UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CAMPUS VII – GOV. ANTÔNIO MARIZ
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA PLENA EM CIÊNCIAS EXATAS

ALLAN MISSAEL HENRIQUES GONÇALVES

UM TRATAMENTO PARTICULAR DA EQUAÇÃO DE PELL

PATOS – PB
2011

ALLAN MISSAEL HENRIQUES GONÇALVES

UM TRATAMENTO PARTICULAR DA EQUAÇÃO DE PELL

Trabalho acadêmico referente à conclusão do Curso de Licenciatura Plena em Ciências Exatas da Universidade Estadual da Paraíba (UEPB CampusVII).

Orientador: Msc. Vilmar Vaz da Silva

PATOS – PB

2011

G635t GONÇALVES, Allan Missael Henriques.

Um Tratamento Particular da Equação de Pell / Allan Missael Henriques Gonçalves.
Patos: UEPB, 2011.
60f

Monografia (trabalho de conclusão de curso - (Tcc) - Universidade Estadual da Paraíba.
Orientadora: Prof. Msc. Vilmar Vaz da Silva

1. Matemática 2. Álgebra I. Titulo
II. Silva, Vilmar Vaz

CDD 512

UNIVERSIDADE ESTADUAL DA PARAÍBA – UEPB
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS – CCEA
CAMPUS VII – GOVERNADOR ANTÔNIO MARIZ
CURSO DE LICENCIATURA EM CIÊNCIAS EXATAS

ATA DE DEFESA DE TCC

Aos 17 dias do mês de novembro do ano de 2011 ; às 09 horas, no Campus VII da Universidade Estadual da Paraíba, ocorreu a apresentação de Trabalho de Conclusão de Curso, requisito da disciplina TCC, do (a) aluno (a) Allan Missael Henriques Gonçalves tendo como tema "Um tratamento Particular da Equação de Pell"

Constituíram a Banca Examinadora os professores:

Professor (a) Vilmar Vaz da Silva (orientador)

Professor (a) Pedro Carlos de Assis Júnior

Professor (a) Syana Monteiro de Alencar Ramos

Após a apresentação e as observações dos membros da banca avaliadora, definiu-se que o trabalho foi aprovado, com nota 10,0 (Dez).

Eu, Vilmar Vaz da Silva, Professor (a) orientador (a), lavrei a presente ata que segue assinada por mim e pelos demais membros da Banca Examinadora.

Vilmar Vaz da Silva
Professor(a) Orientador(a)
Nome Completo

Pedro Carlos de Assis Júnior
Professor(a) Examinador(a) 1
Nome Completo

Syana Monteiro de Alencar Ramos
Professor(a) Examinador(a) 2
Nome Completo

ALLAN MISSAEL HENRIQUES GONÇALVES

UM TRATAMENTO PARTICULAR DA EQUAÇÃO DE PELL

Aprovada em 17 de novembro de 2011.

COMISSÃO EXAMINADORA

_____

Prof. Msc. Vilmar Vaz da Silva – CCEA-UEPB (Orientador)

_____

Prof. Dr. Pedro Carlos de Assis Junior – CCEA-UEPB (Examinador)

_____

Profª. Syana Monteiro de Alencar Ramos – CCEA-UEPB (Examinadora)

Dedico este trabalho primeiramente a Deus, força que rege meu ser. Aos meus pais, minha esposa e meus irmãos que estiveram ao meu lado durante esta jornada.

AGRADECIMENTOS

A Deus, por iluminar meu caminho e me dar forças para seguir sempre em frente.

Aos meus pais pelas orações, conselhos, empenho, estímulo, entusiasmo e amor nas fazes boas e ruins de minha vida.

A minha esposa Flavia de Souza Lima, pela paciência, confiança, incentivo e ajuda nos momentos difíceis.

Ao meu orientador, Vilmar Vaz da Silva, pelas orientações, discussões enriquecedoras, dedicação, paciência e apoio durante esta jornada.

À minha família, por me educar com muito amor e carinho.

Aos meus amigos que me proporcionaram momentos de lazer, imprescindíveis ao bom andamento deste estudo.

A todos os professores, que foram os responsáveis pela minha formação acadêmica, pessoal e profissional.

A todos que de alguma maneira contribuíram para a execução desse trabalho, seja pela ajuda constante ou por uma palavra de amor.

"O único homem que está isento de erros, é aquele que não arrisca acertar"

Albert Einstein

RESUMO

Este trabalho irá abordar um assunto que ainda é pouco explorado na disciplina de Teoria dos números, que é a equação de Pell. O objetivo deste estudo é mostrar as soluções e a infinidade de soluções dessa equação por meio de demonstrações algébricas. Para um melhor entendimento da equação, torna-se necessário que o leitor tenha em mente alguns conceitos da teoria dos números, presentes neste trabalho como algoritmos fundamentais. Veremos que nem sempre é fácil, ou mesmo possível, determinar todas as soluções em inteiros de uma dada equação. Por exemplo, para mostrar todas as soluções de uma equação de Pell, é bem mais fácil mostrar que ela possui uma infinidade de soluções do que determinar todas elas. Podemos gerar infinitas soluções dessa equação a partir de uma só solução não nula. Por fim, notaremos que na teoria das equações diofantinas, a equação de Pell é fundamental, pois muitas outras equações podem ser reduzidas a ela.

Palavras-chave: Equação de Pell, infinidade de soluções, equações diofantinas.

ABSTRACT

This paper will address a subject that is still little explored in the discipline of number theory, which is the Pell equation. The aim of this study is to show solutions and infinitely many solutions of this equation by means of algebraic statements. For a better understanding of the equation, it is necessary that the reader has in mind some concepts of number theory, in this work as fundamental algorithms. We will see that it is not always easy or even possible, determine all solutions in integers of a given equation. For example, to display all solutions of a Pell equation, it is much easier to show that it has an infinite number of solutions to determine all of them. We can generate infinitely many solutions of this equation from one nonzero solution. Finally, we note that the theory of Diophantine equations, Pell's equation it is essential, because many other equations can be reduced to it.

Keywords: Pell's equation, infinitely many solutions, Diophantine equations.

SUMÁRIO

INTRODUÇÃO

Uma equação algébrica com coeficientes inteiros chama-se uma equação Diofantina se suas soluções são números inteiros ou racionais (Matemático Grego Diofanto viveu em Alexandria, 250 a.C.). A equação diofantina:

$$x^2 - dy^2 = N,$$

onde $d, N \in \mathbb{Z}$, é conhecida como equação de Pell. Os primeiros matemáticos Gregos e Hindus consideraram casos especiais dessa equação. Por exemplo, os filósofos Pitagóricos, muito interessados em matemática, conheciam soluções especiais de $x^2 - 2y^2 = 1$, mas foi Fermat (Matemático Francês Pierre Fermat, 1601 - 1665) o primeiro a tratá-la sistematicamente. Ele afirmou ter provado que existia um número infinito de soluções inteiras x e y no caso especial em que $d > 0$ é livre de quadrados e $N = 1$. Como é usual, ele não deu uma prova. A primeira prova publicada foi dada por Lagrange (Matemático Francês Joseph Louis Lagrange, 1736 - 1813), usando as frações contínuas. Anterior a essa prova, Euler (Matemático Suiço Leonard Paul Euler, 1707 - 1783), provou que existia um número infinito de soluções, desde que exista uma.

A equação de Pell foi inicialmente estudada por Brahmagupta e Bhaskara. É importante ressaltar a participação de Bhaskara (aquele que os autores brasileiros de livros didáticos de Matemática atribuíram a fórmula de resolução de equações do 2º grau do tipo $ax^2 + bx + c = 0$ como Fórmula de Bhaskara), pois este está intimamente ligado à resolução de equações do tipo: $ax^2 + b = y^2$, que é exatamente a equação que recebe o nome de Pell. Acredita-se que Bhaskara havia encontrado à solução para esta equação, mas não demonstrou seus resultados.

A razão pela qual uma equação de tal antiguidade acabou ganhando o nome do matemático inglês John Pell (1611-1685) é bastante curiosa. O primeiro matemático europeu há obter soluções para esta equação em tempos recentes foi o inglês Lord Brouncker (1620-1684). Costuma-se dizer que Euler erroneamente atribuiu o trabalho de Brouncker sobre esta equação para Pell. No entanto, a equação aparece em um livro de Rahn (matemático suíço que foi o primeiro a usar o símbolo ÷ para a divisão), que certamente foi escrito com a ajuda de Pell: alguns dizem inteiramente escrito por Pell. Talvez Euler soubesse o que estava fazendo na nomeação da equação.

Diante das muitas possibilidades de aprofundamento de estudo sobre tal equação, nos competiu trabalhar com um caso particular da equação de Pell, mostrando seu valor na teoria

das equações Diofantinas, e sua fundamental importância na resolução de diversas equações que podem ser reduzidas a ela.

De agora em diante, o desenvolvimento do nosso trabalho seguirá o seguinte roteiro: No capítulo 1 apresentaremos uma revisão de teorias que serão indispensáveis para a compreensão dos resultados empregados na equação de Pell, em seguida, no capítulo 2, ingressaremos no estudo do anel $\mathbb{Z}[\sqrt{d}]$ que também será de suma importância, e para finalizarmos entraremos no capítulo 3 que é o resultado mais importante do nosso trabalho, aqui apresentaremos as soluções para um caso particular da equação de Pell.

CAPÍTULO 1

1 RESULTADOS FUNDAMENTAIS

Este capítulo constitui-se de uma revisão de alguns algoritmos e resultados fundamentais que serão úteis para a compreensão das soluções da Equação de Pell, o qual é o objeto central de estudo desse trabalho.

1.1 PRINCÍPIO DA BOA ORDENAÇÃO (P.B.O.)

Todo conjunto não vazio de números inteiros positivos possui um elemento mínimo.

1.2 PRINCÍPIO DA INDUÇÃO FINITA

1ª Forma: Seja B um conjunto de inteiros positivos satisfazendo as seguintes propriedades:
(i) $1 \in B$
(ii) $k+1 \in B$ sempre que $k \in B$.
Então B contém todos os números inteiros positivos.

2ª Forma: Seja B um conjunto de inteiros positivos satisfazendo as seguintes propriedades:
(i) $1 \in B$
(ii) $k+1 \in B$ sempre que $1, 2, 3, \cdots, k \in B$.
Então B contém todos os números inteiros positivos.

Observação (1): Seja $p(n)$, uma afirmação sobre n, onde $n \in \mathbb{Z}_+^*$ se tivermos:
(i) $p(1)$ é verdade;
(ii) $p(k+1)$ é verdade sempre que $p(k)$ for verdade. Então $p(k)$ é verdade para todo n natural.

1ª Forma. Demonstração:
Admita o P.B.O. Seja B um conjunto de inteiros positivos satisfazendo as propriedades:
(i) $1 \in B$
(ii) $k+1 \in B$ sempre que $k \in B$;

Suponha que B não contenha todos os inteiros positivos, ou seja, existe um certo b inteiro positivo tal que $b \notin B$. Considere o conjunto:

$$A = \{x \in \mathbb{Z}_+^* : x \notin B\}.$$

A é claramente não vazio; pois $b \in A$. Pelo P.B.O.; A possui um elemento mínimo, digamos a.

Afirmação: $a > 1$, pois, por *(i)* $1 \in B$.

$\Rightarrow a - 1 > 0$ e $a - 1 < a$ pelo fato de a ser mínimo, tem-se que $a - 1 \notin A$

$\Rightarrow (a-1) \in B \Rightarrow$ *(ii)* $\Rightarrow (a-1) + 1 = a \in B$ $(\longrightarrow\longleftarrow) \Rightarrow A$ é vazio

$\therefore n \in B, \forall\, n \in \mathbb{Z}_+^*$. ■

Observação (2): Seja $p(n)$ uma afirmação sobre n, onde $n \in \mathbb{Z}_+^*$ se tivermos:

(i) $p(1)$ é verdade;

(ii) $p(k)$ é verdade para todo k tal que $1 \leq k \leq n-1$. Então, $p(n)$ é verdade para todo $n \in \mathbb{Z}_+^*$.

2ª Forma. Demonstração:

Seja B um conjunto de inteiros positivos satisfazendo as propriedades:

(i) $1 \in B$

(ii) $k + 1 \in B$ sempre que $1, 2, 3, \cdots, k \in B$.

