UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
INSTITUTO DE GEOCIÊNCIAS E CIÊNCIAS EXATAS

Programa de Pós-Graduação em Matemática em Rede Nacional

Fluxogramas: Uma nova linguagem para trabalhar divisibilidade no Ensino Básico

Ana Flavia Urbano da Silva

PROFMAT

Rio Claro
2020

Universidade Estadual Paulista "Júlio de Mesquita Filho"
Instituto de Geociências e Ciências Exatas
Câmpus de Rio Claro

Fluxogramas: Uma nova linguagem para trabalhar divisibilidade no Ensino Básico

Ana Flavia Urbano da Silva

Dissertação apresentada como parte dos requisitos para obtenção do título de Mestre em Matemática, junto ao Programa de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", Câmpus de Rio Claro.

Orientadora
Profa. Dra. Ariane Luzia dos Santos

Rio Claro
2020

S586f

Silva, Ana Flavia Urbano da

Fluxogramas: Uma nova linguagem para trabalhar divisibilidade no Ensino Básico / Ana Flavia Urbano da Silva. -- Rio Claro, 2020

200 p. : il.

Dissertação (mestrado profissional) - Universidade Estadual Paulista (Unesp), Instituto de Geociências e Ciências Exatas, Rio Claro

Orientadora: Ariane Luzia dos Santos

1. Fluxogramas. 2. Divisibilidade. 3. Congruências. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Instituto de Geociências e Ciências Exatas, Rio Claro. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

TERMO DE APROVAÇÃO

Ana Flavia Urbano da Silva

Fluxogramas: Uma nova linguagem para trabalhar divisibilidade no Ensino Básico

Dissertação APROVADA como requisito parcial para a obtenção do grau de Mestre no Curso de Pós-Graduação – Mestrado Profissional em Matemática em Rede Nacional, do Instituto de Geociências e Ciências Exatas da Universidade Estadual Paulista "Júlio de Mesquita Filho", pela seguinte banca examinadora:

Profa. Dra. Ariane Luzia dos Santos
Orientadora

Prof. Dr. Flávio Andrade Faria
UNESP - Ilha Solteira (SP)

Profa. Dra. Janete de Paula Ferrareze Silva
UFPR - Jandaia do Sul (PR)

Rio Claro, 16 de dezembro de 2020

Dedico esse trabalho a todos os meus colegas de profissão, que assim como eu, sempre estão em busca de saberes para melhorar o ensino e aprendizagem da Matemática para nossos alunos.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado esta oportunidade. Ao meu marido, Prof. Me. Pedro Alvaro da Silva Junior por ter me apoiado em todos os momentos, desde os mais alegres até os mais complicados e também ter me ajudado na construção dos fluxogramas. A minha família por sempre me apoiar.

Agradeço a Sociedade Brasileira de Matemática (SBM) e a UNESP que promovem o Mestrado Profissional em Matemática em Rede Nacional (PROFMAT). Gostaria também de deixar meu agradecimento a todos os professores do departamento de Matemática da UNESP - Rio Claro, que participaram dessa etapa, compartilhando seu saber. Em especial a Profa. Dra. Ariane Luzia dos Santos, pelas orientações e conselhos e aos membros da banca examinadora Prof. Dr. Flávio Andrade Faria e Profa. Dra. Janete de Paula Ferrareze Silva, por terem aceito o convite e pelas contribuições para a dissertação.

Agradeço a todos os meus colegas de turma, que fizeram deste curso mais leve, com seu coleguismo e palavras de incentivo, possibilitando a conclusão desse ciclo, em especial ao Prof. Me. Jefferson David Alves que me ajudou com o LaTex e a Profa. Edilene Ponce do Amaral, minha companheira de viagem para a UNESP. Que a distância entre nós não seja motivo para apagar essa amizade e que possamos sempre estar em contato, compartilhando experiências e alegrias.

Muito obrigada a todos!

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001

A Matemática
é o alfabeto com o qual
Deus criou o Universo
Galileu Galilei

Resumo

Este trabalho pretende contribuir para o ensino da divisibilidade nas escolas, conteúdo no qual os alunos apresentam maior dificuldade em relação as outras operações matemáticas. Esse conteúdo será abordado com uma nova linguagem, os fluxogramas, implementados pela Base Nacional Comum Curricular (BNCC). Em seu decorrer, falaremos sobre a BNCC, sobre os fluxogramas como habilidades da BNCC e sobre a estrutura e conceitos que envolvem essa linguagem algorítmica. Traremos exemplos e análise de fluxogramas oriundos de livros do Programa Nacional do Livro e Material Didático (PNLD), como também, exemplos para serem aplicados em sala de aula. Relacionado a divisibilidade traremos um capítulo em que todo o conteúdo é reescrito em forma de fluxograma, com o objetivo de ajudar na compreensão tanto dos algoritmos, quanto dos conceitos envolvidos. Além disso, abordaremos a importância do resto em resoluções de atividades, por esse motivo, transformamos o conteúdo de congruências lineares em fluxogramas, para aplicação em sala de aula e na orientação de resolução de exercícios de Olimpíadas de Matemática. Concluímos que trabalhar com fluxogramas faz com que o aluno crie estratégias de resolução, fixe os processos em sua memória, otimize seu tempo, ganhe confiança em seus raciocínios, além de ser uma forma mais dinâmica e visual de se trabalhar algoritmos matemáticos.

Palavras-chave: Fluxograma, Divisibilidade, Congruências.

Abstract

This work aims to contribute to the teaching of divisibility in schools, a content in which students have greater difficulty in relation to other mathematical operations. This content will be approached with a new language, flowcharts, implemented by the National Common Curricular Base (BNCC). In its course, we will talk about BNCC, about flowcharts as BNCC skills and about the structure and concepts that involve this algorithmic language. We will bring examples and analysis of flowcharts from books of the National Book and Didactic Material Program (PNLD), as well as examples to be applied in the classroom. Related to divisibility, we will bring a chapter in which all the content is rewritten in the form of a flowchart, in order to help in understanding both the algorithms and the concepts involved. In addition, we will address the importance of the rest in activity resolutions, for this reason, we have transformed the content of linear congruences into flowcharts, for application in the classroom and in the guidance for solving Mathematical Olympics exercises. We concluded that working with flowcharts makes the student create resolution strategies, fix the processes in his memory, optimize his time, gain confidence in his reasoning, in addition to being a more dynamic and visual way of working with mathematical algorithms.

Keywords: Flowchart, Divisibility, congruences.

Lista de Figuras

Sumário

Introdução

Fluxograma é a representação gráfica de um processo ou algoritmo, através de formas geométricas conectadas por setas (fluxos). Cada forma geométrica tem uma função específica. Para a realização do processo ou algoritmo é necessário seguir suas etapas corretamente.

O fluxograma pode ser visto como um algoritmo ilustrado, qualquer pessoa com o mínimo de conhecimento, pode executar o processo, basta apenas seguir as instruções nele contidas. É muito utilizado na área de informática, para definir as etapas de programação de *softwares* e aplicativos. O fluxograma também está sendo utilizado por empresas, pois ajuda a pessoa recém contratada a entender seu cargo, como também o funcionamento e a organização dos departamentos dessa empresa de forma padronizada, clara e objetiva, mas para isso, ela deve possuir conhecimentos básico da estrutura e funcionalidade dos fluxogramas.

Tendo em vista que além do aspecto acadêmico, as escolas têm como responsabilidade social, expandir a capacidade dos alunos em sua atuação profissional e cidadã, formando profissionais aptos para a vida em sociedade e ao mercado de trabalho. Desse modo, para garantir a formação integral dos alunos, a Base Nacional Comum Curricular (BNCC) [1] incorporou ao currículo de Matemática, o fluxograma.

Espera-se também, que o fluxograma atraia o interesse do aluno para os conteúdos matemáticos, pois se trata de um processo mais visual, contemporâneo e dinâmico de executar os algoritmos.

Serão apresentados modelos de fluxogramas para trabalhar os principais resultados do conteúdo da aritmética dos restos, como os conceitos de divisibilidade e congruências lineares. Mostraremos como os fluxogramas podem ser utilizados em sala de aula aplicados a questões retiradas de olimpíadas de Matemática.

Assim, este trabalho pretende contribuir para o ensino de divisibilidade nas escolas, conteúdo no qual os alunos apresentam maior dificuldade em relação às outras operações matemáticas. Também poderá ser utilizado por professores que não tenham conhecimento sobre o assunto e queiram entender melhor o conceito de fluxogramas, antes de trabalhar em sala de aula com seus alunos.

Por se tratar de um conteúdo novo no universo da educação básica, esse tema não é muito difundido, há apenas alguns artigos escritos, mas em sua grande maioria, relacionados a outras áreas, como saúde [2] e [3] engenharia química [4] , por exemplo. Também encontrará artigos referentes a BNCC [5], em que os fluxogramas são apenas citados, por se tratarem de habilidades. Existem alguns sites na internet, que abordam o conceito de fluxogramas, porém neles se encontram informações muitas vezes incertas.

Portanto um dos objetivo deste trabalho é formalizar esses conceitos, dando base e confiança de que, os resultados apresentados aqui são coerentes e podem ser utilizados

pelos profissionais de educação em suas aulas e também por alunos no seu cotidiano escolar.

No primeiro capítulo traremos uma síntese sobre a BNCC e a Área do Conhecimento da Matemática.

O segundo capítulo será referente ao fluxograma, apresentaremos o conceito, as principais formas geométricas utilizadas e suas funções. Daremos ênfase as habilidades da BNCC relacionadas aos fluxogramas, como também traremos exemplos e críticas de fluxogramas contidos em livros aprovados pelo PNLD, visando sempre a compreensão do principal objetivo do fluxograma, ser claro e objetivo.

O terceiro capítulo será a base para o trabalho de divisibilidade, trazendo resultados que nos permitirão construir algoritmos, embasados e devidamente provados, fazendo uso dos teoremas e aplicações nele demonstrados. Assim no quarto capítulo utilizaremos os resultados para construir fluxogramas que representem os principais resultados do conteúdo de divisibilidade.

Em seguida, no capítulo cinco, será abordado o conteúdo de congruências lineares. No Ensino Básico, esse conteúdo quase nunca é trabalhado, porém é fundamental na hora de resolver questões em que temos uma repetição de padrões, questões essas que aparecem com frequências em olimpíadas de Matemática. Portanto, no sexto e último capítulo, traremos exemplos dessas questões resolvidas com auxílio do fluxograma. Esse capítulo justificará todo trabalho desenvolvido, pois questões que parecem ser complexas, com o uso dos fluxogramas, passarão a ser de simples resolução e ainda fornecem argumentos para justificativa dos resultados encontrados.

1 Base Nacional Comum Curricular

Não é de hoje que o governo brasileiro busca uma consolidação da educação, esse processo se inciou com a Constituição Federal de 1988, que criou a Base Nacional Comum para o Ensino Fundamental, se estendendo até 2018:

- 1996 - Aprovação da Lei das Diretrizes e Bases da educação Básica (LDB);
- 1997 a 2000 - Consolidação dos Parâmetros Curriculares Nacionais (PCNs) para o Ensino Fundamental e Médio;
- 2010 a 2012 - Implementação das Novas Diretrizes Curriculares Nacionais (DCNs) para o Ensino Infantil, Fundamental e Médio;
- 2015 - Criação da Lei do Plano Nacional de Educação (PNE) para a Educação Básica;
- 2015 a 2018 - Elaboração da proposta e homologação da Base Nacional Comum Curricular (BNCC):
  - 2015 - Instituição da comissão de Especialistas para a Elaboração de proposta da BNCC e 1° versão;
  - 2016 - Debate para ajustes e revisões e 2° versão;
  - 2017 - O Ministério da Educação (MEC) entrega 3° versão ao Conselho Nacional de Educação (CNE) que homologa as etapas da Educação Infantil e Ensino Fundamental;
  - 2018- Homologação da BNCC para o Ensino Médio.

O texto que se segue é um apanhado do documento da Base Nacional Comum Curricular (BNCC). [1]

A Base Nacional Comum Curricular (BNCC) é um documento que estabelece diretrizes das aprendizagens essenciais que todos os alunos devem desenvolver na Educação Básica (Infantil, Ensino Fundamental e Ensino Médio), assegurando seus direitos de aprendizagens apoiado no Plano Nacional de Educação (PNE) e embasado na Lei de Diretrizes e Bases da Educação Nacional (LDB 9394/1996) [6].

Um dos objetivos da BNCC é a integração das três esferas da educação, municipal, estadual e federal, dispondo de políticas e ações, tanto para a formação de professores como na elaboração de conteúdos e avaliações educacionais. Também pretende assegurar a oferta de infraestrutura nas escolas. Assim escolas mais precárias receberão mais ajuda, visando uma igualdade de condições para que o pleno desenvolvimento do estudante aconteça. Outro aspecto da BNCC é que além de assegurar o acesso e a permanência

do estudante nas escolas, esse documento busca garantir uma igualdade de conteúdos escolares e cada etapa da Educação Básica em todo território nacional, seguindo as Dez Competências Gerais da Educação [7].

Segundo a BNCC, competência refere-se à mobilização de conhecimentos, habilidades, atitudes e valores, relacionados ao cotidiano do aluno, no exercício de sua cidadania e em seu futuro como trabalhador. Ela reconhece que "educação deve afirmar valores e estimular ações que contribuam para a transformação da sociedade, tornando-a mais justa e também voltada para a preservação da natureza"(BNCC página 8).

Essas competências estão inter-relacionadas, articulando-se na edificação dos conhecimentos, no desenvolvimento de habilidades e na formação do caráter do aluno. A BNCC determina que as decisões pedagógicas devem estar orientadas para o desenvolvimento dessas competências, mostrando com clareza o que os alunos devem "saber fazer". O esclarecimento das competências dá referências para o fortalecimento de ações, assegurando o que é essencial a ser aprendido pelo aluno.

Entende-se como educação integral, o desenvolvimento humano global com foco em suas particularidades e diversidades. Assim, espera-se que o aluno se torne um adulto capaz de se comunicar de forma crítica e analítica, que seja participativo e colaborativo, que não tema o novo e seja capaz de se adaptar a mudanças, seja produtivo e responsável.

Para isso a escola deve ser um espaço de aprendizagem e de democracia inclusiva, reprimindo a discriminação, o preconceito, fortalecendo o respeito às diferenças. Deve promover aprendizagens em sintonia com as necessidades e interesses dos alunos, dando sentido aos conteúdos a serem ensinados. Também é de fundamental importância que o aluno seja o protagonista de seu projeto de vida, e que a escola forneça meios para isso.

As instituições de ensino têm seus próprios currículos, baseados no contexto em que os alunos estão inseridos e também na cultura local, a BNCC não vem para abolir esses currículos e sim para complementá-los, garantindo a todos estudantes uma educação igualitária. Sugere-se que todos os sistemas de ensino tenham um currículo escolar e que ele seja elaborado juntamente com as famílias dos alunos e a comunidade a qual a instituição pertence. Esse currículo deve incorporar temas contemporâneos que abranjam a vida humana local, regional e também global de forma transversal e integrada.

O Ministério da Educação (MEC) além de dar apoio técnico e financeiro também deve exercer fiscalização para assegurar o sucesso da implementação da BNCC em todo território brasileiro. Contará para isso com a colaboração de órgãos da área de educação como o Conselho Nacional de Educação (CNE), o Conselho Nacional de Secretários de Educação (Consed) e União Nacional dos Dirigentes de Educação (Undime).

Também é dever do MEC desenvolver inovação de práticas educativas, bem como compartilhar casos de sucesso dessas práticas, deve apoiar experiências curriculares inovadoras, criar oportunidade de acesso ao conhecimento e experiências obtidas em outros países e ainda incentivar e dar subsídios a estudos e pesquisas na área de educação.

Portanto, a BNCC precisa da colaboração não só dos professores, mas sim dos sistemas de educação, das secretarias e de todos os organismos nacionais relacionados a educação. Nosso país precisa urgentemente de práticas pedagógicas inovadoras e de uma educação que nos coloque no patamar dos países com alto nível de educação, e esse documento foi pensado para ser a base desse avanço tão almejado por todos nós.

1.1 A estrutura da BNCC

A Base Nacional Comum Curricular está estruturada de acordo com as competências que os alunos devem desenvolver em cada etapa da Educação Básica (Infantil, Ensino Fundamental e Ensino Médio). Essas competências foram baseadas em conceitos colocados pelo sociólogo suíço *Philippe Perrenound*:

> "O desenvolvimento de uma competência é a construção do indivíduo, se faz lentamente, por meio de situações semelhantes o bastante de modo que a cada uma contribua na construção dessa competência"
>
> "Se aceitarmos que competência é uma capacidade de agir eficazmente num determinado tipo de situação, apoiada em conhecimentos, mas sem se limitar a eles, é preciso que alunos e professores se conscientizem das suas capacidades individuais que melhor podem servir o processo cíclico de Aprendizagem-Ensino-Aprendizagem"

Segundo Maria Ignez Diniz (diretora do Mathema), o desenvolvimento de uma competência não se dá em apenas uma atividade ou uma aula, ele é um processo de construção e aquisição gradual das habilidades. Para isso as aulas devem ser desafiantes, com problematização constante e com bons problemas, selecionados para desestabilizar o estudante e motivá-lo para a buscar a resolução.

Ana Penido (Instituto Inspirar) que foi colaboradora do Capítulo introdutório da Base, relata que a BNCC concebe educação baseada em competências que os alunos devem adquirir em cada ano escolar. Essas competências referem-se a aquisição de conhecimentos (saberes fundamentais para a vida), habilidades (aplicar os conhecimentos na prática do cotidiano), atitudes (intenção necessária para utilizar os conhecimentos e habilidades quando preciso) e valores (utilizar os conhecimentos, habilidades e atitudes de forma consciente e ética).

Ainda segundo Ana Penido, o objetivo principal da base é a educação integral do estudante em todas as suas dimensões: intelectual, física, emocional, social e cultural, preparando-os para serem pessoas, profissionais e cidadãos ativos na sociedade, buscando torná-la mais justa, ética, responsável, democrática, inclusiva, sustentável e solidária.

Nessa busca pela educação integral, a Base dividiu a educação básica em três etapas:

- A etapa da Educação Infantil, que conta com alunos recém nascidos até 6 anos, está estruturada de acordo com os direitos de aprendizagens e desenvolvimento e os campos de experiência.

- No Ensino fundamental, etapa que conta com alunos de 6 a 14 anos, dividida em Anos Iniciais (1° ao 5° ano/série) e Anos Finais (6° ao 9° ano/ série), está estruturada de acordo com as áreas de conhecimento, competências específicas por área, componentes curriculares e competências específicas de componentes.

- O Ensino médio, etapa que conta com alunos de 15 a 18 anos, foi estruturada de acordo com as áreas de conhecimento, competências específicas de área e habilidades.

Como mencionado, essas etapas escolares estão organizadas em áreas de conhecimento. Não iremos nos referir neste trabalho sobre a etapa da Educação Infantil, daremos ênfase nas etapas do Ensino Fundamental (principalmente nos Anos Finais) e do Ensino Médio.

No Ensino fundamental temos as seguintes áreas de conhecimento:

- Linguagens - Língua Portuguesa, Artes, Educação Física e Língua Inglesa.
- Matemática - Matemática.
- Ciências da Natureza - Ciências.
- Ciências Humanas - Geografia e História.
- Ensino Religioso (Facultativo).

No Ensino Médio temos as seguintes áreas do conhecimento:

- Linguagens e suas tecnologias - Língua Portuguesa, Artes, educação Física e Língua Inglesa.
- Matemática e suas tecnologias - Matemática.
- Ciências da Natureza e suas tecnologias - Química, Física e Biologia.
- Ciências Humanas e Sociais aplicadas - Filosofia, História, Geografia e Sociologia.

As habilidades mostram as aprendizagens fundamentais que devem ser asseguradas aos alunos em cada faixa estaria da educação básica. Buscando uma forma simplificada de expor o conjunto habilidades, elas estão estruturadas por códigos alfanuméricos.

- Ensino Fundamental - 8 símbolos (EF06MA01)

  EF (Ensino Fundamental) - 06 (ano/série que a habilidade será trabalhada) - MA (Área de conhecimento - Matemática) - 01 (Sequência da habilidade na série ou ano).

- Ensino Médio - 10 símbolos (EM13MAT102)

  EM (Ensino Médio) - 13 (ano/série que a habilidade será trabalhada) - MAT (Área de conhecimento - Matemática) - 102 (1° número- competência e o 2° e 3° número - sequência da habilidade no ano/série).

As habilidades podem ser trabalhadas em um ou mais anos da etapa escolar, no exemplo da habilidade do Ensino Médio temos o códio 13, ele representa que essa habilidade pode ser desenvolvida em qualquer ano/série.

Assim para o professor fazer seu plano de aula baseado nas habilidades da BNCC é simples, basta buscar pelo código. Não entraremos em detalhes sobre a estruturação da BNCC, o leitor que se interessar pode acessar o documento da Base Nacional Comum curricular para ver mais detalhes.

1.2 A Área do Conhecimento da Matemática

Um dos objetivos da Base Nacional Comum Curricular (BNCC) é evitar a ruptura dos conhecimentos aprendidos em cada etapa da educação escolar. Isso ocorre principalmente no Ensino Fundamental, na etapa dos Anos Iniciais para os Anos Finais, não só com relação aos conteúdos, mas também na rotina do estudante, ele deixa de ter um professor generalista e passa a ter professores especialistas. Muitas vezes os alunos têm dificuldade em se adaptar a nova estrutura escolar, então devemos ter cuidado com essa fase.

Por isso as aprendizagens na BNCC estão interligadas, os conteúdos a serem aprendidos estão presentes em praticamente todos os anos etapa escolar, rememorando os que já foram aprendidos em anos anteriores para serem aprofundados.

1.2.1 A Matemática

"Todas as coisas são números"(Pitágoras)

Olhe ao seu redor e irá compreender o que Pitágoras disse, praticamente tudo o que você vê, ou pode ser contado, ou pode ser construído, ou pode ser visto pela existência da matemática. Vivemos em um mundo de números, por isso é tão importante compreender essa área do conhecimento humano.

Imagine como é difícil a vida de uma pessoa que sofre de discalculia (deficiência em aprendizagem da matemática), não conseguir compreender conceitos básicos relacionados aos números. Essa pessoa, muitas vezes, não consegue nem mesmo relacionar quantidade de objetos que possui, não consegue diferenciar as formas geométricas, não compreende os símbolos matemáticos, então como será capaz de viver em um mundo onde ela precisa conviver com horários, operações monetárias, tecnologias, entre muitas outras coisas em que a matemática está envolvida. Conseguiu imaginar? Complicado né! Por isso os conhecimentos matemáticos são tão importantes para a vida em sociedade, fundamentais para o desenvolvimento de cidadão crítico.

Assim quando ouvimos as pessoas fazerem a pergunta "onde vou usar isso na minha vida?"quando estiver se referindo a algum conteúdo matemático, temos a obrigação de mostrar a ela a matemática por trás das coisas de seu dia a dia.

Essa é a grande missão de nós matemáticos, fazer com que a matemática se torne interessante aos nossos alunos, que eles consigam enxergá-la por trás das coisas e funções que exercem, percebendo que para vivermos em um mundo cada vez mais tecnológico é necessário compreendê-la.

A Base Nacional Comum Curricular (BNCC) vê os conhecimentos matemáticos como essenciais na vida em sociedade, pois eles não se restringem apenas a fazer cálculos, e sim a fazer análises, formular hipóteses, raciocinar, observar e argumentar sobre problemas que podem ou não estar relacionados a problemas do mundo físico. A matemática cria sistemas abstratos para que possamos compreender o mundo real, por isso é fundamental considerar seu papel heurístico na formação dos alunos.

1.2.2 A etapa do Ensino Fundamental

No Ensino Fundamental a BNCC traz como de suma importância o **letramento matemático**, ou seja, que o aluno seja capaz de raciocinar, representar, comunicar e argumentar conceitos matemáticos na resolução de problemas, que envolvam situações aplicadas ao mundo real, principalmente os problemas que estão relacionados ao seu cotidiano, a fim de que haja interesse pelo conteúdo que está sendo trabalhado.

O cotidiano de todas as pessoas, em todas as culturas está impregnado de saberes e fazeres que envolvem a matemática, fazendo comparações, qualificando, quantificando e medindo objetos, fazendo generalizações e aferições. Com o avanço científico tecnológico a matemática se tornou essencial na sociedade contemporânea, pelos elementos enriquecedores do pensamento e da formação intelectual do indivíduo.

A construção do pensamento matemático se dá pela identificação e pelo emprego de sistemas abstratos que se organizam e inter-relacionam a fenômenos do espaço, do movimento, das formas e dos números, associados ou não a fenômenos do mundo físico, fundamentais para sua compreensão e também para a construção de representações significativas para argumentação consciente, nos mais variados contextos.

Segundo a visão da professora doutora Maria Ignez Diniz (diretora do Mathema) deixa de ser a matemática em uso, a matemática na resolução de problemas e a matemática da técnica e das fórmulas. O aluno deve adquirir uma postura mais ativa nos mais diferentes contextos, posicionando-se sobre determinadas questões e buscando meios para solucioná-las, resolvendo problemas dentro e fora da escola.

Faz-se necessário que o estudante expanda sua compreensão sobre o que está aprendendo, por que está aprendendo e a melhor forma de aprender. Assim, ele entenderá que os conhecimentos matemáticos são essenciais para a compreensão e vivência no mundo, e que o desenvolvimento do raciocínio lógico e crítico o tornará um cidadão responsável e capaz de lidar com os problemas que a vida lhe trará, como evitá-los, ou superá-los.

Apesar dos objetos de conhecimentos estarem divididos em unidades temáticas (números, álgebra, geometria, grandezas e medidas, probabilidade e estatística) as atividades devem ser planejadas de forma a mesclar essas unidades temáticas para que os estudantes percebam as conexões entre os objetos de conhecimento.

O professor deve ser responsável pela conduta da aula e o aluno deve ser autônomo, assim a construção do conhecimento se dará de forma colaborativa. A função do professor não é mais apenas a de transmissor do conhecimento matemático que deve ser absorvido pelo aluno e depois fazer uma avaliação do processo, mas sim passa a ser um criador do espaço aprendizagem, provocando o estudante, fazendo-o pensar, estimulando-o a fazer conexões entre os conhecimentos que já possui, construindo soluções de diferentes problemas. O professor deve também reunir as experiências desenvolvidas em sala de aula e sistematizá-la, discutindo com os alunos as diferentes estratégias de resolução que foram obtidas por eles ou pelo grupo de alunos.

O conhecimento matemático é essencial não só por sua aplicabilidade, mas também por sua potencialidade na formação de cidadãos, críticos, autônomos e ativos na sociedade. (Maria Ignez Diniz)

Com um exemplo bem simples de geometria, podemos exemplificar a proposta da Base com relação a maneira de se ensinar matemática.

- Situação 1 - Qual a área de um retângulo que mede $7cm$ de comprimento por $4cm$ de largura?
- Situação 2 - Descubra as diferentes possibilidades de se obter um retângulo com área de $28cm^2$.

Na situação 1, o estudante fará apenas uma multiplicação, já na situação 2 ele deverá relacionar e analisar as diferentes possibilidades para essa área, sistematizando e generalizando suas hipótese e testando-as.

A base não está aí para banalizar o ensino da matemática e sim, para tornar mais complexas as relações matemáticas que o aluno vai estabelecer dentro da sala de aula, por meio do ensino proporcionado, é uma oportunidade de uma arrancada para o ensino da matemática. (Luciana Tenuta)

Também é necessário utilizar metodologias mais ativas e contextualizadas, que utilizem diferente recursos didáticos, inclusive os digitais, para que alunos com diferentes características e necessidades possam aprender no seu ritmo, a partir de seus interesses e de estratégias mais adequadas a seu perfil de aprendizagem.

Porém disponibilizar recursos tecnológicos não é garantia de aprendizagem, estamos passando por grandes mudanças com o avanço com a inteligência artificial (AI), sistemas de programação e robótica, nos dando a perspectiva de uma educação mais dinâmica.

Nessa busca a Base incorporou à área da matemática no campo da álgebra o **pensamento computacional**, outra novidade. Retomaremos esse tema mais adiante neste trabalho no próximo capítulo.

Assim para contemplar a proposta de um ensino mais integral, no Ensino Fundamental a BNCC propõe 8 competências específicas para a área de matemática, são elas:

> 1. Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho.
> 2. Desenvolver o raciocínio lógico, o espírito de investigação e a capacidade de produzir argumentos convincentes, recorrendo aos conhecimentos matemáticos para compreender e atuar no mundo.
> 3. Compreender as relações entre conceitos e procedimentos dos diferentes campos da Matemática (Aritmética, Álgebra, Geometria, Estatística e Probabilidade) e de outras áreas do conhecimento, sentindo segurança quanto à própria capacidade de construir e aplicar conhecimentos matemáticos, desenvolvendo a autoestima e a perseverança na busca de soluções.
> 4. Fazer observações sistemáticas de aspectos quantitativos e qualitativos presentes nas práticas sociais e culturais, de modo a investigar, organizar, representar e comunicar informações relevantes, para interpretá-las e avaliá-las crítica e eticamente, produzindo argumentos convincentes.
> 5. Utilizar processos e ferramentas matemáticas, inclusive tecnologias digitais disponíveis, para modelar e resolver problemas cotidianos, sociais e de outras áreas de conhecimento, validando estratégias e resultados.
> 6. Enfrentar situações-problema em múltiplos contextos, incluindo-se situações imaginadas, não diretamente relacionadas com o aspecto prático-utilitário, expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas, e dados).
> 7. Desenvolver e/ou discutir projetos que abordem, sobretudo, questões de urgência social, com base em princípios éticos, democráticos, sustentáveis e solidários, valorizando a diversidade de opiniões de indivíduos e de grupos sociais, sem preconceitos de qualquer natureza.
> 8. Interagir com seus pares de forma cooperativa, trabalhando coletivamente no planejamento e desenvolvimento de pesquisas para responder a questionamentos e na busca de soluções para problemas, de modo a identificar aspectos consensuais ou não na discussão de uma determinada questão, respeitando o modo de pensar dos colegas e aprendendo com eles.

Os conteúdos matemáticos geralmente estão divididos em quatro campos: aritmética, álgebra, geometria e probabilidade e estatística. Esses campos reúnem um conjunto de ideias fundamentais para o desenvolvimento das competências matemáticas, são elas:

- Equivalência;
- Ordem;

- Proporcionalidade;
- Interdependência e variação;
- Representação e aproximação.

A BNCC traz uma divisão da área de conhecimento da Matemática em cinco Unidades Temáticas, que se correlacionam para a orientação e formulação de habilidades a serem desenvolvidas nessa etapa escolar, para que o aluno consiga fazer observações de situações empíricas e as represente matematicamente.

- **Números** - Desenvolver o pensamento numérico, quantificar, interpretar com base em quantificações, fazer aproximações, identificar proporcionalidades e equivalências, ordenar conjuntos. Deve-se enfatizar os registros, usos, significados e as operações de cada conjunto numérico.

Nessa unidade temática é de fundamental importância o estudo de conceitos básicos de economia e finanças, principalmente trabalhado em conjunto com outras disciplinas. Incorporar no currículo a educação financeira além de desenvolver as competências matemáticas, desenvolverá competências pessoais e sociais do aluno, fundamentais para sua vivência em sociedade.

- **Álgebra** -Desenvolver o pensamento algébrico, utilizar modelos matemáticos para compreender, representar e analisar relações quantitativas de grandezas relacionadas a diferentes contextos, identificar regularidade e padrões em sequências numéricas e não numéricas, representar as leis matemáticas em linguagem simbólica e gráfica. As principais ideias atreladas a essa unidade temática são: equivalência, variação, interdependência e proporcionalidades.

Assim na proposta da BNCC a álgebra deve estar presente desde o Ensino Fundamental - Anos Iniciais, com a representação de padrões e regularidades e nas propriedades da igualdade, sem a representação simbólica, que será trabalhada apenas no Ensino Fundamental-Anos Finais. Nessa fase além de aprofundar os conhecimentos adquiridos na etapa anterior, o aluno deve compreender o conceito de variável, estabelecer generalizações em linguagem simbólica, trabalhar técnicas de resolução de equações e inequações, inclusive sua representação gráfica.

O pensamento algébrico deve contribuir para o pensamento computacional, utilizando formas alternativas na resolução de algoritmos matemáticos. Ao se trabalhar com a resolução de algoritmos complexos, podemos decompor em processos sequenciais mais simples. Esse processo de pensamento simplificado é trabalhado em **linguagem de fluxograma**, que consiste em algoritmos gráficos indicando ações de modo simples e objetivo.

- **Geometria** - Resolver problemas do mundo físico, sua posição e deslocamento no espaço, reconhecer e classificar formas geométricas planas e espaciais e seus elementos, investigar propriedades, fazer conjecturas e produzir argumentos relacionadas as formas, analisar as transformações geométricas, principalmente as simetrias. As ideias relacionadas a essa unidade temática são: construção, representação e interdependência.

Deve-se trabalhar os conceitos de geometria no plano cartesiano, não só com materiais físicos, como o papel quadriculado, mas também com a utilização de *softwares* de geometria, como por exemplo o *GeoGebra*.

O raciocínio hipotético dedutivo deve ser trabalhado nessa unidade temática, aproximando-a da unidade temática de álgebra. Porém a geometria não pode ser tratada apenas como classificação, cálculos e aplicações de teoremas, e sim como o entendimento das formas presentes no mundo real.

- **Grandezas e Medidas** - Compreende medidas e as relações entre elas (métricas), integrar a matemática a outras áreas, consolidar e ampliar a noção de número, de geometria e de álgebra.

As medidas quantificam as grandezas do mundo físico, assim nos primeiros anos do Ensino Fundamental, espera-se que os alunos sejam capazes de medir e comparar grandezas com uma unidade (padronizada ou não padronizada), principalmente em situações envolvendo compra e venda de produtos, a fim de desenvolver atitudes éticas e responsáveis com relação ao consumo. Também deve ser trabalhado interdisciplinarmente como por exemplo na utilização de escalas (Geografia) e densidade de corpos (Ciências).

Nos anos finais do Ensino fundamental além das habilidades adquiridas na etapa anterior serem aprofundadas, espera-se que os alunos consigam reconhecer comprimento, área, volume e ângulo de formas geométricas como grandezas e que resolvam problemas com unidades de medidas. Também deve-se trabalhar junto com outras áreas, grandeza como a velocidade pode ser trabalhada junto com a disciplina de Ciências.

Com a evolução constante das tecnologias no cenário contemporâneo é necessário incorporar o estudo das medidas de capacidade de armazenamento, utilizadas em computadores, *tablets* e *smartphones*, como também suas unidades de medida e os prefixos utilizados em suas nomenclaturas.

- **Probabilidade e Estatística** - Coletar, organizar, representar, interpretar e analisar dados em diferentes contextos. Raciocinar e utilizar conceitos, representações e índices estatísticos para descrever e explicar fenômenos, como também para fazer previsões sobre eles.

Nessa unidade temática deve-se estudar a incerteza e o tratamento de dados, utilizando as tecnologias, como planilha eletrônica e *softwares* para a construção de gráficos, trabalhando interdisciplinarmente principalmente com geografia e utilizando a base de dados do Instituto Brasileiro de Geografia e Estatística (IBGE), analisando situações do mundo real.

Nos anos iniciais, em probabilidade, os alunos devem ser levados a compreender que nem todos os fenômenos são determinísticos e que entendam a noção de aleatoriedade. Devem também ser capazes de interpretar eventos dentro de um espaço amostral. Nessa etapa deve-se trabalhar com temas escolhidos pelos próprios alunos. Já nos anos finais conteúdos anteriores devem ser aprofundados, devem fazer experimentos e simulações comparando dados teóricos com a realidade.

Em estatística, nos anos iniciais os alunos devem saber coletar dados e interpretá-los, construindo tabelas e gráficos (colunas) para representá-los. Nos anos finais devem também saber argumentar e tirar conclusões sobre uma pesquisa, saber calcular medidas de tendência central, como construir gráficos (dos mais variados tipos). É fundamental que saibam analisar quando as pesquisas são amostrais ou censitárias, e quando é necessário fazer uso delas. Trabalhar a interdisciplinaridade também se faz necessário nessa área.

A BNCC organizou as habilidades em cada ano escolar, mas essa organização não é obrigatória, é apenas uma sugestão. Cada entidade escolar tem autonomia para elaborar seu currículo, porém devem garantir que os conteúdos mínimos sejam trabalhados, assim teremos um ensino mais nivelado no território brasileiro, objetivo principal do documento.

A definição das habilidades e a progressão anual foram baseadas na compreensão e utilização de novos conteúdos, aumentando gradativamente o nível de exigência das situações problemas, de acordo com as competências trabalhadas.

As Unidades temáticas mesmo estando separadas, não devem ser pensadas isoladamente na construção de uma atividade, que deve contemplar as competências gerais. Uma situação bem simples em que as unidades temáticas podem ser relacionadas é pedir para o aluno que planeje uma viagem, para isso ele deverá possuir as seguintes competências:

- Ler um mapa para localizar-se e analisar a melhor rota (Geometria);
- Informar-se quanto aos valores de combustível e pedágios, além do valor para acomodação e alimentação (Números);
- Obter informações climáticas para decidir o que levar para vestir (Probabilidade e Estatística);
- Analisar propostas de passeios extras e refeições, individuais ou em grupo (Grandezas e medidas);
- Planejar o gasto total da viagem (Álgebra).

Uma atividade que parece bem simples, mas que contempla a proposta da Base, que exige de nós educadores uma maneira diferenciada de planejar as atividades que levaremos para sala de aula.

Para entender um pouco mais da proposta da BNCC, para o ensino Fundamental - Anos Finais e também para a área da Matemática, fiz dois cursos online, um da Nova Escola - Competências Gerais na BNCC [8] e outro pelo AVAMEC - A BNCC nos Anos Finais do Ensino Fundamental: Matemática [9] .

No documento da BNCC [1] o leitor encontrará um quadro com as unidades temáticas e seus Objetivos de Conhecimentos e também as Habilidades, específicos de cada ano da etapa do Ensino Fundamental - Anos inicias (páginas 276 a 295) e Ensino Fundamental - Anos Finais (páginas 298 a 317).

Não mencionaremos neste trabalho todos os Objetivos de Conhecimentos e as Habilidades da área de matemática do Ensino Fundamental, apenas as que são pertinentes ao desenvolvimento do presente trabalho.

1.2.3 A etapa do Ensino Médio

A intenção da Base Nacional Comum Curricular para o Ensino Médio é a mesma, assegurar uma educação igualitária em todo território brasileiro. Mas nessa etapa é necessário um outro olhar para a matemática, pois os alunos já são jovens e começam a se preparar para seu futuro profissional, assim essa área é chamada de Matemática e suas Tecnologias.

A proposta é aprofundar e ampliar os temas já trabalhados no Ensino Fundamental, porém com uma visão mais integradora da matemática com situações da realidade, levando em conta as vivências e o cotidiano do aluno. Também deve-se levar em conta as condições

socioeconômicas dos alunos, a oferta de trabalhado na região em que estão inseridos e o desenvolvimento tecnológico potencializado pelas mídias sociais.

A finalidade dessa área é aproveitar todo potencial já adquiro do estudante, promovendo e estimulando ações para promover a reflexão e abstração, consolidando o senso crítico, analítico, indutivo, dedutivo e sistêmico, a fim de que tomem decisões orientadas pela ética e pelo senso comum. Para isso os alunos devem desenvolver habilidades que envolvam investigação e construção de modelos na resolução de problemas.

Raciocinar, representar, argumentar, comunicar e argumentar em grupo as validações de conjecturas feitas e também representar os procedimentos são habilidades fundamentais nesta etapa.

Cada habilidade está associada a competências que o aluno deve adquirir:

- Argumentar - espera-se que sejam capazes de investigar, explicar e justificar a resolução de problemas em interação com os demais colegas e o professor.

- Representar - elaborar registros matemáticos para a compreensão dos fatos, de ideias e de conceitos, embasando os resultados obtidos com as atividades.

- Justificar - justificar os resultados e conseguir interpretar os resultados obtidos pelos outros colegas da turma, usando símbolos e conectivos matemáticos como também a língua nativa, são competências relacionadas a habilidade de comunicar.

- Investigar - formular e testar conjecturas, justificando os procedimentos utilizados na obtenção dos resultados.

Assim os cinco Campos da Matemática, aritmética, álgebra, geometria, probabilidade e estatística e grandezas e medidas, estão interligadas no Ensino Médio, foram adotados "pares de ideias"que englobam esses campos:

- **Variação e Constância** - Observar, imaginar, abstrair, discernir e reconhecer características que sofreram ou não variação, expressar e representar padrões. Trabalhar em conjunto com outras áreas do conhecimento, incorporando indagações que mobilizem o processo de abstração essencial para o desenvolvimento da criatividade.

- **Certeza e Incerteza** - Estudar fenômenos aleatórios obtendo medidas do mundo físico, estimar, analisar e fazer inferências estatísticas. Busca pela certeza elaborando conjecturas e predições, criar estratégias e validando-as e também imaginar o que aconteceria na extrapolação dos limites impostos, individual e em grupo, trabalhando com atividades que envolvem contagem e de formas intuitivas de expressar a probabilidade de ocorrência de determinado evento. Essas competências são importantes para a comunicação social dos alunos.

- **Movimento e Posição** - Localizar, números na reta numérica, figuras e configurações no plano cartesiano e no espaço são necessários para entender a ideia de posição de um objeto. Para entender o movimento é necessário que o aluno saiba conceitos de direção, sentido, ângulo, paralelismo, perpendicularismo. As transformações geométricas também se fazem importantes nessa área, como também a utilização de mapas, GPS e softwares de localização e posição.

- **Relações e Inter-relações** - Trabalhar com situações problemas que envolvem proporcionalidade (direta e indireta) entre grandezas que são interdependentes. A

> ideia de inter-relação se dá nos campos da matemática, principalmente entre álgebra e geometria, assim o aluno deve entender a noção de função e sua representação geométrica e também movimento de figuras, reflexão, translação e rotação através da álgebra.

A BNCC traz uma visão da matemática diversificada em suas práticas, tentando mostrar que ela é baseada no desenvolvimento humano. A matemática independe de raça, língua, religião ou condição social para se comunicar, portanto é fundamental para o desenvolvimento do ser humano. Devemos mostrar aos alunos que matemática não são apenas regras e cálculos e sim que faz parte de nossas vidas, cultura e história.

Portanto os conhecimentos adquiridos no Ensino Médio devem consolidar o letramento matemático dos alunos, os capacitando para entender conceitos do mundo físico. Para isso foram desenvolvidas as cinco Competências Específicas para o Ensino Médio na área de Matemática e suas Tecnologias.

> 1. Utilizar estratégias, conceitos e procedimentos matemáticos para interpretar situações em diversos contextos, sejam atividades cotidianas, sejam fatos das Ciências da Natureza e Humanas, ou ainda questões econômicas ou tecnológicas, divulgados por diferentes meios, de modo a consolidar uma formação científica geral.
> 2. Articular conhecimentos matemáticos ao propor e/ou participar de ações para investigar desafios do mundo contemporâneo e tomar decisões éticas e socialmente responsáveis, com base na análise de problemas de urgência social, como os voltados a situações de saúde, sustentabilidade, das implicações da tecnologia no mundo do trabalho, entre outros, recorrendo a conceitos, procedimentos e linguagens próprios da Matemática.
> 3. Utilizar estratégias, conceitos e procedimentos matemáticos, em seus campos (Aritmética, Álgebra, Grandezas e Medidas, Geometria, Probabilidade e Estatística), para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentação consistente.
> 4. Compreender e utilizar, com flexibilidade e fluidez, diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional etc.), na busca de solução e comunicação de resultados de problemas, de modo a favorecer a construção e o desenvolvimento do raciocínio matemático.
> 5. Investigar e estabelecer conjecturas a respeito de diferentes conceitos e propriedades matemáticas, empregando recursos e estratégias como observação de padrões, experimentações e tecnologias digitais, identificando a necessidade, ou não, de uma demonstração cada vez mais formal na validação das referidas conjecturas.

Cada uma das competências possui um conjunto de habilidades que não entraremos em detalhes neste trabalho, o leitor que se interessar pode acessar o documento da BNCC [1] (páginas 525 a 535).

Para o bom desenvolvimento integral do estudante nesta etapa escolar, é fundamental que ele já tenha desenvolvido o "pensamento computacional"e sua representação na solução de problemas e algoritmos na linguagem de fluxogramas, para colocar em prática na programação de *softwares* e aplicativos em linguagem de programação.

No próximo capítulo traremos de forma mais aprofundada o que seria esse pensamento computacional e a linguagem de fluxogramas.

2 Fluxograma

No ano de 2019, participei de uma palestra de formação para professores da área de Matemática, oferecida pela secretaria de educação da cidade onde sou professora efetiva, cujo tema era o fluxograma. O tema foi escolhido pela necessidade e preocupação da prefeitura em adequar-se a BNCC.

Eu já possuía conhecimento sobre o tema, pois foi parte integrante da grade curricular da minha graduação de licenciatura em Matemática, porém foi trabalhado apenas com o conceito de programação de *software*.

Foi nessa palestra que percebi a vantagem de se utilizar os fluxogramas aplicados em algoritmos matemáticos, pois são mais visuais e contemporâneos. Outra vantagem é que nos fluxogramas quebramos um algoritmo considerado complexo em partes mais simples e de fácil entendimento. Assim basta seguir as orientações que o algoritmo será realizado sem maiores dificuldades.

Entretanto, quando comecei a pesquisar, percebi como era difícil encontrar modelos de fluxogramas com aplicações matemáticas. A maioria tratava da realização de tarefas simples do dia a dia, como por exemplo acender uma lâmpada. Infelizmente muitos fluxogramas continham erro de conceito ou de fluxo.

Pesquisei também no Google Acadêmico trabalhos sobre o tema fluxograma, mas os resultados se tratavam de fluxogramas em outras áreas, com por exemplo saúde [2] [3]. Além disso, os fluxogramas tinham apenas a finalidade de organização de processos. Pesquisei também fluxograma aplicado a matemática, os resultados encontrados tratavam-se principalmente da BNCC [5] e de alguns exemplos de atividades de modelagem matemática [10]. Assim, percebi a necessidade de um documento de orientação sobre o conceito e estrutura.

Até mesmo a regulamentação dos fluxogramas (ISO 5807 - 1985) é difícil de encontrar, pois seu acesso não é gratuito. Podemos encontrar alguns trabalhos acadêmicos, principalmente nas áreas de engenharia [11] e computação [12], que trazem em seu conteúdo essa regulamentação.

Procurei também no site do MEC [13] alguma justificativa referente a escolha dos fluxogramas para representar algoritmos matemáticos, porém nada encontrei. Nesse site pode-se encontrar o percurso até a homologação da BNCC, os encontros realizados para discussão da formulação do documento, as críticas, sugestões e pareceres de entidades que foram convidadas a participar do processo. A Sociedade Brasileira de Matemática (SBM), foi uma das entidades convidadas, ela fez críticas aos conteúdos propostos, mas não se encontra nenhuma crítica referente aos fluxogramas. No site da BNCC [14] pode-se encontrar todos os pareceres separados por área de conhecimento.

Ainda procurando por justificativas, encontrei uma carta da Sociedade Brasileira de Computação (SBC), a qual apresenta severas críticas à escolha.

A SBC é o órgão responsável pelas Diretrizes Curriculares de todos os cursos de nível superior de computação no Brasil. É extremamente ativa e possui secretarias regionais em todos os estados. Esteve disposta a ajudar o Ministério da Educação (MEC) e o Conselho Nacional de Educação (CNE), no processo de inclusão da Computação no currículo das redes escolares.

A proposta da Base Nacional Comum Curricular, é de implantar o "pensamento computacional"em todo o território nacional, a SBC fez críticas e sugestões, com embasamentos feitos por uma comissão de especialistas da área de computação, quando participou de várias audiências públicas. O órgão alega não ter sido considerado nada do que propuseram na versão homologada da BNCC.

Eles consideram de fundamental importância do ensino da computação na educação básica, pois, supõe ser a única solução para formar cidadãos habilitados ao século XXI. Caso não fosse incorporada ao currículo das escolas, geraria uma ainda maior desigualdade social e econômica, além de obstruir o desenvolvimento científico do Brasil.

Foram feitas críticas as Competências e Habilidades e aos Objetos de Conhecimentos referentes à área da computação na BNCC. Antes de apresentar a análise técnica, gostaríamos de ressaltar os seguintes pontos:

Análise das habilidades relacionadas à Computação na BNCC do Ensino Fundamental segundo a SBC [15].

- A construção de algoritmos não é ensinada: Não há nenhuma habilidade ou objeto de conhecimento relacionado ao aprendizado de construção de algoritmos, que é o tópico central do pensamento computacional. É ingênuo acreditar que o aluno aprenderá somente "fazendo", sem ser apresentado de forma sistemática às abstrações necessárias e nem às técnicas de construção de algoritmos.

- Linguagem muito específica: É sugerida uma linguagem muito específica para a representação de algoritmos (fluxograma), o que é inadequado para uma base comum curricular, que deve deixar a escolha de linguagens específicas para as implementações. Na área de Computação, como surgem novas linguagens para representar algoritmos com grande frequência, não se define linguagens específicas nem em currículos (que são mais concretos que diretrizes).

- Linguagem inadequada: Fluxograma é uma linguagem criada na década de 60/70, não é uma linguagem que segue o paradigma de programação estruturada e não estimula o uso das principais técnicas de solução de problemas através de algoritmos (decomposição, generalização, transformação). A inclusão de conceitos como "fluxograma"no Ensino Fundamental não somente prejudica o desenvolvimento do pensamento computacional, bem como certamente trará graves problemas na aprendizagem de algoritmos.

- Habilidades mal formuladas: Várias habilidades são extremamente específicas e sua real necessidade é questionável.

- Falta de relação entre habilidade e objeto de conhecimento: algumas habilidades não tem uma relação evidente com o objeto de conhecimento ao qual estão relacionadas.

- Pensamento computacional não é desenvolvido: Não há nenhum objeto de conhecimento ou habilidade que trabalhe os princípios do pensamento computacional. Esta habilidade deve ser construída ao longo dos anos, e de maneira sistemática e incremental.
- Mundo Digital não é apresentado: Na BNCC, todos os conhecimentos sobre o Mundo Digital foram ignorados, a despeito de ser sempre ressaltada a importância da BNCC na formação do cidadão completamente inserido no Mundo Digital.

Segundo a SBC, se não forem feitas as devidas alterações, sugeridas pelo órgão, será extremamente prejudicial a Educação Básica do Brasil. Para eles, o pensamento computacional não se baseia em traduzir situações dadas em outras linguagens, e sim, a habilidade relacionada a construção de soluções para determinados problemas. Envolve descrição e generalização dos processos e sua automação e análise. Outro ponto de divergência trata-se do conceito de variável na Matemática e na Computação, que pode ter diversos sentidos, tornando seus objetivos completamente distintos.

Sua principal crítica as Habilidades de Matemática proposta pela BNCC é o porquê da escolha específica de fluxogramas na representação de algoritmos como pensamento computacional, já que existem diversas linguagens mais atuais, pois consideram os fluxogramas uma forma ultrapassada. Na página da SBC você pode encontrar um vídeo [16] curto sobre o que eles acreditam ser o ensino de computação.

Não encontrei nenhuma devolutiva ou justificativa do Ministério da Educação referente ao questionamento da escolha específica dos fluxogramas por parte da Sociedade Brasileira de Computação.

Mas como a BNCC já foi homologada, e estará vigente por um período de tempo considerável, juntamente com ela vem inserida as habilidades referentes aos fluxogramas, precisamos então, compreender melhor esse novo método algorítmico, "os fluxogramas", que é a grande novidade na área da Matemática na BNCC. Assim, como em toda novidade, é necessário um tempo de adaptação e estudos sobre essa nova maneira de realizar as famosas "continhas", como costuma-se dizer. Será uma novidade para os alunos, e também, para os professores.

Nesse contexto, buscando mais informações sobre esse assunto, participei no ano de 2019 da comissão para a escolha do material didático apostilado que seria implementado na rede municipal de Ensino Infantil e Fundamental da cidade que sou professora. Foram três empresas que participaram do processo de licitação. Fazendo a análise do material fiquei com a impressão de que as empresas, para dizerem estar contemplando a BNCC, incorporaram em seu material alguns exemplos bem básicos de fluxograma, muitas vezes até mesmo com erro de conceito, principalmente confundindo-os com organogramas. Elas pareciam não estar preocupadas em realmente trazer no material didático a estrutura correta, prejudicando assim o aprendizado do aluno quanto ao conteúdo. Não traziam em momento algum, nem mesmo no material do professor, informações sobre o conceito e execução de fluxogramas.

Analisei também o material enviado pelo Programa Nacional do Livro Didático (PNLD) em outra escola que também sou professora. Foram quatro coleções enviadas para a escolha, nelas encontrei os mesmos problemas.

Infelizmente vivemos em um país em que, não só os governantes, mas também a sociedade civil, estão preocupados apenas com dados estatísticos. Me entristece saber que coleções assinadas por matemáticos respeitados pela sociedade, inserem em seus materiais

didáticos conceitos errados, só para poderem participar de licitações. Os profissionais que fazem parte da revisão também não se preocupam em analisar a fundo o material que será entregue aos alunos. As esferas federais, estaduais e municipais, tão pouco se importam, pois só interessa o resultado obtido com as avaliações nacionais.

Quem sai prejudicado com tudo isso são nossos alunos, pois sendo um material respeitado no mercado, o professor irá confiar no que ele apresenta e transferirá ao aluno conceitos errados. Também temos o problema da internet, pois hoje nosso aluno quando desconhece algo, acaba por fazer pesquisas, e infelizmente muitos consultam apenas a primeira página que aparece no site de busca. Entretanto, como já dito, muitos exemplos apresentam erro de conceito e estrutura, e quase nenhum exemplo refere-se a algoritmos matemáticos. Logo toda a ideia proposta pela BNCC "vai por água à baixo". Esse aluno, que deveria estar apto a resolver situações problemas por sistemas de fluxograma e que também conseguiria facilmente compreender a linguagem envolvida por trás da programação de *software*, não terá o conhecimento adequado para tais funções.

Essa foi a grande motivação deste trabalho, ajudar os meus colegas de profissão nessa busca por conhecimento e orientação sobre os fluxogramas.

A computação

A computação originou-se da necessidade humana de efetuar trabalhos repetitivos e rotineiros e, principalmente, no auxílio a cálculos e algoritmos. Ao longo dos anos, com a evolução da internet, vem se tornando imprescindível o uso das mais diversas tecnologias em tarefas do cotidiano, das mais simples, como conversar com outras pessoas sem fazer chamada telefônica, as mais complexas, como por exemplo, encontrar um número Primo de Mersenne. A internet foi responsável por tamanha revolução no modo como vivemos hoje em dia, muito diferente dos nossos antepassados.

O computador é capaz de realizar cálculos e tomar decisões lógicas em velocidade extremamente mais rápida que os humanos. Mas para que ele realize determinada tarefa, é necessário que seja programado. Essa programação deve ser detalhada, pois, qualquer falta de informação pode gerar um erro na execução da tarefa. Esta descrição recebe o nome de *software* (programa) e o computador (*hardware*) é apenas uma máquina, que por si só, não é capaz de realizar nenhuma tarefa, precisando de um usuário para programá-lo.

O *software* nada mais é do que uma sequência de instruções, escritas em linguagem de programação, informando ao *hardware* o que deve fazer e a ordem em que deve fazer determinada tarefa. Para que isso funcione é necessário um sistema operacional que gerencia o acesso dos programas ao teclado, ao monitor, mouse, dispositivos de armazenamento de dados, conexão com internet, entre outros. Ele fica ativo o tempo todo para que os programas e aplicativos possam executar suas funções.

Linguagem de programação é um conjunto de regras que permite a construção de sentenças que descrevem de forma precisa as ações que desejamos ser executada pelo computador. Linguagem de máquina é o conjunto de instruções capazes de ativar diretamente os dispositivos eletrônicos do computador. É constituída somente por algarismos 0 e 1 (que tem 1 *bit* de unidade), muito diferente da linguagem usual, o que é inviável para a leitura e compreensão dos seres humanos, mas é a forma como a máquina lê informações. Por exemplo a letra "A"que conhecemos para o computador é "10000001".

Não daremos ênfase nesse assunto, pois, não é o interesse deste trabalho. Caso o leitor se interesse mais sobre essa parte, sugiro que procure por títulos da área de computação.

O que é um algoritmo?

Um algoritmo nada mais é do que a descrição lógica das ações a serem executadas no cumprimento de uma tarefa, ou seja, é uma sequência de passos que levem ao resultado final. É importante que:

- Cada passo deve ser uma instrução simples e sem ambiguidade;
- A ordem dos passos deve ser precisamente determinada;
- Deve possuir um fim, ou seja, um número finito de passos.

Pode ser representado como:

- Descrição narrativa;
- Fluxograma ou diagrama de blocos;
- Pseudocódigo.

O objetivo deste trabalho são os algoritmos escritos na forma de fluxograma, logo abordaremos esse assunto mais a fundo.

Os fluxogramas

Inicialmente os fluxogramas surgiram para documentar processos de negócios nos anos de 1920 a 1930. Em 1921, Frank e Lillian Gilberth, engenheiros industriais, apresentaram a Sociedade Americana de Engenheiros Mecânicos (ASME), o que chamaram de gráfico de fluxo de processos. No início dos anos 1930, Allan H. Morgensen, também engenheiro industrial, utilizou-se dessa ferramenta para dar palestras aos seus funcionários sobre eficiência em negócios. Na década de 40 dois alunos de Morgensen foram os responsáveis por difundir esse novo método. Em 1947, a ASME adotou um sistema com símbolos gráficos de fluxos e processos, inspirado nos Gilberth.

Já no final da década, Herman Goldstine e Jonh Van Neumann utilizaram-se dos fluxogramas para desenvolver programas de computador, e a partir desse momento a diagramação foi sendo utilizada cada vez mais em programas de computador e algoritmos dos mais variados tipos.

No Japão, Kaoru Ishikawa, importante figura do ramo de produção, visando a qualidade do serviço, tratou os fluxogramas como uma das principais ferramentas de controle de qualidade.

A história sobre os fluxogramas pode ser encontrada no site da Lucidchart [17]. Esse site foi o mais completo que achei na internet, pois além de contar a história, nele encontra-se o conceito e estrutura dos fluxogramas, baseados no ISO 9001 (mesma regulamentação do ISO 5807 - 1985). Ele foi o material inicial de apoio que me baseei para entender a estrutura e os conceitos envolvendo o fluxograma.

Sendo uma representação visual de fluxo de dados, fluxogramas são indicados para elaboração de programas (coleção de instruções que descrevem uma tarefa) ou construção de um algoritmo, sendo de fácil compreensão com a finalidade de explicar de forma simples, aos demais que necessitem ou desejem realizar determinada tarefa. Pode ser utilizado para descrever a lógica de um programa, mesmo antes dele começar a ser codificado em escrita computacional. Ele é de grande ajuda na organização e sua representação, mostra uma

visão geral, agindo como um guia pelas várias etapas do processo, até que se chegue ao resultado final.

Em Engenharia, o fluxograma é muito utilizado para representar processos industriais. Na saúde é utilizados como se fosse um roteiro para diagnósticos e tratamentos e em empresas são utilizados como mapeamento dos processos e etapas de determinadas funções ou documentos.

Em geral os fluxogramas podem:

- Demonstrar como um código é organizado;
- Visualizar a execução do código dentro do programa;
- Mostrar a estrutura de funcionamento desse programa;
- Entender como os usuários se utilizarão desse programa.

Independente da área os fluxogramas têm as seguintes funções:

- Documentar e analisar um processo;
- Padronizar um processo para melhor eficiência e qualidade;
- Comunicar o processo para treinamento ou compreensão dos demais envolvidos;
- Indicar o mal funcionamento ou repetições desnecessárias em um processo.

Em outras áreas, podemos encontrar fluxogramas com outras funções.

Educação	Vendas/Marketing	Negócios	Fabricação de produtos	Engenharia
Planejamentos acadêmicos	Fluxo de levantamento de dados	Processos de pedidos e compras	Indicação da composição química	Fluxos de processos
Criação de um plano de aula	Processo de vendas	Tarefas dos funcionários	Processos de fabricação do começo ao fim	Fluxos de sistemas
Organização de projetos	Estratégias de pesquisa	Plano de realização do produto	Testes de eficiência dos produtos	Fluxos de engenharia reversa
Estruturas de redações	Fluxos de cadastros	Documentos de regularização de produtos ou serviços		Fases de criação de um protótipo
Algoritmos matemáticos	Planos de emergência	Documentação para a distribuição de produtos		Estruturação de produtos
Processos científicos				
Gestão escolar				

Figura 2.1: Função do fluxograma em determinadas áreas

Como descrito, os fluxogramas nada mais são do que instruções para a realização de tarefas, porém ele é dotado de regras, visando seu pleno entendimento por qualquer pessoa que tenha o mínimo de conhecimento sobre o assunto. Não pode ser confundido com os organogramas, que são estruturas mais simples, que como já diz o nome, são úteis em tarefas de organização. No organograma temos instruções e fluxos, determinados por blocos e setas, já no fluxograma, cada ação é representada por uma forma geométrica específica, o que os torna parecidos são os fluxos.

2.1 Estrutura dos fluxogramas

O fluxograma é um diagrama que representa um processo, sistema ou algoritmo. Podem ser utilizados para documentação, estudos, planejamentos, comunicação de processos, entre outros.

A norma ISO explicita os seguintes tipos de fluxogramas:

- *Data Flowcharts* (fluxograma de dados) - representação do caminho dos dados na solução do problema e definição dos passos de processamento tanto como as várias mídias de dados utilizadas;
- *Program Flowcharts* (fluxogramas de programas) - representação da sequência de operações em um programa;
- *System Flowcharts* (fluxogramas de sistemas) - repreentação do controle das operações e do fluxo de dados de um sistema;
- *Program Network Chart* (diagrama de programação em rede) - representação dos caminhos de ativação dos programas e das iterações com os dados relacionados. Cada programa em um diagrama de programa em rede é mostrado uma única vez, onde, como em um fluxograma de sistema, ele pode aparecer em mais de um fluxo de controle;
- *System Resoucers Charts* (diagrama de recursos do sistema) - representação das configurações das unidades de dados e unidades de processos adaptáveis para a solução de um problema ou de um conjunto de problemas.

Os conceitos envolvidos neste trabalho são referentes aos *Data Flowcharts* (fluxogramas de dados), propostos pela BNCC para trabalhar a construção de algoritmos computacionais e da implementação do pensamento computacional (PC) nas escolas brasileiras.

O termo *Flowcharts* foi traduzido para o português como fluxograma, o termo *flow* está relacionado ao "fluxo"e o termo *chart* está relacionado a "diagrama", portanto a tradução adequada seria "diagrama de fluxos". Talvez essa seja a explicação pela confusão de que faz no Brasil envolvendo os fluxogramas com os diagramas.

Nos fluxogramas cada forma geométrica tem uma função específica que são padronizadas, diferentemente dos diagramas, que são estruturas mais simples.

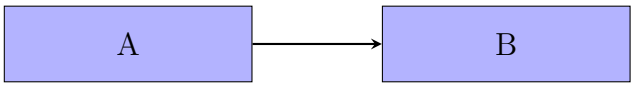
Fazendo pesquisas sobre os fluxogramas pode-se perceber o quanto é difícil encontrar um material sobre o assunto. No início da minha pesquisa acessei a biblioteca da UNESP, lá só encontrei um título que me ajudou a entender alguns conceitos, bem básicos, o livro Fluxogramas e linguagem de programação *basic* e aplicações [18].

Constavam também alguns outros títulos, a maioria referente a fluxogramas utilizados em modelagem matemática. Assim tive que buscar por informações em site da internet e

artigos escritos nas áreas de Engenharia e Computação. Porém os exemplos eram voltados mais para a programação, diferentemente do proposto pela BNCC que é de "pensamento computacional".

É muito complicado trabalhar com um tema novo, não há muito material e precisa ser avaliado a veracidade do que os poucos materiais trazem, assim depois de muito pesquisar obtive os resultados a seguir sobre os símbolos que compõe a estrutura do fluxograma.

Os **Fluxos**, são representados por setas. São responsáveis pela organização das etapas a serem seguidas pelo usuário que precisa realizar a tarefa proposta.



Símbolos mais utilizados nos fluxogramas

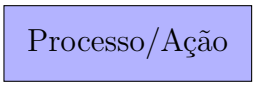
Começaremos com os três símbolos mais básicos e os principais no processo de realização de tarefas e de execução de algoritmos. Nas atividades propostas para o Ensino Fundamental esses três símbolos são de extrema importância.

1 **Terminação**

Todo processo ou algoritmo ou tarefa a ser realizada deve possuir um início e um fim para estar bem definido. Esse símbolo é utilizado com essa finalidade, ou seja, todo fluxograma deve começar e terminar com esse símbolo de formato ovalado.

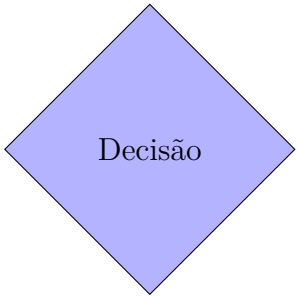
2 **Processo/Ação**

Toda ação deve ser representada por retângulos. Esse símbolo representa um processo, ação ou função. É o símbolo mais usado nos fluxogramas.



