UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL DE MATEMÁTICA EM REDE NACIONAL

LEANDRO FARIAS MAIA

EQUAÇÕES DIOFANTINAS

Belém-PA
2018

UNIVERSIDADE FEDERAL DO PARÁ
INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
MESTRADO PROFISSIONAL DE MATEMÁTICA EM REDE NACIONAL

LEANDRO FARIAS MAIA

EQUAÇÕES DIOFANTINAS

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Pará, como requisito parcial para o Título de Mestre em Matemática.

Belém - Pará
2018

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

F224e Farias Maia, Leandro
Equações Diofantinas / Leandro Farias Maia. — 2018
110 f. : il. color

Dissertação (Mestrado) - Programa de Pós-graduação em Matemática em Rede Nacional (PROFMAT) , Instituto de Ciências Exatas e Naturais, Universidade Federal do Pará, Belém, 2018.
Orientação: Prof. Dr. Mauro de Lima Santos

1. Equação Diofantina. 2. Teoria dos Números. 3. Algoritmo de Euclides. 4. Olimpíada de Matemática. 5. Congruências. I. Santos, Mauro de Lima, *orient.* II. Título

---

CDD 512.7

LEANDRO FARIAS MAIA

EQUAÇÕES DIOFANTINAS

Esta Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional, da Universidade Federal do Pará, como requisito parcial para o Título de Mestre em Matemática, foi julgada e aprovada pela seguinte banca examinadora:

Prof. Dr. Mauro de Lima Santos - PROFMAT/UFPA

Prof. Dr. Anderson David de Souza Campelo - PROFMAT/UFPA

Prof. Dr. João Furtado de Souza - FACULDADE DE FÍSICA/ICEN/UFPA

APROVADA EM: 26/04/2018

Não se pode ensinar nada a um homem,
apenas a ajudá-lo a encontrar as respostas dentro de si mesmo.
Galileu Galilei

AGRADECIMENTOS

Primeiramente, agradeço à Deus por ter me dado saúde física e mental para continuar nesse tão renomado mestrado em matemática, onde tive a oportunidade de conhecer alunos e professores brilhantes.

Agradeço aos meus pais, por me mostrarem que só se alcança os objetivos com trabalho árduo e foco, porém nunca deixando de lado a humildade.

Agradeço aos meus irmãos, Mestre Luís Farias e Doutor José Valmir F Maia Junior, por serem pessoas inspiradoras para mim, além de me ajudarem a tomar inúmeras decisões na vida.

Agradeço a minha esposa, Thais Lima Farias, por sempre me apoiar nos momentos mais difíceis e por me aconselhar nas horas em que sempre precisei.

Agradeço ao grande amigo e Professor Márcio Pinheiro que com a sua sensibilidade de ser humano incrível que és, conseguiu enxergar a minha grande paixão pela matemática e me mostrou o caminho para o PROFMAT.

Agradeço aos grandes amigos de turma do PROFMAT, Emerson Veiga e Haroldo Aires, que puderam sempre disponibilizar conteúdos acadêmicos para um melhor apronfundamento em matemática.

Agradeço a todos os meu amigos de turma do PROFMAT, por me apresentarem as dificuldades da matemática em sala de aula e por contribuir para a minha busca pelo conhecimento.

Agradeço ao Prof. Dr. Rogelio Daniel Benavides Guzman e a Profª Drª. Tânia Madeleine Begazo Valdivia, que buscaram sempre a excelência em sala, em listas e em provas, através de exercícios desafiadores e conteúdos

relevantes para o mundo acadêmico.

Agradeço ao meu orientador, Professor Dr. Mauro de Lima Santos, que sugeriu esse tema tão relevante e deixou que eu trabalhasse em cima de resultados mais desafiadores, além de me proporcinar o tempo ideal para a conclusão desse trabalho.

E por fim agradeço a coordenadora Carmen Almeida, juntamente com sua equipe, e ao Prof. Dr. Valcir João da Cunha Farias, pela excelente dinâmica adotada no PROFMAT da UFPA.

Resumo

As equações diofantinas representam um importante papel na matemática, uma vez que estão inseridas no universo de vários níveis acadêmicos, além de se sobresair em diversos problemas do cotidiano. Esse trabalho foi realizado para apresentar aos alunos de olimpíada de matemática o que é uma equação diofantina, linear e não linear, e suas diversas formas de resolução, além de abordar contextos históricos e demonstrações para auxiliar os docentes no processo do aprendizado. Para introduzir conceitos relevantes de teoria dos números, é realizado uma introdução teórica dos tópicos requeridos ao longo desse trabalho. Em seguida, são apresentadas, em uma primeira parte, as equações diofantinas lineares para, logo em seguida, mostrar um universo de equações diofantinas não linerares acompanhadas de técnicas de resolução de problemas. Para aprofundar os estudos, há diversos problemas de outros países e de competições internacionais de matemática.

Palavras-chave: Equação Diofantina, Equação Diofantina Linear, Equação Diofantina Não Linear, Olimpíadas de Matemática, Teoria dos Números, Algoritmo de Euclides, Congruências.

Abstract

Diophantine equations play an important role in mathematics, since it is inserted in the universe of several academic levels, besides surpassing in several daily problems. This work was carried out to present to the students of Mathematics Olympiad what is a linear and nonlinear Diophantine equation, and its different forms of resolution, besides addressing historical contexts and demonstrations to assist teachers in the learning process. Firstly, to introduce relevant concepts of number theory, a theoretical introduction of the topics required throughout this work is carried out. Second, the linear diophantine equations are presented, and then an universe of nonlinear diophantine equations followed by resolution techniques. As a way to deepen the studies, there are several problems from other countries and from international competitions of mathematics.

Keywords: Diophantine Equation, Linear Diophantine Equation, Nonlinear Diophantine Equation, Mathematical Olympiads, Number Theory, Euclidean Algorithm, Congruences.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

Símbolos	**Significado**
$\mathbb{N}$	Conjunto dos números naturais: $\{0, 1, 2, 3, \ldots\}$
$\mathbb{Z}$	Conjunto dos números inteiros: $\{\ldots, -2, -1, 0, 1, 2, \ldots\}$
$\mathbb{Q}$	Conjunto dos números racionais.
$\mathbb{I}$	Conjunto dos números irracionais.
$\mathbb{R}$	Conjunto dos números reais.
$\mid$	Representa o sinal da divisibilidade.
$\equiv$	Representa o sinal da congruência linear.

LISTA DE ABREVIATURAS

Abreviatura	**Significado**
CIIM	Competencia Iberoamericana Universitária de Matemáticas
Cone Sul	Olimpíada disputada pelos países da América do Sul
OBM	Olimpíada Brasileira de Matemática
OCM	Olimpíada Cearense de Matemática
IMC	International Mathematical Comptetion for University Students
IMO	International Mathematical Olympiad
USAMO	United States of America Mathematical Olympiad

INTRODUÇÃO

Dentre as diversas atribuições do professor de matemática, destaca-se aquela de dá sentido ao algebrismo, ou seja, de buscar aplicações práticas dos cálculos realizados em sala. O professor é o principal elo de comunicação entre o conteúdo ensinado em sala e o aprendizado do aluno. Dessa forma, tentar buscar a motivação desses estudantes é um recorrente trabalho dos docentes que buscam através de aplicações cotidianas o interesse dos discentes.

Nesse trabalho, será realizado um criterioso percurso pelo mundo das Equações Diofantinas, de forma a buscar o foco em aplicações cotidianas, para despertar uma maior motivação pela matemática dentre os alunos de Olimpíada, além de realizar uma exploração da beleza da Teoria dos Números, nessa tão significante equação para o mundo acadêmico.

As Equações Dioafantinas estão intimamente relacionadas ao matemático Diophantus, que é conhecido como o pai da álgebra devido seu livro *Arithmetica*, contendo soluções de equações algébricas e teoria dos números. Entretanto, não se sabe muito a respeito de sua vida. Apenas anos depois tem-se discutido sobre sua existência.

Diophantus fez seus trabalhos na cidade de Alexandria, na idade da prata. A referência idade da prata segue-se logo depois da idade do Ouro, época de Euclid, um matemático inspirador até os dias atuais. Apesar de se saber o período em que Diophantus viveu, não se sabe exatamente os anos. O que torna mais difícil o processo de determinar esse período é o fato dele citar poucas referências em seus trabalhos.

Figura 1: Escultura de Diophantus

Os grandes historiadores acreditam que ele realizou seus trabalhos por volta de 250 CE. Uma informação valiosa é obtida da coleção de ficção escrita por Metrodorus, por volta de 500 CE. Segue-se

> Sua infância durou 1/6 de sua vida; ele se casou depois de 1/7 anos a mais; sua barba cresceu depois de 1/12 a mais, e seu filho nasceu cinco anos depois; o filho viveu até a metade da idade do seu pai, e o pai morreu quatro anos após o filho.[1]

Sendo assim, poderíamos determinar a idade de Diophantus através das equações

$$\frac{D}{6} + \frac{D}{12} + \frac{D}{7} + F + 4 = D \tag{1}$$

sendo D a idade dele e F a idade de seu filho. Também temos a equação

$$F = \frac{D}{2} \tag{2}$$

assim, substituindo (.2) em (.1), obtemos $D = 84$ anos.

Um resultado de grande valia contido em *Arithmetica* é o fato de que os número da forma $8n + 7$, sendo n um número natural, não podem ser quadrados perfeitos.

De modo geral, definimos uma *Equação Diofantina* toda equação da forma

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{3}$$

sendo f uma função de n variáveis. Dizemos que a n-upla $(x_0^0, x_1^0, , \ldots, x_n^0) \in \mathbb{Z}_n$ é solução dessa equação quando satisfaz (.3).

Deve-se levantar os seguintes questionamentos a respeito das equações diofantinas

1. A equação tem solução?

2. Caso tenho solução, esse universo de soluções é um conjunto finito ou infinito ?

3. Caso tenho solução, determinar todas as soluções.

O trabalho de Diphantus foi continuado por matemáticos Chineses, Árabes e apronfudado por Fermat, Euler e Gauss. Este tópico permanece com grande importância nos dias atuais.

A análise desse trabalho foi baseada em duas grandes frentes: Equações Diofantinas Lineares e Equações Diofantinas Não Lineares. Alguns problemas cotidianos são explorados de sites de olimpíadas de matemática [], dos livros [], além de diversos serem de minha própria criação. Para as Equações Diofantinas Não Lineares, são elencadas equações conhecidas que fizeram história na matemática e apresentadas algumas técnicas de resolução.

Ao longo do trabalho é apresentado um método que deve ser seguido, de forma a facilitar a resolução de um Equação Diofantina.

1. Identificar os tipos de Equações Diofantinas.

2. Aplicar as técnicas para resolução de Equações Diofantinas Linerares e Não Lineares.

3. Decidir se há ou não solução.

4. Exibir, se for o caso, as soluções.

Para cumprir o objetivo, esse trabalho é divido da seguinte forma:

a) No primeiro Capítulo, é relembrado alguns tópicos relevantes na Teoria dos Números e que serão de grande importância para aplicações em posteriores Proposições, Lemas e Teoremas.

b) No Segundo Capítulo, é mostrado o método de solução da equação diofantina linear, bem como serão apresentados problemas históricos.

c) No Terceiro Capítulo, são apresentados equações diofantinas não linerares seculares e algumas são resolvidas, bem como são apresentadas técnicas de resolução para essas equações.

d) E, por fim, é proposta uma lista de exercícios desafiadores.

CAPÍTULO 1

ALGUNS CONCEITOS DA TEORIA DOS NÚMEROS

Antes de iniciar nossos estudos sobre as Equações Diofantinas, é preciso destacar algumas definições, proposições e teoremas, presentes na Teoria dos Números, que serão de grande valia e de suma importância para o perfeito entendimento das demonstrações que serão enumeradas no Capítulo 2 e Capítulo 3.

1.1 Números Naturais e Números Inteiros

Definição 1.1.1. (Números Naturais). *Representaremos por* $\mathbb{N}$ *o conjunto do números naturais, formado pelos seguintes elementos*

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\} \tag{1.1}$$

Definição 1.1.2. (Números Inteiros). *Representaremos por* $\mathbb{Z}$ *o conjunto do números inteiros, formado pelos seguintes elementos*

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \tag{1.2}$$

O conjunto dos inteiros positivos pode ser representado tanto por $\mathbb{N}^*$ como por $\mathbb{Z}_+$. Da mesma forma que os inteiros negativos podem ser representados po $\mathbb{Z}_-^*$.

1.2 Divisibilidade

Definição 1.2.1. (Divisibilidade) *Sejam os inteiros a e b, com $a \neq 0$. Dizemos que a divide b, quando existe um inteiro x tal que*

$$b = a \cdot x \tag{1.3}$$

representamos essa divisibilidade por $a \mid b$.

De posse do conceito de divisibilidade, vamos demonstrar uma importante propriedade envolvendo divisibilidade e que é bastante utilizada no mundo das **Equações Diofantinas**.

Proposição 1.2.2. *Sejam a, b, c inteiros. Suponha que $a \mid b$ e $a \mid c$ então a divide qualquer combinação linear entre b e c.*

Demonstração Pela definição, sabemos que existem inteiros x e y tais que

$$b = a \cdot x \quad e \quad c = a \cdot y \tag{1.4}$$

dessa forma sendo r e s inteiros quaisquer, podemos representar uma combinação linear de b e c por $b \cdot r + c \cdot s$, ou seja,

$$b \cdot r + c \cdot s = a \cdot xr + a \cdot ys = a \cdot (xr + ys) \tag{1.5}$$

que é divisível por a, isto é, $a \mid b \cdot r + c \cdot s$. ■

Vejamos alguns exemplos clássicos de aplicação de Divisibilidade.

Exemplo *(Critério de Divisibilidade por 3)* Escrevendo n na forma decimal, mostre que

$$n = \overline{a_1 a_2 \ldots a_k} \tag{1.6}$$

é divisível por 3 se, e somente se, $a_1 + a_2 + \ldots + a_k$ for divisível por 3.

<u>*Solução:*</u> Ora, sabemos que n pode ser escrito como

$$n = 10^{k-1}a_1 + 10^{k-2}a_2 + \ldots + a_k \tag{1.7}$$

Note que 10 deixa resto 1 por 3, da mesma forma que 10^r, para qualquer $r \in \mathbb{N}$, também deixa resto 1, veja

$$10^r = (9+1)^r = \sum_{i=1}^{r} 9^i \binom{r}{i} + 1 \tag{1.8}$$

Logo, o resto de n por 3 terá o mesmo resto que

$$10^{k-1}a_1 + 10^{k-2}a_2 + \ldots + a_k = 1 \cdot a_1 + 1 \cdot a_2 + \ldots + a_k \tag{1.9}$$

ou seja, n será divisível por 3 se, e somente se, essa última soma será divisível por 3.

Os critérios de divisibilidade por 2, 4, 5, 6, 8, 9 e 11 apresentam praticamente o mesmo raciocínio. Aconselho que o leitor demonstre. Todas essas demonstrações podem ser encontradas no livro do Edgar de Alencar Filho [3].

Exemplo Demonstre que $8 \mid n^2 - 1$, para qualquer inteiro n ímpar.

Solução: Esse exemplo é pra nos mostrar que o resto da divisão por 8 de qualquer quadrado de um número ímpar é sempre 1. Suponha que n seja ímpar da forma $2k+1$ então

$$n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \tag{1.10}$$

note agora que $k(k+1)$ é sempre par, pois é o produto de dois números consecutivos. Daí n^2 será da forma $8k' + 1$. Sempre!

Exemplo Suponha que $d > 0$ e x sejam inteiros e que

$$d \mid 4x + 3 \quad e \quad d \mid 3x + 2 \tag{1.11}$$

determine os possíveis valores para d.

Solução: Vamos aplicar a Proposição 1.2.2. Temos que

$$d \mid 3(4x+3) - 4(3x+2) \Rightarrow d \mid 1 \tag{1.12}$$

ou seja, como $d > 0$ então $d = 1$.

1.3 Boa Ordenação e Princípio da Indução

O que vamos abordar nessa seção trata-se de uma das mais importantes parte desse trabalho. O Princípio da Boa Ordenação tem aplicação em um vasto campo da matemática e o Princípio da Indução é amplamente utilizado para demonstrar propriedades e teoremas nos mais variados ramos acadêmicos.

Teorema 1.3.1. (Princípio da Boa Ordenação) *Todo subconjunto não vazio $A \subset \mathbb{N}$ contém um menor elemento.*

Demonstração Essa belíssima demonstração é encontrada em [9]. Defina

$$I_n = \{p \in \mathbb{N}, 1 \leq p \leq n\} \tag{1.13}$$

e consideremos o conjunto $X \subset \mathbb{N}$ formado pelos naturais n tais que $I_n \subset \mathbb{N} - A$. Dessa forma, se $n \in X$ então nem n pertence a A nem os números menores que n.

Perceba que caso $1 \in A$ não há nada o que fazer, uma vez que 1 é o menor elemento dos naturais. Caso contrário, então $1 \in X$. Dessa forma, sabemos que $X \neq \mathbb{N}$ pois $A \neq \emptyset$.

Para concluir, perceba que deve existir um $n \in X$ tal que $n + 1 \notin X$ pois, caso contrário, X seria o conjunto dos números naturais. Dessa forma, defina $a = n + 1$ e sabemos que $a \in A$ é o menor elemento de A, pois todos os elementos de 1 até n pertencetem a X (complementar de A). ■

Teorema 1.3.2. (Segundo Princípio da Indução) *Seja $X \subset \mathbb{N}$ um conjunto com a seguinte propriedade: se X contém todos os números naturais m tais que $m < n$, então $n \in X$. Com essas condições, $X = \mathbb{N}$.*

Demonstração Vamos utilizar o Teorema 1.3.1 para nos auxiliar na demonstração.

Defina $Y = \mathbb{N} - X$. Vamos mostrar que Y é o conjunto vazio. Por contradição, suponha que não seja, assim aplicando o Princípio da Boa Ordenação, Y admite um menor elemento y. Dessa forma, todo elemento menor que y deverá obrigatoriamente pertencer a X (X e Y são complementares e y é o menor elemento de Y). Mas aplicando a hipótese do problema em X,

teríamos que y pertenceria a X também, o que nos levaria a uma contradição.
■

Vamos apresentar alguns exemplos para facilitar o entendimento desse Princípio.

Exemplo *(Soma Telescópica)* Defina a função ϕ para cada $n \in \mathbb{N}$ da seguinte forma

$$\phi(0) = 0 \quad e \quad \phi(n+1) = \phi(n) + (n+1) \tag{1.14}$$

Solução: Vejamos alguns casos iniciais.

$$\phi(1) = 1 = \frac{1 \cdot 2}{2} \;\; ; \;\; \phi(2) = 3 = \frac{2 \cdot 3}{2} \;\; ; \;\; \phi(3) = 6 = \frac{3 \cdot 4}{2} \tag{1.15}$$

então nossa conjectura é que

$$\phi(n) = \frac{n \cdot (n+1)}{2} \tag{1.16}$$

para todo n. Utilizando o segundo princípio da indução, já vericamos os casos iniciais. Vamos supor que seja válido para n e tentar demonstrar que também é válido para $n+1$. Por hipótese,

$$\phi(n+1) = \phi(n) + (n+1) = \frac{n(n+1)}{2} + (n+1) = \frac{(n+1)(n+2)}{2} \tag{1.17}$$

ou seja, a conjectura também é válida pra $n+1$ e ,portanto, pelo Teorema 1.3.2 é válido para todo $n \in \mathbb{N}$

Exemplo Todo natural é o produto de um ímpar e uma potência de 2.

Solução: Utilizaremos novamente o Teorema 1.3.2 para resolver. Assim, faremos o passo a passo:

(a) Casos iniciais: para

- $n = 1$ então $n = 2^0 \times 1$.
- $n = 2$ então $n = 2^1 \times 1$.
- $n = 3$ então $n = 2^0 \times 3$.

(b) Hipótese: suponha que todo k, com $1 \leq k \leq n$, possa ser escrito como uma potência de 2 vezes um ímpar.

(c) Passo indutivo: vamos dividir em dois casos

- Se $n+1$ for ímpar, então $n+1 = 2^0 \times (n+1)$ e o problema acaba.
- Se $n+1$ for par, então $n+1 = 2 \times (n+1)/2$, sendo que

$$\frac{n+1}{2} \leq n \Leftrightarrow n+1 \leq 2n \Leftrightarrow 1 \leq n \tag{1.18}$$

então $(n+1)/2$ se encaixa na nossa hipótese de induÃ§Ã£o, o que nos permite concluir que

$$\frac{n+1}{2} = 2^r \times s \text{ , sendo } s \text{ ímpar} \tag{1.19}$$

ou seja, $n+1 = 2^{r+1} \times s$, conforme queríamos.