Suponha que B não contenha todos os inteiros positivos, ou seja, $b_0 \notin B$ tal que $b_0 \in \mathbb{Z}_+^*$. Considere o conjunto:

$$A = \{x \in \mathbb{Z}_+^* : x \in B\}.$$

Observem que $A \neq \emptyset$, pois, $b_0 \in A$. Pelo P.B.O., A possui um elemento mínimo, digamos a_0. Temos que:

$$a_0 > 1 \Rightarrow a_0 + 1 > 0 \Rightarrow a_0 + 1 \in B.$$

Afirmação: $1, 2, \cdots, a_0 + 1 \in B$, pois, a_0 é elemento mínimo. Daí temos que:

$$(a_0 - 1) + 1 \in B \Rightarrow a_0 \in B \quad (\longrightarrow\longleftarrow) \text{ contradição!}$$ ■

Exemplo: Prove usando indução, que:

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}, \qquad \forall n \in \mathbb{N}^*$$

Solução:

(1) Base de indução:

P/ $n=1$, temos:

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

(2) Hipótese de indução:

P/ $n=k$, temos:

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

(3) Passo indutivo:

P/ $n=k+1$, temos:

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

1.3 DIVISORES

Sejam $a, b \in \mathbb{Z}$**.** Dizemos que a divide b quando existir um inteiro c tal que $b=ac$. Usamos a notação $a|b$, para indicar que a divide b e escrevemos $a \nmid b$ quando a não divide b. Quando $a|b$, dizemos também que b é múltiplo de a ou a é divisor de b.

Teorema 1: Sejam a, b *e* $c \in \mathbb{Z}$, se $a|b$ e $b|c$ então $a|c$.

Demonstração: Como $a|b$ e $b|c$, temos:

$$\begin{cases} b=a\cdot k_1, & k_1 \in \mathbb{Z} \\ c=b\cdot k_2, & k_2 \in \mathbb{Z} \end{cases}$$

$\Rightarrow c=(a\cdot k_1)\cdot k_2 = a\cdot(k_1\cdot k_2) \Rightarrow a|c.$ ■

Teorema 2: A divisibilidade é tal que:

(i) $n|n, \ \forall \ n \in \mathbb{Z}$**.** Significa que todo inteiro divide a si mesmo. Isto segue da definição. Observe que $n = 1 \cdot n$.

(ii) $1|n, \ \forall \ n \in \mathbb{Z}$**.** Isto é, 1 divide qualquer inteiro. Segue da definição, observando que $n = n \cdot 1$.

(iii) $n|0, \ \forall \ n \in \mathbb{Z}$**.** Todo inteiro é divisor de 0. Basta observar que $0 = n \cdot 0$.

(iv) Se $a|n$ então $a \cdot d \ |n \cdot d, \quad a, n, d \ \in \mathbb{Z}$

(v) Se $a \cdot c|a \cdot d$ com $a \neq 0 \Rightarrow c|b, \quad a, c, d \in \mathbb{Z}$

(vi) Se $a|d$ e $d \neq 0 \Rightarrow |a| \leq |d|$

(vii) Se $a|b$ e $b|a \Rightarrow |a| = |b|$

(viii) Se $d|n$ e $d \neq 0 \Rightarrow \dfrac{n}{d} \mid n$.

Demonstração:

(vi) Se $a|d \Rightarrow d = a \ \cdot c$, com $c \in \mathbb{Z}$.

$$\Rightarrow \ |d| = |a \ \cdot c| = |a| \cdot |c| \Rightarrow |a| \leq |d|$$

(vii) Se $a|b$ e $b|a$, então:

$$|a| \leq |b| \quad \text{e} \quad |b| \leq |a| \Rightarrow |a| = |b|$$

1.4 ALGORITMO DA DIVISÃO

Teorema 3 (Euclides): Sejam $a, b \in \mathbb{N}$ com $b \neq 0$. Então, existem únicos $q, r \in \mathbb{N}$ tais que:

$$a = q \cdot b + r, \text{onde } 0 \leq r < b.$$

Demonstração:

(1) Existência: Vamos usar indução na 2ª forma em a, ou seja, temos que o resultado deve ser válido para todo k, tal que:

$$1 \leq k < a.$$

Se $a < b$, então nada a fazer. De fato, basta tomarmos:

$$q = 0 \quad \text{e} \quad r = a \Rightarrow a = 0 \cdot b + a.$$

Então, suponha que $a \geq b$.

$\Rightarrow a - b \geq 0$, ou seja: $0 \leq a - b < a$. Pela hipótese de indução, existem q', $r \in \mathbb{N}$ tais que:

$$a - b = q' \cdot b + r, \quad 0 \leq r < b$$
$$\Rightarrow a = q' \cdot b + b + r \Rightarrow a = (q' + 1) \cdot b + r, \quad 0 \leq r < b.$$

(2) Unicidade: Suponha que existam $q_1, q_2, r_1, r_2 \in \mathbb{N}$, tais que:

$$\begin{cases} a = q_1 \cdot b + r_1, \ com \ 0 \leq r_1 < b \\ a = q_2 \cdot b + r_2, \ com \ 0 \leq r_2 < b \end{cases}$$

$\Rightarrow q_1 \cdot b + r_1 = q_2 \cdot b + r_2 \Rightarrow r_1 - r_2 = (q_2 - q_1) \cdot b \Rightarrow b | (r_1 - r_2)$.

Por outro lado, temos:

$$r_1 - r_2 < b.$$

Suponha que $r_1 \neq r_2$, digamos $r_1 > r_2 \Rightarrow r_1 - r_2 > 0$.

Daí, temos:

$$0 < r_1 - r_2 = (q_2 - q_1) \cdot b < b$$
$$0 < r_1 - r_2 = 0 \quad (\rightarrow \leftarrow)$$
$$\therefore r_1 = r_2$$
$$\Rightarrow q_1 \cdot b = q_2 \cdot b \Rightarrow q_1 = q_2. \qquad \blacksquare$$

Observação: No teorema de Euclides, se $r = 0$ então $b | a$.

1.5 MDC

Definição: O máximo divisor comum dos inteiros a e b (com a ou b diferente de zero) é o maior inteiro que divide a e divide b.
NOTAÇÃO: (a, b).

Teorema 4: Se $d = (a, b)$ então existem $n_0, m_0 \in \mathbb{Z}$, tais que:

$$d = n_0 \cdot a + m_0 \cdot b.$$

Demonstração: Considere o conjunto:

$$B = \{n_0 \cdot a + m_0 \cdot b : n, m \in \mathbb{Z}\}.$$

Tome $c \in \mathbb{Z}$, tal que $c = n_0 \cdot a + m_0 \cdot b$ e c seja o menor inteiro positivo de B.

Afirmação: $c|a$ *e* $c|b$

De fato, pois se $c \nmid a$, temos pelo teorema de Euclides que:

$$a = q \cdot c + r, \text{ onde } 0 < r < c$$
$$\Rightarrow \; r = a - q \cdot c \Rightarrow r = a - q \cdot (n_0 \cdot a + m_0 \cdot b) = a - qn_0a - qm_0b$$
$$= (1 - qn_0) \cdot a + (-qm_0) \cdot b \Rightarrow r \in B \text{ (absurdo!)}$$

$\Rightarrow c|a$. De forma análoga temos que $c|b$.
$\Rightarrow c$ é um divisor comum de a e b. Mas temos que:

$$a = k_1 \cdot d \quad \text{e} \quad b = k_2 \cdot d, \qquad k_1, k_2 \in \mathbb{Z}$$
$$\Rightarrow \; c = n_0 \cdot a + m_0 \cdot b = (n_0 \cdot k_1)d + (m_0 \cdot k_2)d = d \cdot (n_0 \cdot k_1 + m_0 \cdot k_2) \Rightarrow d|c$$
$$\Rightarrow |d| \leq |c| \Rightarrow d \leq c \Rightarrow d = c. \qquad \blacksquare$$

1.5 DIVISIBILIDADE

Vimos que se $d = (a, b) \Rightarrow d = n_0a + m_0b, \quad n_0, m_0 \in \mathbb{Z}$.

Teorema 5: Se $d = (a, b)$, e $d'|a$ *e* $d'|b$, então $d'|d$.

Demonstração: Como $d = (a, b)$, então: $d = n_0 a + m_0 b, \quad n_0; m_0 \in \mathbb{Z}$. (I)
Como $d'|a$ e $d'|b$, temos:

$$a = k_1 \cdot d' \quad \text{e} \quad b = k_2 \cdot d', \quad k_1, k_2 \in \mathbb{Z}.$$

Daí, substituindo a e b em (I), tem-se $d = n_0 k_1 d' + m_0 k_2 d'$

$$\Rightarrow d = d'(n_0 k_1 + m_0 k_2) \Rightarrow d'|d. \qquad \blacksquare$$

Proposição 1: Se t é um inteiro positivo então:

$$(ta; tb) = t \cdot (a, b)$$

Demonstração: Lembre-se que: (ta, tb) é o menor inteiro positivo de $mta + ntb$ que é exatamente igual a t (menor inteiro positivo de $ma + nb$) = $t(a; b)$. $\blacksquare$

Corolário – 1: Se $c > 0$ e $c|a$ e $c|b$, então:

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b).$$

Demonstração: Faça na proposição anterior a como sendo $\frac{a}{c}$, b como sendo $\frac{b}{c}$ e $t = c$. Daí, temos:

$$\left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right) = (a, b) = c\left(\frac{a}{c}, \frac{b}{c}\right) \Rightarrow \left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c} \cdot (a, b). \qquad \blacksquare$$

Corolário – 2: Se $d = (a, b)$, então:

$$\left(\frac{a}{c}, \frac{b}{c}\right) = 1.$$

Demonstração:

Faça no corolário – 1. $c = d$.

Daí, temos:

$$\left(\frac{a}{d},\frac{b}{d}\right) = \frac{1}{d}\,(a;b) = \frac{1}{d}\cdot d = 1. \qquad \blacksquare$$

Definição: Dois inteiros a e b são ditos relativamente primos se: $(a,b) = 1$.

Teorema 6: Sejam a, b e x inteiros. Então: $(a,b) = (a, b+ax)$.

Demonstração: Chame $(a,b) = d$ e $(a, b+ax) = d'$. Temos que:

$$d = n_0 a + m_0 b = n_0 a + m_0 b + m_0 ax - m_0 ax = a(n_0 - m_0 x) + m_0(b+ax).$$

Como $d'|a$ e $d'|(b\ +\ ax)$, temos:

$a = k_1\cdot d' \quad$ e $\quad b + ax = k_2\cdot d', \quad k_1,\ k_2 \in \mathbb{Z}$
$\Rightarrow\ d = k_1\cdot d'(n_0 - m_0 x) + m_0\ \cdot\ k_2\cdot d' \Rightarrow\ d = d'[k_1\cdot\ (n_0 - m_0 x) + m_0\ \cdot\ k_2\,] \Rightarrow$
$d'|d\ \Rightarrow d' \le d.$

Por outro lado, como $d = (a,b)$ temos que: $d|a$ e $d|b \Rightarrow d|(b\ +\ ax)$. Do teorema visto, tem-se que:

$$d|d' \Rightarrow d \le d'\ \ \therefore d = d'. \qquad \blacksquare$$

Teorema 7: Se $c|a\cdot b$ e $(a,c) = 1$, então $c|b$.

Demonstração: Como $(a,c) = 1$,então:

$$1 = n_0 a + m_0 c, \text{ onde } n_0, m_0 \in \mathbb{Z}. (*)$$

Multiplicando-se $(*)$ por b, temos:

$$b = n_0(a\cdot b) + m_0(b\cdot c).$$

Como $c|ab \Rightarrow ab = k\cdot c,\ \ k \in \mathbb{Z}$

$$\Rightarrow\ b = n_0 k\cdot c + m_0 b\cdot c \Rightarrow b = c\ (n_0 k + m_0 b) \Rightarrow\ c|b. \qquad \blacksquare$$

Teorema 8: Sejam a, b inteiros com $a = q \cdot b + r$. Então:

$$(a, b) = (b, r).$$

Demonstração: Da igualdade $a = q \cdot b + r$, temos que se d é um divisor comum de b e r. Então:

$$d|b \text{ e } d|r \Rightarrow b = k_1 \cdot d \quad \text{e} \quad r = k_2 \cdot d, \quad k_1, k_2 \in \mathbb{Z}$$

$$\Rightarrow a = q \cdot k_1 d + k_2 d = d(q \cdot k_1 + k_2) \Rightarrow d|a.$$

Por outro lado considerem a igualdade: $r = a - q \cdot b$. Portanto, todo divisor de a e também divisor de b é um divisor de r. Logo, o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r.

$$\therefore (a, b) = (b, r). \qquad \blacksquare$$

Teorema 9 (Algoritmo Euclidiano): Sejam $r_0 = a$ e $r_1 = b$ inteiros não negativos com $b \neq 0$. Aplicando o algoritmo da divisão sucessivamente, para obtermos:

$$r_j = q_{j+1} \cdot r_{j+1} + r_{j+2}$$

com $0 \leq r_{j+2} < r_{j+1}$, $j = 0, \ldots, n-1$ e $r_{n+1} = 0$; então $(a, b) = r_n$.

