FUNDAÇÃO UNIVERSIDADE FEDERAL DE RONDÔNIA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA – PROPESQ
PROGRAMA INSTITUCIONAL DE BOLSAS E TRABALHO VOLUNTÁRIO DE INICIAÇÃO CIENTÍFICA – PIBIC/UNIR/CNPQ

RELATÓRIO PARCIAL E RESUMO INFORMATIVO DO PIBIC/UNIR/CNPQ
CICLO 2019/2020

Título do Projeto do Grupo de Pesquisa

Título do Projeto de Pesquisa do Orientador

NÚMEROS PRIMOS: OS ÁTOMOS DA ARITMÉTICA

Orientadora: Profª. Dra. Lucia de Fatima de Medeiros Brandão Dias
Orientando: Douglas Vinícius Gonçalves Araújo
( ) Bolsista (X) Voluntário
Período do relatório: 5 de agosto de 2019 a 30 de janeiro de 2020

JI-PARANÁ - RO
2020

RESUMO

Este trabalho tem como objetivo de apresentar um estudo sobre os Números Primos que passa por conteúdos básicos tais como: a infinitude dos números primos; suas propriedas aritméticas; teorema fundamental da aritmética . Além da exposições teóricas temos

Palavras-chave: Lógica. Conjunto e funções. Demonstração. Divisibilidade. Números Primos.

ABSTRACT

verbo thube kkk

Keywords: Adult education. Community schools. Peasants. Popular culture

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

A história da humanidade está inteiramente ligada com a noção de números e suas propriedades. E a ramificação da matemática

A ciencia que tem o objetivo de estudar as propriedades, origem e relação dos numeros é a teoria os numeros, considerada por gauss como a rainha da matematica. O resultado deste trabalho é o estudo da parte elementar, onde estão apresentados provas elementares de preposições e teoremas. Neste trabalho estudamos a lógica matematica, suas preposições, conectivos e suas tabelas verdades. Em seguida foi apresentado uma noção de teoria dos conjuntos e funções e depois enunciamos os tipos de demonstrações: Demontrações diretas e Indiretas, com significativo exemplo, procurando dessa forma adquirir uma linguagem matematica formal. E no campo da introdução da teoria dos números, estudamos propriedades elementares sobre divisibilidades no conjunto dos inteiros, tendo o algoritmo da divisão e sobre a existência e a unicidade doquociente e do resto. Tambem usamos o principio da indução finita em alguns exemplos. Fornecemos alguns resultados clássicos sobre os números primos e o teorema fundamental da aritmética e sobre a unicidade da representação de um inteiro como produto de potências de primos. No teorema de Euclides foi apresentado várias provas de existencia de infinitos números primos.

A teoria dos números é a soma da matematica dita muitas vezes de matematica pura? E conforme (livro), para alguns membros dessa escola, a pesquisa das relações, propriedades entre os numeros é como um jogo de xadrez, cuja a principal recompensa é o estimulo intelectual que fornece. O objetivo deste trabalho é fazer

1.1 CRONOGRAMA

Este projeto tem a duração de 12 meses, de 01/08/2019 a 30/07/2020. O projeto esta sendo desenvolvido conforme o seguinte cronograma:

2 OBJETIVOS

Visando um estruturação mais clara deste relatório parcial, encontra-se resumido nas páginas seguintes, o plano de pesquisa proposto inicialmente.

2.1 OBJETIVO GERAL

Compreender a estrutura lógica

2.2 OBJETIVO ESPECÍFICO

- entender a sistematização da estrutura lógica matemática e suas técnicas de demonstrações;
- compreender e habituar com a linguagem matemática de conjuntos e funções;
- evidenciar e analisar as propriedades básicas dos inteiros;
- demonstrar as propriedades e teoremas.

3 MATÉRIAIS E MÉTODOS

Os materiais utilizados durante a pesquisa foram os livros que se encontram nas Referências Bibliográficas, mas principalmente o livro Introdução à Teoria dos Números de José Plinio.

