 + (x+2)^2 + (x+3)^2 + \cdots + (x+99)^2 = y^z$$

De fato, utilizaremos os seguintes fatos bem conhecidos: $1+2+3+...+n = \frac{n(n+1)}{2}$ e $1^2+2^2+...+n^2 = \frac{n(n+1)(2n+1)}{6}$. Tais igualdades podem ser verificadas por indução matemática. Vejamos então que:

$$\begin{aligned} y^z &= (x+1)^2 + (x+2)^2 + (x+3)^2 + \cdots + (x+99)^2 \\ &= 99x^2 + 2(1+2+3+\cdots+99) + (1^2+2^2+3^2+\cdots+99^2) \\ &= 99x^2 + \frac{2\cdot 99\cdot 100}{2}x + \frac{99\cdot 100\cdot 199}{6} \\ &= 33(3x^2+300x+9950). \end{aligned}$$

O que implica que $3 \mid y$, e como $z \geq 2$, temos que $3^2 \mid y^z$. Note que $(3x^2+300x+9950) \equiv 2 \pmod 3$. Logo vemos que há uma contradição pois $3^2 \nmid 33(3^2+300x+9950)$, em outras palavras, não existe solução em inteiros x, y, z com $z > 1$ para a equação.

4.3 Método da Fatoração

Como já vimos antes, existem diferentes métodos de resoluções de equações diofantinas. Vejamos agora mais um, comecemos primeiro com um exemplo.

Exemplo 18: Determine todos os triângulos retângulos, de lados inteiros, em que um dos catetos mede 30.

Queremos achar as soluções da equação $a^2+900 = c^2$, sendo a e c inteiros positivos. Observe que

$$a^2 + 900 = c^2 \text{ o que implica que } 900 = c^2 - a^2, \text{ logo } 2^2\cdot 3^2\cdot 5^2 = (c+a)(c-a).$$

Note que $c-a$ e $c+a$ possuem a mesma paridade e são distintos, e mais ainda, eles são pares. Logo temos que distribuir os fatores de 900 em 2 números pares, vejamos as possibilidades:

$$\begin{cases} c+a = 450 \\ c-a = 2 \end{cases}, \begin{cases} c+a = 150 \\ c-a = 6 \end{cases}, \begin{cases} c+a = 90 \\ c-a = 10 \end{cases} \text{ e } \begin{cases} c+a = 50 \\ c-a = 18 \end{cases}.$$

Temos as ternas (30, 224, 226), (30, 72, 78), (30, 40, 50), (30, 16, 34).

Perceba que no exemplo usamos fatoração dos termos para resolver a terna, e é esta estratégia que damos o nome de método da fatoração. O método consiste em resolver uma equação $f_1(x_1, x_2, \cdots, x_n)\cdot f_2(x_1, x_2, \cdots, x_n)\cdots f_k(x_1, x_2, \cdots, x_n) = a$ com $a \in \mathbb{Z}$ e os termos $f_1, f_2, \cdots, f_k$ são polinômios com coeficientes inteiros. Posteriormente fatoramos a em fatores primos, conseguimos um número finito de

decomposição em inteiros $a_1, a_2, ..., a_k$. A partir deles formamos os sistemas:

$$\begin{cases} f_1(x_1, x_2, \cdots, x_n) = a_1 \\ f_2(x_1, x_2, \cdots, x_n) = a_2 \\ \vdots \\ f_k(x_1, x_2, \cdots, x_n) = a_k \end{cases}$$

E as soluções deste sistema coincidem com as soluções da equação.

5

Teorema de Lagrange

Este capítulo é baseado no no livro [7] e no trabalho [8]. Em meados de 1770, o matemático inglês Edward Waring apresentou um problema que ficou conhecido como Problema de Waring. Este problema pergunta se para cada inteiro k, existe a ele associado um inteiro positivo s de tal forma que qualquer natural n possa ser representado pela soma de no máximo s potencias de ordem k. Na mesma época, Lagrange ficou sabendo deste problema e formulou uma resposta para um caso, esta resposta ficou conhecida como Teorema de Lagrange.

O Teorema de Lagrange, que veremos mais abaixo, consiste em resolver o problema de Waring para $k = 2$, sendo $s = 4$ o menor s que podemos resolver o problema.Vejamos agora a definição matemática do Problema de Waring:

Definição 16: Problema de Waring. Para um determinado **k**, será que existe um número fixo **s = s(k)** tal que a equação

$$n = x_1^k + x_2^k + x_3^k + \cdots + x_s^k$$

tenha solução para todo $n \in \mathbb{N}$?

Agora enunciaremos alguns teoremas que serão usados para provar o Teorema de Lagrange.

Teorema 21: Seja p um primo ímpar, temos que:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \text{ se } p \equiv 1 \pmod 4 \\ \\ -1 \text{ se } p \equiv 3 \pmod 4 \end{cases}$$

Demonstração: Com base no Critério de Euler (capítulo 3, Teorema 15), sabemos que $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod p$. Sendo p um primo ímpar, duas situações

podem ocorrer,

1) $p \equiv 1 \pmod 4$, ou seja, existe, $k \in \mathbb{Z}$ tal que, $p = 4k + 1$.
2) $p \equiv 3 \pmod 4$, ou seja, existe, $k \in \mathbb{Z}$ tal que, $p = 4k + 3$.

No primeiro caso, $\frac{p-1}{2} = 2k$ e, portanto, $(-1)^{2k} = 1 \equiv \left(\frac{-1}{p}\right) \pmod p$. Isto mostra que $\left(\frac{-1}{p}\right) = 1$ se $p \equiv 1 \pmod 4$.

Quando temos $p \equiv 3 \pmod 4$, $\frac{p-1}{2} = 2k + 1$ e, consequentemente, $(-1)^{2k+1} = -1 \equiv \left(\frac{-1}{p}\right) \pmod p$. Assim $\left(\frac{-1}{p}\right) = -1$, se $p \equiv 3 \pmod 4$.

■

Teorema 22: Seja p um primo, a congruência $x^2 \equiv -1 \pmod p$ tem solução se, e somente se, $p = 2$ ou $p \equiv 1 \pmod 4$.