Demonstração: Pelo algoritmo da divisão, temos que:

$$r_0 = q_1 \cdot r_1 + r_2, \qquad 0 < r_2 < r_1.$$

Aplicando-se novamente o algoritmo da divisão para r_1 e r_2, temos:

$$r_1 = q_2 \cdot r_2 + r_3, \qquad 0 < r_3 < r_2.$$

Continuando este processo e, sabendo que o mesmo deve parar, pois, temos uma sequência decrescente de restos não negativos.

Dessa forma obtemos a seguinte sequência de igualdades:

$$\begin{aligned} r_0 &= q_1 \cdot r_1 + r_2, \qquad 0 < r_2 < r_1. \\ r_1 &= q_2 \cdot r_2 + r_3, \qquad 0 < r_3 < r_2. \\ &\vdots \\ r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n, \qquad 0 < r_n < r_{n-1}. \\ r_{n-1} &= q_n \cdot r_n + 0. \end{aligned}$$

Daí, utilizando um teorema já visto, temos:

$$r_n = (r_{n-1}; r_n) = (r_{n-2}; r_{n-1}) = \cdots = (r_1; r_2) = (r_0; r_1) = (a, b). \qquad \blacksquare$$

1.7 NÚMEROS PRIMOS

Definição: Um número inteiro maior que 1 é primo se os seus únicos divisores são 1 e ele mesmo. Caso contrário ele será dito composto.

Proposição 2: Seja p um primo tal que $p|a \cdot b$, com a, b inteiros. Então: $p|a$ ou $p|b$

Demonstração: Suponha que $p \nmid a$.

$$\Rightarrow (p, a) = 1 \ (p \text{ é } primo) \Rightarrow p|b. \qquad \blacksquare$$

1.8 TEOREMA FUNDAMENTAL DA ARITMÉTICA

Teorema 10 (teorema fundamental da aritmética)

Todo número inteiro maior que 1 pode ser escrito de forma única (a menos de ordem) como um produto de fatores primos.

Demonstração: Seja n um número inteiro tal que $n > 1$. Se n é primo, acabou! Caso contrário, seja p_1, o menor inteiro positivo e maior que 1 tal que $p_1 | n$.

Afirmação: p_1 é primo.

De fato, pois, caso contrário existe p tal que: $1 < p < p_1$ e $p|n$ $(\longrightarrow\longleftarrow)$. Daí, temos que: $n = p_1 \cdot n_1$

Se n_1 é primo, acabou. Caso contrário, seja p_2 o menor inteiro maior que 1 tal que $p_2|n_1$. Pela mesma razão vista anteriormente, p_2 é primo. Portanto:

$$n = p_1 \cdot p_2 \cdot n_2.$$

Aplicando este raciocínio sucessivamente, determina-se uma sequência decrescente, $n_1 > n_2 > n_3 \cdots$ de inteiros maiores que 1. Portanto, esse processo deve parar. Temos então que:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}.$$

Vamos provar a unicidade da fatoração. Para tanto, vamos utilizar indução 2ª forma em n.

(1) Para $n = 2$, acabou.
(2) Admita que o resultado seja válido para todo inteiro t com $1 < t < n$
(3) Para $t = n$, temos:

$n = p_1 \cdot p_2 \cdot \cdots \cdot p_r = q_1 \cdot q_2 \cdot \cdots \cdot q_s$, onde p_i, q_j são primos.

Como p_1 é primo e $p_1|n = q_1 \cdot q_2 \cdot \cdots \cdot q_s$. Pela proposição 2 vista anteriormente, temos que:

$$p_i|q_j \text{ , para algum } j = 1, \cdots, s.$$

Sem perda de generalidade, admita que $p_1|q_1$. Portanto: $p_1 = q_1$. De forma geral, tem-se que $p_i = q_j$ para algum j. Observe ainda que:

$$\frac{n}{p_1} = p_2 \cdot p_3 \cdot \cdots \cdot p_r = q_2 \cdot q_3 \cdot \cdots \cdot q_s$$

$$1 < \frac{n}{p_1} < n.$$

Pela hipótese de indução, temos: $r = s$. ■

Teorema 11: Se $a = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_k^{r_k}$, então o conjunto dos divisores de a é formado por números da forma:

$$\prod_{i=1}^{k} {p_i}^{\alpha_i}$$

onde $0 \leq \alpha_i \leq r_i$.

Observação: Se colocarmos todos os primos positivos em ordem crescente, ou seja, $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $\cdots$, então todo número inteiro positivo pode ser escrito na forma:

$$\prod_{i=1}^{\infty} {p_i}^{k_i}.$$

E como consequência tem-se que os divisores serão dados por:

$$\prod_{i=1}^{\infty} {p_i}^{\alpha_i}$$

com $\alpha_i \geq 0$

Teorema 12: Se $a = \prod_{i=1}^{\infty} {p_i}^{t_i}$ e $b = \prod_{i=1}^{\infty} {p_i}^{s_i}$, então: $(a, b) = \prod_{i=1}^{\infty} {p_i}^{\beta_i}$,

onde $\beta_i = mín\{t_i, s_i\}$.

Demonstração: É claro que nenhum número com expoente maior que o $máx\{t_i, s_i\}$ pode ser divisor dos números a e b. Portanto, divisores comuns de a e b devem ser da forma:

$$\prod_{i=1}^{\infty} {p_i}^{\beta_i}$$

onde β_i não supera o $mín\{\mathrm{t_i}, \mathrm{s_i}\}$, mas como estamos buscando o maior dos divisores comuns; então $\beta = mín\{t_i, s_i\}$. ■

Teorema 13: A sequência dos números primos é infinita.

Demonstração: Suponha que existe apenas uma quantidade finita $p_1, p_2, \cdots, p_n$ de números primos. Considerem o seguinte número:

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_n + 1.$$

Observem que $n \neq p_i$ $(i = 1, \cdots, n)$ e $n > 1$. Pelo teorema fundamental da aritmética temos que n é primo ou n possui um fator primo. Se n possui um fator primo, então o mesmo deve pertencer a lista $p_1, \cdots, p_n$, digamos que p_1 seja fator primo de n. Daí teríamos que:

$$1 = \underbrace{n}_{p_1 | n} - \underbrace{(p_1 \cdot p_2 \cdot \cdots \cdot p_n)}_{p_1 | (p_1 \cdot p_2 \cdots p_n)}$$

$\Rightarrow p_1 | 1$. (absurdo!)
$\Rightarrow n$ é primo (absurdo!)
$\therefore$ A lista de primos é infinita.

Teorema 14: Para todo inteiro k positivo, existem k inteiros consecutivos e todos compostos.

Demonstração: Seja k um inteiro positivo. Temos que:

$$(k+1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot k \cdot (k+1).$$

Observe que $(k+1)!$ É divisível pelos k inteiros e consecutivos $2, 3, 4, \cdots, k$ e $(k+1)$.

Considere a sequência: $(k+1)! + 2,\ (k+1)! + 3, \cdots, (k+1)! + (k+1)$. Tal sequência possui k inteiros consecutivos e todos compostos. ■

Teorema 15: Todo produto de k inteiros consecutivos é divisível por $k!$

Demonstração: Sejam n, k inteiros positivos com $k \leq n$. Temos que:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n-k)!} = \frac{n(n-1) \cdot \cdots \cdot (n-k+1) \cdot (n-k)!}{k! \cdot (n-k)!} = \frac{n(n-1) \cdot \cdots \cdot (n-k+1)}{k!}.$$

Observem que o numerador é composto pelo produto de k inteiros consecutivos. ■

Teorema 15: Seja n um número inteiro maior que 1. Se n é composto, então n possui necessariamente um fator primo menor ou igual $a\sqrt{n}$.

Demonstração: Suponha que n é um número composto. Daí temos que: $n = n_1 \cdot n_2$ com $1 < n_1 < n$ e $1 < n_2 < n$. Sem perda de generalidade podemos admitir que $n_1 \leq n_2$.

Afirmação: $n_1 \leq \sqrt{n}$.

De fato, pois, caso contrário teríamos:

$$n = n_1 \cdot n_2 > \sqrt{n}. \cdot \sqrt{n} = n \text{ (absurdo!).}$$

Pelo T.F.A., n_1 possui um fator primo p. Daí temos:

$$p \leq n_1 \leq \sqrt{n} \Rightarrow p \leq \sqrt{n}\,. \qquad \blacksquare$$

1.9 MMC

Definição: O mínimo múltiplo comum entre dois inteiros positivos a e b é o menor inteiro positivo que é divisível por a e b.

Teorema 16: Se $a = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_n^{r_n}$ e $b = p_1^{s_1} \cdot p_2^{s_2} \cdot \cdots \cdot p_n^{s_n}$, então $[a, b] = p_1^{máx\{r_1, s_1\}} \cdot \cdots \cdot p_n^{máx\{r_n, s_n\}}$.

Demonstração: Nenhum expoente dos fatores primos p_i podem ser menores do que r_i e s_i na definição de m.m.c. daí temos que:

$$[a, b] = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_n^{\alpha_n}, \text{ com } \alpha_i \geq máx\{r_i,\ s_i\}.$$

Como queremos o menor entre todos os múltiplos comuns de a e b, então: $\alpha_i = máx\{r_i,\ s_i\}$. $\blacksquare$

Teorema 17: Sejam a e b inteiros positivos. Então: $(a, b) \cdot [a, b] = a \cdot b$.

Demonstração:

Lema: Se x e $y \in \mathbb{R}$, então: $mín\{x, y\} + máx\{x, y\} = x + y$.

Prova do Lema:

(1) Se $x = y$, acabou!

(2) Suponha que $x \neq y$. Sem perda de generalidade podemos supor que $x < y$. Daí, temos:

$$\begin{cases} mín\{x, y\} = x \\ máx\{x, y\} = y \end{cases} \Rightarrow mín\{x, y\} + máx\{x, y\} = x + y.$$

Sabemos que:

$$\begin{cases} a = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_n^{r_n} \\ b = p_1^{s_1} \cdot p_2^{s_2} \cdot \cdots \cdot p_n^{s_n} \end{cases}$$

$$\Rightarrow (a, b) = p_1^{mín\{r_1, s_1\}} \cdot \cdots \cdot p_n^{mín\{r_n, s_n\}} \text{ e } [a, b] = p_1^{máx\{r_1, s_1\}} \cdot \cdots \cdot p_n^{máx\{r_n, s_n\}}$$

$$\Rightarrow (a, b) \cdot [a, b] = p_1^{máx\{r_1, s_1\}} \cdot \cdots \cdot p_n^{máx\{r_n, s_n\}} \cdot p_1^{mín\{r_1, s_1\}} \cdot \cdots \cdot p_n^{mín\{r_n, s_n\}}.$$

Lema: $= p_1^{r_1 + s_1} \cdot \cdots \cdot p_n^{r_n + s_n} = a \cdot b.$ ■

Teorema 18: Seja b um inteiro maior que 1. Então, todo número inteiro positivo n pode ser escrito, de maneira única na forma:

$n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0$, onde $k \geq 0$, $a_k \neq 0$ e $0 \leq a_i < b$, $i = 0, 1, \cdots, k$.