3 **Decisão**

As decisões devem ser representadas por losangos. Eles indicam que há uma questão a ser respondida, com "sim"ou "não", gerando ações diferentes para cada resposta, por isso é um símbolo de dupla saída.



Com o conhecimento da função desses três símbolos, qualquer pessoa consegue interpretar e se orientar na realização de uma tarefa ou algoritmo expressa em um fluxograma.

Exemplo 2.1. Média final para aprovação na disciplina de Matemática

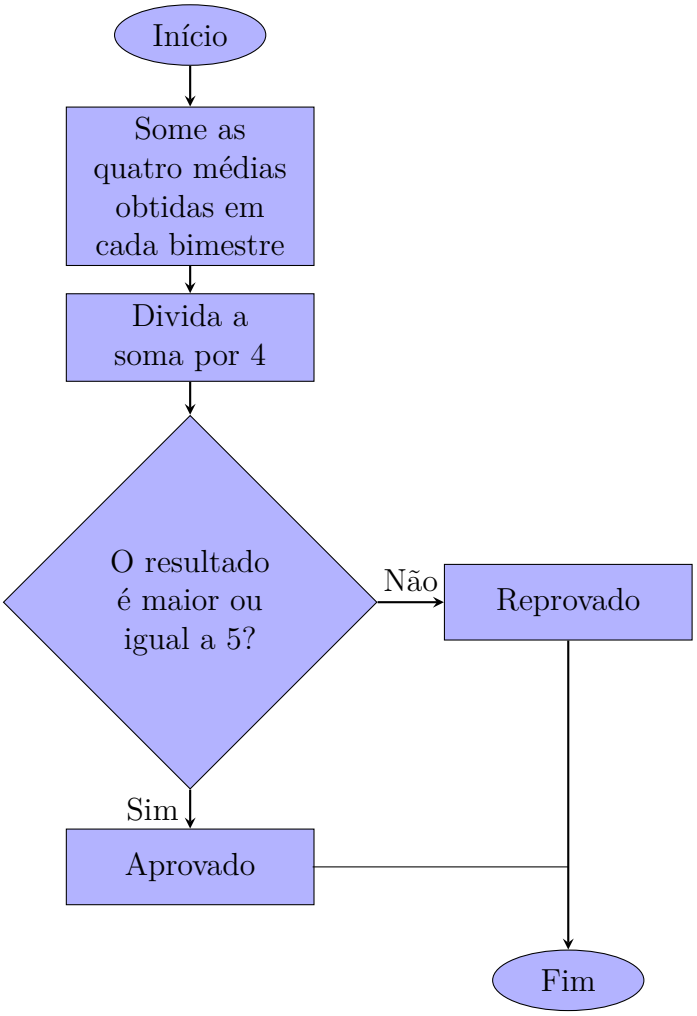


Figura 2.2: Fluxograma de autoria própria - Média aritmética

Esse é um exemplo bem simples, que qualquer aluno com conhecimentos mínimos de matemática e de fluxograma, consegue obter sem que haja explicações de um professor, sua condição ao final do ano letivo: aprovado ou reprovado. Note que nele os comandos são dados de forma simples, facilitando o entendimento. Mais adiante nesse capítulo traremos uma abordagem mais ampla sobre a estrutura dos fluxogramas.

Outros símbolos utilizados nos algoritmos matemáticos

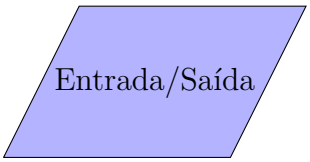
Temos outros símbolos de fluxogramas que não são tão utilizados nos algoritmos matemáticos, mas é fundamental saber sua função. São eles:

4 **Armazenamento de dados**

Este símbolo é utilizado quando precisamos armazenar dados dentro de um processo para posteriormente ser utilizado.

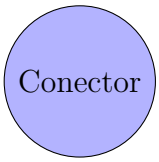
5 **Entrada/Saída**

Este símbolo também é chamado de símbolos de dados, representa dados disponíveis para entradas ou saídas de recursos utilizados ou gerados.



6 **Conector**

Utilizado geralmente em fluxogramas mais complexos e extensos, este símbolo conecta elementos separados em uma página.

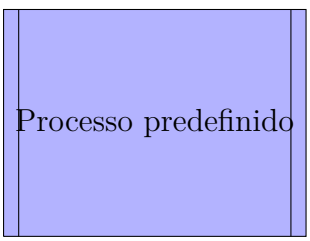


7 **Operação Manual**

Este símbolo indica um passo que deve ser feito manualmente por um ser humano e não automaticamente.

8 **Processo predefinido**

Este símbolo indica um processo ou operação complicada, que é bem-conhecido ou definido, presente em outro local.

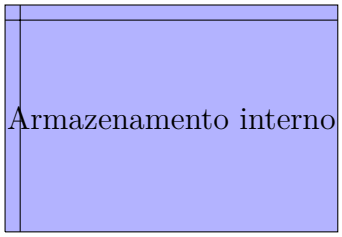


Outros símbolos de fluxograma

Estes símbolos de fluxograma são mais utilizados em processos realizados por uma empresa. Geralmente elas possuem vários departamentos, que precisam se integrar para a obtenção de um produto final.

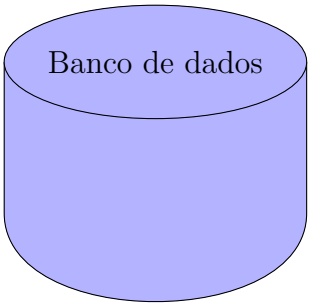
9 **Armazenamento interno**

Este símbolo é utilizado normalmente para mapear projetos de *software*, esta forma indica dados armazenados na memória interna.



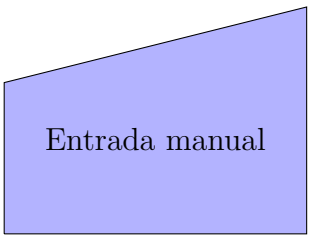
10 **Banco de dados**

Utilizado para representar os dados hospedados em um serviço de armazenamento, que provavelmente permitirá a pesquisa e filtragem por parte de usuários.



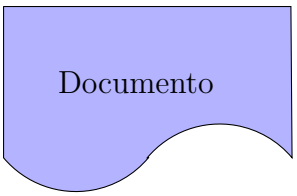
11 **Entrada Manual**

Este símbolo é utilizado para representar a entrada manual de dados em um campo ou passo de um processo, por um teclado ou dispositivo. Como por exemplo um processo de login, em que é solicitado a inserção dos dados manualmente.



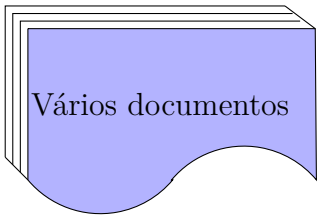
12 **Documento**

Utilizado para representar a entrada ou a saída de um documento. Entrada pode ser o recebimento de um relatório, um e-mail ou um pedido. Já a saída, um memorando ou uma carta.



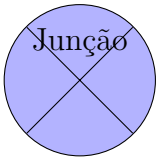
13 **Vários documentos**

Quando temos diversos documentos ou relatórios esse símbolo é utilizado.



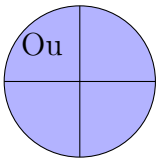
14 **Junção**

Este símbolo é utilizado quando é preciso somar a entrada de vários caminhos convergentes.



15 **Ou**

Este símbolo indica que o fluxo do processo continua para dois caminhos ou mais.



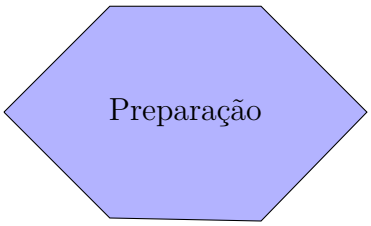
Cuidado para não confundir os símbolos junção e com o ou. Eles são visualmente parecido, mas referem-se a processos diferentes.

16 **Exibição**

Este símbolo é utilizado para indicar onde informações serão exibidas dentro de um fluxo de processo.

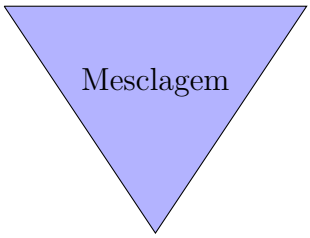
17 **Preparação**

Este símbolo é utilizado na diferenciação entre passos, que preparam para o trabalho e que executam o trabalho. Muito útil na preparação para outra etapa dentro do mesmo processo.



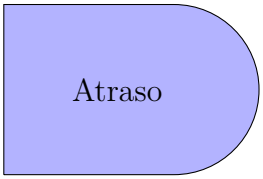
18 **Mesclagem**

Este símbolo combina vários caminhos (fluxos) para virar um só.



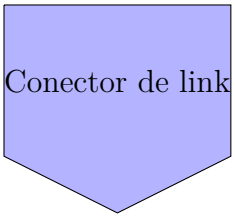
19 **Atraso**

Este símbolo representa um segmento de atraso em um processo.



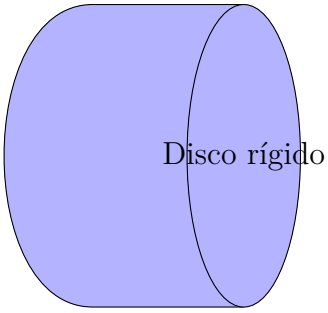
20 **Conector de link**

Utilizado em gráficos mais complexos, que necessita de várias páginas para sua visualização, este símbolo conecta elementos separados pelas páginas. O número da página é normalmente colocado sobre ou dentro da forma.



21 **Disco rígido**

Este símbolo indica onde dados serão armazenados dentro de um disco rígido.



Note que há símbolos para representar funções bem parecidas, com também há símbolos que representam a mesma função, mas o que os diferente é a área em que são empregados.

No pacote Office (*Word, Excel e PowerPoint*) do seu computador ou *smartphone*, você encontra essas formas para criar seus fluxogramas. Porém é um pouco trabalhoso, pois é necessário organizar os símbolos utilizados em seus lugares, verificando o tamanho dos símbolos e o mais dificultoso são os fluxos (setas) que muitas vezes não conseguimos posiciona-las.

Figura 2.3: Formas de fluxograma no pacote *Office*

Você também pode encontrar algumas estruturas prontas, no *SmartArt*, em que é só necessário preencher os campos. Porém, como já mencionado nesse capítulo, não podemos confundir fluxogramas com organogramas. Os modelos predefinidos são, em sua grande maioria, diagramas.

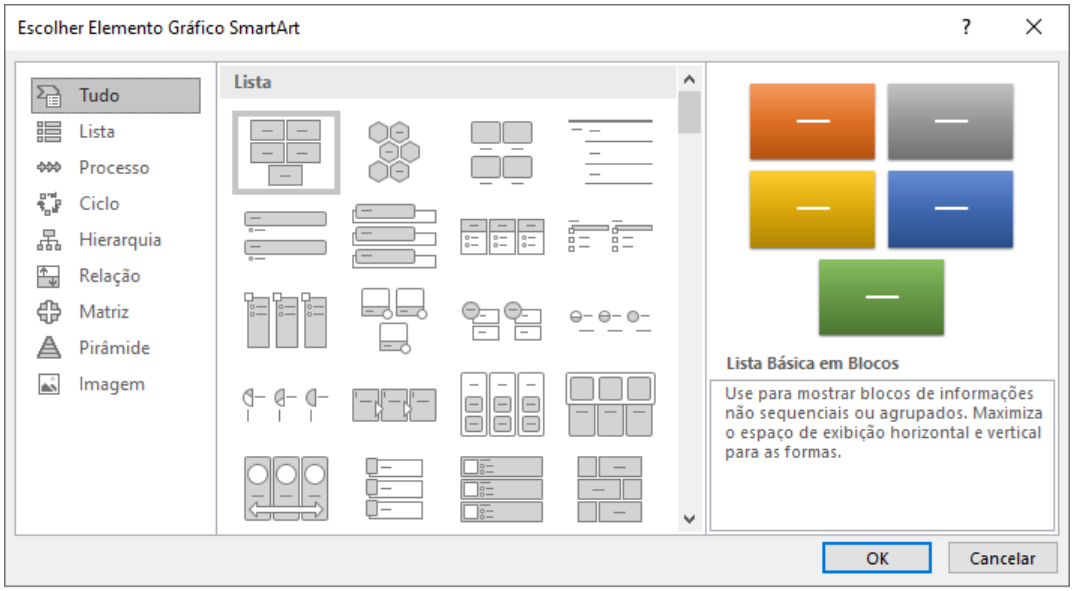


Figura 2.4: *SmartArt*

Também pode ser utilizado o programa *drawio* [19] ou a plataforma *Lucidchart* [17] (parcialmente gratuita) para a construção dos fluxogramas.

Os fluxogramas deste trabalho foram feitos no ambiente *tikz* do *LaTeX*, que é um sistema de preparação de documentos.

Exemplos da utilização dos fluxogramas

A seguir teremos alguns exemplos da utilização dos fluxogramas. O primeiro exemplo é sobre o treinamento de funcionários (atendente de pedidos) no registro de pedido de pizza. Com ele o funcionário estará ciente de todo o processo até a finalização do pedido. Como no fluxograma os processos são expressos de forma bem simples, o novo funcionário não necessita de tanta instrução e supervisão.

Nesse fluxograma pode-se observar a utilização de vários símbolos, que foram especificados, e como não foi suficiente uma folha para visualização, foi utilizado um conector de página.

Exemplo 2.2. Atendimento pizzaria

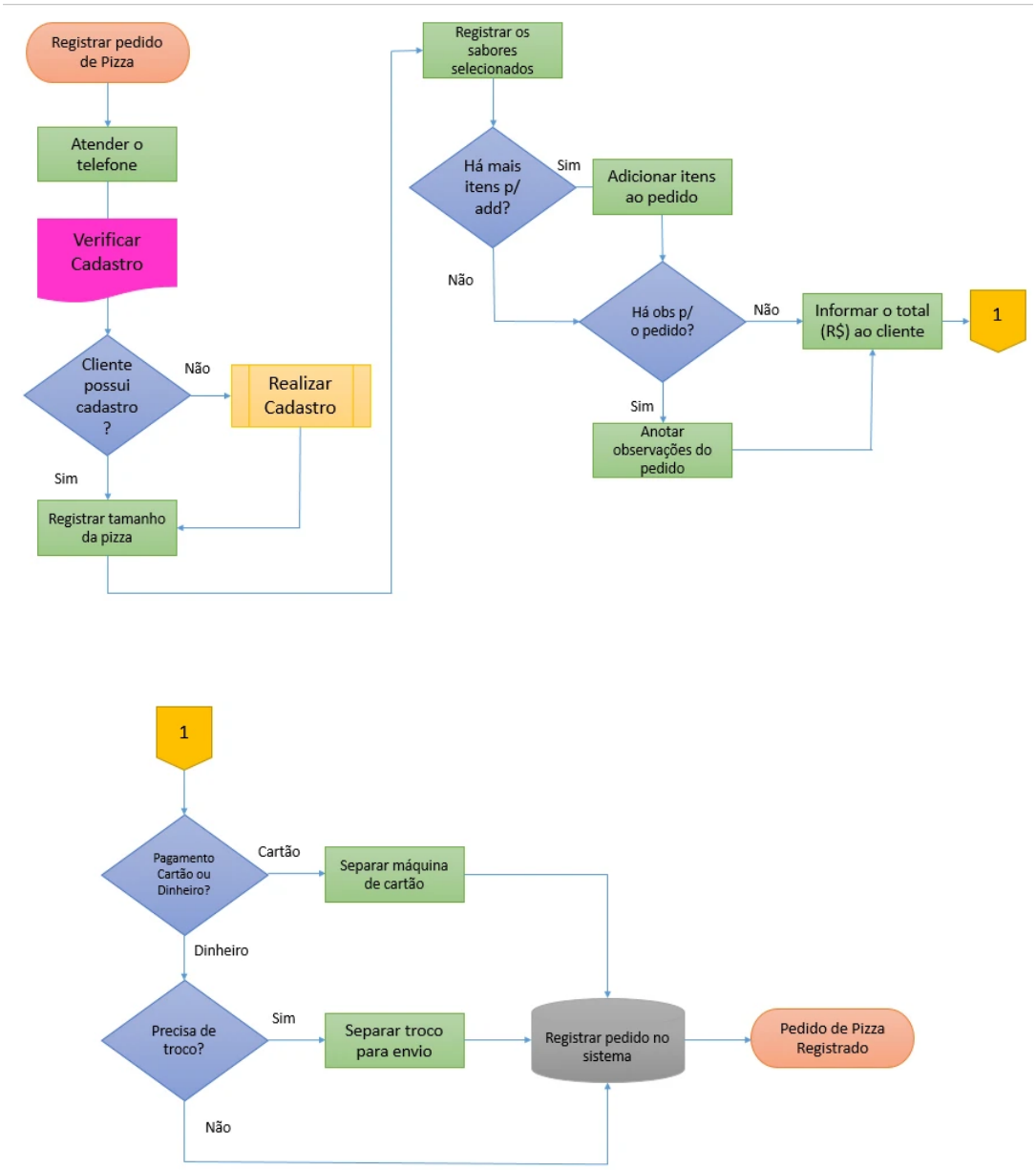


Figura 2.5: Disponível em: https://blog.smlbrasil.com.br/5-passos-para-criacao-de-um-fluxograma/ Acesso em 25/07/2020

Nos símbolos de terminação deveriam conter apenas os dizeres "Inicio"e "Fim", porém da forma como está escrito, não geram confusão na realização da tarefa. Geralmente nos símbolos de processo, chega uma seta e sai uma seta, sendo necessário ajustar os fluxos para garantir a padronização dos fluxogramas. As cores em si, não interferem no fluxograma, podendo ele ser monocromático ou colorido.

Podemos ter fluxogramas bem simples, como no exemplo anterior, como também outros mais elaborados e complexos. Pense na produção de um objeto. Ele passará por vários processos até chegar ao final de sua produção, o exemplo a seguir nos dará uma ideia desse processo.

Exemplo 2.3. Fabricação de um produto

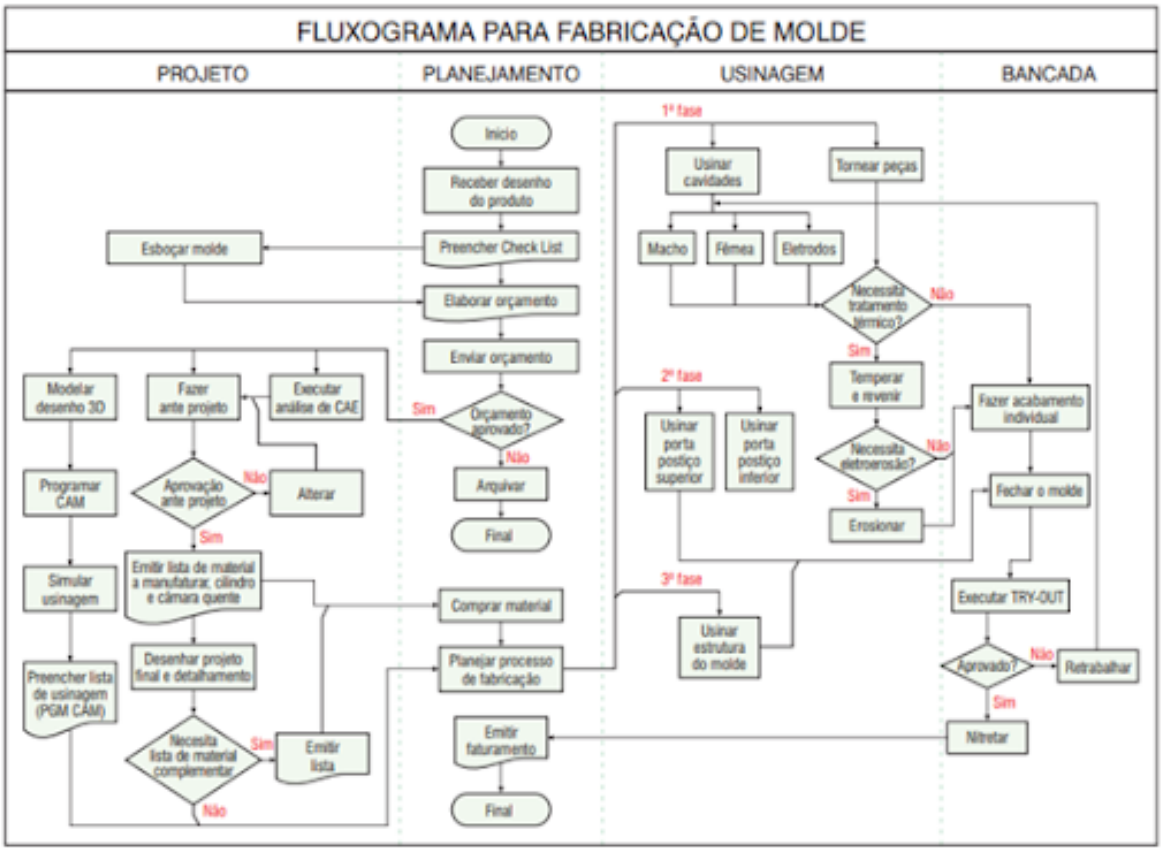


Figura 2.6: Disponível em: http://moldesinjecaoplasticos.com.br/otimizacao-do-fluxograma-do-processo-de-fabricacao-de-moldes-de-injecao-de-termoplasticos/ Acesso em 25/07/2020

As formas, símbolos de fluxogramas, utilizadas neste trabalho, se baseiam nas formas encontradas no *Word, Excel, PowerPoint*, entre outros, que são padronizadas, porém você irá encontrar variações, dependendo da sua pesquisa poderá encontrar símbolos diferentes para a mesma função. Caberá a você a verificação dos conceitos envolvidos. Essas formas são regulamentadas pelo ISO-5807:1985, porém o documento de regulamentação como já dito, não é gratuito, o que dificulta o acesso a informações legítimas.

Existem ainda outras plataformas de construção de fluxogramas e organogramas, a maioria delas não é completamente gratuita. Elas oferecem gratuitamente alguns processos básicos, porém se você realmente quiser utilizar de todos os seus benefícios, terá que pagar uma mensalidade ou comprar um pacote.

Alguns símbolos já ficaram ultrapassados, ou são de pouca utilização, assim não foram citados.

Existem diferentes tipos de fluxogramas, os que utilizaremos neste trabalho são os comumente chamados de **fluxogramas de processos simples**. Outro comumente encontrado é o **fluxograma funcional**, nele é evidenciada a sequência de atividades de um processo entre áreas ou seções por onde ele ocorre.

Exemplo 2.4. Fluxograma funcional

Figura 2.7: Disponível em: https://www.xpms.com.br/blog Acesso em 05/08/2020

Este é um fluxograma funcional bem simples para a fabricação de um determinado produto, nele estão evidenciados os setores do processo sofrido pelo produto.

Exemplo 2.5. Fluxograma vertical

Código do fluxograma: 00025 **Página:** 01 de 01				
Objeto de Estudo / Material / Produto: Pallets	**Atividade**	**Presente**	**Proposto**	**Economia**
	Operação ○	3		
Processo: Recebimento e Armazenagem de Pallets	Transporte ⇨	2		
	Espera D	1		
Local: Armazém W-42	Inspeção □	1		
Método: (X) Presente ( ) Proposto	Armazenagem ▽	1		
Formulado por: Rafael Lima **Data:** 19/03/2016	Distância total (m)	420		
Aprovado por: João Silva **Data:** 23/03/2016	Tempo (min)	105		

	Descrição	Distância (metros)	Tempo (min)	Tipo de Atividade ○ ⇨ D □ ▽	Observações
1	Caminhão estaciona na doca de descarregamento	-	5		
2	Descarregamento dos pallets para a área "Transit"	100	12		Caminhão médio com 10 pallets
3	Conferência do material recebido com NF e *packing list*	-	10		
4	Impressão do relatório de recebimento	20	22		
5	Levar relatório ao motorista e liberar caminhão	10	1		
6	Cadastro dos pallets no sistema e colocação de *tag* RFID	10	22		
7	Empilhadeira armazena pallets nos porta-pallets	250	30		Distância média de 25m por pallet
8	Registro do endereço onde os pallets foram colocados	30	3		

Figura 2.8: Disponível em: https://aprendendogestao.com.br/2016/07/22/fluxograma-vertical-modelo-de-fluxograma/ Acesso em 05/08/2020

Podemos encontrar os **fluxogramas verticais**, também conhecido como diagrama de processo. Seus símbolos são colocados em colunas verticais, sua principal vantagem é a rapidez de preenchimento, a clareza na interpretação e facilidade de leitura. É muito utilizado nos estudos de processos produtivos.

Além da confusão com os organogramas, os fluxogramas também não podem ser confundidos com os chamados **mapas conceituais**, que consistem em um diagrama ou ferramenta gráfica, que representa visualmente as relações entre conceitos e ideias. São utilizados para descrever ideias, utilizam símbolos como caixas ou círculos, são estruturados hierarquicamente e conectados com linhas ou setas, que ajudam a explicar as conexões entre os conceitos.

Exemplo 2.6. Organograma- Hierarquia empresarial

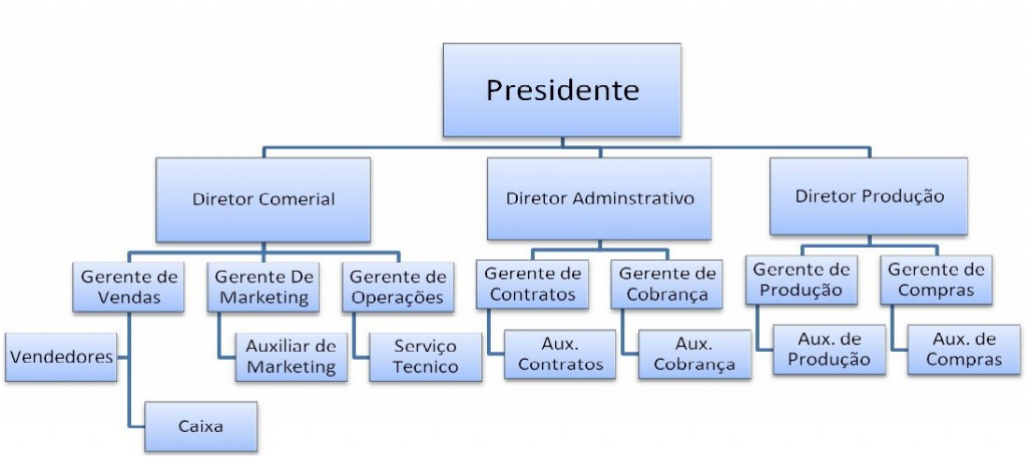


Figura 2.9: Disponível em: https://www.nibo.com.br/blog/modelos-de-organograma-empresarial/ Acesso em 05/08/2020

Exemplo 2.7. Mapa conceitual - Formas geométricas

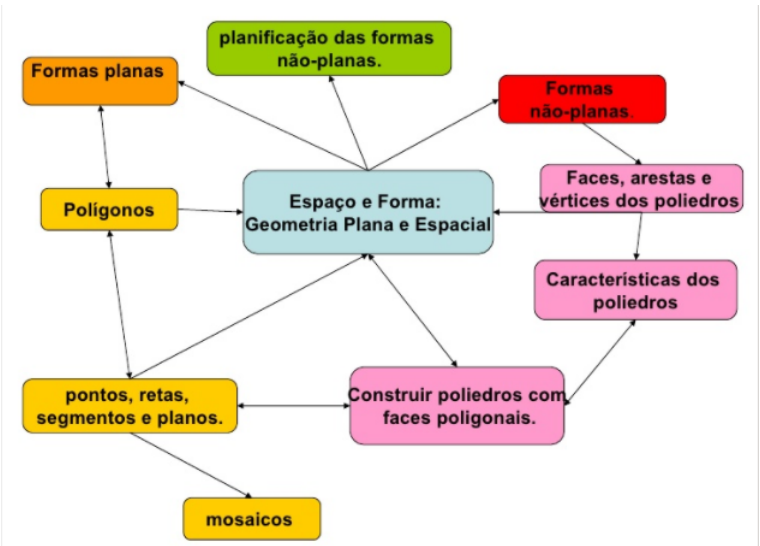


Figura 2.10: Disponível em: https://www.slideshare.net/11021971/mapa-conceitual-4984518 Acesso em 05/08/2020

2.2 Fluxograma na BNCC

A Base Nacional Comum Curricular (BNCC) busca alcançar o letramento matemático, para isso, segundo o documento, é fundamental que o aluno desenvolva três habilidades:

- Resolução de problemas - Desenvolvimento de processos pessoais de resolução de problemas usando diferentes recursos. O aluno aprende enquanto resolve o desafio e também na discussão com os colegas, analisando as estratégias que foram utilizadas na resolução.

- Investigação - Estimula a busca por padrões matemáticos utilizando-se de especulações. O aluno aprende a formular hipóteses e testá-las na busca da solução do desafio. Também é fundamental que ele consiga expressar suas ideias de maneira organizada e de simples compreensão.

- Projetos de modelagem - Construção de modelos para resolver uma situação matemática com base em exemplos já conhecidos. Deve-se relacionar os conteúdos matemáticos com temas significativos para o aluno.

Para alcançar esses objetivos propostos pela base, foi escolhido trabalhar com os fluxogramas, pois atendem as exigências propostas. Os fluxogramas são facilitadores da compreensão de algoritmos , principalmente os mais complexos, pois os "quebram"em partes, mais simples, ajudando o estudante na compreensão do processo de resolução de um problema ou algoritmo, fazendo-os enxergar a Matemática de uma forma diferente.

Os fluxogramas já são utilizados a bastante tempo na área de Computação, tanto na criação como no desenvolvimento de *software* e aplicativos. Antes dos programadores escreverem um programa em linguagem de programação, eles utilizam os fluxogramas para esboçá-lo.

Atrelado ao letramento matemático está o pensamento computacional (PC) que não deve ser confundido como habilidade de manusear aplicativos em dispositivos eletrônicos (Alfabetismo Digital), muito menos como uma forma mecânica de pensamento que limita a criatividade, ou seja, não envolve apenas os conceitos de Computação. Ele também agrega práticas de projetar sistemas, entender o comportamento humano e o pensamento crítico.

A BNCC deixa vago em seu documento o que seria esse pensamento, vamos então nos aprofundar um pouco mais nesse tema, com base em documentos escritos na área da computação. [20] [21]

A ideia do que seria o pensamento computacional passou por mudanças ao longo dos anos. A grande revolução sobre o tema começou em 2006, quando a pesquisadora Jeannette M. Wing alegou que o PC é uma habilidade essencial para qualquer pessoa, independente da área e não somente as pessoas que estão, de uma forma ou de outra, relacionadas com a informática . Ela também definiu o PC como uma combinação do pensamento crítico com fundamentos da computação como metodologia de resolução de problemas, utilizando conceitos básicos da Ciência da Computação para resolver problemas, desenvolver sistemas e para entender o comportamento humano(WING,2006).

Em 2007 ela coloca o PC como um complemento do pensamento matemático, principalmente no campo da Engenharia, que tem base na matemática porém é limitado pela física dos materiais e equipamentos. Com o PC podemos fazer interações com o mundo real porém construindo mundos virtuais contemplando a criatividade da mente humana.

Em 2014 Wing, modifica novamente o termo PC agora como um processo de pensamento envolvido na formulação de problemas e que expressam sua solução ou soluções eficazmente de forma que uma máquina ou uma pessoa possa realizar, podendo ser visto como uma automação ou abstração do pensamento de um cientista da área da computação.

Em 2015 Liukas, coautora do currículo de Computação da Finlândia traz uma interessante visão do PC, como a forma de pensar problemas que podem ser resolvidos por um computador, porém eles não são capazes de executar sozinhos esses problemas, é necessário que uma pessoa os programe. Para que isso aconteça é necessário desenvolver o raciocínio lógico, para decompor um algoritmo complexo e abstrair um problema.

Em 2011 a *International Society for Technology in Education* (ISTE) em conjunto com a *Computer Science Teachers Association* (CSTA) divulga a definição operacional do Pensamento Computacional como um processo de resolução de problemas que inclui (mas não está limitado a) as seguintes características:

- Formulação de problemas de forma que nos permita usar um computador e outras ferramentas para nos ajudar a resolvê-los;
- Organização e análise lógica dos dados;
- Representação de dados através de abstrações, como modelos e simulações;
- Automatização de soluções através do pensamento de algoritmo (uma série de etapas ordenadas);
- Identificação, análise e implementação de possíveis soluções com o objetivo de alcançar a combinação mais eficiente e efetiva de etapas e recursos;
- Generalização e transferências deste processo de resolução para uma grande variedade de problemas.

Para o desenvolvimento pleno dessas habilidades é necessário desenvolver as seguintes qualidades e atitudes:

- Confiança em lidar com a complexividade;
- Persistência ao trabalhar com problemas difíceis;
- Tolerância para ambiguidades;
- Capacidade para lidar com problemas em aberto;
- Capacidade de se comunicar e trabalhar com outros para alcançar um objetivo ou uma solução em comum.

Após estudos sobre o PC os pesquisadores Grover e Pea (2013) elaboraram uma lista com nove habilidades a serem desenvolvidas pelos alunos na escola para que atinjam essa forma de pensamento, são elas:

- Abstração e reconhecimento de padrões (incluindo modelos e simulações);
- Processamento sistemático de informação;

- Sistema de símbolos e representações;
- Noções de controle de fluxo em algoritmos;
- Decomposição de problemas estruturados (modularização);
- Pensamento interativo, recursivo e paralelo;
- Lógica condicional;
- Eficiência e restrições de desempenho;
- Depuração e detecção de erro sistemático

No PC um algoritmo é visto como uma abstração de um processo que recebe uma entrada, executa a sequência de passos e produz uma saída que satisfaça um objetivo específico. É um plano, uma estratégia ou um conjunto de instruções claras necessárias para solucionar um problema. Essas instruções devem ser ordenadas e podem ser escrita em formato de diagramas (como os fluxogramas) ou pseudocódigo (linguagem humana), para depois ser transformado em linguagem de programação.

Atualmente há uma elevada demanda de mão de obra qualificada com conhecimentos em programação, mas compreender o PC vai mais além, pode ajudar na melhoria de processos no nosso cotidiano, possibilitando identificar informações importantes, encontrar e analisar informações úteis, ou até mesmo em tarefas de organização de objetos em um ambiente, como também a organização de documentos em um escritório.

A computação é capaz de expandir horizontes dos seres humanos, através de processos desafiadores, com baixa chances de riscos de dar errado, facilitando a capacidade de abstração, criação e solução de problemas, de várias naturezas e com certa complexividade, de forma crítica.

Outro benefício atrelado ao PC é o desenvolvimento de trabalhos em grupos, onde conhecimentos são compartilhados, análises do resultado são feitas de maneira colaborativa, sempre com busca na otimização dos processos envolvidos na solução de um problema.

Segundo pesquisadores da área de computação, uma estratégia pra inserir o PC no Ensino Básico é ser trabalhado em matérias pré-existentes no currículo escolar, como por exemplo em Matemática. Mas é preciso diferenciar o PC de uma aula de informática, não é apenas saber utilizar a ferramentas tecnológicas, e sim participar de um processo de criação de novas tecnologias, com foco educacional (habilidades de reflexão, solução de problemas, compreensão de mundo e suas necessidades) e também econômico (alta demanda de profissionais nessa área.)

Por esses motivos a BNCC se preocupa com o desenvolvimento desse Pensamento Computacional em nossos alunos. Foi escolhido trabalhar com os fluxogramas na educação básica, pois ele se encaixa nas competências e habilidades que pretende-se atingir com essa maneira de ver o mundo.

No Brasil sabemos da dificuldade de acesso aos recursos tecnológicos, a Fundação *Lemann*, foi fundada em 2002 com a finalidade de desenvolver e apoiar projetos inovadores em educação, realizando pesquisas para embasamento de políticas públicas na educação e oferecendo formação e aprimoramento para profissionais.

O Programae.org.br é um movimento que surgiu para aproximar a programação do cotidianos de jovens brasileiros, pois a veem como um elemento de transformação na vida das pessoas.

Temos também a Supergeeks, que é a primeira escola de robótica para crianças e adolescentes (a partir de 7 anos). Nelas as aulas são baseadas em games, aplicativos, robôs, sistemas, empreendedorismo e língua inglesa (utilizada em programação).

Os alunos que começam um curso de programação (Nível Superior) apresentam dificuldade em codificar processos. Isso causa uma forte evasão e também uma alta taxa de reprovação das disciplinas e até mesmo do curso. Em seu cotidiano o adolescente acha que por se dar bem com os equipamentos tecnológicos, terão o mesmo sucesso em cursos na área de Informática. Eles não conhecem os processos por trás do aparelho, não conhecem ferramentas de programação e não acham que precisarão da Matemática para fazer tudo funcionar, assim quando se deparam com os conteúdos trabalhados no curso, acabam se assustando e muitas vezes ficam desestimulados e acabam por abandonar o curso.

Sabemos da grande dificuldade que nossos alunos e até mesmo as escolas, apresentam com relação a tecnologia. O último censo escolar (MEC/INEP,2017) mostra que 44,2 % das escolas não possuem internet, 48,8% não possuem laboratório de informática e algumas (5,5%) nem sequer possuem energia elétrica.

Esses dados não levam em conta o mal funcionamento e velocidade do *link* da internet, quantidade de computadores, número de máquinas danificadas ou desativadas, instabilidade ou paralisação temporária de energia elétrica. Essas são situações que infelizmente encontramos na maioria das escolas brasileiras.

Visto isso, fica complicado estabelecer as propostas do PC em sala de aula, mas na BNCC foi escolhido os fluxogramas para iniciar esse processo, pois são necessários apenas um papel, um lápis e uma boa aula explicativa para se desenvolver o conteúdo.

A base passou por várias etapas até chegar a sua homologação, sempre focando nas competências que os alunos devem adquirir em seu desenvolvimento escolar e também sua vida profissional e em sociedade. Assim o Pensamento computacional foi inserido apenas na terceira versão do documento, com a finalidade de elaboração, análise e leitura e construção de algoritmos.

Os fluxogramas na BNCC

No documento da Base Nacional Comum Curricular (BNCC) [1], podemos encontrar as seguintes referências aos fluxogramas.

- **Competências específicas de Matemática para o Ensino Fundamental**

  > Enfrentar situações-problema em múltiplos contextos, incluindo-se situações imaginadas, não diretamente relacionadas com o aspecto prático-utilitário, expressar suas respostas e sintetizar conclusões, utilizando diferentes registros e linguagens (gráficos, tabelas, esquemas, além de texto escrito na língua materna e outras linguagens para descrever algoritmos, como fluxogramas, e dados).

  Para a BNCC, competência representa a mobilização de conhecimentos, habilidades, atitudes e valores, desenvolvendo no aluno a capacidade de resolver situações complexas envolvidas em seu cotidiano. Busca também o pleno exercício da cidadania, a formação do caráter e preparo para o mundo do trabalho.

  Portanto para a Base os fluxogramas na área de matemática desempenham seu papel na formação do aluno, devem ser inseridos em seu cotidiano, mas para isso é

necessário que eles compreendam os conceitos envolvidos nessa nova ferramenta e também que consigam utilizá-la na resolução de problemas.

Os fluxogramas são o ponta pé inicial para a compreensão do pensamento computacional (PC), que é um processo a ser desenvolvido ao longo da etapa escolar do estudante e também são facilitadores da compreensão de algoritmos, principalmente os mais complexos, pois "quebram"esse algoritmo em partes simples, ajudando na memorização.

- **No Ensino Fundamental - Anos Finais - Unidade Temática - Álgebra**

> Associado ao pensamento computacional, cumpre salientar a importância dos algoritmos e de seus fluxogramas, que podem ser objetos de estudo nas aulas de Matemática. Um algoritmo é uma sequência finita de procedimentos que permite resolver um determinado problema.
>
> Assim, o algoritmo é a decomposição de um procedimento complexo em suas partes mais simples, relacionando-as e ordenando-as, e pode ser representado graficamente por um fluxograma. A linguagem algorítmica tem pontos em comum com a linguagem algébrica, sobretudo em relação ao conceito de variável. Outra habilidade relativa à álgebra que mantém estreita relação com o pensamento computacional é a identificação de padrões para se estabelecer generalizações, propriedades e algoritmos.

Na BNCC a álgebra será trabalhada em todos os anos do Ensino Fundamental, assim o processo algébrico vai evoluindo com o passar dos anos, o aluno irá se familiarizando e não haverá aquele susto ao se deparar com as equações e cálculos algébricos. Anteriormente a Álgebra era trabalhada no 7° ano em diante, gerando grande estranheza e dificuldade de compreensão dos cálculos, para evitar essa ruptura a álgebra será trabalhada desde os primeiros anos.

Muitas vezes nossos alunos tem dificuldade em compreender algoritmos extensos, por isso a base sugere o uso dos fluxogramas, assim esses algoritmos são "quebrados"em processos mais simples, ajudando o aluno a compreender não somente os cálculos, mas também a teoria envolvida no algoritmo.

- **No 6° ano - Fluxogramas como Objetos de Conhecimento nas unidades temáticas:**
  - Números - Fluxograma para determinar a paridade de um número natural.
  - Probabilidade e estatística - Diferentes tipos de representação de informações: gráficos e fluxogramas.
- **No componente curricular de Ciências - Etapa do processo investigativo**:

> Desenvolver e utilizar ferramentas, inclusive digitais, para coleta, análise e representação de dados (imagens, esquemas, tabelas, gráficos, quadros, diagramas, mapas, modelos, representações de sistemas, fluxogramas, mapas conceituais, simulações, aplicativos etc.).

- **Em todo Ensino Fundamental - Anos finais - Habilidades do componente Matemática.**

Analisaremos mais profundamente essas habilidades refentes aos fluxogramas, trazendo exemplos de livros do Programa Nacional do Livro e do Material Didático [22] (PNLD 2020) e sugestões.

Como dito na seção anterior, não encontrei um documento oficial com uma justificativa do porquê os fluxogramas foram escolhidos para construção de algoritmos. Apesar das críticas feitas pela Sociedade Brasileira de Computação (SBC), eles foram incorporados a BNCC, assim será um conteúdo trabalhado em todo o território nacional.

Em minhas pesquisas encontrei um curso de formação de professores na plataforma da Nova Escola sobre as Competências Gerais da BNCC. Nele a jornalista Ana Penido, que é participante ativa do Instituto Inspirar, que foi uma das colaboradoras do processos de construção e da implementação do capítulo introdutório da BNCC, nos oferece um porquê da escolha dos fluxogramas.

Segundo Ana Penido, a base vê como fundamental para contemplar as competências, a utilização de metodologias mais ativas e contextualizadas, que utilizem diferentes recursos didáticos, inclusive os digitais, para que alunos com diferentes características, possam aprender no seu ritmo, a partir de seus interesses e de estratégias mais adequadas a seu perfil de aprendizagem.

Porém apenas disponibilizar recursos tecnológicos não é garantia de aprendizado, pois estamos passando por tempo de grandes mudanças tecnológicas, com o avanço da Inteligência Artificial (AI), sistemas de programação e robótica, buscamos uma educação mais dinâmica, mas para isso precisamos de estudantes que sejam criativos e inovadores.

Penido vê o letramento matemático como a matemática com foco nos desenvolvimento de habilidades de raciocínio, representação, comunicação e argumentação para a resolução de problemas. Nas aulas de matemática deve ser criado um ambiente de aprendizagens, com o aluno sendo protagonista do seu aprendizado, fazendo-o pensar e estimulando-o a fazer conexões entre seus conhecimentos. O conhecimento matemático é essencial não só por sua aplicabilidade, mas também por sua potencialidade na formação de cidadãos, críticos, autônomos e ativos na sociedade.

Para ela o pensamento computacional tem a finalidade de elaboração, análise e leitura de algoritmos de programação.

Com esse curso de formação da Nova Escola, podemos concluir que os fluxogramas foram a linguagem de programação escolhida para ser inserida na base, pois atende as competências gerais:

- **Conhecimento** - Buscar informação e julgá-la verdadeira ou falsa;
- **Pensamento científico crítico criativo** - Interpretar dados, utilizar lógica e intuição, investigar, formular hipóteses e testá-las para fazer conclusões;
- **Comunicação** - Comunicar-se em várias linguagens se apropriando de tecnologias;
- **Cultura Digital** - Utilizar tecnologias e ferramentas digitais, explorar a capacidade de entender a lógica de programação e o pensamento computacional compreendendo os algoritmos de programas de computadores e aplicativos;
- **Argumentação** - Organizar as ideias que se quer defender;
- **Empatia e colaboração** - Esquematizar o papel de cada estudante em determinada tarefa.

Mediante a esse fato, os professores deverão ter consciência de que precisam ensinar um conceito novo, e de forma correta, aos seus alunos.

Analisando os materiais (livros didáticos PNLD e apostilas), os principais erros que encontrei nos materiais aos quais tive acesso, são:

- Não conter explicação da linguagem e estrutura no material do aluno e do professor;
- Erro de estrutura;
- Falta de exemplos com algoritmos matemáticos.

Por se tratar de um conteúdo novo, os materiais deveriam trazer um capítulo específico sobre os fluxogramas, no 6° ano principalmente, por se tratar de uma habilidade proposta na BNCC - (EF06MA04). Deveriam conter principalmente explicações sobre a finalidade de cada forma geométrica e sua utilização específica (ação). Essa falta de informação acarretam erro na estrutura, sendo muitas vezes confundidos com os organogramas. Nessa parte o principal erro fica por conta de representar as ações, que nos fluxogramas devem ser retângulos, por formas com cantos arredondados. Outro erro também cometido é quando se tem uma tomada de decisão, que nos fluxogramas devem ser representadas por losangos. Nos organogramas não há necessidade de indicar o início e o final da ação, que são essenciais na estrutura dos fluxogramas.

Por fim, os fluxogramas já eram utilizados antes de sua implantação na BNCC, assim na internet, nos livros, documentos acadêmicos e outros meios de pesquisa, são encontrados exemplos em diversas atividades, mas em matemática, ainda não se encontra quase nenhum exemplo prático e os que se encontram na maior parte das vezes estão escritos em linguagem de programação (pseudocódigos).

Vamos então analisar as habilidades que se referem aos fluxogramas em cada ano do Ensino Fundamental (anos finais) e do Ensino Médio.

2.2.1 Habilidades 6º ano - Fluxogramas -BNCC

Neste ano escolar, encontramos as seguintes habilidades relacionadas aos fluxogramas:

- (EF06MA04) Construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par).
- (EF06MA34) Interpretar e desenvolver fluxogramas simples, identificando as relações entre os objetos representados (por exemplo, posição de cidades considerando as estradas que as unem, hierarquia dos funcionários de uma empresa etc.).

Antes de construir um fluxograma é necessário expor ao aluno o conceito e estrutura do conteúdo que se vai trabalhar, em seguida pedir que ele formule, em linguagem natural, os processos que deverão ser efetuados (algoritmo) até que se chegue à resolução do problema. Visto isso, a habilidade temática (EF06MA34) deveria estar antes da (EF06MA04) e teria que conter uma explicação sucinta dos fluxogramas, apresentar alguns exemplos relacionados a diversas áreas, como as propostas na habilidade, assim o aluno poderia se familiarizar com o conceito antes de construir modelos matemáticos.

A seguir estão alguns exemplos encontrados em livros didáticos disponibilizados pela PNLD-2020.

Exemplo 2.8. Etapas de uma pesquisa - livro PNLD 2020

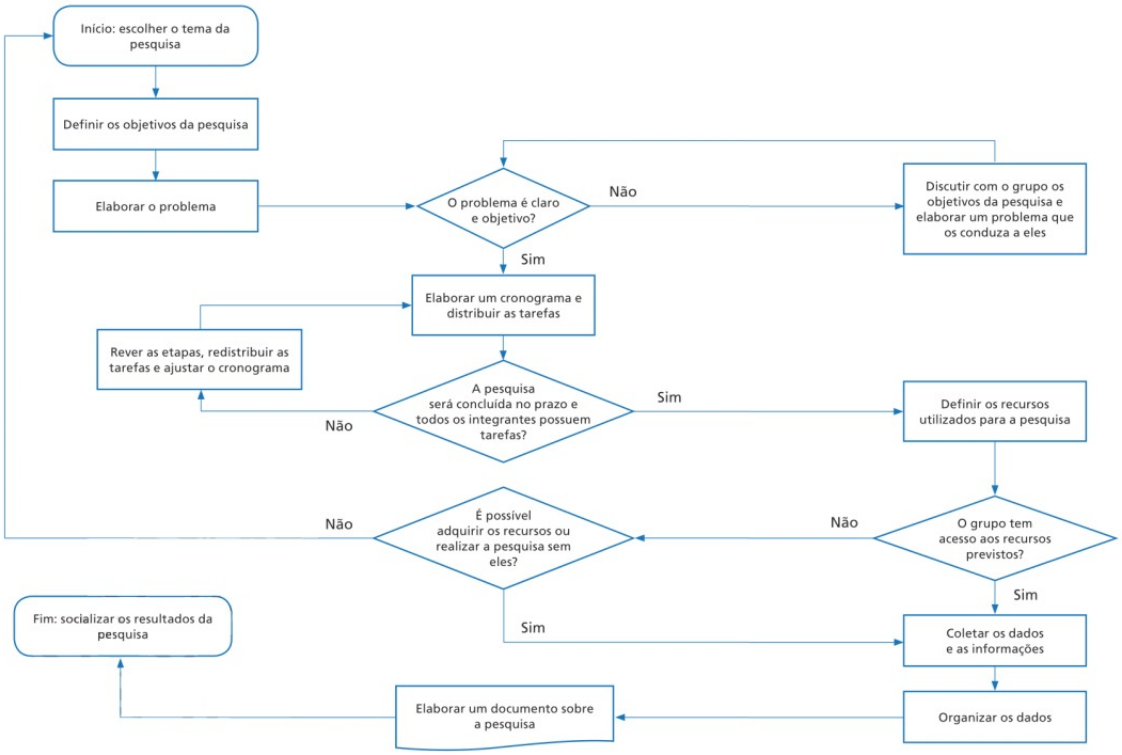
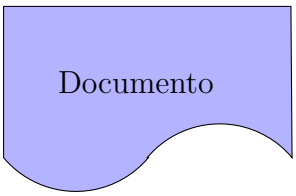


Figura 2.11: Fluxograma habilidade (EF06MA34) - Etapas de uma pesquisa (livro PNLD-2020)

Esse exemplo é muito complexo para um primeiro contato do aluno do 6º ano, ele provavelmente achará difícil de compreender. Deveria-se começar com exemplos mais simples, assim o aluno iria se familiarizando com o conceito para que mais tarde conseguisse interpretar fluxogramas mais elaborados.

Nesse exemplo temos uma forma geométrica, que representa entrada ou saída de um documento. Não faz parte dos símbolos básicos, logo pode gerar confusão de conceito se não for explicado ao aluno sua finalidade. Ela representa um relatório, um e-mail, um pedido, entre outros, documentos que uma empresa utiliza em seus processos.



O próximo fluxograma é um bom exemplo para uma iniciação do conteúdo, pois é de simples entendimento e sua estrutura está correta.

Exemplo 2.9. Pedido de pizza - livro PNLD 2020

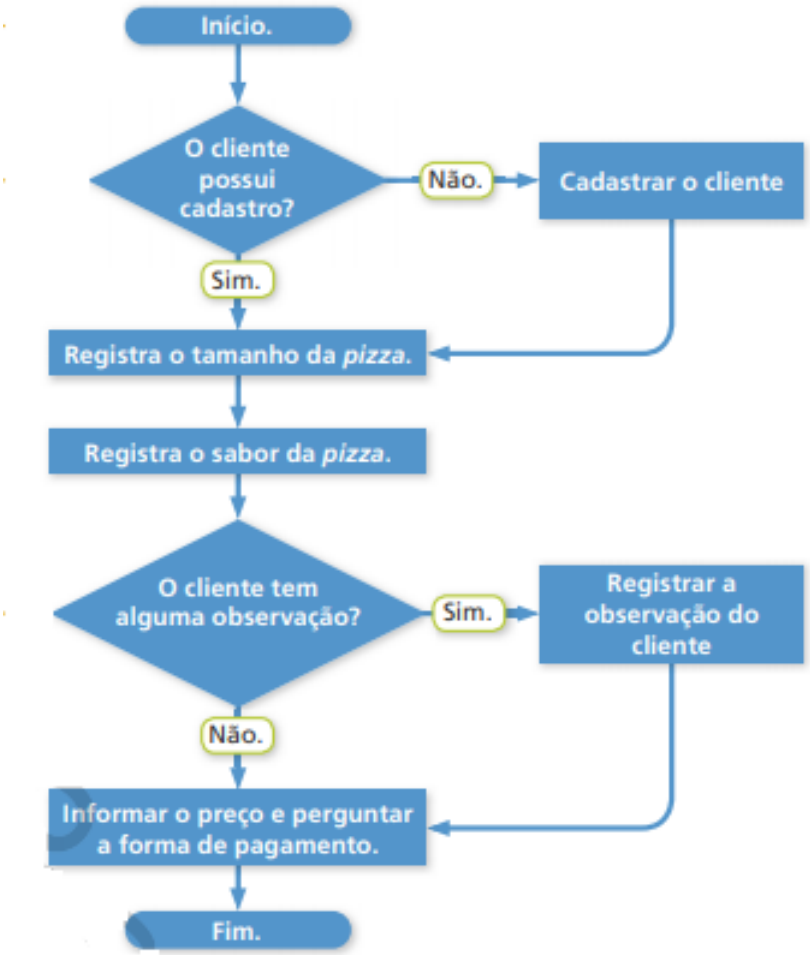


Figura 2.12: Fluxograma habilidade (EF06MA34) - Pedido de pizza (livro PNLD-2020)

Já nesse exemplo, apesar de ser simples seu entendimento, está escrito na terminação "compre"o correto seria estar em um retângulo, pois se trata de uma ação, para em seguida ser colocado o símbolo de terminação. Além disso a estrutura não está correta, pois os símbolos de terminação (início/fim) devem ser representados por formas ovaladas (elipse, por exemplo).

Exemplo 2.10. Necessidade da compra de um produto - livro PNLD 2020

Figura 2.13: Fluxograma habilidade (EF06MA34) - Necessidade de compra de um produto (livro PNLD-2020)

Neste, temos uma pergunta sobre o tipo de lixo, orgânico ou reciclável, o correto seria conter as respostas "sim"ou "não". Também está faltando o símbolo de terminação do processo.

Exemplo 2.11. Destino do lixo domiciliar

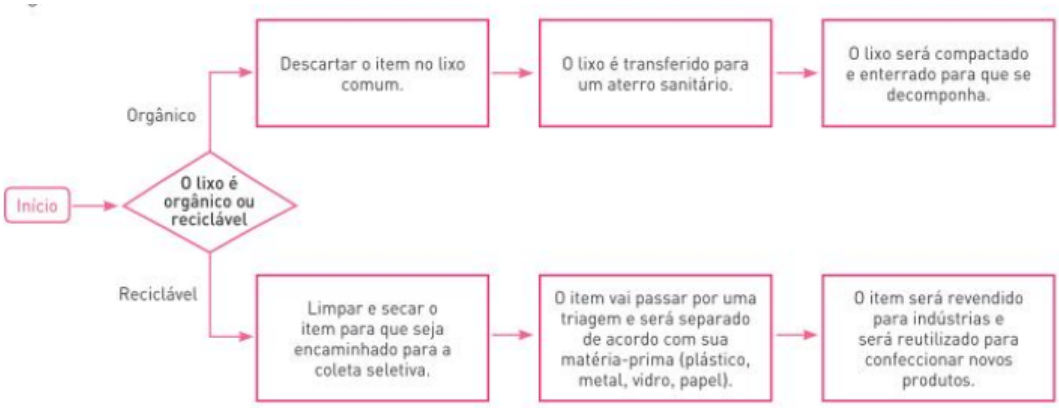


Figura 2.14: Fluxograma habilidade (EF06MA34) - Destino do lixo domiciliar (livro PNLD-2020)

Podemos perceber que os exemplos, encontrados nos livros analisados, pouco contribuem para o aprendizado do conceito e estrutura dos fluxogramas, além de serem em pequena quantidade. Um dos livros analisados nem sequer apresentou essa habilidade em seu material.

Devido a pouca quantidade de exemplos, tanto professor quanto aluno provavelmente recorrerão a internet. Mas é necessário ter cuidado, pois nem sempre o que se encontra nas buscas é confiável.

No site da *wikipédia* [23], que é um dos mais utilizados para pesquisa, temos o seguinte exemplo:

Exemplo 2.12. Teste de lâmpada - Wikipédia

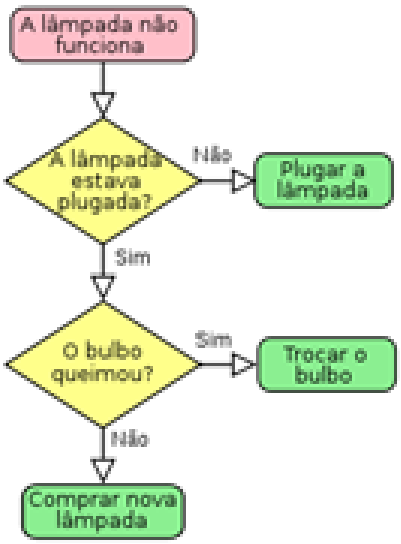


Figura 2.15: Fluxograma habilidade (EF06MA34) - Teste de lâmpada

- Os fluxogramas devem conter os símbolos ovalados com os dizeres "Início"e "Fim"do processo;
- As ações devem ser representadas por retângulos, ou seja, não devem conter cantos arredondados;
- Não está bem claro a tarefa que se pretende executar.

Portanto devemos ter muito cuidado ao escolher um exemplo para trazer para a sala de aula com a finalidade de completar o conteúdo do material didático. Antes verifique se os conceitos estão corretos.

Uma forma muito interessante de mostrar aos alunos o que pode acarretar um erro de conceito ou estrutura na realização de uma tarefa é o vídeo: Como ensinar linguagem de programação para uma criança. [24]. Nele um pai pede a seus dois filhos que escrevam instruções para que ele faça um sanduíche. Os filhos acham que seria uma tarefa extremamente simples, porém conforme eles escrevem o pai executa a tarefa, e o resultado final não é o pretendido. Eles refazem o processo diversas vezes. As crianças se irritam toda vez que tem que refazer as instruções. Com essa brincadeira, o pai pretende mostrar aos filhos como funciona a linguagem de programação, que precisa estar correta para que seja executada a tarefa pretendida. Vale a pena assistir e passar para os alunos. Como sugestão o professor também pode pedir aos alunos que façam algo parecido, tentem escrever instruções para a realização de uma determinada tarefa que será executada por alguém que siga exatamente as instruções dadas. Uma maneira lúdica muito interessante aos alunos nessa fase.

Na habilidade (EF06MA04), é sugerido determinar a paridade de um número. Geralmente os professores ensinam da seguinte forma:

Observe o último algarismo do número, ele termina em 0, 2, 4, 6 ou 8? Se sim ele é par. Caso contrário é ímpar.

E estaria finalizada a tarefa. Bastaria montar o fluxograma, que seria uma tarefa bem fácil. Mas onde está o conceito de paridade de um número natural? O que o aluno aprendeu com isso? Por que basta olhar somente para o último algarismo? Esse é um grande problema da educação, os nossos alunos estão acostumados com essas respostas prontas, que não os levam a pensar e a desenvolver o letramento matemático e o raciocínio lógico.

O correto seria desenvolver com os alunos o conceito de paridade de um número natural. Lógico que não é necessário fazer demonstrações complexas, ainda mais por se tratar do 6° ano. Poderia ser desenvolvidas as seguintes questões:

1) O que significa um número ser par?

2) Caso ele não seja par, existe uma outra classificação para ele?

3) Existe um número que não seja nem par e nem ímpar?

4) Como podemos representar os números que são pares? E os ímpares?

5) Escreva os números 35 e 42 utilizando-se do conceito de paridade (exemplo).

Espera-se que os alunos respondam à questão 1, dizendo que um número é par quando ele é um múltiplo de 2, ou que está na tabuada do 2, ou que quando divide por 2 a divisão

é exata, ou ainda que termina em 0, 2, 4, 6 ou 8. Todas as respostas estão corretas, porém o professor deve orientar os alunos para que realmente entendam o conceito de paridade.

Na questão 2 é muito provável que todos respondam que o número será ímpar.

Na questão 3, possivelmente eles ficarão intrigados, pois talvez nunca tenha passado por suas cabeças que poderiam existir outros tipos de classificações para os números. Essa questão é de fundamental importância no conceito de paridade. O papel do professor é levá-los a entender que os números, com relação a divisibilidade por dois, só podem ser escritos de duas formas, pois dependem do resto resultante da divisão por dois. Isso os ajudará a desenvolver conceitos mais avançados, como congruências entre números, que serão utilizados em questões mais complexas, que envolvam padrões e regularidades, muito frequentes em olimpíadas de matemática.

Na questão 4, entra o conceito algébrico envolvendo uma variável. O professor deve orientá-los em como escrever qualquer que seja o número utilizando o conceito de paridade.

E finalmente na questão 5, os alunos por meio de um exemplo, classificarão os números de acordo com sua paridade.

Em seguida, o professor pode propor para os alunos fazerem uma síntese do que aprenderam em linguagem natural, para em seguida transformar em linguagem de fluxograma.

Definição 2.13. Paridade de um número natural ($\mathbb{N}$).

Dado os números $n, q \in \mathbb{N}$, dizemos que: Um número n , pode ser escrito de forma única como:

i Se o resto da divisão de n por 2 for 0, então $n = 2.q$.

ii Se o resto da divisão de n por 2 for 1, então $n = 2.q + 1$.

O professor pode expor para os alunos o conceito formal de paridade de um número natural, se ele foi capaz de compreender o processo não terá dificuldade para entender a representação algébrica. Não é necessário nessa fase que os alunos escrevam todo o processo em linguagem matemática formal, porém isso os ajudará a entender melhor o conceito algébrico desde cedo, assim ao longo de seus estudos não se apavorarão quando tiverem que desenvolver as temidas equações algébricas.

Assim a atividade proposta poderá ser representada pelo seguinte fluxograma.

Exemplo 2.14. Paridade de um número natural

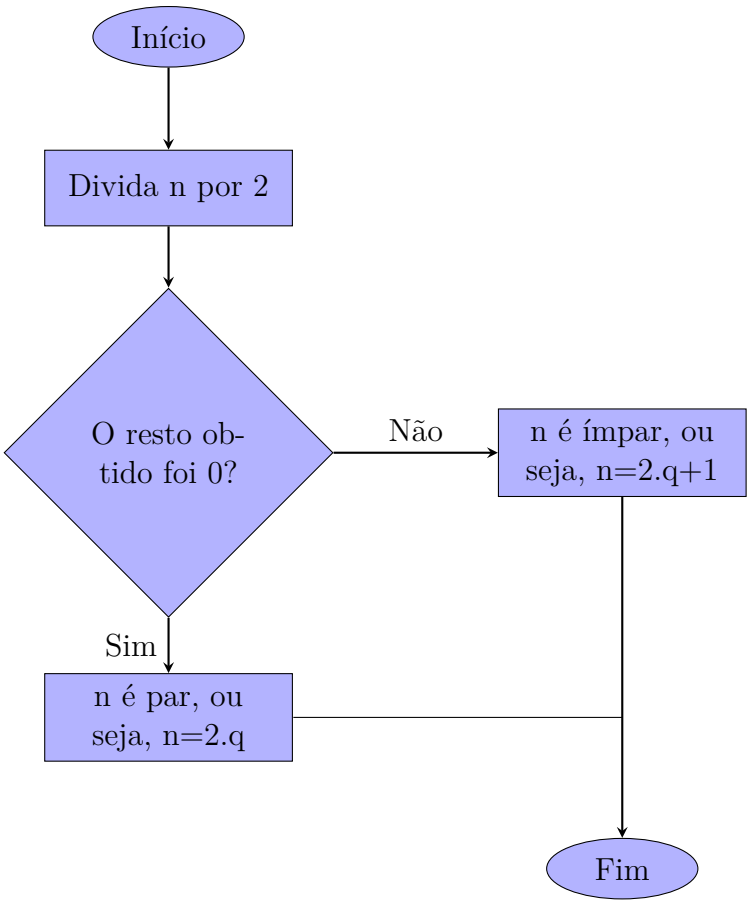


Figura 2.16: Fluxograma de autoria própria - Paridade de um número natural

Essa seria a forma correta de representação utilizando-se dos fluxogramas. As ações estão representadas em retângulos, a decisão por um losango e as terminações por formas ovaladas.

As imagens a seguir foram retiradas de livros didáticos que foram disponibilizados pelo PNLD 2020.