Demonstração: Inicialmente, suponha que $p = 2$ ou que p é um primo ímpar congruente a 1 módulo 4. Quando $p = 2$, a congruência $x^2 \equiv -1 \equiv 1 \pmod 2$ tem solução, a saber : $x \equiv 1 \pmod 2$.

Quando $p \equiv 1 \pmod 4$, segue do Teorema 21 que $\left(\frac{-1}{p}\right) = 1$, isto é, a congruência $x^2 \equiv -1 \pmod p$ tem solução.

Para finalizar, vamos analisar o caso em que $p \equiv 3 \pmod 4$. Novamente pelo Teorema 21, temos que $\left(\frac{-1}{p}\right) = -1$, quer dizer, a congruência $x^2 \equiv -1 \pmod p$ não tem solução.

■

Teorema 23: Para todo primo p, existem $a, b, c \in \mathbb{Z}$, tais que a congruência a seguir é satisfeita:

$$a^2 + b^2 + c^2 \equiv 0 \pmod p.$$

Demonstração: Vejamos, no caso em que $p = 2$ é evidente, basta tomar a = b = 1 e c = 0. Teremos $1^2 + 1^2 + 0^2 \equiv 0 \pmod 2$. Já no caso em que $p \equiv 1 \pmod 4$, se tomarmos $b = 1$ e $c = 0$, teremos que ter a como a solução da equação $x^2 \equiv -1 \pmod p$. Como vimos pelo Teorema 22, esta equação possui solução, uma vez que $p \equiv 1 \pmod 4$. Por fim, basta olhar os casos em que $p \equiv 3 \pmod 4$. Para estes casos, tomaremos $c = 1$. Mostraremos a existência de solução para a congruência $x^2 + y^2 \equiv -1 \pmod p$. Sabemos que existem, módulo p, apenas $\frac{p-1}{2}$ resíduos quadráticos e o mesmo número de resíduos não quadráticos. Então seja d o menor resíduo não-quadrático positivo em $\{0, 1, ..., p-1\}$. Daí temos:

$$\left(\frac{d}{p}\right) = -1$$

por definição. Pelo Teorema 21 temos que $\left(\frac{-1}{p}\right) = -1$, ou seja,

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

Logo $-d$ é um resíduo quadrático módulo p. Por $-d$ ser um resíduo quadrático módulo p, a congruência quadrática $x^2 \equiv -d \pmod{p}$ tem solução.

Mostraremos agora que existe b inteiro tal que $b^2 \equiv d-1 \pmod{p}$. Ao fazer isso, teremos que $x^2 + y^2 \equiv -1 \pmod{p}$ tem solução. De fato, $1 \leq d-1 \leq d$. Da minimalidade de d, segue que $y^2 \equiv d-1 \pmod{p}$ tem solução. O teorema esta demonstrado.

■

O próximo resultado é um teorema clássico da teoria dos números. Trata-se do Teorema de Fermat da soma de dois quadrados. O leitor interessado pode encontrar uma prova deste teorema na página 255 de [3].

Teorema 24: (Fermat) Um inteiro positivo é um quadrado ou a soma de dois quadrados de números naturais se, e só se, ele é da forma

$$a = 2^l b^2 p_1 \cdots p_r,$$

sendo que $l = 0, 1$; $b \in \mathbb{N}^*$, $r \geq 0$ e os p_i com $i = 1, 2, ..., r$ são primos distintos da forma $4k + 1$.

O Teorema de Fermat nos mostra que nem todo número inteiro positivo pode ser escrito como como a soma de dois quadrados. Um exemplo disso é o número 19.

Teorema 25: Todo número inteiro da forma $8a + 7$, com $a \in \mathbb{Z}$, não pode ser expresso como soma de três quadrados

Demonstração: Observe que todo número da forma $8a + 7$ é congruente a 7 módulo 8. Observe também que:

$$0^2 \equiv 0 \pmod{8}$$
$$1^2 \equiv 1 \pmod{8}$$
$$2^2 \equiv 4 \pmod{8}$$
$$3^2 \equiv 1 \pmod{8}$$
$$4^2 \equiv 0 \pmod{8}$$
$$5^2 \equiv 1 \pmod{8}$$
$$6^2 \equiv 4 \pmod{8}$$
$$7^2 \equiv 1 \pmod{8}$$

Com estas oito congruências e alguns cálculos de rotina, verificamos que a soma de três quadrados nunca é congruente com 7 módulo 8. Logo a equação $a^2 + b^2 + c^2 \equiv 7 \pmod 8$ não possui solução em inteiros, o que conclui a demonstração do teorema.

■

Consequentemente, nem todo número inteiro positivo se escreve como a soma de três quadrados. Um exemplo é o número 7.

Sejam a, b, c, d, r, s, t, v inteiros. A partir de manipulações algébricas usuais, podemos expressar $(a^2 + b^2 + c^2 + d^2) \cdot (r^2 + s^2 + t^2 + v^2)$ como a soma de quatro quadrados. Esta forma de reescrever $(a^2 + b^2 + c^2 + d^2) \cdot (r^2 + s^2 + t^2 + v^2)$ esta descrita na identidade abaixo, a Identidade 1.

Lema 25.1: (Identidade 1) Sejam $a, b, c, d, r, s, t, v \in \mathbb{Z}$. Sejam também, $g = a^2 + b^2 + c^2 + d^2,\ h = r^2 + s^2 + t^2 + v^2,\ i = ar + bs + ct + dv,\ j = as - br - cv + dt,\ k = at + bv - cr - ds,\ l = av - bt + cs - dr$.

Então vale a seguinte identidade:

$$g \cdot h = i^2 + j^2 + k^2 + l^2.$$

Teorema 26: Teorema de Lagrange

Todo número inteiro positivo possui uma representação como a soma de quatro quadrados

$$n = a^2 + b^2 + c^2 + d^2.$$

Demonstração

Como vemos pela Identidade 1, o produto entre duas somas de quatro quadrados também é uma soma de quatro quadrados. Mostraremos que todos os primos podem ser escritos como a soma de quatro quadrados.