Exemplo *(Decomposição Binária)* Todo n natural é soma de potências distintas de 2.

Solução: O raciocício também é indutivo. Assim,

(a) Casos iniciais: se

- $n = 1$ então $n = 2^0$.
- $n = 2$ então $n = 2^1$.
- $n = 3$ então $n = 2^1 + 2^0$.
- $n = 4$ então $n = 2^2$.

(b) Hipótese indutiva: suponha que todo k, $1 \leq k \leq n-1$, possa ser escrito como soma de potências distintas de dois.

(c) Passo indutivo: seja $p = \lfloor \log_2 n \rfloor$, ou seja, p é tal que

$$2^p \leq n < 2^{p+1} \tag{1.20}$$

Vamos olhar para o número $n - 2^p$. Esse número satisfaz a hipótese de indução, pois

$$n - 2^p < 2^p \Leftrightarrow n < 2^{p+1} \tag{1.21}$$

Daí esse número pode ser escrito como soma de potências distintas de dois. Além disso, a maior potência é estritamente menor que 2^p, uma vez que $n - 2^p < 2^p$. Dessa forma, se

$$n - 2^p = \sum_{i=1}^{j} 2^{r_i} \text{ , com } r_a \neq r_b \text{ e } \max\{r_i\}_{1 \leq i \leq j} < p \tag{1.22}$$

podemos concluir que

$$n = 2^p + \sum_{i=1}^{j} 2^{r_i} \tag{1.23}$$

com $r_a \neq r_b$ e $r_i < p$, o que conclui a demonstração.

1.4 Máximo Divisor Comum

Definição 1.4.1. (Maximo Divisor Comum) *Sejam a e b números inteiros, não nulos. Defina o conjunto*

$$S = \{d \in \mathbb{N} \text{ } tal \text{ } que \text{ } d \mid a \text{ } e \text{ } d \mid b\} \tag{1.24}$$

Dizemos que $mdc(a, b) = max\{S\}$, ou seja, é o maior dos dividores de a e b.

Vamos apresentar um teorema que será muito importante para nós no Capítulo 2: Teorema de Bezout. Como ele conseguimos expressar combinações lineares do *mdc* de dois números positivos.

Teorema 1.4.2. (Bezout - Existência e Unicidade do MDC) *Sejam os inteiros positivos a e b com $d = mdc(a, b)$. Então existem inteiros x e y tais que*

$$ax + by = d \tag{1.25}$$

Demonstração Considere o conjunto

$$S = \{ax + by \Big| x, y \in \mathbb{Z}\} \tag{1.26}$$

Pelo Princípio da Boa Ordenação, considerando apenas os valores positivos em S, garantimos que S possui um menor elemento positivo, digamos que seja $m = a \cdot x_0 + b \cdot y_0$.

Afirmação: m divide qualquer outro elemento de S. Ora, tome $n = ax_1 + by_1$ um elemento de S e suponha que

$$n = mq + r, \text{ , com } 0 \leq r \leq m \tag{1.27}$$

Então

$$r = n - m \cdot q = (ax_1 + by_1) - (ax_0 + by_0)q = a(x_1 - qx_0) + b(y_1 - qy_0) \tag{1.28}$$

ou seja, $r \in S$, o que nos permite afirmar que $r = 0$ e, consequentemente, $m \mid n$.

Agora perceba que $a \in S$ e $b \in S$, pois basta fazer $(x, y) = (0, 1), (1, 0)$, dessa forma $m \mid a$ e $m \mid b$, ou seja $m \mid mdc(a, b)$ implicando em $m \leq mdc(a, b)$. Por outro lado, como

$$m = a \cdot x_0 + b \cdot y_0 \tag{1.29}$$

então $mdc(a, b) \mid m$, ou seja, $mdc(a, b) \leq m$. Concluindo, $m = mdc(a, b)$. ■

Vejamos dois exemplos do Teorema 1.4.2.

Exemplo Considere $a = 6$ e $b = 27$ e em seguida $a = 7$ e $b = 15$. Temos que

$$6 \cdot (-3) + 27 = 3 \quad \text{e} \quad 7 \cdot (-2) + 15 = 1$$

Vamos explorar um pouco mais o Teorema 1.4.2, ou seja, vejamos que são os elementos do conjunto S definido da demonstração desse Teorema.

Teorema 1.4.3. *Sejam a e b dois inteiros, não simultaneamente nulos. Então o conjunto dos múltiplos de $d = mdc(a, b)$ é o conjunto*

$$S = \{ax + by \mid x, y \in \mathbb{Z}\}$$

Demonstração Ora, como $d \mid$ a e $d \mid b$ então d divide qualquer elemento de S. Sabemos que existem inteiros x_0 e y_0 tais que

$$d = ax + by_0 \tag{1.30}$$

sendo assim, $r \cdot d = a(rx_0) + b(ry_0)$ e assim todo múltiplo de d pode ser escrito como queríamos. ■

1.5 Algoritmo de Euclides e MMC

O Algoritmo de Euclides nos ajudará imensamente nas equações diofantinas lineares. Através dele, poderemos determinar variáveis determinantes em nosso problema.

Antes de introduzí-lo, vamos apresentar um Lema muito importante para nós.

Lemma 1.5.1. *Suponha que a e b sejam inteiros e que*

$$a = bq + r \tag{1.31}$$

Então, $mdc(a, b) = mdc(b, r)$

Demonstração Seja $d = mdc(a, b)$. Então $d \mid (a - bq)$ ou seja $d \mid r$ assim $d \mid mdc(b, r)$. Da mesma forma, se definirmos $d' = mdc(b, r)$ teremos que $d' \mid bq + r$ ou seja $d' \mid a$ assim d' divide o mdc entre a e b.

Portanto, $d \mid d'$ e $d \mid d'$, mas como ambos são positivos então $d = d'$. ■

Teorema 1.5.2. (Algoritmo de Euclide) *Sejam a e b inteiro positivos, com $a > b$ e $b \nmid a$. Então para se determinar o $mdc(a, b)$ basta utilizar o algoritmo da divisão e o Lema 1.5.*

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_4 \\ \vdots &= \vdots \end{aligned}$$

o algoritimo para quando $r_n = 0$. O algortimo é utilizado para se determinar os inteiros x e y tais que $ax + by = mdc(a, b)$.

Perceba que $mdc(a, b) = mdc(a, -b)$, ou seja, não precisamos nos preocupar com a ou b negativos. Basta supor a e b positivos.

Vejamos alguns exemplos.

Exemplo Determine $mdc(132, 39)$ pelo algoritmo de Euclides. Temos

$$\begin{aligned} 132 &= 39 \cdot 3 + 15 \\ 39 &= 15 \cdot 2 + 9 \\ 15 &= 9 \cdot 1 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 \end{aligned}$$

assim, $mdc = 3$

Exemplo Determine $mdc(280, 64)$ pelo algoritmo de Euclides. Temos

$$\begin{aligned} 280 &= 64 \cdot 4 + 24 \\ 64 &= 24 \cdot 2 + 16 \\ 24 &= 16 \cdot 1 + 8 \\ 16 &= 8 \cdot 2 \end{aligned}$$

assim $mdc = 8$

Agora, vamos definir o Mínimo Múltiplo Comum entre dois números quaisquer.

Definição 1.5.3. (Mínimo Múltiplo Comum) *Sejam a e b números inteiros, não simultaneamente nulos. Dizemos que m é o $mmc(a, b)$ quando $m > 0$, $m \mid a$ e $m \mid b$, e todo c positivo tal que $a \mid c$ e $b \mid c$ então $m \leq c$.*

De posse dos conhecimentos de máximo divisor comum e mínimo múltiplo comum, demonstraremos um teorema envolvendo os dois conceitos.

Teorema 1.5.4. *Sejam a e b números inteiros positivos, então*

$$mdc(a, b) \cdot mmc(a, b) = a \cdot b \tag{1.32}$$

Demonstração Sejam $d = mdc(a, b)$ e $m = mmc(a, b)$. Perceba que

$$a \mid a\frac{b}{d} \quad \text{e} \quad b \mid b\frac{a}{d} \tag{1.33}$$

ou seja, (ab/d) é um múltiplo de m assim

$$\frac{ab}{d} = mk \Rightarrow \frac{a}{d} = \frac{m}{b}k \quad e \quad \frac{b}{d} = \frac{m}{a}k \tag{1.34}$$

assim, $k \mid (a/d)$ e $k \mid (b/d)$ mas sabemos que $mdc(a/d, b/d) = 1$, ou seja, $k = 1$. Portanto

$$a \cdot b = m \cdot d \tag{1.35}$$

■

1.6 Números Primos

Definição 1.6.1. *Dizemos que n é um número primo quando os únicos divisores positivos de n são 1 e n.*

Definição 1.6.2. *Sejam n um inteiro positivo e p um divisor primo de n. A maior potência de p que divide n é presentado por α, onde*

$$p^{\alpha} \Big|\Big| n \tag{1.36}$$

Proposição 1.6.3. *Seja n um inteiro positivo, cuja fatoração canônica é dada por*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \tag{1.37}$$

então, a soma dos divisores positivos de n é dada por

$$D(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \times \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \times \ldots \times \frac{p_m^{\alpha_m+1} - 1}{p_m - 1} \tag{1.38}$$

Demonstração Seja d um divisor de n. Assim, todos os fatores primos de d também são de n. Além disso, suponha que $p_k \Big| d$ e

$$p_k^{\beta} \Big|\Big| d \tag{1.39}$$

então, podemos concluir que $\beta \leq \alpha_k$. Portanto, perceba que todo divisor de n tem a seguinte representação canônica

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_m^{\beta_m} \tag{1.40}$$

sendo $\beta_i \leq \alpha_i$, com $1 \leq i \leq m$. Dessa forma, ao expandirmos a expressão

$$\left(1 + p_1 + \ldots + p_1^{\alpha_1}\right)\left(1 + p_2 + \ldots + p_2^{\alpha_2}\right) \ldots \left(1 + p_m + \ldots + p_m^{\alpha_m}\right) \tag{1.41}$$

observamos que há todos os divisores positivo de n e como

$$1 + p_i + \ldots + p_i^{\alpha_i} = \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \tag{1.42}$$

e, assim, concluímos o que queríamos. ■

Apresentaremos alguns exemplos que envolvam os conceitos de números primos na teoria dos números.

Exemplo Existem infinitos números primos.

Solução: Vamos mostrar por absurdo. Assim, suponha que $\{p_1, p_2, \ldots, p_m\}$ seja o conjunto com todos os primos. Considere o número

$$N = p_1 p_2 \ldots p_n + 1 \tag{1.43}$$

Note que $p_i \nmid N$ para qualquer $1 \leq i \leq n$, pois caso contrário, $p_i = 1$. Assim, N seria um novo número primo, uma vez que $N > p_n$ e ninguém o divide. Mas chegamos a uma contradição, pois supomos que a quantidade total de primos era n. Portanto, existem infinitos primos.

Exemplo Existem infinitos números primos da forma $4k + 3$, para k inteiro positivo.

Solução: Vamos mostrar por absurdo. Assim, suponha que $\{p_1 = 3, p_2 = 7, \ldots, p_m\}$ seja o conjunto com todos os primos da forma $4k+3$. Considere o número

$$N = 4p_2 \ldots p_n + 3 \tag{1.44}$$

Note que $p_i \nmid N$ para qualquer $1 \leq i \leq n$, pois caso contrário, $p_i = 3$, para $i > 1$, ou $p_1 \mid p_k$, para $k > 1$, e ambos os casos são um absurdo.

Dessa forma, podemos concluir que N é o produto apenas de primos da forma $4k' + 1$. Mas o produto de números congruos a 1 módulo 4 também é côngruo a 1 módulo 4. Mas N é congruo a 3 módulo 4, que é um absurdo.

Portanto, a quantidade de primos da forma $4k + 3$ deve ser infinita.

1.7 Congruências

Muitas vezes trabalhar com congruências é mais vantajoso, uma vez que suas propriedades são mais fáceis de serem utilizadas nos problemas.

Definição 1.7.1. *Dados os inteiros a e b e o inteiro positivo m, dizemos que a e b são congruentes quando $m \mid a - b$ e escrevemos como*

$$a \equiv b \pmod{m} \tag{1.45}$$

Proposição 1.7.2. *Dados os inteiros a, b, c, d e o inteiro positivo m então*

a) Se $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$ então $a \pm c \equiv b \pm d \pmod{m}$.

b) Se $a \equiv c \pmod{m}$ e $b \equiv d \pmod{m}$ então $ab \equiv cd \pmod{m}$.

c) Se $a \equiv c \pmod{m}$ então $a^n \equiv c^n \pmod{m}$ para qualquer $n \in \mathbb{N}$

Demonstração Para os itens (a) e (b) sabemos que por definição existem inteiros r e s tais que

$$a = c + mr \quad b = d + ms \tag{1.46}$$

então $a \pm b = c \pm d + m(r + s)$ e $ab = cd + m(cs + dr + mrs)$ o que conclui a demonstração.

Para o item (c) temos que

$$a^n = c^n + \sum_{i=1}^{n} \binom{n}{i} c^{n-i} m^i \tag{1.47}$$

sendo que $m \mid c^{n-i}m^i$ para $i = 1, 2, \ldots, n$. Entao $a^n \equiv c^n \pmod{m}$. ■

Definição 1.7.3. (Classe de Resíduos) *Sejam m um inteiro positivo. Dizemos que $(r_1, r_2, \ldots, r_m)$ é uma classe de resíduos módulo m, quando para qualquer inteiro y existe um único i tal que*

$$y \equiv r_i \pmod{m} \tag{1.48}$$

Por exemplo, se $m = 5$ então os conjunto $\{0, 1, 2, 3, 4\}$, $\{-1, 0, 1, 2, 3\}$ e $\{10, 26, 13, 122, 1004\}$ obviamente são classes de resíduos módulo 5, uma vez que cada conjunto apresenta todos os restos na divisão por 5 e contém exatamente 5 elementos.

Definição 1.7.4. (resíduo quadrático) *Sejam a e m inteiros, com $m > 1$. Dizemos que o a é resíduo quadrático módulo m, se existe x inteiro tal que*

$$x^2 \equiv a \pmod{m} \tag{1.49}$$

Por exemplo, os resíduos quadráticos módulo 7 são 0, 1, 2, e 4. Já módulo 8 são 0, 1, e 4, apenas.

Proposição 1.7.5. *Seja $(r_1, r_2, \ldots, r_m)$ uma classe de resíduos módulo m, sendo m um inteiro positivo. Se a é um inteiro tal que $mdc(a, m) = 1$, então, $(ar_1, ar_2, \ldots, ar_m)$ também é uma classe de resíduos módulo m.*

Demonstração Deveremos mostrar apenas que $m \nmid ax_i - ax_j$, para $i \neq j$, assim garantimos m restos distintos no novo conjunto. Temos

$$ax_i - ax_j = a(x_i - x_j) \tag{1.50}$$

Ora, como $mdc(a, m) = 1$, não existe nenhum fator primo em comum entre a e m, assim nos resta verificar se $m \mid (x_i - x_j)$. Mas, por hipótese, os inteiros x_i,$1 \leq i \leq m$, é um sistema completo de restos, isto é, $m \nmid (x_i - x_j)$, para $i \neq j$. Portanto, concluímos que nosso novo conjunto é uma classe de resíduos módulo m. ■

Definição 1.7.6. (inverso multiplicativo) *Seja a um número inteiro e m um número inteiro positivo. Dizemos que x é o inverso de a módulo m quando*

$$a \cdot x \equiv 1 \pmod{m} \tag{1.51}$$

Proposição 1.7.7. *Seja m um inteiro positivo. Então todo inteiro a, tal que $mdc(a, m) = 1$, apresenta um inverso multiplicativo módulo m.*

Demonstração Na verdade, queremos encontrar y tal que

$$ax = 1 + my \Leftrightarrow ax - my = 1 \tag{1.52}$$

mas o Teorema de Bézout nos garante que quando $mdc(a, m) = 1$ existem tais inteiros x e y. Dessa forma, podemos garantir que existe um inteiro x tal que

$$ax \equiv 1 \pmod{m} \tag{1.53}$$

■

Vamos apresentar uma série de exemplos de suma importância para as Equações Dioafantinas apresentadas no Capítulo 4.

Exemplo Mostrar que todo número primo, exceto 2 e 3, deixa resto 1 ou 5 na divisão por 6.

Solução. Ora, sabemos que todo primo maior que 3 pode ser escrito como

$$p \equiv r \pmod 6, \text{ com } r = 0, 1, 2, 3, 4, \text{ ou } 5 \tag{1.54}$$

mas

- r não pode ser 0, pois assim $6 \mid p$;
- r não pode ser 2, pois assim $2 \mid p$;
- r não pode ser 3, pois assim $3 \mid p$;
- r não pode ser 4, pois assim $2 \mid p$;

e então $r = 1$ ou 5.

Exemplo Mostrar que 11^{10} deixa resto 1 na divisão por 100.

Solução. Como $100 = 25 \times 4$ e $mdc(25, 4) = 1$ vamos analisar cada congruência. Temos

$$11^2 \equiv 1 \pmod 4 \Rightarrow 11^{10} \equiv 1^5 = 1 \pmod 4 \tag{1.55}$$

e

$$11^2 \equiv -4 \pmod{25} \Rightarrow 11^{10} \equiv (-4)^5 = -2^{10} = -1024 \equiv 1 \pmod{25} \tag{1.56}$$

portanto $11^{10} \equiv 1 \pmod 1$00.

Exemplo Ache os restos das divisões de 2^{50} e 41^{65} por 7

Solução. Temos que

$$2^3 \equiv 1 \pmod 7 \Rightarrow 2^{48} \equiv (1)^{16} \pmod 7 \Rightarrow 2^{50} \equiv 4 \pmod 7 \tag{1.57}$$

e

$$41 \equiv -1 \pmod 7 \Rightarrow 41^{65} \equiv (-1)^{65} = -1 \pmod 7 \tag{1.58}$$

Exemplo Sendo a um número inteiro, determine os restos da divisão de a^2 e a^3 por 8.

Solução. Dado a qualquer inteiro, temos que

$$a \equiv 0, \pm 1, \pm 2, \pm 3, 4 \pmod 8 \tag{1.59}$$

então

$$a^2 \equiv 0, 1, 4 \pmod 8 \tag{1.60}$$

e

$$a^3 \equiv -1, 0, 1, 3, \pmod 8 \tag{1.61}$$

Exemplo Seja p um número primo. Se $x^2 \equiv 1 \pmod p$ então $x \equiv \pm 1 \pmod p$.

Solução. Temos que

$$p \mid (x-1)(x+1) \Rightarrow p \mid x-1 \text{ ou } p \mid x+1 \tag{1.62}$$

Os dois casos implica em $x \equiv \pm 1 \pmod p$. Note que caso p divida ambos os números, então $p = 2$

1.8 Exercícios de Aprofundamento

Apresentaremos uma série de problemas envolvendo a Teoria dos Números vista no Capítulo 1 e que, de alguma forma, nos ajudará posteriormente na resolução das equações diofantinas.

Problema 1.8.1. *Prove que para qualquer número natural n*

$$mdc(n!+1,(n+1)!+1)=1 \tag{1.63}$$

Solução Seja $d=mdc(n!+1,(n+1)!+1)$. Temos que $(n+1)(n!+1)=(n+1)!+(n+1)$ e daí

$$d \mid [(n+1)!+1]-[n!+1] \Rightarrow d \mid n \Rightarrow d \mid n! \tag{1.64}$$

e assim $d \mid 1$, ou seja, $d=1$.

Problema 1.8.2. *Seja p um número primo. Então, a equação*

$$x^2 \equiv -1 \pmod{p} \tag{1.65}$$

tem solução se, e somente se, $p=2$ ou $p \equiv 1 \pmod 4$.

Solução É fácil notar que 2 apresenta solução para a equação dada. Suponha p primo ímpar. Perceba que

$$(p-1)!=\underbrace{\left(1.2.\ldots.\frac{(p-1)}{2}\right)}_{A}\underbrace{\left(\frac{(p+1)}{2}\ldots.(p-1)\right)}_{B} \tag{1.66}$$

ou seja, dividimos esse produto em dois números, A e B, com a mesma quantidade de fatores. Perceba que se $j \in A$ então $(p-j) \in B$. Note também que

$$j(p-j)=pj-j^2 \equiv -j^2 p mod p \tag{1.67}$$

Portanto,

$$(p-1)! \equiv (-A^2)^{\frac{p-1}{2}} \pmod{p} \Rightarrow (p-1)! \equiv (-1)^{\frac{p-1}{2}} A^{p-1} \pmod{p} \tag{1.68}$$

Utilizando o Teorema de Wilson e o Teorema de Fermat, concluímos que

$$(-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p} \tag{1.69}$$

ou seja, $p-1$ deve ser o dobro de um ímpar, digamos que $2(2k+1)$, e assim $p = 4k+3$.