Exemplo 2.15. Paridade I - livro PNLD 2020

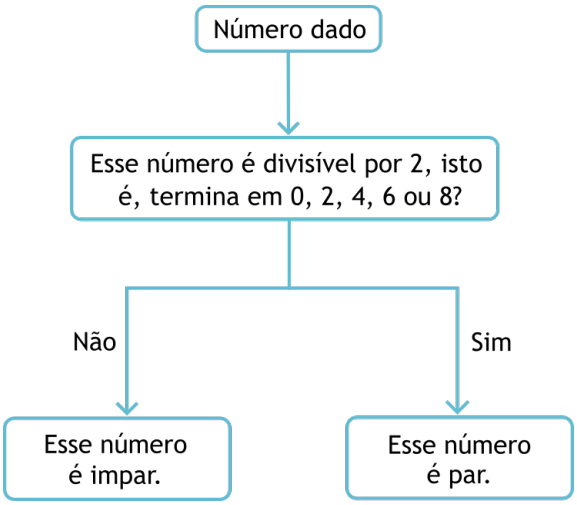


Figura 2.17: Fluxograma habilidade (EF06MA04) - Paridade I (livro PNLD-2020)

Exemplo 2.16. Paridade II - livro PNLD 2020

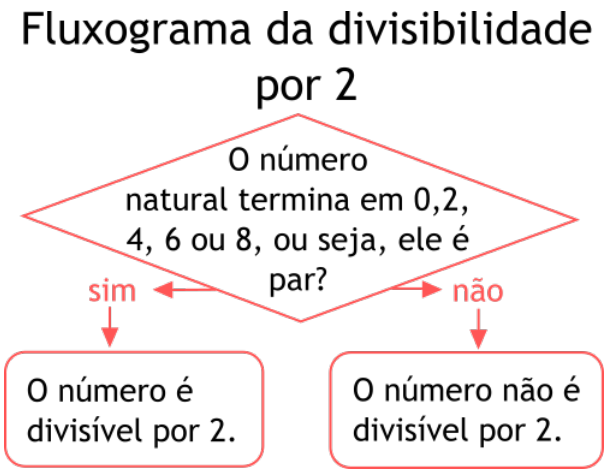


Figura 2.18: Fluxograma habilidade (EF06MA04) - Paridade II (livro PNLD-2020)

Exemplo 2.17. Paridade III - livro PNLD 2020

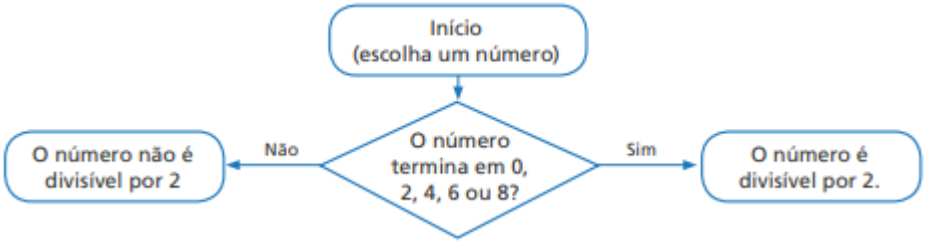


Figura 2.19: Fluxograma habilidade (EF06MA04) - Paridade III (livro PNLD-2020)

Nelas podemos observar vários erros:

- Os fluxogramas devem começar e terminar com os dizeres "Início"e "fim"representados por formas ovaladas, pois se tratando de um algoritmo matemático devem estar bem definidos as terminações do processo.
- As ações devem ser representadas por retângulos e não por formas com cantos arredondados.
- O conceito matemático de paridade não foi empregado, apenas uma forma de identificação.

Da forma em que foram apresentados, os exemplos de fluxogramas não contemplam nem o conhecimento do conceito matemático, que envolve a paridade e nem desenvolvem conhecimento sobre a estrutura dos fluxogramas. É apenas um esquema, em que o aluno identifica se um número é par ou ímpar, porém não aprendeu nada relevante.

2.2.2 Habilidades 7º ano - Fluxogramas- BNCC

Neste ano o material didático deve apresentar as seguintes habilidades:

- (EF07MA07) Representar por meio de um fluxograma os passos utilizados para resolver um grupo de problemas.

- (EF07MA26) Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um triângulo qualquer, conhecidas as medidas dos três lados.

- (EF07MA28) Descrever, por escrito e por meio de um polígono regular (como quadrado e triângulo equilátero), conhecida a medida de seu lado.

A maioria dos fluxogramas encontrados nas quatro coleções disponibilizadas pelo PNLD-2020 refere-se à habilidade (EF07MA07), elas trazem os mais variados tipos de problemas, envolvendo principalmente os conceitos de frações e potências.

Exemplo 2.18. Resolução de um grupo de problemas - Comparação de números racionais na forma decimal - livro PNLD 2020

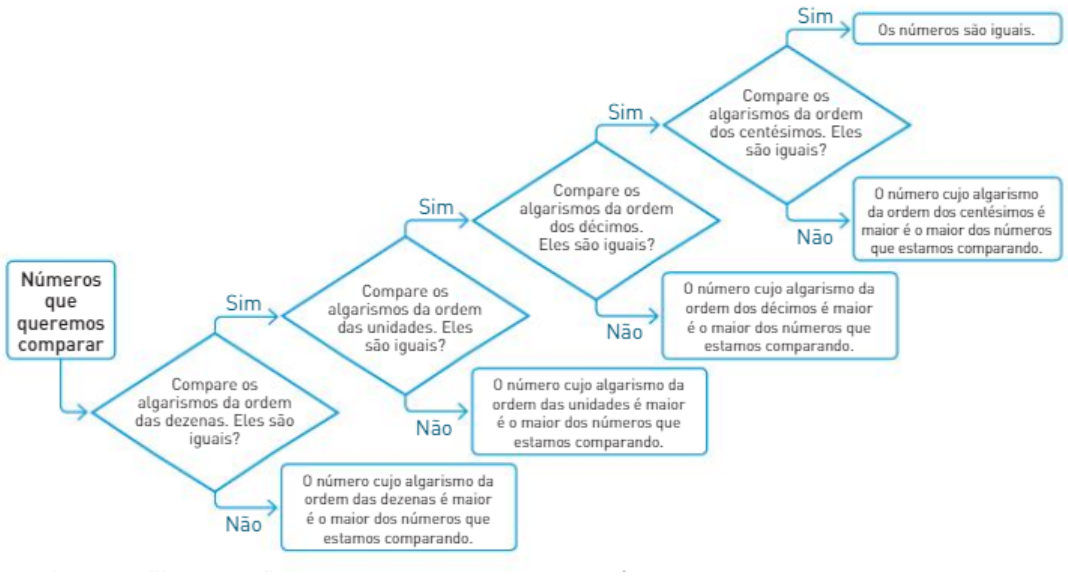


Figura 2.20: Fluxograma habilidade (EF07MA07) - Comparação de números racionais na forma decimal (livro PNLD-2020)

Exemplo 2.19. Resolução de um grupo de problemas - Comparação de números racionais na forma fracionária - livro PNLD 2020

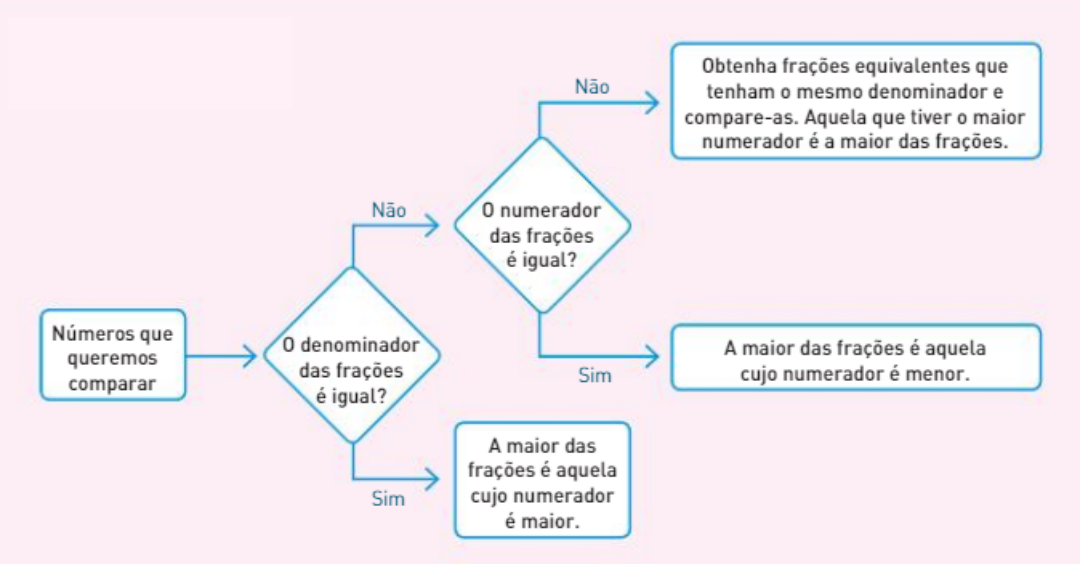
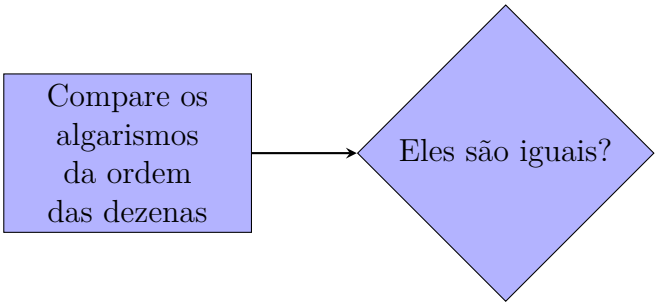


Figura 2.21: Fluxograma habilidade (EF07MA07) - Comparação de números racionais na forma fracionária I (livro PNLD-2020)

Nesses dois exemplos, do mesmo material didático, o grupo de problemas escolhido foi de comparar números racionais, tanto na forma fracionária (exemplo no material didático), quanto na forma decimal (exercício para o aluno), assim eles possuem os mesmo erros de estrutura.

- Nas terminações devem ser usadas formas ovaladas contendo os dizeres "Início"e "Fim"que demarcam o andamento do processo.
- As ações deveriam estar em retângulos, e não com formas que possuem cantos arredondados.
- Nos losangos devemos apenas colocar tomadas de decisões, logo a parte referente as ações devem ser representadas por retângulos, conforme o exemplo a seguir.



Esse fluxograma também poderia ser simplificado utilizando o conceito de completar as casas decimais com zeros para que fiquem com a mesma quantidade de algarismos na parte decimal do número, facilitando a comparação. Como sugestão, temos o seguinte fluxograma para comparação de números racionais na forma decimal.

Exemplo 2.20. Comparação de números racionais na forma decimal

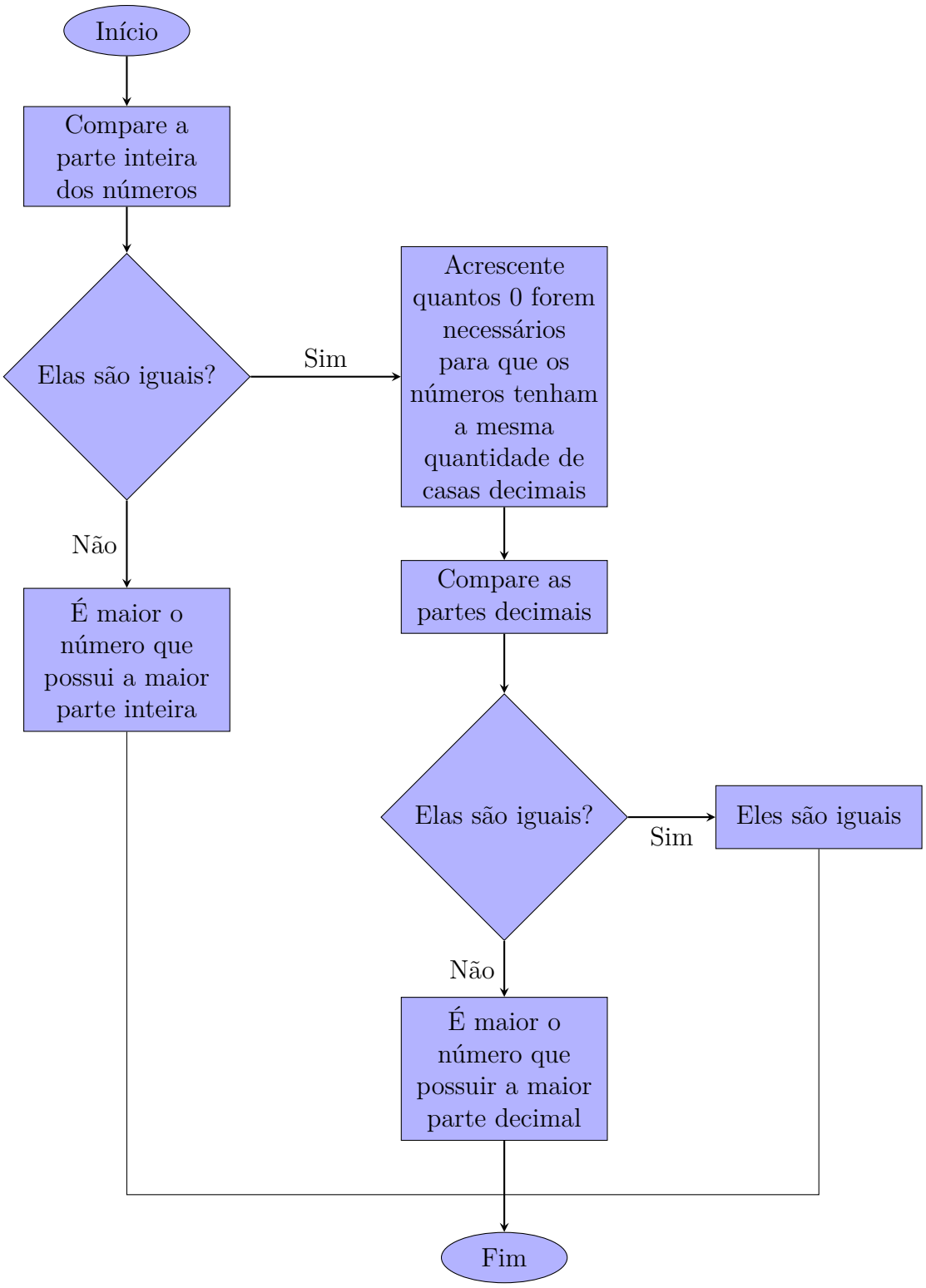


Figura 2.22: Fluxograma de autoria própria- Comparação de números decimais

Em outro material, também encontramos um fluxograma para comparação de números racionais na forma fracionária. Ele é um bom exemplo, pois sua estrutura está correta e as ações estão escritas de forma simples. O único problema fica por conta das frações equivalente, pois se o aluno não souber como determiná-las não conseguirá terminar o algoritmo.

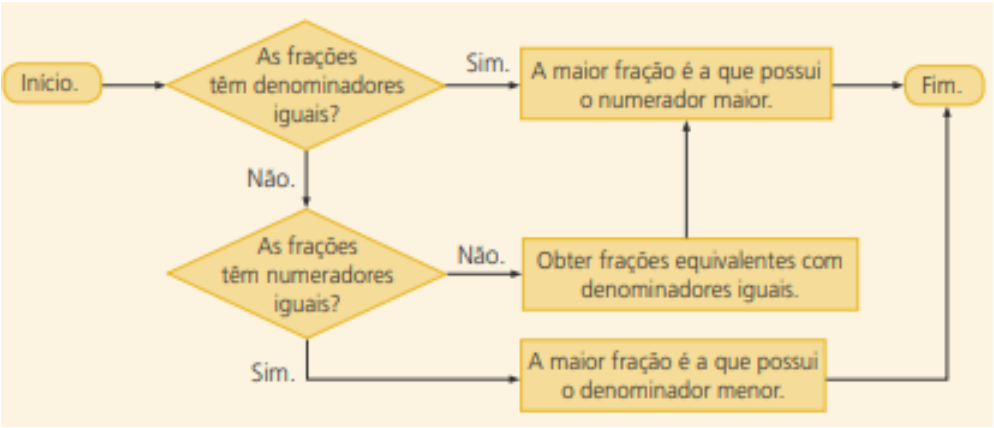


Figura 2.23: Fluxograma habilidade (EF07MA07) - Comparação de números racionais na forma fracionária II (livro PNLD-2020)

Esses fluxogramas são mais um lembrete do que propriamente a representação de um algoritmo, pois não expressam como determinar as frações equivalentes, que os alunos apresentam maior dificuldades. Seria interessante para o aluno um fluxograma que o ajudasse a transformar frações pelo conceito de equivalência para então compará-las.

Antes do aluno confeccionar um fluxograma o ideal é montar um roteiro:

Observe os numeradores e denominadores das frações.

As frações possuem numeradores ou denominadores iguais?

Sim: Compare-as

Não: Siga as instruções.

1) Encontre um múltiplo comum aos denominadores.

2) Determine o valor que se deve multiplicar cada denominador para se obter o múltiplo comum.

3) Multiplique o numerador pelo mesmo número que o denominador foi multiplicado para de obter o múltiplo comum.

4) Compare-as.

Em seguida o aluno montaria um fluxograma:

Exemplo 2.21. Comparação de frações utilizando a equivalência

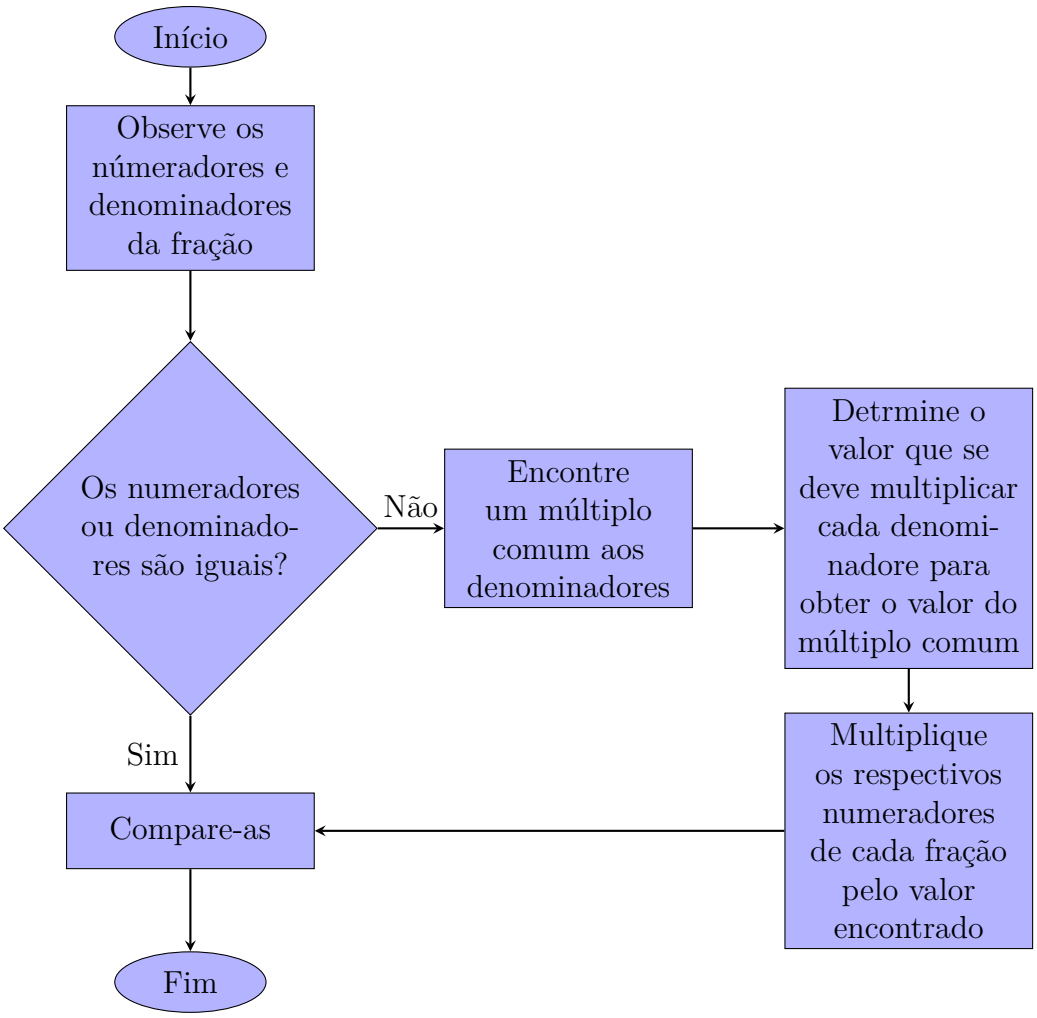


Figura 2.24: Fluxograma de autoria própria- Comparação de frações

Ainda no que diz respeito aos números racionais, os livros pesquisados, trazem um fluxograma envolvendo razões. Nesse exemplo encontramos um fluxograma para resolver problemas envolvendo razões entre grandezas diretamente proporcionais. O aluno já deve possuir o conceito de grandezas diretamente proporcionais e também que razão é uma comparação entre grandezas proporcionais escrita na forma de fração (ou divisão).

Exemplo 2.22. Grandezas proporcionais

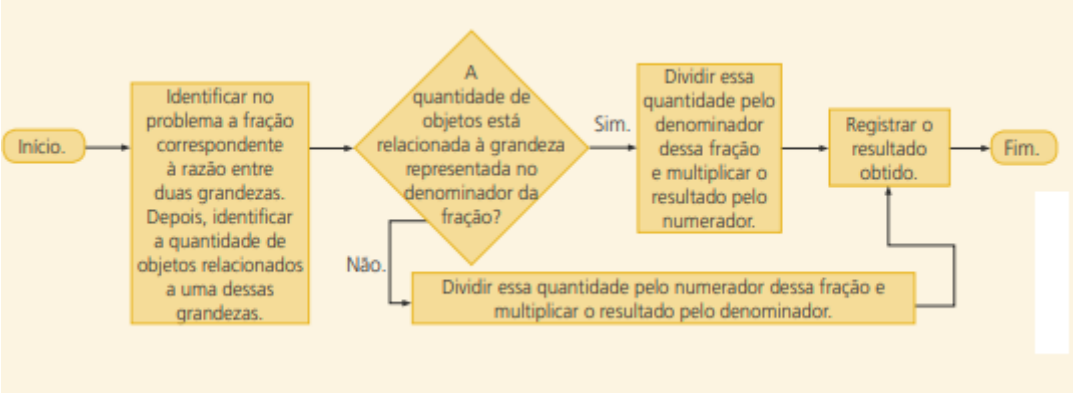


Figura 2.25: Fluxograma habilidade (EF07MA07) - Grandezas proporcionais (livro PNLD-2020)

No primeiro retângulo temos duas ações que deveriam ser separadas em dois retângulos, pois nos fluxogramas devemos ter sentenças curtas. Deveriam estar separadas as ações da seguinte forma:

- Identificar no problema a fração correspondente a razão entre as duas grandezas .
- Identificar a quantidade de objetos relacionados a uma dessas grandezas.

Esse exemplo também poderia estar escrito de maneira mais prática utilizando-se da escrita algébrica.

1. Identificar no problema a fração a/b correspondente a razão entre as duas grandezas diretamente proporcionais.
2. Identificar a quantidade de objetos relacionados a uma dessas grandezas escrever a fração correspondente na forma c/d, onde uma delas será o valor que se pretende determinar (incógnita).
3. A incógnita se encontra no denominador da fração?
4. Sim - Calcule $(b.c)/a$.
5. Não - Calcule $(a.d)/b$.
6. O resultado encontrado é o valor da incógnita.

Assim, poderia ser construído o seguinte fluxograma:

Exemplo 2.23. Grandezas diretamente proporcionais

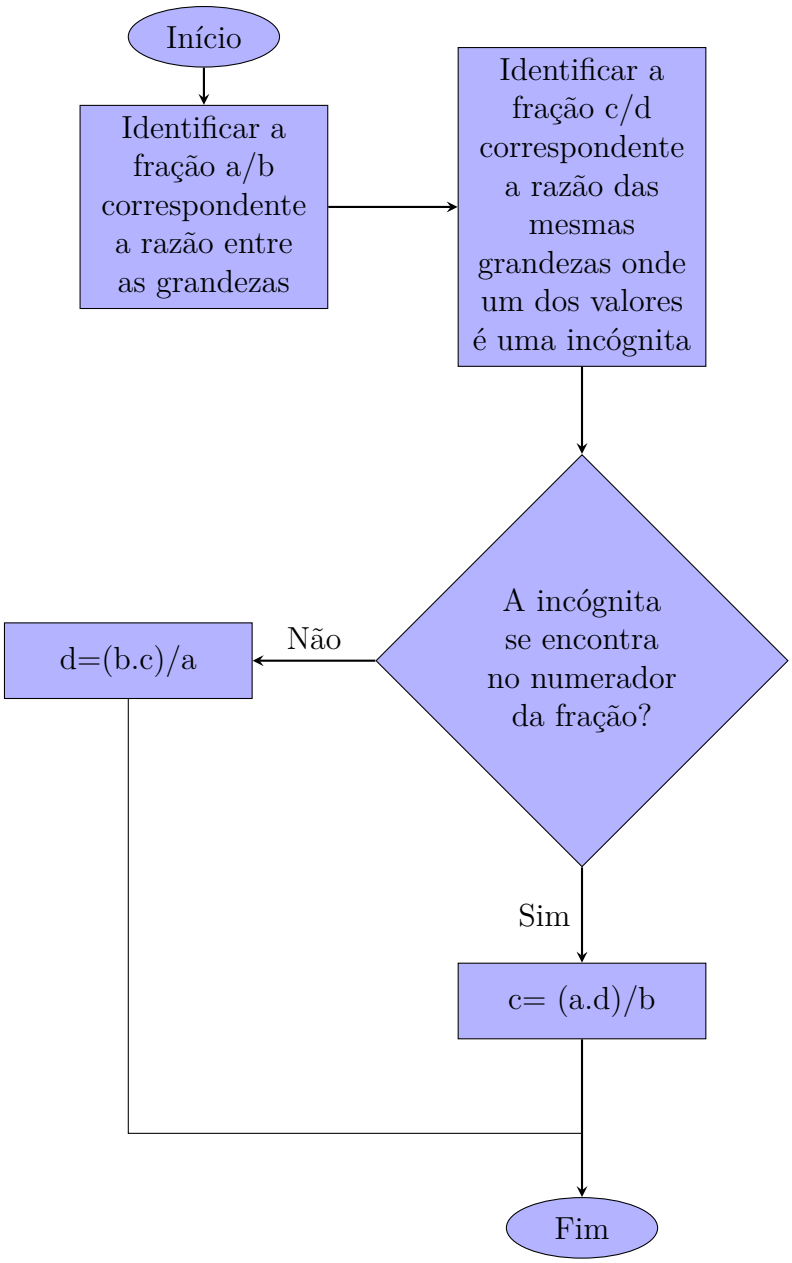


Figura 2.26: Fluxograma de autoria própria- Grandezas diretamente proporcionais

Um dos materiais escolheu como grupo de questões trabalhar o conteúdo de potência. O material didático traz como exemplo o fluxograma para calcular potência com base e expoente pertencentes ao conjunto dos inteiros ($\mathbb{Z}$) e como atividade, o aluno deve construir um fluxograma para calcular potência com base pertencente conjunto dos números inteiros ($\mathbb{Z}$).

Novamente, por se tratar do mesmo material didático, os erros são os mesmos:

- Não contém os símbolos de terminação (Início e Fim).
- As ações não estão representadas por retângulos.

Exemplo 2.24. Cálculo de potência com base pertencente ao conjunto dos números inteiros - livro PNLD 2020

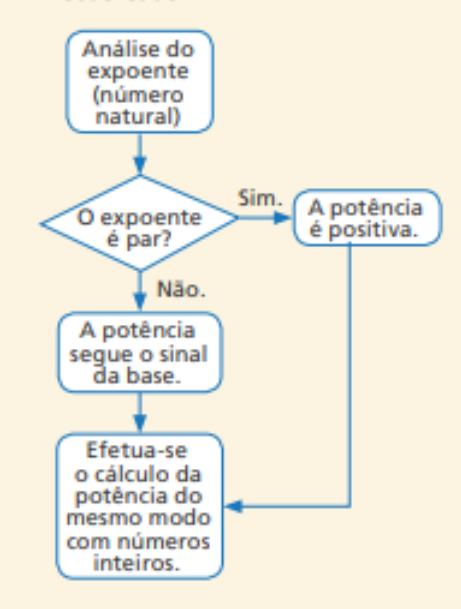


Figura 2.27: Fluxograma habilidade (EF07MA07) - Cálculo de potência I (livro PNLD-2020)

Fora os erros já comentados, nesse fluxograma o conteúdo está apresentado de forma correta, as instruções também são simples de compreender.

Exemplo 2.25. Cálculo de potência com base e expoentes pertencente ao conjunto dos inteiros - livro PNLD 2020

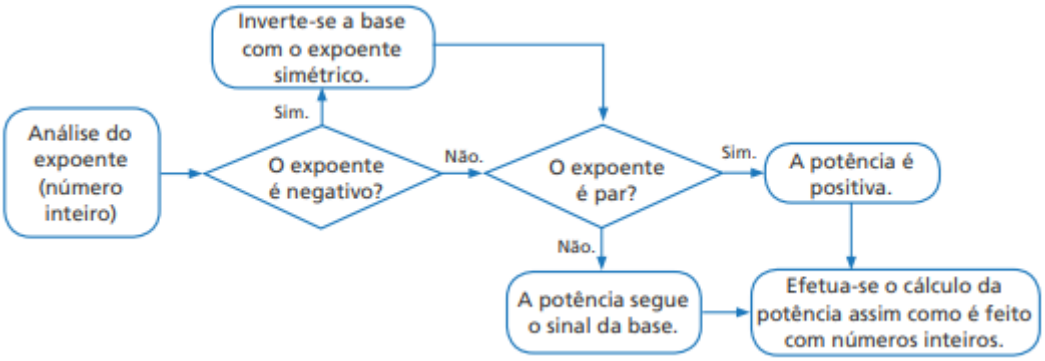


Figura 2.28: Fluxograma habilidade (EF07MA07) - Cálculo de potência II (livro PNLD-2020)

Além dos erros de estrutura já mencionados, esse fluxograma não traz de forma simples o processo a ser realizado, pois quando ele diz "inverte-se a base com o expoente simétrico"está se referindo a duas ações ao mesmo tempo, o que pode gerar confusão para o aluno. O correto seria dividir essa ação em duas:

- Inverta a base
- Escreva a nova base com o expoente simétrico.

Também quando se refere ao expoente não ser par (ímpar) poderia estar escrito simplesmente "a potência terá o mesmo sinal da base". E no final poderia também escrever de forma mais simplificada, "calcule a potência".

Temos como sugestão o seguinte fluxograma:

Exemplo 2.26. Fluxograma - Potência de base e expoente pertencentes ao conjunto dos números inteiros

Figura 2.29: Fluxograma de autoria própria - Potência com base e expoente inteiros

Vamos agora, analisar alguns fluxogramas referente a habilidade (EF07MA26)- Des-

crever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um triângulo qualquer, conhecida as medidas dos três lados.

Exemplo 2.27. Construção de um triângulo com régua e compasso - livro PNLD 2020

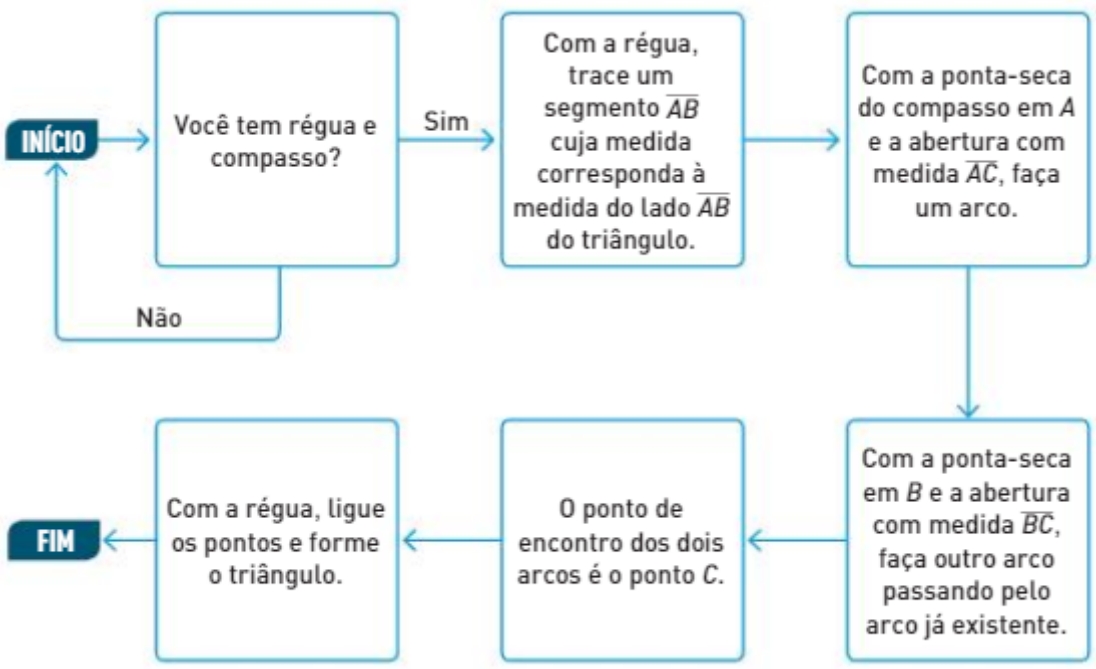


Figura 2.30: Fluxograma habilidade (EF07MA26) - Construção de um triângulo I (livro PNLD-2020)

Nesse fluxograma os mesmos erros em relações as formas de terminações e ações são encontradas. Mas o principal está em representar uma pergunta sem estar expressa por um losango, descaracterizando esse fluxograma. Particularmente, não vejo a necessidade de se fazer essa pergunta, pois, se o aluno não tiver o material ele não irá construir o triângulo, isso é uma condição necessária.

Exemplo 2.28. Construção do triângulo com régua e compasso - livro PNLD 2020

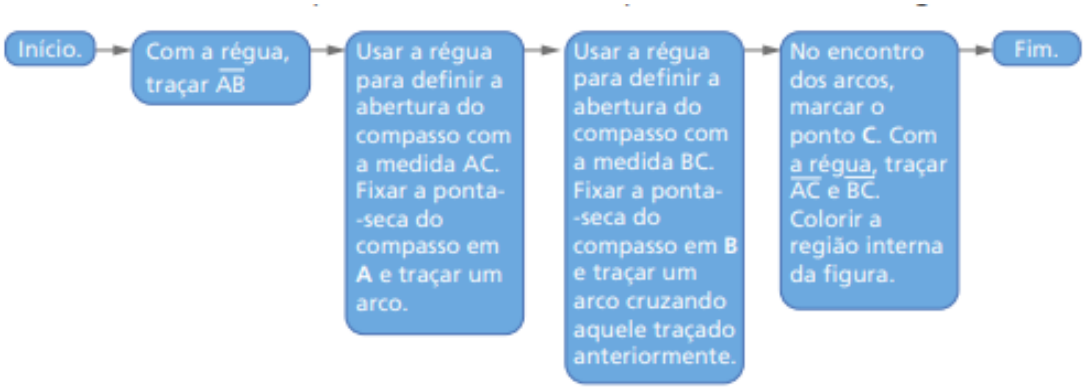


Figura 2.31: Fluxograma habilidade (EF07MA26) - Construção de um triângulo II (livro PNLD-2020)

Nesse fluxograma o único erro na estrutura são as formas que representam as ações, elas deveriam ser expressas por retângulos.

Com relação ao conceito, as ações devem ser expressas de forma simples, ou seja, devem conter apenas uma informação, o quê não é o caso.

As ações poderiam ser separadas da seguinte forma:

1) Com a régua traçar o segmento AB.
2) Utilizando a régua, abra no compasso um arco com a medida do segmento AC.
3) Com a ponta seca em A, trace um arco com a abertura do compasso que intercepte o segmento AB.
4) Utilizando a régua, abra no compasso um arco com a medida do segmento BC.
5) Com a ponta seca em B, trace um arco com abertura do compasso que intercepte o segmento AB.
6) Os arcos se interceptaram?

   Sim ⇒ Marque o ponto C onde os arcos se interceptaram.

   Não ⇒ Confira se você mediu corretamente os segmentos.
7) Ligue com a régua os pontos A, B e C.
8) O triângulo desejado é o △ABC.

Exemplo 2.29. Construção do triângulo com régua e compasso - Condição de existência - livro PNLD 2020

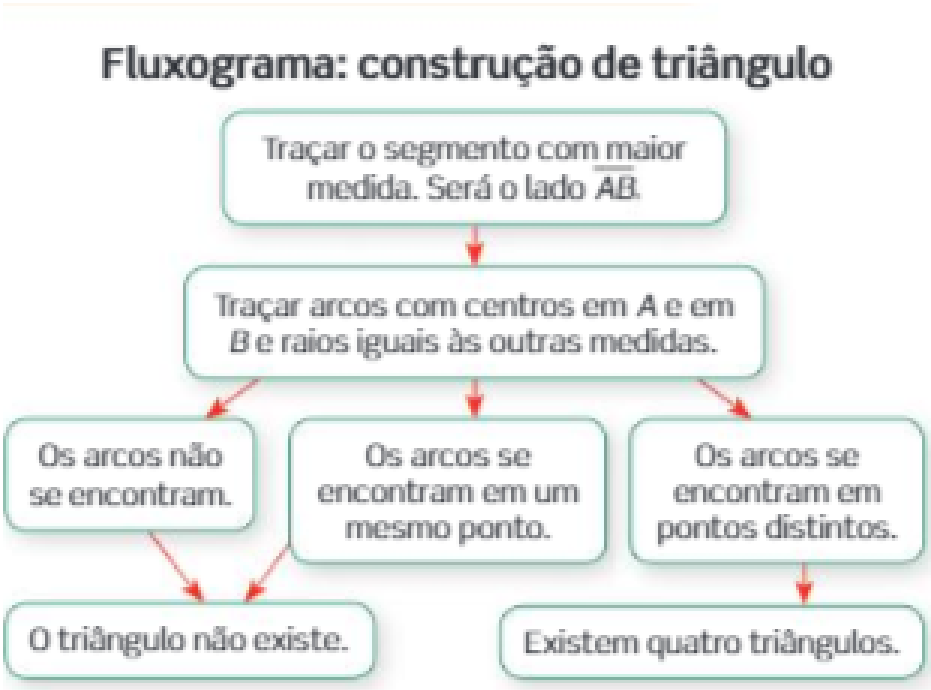


Figura 2.32: Fluxograma habilidade (EF07MA26) - Construção de um triângulo III (livro PNLD-2020)

Este exemplo nem poderia ser chamado de fluxograma, pois está completamente equivocado. Os erros são os seguintes:

- Não contém as formas que indicam terminação (Início/Fim);
- As ações não estão representadas por retângulos (contos arredondados);
- Temos fluxos saindo em várias direções.

Além disso os conceitos matemáticos não estão empregados de maneira correta, o que causaria confusão para o aluno.

- Por que começar com o maior lado? Isso não é uma obrigação.
- O que ele quer dizer com "traçar arcos com centros em A e B e raios iguais às outas medidas"?
- Em "os arcos se encontram em um mesmo ponto"deveria estar escrito em um único ponto.
- Quando os arcos se encontram em pontos distintos, ele afirmar existirem 4 triângulos, mas com essa construção só podemos afirmar a congruência de 2 triângulos.

Poderíamos construir um fluxograma mesclando os dois conceitos, construção e existência de triângulos.

Exemplo 2.30. Fluxograma - Construção de um triângulo com régua e compasso

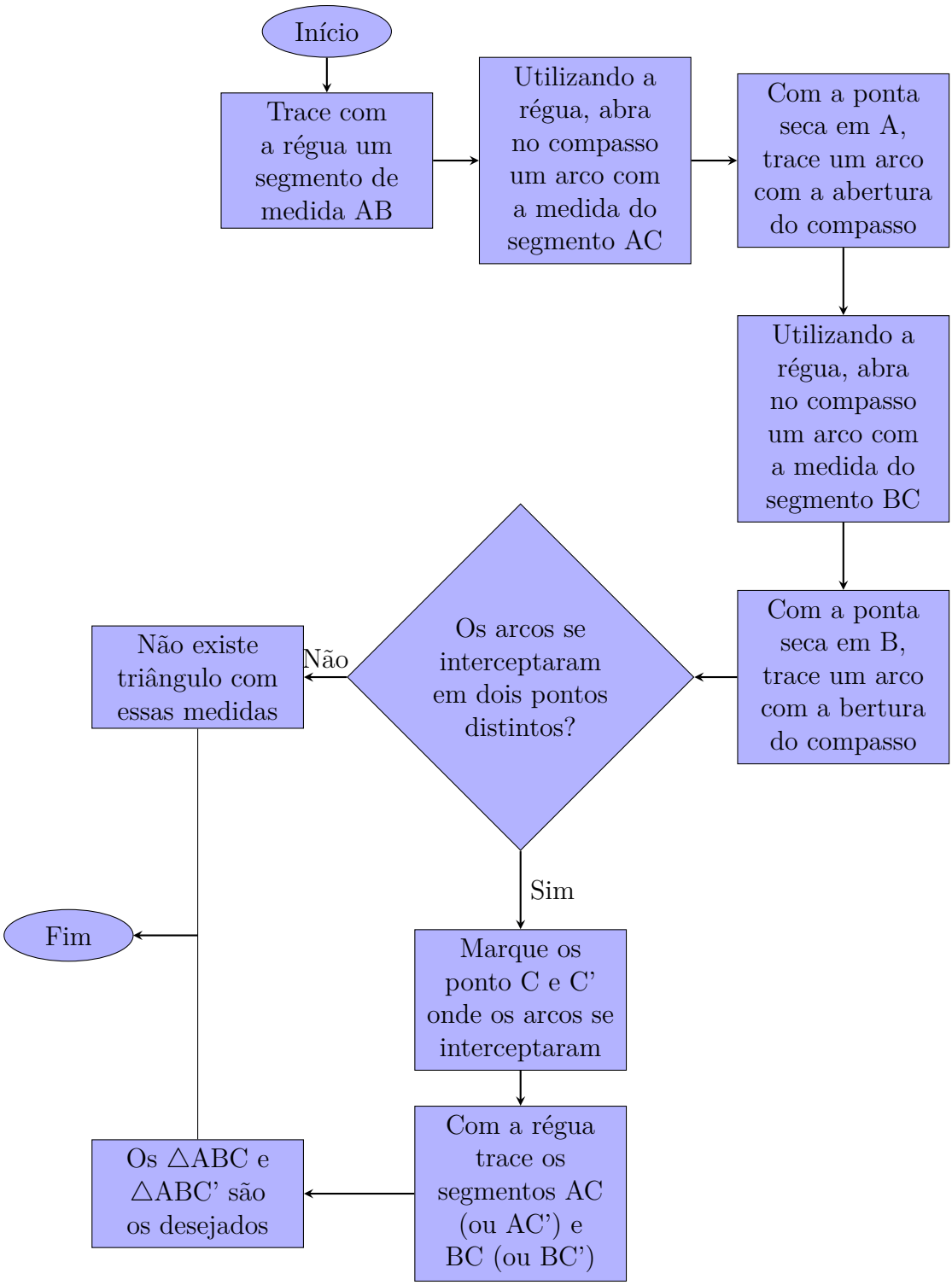


Figura 2.33: Fluxograma de autoria própria - Construção de um triângulo

Referido-se a habilidade (EF07MA28) - Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um polígono regular (como quadrado e triângulo equilátero), conhecida a medida de seu lado, encontrei os seguintes fluxogramas:

Exemplo 2.31. Construção de um polígono regular de n lados - livro PNLD 2020

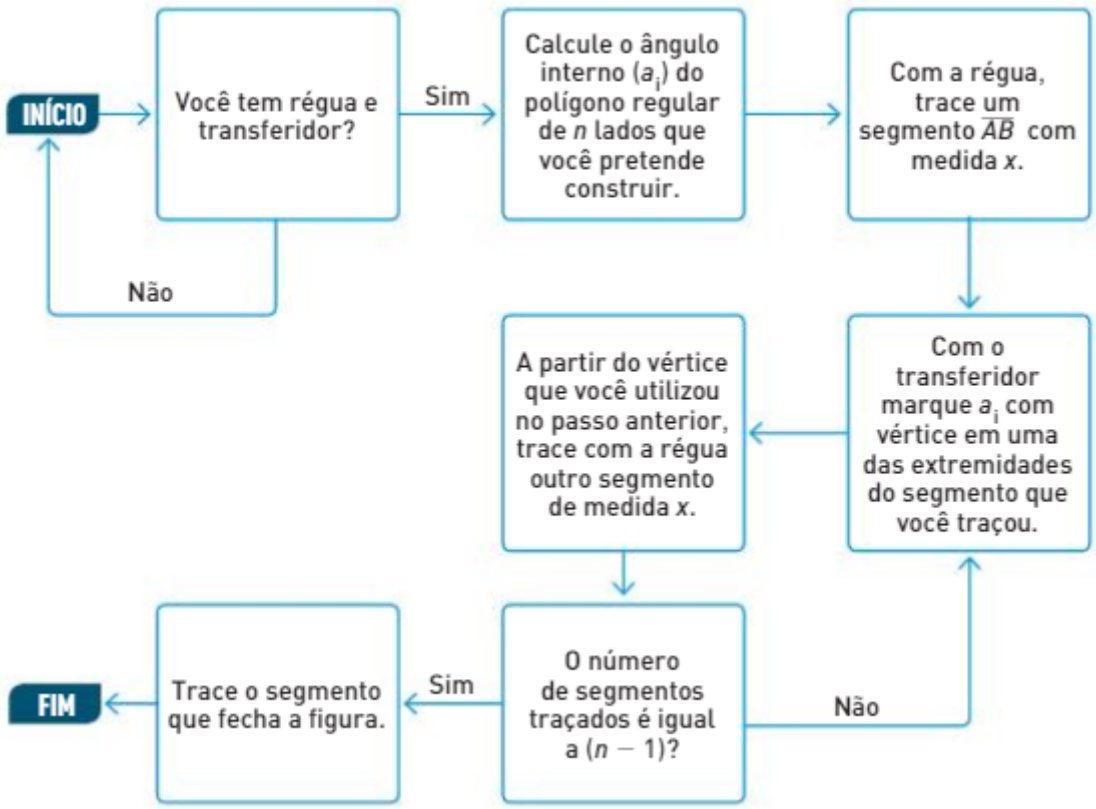


Figura 2.34: Fluxograma habilidade (EF07MA28) - Construção de um polígono regular I (livro PNLD-2020)

Mais uma vez, temos um fluxograma com erro de estrutura. A pergunta não estão representada por um losango, e a primeira é desnecessária, pois, se o aluno não tiver transferidor não fará a atividade. As terminações (Início/Fim) também estão erradas, deveriam ser formas ovaladas.

Já o conceito de construção de um polígono está correto, as ações estão representadas de forma simples e clara, assim o aluno não teria dificuldade em construir um polígono utilizando-se desse fluxograma. Porém a habilidade referente ao fluxograma não está sendo contemplada, pois há erro na estrutura.

Mas para se utilizar desse fluxograma o aluno deve conhecer a fórmula para calcular a medida do ângulo interno (a_n) de um polígono regular de n lados ($a_n = \frac{(n-2).180}{n}$), e também utilizar o transferidor para traçar ângulos.

Exemplo 2.32. Construção de um polígono regular de n lados - livro PNLD 2020

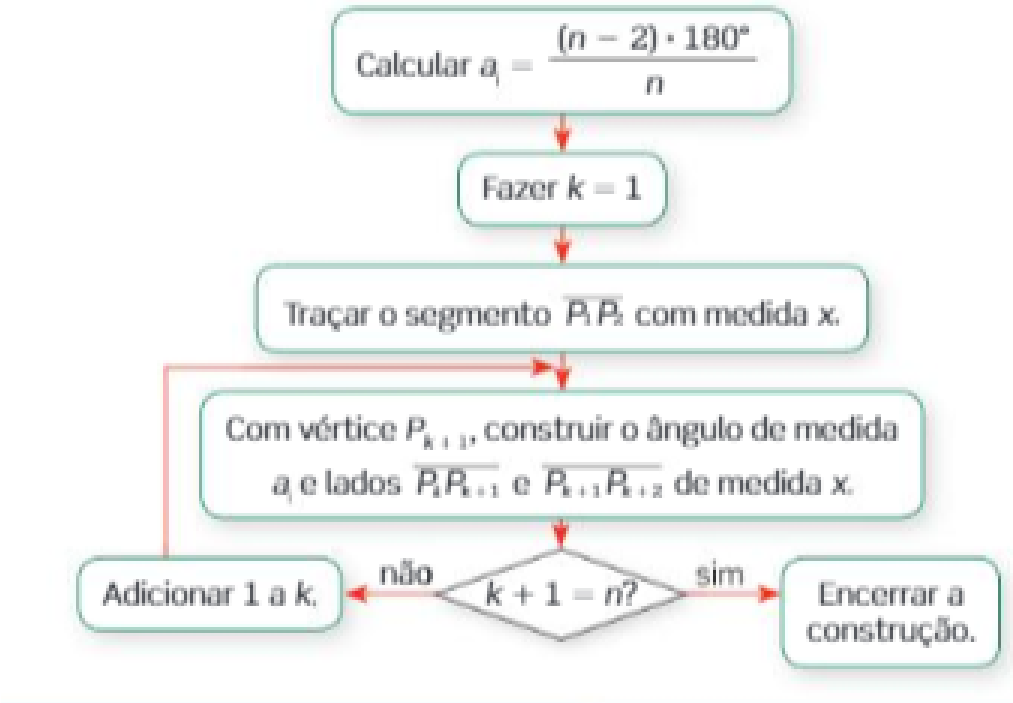


Figura 2.35: Fluxograma habilidade (EF07MA28) - Construção de um polígono regular II (livro PNLD-2020)

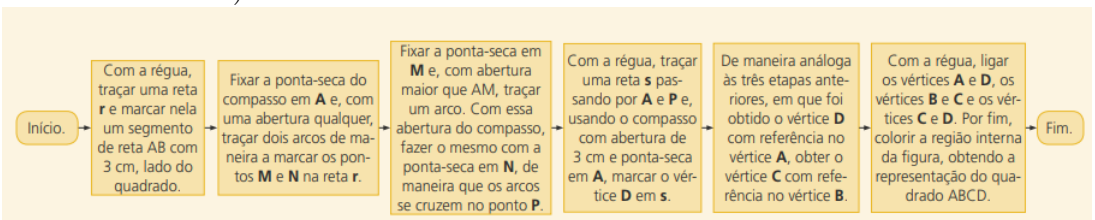
Esse fluxograma, além de conter erros de estrutura, suas ações não estão escritas de forma clara, o aluno terá muita dificuldade em compreender os passos para a construção de um polígono seguindo esse fluxograma. Está muito complexo, pois a linguagem algébrica como está escrito, causaria confusão por se tratar de alunos do 7° ano.

Ele indica como calcular a medida do ângulo interno (a_i) de um polígono regular de n lados, mas depois ele pede para fazer $k = 1$, mas o quê seria esse k? Depois ele indica o vértice como P_k e manda construir o ângulo, mas não indica como e nem qual ferramenta usar (transferidor ou compasso). Veja que há muitos erros com relação aos conceitos matemáticos, assim esse fluxograma não deveria nem sequer estar em um material didático de matemática. Isso só monstra do descaso com a educação dos nossos alunos, a BNCC pedia para colocar um fluxograma e foi colocado, porém não um fluxograma, e sim algo que visualmente se parece com um fluxograma.

Um dos materiais trazia o fluxograma refente a construção do quadrado, que era uma sugestão da BNCC.

Exemplo 2.33. Construção do quadrado - livro PNLD 2020

Figura 2.36: Fluxograma habilidade (EF07MA28) - Construção de um polígono regular III (livro PNLD-2020)



Ele traz um método muito confuso para a construção de um quadrado. Além de conter mais de uma ação por retângulo, o que é errado, pois tira a facilidade que se pretende ao se utilizar o fluxograma, quando o aluno for executá-lo obterá um desenho muito confuso.

Quando se trabalha com construções geométrica é importante que o professor oriente os alunos, justificando cada passo da construção. Pode lhes fazer as seguintes indagações:

- O que são retas paralelas? E retas perpendiculares?
- Quando construímos uma circunferência o que obtemos?
- Quando temos um seguimento de reta e construímos circunferências de centro em suas extremidades, elas se intersectam em dois pontos distintos, o que representa a reta que passa por esses pontos?

Com essas perguntas, o professor leva o aluno a entender que quando ele traça uma circunferência ele obtém todos os pontos do plano que estão a distância de um raio com relação ao centro da mesma, além de refletirem sobre as propriedades do quadrado.

Quando duas circunferências se intersectam em dois pontos, eles determinam uma reta, a mediatriz, que é o lugar geométrico dos pontos que equidistam de seus centros.

Assim o aluno vai entender o processo da construção não precisando decorar o passo a passo, trazendo-lhe mais conhecimento das propriedades que estão sendo utilizadas. O interessante nesse caso seria trazer fluxogramas sobre a construção de retas paralelas e perpendiculares antes das construções de polígonos.

Para a construção do quadrado, que iremos apresentar em forma de fluxograma, utilizaremos apenas as retas perpendiculares. Assim o exemplo a seguir ajudará o aluno na construção delas.

Exemplo 2.34. Fluxograma - Construção de retas perpendiculares

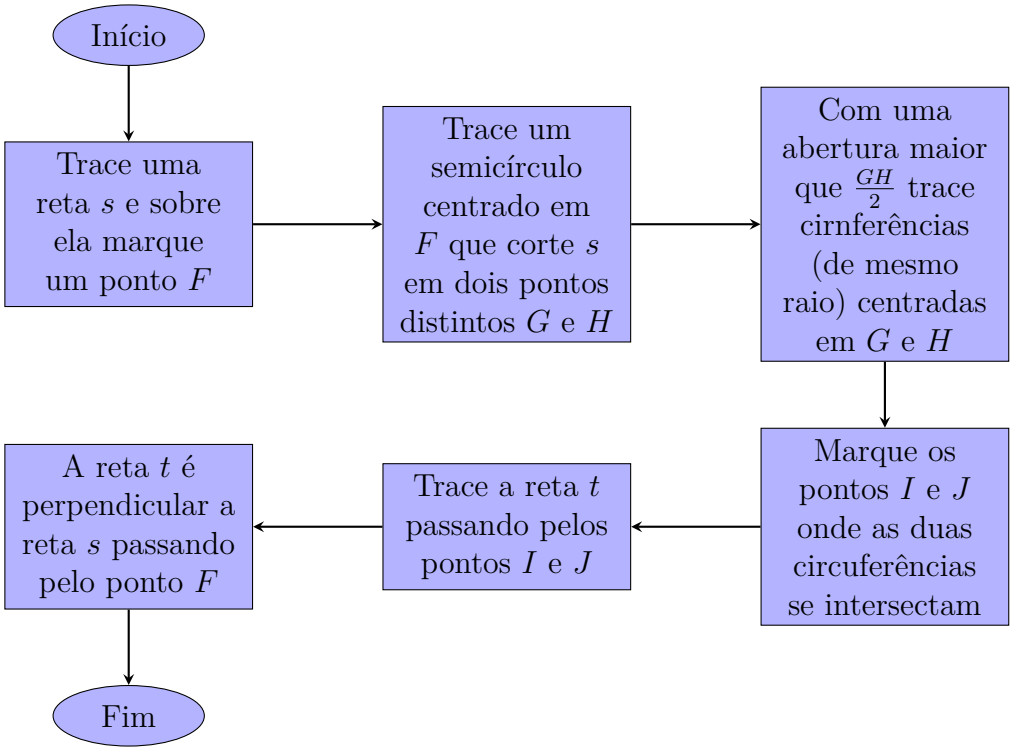


Figura 2.37: Fluxograma de autoria própria - Construção de retas perpendiculares

Tendo em mãos o fluxograma para construir retas perpendiculares e seguindo os passos do seguinte fluxograma, o aluno realizaria a construção de um quadrado sem maiores dificuldades.

Exemplo 2.35. Fluxograma - Construção do quadrado de lado l

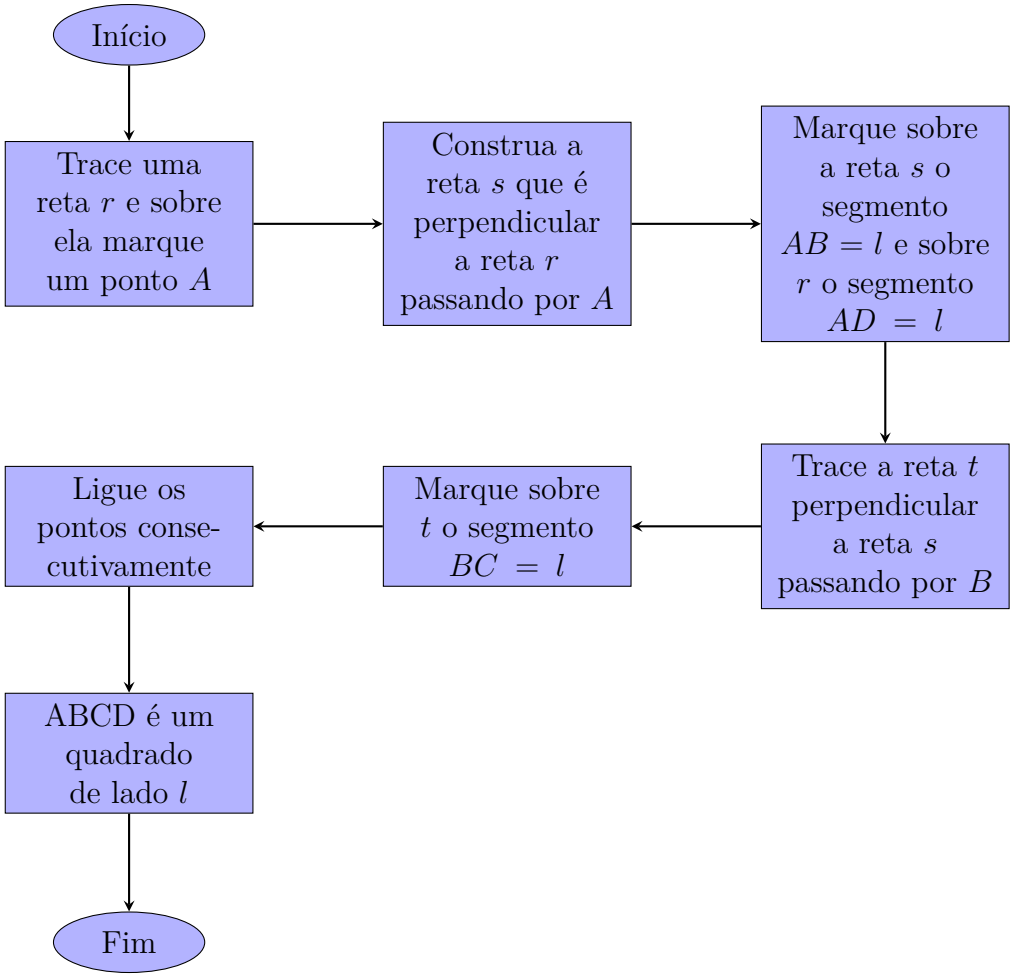


Figura 2.38: Fluxograma de autoria própria - Construção de um quadrado

Com esses dois fluxogramas além da construção o aluno consegue compreender todo o processo envolvido nela, conseguindo justificar os passos, baseado nas propriedades do quadrado, em todas as etapas da construção.

2.2.3 Habilidades 8º ano - Fluxogramas- BNCC

Neste ano escolar devemos encontrar fluxogramas que contemplem as seguintes habilidades:

- (EF08MA10) Identificar a regularidade de uma sequência numérica ou figural não recursiva e construir um algoritmo por meio de um fluxograma que permita indicar os números ou as figuras seguintes.
- (EF08MA11) Identificar a regularidade de uma sequência numérica recursiva e construir um algoritmo por meio de um fluxograma que permita indicar os números seguintes.

- (EF08MA16) Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um hexágono regular de qualquer área, a partir da medida do ângulo central e da utilização de esquadros e compasso.

As habilidades (EF08MA10) e (EF08MA11) estão relacionadas ao conteúdo de álgebra e ao tão almejado pensamento computacional, pois pede que os alunos construam um algoritmo que irão representar sequências. A fórmula algébrica deve ser criada, testadas para só então poder afirmar que ela representa aquela sequência, como se fosse um programa de computador.

Para contemplar essas habilidades, primeiramente o professor deve introduzir a sua aula o conceito de sequência, dando alguns exemplos de sequências numéricas simples, por exemplo a dos números pares, dos quadrados perfeitos, pode também introduzir padrões de repetição em figuras geométricas e pedir aos alunos que por observação e intuição façam as próximas figuras da sequência. Em seguida deve ficar bem claro para o aluno o que são sequências recursivas e não recursivas.

Definição 2.36. Sequências definidas recursivamente

São sequências definidas por intermédio de uma regras que permite calcular qualquer termo em função do(s) antecessor(es) imediato(s). São chamadas também de recorrências.

Logo, as sequências não recursivas não necessitam do(s) termo(s) antecessor(es).

Deve-se tomar cuidado, pois a mesma sequência pode ser expressa recursivamente ou não recursivamente.

Observe a seguinte sequência: Qual a quantidade de triângulos pretos da figura que ocupa a 20º posição? **(Triângulo de Sierpinski)**

Figura 2.39: Triângulo de Sierpinski

Inicialmente o aluno deve observar as figuras, contando em cada uma delas a quantidade de triângulos pretos que elas contém. Para facilitar a percepção do aluno pode-se pedir que montem uma tabela registrando sua contagem. A tabela a seguir pode ser utilizada para esse exemplo.

Posição da figura	Número de triângulos pretos
1	1
2	3
3	9
4	27
5	Por tentativa = 81
6	
...	
20	

Essa sequência pode ser definida não recursivamente, sendo $F_{(n)}$ o número de triângulos pretos na figura que ocupa a n-ésima posição, assim $F_{(n)} = 3^{n-1}$.

Ou recursivamente, sendo (X_n) a sequência da figura que ocupa a n-ésima posição. Para determinar a quantidade de triângulos pretos da figura que ocupa a n-ésima posição, temos a seguinte recorrência $X_{n+1} = 3.X_n$, com $x_1 = 1$.

Mas como fazer um fluxograma que represente a situação? Na verdade seria um fluxograma muito específico.

Os fluxogramas que estão relacionados a habilidade de sequências (recursiva ou não recursiva) encontrados no livros didáticos analisados trazem exemplos com sequências específicas.

Exemplo 2.37. Fluxogramas - Sequências não recursivas - livro PNLD 2020

Figura 2.40: Fluxograma habilidade (EF08MA10) - Sequência não recursiva (livro PNLD-2020)

Esse exemplo além dos erros na estrutura, já comentados, ele é específico, serve apenas para a sequência não recursiva $F_n = \frac{5.n+2}{3}$.

Exemplo 2.38. Fluxogramas - Sequências recursivas - livro PNLD 2020

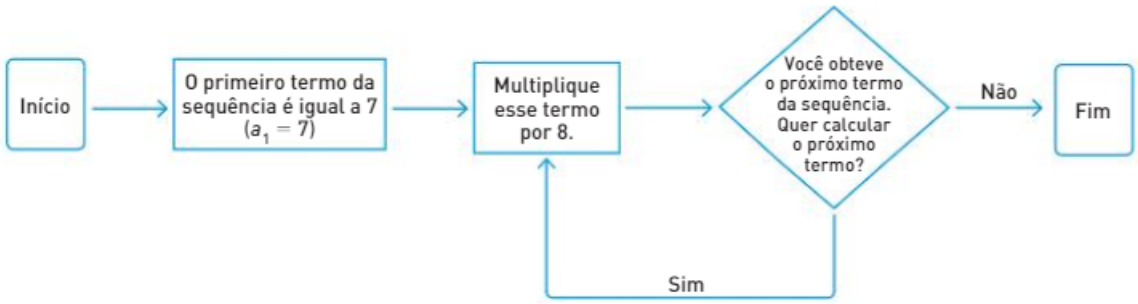


Figura 2.41: Fluxograma habilidade (EF08MA11) - Sequência recursiva I (livro PNLD-2020)

Este serve apenas para as sequências recursivas $A_{n+1} = 8.A_n$, onde $a_1 = 7$.

Exemplo 2.39. Fluxogramas - Sequências recursivas - livro PNLD 2020

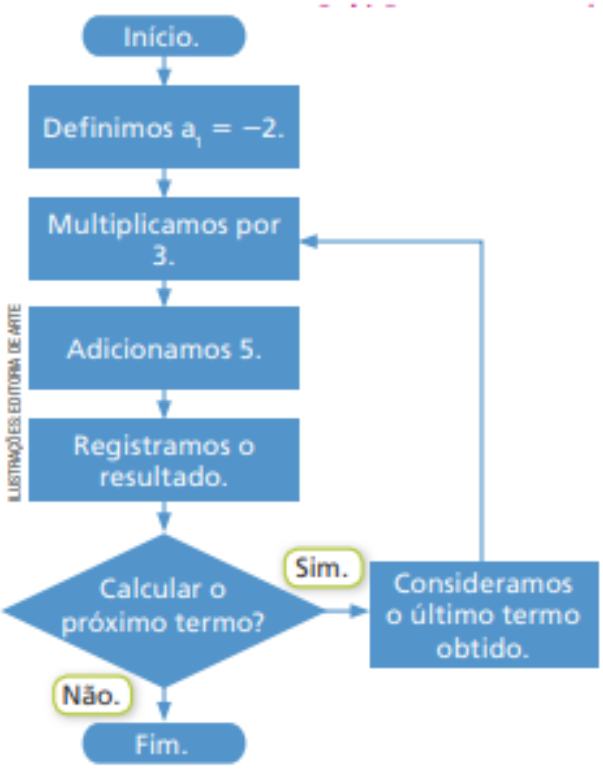


Figura 2.42: Fluxograma habilidade (EF08MA11) - Sequência recursiva II (livro PNLD-2020)

Neste exemplo a estrutura está correta, mas temos novamente um fluxograma para um sequência recursiva específica $A_{n+1} = 3.A_n + 5$, com $a_1 = -2$.