Temos que $2 = 1^2 + 1^2 + 0^2 + 0^2$. Para p primo ímpar , pelo Teorema 23, existem $a, b, c \in \mathbb{Z}$ tais que

$$(1) \quad a^2 + b^2 + c^2 \equiv 0 \pmod p.$$

Ou seja

$$(2) \qquad a^2 + b^2 + c^2 + d^2 = Mp,$$

com M inteiro e $d = 0$. Considere o conjunto dos múltiplos de p que podem ser escritos como a soma de quatro quadrados $a^2 + b^2 + c^2 + d^2$, com d no intervalo $\left[0, \frac{p}{2}\right)$. Note que este conjunto é não vazio, pois Mp é um elemento deste conjunto. Então existe um m mínimo inteiro positivo que satisfaz:

$$a^2 + b^2 + c^2 + d^2 = mp \text{ com } d \in \left[0, \frac{p}{2}\right).$$

Note que podemos tomar a, b, c no intervalo $\left[0, \frac{p}{2}\right)$, uma vez que os termos estão ao quadrado em (1) e estamos trabalhando módulo p.

Logo

$$mp = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{p}{2}\right)^2 = p^2 \text{ o que implica que } m < p.$$

Agora basta provar que $m = 1$. Logo vamos supor por absurdo que $m > 1$. Separemos em dois casos, m ímpar e m par.

Seja $m > 1$ e m ímpar. Em

$$a^2 + b^2 + c^2 + d^2 = mp$$

podemos escolher a_1, b_1, c_1, d_1 em $\left[0, \frac{m}{2}\right)$ tais que,

$$a \equiv a_1 \pmod{m},\ b \equiv b_1 \pmod{m},\ c \equiv c_1 \pmod{m},\ d \equiv d_1 \pmod{m}.$$

E daí temos que $a_1^2 + b_1^2 + c_1^2 + d_1^2 \equiv 0 \pmod{m}$, o que garante a existência de $m' \geq 0$ tal que

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = mm',\ \text{com } m' < m \text{ pois } a_1, b_1, c_1, d_1 < \frac{m}{2}.$$

Supor $m' = 0$ nos leva a um absurdo, pois se $m' = 0$ temos que $a_1^2+b_1^2+c_1^2+d_1^2 = 0$ e portanto, $a_1 = b_1 = c_1 = d_1 = 0$. Logo $a \equiv b \equiv c \equiv d \equiv 0 \pmod{m}$, o que implica $m^2|mp$, daí, $m|p$, isto é absurdo, pois $m > 1$ e p é primo maior que m. Logo $m' \neq 0$. Usando a Identidade 1, temos:

$$mpm'm = (a^2 + b^2 + c^2 + d^2)(a_1^2 + b_1^2 + c_1^2 + d_1^2) = u^2 + v^2 + w^2 + x^2 \quad (3)$$

Em que $u = (aa_1+bb_1+cc_1+dd_1)$, $v = (ab_1-ba_1-cd_1+dc_1)$, $w = (ac_1+bd_1-ca_1-db_1)$ e $x = (ad_1 - bc_1 + cb_1 - da_1)$. E como $a \equiv a_1$, $b \equiv b_1$, $c \equiv c_1$, $d \equiv d_1 \pmod{m}$ e $a^2 \equiv aa_1$, $b^2 \equiv bb_1$, $c^2 \equiv cc_1$, $d^2 \equiv dd_1 \pmod{m}$ vemos que todos os termos do lado direito, dentro dos parênteses, são múltiplos de m. Logo existem inteiros $\overline{a}, \overline{b}, \overline{c}, \overline{d}$, tais que (3) pode ser escrito como

$$m^2m'p = (\overline{a}m)^2 + (\overline{b}m)^2 + (\overline{c}m)^2 + (\overline{d}m)^2.$$

Ou seja, $m'p = (\overline{a})^2 + (\overline{b})^2 + (\overline{c})^2 + (\overline{d})^2$ com $m' < m$, o que nos leva ao absurdo. Isso ocorre porque m é o menor inteiro positivo tal que mp se escreve como a soma de quatro quadrados.

Resta-nos agora mostrar que no caso m par também podemos encontrar $\overline{m} < m$ tal que $\overline{m}p$ é a soma de quatro quadrados.

É fácil ver que, para m par, necessariamente os inteiros a, b, c e d devem ser todos pares, dois pares e dois ímpares ou todos ímpares. Em qualquer um destes três casos, podemos escolher a, b, c e d satisfazendo $a \equiv b \pmod{2}$ e $c \equiv d \pmod{2}$, o que nos

permite escrever:

$$p\frac{m}{2} = \frac{a}{2}^2 + \frac{b}{2}^2 + \frac{c}{2}^2 + \frac{d}{2}^2 = \left(\frac{a-b}{2}\right)^2 + \left(\frac{a+b}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 + \left(\frac{c+d}{2}\right)^2.$$

Portanto, tomando $\overline{m} = \frac{m}{2} < m$, obtemos uma expressão para $\overline{m}p$ como a soma de quatro quadrados, o que é um absurdo.

Pelas observações feitas anteriormente, concluímos que $m = 1$, ou seja, o primo p pode ser expresso como soma de quatro quadrados.

O resultado geral segue do Teorema Fundamental da Aritmética e da Identidade 1.

■

6

Último Teorema de Fermat para n = 3 e 4

Este capítulo foi escrito baseado em [1] e no livro [4]. Enunciado por Fermat em 1637, este teorema, conhecido como Último Teorema de Fermat, intrigou, por muitos e muitos anos, por volta de 300 anos, vários matemáticos. Somente em 1995 Andrew Wiles, com apoio de Richard Taylor, conseguiu provar o teorema.

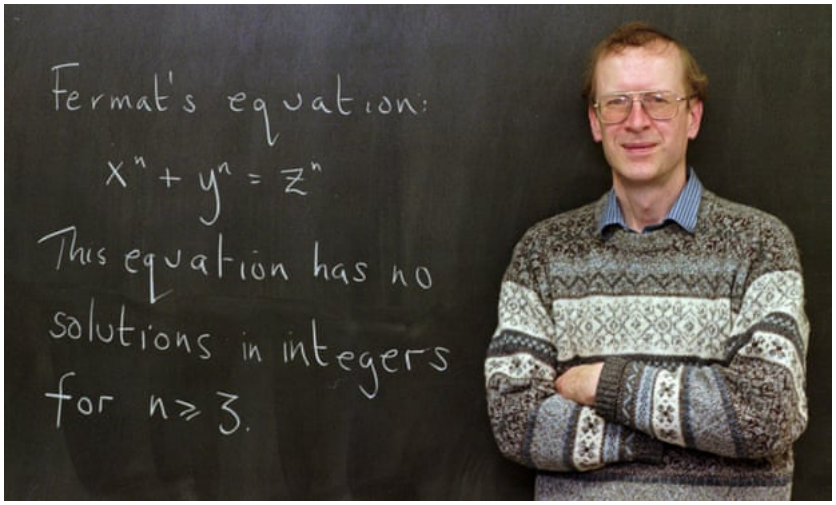


Figura 6.1: Andrew Wiles.
Fonte:(https://bityli.com/lxirZ) acessado em 10/06/21.