Agora suponha que p é primo tal que $p \equiv 3 \pmod 4$. Vamos mostrar que existe x que satisfaça a congruência. Basta tomar $x = A$ e assim conseguimos uma solução.

Problema 1.8.3. *Demonstre que para todo inteiro positivo n,*

$$7 \mid 3^{2n+1} + 2^{n+2} \tag{1.70}$$

Solução Faremos por indução sobre n. Para $n = 1$ e $n = 2$ verificamos a veracidade do problema. Suponha então que para $k = 1, 2, \ldots, n$ então

$$3^{2n+1} \equiv -2^{n+2} \pmod 7 \Rightarrow 3^{2(n+1)+1} \equiv -2^{n+2} \cdot 3^2 \pmod 7 \tag{1.71}$$

mas é fácil observar que

$$2^{n+2} \cdot 3^2 \equiv 2^{n+3} \pmod 7 \Leftrightarrow 3^2 \equiv 2 \pmod 7 \tag{1.72}$$

essa última congruência sendo facilmente constatada. Portanto, pelo Princípio da Indução Finita, é válido para todo n natural.

Problema 1.8.4. (Bulgária) *Mostre que para todo n natural, $n \geq 3$, existem pares de inteiros positivos (x_n, y_n) tais que*

$$7x_n^2 + y_n^2 = 2^n \tag{1.73}$$

Solução Faremos alguns casos pequenos

- Para $n = 3$ tome $x_n = y_n = 1$;

- Para $n = 4$ tome $x_n = 1$ e $y_n = 3$;
- Para $n = 5$ tome $x_n = 1$ e $y_n = 5$;
- Para $n = 6$ tome $x_n = 3$ e $y_n = 1$;
- Para $n = 7$ tome $x_n = 1$ e $y_n = 11$;

Vamos conjecturar nossa sequência da seguinte forma

$$x_{n+1} = \frac{x_n \pm y_n}{2} \quad \text{e} \quad y_{n+1} = \frac{7x_n \mp y_n}{2} \tag{1.74}$$

pois assim,

$$7x_{n+1}^2 + y_{n+1}^2 = \frac{1}{4}(7x_n^2 + y_n^2 + 7(7x_n^2 + y_n^2)) = 2^{n+1} \tag{1.75}$$

ou seja, nossa conjectura obedece a hipótese. Mas devemos observar apenas se x_{n+1} e y_{n+1} são número inteiros.

Sempre deveremos escolher x_n e y_n para ser ímpares. Assim, se

- $x_n \equiv 1 \pmod 4$ e $y_n \equiv 1 \pmod 4$. Então escolhemos

$$x_{n+1} = \frac{x_n + y_n}{2} \quad \text{e} \quad y_n = \frac{7x_n - y_n}{2} \tag{1.76}$$

  pois assim $x_{n+1} \equiv 1 \pmod 2$ e $y_{n+1} \equiv 1 \pmod 2$.

- $x_n \equiv 1 \pmod 4$ e $y_n \equiv -1 \pmod 4$. Então escolhemos

$$x_{n+1} = \frac{x_n - y_n}{2} \quad \text{e} \quad y_n = \frac{7x_n + y_n}{2} \tag{1.77}$$

  pois assim $x_{n+1} \equiv 1 \pmod 2$ e $y_{n+1} \equiv 1 \pmod 4$

- $x_n \equiv -1 \pmod 4$ e $y_n \equiv 1 \pmod 4$. Então escolhemos

$$x_{n+1} = \frac{x_n - y_n}{2} \quad \text{e} \quad y_n = \frac{7x_n + y_n}{2} \tag{1.78}$$

  pois assim $x_{n+1} \equiv 1 \pmod 2$ e $y_{n+1} \equiv 1 \pmod 2$

- $x_n \equiv -1 \pmod 4$ e $y_n \equiv -1 \pmod 4$. Então escolhemos

$$x_{n+1} = \frac{x_n + y_n}{2} \quad \text{e} \quad y_n = \frac{7x_n - y_n}{2} \tag{1.79}$$

  pois assim $x_{n+1} \equiv 1 \pmod 2$ e $y_{n+1} \equiv 1 \pmod 4$

Agora podemos garantir que as soluções são inteiras positivas e pelo Princípio da Indução Finita, para cada $n \geq 3$ existirão x_n e y_n que satisfaça a equação.

Problema 1.8.5. (Teorema de Thue) *Sejam m um número natural e a um inteiro primo com m. Então, existem naturais x e y, ambos menores que $\sqrt{m}$ tais que $\pm ax \pm y$ é divisível por m para alguma escolha ótima de x e y e dos sinais.*

Solução Defina $q = \lfloor \sqrt{m} \rfloor$ e assim $(q+1)^2 > m$. Vamos considerar as expressões $ax - y$ para x e y assumindo os valores $0, 1, \ldots, q$. Como teremos $q+1$ números, Pelo Princípio da Casa dos Pombos dois deles deixarão o mesmo resto na divisão por m. Digamos que

$$ax_1 - y_1 \equiv ax_2 - y_2 \pmod{m} \tag{1.80}$$

assim $m \mid a(x_1 - x_2) - (y_1 - y_2)$. Perceba que $x_1 \neq x_2$ pois caso contrário $m \mid y_1 - y_2$. Da mesma forma $y_1 \neq y_2$. Agora veja que

$$-\sqrt{m} \leq 0 - q < x_1 - x_2 < q - 0 \leq \sqrt{m} \tag{1.81}$$

analogamente $|y_1 - y_2| \leq \sqrt{m}$ e assim o número $a(x_1 - x_2) - (y_1 - y_2)$ satisfaz nosso problema.

Problema 1.8.6. (Coréia) *Demonstre que para qualquer número primo p, existem inteiros x, y, z, w tais que*

$$x^2 + y^2 + z^2 - wp = 0 \tag{1.82}$$

Solução Sejam os resíduos quadráticos de p os números pertencente ao conjunto $\{a_1, \ldots, a_r\}$ sendo $r = (p-1)/2$. Vamos mostrar que podemos achar dois elementos nesse conjunto, a e b, tais que $a + b = p - 1$.

Ora, os casos $(0, p-1)$ são facilmente verificados. Logo, suponha que $p - 1$ não seja um resíduo quadrático. Suponha também que não seja possível encontrar dois elementos desse conjunto cuja soma é $p - 1$. Considere o conjunto

$$\{p - 1 - a_1, \ldots, p - 1 - a_r\} \tag{1.83}$$

Vamos olhar para o número $(p-1)/2$. Caso ele pertence a classe de redísuos, então $p-1-(p-1)/2 = (p-1)/2$ pertenceria ao outro grupo, que não é a classe de resíduos. Mas trata-se do mesmo número e chegamos a um absurdo.

Portanto há dois resíduos quadráticos, a_x e a_y tais que $a_x + a_y = p-1$. Dessa forma, podemos escolher $x = a_x$, $y = a_y$, $z = 1$ e w o quociente da divisão, isto é,

$$w = \frac{x^2 + y^2 + 1}{p} \tag{1.84}$$

que é inteiro, uma vez que $p \mid a_x^2 + a_y^2 + 1$

Problema 1.8.7. (Índia)

(a) Mostre que o produto dois números da forma a^2+3b^2, com a e b inteiros, também é desta forma.

(b) Se um inteiro n é tal que $7n$ é da forma a^2+3b^2, com a e b inteiros,prove que n também é desta forma.

Solução a) Note que

$$\begin{aligned}(a^2+3b^2)(c^2+3d^2) &= (a^2c^2+9b^2d^2)+3(a^2d^2+b^2c^2) &(1.85)\\ &= (ac+3bd)^2+3(ad-bc)^2 &(1.86)\end{aligned}$$

b) Temos que $a^2 \equiv -3b^2 \equiv 4b^2 \pmod 7$. Logo temos duas possibilidades

- Se $a \equiv 2b \pmod 7$. Tome os inteiros

$$c = \frac{2a+3b}{7} \quad \text{e} \quad d = \frac{a-2b}{7} \tag{1.87}$$

e assim

$$c^2 + 3d^2 = \frac{7a^2+21b^2}{49} = \frac{a^2+3b^2}{7} = n \tag{1.88}$$

Problema 1.8.8. (Cone Sul) *Considere a sequência a_n definida da seguinte maneira:*

$$\begin{aligned} a_1 &= 1 \\ a_2 &= 3 \\ a_{n+2} &= 2a_{n+1}.a_n + 1, \text{ para todo inteiro } n \geq 1. \end{aligned}$$

Prove que a máxima potência de 2 que divide $a_{4006} - a_{4005}$ é 2^{2003}

Solução Defina a nova sequência $x_n = a_n - a_{n-1}$, para $n \geq 2$. Vamos mostrar por indução que $2^n \mid x_{2n}$ mas $2^{n+1} \nmid x_{2n}$ e que $2^{n+1} \mid x_{2n+1}$.

Vejamos os apenas um caso inicial. Para $n = 2$ então

$$\begin{aligned} x_2 = a_2 - a_1 = 2 &\Rightarrow 2^1 \mid x_2, \text{ mas } 2^2 \nmid 2 \\ x_3 = a_3 - a_2 = 4 &\Rightarrow 2^2 \mid x_3 \end{aligned}$$

Suponha nossa hipótese válida para $k = 2, 3, \ldots, n$. Daí,

$$x_{2n+2} = a_{2n+2} - a_{2n+1} = 2a_{2n}(a_{2n+1} - a_{2n-1}) \tag{1.89}$$

Por hipótese de indução, sabemos que

$$\begin{aligned} x_{2n+1} = 2^{n+1}k_1 &\Rightarrow a_{2n+1} - a_{2n} = 2^{2n+1}k_1 \\ x_{2n} = 2^n k_2 &\Rightarrow a_{2n} - a_{2n-1} = 2^{2n}k_2 \end{aligned}$$

sendo k_2 ímpar. Daí $a_{2n+1} - a_{2n-1} = 2^{2n}\underbrace{(2k_1 + k_2)}_{\text{ímpar}}$. Substituindo na equação que define x_{2n+2},

$$x_{2n+2} = 2^{n+1} \underbrace{a_{2n}}_{\text{ímpar}} \underbrace{(2k_1 + k_2)}_{\text{ímpar}} \tag{1.90}$$

portanto provamos que a máxima potência que divide x_{2n+2} é 2^{n+1}. Analogamente, perceba que

$$x_{2n+3} = a_{2n+3} - a_{2n+2} = 2a_{2n+1}(a_{2n+2} - a_{2n}) \tag{1.91}$$

e

$$x_{2n+2} = 2^{n+1}k_3 \Rightarrow a_{2n+2} - a_{2n+1} = 2^{2n+1}k_3 \tag{1.92}$$

$$x_{2n+1} = 2^{n+1}k_1 \Rightarrow a_{2n+1} - a_{2n} = 2^{2n+1}k_1 \tag{1.93}$$

$$\tag{1.94}$$

com k_3 ímpar. Daí $a_{2n+2} - a_{2n} = 2^{2n+1}(k_1 + k_3)$. Substituindo na equação que define x_{2n+3},

$$x_{2n+3} = 2^{n+2} a_{2n+1}(k_2 + k_3) \tag{1.95}$$

ou seja, $2^{n+2} \mid a_{2n+3}$. Portanto, pelo Princípio da Indução Finita, nossa hipótese é válida para qualquer natural n, tal que $n \geq 2$.

Problema 1.8.9. *Demonstre que para a, r e s inteiros positivos, com $a > 2$ então*

$$mdc(a^r - 1, a^s - 1) = a^{mdc(r,s)} - 1 \tag{1.96}$$

Solução Seja $d = mdc(a^r - 1, a^s - 1)$. Assim $a^r \equiv 1 \pmod{d}$ e $a^s \equiv 1 \pmod{d}$. Pelo teorema de Bezout, sabemos que existem inteiros positivos x e y tais que (sem perda de generalidade suponha eles positivos)

$$rx - sy = m \tag{1.97}$$

onde $m = mdc(r, s)$. Daí $a^{xr} \equiv 1 \pmod{d}$ e $a^{ys} \equiv 1 \pmod{d}$ ou seja

$$a^{rx} \equiv a^{sy} \pmod{d} \Rightarrow a^{rx-sy} \equiv 1 \pmod{d} \tag{1.98}$$

e assim $a^m \equiv 1 \pmod{d}$, ou seja, $d \mid a^m - 1$. Mas é fácil verificar que

$$a^m - 1 \mid a^r - 1 \quad \text{e} \quad a^m - 1 \mid a^s - 1 \tag{1.99}$$

ou seja $a^m - 1 \mid d$. Portanto $d = a^m - 1$.

Problema 1.8.10. (*OBM) Qual é o menor inteiro $a > 1$ para o qual existe n inteiro positivo tal que $a^{2^n} - 1$ é múltiplo de 2015?*

Solução Note que $n = 1$ implica $a = 2014$. Suponha então $n > 1$. Note que $2015 = 5 \cdot 13 \cdot 31$, então queremos que $a^{2^n} - 1$ seja múltiplo de 5, 13 e 31.

Pelo pequeno teorema de Fermat, sabemos que

- $a^4 \equiv 1 \pmod 5$, basta que a não seja múltiplo de 5.
- $a^{12} \equiv 1 \pmod{13}$ e como $n \geq 2$ (basta testar no problema), $mdc(a^{2^n} - 1, a^{12} - 1) = a^4 - 1$, de acordo com o problema anterior. Assim $13 \mid a^4 - 1$ o que nos dá

$$a \equiv \pm 1, \pm 5 \pmod{13} \tag{1.100}$$

- $a^{30} \equiv 1 \pmod{31}$. Da mesma forma temos que $31 \mid a^{mdc(30,2^n)} - 1$, ou seja, $31 \mid a^2 - 1$, o que nos dá

$$a \equiv \pm 1 \pmod 3 1 \tag{1.101}$$

Portanto, basta testarmos os valores e encontramos $n = 2$ e $a = 92$

Problema 1.8.11. *Mostre que existem infinitos números naturais n, tais que* $n \mid 2^n + 1$.

Solução Vamos mostrar que

$$3^k \mid 2^{3^k} + 1, \text{ para } k \geq 1 \tag{1.102}$$

e assim o problema acaba. A demonstração será por indução. Os casos iniciais são facilmente verificados. Ora, queremos mostrar que

$$3^{k+1} \mid 2^{3^{k+1}} + 1 \tag{1.103}$$

Perceba que

$$2^{3^{k+1}} + 1 = \left(2^{3^k}\right)^3 + 1 = (2^{3^k} + 1)(2^{2\times 3^k} - 2^{3^k} + 1) \tag{1.104}$$

Ora, por hipótese de indução, sabemos que $(2^{3^k} + 1)$ é divisível por 3^k. Basta a gente mostrar que

$$(2^{2\times 3^k} - 2^{3^k} + 1) \text{ é divisível por } 3 \tag{1.105}$$

Mas isso é imediato, uma vez que módulo 3

$$2^{2\times 3^k} \equiv 1 \text{ , } 2^{3^k} \equiv 2 \text{ e } 1 \equiv 1 \tag{1.106}$$

portanto $2^{2\times 3^k} - 2^{3^k} + 1 \equiv 0 \pmod 3$ e nosso problema acaba.

CAPÍTULO 2

EQUAÇÕES DIOFANTINAS LINEARES

Esse capítulo será destinado exclusivamente às equações Diofantinas Lineares. Será abordado um viés para alunos de olimpíadas de matemática e para professores que desejam seguir uma metodologia de ensino para esses alunos.

2.1 Definição

Define-se como *Equação Diofantina Linear* uma equação do tipo

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c \tag{2.1}$$

onde n, c e a_i, $1 \leq i \leq n$, são todos números inteiros. Nós vamos admitir que $n > 1$ e $a_i \neq 0$, para todo $1 \leq i \leq n$.

Primeiramente, vamos estudar um caso básico para facilitar o entendimento das soluções geradas a partir de uma solução inicial.

2.2 Solução da equação diofantina para o caso $n = 2$

Teorema 2.2.1. (Caso Particular) *Suponha que a, b e c seja números inteiros tais que*

$$ax + by = c \tag{2.2}$$

sendo a e b não nulos. Então é válido que

a) A equação 2.2 tem solução se, e somente se, $mdc(a, b) \mid c$

b) Sendo (x_0, y_0) *uma solução particular para a equação 2.2, então toda solução apresenta a forma*

$$x = x_0 + \frac{b}{d}k \quad e \quad y = y_0 - \frac{a}{d}k \tag{2.3}$$

sendo k um número inteiro e $d = mdc(a, b)$.

Demonstração a) Suponha que a equação 2.2 apresente uma solução particular (x_0, y_0), assim

$$ax_0 + by_0 = c \tag{2.4}$$

Defina $r = mdc(a, b)$. Temos que $r \mid a$ e $r \mid b$, isto é, por proriedades visto no Capítulo 1 envolvendo dividisibilidade, r divide qualquer combinação linear de a e b,

$$r \mid ax_0 + by_0 \Rightarrow r \mid c \tag{2.5}$$

Agora suponha que $mdc(a, b) \mid c$. Precisamos mostrar que isso é a única condição para a equação 2.2 apresentar soluções. Ora, dividindo a equação original por d, ficamos com

$$\frac{a}{d}x + \frac{b}{d}y = 1 \tag{2.6}$$

e isso nos reduz ao *Teorema de Bézout*, também visto no Capítulo 1, pois $mdc(a/d, b/d) = 1$. Dessa forma, existe solução para a equação 2.6 e, portanto, para a equação 2.2.

b) Tome (x_0, y_0) uma solução inicial e suponha que (x, y) seja uma outra solução da equação 2.2. Temos que

$$ax_0 + by_0 = ax + by \Rightarrow a(x - x_0) = b(y_0 - y) \tag{2.7}$$

Suponha ainda que $a = da_0$ e $b = db_0$, assim $mdc(a_0, b_0) = 1$, uma vez que a_0 e b_0 não possuem fator primo em comum. Substituindo na última equação, ficamos com

$$a_0(x - x_0) = b_0(y_0 - y) \tag{2.8}$$

Note que $a_0 \mid b_0(y_0 - y)$, mas como a_0 e b_0 não apresentam nenhum fator primo em comum, então podemos concluir que

$$a_0 \mid y_0 - y \Rightarrow y_0 - y = a_0 t, \texttt{ sendo } t \in \mathbb{Z} \tag{2.9}$$

ou seja,

$$a_0(x - x_0) = b_0(y_0 - y) = b_0 a_0 t \Rightarrow x - x_0 = b_0 t \tag{2.10}$$

Dessa forma, concluímos que

$$x = x_0 + \frac{b}{d}t \quad e \quad y = y_0 - \frac{a}{d}t \tag{2.11}$$

sendo t um número inteiro.

■

Vejamos alguns exemplos númericos das Equações Diofantinas com o método de Euclides para descobrir uma primeira combinação linear.

Exemplo Determine as soluções das seguintes equações

a) $172x + 20y = 1000$

Solução: Primeiramente, vamos aplicar o algoritmo de Euclide para determinar o *mdc* entre 172 e 20,

$$\begin{aligned} 172 &= 20 \cdot 8 + 12 \\ 20 &= 12 \cdot 1 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2 \end{aligned}$$

daí $mdc(172, 20) = 4$. Daí, procedemos da seguinte forma

$$4 = 12 - 8 = 12 - (20 - 12 \cdot 1) = 12 \cdot 2 - 20 = (172 - 20 \cdot 8) \cdot 2 - 20 \tag{2.12}$$

ou seja,

$$4 = 172 \cdot 2 - 17 \cdot 20 \tag{2.13}$$

b) $18x + 5y = 48$

Solução: Assim como feito no exemplo anterior, faremos o algoritmo de Euclides para determinar o mdc entre 18 e 5.

$$\begin{aligned} 18 &= 5 \cdot 3 + 3 \\ 5 &= 3 \cdot 1 + 2 \\ 3 &= 2 \cdot 1 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

e daí $1 = mdc(18, 5)$ ou seja,

$$1 = 3 - 2 \cdot 1 = 3 - (5 - 3 \cdot 1) \cdot 1 = 3 \cdot 2 - 5 \cdot 1 = (18 - 5 \cdot 3) \cdot 2 - 5 \cdot 1 \quad (2.14)$$

ou melhor,

$$1 = 18 \cdot 2 - 5 \cdot 7 \quad (2.15)$$

2.3 Solução da equação diofantina para o caso geral

Agora vamos um pouco além. Mostraremos um importante teorema a respeito da solução da Equação Diodantina Linear envolvendo mais de duas incógnitas.