Exemplo 2.40. Fluxogramas - Sequências recursivas - livro PNLD 2020

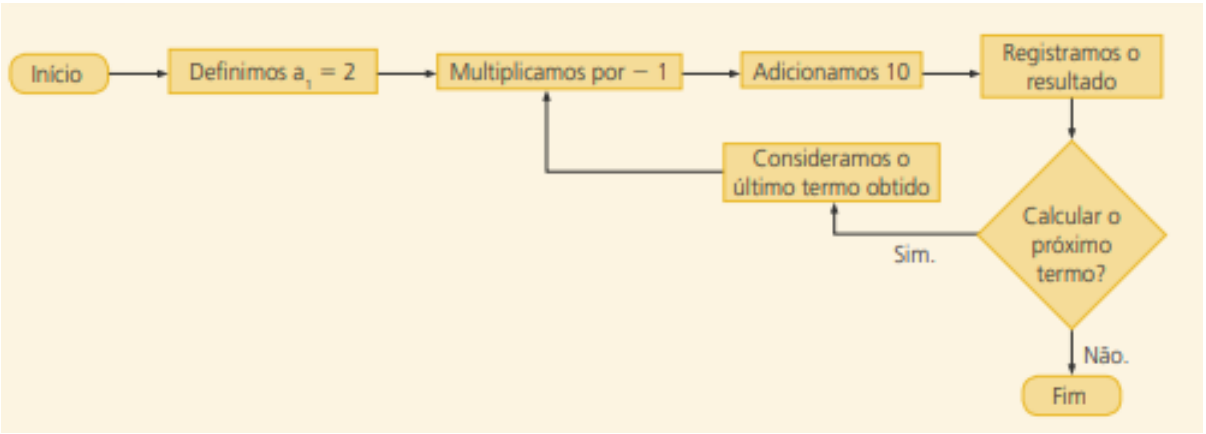


Figura 2.43: Fluxograma habilidade (EF08MA11) - Sequência recursiva III (livro PNLD-2020)

Temos mais uma vez um exemplo específico, a sequência recursiva $A_{n+1} = (-1).A_n + 10$, com $a_1 = 2$.

Foram encontrados outros exemplos, mas todos referente a sequências (recursivas ou não recursivas) específicas, que não foram colocados, pois, a análise seria a mesma.

Note que os exemplos não levam o aluno a pensar, eles já apresentam os passos do algoritmo, o aluno apenas vai utilizá-los para encontrar as figuras. Esses fluxogramas não contemplam as ideias da BNCC com relação ao pensamento computacional.

O interessante seria ter um fluxograma para que o aluno crie hábitos de investigação de padrões e consiga formular hipóteses e testá-las.

Esse exemplo encontrado sugere que o aluno crie sua própria sequência recursiva, com seu padrão de regularidade e primeiro termo definido. Porém qual habilidade está sendo contemplada? Ele apenas explica como encontrar o próximo termos da sequência. Sem contar os erros estruturais.

Exemplo 2.41. Como determinar o próximo termos de uma sequência recursiva - livro PNLD 2020

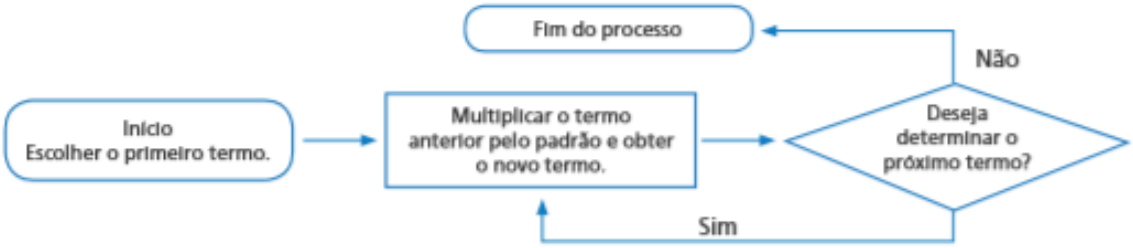


Figura 2.44: Fluxograma habilidade (EF08MA11) - Sequência recursiva IV (livro PNLD-2020)

Mas caso o termo que se procure for, por exemplo, o 100° termo de uma sequência? O aluno teria que ir fazendo um por um até chegar nele, ou seja, seria um trabalho exaustivo e entediante.

Seria muito mais interessante ter um fluxograma que ajudasse o aluno no processo de investigação dos padrões de uma sequências, que os levasse a formular hipóteses e realizar verificações (individuais ou em grupos) dos cálculos.

Como sugestão para as habilidades (EF08MA10) e (EF08MA11) referentes as sequências (não recursiva e recursiva) temos o fluxograma a seguir.

Exemplo 2.42. Termo geral de uma sequência

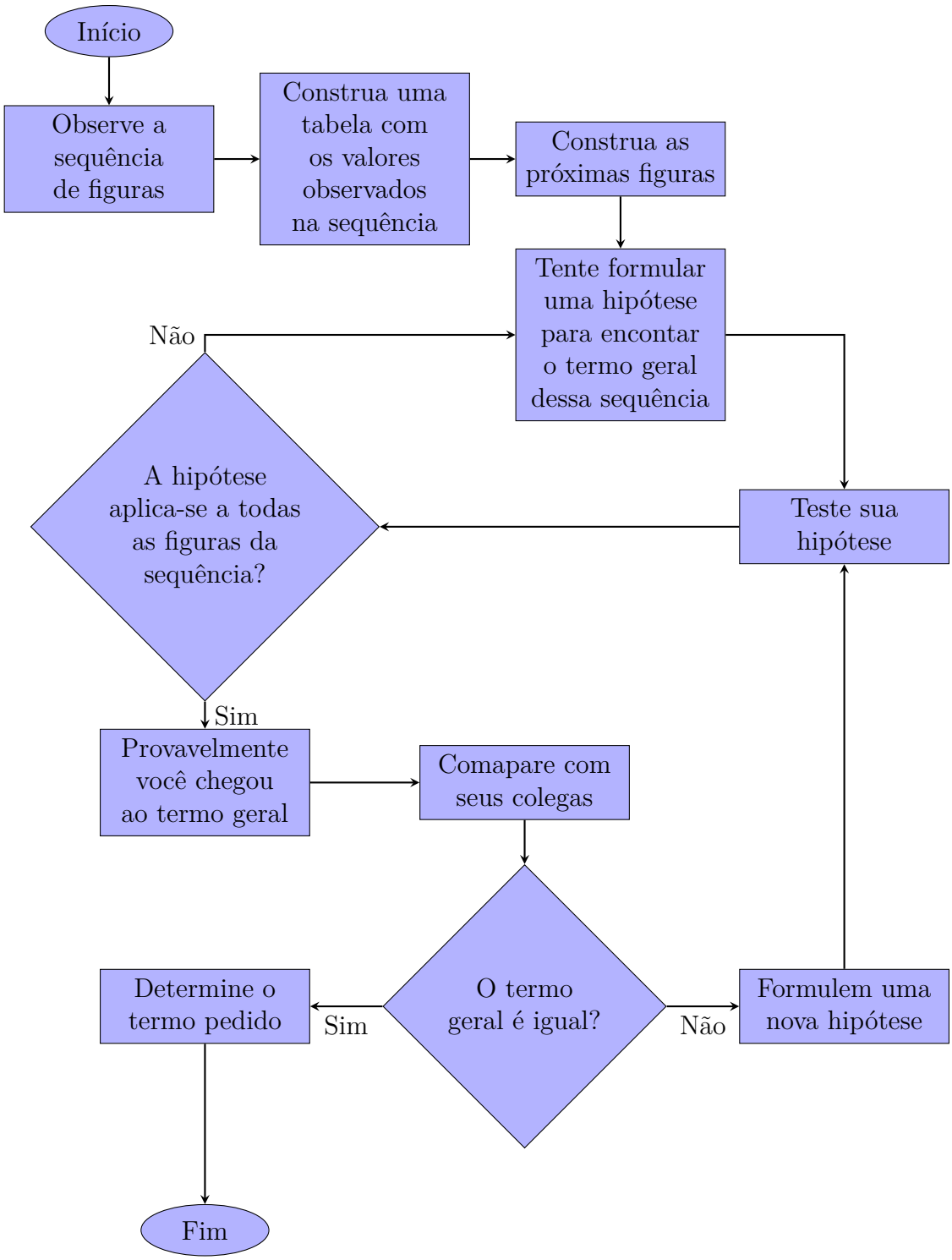


Figura 2.45: Fluxograma de autoria própria - Termo geral de uma sequência

Nessa próxima habilidade (EF08MA16) os alunos devem estar aptos a: Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um hexágono regular de qualquer área, a partir da medida do ângulo central e da utilização de esquadros e compasso.

Para isso os alunos devem saber que:

- Todo polígono regular pode ser inscrito em uma circunferência.

- O ângulo central de uma circunferência mede 360° e se a dividirmos em 6 partes, de mesma medida, teremos ângulos 6 centrais de 60°.
- Um hexágono regular pode ser decomposto em 6 triângulos equiláteros congruentes, que possuem ângulos internos com medida de 60°.
- A abertura do compasso, com o mesmo raio que foi construída a circunferência, é equivalente a um ângulo central de 60°.
- Um esquadro escaleno, possui ângulos com medidas de 30°, 60° e 90°.

Portanto para a construção de um hexágono regular de lado l devemos construir uma circunferência de raio l e dividi-la em 6 partes iguais utilizando o compasso, ou utilizar o ângulo de 60° de um esquadro escaleno, para a divisão do ângulo central da circunferência em 6 partes iguais.

O único exemplo que encontrei nos livros analisados foi esse.

Exemplo 2.43. Construção de um hexágono regular utilizando esquadro e compasso - livro PNLD 2020

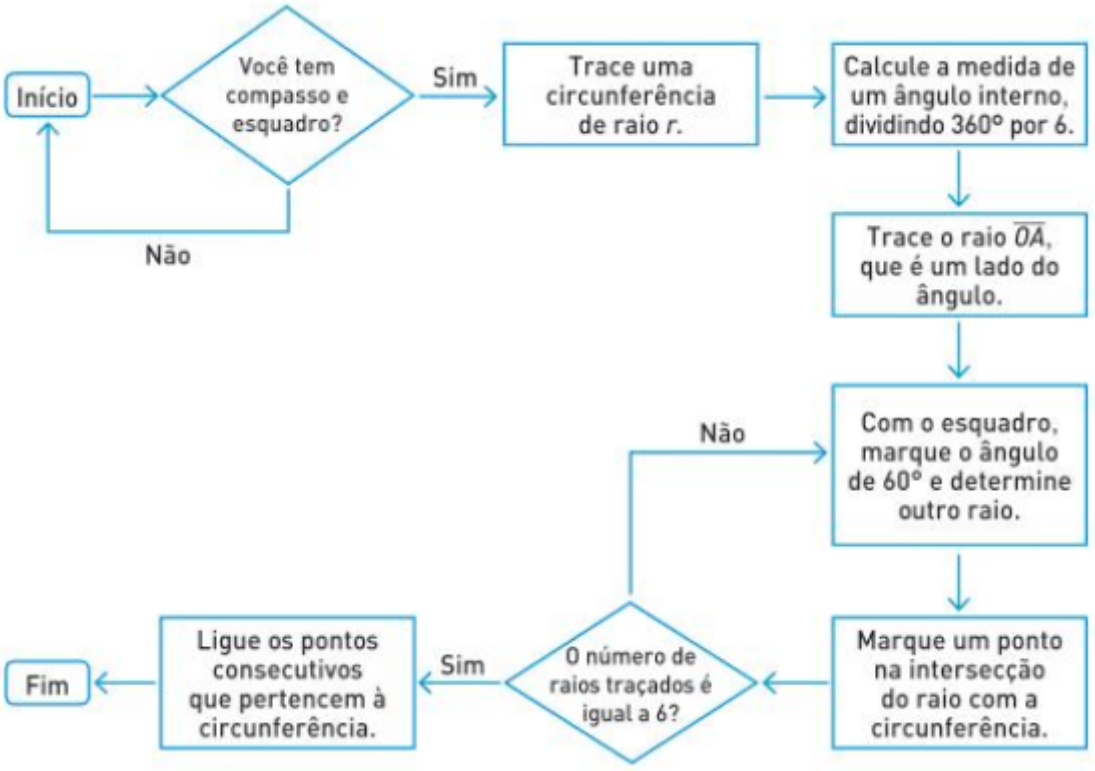


Figura 2.46: Fluxograma habilidade (EF08MA16) - Construção de um hexágono regular (livro PNLD-2020)

A primeira pergunta é desnecessária, porque o aluno não vai realizar a atividade se não tiver os instrumentos necessários.

Os passos para a construção estão corretos, porém poderia ser um pouco mais simples.

No caso específico de um hexágono regular, não há a necessidade de se utilizar um esquadro na construção, pois, se aluno tiver o conhecimento de que a abertura do compasso

representa uma arco de 60°, que é o ângulo central de um hexágono regular, poderá construí-lo apenas com o compasso e uma régua.

Daremos então um exemplo de como seria o fluxograma para construção de um hexágono regular utilizando o compasso e a régua. Podemos então construir o seguinte fluxograma.

Exemplo 2.44. Construção de um hexágono regular de lado l com compasso e régua

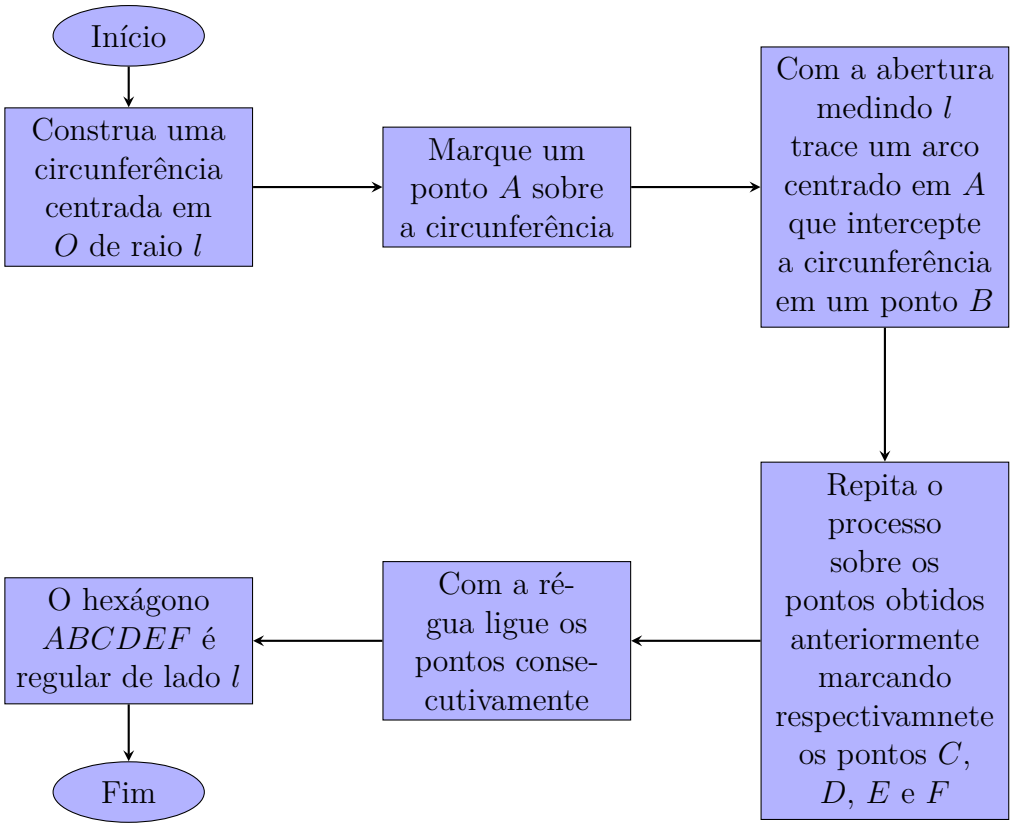


Figura 2.47: Fluxograma de autoria própria - Construção de um hexágono

Um dos materiais analisados trouxe um fluxograma referente a classificação de quadriláteros de acordo com suas propriedades. Na habilidade (EF08MA14) pede-se para demonstrar propriedades dos quadriláteros por meio da identificação da congruência de triângulos.

Exemplo 2.45. Classificação de quadriláteros - livro PNLD 2020

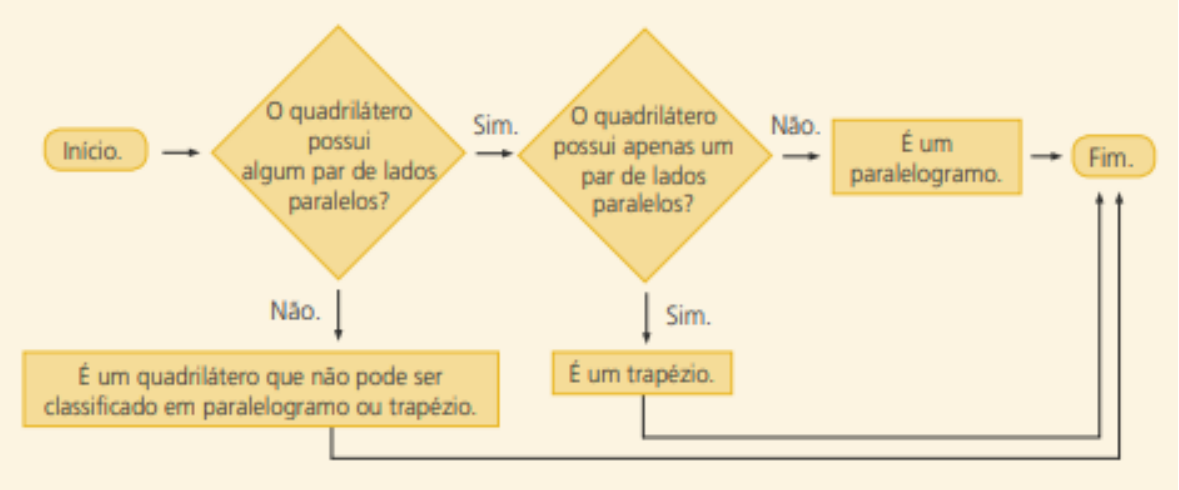


Figura 2.48: Fluxograma habilidade (EF08MA14) - Classificação dos quadriláteros (livro PNLD-2020)

Ele aborda apenas as classificações referente a seus lados, restringindo-se apenas a classificação como paralelogramo ou trapézio, porém poderia conter as classificações em retângulo, losango ou quadrado. Essa habilidade não pede para que seja escrito um algoritmo em linguagem de fluxograma.

2.2.4 Habilidades 9º ano - Fluxogramas - BNCC

Nesse ano é pedido que o aluno desenvolva a seguinte habilidade com relação aos fluxogramas.

(EF09MA15) Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um polígono regular cuja medida do lado é conhecida, utilizando régua e compasso, como também softwares.

Com régua e compasso podemos construir alguns polígonos regulares, como:

- Triângulo, que possui ângulo central de 120^o
- Quadrado, que possui ângulo central de 90^o
- Hexágono, que possui ângulo central de 60^o
- Dodecágono, que possui ângulo central de 30^o

Esses polígonos possuem ângulos internos que são facilmente obtidos dividindo-se a circunferência, pois como uma abertura do compasso é equivalente a um ângulo central de 60^o, ou seja, o triângulo e o hexágono podem ser construídos. E como a bissetriz de um arco de 60^o corresponde a um arco de 30^o, podemos com ela, construir o quadrado e o dodecágono.

Nos livros didáticos analisados foram encontrados exemplos de fluxogramas que trazem a construção de polígonos específicos.

Exemplo 2.46. Construção de polígonos regulares com régua e compasso (Hexágono) - livro PNLD 2020

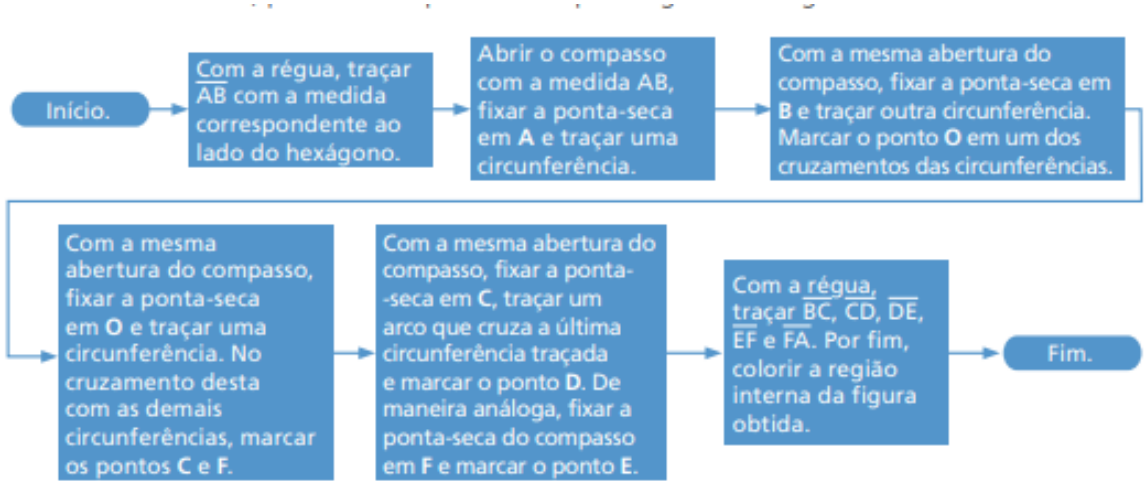


Figura 2.49: Fluxograma habilidade (EF09MA15) - Construção de um polígono regular I (livro PNLD-2020)

Esse fluxograma orienta o aluno para a construção de um hexágono regular com uso de compasso e régua. Essa construção, como mostramos e demos um exemplo, pode ser apresentada no 8° ano .

Exemplo 2.47. Construção de polígonos regulares com régua e compasso (Quadrado) - livro PNLD 2020

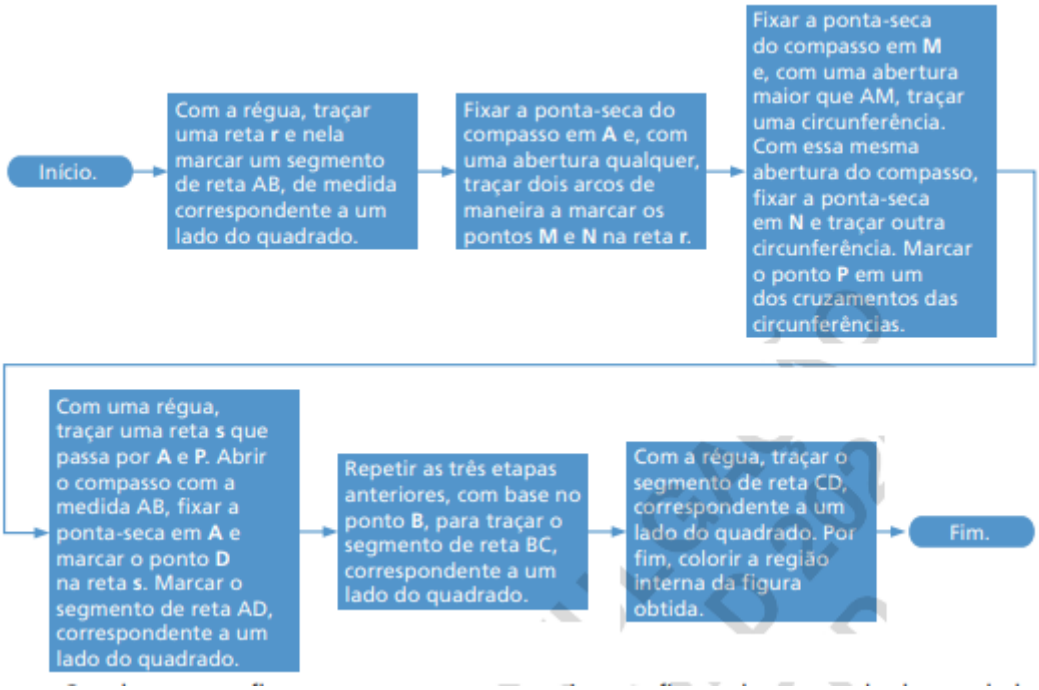


Figura 2.50: Fluxograma habilidade (EF09MA15) - Construção de um polígono regular II (livro PNLD-2020)

Neste exemplo temos a construção de um quadrado com compasso e régua, também já foi dado um exemplo de construção nas habilidades do 8° ano.

Exemplo 2.48. Construção de polígonos regulares com régua e compasso (Triângulo) - livro PNLD 2020

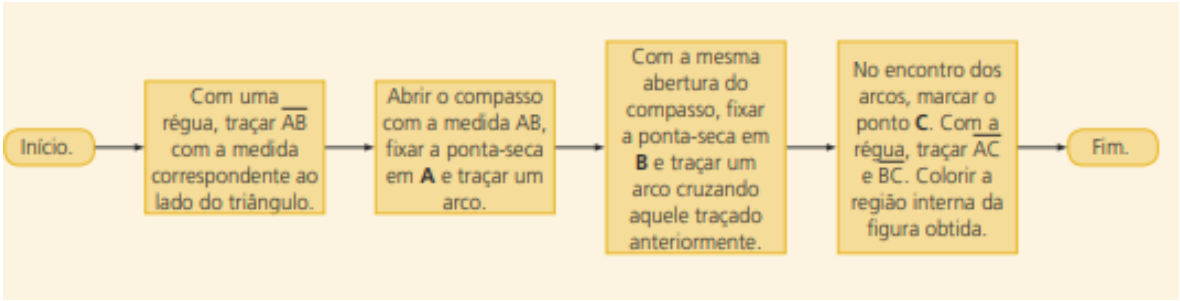


Figura 2.51: Fluxograma habilidade (EF09MA15) - Construção de um polígono regular III (livro PNLD-2020)

Este fluxograma é um exercício do livros didático para que o aluno construa um triângulo equilátero utilizando régua e compasso.

Nos três exemplos a estrutura dos fluxogramas está correta, porém suas informações não se encontram de forma clara, dificultando a compreensão do aluno.

Exemplo 2.49. Construção de polígonos regulares com régua e compasso (Hexágono) - livro PNLD 2020

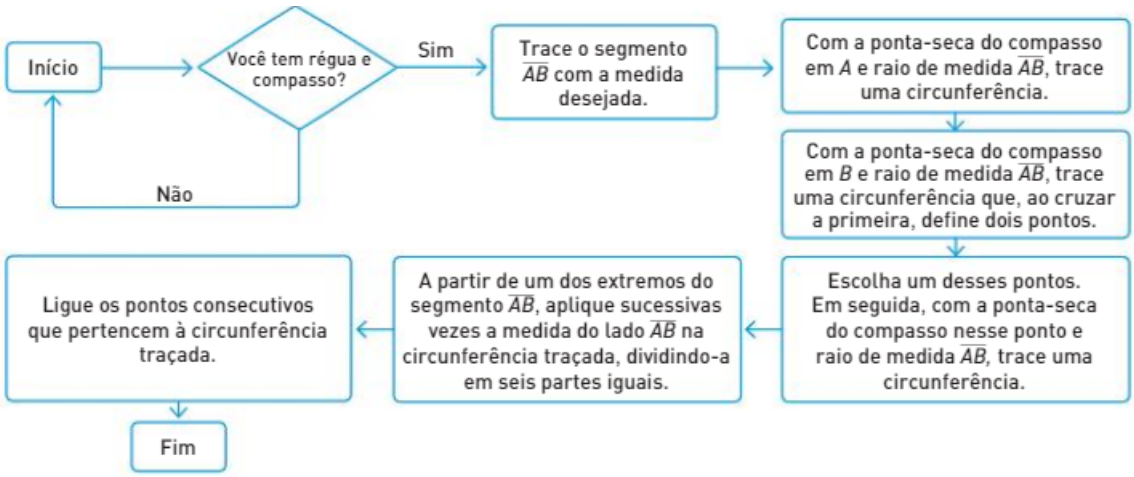


Figura 2.52: Fluxograma habilidade (EF09MA15) - Construção de um polígono regular IV (livro PNLD-2020)

Temos novamente um exemplo de construção de um hexágono regular, mas esse fluxograma contém pequenos erros de estrutura.

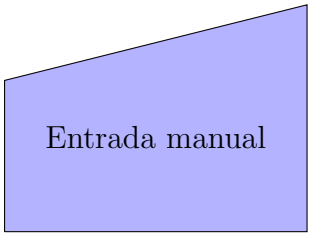
Os símbolos de terminação (início/fim) devem ser formas ovaladas e novamente temos uma pergunta desnecessária sobre ter os instrumentos necessários para a construção.

Foram escolhidas, pelos materiais didáticos analisados, as construções mais simples e já contempladas em anos anteriores. Os demais polígonos regulares teriam um grau elevado para a construção apenas com régua e compasso, seria necessário um transferidor para isso. Porém não é o que essa habilidade exige, assim o uso do *software* seria de grande valia.

Porém, não encontrei nenhum fluxograma orientando a construção de polígonos regulares utilizando *softwares*. O *GeoGebra* talvez seja o *software* de construção geométrica mais utilizado, por isso utilizaremos ele no nosso exemplo, a versão utilizada é a *GeoGebra Classic* para computador, mas também pode ser utilizada a versão para *smartphone*, os comandos são os mesmos.

O fluxograma mostra como construir um polígono regular de n lados de medida l.

Nesse exemplo foi utilizado uma forma não convencional no fluxograma, ela é utilizada quando tem-se que realizar um processo manual, ou seja, um passo que deve ser feito manualmente e não automaticamente.



Sempre que aparecer uma forma não convencional em um fluxograma é necessário que se explique ao aluno sua funcionalidade, pois, a grande diferença entre os fluxogramas e as outras estruturas de organização é justamente essa, cada forma representa uma determinada ação a ser realizada. E como a BNCC específica os fluxogramas, o aluno deve ter conhecimento de sua estrutura.

Exemplo 2.50. Construção de polígonos regulares no *GeoGebra*

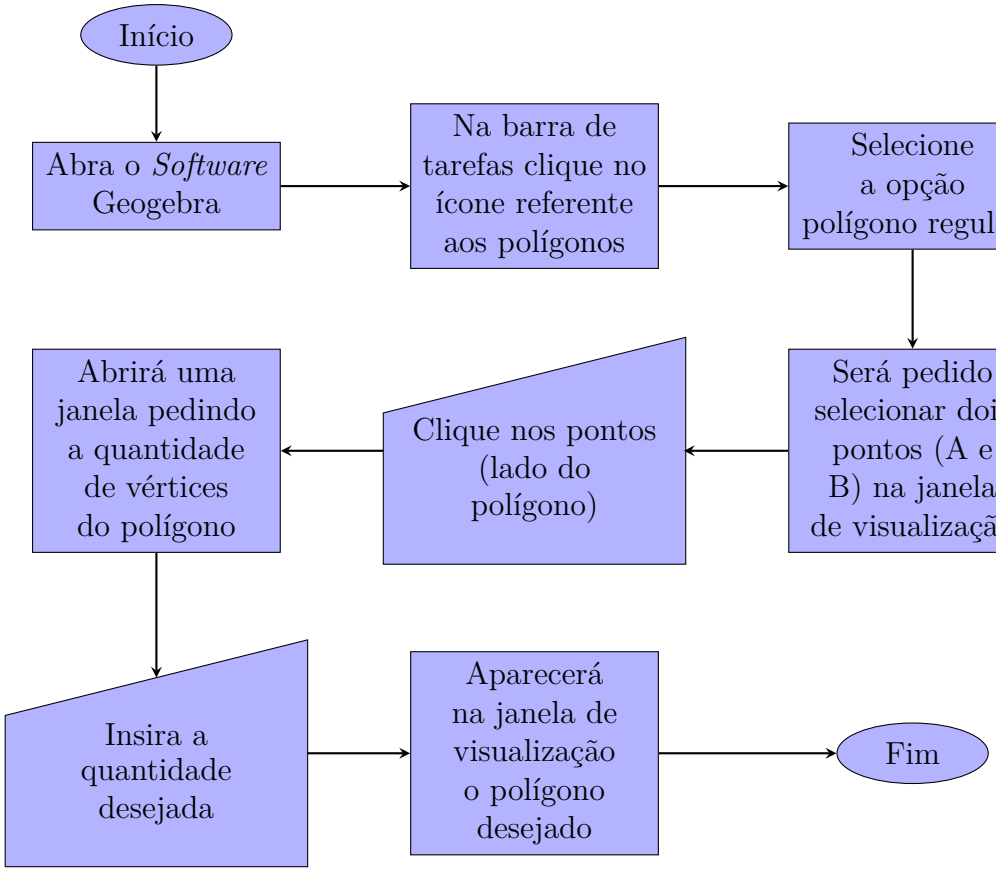


Figura 2.53: Fluxograma de autoria própria - Construção de polígonos regulares no *GeoGebra*

A seguir estão as imagens da construção de um heptágono regular, com elas o leitor que não estiver familiarizado com o *software GeoGebra* poderá seguir as instruções sem maiores dificuldades.

Exemplo 2.51. Utilização do *software GeoGebra* para construção de um heptágono regular

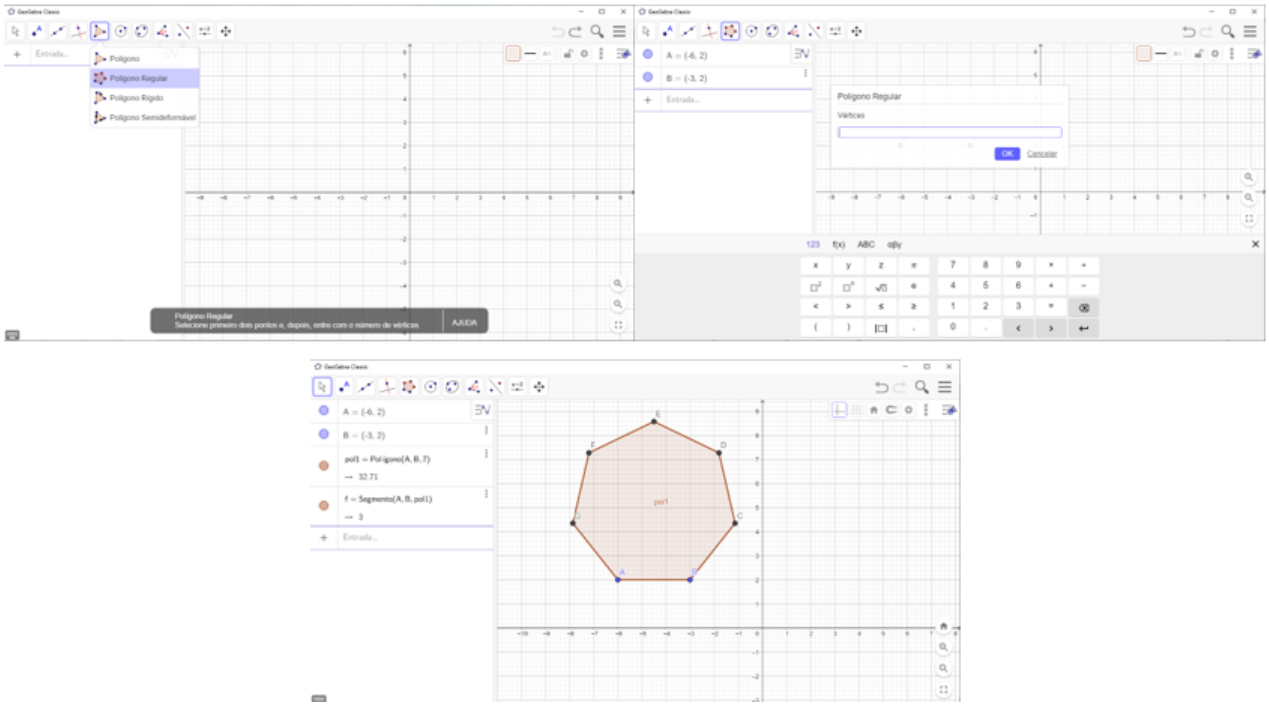


Figura 2.54: Construção de polígonos utilizando o *GeoGebra*

2.2.5 Habilidade Ensino Médio - Fluxogramas - BNCC

Os alunos dessa etapa já devem estar aptos a transformar algoritmos em fluxogramas, pois o conceito é trabalhado nos anos finais do Ensino Fundamental. Assim a proposta da BNCC para o Ensino Médio em relação aos fluxogramas é a seguinte habilidade:

- (EM13MAT315) Reconhecer um problema algorítmico, enunciá-lo, procurar uma solução e expressá-la por meio de um algoritmo, com o respectivo fluxograma.

Os exemplos de fluxogramas dos anos finais do Ensino Fundamental, apresentados nesse trabalho foram retirados do Programa Nacional do Livro e Material Didático (PNLD 2020), porém para o Ensino médio o PNLD é referente ao ano de 2021 e as obras que serão distribuídas para analise, até o presente momento não estão liberadas.

Os livros que estão a disposição são da versão anterior, referentes aos anos de 2015 e 2016, em que a Base Nacional Comum Curricular (BNCC), ainda não estava homologada, estava apenas começando a ser pensada e estruturada. Por isso não teremos exemplos de fluxogramas desta etapa escolar.

Uma sugestão seria por exemplo a resolução de problemas envolvendo equações do segundo grau utilizando o método resolutivo (Bhaskara).

Exemplo 2.52. Fluxograma para resolver problemas que envolvam equação do tipo $ax^2 + bx + c = 0$

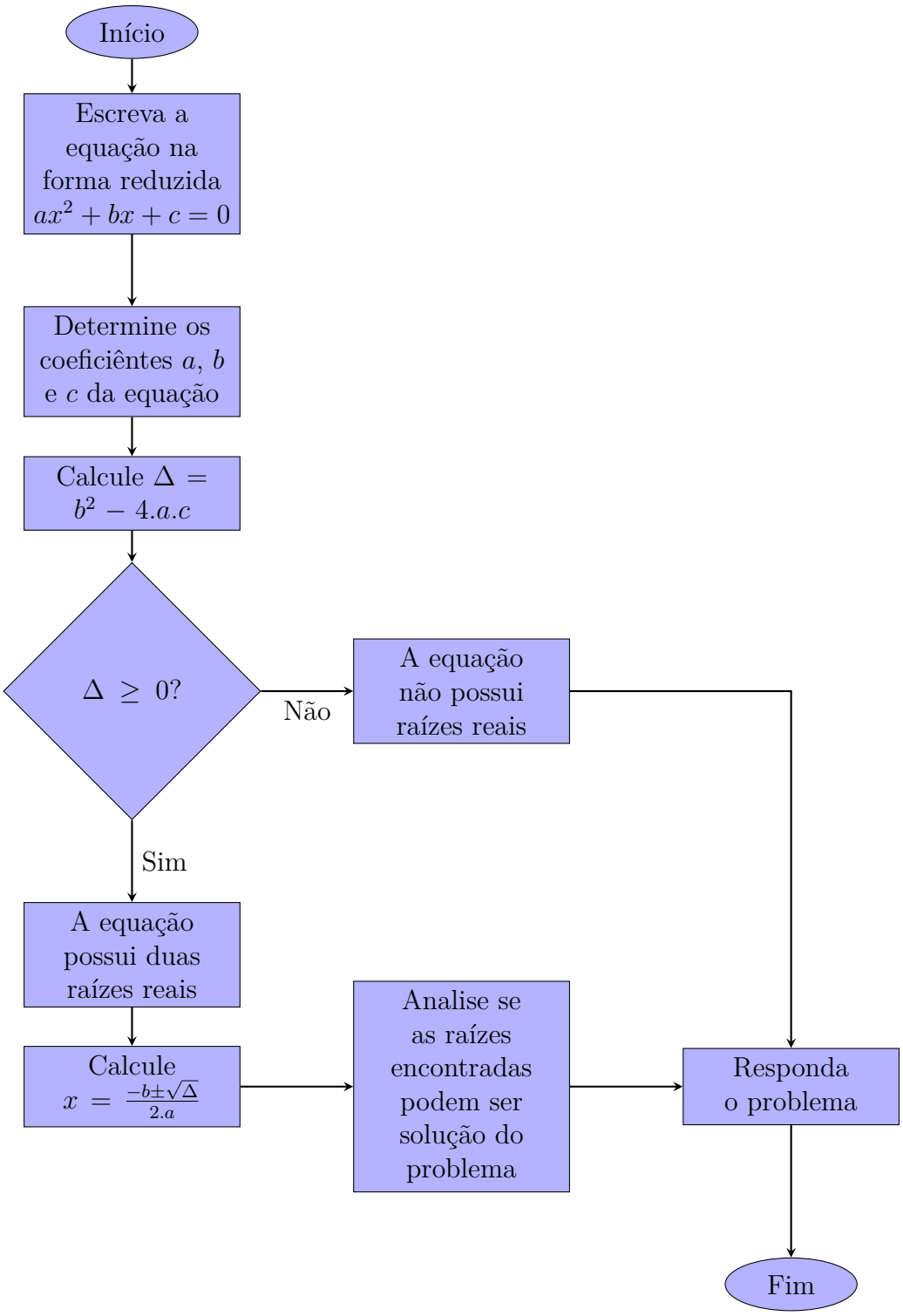


Figura 2.55: Fluxograma de autoria própria - Fórmula resolutiva da equação do 2° grau com uma incógnita

O aluno já conhece os algoritmos, pois trabalhou com ele no 9° ano do Ensino Fundamental (fórmula resolutiva da equação do 2° grau com uma incógnita), como também o conceito de fluxograma, assim para contemplar a habilidade ele deve ser capaz de representar o algoritmo em forma de fluxograma.

Assim, se as habilidades referente aos fluxogramas foram bem desenvolvidas durante a etapa do Ensino Fundamental, o aluno não deve apresentar maiores dificuldades com

relação a essa habilidade.

Com esse último exemplo, finalizamos o capítulo de fluxograma. Seguiremos com o conteúdo de divisibilidade, que dará o suporte teórico para este trabalho, para então chegarmos ao objetivo do mesmo, construir fluxogramas que auxiliem no aprendizado do conteúdo de divisibilidade.

3 Divisibilidade

A Aritmética, como é chamada a parte elementar da Teoria dos Números, teve como principal marco inicial a obra "Os Elementos de Euclides"(aproximadamente 300 a.C), tendo seu ápice nos trabalhos de Pierre de Fermat (1601-1665) e Leonhard Euler (1707-1783), tornando-a um dos principais pilares da Matemática. A partir do início do século XIX, graças a obra de Carl Friedrich Gauss (1777-1855), a Aritmética transforma-se em Teoria dos Números e começa a ter um desenvolvimento extraordinário.

Esse capítulo teve como base para sua escrita o livro Aritmética da Coleção PROFMAT-SBM. [25]

3.1 Números Inteiros

O desenvolvimento histórico dos números negativos é algo ainda muito discutido, principalmente quanto a cronologia. Ainda não se pode afirmar com certeza quando se deu o início do conceito de número negativo.

Os egípcios faziam uso de linhas de níveis, onde *nfr*, era a linha base e se tinha linhas acima e abaixo dela, com medidas de um cúbito. Mas os egípcios não tinham sequer a representação para o zero, muito menos para os números negativos. Logo não foi no Egito o surgimento dos números negativos.

Na China foram encontrados os primeiros registros de números negativos, não se tem precisão da data, estima-se que foi durante a dinastia *Han* (206a.C a 220 d.C).

Os números negativos, provavelmente surgiram no contexto de resolução de equações, porém, não se tinha nesse período uma simbologia para essas equações como conhecemos hoje. Eles se utilizavam de varas, vermelhas para representar os negativos e pretas para representar os positivos. A ideia de positividade e negatividade dos chineses era vista como características complementares. Também não tratavam os negativos como independentes, e sim como intermediários na resolução de algum algoritmo, como por exemplo, no cálculo de raízes de um polinômio.

Paralela a dinastia *Han*, na Mesopotâmia, surgiam o uso de regras de sinais em tábuas astronômicas, mas o fato se deu devido a um erro de interpretação, originando a concepção dos números negativos. Logo é um equívoco pensar que eles tinham conhecimento e se utilizavam desses números.

Influenciada pela civilização chinesa, a matemática *hindu* é reconhecida pelo trato com números negativos, porém não se sabe precisamente a data da concepção desses números em sua matemática. A forma estruturada que os números negativos tinham na matemática hindu, está atribuída ao matemático *Bhahmagupta*(598-665 d.C.). Mas mesmo entre os matemáticos hindus, não se tinham um acordo sobre os números negativos, pois o famoso *Bhaskara*, desconsiderava as raízes negativas da equação $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$.

Ao longo dos anos, muitos matemáticos importantes discutiram sobre o conceito dos números negativos. Essa discussão teve um fim em meados do século XIX, com o trabalho *Treatise on Algebra*, no qual por meio de uma estrutura lógica, propiciou a aceitação completa dos números negativos.

O leitor que se interessar pode consultar o livro "Um estudo histórico- Epistemológico do conceito de números negativos". [26]

Nos dias atuais, os números negativos fazem parte do *Conjunto dos Números Inteiros* $\mathbb{Z}$, que será assunto desta seção.

Seja :

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

juntamente com as operações de adição $(a, b) \longmapsto a + b$ e de multiplicação $(a, b) \longmapsto a \cdot b$.

A base para a construção do conjunto dos números inteiros $\mathbb{Z}$ é dada de forma axiomática.

1) A adição e a multiplicação estão bem definidas nos Inteiros:

$$\forall\ a, b, a', b' \in \mathbb{Z}, \quad a = a' \quad \text{e} \quad b = b' \Rightarrow a + b = a' + b' \quad \text{e} \quad a.b = a'.b'.$$

2 A adição e a multiplicação são *comutativas*:

$$\forall\ a, b \in \mathbb{Z}, \quad a + b = b + a \quad \text{e} \quad a.b = b.a.$$

3) A adição e a multiplicação são *associativas*:

$$\forall\ a, b, c \in \mathbb{Z}, \quad (a + b) + c = a + (b + c) \quad \text{e} \quad (a.b).c = a.(b.c).$$

4) A adição e a multiplicação possuem *elemento neutro*:

$$\forall\ a \in \mathbb{Z}, \quad a + 0 = a \quad \text{e} \quad a.1 = a.$$

5) A adição possui *elemento simétrico*

$$\forall\ a \in \mathbb{Z},\ \text{existe} \quad b = (-a) \quad \text{tal que} \quad a + b = a + (-a) = 0.$$

6) A multiplicação é *distributiva* com relação à adição:

$$\forall\ a, b, c \in \mathbb{Z},\ a \cdot (b + c) = a \cdot b + a \cdot c.$$

Os números inteiros, juntamente com suas propriedades, na terminologia moderna é o que chamamos de *anel*.

O conjunto dos números inteiros é composto de três subconjuntos:

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N},$$

onde $-\mathbb{N}$ é o conjunto dos simétricos de $\mathbb{N}$.

Proposição 3.1.

$$a \cdot 0 = 0,\ \textit{para todo}\ a \in \mathbb{Z}.$$

Demonstração.

$$a \cdot 0 = a.(0 + 0) = a \cdot 0 + a \cdot 0.$$

Somando $-(a \cdot 0)$ em ambos os membros da igualdade, obtemos:

$$a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) = a \cdot 0 + a \cdot 0 - (a \cdot 0) =$$

$$0 = -(a \cdot 0) + a \cdot 0 = -(a \cdot 0) + (a \cdot 0) + (a \cdot 0) = (-(a \cdot 0) + a \cdot 0) + a \cdot 0 = 0 + a \cdot 0 = a \cdot 0.$$

□

Proposição 3.2. *A adição é compatível e cancelativa com respeito a igualdade:*

$$\forall\, a, b, c, \in \mathbb{Z}, \quad a = b \Leftrightarrow a + c = b + c.$$

Demonstração. $a = b \Rightarrow a + c = b + c$ é consequência do fato da adição ser bem definida. Suponha agora que $a+c = b+c$. Somando $(-c)$ a ambos os membros da igualdade, temos

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

$$a = b.$$

□

A operação de adição permite-nos definir uma nova operação chamada de *subtração*. Dados dois números inteiros a e b, define-se o número b menos a, denotado por $b - a$, como sendo:

$$b - a = b + (-a).$$

Dizemos que $b - a$ é o resultado da *subtração* de b por a.

Admitiremos que em $\mathbb{Z}$ valem as seguintes propriedades:

7) *Fechamento de* $\mathbb{N}$: O conjunto $\mathbb{N}$ é fechado para adição e para multiplicação, ou seja, para todos $a, b \in \mathbb{N}$, tem-se que $a + b \in \mathbb{N}$ e $a \cdot b \in \mathbb{N}$.

8) *Tricotomia*: Dados $a, b \in \mathbb{Z}$, uma, e apenas uma, das seguintes possibilidades é verificada:

i) $a = b$.

ii) $b - a \in \mathbb{N}$.

iii) $-(b - a) \in \mathbb{N}$.

Dizemos que a é *menor do que* b, simbolizando $a < b$, toda vez que a propriedade (ii) for verificada. Com base na propriedade (iii) acima, equivale a afirmar que $b < a$. Utilizaremos a notação $b > a$, para representar $a < b$.

Como $a - 0 = a$, decorre das definições que $a > 0$ se, e somente se, $a \in \mathbb{N}$. Portanto,

$$\{x \in \mathbb{Z}; x > 0\} = \mathbb{N} \quad \text{e} \quad \{x \in \mathbb{Z}; x < 0\} = -\mathbb{N}$$

Decorre então que $a > 0$ se, e somente se, $-a < 0$.

Proposição 3.3. *A relação "menor do que"é transitiva:*

$$\forall\, a, b, c \in \mathbb{Z}, \quad a < b \quad e \quad b < c \quad \Rightarrow \quad a < c.$$

Demonstração. Supondo que $a < b$ e $b < c$, temos que $(b-a) \in \mathbb{N}$ e $(c-b) \in \mathbb{N}$. Como $\mathbb{N}$ é aditivamente fechado, temos que

$$c - a = c - a + b - b = (b-a) + (c-b) \in \mathbb{N}.$$

logo $a < c$.

□

Proposição 3.4. *A adição é compatível e cancelativa com respeito à relação "menor do que":*

$$\forall\, a, b, c \in \mathbb{Z}, \quad a < b \quad \Leftrightarrow \quad a + c < b + c.$$

Demonstração. Suponha que $a < b$. Logo, $b - a \in \mathbb{N}$. Portanto,

$$(b + c) - (a + c) = b - a \in \mathbb{N},$$

o que implica que $a + c < b + c$.

Reciprocamente, suponha que $a+c < b+c$. Pela Proposição 3.2, podemos somar $(-c)$ a ambos os lados da desigualdade.

$$a + c + (-c) < b + c + (-c) \quad \Rightarrow \quad a < b.$$

□

Proposição 3.5. *A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação "menor do que":*

$$\forall\, a, b \in \mathbb{Z}, \quad \forall\, c \in \mathbb{N}, \quad a < b \quad \Leftrightarrow \quad ac < bc.$$

Demonstração. Suponha que $a < b$. Logo $b - a \in \mathbb{N}$. Assim, se $c \in \mathbb{N}$, pelo fato de $\mathbb{N}$ ser multiplicativamente fechado, temos

$$bc - ac = (b-a)c \in \mathbb{N},$$

logo, $ac < bc$. Reciprocamente, suponha que $ac < bc$, com $c \in \mathbb{N}$. Pela tricotomia, temos três possibilidades a analisar:

i) $a = b$. Isso acarretaria $ac = bc$, o que é falso.

ii) $b < a$. Isso acarretaria, que $bc < ac$, como provado na primeira parte, também é falso.

iii) $a < b$. Está é a única possibilidade válida.

□

Proposição 3.6. *A multiplicação é compatível e cancelativa com respeito à igualdade:*

$$\forall\, a, b \in \mathbb{Z},\ \forall\, c \in \mathbb{Z} \setminus \{0\}, \quad a = b \quad \Leftrightarrow \quad ac = bc.$$

Demonstração. A implicação $a = b \ \Rightarrow \ ac = bc$ vale também quando $c = 0$ e decorre imediatamente do fato da multiplicação ser bem definida.

Suponha agora que $ac = bc$. Temos duas possibilidades:

i) Caso $c > 0$. Se $a < b$, temos $ac < bc$, o que é um absurdo. Se $b < a$, temos $bc < ac$, o que também é um absurdo. Portanto a única alternativa válida é $a = b$.

ii) Caso $-c > 0$. A mesma argumentação se segue para o caso $c > 0$, levando em conta que $d <$ e se, e somente se, $-d > -$e.

□

Concluímos com as proposições acima que $\mathbb{Z}$ é um *domínio de integridade*, isto é, se a e b são inteiros tais que $ab = 0$, então $a = 0$ ou $b = 0$. De fato, se $a \neq 0$, então $ab = 0 = a \cdot 0$. Pelo cancelamento de $a \neq 0$ segue-se que $b = 0$.

Observe que a relação $<$ não é uma relação de ordem, pois não é reflexiva. Podemos no entanto, por meio dela obter uma relação de ordem. Diremos que a é o *menor ou igual* do que b, ou que b é *maior ou igual* que a, em simbologia, $a \leq b$ ou $b \geq a$, se $a < b$ ou $a = b$.

Note que $a \leq b$ se, e somente se, $b - a \in \mathbb{N} \cup \{0\}$. Agora, podemos verificar efetivamente uma relação de ordem, pois possui as seguintes propriedades:

1) É reflexiva: $\forall\, a \in \mathbb{Z},\ a \leq a$.

2) É antissimétrica: $\forall\, a, b \in \mathbb{Z}, \quad a \leq b \quad \text{e} \quad b \leq a \quad \Rightarrow \quad a = b$.

3) É transitiva: $\forall\, a, b, c \in \mathbb{Z}, \quad a \leq b, \quad \text{e} \quad b \leq c \quad \Rightarrow \quad a \leq c$.

Vamos precisar de uma importante definição para prosseguir.

Definição 3.7. Valor *absoluto*, ou *módulo*.

Seja $a \in \mathbb{Z}$, definimos

$$|a| = \begin{cases} a, & \text{se } a \geq 0, \\ -a, & \text{se } a < 0. \end{cases}$$

Note que para todo $a \in \mathbb{Z}$, tem-se que $|a| \geq 0$ e $|a| = 0$ se, e somente se, $a = 0$.

O valor absoluto possui as seguintes propriedades:

Proposição 3.8. *Para todo $a, b \in \mathbb{Z}$ e $r \in \mathbb{N}$, temos*

i) $|ab| = |a|\,|b|$;

ii) $|a| \leq r$, *se, e somente se,* $-r \leq a \leq r$;

iii) $-|a| \leq a \leq |a|$;

iv) a desigualdade triangular

$$|\,|a| - |b|\,| \quad \leq \quad |a \pm b| \quad \leq \quad |a| + |b|.$$

Vamos demostrar apenas a propriedade da desigualdade triangular, as demais deixaremos a cargo do leitor.

Demonstração. Se a e b são números inteiros, temos

$$-|a| \leq a \leq |a| \quad \text{e} \quad -|b| \leq b \leq |b|.$$

Somando membro a membro, obtemos

$$-(|a| + |b|) \leq a + b \leq (|a| + |b|).$$

Se $a+b \geq 0$, então $|a+b| = a+b \leq (|a|+|b|)$. Se $a+b < 0$, então $|a+b| = -(a+b) \leq |a|+|b|$.

Agora, pelo resultado anterior temos que $|a| = |b+(a-b)| \leq |b|+|a-b| \Rightarrow |a|-|b| \leq |a-b|$ e $|b| = |a+(b-a)| \leq |a| + |a-b| \Rightarrow -|a-b| \leq |a| - |b|$.

Assim, $-|a-b| \leq |a|-|b|$ e $|a|-|b| \leq |a-b|$, segue por (ii) que $||a|-|b|| \leq |a-b|$. □

3.1.1 Princípio da Boa Ordenação

As propriedades de números inteiros e suas operações ainda não são suficientes para caracterizá-los. No entanto, há uma propriedade que só os inteiros possuem, que é o *Princípio da Boa Ordenação.*

Definição 3.9. Diremos que um subconjunto $S \in \mathbb{Z}$ é *limitado inferiormente*, se existir $c \in \mathbb{Z}$ tal que $c \leq x$ para todo $x \in \mathbb{S}$. Diremos que $a \in S$ é *um menor elemento* de S se $a \leq x$ para todo $x \in S$.

O conjunto vazio, apesar de não possuir nenhum elemento, consideraremos possuir um menor elemento, ou seja ser limitado inferiormente por qualquer que seja a cota inferior.

Observação: O menor elemento de S se existir é único, pois se a e a' são dois menores elementos de S, temos $a \leq a'$ e $a' \leq a$, o que implica $a = a'$.

Os conjuntos $\mathbb{Z}$ e $-\mathbb{N}$ não são limitados inferiormente, portanto não possuem um menor elemento, já o conjunto $\mathbb{N}$ é limitado inferiormente e possui 1 como menor elemento.

9) *Princípio da Boa Ordenação*: Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.

Agora os números inteiros estão completamente caracterizados e podemos nos utilizar do Princípio da Boa Ordenação para demonstrar algumas proposições.

Proposição 3.10. *Não existe nenhum inteiro n tal que $0 < n < 1$.*

Demonstração. Suponha por absurdo que exista n com essa propriedade. Logo o conjunto $S = \{x \in \mathbb{Z}; \quad 0 < x < 1\}$ é não vazio, além de ser limitado superiormente. Portanto S possui um menor elemento a, com $0 < a < 1$, multiplicando a desigualdade por a, obtemos $0 < a^2 < a$ e como $a < 1$, temos $0 < a^2 < a < 1$, logo $a^2 \in S$ e $a^2 < a$, uma contradição, pois, a é o menor elemento de S. Concluímos então que $S = \varnothing$. □

Corolário 3.11. *Dado um número inteiro n qualquer, não existe nenhum inteiro m tal que $n < m < n + 1$.*

Demonstração. Suponha por absurdo que exista, um número m com tal propriedade, $n < m < n+1$, somando $-n$ em ambos os membros da desigualdade obtemos $0 < m - n < 1$, contradizendo a proposição anterior. □

Corolário 3.12. *Sejam $a, b \in \mathbb{Z}$. Se $ab = 1$, então $a = b = \pm 1$.*

Demonstração. Primeiramente note que se $a = 0$ e $b = 0$ temos $ab = 0$, logo a e b são ambos não nulos. Suponha $a > 0$. Como $ab = 1 > 0$, temos $b > 0$. Segue da proposição 3.10 que $a \geq 1$ e $b \geq 1$. Logo, $1 = ab \geq b \geq 1$, o que implica $b = 1$. Como $ab = 1$, temos também $a = 1$. O caso em que $a < 0$ é análogo, pois $b < 0$ e $ab = 1 > 0$. □

Corolário 3.13. *Se $a, b \in \mathbb{Z}$, com $b \neq 0$, então $|ab| \geq |a|$.*

Demonstração. Como $b \neq 0$, temos $|b| \geq 1$. Multiplicando ambos os membros da inequação por $|a|$ obtemos $|a|\ |b| \geq |a|$, pela propriedade do valor absoluto, temos $|ab| = |a|\ |b| \geq |a|$. □

Uma importante propriedade dos números inteiros é a *Arquimediana* que é dada a seguir.

Corolário 3.14. *Propriedade Arquimediana*
Sejam, $a, b \in \mathbb{Z}$, com $b \neq 0$. Então existe $n \in \mathbb{Z}$ tal que $nb > a$.

Demonstração. Como $|b| \neq 0$, temos que $|b| \geq 1$, logo

$$(|a| + 1)|b| \geq |a| + 1 > |a| \geq a.$$

Basta agora tomar $n = |a| + 1$, se $b > 0$ e $n = -(|a| + 1)$, se $b < 0$.

□

Definição 3.15. Um subconjunto T de $\mathbb{Z}$ será dito *limitado superiormente* se for vazio ou se existir um número $d \in \mathbb{Z}$ tal que

$$\forall\ x \in T, \quad x \leq d.$$

Neste caso , diremos que d é uma *cota superior* para T.

Note que definimos o conjunto vazio como limitado superiormente, logo qualquer número é uma cota superior.

O maior elemento de um conjunto, quando existir é único. De fato, sejam d e d', dois maiores elementos de T, temos $d \geq d'$ e $d' \geq d$, logo $d = d'$.

O *Princípio da Boa Ordenação* pode ser formulado da seguinte maneira:

Proposição 3.16. *Se T é um subconjunto não vazio de $\mathbb{Z}$ e limitado superiormente, então T possui um maior elemento.*

Demonstração. Suponha que d seja uma cota superior para T. Logo $x \leq d$ para todo $x \in \mathbb{Z}$. seja

$$S = \{y \in \mathbb{Z};\ y = d - x, \quad \text{com } x \in T\}.$$

O conjunto S é não vazio, e como $y = d - x \geq 0$, para todo $x \in T$, ele é limitado inferiormente. Logo pelo Princípio da Boa Ordenação, ele tem um menor elemento $d - b$, com $b \in T$. Vamos mostrar que b é o maior elemento de T. De fato, $d - x \in S$ e, portanto $d - x \geq d - b$, o que implica $x \leq b$.

□

Como consequência do Princípio da Boa Ordenação, temos um importante instrumento de demostração nos números inteiros, que é o *Princípio de Indução Matemática.*

Teorema 3.17. *Princípio de Indução Matemática*
Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que

i) $a \in S$.

ii) S é fechado com relação a operação de "somar 1"a seus elementos, ou seja,

$$\forall\, n \in S \quad \Rightarrow \quad n+1 \in S.$$

Então, $\{x \in \mathbb{Z};\ x \geq a\} \subset S$.

Demonstração. Pondo $S' = \{x \in \mathbb{Z}, x \geq a\}$ e suponhamos por absurdo que $S' \not\subset S$, logo $S' \setminus S \neq \varnothing$. Como esse conjunto é limitado inferiormente por a, existe um menor elemento c em $S' \setminus S$. Assim, $c \in S'$ e $c \notin S$, temos que $c > a$, o que implica que $c - 1 \in S$. Pela hipótese sobre S, temos que $c = (c-1) + 1 \in S$, como $c \in S'$, obtemos uma contradição com o fato de $c \in S' \setminus S$. □

Segue-se do Princípio de Indução Matemática o importante método para prova de teoremas.

Teorema 3.18. *Prova por Indução Matemática*
Sejam $a \in \mathbb{Z}$ *e seja* $p(n)$ *uma sentença aberta em* n. *Suponha que*

i) $p(a)$ *é verdadeira, e que*

ii) $\forall\, n \geq a, \quad p(n) \quad \Rightarrow \quad p(n+1)$ *é verdadeiro.*

Então, $p(n)$ *é verdadeiro para todo* $n \geq a$.

Demonstração. Seja $\mathbb{V} = \{n \in \mathbb{Z};\ p(n)\}$, ou seja, $\mathbb{V}$ é o subconjunto dos elementos de $\mathbb{Z}$ para os quais $p(n)$ é verdadeiro.
Como por (i) $a \in \mathbb{V}$ e por (ii)

$$\forall\, n, \quad n \in \mathbb{V} \quad \Rightarrow \quad n+1 \in \mathbb{V},$$

segue-se do Princípio de Indução Matemática que $\{x \in \mathbb{Z}; x \geq a\} \subset \mathbb{V}$.

□

Note que, para provar que $p(n) \Rightarrow p(n+1)$ é verdadeiro para todo n, é preciso mostrar que, se $p(n)$ é verdadeiro para algum n, então $p(n+1)$ é verdadeiro, já que a implicação é verdadeira sempre que $p(n)$ é falso. Não confunda com usar a tese do teorema para provar o teorema, pois não é o caso, a tese é que $p(n)$ é verdadeiro para todo $n \geq a$.

A indução matemática, é utilizada para estabelecer verdades matemáticas, válidas sobre determinados subconjuntos infinitos de $\mathbb{Z}$. Não basta mostrar que certa sentença matemática aberta é verdadeira para um grande número de casos, mas sim, de provar que tal sentença é verdadeira para todo número natural maior ou igual do que algum $a \in \mathbb{Z}$.

O Princípio de Indução Matemática admite uma variação, denominada *Princípio da Indução Completa* ou *Segunda Forma do Princípio de Indução* ou ainda *Princípio de Indução Forte*, que é de grande utilidade.

Teorema 3.19. *Prova por Indução Completa*
Seja $p(n)$ *uma sentença aberta tal que*

i) $p(a)$ *é verdadeiro, e que*

ii) $\forall n,\ p(a)$ *e* $p(a+1)$ *e* $\ldots$ *e* $p(n)$ *é verdadeiro* $\quad \Rightarrow \quad p(n+1)$ *é verdadeiro.*

Então $p(n)$ é verdadeiro para todo $n \geq a$.