Nesta parte iremos ver uma prova do Último Teorema de Fermat para os casos $n = 3$ e $n = 4$. Primeiramente vejamos o enunciado deste teorema.

Teorema 27: (Último Teorema de Fermat)
A equação $x^n + y^n = z^n$ não possui solução em inteiros positivos quando n é um número natural é maior que 2.

Figura 6.2: Pierre de Fermat.
Fonte:(https://bityli.com/mts8i) acessado em 10/06/2021.

Este famoso teorema, como dito anteriormente, intrigou os matemáticos por mais de 300 anos até ser provado. Lagrange e Euler são alguns exemplos de pessoas que tentaram resolver este problema, este último ainda conseguiu provar o caso $n = 3$. Fermat, em suas anotações, as margens do livro *Aritmética* de Diofanto, escreveu que tinha a prova e que era bela, porém não caberia naquele espaço. Todavia esta prova nunca foi encontrada.

Agora, vamos ver estes casos, para provarmos o caso $n = 4$, usaremos o Descenso Infinito de Fermat.

Definição 17: Descenso Infinito de Fermat.

O método do Descenso Infinito de Fermat consiste em :

1. Suponha que a equação dada possui solução .
2. Daí suponha que exista uma solução, de alguma forma, mínima.
3. E por fim, encontre uma solução menor do que a mínima, contradizendo a hipótese de existir uma solução.

A resolução do problema abaixo implica o Último Teorema de Fermat para $n = 4$

Teorema 28: A equação $x^4 + y^4 = z^2$ não possui solução em inteiros positivos.

Demostração: Suponha que exista uma solução $x, y, z > 0$. Logo existe a solução (a, b, c) com c mínimo. Em particular temos que $mdc(a, b) = 1$, pois se $mdc(a, b) = d > 1$, poderíamos substituir (a, b, c) por $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d^2})$ que é uma solução com c menor. Agora observe que

$$a^4 + b^4 = c^2 \text{ o que implica que } (a^2)^2 + (b^2)^2 = c^2.$$

Logo (a^2, b^2, c) é uma tripla primitiva, ou seja, existem $m, n \in \mathbb{Z}$ com $m+n$ ímpar e $mdc(m,n) = 1$, tais que

$$a^2 = m^2 - n^2, \qquad b^2 = 2mn, \qquad c = m^2 + n^2.$$

Como m e n possuem paridades distintas, neste caso temos que m é ímpar, pois caso

o contrário teríamos $m = 2e$ e $n = 2f + 1$ com $e, f \in \mathbb{N}^*$, e então $a^2 \equiv 0 - 1 \equiv 3 \pmod 4$, absurdo. Isto porque $a^2 \equiv 0 \pmod 4$ ou $a^2 \equiv 1 \pmod 4$.

Observando que $b^2 = (2n)m$ é um quadrado perfeito e $mdc(2n, m) = 1$ (pois $mdc(m, n) = 1$ e m é impar), concluímos que tanto $2n$ como m são quadrados perfeitos. Podemos encontrar inteiros positivos s e t tais que

$$2n = s^2, \quad m = t^2.$$

Por outro lado, dado que $a^2 + n^2 = (m^2 - n^2) + n^2 = m^2$, existirão inteiros positivos i e j, são relativamente primos, tais que

$$a = i^2 - j^2, \;\; n = 2ij \text{ e } \; m = i^2 + j^2.$$

Portanto, $\frac{s^2}{4} = \frac{n}{2} = ij$; logo, i e j serão quadrados perfeitos. Digamos $i = u^2$ e $j = v^2$.

Logo, temos que $m = i^2 + j^2, i = u^2, j = v^2$ e $m = t^2$, consequentemente,

$$t^2 = u^4 + v^4.$$

Isto é, (u, v, t) é outra solução da equação original. Porém,

$$t \leq t^2 = m \leq m^2 < m^2 + n^2 = c,$$

e $t \neq 0$, pois m é diferente de 0. Isto contradiz a minimalidade de c, o que conclui a demonstração.

■

Teorema 29: (Ultimo Teorema de Fermat para n=4)
Não existem inteiros x, y e z tais que $x^4 + y^4 = z^4$.

Demonstração Suponha por absurdo que existam inteiros positivos x', y' e z' tais que $(x')^4 + (y')^4 = (z')^4$. Sendo assim $(x')^4 + (y')^4 = ((z')^2)^2$. Ou seja a equação $x^4 + y^4 = z^2$ possui solução no universo de inteiros positivos. Este fato vai de encontro com o teorema anterior. Contradição.

■

Vejamos agora alguns resultados que serão usados na demonstração do caso $n = 3$.

Lema 29.1: Lema de Thue
Sejam m um número natural maior que 1 que não seja um quadrado perfeito e $a \in \mathbb{Z}$ tais que $mdc(m,a) = 1$. Então existem inteiros não nulos x, y com $|x|,|y| < \sqrt{m}$ tais que $ax \equiv y \pmod m$.

Demosntração
Seja $q = \sqrt{m}$. Então $q^2 = m$, e por isso, $q^2 + 1 > m$, com $m > 1$. Considere como $ax - y$ em que x e y podem assumir os valores de $0, 1, 2, 3, ..., q$. O conjunto

A=$\{(x,y) \in \mathbb{Z}^2; 0 \leq x,y \leq q\}$ possui $(q+1)^2$ elementos. Como só existem m restos na divisão por m, pelo Princípio da Casa dos Pombos, temos que, módulo m, existirão dois números $ax_1 - y_1$ e $ax_2 - y_2$ congruentes. Disto temos que $a(x_1 - x_2) - (y_1 - y_2)$ é divisível por m.