Demonstração:

***(1)* Existência:** Vamos utilizar o algoritmo de Euclides. Inicialmente vamos dividir n por b. Daí, existem q_0 , a_0 tais que:

$$n = b \cdot q_0 + a_0; \qquad 0 \leq a_0 < b.$$

Temos ainda que:

$$q_0 = b \cdot q_1 + a_1; \qquad 0 \leq a_1 < b.$$
$$q_1 = b \cdot q_2 + a_2; \qquad 0 \leq a_2 < b.$$
$$\vdots$$
$$q_{k-2} = b \cdot q_{k-1} + a_{k-1}; \qquad 0 \leq a_{k-1} < b.$$
$$q_{k-1} = b \cdot 0 + a_k; \qquad 0 \leq a_k < b.$$

Portanto, temos que:

$$\begin{aligned} n &= b\cdot(b\cdot q_1 + a_1) + a_0 = b^2\cdot q_1 + b\cdot a_1 + a_0 \\ &= b^2\cdot(b\cdot q_2 + a_2) + b\cdot a_1 + a_0 \\ &= b^3\cdot q_2 + b^2\cdot a_2 + b\cdot a_1 + a_0 \\ &\vdots \\ &= b^{k-1}\cdot(b\cdot q_{k-1} + a_{k-1}) + \cdots + b\cdot a_1 + a_0 \\ &= b^k\cdot q_{k-1} + b^{k-1}\cdot a_{k-1} + \cdots + b\cdot a_1 + a_0 \\ &= a_k\cdot b^k + a_{k-1}\cdot b^{k-1} + \cdots + a_1\cdot b + a_0. \end{aligned}$$

***(2)* Unicidade:** Suponha que n possua duas formas diferentes, a saber:

$$\begin{cases} n = a_k\cdot b^k + a_{k-1}\cdot b^{k-1} + \cdots + a_1\cdot b + a_0. \\ n = d_m\cdot b^m + d_{m-1}\cdot b^{m-1} + \cdots + d_1\cdot b + d_0. \end{cases}$$

$$0 = h_s\cdot b^s + h_{s-1}\cdot b^{s-1} + \cdots + h_1\cdot b + h_0\ ,$$

onde s é o maior valor de i para o qual $a_i \neq d_i$. Daí, temos que:

$$h_s\cdot b^s = -(h_{s-1}\cdot b^{s-1} + \cdots + h_1\cdot b + h_0) \Rightarrow |h_s\cdot b^s| = |h_{s-1}\cdot b^{s-1} + \cdots + h_1\cdot b + h_0|$$

mas, observem que:

$$|h_i| \leq b-1, i = 0,\cdots, s-1.$$

Temos que:

$$\begin{aligned} b^s = |b^s| < |h_s\cdot b^s| &= |h_{s-1}\cdot b^{s-1} + \cdots + h_1\cdot b + h_0| \leq |h_{s-1}|\cdot b^{s-1} + \cdots + |h_1|\cdot b + \\ &|h_0| \leq (b-1)\cdot b^{s-1} + \cdots + (b-1)\cdot b + (b-1) \\ &= (b-1)(b^{s-1} + b^{s-2} + \cdots + b + 1) = b^s - 1 \text{ (absurdo!)} \end{aligned}$$ ■

1.10 NÚMEROS DE FERMAT

Definição: Um número da forma: $2^{2^n}+1$, com $n \in \mathbb{N}$ é denominado de número de Fermat.

Exemplos: 3 é um número de Fermat, pois, $3 = 2^{2^0} + 1 = \mathrm{F}_0$.

Proposição 3: Tem-se que:

$$F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{n-1} = F_n - 2.$$

Demonstração: Indução em n (1ª forma)

(1) Para $n = 1$, temos:

$$F_0 = F_1 - 2, \text{ temos que:}$$

$$F_0 = 2^{2^0} + 1 = 3 = \left(2^{2^1} + 1\right) - 2, \text{ ok!}$$

(2) Suponha válido para $n = k$, ou seja:

$$F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{k-1} = F_k - 2.$$

(3) Para $n = k + 1$, temos:

$$F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_{k-1} \cdot F_k - 2 = (F_k - 2) \cdot F_k$$

$$= (2^{2^k} + 1 - 2)(2^{2^k} + 1) = (2^{2^k} - 1)\,(2^{2^k}+1) = (2^{2^k})^2 - 1$$

$$= 2^{2 \cdot 2^k} - 1 = 2^{2^{k+1}} - 1 = (2^{2^{k+1}} + 1) - 2 \Rightarrow F_{k+1} - 2.$$

$\therefore$ O resultado é válido para todo natural n. ■

Teorema 19: Se F_n e F_m são números de Fermat distintos, então $(F_n, F_m) = 1$.

Demonstração: Como $n \neq m$, podemos admitir que $n > m$. Daí, temos pela proposição anterior que:

$$F_0 \cdot F_1 \cdot F_2 \cdot \cdots \cdot F_m \cdot F_{m+1} \cdot \cdots \cdot F_{n+1} = F_n - 2 \Rightarrow F_n - F_o \cdot F_1 \cdot \cdots \cdot F_m \cdot \cdots \cdot F_{n-1} = 2\,.\,(*)$$

Seja d um divisor comum de F_n e F_m. Mas, em virtude de $(*)$ tem-se que: $d|2$ $\Rightarrow d = 1$ ou $d = 2$. Como os números de Fermat são ímpares tem-se que $d = 1$. ■

1.11 CRITÉRIOS DE DIVISIBILIDADE

Observe inicialmente que, como usamos um sistema de numeração de base 10, se um inteiro a é escrito como $a = a_k \cdot a_{k-1} \cdot \cdots \cdot a_1 \cdot a_0$. Então:

$$a = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \cdots + a_1 \cdot b + a_0 .$$

Por exemplo, se $a = 123$, então $a = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$.

Observação: Considerem n um número natural tal que: $n = abcde$.

Divisibilidade por 2: Temos que:

$$n = a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e.$$

Como 2|10, então para que 2 divida n devemos ter que:

$$2|e \Rightarrow e = 0, 2, 4, 6 \text{ ou } 8$$

Divisibilidade por 3 e 9:

$$n = a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e.$$

Faça: $10 = 9 + 1,\ 100 = 9 + 1,\ 1000 = 999 + 1,\ 10000 = 9999 + 1$

$$\Rightarrow n = a \cdot (9999 + 1) + b \cdot (999 + 1) + c \cdot (99 + 1) + d \cdot (9 + 1) + e$$

$$\Rightarrow\ (a + b + c + d + e) + 3 \cdot (3333a + 333b + 33c + 3d).$$

Para que n seja divisível por 3 devemos ter que: $(a + b + c + d + e)$ seja divisível por 3.

Critério análogo para a divisibilidade por 9.

Divisibilidade por 5:

$$n = a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10 + e$$

Para que 5 divida n devemos ter: $5|e \Longrightarrow e = 0$ ou $e = 5$.

Divisibilidade por 7:

Seja n um número natural tal que i seja o algarismo das unidades de n. Considere ainda o número natural k obtido de n retirando-se o algarismo i. Daí, podemos escrever:

$$n = 10k + i.$$

Teorema 20: $10k + i$ é divisível por 7 se, e somente se, $k - 2i$ é divisível por 7.

Demonstração: Suponha que $10k + i = 7 \cdot m$

$\Longrightarrow i = 7m - 10k$

$\Rightarrow k - 2i = k - 2 \cdot (7m - 10k) = k - 14m + 20k \Rightarrow 21k - 14m = 7 \cdot (3k - 2m)$

$\Rightarrow\ 7|(k - 2i)$.

$\Longleftarrow$ Suponha que $k - 2i = 7n$

$\Rightarrow\ k = 7n + 2i$

$\Rightarrow\ 10k + i = 10 = 10 \cdot (7n + 2i) + i = 70n + 20i + i = 70n + 21i = 7 \cdot (10n + 3i)$

$\Rightarrow\ 7|(10k + i)$. ■

1.12 CONGRUÊNCIA

Definição: Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$. Dizemos que a é congruente a b módulo m se $m|(a - b)$.

NOTAÇÃO: $a \equiv b\ (mod\ m)$

Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m e representamos $a \not\equiv b\ (mod\ m)$.

Proposição 4: $a, b, m \in \mathbb{Z}$ com $m > 0$. $a \equiv b\ (mod\ m) \iff \exists\ k \in \mathbb{Z}$ tal que $a = b + k \cdot m$.

Demonstração:

⇒ Suponha que $a \equiv b \ (mod\ m)$

$$\Rightarrow\ m|(a-b)\ \Rightarrow\ \exists\ k \in Z \text{ tal que } a-b=k\cdot m\ \Rightarrow a=b+k\cdot m.$$

⇐ Suponha que existe $k \in \mathbb{Z}$ com $a=b+k\cdot m$.

$$\Rightarrow\ a-b=k\cdot m\ \Rightarrow\ m|(a-b)\ \Rightarrow\ a\equiv b\ (mod\ m).$$ ■

Exemplo:

$8 \equiv 0\ (mod\ 2)$;

$10 \equiv 0\ (mod\ 2)$;

$13 \equiv 1\ (mod\ 2)$;

$155 \equiv 1\ (mod\ 2)$;

$8870 \equiv 0\ (mod\ 2)$.

Então:

(a) Se $a \in \mathbb{Z}$ e a é par, temos que $a \equiv 0\ (mod\ 2)$.

(b) Se $a \in \mathbb{Z}$ e a é ímpar, temos que $a \equiv 1\ (mod\ 2)$.

Proposição 5: $a, b, c, m \in \mathbb{Z}$ com $m > 0$. Então:

(1) $a \equiv a\ (mod\ m)$; reflexiva

(2) Se $a \equiv b\ (mod\ m)$ então $b \equiv a\ (mod\ m)$; simétrica

(3) Se $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$ então $a \equiv c\ (mod\ m)$ transitiva.

Demonstração:

(1) É claro que $m|(a-a)\ \Rightarrow\ a \equiv a\ (mod\ m)$.

(2) Se $a \equiv b\ (mod\ m)\ \Rightarrow\ a=b+k\cdot m\ \Rightarrow b=a+(-k)\cdot m\ \Rightarrow b \equiv a\ (mod\ m)$

(3) $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então:

$$a-b=k_1\cdot m \quad \text{e} \quad b-c=k_2\cdot m, \qquad k_1, k_2 \in \mathbb{Z}.$$

$$\begin{cases} a-b=k_1\cdot m \\ b-c=k_2\cdot m \end{cases} + a-c=(k_1+k_2)m\ \Rightarrow\ a \equiv c\ (mod\ m).$$ ■

Observação: Tal proposição garante que a congruência módula m é uma relação de equivalência (reflexiva + simétrica + transitiva).

Proposição 6: $a, b, c, m \in \mathbb{Z}$ com $m > 0$. Se $a \equiv b\ (mod\ m)$, então:

(1) $(a + c) \equiv (b + c)\ (mod\ m)$

(2) $(a - c) \equiv (b - c)\ (mod\ m)$

(3) $a \cdot c \equiv b \cdot c\ (mod\ m)$.

Demonstração:

(1) $a \equiv b\ (mod\ m) \Rightarrow\ a = b + k \cdot m, \quad k \in \mathbb{Z}$

$\Rightarrow\ (a + c) = (b + c) + km \Rightarrow\ (a + c) - (b + c) + km$

$\Rightarrow\ m|[(a + c) - (b + c)]\ \Rightarrow\ (a + c) \equiv (b + c)\ (mod\ m)$. ■

(2) Segue de forma análoga a *(1).*

(3) $a \equiv b\ (mod\ m)\ \Rightarrow\ a = b + k \cdot m, \quad k \in \mathbb{Z}$

$\Rightarrow a \cdot c = (b + km) \cdot c \Rightarrow a \cdot c = b \cdot c + (k \cdot c)m\ \Rightarrow a \cdot c \equiv b \cdot c\ (mod\ m)$. ■

Proposição 7: Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 0$. Se $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então:

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

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

(iii) $a \cdot c \equiv b \cdot d\ (mod\ m)$.

Demonstração:

(i) $a \equiv b\ (mod\ m) \Rightarrow\ a - b = k_1 \cdot m, \quad k_1 \in \mathbb{Z}$

$c \equiv d\ (mod\ m) \Rightarrow\ c - d = k_2 \cdot m, \quad k_2 \in \mathbb{Z}$

$\Rightarrow a - b + c - d = (k_1 + k_2) \cdot m \Rightarrow (a + c) - (c + d) = (k_1 + k_2) \cdot m$

$\Rightarrow (a + c) \equiv (b + d)\ (mod\ m)$.

(ii) Segue de forma análoga a *(i).*

(iii) $\begin{cases} a - b = k_1 \cdot m \\ c - d = k_2 \cdot m \end{cases} \Rightarrow \begin{cases} a = b + k_1 \cdot m \\ c = d + k_2 \cdot m \end{cases}$

$\Rightarrow ac = (b + k_1 m) \cdot (d + k_2 m) \Rightarrow ac = bd + bk_2 m + dk_1 m + k_1 k_2 m^2 \Rightarrow ac = bd + km$
$\Rightarrow a \cdot c \equiv b \cdot d \ (mod\ m)$. ■

Proposição 8: Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 0$. Se $ac \equiv bd \ (mod\ m)$, então:

$$a \equiv b \left(mod\ \left(\frac{m}{d}\right)\right), \text{onde } d = (c, m).$$

Demonstração: $ac \equiv bd \ (mod\ m)$

$$\Rightarrow\ ac - bc = km \Rightarrow\ c\ (a - b) = km\ (\div d) \Rightarrow \frac{c}{d}(a - b) = k \cdot \frac{m}{d}, \text{mas,} \left(\frac{c}{d}, \frac{m}{d}\right) = 1$$

e daí temos:

$$\frac{m}{d} | (a - b) \Rightarrow a \equiv b \left(mod\ \left(\frac{m}{d}\right)\right).$$

Exemplo: $24 \equiv 18\ (mod\ 3)$

$$\Rightarrow\ 12 \cdot 2 \equiv 9 \cdot 2\ (mod\ 3) \Rightarrow (2, 3) = 1 \Rightarrow\ 24 \equiv 9\ (mod\ 3).$$

Definição 1: Dizemos que k é um resíduo de h módulo m se $h \equiv k\ (mod\ m)$.