Demonstração. Considere o conjunto

$$\mathbb{V} = \{n \in (a + \mathbb{N}) \, ; p(n)\}.$$

Vamos mostrar que o conjunto $\mathbb{W} = (a + \mathbb{N}) \setminus \mathbb{V}$ é vazio. Suponha por absurdo, que vale o contrário. Logo, pelo Princípio da Boa Ordenação, $\mathbb{W}$ teria um menor elemento k, e, como sabemos por (i) que $a \notin \mathbb{W}$, segue-se que existe n tal que $k = a + n > a$. Portanto, $a, a+1, \ldots, k-1 \notin \mathbb{W}$; logo $a, a+1, \ldots k-1 \in \mathbb{V}$. Por (ii) conclui-se que $k = (k-1) + 1 \in \mathbb{V}$, o que contradiz o fato de $k \in \mathbb{W}$. □

Seja $\mathbb{A}$ um conjunto qualquer. Uma *sequência* em $\mathbb{A}$ é uma função

$$\begin{array}{rccc} s: & \mathbb{N} & \longrightarrow & \mathbb{A} \\ & n & \mapsto & s(n) \end{array}$$

Podemos denotar o elemento $s(n)$ de $\mathbb{A}$ por s_n. Uma sequência s também denotada por (s_n). Algumas vezes poderemos ter que o domínio de uma sequência seja o conjunto $\mathbb{N} \cup \{0\}$ em vez do conjunto $\mathbb{N}$.

O Princípio de Indução Completa será muito útil quando precisarmos provar que determinada sentença é verdadeira, sendo conhecido seus primeiros termos.

3.2 Divisibilidade

A divisão de um número inteiro por outro nem sempre é possível. Quando essa relação não existir, veremos que ainda será possível efetuar uma divisão com resto, chamada *divisão euclidiana*. Neste capítulo abordaremos várias propriedades nos inteiros.

Dados dois números inteiros a e b com $a \neq 0$, diremos que a *divide* b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$. Nesse caso diremos também que a é um *divisor* ou um *fator* de b ou, ainda, que b é um *múltiplo* de a. A negação dessa sentença é representada por $a \nmid b$. Note que a notação $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$.

Exemplo 3.20.

$$\pm 3 \mid 12 \Rightarrow 12 = 3 \cdot 4 \quad \text{e} \quad 12 = (-3) \cdot (-4)$$
$$\pm 3 \nmid 10 \Rightarrow 10 = 3 \cdot 3 + 1 \quad \text{e} \quad 10 = (-3) \cdot (-3) + 1.$$

Proposição 3.21. *Sejam $a, b, c \in \mathbb{Z}$. Tem-se que*

i) $1 \mid a, \quad a \mid a \quad e \quad a \mid 0.$

ii) $0 \mid a \quad \Leftrightarrow \quad a = 0.$

iii) a divide b se, e somente se $|a|$ divide $|b|$.

iv) se $a \mid b$ e $b \mid c$, então $a \mid c$.

Demonstração. Temos que

i) $a = a \cdot 1, \quad a = 1 \cdot a \quad \text{e} \quad 0 = 0 \cdot a.$

ii) Suponha que $0 \mid a$; logo, existe $c \in Z$ tal que $a = c \cdot 0$. Como $a \cdot 0 = 0$, conclui-se que $a = 0$. Para a recíproca basta observar que $0 \mid 0$, assim $0 = 0 \cdot a$.

iii) Suponha que $a \mid b \Rightarrow b = t \cdot a$, com $t \in \mathbb{Z}$. Tomando módulo em ambos os lados temos,

$$|b| = |a \cdot t| = |a| \cdot |t| \Rightarrow |a| \mid |b|.$$

Agora suponha que $|a| \mid |b|$, assim $|b| = t|a|$ com $t \in \mathbb{Z}$.

Pela definição de módulo,

$$|b| = \begin{cases} b & \text{se} \quad b \geq 0 \\ -b & \text{se} \quad b < 0 \end{cases}$$

Assim, $b = t|a|$, como $|a| \geq 0$, temos $t \geq 0$. Agora se $-b = t|a|$, temos $t < 0$. Portanto

$$|b| = |t| \cdot |a| \Rightarrow |b| = |t \cdot a| \Rightarrow b = t \cdot a \Rightarrow a \mid b.$$

iv) $a \mid b$ e $b \mid c$, ou seja, existem $f, g \in Z$, tais que $b = f \cdot a$ e $c = g \cdot b$. Substituindo o valor de b, temos

$$c = g \cdot b = g \cdot (f \cdot a) = (g \cdot f) \cdot a,$$

logo $a \mid c$.

□

Os itens (i) e (ii) da proposição acima nos dizem que todo $a \in \mathbb{Z}$ é divisível por ± 1 e por $\pm a$.

Observe que (i) inclui o caso $0 \mid 0$ e, portanto, todo número inteiro divide 0, ou seja, 0 tem infinitos divisores.

Suponha que $a \mid b$ e que $a \neq 0$ e seja $c \in \mathbb{Z}$ tal que $b = ac$. O número c, univocamente determinado, pois se $b = c \cdot a$ e $b = c' \cdot a$, temos $c = c'$ é chamado de *quociente* de b por a e denotado $c = \frac{b}{a}$. Uma observação importante é que $\frac{b}{a}$ só está definido quando $a \neq 0$ e $a \mid b$. Por exemplo,

$$\frac{0}{5} = \frac{0}{6} = 0, \quad \frac{7}{1} = 7, \quad \frac{15}{5} = 3, \quad \frac{20}{-4} = -5, \quad \frac{-27}{-9} = 3, \quad \frac{12}{12} = 1.$$

Assim,

$$a \mid b \Leftrightarrow \exists\, c \in \mathbb{Z};\ b = a \cdot c.$$

Proposição 3.22. *Se $a, b, c, d \in \mathbb{Z}$, então*

$$a \mid b \text{ e } c \mid d \quad \Rightarrow \quad ac \mid bd.$$

Demonstração. Se $a \mid b$ e $c \mid d$, então existem $f, g \in \mathbb{Z}$, tais que $b = f \cdot a$ e $d = g \cdot c$, e $bd = (fa) \cdot (gc)$, ou seja, $bd = (fg) \cdot (ac)$. Portanto $ac \mid bd$. □

Proposição 3.23. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então*

$$a \mid b \quad \Leftrightarrow \quad a \mid c.$$

Demonstração. Suponha que $a \mid (b+c)$. Logo , existe $f \in \mathbb{Z}$ tal que $b+c = f \cdot a$. Agora se $a \mid b$, temos que existe um $g \in \mathbb{Z}$ tal que $b = g \cdot a$, substituindo o valor de b obtemos

$$b + c = g \cdot a + c = f \cdot a \quad \Rightarrow \quad c = (f-g) \cdot a \Rightarrow a \mid c.$$

A implicação contrária é análoga.

Agora, se $a \mid (b-c)$ e $a \mid b$, pelo caso anterior temos que $a \mid -c = -1 \cdot c$, o que implica que $a \mid c$. Novamente a implicação contrária é análoga. □

Proposição 3.24. *Se $a, b, c \in \mathbb{Z}$ são tais que $a \mid b$ e $a \mid c$, então para todo $x, y \in \mathbb{Z}$ temos que*

$$a \mid (xb + yc).$$

Demonstração. $a \mid b$ e $a \mid c$ implica que existem $f, g \in \mathbb{Z}$ tais que $b = f \cdot a$ e $c = g \cdot a$. Logo,

$$xb + yc = x(f \cdot a) + y(g \cdot a) = (xf + yg)a,$$

o que prova o resultado. □

Proposição 3.25. *Dados $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que*

$$a \mid b \quad \Rightarrow \quad |a| \leq |b|.$$

Demonstração. Se $a \mid b$, existe $c \in \mathbb{Z}$ tal que $b = ca$. Tomando módulos, temos que $|b| = |c| \cdot |a|$. Como $b \neq 0$, temos que $c \neq 0$, logo $1 \leq |c|$ e, consequentemente, $|a| \leq |a| \cdot |c| = |b|$. □

Em particular, se $a \in \mathbb{Z}$ e $a \mid 1$, então $0 < |a| \leq 1$, logo $|a| = 1$ e, portanto, $a = \pm 1$.

Como, para $b \neq 0$, temos que todo divisor a de b é tal que $|a| \leq |b|$, segue-se, nesse caso, que b tem um número finito de divisores que estão o intervalo $-|b| \leq a \leq |b|$.

Note que a relação de divisibilidade em $\mathbb{N} \cup \{0\}$ é uma relação de ordem, pois

i) é reflexiva: $\forall\, a \in \mathbb{N},\ a \mid a$.

ii) é transitiva: se $a \mid b$ e $b \mid c$, então $a \mid c$.

iii) é antissimétrica: se $a \mid b$ e $b \mid a$, então $a = b$.

Entretanto, a relação de divisibilidade não é uma relação de ordem em $\mathbb{Z}$, pois, apesar de ainda ser reflexiva e transitiva, ela não é antissimétrica. Note que se $a \in \mathbb{Z}$ temos $-a \mid a$ e $a \mid -a$, mas $a \neq -a$.

As proposições a seguir serão utilizadas em seções posteriores.

Proposição 3.26. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a - b$ divide $a^n - b^n$.*

Demonstração. Faremos a prova por indução sobre n.

É fácil verificar que a afirmação é verdadeira para $n = 1$, pois, $a-b$ divide $a^1 - b^1 = a-b$.

Suponhamos agora, a afirmação ser verdadeira para n, logo $a-b$ divide $a^n - b^n$. Vamos provar que a afirmação é verdadeira para $n+1$.

$$a^{n+1} - b^{n+1} = aa^n - bb^n = aa^n - ba^n + ba^n - bb^n = (a-b)a^n + b(a^n - b^n).$$

Pelo caso base $a-b$ divide $a-b$, logo $a-b$ divide $(a-b)a^n$ e pela hipótese $a-b$ divide $a^n - b^n$, e portanto, $a-b$ divide $b(a^n - b^n)$. Assim concluímos que $a-b$ divide $a^{n+1} - b^{n+1}$. Pelo Princípio de Indução Matemática $a - b$ divide $a^n - b^n$ para todo $n \in \mathbb{N}$. □

Note que não depende do expoente ser par ou ímpar, quando se trata de $a-b$ dividir $a^n - b^n$.

Agora se tivermos uma soma, veremos que precisamos dividir em dois casos.

Proposição 3.27. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $a+b$ divide $a^{2n+1} + b^{2n+1}$.*

Demonstração. Também a faremos por indução sobre n.

A afirmação é verdadeira para $n = 0$ pois, $a^{2\cdot 0+1} + b^{2\cdot 0+1} = a^1 + b^1 = a + b$.

Suponhamos ser válida para n, ou seja, $a+b$ divide $a^{2n+1} + b^{2n+1}$, e mostraremos ser válida para $n+1$.

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

Temos que $(a^2 - b^2) = (a+b)(a-b)$ e pelo caso base $a+b$ divide $a+b$ e portanto $a+b$ divide $(a+b)(a-b)$. Pela hipótese de indução $a+b$ divide $a^{2n+1} + b^{2n+1}$. Assim podemos concluir que $a+b$ divide $a^{2(n+1)+1} + b^{2(n+1)+1}$.

Portanto pelo Princípio de Indução temos que $a+b$ divide $a^{2n+1} + b^{2n+1}$ para todo $n \in \mathbb{N}$.

□

Proposição 3.28. *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $a+b$ divide $a^{2n} - b^{2n}$.*

Demonstração. Faremos também por indução sobre n.

A afirmação é verdadeira para $n = 1$, pois $a+b$ divide $a^{2\cdot 1} - b^{2\cdot 1} = a^2 - b^2 = (a-b)(a+b)$.

Suponhamos agora, que $a+b$ divide $a^{2n} - b^{2n}$, e vamos provar ser verdadeira para $n+1$.

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

Como provado no caso base $a+b$ divide $(a^2 - b^2)$, logo $a+b$ divide $(a^2 - b^2)a^{2n}$ e pela hipótese de indução $a+b$ divide $a^{2n} - b^{2n}$, portanto $a+b$ divide $b^2(a^{2n} - b^{2n})$.

Assim, temos que $a+b$ divide $a^{2(n+1)} - b^{2(n+1)}$ e pelo princípio da indução $a+b$ divide $a^{2n} - b^{2n}$ para todo $n \in \mathbb{N}$.

□

Portanto, se o expoente t da potência for ímpar, $a+b$ divide $a^t + b^t$, e se, por outro lado, o expoente s for par, $a+b$ divide a $a^s - b^s$.

3.3 Divisão Euclidiana

Não se sabe muito sobre Euclides, as fontes históricas sobre sua vida são poucas e muitas vezes incertas. Um suposto relato de Eudemo, diz que Euclides estudou em Atenas, juntamente com alunos de Platão. Depois teria mudado para Alexandria, onde foi convidado a ser professor de um importante museu.

Euclides além da matemática se interessava por astronomia e óptica. Seus escritos sobrevivem até os dias de hoje, os famosos *Elementos*.

Os *Elementos* foram divididos em 13 livros, onde pode-se encontrar estudos sobre: geometria plana, teoria das proporções, aritmética, entre outros. O fascínio da humanidade sobre os *Elementos*, deve-se da forma como Euclides tratou a Matemática, construindo-a de método *axiomático*. Os *Elementos* foram a obra científica mais influente por muitos anos.

Mesmo quando um número inteiro não é divisível por outro, também inteiro, podemos efetuar uma divisão com resto. A essa divisão se dá o nome de *Divisão Euclidiana*, que será a base para a construção do conceito de divisibilidade.

Teorema 3.29. *Divisão Euclidiana*

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

$$a = bq + r, \quad com\ 0 \leq r < |b|.$$

Demonstração. Considere o conjunto

$$\mathbb{S} = \{x = a - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\}).$$

Vamos primeiramente provar a existência. Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$, tal que $n(-b) > -a$, logo $a - nb > 0$, o que nos mostra que $\mathbb{S}$ não é vazio. O conjunto $\mathbb{S}$ possui um menor elemento r. Suponhamos então que $r = a - bq$. Como $r \geq 0$, temos que mostrar que $r <\mid b \mid$. Suponhamos por absurdo que $r \geq |b|$, assim, existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |b| + s$, logo $0 \leq s < r$. Mas isso contradiz o fato de r ser o menor elemento de $\mathbb{S}$, pois $s = a - (q \pm 1)b \in \mathbb{S}$, com $s < r$.

Agora para provar a unicidade, suponha $a = bq + r = bq' + r'$, onde $q, q', r, r' \in \mathbb{Z}$, $0 \leq r < |b|$ e $0 \leq r' < |b|$.

Assim, temos que $-|b| < -r \leq r' - r \leq r' < |b|$. Logo, $|r' - r| < |b|$. Por outro lado, $b(q - q') = r' - r$, o que implica

$$|b| \cdot |q - q'| = |r' - r| < |b|,$$

o que só é possível se $q = q'$ e $r = r'$.

□

Nas condições do teorema acima, q e r são chamados, respectivamente, de *quociente* e de *resto* da divisão de a por b.

Note que o resto da divisão de a por b é zero se, e somente se, b divide a.

A demonstração desse teorema nos fornece um algoritmo para calcular o quociente e resto da divisão de um número por outro, por subtrações sucessivas.

Exemplo 3.30. Vamos achar o resto da divisão de 27 por 6.

$$27 - 6 = 21, \quad 27 - 2 \cdot 6 = 15, \quad 27 - 3 \cdot 6 = 9, \quad 27 - 4 \cdot 6 = 3 < |6|.$$

Isto é $q = 4$ e $r = 3$.

Exemplo 3.31. Vamos determinar o quociente e o resto da divisão de -18 por 4.

$$-18 - (-1) \cdot 4 = -14, \quad -18 - (-2) \cdot 4 = -10, \quad -18 - (-3) \cdot 4 = -6$$
$$-18 - (-4) \cdot 4 = -2, \quad -18 - (-5) \cdot 4 = 2 \leq |4|$$

Isto é $q = -5$ e $r = 1$.Note que o resto tem que ser maior que zero e menor que o módulo do divisor, no exemplo $0 \leq 2 < |4|$.

Denotado por $q_b(a)$ o quociente da divisão do número a por b, definimos a função *quociente* por b como segue:

$$q_b : \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$a \longmapsto q_b(a).$$

Corolário 3.32. *Dados dois números naturais a e b com $b > 0$, existe um número inteiro $n = q_b(a)$, tal que*

$$nb \leq a < (n+1)b.$$

Demonstração. Pela divisão euclidiana, temos que existem $q, r \in \mathbb{Z}$ com $0 \leq r < b$, univocamente determinados, tais que $a = bq + r$. Basta agora tomar $n = q$.

$$r < b \Rightarrow nb + r < nb + b \Rightarrow nb \leq a < nb + b = (n+1)b.$$

□

O corolário acima também nos fornece uma prova da Propriedade Arquimediana, já provada anteriormente.

3.4 Sistemas de Numeração

Utilizamos em nosso dia a dia o sistema de numeração decimal, que recebe esse nome por ser representado por dez símbolos, chamados algarismos que são:

$$0, 1, 2, 3, 4, 5, 6, 7, 8 \text{ e } 9.$$

O sistema decimal é posicional, ou seja cada algarismo representa o valor de sua *ordem* contada da direta para esquerda.

Exemplo 3.33. O número 5362 pode ser expresso no sistema decimal utilizando-se das potências de base 10 da seguinte forma

$$5 \cdot 10^3 + 3 \cdot 10^2 + 6 \cdot 10^1 + 2 \cdot 10^0.$$

Os sistemas de numeração posicionais baseiam-se no teorema a seguir, que é uma aplicação da divisão euclidiana.

Teorema 3.34. *Sejam dados $a, b \in \mathbb{Z}$, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $r_0, r_1, r_2, \ldots r_n \neq 0$ menores do que b, univocamente determinados, tais que*

$$a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n.$$

Demonstração. Indução completa sobre a:

Se $0 < a < b$, basta tomar $n = 0$ e $r_0 = a$. Supondo o resultado válido para todo natural menor do que a, vamos prová-lo para $a \geq b$. Pela divisão euclidiana, existem q e r únicos tais que

$$a = bq + r, \quad com \quad 0 \leq r < b$$

.

Como $0 < q < a$, (basta dividir a equação acima por b), pela hipótese de indução, segue-se que existem números inteiros $n' \geq 0$ e $0 \leq, r_1, r_2, \ldots, r_{n'+1}$ com $r_{n'+1} \neq 0$, univocamente determinados, tais que

$$q = r_1 + r_2 b + r_3 b^2 + \ldots + r_{n'+1} b^{n'},$$

temos então

$$a = bq + r = b(r_1 + r_2 b^1 + \ldots + r_{n'} b^{n'}) + r.$$

Segue do resultado que $r_0 = r$ e $n = n' + 1$.

□

A unicidade segue-se facilmente das unicidades antes estabelecidas.

A representação acima é chamada de *expansão relativa à base b*. Assim podemos representar os números inteiros em diversas bases, por exemplo se $b = 10$, temos a *expansão decimal*. Outra expansão muito utilizada é a *binária*, ou seja, quando $b = 2$, utilizada na linguagem computacional.

A representação dada no teorema acima também fornece um algoritmos para determinar a expansão de um número qualquer relativamente a base b.

Basta aplicar sucessivamente, a divisão euclidiana, como segue:

$$a = bq_0 + r_0, \quad r < b,$$

$$q_0 = bq_1 + r_1, \quad r_1 < b,$$

$$q_1 = bq_2 + r_2, \quad r_2 < b,$$

e assim por diante. Como $a > q_0 > q_1 > q_2 \ldots$ deveremos, em certo ponto, ter $q_{n-1} < b$ e, portanto

$$q_{n-1} = bq_n + r_n,$$

decorre que $q_n = 0$, o que implica $0 = q_n = q_{n+1} = q_{n+2} = \ldots$, e portanto, $0 = r_{n+1} = r_{n+2} = \ldots$.

Temos, então que

$$a = r_0 + r_1 b + r_2 b^2 + \ldots + r_n b^n.$$

A expansão na base b nos fornece um método para representar números naturais. Para tanto, escolha um conjunto S com b símbolos

$$S = \{s_0, s_1, \ldots s_{b-1}\},$$

com $s_0 = 0$, para representar os números de 0 a $b - 1$. Um número a na base b se escreve da forma

$$a = x_n x_{n-1} \ldots x_1 x_0,$$

com $x_0, \ldots, x_n \in \mathbb{S}$ e n variando, dependendo de a, representando o número

$$x_0 + x_1 b + \ldots + x_n b^n.$$

Exemplo 3.35. Dado um número natural $n \in \mathbb{N}$ qualquer, temos duas possibilidades:

i) O resto da divisão de n por 2 é 0, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q$; ou

ii) O resto da divisão de n por 2 é 1, isto é, existe $q \in \mathbb{N}$ tal que $n = 2q + 1$.

O exemplo acima nos diz que todo número natural pode ser escrito de forma única como $2q$, sendo chamado de *número par* ou $2q+1$, sendo chamado de *número ímpar*. O conceito de paridade de um número diz respeito a ele ser *par* ou *ímpar*.

Assim $18 = 2 \cdot 9$ é um número par, já $23 = 2 \cdot 11 + 1$ é um número ímpar.

Exemplo 3.36. Observe agora como podemos escrever um número na base binária utilizando-se de sua expansão.

$$54 = 1.2^5 + 1.2^4 + 0.2^3 + 1.2^2 + 1.2^1 + 0.2^0$$

podemos representá-lo na seguinte forma:

$$54 = (110110)_2$$

A representação na base binária pode ser feita pelo processo de seguidas divisões por 2,

$$54 \div 2 = 27, r = 0$$

$$27 \div 2 = 13, r = 1$$

$$13 \div 2 = 6, r = 1$$

$$6 \div 2 = 3, r = 0$$

$$3 \div 2 = 1, r = 1$$

$$1 \div 2 = 0, r = 1$$

Agora basta escrever a sequência de resto, note que a sequência é da ultima divisão para a primeira.

Dessa forma podemos escolher qualquer número como base para um sistema de numeração, basta para isso, efetuar sucessivas divisões euclidianas. Devemos nos lembrar que o resto é sempre menor que o divisor. Portanto se queremos escrever um número na base n, n-ésimal, os possíveis restos são

$$n-1, n-2, n-3, \ldots, 3, 2, 1, 0.$$

Mais geralmente, fixando um número natural $m \geq 2$, pode-se sempre escrever um número $n \in \mathbb{N}$ qualquer, de modo único, na forma $n = mk + r$, onde $k, r \in \mathbb{N}$ e $r < m$.

Uma outra aplicação que podemos dar a esse resultado é uma forma simples para se encontrar a quantidade de múltiplos de um certo número, dado um intervalo.

Exemplo 3.37. Quantos múltiplos de 8 podemos encontrar entre 1 e 247?

Pelo algoritmo da divisão euclidiana temos que

$$247 = 8.30 + 7$$

ou seja, o maior múltiplo de 8 nesse intervalo é $240 = 8.30$, onde 30 é o quociente da divisão de 247 por 8. Portanto, os múltiplos de 8 entre 1 e 247 são

$$1.8, \quad 2.8, \quad 3.8, \ldots, 30.8,$$

consequentemente, são 30 números.

Generalizando, dados $a, b \in \mathbb{N}$ com $a < b$, o número de múltiplos não nulos de a menores ou iguais a b é igual ao quociente da divisão de b por a.

Vamos agora estabelecer alguns critérios de divisibilidade, para isso, faremos uso da representação de números na expansão decimal.

Proposição 3.38. ***Divisibilidade por 5 e 10***

Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível po 5 (respectivamente por 10) é que r_0 seja 0 ou 5 (respectivamente 0).

Demonstração. Sendo $a = r_n 10^n + r_{n-1} 10^{n-1} + \ldots + r_1 10 + r_0 = 10(r_n 10^{n-1} + \ldots + r_1) + r_0 = 10q + r_0$, temos que $5 \mid 10q$, assim a é divisível por 5 se, e somente se, r_0 é divisível por 5, e, portanto $r_0 = 0$ ou $r_0 = 5$. Por outro lado, a é divisível por 10 se, e somente se r_0 é divisível por 10, logo $r_0 = 0$. □

Proposição 3.39. ***Divisibilidade por 3 e 9***

Seja $a = r_n \dots r_1 r_0$ um número representado no sistema decimal. Uma condição necessária e suficiente para que a seja divisível por 3 (respectivamente por 9) é que $r_n + \ldots + r_1 + r_0$ seja divisível por 3 (respectivamente por 9)

Demonstração. Temos que

$$a - (r_n + \ldots r_1 + r_0) = (r_n 10^n + \ldots + r_1 10 + r_0) - (r_n + \ldots + r_1 + r_0) =$$

$$= r_n(10^n - 1) + \ldots + r_1(10 - 1).$$

Como $9 = 10 - 1$ e $10 - 1 \mid 10^n - 1^n$ (Proposição 3.26), temos que $9 \mid 10^n - 1$ para todo $n \in \mathbb{N}$, assim para algum número q, que

$$a = (r_n + \ldots + r_1 + r_0) + 9q.$$

Como $3 \mid 9 \Rightarrow 3 \mid 9q$, assim para que $3 \mid a$ é necessário que $3 \mid (r_n + \ldots + r_1 + r_0)$. Respectivamente $9 \mid 9 \Rightarrow 9 \mid 9q$, logo para que $9 \mid a$ precisamos ter que $9 \mid (r_0 + \ldots + r_1 + r_0)$. □

3.5 Máximo Divisor Comum

Sejam dados dois inteiros a e b, distintos ou não. Um número inteiro d será dito um *divisor comum* de a e b se $d \mid a$ e $d \mid b$.

Por exemplo, os números ± 1, ± 2 ± 5 e ± 10 são os divisores comuns de 10 e 30.

A definição a seguir é praticamente a mesma dada por Euclides nos *Elementos*, ela nos fornece um dos suportes de sua aritmética.

Diremos que um número inteiro $d \geq 0$ é um *máximo divisor comum* (mdc) de a e b, se possuir as seguintes propriedades:

i) d é um divisor comum de a e b, e

ii) d é divisível por todo divisor comum de a e b.

A condição (ii) pode ser reescrita da seguinte forma:

Se c é um divisor comum de a e b, então $c \mid d$.

Pelo exemplo citado acima um *máximo divisor comum* de 10 e 30 é 10, pois $\pm 1 \mid 10$, $\pm 2 \mid 10$, $\pm 5 \mid 10$ e $\pm 10 \mid 10$.

A condição (ii) acima, implica que, se d e d' são dois máximos divisores comuns de a e b, então $d \mid d'$ e $d' \mid d$, e como $d > 0$ e $d' > 0$, implicam que $d = d'$. Ou seja o mdc de dois números, quando existir, é único e será denotado por (a, b).

Como o mdc de a e b não depende da ordem de a e b, temos que $(a, b) = (b, a)$.

Em alguns casos particulares, é fácil verificar a existência do mdc. Por exemplo, se $a \in \mathbb{Z}$, é certo que $(0, a) = |a|$, $(1, a) = 1$ e que $(a, a) = |a|$.

Mais ainda, para todo $b \in \mathbb{Z}$, temos que

$$a \mid b \Leftrightarrow (a, b) = |a|.$$

Claramente, se $a \mid b$, temos que $|a|$ é um divisor comum de a e b, e se c é um divisor comum de a e b, então $c \mid |a|$, o que implica dizer $|a| = (a, b)$.

Agora, se $(a, b) = |a|$, segue-se que $|a| \mid b$, logo $a \mid b$.

Como todo número inteiro divide 0, o mdc de a e b, onde $a = b = 0$, é 0, pois esse é um divisor comum de 0 e é o único número divisível por todos os divisores de 0. Reciprocamente se $(a, b) = 0$, então $0 \mid a$ e $0 \mid b$, mas o único número divisível por 0 é o próprio 0, logo $a = b = 0$.

Agora vamos provar que o máximo divisor de dois números inteiros sempre existe.

Seja $d > 0$ um mdc de a e b, não nulos, supondo que exista, e seja c um divisor comum qualquer desses números, então $|c|$ divide d e, portanto, $c \leq |c| \leq d$. Isso nos mostra que o mdc de dois números, não ambos nulos, quando existe, é o maior dentre todos os divisores comuns desses números.

Observe que dados $a, b \in \mathbb{Z}$, se existir o (a, b), então

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

Assim para efeito de cálculo do mdc de dois números, podemos sempre supô-los não negativos.

Lema 3.40. *Sejam $a, b, n \in \mathbb{Z}$. Se existe $(a, b - na)$, então (a, b) existe e*

$$(a, b) = (a, b - na)$$

Demonstração. Seja $d = (a, b - na)$. Como $d \mid a$ e $d \mid (b - na)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c é um divisor comum de a e $b - na$ e, portanto, $c \mid d$. Isso prova que $d = (a, b)$. □

O lema acima é útil para calcular o mdc, e será fundamental para demonstrar o Algoritmo de Euclides, que nos permitirá calcular o mdc entre dois números naturais quaisquer.

Exemplo 3.41. Dados $a \in \mathbb{Z}$, com $a \neq 0$ e $m \in \mathbb{N}$, temos que

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

A igualdade acima é facilmente verificada se $m = 1$. Suponhamos que $m \geq 2$. Sendo d o primeiro membro da igualdade acima, temos que

$$d = (a^{m-1} + a^{m-2} + \ldots + a + 1, a - 1) =$$

$$((a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1) + (1 - 1) + m, a - 1).$$

Sabemos que $a - 1 \mid a^{n-1} - 1$ para todo $n \in \mathbb{N}$, temos que

$$a - 1 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \ldots + (a - 1) = s(a - 1),$$

para algum $s \in \mathbb{N}$ e portanto, tem-se que

$$d = (s(a - 1) + m, a - 1) = (a - 1, s(a - 1) + m) = (a - 1, m).$$

Exemplo 3.42. Sejam, $a \in \mathbb{Z}$ e $n \in \mathbb{N}$, vamos determinar $(a + 1, a^{2n} + 1)$

Note inicialmente que

$$a^{2n} + 1 = a^{2n} - 1 + 2.$$

Como $a + 1 \mid a^{2n} - 1$, segue-se que

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

Sendo $(a + 1, 2) = 2$ se a é ímpar, ou $(a + 1, 2) = 1$ se a é par.

Exemplo 3.43. Sejam $a \in \mathbb{Z}$ e $n \in \mathbb{N}$, vamos determinar $(a + 1, a^{2n+1} - 1)$.

Note que

$$a^{2n+1} - 1 = a^{2n+1} + 1 - 2.$$

Como $a + 1 \mid a^{2n+1} + 1$, segue-se que

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

Sendo $(a + 1, 2) = 2$ se a é ímpar, ou $(a + 1, 2) = 1$ se a é par.

3.5.1 Algoritmo de Euclides

Apresentaremos agora a prova construtiva da existência do máximo divisor comum dada por Euclides em seu livro VII, proposição 2. O método, nomeado por Euclides como *Algoritmo de Euclides*, é uma elegância do ponto de vista computacional e pouco se conseguiu melhorá-lo desde sua publicação (300 a.C.).

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b \mid a$, já sabemos que $(a, b) = b$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão euclidiana, podemos escrever

$$a = bq_1 + r_1, \quad \text{com } 0 < r_1 < b.$$

Temos duas possibilidades:

a) $r_1 \mid b$. Em tal caso, $r_1 = (b, r_1)$ e , pelo Lema 3.40, temos que

$$r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b),$$

e o algoritmo termina.

b) $r_1 \nmid b$. Em tal caso,podemos efetuar a divisão de b por r_1, obtemos

$$b = r_1 q_2 + r_2, \quad \text{com } 0 < r_2 < r_1.$$

Novamente temos duas possibilidades:

a') $r_2 \mid r_1$. Nesse caso, $(r_1, r_2) = r_2$ e novamente pelo Lema 3.40

$$r_2 = (r_1, r_2) = (r_1, b - q_2 r_1) = (r_1, b) = (a - q_1 b, b) = (a, b),$$

e o algoritmo termina.

b') $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2, obtemos

$$r_1 = r_2 q_3 + r_3, \quad \text{com} \quad 0 < r_3 < r_2.$$

Continuando nesse processo até que pare, isto sempre ocorre, pois , caso contrário, teríamos uma sequência de números naturais $b > r_1 > r_2 > \ldots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

O algoritmo acima pode ser sistematizado e realizado na prática como mostramos a seguir.

Inicialmente efetue a divisão de a por b e encontre $a = bq_1 + r_1$, agora coloque os valores encontrados no diagrama.

	q_1	
a	b	
r_1		

Continuando, vamos efetuar a divisão de b por r_1, obtendo $b = r_1 q_2 + r_2$ e colocamos novamente os números no diagrama.

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Exemplo 3.44. Vamos calcular o mdc de 8485 e 7325

	1	4	1	3	1	14	1	2
8485	7325	1160	925	235	220	15	10	$5 = (8485, 7325)$
1160	925	235	220	15	10	5	0	

O Algoritmo de Euclides também fornece uma maneira de expressar o máximo divisor comum de dois números naturais como a soma de múltiplos dos números dados.

Quando utilizarmos o Algoritmo de Euclides para expressar (a, b) na forma $ma + nb$, com $m, n \in \mathbb{Z}$, estamos nos referindo ao *Algoritmo de Euclides Estendido*, que será abordado mais adiante nesse capítulo.

3.5.2 Propriedades do mdc

Sejam $a, b \in \mathbb{Z}$. Definimos o conjunto

$$\mathbb{I}(a, b) = \{xa + yb; \quad x, y \in \mathbb{Z}\}.$$

Note que se a e b não são simultaneamente nulos, então $\mathbb{I}(a, b) \cap \mathbb{N} \neq \emptyset$. De fato, teremos que $a^2 + b^2 = a \cdot a + b \cdot b \in \mathbb{I}(a, b) \cap \mathbb{N}$.

A seguir utilizaremos a notação

$$d\mathbb{Z} = \{ld; \ l \in \mathbb{Z}\}.$$

Teorema 3.45. *Sejam, $a, b \in \mathbb{Z}$, não ambos nulos. Se $d = min\, \mathbb{I}(a, b) \cap \mathbb{N}$, então*

i) d é o mdc de a e b; e

ii) $\mathbb{I}(a, b) = d\mathbb{Z}$.

Demonstração. (i) Suponha que $c \mid a$ e $c \mid b$, logo c divide todos os números naturais da forma $ax + by$. Portanto c divide todos os elementos de $\mathbb{I}(a, b)$, e, consequentemente, $c \mid d$.

Agora, vamos provar que d divide todos os elementos de $\mathbb{I}(a, b)$. Seja $z \in \mathbb{I}(a, b)$ e suponha por absurdo, que $d \nmid z$. Logo pela divisão euclidiana

$$z = dq + r, \quad \text{com } 0 < r < d.$$

Como $z = xa + yb$ e $d = ma + nb$, para algum $x, y, m, n \in \mathbb{Z}$, segue-se que

$$z = dq + r \Rightarrow r = z - dq = (xa + yb) - (ma + nb)q =$$

$$= (x - qm)a + (y - qn)b \ \in \mathbb{I}(a, b) \cap \mathbb{N},$$

o que é um absurdo, pois $d = \text{mim}\, \{\mathbb{I}(a, b) \cap \mathbb{N}\}$ e $r < d$. Em particular, $d \mid a$ e $d \mid b$.

Provamos então que $d = (a, b)$.

(ii) Todo elemento de $\mathbb{I}(a, b)$ é divisível por d, temos que $\mathbb{I}(a, b) \subset d\mathbb{Z}$. Por outro lado, para todo $ld \in d\mathbb{Z}$, temos que

$$ld = l(ma + nb) = (lm)a + (ln)b \ \in \mathbb{I}(a, b),$$

e, portanto, $d\mathbb{Z} \subset \mathbb{I}(a, b)$. Assim se $\mathbb{I}(a, b) \subset d\mathbb{Z}$ e $d\mathbb{Z} \subset \mathbb{I}(a, b)$, então $\mathbb{I}(a, b) = d\mathbb{Z}$.

□

O teorema acima nos dá outra demonstração da existência do máximo divisor comum de dois números inteiros, porém, ela não nos fornece um método prático para determiná-lo.

Portanto podemos escrever $(a, b) = ma + nb$, com $a, b, m, n \in \mathbb{Z}$.

Corolário 3.46. *Quaisquer que sejam $a, b \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se*

$$(na, nb) = n(a, b).$$

Demonstração. Inicialmente temos que

$$\mathbb{I}(na, nb) = n\mathbb{I}(a, b), \quad \text{com } \{nz;\ z \in \mathbb{I}(a, b)\}.$$

Agora, o resultado segue-se do teorema anterior,

$$\text{mim } \{n\mathbb{I}(a, b) \cap \mathbb{N}\} = n \text{ mim } \{\mathbb{I}(a, b) \cap \mathbb{N}\}.$$

□

Corolário 3.47. *Dados $a, b \in \mathbb{Z}$, não ambos nulos, tem-se que*

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

Demonstração. Pelo corolário anterior, temos que

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

O que prova o resultado. □

Dois números a e b serão ditos *primos entre si*, ou *coprimos*, se $(a, b) = 1$; ou seja , se o único divisor positivo comum de a e b é 1.

Proposição 3.48. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros m e n tais que $ma + nb = 1$.*

Demonstração. Suponha que a e b são primos entre si. Logo, $(a, b) = 1$. Como $(a, b) = ma + nb$, para $m, n \in \mathbb{Z}$, temos $ma + nb = 1$. Reciprocamente, suponha que existam números inteiros m e n tais que $ma + nb = 1$. Se $d = (a, b)$, temos que $d \mid (ma + nb)$, o que nos mostra que $d \mid 1$, logo $d = 1$.

□

Essa proposição estabelece uma relação de extrema importância, entre as estruturas aditivas e multiplicativas dos números naturais, os que nos permitirá provar vários resultados

Teorema 3.49. ***Lema de Gauss***

Sejam, $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.

Demonstração. Se $a \mid bc$, então existe $f \in \mathbb{Z}$, tal que $bc = af$. Se $(a, b) = 1$, então temos que existem $m, n \in \mathbb{Z}$, tais que

$$ma + nb = (a, b) = 1 \Rightarrow c(ma) + c(nb) = m(ac) + n(bc) = c.$$

Substituindo bc por af na igualdade acima, obtemos

$$c = m(ac) + n(af) = a(mc + nf),$$

e, portanto $a \mid c$.

□

Corolário 3.50. *Dados $a, b, c \in \mathbb{Z}$, com b e c não ambos nulos, temos que*

$$b \mid a \quad e \quad c \mid a \Leftrightarrow \frac{bc}{(b,c)} \mid a.$$

Demonstração. Suponha que $a \mid b$ e $a \mid c$, assim $a = nb = mc$, para algum $n, m \in \mathbb{Z}$. Logo,

$$n\frac{b}{(b,c)} = m\frac{c}{(b,c)}.$$

Como $\left(\frac{b}{(b,c)}, \frac{c}{(b,c)}\right) = 1$, segue-se que $\frac{b}{(b,c)} \mid m \Rightarrow \frac{b}{(b,c)}c \mid mc$. Como $mc = a$, está provada a implicação. Para a recíproca suponha $\frac{bc}{(b,c)} \mid a$, assim existe um $f \in \mathbb{Z}$ tal que $af = \frac{bc}{(b,c)} = c\frac{b}{(b,c)} = b\frac{c}{(b,c)}$, logo $a \mid \frac{b}{(b,c)} \Rightarrow a \mid b$ e $a \mid \frac{c}{(c,b)} \Rightarrow a \mid c$.

□

A noção de máximo divisor comum pode ser generalizada com a seguir.

Um número natural d será dito o máximo divisor comum (mdc) de dados números inteiros $a_1, a_2, \ldots, a_n$, não todos nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de $a_1, a_2, \ldots, a_n$.

ii) Se c é um divisor comum de $a_1, a_2, \ldots, a_n$, então $c \mid d$.

O mdc, quando existe, é certamente único e será representado por

$$d = (a_1, a_2, \ldots, a_n).$$

A proposição a seguir nos fornece um método indutivo para o cálculo do mdc de n inteiros, reduzindo-o á aplicação do Algoritmo de Euclides a $n-1$ pares de inteiros.

Proposição 3.51. *Dados números inteiros $a_1, a_2, \ldots, a_n$, não todos nulos, existe seu mdc e*

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

Demonstração. Faremos por indução sobre $n \geq 2$. Para $n = 2$, já provamos anteriormente. Suponha que a afirmação é válida para n, vamos provar que também é válido para $n+1$. Seja d o máximo divisor comum de $a_1, a_2, \ldots, (a_n, a_{n+1})$, ou seja $d = (a_1, a_2, \ldots, a_n, a_{n+1})$, pois isso provará também sua existência.

Temos então que $d \mid a_1$ $d \mid a_2, ...,$ $d \mid a_{n-1}$ e $d \mid (a_n, a_{n+1})$. Portanto $d \mid a_1, \ldots, a_{n-1},$ $d \mid a_n$ e $d \mid a_{n+1}$.

Por outro lado, seja c um divisor comum de $a_1, \ldots, a_n,$ a_{n+1}; logo c é um divisor comum de $a_1, \ldots a_{n-1}$ e de $(a_n,\ a_{n+1}) = d$, assim $c \mid d$.

□

Os inteiros $a_1, a_2, \ldots a_n$ serão ditos *primos entre si*, ou *coprimos*, quando

$$(a_1, a_2, \ldots, a_n) = 1.$$

Dados um subconjunto finito $A = \{a_1, a_2, \ldots, a_n\}$ de $\mathbb{Z}$, como máximo divisor comum dos inteiros $a_1, a_2, \ldots, a_n$ independente da ordem que eles são tomados, podemos definir o mdc de A como sendo

$$\text{mdc } A = (a_1, a_2, \ldots, a_n).$$

No caso em que $A = \{a_1, a_2, \ldots\}$ é um subconjunto infinito de $\mathbb{Z}$, ainda existe $d = \text{mdc } A$, ou seja, existe um número natural d, que divide todos os elementos de A e tal que, dados um divisor comum d' dos elementos de A, tem-se que $d' \mid d$.

3.5.3 Mínimo Múltiplo Comum

Diremos que um número inteiro é um *múltiplo comum* de dois inteiros dados, se ele é simultaneamente múltiplo de ambos os números.

Sejam $a, b \in \mathbb{Z}$ quaisquer, temos que ab e 0 são sempre múltiplos de a e b.

Diremos que um número inteiro $m \geq 0$ é um *mínimo múltiplo comum* (mmc) dos números inteiros a e b, se possuir as seguintes propriedades.

i) m é um múltiplo comum de a e de b, e

ii) Se c é um múltiplo comum de a e b, então $m \mid c$.

Por exemplo, 40 é um múltiplo de 4 e 5, mas não é um mmc desses números, e sim 20, pois $20 \mid 40$.

Se m e m' são dois mínimos múltiplos comuns de a e b, então por (ii), temos que $m \mid m'$ e $m' \mid m$ logo $m = m'$. Assim quando existir o mínimo múltiplo comum de dois números inteiros ele será único.

Agora se m é o mmc de a e b, e seja c um múltiplo comum de a e b, então $m \mid c$. Portanto, se c é positivo, temos que $m \leq c$, o que nos mostra que m é o menor dos múltiplos comuns positivos de a e b.

O mínimo múltiplo comum de a e b, se existe, é denotado por $[a, b]$.

Note que, caso exista, é fácil mostrar que

$$[-a, b] = [a, -b] = [-a, -b] = [a, b].$$

Assim para efeito do cálculo do mmc de dois números, podemos sempre supô-los não negativos.

Note também que se $[a, b] = 0$ temos $a = 0$ ou $b = 0$, pois se $[a, b] = 0$, então $0 \mid ab$, que é múltiplo de a e de b, ou seja $ab = 0$ e portanto $a = 0$ ou $b = 0$. Reciprocamente, se $a = 0$ ou $b = 0$, então 0 é o único múltiplo comum de a e b, logo $[a, b] = 0$.

Proposição 3.52. *Dados dois números inteiros a e b, temos que $[a, b]$ existe e*

$$[a, b] \cdot (a, b) = |ab|.$$

Demonstração. Se $a = 0$ ou $b = 0$, a igualdade a cima é trivialmente satisfeita. É também fácil verificar que a igualdade é verificada para a e b se, e somente se, ela é verificada para $\pm a$ e $\pm b$. Então, sem perda de generalidade, podemos supor $a, b \in \mathbb{N}$. Consideremos $m = \frac{ab}{(a,b)}$. Como

$$m = a\frac{b}{(a, b)} = b\frac{a}{(a, b)},$$

temos que $a \mid m$ e $b \mid m$. Portanto $m = [a, b]$.

Seja c um múltiplo comum de a e b, logo, $c = na = n'b$, com $n, n' \in \mathbb{Z}$. Assim

$$n\frac{a}{(a, b)} = n'\frac{b}{(a, b)}.$$

Como $\frac{a}{(a,b)}$ e $\frac{b}{(a,b)}$ são primos entre si, logo $\frac{a}{(a,b)} \mid n'$ e, portanto $m = \frac{a}{(a,b)}b$ divide $n'b = c$. □

Pela proposição acima, o mínimo múltiplo comum de dois inteiros, não ambos nulos, pode ser encontrado por meio do Algoritmo de Euclides para o cálculo do mdc, pois $[a,b] = \frac{|ab|}{(a,b)}$.

Corolário 3.53. *Se a e b são números inteiros primos entre si, então $[a,b] = |ab|$.*

Demonstração. Se a e b são primos entre si, temos que $(a,b) = 1$, assim pela proposição acima fica provado o corolário.

□

Como no mdc, podemos estender o conceito de mmc para vários números inteiros. Diremos que um número natural m é um mínimo múltiplo comum dos inteiros não nulos $a_1, a_2, \ldots, a_n$, se m é um múltiplo comum de $a_1, a_2, \ldots, a_n$ e, se para todo múltiplo comum m' desses números, tem-se que $m \mid m'$. É fácil notar que o mmc, se existe, é único, sendo denotado por $m = [a_1, a_2, \ldots, a_n]$. Além disso, o mmc de vários inteiros não nulos é o menor múltiplo comum positivo desses inteiros.

Proposição 3.54. *Sejam $a_1, a_2, \ldots, a_n$ números inteiros não nulos. Então existe o número $[a_1, a_2, \ldots, a_n]$ e*

$$[a_1, a_2, \ldots, a_n] = [a_1, \ldots, [a_{n-1}, a_n]].$$

Demonstração. Basta provar que, se existe $[a_1, \ldots, [a_{n-1}, a_n]]$, vale a igualdade acima. A existência do mmc, segue facilmente disso, por indução.

Seja $m = [a_1, \ldots, [a_{n-1}, a_n]]$. Logo, $a_1, \ldots, a_{n-2}$ e $[a_{n-1}, a_n]$ dividem m. Como $a_{n-1} \mid [a_{n-1}, a_n]$ e $a_n \mid [a_{n-1}, a_n]$, segue que m é um múltiplo comum de $a_1, \ldots, a_n$.

Por outro lado, suponha que m' seja múltiplo comum de $a_1, \ldots, a_n$. Logo, $a_1 \mid m', \ldots, a_{n-2} \mid m'$ e $[a_{n-1}, an] \mid m'$, daí segue que m' é múltiplo de $m = [a_1, \ldots, [a_{n-1}, a_n]]$.

□

Exemplo 3.55. Determinar o mmc dos números -32, 16, 72.

$$[-32, 16, 72] = [32, [16, 72] = [32, 144] = 288.$$

3.6 Equações Diofantinas Lineares

Diofanto de Alexandria, quase nada se sabe sobre sua vida, ficou conhecido por um suposto problema escrito em sua lápide. Era um matemático de talento, ganhou importância no cenário matemático por sua Aritmética. Os aspectos algébricos da obra de Diofanto são fundamentados no pioneirismo em que as soluções são encontradas para problemas particulares, que vão se acumulando e tornando-se regras de manipulação de equações diversas. Um dos seus principais estudos são as chamadas "Equações Diofantinas Lineares".

Nesta seção, utilizaremos as propriedades do mdc para resolver equações diofantinas lineares.

Para solucionar vários problemas de aritmética precisamos resolver equações do tipo

$$aX + bY = c,$$

com $a, b, c \in \mathbb{Z}$.

Tais equações são chamadas *Equações Diofantinas Lineares* em homenagem a Diofanto de Alexandria (aproximadamente 300d.C.).

Nem sempre será possível obter uma solução da equação no conjunto dos inteiros.

Note que a equação

$$2X + 8Y = 17,$$

não possui solução x_0 e y_0 no conjunto dos números inteiros, pois, teríamos $2x_0 + 8y_0 = 2(x_0 + 4y_0)$, que será um número par, mas 17 é um número ímpar (17=2.8+1).

Haveria uma forma de saber se existem soluções e como determiná-las? A resposta para essa pergunta é sim, e será mostrada a seguir.

Proposição 3.56. *Sejam $a, b, c \in \mathbb{Z}$. A equação $aX + bY = c$ admite solução em números inteiros se, e somente se, $(a, b) \mid c$.*

Demonstração. Pela definição temos que

$$I(a, b) = \{ma + nb; \quad m, n \in \mathbb{Z}\}$$

e seja d o máximo divisor comum de a e b, logo

$$I(a, b) = d\mathbb{Z} = (a, b)\ \mathbb{Z}$$

É claro que a equação $aX + bY = c$ possui solução se, e somente se, $c \in I(a, b)$, que é equivalente a $c \in (a, b)\mathbb{Z}$, que por sua vez, é equivalente a $(a, b) \mid c$.

Note que a equação $aX + bY = c$, com a e b não ambos nulos, e $(a, b) \mid c$ é equivalente a equação

$$a_1X + b_1Y = c_1,$$

onde

$$a_1 = \frac{a}{(a, b)}, \quad b_1 = \frac{b}{(a, b)} \quad \text{e} \quad c_1 = \frac{c}{(a, b)}.$$

Como já provado anteriormente $(a_1, b_1) = 1$ e, portanto, podemos nos limitar as equações do tipo

$$aX + bY = c, \quad \text{com } (a, b) = 1,$$

que sempre possuirá solução nos inteiros.

□

A seguir, mostraremos como encontrar soluções (se existirem) particulares x_0 e y_0 das equações nos inteiros.

Proposição 3.57. *Seja x_0 e y_0 uma solução da equação $aX + bY = c$, onde $(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são*

$$x = x_0 + tb, \quad y = y_0 - ta;\ t \in \mathbb{Z}.$$

Demonstração. Seja x, y uma solução da equação $aX + bY = c$, logo

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

que podemos reescrever da seguinte forma

$$a(x - x_0) = b(y_0 - y).$$

Como

$$(a, b) = 1 \Rightarrow b \mid x - x_0 \text{ e } a \mid y - y_0,$$

assim

$$x - x_0 = tb \Rightarrow x = x_0 + tb, \in \mathbb{Z}.$$

Agora, note que

$$a(x - x_0) = a(tb) = b.(ta) = b(y_0 - y) \Rightarrow y_0 - y = ta \Rightarrow y = y_0 - ta.$$

Por outro lado, como x, y é solução, pois

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + b_0 = c.$$

□

Da propriedade acima temos que, quando existem soluções, elas são em quantidade infinita nos inteiros.

Podemos ter também como solução da equação $aX + bY = c$, os valores $x = x_0 - tb$ e $y = y_0 + at$, bastando substituir t por $-t$ com $t \in \mathbb{Z}$.

Vamos agora, expor um método para encontrar uma solução particular de uma equação do tipo $aX + bY = c$, quando $(a, b) = 1$.

Se $|a|$, $|b|$ e $|c|$ são pequenos, muitas vezes é fácil encontrar uma solução particular para a equação, basta faze-la por inspeção. Mas geralmente, o método que vamos expor a seguir, sempre nos permitirá encontrar uma solução particular para a equação.

Usando o algoritmo de Euclides estendido, é possível determinar $m, n \in \mathbb{Z}$ tais que

$$ma + nb = (a, b) = 1,$$

multiplicando ambos os membros da igualdade acima por c, obtemos

$$cma + cnb = c.$$

Assim $x_0 = cm$ e $y_0 = cn$ é uma solução particular da equação $aX + bY = c$.

Exemplo 3.58. Vamos resolver a equação $90X + 28Y = 22$ nos inteiros.

Primeiramente vamos calcular o mmc dos números 90 e 28, afim de determinar se a equação possui solução nos inteiros.

$$(90, 28) = (90 - 3 \cdot 28, 28) = (6, 28) = (6, 28 - 4 \cdot 6) =$$

$$= (6, 4) = (6 - 1 \cdot 4, 4) = (2, 4) = (4 - 2 \cdot 2, 2) = (0, 2) = 2.$$

Logo a equação $90X + 28Y = 22$ tem solução pois $(90, 28) = 2$ e $2 \mid 22$. Como $2 \mid 90$, $2 \mid 28$ e $2 \mid 22$ podemos utilizar a equação equivalente, $45X + 14Y = 11$ em nossos cálculos.

Vamos em seguida encontrar uma solução particular x_0, y_0, utilizando o algoritmo de Euclides temos,

$$45 = 14 \cdot 3 + 3$$

$$14 = 3 \cdot 4 + 2$$

$$3 = 2 \cdot 1 + 1.$$

Pelas igualdades obtemos

$$1 = 3 - 1 \cdot 2 = 3 - 1 \cdot (14 - 3 \cdot 4) = 5 \cdot 3 - 1 \cdot 14 =$$

$$= 5 \cdot (45 - 3 \cdot 14) - 1 \cdot 14 = 5 \cdot 45 - 16 \cdot 14.$$

Temos então que $45 \cdot (5) + 14 \cdot (-16) = 1$, agora multiplicando ambos os membros da equação por 11,

$$45.(5.11) + 14.(5.(-16)) = 11.1 \Rightarrow 45 \cdot (55) + 14 \cdot (-176) = 11,$$

determinamos assim uma solução particular $x_0 = 55$ e $y_0 = -176$, consequentemente as soluções da equação $45X + 14Y = 11$ serão

$$x = 55 + 14t \quad \text{e} \quad y = -176 - 45t, \quad \text{com } t \in \mathbb{Z}.$$

Em algumas situações é necessário resolver em $\mathbb{N} \cup \{0\}$ equações diofantinas da forma $aX + bY = c$, onde $a, b, c \in \mathbb{N}$. Para isso precisaremos do seguinte resultado.

Proposição 3.59. *Sejam, $a, b \in \mathbb{N}$, com $(a, b) = 1$. Todo número inteiro c pode ser escrito, de modo único, da seguinte forma:*

$$c = ma + nb, \quad \textit{com} \quad 0 \leq m < b \quad \textit{e} \quad n \in \mathbb{Z}.$$

Demonstração. Primeiramente vamos provar a existência.

Sabemos que existem $u, v \in \mathbb{Z}$ tais que

$$ua + vb = (a, b) = 1.$$

Multiplicando a equação por c, temos que

$$auc + bvc = c.$$

Como $auc + bvc = c = ma + na \Rightarrow uc = m + b\frac{(n-vc)}{a}$, assim pela divisão euclidiana, temos que existem $q, m \in \mathbb{Z}$ com $0 \leq m < b$ e $q = \frac{n-vc}{a}$ tais que $uc = qb + m$.

Substituindo esse valor na equação $avc + bvc = c$, obtemos $a(qb + m) = bvc = c \Rightarrow am + b(aq + vc) = c \Rightarrow am + bn = c$, com $0 \leq m < b$ e $aq + vc = n \in \mathbb{Z}$.

Para provar a unicidade, suponha que $ma + nb = m'a + n'b$, com $0 \leq m, m' < b$. Logo, $a(m - m') = (n' - n)b$, com $\mid m - m' \mid < b$. Como $(a, b) = 1$, devemos ter $b \mid m - m'$, o que só é possível se $m = m'$ e em tal caso $n = n'$.

□

Sejam $a, b \in \mathbb{N}$. Definimos o conjunto

$$\mathbb{S}(a, b) = \{xa + yb; \in \mathbb{N} \cup \{0\}\},$$

chamado de *semigrupo* gerado por a e b.

É claro que $aX + bY = c$, com $(a, b) = 1$, tem solução em $\mathbb{N} \cup \{0\}$ se, e somente se $c \in \mathbb{S}(a, b)$. Portanto é de fundamental importância caracterizar os elemnros de $\mathbb{S}(a, b)$.

Proposição 3.60. *Tem-se que $c \in \mathbb{S}(a, b)$ se, e somente se, existem $m, n \in \mathbb{N} \cup \{0\}$, com $m < b$ (univocamente determinados por c) tais que $c = ma + nb$.*

Demonstração. Se $c = ma + nb$, com $m, n \in \mathbb{N} \cup \{0\}$, é claro que $c \in \mathbb{S}(a, b)$. Agora se $c \in \mathbb{S}(a, b)$, então $c = xa + yb$, com $x, y \in \mathbb{N} \cup \{0\}$. Pela divisão euclidiana, $x = bq + m$, com $0 \leq m < b$; Substituindo esse valor na igualdade temos

$$c = xa + yb = a(bq + m) + yb = am + b(aq + y) = ma + nb,$$

onde $m < b$, e $n = aq + y \in \mathbb{N} \cup \{0\}$.

A unicidade vem da Proposição 3.59.

□

Definimos agora o *conjunto das lacunas* se $\mathbb{S}(a,b)$ como sendo o conjunto

$$\mathbb{L}(a,b) = \mathbb{N} \setminus \mathbb{S}(a,b).$$

Corolário 3.61. *Temos que*

$$\mathbb{L}(a,b) = \{ma - nb \in \mathbb{N}; \quad m,n \in \mathbb{N},\ m < b\}.$$

Demonstração. Decorre imediatamente das Proposições 3.59 e 3.60.

□

Teorema 3.62. *A equação $aX + bY = c$, onde $(a,b) = 1$, tem solução em números naturais se, e somente se,*

$$c \notin \mathbb{L}(a,b) = \{ma - nb \in \mathbb{N}; \quad m,n \in \mathbb{N},\ m < b\}.$$

Demonstração. Como a equação $aX + bY = c$ tem solução se, e somente se, $c \in \mathbb{S}(a,b)$, o resultado segue do Corolário 3.61.

□

Corolário 3.63. *Sejam $a,b \in \mathbb{N}$ tais que $(a,b) = 1$. Tem-se que $(a-1)(b-1)$ é o maior inteiro tal que $c \in \mathbb{S}(a,b)$ para todo $c \geq (a-1)(b-1)$.*

Demonstração. Temos que o conjunto $\mathbb{L}(a,b)$ é finito e seu maior elemento é

$$\max\{\mathbb{L}(a,b)\} = \max\{ma - nb\} = \max\{(m/n)a - b = (b-1)a - b\}.$$

Pois $0 \leq m < b$, portanto, se

$$c \geq (b-1)a - b + 1 = ab - a - b + 1 = (b-1)(a-1),$$

a equação $aX + bY = c$ admite solução nos naturais. Se $c = (b-1)(a-1) - 1$, ela não admite solução.

□

O número natural $\kappa = (a-1)(b-1)$ é chamado *condutor* de $\mathbb{S}(a,b)$.

Portanto, o número $\kappa - 1 = (a-1)(b-1) - 1 = (b-1)a - b$ é a maior lacuna de $\mathbb{S}(a,b)$.

Note que não é difícil determinar se a equação $aX + bY = c$ admite solução, pois se $(a,b) \nmid c$, a equação não tem soluções inteiras. E se $(a,b) \mid c$, a equação é equivalente a uma outra com $(a,b) = 1$. Com o algoritmo euclidiano estendido, basta escrever

$$1 = (a,b) = m'a - n'b.$$

Logo,

$$c = cm'a - cn'b.$$

Agora com a divisão euclidiana, escrevemos $cm' = qb + m$, com $m < b$, logo,

$$c = \begin{cases} ma + (qa - cn')b \in \mathbb{S}(a,b), & \text{se } qa \geq cn' \\ ma - (cn' - qa)b \in \mathbb{L}(a,b), & \text{se } cn' > qa \end{cases}$$

A equação tem solução no primeiro caso, mas não no segundo.

A única solução m,n da equação $aX + bY = c$, com $m < b$, é uma *solução minimal*, no sentido de que se x,y é uma solução, então $x \geq m$.

Com essa definição vamos enunciar o resultado a seguir.

Proposição 3.64. *Suponha que a equação $aX + bY = c$, com $(a, b) = 1$, tenha solução e seja $x_0 = m$, $y_0 = n$ a solução minimal. As soluções x, y da equação são dadas pelas fórmulas*

$$x = m + tb, \quad e \quad y = n - ta, \quad t \in \mathbb{N} \cup \{0\}, \quad n - ta \geq 0.$$

Demonstração. Note que esse tipo de equação tem, no máximo, um número finito de soluções, correspondentes aos seguintes valores de t:

$$0, 1, 2, \ldots, [\frac{n}{a}],$$

onde $[\frac{n}{a}]$ representa o quociente da divisão euclidiana de n por a, ou seja a parte inteira de $\frac{n}{a}$.

□

Exemplo 3.65. Vamos determinar para quais valores de $c \in \mathbb{N}$ a equação $14X + 5Y = c$ tem solução em $\mathbb{N} \cup \{0\}$.

Primeiramente note que $(14, 5) = 1$ e $1 \mid c$, assim a equação possui solução. Vamos determinar o conjunto das lacunas

$$\mathbb{L}(14, 5) = \{14m - 5n \in \mathbb{N}, \quad m, n \in \mathbb{N}, \ m < 5\}.$$

Fixando o valor de m e fazendo n variar até que seja possível temos:
Para $m = 1 \Rightarrow 14 - 5n > 0 \Rightarrow n = \{1, 2\}$, ou seja $c \neq \{9, 4\}$.
Para $m = 2 \Rightarrow 28 - 5n > 0 \Rightarrow n = \{1, 2, 3, 4, 5\}$, ou seja $c \neq \{23, 18, 13, 8, 3\}$.
Para $m = 3 \Rightarrow\Rightarrow 42 - 5n > 0 \Rightarrow n = \{1, 2, 3, 4, 5, 6, 7, 8\}$, ou seja,
$c \neq \{37, 32, 27, 22, 17, 12, 7, 2\}$.
Finalmente para $m = 4 \Rightarrow 56 - 5n > 0 \Rightarrow n = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$, ou seja,
$c \neq \{51, 46, 41, 36, 31, 26, 21, 16, 11, 6, 1\}$.
Portanto, a equação $14X + 5Y = c$ admite solução em $\mathbb{N} \cup \{0\}$ se, e somente se $c \neq \mathbb{L}(a, b)$.
$c \neq \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 16, 17, 18, 21, 22, 23, 26, 27, 31, 32, 36, 37, 41, 46, 51\}$.

Exemplo 3.66. Resolva a equação $14X + 5Y = 30$ em $\mathbb{N} \cup \{0\}$.

Note que pelo cálculo feito no exemplo acima $30 \notin \mathbb{L}(14, 5)$, assim a equação possui soluções (minimal). Para determiná-las utilizaremos o algoritmo de Euclides,

$$14 = 2 \cdot 5 + 4 \quad \text{e} \quad 5 = 1 \cdot 4 + 1$$

Substituindo os valores encontramos:

$$1 = 5 - 1 \cdot 4 = 5 - 1 \cdot (14 - 2 \cdot 5) = 5 - 1 \cdot 14 + 2 \cdot 5 = (-1) \cdot 14 + 3 \cdot 5.$$

Multiplicando o último resultado por 30 obtemos:

$$30 = (-30) \cdot 14 + 90 \cdot 5$$

Note que pela condição $0 \leq m < b$, assim precisamos reescrever a equação:

$$30 = (-30).14 + (14.6 + 6).5 \Rightarrow (-30).14 + (30.14) + (6).5 \Rightarrow 0.14 + 6.5.$$

Assim temos que

$$\begin{cases} x = 0 + 5t, \\ y = 6 - 14t \end{cases}$$

Que só faz sentido para $t = 0$, pois $6 - 14t \geq 0 \Rightarrow t \leq [\frac{6}{14}] \Rightarrow t \leq 0$.
Portanto a solução minimal da equação $14X + 5Y = 30$ é $x_0 = 0$ e $y_0 = 6$.

Exemplo 3.67. Para quais valores de $c \in \mathbb{N}$, a equação $10X + 14Y = c$ não possui solução em $\mathbb{N} \cup \{0\}$?

Primeiramente observe que $(10, 14) = 2$, assim podemos escrever uma equação equivalente e essa

$$5X + 7Y = \frac{c}{2} \quad \text{com} \quad (5, 7) = 1 \quad \text{e} \quad 1 \mid \frac{c}{2}.$$

Assim, o conjunto das lacunas de $\mathbb{L}(5, 7)$ é:

$$\mathbb{L}(5, 7) = \{7m - 5n \in \mathbb{N}, \quad m, n \in \mathbb{N},\ m < 5\} =$$

$$= \{1, 2, , 3, 4, 6, 8, 9, 11, 13, 16, 18, 23\}.$$

Portanto a equação $10X + 14Y = c$ não possuirá solução em $\mathbb{N} \cup \{0\}$ se $\frac{c}{2} \in \mathbb{L}(5, 7)$, ou seja $c = \{2, 4, 6, 8, 12, 16, 18, 22, 26, 32, 36, 46\}$.

Se quisermos resolver a equação acima para $c = 38$ por exemplo, temos

$$10X + 14Y = 38 \Rightarrow 5X + 7Y = 19.$$

Por inspeção é fácil notar que $5 \cdot 1 + 7 \cdot 2 = 19$, assim uma solução é $x_0 = 1, y_0 = 2$, podemos então obter as soluções

$$\begin{cases} x = 1 + 7t, \\ y = 2 - 5t \end{cases}$$

Como $t \in \mathbb{N} \cup \{0\}$ e $2 - 5t > 0 \Rightarrow t = 0$. Assim a solução minimal é $x = 1$ e $y = 2$.