Observe que:

$$0 \leq x_i, y_i \leq \sqrt{m} \text{ implica que } |x_1 - x_2|, |y_1 - y_2| \leq \sqrt{m}.$$

Se $x_1 - x_2 = 0$, temos $m \mid y_1 - y_2$ o que implica $y_1 = y_2$. Mas isso é um absurdo pois $(x_1, y_1) \neq (x_2, y_2)$. De forma análoga, se $y_1 - y_2 = 0$, teremos $m \mid x_1 - x_2$ o que implica $x_1 = x_2$, novamente um absurdo. Sendo assim tomamos $x = x_1 - x_2$ e $y = y_1 - y_2$

■

Exemplo 19: Sejam $d \in \{1, 2, 3\}$ e $p > 3$ um primo tal que $\left(\frac{-d}{p}\right) = 1$, então existem x , y inteiros tais que $p = y^2 + dx^2$

Demonstração Por hipótese, $(\frac{-d}{p}) = 1$. Logo a congruência $x^2 \equiv -d \pmod{p}$ tem solução. Existe $a \in \mathbb{Z}$ tal que $a^2 \equiv -d \pmod{p}$. Note que $mdc(a, p) = 1$. De acordo com o Lema de Thue, existem inteiros x e y, com $0 \leq |x|, |y| \leq \sqrt{p}$, tais que

$$(ax + y)(ax - y) \equiv 0 \pmod{p}, \text{, isto é, } a^2x^2 - y^2 \equiv 0 \equiv -a^2d - y^2 \pmod{p}$$

Visto que $a^2d + y \equiv 0 \pmod{p}$, $p \mid a^2d + y$. À luz de $0 \leq |x|, |y| < \sqrt{p}$, segue que $0 < y^2 + dx^2 < (d + 1)p$ e, portanto, $y^2 + dx^2 = kp$ para algum $k \in \{1, 2, ..., d\}$.

Se $k = d$, temos $y^2 + dx^2 = dp$. Deste modo, $y^2 = d(p - x^2)$ e consequentemente $d \mid y^2$. Recorde-se que $d \in \{1, 2, 3\}$. Deste modo, segue que $d \mid y$. Por $d \mid y$, sabemos que existe $l \in \mathbb{Z}$ tal que $y = dl$. Desta feita, $d^2l^2 + dx^2 = dp$. Ao dividir os dois membros por d temos $dl^2 + x^2 = p$. A seguir, analisaremos os casos $d = 1$, $d = 2$ e $d = 3$.

Se $d = 1$, a igualdade pode ser escrita como $l^2 + x^2 = p$.

Se $d = 2$, tendo em mente que $y^2 + dx^2 = kp$ para algum $k \in \{1,2\}$, podemos ter: $y^2 + 2x^2 = p$ ou $y^2 + 2x^2 = 2p$. Neste último caso, $k = d = 2$. Ao substituir d por 2 em $dl^2 + x^2 = p$, concluímos que $2l^2 + x^2 = p$.

Se $d = 3$, três situações podem ocorrer com $y^2 + dx^2 = kp$, são elas: $y^2 + 3x^2 = p$, $y^2 + 3x^2 = 2p$, $y^2 + 3x^2 = 3p$. No caso em que $y^2 + 3x^2 = 2p$, não é difícil constatar que x e y tem a mesma paridade. Se x e y são ambos pares, $4 \mid y^2 + 3x^2$. Consequentemente $4 \mid 2p$, o que é um absurdo, pois p é um primo ímpar. Se x e y são ambos ímpares, existem k_1 e k_2 inteiros tais que $x = 2k_1 + 1$ e $y = 2k_2 + 1$. Assim $y^2 = 4k_2^2 + 4k_2^2 + 1$ e $x^2 = 4k_1^2 + 4k_1 + 1$. Independente, se k_1 e k_2 é par ou ímpar teremos $x^2 \equiv y^2 \equiv 1 \pmod{8}$. Logo, módulo 8, a igualdade $y^2 + 3x^2 = 2p$ se reduziria a $y^2 + 3x^2 \equiv 1 + 3 \cdot 1 \equiv 2p \pmod{8}$. Ou seja, $8 \mid 2p - 4$ com p primo ímpar. Isto é um absurdo, pois $8 \mid 2p - 4$ implica $4 \mid p - 2$. Concluímos assim que o caso. Concluímos assim que o caso $y^2 + 3x^2 = 2p$ não pode acontecer.

Por fim, temos o caso $y^2 + 3x^2 = 3p$. Nesta situação, $k = d = 3$. Portanto, ao substituir d por 3, em $dl^2 + x^2 = p$, obtemos $3l^2 + x^2 = p$.

Lema 29.2: Todas as soluções de $z^3 = y^2 + 3x^2$ em inteiros positivos tais que o $mdc(x,y) = 1$ e z ímpar são dadas por

$$z = m^2 + 3n^2, \quad y = m^3 - 9mn^2, \quad x = 3m^2n - 3n^3$$

com $m + n$ ímpar e $mdc(m,3n) = 1$.

Demonstração : Verificaremos inicialmente que esses valores satisfazem a equação. Temos que:

$$(m^2 + 3n^2)^3 = m^6 + 9m^4n^2 + 27m^2n^4 + 27n^6 =$$

$$(m^6 - 18m^4n^2 + 81m^2n^4) + (27m^4n^2 - 54m^2n^4 + 27n^6) = (m^3 - 9mn^2)^2 + 3(3m^2n - 3n^3)^2.$$

Ou seja, estes números satisfazem a equação.

Como $m + n$ é ímpar, ambos possuem paridades distintas e disto temos que $z = m^2 + 3n^2$ também é ímpar.