4 RESULTADOS E DISCUSSÕES

4.1 LÓGICA MATEMÁTICA

Conforme (FILHO, 2002) a lógica matemática adota como regra fundamentais do pensamento os dois seguintes princípios (ou axiomas):

Axioma 4.1 ***PRINCÍPIO DA NÃO CONTRADIÇÃO:*** *uma proposição não pode ser verdadeira e falsa ao mesmo tempo.*

Axioma 4.2 ***PRINCÍPIO DO TERCEIRO EXCLUÍDO:*** *toda proposição ou é verdadeira ou falsa, isto é, verifica-se sempre um destes casos e nunca um terceiro.*

Em virtude desses dois princípios temos que a Lógica Matemática é uma lógica bivalente. Por definição, proposição significa uma oração declarativa, que tem sentido afirmativo completo.

4.1.1 Proposições Simples e Compostos

Definição: chama-se de proposição simples ou proposições atômicas aquela que não contém nenhuma outra proposição como parte integrante de si mesma. Normalmente representado por letras latina minúsculas: *p, q, r*.

Exemplo: O número 25 é quadrado perfeito.

Definição: chama-se proposição composta ou proposição molecular aquela formada pela combinação de duas ou mais proposições. Representado por letras latinas maiúsculas: *P, Q, R*.

Exemplo: O número π é irracional e maior do que 4.

Usualmente as proposições compostas que são formadas pela combinação das proposições simples *p, q, r,...*, escreve-se: $P(p,q,r,...)$

4.1.2 Conectivos

Definição: chama-se conectivos palavras ou expressões que se usam para formar, interligar novas proposições a partir de outras. São conectivos usuais em lógica as palavras: "e", "ou", "não", "se... então... ", "... se e somente se...".

4.1.2.1 Negação

Definição: negação de uma preposição *p* representada por "não *p*"cujo o valor lógico é verdadeiro quando *p* é falso e vice-verso.

p	$\sim$ p
V	F
F	V

4.1.2.2 Conjunção

Definição: a conjunção de duas proposições *p* e *q* a proposição representada por "*p* e *q*, cujo o valor lógico é a verdade (**V**) quando ambas proposições são verdadeiras e falsa nos demais casos.

p	q	p $\wedge$ q
V	V	V
V	F	F
F	V	F
F	F	F

4.1.2.3 Disjunção

Definição: a disjunção de duas proposições *p* e *q*, representadas por "*p* ou *q*", cujo o valor lógico é a verdade quando ao menos uma das proposições é verdadeira e falsa quando ambas as preposições são falsas.

p	q	p $\vee$ q
V	V	V
V	F	V
F	V	V
F	F	F

4.1.2.4 Disjunção Exclusiva

Definição: disjunção exclusiva de duas proposições *p* e *q* representada por "ou *p* ou *q*"ou "ou *p* ou *q*, mas não ambas", cujo o valor lógico é a verdade somente quando *p* é verdadeiro ou *q* é verdadeiro

p	q	p $\veebar$ q
V	V	F
V	F	V
F	V	V
F	F	F

4.1.2.5 Condicional

Definição: Proposição condicional representado por "se p, então q, cujo o valor lógico é falsidade no caso que p é verdadeira e q é falso e verdade nos demais casos. Os valores lógicos de duas proposições, definido pela seguinte tabela-verdade:

p	q	p $\rightarrow$ q
V	V	V
V	F	F
F	V	V
F	F	V

Também se lê de uma das seguintes maneiras:

(i) p é condição suficiente para q;

(ii) q é condição necessária para p.

Neste conectivo lógico é diz que p é o **antecedente** e q o **consequente**. O símbolo "$\rightarrow$"é chamado de símbolo de implicação.

4.1.2.6 Bicondicional

Definição: Proposição bicondicional representada por "p se e somente se q", cujo o valor lógico é a verdade quando p e q são ambas verdadeiras ou ambas falsas, e falsidade nos demais casos. O valor lógico da bicondicional de duas proposições definidas pela seguinte tabela-verdade:

p	q	p $\leftrightarrow$ q
V	V	V
V	F	F
F	V	F
F	F	V

Simbolicamente, "$\Leftrightarrow$"também se lê de uma das seguintes maneiras:

1. p é condição necessária e suficiente para q;

2. q é condição necessária e suficiente para p.