Para resolver equações do tipo $aX + bY = c$, com $(a, b) \mid c$, não é necessário, usar toda a técnica desenvolvida, pois sendo b suficientemente pequeno, é viável determinar soluções por inspeção, como fizemos no exemplo anterior.

3.7 Números Primos

Os números primos teriam surgido na Grécia Antiga, com sua definição e representação. Estudos relatam que a Escola Pitagórica (530 a.C.) analisava a *mística numérica* e já estudavam e conheciam os números primos, que ainda não possuíam essa nomenclatura. Eles se referiam aos números primos como números lineares, e aos compostos como não lineares, pois poderiam ser representados por retângulos, ou seja, produto dos lineares.

Por volta de 300 a.C., Euclides trouxe uma referência aos números primos em seu livro *Os Elementos*, no que diz respeito ao cálculo do máximo divisor comum (mdc), e sobre a infinidade de números primos. No livro VII ele escreveu "Número primo é todo aquele que só pode ser medido através da unidade", e no livro IX, "Números primos são mais do que qualquer quantidade fixada de números primos".

Após Euclides, o primeiro a formular uma regra de determinação de números primos foi Eratóstenes de Cirene. Seu algoritmo consistia em eliminar os números compostos, e assim sobrariam apenas os números primos. Esse algoritmo ficou conhecido como *Crivo de Eratóstenes*.

Por volta do ano 500, os números primos ganharam o mundo, Boethius, em seu livro *De Institutione Arithmetica*, foi o primeiro a usar a denominação de *números primus*. Somente em 1200, os árabes, complementados por estudos hebraicos, hindus e egípcios passam a estudar os números primos. Nessa época surge a principal obra de Fibonacci, *Liber Abacci*.

Em 1621 Bachelet traduziu a obra *Aritmética* de Diofanto, e fazendo uso dela, Fermat desenvolveu sua análise sobre os números primos.

Os números primos eram estudados até a Idade Moderna apenas com fins teóricos. Hoje eles são estudados principalmente por questões computacionais, como na criptografia. Em 2001, Manindra Agrawal desenvolveu um algoritmo computacional que facilitou a procura por esses números tão preciosos.

Abordaremos nessa sessão o estudo sobre números primos, um dos mais importantes conceitos da Matemática, eles desempenham papel fundamental e estão associados a muitos problemas famosos, cujas soluções ainda não foram obtidas até os dias de hoje.

As informações acima foram retiradas da Revista de História da Matemática para professores. [27]

3.7.1 Teorema Fundamental da Aritmética

Definição 3.68. Um número natural maior que 1 que só possui como divisores positivos 1 e ele próprio, é chamado *número primo*.

Dados dois números primos p e q e um número inteiro a qualquer, decorrem da definição acima os seguintes fatos:

i) Se $p \mid q$, então $p = q$.

De fato, como $p \mid q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p também um número primo, tem-se que $p > 1$, logo $p = q$.

ii) Se $p \nmid a$, então $(p, a) = 1$.

De fato, se $(p, a) = d$, temos que $d \mid p$ e $d \mid a$. Como p é primo, temos $d = p$ ou $d = 1$. Mas como $d \neq p$, pois $p \nmid a$ e, consequentemente , $d = 1$.

Um número maior do que 1 e que não é primo será dito *composto*.

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $1 < n_1 < n$. Logo existirá um número natural n_2 tal que

$$n = n_1 n_2, \quad \text{com} \quad 1 < n_1 < n \quad \text{e} \quad 1 < n_2 < n.$$

Por exemplo $2, 3, 5, 7, 11, 13, 17, 19, 23$ são os primeiros números primos, enquanto $4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 22$ são os primeiros números compostos.

Analisando a estrutura multiplicativa dos números naturais, os números primos são os mais simples, e ao mesmo tempo são suficientes para gerar todos os números naturais, logo, todos os números inteiros não nulos, conforme será visto mais adiante nessa seção, quando falaremos sobre o *Teorema Fundamental da Aritmética*.

A seguir, estabeleceremos um resultado fundamental atribuído a Euclides (*Os Elementos*, Proposição 30, Livro VII), chamado *Lema de Euclides*.

Proposição 3.69 (Lema de Euclides)**.** *Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Basta provar que, se $p \nmid a$, então $p \mid b$.

Se $p \mid a$, então $p = a$ ou $p = 1$, pois p é primo. Agora se $p \mid b$ e como $p \neq a$, pois $(a, p) = 1$ temos que $p = 1$ ou $p = b$, logo $p \nmid a$, contradição. Do Lema de Gauss (3.49) temos que se $p \mid ab$ e $(a, p) = 1$, então $p \mid b$.

□

A proposição descrita acima caracteriza completamente os números primos, fato que pode ser observado com o seguinte problema.

Exemplo 3.70. Dados dois números naturais d e m, vamos resolver em X, Y nos naturais, o sistema de equações

$$(X, Y) = d, \quad [X, Y] = m.$$

Ainda precisamos de mais informações para resolvê-lo, portanto deixaremos pra mais adiante.

Corolário 3.71. *Se $p, p_1, p_2, \ldots, p_n$ são números primos e, $p \mid p_1 p_2 \ldots p_n$, então $p = p_i$, para algum $i = 1, 2, \ldots, n$.*

Demonstração. A demostração pode ser feita sem dificuldades por indução sobre n, basta utilizar a Proposição 3.69 (Lema de Euclides).

□

Teorema 3.72 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.*

Demonstração. Utilizaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado, pois 2 é primo.

Suponhamos o resultado válido para todo número natural menor do que n e vamos provar que vale para n. Se o número n é primo, nada temos a demonstrar. Suponhamos então, que n seja composto. Logo, existem números naturais n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1, p_2, \ldots, p_r$ e $q_1, q_2, \ldots q_s$ tais que $n_1 = p_1 p_2 \ldots p_r$ e $n_2 = q_1 q_2 \ldots q_s$.

Para provar a unicidade da escrita, suponha que tenhamos $n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$, onde os p_i e os q_j são números primos. Como $p_1 \mid q_1 q_2 \ldots q_s$, pelo corolário acima, temos que $p_1 = q_j$, que após o reordenamento de $q_1, q_2, \ldots q_j$, podemos supor que seja q_1. Portanto

$$p_2 \ldots p_r = q_2 \ldots q_s.$$

Como $p_2 \ldots p_r < n$, a hipótese de indução acarreta que $r = s$ e os p_i e q_j são iguais aos pares.

□

Este resultado, não tão completo como se encontra acima, pode ser encontrado nos *Elementos de Euclides*, pois é consequência quase que imediata de proposições que lá se encontram.

Agrupando, no Teorema acima, os fatores primos repetidos, se necessário, e ordenando os primos em ordem crescente, temos o seguinte enunciado.

Teorema 3.73. *Dado um número inteiro $n \neq -1, 0, 1$, existem primos $p_1 < p_2 < \ldots < p_r$ e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

Demonstração. Quando estivermos tratando de decomposição em fatores primos de dois, ou mais, números naturais, usaremos o recurso de adicionar fatores da forma $p^0 = 1$ (elemento neutro multiplicativo), onde p é um número primo qualquer. Assim, dados $n, m \in \mathbb{N}$, com $n > 1$ e $m > 1$ quaisquer, podemos então escrever

$$n = p_1^{\alpha_1} \ldots p_r^{\alpha_r} \quad \text{e} \quad m = p_1^{\beta_1} \ldots p_r^{\beta_r},$$

usando o mesmo conjunto de primos $p_1, \ldots, p_r$, desde que permitamos que os expoentes $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s$ variem em $\mathbb{N} \cup \{0\}$ e não apenas em $\mathbb{N}$.

□

Por exemplo, os números $2^3 \cdot 3^2 \cdot 7 \cdot 11$ e $2 \cdot 5^2 \cdot 13$ podem ser representados de forma respectiva como $2^3 \cdot 3^2 \cdot 5^0 \cdot 7 \cdot 11 \cdot 13^0$ e $2 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11^0 \cdot 13$.

Podemos tirar uma interessante conclusão com o teorema acima, um número natural $n > 1$, escrito na forma $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, é um quadrado perfeito se, e somente se, cada expoente α_i é par.

Proposição 3.74. *Seja $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, um número natural, escrito na forma acima. Se n' é um divisor positivo de n, então*

$$n' = p_1^{\beta_1} \ldots p_r^{\beta_r},$$

onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1, 2, \ldots, r$.

Demonstração. Seja n' um divisor positivo ne n e seja p^β a potência de um primo p que figura na decomposição de n' em fatores primos. Como $p^\beta \mid n$, segue que p^β divide algum $p_i^{\beta_i}$, por ser primo com os demais $p_j^{\alpha_j}$, e consequentemente, $p = p_i$ e $0 \leq \beta_i \leq \alpha_i$.

□

Denotando por $d(n)$ o número de divisores positivos do número natural n, segue-se que $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, onde $p_1, \ldots, p_r$ são números primos e $\alpha_1, \ldots, \alpha_r \in \mathbb{N}$ são os expoentes, então

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

Pela fórmula acima, um número natural possui uma quantidade ímpar de divisores, se, e somente se, n é um quadrado perfeito.

A fatoração de números naturais em primos, mostra-nos toda a estrutura multiplicativa desses números, permitindo-nos entre várias coisas, determinar sem dificuldade o *mdc* e *mmc* de um conjunto de quaisquer.

Teorema 3.75. *Sejam, $a = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} \ldots p_r^{\beta_n}$. Pondo*

$$\gamma_i = min\{\alpha_i, \beta_i\}, \quad \delta_i = max\{\alpha_i, \beta_i\}, \quad i = 1, 2, \ldots, n,$$

tem-se que

$$(a, b) = p_1^{\gamma_1} \ldots p_n^{\gamma_n} \quad e \quad [a, b] = p_1^{\delta_1} \ldots p_n^{\delta_n}.$$

Demonstração. Pela proposição anterior , temos que $p_1^{\gamma_1} \dots p_n^{\gamma_n}$ é um divisor comum de a e b. Seja c um divisor comum de a e b, logo $c = \pm p_1^{\epsilon_1} \dots p_n^{\epsilon_n}$, onde $\epsilon_i \leq min\{\alpha_i, \beta_i\}$ e, portanto $c \mid p_1^{\gamma_1} \dots p_n^{\gamma_n}$. Do mesmo modo, facilmente se prova a afirmativa sobre o mmc. □

Agora temos ferramentas para resolver o exemplo que nos foi deixado.

Exemplo 3.76. Dados dois números naturais d e m, vamos resolver em X, Y, nos naturais, o sistema de equações

$$(X, Y) = d, \quad [X, Y] = m.$$

Claramente uma condição necessária para que o sistema tenha solução é que $d \mid m$. Essa condição também é suficiente, pois $(m, d) = d$ e $[m, d] = m$.

Assim limitaremos nossa análise para o caso em que $d \mid m$.

Seja $d = p_1^{\gamma_1} \dots p_r^{\gamma_r}$ e $m = p_1^{\delta_1} \dots p_r^{\delta_r}$, onde $\gamma_i \leq \delta_i$. Então pelo Teorema 3.75, temos que $X = a$ e $Y = b$ é uma solução do sistema se, e somente se,

$$a = p_1^{\alpha_1} \dots p_r^{\alpha_r}, \quad b = p_1^{\beta_1} \dots p_r^{\beta_r}$$

onde

$$\gamma_i = min\{\alpha_i, \beta_i\} \quad \text{e} \quad \delta_i = max\{\alpha_i, \beta_i\}, \quad i = 1, 2, \dots, r.$$

Portanto temos para a uma ou duas escolhas, para α_i, segundo $\gamma_i = \delta_i$, ou $\gamma_i \neq \delta_i$. Consequentemente, temos 2^s escolhas para a, onde

$$s = \{i; \quad \gamma_i \neq \delta_i\}.$$

Como para cada escolha de a, o número b é univocamente determinado, temos que o problema admite 2^s soluções. Se ainda precisarmos identificar as soluções a, b com b, a, devemos dividir o número de soluções por 2, ou seja, teríamos 2^{s-1} soluções.

Relacionado ao Teorema Fundamental da Aritmética, temos uma importante notação: Se $n \in \mathbb{Z} \setminus \{0\}$ e p é um número primo, denotemos por $E_p(n)$ *o expoente da maior potência de* p *que divide* n.

A seguir temos a relação do Teorema Fundamental da Aritmética com a notação acima.

Proposição 3.77. *Se* m *e* n *são dois números naturais, então*

$$m = n \Leftrightarrow E_p(m) = E_p(n)$$

para todo número primo.

Demonstração. De fato se $m = n$, é obvio que $E_p(m) = E_p(n)$ para todo primo p.

Reciprocamente, suponhamos que $E_p(m) = E_p(n)$ para todo primo p. Se $E_p(m) = E_p(n) = 0$, para todo primo p, então $m = n = 1$. Caso contrário, pelo Teorema Fundamental da Aritmética, podemos escrever $m = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ e $n = q_1^{\beta_1} \dots q_s^{\beta_s}$, onde $\{p_1, \dots, p_r\}$ e $\{q_1, \dots, q_s\}$ são dois conjuntos cada um deles composto por números primos, dois a dois distintos. Como

$$\{p; \quad p \quad \text{é primo e} \quad E_P(m) > 0\} = \{p_1, \dots, p_r\}$$

e

$$\{p; \quad p \quad \text{é primo e} \quad E_P(n) > 0\} = \{q_1, \dots, q_s\},$$

segue-se que

$$\{p_1, \ldots, p_r\} = \{q_1, \ldots, q_s\}.$$

Assim, $r = s$ e, após o reordenamento dos elementos $q_1, \ldots, q_r$, podemos supor $q_i = p_i$ para $i = 1, \ldots, r$. Como $\alpha_i = E_{pi}(m) = E_{pi}(n) = \beta_i$, para $i = 1, \ldots, r$, conclui-se que $n = m$.

□

Temos portanto, para todo primo p, que

$$E_p((m,n)) = min\{E_p(m), E_p(n)\}, \quad E_p([m,n]) = max\{E_p(m), E_p(n)\}.$$

Distribuição dos Números Primos

Será que existe uma quantidade finita de números primos? A resposta para essa pergunta já foi dada por Euclides no Livro IX dos *Elementos*. Essa prova trás consigo o primeiro registro de uma demonstração por redução ao absurdo, portanto é considerada uma das pérolas da Matemática.

Teorema 3.78. *Existem infinitos números primos.*

Demonstração. Suponha que exista apenas um número finito de números primos $p_1, \ldots, p_r$. Considere o número natural

$$n = p_1 p_2 \ldots p_r + 1.$$

Pelo Teorema Fundamental da Aritmética, o número n possui um fator primo p que, portanto, deve ser um dos $p_1, \ldots, p_r$ e, consequentemente, divide o produto $p_1 p_2 \ldots p_r$. Mas isso implicaria dizer que $p \mid 1$, ou seja $p = 1$, o que é absurdo, pois p é primo, e portanto é maior que 1.

□

Agora que já sabemos a existência de infinitos números primos, como podemos obter uma lista com os números primos até um determinado valor?

Uma das mais antigas formas de se obter essa sequência foi criada por Eratóstenes, por volta de 230a.C., e recebeu o nome de *Crivo de Eratóstenes*. Porém não é muito útil para valores muito grandes.

Você pode consultar o método para a realização do *Crivo de Eratóstenes* em livros de Aritmética ou até mesmo em Livros Didáticos para o 6º ano do Ensino Fundamental no conteúdo de divisibilidade.

Mas será que podemos definir um limite de testes para determinar a *primalidade* de um número? O Lema a seguir nos fornecerá essa resposta.

Lema 3.79. *Se um número natural $n > 1$ não é divisível por nenhum número primo $p^2 \leq n$, então ele é primo.*

Demonstração. Suponhamos, por absurdo, que n não seja divisível por nenhum número primo p, tal que $p^2 \leq n$, e não seja primo. Seja q o menor número primo que divide n; então $n = qn_1$, com $q \leq n_1$. Segue daí que $q^2 = q \cdot q \leq qn_1 = n$. Logo, n é divisível por um número primo q tal que $q^2 \leq n$, absurdo.

□

Note que o Lema acima, nos fornece um teste de primalidade, pois para verificar se um certo número n é primo, basta verificar que ele não é divisível por nenhum primo p que não supere $\sqrt{n}$.

Porém esse método para encontrar números primos, é muito lento e trabalhoso, veremos mais adiante neste capítulo métodos mais eficientes.

Uma questão importante que se coloca é de como números primos se distribuem dentro do conjunto dos naturais. Qual poderia ser a distância entre dois números primos consecutivos? Essa distância é fixa? Existe um limite para essa distância? Analisando os primeiros números primos não conseguimos encontrar um padrão pré definido, imagine esse número contendo milhares, milhões, bilhões de algarismos, essa conclusão fica ainda mais difícil.

Podemos destacar alguns números primos consecutivos cuja distância é de duas unidades, como por exemplo (3,5), (5,7), (11,13), (17,19), (41,43), (59,61), (71,73), (101,103), (107,1709), e muitos mais. A esses números é dada a denominação de *primos gêmeos*. Mesmo hoje, com tanta tecnologia, não se sabe se há infinitos pares de números primos gêmeos.

Ao contrário dos primos gêmeos, existem pares de primos consecutivos, cuja distância é muito grande. Portanto não há nenhum padrão entre as distâncias de dois primos consecutivos.

Para mensurar a frequência em que os primos aparecem em um intervalo de naturais, podemos determinar uma probabilidade, ou seja, algo incerto.

Denotemos por $\pi(x)$, a quantidade de números primos menores ou igual a x, a probabilidade de um elemento do conjunto $\{1, 2, \ldots, x\}$ ser primo, é dada por

$$\frac{\pi(x)}{x}.$$

Como esse quociente é muito complexo, o que se poderia fazer é achar uma função de comportamento bem próximo, quando x é relativamente grande.

Legendre e *Gauss*, através da análise de tabelas, chegaram a conclusão que a função desejada poderia ser $\frac{1}{\ln x}$. Por volta do ano 1900, *J. Hadamard* e *Ch. de la Vallée-Poussin*, independentemente provaram o profundo Teorema dos números primos, cujo enunciado é

$$\lim_{x \longrightarrow \infty} \frac{\pi(x)}{x} \left(\frac{1}{lnx}\right)^{-1} = 1.$$

Em 1949, *P. Erdos* e *A. Selberg* simplificaram a prova desse teorema.

A distribuição dos primos ainda é um mistério e a ela estão associados vários problemas ainda sem solução. Como por exemplo:

1) Sempre existe um número primo entre n^2 e $(n+1)^2$ para qualquer $n \in \mathbb{N}$?

2) Para $n = 0, 1, \ldots, 40$, tem-se que $n^2 - n + 41$ é primo. Existem infinitos números primos dessa forma?

3) A sequência de Fibonacci contém infinitos números primos?

4) Todo número natural maior que 3, pode ser escrito como soma de dois números primos? *Conjectura de Goldbach.*

Entre outros.

3.7.2 Teorema de Fermat

Desde, pelo menos 500 anos antes de Cristo, os chineses sabiam que, se p é um número primo, então $p \mid 2^p - 2$. No século XVII, *Pierre de Fermat*, generalizou esse resultado, escrevendo um teorema de curto enunciado, mas de grande valia. Para a demonstração desse teorema, precisamos do lema a seguir.

Lema 3.80. *Seja, p um número primo. Os números $\binom{p}{i}$, onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. O resultado vale trivialmente para $i = 1$. Podemos então supor $1 < i < p$. Neste caso, $i! \mid p(p-1)\dots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i! \mid (p-1)\dots(p-i+1)$, e o resultado se segue, pois

$$\binom{p}{i} = \frac{p!}{i!(p-i!)} = p\frac{(p-1)\dots(p-i+1)}{i!}.$$

□

Teorema 3.81 (Pequeno Teorema de Fermat)**.** *Dado um número primo p, tem-se que p divide o número $a^p - a$, para todo $a \in \mathbb{Z}$.*

Demonstração. Se $p = 2$, o resultado é óbvio já que $a^2 - a = a(a-1)$ é par (produto de dois números consecutivos). Suponhamos p ímpar. Neste caso, basta mostrar o resultado para $a \geq 0$. A demonstração será feita por indução sobre a.

O resultado vale claramente para $a = 0$, pois $p \mid 0$. Supondo o resultado válido para a, iremos prová-lo para $a + 1$. Pela fórmula do Binômio de Newton,

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

Pelo lema anterior e pela hipótese de indução, o segundo membro da igualdade acima é divisível por p, o que implica $p \mid (a+1)^p - (a+1)$ portanto $p \mid a^p - a$ para todo $a \in \mathbb{Z}$.

□

Um exemplo da aplicação desse teorema, bastante interessante é o que traremos a seguir.

Exemplo 3.82. Dado um número qualquer $n \in \mathbb{N}$, tem-se que n^9 e n, quando escritos na base 10, tem o mesmo algarismo da unidade.

A afirmação acima é a mesma que dizer $10 \mid n^9 - n$. Como n^9 e n tem a mesma paridade, pois:

i) Se n é par, ele pode ser escrito da forma $2K$, com $K \in \mathbb{Z}$ assim $(2K)^9 = 512k^9 = 2(256K^9) = 2L$, portanto é par. Como a diferença entre dois números pares é par temos que $2 \mid n^9 - n$.

ii) Se n é ímpar, ele pode ser escrito da forma $2K + 1$, com $K \in \mathbb{Z}$, assim $(2K+1)^9 = 2S + 1$ (desenvolver o binômio) que é ímpar. Como a diferença de dois números ímpares é par, $2 \mid n^9 - n$.

Concluímos que $n^9 - n$ é par, logo $2 \mid n^9 - n$, $\forall n \in \mathbb{N}$. Por outro lado,

$$n^9 - n = n(n^4 - 1)(n^4 + 1) = (n^5 - n)(n^4 + 1)$$

Logo, pelo Pequeno Teorema de Fermat, temos que $5 \mid (n^5 - n)$, o que implica que $5 \mid (n^5 - n)(n^4 + 1) = n^9 - n$. Portanto, $2 \mid n^9 - n$ e $5 \mid n^9 - n$ e como $(2, 5) = 1$ então $2.5 = 10 \mid n^9 - n$, para todo $n \in \mathbb{N}$.

Corolário 3.83. *Se p é um número primo e se a é um número natural não divisível por p, então p divide $a^{p-1} - 1$.*

Demonstração. Como pelo Pequeno Teorema de Fermat $p \mid a^p - a = a(a^{p-1} - 1)$ e como $p \nmid a$, segue-se imediatamente que $p \mid a^{p-1} - 1$.

□

O corolário acima também será chamado de *Pequeno Teorema de Fermat*. Ele também nos fornece um teste de primalidade. Dado um número $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{m-1} - 1$, então m é primo.

O Pequeno Teorema de Fermat também nos diz que se $p > 2$ é um número primo e a um número natural tal que $p \nmid a$,

$$p \mid a^p - a = a(a^{p-1} - 1) \Rightarrow p \mid \left(a^{\frac{p-1}{2}}\right)\left(a^{\frac{p+1}{2}}\right).$$

Como p é primo, temos que $p \mid \left(a^{\frac{p-1}{2}}\right)$ ou $\left(a^{\frac{p+1}{2}}\right)$. Determinar qual das duas condições de divisibilidade acima é a correta, pode ser um problema bem difícil se tivermos números grandes.

3.8 Números Especiais

Nesta seção falaremos um pouco sobre alguns números primos que se destacam, por terem características específicas e serem de grande valia, principalmente em codificações, na área de computação. São eles os números de *Fermat* e *Mersenne*.

Pierre de Fermat nasceu em 20 de agosto de 1601 na França. Seu pai era rico, portanto pôde receber uma educação privilegiada. Mas nos anos de colégio o jovem Fermat não demonstrava ser um grande gênio da Matemática.

Por pressão familiar, foi nomeado conselheiro da Câmara de Requerimentos ao Rei. Além do cargo, ele exercia algumas funções paralelas, como a de juiz. Teve ascensão rápida em sua carreira, tornando-se membro da elite. Apesar disso, procurava não se envolver muito com a política da época, afim de evitar atritos com os governantes. O tempo que lhe sobrava era dedicado a seu *hobby*, a Matemática. Assim era considerado um estudioso amador.

Nesse período a Matemática se recuperava do chamado *Período das Trevas*, os matemáticos não tinham prestígio, e muitos eram obrigados a custear seus estudos. O padre Mersenne, foi um dos responsáveis por avanços na Matemática do século XVII. Após entrar para a ordem em 1611, Mersenne estudou matemática e deu aulas para monges.

As descobertas matemáticas eram sigilosas na época, assim quando Mersenne se mudou para a capital Paris, tentou ir contra esse costume. Ele organizou encontros em grupos, para encorajar os matemáticos a trocarem ideias. Quando ficava sabendo de alguma informação, mesmo que fosse uma carta sigilosa, ele compartilhava com o grupo. Este

comportamento não era considerado ético, principalmente por se tratar de um membro do clero.

Mersenne viajou pela França e exterior divulgando os trabalhos matemáticos. Assim conheceu Fermat, que tinha grande relutância em divulgar suas descobertas, ele ficava plenamente satisfeito em criar teoremas sem ser incomodado. Entretanto, Fermat tinha uma face zombeteira, que o levava a comunicar-se com outros matemáticos para debochar de seus conhecimentos, apesar de sua grande timidez. Ele escrevia cartas com seus teoremas recém criados, mas sem a demonstração, desafiando a quem se interessa-se em demonstra-los.

A influência de Mersenne sobre Fermat, deve ter sido significativa, pois sempre que o padre não podia ir a seu encontro, eles se correspondiam por cartas. Quando Mersenne faleceu, foi encontrado em seu quarto um acumulado de cartas, enviadas a vários pensadores da época.

Fermat, não se relacionava muito bem com os demais matemáticos de sua época, em uma das únicas ocasiões, discutiu com Pascal sobre um novo ramo da matemática, que viria a se chamar teoria da probabilidade. Juntos demonstraram as primeiras certezas da teoria da probabilidade. Fermat e Pascal determinaram as regras básica dos jogo de *azar*.

Fermat também esteve envolvido em outro ramo da Matemática, o Cálculo. A Matemática de Fermat, permitiu aos cientistas compreender melhor conceitos como a velocidade e sua relação com a aceleração. Depois de muitos anos ser considerado Isaac Newton, como inventor do cálculo, foi acreditado a Fermat esse feito.

Isso já teria feito de Fermat um dos maiores matemáticos da história, entretanto sua grande paixão era a Teoria dos Números. Ele era obcecado por desvendar as relações entre os números.

Sua teoria é utilizada até os dias de hoje, e pode ser encontrada em diversas áreas como: criptografia, revestimento acústico, comunicações espaciais de longa distância, entre outras.

Para o leitor que se interessar por essa fascinante história pode procurar pelo livro "O Último Teorema de Fermat" [28] .

Primeiramente falaremos sobre os *primos de Fermat*, nome atribuído em homenagem a Pierre Fermat.

Antes de conhecer esses números vamos precisar da seguinte proposição.

Proposição 3.84. *Sejam a e n números naturais maiores do que 1. Se $a^n + 1$ é primo, então a é par e $n = 2^m$, com $m \in \mathbb{N}$.*

Demonstração. Suponha que $a^n + 1$ seja primo, onde $a, n > 1$. Logo a tem que ser par, pois caso contrário $a^n + 1$ seria par e maior que 2, já que a e a^n tem a mesma paridade.

Se n tivesse um divisor primo p diferente de 2, teríamos $n = n'p$, com $n' \in \mathbb{N}$. Portanto $a^{n'}+1 \mid (a^{n'})^p+1 = a^n+1$, pois pela Proposição 3.27 n' e $n'p$ seriam ímpar, contradizendo o fato de $a^n + 1$ ser primo. Isso significa que n é da forma 2^m.

□

Os *números primos de Fermat* são os números da forma

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, 2 \ldots$$

Diz a história que em 1640, Fermat escreveu em uma de suas cartas a Mersenne que achava que todos os números dessa forma eram primos. Após verificação Mersenne observou que

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17, a; F_3 = 257 \text{ e } F_4 = 65537,$$

são todos primos.

Porém

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417,$$

é um número composto. Foi Leonhard Euler que em 1732, desvendou esse problema, mostrando que Fermat estava errado.

Não se sabe ao certo se realmente Fermat achava que todos esses números (F_n) eram primos, pois Fermat foi uma das mentes mais brilhantes de sua geração, ou se queria apenas instigar Mersenne a procurar números que realmente fossem em sua forma, todos primos.

Mesmo nos dias de hoje, com toda a tecnologia, não se sabe afirmar se existem outros Primos de Fermat além dos cinco primeiros. Os matemáticos *Hardy* e *Wright*, conjecturaram que os Primos de Fermat são em número finito.

A proposição a seguir nos fala sobre outros números que são sempre primos.

Proposição 3.85. *Sejam a e n números naturais maiores do que 1. Se $a^n - 1$ é primo, então $a = 2$ e n é primo.*

Demonstração. Admitamos que $a^n - 1$ seja primo, com $a, n > 1$. Suponhamos por absurdo que $a > 2$. Logo , $a - 1 > 1$ e $a - 1 \mid a^n - 1$, pela Proposição 3.26, contradizendo o fato de ser primo. Portanto $a = 2$.

Por outro lado, suponhamos por absurdo, que n não é primo, então seja $n = rs$, com $r > 1$ e $s > 1$. Como $2^r - 1 \mid (2^r)^s - 1$, segue que $2^n - 1$ não é primo, contradição. Logo n é primo.

□

Os números chamados de *Primos de Mersenne* são os da forma

$$M_p = 2^p - 1,$$

onde p é primo.

No intervalo $2 \leq p \leq 5000$ os números de Mersene que são primos corresponde aos seguintes valores de p,

$$p = \{2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423\}$$

Até o presente momento , o maior número primo conhecido de Mersenne é o $M_{82589933}$, descoberto no dia 07 de dezembro de 2018, pelo projeto de pesquisa mundial **Great Internet Mersenne Prime Search (GIMPS)**. Esse número contém 24.862.048 dígitos, este é o 51° Primo de Mersenne já descoberto. Esse projeto é responsável por encontrar 17 Primos de Mersenne.

O $M_{82589933}$ foi descoberto por Patrick Laroche, de 35 anos que é profissional de TI, essa descoberta lhe rendeu um prêmio de aproximadamente 11 mil reais.

Essas informações foram encontradas no site do IMPA [29] .

O teorema a seguir é muito profundo, dado no século XIX pelo alemão *Johann P. G. Lejeune Dirichlet*:

Teorema 3.86. *Em uma progressão aritmética (PA) de números naturais, com primeiro termo e razão primos entre si, exitem infinitos números primos.*

Omitiremos a demostração desse teorema por ser muito complexa e pertencer a teoria analítica dos números. O que faremos é demostrar alguns casos particulares e interessantes desse teorema.

Proposição 3.87. *Na progressão aritmética* $3, 7, 11, 15, \ldots, 4n+3, \ldots$ *existem infinitos números primos.*

Demonstração. Queremos mostrar que os números primos da forma $4n+3$ são em quantidade infinita.

Um número primo é da forma $4n+1$ ou $4n+3$. Assim, note que o conjunto

$$A = \{4n+1;\ n \in \mathbb{N}\},$$

é fechado multiplicativamente.

Isso significa que $(4n+1)(4n'+1) = 16nn'+4n+4n'+1 = 4(4nn'+n+n')+1 = 4m+1$, com $m \in \mathbb{N}$.

Suponhamos agora, por absurdo, que os números da forma $4n+3$ sejam em quantidade finita, ou seja $3 < p_1 < \ldots < p_k$. Portanto o número $a = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 3$ não é divisível por nenhum dos primos $3, p_1, p_2, \ldots p_k$ e, consequentemente, sua decomposição em fatores primos só pode conter primos da forma $4n+1$, pois $(4n+3)(4n'+3) = 4(4nn'+3n+3n'+2)+1 = 4m+1$ com $m \in \mathbb{N}$. Assim $a = 4m+1$, com $m \in \mathbb{N}$ o que é uma contradição, portanto a é da forma $4n+3$.

□

Para provar que existem infinitos números primos da forma $4n+1$ vamos precisar do seguinte lema:

Lema 3.88. *Seja* $x \in \mathbb{N}$*, com* $x \geq 2$*. Todo divisor ímpar de* x^2+1 *é da forma* $4n+1$*.*

Demonstração. Primeiramente vamos mostrar que todo divisor primo $p \neq 2$ de x^2+1 é da forma $4n+1$. Pela proposição 3.87, o conjunto $A = \{4n+1;\ n \in \mathbb{N}\}$ é fechado multiplicativamente.

Suponhamos que $p \mid x^2+1$, com $p > 2$ e primo. Como p é ímpar temos que $2 \mid (p-1)$, assim, para algum $\lambda \in \mathbb{N}$, temos $x^2+1 = \lambda p \Rightarrow x^2 = \lambda p - 1$. Elevando a potência $\frac{(p-1)}{2}$ em ambos os lados da igualdade acima temos

$$(x^2)^{\frac{p-1}{2}} = (\lambda p - 1)^{\frac{p-1}{2}} \Rightarrow x^{p-1} = (\lambda p - 1)^{\frac{p-1}{2}} = \begin{cases} \mu p + 1, & \text{se } \frac{p-1}{2} \text{ é par.} \\ \mu' p - 1, & \text{se } \frac{p-1}{2} \text{ é ímpar} \end{cases}$$

Se

$$x^{p-1} = \mu' p - 1,$$

Subtraindo 1 em ambos os lados, teríamos

$$x^{p-1} - 1 = \mu' p - 2.$$

Como $p \mid x^2+1$, segue que $p \nmid x$.

Note que, se $p \mid x \Rightarrow x = kp$, então $x^2+1 = k^2p^2+1$. Como $p \mid x^2+1 \Rightarrow p \mid k^2p^2+1$ e como $p \mid k^2p^2 \Rightarrow p \mid 1 \Rightarrow p = 1$. Absurdo, logo pelo Pequeno Teorema de Fermat, temos que $p \mid x^{p-1} - 1$ e pela Proposição 3.84 $x^{p-1} - 1 = \mu' p - 2$, temos que $p \mid 2$, o que é uma contradição.

Portanto, a única alternativa possível é que $\frac{p-1}{2}$ seja par, o que implica que p é da forma $4n+1$.

□

Proposição 3.89. *Na progressão aritmética* $1, 5, 9, 13, 17, \ldots, 4n+1, \ldots$ *existem infinitos números primos.*

Demonstração. Suponha por absurdo que existam finitos números primos da forma $4n+1$. Considere o número

$$a = 4p_1^2 \ldots p_k^2 + 1,$$

com os p_i com $i = 1, 2, \ldots k$, todos da forma $4n + 1$. Como $p_1 \nmid a$, segue que todo divisor primo de a é da forma $4n + 3$, o que é um absurdo, pois

$$a = 4p_1^2 \ldots p_k^2 + 1 = a = 2^2 p_1^2 \ldots p_k^2 + 1 = x^2 + 1,$$

e pelo lema anterior todo divisor ímpar de $x^2 + 1$ é da forma $4n + 1$.

□

3.8.1 Números Perfeitos

Seja n um número natural. Denotemos por $S(n)$ a soma de todos os seus divisores naturais.

Exemplo 3.90.

$$S(1) = 1, \quad S(2) = 1+2 = 3, \quad S(4) = 1+2+4 = 7, \quad S(12) = 1+2+3+4+6+12 = 28.$$

Note que se um número p é primo, seus únicos divisores são 1 e p, assim

$$S(p) = p + 1.$$

Quando tivermos $n \geq 2$, podemos obter $S(n)$ através da seguinte proposição:

Proposição 3.91. *Seja* $n = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$ *a decomposição de* n *em fatores primos. Então*

$$S(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \ldots \frac{p_r^{\alpha_r+1} - 1}{p - 1}.$$

Demonstração. Considere a igualdade

$$(1 + p_1 + \ldots + p_1^{\alpha_1}) \ldots (1 + p_r + \ldots + p_r^{\alpha_r}) = \sum p_1^{\beta_1} \ldots p_r^{\beta_r},$$

onde o somatório do lado direito da igualdade é tomado sobre todas a r-uplas $(\beta_1 \ldots \beta_r)$ ao variar cada β_i no intervalo $0 \leq \beta_i \leq \alpha_1$, para $i = 0, 1, 2, \ldots, r$. Como tal somatório representa a soma de todos os divisores de n, a fórmula $S(n)$ resulta aplicando a fórmula da soma de uma progressão geométrica a cada soma do lado direito da igualdade acima.

□

Do resultado acima, temos imediatamente o seguinte corolário.

Corolário 3.92. *A função* $S(n)$ *é multiplicativa, isto é, se* $(n, m) = 1$*, então*

$$S(nm) = S(n) \cdot S(m).$$

Exemplo 3.93.

$$S(5) = \frac{5^2-1}{5-1} = \frac{24}{4} = 6.$$

$$S(14) = S(2)\cdot S(7) = \frac{2^2-1}{2-1}\cdot\frac{7^2-1}{7-1} = \frac{3}{1}\cdot\frac{48}{6} = 24.$$

$$S(12) = S(2^2)\cdot S(3) = \frac{2^3-1}{2-1}\cdot\frac{3^2-1}{3-1} = \frac{7}{1}\cdot\frac{8}{2} = 28.$$

Note que $S(18) = S(3)\cdot S(6) = \frac{3^2-1}{3-1}\cdot\frac{6^2-1}{6-1} = 39 \neq 48$, pois $(3,6) = 3$, quando o correto seria $S(18) = S(2)\cdot S(9)$, pois $(2,9) = 1$.

Alguns raros números possuem a propriedade especial de serem iguais a metade da soma de seus divisores, e são chamados de *Números Perfeitos*, que receberam esse nome, pois fascinaram os gregos com sua característica especial.

Assim um número natural n é chamado de número perfeito, se $S(n) = 2.n$ ou $n = \frac{S(n)}{2}$, ou ainda que ele é igual a soma de seus divisores distintos dele próprio.

Na idade média foram encontrados os números perfeitos 6, 28, 496, 8128 e 33550336. Atualmente se conhecem mais alguns desses números, e curiosamente todos ele são pares, porém não se sabe nada sobre existir, ou não, números perfeitos ímpares.

O teorema a seguir, deve-se parte a Euclides e parte a Euler, ele caracteriza os números perfeitos que são pares, relacionando-os com os primos de Mersenne.

Teorema 3.94. *Um número natural n é um número perfeito par se, e somente se, $n = 2^{p-1}(2^p-1)$, onde 2^p-1 é um primo de Mersenne.*

Demonstração. Suponha que $n = 2^{p-1}(2^p-1)$, onde 2^p-1 é um primo de Mersenne. Logo $p > 1$, e, consequentemente n é par.

Como 2^p-1 é ímpar, temos que $(2^{p-1}, 2^p-1) = 1$. Logo, pela Proposição 3.91 e pelo corolário anterior e sabendo que se n é primo, então $S(n) = n+1$, temos

$$S(n) = S(2^{p-1}, 2^p-1) = S(2^{p-1})\cdot S(2^p-1) = \frac{2^p-1}{2-1}\cdot 2^p = 2.[2^{p-1}(2^p-1)] = 2n.$$

Portanto n é um primo perfeito.

Reciprocamente, suponha que n é perfeito e par. Seja 2^{p-1}, a maior potência de 2 que divide n. Logo, $p > 1$ e $n = 2^{p-1}b$, com b ímpar. Temos então que $(2^{p-1}, b) = 1$, e novamente pela Proposição 3.91 e pelo corolário anterior, temos que $S(n) = S(2^{p-1})\cdot S(b)$. Como $S(n) = 2n$, segue-se que

$$(2^p-1)S(b) = 2^p\cdot b.$$

Portanto $(2^p-1) \mid b$, pois $(2^p, 2^p-1) = 1$. Logo, existe $c \in \mathbb{N}$ com $c < b$ tal que

$$b = c(2^p-1).$$

Substituindo o valor de b, temos

$$(2^p-1)S(b) = 2^p(2^p-1)c;$$

assim,

$$S(b) = 2^p c.$$

Da equação $b = c(2^p - 1)$, temos que c e b são dois divisores distintos de b, tais que $c + b = 2^p c$. Nesta situação $c = 1$. De fato, suponha, por absurdo, que $c \neq 1$. Temos então , que $S(b) \geq 1 + c + b > c + b = 2^p c$. Segue-se então que

$$2^p c = c + b < S(b) = 2^p c,$$

contradição.

Portanto $S(b) = b + 1$. Logo, b é primo. Temos assim, que $n = 2^{p-1}(2^p - 1)$, com $2^p - 1$ primo.

□

Note que o teorema reduz a existência ou não de um número infinito de números perfeitos pares ao problema análogo aos primos de Mersenne, que ainda se encontram sem solução.

O leitor que se interessar pelos números primos, pode se aprofundar muito mais, pois há características dos primos muito interessantes que não citaremos neste trabalho.

Uma aplicação muito interessante sobre os números primos é a na criptografia, pois as chaves de segurança de uma determinada mensagem criptografada são números primos. Quanto mais sigiloso o conteúdo da mensagem, maior deve ser a segurança por trás dela, assim precisa-se de números primos cada vez mais raros e difíceis de se determinar.

4 Fluxograma e Divisibilidade

Este capítulo trará exemplos de fluxogramas para serem aplicados em atividades relacionadas aos conceitos de divisibilidade de números inteiros.

A divisão é a operação matemática em que os alunos apresentam maior dificuldade, tanto na compreensão, quanto na execução do algoritmo. Visando ajudar alunos e professores com relação a essa operação tão fundamental, e aproveitando o gancho da BNCC, trabalharemos os conceitos de divisibilidade de uma forma diferenciada, através dos fluxogramas.

Fazendo pesquisa sobre exemplos de fluxogramas para efetuar a divisão, encontrei apenas alguns voltados para programação. Nesses exemplos sugere-se que o programa faça os cálculos, assim o programador apenas obtém o resultado final. Esse não é o nosso objetivo, e sim que o aluno finalmente entenda os conceitos envolvidos por trás do algoritmo.

Vamos então relembrar o conceito de divisibilidade.

Divisibilidade - Dados dois inteiros a e b, com $b \neq 0$, diremos que b divide a, quando existir um $c \in \mathbb{Z}$, tal que $a = b \cdot c$, em símbolos $b \mid a$. Caso contrário diremos que b não divide a, em símbolos $b \nmid a$. Chamaremos a de *dividendo* e b de *divisor*.

Se $b \nmid a$, pela divisão euclidiana temos $q, r \in \mathbb{N}$, tais que

$$a = b \cdot q + r$$

com $0 \leq r <\mid b \mid$. Onde q e r são chamados, respectivamente, *quociente* e *resto* da divisão de a por b.

Exemplo 4.1. Fluxograma Divisibilidade

Sejam os números naturais a, b, q e r, chamados respectivamente de dividendo, divisor, quociente e resto. Determine se o número a é divisível por b seguindo os passos do fluxograma.

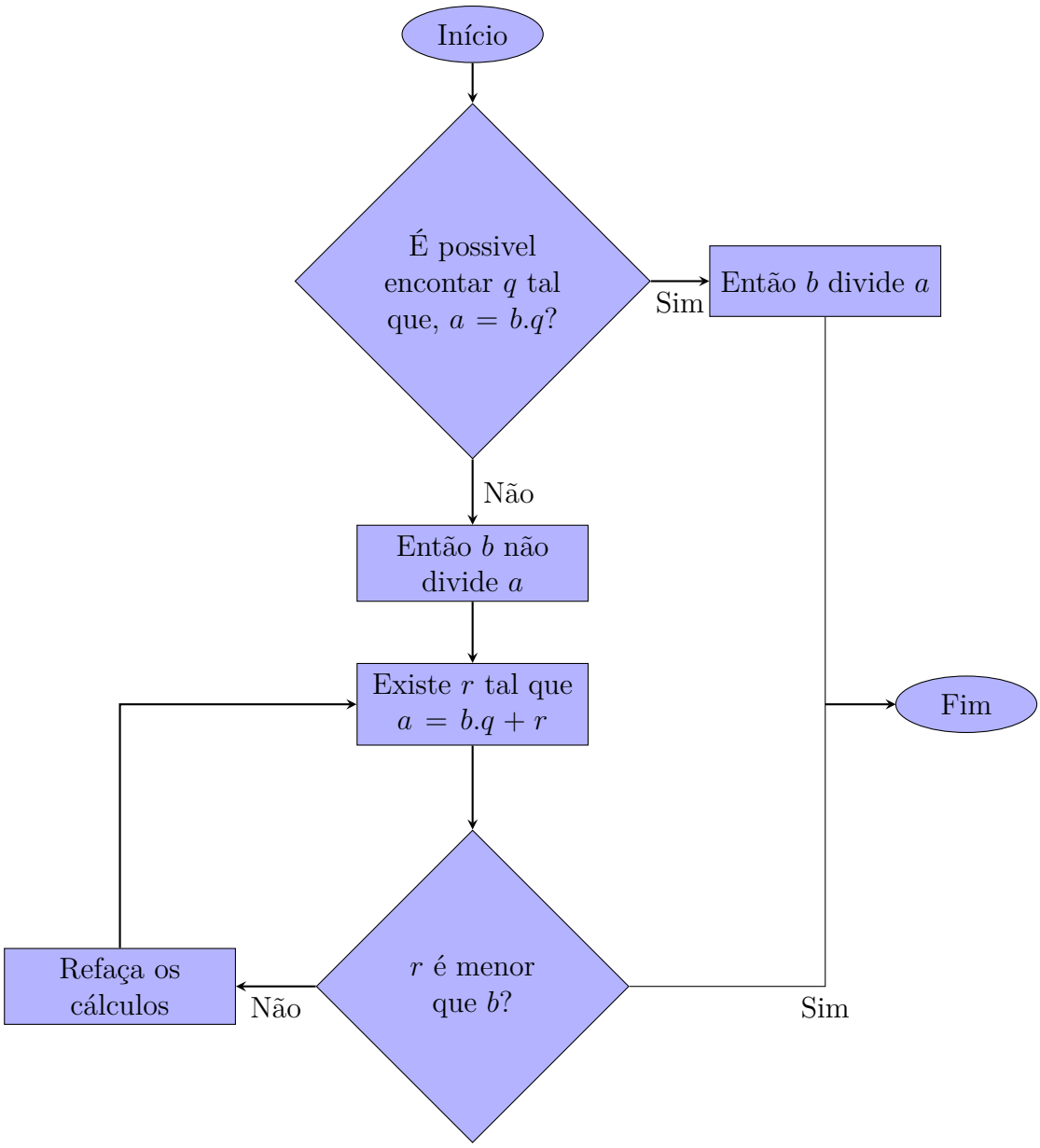


Figura 4.1: Fluxograma de autoria própria - Divisibilidade

Expansão na base b - Uma importante função da divisão é escrever um número inteiro qualquer em outra base. Uma das bases mais utilizadas é a binária (2 símbolos), que dão origens a códigos de barras e também linguagem computacional. O nosso sistema numérico é representado em base decimal (10 símbolos), existem também outras bases, a sexagesimal (60 símbolos) e a hexadecimal (16 símbolos), essa última está vinculada a informática como unidade de memória.

Vamos então construir um fluxograma para representar números inteiros em qualquer base.

Sejam a e b números inteiros, com $a > 0$ e $b > 1$. Existem números inteiros $n \geq 0$ e $r_0, r_1, r_2, \ldots, r_n$ menores que b, com ,$r_n \geq 0$, univocamente determinados, tais que

$$a = r_0 + r_1 b^1 + r_2 b^2 + \ldots r_n b^n.$$

Pela divisão euclidiana, temos que

$$a = bq + r, \text{ com } q, r \in \mathbb{N} \text{ e } 0 \leq r < b.$$

Como $0 < q < a$, podemos construir um algoritmo para escrever a na base b.

$$a = bq_0 + r_0 \ , \ r < b;$$

$$q_0 = bq_1 + r_1 \ , \ r_1 < b;$$

$$q_1 = bq_2 + r_2 \ , \ r_2 < b;$$

$$\vdots$$

$$q_{n-1} = bq_n + r_n \ , \ \text{com } q_n = 0 \text{ e } r_n < b.$$

Vamos agora representar esse algoritmo por meio de um fluxograma.

Exemplo 4.2. Fluxograma - Expansão na base b

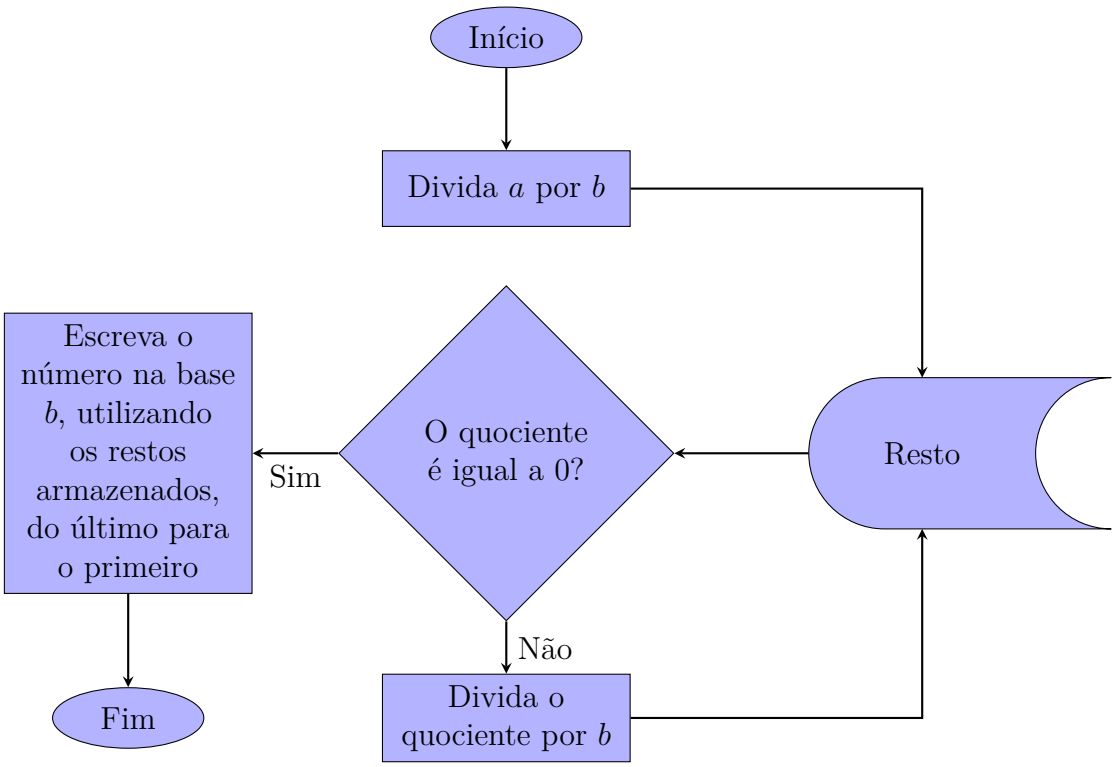


Figura 4.2: Fluxograma de autoria própria - Expansão na base b

Uma outra aplicação para o algoritmo da divisão euclidiana é a obtenção do **máximo divisor comum** (mdc) de dois números inteiros.

Sejam a e b dois números inteiros não nulos, e seja seu d o máximo divisor comum se a e b se:

i d divide a e b.

ii d é divisível por todo divisor comum de a e b.

O mdc dos números a e b será representado por $d = (a, b)$.

Pela divisão euclidiana podemos encontrar o máximo divisor comum de dois números inteiros, que podemos supor serem positivos, pois $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

Pela definição o algoritmo pode ser sistematizado e realizado na prática como mostramos a seguir.

Inicialmente efetue a divisão de a por b e encontre $a = bq_1 + r_1$, agora coloque os valores encontrados no diagrama.

	q_1	
a	b	
r_1		

Seguindo, continuamos efetuando a divisão de b por r_1, obtendo $b = r_1q_2 + r_2$ e colocamos novamente os números no diagrama.

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Vejamos agora esse mesmo algoritmo em linguagem de fluxograma.

Exemplo 4.3. Fluxograma - máximo divisor comum (mdc)

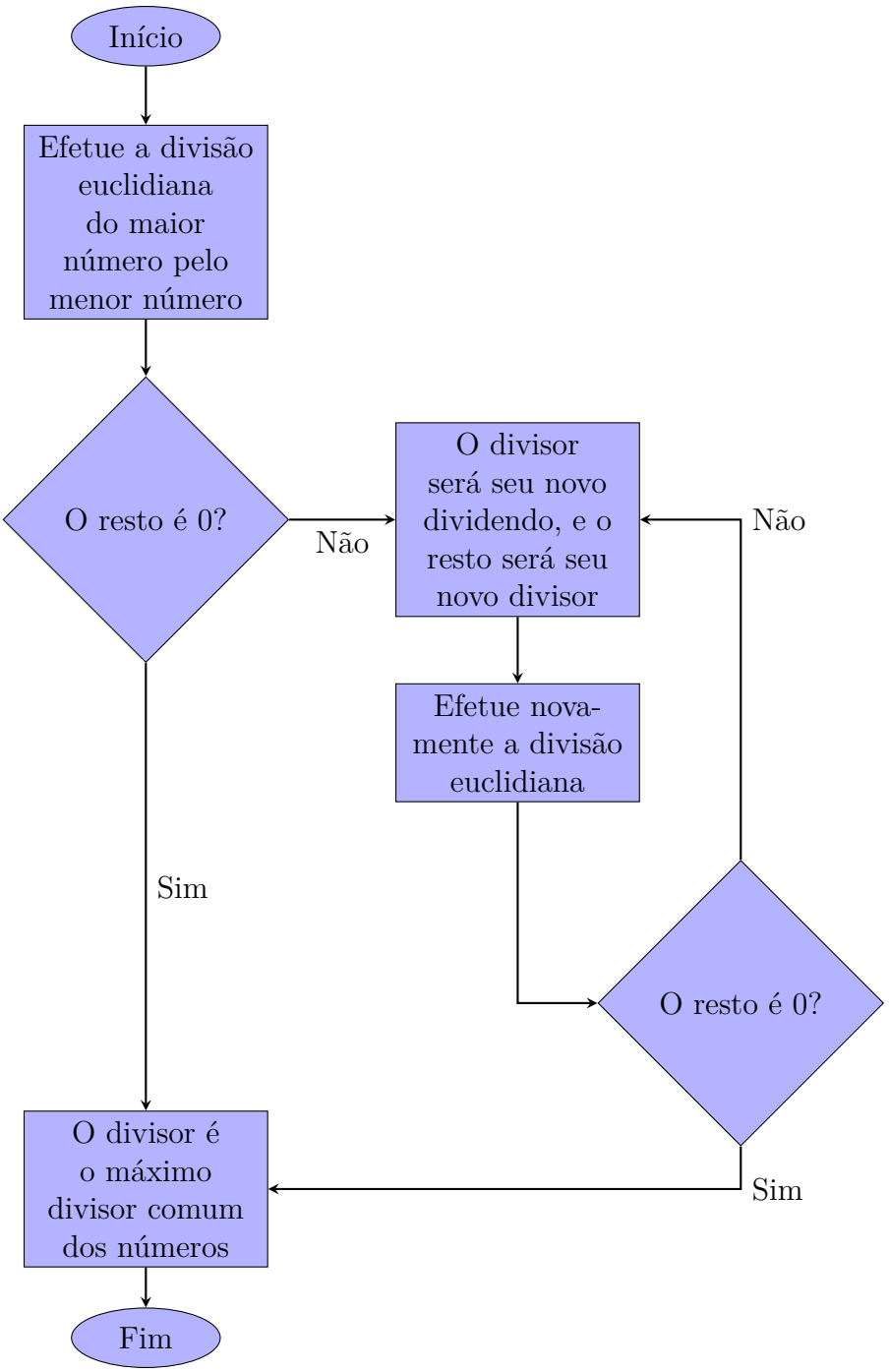


Figura 4.3: Fluxograma de autoria própria - Máximo divisor comum (mdc)

Seguindo no conteúdo de divisibilidade temos as equações diofantinas lineares, que são equações do tipo:

$$aX + bY = c,$$

sendo a, b e c números inteiros. Tais equações nem sempre tem solução, mas caso tenham podemos encontrá-las usando o método de tentativa e erro, quando forem simples de se obter a solução, ou então por meio de algumas técnicas.

Vamos fazer um exemplo bem simples por tentativa e erro.

$$2x + 3y = 7$$

É fácil perceber que $x = 2$ e $y = 1$ pois $2.\mathbf{2} + 3.\mathbf{1} = 7$.

Mas como já mencionado, alguma equações diofantinas lineares não possuem solução inteira, por exemplo

$$8x + 6y = 21.$$

Note que $8x + 6y = 2.(4x + 3y)$, logo o resultado teria que ser um número par, o que não é o caso, $2 \nmid 21$.

Pelas definições já apresentadas neste trabalho sabemos que as equações diofantinas lineares só admitirão soluções inteiras se:

Dados a, b e c números inteiros. A equação $aX + bY = c$ admite soluções inteiras se, e somente se, $(a, b) \mid c$.

Podemos então, nesses casos, encontrar soluções particulares x_0 e y_0 das equações $aX + bY = c$, onde $(a, b) = 1$. A partir destas, tem-se a solução geral dada por

$$x = x_0 + b.t, \text{ e } y = y_0 - a.t; \text{ com } t \in \mathbb{Z}.$$

Portanto quando houver solução, elas serão em quantidades infinitas no conjunto dos inteiros.

No exemplo acima, $2x + 3y = 7$ encontramos a solução particular $x_0 = 2$ e $y_0 = 1$, podemos então determinar todas as soluções no conjunto dos inteiros para essa equação escrevendo:

$$x = 2 + 3.t \text{ e } y = 1 - 2.t, \text{ com } t \in \mathbb{Z}.$$

Podemos também ter como solução os valores $x = x_0 - b.t$ e $y = y_0 + a.t$, com $t \in \mathbb{Z}$.

Vamos então construir um fluxograma para determinar soluções particulares por inspeção (tentativa e erro) das equações diofantinas lineares e então determinar todas a soluções inteiras da mesma.

Exemplo 4.4. Fluxograma - Equações diofantinas lineares - por inspeção

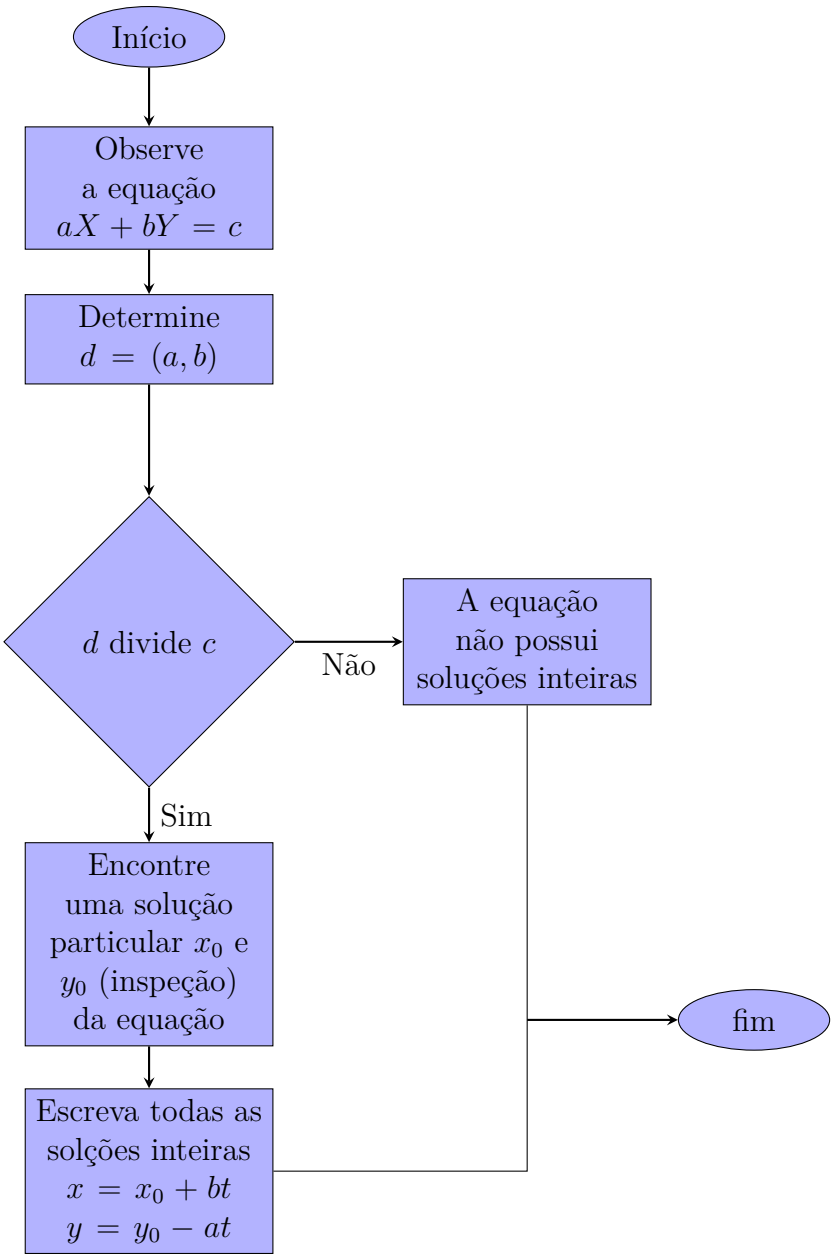


Figura 4.4: Fluxograma de autoria própria - Equações diofantinas lineares (Inspeção)

Caso seja difícil encontrar soluções particulares por inspeção, elas ainda podem ser obtidas com uso de algumas técnicas. Da definição de máximo divisor comum (mdc) temos que existem números inteiros m e n, tais que

$$ma + nb = (a, b) = 1.$$

Multiplicando por c temos

$$c.ma + c.nb = c,$$

assim $x_0 = cm$ e $y_0 = cn$ é uma solução particular da $aX + bY = c$.

Vamos sintetizar esse método com ajuda de um fluxograma.

Exemplo 4.5. Fluxograma - Equações diofantinas lineares - Máximo divisor comum

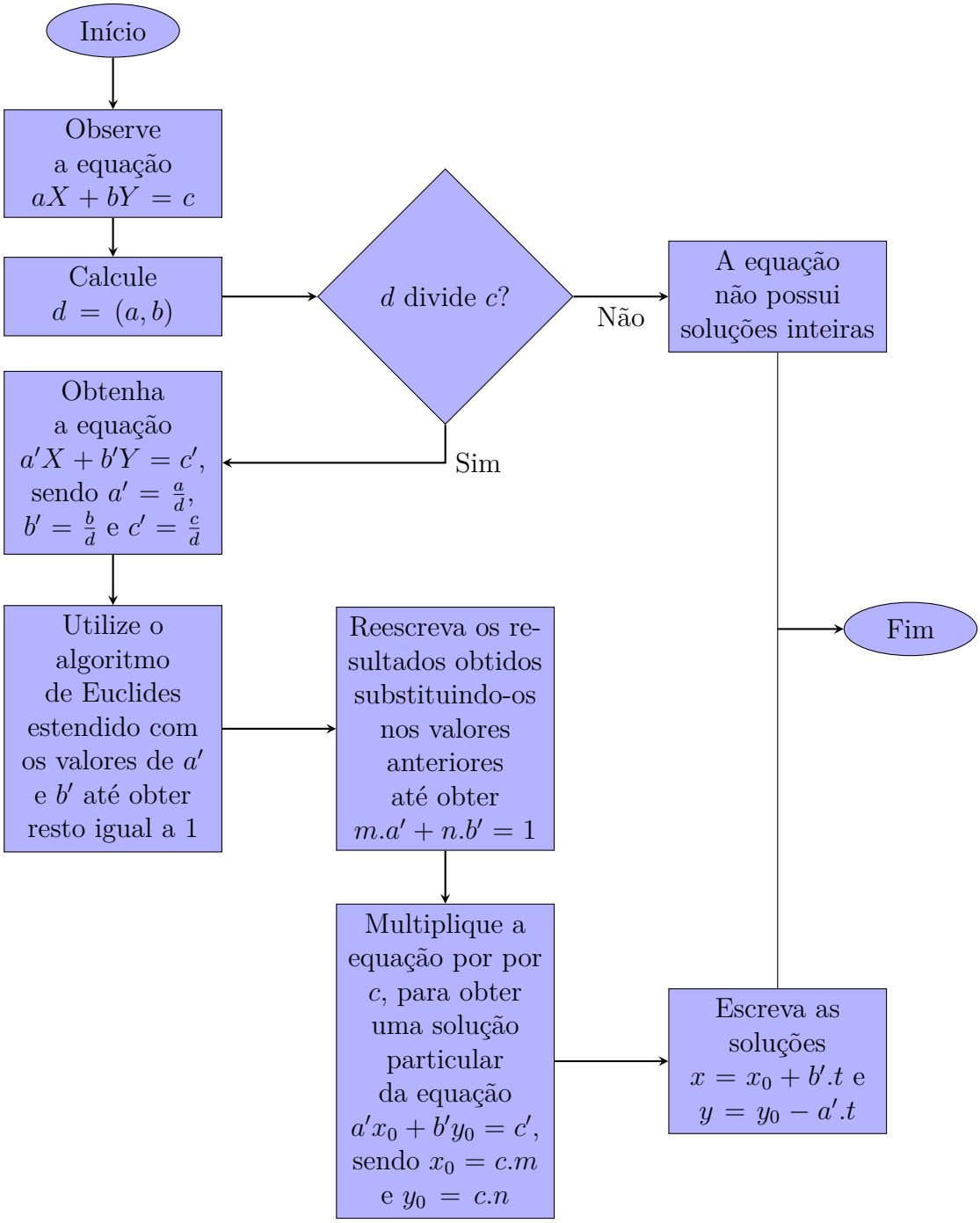


Figura 4.5: Fluxograma de autoria própria - Equações diofantinas lineares (mdc)

Outro importante e fundamental conceito quando se trata de divisibilidade é saber se um número é primo ou composto.