Teorema 2.3.1. (Generalização Equação Diofantina) *Considere a Equação Diofantina 2.1. Essa equação tem solução se, e somente se,*

$$mdc(a_1, a_2, \ldots, a_n) \mid c \quad (2.16)$$

Demonstração Primeiramente, vamos mostrar que se a equaçãoo 2.1 apresenta solução então $mdc(a_1, a_2, \ldots, a_n) \mid c$. Ora, sabemos que $mdc(a_1, a_2, \ldots, a_n)$ divide cada inteiro a_i, $1 \leq i \leq n$. Pela Proposição 1.2.2, vista no Capítulo 1, também divide qualquer combinação linear desses inteiros. Em particular, divide a combinação linear

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c \quad (2.17)$$

e assim $mdc(a_1, a_2, \ldots, a_n) \mid c$.

Para demonstrar que outra parte do Teorema utilizaremos o Princípio da Indução, apresentada no Teorema 1.3.2 do Capítulo 1 desse Trabalho.

O caso $n = 2$ já pode ser constatado através do Teorema 2.2.1. Vamos fazer o que caso $n = 3$, ou seja, queremos mostrar que

$$ax + by + cz = d \tag{2.18}$$

tem sempre solução, quando $mdc(a, b, c) \mid d$. Note que

$$mdc(a, b, c) = mdc(mdc(a, b), c) \tag{2.19}$$

Já sabemos que podemos escrever o mdc de dois números como combinação linear deles, assim

$$mdc(a, b, c) = mdc(a, b) \cdot x + c \cdot y \tag{2.20}$$

sendo x e y números inteiros. Também sabemos que $mdc(a, b) = a \cdot k + b \cdot t$. Daí,

$$mdc(a, b, c) = a \cdot (kx) + b \cdot (tx) + c \cdot z \tag{2.21}$$

e dessa forma

$$a \cdot \frac{kxd}{mdc(a, b, c)} + b \cdot \frac{txd}{mdc(a, b, c)} + c \cdot \frac{zd}{mdc(a, b, c)} = d \tag{2.22}$$

sendo $\dfrac{d}{mdc(a, b, c)}$ um número inteiro, então conseguimos uma solução inteira para a equação 2.1 quando $n = 3$.

Supomos verdade para $k = 2$ até $n - 1$. Vamos mostrar que é verdade para $k = n$ e assim pelo Princípio da Indução Finita podemos garantir a solução para qualquer n natural.

Mas antes, vamos mostrar, também pelo Princípio da Indução Finita, que

$$mdc(a_1, a_2, \ldots, a_n) \tag{2.23}$$

pode ser escrita como combinação linear de $a_1, a_2, \ldots, a_n$, sendo $a_i, 1 \leq i \leq n$, números inteiros não nulos. Os casos $n = 2$ e $n = 3$ já estão feitos. Suponha verdade para $k = 2, 3, \ldots, n-1$. Considere agora os n números a_i, $1 \leq i \leq n$, onde queremos mostrar que

$$mdc(a_1, a_2, \ldots, a_n) \tag{2.24}$$

é combinação linear de seus elementos. Note que

$$mdc(a_1, a_2, \ldots, a_n) = mdc(mdc(a_1, a_2, \ldots, a_{n-1}), a_n) \tag{2.25}$$

Assim, pelo Teorema 1.4.2 existem inteiros x e y tais que

$$mdc(a_1, a_2, \ldots, a_n) = mdc(a_1, a_2, \ldots, a_{n-1}) \cdot x + a_n \cdot y \tag{2.26}$$

Agora utilizando indução em $mdc(a_1, a_2, \ldots, a_{n-1})$, sabemos que

$$mdc(a_1, a_2, \ldots, a_{n-1}) = a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} \tag{2.27}$$

e dessa forma, substituindo 2.27 in 2.26,

$$mdc(a_1, a_2, \ldots, a_n) = a_1(x_1x) + a_2(x_2x) + \ldots + a_{n-1}(x_{n-1}x) + a_ny \tag{2.28}$$

concluindo nossa demonstração. Assim, o Princípio da Indução Finita garante que para todo $n \in \mathbb{N}$, com $n \geq 2$, o mdc de n números inteiros, não nulos, pode ser escrita como combinação linear de seus elementos.

Vamos ao que nos interessa agora. Já sabemos que existem inteiros x_i, $1 \leq i \leq n$ tais que

$$mdc(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \ldots + a_{n-1}x_{n-1} + a_nx_n \tag{2.29}$$

Chamando de $d = mdc(a_1, a_2, \ldots, a_n)$, sabemos que $d \mid c$. Logo,

$$d = a_1 \cdot \left(x_1\frac{d}{c}\right) + a_2 \cdot \left(x_2\frac{d}{c}\right) + \ldots + a_n \cdot \left(x_n\frac{d}{c}\right) \tag{2.30}$$

como queríamos demonstrar. ■

Exemplo Encontre as soluções inteiras da equação

$$3x + 4y + 5z = 6 \tag{2.31}$$

Queremos encontrar as soluções de

$$3x + 4y = 6 - 5z = 1 - 5(-1 + z) = 1 - 5z' \tag{2.32}$$

uma solução particular é $x_0 = -1 + 3z'$ e $y_0 = 1 - z'$. Assim, a solução geral pode ser escrita como

$$x = x_0 + 4t \quad e \quad y = y_0 - 3t \tag{2.33}$$

com $t \in \mathbb{Z}$. Assim, encontramos todas as soluções como

$$(x, y, z) = (-1 + 3z' + 4t, 1 - z' - 3t, +1 + z') \tag{2.34}$$

2.4 The Frobenius Coin Problem

Considere os inteiros positivos a_i, com $1 \leq i \leq n$, sendo n um número positivo. Definimos $g(a_1, a_2, \ldots, a_n)$ como o maior inteiro N tal que a equação

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = N \tag{2.35}$$

não apresenta solução em $\mathbb{Z}_+^n$. Dizemos que não conseguimos pagar o valor N com as moedas cujos valores são $a_1, a_2, \ldots, a_n$.

Teorema 2.4.1. (Sylvester, 1884) *Sejam a e b inteiros positivos com* $mdc(a, b) = 1$. *Então*

$$g(a, b) = ab - a - b \tag{2.36}$$

Demonstração Vamos mostrar que qualquer inteiros maior que $ab - a - b$ pode ser escrito como combinação linear de a e b. Pelo Teorema 1.4.2, sabemos que existem inteiros x_0 e y_0 tais que

$$ax_0 + by_0 = 1 \tag{2.37}$$

e dessa forma, multiplicando ambos os membros da última equação por $g(a, b)$,

$$ax_1 + by_1 = g(a, b) \tag{2.38}$$

Vamos supor, sem perda de generalidade, que $x_1 \geq 0$, e então a equação

$$ax + by = g(a, b) \tag{2.39}$$

tem solução do tipo $x = x_0 + bt$ e $y = y_0 - at$, de acordo com o que provamos no Teorema 2.2.1.

Seja t o menor inteiro positivo tal que $y_0 - at \geq 0$. Temos que

$$a(x_0 + bt) + b(y_0 - at) = g(a, b) \geq (a - 1)(b - 1) = ab - a - b + 1 \tag{2.40}$$

Nosso t é escolhido de forma que $0 \leq y_0 - at \leq a - 1$, pois caso contrário incrementamos uma unidade em t. Assim,

$$a(x_0 + bt) \geq ab - a - b + 1 - b(a - 1) = -a + 1 > -a \tag{2.41}$$

ou seja,

$$x_0 + bt > -1 \Rightarrow x_0 + bt \geq 0 \tag{2.42}$$

o que completa nossa demonstração. ■

Vamos agora tentar achar um valor máximo para $g(a_1, \ldots, a_n)$, isto é, mostraremos que determinado valor K é possível obter combinações lineares inteiras, não negativas, de $a_1, a_2, \ldots, a_n$ tal que

$$\sum_{i=1}^{n} x_i a_i = K \tag{2.43}$$

Antes, precisamos demonstrar uma proposição que nos vai auxiliar bastante na demonstração do Teorema 2.4.3.

Proposição 2.4.2. *Considere os inteiros* $2 \leq a_1 < a_2 < \ldots < a_n$, *com* $n > 2$, *tal que* $mdc(a_1, a_2, \ldots, a_n) = 1$. *Assim, qualquer* $k \geq (a_1 - 1)(a_2 + \ldots + a_n - 1)$ *pode ser obtido através de uma combinação linear inteira não negativa de* $a_1, a_2, \ldots, a_n$, *isto é, existem inteiros não negativos* x_i, $1 \leq i \leq n$, *tal que*

$$\sum_{i=1}^{n} x_i a_i = k \tag{2.44}$$

Demonstração Sabemos, pelo Teorema 2.3.1 que existem inteiros x_i,$1 \leq i \leq n$, tais que

$$a_1 x_1 + \ldots + a_n x_n = k \tag{2.45}$$

uma vez que $mdc(a_1, \ldots, a_n) = 1$. Vamos dividir cada inteiro x_i, com $2 \leq i \leq n$, por a_1,

$$x_i = a_1 q_i + r_i, \text{ com } 0 \leq r_i \leq a_1 \tag{2.46}$$

e vamos substituir na equação 2.45, onde obtemos

$$k = a_1(x_1 + a_2 q_2 + \ldots + a_n q_n) + a_2 r_2 + \ldots + a_n r_n \tag{2.47}$$

Dessa forma, nos provamos que qualquer inteiro k pode ser escrito como

$$\sum_{i=1}^{n} j_i a_i \tag{2.48}$$

com $j_1 \in \mathbb{Z}$ e $0 \leq j_i \leq a_1 - 1$, para $2 \leq i \leq n$ e $j_i \in \mathbb{Z}$. Agora vamos definir o seguinte conjunto

$$S = \{k \mid k = \sum_{i=1}^{n} j_i a_i, j_1 < 0, 0 \leq j_i \leq a_1 - 1 \text{ para } i = 2, \ldots, n\} \tag{2.49}$$

Perceba que S é limitado superiormente e, de fato, seu maior elemento é

$$-a_1 + (a_1 - 1)(a_2 + \ldots + a_n) \tag{2.50}$$

Também sabemos que qualquer elemento em $\mathbb{Z}$ pode ser representado como combinação linear e assim qualquer inteiro em $\mathbb{Z} - \mathbb{S}$ pode ser representado tal que $j_1 \geq 0$. Ora, como o menor elemento em $\mathbb{Z} - \mathbb{S}$ é

$$-a_1 + (a_1 - 1)(a_2 + \ldots + a_n) + 1 = (a_1 - 1)(a_2 + \ldots + a_n - 1) \tag{2.51}$$

significa que qualquer inteiro $k \geq (a_1 - 1)(a_2 + \ldots + a_n - 1)$ pode ser escrito como combinação linear inteira não negativa de $a_1, a_2, \ldots, a_n$. ■

O próximo Teorema reduz o valor de k, mas ainda não é o menor, como mostraremos um exemplo mais a frente.

Teorema 2.4.3. *(Upper Bounds on Frobenius Coin Problem) Considere os inteiros $2 \leq a_1 < a_2 < \ldots < a_n$, com $n > 2$, tal que $mdc(a_1, a_2, \ldots, a_n) = 1$. Assim, qualquer $k \geq (a_1 - 1)(a_n - 1)$ pode ser obtido através de uma combinação linear inteira não negativa de $a_1, a_2, \ldots, a_n$, isto é, existem inteiros não negativos x_i, $1 \leq i \leq n$, tal que*

$$\sum_{i=1}^{n} x_i a_i = k \tag{2.52}$$

Demonstração Mostraremos por indução sobre n. Para $n = 2$, caímos no caso particular da Proposição 2.4.2. Para $n \geq 3$, vamos definir $d = mdc(a_1, a_3, \ldots, a_n)$ (sem incluir o a_2). Como $mdc(d, a_2) = 1$ então pelo Teorema 2.2.1 existem inteiros x e y tais que

$$a_2 x + dy = k \tag{2.53}$$

Note que podemos escolher uma solução $x = j_2$ tal que $0 \leq j_2 \leq d - 1$. Agora, utilizando o Teorema 2.3.1 sabemos que a equação

$$\frac{k - j_2 a_2}{d} = j_1 \frac{a_1}{d} + j_3 \frac{a_3}{d} + \ldots + j_n \frac{a_n}{d} \tag{2.54}$$

admite solução, pois $d \mid k - j_2 a_2$ e $d \mid a_i$, para $i = 1, 3, \ldots, n$, e

$$mdc\Big(\frac{a_1}{d}, \frac{a_3}{d}, \ldots, \frac{a_n}{d}\Big) = 1 \tag{2.55}$$

Cautelosamente, perceba que se

$$\frac{k - j_2 a_2}{d} \geq \Big(\frac{a_1}{d} - 1\Big)\Big(\frac{a_n}{d} - 1\Big) \tag{2.56}$$

utilizamos o critério de indução e descobrimos que há solução para a nossa equação no caso n. Ou seja, se

$$k \geq j_2 a_2 + \Big(\frac{a_1}{d} - 1\Big)(a_n - d), \text{ para } 0 \leq j_2 \leq d-1 \tag{2.57}$$

Basta mostrarmos que

$$(a_1 - 1)(a_n - 1) \geq j_2 a_2 + \Big(\frac{a_1}{d} - 1\Big)(a_k - d) \tag{2.58}$$

que é válida se, e somente se,

$$a_1 a_n - a_1 - a_n + 1 \geq j_2 a_2 + \frac{a_1 a_n}{d} - a_1 - a_n + d \tag{2.59}$$

melhor ainda,

$$\Leftrightarrow a_1 a_n \geq d(a_2 + 1) \tag{2.60}$$

que é verdade, pois $d \mid a_1$ e $a_n \geq a_2$. Assim, nossa prova por indução está completa. ■

2.5 Exercícios de Aprofundamento

Problema 2.5.1. *Determine todas as soluções da equação em inteiros positivos*

$$11x - 4y = 7 \tag{2.61}$$

Solução A equação pode ser reequacionada como

$$11x + 4(-y) = 7 \Rightarrow 11x + 4y' = 7 \tag{2.62}$$

Uma solução particular é dada por $(x_0, y_0') = (1, -1)$. As soluções são dadas por

$$x = 1 + 4t \quad \text{e} \quad y' = -1 - 11t \tag{2.63}$$

sendo t um número inteiro. Para x e y serem positivos, basta que $t \geq 0$. Portanto, $x = 1 + 4t$ e $y = 1 + 11t$.

Alternativamente, seguindo o algoritmo de Euclides, temos que

$$11 = 4 \cdot 2 + 3 \tag{2.64}$$

$$4 = 3 \cdot 1 + 1 \tag{2.65}$$

assim,

$$1 = 4 - 3 \cdot 1 = 4 - (11 - 4 \cdot 2) = 11 \cdot (-1) + 4 \cdot (3) \tag{2.66}$$

ou seja,

$$7 = 11 \cdot (-7) + 4 \cdot (21) \tag{2.67}$$

e a partir de agora seriam utilizados os passos já apresentados.

Problema 2.5.2. *Haroldo e Emerson desejam comprar livros da coleção do PROFMAT da SBM. Os alunos possuem notas de* $R\$2,00$ *e* $R\$5,00$*, além de possuírem moedas de* 10 *e* 25 *centavos. No total, perceberam que precisariam de* $R\$338,55$*. Determine a menor quantidade possível de cédulas de moedas utilizadas por esses alunos.*

Solução A ideia é utilizar a uma alta quantidade de cédulas de $R\$5,00$ e assim notar o que pode ser feito com o dinheiro restante. Vejamos

- $R\$335,00$ reais em 67 notas de $R\$5,00$ e daí nos resta pagar $R\$3,55$. Podemos utilizar uma cédula de $R\$2,00$, 5 moedas de 25 centavos e 3 moedas de 10 centavos.
- $R\$330,00$ reais em 66 notas de $R\$5,00$ e daí nos resta pagar $R\$8,55$. Podemos utilizar 4 notas de $R\$2,00$, 1 moeda de 25 centavos e 3 moedas de 10 centavos.

assim, o segundo caso utiliza uma quantidade menor de cédulas e moedas. Como mostrar que esse é o mínimo? Note que

- a quantidade de moedas de 25 e 10 centavos é sempre maior ou igual que 4.
- Vamos determinar a quantidade mínima de cédulas. Se

$$2x + 5y \leq 338 \tag{2.68}$$

então

$$\min\{x+y\} = \frac{1}{2}\min\{2x+2y\} = \frac{1}{2}\min\{[338-5y]+2y\} \tag{2.69}$$

ou seja,

$$\min\{x+y\} = \frac{1}{2}\min\{338-3y\} \tag{2.70}$$

que acontece quando y é máximo, ou seja, $5y = 335$ e assim $y = 67$. Mas esse caso já sabemos que não obtemos o mínimo, daí $y \leq 66$. Logo,

$$\min\{x+y\} = \frac{1}{2}(338 - 3\cdot 66) = 70 \tag{2.71}$$

Portanto, sempre são usadas uma quantidade maior ou igual que 74 cédulas e moedas.

Problema 2.5.3. *Uma determinada quantidade de bananas é dividida em*

31 *montes de igual número. Após serem retiradas* 17 *frutas, as restantes são guardadas em* 61 *caixas, cada uma com a mesma quantidade. Quantas bananas foram colocadas em cada caixa? Quantas bananas tinha cada monte?*

Solução Vamos montar as equações. Se cada monte possui a bananas, então há $31a$ bananas. Se cada caixa possui b bananas, então

$$31a - 17 = 61b \Rightarrow 31a - 61b = 17 \Rightarrow 31a + 61b' = 17 \tag{2.72}$$

e daí encontramos a solução particular $a_0 = 34$ e $b'_0 = -17$. Logo,

$$a = 34 + 61t \quad \text{e} \quad b' = -17 - 31t \tag{2.73}$$

ou seja $a = 34 + 61t$ e $b = 17 + 31t$, para $t \geq 0$, pois queremos as soluções em que a e b são positivos.

Problema 2.5.4. *De que maneiras podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?*

Solução Queremos resolver a equação

$$5a + 7b = 100 \tag{2.74}$$

onde a e b representam as quantidades de selos de cinco e sete reiais, respectivamente. Uma solução particular é dada por $a_0 = 20$ e $b_0 = 0$ assim as demais são

$$a = 20 + 7t \quad \text{e } b = -5t \tag{2.75}$$

dessa forma, como $0 \geq 5a \leq 100$ basta que

- $7t \geq -20$ e daí $t \geq -2$
- $35t \geq 0$ e assim $t \leq 0$

Logo $t = 0$, -1 e -2 e encontramos três soluções para a equação.

Problema 2.5.5. *Valdeire deseja fazer uma cesta para doar para crianças carentes em Marabá. Seu universo de material inclui papel higiênico, sabonete, pasta de dente e shampoo. Sabe-se que cada pacote de papel higiênico contém 8 unidades; cada pacote de sabonete contém 16 unidades; cada pacote de pasta de dente contém 12 unidades; e cada pacote de shampoo contém 4 unidades. De quantas maneiras distintas existem para montar quites com* 56 ***unidades****, que contenham pelo menos um pacote de cada produto?*

Solução Precisamos resolver a equação

$$8a + 16b + 12c + 4d = 56 \tag{2.76}$$

sendo a, b, c, d inteiros e maiores que zero. Como $mdc(4, 8, 12, 16) = 4$ e $4 \mid 56$ a equação possui solução. Vamos dividir em casos

- Se $b = 3$ então $8a+12c+4d = 8$ e assim não não solução pois $c \geq 1$.
- Se $b = 2$ então $8a + 12c + 4d = 24$ e assim ficamos com $c = 1$ ou $c = 2$. Esse último caso é um absurdo. Analisando $c = 1$ então

  $$8a + 4d = 12 \tag{2.77}$$

  e, portanto, $a = d = 1$ é a única **solução**.
- Se $b = 1$ então $8a + 12c + 4d = 40$ e assim ficamos com $c = 3$, 2 ou 1. Se $c = 3$ então

  $$8a + 12c + 4d \geq 8 + 36 + 4 = 48 \tag{2.78}$$

  que é um absurdo. Portanto $c = 2$ ou $c = 1$. Se $c = 2$ então

  $$8a + 4d = 16 \tag{2.79}$$

  e daí temos a **solução** $a = 1$ e $d = 2$. Se $c = 1$ ficamos com

  $$8a + 4d = 28 \tag{2.80}$$

  e daí temos as **soluções** $(a, d) = (1, 5), (2, 3), (4, 1)$.

Portanto temos 5 soluções.