Definição 2: O conjunto de números inteiros $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo m se:

(i) $r_i \not\equiv r_j\ (mod\ m)$, se $i \neq j$;

(ii) $\forall\ n \in \mathbb{Z}$, tem-se que $n \equiv r_i\ (mod\ m)$ para algum $i = 1, \cdots, s$.

Exemplo 1: O conjunto $\{0, 1, 2, \cdots, m - 1\}$ forma um sistema completo de resíduos módulo m. De fato:

(i) $r_i = i$; para algum $i = o, \cdots, m - 1$. É claro que $r_i \not\equiv r_j\ (mod\ m)$, $|r_i - r_j| \leq m - 1$ para $i \neq j$

(ii) Seja $n \in \mathbb{Z}$. Pelo algoritmo de Euclides, existem q e r tais que:

$$n = q \cdot m + r, \text{ onde } 0 \leq r \leq m - 1$$

$$\Rightarrow n \equiv r_i \ (mod\ m), \text{ onde } r = r_j \text{ para algum } j = 0, \cdots, m - 1.$$

Exemplo 2: O conjunto $C = \{0, 1, 2, 3\}$ é um sistema completo de resíduos módulo 4. Vamos responder as seguintes perguntas:

(1) 15 é congruente a qual elemento do conjunto C?
Solução: $15 \equiv 3 \ (mod\ 4)$.

(2) 27 é congruente a qual elemento do conjunto C?
Solução: $27 \equiv 3 \ (mod\ 4)$.

(3) -5 é congruente a qual elemento do conjunto C?
Solução: $-5 \equiv 3 \ (mod\ 4)$.

Daí, tem-se que: $\overline{3} = \{a \in \mathbb{Z}: a \equiv 3 \ (mod\ 4)\}$

De forma análoga, temos: $\overline{0} = \{b \in \mathbb{Z}: b \equiv 0 \ (mod\ 4)\}$;

$$\overline{1} = \{c \in \mathbb{Z}: c \equiv 1 \ (mod\ 4)\};$$

$$\overline{2} = \{d \in \mathbb{Z}: d \equiv 2 \ (mod\ 4)\}.$$

Podemos então escrever: $\mathbb{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \overline{3}$.

Exemplo 3: Se $m \in \mathbb{Z}$ e m é impar então o conjunto:

$$C = \left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-3}{2}, \frac{m-2}{2}\right\}.$$

É um sistema completo de resíduos módulo m.

Solução: Vimos anteriormente que $\{0, 1, 2, \cdots, m - 1\}$ é um sistema completo de resíduos módulo m.

Logo, temos que:

$$-\frac{m-1}{2}+m=\frac{-m+1+2m}{2}=\frac{m+1}{2}$$
$$-\frac{m-3}{2}+m=\frac{-m+3+2m}{2}=\frac{m+3}{2}$$
$$\vdots$$
$$-1+m=m-1.$$

Teorema 21: Se $\{r_1, r_2, \cdots, r_s\}$ é um sistema completo de resíduos módulo m então $s = m$.

Demonstração: Considere o conjunto $\{t_0, t_1, \cdots, t_{m-1}\}$, onde $t_i = i$. Já provamos que tal conjunto é um sistema completo. Portanto $r_i \equiv t_j$, para algum i e algum j. Portanto $s \leq m$. Por outro lado, sendo $\{r_1, r_2, \cdots, r_s\}$ um sistema completo então cada $t_i \equiv r_j \ (mod\ m) \Rightarrow m \leq s$.

$$\therefore\ m = s. \qquad \blacksquare$$

Teorema 22: Seja $r_1, r_2, \cdots, r_m$ um sistema completo de resíduos módulo m. Se a e b são inteiros com $(a, m) = 1$, então: $ar_1 + b, ar_2 + b, \cdots, ar_m + b$, é um sistema completo de resíduos módulo m.

Demonstração: Pelo teorema anterior, basta provarmos que:

$$(ar_i + b) \not\equiv \left(ar_j + b\right) (mod\ m) \text{ se } i \neq j.$$

Suponha que $(ar_i + b) \not\equiv \left(ar_j + b\right) (mod\ m)$ se $i \neq j$.

$$ar_i + b = ar_j + b + k\,m, \quad k \in \mathbb{Z}$$
$$\Rightarrow ar_i \equiv ar_j (mod\ m)$$

$$\Rightarrow\ r_i \equiv r_j \left(mod\ \frac{m}{d}\right), \text{onde } d = (a, m) = 1 \Rightarrow r_i \equiv r_j (mod\ m), \text{ se } i \neq j \text{ (absurdo!)}$$

$\therefore ar_1 + b, ar_2 + b, \cdots, ar_m + b$ é um sistema completo de resíduos módulo m. $\blacksquare$

Proposição 9: Sejam a, b, m, $k \in \mathbb{Z}$, com $k > 0$. Se $a \equiv b\ (mod\ m)$, então:

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

Demonstração: Observem que:

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2} \cdot b + \cdots + b^{k-1}).$$

Como $m|(a-b)$, então $m|(a^k - b^k) \Rightarrow a^k \equiv b^k\ (mod\ m)$. ■

Teorema 23: Se $a \equiv b\ (mod\ m_1)$, $a \equiv b (mod\ m_2), \cdots, a \equiv b\ (mod\ m_k)$,com $m_1, m_2, \cdots, m_k > 0$, então $a \equiv b\ (mod\ [m_1, m_2, \ldots, m_k])$.

Demonstração: Temos que:

$m_1|(a-b)$, $m_2|(a-b), \cdots, m_k|(a-b)$, mas, pelo T.F.A., temos:

$m_i = p_1^{\propto_i,1} \cdot\ p_2^{\propto_i,2} \cdot \cdots \cdot\ p_r^{\propto_i,r}$, com $i = 1, \cdots, k$. Como $m_i|(a-b) \Rightarrow\ p_j^{\propto_i,j}|(a-b)$

$\Rightarrow\ p_j^{máx\{\propto_i,j\}}\ |(a-b)$.

Daí, temos que:

$$p_1^{máx\{\propto_i,j\}} \cdot p_2^{máx\{\propto_i,j\}} \cdot \cdots \cdot p_r^{máx\{\propto_i,j\}}\ |(a-b) \Rightarrow a \equiv b\ (mod\ [m_1, m_2, \cdots, m_k]).$$ ■

1.13 CONGRUÊNCIAS LINEARES

Definição: Uma congruência da forma $ax_0 \equiv b\ (mod\ m)$, onde a, $b \in \mathbb{Z}$ e x é uma variável, é chamada de congruência linear na variável x.

Observação 1: Uma solução de $ax_0 \equiv b\ (mod\ m)$ é um inteiro x_0 tal que: $ax_0 \equiv b\ (mod\ m)$.

Observação 2: Se x_0 é uma solução de $ax \equiv b\ (mod\ m)$ e $x_1 \in \mathbb{Z}$ é tal que $x_1 \equiv x_0\ (mod\ m)$, então x_1 também é solução de $ax \equiv b\ (mod\ m)$. De fato, como x_0 é solução $\Rightarrow$ $ax_0 \equiv b\ (mod\ m)$. Mas, temos: $x_1 \equiv x_0\ (mod\ m)\ \Rightarrow ax_1 \equiv ax_0\ (mod\ m) \equiv b\ (mod\ m) \Rightarrow$ x_1 é solução.

1.14 EQUAÇÃO DIOFANTINA

Definição: Uma equação da forma: $ax + by = c$, onde $a, b, c \in \mathbb{Z}$ é dita equação linear Diofantina nas variáveis x e y.

Teorema 24: Sejam $a, b, c, m \in \mathbb{Z}$ com $(a, b) = d$. Se $d \nmid c$ então a equação Diofantina $ax + by = c$ não possui nenhuma solução inteira, mas se $d|c$ então a mesma possui infinitas soluções. Mais ainda se x_0 e y_0 (x_0, y_0) é uma solução particular, então todas as soluções são da forma:

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

Demonstração: Sabemos que $d = (a, b) \Rightarrow d|a$ e $d|b$. Suponha que $d \nmid c$. Mas temos:

$$ax + by = c\ \Rightarrow (k_1 \cdot d)x + (k_2 \cdot d)y = c$$

$\Rightarrow d \cdot (k_1 x + k_2 y) = c \Rightarrow d|c$ (absurdo!). Portanto a equação não possui solução.

Suponha agora que $d|c$. Como $d = (a, b)$, então existem $n_0, m_0 \in \mathbb{Z}$ tais que:

$$n_0 a + m_0 b = d\ (*), \text{ como } d|c, \text{ então: } c = k \cdot d, \qquad k \in \mathbb{Z}.$$

De $(*)$, temos:

$$a \cdot (n_0 k) + b \cdot (m_0 k) = kd = c.$$

Tomando-se $x_0 = n_0 k$ e $y_0 = m_0 k,\ k \in \mathbb{Z}$, temos uma solução. Vamos provar então que:

$$x = x_0 + \frac{b}{d} \cdot k\ e\ y = y_0 - \frac{a}{d} \cdot k, \text{é uma solução da equação.}$$

De fato:

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

Seja (x, y) uma solução qualquer da equação Diofantina. Ou seja:

$$ax + by = c = ax_0 + by_0 \Rightarrow a(x - x_0) = b(y_0 - y) = 0 \quad (\div d)$$

$$\Rightarrow \frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)\ (**) \Rightarrow \frac{b}{d} \mid \frac{a}{d}(x - x_0).\ \text{Mas,}$$

$$\left(\frac{b}{d}, \frac{a}{d}\right) = 1 \Rightarrow \frac{b}{d} \mid (x - x_0).\ \exists\, k \in \mathbb{Z} \quad \text{tal que: } x - x_0 = \frac{b}{d} \cdot k \Rightarrow x = x_0 + \frac{b}{d} \cdot k$$

substituindo x em $(**)$, temos:

$$\frac{a}{d}\left(x_0 + \frac{b}{d} \cdot k - x_0\right) = \frac{b}{d}(y_0 - y) \Rightarrow \frac{ab}{d} \cdot k = b \cdot (y_0 - y) \Rightarrow y = y_0 - \frac{a}{d} \cdot k$$

Teorema 25: Sejam $a, b, m \in \mathbb{Z}$ com $m > 0$ e $d = (a, m)$. Se $d \nmid b$, então a congruência linear $ax \equiv b\ (mod\ m)$, não possui nenhuma solução inteira. Por outro lado, se $d \mid b$, então a congruência possui, exatamente d soluções incongruentes módulo m.

Demonstração: Se x é solução da congruência, então:

$$ax \equiv b\ (mod\ m) \Rightarrow \exists\, y \in \mathbb{Z}, \text{ tal que:}$$
$$ax = b + my \Rightarrow ax - my = b.$$

Pelo teorema anterior, se $d \nmid b$ a equação não possui nenhuma solução inteira, e portanto, a congruência também não possui soluções inteiras. Por outro lado, se $d \mid b$ então a equação diofantina possui infinitas soluções dadas por:

$$x = x_0 - \left(\frac{m}{d}\right) \cdot k \quad e \quad y = y_0 - \left(\frac{a}{d}\right) \cdot k, \qquad k \in \mathbb{Z}.$$

Daí, a congruência possui infinitas soluções dadas por:

$$x = x_0 - \left(\frac{m}{d}\right) \cdot k, \qquad k \in \mathbb{Z}.$$

Sejam x_1 e x_2 soluções da congruência, temos:

$$x_1 = x_0 - \left(\frac{m}{d}\right) \cdot k_1 \quad e \quad x_2 = x_0 - \left(\frac{m}{d}\right) \cdot k_2 .$$

Se $x_1 \equiv x_2 \ (mod\ m) \Rightarrow \left(x_0 - \left(\frac{m}{d}\right) \cdot k_1\right) \equiv \left(x_0 - \left(\frac{m}{d}\right) \cdot k_2\right) \ (mod\ m)$

$$\Rightarrow \frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \ (mod\ m) \Rightarrow k_1 \equiv k_2 \ (mod\ m), \qquad \text{pois : } \left(\frac{m}{d}, m\right) = \frac{m}{d} .$$

Daí as soluções incongruentes percorrem um sistema completo de resíduos módulo d, totalizando d soluções incongruentes. ■

Definição I: Uma solução x_0 de $ax \equiv b \ (mod\ m)$ é única se qualquer outra solução x_1 for congruênte a x_0 módulo m.