Outro fato é que $mdc(m^3 - 9mn^2, 3m^2n - 3n^3) = mdc(m(m^2 - 9n^2), 3n(m^2 - n^2))$. Pelo Teorema 4 e pelo fato de que $mdc(m, 3n) = 1$, segue que,

$$\begin{aligned} mdc(m(m^2 - 9n^2), 3n) &= mdc(m^2 - 9n^2, 3n) \\ &= mdc(m^2 - 9n^2 + 3n \cdot 3n, 3n) \\ &= mdc(m^2, 3n) = mdc(m \cdot m, 3n) \\ &= mdc(m, 3n) = 1. \end{aligned}$$

De modo análogo, usando o fato de que $mdc(m(m^2 - 9n^2), 3n) = 1$, $mdc(m(m^2 - 9n^2), 3n(m^2 - n^2)) = mdc(m(m^2 - 9n^2), m^2 - n^2)$. Calcularemos $mdc(m(m^2 - 9n^2), m^2 - n^2)$. Primeiro observe que

$$\begin{aligned} mdc(m, m^2 - n^2) &= mdc(m, m^2 - n^2 - m \cdot m) \\ &= mdc(m, -n^2) \\ &= mdc(m, n^2) = 1, \end{aligned}$$

pois o $mdc(m,3n) = 1$. De fato, como m e $3n$ não possuem fatores comuns, m e n também não possuem, e por decorrência disto m e n^2 são relativamente primos. Daí, como $mdc(m, m^2 - n^2) = 1$, temos $mdc(m(m^2 - 9n^2),(m^2 - n^2)) = mdc(m^2 -$

$9n^2, m^2 - n^2$). Vejamos então o $mdc(m^2 - 9n^2, m^2 - n^2)$:

$$\begin{aligned} mdc(m^2 - 9n^2, m^2 - n^2) &= (m^2 - 9n^2 - m^2 + n^2, m^2 - n^2) \\ &= mdc(-8n^2, m^2 - n^2) = mdc(8n^2, m^2 - n^2) \\ &= mdc(8n^2 + 8m^2 - 8n^2, m^2 - n^2) \\ &= mdc(8m^2, m^2 - n^2) = 1. \end{aligned}$$

De fato $mdc(8m^2, m^2 - n^2) = 1$, pois o m e $m^2 - n^2$ são relativamente primos e, consequentemente, m^2 e $m^2 - n^2$ também serão, assim como $8m^2$ e $m^2 - n^2$. Note que $m^2 - n^2$ é ímpar.

Provamos assim que $mdc(x,y) = 1$, em que $x = 3m^2n - 3n^2$ e $y = m^3 - 9mn^2$.

Provaremos agora a recíproca. Suponha que a equação possua uma solução (x, y, z) . Seja p um primo tal que $p \mid z$. Como z é ímpar, temos $p \geq 3$. Observe que se $p \mid x$, como $p \mid z$, então $p \mid y$; absurdo pois $mdc(x, y) = 1$. De modo análogo, verificamos que $p \nmid y$. Logo p não divide nem x e nem y e é maior que 3.

Como $p \mid z$, $p \mid z^3$ e, por consequência, $p \mid y^2 + 3x^2$ se, e só se, $y^2 \equiv -3x^2 \pmod{p}$. Como já vimos $p \nmid x$, e $mdc(x,p) = 1$, daí temos que x é invertível módulo p. E por este fato temos que $(\frac{-3}{p}) = 1$ e pelo Teorema da Reciprocidade Quadrática e pelo Corolário 19.1, vistos no capítulo 3,$(\frac{p}{3}) = 1$. Usando o exemplo 17, sabemos que existem inteiros m_1 e n_1 tais que $p = m_1^2 + 3n_1^2$. Com as ideias da primeira parte da prova, $p^3 = d^2 + 3c^2$, em que $d = m_1^3 - 9m_1n_1^2$ e $c = 3m_1^2n_1 - 3n_1^3$ em que o $mdc(p, d) = mdc(p,c) = 1$, assim como $mdc(p,m_1) = mdc(p,n_1) = 1$.

Por indução matemática em z, se $z = 1$, então a única resolução é $x = 0$, $y = 1$. Dito isto, suponhamos que valha para todo z com k fatores primos não necessariamente distintos. Então se z tem $(k + 1)$ fatores, ou seja, $z = p \cdot q$ com p primo ($p \geq 3$) e q é um produto de k fatores primos não necessariamente distintos.

Agora observe que:

$$q^3p^6 = q^3p^3p^3 = z^3p^3 = (y^2 + 3x^2)(d^2 + 3c^2) = (yd \pm 3xc)^2 + 3(yc \mp xd)^2.$$

Outro fato a se atentar é:

$$(yx + xd)(yc - xd) = (yc)^2 - (xd)^2 = c^2(y^2 + 3x^2) - x^2(d^2 + 3c^2) = p^3(c^2q^3 - x^2).$$

Ou seja, $p^3 \mid (yx + xd)(yc - xd)$. Suponha que $p^3 \mid yc + xd$ e $p^3 \mid yc - xd$.

Na suposição que $p \mid yc + xd$ e $p \mid yc - xd$, concluímos que $p \mid 2yc$. Visto que p é um primo ímpar, $p \mid yc$. Portanto do fato que $p \mid yc$ e $p \mid yc - xd$, segue que $p \mid xd$. Haja vista que $mdc(p,c) = mdc(p,d) = 1$, teríamos $p \mid x$ e $p \mid y$. Ora, isso é um absurdo, pois $mdc(x,y) = 1$. Desta maneira, uma, e apenas uma, das divisibilidades ocorre: $p^3 \mid yc + xd$ ou $p^3 \mid yc - xd$. Análogo para $(yd + 3xx)(yd - 3xc)$.

Fazendo a escolha dos sinais, existem u e $v \in \mathbb{Z}$ de modo que:

$$p^3u = yd \pm 3xc \text{ o que implica } u = \frac{yd \pm 3xc}{p^3}, p^3v = yc \mp xd \text{ logo } v = \frac{yc \mp xd}{p^3}$$

sendo que $q^3 = u^2 + 3v^2$, pois:

$$\frac{(yd \pm 3xc)^2}{p^6} + 3 \cdot \frac{(yc \mp xd)^2}{p^6} = \frac{(yd \pm 3xc)^2 + 3(yc \mp xd)^2}{p^6} = \frac{q^3p^6}{p^6} = q^3$$

E por q ter k fatores primos, segue da hipótese de indução que existem m_2 e $n_2 \in \mathbb{Z}$ de modo que, $q = m_2^2 + 3n_2^2, u = m_2^3 - 9m_2n_2^2$ e $v = 3m_2^2n_2 - 3n_2^3$.