4.2 CONJUNTOS

4.3 TIPOS DE DEMONSTRAÇÕES

Resumidamente existem dois tipos de demonstrações em matemática: as demonstrações direta e demonstrações indiretas. Grande parte dos teoremas tem a estrutura "se P, então Q, onde P e Q são afirmações falsas ou verdadeiras. Chamamos de P de hipótese ou premissa e Q de tese ou conclusão.

4.3.1 Demonstrações Diretas

O procedimento para uma demonstração direta é através de implicações lógicas encadeadas que levam P diretamente a Q. Ou seja, de uma sentença $p \rightarrow q$ funciona da seguinte forma: assuma que o antecedente p é verdade (hipótese) e deduza o consequente (tese) q.

Exemplo 1: Quaisquer dois quadrados perfeitos consecutivos diferem por um número ímpar.

Demonstração: Suponhamos que a e b sejam inteiros quadrados perfeitos consecutivos, ou seja, $a = n^2$ e $b = (n+1)^2$. Queremos mostrar que eles diferem por um número ímpar, ou seja, $b-a$ ou $a-b$ é um número ímpar. Como $a = n^2$ e $b = (n+1)^2$ então $b-a = (n+1)^2 - n^2 = n^2 + 2n + 1 - n^2 = 2n+1$. Portanto, $b-a$ é um número ímpar.

Exemplo 2: Sejam A e B conjuntos. Mostre que $A \subset B \Leftrightarrow \complement_B \subset \complement_A$.

Demonstração: Suponhamos que $A \subset B$. Então um elemento $x \in \complement_B$ não pode pertencer ao conjunto B, principalmente não pertencer a A. Logo $x \in \complement_B \Rightarrow x \in \complement_A$, ou seja, $\complement_B \subset \complement_A$. Semelhantemente pela propriedade reflexiva, $\complement(\complement_A) = A$, temos $\complement_B \subset \complement_A$ então, $\complement(\complement_A) \subset \complement(\complement_B)$, obtemos $A \subset B$.

4.3.2 Demonstrações Indiretas

Existem dois tipos de demonstrações indireta que podemos usar para estabelecer uma afirmação condicional da forma $P \Rightarrow Q$: demonstração por absurdo e demonstração por contra-positiva.

Demonstração por absurdo: Na demonstração por absurdo nós assumimos que a hipótese P é verdadeira, mas nesse caso supomos que a conclusão Q é falsa. O objetivo é mostrar que a combinação da validade da hipótese P com a não validade da tese Q produz um resultado absurdo. Dessa forma segue que Q é verdadeira.

Exemplo: Mostre que $\sqrt{2} \notin \mathbb{Q}$. Isso é o mesmo que dizer: Se $x \in \mathbb{R},\ x > 0$ e $x^2 = 2$, então $x \notin \mathbb{Q}$.

Demonstração: Sabemos que um número $r \in \mathbb{R}$ é dito racional se existem inteiros $p,\ q$ sendo $q \neq 0$ tais que $r = \frac{p}{q}$.

4.4 INDUÇÃO FINITA E BOA ORDENAÇÃO

Uma propriedade básica dos números naturais e uma ferramenta indispensável na demonstração de muitos teoremas é: o Princípio da Indução Finita (PIF) que é divida em duas formas.

Seja $P(n)$ uma propriedade do número natural n, por exemplo:

- $1+2+...+n = \frac{n(n+1)}{2}$;
- $1^2+2^2+...+n^2 = \frac{n(n+1)(2n+1)}{6}$;
- $1^3+2^3+...+n^3 = (1+2+...+n)^2$;
- $F_1+F_2+...+F_n = F_{n+2}-1$;

Para provar que a sentença aberta $P(n)$ é válida para todo natural $n \geq n_0$ é necessário utilizar o *Princípio da Indução Finita* (PIF), que é um dos axiomas só o conjunto dos números naturais possuem. O PIF consiste em verificar duas etapas:

1. (Base de Indução): $P(n_0)$ é verdadeira;
2. (Passo Indutivo): Se $P(n)$ é verdadeira para algum número natural $n \geq n_0$, então $P(n+1)$ também é verdadeira.