Problema 2.5.6. *Dois fazendeiros acordam que cada porco custa* $R\$300,00$ *e que cada cabra custa* $R\$210,00$. *Quando algum dos fazendeiros recebe o dinheiro do outro, aquele paga o débito em porcos ou cabras, sendo a diferença também paga em porcos e cabras se necessário. For exemplo, um débito de* $R\$390,00$ *pode ser paga com dois porcos e a difereçca ser recebida uma cabra. Dentre os valores abaixo, qual é a menor quantidade positiva que pode ser cambiada dessa forma?*

(A) 5 (B) 10 (C) 30 (D) 90 (E) 210

Solução Note que queremos k tal que $300a + 210b = k$. Como $mdc(300, 210) = 30$ então $30 \mid k$. Sabemos que para $k = 30$ existe solução, basta tomar

$$300 \cdot (2) + 220 \cdot (-3) = -30 \tag{2.81}$$

CAPÍTULO 3

EQUAÇÕES DIOFANTINAS NÃO LINEARES

Esse capítulo será dedicado a Equações Diofantinas Não Lineares. No universo linear, as variáveis parecem se comportar de maneira mais regular, homogênea, ao contrário do que veremos a partir de agora. Não deixaremos de lado o fato de que nossas variáveis são inteiras. Esse tópico foi baseado nas referências [1] e [10], além de conter exercícios de [2], [4], [11].

3.1 Ternas Pitagóricas

3.1.1 Contexto Histórico

Nascido na ilha de Samos, em 570 a.C., o grande matemático e filósofo Pitágoras viveu até 497 ou 496 a.C. na rigião conhecida hoje como o Sul da Itália. a Figura 3.1 representa uma esculta desse brilhante matemático.

Naquela época, a busca pela ligação entre a geometria e a aritmética por Pitágoras e seus discípulos alavancaram extraordinários resultados na matemática, que até hoje são reconhecidos no mundo acadêmico.

Os Babilônicos elaboraram escrituras com números inteiros x, y e z tais que

$$x^2 + y^2 = z^2 \tag{3.1}$$

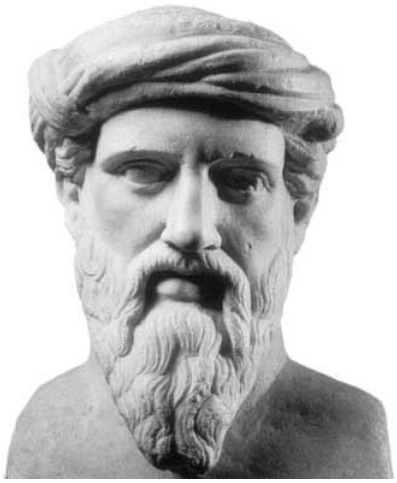

Figura 3.1: Escultura de Pitágoras

aproximadamente em 1700 a.C. e há comprovações por historiadores que essas equações matemáticas eram utilizadas no Egito Antigo. Talvez isso tenha intrigado os grandes pensadores da época a continuar os estudos e a se questionar por que não determinar todas as ternas de números inteiros que satisfazem a equação em 3.1.

Tentando alinhar a geometria à aritméticas, Pitágorias e seus discipulos estavam determinados a encontrar uma generalização e, assim, acharam um método de se determinar infinitas soluçoes para o sistema, a partir de um dado número, vejamos

$$x = 2n \quad y = n^2 - 1 \quad \text{e } z = n^2 + 1 \tag{3.2}$$

sendo n um número inteiro. Sabemos, hoje, que ainda faltava muito para Pitágoras chegar onde é a verdadeira solução para esse problemas, entretanto foi um grande avanço na matemática.

Por ser um problema que demandou tempo e alcançou grandes matemáticos, o filósofo Platão também deu sua contribuição através das triplas

$$x = 4n \quad y = 4n^2 - 1 \quad \text{e} \quad z = 4n^2 + 1 \tag{3.3}$$

Entretanto, não foi muito diferente dàquelas apresentadas pelo nosso glorioso Pitágoras. A Figura 3.2 representa uma escultura dessa tão renomado filósofo.

Toda esse mistério desvendou-se com o brilhante matemático Euclide, aproximadamente em 300 a.C., quando apresentou todas as ternas Pitagóricas

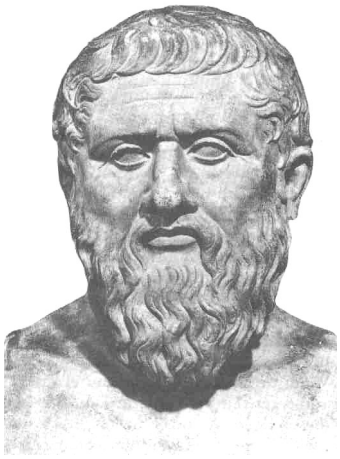

Figura 3.2: Escultura de Platão

em um dos seus famosos 13 livros. A Figura 3.3 representa uma foto de Euclides.

Figura 3.3: Escultura de Euclides

3.1.2 Resolução do Problema

Com grande motivação, vamos então apresentar todas as soluções da equação que atravessou fronteiras durante mais de 1000 anos a.C. e que é associado ao glorioso matemático Pitágoras.

Ternas pitatóricas e triângulos retângulos estão intrinsecamente relacionados, como já descoberto por Pitágoras. Mas esse filósofo queria determinar todas as triplas de inteiros que satisfaria essa equação. Por quê esse problema o levou a passar tanto tempo? Talvez a quantidade de soluções que não parasse de crescer.

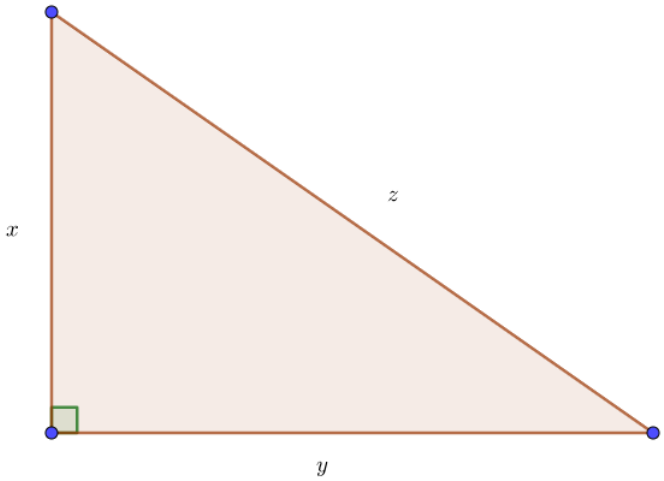

Figura 3.4: Triângulo retângulo com lados x, y e z

Definição 3.1.1. *Uma terna pitagórica é uma terna de números inteiros positivos* (x, y, z) *que obedecem a relação*

$$x^2 + y^2 = z^2 \tag{3.4}$$

Quando notamos uma terna pitagórica, como no caso dos triângulos retângulos: 3, 4 e 5, percebemos que qualquer múltiplo inteira dessa terna também é uma terna pitagórica, pois

$$(3k)^2 + (4k)^2 = (3^2 + 4^2)k^2 = 5^2k^2 \tag{3.5}$$

Percebe-se, também, que se escrevermos

$$x = r^2 - s^2 \quad y = 2rs \quad z = r^2 + s^2 \tag{3.6}$$

essa última terna também é pitagórica. Então surge o questionamento: existe uma fórmula para as terna Pitagóricas? A resposta é: Sim! Vamos encontrar uma fórmula para todas essas triplas de inteiros.

Teorema 3.1.2. (Terna Pitagórica) *Qualquer solução primitiva da equação*

$$x^2 + y^2 = z^2 \tag{3.7}$$

com y *par é dada por* $x = r^2 - s^2$, $y = 2rs$ *e* $z = r^2 + s^2$, *sendo* $mdc(m, n) = 1$ *e* $m > n$.

Demonstração Primeiramente, note que x e y não podem ser ambos ímpares, pois caso contrário,

$$x^2 + y^2 = (2x_0 + 1)^2 + (2y_0 + 1)^2 = 4(x_0^2 + y_0^2 + x_0 + y_0) + 2 \tag{3.8}$$

mas nenhum quadradro perfeito deixa resto 2 por 4 (veja Exercícios no Capítulo 2). Vamos demonstrar o seguinte Lemma que será muito útil em nossa demonstração.

Lemma 3.1.3. *Se a e b são inteiros positivos tais que $a \cdot b$ é quadrado perfeito, com $mdc(a,b) = 1$, então a e b são quadrado perfeitos.*

Demonstração Seja $p^{2\alpha}$ a maior potência de um primo em $a \cdot b$. Como $mdc(a,b) = 1$ então p *mida* ou $p \mid b$. Caso $p \mid a$ então $p^{2\alpha} \mid a$, uma vez que existe apenas em a o primo p. Fazemos isso para todos os primos que dividem $a \cdot b$.

Voltando ao problema, sabemos que $mdc(x,y) = mdc(x,z) = mdc(y,z) = 1$. Temos

$$\left(\frac{y}{2}\right)^2 = \frac{z-x}{2} \cdot \frac{z+x}{2} \tag{3.9}$$

Se

$$d = mdc\Big(\frac{z-x}{2}, \frac{z+x}{2}\Big)$$

então $d \mid z$ e $d \mid x$, ou seja, $d = 1$. Assim, nosso Lemma garante que existem r e s, com $mdc(r,s) = 1$, tal que

$$\frac{z-x}{2} = r^2 \quad e \quad \frac{z+x}{2} = s^2 \tag{3.10}$$

o que nos dá

$$x = s^2 - r^2, \quad y = 2rs, \quad z = r^2 + s^2 \tag{3.11}$$

Vejamos agora a Tabela **??** que apresenta vários valores para r e s.

3.1.3 Triângulos Pitagóricos de mesma Área

Nosso objetivo aqui é encontrar triângulos de retângulos de lados inteiros que apresentam diferentes hipotenusas e mesma áreas. Por exemplo, os triângulos de lados

$$(21, 20, 29) \quad \text{e } (35, 12, 37) \tag{3.12}$$

apresentam área 210. Perceba também que os triângulos de lados

$$(15, 112, 113) \quad , \quad (42, 40, 58) \quad \text{e} \quad (70, 24, 74) \tag{3.13}$$

(a) Valores iniciais para m e n

m	**n**	**x**	**y**	**z**	**Área**
2	1	3	4	5	6
3	2	5	12	13	30
4	1	15	8	17	60
4	3	7	24	25	84
5	2	21	20	29	210
5	4	9	40	41	180
6	1	35	12	37	210
6	5	11	60	61	330
7	2	45	28	53	630
7	4	33	56	65	924

(b) Valores maiores para m e n

s	**r**	**x**	**y**	**z**	**Área**
7	6	13	84	53	546
8	1	63	16	65	504
8	3	55	48	73	1320
8	5	39	80	89	1560
8	7	15	112	113	840
9	2	77	36	85	1386
9	4	65	72	97	2340
9	8	17	144	145	1224
10	1	99	20	101	990
10	3	91	60	109	2730

Tabela 3.1: Valores para formar ternas pitagóricas para m e n

também apresentam mesma área e dois deles não são primitivos, isto é, o *mdc* dos lados não é 1.

Vamos exibir o seguinte Teorema que nos garante a existência desses triângulos.

Teorema 3.1.4. *Para qualquer número natural n existem n triângulos Pitagóricos com diferentes hipotenusas e de mesma área.*

A demonstração desse Teorema é feita a partir do Lemma a seguir.

Lemma 3.1.5. *Se são dados n triângulos Pitagóricos com valores diferentes de hipotenusa e com mesma área, além de que existe pelo menos uma hipotenusa cujo valor é um número ímpar, então podemos construir $n+1$ triângulos Pitagóricos com valores diferentes de hipotenusa e com mesma área, além de que pelo menos um triângulo apresenta hipotenusa cujo valor é ímpar.*

Demonstração Suponha que cada um dos n triângulos retângulos tenham catetos a_i, b_i e hipotenusa c_i, para cada $i = 1, 2, \ldots, n$. Suponha também que $a_i \leq b_i$, $c_i \neq c_j$ e que c_1 seja ímpar.

A construção dos novos n triângulos é feita de seguinte forma: escolhemos o triângulo (a'_k, b'_k, c'_k) para ser semelhante ao triângulo (a_k, b_k, c_k), veja

$$a'_k = 2c_1(b_1^2 - a_1^2)a_k \quad \text{e } b'_k = 2c_1(b_1^2 - a_1^2)b_k \tag{3.14}$$

além de que

$$c'_k = 2c_1(b_1^2 - a_1^2)c_k \tag{3.15}$$

O $(n+1)$-ésimo triângulo é obtido da seguinte forma

$$a'_{n+1} = (b_1^2 - a_1^2)^2 \ , \ b'_{n+1} = 4a_1b_1c_1^2 \ , \ c'_{n+1} = 4a_1^2b_1^2 + c_1^4 \tag{3.16}$$

É fácil observar que

- Todos os triângulos são Pitagóricos;
- Todos os triângulos apresentam a mesma área;
- Todas as hipotenusas são distintas;
- c_{n+1} tem a mesma paridade que c_1 que é ímpar, enquanto as demais hipotenusas são pares.

sendo assim a demonstração do nosso Lemma está completa.

Seguimos um exemplo para $n = 1$. Começamos com

$$(3, 4, 5) \tag{3.17}$$

e, assim, aplicando o algoritmo, construimos os dois triângulos retângulos de lados

$$(210, 280, 350) \text{ e } (49, 1200, 1201) \tag{3.18}$$

3.2 $x^n + y^n = z^n$

Nessa seção mostraremos de onde essa magnífica equação surgiu e o que a levou tornar-se tão famosa nos dias atuais.

Figura 3.5: Pierre de Fermat

3.2.1 Contexto Histórico

Fermat

Pierre de Fermat estudava matemática por diversão, porque seguiu a carreira pública de juiz como principal função na França, onde nasceu. Também tinha uma enorme conhecimento em outras áreas, como filosofia e poesia.

Esse matemático tinha a fama de desafiar a comunidade acadêmica, uma vez que não publicava suas soluções nem mesmo as revelava quando solicitado. Sabe-se que grande parte de seu trabalho foi solicionado apenas 250 anos após a sua morte.

O Nascimento de um Enigma

Fermat adquiriu boa base do conhecimento aritmético matemático através do livro de Diofante, fazendo-o progredir na matemática bem como tornando-o conhecedor das ternas Pitagóricas e do magnífico Euclides.

Fermat era entusiasmado em escrever novos problemas e nesse contexto, por conhecer as equações de Pitágoras, criou a tão famosa equação de Fermat

$$x^n + y^n = z^n \tag{3.19}$$

Fermat dizia não existir solução e até tentou estudar a variante, para $n = 3$, porém o que se sabe é que esse matemático deixou uma frase às mergens de um livro onde afirmava: *"Eu tenho uma demonstração realmente maravilhosa para esta proposição, mas esta margem é muito estreita para*

conte-la"

Andrew Wiles

Esse matemático inglês sempre foi apaixonado por matemática, quando desde criança, em 1963, já se desafiava com problemas mais difíceis.

Sua história se cruza com a de Fermat quando ele conheceu a equação do Francês em um livro de enigmas e, a partir de então, ficou fascina por pelas ternas de números que obedeciam (ou não) a equação.

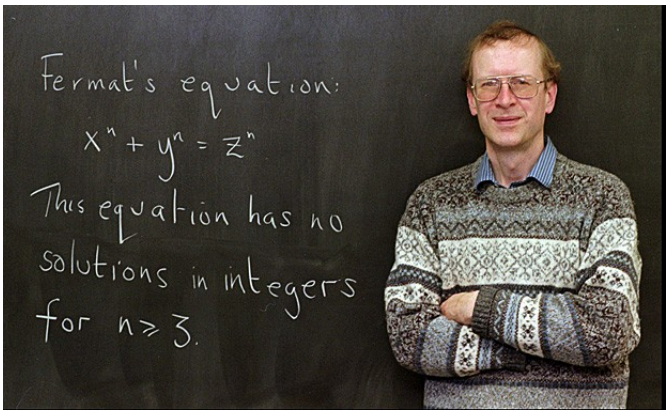

Figura 3.6: Andew Wiles

Pesquisadores que colaboraram para a Resolução do Último Teorema de Fermat

Por ser um problema muito intrigante, muitos matemáticos famosos tentaram esse problema e não conseguiram a sua total demonstração. Entretanto, sabe-se que alguns deles deram especiais contribuições, de grande valia para os congressos acadêmicos, e que repercutiram muito.

Euler, por exemplo, demonstrou por volta do ano 1730 que não existem soluções para $n = 3$. *Sophie Germain* trabalhou em cima de teoria que, logo em cima, outros matemáticos aplicaram e demonstraram que para $n = 5$ e $n = 7$ também não há soluções. *Taniyama* e *Shimura* apresentaram grandes avanços através das curvas elípticas, o que deu a Wiles todas as ferramentas para uma completa demonstração do teorema.

Resolução do Último Teorema de Fermat - Andrew Wiles

Em 1968, Andrew decidiu se isolar para tentar encontrar as soluções da

equação de Fermat. Ele manteve distante de congressos e outros tópicos, em busca apenas da solução do que tanto procurava. Sua esposa era a única pessoa a saber dos avanços nessa corrida.

Wiles tentava se basear em algo descoberto até o presente momento por Taniyama-Shimura. Depois de 7 anos e com ajuda de Katz, utilizando conceitos de curvas elípticas, Andrew finalmente consegue demonstrar o teorema.

Entretanto, Wiles é avisado por Katz, em segredo, sobre um erro em parte da demonstração, o que levou esse matemático demandar mais 1 ano e meio para corrigir e submeter a banca avaliadora.

Potanto, levaram-se oito anos para a completa demontração do último teorema de fermat pelo matemática inglês Andrew Wiles.

Conclusão

Para a comunidade acadêmica, Fermat foi um matemático soberbo, por não admitir a incapacidade de solucionar a equação proposta por ele mesmo.

Sabe-se que os mais brilhantes matemáticos já tentaram de alguma forma esse renomado teorema em alguma fase da sua vida e graças ao ilustre Andrew Wiles esse mistério foi desvendado, após um trabalho árduo em sua vida de completa dedicação à matemática.

Esse magnífico teorema é, sem dúvidas, o teorema mais conhecido no mundo da matemática desde que Fermat o lançou como desafio para a comunidade acadêmica.

3.2.2 Resolvendo casos Particulares

A equação $x^n + y^n = z^n$ trata-se do famoso último teorema de Fermat, conjecturado por Fermat, porém nunca se achou a publicação da demonstração feita por esse matemático, que afirmou que a equação não apresentava solução para n natural e $n \geq 3$.

Por volta de 1630, Fermat escreveu uma nota nas margens do livro Diophantus?s Arithmetica: "*Eu descobri uma solução relevante mas essa margem ém muito pequena para exibí-la*".

Sua demonstração foi publicada pelo Britânico Andrew Wiles que, em um primeiro momento apresentou uma demonstração com erros, mas anos

depois os corrigiu e acabou demonstrando.

Vamos demonstrar uma variante desse Teorema, isto é, que para todo n múltiplo de 4 o Último Teorema de Fermat não admite solução. Na verdade, faremos um outro teorema mais genérico.

Teorema 3.2.1. *A equação*

$$x^4 + y^4 = z^2 \tag{3.20}$$

não possui solução em inteiros positivos.

Demonstração Suponha, sem perda de generalidade, que $mdc(x, y) = 1$ e que z seja a **menor** solução encontrada. Dessa forma recaímos na equação Pitagórica

$$(x^2)^2 + (y^2)^2 = z^2 \tag{3.21}$$

que sabemos, de acordo com o Teorema 3.1.2, que existem inteiros m e n tais que

$$x^2 = m^2 - n^2 \quad \text{e} \quad y^2 = 2mn \tag{3.22}$$

com $mdc(m, n) = 1$ e m ou n par. Perceba que se m for par e n ímpar então x será ímpar, porém

$$4 \mid x^2 - 1 \quad \text{e} \quad 4 \mid m^2 - n^2 + 1 \tag{3.23}$$

pois todo quadrado de número ímpar deixa resto 1 por 4 e todo quadrado de número par deixa resto 0 por 4. Mas essa última equação nos implicaria em $4 \mid 2$, um absurdo!

Assim, m é ímpar e n é par, digamos $n = 2r$, com $mdc(m, r) = 1$. Substituindo, ficamos com

$$y^2 = 4mr \tag{3.24}$$

e assim, pelo fato de $mdc(m, r) = 1$, existem inteiros positivos a e b tais que $m = a^2$ e $r = b^2$.