Definição II: Uma solução $\bar{a}$ de $ax \equiv 1 \ (mod\ m)$ é dita um inverso de a módulo m.

Observação: Se $(a, m) = 1$, então o inverso de a módulo m é único.

Proposição 10: Seja p um primo. O número inteiro a é seu próprio inverso módulo p se, e somente se, $a \equiv 1 \ (mod\ p)$ ou $a \equiv -1 \ (mod\ p)$.

Demonstração:

⇒ Suponha que a seja o seu próprio inverso. Então:

$$a \cdot a \equiv 1 \ (mod\ p) \Leftrightarrow a^2 \equiv 1 \ (mod\ p) \Leftrightarrow p|(a^2 - 1) \Leftrightarrow p|(a + 1) \cdot (a - 1) \Leftrightarrow$$
$$p|(a + 1) \text{ ou } p|(a - 1) \Leftrightarrow a \equiv 1 \ (mod\ p) \text{ ou } a \equiv -1 \ (mod\ p).$$ ■

Exemplo 2: Determine os elementos que são os seus próprios inversos módulo p, com p primo.

Solução: $1 \equiv 1\ (mod\ p)$e $6\ \equiv -1\ (mod\ p)$.

1.15 TEOREMA DE WILSON

Teorema 26 (Wilson): Se p é primo, então $(p-1)!\ \equiv -1\ (mod\ p)$.

Demonstração:

Como $(a,p) = 1$, com $1 \leq a \leq\ p-1$, então estes elementos possuem inversos únicos. Mas 1 e $p-1$ são os únicos que possuem inverso próprio. Daí, temos que existem $\frac{p-3}{2}$ pares, cada um congruente (em produto) a 1 módulo p. Daí, multiplicando-se estes produtos, temos:

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-2)\ \equiv 1\ (mod\ p) \Rightarrow 1 \cdot 2 \cdot 3 \cdot 4 \cdot \cdots \cdot (p-1) \equiv (p-1) \equiv -1(mod\ p)$$
$$\Rightarrow (p-1)! \equiv -1(mod\ p).$$ ■

Teorema 27: Se n é um inteiro e $(n-1)! \equiv -1(mod\ n)$ então n é primo.

Demonstração: Suponha que n não é primo. Então: $n = n \cdot s$, com $1 < r < n$ e $1 < s < n$.
$\Rightarrow r|(n-1)!$. Mas, por hipótese, tem-se que:

$$n|(n-1)! + 1\ \Rightarrow\ r|(n-1)! + 1 \Rightarrow \text{r|1 (Absurdo!) } (r > 1)$$
$$\therefore n \text{ é primo.}$$ ■

1.16 TEOREMA DE FERMAT

Teorema 28 (Fermat): Se p é primo e a é um inteiro com $p \nmid a$, então $a^{p-1} \equiv 1\ (mod\ p)$.

Demonstração: Qualquer subconjunto com p elementos incongruentes pode ser colocado em correspondência biunívoca com o conjunto $\{0, 1, 2, \cdots, \mathrm{p}-1\}$.

Considere o conjunto:

$$\{a, 2a, 3a, \cdots (p-1)a\}.$$

Note que $ia \not\equiv ja\ (mod\ p)$ se $i \neq j$. De fato, se $ia \equiv ja\ (mod\ p)$

$$\Rightarrow i \equiv j\ (mod\ m),\ 1 \leq i \leq p-1 \text{ e } 1 \leq j \leq p-1 \Rightarrow i \equiv j.$$

Note ainda que nenhum dos elementos da forma $ia\ (1 \leq i \leq p-1)$ é côngruo a o módulo p. Daí $i \cdot a$ é congruente a exatamente um elemento do conjunto:

$\{0, 1, 2, \cdots, p-1\}$. Multiplicando-se temos:

$$a \cdot 2a \cdot 3a \cdot \cdots \cdot (p-1)a \equiv (p-1)!\ (mod\ p) \Rightarrow (p-1)! \cdot a^{p-1} \equiv (p-1)!\ (mod\ p).$$

Mas, $\big((p-1)!, p\big) = 1$ então: $a^{p-1} \equiv 1\ (mod\ p)$. ■

1.17 A FUNÇÃO **Φ** DE EULER

Definição I: Se n é um inteiro positivo, então a função Φ de Euler, denotada por $\Phi(n)$ é definida como:

$$\Phi(n) = \#\ \{a \in \mathbb{Z} : 1 \leq a \leq n \quad \text{e} \quad (a, n) = 1\}.$$

Exemplo: Se p é primo. Calcule $\Phi(\mathrm{p})$.

$\Phi(p) = p - 1$.

Definição II: Um sistema reduzido de resíduos módulo m é um conjunto de $\Phi(m)$ inteiros $r_1, r_2, \cdots, r_{\Phi(m)}$, tais que:

(i) $\big(r_{i,m}\big) = 1, 1 \leq i \leq \Phi(m)$;

(ii) $r_i \not\equiv r_j\ (mod\ m)$, se $i \neq j$.

Teorema 29: Seja m um inteiro positivo e a um inteiro com $(a, m) = 1$. Se $r_1, r_2, \cdots, r_{\Phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \cdots, ar_{\Phi(m)}$ também o é.

Demonstração: Observem que $\# \{ar_1, ar_2, \cdots, ar_{\Phi(m)}\} = \Phi(m)$. Vamos provar que:

(i) $(ar_i, m) = 1$
(ii) $ar_i \not\equiv ar_j \ (mod\ m)$ se $i \neq j$.

Prova de *(i):* Seja $d = (ar_i, m)$. Daí, temos:

$$d|ar_i \text{ e } d|m. \text{ Por outro lado sabemos que: } (a, m) = 1 = (r_i, m).$$

Portanto temos: $ax + my = 1 \quad x(r_1) \quad \text{e} \quad r_i s + mt = 1$

$$\Rightarrow (ar_i)x + m(r_i y) = r_i \Rightarrow d|r_i \text{ . Como } d|m \text{ e } d|r_i \Rightarrow d|1$$

(ii) $ar_i \equiv ar_j (mod\ m) \Rightarrow r_i \equiv r_j (mod\ m) \Rightarrow i = j$, pois, $r_1, \cdots, r_{\Phi(m)}$ é um sistema reduzido. ■

1.18 TEOREMA DE EULER

Teorema 30 (Euler): Se m é um inteiro positivo e a é um inteiro tal que $(a, m) = 1$, então:

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

Demonstração: Seja $\{r_1, r_2, \cdots, r_{\Phi(m)}\}$ um sistema reduzido de resíduos módulo m. Como $(a, m) = 1$, temos pelo teorema anterior que: $\{ar_1, ar_2, \cdots, ar_{\Phi(m)}\}$ também é um sistema reduzido de resíduos módulo m. Daí, cada ar_i é congruente a um só r_j módulo m. Multiplicando-se estas congruências, temos:

$ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\Phi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\Phi(m)} (mod\ m)$
$\Rightarrow a^{\Phi(m)} \cdot r_1 \cdot r_2 \cdot \cdots \cdot r_{\Phi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\Phi(m)} (mod\ m)$. Mas, $(r_1 \cdot r_2 \cdot \cdots \cdot r_{\Phi(m)},\ m) = 1$.

Portanto: $a^{\Phi(m)} \equiv 1 (mod\ m)$. ■

1.19 TEOREMA CHINÊS DO RESTO

Se a_i, m_i são inteiros $(i = 1, \cdots, r)$ tais que $(a_i, m_i) = 1$ e $(m_i, m_j) = 1$ para $i \neq j$ e c_i é inteiro, então o sistema:

$$\begin{cases} a_1 x \equiv c_1 (mod\ m_1) \\ a_2 x \equiv c_2 (mod\ m_2) \\ \vdots \\ a_r x \equiv c_r (mod\ m_r) \end{cases}$$

Possui solução única módulo (m), onde $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Demonstração: Como $(a_1, m_1) = 1$, então a congruência $a_i x \equiv c_i (mod\ m_i)$ possui solução única b_i.

$$\text{Tome } y_i = \frac{m}{m_i}; \text{ onde } m = m_1 \cdot m_2 \cdot \cdots \cdot m_r \Rightarrow (y_i, m_i) = 1, \text{então a congruência:}$$

$$y_i x \equiv 1 (mod\ m_i) \text{ tem solução única } \overline{y_i}\ .$$

Tome: $x = b_1 \cdot y_1 \cdot \overline{y_1} + b_2 \cdot y_2 \cdot \overline{y_2} + \cdots + b_r \cdot y_r \cdot \overline{y_r}$.

Afirmação: x é solução do sistema.

$$\begin{aligned} a_i x = a_i \cdot b_1 \cdot y_1 \cdot \overline{y_1} + \cdots + a_i \cdot b_i \cdot y_i \cdot \overline{y_1} + \cdots + a_r \cdot b_r \cdot y_r \cdot \overline{y_r} &\equiv a_i \cdot b_i \cdot y_i \cdot \overline{y_i} (mod\ m_i) \\ &\equiv a_i \cdot b_i (mod\ m_i) \\ &\equiv c_i (mod\ m_i) \end{aligned}$$

1.20 O PRINCÍPIO DA CASA DOS POMBOS

O Princípio da Casa dos Pombos nos diz que para colocarmos $n + 1$ pombos em n gaiolas, pelo menos uma gaiola deverá conter pelo menos dois pombos. Esta ideia tão óbvia é, na realidade, uma poderosa ferramenta na demonstração de muitos resultados bastante difíceis. O que, muitas vezes, torna o problema difícil é a construção de um conjunto ou conjuntos aos quais se possa aplicar esse princípio.

Este princípio é também conhecido como “Princípio das Gavetas de Dirichlet” por ter sido por ele enunciado como: “Se $n + 1$ objetos são colocados em n gavetas, então pelo menos uma gaveta deverá conter, pelo menos, dois objetos”.

Exemplo: Mostrar que numa festa de aniversário com mais de 12 crianças, existem pelo menos duas nascidas no mesmo mês e que também existem pelo menos duas nascidas no mesmo dia da semana.

Solução:

Como temos mais crianças (pombos) do que meses (gaiolas), pelo menos um “mês” deverá conter pelo menos duas “crianças”. Na segunda parte, sendo o número de crianças maior do que 7, necessariamente duas ou mais terão nascido no mesmo dia da semana.

CAPÍTULO 2

2 ANÉIS, DOMÍNIO DE INTEGRIDADE E CORPO

Definição*:* Seja um conjunto não vazio A, munido das operações:

$$\textbf{Adição: } +: A\ x\ A \longrightarrow A$$
$$(a,b) \longmapsto a+b$$
$$\textbf{Multiplicação: } \cdot: A\ x\ A \longrightarrow A$$
$$(a,b) \longmapsto a \cdot b.$$

Diremos que $(A,+,\cdot)$ é um anel quando satisfaz as seguintes condições:

(1) " $+$ " Comutativo

$\forall\ a,b \in A, \qquad a+b=b+a.$

(2) "$+$" Associativo

$\forall\ a,b,c \in A, \qquad (a+b)+c=a+(b+c).$

(3) Elemento neutro aditivo

$\exists\ 0 \in A$ tal que: $\qquad 0+a=a+0=a, \qquad \forall a \in A.$

(4) Oposto aditivo

Para cada $a \in A$, existe $b \in A$ tal que: $\qquad a+b=b+a=0.$

Notação: $b=-a.$

(5) " $\cdot$ " Associativo

$\forall\ a,b,c \in A \qquad (a \cdot b) \cdot c = a \cdot (b \cdot c).$

(6) Distributiva à direita e à esquerda

$\forall\ a,b,c \in A \qquad a \cdot (b+c) = a \cdot b + a \cdot c$

$(a+b) \cdot c = a \cdot c + b \cdot c.$

Observações:

(I) Seja $(A, +, \cdot)$ um anel.

$$\text{Se } a \cdot b = b \cdot a; \qquad \forall\, a, b \in A.$$

Diremos que é um anel comutativo**.**

(II) Se existe $1 \in A$ tal que:

$$1 \cdot a = a \cdot 1 = a; \qquad \forall\, a \in A.$$

Diremos que o anel possui unidade, ou ainda, que $(A, +, \cdot)$ é um anel com unidade 1**.**

(III) Sejam $a, b \in A$, tais que:

$$a \cdot b = 0 \Rightarrow a = 0 \text{ ou } b = 0.$$

Diremos então que $(A, +, \cdot)$ é um anel sem divisores zeros.