Exemplo 4.1 *Demonstrar que para todo inteiro positivo n,*

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

Solução: Sabemos que para $P(1): 1 = \frac{1(1+1)}{2}$, onde a igualdade é verdadeira para $n = 1$ (base de indução). Suponhamos que seja verdadeiro para um $n = k$ (hipótese de indução):

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

Somando $k+1$ em ambos os lados da igualdade, obtemos

$$\begin{aligned} 1 + 2 + ... + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) \\ &= \frac{(k+1)(k+2)}{2}, \end{aligned}$$

neste caso a igualdade também é válida para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

Exemplo 4.2 *Demonstrar que para todo inteiro positivo n,*

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

Solução: Observamos que para $P(1): 1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$, donde a igualdade é válida para $n = 1$ (base de indução). Suponhamos que seja válida para um $n = k$ (hipótese de indução):

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

Acrescentando o sucessor (k+1) em ambos lados da igualdade, obtemos

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

de modo que a igualdade também vale para $n = k+1$. Pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

Exemplo 4.3 *Demonstrar que para todo inteiro positivo n,*

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

Solução: Neste caso vemos que $P(1): 1^3 = (1)^2$ é válido para $n = 1$ (base de indução). Observamos que o termo do segundo membro da igualdade mostrado no exemplo 4.1 pode ser substituído por

$$1^3 + 2^3 + ... + n^3 = \left[\frac{n(n+1)}{2}\right]^2.$$

Suponhamos que seja verdadeiro para $n = k$ (hipótese de indução).

$$1^3 + 2^3 + ... + k^3 = \left[\frac{k(k+1)}{2}\right]^2.$$

Acrescentando o sucessor $n = k+1$ em ambos os lados da igualdade, obtemos

$$\begin{aligned} 1^3 + 2^3 + ... + k^3 + (k+1)^3 &= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 \\ &= \frac{k^2(k+1)^2}{4} + (k+1)^3 \\ &= \frac{k^2(k+1)^2 + 4(k+1)^3}{4} \\ &= \frac{(k+1)^2[k^2 + 4(k+1)]}{4} \\ &= \frac{(k+1)^2(k+2)^2}{4} \\ &= \left(\frac{(k+1)(k+2)}{2}\right)^2. \end{aligned}$$

Vemos que é válido para $n = k+1$. Portanto, pelo PIF, a igualdade vale para todo número natural $n \geq 1$.

A segunda forma do PIF (às vezes chamada de princípio de indução forte), possuem as seguintes propriedades

1. (Base de Indução): $P(n_0)$ é verdadeira; e
2. (Passo Indutivo): Se $P(k)$ é verdadeira para todo natural k tal que $n_0 \leq k \leq n$, então $P(n+1)$ também é verdadeira.

O *princípio da boa ordenação* (PBO) dos números naturais, afirma que todo subconjunto A não vazio de $\mathbb{N}$ tem um elemento mínimo. Ou seja,

- Se $A \subseteq \mathbb{N}$ e $A \neq \emptyset$, então existe $n_0 \in A$ tal que $n_0 \leq n$, $\forall n \in A$

Exemplo 4.4

4.5 DIVISIBILIDADE E CONGRUÊNCIA

4.5.1 Divisibilidade

Nesta secção descreveremos algumas propriedades da divisão, existência e unicidade do quociente e do resto na divisão de inteiros.

Definição: Dado dois inteiros a e b, dizemos que a divide b ou que a é divisor de b ou ainda que b é um múltiplo de a e denotado

$$a|b$$

se existir um inteiro c tal que $b = ac$.

Proposição: Se a, b e c são inteiros, $a|b$ e $b|c$, então $a|c$.

Demonstração: Temos que $a|b$ e $b|c$, neste caso existem inteiros k_1 e k_2 que $b = k_1 a$ e $c = k_2 b$. Substituindo a igualdade de b na segunda equação, teremos $c = k_1 k_2 a$ o que implica que $a|c$. Esta proposição é chamada de *"Transitividade"*.