Vamos olhar agora para a equação $x^2 + n^2 = m^2$. Sabemos que n é par e $mdc(m, n) = 1$, com isso podemos concluir que $mdc(x, n) = 1$. Daí temos uma solução primitiva da terna Pitagórica e, portanto,

$$m^2 = m_1^2 + n_1^2 \quad \text{e} \quad n^2 = 2m_1n_1 \tag{3.25}$$

sendo $mdc(m_1, n_1) = 1$. Ora, temos que

$$n^2 = 2b^2 \quad \text{e} \quad n^2 = 2m_1 n_1 \tag{3.26}$$

ou seja, existem inteiros positivos a_1 e b_1 tais que $m_1 = a_1^2$ e $n_1 = b_1^2$. Mas isso nos levaria a

$$m^2 = m_1^2 + n_1^2 = a_1^4 + b_1^4 \tag{3.27}$$

mas $z = m^2 + n^2 > m^2 \geq m$ e isso contradiz nossa hipótese de que z é o menor inteiro positivo que satisfaz nossa equação.

Uma outra variante do Teorema de Fermat é o caso $n = 3$, que pode ser encontrada em [1]. A demonstração envolve os conceitos da Lei da Reciprocidade Quadrática e é muito interessante pois é cheio de técnicas interessantes. A primeira pessoa a estudar e fazer essa variante do problema foi Leonard Euler.

Teorema 3.2.2. (Último Teorema de Fermat. $n = 3$) *Não existe solução para a equação*

$$x^3 + y^3 = z^3 \tag{3.28}$$

em inteiros positivos.

3.3 Aproximações Diofantinas

Antes de estudar as Equações de Pell, vamos estudar um pouco de análise e apresentar três Teoremas e três problemas muito interessantes, sendo dois problemas destaques da **International Mathematical Olympiad**.

Teorema 3.3.1. (Dirichlet) *Sendo ϵ um irracional qualquer, então existem infinitos racionais r, escrito como*

$$r = \frac{a}{b} \tag{3.29}$$

com $mdc(a, b) = 1$, tal que

$$\left| \frac{a}{b} - \epsilon \right| < \frac{1}{a^2} \tag{3.30}$$

Demonstração Esse é uma lemma muito interessante e que a demonstração pode ser simplesmente demonstrada pelo Princípio da Casa dos Pombos.

Seja n um número natural não nulo. Considere os n intervalos

$$\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right], \ldots, \left[\frac{n-1}{n}, 1\right] \tag{3.31}$$

Considere os n números $\{i\epsilon\} = i\epsilon - \lfloor i\epsilon \rfloor$, com $1 \leq i \leq n$. Pelo Princípio da Casa dos Pombos, existem dois inteiros r e s tais que

$$\{r\epsilon\} - \{s\epsilon\} \in \left[0, \frac{1}{n}\right) \tag{3.32}$$

ou seja,

$$|\epsilon(r-s) - (\lfloor r\epsilon \rfloor - \lfloor s\epsilon \rfloor)| < \frac{1}{n} \tag{3.33}$$

e, dessa forma,

$$\left|\epsilon - \frac{\lfloor r\epsilon \rfloor - \lfloor s\epsilon \rfloor}{r-s}\right| < \frac{1}{n(|r-s|)} < \frac{1}{(r-s)^2} \tag{3.34}$$

uma vez que $0 \leq r, s \leq n$. Denotamos $a = \lfloor r\epsilon \rfloor - \lfloor s\epsilon \rfloor$ e $b = r - s$. Caso $r = d \cdot a_1$ e $b = d \cdot b_1$, teremos

$$\left|\epsilon - \frac{da_1}{db_1}\right| < \frac{1}{(db_1)^2} < \frac{1}{(b_1)^2} \Rightarrow \left|\epsilon - \frac{a_1}{b_1}\right| < \frac{1}{b_1^2} \tag{3.35}$$

Perceba que conseguimos apenas um par de inteiros que satisfaça nosso lemma. Para garantir a existência de infinitos, tome n_2 natural tal que

$$\frac{1}{n_2} < \left|\epsilon - \frac{a_1}{b_1}\right| \tag{3.36}$$

Dessa forma, de modo análogo, conseguiremos inteiros a_2 e b_2 tais que

$$\left|\epsilon - \frac{a_2}{b_2}\right| < \frac{1}{n_2 b_2} < \frac{1}{n_2} \tag{3.37}$$

e assim garantimos que $(a_1, b_1) \neq (a_2, b_2)$

Exemplo *(Teste Brasil/Cone Sul)* Mostre que para quaisquer inteiros positivos a e b

$$|a\sqrt{2} - b| > \frac{1}{2a+b} \tag{3.38}$$

Solução: Ora, sabemos que $2a^2 - b^2$ nunca pode ser zero, uma vez $\sqrt{2}$ ser irracional. Dessa forma,

$$|2a^2 - b^2| \geq 1 \Rightarrow |a\sqrt{2} - b| \geq \frac{1}{a\sqrt{2} + b} > \frac{1}{2a+b} \tag{3.39}$$

Agora vamos a um problema que utiliza a ideia mais profunda de análise relacionado ao Teorema 3.3.1. É cosiderada uma questão dificílima pela escolha da sequência para obedecer o que se pede.

Exemplo *(IMO)* Uma sequência infinita $x_0, x_1, x_2, \ldots$ de números reais é dita limitada quando existe uma constante C tal que $|x_i| \leq C$ para todo $i \geq 0$. Dado um real $a > 1$, construa uma sequência infinita limitada $x_0, x_1, x_2, \ldots$ tal que

$$|x_i - x_j||i - j|^a \geq 1 \tag{3.40}$$

para todo i, j inteiros não negativos distintos.

Solução: Em um primeiro momento, esse problema não aparenta em nada com aproximações diofantinas. Mas e se escrevermos $x_i = k\{i\sqrt{2}\}$, pois

- x_i é limitado por k.
- De alguma forma, vamos tentar utilizar o teorema de Dirichlet.

Dessa forma,

$$x_i - x_j = k[(i-j)\sqrt{2} - (\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor)] \tag{3.41}$$

Vamos tentar mostrar que

$$|x_i - x_j||i - j| \geq 1 \tag{3.42}$$

ou seja, uma versão mais forte do problema. Olhando para o Exemplo anterior, sabemos que

$$|(i-j)\sqrt{2} - (\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor)| \geq \frac{1}{(i-j)\sqrt{2} + (\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor)} \tag{3.43}$$

supondo, sem perda de generalidade que $i > j$. Agora note que

$$\lfloor i\sqrt{2} \rfloor - \lfloor j\sqrt{2} \rfloor \leq i\sqrt{2} - j\sqrt{2} + 1 = \sqrt{2}(i-j) + 1 < 2(i-j) \tag{3.44}$$

Portanto,

$$|x_i - x_j||i - j| \geq k \times \frac{1}{(i-j)(2+\sqrt{2})} \times (i-j) = \frac{k}{2+\sqrt{2}} \tag{3.45}$$

Dessa forma, tome $k = 2 + \sqrt{2} + \epsilon$ e nosso problema acaba.

Esse Teorema é muito importante no mundo na análise e está intrinsicamente relacionado as Equações Diofantinas.

Teorema 3.3.2. (Lema de Kronecker) *Seja α um irracional. Então o conjunto*

$$M_\alpha = \{m + n\alpha \mid m, m \in \mathbb{Z}\} \tag{3.46}$$

é denso no conjunto dos números reais.

Demonstração Seja o número natural $q > 0$ e considere os $q + 1$ números

$$\{0\alpha\}, \{1\alpha\}, \{2\alpha\}, \ldots, \{q\alpha\} \tag{3.47}$$

e considere os q intervalos

$$I_j = \Big[\frac{j-1}{q}, \frac{j}{q}\Big), \text{ para } 1 \leq j \leq q \tag{3.48}$$

Assim, pelo Pricípio da Casa dos Pombos existem dois inteiros r e s tais que

$$\{r\alpha\} \text{ e } \{r\alpha\} \in I_j, \text{ para algum } j \tag{3.49}$$

vamos supor sem perda de generalidade que $r < r$, daí

$$|\{r\alpha\} - \{s\alpha\}| < \frac{1}{q} \Rightarrow |(r-s)\alpha - (\lfloor r\alpha \rfloor - \lfloor s\alpha \rfloor)| < \frac{1}{q} \tag{3.50}$$

Tome $k = r - s$ e $h = \lfloor r\alpha \rfloor - \lfloor s\alpha \rfloor$ pois assim temos que

$$|k\alpha - h| < \frac{1}{q} \tag{3.51}$$

Dessa forma, dado um intervalo $I = (A - \epsilon, A + \epsilon)$ basta tomar q tal que

$$\frac{1}{q} < 2\epsilon \tag{3.52}$$

pois teremos que

- $x_0 = k\alpha - h \in M_\alpha$ pois k, h são inteiros.
- $\{mx_0 \mid m \in \mathbb{Z}\} \cap I \neq \emptyset$ pois $|x_0| < 1/q < 2\epsilon$.

e assim nosso problema acaba, pois em qualquer intervalo real há um número da forma $m\alpha + n$.

■

Agora vamos mostrar um importante teorema a respeito de partições do conjunto dos números naturais e que envolve de certa forma um pouco de equações diofantinas

Teorema 3.3.3. (Beatty) *Sejam α e β irracionais positivos tais que*

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1 \tag{3.53}$$

Sejam também os conjuntos $A = \{\lfloor n\alpha \rfloor \mid n \in \mathbb{N}\}$ e $B = \{\lfloor n\beta \rfloor \mid n \in \mathbb{N}\}$. Assim A e B formam uma partição de $\mathbb{N}$, isto é,

$$A \cup B = \mathbb{N} \quad e \quad A \cap B = \emptyset \tag{3.54}$$

Demonstração Primeiramente vamos mostrar que $A \cup B = \mathbb{N}$. Por absurdo, suponha que não seja verdade, isto é, que existe m natural tal que $m \notin A \cup B$. Dessa forma, existirão inteiros n_1 e n_2 tais que

$$\lfloor n_1\alpha \rfloor < m < \lfloor (n_1+1)\alpha \rfloor \text{ e } \lfloor n_2\beta \rfloor < m < \lfloor (n_2+1)\beta \rfloor \tag{3.55}$$

Dessa forma, utilizando também o fato que α é irracional, temos que $n_1\alpha < m$ e $(m+1) < (n_1+1)\alpha$, ou seja,

$$\frac{n_1}{m} < \frac{1}{\alpha} < \frac{n_1+1}{m+1} \tag{3.56}$$

analogamente,

$$\frac{n_2}{m} < \frac{1}{\alpha} < \frac{n_2+1}{m+1} \tag{3.57}$$

e somando essas duas últimas desigualdades membro a membro, ficamos com

$$\frac{n_1+n_2}{m} < \frac{1}{\alpha} + \frac{1}{\beta} < \frac{n_1+n_2+2}{m+1} \tag{3.58}$$

assim teremos que

- $n_1 + n_2 < m$;
- $m < n_1 + n_2 + 1$;

que é um absurdo, pois não existe número natural entre dois números consecutivos.

Agora vamos supor que $A \cap B = \emptyset$. Por absurdo, suponha que exista um número, m, que pertença a ambos os conjuntos. Assim $\lfloor n_1\alpha \rfloor = m = \lfloor n_2\beta \rfloor$, ou seja,

$$m < n_1\alpha < m+1 \quad \text{e} \quad m < n_2\beta < m+1 \tag{3.59}$$

assim,

$$\frac{n_1}{m+1} < \frac{1}{\alpha} < \frac{n_1}{m} \quad \text{e} \quad \frac{n_2}{m+1} < \frac{1}{\beta} < \frac{n_2}{m} \tag{3.60}$$

somando membro a membro essas duas últimas desigualdades,

$$\frac{n_1+n_2}{m+1} < 1 < \frac{n_1+n_2}{m} \tag{3.61}$$

ou seja, $n_1 + n_2 - 1 < m < n_1 + n_2$ que é um absurdo conforme vimos.

■

3.4 Equações de Pell

3.4.1 Contexto Histórico

A equação $x^2 - dy^2 = 1$ foi atribuída, erroneamente, por Euler a John Pell, pois não há evidências de estudo dessa equação por aquele matemático.

Euler foi o primeiro a desvendar as primeiras propriedades das soluções não triviais dessa tão importante equação.

Voltando um pouco no tempo, *Theon de Smyrna*, matemático Grego, foi um dos primeiros a investigar aproximações racionais de $\sqrt{2}$ e através de soluções do tipo $x^2-2y^2 = 1$. Em seguida, surgiu o problema de Arquimedes, que buscava uma solução para a aproximação racional de $\sqrt{d}$. Sabe-se que sendo $x^2 - dy^2 = 1$ então $x^2/y^2 = d + 1/y^2$ e assim para y grande o par de solução da equação representa uma boa escolha para a aproximação.

Diophantus apresentou uma soluçao para a equação $x^2 - dy^2 = 1$ em seu livro *Arithmetica*, com a hipótese $d = m^2 + 1$, pois assim

$$x = 2m^2 + 1 \quad \text{e} \quad y = 2m \tag{3.62}$$

Fermat propôs, em 1657, que a equação $x^2-dy^2 = 1$ apresentava infinitas soluções se d é livre de quadrados, entretanto não havia demonstração.

Finalmente, em 1766, Lagrange demonstrou que a equação $x^2 = dy^2 + 1$ possui infinitas soluções, sendo d livre de quadrados.

3.4.2 Resolução da Equação

Dizemos que um inteiro é livre de quadrados quando todas as potências de seus divisores primos são exatamente 1. Por exemplo,

$$6, 22, 110 \text{ e } 42$$

são números livre de quadrados, enquanto

$$12, 16, 18 \text{ e } 75$$

não são números livres de quadrados.

Definição 3.4.1. *A equação de Pell é a equação definida por*

$$x^2 - Dy^2 = m \tag{3.63}$$

onde D é um inteiro positivo livre de quadrados e m um número inteiro.

Nosso objetivo é demonstrar e encontrar todas as soluções para a equação

$$x^2 - Dy^2 = 1 \tag{3.64}$$

sendo D livre de quadrados. A demonstração requer uma série de resultados premilinares. Sendo assim, mostraremos esses Lemmas para nos ajudar no cálculo de todas as soluções.

Lemma 3.4.2. (Existência de m) *Seja d um inteiro positivo livre de quadrados. Assim, existe um inteiro m para o qual a equação*

$$x^2 - dy^2 = m \tag{3.65}$$

admite infinitas soluções inteiras.

Demonstração Por hipótese, sabemos que $\sqrt{d}$ é irracional, assim de acordo com o Lemma 3.3.1, existem infinitos pares (a, b) de inteiros com $mdc(a, b) = 1$ tais que

$$\left|\frac{a}{b} - \sqrt{d}\right| < \frac{1}{b^2} \tag{3.66}$$

assim, existirão infinitos inteiros a e b tais que

$$|a^2 - db^2| = |a - b\sqrt{d}||a + b\sqrt{d}| < \frac{1}{b}(|a - b\sqrt{d}| + 2b\sqrt{d}) \tag{3.67}$$

isto é,

$$|a^2 - db^2| < \frac{1}{b}\Big(\frac{1}{b} + 2b\sqrt{d}\Big) < 2\sqrt{d} + 1 \tag{3.68}$$

Daí, pelo Princípio da Casa dos Pombos, algum valor m entre $-(2\sqrt{d}+1)$ e $(2\sqrt{d}+1)$ se repete um número infinito de vezes. Isso é o mesmo que dizer que a equação

$$x^2 - dy^2 = m \tag{3.69}$$

tem infinitas soluções para um determinado valor de m ■

Agora vamos ao nosso grande Teorema que, além de mostrar que para $m = 1$ a equação sempre tem solução, encontra todas as soluções a partir de uma solução inicial. Os Lemmas recentemente visto serão de suma importância para a demonstração de nosso teorema.

Teorema 3.4.3. *(Equação de Pell) Seja d um inteiro positivo livre de quadrados. Então a equação*

$$x^2 - dy^2 = 1 \tag{3.70}$$

possui infinitas solução e todas as soluções podem ser escritas a partir de uma soluçao inicial como

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \tag{3.71}$$

sendo n um número natural não nulo.

Demonstração Primeiramente, suponha que a equação $x^2 - dy^2 = 1$ possua solução em inteiros positivos. Vamos escolher a solução $\alpha = x_1 + y_1\sqrt{d}$ tal que α seja mínimo, com x e y positivos. Ora, escreva $(x_1 + y_1\sqrt{d})^n$ da seguinte forma

$$(x_1 + y_1\sqrt{d})^n = x_n + y_n\sqrt{d} \tag{3.72}$$

É fácil notar que

$$(x_1 - y_1\sqrt{d})^n = x_n - y_n\sqrt{d} \tag{3.73}$$

Portanto,

$$1 = (x_1^2 - y_1^2\sqrt{d})^n = (x_1 - y_1\sqrt{d})^n(x_1 + y_1\sqrt{d})^n \tag{3.74}$$

ou seja,

$$1 = (x_n - y_n\sqrt{d})(x_n + y_n\sqrt{d}) = (x_n^2 - y_n^2 d) \tag{3.75}$$

nos garantindo que (x_n, y_n) é outra solução.

Agora vamos mostrar que qualquer solução pode ser escrita como uma potência de α. Suponha o contrário, isto é, que existe n tal que

$$\alpha^n < x + y\sqrt{d} < \alpha^{n+1} \tag{3.76}$$

Dessa forma,

$$1 < \alpha^{-n}(x + y\sqrt{d}) < \alpha \tag{3.77}$$

Perceba que

$$\alpha^{-n} = (x_1 + y_1\sqrt{d})^{-n} = (x_n + y_n\sqrt{d})^{-1} = (x_n - y_n\sqrt{d}) \tag{3.78}$$

assim,

$$\alpha^{-n}(x + y\sqrt{d}) = \underbrace{(x_n x - y_n y d)}_{R} + \underbrace{(x_n y - y_n x)}_{S}\sqrt{d} \tag{3.79}$$

fazendo com que (R, S) também seja uma solução da equação de Pell, veja

$$R^2 - S^2 d = x_n^2(x^2 - dy^2) + y_n^2(y^2 d^2 - dx^2) = x_n^2 - dy_n^2 = 1 \tag{3.80}$$

Descobrimos uma solução $(R, S) = \alpha(x+y\sqrt{d})$ menor que α. Para chegarmos a um absurdo, devemos mostrar ainda que tanto R quanto S são positivos. Sabemos que

$$R + S\sqrt{d} = 1 > 0 \quad e \quad R^2 - S^2 d = 1 \tag{3.81}$$

assim, $R - S\sqrt{d} > 0$, ou melhor, $2R > 0$ e implica que $R > 0$. Como

$$R + S\sqrt{d} > 1 \Rightarrow R - S\sqrt{d} = \frac{1}{R + S\sqrt{d}} < 1 \tag{3.82}$$

com isso $S\sqrt{d} > R - 1 > 0$, ou seja, $S > 0$. Daí chegamos a uma contradição pois encontramos uma solução menor que α. A conclusão é que todas as solução são potências de α.

Pronto, para acabar com a demonstração do Teorema, basta provarmos que $m = 1$ tem solução. O Lemma 3.4.2 nos garante que $x^2 - y2d = m$ admite uma inifidade de soluções. Vamos escolher duas soluções (a_1, b_1) e (a_2, b_2), com $|a_1| \neq |a_2|$, tais que

$$m \mid a_1 - a_2 \quad \text{e} \quad m \mid b_1 - b_2 \tag{3.83}$$

Agora note que

$$(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = (a_1 a_2 - d b_1 b_2) + (a_2 b_1 - b_2 a_1)\sqrt{d} \tag{3.84}$$

e que

$$(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1a_2 - db_1b_2) - (a_2b_1 - b_2a_1)\sqrt{d} \tag{3.85}$$

utilizando os conceitos de divisibilidade, temos que

$$m \mid (a_1a_2 - db_1b_2) \quad \text{e} \quad m \mid a_2b_1 - b_2a_1 \tag{3.86}$$

Portanto, se

$$(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = m(u + v\sqrt{d}) \tag{3.87}$$

$$(a_1 - b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = m(u - v\sqrt{d}) \tag{3.88}$$

logo,

$$(a_1^2 - b_1^2d)(a_2^2 - b_2^2d) = m^2(u^2 - v^2d) \tag{3.89}$$

e assim,

$$u^2 - v^2d = 1 \tag{3.90}$$

Para acabar, basta provarmos que u e v são não nulos. Caso $u = 0$ então $-v^2d = 1$ que é absurdo. Caso $v = 0$ então $(a_1 + b_1\sqrt{d})(a_2 - b_2\sqrt{d}) = \pm m$ o que nos dá

$$a_1 + b_1\sqrt{d} = \pm(a_2 + b_2\sqrt{d}) \Rightarrow |a_1| = |a_2| \tag{3.91}$$

que também é um absurdo.

■

Agora vamos aplicar esses conhecimentos em alguns exercícios.