Um número natural maior que 1, que só possui como divisores positivos 1 e ele próprio, é chamado **primo**. Pelo **teorema fundamental da aritmética**, todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

Dados dois números primos p e q e um inteiro a qualquer, sabemos que:

i se $p \mid q$, então $p = q$.

ii Se $p \nmid a$ então o máximo divisor comum de p e a é 1.

iii Se um número natural não é primo, então ele é chamado de **composto**.

iv *Lema de Euclides* - Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.

v *Teorema Fundamental da Aritmética* - Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de números primos.

vi Dado um número inteiro n diferente de -1, 0 e 1, existem primos $p_1 < p_2 < \ldots < p_r \in \mathbb{Z}$, univocamente determinados, tais que

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}.$$

vii Se n' e um divisor de $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, então $n' = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ com $\beta_i \leq \alpha_i$.

vii Denotando por $d(n)$ o número de divisores positivos de um número natural $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, então

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_r + 1).$$

ix Sejam $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ e $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}$, sendo $\gamma_i = min\{\alpha_i, \beta_i\}$ e $\delta_i = max\{\alpha_i, \beta_i\}$, então

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_n^{\gamma_n} \quad \text{e} \quad [a, b] = p_1^{\delta_1} p_2^{\delta_2} \ldots p_n^{\delta_n}.$$

x *Teste de primalidade* - Se um número natural $n > 1$ não é divisível por nenhum número primo, tal que $p^2 \leq n$, então ele é primo.

Todos os itens foram devidamente provados no capítulo de divisibilidade deste trabalho, vamos então utilizá-los para construir fluxogramas relacionados aos itens acima.

No item v temos a decomposição em fatores primos, que consiste em fazer sucessivas divisões por números primos, como mencionado ela é única, a menos da ordem dos fatores. Assim seja n um número inteiro, basta efetuar divisões exatas utilizando-se apenas de números primos. No item *vii* podemos encontrar a quantidade de divisores que um número inteiro possui através de sua decomposição em fatores primos. Mas para isso precisamos primeiramente saber quem são esses fatores primos, então começaremos pelo teste de primalidade.

Para números não muito grandes, podemos utilizar o crivo de Eratóstenes, que consiste em eliminar os múltiplos de um número primo, começando pelo 2 e repetir o processo para os demais números primos. Mas até quando devemos testar o crivo para garantir a primalidade de um número? É isso que nos mostra o item x. Por exemplo, se queremos saber quem são os números primos menores que 100 devemos aplicar o crivo até um número primo p desde $p^2 < 100$, ou seja $p < \sqrt{100} = 10$.

Exemplo 4.6. Fluxograma - Crivo de Eratóstenes

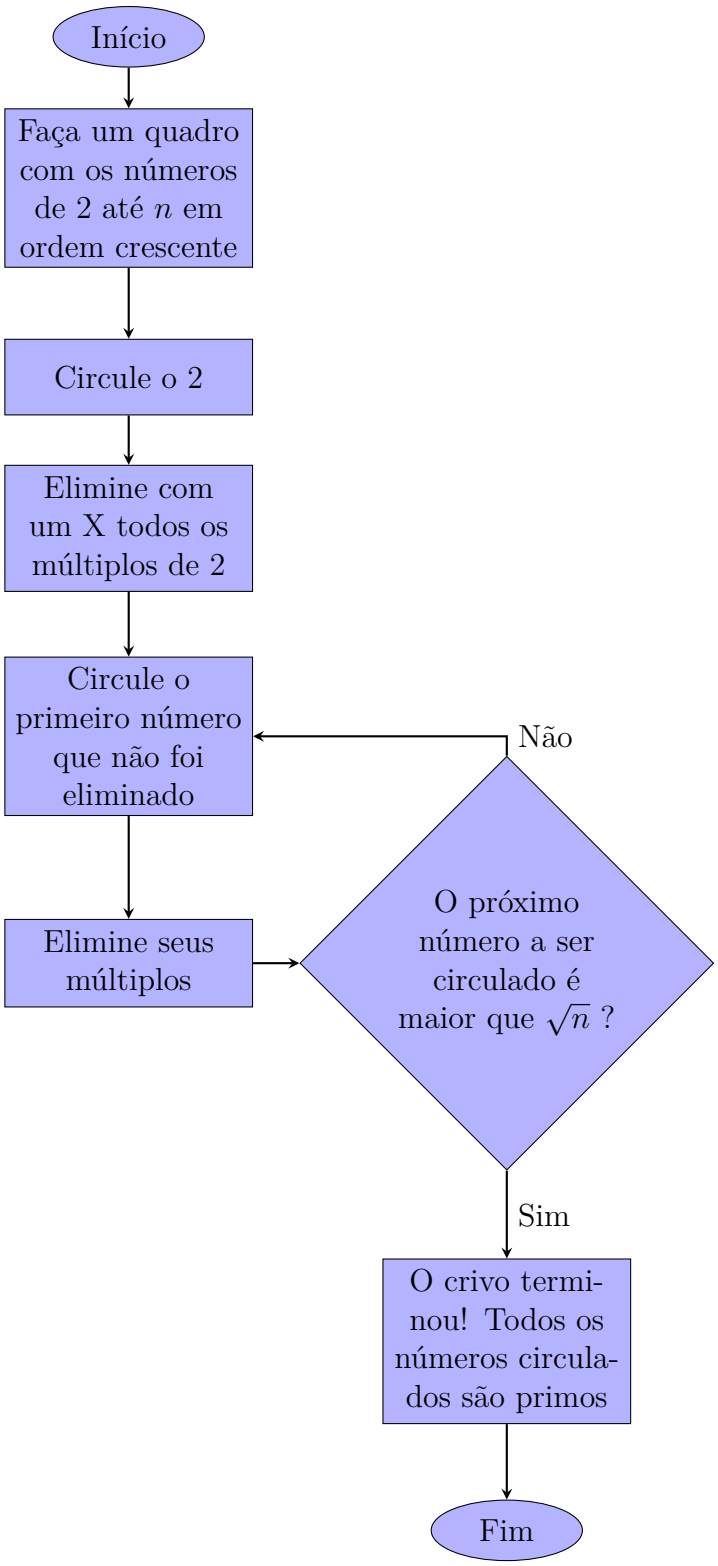


Figura 4.6: Fluxograma de autoria própria - Crivo de Eratóstenes

Podemos também aplicar a divisão euclidiana para determinar a primalidade de um número inteiro, pois caso ele seja muito grande, o crivo de Eratóstenes se tornará um trabalho demorado. Para isso basta efetuar a divisão desse número pelos primos menores que ele, até obter um quociente menor ou igual ao divisor. Se nenhuma das divisões for

exata esse número é primo, caso contrário é composto. Note que pela divisão euclidiana

$$n = p.q + r \Rightarrow p = \frac{(n-r)}{q} \Rightarrow p^2 = p.\frac{(n-r)}{q} = \frac{p.(pq)}{q} \Rightarrow p^2 \leq n.$$

Exemplo 4.7. Divisão euclidiana - Teste de primalidade

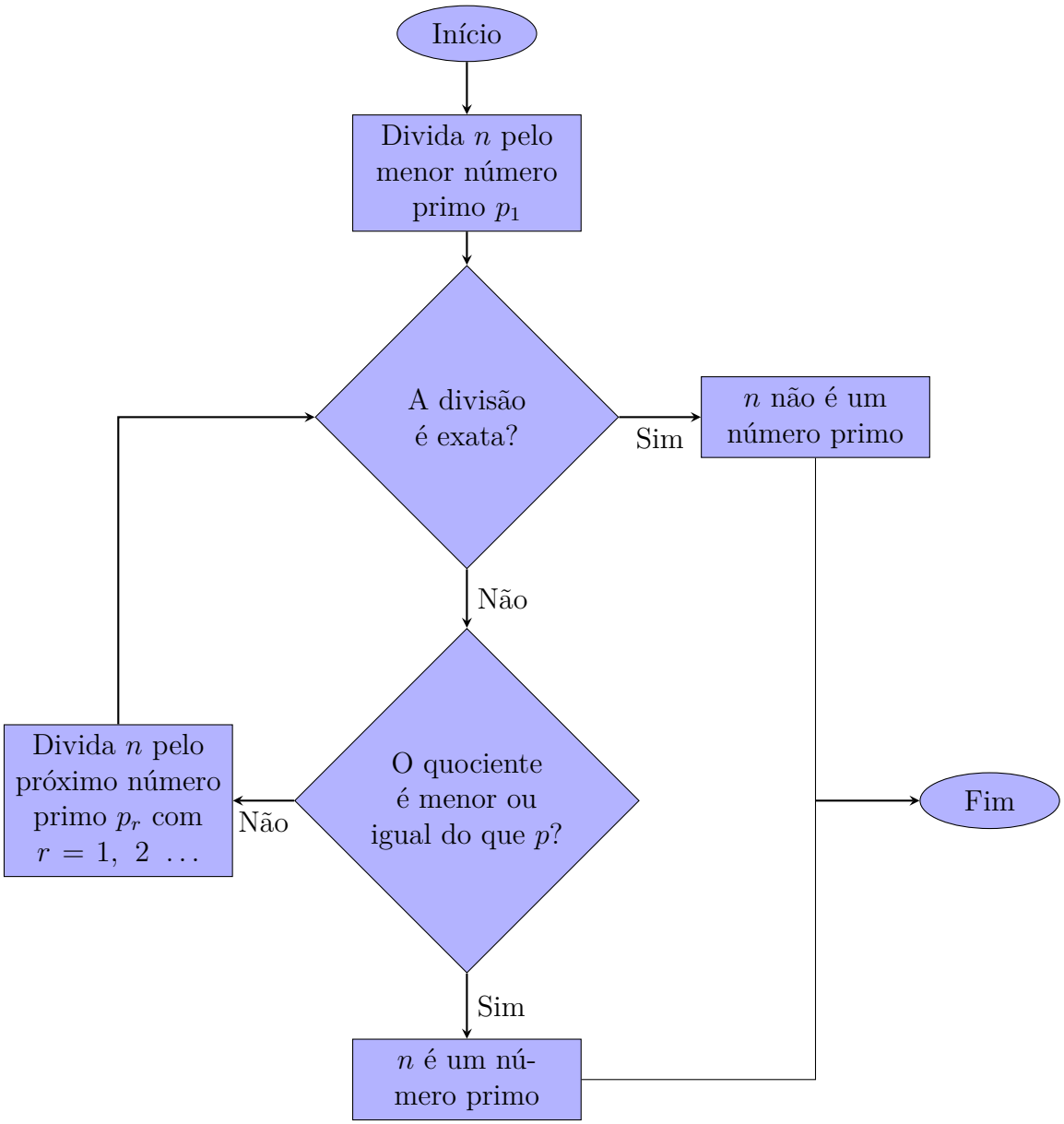


Figura 4.7: Fluxograma de autoria própria - Teste de primalidade (Divisão euclidiana)

Podemos afirmar se tratar do mesmo método, assim os dois podem ser aplicados, a divisão euclidiana é mais interessante quando precisamos apenas testar a primalidade do número, já o crivo nos dá uma lista de primos.

5 Congruências Lineares

Muitas vezes, quando falamos de divisão, não damos a devida importância ao resto, pois o próprio nome faz referência a uma sobra! Mas por trás do resto está um importante resultado, as **congruências**, que nos ajudam a resolver problemas matemáticos, principalmente quando se trata de padrões de repetições e sequências. Muitas dessas questões estão presentes em Olimpíadas de Matemática, porém não são muito trabalhadas em sala de aula.

Neste capítulo traremos a teoria matemática que envolve as congruências, como também fluxogramas, ele teve como base para sua escrita o livro Aritmética da Coleção PROFMAT-SBM. [25]

5.1 Aritmética dos restos

A aritmética dos restos, como eram chamados os estudos de congruências, foi introduzida por *Gauss* em seu livro *Disquisitiones Arithmeticae*, de 1081.

Vamos a definição!

Seja m um número natural, diremos que dois inteiros a e b são *congruentes módulo* m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \bmod m.$$

Quando essa relação for falsa, ou seja os restos da divisão de a e b por m forem diferentes, diremos que a e b *não são congruentes módulo* m, ou *são incongruentes módulo* m, e escreveremos $a \not\equiv b \bmod m$.

Como o resto da divisão por 1 é sempre zero, temos que $a \equiv b \bmod 1$, para quaisquer números inteiros a e b. Portanto consideraremos $m > 1$.

Da definição de congruência módulo um inteiro fixado m, é uma relação de equivalência, o que nos mostra a seguinte proposição.

Proposição 5.1. *Seja $m \in \mathbb{N}$. Para todos $a, b, c \in \mathbb{Z}$, tem-se que*

i Reflexiva : $a \equiv a \bmod m$,

ii Comutativa : $a \equiv b \bmod m$, então $b \equiv a \bmod m$,

iii Transitiva : $a \equiv b \bmod m$, e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Não precisamos efetuar a divisão euclidiana para saber se dois números são congruentes módulo m, é suficiente aplicar o resultado da seguinte proposição:

Proposição 5.2. *Suponha $a, b, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a \equiv b \mod m$, se, e somente se, $m \mid b - a$.*

Demonstração. Sejam $a = mq + r$, com $0 \leq r < m$ e $b = mq' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, logo

$$b - a = m(q' - q) + (r' - r).$$

Assim $a \equiv b \bmod m$ se, e somente se, $r - r' = 0 \Rightarrow r = r'$, ou seja, $b - a = m(q' - q)$ que é equivalente a dizer que $m \mid b - a$. □

Perceba que todo número inteiro é congruente módulo m ao seu resto da divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $0,\ 1,\ \ldots,\ m-1$. Além disso, tomando dois a dois quaisquer números desse grupo, ele serão incongruentes módulo m.

Diremos ter um *sistema completo de resíduos* módulo m a todo conjunto de números inteiros cujos restos pela divisão euclidiana por m são os números $0,\ 1,\ \ldots,\ m-1$, sem repetições e em ordem qualquer. Portanto esse conjunto possuirá m elementos. Particularmente um conjunto formado por m números inteiros consecutivos é um sistema completo de resíduos módulo m.

Seja R esse sistema, então pela divisão euclidiana por m pode ser generalizado da seguinte forma:

Para todo $a \in \mathbb{Z}$ existem inteiros q e r univocamente determinados tais que $a = mq+r$, com $r \in R$, diremos se tratar de uma divisão com resto no conjunto R. Por se tratar de uma divisão euclidiana temos que $R = \{0, 1, \ldots, m-1\}$.

Tomando

$$R = \{r \in \mathbb{Z};\ -\frac{m}{2} \leq r < \frac{m}{2}\},$$

que é um conjunto de m inteiros consecutivos ($\frac{m}{2} - \frac{-m}{2} = m$), a correspondente divisão será chamada de *divisão com menor resto.*

A grande utilidade da noção de congruência é se tratar de uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros.

Proposição 5.3. *Seja $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$.*

i Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $a + c \equiv b + d \mod m$.

ii Se $a \equiv b \mod m$ e $c \equiv d \mod m$, então $ac \equiv bd \mod m$.

Demonstração. Suponha que $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$.

Para provar o item i, temos que $m \mid (b - a) + (d - c) = (d + b) - (a + c)$ (Proposição 3.23), o que acarreta que $a + c \equiv b + d \bmod m$.

Para o item ii, basta verificar que $bd - ac = d(b - a) + a(d - c)$, concluímos então que $m \mid bd - ac$, ou seja $ac \equiv bd \bmod m$.

□

Dessa proposição podemos tirar o seguinte resultado:

Corolário 5.4. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b \mod m$, então tem-se que $a^n \equiv b^n \mod m$.*

Demonstração. Faremos por indução sobre n.

Sabemos que se $a \equiv b \bmod m$, então $m \mid b^1 - a^1$. Vamos supor que $m \mid b^n - a^n$, e vamos provar que $m \mid b^{n+1} - a^{n+1}$.

$$m \mid b^{n+1} - a^{n+1} \Rightarrow m \mid b.b^n - a.a^n \Rightarrow m \mid b.b^n + ba^n - ba^n - a.a^n \Rightarrow m \mid b(b^n - a^n) + a^n(b-a)$$

Portanto $m \mid b^n - a^n$, logo $a^n \equiv b^n \bmod m$.

□

5.1.1 Pequeno teorema de Fermat

Com a notação de congruência podemos enunciar o seguinte resultado chamado de *Pequeno Teorema de Fermat*, atribuído ao matemático amador Pierre de Fermat. Apesar de ter ficado conhecido como pequeno, esse teorema é de grande valia, teria recebido esse nome por causa de sua demonstração ser bem simples, ou seja, pequena.

Se p é um número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \bmod m.$$

Além disso, se $p \nmid a$ então

$$a^{p-1} \equiv 1 \bmod m,$$

pois, se p é um número primo $p \mid a^p - a \Rightarrow p \mid a(a^{p-1} - 1)$.

Podemos também obter o seguinte resultado:

Se p é um número primo e a e b números inteiros temos que

$$(a \pm b)^p \equiv a^p \pm b^p \bmod m.$$

Pelo pequeno teorema de Fermat sabemos que $(a \pm b)^p \equiv a \pm b \equiv a^p \pm b^p \bmod m$.

Como consequência dos resultados anteriores, se tivermos $a_1,\ a_2, \ldots, a_r \in \mathbb{Z}$ e p primo, então

$$(a_1 + a_2 + \Rightarrow + a_r)^p \equiv (a_1^p + a_2^p + \ldots + a_r^p) \bmod m.$$

Mostraremos agora que vale o cancelamento com relação a adição nas congruências.

Proposição 5.5. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que*

$$a + c \equiv b + c \ mod\, m \Rightarrow a \equiv b \ mod\, m.$$

Demonstração. Se $a \equiv b \bmod m$, então $a + c \equiv b + c \bmod m$ pois $c \equiv c \bmod m$.

Reciprocamente, se $a + c \equiv b + c \bmod m$, então $m \mid (b + c) - (a + c)$, ou seja $m \mid b - a$, portanto $a \equiv b \bmod m$.

□

Porém o cancelamento em relação a multiplicação nem sempre é válido, a proposição a seguir nos dará a condição necessária para o cancelamento de um fator nas congruências.

Proposição 5.6. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$. Temos que*

$$ac \equiv bc \ mod\, m \Leftrightarrow a \equiv b \ mod\, \frac{m}{(c, m)}.$$

Demonstração. Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são coprimos, ou seja $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1$, temos que

$$ac \equiv bc \bmod m \Leftrightarrow m \mid (b-a)c \Leftrightarrow \frac{m}{(c,m)} \mid (b-a)\frac{c}{(c,m)}$$

$$\Leftrightarrow \frac{m}{(c,m)} \mid b-a \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}.$$

□

De mão desta proposição, temos o seguinte corolário:

Corolário 5.7. *Sejam $a, b, c, m \in \mathbb{Z}$ com $m > 1$ e $(c, m) = 1$. Temos que*

$$ac \equiv bc \ mod\, m \Leftrightarrow a \equiv b \ mod\, m.$$

Traremos agora algumas propriedades adicionais das congruências.

Proposição 5.8. *Sejam $a, b \in \mathbb{Z}$ e $m, n, m_1, m_2, \ldots, m_r$ inteiros maiores do que 1. Temos que*

i se $a \equiv b \ mod\, m$ e $n \mid m$, então $a \equiv b \ mod\, n$;

ii se $a \equiv b \ mod\, m_i$, $\forall i = 1, \ldots, r \Leftrightarrow a \equiv b \ mod\, [m_1, \ldots, m_r]$;

iii se $a \equiv b \ mod\, m$, então $(a, m) = (b, m)$.

Demonstração. Se $a \equiv b \bmod m$, então $m \mid b - a$. Como $n \mid m \Rightarrow n \mid b - a$, ou seja, $a \equiv b \bmod n$.

Se $a \equiv b \bmod m_i$, $\forall i = 1, \ldots, r$, então $m_i \mid b - a$, $\forall i$. Sendo $b - a$ um múltiplo de m_i, temos que $[m_1, \ldots, m_r] \mid b - a$, ou seja $a \equiv b \bmod [m_i, \ldots, m_r]$. A recíproca decorre do item i.

Se $a \equiv b \bmod m$, então $m \mid b - a$, portanto, $b = a + tm$ com $t \in \mathbb{Z}$. Logo pela propriedade do máximo divisor comum, temos

$$(a, m) = (a + tm, m) = (b, m).$$

□

5.1.2 Teorema de Euler

O teorema de Euler é uma generalização do pequeno teorema de Fermat. Esse teorema e suas consequências são de grande importância para o estudo de *criptografia*.

No que se segue, será um facilitador nos cálculos, saber determinar a congruência $aX \equiv 1 \bmod m$, e também verificar se ela possui solução em X. Precisaremos para isso do seguinte resultado:

Proposição 5.9. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \ mod\, m$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x é uma solução da congruência se, e somente se, $x \equiv x_0 \ mod\, m$.*

Demonstração. A congruência $ax_0 \equiv 1 \bmod m$ tem solução se, e somente se, $m \mid ax_0 - 1$, o que é equivalente a escrever $aX - mY = 1$, que já sabemos possuir solução única nos inteiros se, e somente se, $(a, m) = 1$.

Por outro lado, se x_0 e x são soluções da congruência $aX \equiv 1 \bmod m$, então $ax \equiv ax_0 \bmod m$ e $(a, m) = 1$ o que implica $\frac{ax}{(a,m)} \equiv \frac{ax_0}{(a,m)} \bmod \frac{m}{(a,m)} \Rightarrow x \equiv x_0 \bmod m$.

Note que, se x_0 é solução da congruência $aX \equiv 1 \bmod m$, e $x \equiv x_0 \bmod m$, então x é também solução da congruência, pois

$$ax \equiv ax_0 \equiv 1 \bmod m.$$

□

Uma solução da congruência $aX \equiv 1 \bmod m$ determina e é determinada por qualquer outra solução, considerando que duas soluções módulo m são a mesma, temos então sua unicidade.

Um *sistema reduzido de resíduos* módulo m é um conjunto de inteiros $r_1, \ldots, r_s$, tais que

a) $(r_i, m) = 1$, para todo $i = 1, \ldots, s$;

b) $r_i \not\equiv r_j \bmod m$, se $i \neq j$;

c) Para cada $n \in \mathbb{Z}$ tal que $(m, n) = 1$, existe i tal que $n \equiv r_i \bmod m$.

Podemos então obter um sistema reduzido de resíduos módulo m, eliminando os elementos que não são primos com m.

Por exemplo se $m = 4$ temos $r_i = \{0, 1, 2, 3\}$ é um sistema completo de resíduos módulo 4, mas como $(0, 4) = 4$ e $(2, 4) = 2$, temos $r_i = \{1, 3\}$ é um sistema reduzido de resíduos módulo 4.

Função fi de Euler ($\varphi(m)$)

Tomaremos por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde a quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Pondo $\varphi(1) = 1$, isso define um função muito importante

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N},$$

chamada, *função fi de Euler*.

Pela definição

$$\varphi(m) \leq m - 1, \ \forall\, m \geq 2.$$

Além disso, se $m \geq 2$, então $\varphi(m) = m - 1$ se, e somente se, m é um número primo, pois possui apenas 1 e m como seus divisores. Logo se $1, 2, \ldots, m-1$ formam um sistema de resíduos módulo m, temos $m - 1$ elementos nesse conjunto. Essa função tem grande utilidade em Teoria dos Números.

Antes de enunciar o teorema de Euler, vamos precisar do seguinte resultado:

Proposição 5.10. *Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. Então $ar_1, \ldots, ar_{\varphi(m)}$ é um sistema reduzido de resíduos módulo m.*

Omitiremos a demostração da proposição por não ser de importância ao propósito deste capítulo, o leitor que se interessar pode procurar demostrá-la, ou pode consultar um livro de aritmética.

Vamos enfim enunciar o teorema atribuído a Euler.

Teorema 5.11. *Teorema de Euler*
Sejam $a, m \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então,

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

Demonstração. Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m, assim pela proposição anterior $ar_1, \ldots, ar_{\varphi(m)}$ também é um sistema reduzido de resíduos módulo m e, portanto,

$$ar_1.ar_2. \ \ldots \ .ar_{\varphi(m)} \equiv r_1.r_2. \ \ldots \ .r_{\varphi(m)} \bmod m.$$

Pois,

$$a^{\varphi(m)} r_1.r_2. \ \ldots \ .r_{\varphi(m)} \equiv ar_1.ar_2. \ \ldots \ .ar_{\varphi(m)} \equiv r_1.r_2. \ \ldots \ .r_{\varphi(m)} \bmod m.$$

Como $(r_1 r_2. \ \ldots \ r_{\varphi(m)}, m) = 1$ e segue-se que vale o cancelamento com relação a multiplicação, logo

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

□

Desse resultado juntamente com o teorema atribuído a Fermat, podemos tirar o seguinte corolário:

Corolário 5.12. *Pequeno Teorema de Fermat*
Sejam $a \in \mathbb{Z}$ e p um número primo tais que $(a, m) = 1$. Tem-se que

$$a^{p-1} \equiv 1 \ mod\, p.$$

Demonstração. De mão do resultado anterior, basta tomar $\varphi(p) = p - 1$, pois p é um número primo. □

A proposição enunciada a seguir, nos trará uma maneira facilitada de calcular o valor da função fi de Euler. Não faremos sua demostração, pois estamos interessados apenas em sua aplicação.

Proposição 5.13. *Sejam $m, m' \in \mathbb{N}$ tais que $(m, m') = 1$. Então*

$$\varphi(m, m') = \varphi(m)\varphi(m').$$

Outro interessante resultado que podemos tirar dos já vistos é o seguinte corolário:

Corolário 5.14. *Seja m um inteiro **livre de quadrados**, então para todo $a \in \mathbb{Z}$ e todo $k \in \mathbb{N}$ tem-se que*

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

Demonstração. Vamos escrever m em sua decomposição em fatores primos, todos distintos, assim $m = p_1 p_2 \ldots p_r$. Como $\varphi(m) = \varphi(p_1)\varphi(p_2)\ldots\varphi(p_r) = (p_1-1)(p_2-1)\ldots(p_r-1)$, e sendo

$$k_i = k(p_1 - 1)(p_2 - 1)\ldots(p_r - 1),$$

tem-se que, para todo $a \in \mathbb{Z}$, todo $k \in \mathbb{N}$ e todo $i = 1, \ldots, r$, que

$$a^{k\varphi(m)+1} = a^{k_i(p_i-1)+1} \equiv a \bmod p_i \equiv a \bmod [p_1, p_2, \ldots, p_r],$$

como $[p_1, p_2, \ldots, p_r] = p_1.p_2. \ \ldots \ .p_r = m$, fica provado o resultado.

□

Precisaremos de mais um resultado para conseguir obter uma fórmula para o cálculo da função fi de Euler.

Proposição 5.15. *Se p é um número primo e r, um número natural, então tem-se que*

$$\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right).$$

Demonstração. De 1 até p^r, temos p^r números naturais. Temos que excluir, desses números, os que não são primos com p^r, ou seja, todos os múltiplos de p, são eles $p, 2p, \ldots\ p^{r-1}p$, que são em quantidade de p^{r-1}. Assim $\varphi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$. □

O próximo resultado formalizará a maneira de obter o valor da função fi de Euler.

Teorema 5.16. *Seja $m > 1$ e $m = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$ a decomposição de m em fatores primos. Então,*

$$\varphi(m) = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_n}\right).$$

Que pode ser escrita também na seguinte forma

$$\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}) = p_1^{\alpha_1-1}p_2^{\alpha_2-1}\ldots p_n^{\alpha_n-1}(p_1-1)(p_2-1)\ldots(p_n-1).$$

Demonstração. A demonstração decorre da função fi de Euler ser distributiva com relação ao produto dos fatores primos da decomposição de m e da aplicação da proposição acima. □

Teorema de Wilson

Outro resultado interessante que podemos extrair das congruência é o teorema de Wilson, mas que foi provado por Lagrange.

Teorema 5.17. *Teorema de Wilson*
Se p é um número primo, então

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

Demonstração. Note que é fácil verificar a validade do teorema para $p = 2$ e $p = 3$. Suponhamos então $p \geq 5$ primo. Para todo $i = \{1, \ldots, p\}$, sabemos que a congruência $i \equiv 1 \bmod p$ possui solução única módulo p, pois $(i, p) = 1$, ou seja, dado $i \in \{1, \ldots, p-1\}$ existe um único $j \in \{1, \ldots, p-1\}$ tal que $ij \equiv 1 \bmod p$. Agora, se $i = \{1, \ldots, p\}$ é tal que $i^2 \equiv 1 \bmod p$, então $p \mid i^2 - 1$, que é equivalente a dizer que $p \mid i - 1$ ou $p \mid i + 1$, e como p é um número primo só poderá ocorrer se $i = 1$ ou $i = p - 1$. Logo

$$2\ldots(p-2) \equiv 1 \bmod p,$$

e portanto

$$1.2\ldots(p-2)(p-1) \equiv 1.1.(p-1) \equiv p - 1 \equiv -1 \bmod p.$$

□

Vale a recíproca desse teorema, ou seja se $(p-1)! \equiv -1 \bmod p$ então p é primo. Podemos então utilizar desse teorema como um teste de primalidade.

Desse interessante teorema deriva outro resultado, que pode ser utilizado como um facilitador nos cálculos de congruências.

Teorema 5.18. *Sejam p um número primo e $m, n \in \mathbb{N} \cup \{0\}$ tais que $m+n = p-1$. Tem-se que*

$$m!n! \equiv (-1)^{n+1} \bmod p.$$

Demonstração. Seja $0 \leq n \leq p-1$. Temos que

$$(p-n)(p-(n+1)) \ldots (p-2)(p-1) \equiv (-1)^n n! \bmod p.$$

Pondo $m = p-1-n$, temos que

$$(p-1)! = 1.2 \ldots (p-1-n)(p-n) \ldots (p-2)(p-1) \equiv m!(-1)^n n! \bmod p.$$

Pelo teorema de Wilson temos que $(p-1)! \equiv -1 \bmod p$, assim

$$m!(-1)^n n! \equiv -1 \bmod p.$$

Agora como $(p, (-1)^n) = 1$ temos $m!n! \equiv -1(-1)^n = (-1)^{n+1} \bmod p$ o que prova o teorema.

□

5.1.3 Sistemas de Congruências

As congruências lineares são definidas a partir do resto que deixam em uma divisão de números inteiros. Pela divisão euclidiana temos que na divisão de a por m obtemos $a = m.q + b$ com $0 \leq b < m$, sendo $a, b, m \in \mathbb{Z}$. Podemos reescrever essa mesma operação com foco no resto, em forma de congruência linear,

$$aX \equiv b \bmod m,$$

onde $a, b, m \in \mathbb{Z}$, com $m > 1$.

Primeiramente daremos um critério para a existência de solução para uma congruência linear.

Proposição 5.19. *Dados $a, b, m \in \mathbb{Z}$, com $m > 1$, a congruência linear*

$$aX \equiv b \bmod m$$

possui solução se, e somente se, $(a, m) \mid b$.

Demonstração. Suponhamos que $x \in \mathbb{Z}$ seja a solução da congruência $aX \equiv b \bmod m$, logo temos que $m \mid (a.x - b)$, o que é equivalente a existência de um $y \in \mathbb{Z}$ tal que $ax - b = m.y$. Temos então que $aX - mY = b$ admite solução, o que implica $(a, m) \mid b$, pois é condição necessária para que essa equação diofantina possua solução no conjunto dos números inteiros, como demonstrado neste mesmo trabalho na seção de Equações Diofantinas no capítulo de Divisibilidade.

Agora suponha que $(a, m) \mid b$. Logo a equação diofantina $aX - mY = b$ admite pelo menos uma solução $x, y \in \mathbb{Z}$, então $ax = b + my$, o que nos leva a ter que x é solução da congruência $ax \equiv b \bmod m$. □

Note que se x_0 é uma solução da congruência $aX \equiv b \bmod m$, então todo x tal que $x \equiv x_0 \bmod m$ também é uma solução, pois

$$ax \equiv ax_0 \equiv c \bmod m.$$

Ou seja, toda solução particular determina uma infinidade de soluções da congruência, entretanto serão consideradas como uma só (módulo m), pois são congruentes entre si, e portanto, se determinam mutualmente.

Podemos determinar uma coleção completa de soluções duas a duas incongruentes módulo m, as quais chamaremos de *sistema completo de soluções incongruentes* da congruência. Ou seja, todas as classes residuais de uma congruência.

Teorema 5.20. *Sejam $a, b, m \in \mathbb{Z}$, com $m > 1$ e $(a, m) \mid b$. Se x_0 é uma solução da congruência $aX \equiv b \bmod m$, então*

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d}, \ldots, x_0 + (d-1)\frac{m}{d},$$

onde $d = (a, m)$, formam um sistema completo de soluções da congruência, duas a duas incongruentes módulo m.

Demonstração. Toda solução x da congruência $aX \equiv b \bmod m$ é congruente, módulo m, a $x_0 + i\frac{m}{d}$ para algum $0 \leq i < d$. Como

$$ax \equiv ax_0 \bmod m,$$

podemos dividir a congruência por $d = (a, m)$, obtendo

$$x \equiv x_0 \bmod \frac{m}{(a,m)} = x_0 \bmod \frac{m}{d}.$$

Logo $x - x_0 = k\frac{m}{d}$. Pela divisão euclidiana, existe $0 \leq i < d$ tal que $k = qd + i$, e portanto,

$$x = x_0 + qm + i\frac{m}{d} \equiv x_0 + i\frac{m}{d} \bmod m.$$

Agora, sendo os números $x_0 + i\frac{m}{d}$, com $0 \leq i < d$, soluções da congruência, pois

$$a\left(x_0 + i\frac{m}{d}\right) = ax_0 + i\frac{a}{d}m \equiv ax_0 \equiv b \bmod m.$$

Por fim, esses números são dois a dois incongruentes módulo m, pois se, para $0 \leq i, j < d$,

$$x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \bmod b \ \Rightarrow\ i\frac{m}{d} \equiv j\frac{m}{d} \bmod m.$$

Como $0 \leq i, j < d$, então $0 \leq i\frac{m}{d}, j\frac{m}{d} < m$, e como m divide $\mid i\frac{m}{d} - j\frac{m}{d} \mid$, temos que $i\frac{m}{d} = j\frac{m}{d}$ e portanto $i = j$.

□

Corolário 5.21. *Se $(a, m) = 1$, então a congruência $aX \equiv b \bmod m$ possui uma única solução módulo m.*

A congruência $aX \equiv 1 \bmod m$, com $(a, m) = 1$, admite uma única solução módulo m. Está solução será chamada de *inverso multiplicativo módulo m.*

Corolário 5.22. *Sejam $m > 1$ e R' um conjunto reduzido de resíduos módulo m. Se $b \in \mathbb{Z}$, então para todo $r \in R'$, a congruência $rX \equiv b \bmod m$ possui uma única solução módulo m em R'.*

Demonstração. Como $r \in R'$, temos que $(r, m) = 1$, logo a congruência tem uma única solução módulo m. Toda solução $x \in \mathbb{Z}$ é tal que $(x, m) = 1$, logo tem um único representante módulo m no conjunto R'. □

É impostante notar que a congruência $aX \equiv b \bmod m$ que possui solução é equivalente a uma congruência da forma

$$X \equiv c \bmod n.$$

Pois, se $aX \equiv b \bmod m$ possui solução, então $d = (a, m)$ divide b. Assim pondo $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $n = \frac{m}{d}$, obtemos a seguinte congruência

$$a'X \equiv b' \bmod n, \quad \text{com } (a', n) = 1.$$

Agora sendo a'' o inverso multiplicativo a' módulo n, sabemos que

$$a'a'' \equiv 1 \bmod n \;\Rightarrow\; a'a''X \equiv a''b \bmod n \;\Rightarrow\; X \equiv c \bmod n,$$

com $c = a''b$.

As congruências $aX \equiv b \bmod m$ que possuem valor de m pequeno, muita vezes são fáceis de resolver, podendo ser feita por inspeção. Assim fazer uso da propriedade descrita acima, pode nos ajudar a diminuir o valor do módulo.

Teorema Chinês dos restos

Há muitos anos atrás, o matemático chinês *Sun-Tsu* fez a seguinte indagação:

Qual é o número que deixa resto 2,3 e 2 quando dividido, respectivamente, por 3,5 e 7?

O qual foi dada a resposta 23.

Podemos reescrever esse problema fazendo uso das congruências:

$$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \\ X \equiv 2 \bmod 7 \end{cases}$$

De maneira geral, estudaremos sistemas de congruências da forma

$$a_iX \equiv b_i \bmod m_i \;\; i = 1, \ldots, r.$$

Para que haja solução, é necessário assegurar que $(a_i, m_i) \mid b_i$ para todo $i = 1, \ldots, r$, assim os sistema acima é equivalente a

$$X \equiv c_i \bmod n_i, \quad i = 1, \ldots, r.$$

Com esses resultados podemos enunciar o seguinte teorema:

Teorema 5.23. *Se $(n_i, n_j) = 1$, para todo par n_i, n_j com $i \neq j$, então o sistema $X \equiv c_i \bmod n_i$, com $i = 1, \ldots, r$ possui uma única solução módulo $N = n_1n_2 \ldots n_r$. As soluções são*

$$x = N_1y_1c_1 + \ldots + N_ry_rc_r + tN,$$

onde $t \in \mathbb{Z}$, $N_i = N/n_i$ e y_i é solução de $N_iY \equiv 1 \bmod n_i$ para $i = 1, \ldots, r$.

Demonstração. Primeiramente, vamos mostrar que x é uma solução simultânea do sistema $X \equiv c_i \bmod n_i$ para $i = 1, \ldots, r$. De fato, com $n_i \mid N_j$, se $i \neq j$, e $N_i y_i \equiv 1 \bmod n_i$, segue-se que

$$x = N_1 y_1 c_1 + \ldots + N_r y_r c_r \equiv N_i y_i c_i \equiv c_i \bmod; n_i.$$

Por outro lado, se x' também é solução do mesmo sistema de congruências, então

$$x \equiv x' \bmod n_i, \quad \forall i = 1, \ldots, r.$$

Como $(n_i, n_j) = 1$, para $i \neq j$, segue-se que $[n_1, \ldots, n_r] = N$ e, consequentemente,

$$x \equiv x' \bmod n_i \Rightarrow x \equiv x' \bmod N.$$

□

Vamos a alguns exemplos.

Exemplo 5.24. Uma pessoa ao subir uma escada de 2 em 2 degraus, precisará subir mais um degrau para chegar ao final da escada. Se ela subir de 3 em 3 degraus, faltará 2 degraus para chegar ao fim da escada. Caso suba de 5 em 5 degraus, faltará 3 degraus para chegar ao fim da escada. Sabe-se que essa escada tem entre 150 e 200 degraus. Quantos degraus tem a essa escada?

Podemos reescrever esse problema da seguinte forma

$$\begin{cases} X \equiv 1 \bmod 2 \\ X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \end{cases}$$

onde X é a quantidade de degraus da escada. Vamos então resolver esse sistema de congruências lineares.

Primeiramente note que $(2, 3, 5) = 1$, assim o sistema de equações lineares possui solução única. Vamos então calcular os M_i.

$$M = [2, 3, 5] = 2.3.5 = 30$$
$$M_1 = 30 : 2 = 15, \quad M_2 = 30 : 3 = 10, \quad M_3 = 30 : 5 = 6,$$

agora temos que determinar os inversos multiplicativos

$$\begin{cases} 15.y_1 \equiv 1 \bmod 2 \Rightarrow y_1 = 1, \\ 10.y_2 \equiv 1 \bmod 3 \Rightarrow y_2 = 1, \\ 6.y_3 \equiv 1 \bmod 5 \Rightarrow y_3 = 1, \end{cases}$$

Temos então que

$$15.1.1 + 10.1.2 + 6.3.1 = 15 + 20 + 18 = 53,$$

agora podemos resumir o nosso sistema a uma única congruência

$$X \equiv 53 \bmod 30 \Rightarrow X \equiv 23 \bmod 30.$$

As soluções desse sistema são

$$23 + 30t \text{ com } t \in \mathbb{Z},$$

mas como $150 < 23 + 30t < 200$ temos que $t = 5 \Rightarrow 23 + 30.5 = 173$.

Portanto essa escada possui 173 degraus.

Alguns sistemas de equações são facilmente resolvidos, utilizando a propriedade aditiva das congruências,

$$a \equiv\ b \bmod m \Rightarrow a + c \equiv\ b + c \bmod m.$$

Vamos a mais um exemplo então:

Exemplo 5.25.

$$\begin{cases} X \equiv\ 2 \bmod 3 \\ X \equiv\ 3 \bmod 4 \\ X \equiv\ 4 \bmod 5 \\ X \equiv\ 5 \bmod 6 \end{cases}$$

Vamos reescrever esse sistema utilizando a propriedade aditiva

$$\begin{cases} X + 1 \equiv\ 2 + 1 \bmod 3 \\ X + 1 \equiv\ 3 + 1 \bmod 4 \\ X + 1 \equiv\ 4 + 1 \bmod 5 \\ X + 1 \equiv\ 5 + 1 \bmod 6 \end{cases}$$

$$\begin{cases} X + 1 \equiv\ 0 \bmod 3 \\ X + 1 \equiv\ 0 \bmod 4 \\ X + 1 \equiv\ 0 \bmod 5 \\ X + 1 \equiv\ 0 \bmod 6 \end{cases}$$

Agora, como $[3, 4, 5, 6] = 60$ e $(3, 4, 5, 6) = 1$, o sistema possui solução única

$$X + 1 \equiv\ 0 \bmod 60,$$

ou seja, $x = 59$ e as soluções desse sistema são da forma $59 + 60t$ com $t \in \mathbb{Z}$.

Muitas vezes, o que pode ocorrer é a congruência possuir um valor $\alpha_i \in \mathbb{N}$ com $i = 1, 2, \ldots, n$ multiplicando o valores de N, assim

$$\begin{cases} \alpha_1 N \equiv a_1 \bmod m_1 \\ \alpha_2 N \equiv a_2 \bmod m_2 \\ \qquad\vdots \\ \alpha_n N \equiv a_n \bmod m_n, \end{cases}$$

precisará ser reescrito da seguinte forma

$$\begin{cases} N \equiv a_1.\alpha_1' \bmod m_1 \\ N \equiv a_2.\alpha_2' \bmod m_2 \\ \qquad\vdots \\ N \equiv a_n.\alpha_n' \bmod m_n, \end{cases}$$

sendo α_i' o inverso multiplicativo módulo m_i de α_i, ou seja $\alpha_i.\alpha_i' \equiv 1 \bmod m_i$.

Bastando assim utilizar-se dos dois fluxogramas anteriores para determinar a solução desse sistema de congruências.

Em livros de aritmética, o leitor que desejar se aprofundar no tema, poderá encontrar mais resultados interessantes sobre a aritmética dos restos e as congruências. Como este

trabalho tem finalidade de orientar professores e alunos do Ensino Fundamental - Anos finais, pararemos por aqui.

Na próximo capítulo traremos alguns exemplos de atividades que recaem em identificar um padrão de repetição, ou seja, identificar sequências lógicas. Mostraremos que o estudo da aritmética dos restos deixa esse processo mais simples.

5.2 A aritmética dos restos em forma de fluxograma

Nesta seção construiremos fluxogramas relacionados a aritmética dos restos, principalmente o conceito de congruência. Muitas vezes, mesmos nós professores, encontramos dificuldade em entender as demonstrações e aplicações de determinados conteúdos, pois tantas fórmulas, propriedades e cálculos, podem nos deixar confusos, imagina para o aluno então como é! Assim, vamos trabalhar com os fluxogramas, que nos permitirá ver os resultados de uma maneira mais simples e de fácil aplicação.

Todos os resultados dessa seção já foram devidamente provados nesse capítulo, assim nos apegaremos apenas à utilização dos mesmos.

O primeiro resultado que utilizaremos será o de determinação das soluções (quando existirem) de uma congruência no conjunto dos números inteiros. Para isso utilizaremos a divisão euclidiana.

Queremos determinar a congruência módulo m de um número inteiro a, para isso devemos efetuar a divisão euclidiana de a por m e lembrar que o resto r dessa divisão deve ser menor que m. Pela divisão euclidiana $a = q.m + r$, podemos então reescrever essa equação na forma de congruência, $a \equiv r \mod m$.

Exemplo 5.26. Congruência módulo m

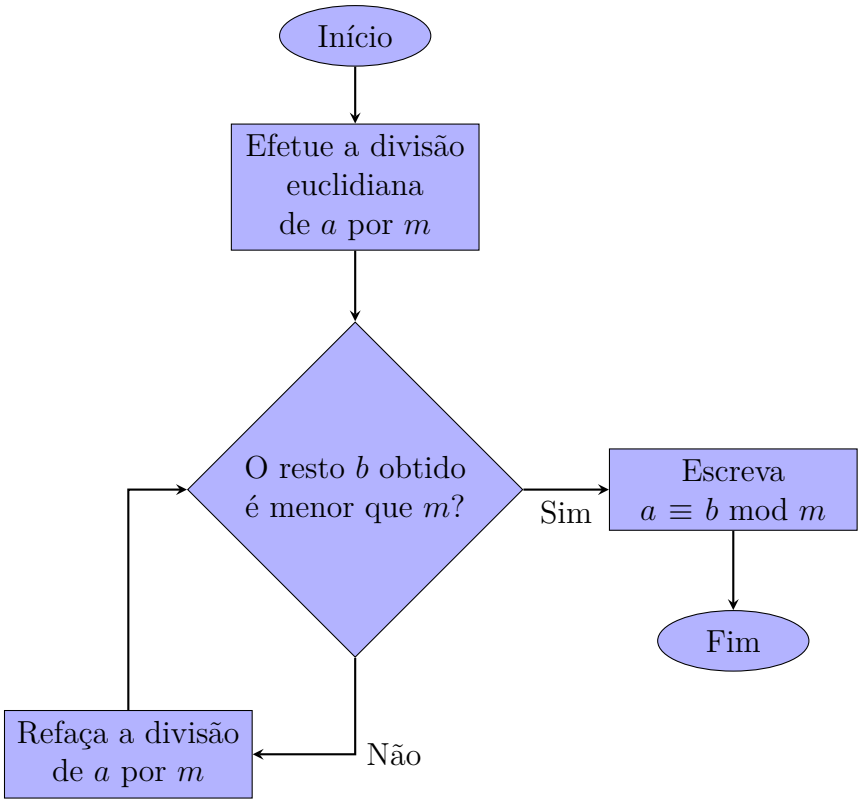


Figura 5.1: Fluxograma de autoria própria - Congruência módulo m

Um resultado muito útil, quando se trata de congruências é o *Pequeno teorema de Fermat*. Com ele obtemos a congruência módulo p, sendo p um número primo.

Exemplo 5.27. Teorema de Fermat

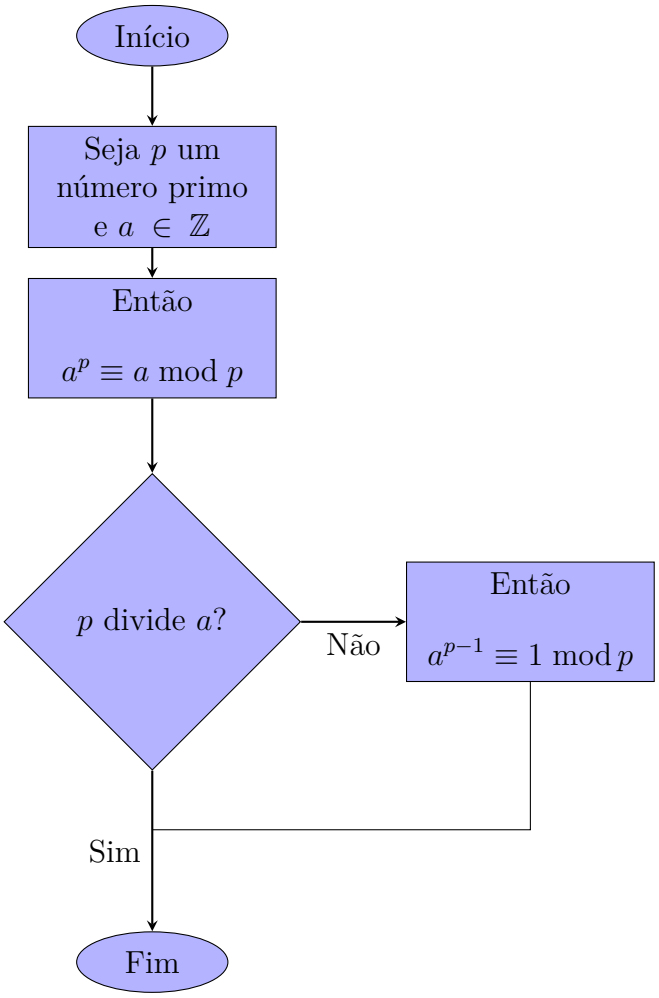


Figura 5.2: Fluxograma de autoria própria - Teorema de Fermat

Há um resultado, em particular, que ajuda nos cálculos para encontrar soluções de um sistema de uma congruência, como por exemplo quando temos um problema no qual precisamos descobrir qual número inteiro a que quando dividido por $m_1, m_2, \ldots, m_n$ deixa o mesmo resto. Pelas propriedades já apresentadas nesse capítulo, podemos calcular o mínimo múltiplo comum (mmc) desses m_i com $i = 1, 2, \ldots$ e transforma-los em uma única congruência. Ou seja,

$$a \equiv r \bmod m_i, \text{ com } i = 1, 2, \ldots \Leftrightarrow a \equiv r \bmod [m_1, m_2, \ldots, m_n].$$

Exemplo 5.28. Congruência módulo mínimo múltiplo comum (mmc)

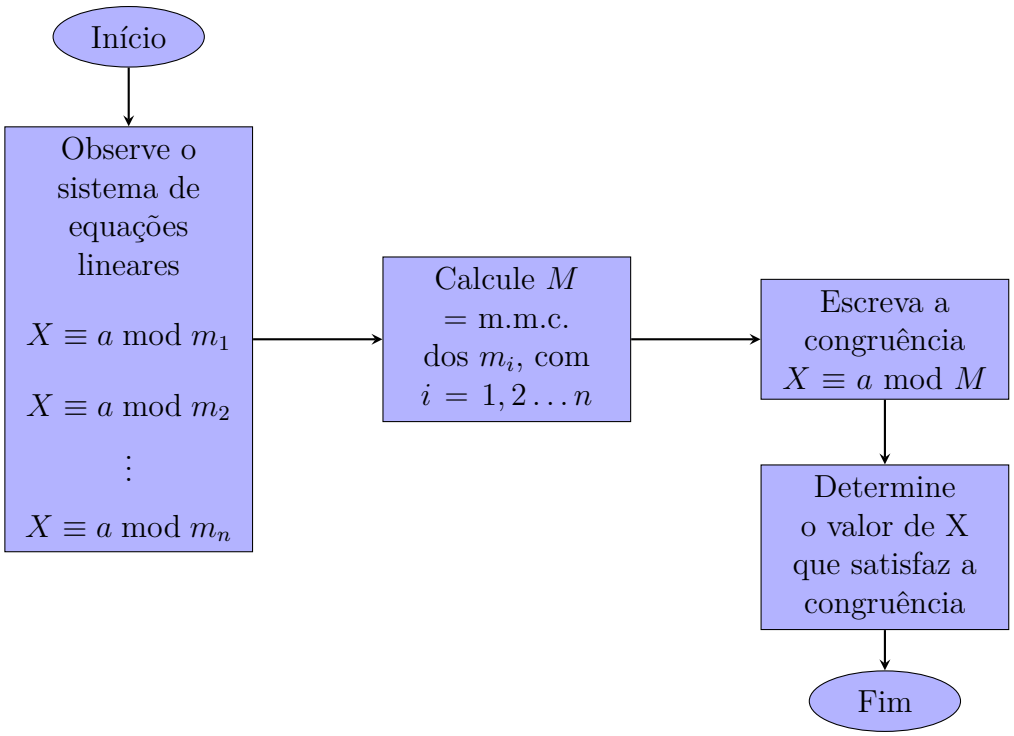


Figura 5.3: Fluxograma de autoria própria - Congruência módulo mínimo múltiplo comum

Agora vamos construir um fluxograma para o cálculo da *função(φ) de Euler*, que determina a quantidade de elementos de um sistema reduzido de resíduos módulo m que são primos com m.

Temos que

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

que também pode ser calculada da seguinte maneira,

$$\varphi(m) = p_1^{\alpha_1 - 1} \ldots p_n^{\alpha_n - 1}(p_1 - 1) \ldots (p_n - 1),$$

sendo os p_i os primos envolvidos na decomposição em fatores primos do número que se deseja calcular a função fi de Euler.

Utilizaremos a segunda opção, pois os cálculos são mais simples.

Exemplo 5.29. Função φ de Euler

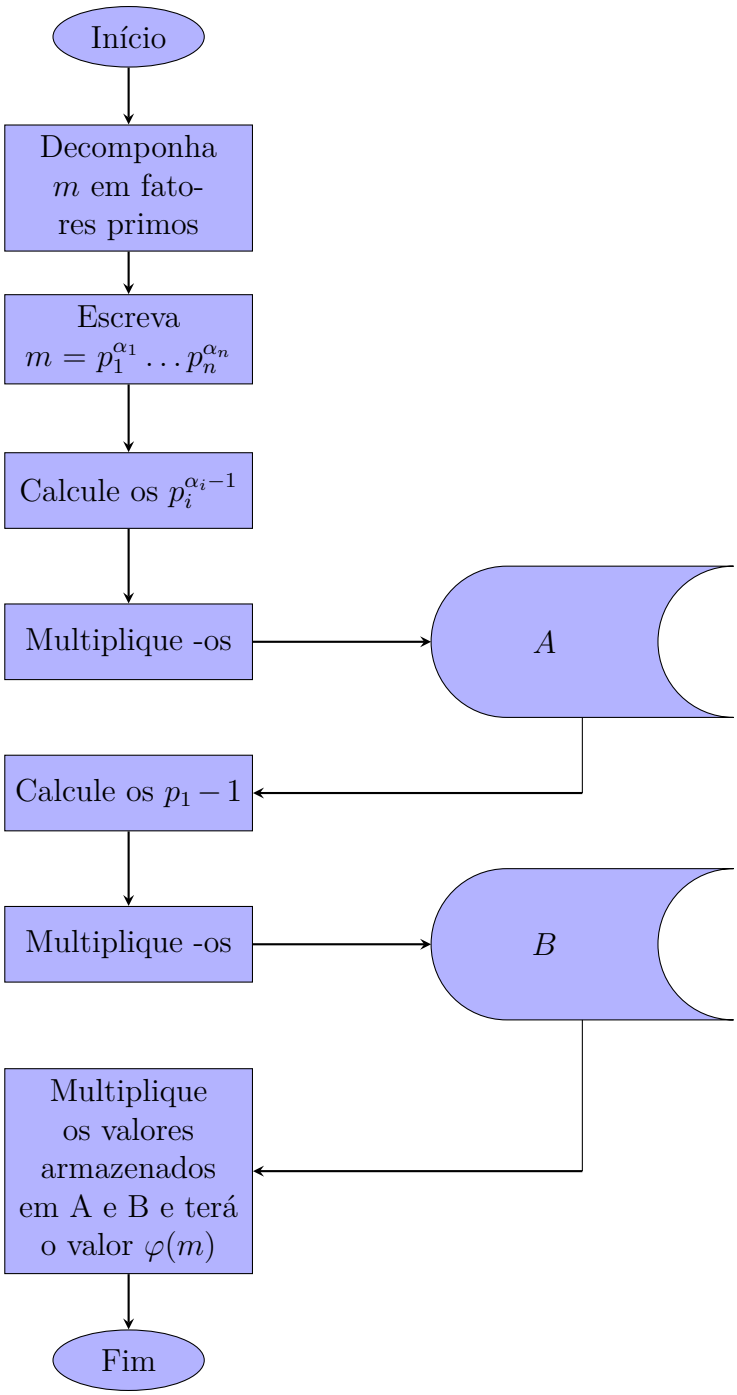


Figura 5.4: Fluxograma de autoria própria - Função φ de Euler

Nesse fluxograma foi utilizado uma forma (símbolos de fluxograma) não muito convencional, ela deve ser utilizada em um fluxograma quando é necessário armazenar dados, que serão utilizados posteriormente.

Veremos agora um importante resultado, que facilitará os cálculos quando precisarmos

resolver um sistema de congruências lineares. Esse resultado recebe o nome de *Teorema Chinês dos Restos*. Ele será útil quando tivermos congruência com valores pequenos para os módulos. Se o valor do módulo for grande, pode-se utilizar alguns dos resultados apresentados nesta seção.

Primeiramente precisaremos saber calcular o inverso multiplicativo de um número módulo m. Ou seja, se $a \equiv x \bmod m$ então seu inverso é um número a' tal que $aa' \equiv 1 \bmod m$.

Exemplo 5.30. Inverso multiplicativo da congruência $a \equiv x$ mod m

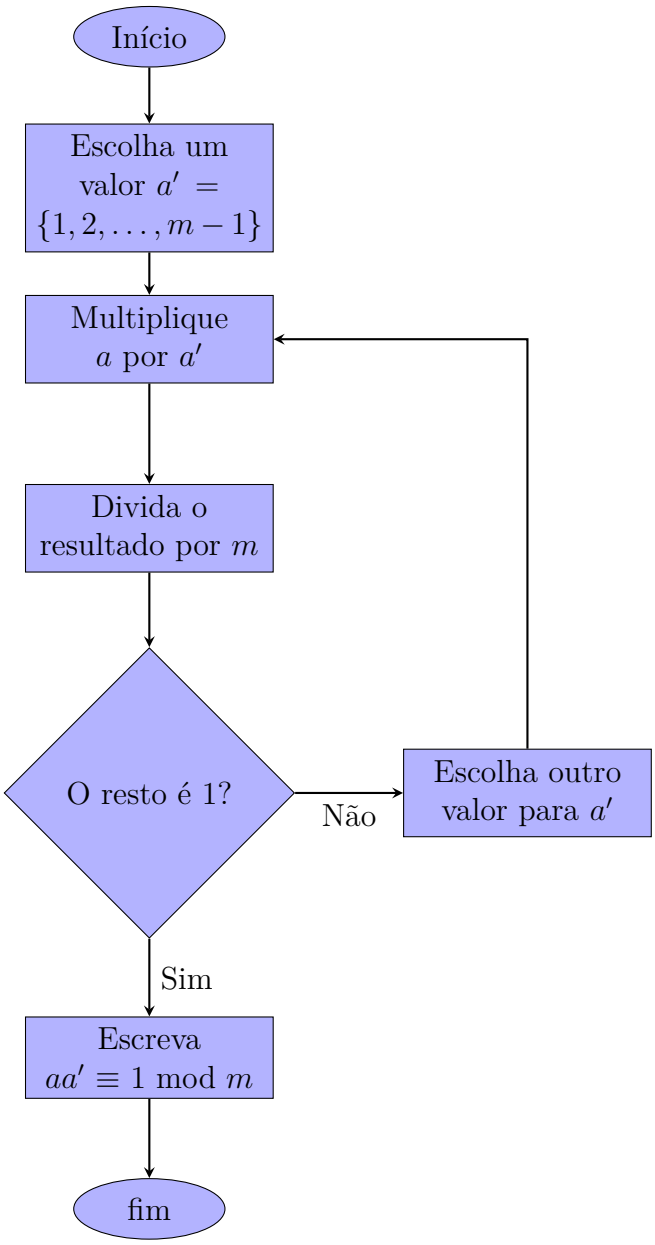


Figura 5.5: Fluxograma de autoria própria - Inverso multiplicativo (Congruência)

O teorema chinês do resto nos auxilia a resolver problemas em que, devemos determinar qual o número que deixa tais restos quando dividimos por determinados valores. Ou seja, determinar a solução do seguinte sistema de congruências:

$$\begin{cases} N \equiv c_1 \bmod n_1 \\ N \equiv c_2 \bmod n_2 \\ \quad\vdots \\ N \equiv c_r \bmod n_r \end{cases}$$

que terá solução única, $x = Z + nt$, com $t \in \mathbb{Z}$ se os números $n_i \in \mathbb{N}$ forem primos entre si.

Vamos então, com ajuda de um fluxograma, descrever o passo a passo para a resolução desse sistema de congruências. Estamos apenas interessados em sistemas de congruências que possuem solução única.

Exemplo 5.31. Teorema Chinês do Resto

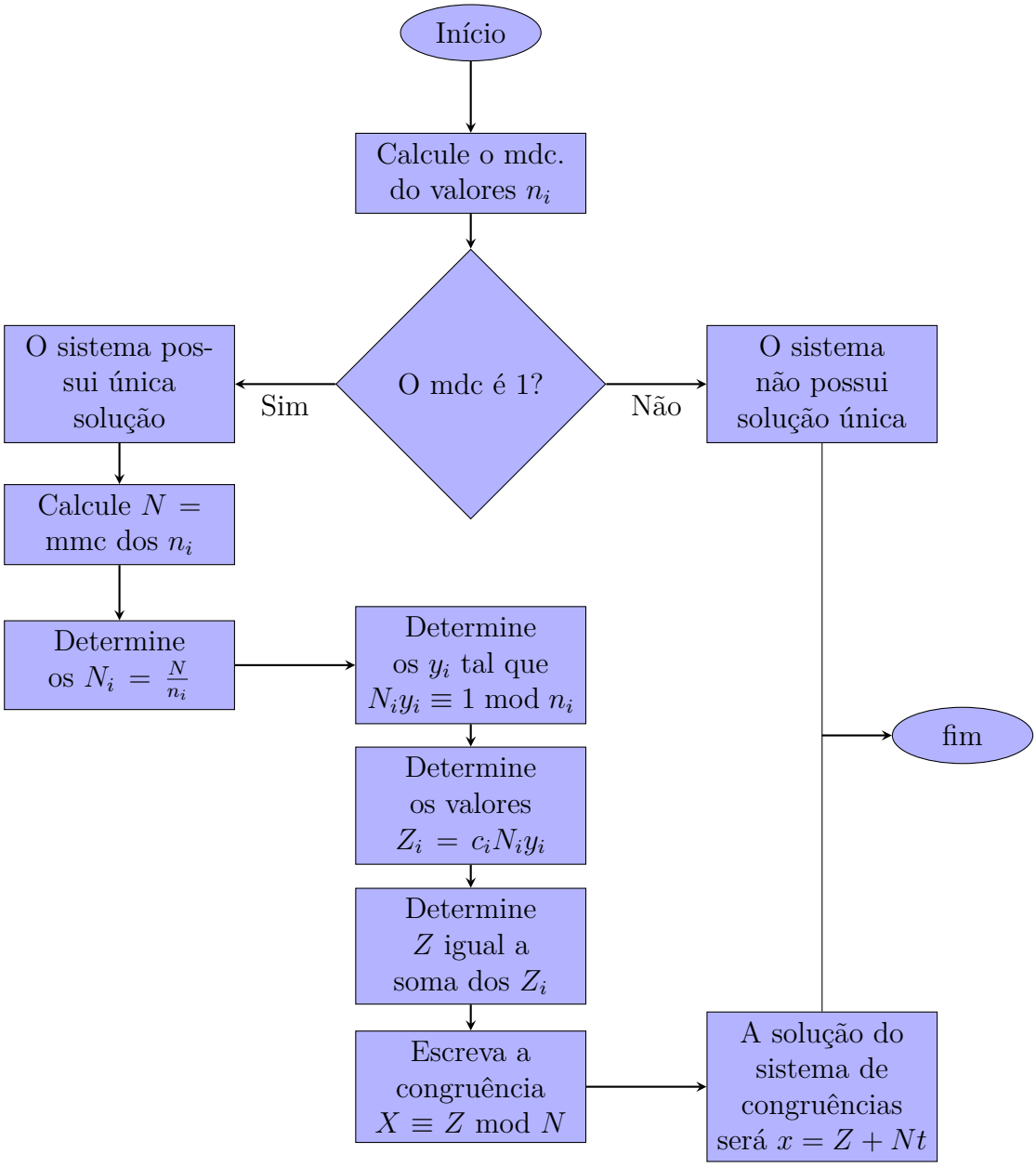


Figura 5.6: Fluxograma de autoria própria - Teorema chinês do resto

No próximo capítulo, traremos exemplos de problemas oriundos de olimpíadas de matemática, resolvidos utilizando-se da aritmética dos restos com uso dos fluxogramas.

6 A importância do resto

Coma já dito neste trabalho, muitos de nós não damos a devida importância ao resto de uma divisão euclidiana, pois é apenas um "resto", não é mesmo? Não, ele pode ser fundamental em alguma situações!

Neste capítulo, abordaremos alguns exemplos, oriundos de olimpíadas de Matemática. Foram escolhidas questões que abordam conceitos em que é importante observar o resto de uma divisão, muito mais do que realizar a própria divisão em si.