(IV) Um anel $(A, +, \cdot)$ comutativo, com unidade e sem divisores zeros é dito **DOMÍNIO DE INTEGRIDADE.**

(V) Se um domínio de integridade $(A, +, \cdot)$ satisfaz: $\forall x \in A, x \neq 0, \exists\, y \in A$ tal que:

$$x \cdot y = y \cdot x = 1.$$

Diremos então que $(A, +, \cdot)$ é um **CORPO**.

2.1 O ANEL $\mathbb{Z}[\sqrt{d}\,]$

O objetivo desta seção é examinar algumas propriedades do anel $\mathbb{Z}[\sqrt{d}\,]$. Vamos denotar por $R = \mathbb{Z}[\sqrt{d}\,]$ o conjunto:

$$R = \{x + y\sqrt{d} : \ x, y \in \mathbb{Z}\}.$$

É fácil verificar que R munido com as operações de adição

$$\left(x_1 + y_1\sqrt{d}\right) + \left(x_2 + y_2\sqrt{d}\right) = (x_1 + x_2) + (y_1 + y_2)\sqrt{d}$$

e de multiplicação

$$\left(x_1 + y_1\sqrt{d}\right) \cdot \left(x_2 + y_2\sqrt{d}\right) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d}$$

é um domínio de integridade.

Sejam $n \in \mathbb{N}$ e $\alpha = x + y\sqrt{d} \in R$ com $x, y \in \mathbb{Z}$. Dizemos que n divide α se n divide x e y. Neste caso, denotaremos por:

$$\alpha \equiv 0 \pmod{n}.$$

Em particular, se $\alpha, \beta \in R$, dizemos que:

$$\alpha \equiv \beta \pmod{n} \Leftrightarrow \alpha - \beta \equiv 0 \pmod{n}.$$

Um elemento $\alpha \in R$ é chamado uma *unidade* de R se existir $\beta \in R$ tal que $\alpha\beta = \beta\alpha = 1$ ou, equivalentemente, α divide 1. Denotaremos por $U(R)$ o conjunto de todas as unidades de R.

Seja $\alpha = x + y\sqrt{d} \in R$ com $x, y \in \mathbb{Z}$, o *conjugado* de α, denotado por α^*, é definido como:

$$\alpha^* = x - y\sqrt{d}.$$

A *norma* de α, denotada por $N(\alpha)$, é definida como:

$$N(\alpha) = \alpha\alpha^*.$$

Note que, se $\alpha = x + y\sqrt{d} \in R$ com $x, y \in \mathbb{Z}$, então:

$$N(\alpha) = \alpha\alpha^* = \left(x + y\sqrt{d}\right)\left(x - y\sqrt{d}\right) = x^2 - dy^2.$$

Em particular, se $\alpha \neq 0$, então:

$$\alpha^{-1} = \frac{1}{N(\alpha)}\alpha^* = \frac{x}{x^2 - dy^2} - \frac{y}{x^2 - dy^2}\sqrt{d}$$

é um elemento de R se $x^2 - dy^2$ divide x e y. É claro que:

$$N(\alpha\beta) = (\alpha\beta)(\alpha\beta)^* = (\alpha\beta)(\alpha^*\beta^*) = (\alpha\alpha^*)(\beta\beta^*) = N(\alpha)N(\beta), \forall\, \alpha, \beta \in R.$$

Além disso, sejam $\alpha, \beta \in R$. Então:

$$N(\alpha) = N(\beta) \Leftrightarrow \beta = \omega\alpha, \text{ onde } \omega \in U(R).$$

CAPÍTULO 3

3 EQUAÇÃO DE PELL

Neste capítulo estudaremos um caso particular da equação de Pell: $x^2 - dy^2 = N$, ou seja, estudaremos as soluções da equação: $x^2 - dy^2 = 1$, onde $x, y \in \mathbb{Z}$ e $d \in \mathbb{N} - \{1\}$ livre de quadrados.

Na teoria das equações Diofantinas, a equação de Pell é essencial, pois diversas equações podem ser reduzidas a ela, por exemplo, determinar as soluções inteiras da equação quadrática geral:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

onde $a, b, c, d, e, f \in \mathbb{Z}$. Note que essa equação pode ser reescrita sob a forma

$$ax^2 + (by + d)x + cy^2 + ey + f = 0.$$

Assim, se essa equação tem uma solução para algum $y \in \mathbb{Z}$ fixado, então o discriminante:

$$(by + d)^2 - 4a(cy^2 + ey + f) = b^2 - 4ac)y^2 + (2bd - 4ae)y + d^2 - 4af.$$

Deve ser um quadrado perfeito, digamos z^2. Assim, fazendo

$$p = b^2 - 4ac, \qquad q = 2bd - 4ae \qquad \text{e} \qquad r = d^2 - 4af,$$

obtemos

$$py^2 + qy + r - z^2 = 0.$$

Novamente, o discriminante dessa equação quadrática em y deve ser um quadrado perfeito, digamos:

$$q^2 - 4p(r - z^2) = w^2.$$

Portanto, temos que considerar a equação de Pell

$$w^2 - 4pz^2 = q^2 - 4pr.$$

Assim, conhecendo as soluções dessa equação, podemos de qualquer modo, obtermos as soluções racionais da equação quadrática original.

3.1 SOLUÇÕES DA EQUAÇÃO DE PELL

Nesta seção apresentaremos as soluções da equação de Pell

$$x^2 - dy^2 = 1.$$

Seja $d \in \mathbb{Z}$. Dizemos que d é livre de quadrados ou não é um quadrado perfeito se ele não for divisível pelo quadrado de nenhum número inteiro maior do que 1. Todo $n \in \mathbb{N}$ pode ser escrito sob a forma:

$$n = c^2 d,$$

onde d livre de quadrados. De fato, sabemos que todo $n \in \mathbb{N}$ pode ser fatorado de modo único, a menos da ordem dos fatores, sob a forma:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_m^{r_m},$$

onde $p_1 < p_2 < \cdots < p_m$ são números primos e $r_i \in \mathbb{N} \cup \{0\}$. Como $r_i = 2s_i + t_i$, onde $t_i = 0$ ou $t_i = 1$, temos que:

$$n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_n^{r_n} = p_1^{2s_1+t} \cdot p_2^{2s_2+t} \cdot \cdots \cdot p_m^{2s_m+t} = c^2 d$$

onde:

$$c = p_1^{s_1} \cdot p_2^{s_2} \cdot \cdots \cdot p_m^{s_m} \qquad \text{e} \qquad d = p_1^{t_1} \cdot p_2^{t_2} \cdot \cdots \cdot p_m^{t_m}.$$

Note que:

1. Se $d \in \mathbb{N}$ livre de quadrados, então $\sqrt{d}$ é irracional.
2. Se $\sqrt{d}$ é racional, então $\sqrt{d}$ é inteiro.

Agora trataremos os casos triviais da equação de Pell $x^2 - dy^2 = 1$.

- Se $d < -1$, então:

$$1 = x^2 - dy^2 = x^2 + |d|\, y^2 \geq |d|\, y^2 \geq 0.$$

Logo, devemos ter:

$$x = \pm 1 \quad \text{e} \quad y = 0.$$

De fato, pois:

$$d < -1 \Rightarrow |d| > 1$$

- Se $d = -1$, então $x^2 + y^2 = 1$. Logo, devemos ter:

$$x = \pm 1 \quad \text{e} \quad y = 0; \quad x = 0 \quad \text{e} \quad y = \pm 1$$

Observem que se $d = -1$, temos um circunferência de raio 1.

- Se $d = a^2 > 0$, então:

$$x^2 - dy^2 = x^2 - a^2y^2 = (x + ay)(x - ay) = 1.$$

É claramente possível se

$$(x + ay) = (x - ay) = \pm 1.$$

Neste caso:

$$x = \frac{(x + ay) + (x - ay)}{2} = \pm 1 \quad \text{e} \quad y = 0.$$

- Se $d = 0$, então $x^2 = 1$. Logo, $x = \pm 1$ e y é arbitrário.

Finalmente, se $d > 0$ é livre de quadrados, então a equação de Pell tem certamente as soluções:

$$x = \pm 1 \quad \text{e} \quad y = 0.$$

Nosso objetivo, agora, é provar que a equação de Pell, além dessas soluções, tem mais um número infinito de soluções. Note que, se o par (x, y) é uma solução da equação de Pell com $xy \neq 0$, então os pares $(-x, y), (x, -y)$ e $(-x, -y)$ também o são. Assim, basta determinar as soluções no primeiro quadrante, isto é, $x > 0$ e $y > 0$. Além disso, a equação de Pell pode ser escrita sob a forma:

$$x - y\sqrt{d} = y\left(\frac{x}{y} - \sqrt{d}\right) = \frac{1}{x + y\sqrt{d}}.$$

Lema 1: Seja $d \in \mathbb{N} - \{1\}$ livre de quadrados. Então, para cada $n \in \mathbb{N}$, existem $x, y \in \mathbb{N}$, tais que:

$$0 < \left|x - y\sqrt{d}\right| < \frac{1}{n} \leq \frac{1}{y}.$$

Prova: Para cada $x \in \mathbb{R}$, temos que:

$$x - \lfloor x \rfloor \in [1, 0), \text{onde } \lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leq x\}.$$

Assim, os $n + 1$ números reais distintos, pois $\sqrt{d}$ é irracional,

$$0, \sqrt{d} - \lfloor \sqrt{d} \rfloor, \cdots, n\sqrt{d} - \lfloor n\sqrt{d} \rfloor \tag{1}$$

pertencem ao intervalo $[0, 1)$. Agora, consideremos a partição de $[0, 1)$ sob a forma:

$$[0, 1) = \bigcup_{k=0}^{n-1} \left[\frac{k}{n}, \frac{k+1}{n}\right). \tag{2}$$

É claro que, pelo menos, dois dos reais em (1) estejam em um mesmo intervalo em (2) (Princípio da Casa do Pombo ou dos Escaninhos), digamos.

$$k_1\sqrt{d} - \lfloor k_1\sqrt{d} \rfloor \quad \text{e} \quad k_2\sqrt{d} - \lfloor k_2\sqrt{d} \rfloor, \qquad com\ 0 \leq k_1 < k_2 \leq n.$$

Então:

$$\left|(k_2 - k_1)\sqrt{d} - \left(\lfloor k_2\sqrt{d}\rfloor - \lfloor k_1\sqrt{d}\,\rfloor\right)\right| < \frac{1}{n}.$$

Assim existem:

$$x = \lfloor k_2\sqrt{d}\rfloor - \lfloor k_1\sqrt{d}\,\rfloor, \qquad \mathrm{y} = k_2 - k_1 \in \mathbb{N}$$

tais que:

$$\left|x - y\sqrt{d}\right| < \frac{1}{n}, \text{ pois d} \geq 2.$$

Como $0 \leq k_2 - k_1 \leq k_2 \leq n$, temos que:

$$\frac{1}{n} \leq \frac{1}{y}.$$

Portanto,

$$\left|x - y\sqrt{d}\right| < \frac{1}{n} \leq \frac{1}{y}\ .$$

■

Lema 2: Seja $d \in \mathbb{N} - \{1\}$ livre de quadrados. Então existe um número infinito de pares $(x, y) \in \mathbb{N} \times \mathbb{N}$, tais que:

$$0 < \left|x - y\sqrt{d}\right| < \frac{1}{y} \qquad \text{e} \qquad 0 < |x^2 - dy^2| < 1 + 2\sqrt{d}.$$

Prova: Suponhamos, por absurdo, que exista um número finito de pares:

$$(x_1,\ y_1), \cdots, (x_k,\ y_k) \in \mathbb{N} \times \mathbb{N}$$

tais que:

$$\left|x_j - y_j\sqrt{d}\right| < \frac{1}{y_j} \qquad \text{e} \qquad x_j^2 - dy_j^2 < 1 + 2\sqrt{d}, \mathrm{j} = 1, \cdots, \mathrm{k}.$$

Tomando:

$$\delta = min\left\{\left|x_j - y_j\sqrt{d}\right|, \mathrm{j} = 1, \cdots, \mathrm{k}\right\} \in \mathbb{R},$$

temos que existe $m \in \mathbb{N}$ tal que $0 < \frac{1}{m} < \delta$, pois $\mathbb{R}$ é Arquimediano. Pelo Lema 1, existem $x, y \in \mathbb{N}$ tais que:

$$\left|x - y\sqrt{d}\right| < \frac{1}{m} \leq \frac{1}{y} \qquad \text{e} \qquad |x^2 - dy^2| < 1 + 2\sqrt{d},$$

pois:

$$|x^2 - dy^2| = \left|x - y\sqrt{d}\right|\left|x + y\sqrt{d}\right| \quad \text{e} \quad \left|x + y\sqrt{d}\right| \leq \left|x - y\sqrt{d}\right| + \left|2y\sqrt{d}\right| < \frac{1}{y} + 2y\sqrt{d}$$

implicam que:

$$|x^2 - dy^2| < \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{d}\right) = \frac{1}{y^2} + 2\sqrt{d} \leq 1 + 2\sqrt{d}.$$

Como $\frac{1}{m} < \delta$ temos que $(x, y) \neq (x_j, y_j), j = 1, \cdots, \text{k}$, o que é uma contradição. ■

Corolário 1: Seja $d \in \mathbb{N} - \{1\}$ livre de quadrados. Então existe um $r \in \mathbb{R} - \{0\}$ (dependendo de d) tal que a equação:

$$x^2 - dy^2 = r$$

tenha um número infinito de soluções $(x, y) \in \mathbb{N}$ x $\mathbb{N}$. ■

Lema 3: Seja $d \in \mathbb{N} - \{1\}$ livre de quadrados. Então a equação de Pell $x^2 - dy^2 = 1$, tem uma solução não nula $(x, y) \in \mathbb{N}$ x $\mathbb{N}$ com $(x, y) \neq (1, 0)$.