Exemplo Determine todas as soluções inteiras positivas da equação

$$x^2 - 3y^2 = 1 \tag{3.92}$$

Solução: O Teorema 3.4.3 nos garante que todas as soluções positivas são da forma $(x_0 + y_0\sqrt{3})^n$, sendo n um natural não nulo e (x_0, y_0) a solução primitiva. Ora, sabemos que

$$2^2 - 3.(1)^2 = 1 \tag{3.93}$$

além de que $(1, 1)$ e $(1, 2)$ não são soluções. Assim $(x_0, y_0) = (2, 1)$

Exemplo Determine todas as soluções positivas da equação $x^2 - 2y^2 = 1$.

Solução: É fácil notar que a solução mínima é $x_0 = 3$ e $y_0 = 2$, pois nenhum par menor que esse é solução da equação. Portanto, todas as soluções são dadas por

$$x_n + y_n\sqrt{2} = (3 + \sqrt{2})^n \tag{3.94}$$

Exemplo Seja F_n e L_n as sequências de Fibonacci e Luccas, respectivamente, definidas por

$$F_{n+2} = F_{n+1} + F_n \quad , \forall n \in \mathbb{Z} \quad , F_1 = F_2 = 1 \tag{3.95}$$

$$L_{n+2} = L_{n+1} + L_n \quad , \forall n \in \mathbb{Z} \quad , L_1 = 1, L_2 = 2 \tag{3.96}$$

Mostre que a equação $5a^2 - b^2 = 4$ possui a solução (a, b) se, e somente se, existe existe n tal que $(a, b) = (F_{2n-1}, L_{2n-1})$.

Solução: Sendo α e β tais que

$$\alpha + \beta = -1 \quad \text{e} \quad \alpha\beta = 1 \tag{3.97}$$

então sabemos que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{e} \quad L_n = \alpha^n + \beta^n \tag{3.98}$$

Dessa forma, é fácil observar que o par (F_{2n-1}, L_{2n-1}) é solução da equação de Pell.

Suponha agora que existam soluções que não sejam da forma (F_{2n-1}, L_{2n-1}). Defina assim o conjunto $S = \{(x, y); x = F_{2n-1}, y = L_{2n-1}\}$. Das soluções que não estão em S, escolha (p, q) tal que p seja mínimo. Note que p e q tem a mesma paridade. Veja que se $3p \leq q$ então

$$9p^2 \leq q^2 = 5p^2 - 4 \Rightarrow 4p^2 \leq -1 \tag{3.99}$$

que é um absurdo. Analogamente temos que $3q - 5p > 0$. Vamos olhar para o par

$$\left(\frac{3p - q}{2}, \frac{3q - 5p}{2}\right) \tag{3.100}$$

Note que

$$5\Big(\frac{3p-q}{2}\Big)^2 - \Big(\frac{3q-5p}{2}\Big)^2 = \frac{20p^2-5q^2}{4} = 4 \tag{3.101}$$

perceba também que

$$\frac{3p-q}{2} + \frac{3q-5p}{2} > 0 \Rightarrow q > p \tag{3.102}$$

ou seja,

$$\frac{3p-q}{2} < p \Leftrightarrow p < q \tag{3.103}$$

que é verdade. Dessa forma, encontramos uma solução menor que (p, q) e assim, essa solução deve pertencer ao conjunto S. Logo,

$$\frac{3p-q}{2} = F_{2n-1} \quad \text{e} \quad \frac{3q-5p}{2} = L_{2n-1} \tag{3.104}$$

ou seja, $p = F_{2n+1}$ e $q = L_{2n+1}$ e assim $(p, q) \in S$, um absurdo. Portanto todas as soluções devem estar em S.

3.4.3 A equação $x^2 - dy^2 = -1$

Nessa seção, procuramos por inteiros positivos (x_0, y_0) e $m = -1$. De imediato, adianto que nem sempre haverá solução. Estudaremos, então os casos em que essa solução não admite solução.

Proposição 3.4.4. *Se existir um primo da forma $4k+3$ ou se $4 \mid d$ então a equação $x^2 - dy^2 = -1$ não possui solução.*

Demonstração Se $p \mid d$ e p for da forma $4k+3$ então

$$x^2 \equiv -1 \pmod{p} \Rightarrow x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p} \tag{3.105}$$

mas sabemos que $(p-1)/2$ é ímpar o pequeno Teorema de Fermat nos afirma que $x^{p-1} \equiv 1 \pmod{p}$, para qualquer x inteiro tal que $p \nmid x$. Daí, teríamos que

$$1 \equiv -1 \pmod{p} \Rightarrow p = 2 \tag{3.106}$$

um absurdo.

Caso $4 \mid d$ e como $d \mid x^2 + 1$ então $4 \mid x^2 + 1$ que também não é possível de acordo com o que vimos no capítulo 2.

■

Vamos determinar as soluções positivas da equação $x^2 - dy^2 = -1$. Da mesma forma como antes, vamos definir a solução primitiva (x_0, y_0) aquela que minima $x_0 + y_0\sqrt{d}$.

Lemma 3.4.5. (Solução Inicial) *Seja* $(x_0 + y_0\sqrt{d})$ *a solução primitiva de* $x^2 - yd^2 = -1$. *Então* $u + v\sqrt{d} = (x_0 + y_0\sqrt{d})^2$ *é a solução primitiva de* $x^2 - yd^2 = 1$.

Demonstração Primeiramente vamos demonstrar que $u + v\sqrt{d}$ é solução para a equação que desejamos. Temos

$$u = x_0^2 + dy_0^2 \quad \text{e} \quad v = 2x_0y_0 \tag{3.107}$$

Logo,

$$u^2 - dv^2 = x_0^4 - 2dx_0^2y_0^2 + d^2y_0^4 = (-1)^2 = 1 \tag{3.108}$$

Seja agora $x_1 + y_1\sqrt{d}$ a solução primitiva de $x^2 + dy^2 = 1$. Já vimos que toda solução da Equação de Pell, para $m = 1$, é uma potência de $(x_1+y_1\sqrt{d})$, assim,

$$(x_0 + y_0\sqrt{d})^2 = u + v\sqrt{d} = (x_1 + y_1\sqrt{d})^n \tag{3.109}$$

Vamos dividir em dois casos

- Se n é par. Daí $x_0 + y_0\sqrt{d} = (x_1 + y_1\sqrt{d})^{n'}$, mas isso implicaria em dizer que (x_0, y_0) seria solução da equação de Pell para $m = 1$, uma vez que é uma potência de primitiva, que é um absurdo, pois definimos (x_0, y_0) como solução da equação de Pell para $m = -1$.

- Se n é ímpar. Daí

$$x_0 + y_0\sqrt{d} = (x_1 + y_1\sqrt{d})^{n/2} < (x_1 + y_1\sqrt{d})^{n-1} \tag{3.110}$$

  Defina agora o número $r + s\sqrt{d} = (x_1 + y_1\sqrt{d})^{n-1}(-x_0 + y_0\sqrt{d})$. É fácil notar que (r, s) é uma solução da equação de Pell para $m = -1$, veja

$$r = -x_{n-1}x_0 + dy_{n-1}y_0 \quad \text{e} \quad s = x_{n-1}y_0 - x_0y_{n-1} \tag{3.111}$$

  e daí,

$$r^2 - ds^2 = x_{n-1}^2(x_0^2 - dy_0^2) + dy_{n-1}^2(dy_0^2 - x_0^2) = -x_{n-1}^2 + dy_{n-1}^2 = -1 \tag{3.112}$$

Agora, perceba que $r + s\sqrt{d} > 1$ é verdade se, e somente se,

$$(x_1 + y_1\sqrt{d})^{n-1} > x_0 + y_0\sqrt{d} \tag{3.113}$$

que é verdade. Com isso obtermos $0 > r - s\sqrt{d} > -1$ e, portanto,

$$2r = r + s\sqrt{d} + r - s\sqrt{d} > 0 \tag{3.114}$$

e $s\sqrt{d} > r > 0$ o que implica em $s > 0$. Para acabar, note que a Equação 3.109 nos dá

$$x_0 + y_0\sqrt{d} = (x_1 + y_1\sqrt{d})^n(-x_0 + y_0\sqrt{d}) > r + s\sqrt{d} \tag{3.115}$$

sendo essa última desigualdade verdade se, e somente se,

$$x_1 + y_1\sqrt{d} > 1 \tag{3.116}$$

sendo verdade. Mas dessa forma, (r, s) seria uma solução inteira positiva menor que (x_0, y_0) que é um absurdo.

Por fim, vamos descobrir todas as solução da Equação de Pell para $m = -1$, caso existe a solução primitiva.

Teorema 3.4.6. $(m = -1)$ *Seja* (x_0, y_0) *a solução primitiva da equação* $x^2 - dy^2 = -1$. *Então todas as soluções positivas dessa equação são da forma*

$$x_{2k+1} + y_{2k+1}\sqrt{d} = (x_0 + y_0\sqrt{d})^{2k+1}, \text{ para } k \in \mathbb{N} \tag{3.117}$$

Demonstração Note que $x_{2k+1} + y_{2k+1}\sqrt{d}$ são soluções da Equação de Pell para $m = -1$, pois

$$\underbrace{(x_0 + y_0\sqrt{d})^{2k}}_{\text{solução para } m=1} \quad \times \quad \underbrace{(x_0 + y_0\sqrt{d})}_{\text{solução para } m=-1} \tag{3.118}$$

e já vimos que esse último produto resulta numa solução da Equação de Pell para $m = -1$.

Suponhamos, portanto, que $u + v\sqrt{d}$ seja uma solução tal que

$$(x_0 + y_0\sqrt{d})^{2k-1} < u + v\sqrt{d} < (x_0 + y_0\sqrt{d})^{2k+1} \tag{3.119}$$

e assim, elevando ao quadrado

$$(x_0 + y_0\sqrt{d})^{4k-2} < (u + v\sqrt{d})^2 < (x_0 + y_0\sqrt{d})^{4k+2} \tag{3.120}$$

Já sabemos que $(u + v\sqrt{d})^2$ é solução da Equação $x^2 - yd^2 = 1$ e como está entre duas soluções, a única possibilidade é de que

$$(u + v\sqrt{d})^2 = (x_0 + y_0\sqrt{d})^{4k} \tag{3.121}$$

mas isso implicaria $u + v\sqrt{d} = (x_0 + y_0\sqrt{d})^{2k}$, ou seja, (u, v) seria solução da Equação de Pell para $m = 1$, uma contradição.

Vejamos agora alguns exercícios que seriam facilmente resolvidos utilizando as Equações de Pell.

Exemplo *(Cone Sul/94)* Determinar infinitas ternas x, y, z de inteiros positivos que sejam soluções da equação $x^2 + y^2 = 2z^2$, tais que o máximo divisor comum de x, y, z seja 1.

Solução: Vamos tomar $y = 1$ e assim já garantimos que $mdc(x, y, z) = 1$. Substituindo na equação, ficamos com

$$x^2 - 2z^2 = -1 \tag{3.122}$$

Daí, basta encontrarmos uma solução inicial (x_0, y_0) que o Teorema 3.4.6 nos garante infinitas soluções a partir de

$$x_{2k+1} + y_{2k+1} = (x_0 + y_0\sqrt{d})^{2k+1} \tag{3.123}$$

para todo k natural. Sendo assim, tome $(x_0, y_0) = (1, 1)$ que é a solução primitiva.

3.5 Método da descida de Fermat

Fermat foi um dos primeiros a descrever esse método de resolução que é muito eficaz para demonstrar que determinadas equação não possui solução no universo em que se está sendo analisado. Vamos a alguns exemplos para a melhor compreensão dos resultados.

Exemplo Determine todos os inteiros não negativos que satisfazem a equação

$$x^3 + 2y^3 = 4z^3 \tag{3.124}$$

Solução. Temos a solução $(x, y, z) = (0, 0, 0)$. Suponha então a solução mínima (x_0, y_0, z_0) em inteiros não negativos. Temos que $2 \mid x_0$, assim defina $x_0 = 2x_1$, com $x_1 \in \mathbb{N}$. Substituindo na equação ficamos com

$$8x_1^3 + 2y_0^3 = 4z_0^3 \Rightarrow 4x_1^3 + y_0^3 = 2z_0^3 \tag{3.125}$$

e agora temos que $2 \mid y_0$, ou seja, $y_0 = 2y_1$, com $y_1 \in \mathbb{N}$, daí

$$4x_1^3 + 8y_1^3 = 2z_0^3 \Rightarrow 2x_1^3 + 4y_1^3 = z_0^3 \tag{3.126}$$

agora $2 \mid z_0$ e assim $z_0 = 2z_1$. Substituindo,

$$2x_1^3 + 4y_1^3 = 8z_1^3 \Rightarrow x_1^3 + 2y_1^3 = 4z_1^3 \tag{3.127}$$

ou seja, encontramos uma solução (x_1, y_1, z_1) menor que nossa inicial. Isso contraria nossa hipótese. Portanto não existe nenhuma solução diferente da trivial.

Exemplo Determine todas as solução da equação

$$a^2 + b^2 + c^2 + d^2 = 2abcd \tag{3.128}$$

no conjunto dos inteiros positivos.

Solução. Suponha a solução (x, y, z, w) mínima em inteiros positivos. Vamos analisar essa equação módulo 4. Como a soma $x^2 + y^2 + z^2 + w^2$ é par, temos as possibilidade quanto a paridade de cada número x, y, z e w

- Todos os números serem ímpares. Assim $2xyzw \equiv 0 \pmod 4$, enquanto

  $$x^2 + y^2 + z^2 + w^2 \equiv 0 + 0 + 1 + 1 \equiv 2 \pmod 4 \tag{3.129}$$

  assim esse caso não convém.

- dois números ímpares e dois números pares. Assim $2xyzw \equiv 0 \pmod 4$ e

  $$x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod 4 \tag{3.130}$$

Logo só nos resta a possibilidade em que $x = 2x'$, $y = 2y'$, $z = 2z'$, $w = 2w'$ com x', y', z', $w' \in \mathbb{N}$. Substituindo,

$$4(x'^2 + y'^2 + z'^2 + w'^2) = 32x'y'z'w' \Rightarrow x'^2 + y'^2 + z'^2 + w'^2 = 8x'y'z'w' \tag{3.131}$$

analogamente encontramos que $2 \mid x'$, $2 \mid y'$, $2 \mid z'$, $2 \mid w'$. Portanto, para todo inteiro positivo n, os números $x/2^n$, $y/2^n$, $z/2^n$ e $w/2^n$ devem ser inteiros, o que é um absurdo.

Apresentaremos esse magnífico problema da International Mathematical Olympiada, do ano de 1981, que além de utilizar o métoda da descida de Fermat, era preciso fazer o método inverso para se determinar todas as soluções do problema.

Exemplo *(IMO)* Encontrar todas as soluções inteiras positivas da equação

$$m^2 - mn - n^2 = \pm 1 \tag{3.132}$$

Solução. Perceba que $m = n = 1$ é uma solução do nosso problema. Veja que

$$m^2 = n^2 + mn \pm 1 \geq n^2 \Rightarrow m \geq n \tag{3.133}$$

Vamos demonstrar que se (m, n) é uma solução, então $(n, m-n)$ também é uma solução.

$$n^2 - n(m-n) - (m-n)^2 = -(n^2 + mn - m^2) = \pm 1 \tag{3.134}$$

dessa forma, qualquer solução, através desse procedimento chega na solução $(1, 1)$. Fazendo o processo inverso, encontramos todas as soluções

$$(1,1), (2,1), (3,2), \ldots, (F_n, F_{n-1}), \ldots \tag{3.135}$$

Exemplo *(USAMO)* Encontre todas as soluções em inteiros positivos da equação

$$x^2 + y^2 + z^2 = x^2y^2 \tag{3.136}$$

Solução. Vamos analisar a equação módulo 4. Primeiro suponha que a equação tenha uma solução mínima (a, b, c)

- Se a e b forem ímpares então c^2 deverá ser congruene a $1 - 2 \equiv 3 \pmod 4$, um absurdo.
- Se a ímpar e b par então c^2 deverá ser congruente a $0 - 1 \equiv 3 \pmod 4$, um absurdo.

Assim provamos que $a = 2a'$, $b = 2b'$ e $c = 2c'$. Substituindo na equação, ficamos com

$$a'^2 + b'^2 + c'^2 = 4a'^2b'^2 \tag{3.137}$$

analogamente, prova-se que a', b' e c' são pares e assim recairemos na equação

$$a''^2 + b''^2 + c''2 = 16a''^2b''2 \tag{3.138}$$

Fazendo novamente os passos os números $a/2^n$, $b/2^n$ e $c/2^n$ devem ser inteiros para todo n, o que é um absurdo.

3.6 Técnicas de Congruência

Nem sempre as Equações Diofantinas não Lineares apresentam soluções. Sendo assim, é importante buscar por técnicas que nos permita encontrar alguma propriedade inválida a respeito da teoria dos números, implicitamente no problema.

Por exemplo, suponha que queiramos determinar todos os inteiros x tais que exista um inteiro **par** y tal que

$$x^2 + 7y^3 = 2018 \tag{3.139}$$

Ora, sabemos que $8 \mid y$ e assim deveríamos ter que $8 \mid x^2 - 2018$ ou melhor $8 \mid x^2 - 2$, já que $2016 = 8 \times 252$. Mas vimos no Capítulo 1 que os restos de x^2 por 8 são apenas 0, 1 e 4. Dessa forma, esse problema nunca vai apresentar solução.

Agora apresentaremos uma série de equações e as técnicas envolvidas para se verificar quando uma equação terá solução. Digamos que esse é um dos primeiros passos antes de se buscar as soluções.

Exemplo Mostre que a equação

$$x^2 - 7y = 10 \tag{3.140}$$

não possui solução em $\mathbb{Z}$.

Solução. Para que a equação tenha solução, é necessário que

$$x^2 \equiv 10 \equiv 3 (\text{mod } 7) \tag{3.141}$$

mas sabemos que os **resíduos quadráticos** módulo 7 são apenas 0, 1 e 4.

Exemplo Mostre que a equação

$$15x^2 - 7y^2 = 9 \tag{3.142}$$

não possui solução em $\mathbb{Z}$.

Solução. Note que 3 deve dividir y, assim $y = 3y_1$. Substituindo,

$$5x^2 - 3y_1^2 = 3 \tag{3.143}$$

e com isso $3 \mid x$, digamos $x = 3x_1$. Substiuindo, ficamos com

$$15x_1^2 - y_1^2 = 1 \tag{3.144}$$

ou seja, como $3 \mid 15$ então $3 \mid y_1^2 + 1$. Mas sabemos que para qualquer a inteiro, $a^2 + 1$ deixa resto 1 ou 2 na divisão por 3.

Exemplo Mostre que a equação

$$x^3 + 2y^3 + 4z^3 = 9w^3 \tag{3.145}$$

não possui solução em $\mathbb{Z}$, a menos da trivial $(0, 0, 0, 0)$.

Solução. Vamos supor que $mdc(x, y, z, w, 3) = 1$. Sabemos que para qualquer $a \in \mathbb{Z}$

$$a^2 \equiv -1, 0 \text{ ou } 1 \pmod 9 \tag{3.146}$$

Dessa forma, para $9 \mid x^3 + 2y^3 + 4z^3$ a única possibilidade é que x^3, y^3 e z^3 deixem resto zero na divisão por 9, isto é,

$$x \equiv 0 \pmod 3 \quad y \equiv 0 \pmod 3 \quad z \equiv 0 \pmod 3 \tag{3.147}$$

mas essa última constatação nos implicaria em $27 \mid x^3 + 2y^3 + 4z^3$, ou seja, $27 \mid 9w^3$ e assim $3 \mid w$. Portanto teríamos que $mdc(x, y, z, w, 3) \neq 1$, gerando uma contradição.

Exemplo Mostre que a equação

$$y^2 = x^3 + 7 \tag{3.148}$$

não possui solução em $\mathbb{Z}$.

Solução. Perceba que se x for par, então teríamos que $4 \mid x^3 = y^2 - 7$, ou seja, $4 \mid y^2 - 3$ mas sabemos que isso não é possível. Dessa forma x é ímpar e y é par. Note que se $x \equiv 3 \pmod 4$ então

$$x^3 + 7 \equiv 3 + 7 \pmod 4 \Rightarrow y^2 \equiv 2 \pmod 4 \tag{3.149}$$

um absurdo. Assim $x \equiv 1 \pmod 4$. Temos

$$y^2 + 1 = (x + 2)(x^2 - 2x + 4) \tag{3.150}$$

Seja p um fator primo que dividir $y^2 + 1$. Será que pode $p \equiv 3 \pmod 4$? Vejamos:

$$y^2 \equiv -1 \pmod p \Rightarrow y^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod p \tag{3.151}$$

Daí, caso $p \equiv 3 \pmod 4$, então $1 \equiv -1 \pmod p$, ou seja, $p \pmod 2$, um absurdo. Nossa conclusão é que todo fator primo de $y^2 + 1$ deixa resto 1 na divisão por 4.