Observe que $ud + 3vc = \frac{y^2 \pm 3xcd}{p^3} + \frac{3yc^2 \mp 3xcd}{p^3} = \frac{y(3c+d^2)}{p^3} = y$ e $-(uc - vd) = -(\frac{ycd \pm 3xc^2}{p^3} - \frac{ycx \pm xd^2}{p^3}) = -(\frac{\pm x(3c^2+d)}{p^3}) = \pm x$, substituindo u, v, d e c em termos de m_i e $n_i (i = 1,2)$ em z, y e x e fazendo $m = m_1m_2 + 3n_1n_2$ e $n = m_1n_2 - m_2n_1$, obtemos:

$$\begin{aligned} y = ud + 3vc &= \left(m_2^3 - 9m_2n_2^2\right)\left(m_1^3 - 9m_1n_1^2\right) + 3\left(3m_2^2n_2 - 3n_2^3\right)\left(3m_1^2n_1 - 3n_1^3\right) \\ &= m_1^3m_2^3 - 9m_1n_1^2m_2^3 - 9m_1^3m_2n_2^2 + 81m_1n_1^2m_2n_2^2 \\ &+ 27m_1^2n_1m_2^2n_2 - 27n_1^3m_2^2n_2 - 27m_1^2n_1n_2^3 + 27n_1^3n_2^3 \\ &= (m_1m_2 + 3n_1n_2)^3 - 9(m_1m_2 + 3n_1n_2)(m_1^2n_2^2 - 2m_1n_1m_2n_2 + n_1^2m_2^2) \\ &= m^3 - 9mn^2. \end{aligned}$$

$$\begin{aligned} \pm x = -(uc - vd) &= -\left(m_2^3 - 9m_2n_2^2\right)\left(3m_1^2n_1 - 3n_1^3\right) + \left(3m_2^2n_2 - 3n_2^3\right)\left(m_1^3 - 9m_1n_1^2\right) \\ &= -3m_1^2n_1m_2^3 + 3n_1^3m_2^3 + 27m_1^2n_1m_2n_2^2 \\ &- 27m_2n_2^2n_1^3 + 3m_1^3m_2^3n_2 - 27m_1n_1^2m_2^2n_2 - 3m_1^3n_2^3 + 27m_1n_1^2n_2^3 \\ &= 3(m_1m_2 + 3n_1n_2)^2(m_1n_2 - n_1m_2) - 3(m_1n_2 - n_1m_2)^3 \\ &= 3m^2n - 3n^3. \end{aligned}$$

E:

$$y^2 + 3x^2 = \left(m^3 - 9mn^2\right)^2 + 3\left(3m^2n - 3n^3\right)^2 = \left(m^2 + 3n^2\right)^3 = z^3$$

Isto mostra que a única solução de $z^3 = y^2 + 3x^2$ é $x = m^2n - 3n^3$, $y = m^3 - 9mn^2$ e $z = (m^2 + 3n^2)^3$

■

Teorema 30: A equação diofantina $x^3 + y^3 = z^3$ não possui soluções inteiras com x,$y, z > 0$.

Demonstração: Suponhamos que exista uma solução (x, y, z) com $x, y, z > 0$. Tomemos a solução que xyz seja o menor numero possível. Observe que se existir um

fator em comum com dois elementos, ele será comum com o terceiro, daí podemos supor que sejam primos relativos dois a dois, caso contrário teríamos $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d})$ menor que (x, y, z). Observe que pelo menos um será par.

Vejamos se $x = y$, temos $2x^3 = z^3$, o que é impossível, pois, o expoente de 2 em $2x^3$ é da forma $3k+1$; já o expoente 2 em z^3 é da forma $3l$. Assim podemos considerar, sem perda de generalidade $x > y$, o caso em que $y > x$ é análogo. Suponha que x e y sejam ímpares, dessa forma z é par e podemos escrever $x = p + q$ e $y = p - q$ com $p, q > 0$ e $mdc(p,q) = 1$ já que x, y tem paridades iguais e são primos relativos.

De fato note que $p = \frac{x+y}{2}$ e $q = \frac{x-y}{2}$. Visto que $mdc(x,y) = 1$, podemos constatar por argumento de rotina que $mdc(x + y, x - y) = 2$. Logo $mdc(\dfrac{x+y}{2}, \dfrac{x-y}{2}) = 1$

Assim:

$$\begin{aligned} z^3 = x^3 + y^3 &= (x+y)(x^2 - xy + y^2), \\ &= [(p+q) + (p-q)] \cdot [(p+q)^2 - (p+q)(p-q) + (p-q)^2], \\ &= 2p[(p^2 + 2pq + q^2) - (p^2 - q^2) + (p^2 - 2pq + q^2)], \\ &= 2p(p^2 + 2pq + q^2 - p^2 + q^2 + p^2 - 2pq + q^2), \\ &= 2p(p^2 + 3q^2). \end{aligned}$$

Ou seja, $2p(p^2 + 3q^2)$ é um cubo perfeito.

De forma igual, no caso em que z é ímpar e x ou y também é, teremos algo parecido. Supondo que y também é ímpar, podemos escrever $z = q + p$ e $y = q - p$, e assim temos:

$$\begin{aligned} x^3 = z^3 - y^3 &= (q+p)^3 - (q-p)^3, \\ &= [q^3 + 3q^2p + 3qp^2 + p^3] - [q^3 - 3q^2p + 3qp^2 - p^3], \\ &= q^3 + 3q^2p + 3qp^2 + p^3 - q^3 + 3q^2p - 3qp^2 + p^3, \\ &= 6q^2p + 2p^3, \\ &= 2p(p^2 + 3q^2). \end{aligned}$$

Se $z = q + p$ é ímpar, então $p^2 + 3q^2$ também é, pois p e q tem paridades distintas. Provaremos agora que $mdc(p, p^2 + 3q^2) = mdc(p, 3)$. Partindo do fato que $mdc(p,q) = 1$, segue que:

$$\begin{aligned} mdc(p, p^2 + 3q^2) &= mdc(p, p^2 + 3q^2 - p \cdot p) \\ &= mdc(p, p^2 + 3q^2 - p^2) \\ &= mdc(p, 3q^2) \\ &= mdc(p, 3q \cdot q) \\ &= mdc(p, 3q) = mdc(p, 3). \end{aligned}$$

Logo, existem dois casos, $mdc(p,3) = 1$ ou $mdc(p,3) = 3$.