Prova: Pelo corolário1, existe pelo menos um $r \in \mathbb{R}$ que corresponde a um número infinito de pares $(x, y) \in \mathbb{N}$ x $\mathbb{N}$ tais que:

$$|x^2 - dy^2| = r, \text{ com } 0 < r < 1 + 2\sqrt{d}.$$

Assim, para pelo menos um dos números $\varepsilon \in \{-1, 1\}$, existe um número infinito de pares $(x, y) \in \mathbb{N}$ x $\mathbb{N}$ tais que:

$$x^2 - dy^2 = \varepsilon r.$$

Como existem somente r^2 restos módulo r,

$$x \equiv 0, 1, \cdots, (r-1)\ (mod\ r) \quad \text{e} \quad y \equiv 0, 1, \cdots, (r-1)\ (mod\ r),$$

temos, pelo princípio da Casa do Pombo ou dos Escaninhos, que existem duas soluções diferentes $(x_1,\ y_1),\ (x_2,\ y_2) \in \mathbb{N}$ x $\mathbb{N}$ tais que:

$$x_1^2 - dy_1^2 = \varepsilon r, \qquad x_2^2 - dy_2^2 = \varepsilon r, \qquad x_1 \equiv x_2\ (mod\ r) \quad \text{e} \quad y_1 \equiv y_2\ (mod\ r).$$

Então:

$$\alpha = \frac{x_1x_2 - dy_1y_2}{r}, \qquad \beta = \frac{x_2y_1 - x_1y_2}{r} \quad \in \mathbb{Z},$$

pois:

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv r \equiv 0\ (mod\ r) \quad \text{e} \quad x_2y_1 - x_1y_2 \equiv x_1y_1 - x_1y_1 \equiv 0\ (mod\ r).$$

Logo:

$$\left(x_1 + y_1\sqrt{d}\right)\left(x_2 - y_2\sqrt{d}\right) = r\left(\alpha + \beta\sqrt{d}\right). \tag{3}$$

Tomando a conjunção na equação (3), obtemos:

$$\left(x_1 - y_1\sqrt{d}\right)\left(x_2 + y_2\sqrt{d}\right) = r\left(\alpha - \beta\sqrt{d}\right). \tag{4}$$

Multiplicando membro a membro as equações (3) e (4), temos que:

$$r^2(\alpha^2 - d\beta^2) = (x_1^2 - dy_1^2)\ (x_2^2 - dy_2^2) = (\varepsilon r)\ (\varepsilon r) = \varepsilon^2 r^2 = r^2.$$

Assim,

$$\alpha^2 - d\beta^2 = 1.$$

Portanto, o par $(|\alpha|, |\beta|) \in \mathbb{N}$ x $\mathbb{N}$ é uma solução da equação de Pell.

Afirmação. $\beta \neq 0$.

De fato, se $\beta = 0$, então:

$$\frac{x_1}{x_2} = \frac{y_1}{y_2} = k > 0,$$

de modo que:

$$\varepsilon r = x_1^2 - dy_1^2 = k^2(x_2^2 - dy_2^2) = k^2 \varepsilon r \Rightarrow k^2 = 1 \Rightarrow k = 1.$$

Logo, $(x_1, y_1) = (x_2, y_2)$, o que é uma contradição. ■

Determinar as soluções da equação $x^2 - dy^2 = r$, significa determinar os elementos $\alpha = x + y\sqrt{d} \in R$ tais que $N(\alpha) = r$.

Se $\alpha = x + y\sqrt{d} \in R$ com $x, y \in \mathbb{Z}$, é uma solução da equação $N(\alpha) = \alpha\alpha^* = x^2 - dy^2 = 1$, então os números reais:

$$\alpha, \quad \frac{1}{\alpha}, \quad -\alpha \quad \text{e} \quad -\frac{1}{\alpha}$$

são também soluções da equação e satisfazem:

$$\begin{array}{cc} \alpha > 1 & \text{se } x > 0 \text{ e } y > 0 \\ 0 < \alpha < 1 & \text{se } x > 0 \text{ e } y < 0 \\ \alpha < -1 & \text{se } x < 0 \text{ e } y < 0 \\ -1 < \alpha < 0 & \text{se } x < 0 \text{ e } y > 0. \end{array}$$

Por exemplo, se $x > 0$ e $y > 0$, então:

$$\alpha = x + y\sqrt{d} > y \geq 1.$$

Lema 4 Sejam $(x_1, y_1), (x_2, y_2) \in \mathbb{N} \times \mathbb{N}$ soluções da equação de Pell, x e y a serem determinados por:

$$\left(x_1 + y_1\sqrt{d}\right) \cdot \left(x_2 + y_2\sqrt{d}\right) = x + y\sqrt{d}.$$

Então (x, y) é, também, uma solução da equação de Pell.

Prova. Sejam $\alpha = \left(x_1 + y_1\sqrt{d}\right)$ e $\beta = \left(x_2 + y_2\sqrt{d}\right)$. Então:

$$N(\alpha\beta) = N(\alpha)N(\beta) = 1 \cdot 1 = 1,$$

é uma solução. ■

Pelo Lema 3, existe $\alpha \in R$ tal que $\alpha > 1$ e $N(\alpha) = 1$ e, o Lema 4, mostra que todas as potências α^n, para todo $n \in \mathbb{N}$, são soluções da equação de Pell, pois:

$$N(\alpha^n) = N(\alpha)^n = 1^n = 1, \forall\, n \in \mathbb{N}.$$

Note que:

$$\cdots < \alpha^{-n} < \cdots < \alpha^{-1} < \alpha < \alpha^2 < \alpha^3 < \cdots < \alpha^n < \cdots$$

são todas distintas.

Teorema 1 Sejam $d \in \mathbb{N} - \{1\}$ livre de quadrados e $R = \mathbb{Z}\left[\sqrt{d}\,\right]$.

Se $d > 0$, então:

$$U(R) = \{\pm\omega^n : \ n \in \mathbb{Z}\},$$

onde ω é a unidade fundamental de R com $\omega > 1$, isto é, ω é a menor unidade de R com $\omega > 1$ e $N(\omega) = 1$.

Prova. Vamos provar apenas o item (4), para os elementos $\alpha = \left(x + y\sqrt{d}\right) \in R$ tais que $N(\alpha) = 1$. Já vimos que os números reais:

$$\alpha^n, \qquad \frac{1}{\alpha^n}, \qquad -\alpha^n \qquad \text{e} \qquad -\frac{1}{\alpha^n}$$

são soluções da equação $N(\alpha) = x^2 - dy^2 = 1$ e que diferem unicamente nas coordenadas x e y de α. Logo, basta mostrar que todo $\alpha \in R$ tal que $\alpha > 1$ e $N(\alpha) = 1$ pode ser escrito sob a forma:

$$\alpha = \omega^n, \text{ onde } n \in \mathbb{N}$$

e ω é a menor unidade de R com $\omega > 1$ e $N(\omega) = 1$, pois $\mathbb{N}$ é um conjunto discreto. Como $\alpha > 1$ temos, pela minimalidade de ω, que existe um $n \in \mathbb{N}$ tal que:

$$\omega^n \leq \alpha < \omega^{n+1},$$

pois

$$[1, \infty) = \bigcup_{n \in \mathbb{N}} [\omega^{n-1},\ \omega^n).$$

Agora,

$$\frac{\alpha}{\omega^n} = \alpha\omega^{-n} \in R \; e \; N\left(\frac{\alpha}{\omega^n}\right) = 1.$$

Assim, $\beta = \alpha\omega^{-n}$ é uma solução da equação de Pell com:

$$1 \leq \beta < \omega.$$

Logo, pela definição de ω, não podemos ter $1 < \beta < \omega$. Portanto, $\beta = 1$ e $\alpha = \omega^n$. ■

3.2 APLICAÇÃO

Encontrar todas as soluções inteiras do sistema abaixo:

$$\begin{cases} n - 1 = x^2 \\ \frac{n}{2} - 1 = y^2 \end{cases} \qquad n,\ x,\ y \in \mathbb{N}.$$

***Solução*:** Podemos escrever o sistema da seguinte forma:

$$\begin{cases} n = x^2 + 1 \\ n = 2y^2 + 2 \end{cases} \Rightarrow x^2 + 1 = 2y^2 + 2 \Rightarrow x^2 - 2y^2 = 1$$

e agora temos que considerar a equação de Pell: $x^2 - 2y^2 = 1$, pois conhecendo as soluções dessa equação, poderemos de qualquer forma, obter as soluções naturais para o sistema. Percebam que as soluções positivas dessa equação são pares da forma (x_r, y_r) onde: $x_r + y_r\sqrt{d} = (x_1 + y_1\sqrt{d})^r$ com $r = 1, 2, 3, \cdots$, e o par (3, 2) é solução primitiva dessa equação, portanto, as demais soluções serão da forma: $x_r + y_r\sqrt{2} = (3 + 2\sqrt{2})^r$ com $r = 1, 2, 3, \cdots$.

Se $r = 2$, temos:

$$x_2 + y_2\sqrt{2} = (3 + 2\sqrt{2})^2 = (17 + 12\sqrt{2})$$
$$\Rightarrow x_2 = 17 \quad \text{e} \quad y_2 = 12$$

logo: (17, 12) também é solução e, consequentemente $n = 290$, pois:

$$n = x^2 + 1 \Rightarrow n = 289 + 1 = 290.$$

Portanto o sistema possui infinitas soluções.

CONSIDERAÇÕES FINAIS

Durante séculos a equação de Pell foi motivo de muita discussão e apreciação por grande parte dos matemáticos que dedicaram suas vidas ao estudo dessa ciência, portanto ao estudá-la, percebemos seu imenso valor na teoria das equações diofantinas e sua fundamental importância na resolução de outras equações, que ao serem reduzidas, recaem no modelo da equação de Pell.

Este trabalho é fruto de muita determinação, paciência, investigação e pesquisas a diversos livros de matemática. Acolher o desafio de estudar mais a fundo um caso particular de uma equação tão antiga não foi nada fácil, pois apesar de produzir resultados aparentemente simples, sua demonstração é rica em detalhes que necessitam de um estudo sério em teoria dos números e estruturas algébricas. Uma característica marcante desse trabalho foi à perseverança em vencer os obstáculos, pois isto nos motivou a estudar cada vez mais.

Esperamos que este trabalho sirva de apoio a um estudo mais intenso sobre soluções da equação de Pell, e que o mesmo sirva de base para uma aprendizagem mais significativa, valorizando a construção do conhecimento matemático.

BIBLIOGRAFIA

[1] SILVA, A. A. *Notas de aula*. UFPB.

[2] GONÇALVES, Adilson. *Introdução à Álgebra*. IMPA, 2009.

[3] LANDAU, E. – *Teoria Elementar dos Números*, Euclides Ciência Moderna, 2002.

[4] NIVEN, I., ZUKERMAN, H. S. and MONTGOMERY, H. L. – *An Introducion to the Theory of Numbers*, Wiley (New York), 1991.

[5] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. RJ: IMPA, 2007.