UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

ARITMÉTICA E APLICAÇÕES

Jair da Silva Matos

MANAUS
2017

UNIVERSIDADE FEDERAL DO AMAZONAS
INSTITUTO DE CIÊNCIAS EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
PROGRAMA DE MESTRADO PROFISSIONALIZANTE EM MATEMÁTICA

Jair da Silva Matos

ARITMÉTICA E APLICAÇÕES

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Nilomar Vieira de Oliveira

MANAUS
2017

Ficha Catalográfica

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Matos, Jair da Silva
M433a Aritmética e aplicações / Jair da Silva Matos. 2017
68 f.: 31 cm.

Orientador: Nilomar Vieira de Oliveira
Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal do Amazonas.

1. Divisibilidade . 2. Algoritmo de Euclides. 3. Congruências Modulares. 4. Pequeno Teorema de Fermat. I. Oliveira, Nilomar Vieira de II. Universidade Federal do Amazonas III. Título

Jair da Silva Matos

Aritmética e Aplicações

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Amazonas, como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovado em 29 de Novembro de 2017.

BANCA EXAMINADORA

Prof. Dr. Nilomar Vieira de Oliveira
Presidente

Prof. Dr. Roberto Antonio Cordeiro Prata
Membro

Prof. Dr. Alcides de Castro Amorim Neto
Membro

AGRADECIMENTOS

A Deus, por todas as bênçãos concedidas a meu ser até aqui, pelo dom da vida e por inspirar a humanidade à descobrir grandes coisas e realizar grandes obras especialmente na matemática.

A meus pais , pela criação que me deram, pelos ensinamentos, lições de vida e exemplo. Especialmente a meu pai por ter decidido um certo momento de nossas vidas mudar-se de uma cidade que fica interior do estado do Amazonas e buscar uma melhoria de vida na capital, Manaus, onde pude ter acesso a oportunidades educacionais que provavelmente não teria no interior onde vivíamos, e hoje tenho a oportunidade de defender um título de mestre graças as oportunidades que encontrei e abracei.

A meus colegas da turma 2015 do PROFMAT, no polo UFAM, especialmente a Mike de Souza Moraes e Francinaldo da Silva Bezerra. Durante o curso nos reuníamos eu , Naldo e Mike na residência do Mike com o fito de estudarmos para as disciplinas e exame de qualificação, por fim logramos êxito.

Ao meu orientador o professor doutor Nilomar Vieira de Oliveira, pelas contribuições a esse trabalho, pela paciência e humildade que são atributos deste grande professor.

A minha querida e amada esposa, Elça Otília Figueiredo Matos, pelo apoio e incentivo nos momentos mais difíceis que tal curso nos proporciona.

A Coordenação de Aperfeiçoamento de Pessoal de Nível Superior(CAPES) pelo incentivo financeiro, tal incentivo possibilitou-me trabalhar em meio período para dedicar-me aos estudos com mais afinco.

RESUMO

Essa dissertação de conclusão de curso tem por objetivo apresentar sucintamente algumas aplicações imediatas, embora não-triviais de Teoria dos Números-Aritmética, dentre as quais podemos destacar o Algoritmo de Euclides, congruências modulares e o Teorema Chinês dos Restos. Além destes tópicos abordados, damos uma atenção especial no início deste trabalho de conclusão de curso a alguns dos grandes matemáticos que contribuíram à aritmética entre eles, Diofante de Alexandria, Pierre de Fermat, Euclides de Alexandria entre outros. A estrutura da dissertação é a seguinte: No capítulo 2 tratamos da revisão teórica sobre os números inteiros e suas propriedades. Destacamos o Princípio da Boa Ordenação, que caracteriza os números inteiros, tratamos de algumas proposições importantes, máximo divisor comum e suas propriedades, números primos, o Teorema Fundamental da Aritmética, o Pequeno Teorema de Fermat, números de Fermat, números de Mersenne, números Perfeitos e finalizamos o capítulo 2 com o estudo das congruências e a aritmética dos restos. No capítulo 3 apresentamos algumas aplicações e iniciamos com as Equações Diofantinas Lineares, Congruências Lineares e suas resoluções, o Teorema Chinês dos Restos, Classes Residuais e, finalmente, resolvemos problemas que fizeram parte dos Exames Nacionais de Qualificação do PROFMAT desde 2012 até 2017. Tais problemas são resolvidos com as ferramentas propostas no texto, lemas, teoremas, proposições e propriedades, que facilitam a resolução. Acreditamos que tais conteúdos servem para contribuir na formação do futuro professor do Ensino Básico, assim como aprofundar os conhecimentos daqueles que já labutam na área do Ensino de Matemática.