Vejamos se $mdc(p,3) = 1$, então pelo Teorema Fundamental da Aritmética,

existem a e b naturais tais que $a^3 = 2p$ e $b^3 = p^2 + 3q^2$, lembre-se que $2p(p^2 + 3q^2)$ é um cubo perfeito. Pelo Lema 29.2 existem m e n com paridades distintas e relativamente primos tais que $b = m^2 + 3n^2$, $p = m^3 - 9mn^2$ e $q = 3m^2n - 3n$. Portanto, $a^3 = 2p = 2(m^3 - 9mn^2) = 2m(m^2 - 9n^2) = 2m(m+3n)(m-3n)$. Observe que $mdc(2m, m + 3n) = mdc(2m,m - 3n) = mdc(m + 3n,m - 3n) = d$. Então existem e, f e g tais que $\frac{2m}{d} = e^3$, $\frac{m+3n}{d} = f^3$ e $\frac{m-3n}{d} = g^3$. Observe que $f^3 + g^3 = e^3$. Como

$$efg < e^3f^3g^3 = \frac{a^3}{d^3} = \frac{2p}{d^3} \leq x + y < xy < xyz,$$

temos assim, uma solução menor que a mínima, o que contradiz com a escolha de x,y,z.

Vejamos agora o caso em que $mdc(p,3) = 3$. Temos que $3|p$, ou seja, existe $r \in \mathbb{Z}$ tal que $p = 3r$ com $mdc(p,r) = 1$. Deste modo temos :

$$z^3 = 2p(p^2+3q^2) = 2(3r)((3r)^2+3q^2) = 6r(9r^2+3q^2) = 6r(3)(3r^2+q^2) = 18r(3r^2+q^2).$$

Lembre-se que $mdc(p, p^2+3q^2) = mdc(p, 3) = 3$. Assim, temos $mdc(18r,3r^2+q^2) = 1$. Daí, existem i, j inteiros tais que $18r = i^3$ e $3r^2 + q^2 = j^3$. E, novamente, existem u,v inteiros relativamente primos tais que $j = u^2+3v^2, q = u^3-9uv^2$ e $r = 3u^2v-3v^3$. Assim temos

$$i^3 = 18r = 18(3u^2v - 3v^3) = 18(3v)(u^2 - v^2) = 27(2v)(u + v)(u - v).$$

De forma igual, temos $mdc(2v, v + u) = mdc(2v, v - u) = mdc(u + v, v - u) = d$. E então existem inteiros l, k e o tais que $\frac{2v}{d} = k^3$, $\frac{u+v}{d} = l^3$ e $\frac{u-v}{d} = o^3$. Como já vimos, segue que $k^3 = l^3 + o^3$. Ou seja, (l, o, k) também é solução, menor que (x,y,z), o que contradiz a minimalidade suposta da solução.

Logo não existem $x, y, z \in \mathbb{N}^*$ tais que $x^3 + y^3 = z^3$.

■

Corolário 30.1: Último Teorema de Fermat para $n = 3$.

Não existem inteiros positivos x,y,z tais que $x^3 + y^3 = z^3$.

Demonstração: Suponha por absurdo que existam $x', y', z' > 0$ tais que $x'^3 + y'^3 = z'^3$. Ora $x'y'z' \neq 0$. Isto vai de encontro com o Teorema 30. Contradição.

7

Considerações Finais

No capítulo 1, apresentamos uma introdução à aritmética, com alguns conceitos iniciais, tais como, divisibilidade dos inteiros, mdc, mmc e as congruências lineares. No fim desta parte, começamos os nossos estudos sobre as equações diofantinas com as equações diofantinas lineares.

No próximo capítulo estudamos as congruências de grau 2, provamos que existem $\frac{p-1}{2}$ resíduos quadráticos, introduzimos a definição do símbolo de Legendre, e demonstramos o Teorema da Reciprocidade Quadrática de Gauss.

Depois vimos as ternas pitagóricas, que são ternas que satisfazem o famoso Teorema de Pitágoras para triângulos retângulos, investigamos métodos alternativos que podem ser utilizados para resolução alguns problemas, como o método geométrico, o método aritmético modular e o método de fatoração.

Expusemos também o Problema de Waring e um de suas soluções parciais, que leva o nome de Teorema de Lagrange. O Teorema de Lagrange diz, se n é um número natural, então existem a, b, c, d inteiros tais que $n = a^2 + b^2 + c^2 + d^2$.

Por fim, exibimos uma prova dos casos $n = 3$ e $n = 4$ do famoso Teorema de Fermat (não existem inteiros positivos x, y, z tais que $x^n + y^n = z^n$ com $n \geq 3$).

No espírito deste trabalho de conclusão de curso, sugerimos alguns tópicos que seriam uma continuação deste trabalho. O primeiro seria na linha do Problema de Waring e consistiria em provar que todo inteiro maior ou igual a zero pode ser escrito como a soma de nove cubos de inteiros não negativos.

O segundo tem a ver com o Último Teorema de Fermat e consiste em apresentar uma prova para o caso $n = 5$, uma referência para estudo pode ser [6].

Bibliografia

[1] Castro, I. S. "O Último Teorema de Fermat nos Ensinos Fundamental e Médio". *Universidade Federal de Viçosa - Florestal* (2019).

[2] Eves, H. *Introdução à Historia da Matemática.* Editora da Unicamp, 2011.

[3] Hefez, A. *Aritmética.* Coleção Profmat, 2016.

[4] Martinez, F. E. B. et al. *Teoria dos Números: Passeio de primos e outros números familiares pelo mundo inteiro.* IMPA, 2015.

[5] Milies, C. P. e Coelho, S. P. *Números : Uma Introdução à Matemática.* Edusp, 2001.

[6] Oliveira Cardoso, S. de. "O Último Teorema de Fermat para n = 5". *UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO* (2020).

[7] Oliveira Santos, J. P. de. *Introdução à Teoria dos Números.* Coleção Matemática Universitária, 2009.

[8] Silva, O. N. da e Câmara, M. A. da. "O Problema de Waring e o Teorema de Lagrange". *FAMAT em revista* 11 (2008).

[9] Silva Neto, A. da. "Convite às equações diofantinas: uma abordagem para a educação básica". *Universidade Federal de Roraima* (2016).