Agora vamos observar o número $(x+2) \equiv 3 \pmod 4$. Esse número é ímpar e deixa resto 3 na divisão por 4, então algum de seu divisor também deverá deixar resto 3 na divisão por 4. A explicação para isso é simples: caso todos os divisores primos de $(x+2)$ fossem da forma $4k+1$ então $(x+2)$ também seria da forma $4k'+2$, uma vez que se

$$a \equiv 1 \pmod 4 \tag{3.152}$$

$$b \equiv 1 \pmod 4 \tag{3.153}$$

então $a \times b \equiv 1 \pmod 4$.

Para concluir o absurdo do problema, vimos que em y^2+1 não temos primos da forma $4k+3$ mas em $x+2$, que divide y^2+1, sim.

Exemplo *(Olimpíada Balcânica)* Prove que a equação

$$x^5 - y^2 = 4 \tag{3.154}$$

não possui solução em inteiros.

Solução. Sabemos que

$$x^{10} \equiv 0 \text{ ou } 1 \pmod{11} \Rightarrow x^5 \equiv -1, 0 \text{ ou } 1 \pmod{11} \tag{3.155}$$

Assim $y^2 = x^2 - 4 \equiv 6, 7, 8 \pmod{11}$. Mas os resíduos módulo 11 possíveis são 0,1, 3,4, 5 e 9, o que nos permite concluir que a equação não possui solução.

Exemplo *(Olimpíada Húngara)* Prove que a equação

$$(x+1)^2 + (x+2)^2 + \ldots + (x+99)^2 = y^z \tag{3.156}$$

não possui solução em inteiros, para $z > 1$.

Solução. Supunha que haja solução, assim temos que

$$33(3x^2 + 300x + 50 \cdot 199) = y^z \tag{3.157}$$

ou seja, $3 \mid y^z$ e como $z > 1$ concluímos que $3^2 \mid y^z$. Agora perceba que $3 \nmid (3x^2 + 300x + 50 \cdot 199)$, o que nos permite chegar a um absurdo.

Exemplo Prove que a equação

$$x^3 + y^4 = 7 \tag{3.158}$$

Solução. Essa é uma questão muito difícil e trabalhosa. Deve-se testar todas as congruências menores antes de chegar a solução completa.

Por isso, vamos utilizar congruência módulo 13. Temos que para todo x e y

$$x^3 \equiv 0, 1, 5, 8, 12 \pmod{13} \quad \text{e} \quad y^3 \equiv 0, 1, 3, 9 \pmod{13} \tag{3.159}$$

então como se pode observar, $x^3 + y^4$ nunca deixará resto 7 na divisão por 13.

Exemplo *(EUA)* Determine todas as soluções da equação

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 = 15999 \tag{3.160}$$

no conjuntos dos inteiros.

Solução. Vamos olhar a congruência módulo 16. Se a é um inteiro par então $16 \mid a^4$. Se a é ímpar, observe que

$$a^4 - 1 = (a^2 - 1)(a^2 + 1) \tag{3.161}$$

assim já sabemos que $8 \mid a^2 - 1$ e que $a^2 + 1$ é par, ou seja, $16 \mid a^4 - 1$. Portanto, podemos concluir que

$$x_1^4 + x_2^4 + \ldots + x_{14}^4 \in \{0, 1, 2, \ldots, 14\} \tag{3.162}$$

enquanto $15999 \equiv 15 \pmod{16}$. Vemos claramente que a equação não possuirá soluções.

3.7 Exercícios de Aprofundamento

Vamos resolver uma série de exercícios para mostrar a aplicabilidade dos assuntos vistos nesse Capítulo.

Problema 3.7.1. *Prove que há infinitos inteiros n tais que $n^2 + (n+1)^2$ seja um quadrado perfeito.*

Solução Ora, queremos que exista inteiros positivos p tais que

$$2n^2 + 2n + 1 = p^2 \Leftrightarrow (2n+1)^2 - 2p^2 = -1 \tag{3.163}$$

Ora, chegamos a uma Equação de Pell no caso $m = -1$. Uma solução inicial é $2n + 1 = 1$ e $p = 1$ e as demais soluções são obtidas conforme o Teorema 3.4.6.

Problema 3.7.2. *Prove que a soma dos n primeiros naturais é um quadrado perfeito para infinitos valores de n.*

Solução Queremos infinitos inteiros positivos n tais que

$$n^2 + n = 2p^2 \Leftrightarrow (2n+1)^2 - 8p^2 = 1 \tag{3.164}$$

Problema 3.7.3. (Cone Sul/97) *Demonstrar que existem infinitas ternas (a, b, c), com a, b, c números naturais, que satisfazem a relação:*

$$2a^2 + 3b^2 - 5c^2 = 1997 \tag{3.165}$$

Solução A ideia é chegar bem próximo de 1997 através de a ou b. Assim, tome $a = 31$

$$3b^2 - 5c^2 = 75 \Rightarrow 3 \mid c \text{ e } 5 \mid b \tag{3.166}$$

faça $c = 3c'$ e $b = 5b'$. Substuindo,

$$5b'^2 - 3c'^2 = 3 \Rightarrow 3 \mid b' \tag{3.167}$$

faça $b' = 3b''$. Substituindo,

$$c'^2 - 15b''^2 = -1 \tag{3.168}$$

agora toma $(c'_0, b''_0) = (4, 1)$ que o Teorema 3.4.6 nos faz encontrar as infinitas soluções.

Problema 3.7.4. (Banco IMO/2002) *Ache o menor inteiro positivo t para o qual existem inteiros $x_1, x_2, \ldots, x_t$ tais que*

$$x_1^3 + x_2^3 + \ldots + x_t^3 = 2002^{2002} \tag{3.169}$$

Solução Sabemos que para qualquer inteiro a, $a^3 \equiv 0, 1, -1 \pmod 9$. Como

$$2002^{2002} \equiv 4^{2002} \equiv 2^{4004} \equiv 4 \pmod 9 \tag{3.170}$$

pois $2^6 \equiv 1 \pmod 9$, assim podemos concluir que $t \geq 4$. Agora tome

$$x_i = 2002^{\frac{2001}{3}} y_i, \text{ para } 1 \leq i \leq 4 \tag{3.171}$$

e assim teremos que

$$x_1^3 + x_2^3 + x_3 + x_4^3 = 2002^{2002} \Leftrightarrow y_1^3 + y_2^3 + y_3^3 + y_4^3 = 2002 \tag{3.172}$$

agora basta tomar $y_1 = y_2 = 10$ e $y_3 = y_4 = 1$. Assim $t = 4$.

Problema 3.7.5. (OBM) *Mostre que a equação*

$$x^2 + y^2 + z^2 = 3xyz \tag{3.173}$$

tem infinitas soluções inteiras com $x > 0$, $y > 0$, $z > 0$.

Solução Tome $z = 1$, assim fazendo um pouco de algebrismo ficamos com

$$(2x - 3y)^2 - 5y^2 = -4 \tag{3.174}$$

Trata-se de uma equação de Pell generalizada, onde a solução é dada por

$$x_n + y_n\sqrt{d} = (x_0 + y_0\sqrt{d})^n(x_0' + y_0'\sqrt{d}) \tag{3.175}$$

sendo (x_0, y_0) a solução inicial para $x^2 - dy^2 = 1$ e (x_0', y_0') a solução inicial para $x^2 - dy^2 = -4$. Substituindo, ficamos com

$$x_n + y_n\sqrt{d} = (9+4\sqrt{5})^n(1+\sqrt{5}) = (9+4\sqrt{5})^n + \sqrt{5}(9+4\sqrt{5})^n \tag{3.176}$$

assim,

$$y_n\sqrt{5} = \Big(\sum_{i=0}\binom{n}{2i}9^{n-2i}(4\sqrt{5})^{2i}\Big)\sqrt{5} + \Big(\sum_{i=0}\binom{n}{2i+1}9^{n-2i-1}(4\sqrt{5})^{2i+1}\Big)$$

e

$$x_n\sqrt{5} = \Big(\sum_{i=0}\binom{n}{2i}9^{n-2i}(4\sqrt{5})^{2i}\Big) + \Big(\sum_{i=0}\binom{n}{2i+1}9^{n-2i-1}(4\sqrt{5})^{2i+1}\Big)\sqrt{5}$$

daí é facíl notar que que x_n e y_n são ambos ímpares, ou seja, como

$$2x - 3y = x_n \quad \text{e} \quad y = y_n \tag{3.177}$$

podemos concluir que x e y são inteiros.

Problema 3.7.6. *Ache todos os inteiros positivos x, y, e z tal que*

$$5x^2 - 14y^2 = 11z^2 \tag{3.178}$$

Solução Suponha que a equação tenha uma solução mínima (a, b, c). Temos que

$$5a^2 \equiv 11b^2 \equiv 4b^2 \pmod 7 \Rightarrow 15a^2 \equiv 12b^2 \pmod 7 \tag{3.179}$$

ou seja, $a^2 \equiv 5b^2 \pmod 7$. Os resíduos quadráticos módulo 7 são 0, 1, 2 e 4. O único par que satisfaz essa última congruência é $(0, 0)$. Logo $a = 7a'$ e $b = 7b'$ e consequentemente $c = 7c'$. Substituindo na equação, ficamos com

$$5a'^2 - 14b'^2 = 11c'^2 \tag{3.180}$$

ou seja, encontramos uma solução menor que a mínima e isso é um absurdo. Portanto, não existe solução para a equação.

CAPÍTULO 4

PROBLEMAS PROPOSTOS

Como desafio, deixo alguns problemas que envolvem todos os assuntos até aqui abordados.

Problema 4.0.1. *Mostre que se p é um número primo da forma $4k+1$, então*

$$p \mid \left[\left(\frac{p-1}{2}\right)!\right]^2 + 1 \tag{4.1}$$

Problema 4.0.2. (Decomposição Canônica) *Todo número n pode ser escrito como*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m} \tag{4.2}$$

sendo p_i, para $1 \leq i \leq m$, primo e $p_i \neq p_j$, para $1 < i < j < m$.

Problema 4.0.3. (Coréia) *Ache todos os inteiros positivos x, y, z tais que*

$$x^2 + y^2 + z^2 - 2xyz = 0 \tag{4.3}$$

Problema 4.0.4. (Balcânica) *Mostre que existe um múltiplo de 2004 que se escreve apenas com* 2004 1*'s e* 2004 0*'s.*

Problema 4.0.5. (IMO) *Sejam p e q números naturais tais que*

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \dots - \frac{1}{1318} + \frac{1}{1319} \tag{4.4}$$

Problema 4.0.6. (Balcânica) *Ache os números primos p e q tais que*

$$p^q - q^p = pq^2 - 19 \tag{4.5}$$

Problema 4.0.7. (Romênia) *Sejam p, q e r três números primos e n um inteiro positivos tal que*

$$p^n + q^n = r^2 \tag{4.6}$$

mostre que $n = 1$.

Problema 4.0.8. (Romênia) *Prove que a equação $3y^2 = x^4 + x$ não possui soluções em inteiros positivos.*

Problema 4.0.9. *Considere $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = n\phi(n)$ onde $\phi(n)$ a quantidade de números menores que n e que são primos com n. Mostrar que f é injetiva.*

Problema 4.0.10. (Banco IMO/2002) *Seja n um inteiro positivo que não é um cubo perfeito. Defina os números reais a, b, c por*

$$a = \sqrt[3]{n} \quad , \quad b = \frac{1}{a - \lfloor a \rfloor} \quad e \quad c = \frac{1}{b - \lfloor b \rfloor} \tag{4.7}$$

Prove que existem infinitos n com a propriedade que existem inteiros r, s e t tais que

$$ra + sb + tc = 0 \tag{4.8}$$

Problema 4.0.11. (Banco IMO) *Seja k um inteiro positivo. Mostre que existem infinitos quadrados perfeitos da forma $n \cdot 2^k - 7$, onde n é um inteiro positivo.*

Problema 4.0.12. (Rússia) *Prove que a equação $x^2 + y^2 - z^2 = 1997$ tem infinitas soluções nos inteiros x, yez.*

CONCLUSÃO E TRABALHOS FUTUROS

Pode-se perceber o vasto campo de aplicação das Equações Diofantinas em problemas do cotidiano e no mundo acadêmico, além dos diversos métodos de resoluções das não lineares. Os assuntos abordados neste trabalho trouxeram uma ramificação dessas equações de forma a abordar de maneira mais didática para o leitor, além de propiciar uma leitura mais compreensível dessas equações. Os problemas resolvidos são uma forma prática de aplicar toda a teoria aprendida.

Para o aluno de olimpíada de matemática, o capítulo inicial é de extrema importância pois é a base adotada nos exercícios posteriores. Para um melhor compreensão e aprimoramente dos conhecimentos de teoria dos números, sugere-se o livro [3] da bibliografia desse trabalho.

Para o docente, é crucial entender todos os tópicos teóricos para aplicar nas resoluções de todos os problemas apresentados nesse trabalho. A resolução dos problemas propostos faz parte da atividade do professor, como desafio. Caso o aluno já tenha uma boa base de teoria dos números, recomenda-se trabalhar por um longo período nas equações diofantinas lineares com bastante exercícios, de maneira que as fórmulas obtidas consigam ser demontradas pelos próprios alunos. Caso contrário, há a necessidade de trabalhar essa base por um bom tempo. Apenas após esse estudo, deve-se apresentar as equações diofantinas não lineares, através dos métodos de resolução,

conforme vistos nesse trabalho.

Por fim, acreditamos que esse trabalho possa servir como motivação para os docentes e discentes na continuação das equações diofantinas e buscar o estudo da geometria diofantina, onde se busca conexões entre a geometria algébrica e equações diofantinas.

APÊNDICE A

NOÇÕES TOPOLÓGICAS

Definição A.0.1. (Ponto Interior) *O ponto $x \in X$ é interior do conjunto X quando existe um intervalo aberto (a, b) tal que $x \in (a, b) \subset X$.*

Definição A.0.2. *(Conjunto Aberto)o conjunto $A \subset \mathbb{R}$ é aberto quando todos seus pontos são interiores.*

Definição A.0.3. (Ponto Aderente) *Dizemos que x é ponto aderente a um conjunto $X \subset \mathbb{R}$ quando a for limite de uma sequência de pontos $x_n \in X$.*

Definição A.0.4. *Sejam X e Y conjunto de números reais, com $X \subset Y$. Dizemos que X é denso em Y quando todo ponto de T for aderente a X.*

APÊNDICE B

O PEQUENO TEOREMA DE FERMAT

Teorema B.0.1. *Dado um número primo $p > 2$ então qualquer que seja o inteiro a,*

$$a^p \equiv a \pmod{p} \tag{B.1}$$

Demonstração Há diversas demonstrações para esse Teorema. Faremos por indução em a. Vejamos

$$0^p = 0 \equiv 0 \pmod{p} \tag{B.2}$$

e assim a equação é válida para $n = 1$. Para $n = 1$, temos

$$1^p = 1 \equiv 1 \pmod{p} \tag{B.3}$$

Suponha verdade para $k = 1, 2, \ldots, n$. Assim

$$(n+1)^p = n^p + \sum_{i=1}^{p-1} \binom{p}{i} n^i + 1 \tag{B.4}$$

Agora note que para $i = 1, 2, \ldots, p-1$

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \tag{B.5}$$

sendo que no numerador temos o número p, enquanto no denominador aparece apenas produto de números estritamente menores que p. Como p é

primo, podemos concluir que

$$p \mid \binom{p}{i} \tag{B.6}$$

Potanto, utilizando indução e essa última propriedade, temos

$$(n+1)^p \equiv n + \sum_{i=1}^{p-1} 0 + 1 \equiv n + 1 \pmod{p} \tag{B.7}$$

APÊNDICE C

SEQUÊNCIA DE FERMAT

Definição C.0.1. *A sequência de Fermat é definida da seguinte forma*

$$F_1 = F_2 = 1 \tag{C.1}$$

e para $n \geq 1$,

$$F_{n+2} = F_{n+1} + F_n \tag{C.2}$$

Fórmula para F_n

Sendo α e β tais que

$$\alpha + \beta = -1 \quad \text{e} \quad \alpha\beta = 1 \tag{C.3}$$

demonstra-se que

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \tag{C.4}$$

APÊNDICE D

SEQUÊNCIA DE LUCAS

Definição D.0.1. *A sequência de Lucas é definida da seguinte forma*

$$L_1 = 1 \quad e \quad L_2 = 2 \tag{D.1}$$

e para $n \geq 1$,

$$L_{n+2} = L_{n+1} + L_n \tag{D.2}$$

Fórmula para L_n

Sendo α e β tais que

$$\alpha + \beta = -1 \quad \text{e} \quad \alpha\beta = 1 \tag{D.3}$$

demonstra-se que

$$L_n = \alpha^n + \beta^n \tag{D.4}$$

APÊNDICE E

TEOREMA DE WILSON

Teorema E.0.1. *Seja p um número inteiro positivo, com $p > 1$. Então p é primo se, e somente se,*

$$(p-1)! \equiv -1 \pmod{p} \tag{E.1}$$

Demonstração Primeiramente, suponha que $p \mid (p-1)! + 1$. Testando alguns casos pequenos ($p = 2, 3, 4$) verificamos a veracidade da hipótese. Suponha então $p \geq 5$. Caso p fosse composto, então $p = a \cdot b$, com $1 < a \leq b \leq p-1$. Vamos dividir em dois casos

Caso 1: Se $a = b$ assim $p = a^2$. Mas note que

$$2a \leq a^2 - 1 \Leftrightarrow a > 1 + \sqrt{2} \tag{E.2}$$

que é verdade. Portanto, nosso número $(p-1)!$ será da forma

$$(p-1)! = 1 \times 2 \times \ldots \times a \times \ldots \times 2a \times \ldots \times (p-1) \tag{E.3}$$

assim $p = a^2 \mid (p-1)!$, mas como $a^2 \mid (p-1)^2 + 1$ então $p = a^2 \mid 1$ e assim $a^2 = 1$.

Caso 2: Se $p = a \cdot b$, com $1 < a < b \leq (p-1)$. Assim

$$(p-1)! = 1 \times 2 \times \ldots \times a \times \ldots \times b \times \ldots \times (p-1) \tag{E.4}$$

e assim $p = a \cdot b \mid (p-1)!$. Mas por hipótese $p \mid (p-1)! + 1$ p que nos implicaria $p \mid 1$, um absurdo. Então p deve ser primo.

Agora, suponha p primo.

APÊNDICE F

PRINCÍPIO DA CASA DOS POMBOS

Teorema F.0.1. *Se dispusermos* $nk+1$ *objetos em* n *caixas então pelo menos uma caixa conterá no mínimo* $k+1$ *objetos.*

Demonstração Ora, suponha que cada caixa tenha no máximo k objetos. Assim, no total teríamos $n \cdot k$ objetos, sendo um absurdo. Dessa forma, ao menos uma caixa deve contar $k+1$ objetos.

■

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDREESCU, T., ANDRICA, D., CUCUREZEANU, I.. **An Introduction to Diophantine Equations** - A problem Based Approach. Birkhauser Ed., New York, 2010.

[2] HEFEZ, A., **Aritmética** - Coleção PROFMAT. Editora SBM, Rio de Janeiro, 2016.

[3] ALENCAR FILHO, E., **Teoria Elementar dos Números**. Editora Nobel, São Paulo, 1981.

[4] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar - Teoria dos Números, volume 5.** SBM, Rio de Janeiro, 2012.

[5] Plínio, O. dos Santos. **Introdução à Teoria dos Números.** Coleção Matemática Universitária. IMPA. 1999.

[6] ANDREESCU, T.; GELCA, R. **PUTNAM and BEYOND.** Ed. Springer. - New York, 2007.

[7] MUNIZ NETO, A. C. **Tópicos de Matemática Elementar: Introdução à Análise.** Coleção Professor de Matemática. v. 3. Ed. SBM: 2ª ed. - Rio de Janeiro, 2012.

[8] LIMA, E. L. **Números e Funções Reais.** Coleção PROFMAT. Ed. SBM: 1ª ed. - Rio de Janeiro, 2013.

[9] LIMA, E. L. **Curso de Análise, vol. 1.** Ed. IMPA: 14ª ed. - Rio de Janeiro, 2016.

[10] ANDREESCU, T.; GELCA, R. **Mathematical Olympiad Challenges.** Ed. Birkha¨user: 2a ed. - Boston, 2009.

[11] ANDREESCU, T.; ANDRICA, D. **360 Problems for Mathematical Contests.** Ed. GIL. - Zalau, 2003.

[12] SHINE, C. Y. **21 Aulas de Matemática Olímpica.** Rio de Janeiro, SBM Editora, 2009.