Palavras-chave: Aritmética, Exame de Qualificação, História da Aritmética.

ABSTRACT

This dissertation aims to present succinctly some immediate, thout not trivial, Number Theory-Arithmetic applications, among which we can highlight the Euclidean Algorithm, Modular Congruences and the Chinese Remainder Theorem. In addition to these topics, we give special attention at the great mathematicians who contributed to the arithmetic among them, Diophantus od Alexandria, Pierre de Fermat, Euclides of Alexandria among others. The structure of the dissertation is as follows: in chapter 2 we deal with the theoretical revision of integers and their properties. We emphasize the Well Ordering Principle, wich characterizes whole number, we deal with some important propositions, common maximum divisor and it´s properties, prime numbers, the Fundamental Theorem of Arithmetic, Fermat´s Little Theorem, Fermat numbers, Mersenne´s Numbers, Numbers Perfect, and we end with the study of Congruences and the Arithmetic of the Remains. In chapter 3 we present some applications that we started with the Linear Diophantine Equations, Linear Congruences and Their resolutions, the Chinese Residue Theorem, Residual Classes, and finaly we solve problems that were part of the PROFMAT National Qualification Exams from 2012 to 2017. Such proplems are solved with the tools proposed in the text, lemmas, theorems, propositions and properties that facilitate resolution. We believe that these contents serve to contribute to the formation of the future teacher of Basic Education, as well as to deepen the knowledge of those who already work in the area of Mathematics Teaching.

Keywords: Arithmetic, Qualification Exam, Arithmetic History

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Conjunto dos números inteiros.
$\mathbb{Z}^+$	Conjunto dos números inteiros não negativos.
$\mathbb{Z}_*^+$	Conjunto dos números inteiros não nulos e não negativos.
$\mathbb{R}$	Conjunto dos números reais.
$=$	Igual.
$\neq$	Diferente.
$\equiv$	Congruente.
$\not\equiv$	Incongruente.
$\cong$	Aproximado.
$>$	Maior.
$<$	Menor.
$\geq$	Maior ou igual.
$\leq$	Menor ou igual.
$\cap$	Interseção.
$\cup$	União.
$\in$	Pertence.
$\notin$	Não pertence.
$\mathbb{N} \cup 0$	O conjunto dos números naturais unido com o número zero.
$\blacksquare$	Indica o fim de uma demonstração.

Sumário

Introdução

A motivação para escolher o tema e os assuntos abordados foi principalmente a necessidade de compreensão por parte dos alunos de graduação em resolver problemas de divisibilidade com números grandes, as proposições aqui abordadas tornam alguns problemas que aparentemente são muito difíceis de resolver, mas que, com a proposição ou teorema certo podem ser solucionadas de maneira fácil.

Esse trabalho pretende servir como bibliografia para alunos e professores no que tange os assuntos em aritmética, serve como fonte de estudo para alunos do PROFMAT, por resolver alguns problemas dos Exames Nacional de Qualificação.

Iniciaremos com um pouco de história da Aritmética, falando de alguns dos matemáticos antigos que contribuíram a essa área, muitos dos relatos históricos foram encontrados em [1] e em [2].