Proposição: Se a, b, c, m e n são inteiros,

Além das proposições que apresentamos a divisibilidade tem as seguintes propriedades:

(i) $n|n$

Demonstração: Se $n|n$, então existe um inteiro $k = 1$ para ser válido a igualdade $n = 1n$.

(ii) $d|n \Rightarrow ad|an$

Demonstração: Se $d|n$, então n é múltiplo de d, ou seja, existe um k fixo que $n = kd$. Multiplicando um inteiro qualquer a nos membros desta equação, temos $an = akd$, o que implica $ad|an$. Logo $d|n \Rightarrow ad|an$.

(iii) $ad|an$ e $a \neq 0 \Rightarrow d|n$

Demonstração: Se $ad|anen \neq 0$, então an é múltiplo de ad, ou seja, $an = kad$ e sendo $a \neq 0$ dividimos os dois membros da equação por a, assim temos que $n = kd$, o que implica $d|n$.

(iv) $1|n$

Demonstração: Se $1|n$, então $n = 1k$, sendo válida apenas com inteiro fixo $k = n$, o que nos mostras que 1 divide qualquer inteiro.

(v) $n|0$

Demonstração: Seja $n|0$, ou seja, $0 = nk$

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

Demonstração: Seja $d|n$ e $n \neq 0$, então n é múltiplo de d, ou seja, $n = kd$ neste caso temos que $|d| < |n|$ ou $|d| = |n|$ para o caso $k = 1$, o que implica que $|d| \leq |n|$.

(vii) $d|n$ e $n|d \Rightarrow |d| = |n|$

Demonstração: Temos que $d|n$ e $n|d$, então $n = k_1 d$ e $d = k_2 n$. Substituindo a igualdade de n na 2ª equaçao $d = k_1 k_2 d$, dividindo os membros por d, $1 = k_1 k_2$. Como 1 é elemento neutro no operador de multiplicação, implica que $|d| = |n|$.

(viii) $d|n$ e $d \neq 0 \Rightarrow (n/d)|n$

Demonstração: Temos que $d|n$ sendo que $d \neq 0$, então existe um k fixo que $n = kd$, como $d \neq 0$ podemos dividir os membros da igualdade por d, $\frac{n}{d} = k$, substituindo a igualdade de k na equação $n = kd \Rightarrow n = \frac{n}{d}d$, o que nos leva a entender que $(n/d)|n$.

4.5.2 O Algoritmo da Divisão

No célebre livro VII dos "Elementos"de Euclides escrito aproximadamente 300 a.c. é enunciado o teorema de Eudoxius, que será uma ferramenta essencial para demonstrar o Algoritmo da divisão.

Teorema de Eudoxius: Dado dois inteiros a e b, $b \neq 0$, então ou a é múltiplo de b ou a se encontra entre dois múltiplos consecutivos de b. Ou seja, correspondendo a cada par de inteiros a e $b \neq 0$ existe um inteiro q tal que, para $b > 0$,

$$qb \leq a < (q+1)b$$

e para $b < 0$,

$$qb \leq a < (q-1)b$$

Demonstração:

Podemos finalmente enunciar e provar o Algoritmo da Divisão

Teorema: Dado dois inteiros a e b, $b > 0$, existe um único par de inteiros q e r tais que

$$a = qb + r, \text{ com } 0 \leq r < b \ \ (r = 0 \Leftrightarrow b|a)$$

Os números q e r são chamados, respectivamente, **quociente** e **resto** da divisão de a por b.

Demonstração:

4.5.3 mdc, mmc e Algoritmo Euclidiano

O *máximo divisor comum* de dois inteiros a e b (a ou b diferentes de 0), é denotado por (a,b), é o maior inteiro que divide a e b.