A seguir apresentaremos algumas questões retiradas das principais olimpíadas, que os alunos do Ensino Fundamental e Médio, participam relacionadas a área da Matemática no Brasil. São elas, a Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP), que também é aberta a participação das escolas particulares (não gratuitamente), a Olimpíada Internacional Matemática Sem Fronteiras (*Mathématiques Sans Frontières*) gratuita apenas para a rede pública e também a Olimpíada Brasileira de Matemática (OBM) que em 2017 passou a ser apenas para participantes convidados (os melhores de cada nível na 2° fase da OBMEP e participantes que se destacam em olimpíadas regionais com apoio da OBM).

Mathématiques sans frontieres

A Olimpíada Internacional Matemática Sem Fronteiras (edição brasileira), é uma competição criada em 1989 na França, o Brasil foi convidado a participar somente em 2010. Participam dela mais de 30 países, contando com a participação de mais de 200 mil alunos.

O diferencial dessa olimpíada se dá ao fato da classe inteira ser inscrita para a participação. Seu principal objetivo é que os alunos cooperem na resolução das atividades, estimulando a imaginação, a racionalização e a formalização de situações cotidianas. Com isso os alunos devem se organizar para a realização da prova, incentivando a participação de todos, não somente dos que possuem altas habilidades em Matemática.

As provas são realizadas na própria escola, na data estipulada pela organização. Conta com questões dissertativas, que devem ser resolvidas em equipes por cada sala, o professor não pode auxiliar no processo de realização da prova.

Cada nível conta com um determinado número de questões, que devem ser resolvidas em no máximo 90 minutos. São três níveis:

i Básico - 4º ao 6º ano do Ensino Fundamental, conta com 8 questões dissertativas.

ii Júnior - 7º ao 9º ano do Ensino Fundamental, conta com 9 questões para os 7º e 8º anos e 10 questões para o 9º ano.

iii Sênior - Ensino Médio, conta com 11 questões para o 1º ano, 12 para o 2º ano e 13 para o 3º ano.

Para a realização os estudantes podem fazer uso dos seguintes materiais: Lápis ou lapiseira, borracha, caneta azul ou preta, apontador, régua, esquadro, tesoura, anotações no caderno, livros, atlas geográficos, dicionários (pois toda prova possui um questão em língua estrangeira), fita adesiva e calculadora não programável. É proibido o acesso a internet e uso de celulares, ou qualquer outro dispositivo eletrônico. Também é proibido receber informações vinda de professores, funcionários da escola ou de demais alunos, que não fazem parte da classe.

Várias turmas da mesma escola podem participar, porém cabe a escola escolher apenas uma classe por ano/série, que serão enviadas para a correção. Uma banca, coordenada pelo Departamento de Matemática da Universidade Metodista de São Paulo, corrigirá as provas. É analisado principalmente o esforço, a criatividade e a profundidade das resoluções apresentadas.

As escolas com classes premiadas (medalhas de ouro, prata, bronze e menção honrosa) receberão um certificado de premiação. Elas serão convidadas (por meio de seleção), a integrar a delegação brasileira para olimpíadas internacionais.

A participação para as escola públicas é gratuita, sendo cobrada apenas uma taxa para envio de premiações (certificados ou medalhas), já as escolas particulares pagam uma taxa de participação.

A participação nessa olimpíada deveria ser mais incentivada pelas escolas, pois vai de encontro com a proposta da BNCC [1]. Os alunos são responsáveis pela organização na hora de fazer a prova, são levados a cooperar com seus conhecimentos e incentivados e resolver situações problemas em conjunto. Sabemos que cada aluno possui pelo menos uma habilidade e que existem múltiplas habilidades, assim essa olimpíada visa a integração dos alunos da sala, pois para a realização da prova, são necessárias várias habilidades, não só as referentes a matemática, ou seja, todos conseguem contribuir na resolução do problema.

Como na realização da prova, os alunos podem fazer uso de anotações, seria muito útil ter em mãos fluxogramas, que os ajudassem no processo de resolução de problemas e também na justificativa do processo de resolução, já que a prova conta apenas com questões dissertativas. Assim os fluxogramas apresentados nesse trabalho, os ajudaria a resolver problemas envolvendo a divisibilidade.

A seguir temos alguns problemas que envolvem padrões de repetições, conteúdo em que é fundamental saber o resto de uma divisão euclidiana. Essas questões foram retiradas do banco de questões dessa olimpíada.

Exemplo 6.1. Questão retirada da prova nível Junior 2011. Vamos resolve-la utilizando o fluxograma.

Nós temos uma sequência de números: 2010 é o primeiro. Você obtém o número seguinte da sequência a partir da soma dos quadrados dos dígitos do número considerado: $2^2 + 0^2 + 1^2 + 0^2 = 5$. E assim por diante. O 3º. portanto é 25, o 4º. número é 29 etc.

Qual é o 2011º número? Justifique sua resposta.

Figura 6.1: Questão - *Mathématiques sans frontieres* - Nível Junior 2011

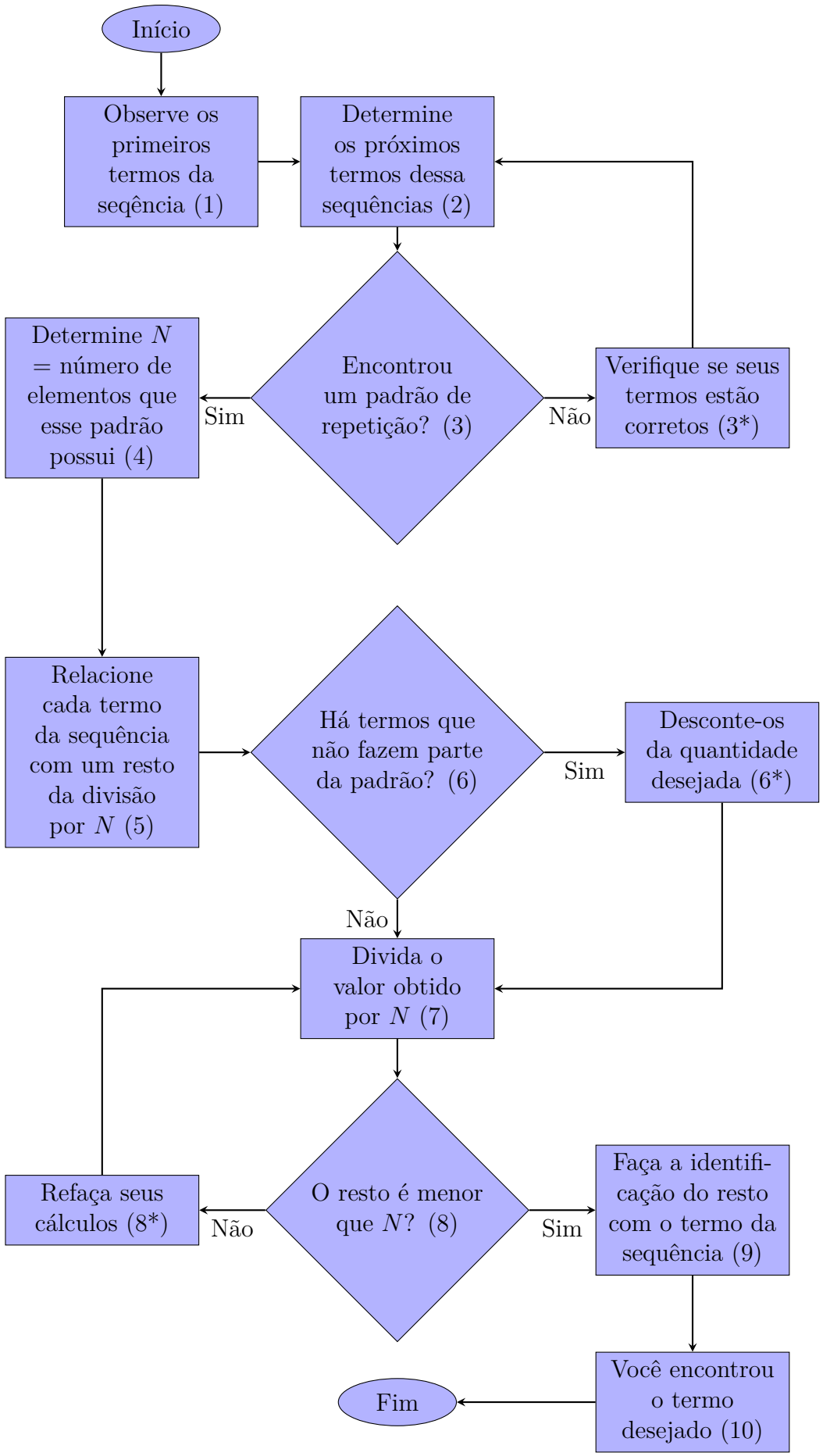


Figura 6.2: Fluxograma de autoria própria - Resolução de problemas que envolvem padrões e regularidades

Seguindo os passos do fluxograma o aluno deverá raciocinar da seguinte forma:

(1) 2010, 5, 25 e 29.

(2) 2010, 5, 25, 29, 85, 89, **145, 42, 20, 4, 16, 37, 58, 89**, 145, 42, 20, 4, 16, 37, 58, 89, ...

(3) Sim.

(4) $N = 8$.

(5) 145=resto 1, 42=resto 2, 20=resto 3, 4=resto 4, 16=resto 5, 37=resto 6, 58=resto 7 e 89=resto 0. (89 foi considerado o último termo do padrão)

(6) Sim

(6*) 2011-6=2005 (2010, 5, 25, 29, 85 e 89).

(7) $2005 \div 8 \Rightarrow 250.8 + 5$.

(8) Sim.

(9) Resto 5=16.

(10) O 2011º termo dessa sequência é 16.

Ao fazer uso do fluxograma, além de facilitar os cálculos, ele também fornece aos alunos a justificativa do processo. Assim para questões dissertativas como essa, ter esse fluxograma em mão, seria muito útil.

Exemplo 6.2. Questão retirada da prova nível Junior de 2017.

Simão escreve uma lista de números. O primeiro número é 3,2. Para se descobrir o próximo número, ele utiliza a seguinte regra :

Troque o número inteiro pela parte decimal (exemplo: 3,2 se torna 2,3), e então subtraia o menor do maior (3,2 – 2,3 = 0,9)

Obtido o número novo (0,9) ele aplica a regra novamente, obtendo o número seguinte de sua lista. Os três primeiros números de sua lista são : 3,2 / 0,9 / 8,1

Encontre o 38º. número da lista de Simão.
Proponha um novo método para se descobrir qualquer número da lista sem precisar calcular todos.
Utilize seu método para determinar o 2017º. número.

Figura 6.3: Questão - *Mathématiques sans frontieres* - Nível Junior 2017

Novamente utilizando o fluxograma teremos:

(1) 3,2 ; 0,9 ; 8,1.

(2) 3,2 ; 0,9 ; **8,1; 6,3 ; 2,7 ; 4,5 ; 0,9 ; 8,1 ; 6,3 ;...**

(3) Sim.

(4) $N = 5$.

(5) resto 1=8,1; resto 2=6,3; resto 3=2,7; resto 4=4,5 e resto 0=0,9.

(6) Sim

(6*) 38-2=36. (3,2 não faz parte da repetição e consideramos 0,9 como o último termo do padrão)

(7) $36 \div 5 \Rightarrow 5.7 + 1$

(8) Sim.

(9) resto 1= 8,1.

(10) O 38º termo dessa sequência será 8,1.

Para encontrar o 2017º termo da sequência o processo seria o mesmo até o item (5), depois teríamos:

(6) 2017-2=2015.

(7) $2015 \div 5 \Rightarrow 5.403 + 0$.

(8) Sim.

(9) resto 0 = 0,9.

(10) O 2017º termo dessa sequência será 0,9.

OBMEP

A Olimpíada Brasileira de Matemática das Escolas Públicas (OBMEP),é realizada todos os anos, por alunos do Ensino Fundamental e Médio do Brasil inteiro, composta de três níveis:

i Nível 1, para os alunos matriculados nos 6º e 7º anos.

ii Nível 2, para alunos matriculados nos 8º e 9º anos.

iii Nível 3, para alunos matriculados no Ensino Médio.

No ano de 2018 a OBMEP passou a contar com mais um nível, destinado aos alunos dos 4º e 5º anos do Ensino Fundamental, como se fosse uma preparação do aluno para a realização das provas nos anos seguintes. Chamado de Nível A, conta apenas com uma fase, os alunos são premiados refente a colocação da rede educacional á qual pertencem, não há uma concorrência com os alunos de todo o território nacional, como nos outros níveis da OBMEP.

A OBEMP nos Níveis 1, 2 e 3 é composta de duas fases:

i Fase 1 é composta de 20 questões alternativas. Todos os alunos inscritos participam. Nessa fase é importante a quantidade de alunos inscritos, pois os que passarão para a Fase 2 dependem dessa quantidade, conforme mostram as tabelas.

OBMEP -Nível 1 e 2	
Quantidade de alunos inscritos na 1º fase	**Vagas para a 2º fase**
1 a 40	2
41 a 80	4
81 a 140	7
141 a 240	12
241 ou mais	5% dos inscritos

OBMEP -Nível 3	
Quantidade de alunos inscritos na 1º fase	**Vagas para a 2º fase**
1 a 120	6
121 a 240	12
241 a 380	19
381 a 620	31
621 ou mais	5% dos inscritos

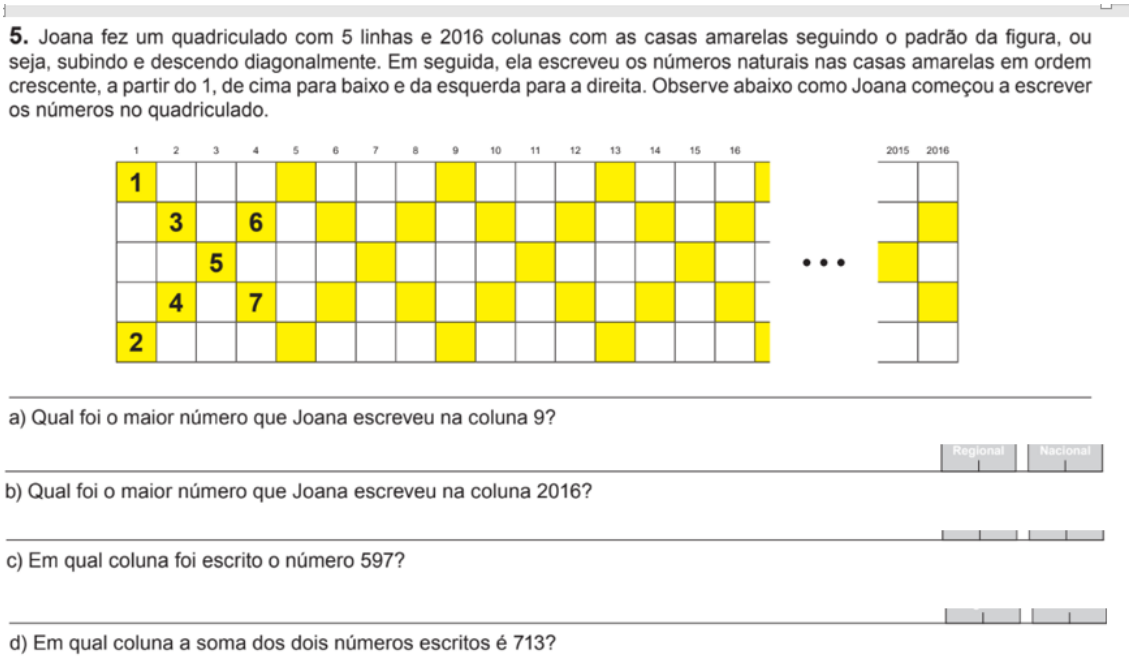
Figura 6.4: Quantidade de alunos que passam para o Fase 2 - OBMEP

ii Fase 2 é composta 6 questões dissertativas, os alunos aprovados para essa fase competem com os demais alunos espalhados pelo Brasil. São premiados dependendo do seu resultado com: Menção Honrosa ou Medalha de bronze, prata ou ouro.

Todas as olimpíadas, regulamentadas pelo MEC, valem pontos para o aluno entrar em uma Universidade Pública, logo é importantíssimo que os alunos participem e obtenham bons resultados nessas olimpíadas.

Na OBMEP os alunos podem se utilizar apenas de lápis, borracha e caneta para a realização das provas, tanto na fase 1, como na fase 2. Assim eles não poderiam se utilizar, fisicamente, de fluxogramas para auxilio nas questões. Porém se esse fluxograma for trabalhado no cotidiano das aulas, ficará fixado o processo na memória do aluno e o ajudará na resolução da questão.

Exemplo 6.3. Vamos agora utilizar desse fluxograma para resolver uma questão da OBMEP 2016 Nível 1 segunda fase.



5. Joana fez um quadriculado com 5 linhas e 2016 colunas com as casas amarelas seguindo o padrão da figura, ou seja, subindo e descendo diagonalmente. Em seguida, ela escreveu os números naturais nas casas amarelas em ordem crescente, a partir do 1, de cima para baixo e da esquerda para a direita. Observe abaixo como Joana começou a escrever os números no quadriculado.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ... 2015 2016

1 3 6 5 4 7 2

a) Qual foi o maior número que Joana escreveu na coluna 9?

b) Qual foi o maior número que Joana escreveu na coluna 2016?

c) Em qual coluna foi escrito o número 597?

d) Em qual coluna a soma dos dois números escritos é 713?

Figura 6.5: Questão I - OBMEP - Nível 1 - Segunda fase 2016

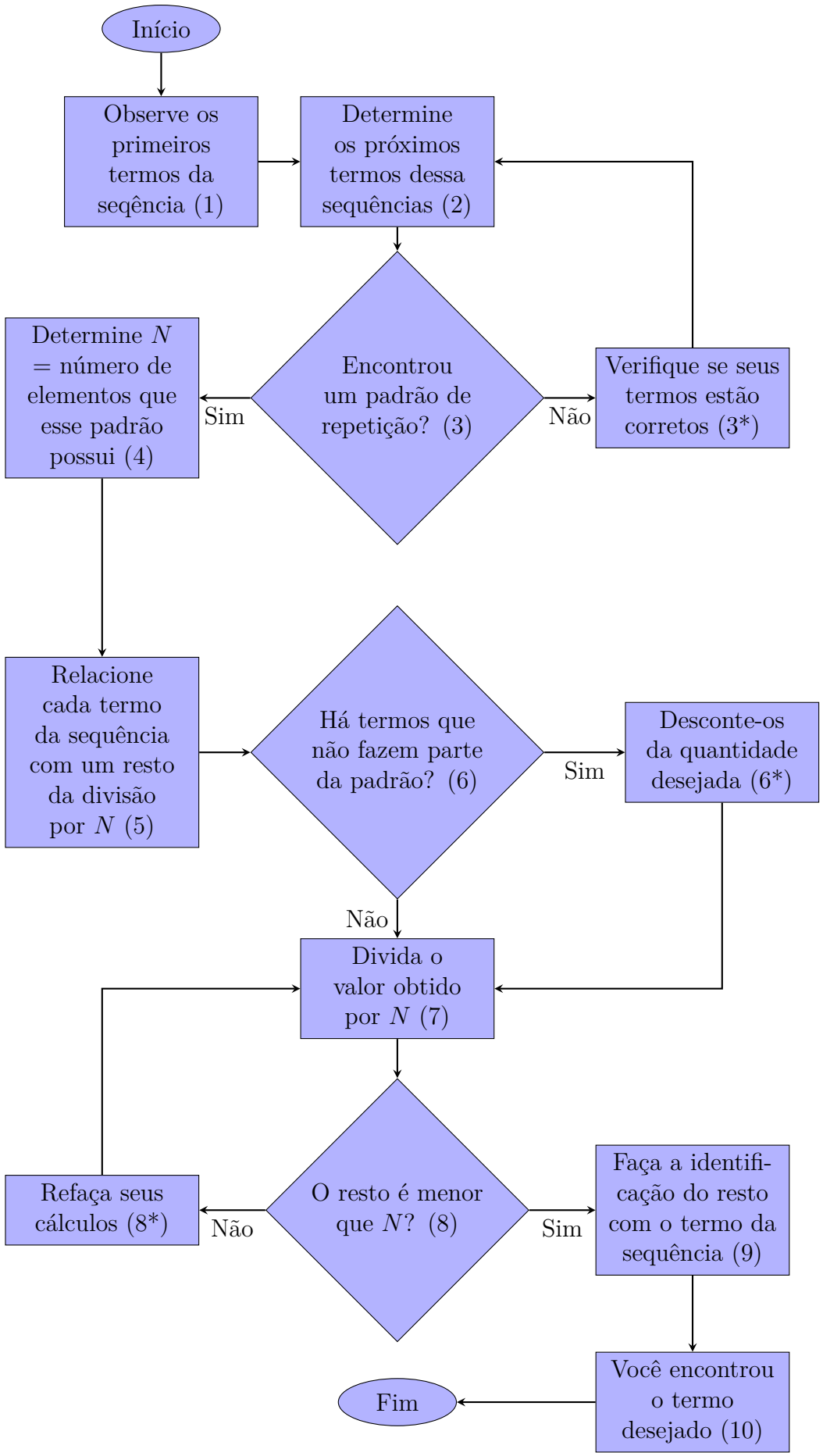
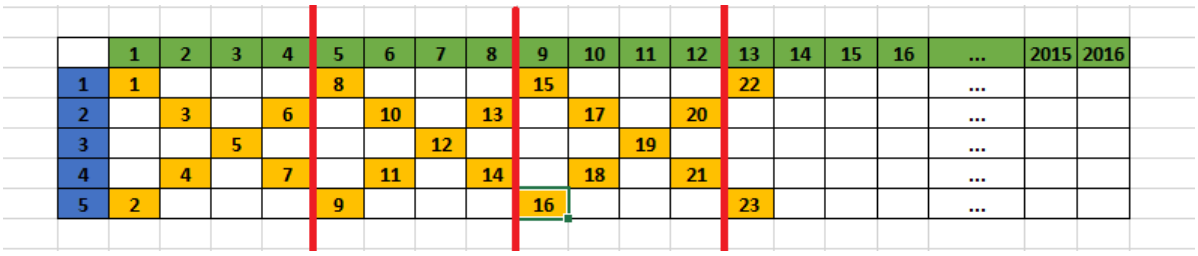


Figura 6.6: Fluxograma de autoria própria - Resolução de problemas que envolvem padrões e regularidades

(1) e (2) Imagem (Pode-se construir a seguinte tabela).



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...	2015	2016
1	1				8				15				22				...		
2		3		6		10		13		17		20					...		
3			5				12				19						...		
4		4		7		11		14		18		21					...		
5	2				9				16				23				...		

Figura 6.7: Questão II - OBMEP - Nível 1 - Segunda fase 2016

(3) Sim.

alternativa a) - Podemos verificar que o 16 encontra-se na coluna 9.

alternativa b) - Para encontrar o maior número da coluna 2016 , sabemos que o padrão se repete a cada 4 colunas, assim,

(4) $N = 4$.

(5) resto 1=coluna 1, resto 2=coluna 2, resto3=coluna 3 e resto 0= coluna 4.

(6) Não.

(7) $2016 \div 4 \Rightarrow 4.504 + 0$.

(8) Sim.

(9) Resto 0 = coluna 4.

(10) 504 blocos completos com 7 números cada bloco. Assim $504.7 = 3528$.

Portanto 3528 é o maior número da coluna 2016.

alternativa c) - Para encontrar em qual coluna o número 597 foi escrito, sabemos que o padrão se repete a cada 7 números, assim,

(4) $N = 7$.

(5) Por temos, resto 1=posição do número 1, resto 2=posição do número 2, resto 3=posição do número 3, resto 4=posição do número 4, resto 5=posição do número 5, resto 6=posição do número 6 e resto 0=posição do número 7.

(6) Não.

(7) $597 \div 7 \Rightarrow 7.85 + 2$.

(8) Sim.

(9) Posição do número 2.

(10) 85 blocos de 7 números cada bloco. Assim $85.4 = 340$ e como o 2 se encontra na 1º coluna do bloco temos que acrescentar uma coluna.

Portanto o número 597 foi escrito na coluna de número 341.

alternativa d) - Os números que estão na mesma coluna são consecutivos, utilizando-se da álgebra podemos escrever $x + (x + 1) = 713$, ou seja $x = 356$ e $x + 1 = 357$, pois $356 + 357 = 713$. Repetindo os passos na **alternativa c)**, temos:

$357 \div 7 \Rightarrow 7.51 + 0$, ou seja temos 51 blocos completos com 4 colunas em cada bloco. Assim $4.51 = 204$, portanto os números que somados resultam em 713, estarão na coluna de número 204.

Como nessa fase as questões são dissertativas, seguindo os passos do fluxograma o aluno também encontrar as justificativas para a resolução das questões, mais uma vez, lembrar-se do fluxograma seria muito útil nessa hora.

Exemplo 6.4. Questão retirada da OBMEP 2015 Nível 1-2º fase

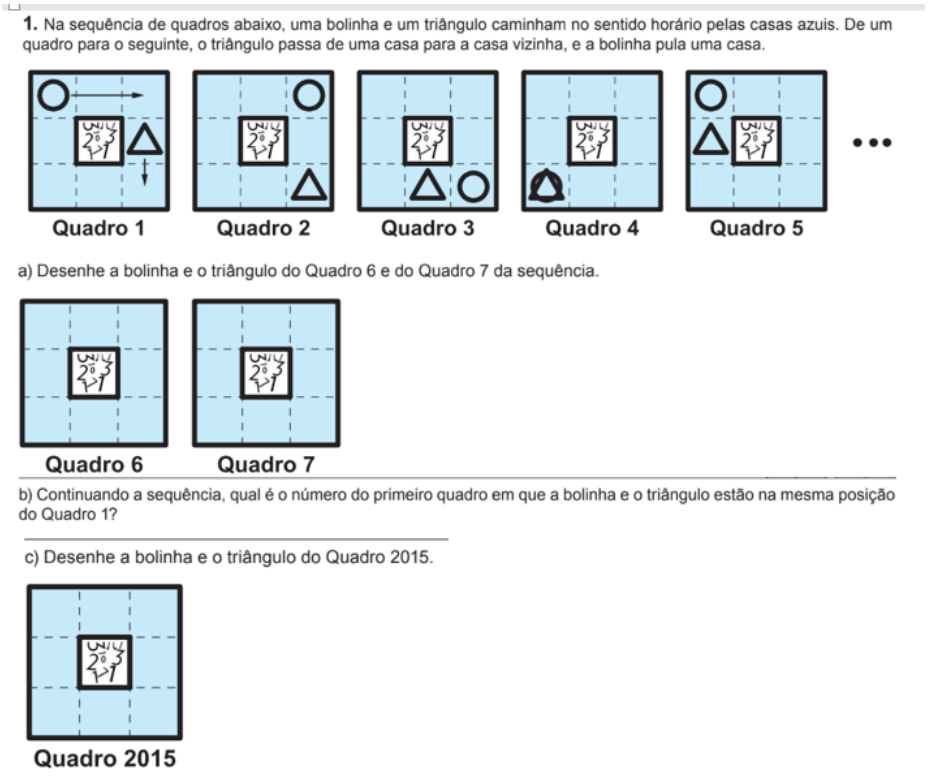


Figura 6.8: Questão I - OBMEP - Nível 1 - Segunda fase 2015

Novamente vamos nos utilizar do mesmo fluxograma para resolver essa questão.

(1) e (2) Imagem (Pode-se fazer essas representações).

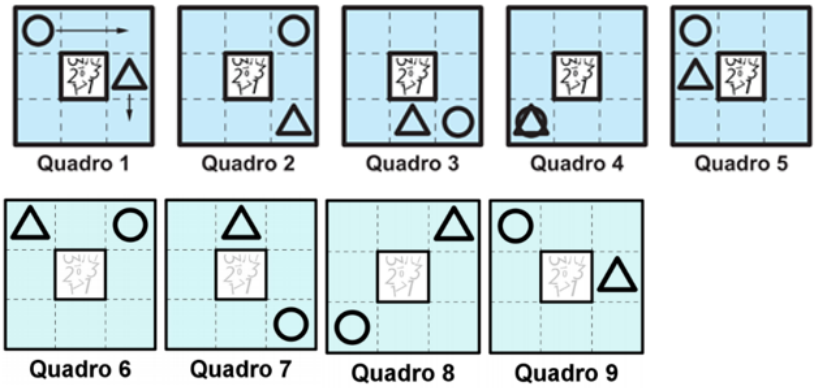


Figura 6.9: Questão II - OBMEP - Nível 1 - Segunda fase 2015

alternativa a) - Basta copiar os quadros 6 e 7.

(3) Sim.

(4) $N = 8$.

alternativa b) - No quadro 9 a bolinha e o triângulo estão na mesma posição do quadro 1.

(5) resto 1=quadro 1, resto 2=quadro 2, resto 3=quadro 3, resto 4=quadro 4, resto 5=quadro 5, resto 6=quadro 6, resto 7=quadro 7 e resto 0=quadro 8.

(6) Não.

(7) $2015 \div 8 \Rightarrow 8.251 + 7$.

(8) Sim.

(9) resto 7=quadro 7.

(10) **alternativa c)** - A bolinha e o triângulo estarão representados no quadro 2015 conforme mostra a figura.

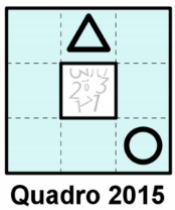


Figura 6.10: Questão III - OBMEP - Nível 1 - Segunda fase 2015

Olimpíada Brasileira de Matemática (OBM)

Na Olimpíada Brasileira de Matemática (OBM) participam alunos do Ensino Fundamental-Anos Finais, Médio e Universitário, de escolas públicas e privadas do Brasil. É realizada em conjunto com o Instituto de Matemática Pura e Aplicada (IMPA) e da Sociedade Brasileira de Matemática (SBM).

Sua primeira edição foi realizada no ano de 1979, passando por diversas mudanças em seu formato, a mais recente no ano de 2017, quando foi integrada da OBMEP, assim passou a ser constituída de uma única fase nos níveis 1, 2 e 3, anteriormente tinha-se três fases.

A OBM é composta de quatro níveis:

i Nível 1 - alunos matriculados no 6° ou 7° ano do Ensino Fundamental.

ii Nível 2 - alunos matriculados no 8° ou 9° ano do Ensino Fundamental.

iii Nível 3 - alunos matriculados no Ensino Médio.

iv Nível Universitário - alunos matriculados em instituições de Ensino Superior.

A prova dos níveis 1, 2 e 3 é composta de uma única fase com questões dissertativas, no nível 1 são 5 questões, nos níveis 2 e 3 são 6 questões.

Já no nível Universitário a OBM é composta de duas fases:

i 1° fase - 25 questões alternativas.

ii 2° fase - 6 questões dissertativas.

Para a participação na OBM, os alunos dos níveis 1, 2 e 3 são selecionados por resultados obtidos na OBMEP (300 alunos em cada nível), na Copa Multilaser de Matemática (100 melhores classificados) e em Olimpíadas Regionais apoiadas pela OBM (3 a 10 alunos de cada nível). No nível Universitário para a 1° fase, basta os estudantes se inscreverem no site da OBM. Os que obtiverem melhor desempenho são classificados para a 2° fase.

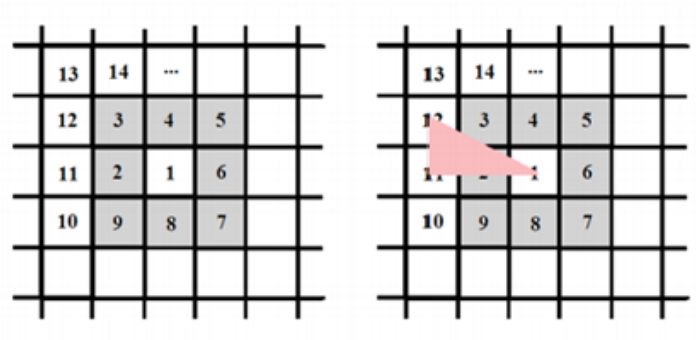
Os principais objetivos da OBM são interferir em prol da melhoria do ensino de Matemática, descobrir jovens talentos, selecionar estudantes para a participação de Olimpíadas Internacionais de Matemática, apoiar competições regionais e organizar competições sediadas no Brasil.

Como já mencionado é importante incentivar a participação dos alunos nessas olimpíadas, pois contarão pontos para seu futuro ingresso em universidades públicas, como também em seu desenvolvimento matemático.

A questão a seguir foi retirada da prova do Nível 1 no ano de 2019. Ela se encaixa na proposta desse capítulo, a importância do resto, e como feito com as questões de outras olimpíadas vamos resolve-la utilizando o fluxograma.

Exemplo 6.5. Questão retirada da OBM 2019

A figura a seguir representa um tabuleiro muito grande, formado por quadradinhos de lado $1\,cm$, em que os números inteiros positivos são preenchidos em ordem crescente, começando pelo 1 e formando "camadas" em torno do 1, conforme mostrado na figura abaixo. A primeira camada é formada apenas pelo número 1, a segunda camada é formada pelos números de 2 até 9 e, imediatamente após completar a segunda camada, começa a terceira camada com o número 10 no quadradinho à esquerda do 9.



a) Qual é o último número da terceira camada?

Para calcular a distância do quadrado 1 até um quadrado N que não esteja na sua linha nem na sua coluna, podemos formar um triângulo com um lado horizontal, um lado vertical e o terceiro lado ligando o centro do quadrado 1 até o centro do quadrado N. Por exemplo, na figura à direita temos o triângulo que poderia ser usado para calcular a distância do quadrado 1 até o quadrado 12. Veja que ele possui vértices nos centros dos quadrados 1, 11 e 12. O lado horizontal mede $2\,cm$ e o lado vertical mede $1\,cm$.

b) Determine os lados horizontal e vertical do triângulo que poderia ser usado para calcular a distância do quadrado 1 até o quadrado 33.

c) Determine os lados horizontal e vertical do triângulo que poderia ser usado para calcular a distância do quadrado 1 até o quadrado 2019.

Figura 6.11: Questão I - OBM - Nível 1 2019

As questões dessa olimpíada são mais complexas, em relação as demais já apresentadas, assim exige maior conhecimento por parte do aluno.

Temos novamente uma questão onde é de fundamental importância a observação de padrões de repetições, além de envolver conceitos como a representação de um número ímpar, quadrado perfeito, entre outros.

Assim o fluxograma utilizado nesse capítulo, mas uma vez, seria útil para responder essa questão dissertativa.

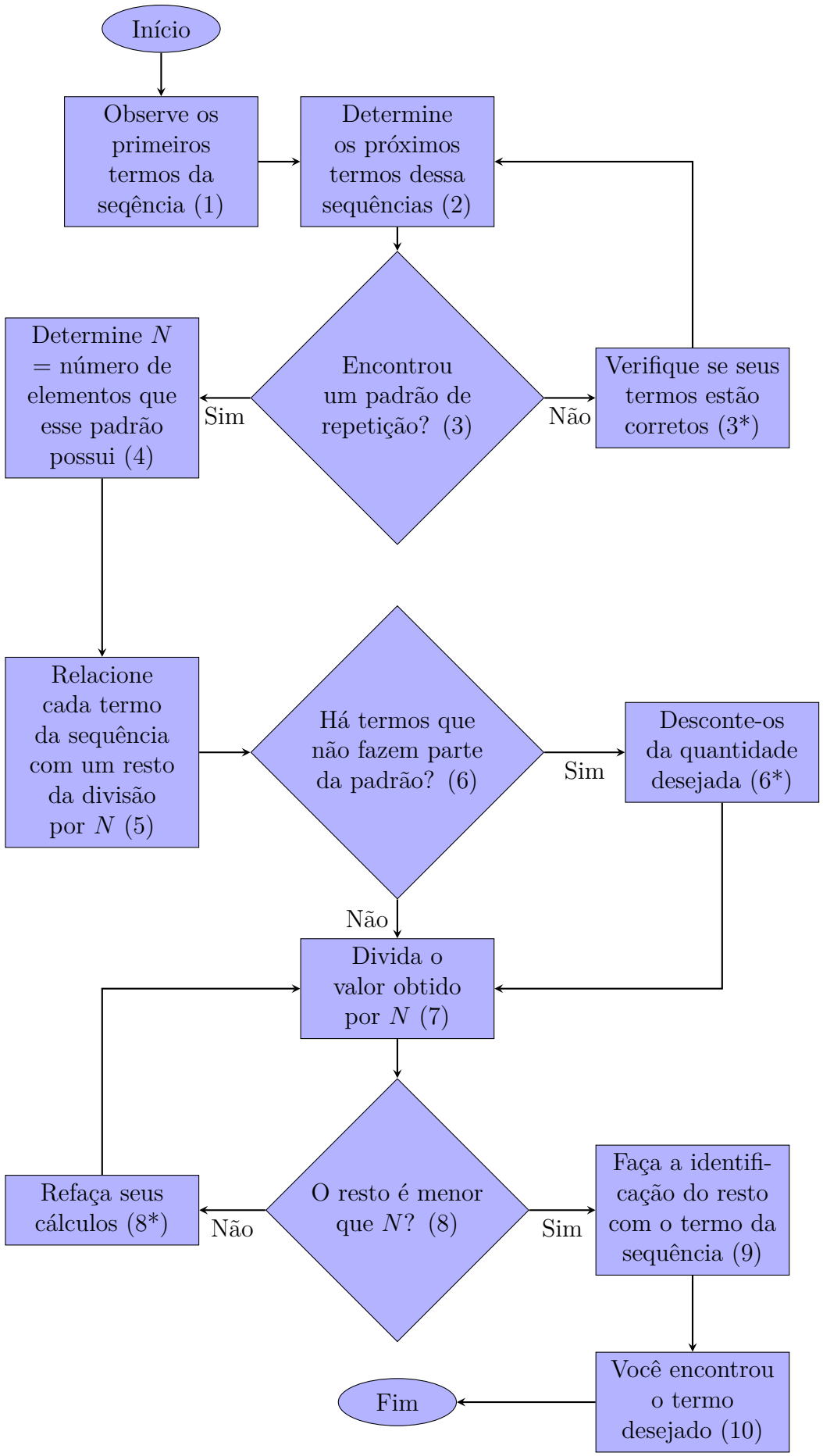


Figura 6.12: Fluxograma de autoria própria - Resolução de problemas que envolvem padrões e regularidades

Para responder as **alternativas a) e b)** devemos seguir os passos (1) e (2) do fluxograma.

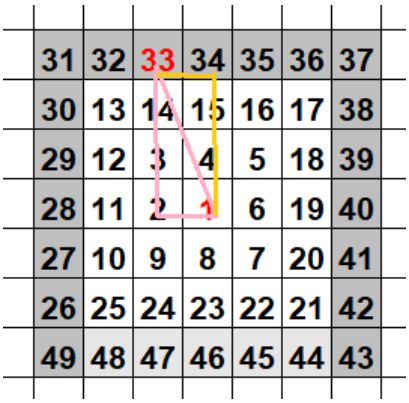


Figura 6.13: Questão II - OBM - Nível 1 2019

Assim na **alternativa a)** o último número da terceira camada é 25. E para responder a **alternativa b)** temos que os triângulos em rosa e amarelo são congruentes (Caso LLL), logo começar pelo sentido vertical ou pelo horizontal resulta no mesmo triângulo (com relação a forma), lado horizontal = 1cm e lado vertical = 3cm.

Para responder a **alternativa c)** deve-se primeiramente encontrar um padrão, prosseguindo com a instrução (2).

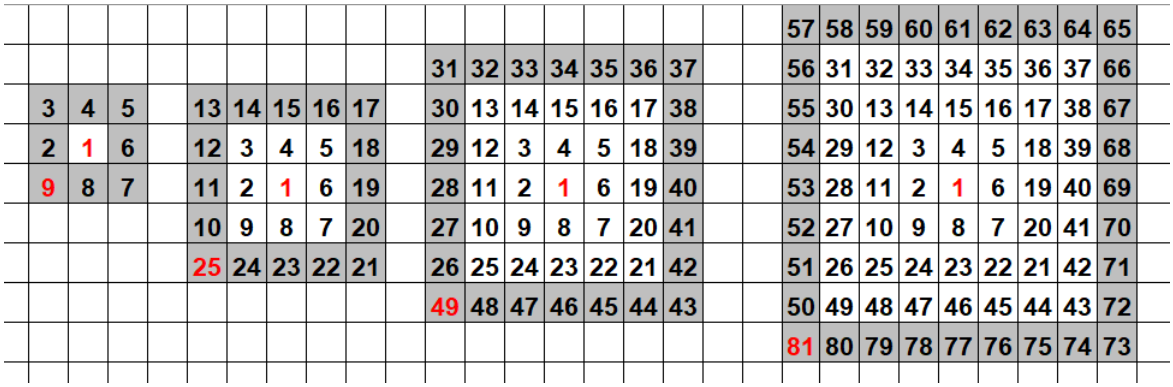


Figura 6.14: Questão III - OBM - Nível 1 2019

Em (3) o estudante deve perceber que cada camada termina com um quadrado perfeito ímpar, assim sendo n esse número, $n = (2.k + 1)^2$, com $k \in \mathbb{N}$.

Isso o ajudará a determinar em qual camada o número 2019 estará escrito,mais uma vez ele terá que observar as sequências já escritas:

$1 = 1^2$ está na camada 1, $9 = 3^2$ está na camada 2, $25 = 5^2$ está na camada 3, $49 = 7^2$ está na camada 4, $81 = 9^2$ está na camada 5, assim

Como 2019 não é um quadrado perfeito, vamos utilizar o quadrado perfeito ímpar mais próximo a ele: $1936 < 2019 < 2025 \Rightarrow 44^2 < 2019 < 45^2$, usaremos portanto o 2025, pois está mais próximo de 2019.

Para descobrir em qual camada está 2025, devemos observar que m cresce uma unidade a cada quadrado ímpar, assim de 1 até 45 temos 23 números ímpares. Logo $\sqrt{2025} - 23 = 45 - 23 = 22$, portanto o número 2025 é o último número da camada 22.

Para prosseguir com seus cálculos, o estudante deve agora determinar a medida dos lados vertical e horizontal do triângulo que determina a distância de 1 ate N. Fazendo alguns testes, com os números já escritos, podemos perceber uma regularidade, como mostra a imagem.

Note que, um dos lados tem medida igual ao número da camada e a medida do outro lado depende da posição que o número ocupa na nessa camada.

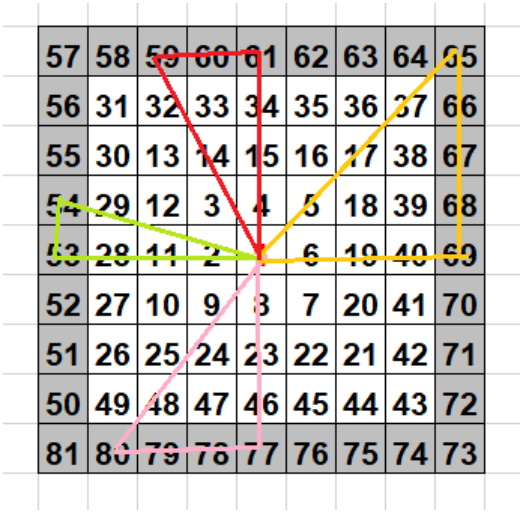


Figura 6.15: Questão IV - OBM - Nível 1 2019

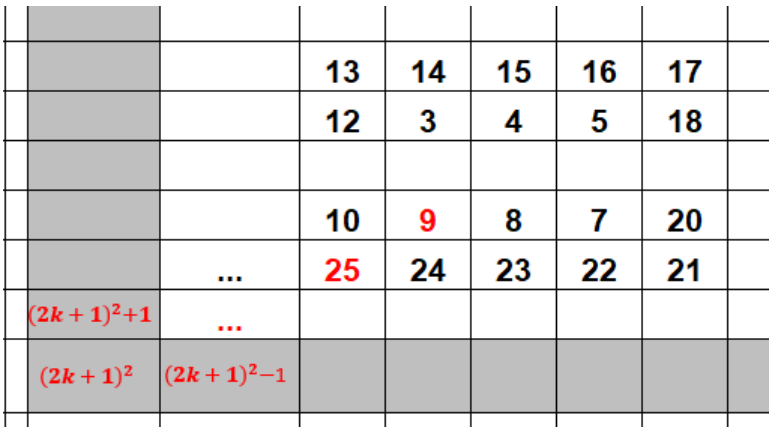


Figura 6.16: Questão V - OBM - Nível 1 2019

Assim para determinar a posição do número 2019 na linha, pode-se pular para o passo (7) do fluxograma, $2025 = 2019.1 + 6 \Rightarrow 2019 = 2025 - 6$, em seguida no passo (9) teríamos

Para responder a esse problema o aluno deve observar que, como 2019 está na camada 22, um dos lados será 22 cm, e como essa camada tem 45 números e o número que se encontra verticalmente com o 1 nessa camada é o 2003 ($45 \div 2 \Rightarrow 2.22 + 1$, ou seja temos 22 números a direita e 22 números a esquerda, assim temos $2025 - 22 = 2003$) e 2003 está a 16 unidades de distância de 2019, temos o seguinte mostrado na imagem.

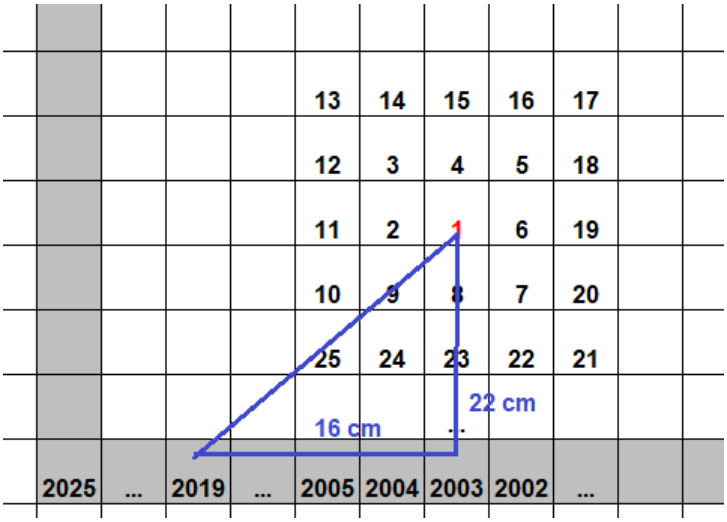


Figura 6.17: Questão VI - OBM - Nível 1 2019

Portanto como cada quadrado tem 1 cm de medida, podemos medir a distância entre o 1 e o 2019 da seguinte forma: lado horizontal mede 16 cm e o lado vertical mede 22 cm. Finalizando assim o problema.

Mais uma vez, o fluxograma ajuda o aluno na resolução do problema, e na justificativa do processo, fundamental em questões dissertativas. Nesse exemplo só com ele o aluno não resolveria o problema, mas se lembrando das etapas nele sugeridas e nos conteúdo necessário na resolução, o estudante teria um bom desempenho nessas provas.

Infelizmente a Matemática ainda é vista por muitos apenas como efetuar cálculos, mas ela vai além disso, é necessário saber os processos envolvidos nos cálculos para entender sua aplicação. Garantir que a resolução é coerente com o que o problema propõe. Saber fazer análise sobre os resultados obtidos é importante na formação desse indivíduo.

Assim o fluxograma não é apenas um algoritmo para realizar cálculos, mas sim uma maneira de analisar se o processo está sendo realizado de forma correta e de acordo com o que está sendo exigido, fornecendo justificativas de cada etapa.

7 Considerações finais

Em vista dos argumentos apresentados neste trabalho, percebe-se que mesmo que a Sociedade Brasileira de Computação (SBC) não seja a favor do ensino dos fluxogramas no Ensino Básico, eles são de grande valia quando se trata da compreensão de algoritmos matemáticos, uma vez que desmembram o processo em partes mais simples.

Nossa missão como educadores é sempre buscar formas alternativas de ensinar, visando a compreensão por parte do aluno, que está inserido em um contexto mais tecnológico e prático do que nós professores estamos acostumados. Assim, por que não buscar uma forma diferente de trabalhar o conteúdo de divisibilidade, tão incompreendido por nossos alunos? Por que ficar insistindo em ensinar o algoritmo da divisão de forma convencional, mesmo que boa parte de nossos alunos não o consiga realizar?

O desconhecido traz medo e insegurança, mas devemos tentar práticas novas, e o fluxograma está inserido na proposta da Base Nacional Comum Curricular (BNCC) e deverá ser trabalhado nas etapas do Ensino Básico, então vamos fazer uso dele.

Desta forma, antes de iniciar o trabalho em sala de aula com os alunos, o professor deve procurar por materiais que o deem suporte e segurança de que estão corretos. E este foi o grande objetivo deste trabalho, trazer de forma clara, objetiva e correta os conceitos de fluxograma, a fim de serem aplicados em sala de aula, principalmente no que se refere ao conteúdo da aritmética do resto, tão menosprezado na nossa grade curricular de matemática na Educação Básica.

Comprovamos com exemplos oriundos de olimpíadas de matemática, que para resolver problemas complexos, os alunos não precisam ter decorado o algoritmo completo e sim lembrar dos processos do fluxograma, que foram divididos em etapas mais simples, facilitando sua compreensão do que está sendo realizado. Também ao longo do percurso de um fluxograma, há etapas de verificação, assim caso tenha errado, o aluno é capaz de perceber e refazer seus cálculos, antes da finalização da tarefa. Outra ferramenta de ensino importante que os fluxogramas trazem é a justificativa dos cálculos que estão sendo feito, algo que infelizmente não é muito trabalhado em sala de aula, busca-se apenas o resultado final, mas quando as questões são dissertativas, os alunos ficam sem saber como proceder, ao se utilizar o fluxograma isso já é feito normalmente em cada etapa do processo.

Concluímos então que o fluxograma é uma ferramenta útil, que deve sim ser trabalhada com mais frequência no dia a dia da sala de aula, não só no conteúdo de divisibilidade, como também em outros conteúdos matemáticos e porque não em outras áreas do conhecimento.

Convido a você caro leitor que se interessou por essa nova ferramenta de ensino - aprendizagem, criar também algoritmos em forma de fluxograma e compartilhá-los. Quanto mais essa rede de saber crescer, mais teremos exemplos práticos para a utilização em nosso cotidiano, beneficiando não só os professores, mas também aos alunos. Quanto

mais conhecimento pudermos disseminar melhor!

Espero que tenham gostado da leitura.

Referências

[1] BRASIL. *Base Nacional Comum Curricular: Educação é a base*. Brasilia-DF: [s.n.], MEC,2018. v. 11.

[2] BARBOZA, T. A. V.; FRACOLLI, L. A. A utilização do "fluxograma analisador" para a organização da assistência à saúde no programa saúde da família. *Cadernos de Saúde Pública*, SciELO Public Health, v. 21, p. 1036–1044, 2005.

[3] FRANCO, T. B. O uso do fluxograma descritor e projetos terapêuticos para análise de serviços de saúde em apoio ao planejamento: o caso de luz (mg). *O trabalho em saúde: olhando e experienciando o SUS no cotidiano. São Paulo: Hucitec*, 2003.

[4] PERLINGEIRO, C. A. G. *Engenharia de processos: análise, simulação, otimização e síntese de processos químicos*. [S.l.]: Editora Blucher, 2005.

[5] LIMA, P.; VIEIRA, P.; AO, L. B. Ensino de algoritmos, programação e matemática: panorama e estudo de caso para estudantes de escolas públicas brasileiras. In: *Anais do Workshop de Informática na Escola*. [S.l.: s.n.], 2019. v. 25, n. 1, p. 697.

[6] LEI de Diretrizes e Bases. `http://presrepublica.jusbrasil.com.br/legislacao/109224/lei-de-diretrizes-e-bases-lei-9394-96`. Acessado em 01/06/2020.

[7] BRASIL. *Base Nacional Comum Curricular: Educação é a base - Dez Competências Gerais de Educação*. Brasilia-DF: [s.n.], MEC, 2018. v. 11. 9–10 p.

[8] NOVA Escola. `https://cursos.novaescola.org.br/curso/12/competencias-gerais-na-bncc/resumo`. Acessado em 20/08/2020.

[9] AVAMEC. `https://avamec.mec.gov.br/#/instituicao/seb/curso/2817/visualizar`. Acessado em 08/09/2020.

[10] JESUS, J. A. O. d. *Utilização de modelagem matemática 3D na gestão da qualidade da água em mananciais-aplicação no Reservatório Billings*. Tese (Doutorado) — Universidade de São Paulo, 2006.

[11] SOARES, M. V. et al. Os elementos de fluxogramas: a padronização iso.

[12] MANZANO, J. A. N. G. Revisão e discussão da norma iso 5807-1985 (e) proposta para padronização formal da representação gráfica da linha de raciocínio lógico utilizada no desenvolvimento da programação de computadores a ser definida no brasil. *Revisa eletrônica Thesis. São Paulo: Faculdade Cantareira, ano*, v. 1, p. 1–31, 2004.

[13] BASE Nacional Comum - MEC. http://basenacionalcomum.mec.gov.br/implementacao. Acessado em 11/06/2020.

[14] PARECERES sobre a BNCC. http://basenacionalcomum.mec.gov.br/relatorios-e-pareceres. Acessado em 15/06/2020.

[15] NOTA técnica da Sociedade Brasileira de Computação sobre a BNCC. http://www.sbc.org.br/institucional-3/cartas-abertas/send/93-cartas-abertas/1197-nota-tecnica-sobre-a-bncc-ensino-medio-e-fundamental. Acessado em 20/01/2020.

[16] COMPUTAÇÃO na Educação Básica. http://www.youtube.com/watch?v=HOx6cpnsbpw&feature=emb_logo. Acessado em 15/06/2020.

[17] LUCIDCHART. http://www.lucidchart.com/pages/pt/o-que-e-um-fluxograma. Acessado em 25/01/2020.

[18] FLUXOGRAMAS e linguagem de programação basic e aplicações. [S.l.]: Editora Lighthouse, 2015.

[19] JGRAPH SPECIALISES IN BROWSER-BASED DIAGRAMMING COMPONENTS AND APPLICATIONS. *Draw.io*. 2020. Disponível em: <https://app.diagrams.net/>. Acesso em: 20 ago. 2020.

[20] VICARI, R. M.; MOREIRA, A. F.; MENEZES, P. F. B. Pensamento computacional: revisão bibliográfica. 2018.

[21] BRACKMANN, C. P. Desenvolvimento do pensamento computacional através de atividades desplugadas na educação básica. 2017.

[22] PROGRAMA Nacional do Livro e do Material Didático. http://portal.mec.gov.br/component/content/article?id=12391:pnld. Acessado em 15/07/2020.

[23] WIKIPEDIA/FLUXOGRAMAS. https://pt.wikipedia.org/wiki/Fluxograma. Acessado em 15/07/2020.

[24] COMO ensinar linguagem de programacao para uma criança. https://www.youtube.com/watch?v=pdhqwbUWf4U&has_verified=1. Acessado em 15/07/2020.

[25] HEFEZ, A. *Aritmética - PROFMAT*. [S.l.]: SBM, 2016.

[26] ANJOS, M. F. d. *Um estudo histórico-epistemológico do conceito de número negativo*. [S.l.]: EDUFRN, 2012.

[27] ANDRADE, R. Thé Bonifácio de. A história dos números primos. *Revista história da matemática para professores*, v. 4, n. 1, p. 18–27, mar. 2018. Disponível em: <http://www.rhmp.com.br/index/index.php/rhmp/article/view/37>.

[28] SINGH, S. *O último Teorema de Fermat*. [S.l.]: RECORD, 2000.

[29] IMPA. *Primo de Mersenne*. Disponível em: <https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/>. Acesso em: 15 de janeiro de 2019, 09:06h.

A Apêndice

A.1 Fluxogramas - Algoritmo da divisão

Relendo o trabalho para a minha defesa, percebi que ficou faltando fluxogramas que representassem o algoritmo da divisão, tanto para a divisão euclidiana, quanto para a divisão por aproximação (mais conhecida como divisão americana), que poderiam ser trabalhados no o Ensino Fundamental - Anos Iniciais, como também em aulas de reforço escolar, ajudando os alunos a realizar esses algoritmos. Então me debrucei novamente sobre o conteúdo para construir os fluxogramas a seguir.

O primeiro fluxograma é referente ao algoritmo para se efetuar a divisão euclidiana, do modo convencional. Ele serve como um roteiro para ajudar o aluno a efetuar esse algoritmo.

Fluxograma - Divisão euclidiana

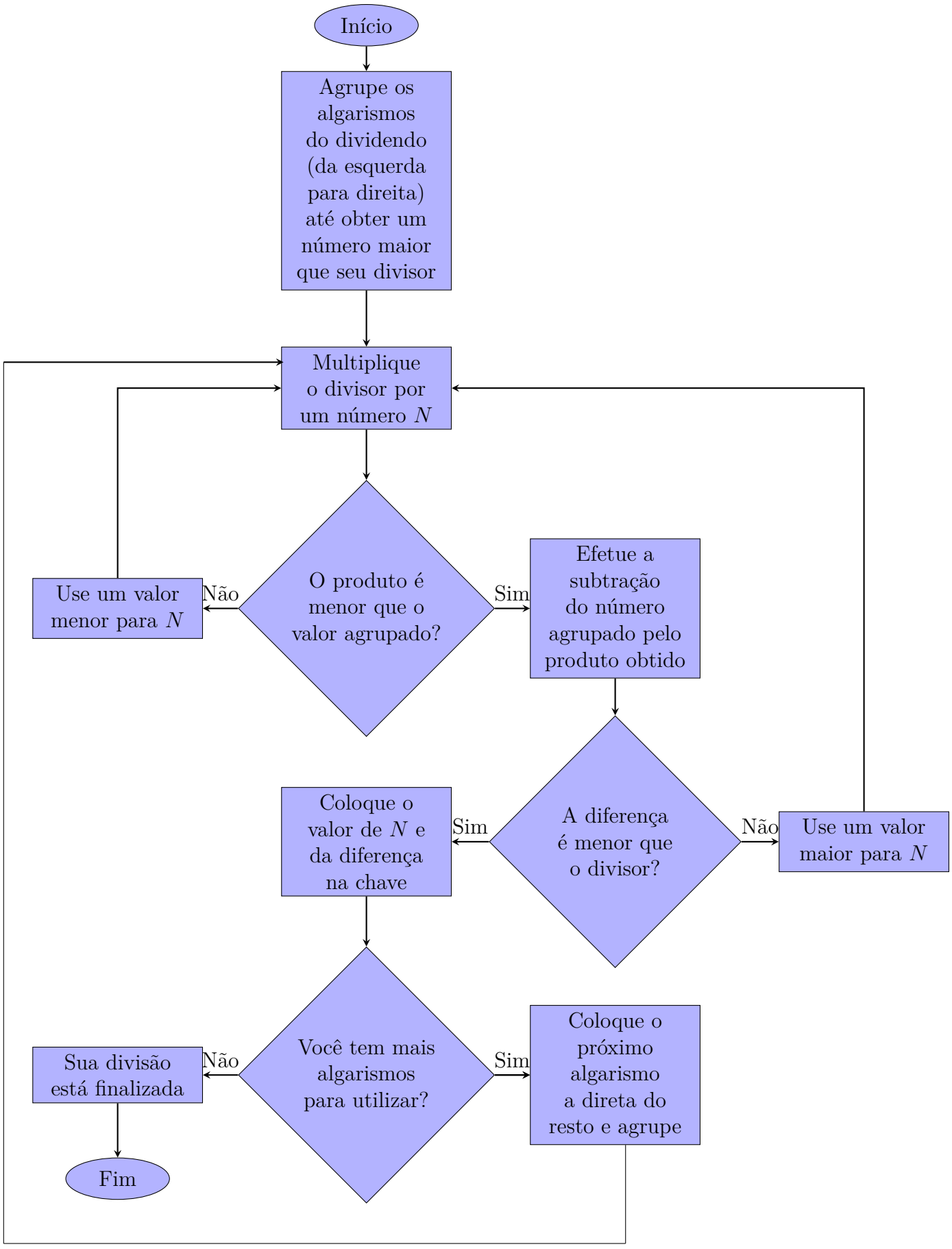


Figura A.1: Fluxograma de autoria própria - Algoritmo da divisão euclidiana

O fluxograma ficou um pouco extenso, mas como suas ações são dadas de forma simples e clara, se o aluno seguir seus passos corretamente não terá dificuldade em efetuar o algoritmo.

Agora, sejam D o dividendo e d o divisor, a divisão por aproximação, como o próprio nome diz, consiste em fazer aproximações, onde o produto de um determinador número natural n por d, não ultrapasse o valor de D.

O fluxograma a seguir, nos mostra como efetuar essa divisão utilizando esse método.

Fluxograma - Divisão por aproximação (Americana)

.

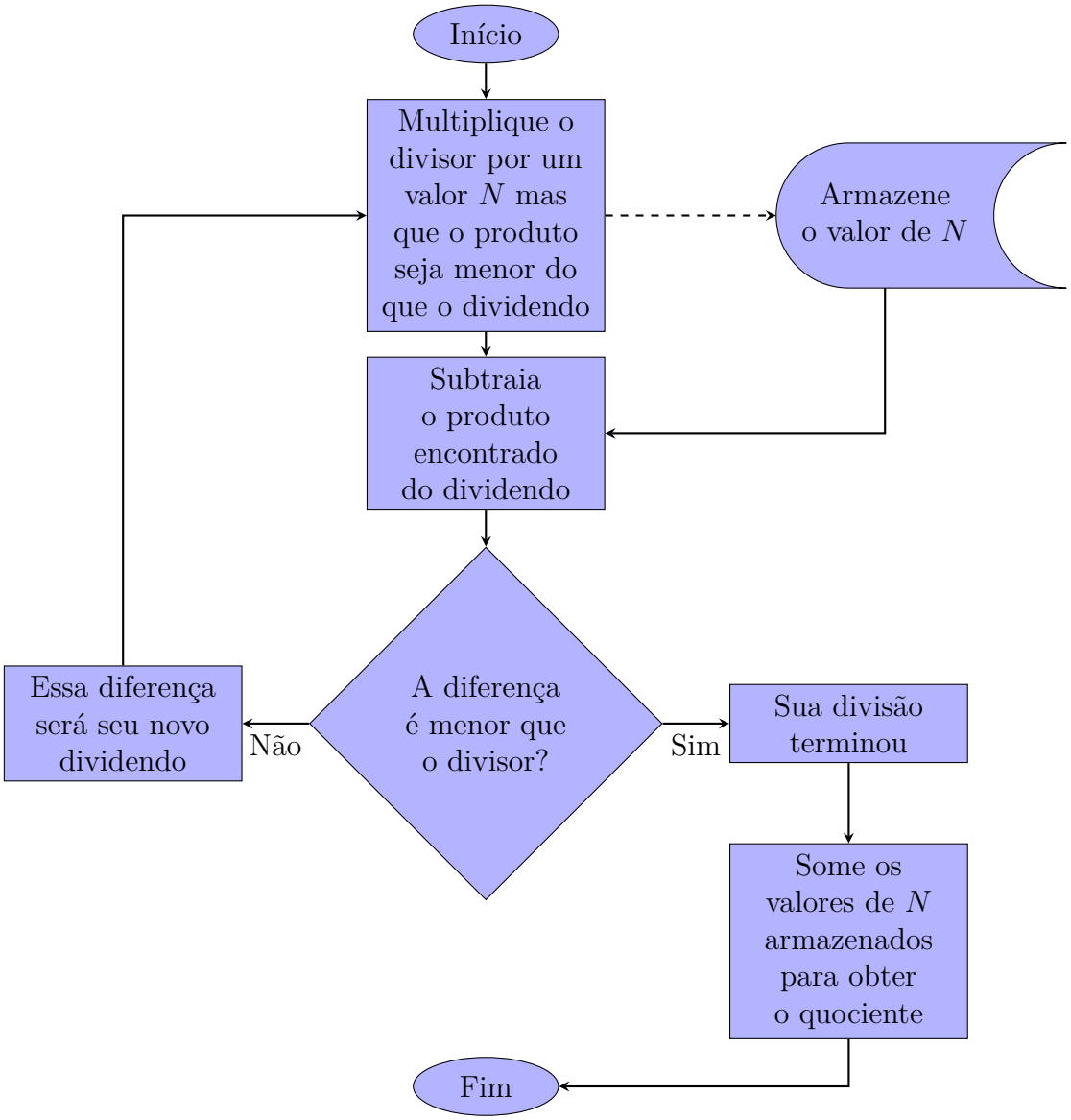


Figura A.2: Fluxograma de autoria própria - Algoritmo da divisão por aproximação (Americana)

Vamos agora ver como esse fluxograma funciona na prática.

Exemplo A.1. Divisão por aproximação - 526 dividido por 12.

$12 \times 10 = 120$ e $120 + 120 + 120 + 120 = 480$ então $(4 \times 10) \times 12 = 480$, logo $40 \times 12 = 480 \Rightarrow$ armazenar o 40.

$526 - 480 = 46$ e $46 > 12 \Rightarrow$ A divisão continua.

$12 \times 1 = 12$ e $12 + 12 + 12 = 36$ então $(1 \times 3) \times 12 = 36$ logo $3 \times 12 = 36 \Rightarrow$ armazenar o 3.

$46 - 36 = 10$ e $10 < 12 \Rightarrow$ A divisão terminou.

Somar os valores armazenados $\Rightarrow 40 + 3 = 43$ Temos então que $256 \div 12 = 43$ e o resto é 10.

Na divisão por aproximação pode ser efetuada de várias formas, dependendo dos valores utilizados na aproximação.