No segundo capítulo, principiamos o estudo dos números inteiros, suas propriedades e operações. Mostramos proposições importantes em divisibilidade, máximo divisor comum e suas propriedades. Em se tratando da teoria dos números, não podemos deixar de falar em números primos, no Teorema Fundamental da Aritmética, os chamados números de Mersenne, números de Fermat e números perfeitos. O capítulo 2 é finalizado com a definição de congruências, algumas observações importantes, proposições que podem nos ajudar resolver problemas, o Pequeno Teorema de Fermat em forma de congruência, que é de grande ajuda para solucionar problemas que a primeira vista são difíceis.

No capítulo 3, tratamos das aplicações das proposições, lemas, teoremas e corolários apresentados no textos. As aplicações tratam da resolução de exercícios e outros assuntos que podem ser construídos a partir das proposições. A grande maioria dos exercícios fizeram parte dos Exames Nacionais de Qualificação do PROFMAT compreendidos entre 2012 e 2017.

Capítulo 1

Um pouco de história

Neste capítulo inicial, trataremos alguns pontos da história e desenvolvimento da aritmética comentando sobre alguns dos grandes contribuidores a tal área da matemática e suas importantes contribuições. Iniciaremos com algumas contribuições de Diofante, em seguida de Pierre de Fermat, Gauss entre outros.

1.1 Diofante de Alexandria

Não sabemos ao certo o século em que viveu Diofante, mas um período aproximado de sua existência compreende os anos de 250 a 350 a.C.

Diofante publicou uma obra intitulada *Arithmetica*, onde usa uma abordagem diferente dos livros anteriormente publicados na Idade Alexandrina anterior. Na obra encontramos resoluções exatas de equações determinadas e indeterminadas com ênfase nas resoluções indeterminadas,método que ficou conhecido como análise diofantina.

Segundo Boyer, a álgebra hoje se baseia quase exclusivamente em formas simbólicas de enunciados, em lugar da linguagem escrita usual da comunicação comum em que a matemática grega anterior bem como a literatura grega se expressavam. Tem-se afirmado que podem ser reconhecidos três estágios no desenvolvimento histórico da álgebra: (1) o primitivo, ou retórico, em que tudo é completamente escrito em palavras; (2) em estágio intermediário ou sincopado, em que são adotadas algumas abreviações; e (3) um estagio simbólico ou final. Tal divisão arbitrária do desenvolvimento da álgebra em três estágios é, naturalmente, uma simplificação superficial excessiva; mas serve efetivamente como primeira aproximação ao que aconteceu, e nesse esquema a *Arithmetica* de Diofante deve ser colocada na segunda categoria. [1]

A conclusão que Boyer chegou na citação acima de que *Arithmetica* se encontra na segunda categoria deu-se devido o uso de abreviações encontradas em seis livros desta obra *Arithmetica*, neles encontramos abreviações para potências de números, para relações e operações e pra incógnitas. *Arithmetica* não expõe as operações algébricas de forma sistemática, ou funções e equações algébricas. Ela contém cerca de 150 problemas, todos com exemplos numéricos como

resolução, não se tem esforço para provar um caso geral ou achar todas as soluções possíveis.

Diofante teve maior influência na moderna teoria dos números do que qualquer outro matemático grego não geômetra. [1]

1.2 Pierre de Fermat

Em 1621, a *Arithmética* de Diofante tinha ressurgido na edição grega e latina publicada por Claude Gaspard de Bachert $(1591 - 1639)$, membro de um grupo informal de cientistas em Paris.

Essa obra de Diofante influenciou um, dos que vieram a se tornar grandes matemáticos, Pierre de Fermat. Pierre de Fermat viveu entre 1601 e 1665, ele foi o fundador da teoria moderna dos números. Suas contribuições abrangem; divisibilidade, números perfeitos, amigáveis, números figurados, quadrados mágicos, ternas pitagóricas e números primos.

Uma prova de que a versão de *Arithmética* publicada por Bachert influenciou Fermat é, que ele escreveu em seu exemplar da obra que tinha uma demontração para um teorema $x^n+y^n = z^n$ com $n > 2$ inteiro, tal demonstração permanece perdida.