Teorema:

Demonstração:

4.5.4 Teorema Fundamental da Aritmética

4.5.5 Congruência

As bases teóricas sobre congruência ou aritmética modular teve início com os trabalhos do matemático suíço Leonhard Euler. Porém, no livro *Disquisitiones Arithmeticae* publicado em 1801, por Carl Friedrich Gauss que tinha apenas 24 anos de idade, tornou mais explícita com as anotações, simbologia e definições usados até hoje.

Definição 4.1 *Sejam a, b e $n \in \mathbb{Z}$, dizemos que a e b são congruentes módulo n se os restos de sua divisão euclidiana por n são iguais. Escreve-se $a \equiv b \pmod{n}$, quando está relação é falsa, denotamos por $a \not\equiv b \pmod{n}$ e denominamos de incongruentes.*

Exemplo 4.5 $11 \equiv 3$ (*mod* 2) *pois* $2|(11-3)$.

Proposição 4.5.1 *Sejam a, b e $n \in \mathbb{Z}$, temos que $a \equiv b \pmod{n}$ se, e somente se, existir um $k \in \mathbb{Z}$ tal que $a = b + km$.*

Demonstração: Se $a \equiv b \pmod{n}$, então $n|(a-b)$ o que implica a existência de um $k \in \mathbb{Z}$ tal que $a - b = kn$, isto é, $a = b + kn$. A recíproca é trivial.

Conforme Landau (2002) todos os conceitos como "congruente", "equivalente", "igual"ou "similar"devem satisfazer três propriedades chamadas reflexiva, simétrica e transitiva. Além desses, apresentamos mais propriedades importantes sobre congruência segundo Brochero Carlos Gustavo T. de A. Moreira (2011).

Proposição 4.5.2 *Se a, b, c e $n \in \mathbb{Z}$, $n \leq 0$, as seguintes propriedades são válidas:*

1. *(Reflexiva): $a \equiv a \pmod{n}$;*

2. *(Simétrica): Se* $a \equiv b \pmod{n}$*, então* $b \equiv a \pmod{n}$*;*

3. *(Transitiva): Se* $a \equiv b \pmod{n}$ *e* $b \equiv c \pmod{n}$*, então* $a \equiv c \pmod{n}$*;*

4. *(Compatibilidade com a soma e diferença): Podemos somar e subtrair membro a mebro*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Longrightarrow \begin{cases} a+c \equiv b+d \pmod{n} \\ a+c \equiv b-d \pmod{n} \end{cases}$$

Em particular, se $a \equiv b \pmod{n}$*, então* $ka \equiv kb \pmod{n}$ *para todo* $k \in \mathbb{Z}$*.*

5. *(Compatibilidade com o produto): Podemos multiplicar membro a membro*

$$\begin{cases} a \equiv b \pmod{n} \\ c \equiv d \pmod{n} \end{cases} \Longrightarrow \begin{cases} ac \equiv bd \pmod{n} \end{cases}$$

Em particular, se $a \equiv b \pmod{n}$*, então* $a^k \equiv b^k \pmod{n}$ *para todo* $k \in \mathbb{N}$*.*

6. *(Cancelamento): Se* $mdc(c,n) = 1$*, então*

$$ac \equiv bc \pmod{n} \Longleftrightarrow a \equiv b \pmod{n}$$

Demonstração:

4.5.5.1 Congruência Linear

4.5.6 Teoremas de Euler, Fermat e Wilson

4.6 PSEUDOPRIMOS E TESTE DE PRIMALIDADE

O prefixo *pseudo* é usado para marcar algo que superficial, imitação, engano - ou seja, parece ser uma coisa, mas é outra coisa. Neste caso pseudoprimos não números que apresentam propriedades de números primos, mas não são primos.

4.6.1 Números de Carmichael

4.6.2 Teste de Primalidade

4.6.3 Distribuição dos Números Primos

5 CONCLUSÕES

REFERÊNCIAS

BROCHERO CARLOS GUSTAVO T. DE A. MOREIRA, N. C. S. E. T. F. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 2011.

FILHO, E. de A. **Iniciação à lógica matemática**. [S.l.]: NBL Editora, 2002.

LANDAU, E. **Teoria elementar dos números**. [S.l.]: Ciência Moderna, 2002.