Desde os tempos antigos, até o presente, tem havido uma busca para determinar uma fórmula geral que defina todos o números primos, antes do tempo de Fermat havia uma "hipótese chinesa"de que, o n é primo se e somente se, $2^n - 2$ é divisível por n pra $n > 1$ inteiro. Hoje sabemos que essa hipótese é falsa. Uma generalização para isso ficou conhecida com Pequeno Teorema de Fermat.

Fermat foi um dos que conjecturou fórmula para os números primos, $2^{2^n} + 1$ que ficaram conhecidos como "números de Fermat", entretanto ele examinou apenas os números $(0, 1, 2, 3, 4)$ como possíveis valores para n, Euler mostrou que essa conjectura era falsa, pois $2^{2^5} + 1$ é composto. Se Fermat tivesse feito mais um pouco de cálculo, ele mesmo veria que não é um caso geral. Mas além do 5 muitos outros não resultam em número primo.

Uma das contribuições de Pierre de Fermat foi o Pequeno Teorema de Fermat (P.T.F), Leibniz demonstrou tal teorema e Euler em 1736 foi o primeiro a publicar uma demonstração. Fermat fez maiores descobertas em matemática, ou contribuiu mais para ela, do que qualquer outro matemático profissional de sua época, mas por ser modesto não publicava muito. Havia um matemático chamado Marin Mersenne, um frade Minimita, ao qual Fermat escrevia suas descobertas, ele serviu como centro de distribuição da informação matemática pois, quando sabia de alguma coisa, toda a "República das Cartas"eram prontamente informadas.

1.3 Leonard Euler

Euler $(1707 - 1783)$ nascido na Suíça e um dos matemáticos mais importantes de sua época, aos 26 anos tornou-se um dos principais matemáticos da academia de S. Petersburgo. Euler

publicou mais de 500 livros e artigos durante sua vida, devido sua facilidade em escrever tais artigos.

Euler foi atraído pela teoria dos números assim como Fermat, apesar de Euler não ter publicado um livro sobre a teoria dos números, escreveu cartas e artigos sobre o assunto. Lembremos que ele derrubou umas das conjecturas de Fermat sobre a fórmula dos números primos, isso graças a sua facilidade em computação.

Uma conjectura formulada por Euler foi que se $n > 2$ pelo menos n potências n-ésimas são necessárias para fornecer uma soma que seja ela própria uma potência n-ésima, mas em 1966 foi provado que essa afirmação é falsa com o seguinte contra-exemplo:

$$27^5 + 84^5 + 110^5 + 133^5 = 144^5$$

Ele foi o primeiro a publicar uma demonstração para o pequeno teorema de Fermat, após ele generalizou o P.T.F e criou o que veio a se chamar a "função de Euler"com o seguinte enunciado. Se m é um inteiro positivo maior que um, a função de $\phi(m)$ é definida como o número de inteiros menores que m que são primos com m (mas incluindo o inteiro 1 em cada caso). Costuma-se definir $\phi(1) = 1$; para $n = 2, 3$ e 4, por exemplo, os valores de $\phi(n)$ são $1, 2$ e 2 respectivamente. Se p é um primo, então claramente $\phi(p) = p - 1$ e pode-se demonstrar que

$$\phi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_r}).$$

Ele também resolveu pesquisar números amigáveis, que Fermat conhecia apenas três pares, Euler acrescentou mais outros números aos conhecidos por Fermat, totalizando mais de sessenta pares de números amigáveis conhecidos por Euler.

Euler deu Contribuições também aos números perfeitos, demonstrando que todos os números perfeitos pares são da forma dada por Euclides:

$$2^{n-1}(2^n - 1), \text{ onde } 2^n - 1 \text{ é primo.}$$

Não sabemos se existe número perfeito ímpar é algo que ainda está sujeito a demonstração.

Em correspondência com Euler um matemático chamado Christian Goldbach disse que , todo inteiro par maior que dois é a soma de dois primos. Tal afirmação ficou conhecida como teorema de Goldbach e apareceu impresso em 1770, na Inglaterra, mas sem demonstração. Euler também demonstrou que todo inteiro positivo é a soma de não mais que quatro quadrados.

1.4 Euclides de Alexandria

Sabe-se que ele viveu no século III a.C. Ele também deu importantes contribuições em aritmética, uma das publicações mais conhecidas dele é *Os elementos*, sua primeira edição impressa foi em 1482, composto por treze livros, dos quais três tratam da teoria dos números, vale

ressaltar que quando os gregos falavam sobre número referiam-se aos números naturais que conhecemos hoje.

Dos livros de *Os elementos* o VII, VIII e IX tratam de teoria dos números, no VI contém definições que distingue vários tipos de números, como por exemplo, números ímpares, pares, primos, compostos, planos (ou múltiplos de dois inteiros) e sólidos (múltiplos de três inteiros). Nesse livro Euclides define também número perfeito.

No livro VII encontramos o conhecido "algoritmo de Euclides"para encontrar o máximo divisor comum entre dois números. O método é um primor do ponto de vista educacional e pouco conseguiu-se aperfeiçoar em mais de dois mil anos.

No livro VIII, encontramos proposições sobre números em progressão aritmética, propriedades de quadrados e cubos de números e finaliza com a proposição a seguir:

Números sólidos semelhantes têm entre si a razão que um número cúbico tem para um número cúbico.

No livro IX demonstra-se uma proposição que mostra contradição em haver um número finito de primos, levando a conclusão que há infinitos números primos. Nesse livro Euclides mostra uma fórmula para a soma dos termos de uma progressão geométrica, e a última proposição do livro trata dos números perfeitos.

1.5 Carl Friedrich Gauss

Gauss $(1777 - 1855)$ contribuiu com importantes publicações em teoria dos números, sua tese de doutorado, intitulada *Disquisitiones Arithmeticae*, é um dos clássicos da literatura matemática.

Disquisitiones Arithmeticae possui sete seções, as quatro primeiras tratam de uma reformulação compacta da teoria dos números so século $XVIII$, inclusive os conceitos de congruências e classes de restos.

A secção cinco trata da teoria das formas quadráticas binárias, onde as técnicas para a solução de equações do tipo $ax^2 + bxy + cy^2 = m$ serviram de base para muitos trabalhos de gerações posteriores na teoria dos números. A seção seis consiste em várias aplicações. A última seção trata da resolução da equação ciclotômica geral de grau primo.

Nessa obra Gauss inclui também o teorema fundamental da aritmética com uma rigorosa demonstração. Na época a introdução de novos métodos era vista com ceticismo até que fosse provado que, além de úteis eram superiores às técnicas existentes e que contribuiriam até mesmo para um experiente pesquisador, por isso poucos corresponderam-se com Gauss para trocar conhecimento sobre teoria dos números. Um desses poucos era um monge chamado "Monsieur Leblanc ", que na verdade era Sophie Germain, matemática francesa, que usava o pseudo de Leblanc para se corresponder com grandes matemáticos de sua época, onde era proibida às mulheres o acesso à matemática [4] página 60.

Gauss deu outras contribuições em aritmética, ele procurou teoremas para congruências do tipo $x^n \equiv p(\mod q)$ para $n = 3$ *e* $n = 4$. Para esses casos criou os chamados inteiros de Gauss, números da forma $a + bi$ com $a, b \in \mathbb{Z}$. Mas encontrou um problema quando se tratava de números primos, pois 5 já não é primo da forma $a + bi$ já que $(1 + 2i)(1 - 2i) = 5$. Os números primos da forma $4n + 1$ não são primos de Gauss, mas os números primos da forma $(4n - 1)$ são primos da forma $(a + bi)$, ou seja, primos de Gauss.

1.6 Pitágoras de Salmos e alguns pitagóricos

Foi um contemporâneo de Buda, Confúsio e Laozi(Lao-TZU), viveu aproximadamente (580 $A.C$ - 500 $A.C$). Estabeleceu-se em Crotona ao retornar ao mundo Grego. Fundou uma sociedade secreta para estudos matemáticos e filosóficos, a frase "tudo é número", é um possível lema dessa sociedade. Os pitagóricos tiveram um papel importante na teoria dos números, seus escritos aritméticos eram essencialmente exercícios de aplicação de processos numéricos a problemas específicos. Eles tinham uma adoração pelos números, baseavam neles o seu modo de vida e sua filosofia.

O número *um* é o gerador dos números, o *dois* o primeiro par, ou feminino, pois para eles os números pares tinham atributos femininos e os ímpares atributos masculinos, *dois* era o número da opinião. *Três* é o primeiro número masculino verdadeiro, o da harmonia, sendo composto de unidade e diversidade. *Quatro* indicava o ajuste de contas, a justiça, *cinco* o casamento, *seis* a criação, *sete* era muito respeitado (talvez pelas sete estrelas errantes), a semana derivou do respeito que eles tinham pelo *sete*, *dez* era o mais sagrado, não fazendo alusão aos dedos dos pés ou mãos humanos, mas era para eles o número do universo.

As idéias de Pitágoras e seus seguidores deram maior desenvolvimento a aritmética, eles a tornaram um ramo da filosofia e parecem ter feito dela uma base para unificar todos os aspectos do mundo que os rodeava. Com as contribuições pitagóricas a aritmética passou a um nível intelectual, ao invés de ser vista apenas como aritmética prática. Na época, aritmética prática, não merecia atenção dos filósofos e portanto não eram registradas nas grandes bibliotecas.

Um dos últimos pitagóricos e figura de transição na matemática no tempo de Platão foi Arquitas, ele acreditava que o número era o que havia de mais importante na vida e na matemática. O *quadrivium*, que era composto por, aritmética, geometria, música e astronomia, foi disponibilizado para estudo liberal possivelmente por Arquitas, seus pensamentos iriam dominar o pensamento pedagógico até nossos dias. Mais tarde, também possivelmente por influência de Arquitas, Platão teve influência para que a matemática fizesse parte do currículo para a educação de "homens de estado".

Nicômaco de Gerasa foi um dos que contribuíram à aritmética, neopitagórico que viveu por volta de 100 d.C perto de Jerusalém, escreveu uma obra intitulada *Introductio arithmeticae*, tal obra possui dois livros, mas acredita-se que é uma obra resumida e que havia outra publicação mais extensa.

Nicômaco não era um matemático tão competente e se ocupava com os tratados mais elementares dos números. Na obra citada, ele principia em classificar os números em pares e ímpares, em seguida classifica-os em parmente pares (potência de dois) e parmente ímpares $(2^n p)$ onde p é ímpar maior que 1 e $n > 1$, ele classifica também em imparmente pares ($2p$, onde p é ímpar maior que 1). Ele define os números primos, compostos e perfeitos, descreve o crivo de Eratóstenes, uma lista dos quatro primeiros números perfeitos $(6, 28, 496, 8128)$, entre outros assuntos.

Para Nicômaco o número *três* era o primeiro número no sentido estrito da palavra, os números *um* e *dois* eram apenas geradores do sistema numérico.

Um teorema mais sofisticado que aparece na obra de Nicômaco é o que descreve que se os inteiros ímpares são agrupados da seguinte forma $1; 3 + 5; 7 + 9 + 11; 13 + 15 + 17; \ldots$ as somas sucessivas são cubos dos inteiros. Note que $1 = 1^3$, $8 = 2^3$(que é o número de parcelas que aparece na soma), $27 = 3^3$, assim por diante. Tal observação unida com a observação pitagórica de que a soma dos n primeiros ímpares é igual a n^2, leva-nos a concluir que a soma dos n primeiros cubos perfeitos é igual ao quadrado da soma dos n primeiros inteiros.

Capítulo 2

Noções de Aritmética

2.1 Números inteiros

Iniciaremos com uma noção do Conjunto dos números inteiros, mas admitindo que o leitor já possua um bom conhecimento do mesmo.

O Conjunto dos números inteiros é representado pela letra $\mathbb{Z}$ e possui os seguintes elementos

$$\mathbb{Z} = \{ \cdots, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 \cdots \}.$$

No decorrer desta secção enunciaremos as propriedade dos números inteiros em relação a adição e multiplicação.

Propriedades dos números inteiros.

Observação 2.1. *As operações de multiplicação e adição estão bem definidas nos inteiros, ou seja, todo número inteiro quando somado ou multiplicado por outro número inteiro obtemos como resultado um número inteiro. Isso nos permite somar ou multiplicar um número qualquer a ambos lados de uma igualdade. No entanto a operação de divisão não está bem definida.*

A seguir enunciaremos as propriedades em relação as operações de adição e multiplicação de números inteiros.

Propriedade 2.1. *A multiplicação e a adição de números inteiros são comutativas:*

$$\forall x, y \in \mathbb{Z} \;\; x \cdot y = y \cdot x \; \textbf{e} \; x + y = y + x.$$

Propriedade 2.2. *A multiplicação e a adição de números inteiros são associativas:*

$$\forall x, y, z \in \mathbb{Z} \;\; (x \cdot y) \cdot z = x \cdot (y \cdot z) \; \textbf{e} \; (x + y) + z = x + (y + z).$$

Propriedade 2.3. *A multiplicação e a adição de números inteiros possuem elementos neutros:*

$$\forall x \in \mathbb{Z} \;\; x \cdot 1 = x \; \textbf{e} \; x + 0 = x.$$

Propriedade 2.4. *A adição de números inteiros possui elemento simétrico:*

$$\forall x \in \mathbb{Z} \ \exists y(=-x) \textit{ tal que } x+y=0\textit{, onde } 0 \textit{ é o elemento neutro da adição.}$$

Propriedade 2.5. *A multiplicação é distributiva em relação à adição:*

$$\forall x, y, \in \mathbb{Z} \textit{ temos, } x \cdot (y+z) = xy + xz.$$

Aceitaremos as propriedades acima como axiomas, ou seja, sem necessidade de prova. Entretanto tais propriedades não caracterizam os números inteiros, visto que, um conjunto munido das operações soma e multiplicação que satisfazem a propriedades acima descritas é chamado *anel* e além dos inteiros outros conjuntos satisfazem tais axiomas, como por exemplo, os números reais($\mathbb{R}$), os números racionais($\mathbb{Q}$) e os números complexos($\mathbb{C}$). Sendo assim ao observar um número x satisfazendo os referidos axiomas não podemos garantir que x seja um número inteiro. Trataremos aqui de outras propriedades que diferenciam o conjuntos dos números inteiros desses outros conjuntos.

Observação 2.2. *O conjunto dos números inteiros é formado pela união de três conjuntos, a saber: Os números naturais, o conjunto contendo apenas o número zero e o conjunto dos simétricos dos números naturais, em símbolos* $\mathbb{Z} = \mathbb{N} \cup \{0\} \cup (-\mathbb{N})$.

Proposição 2.1. $x \cdot 0 = 0 \ \forall \ x \in \mathbb{Z}$.

Demonstração. Pela Propriedade 2.3 , transformamos o 0 do primeiro membro da igualdade em, $0 = (0+0)$, o que resulta em, $x \cdot (0+0) = x \cdot 0$. Usando a Propriedade 2.5 obteremos $x \cdot 0 + x \cdot 0 = x \cdot 0$, somando $(-x \cdot 0)$ a ambos membros a igualdade temos:

$$x \cdot 0 + x \cdot 0 - x \cdot 0 = x \cdot 0 - x \cdot 0$$

usando a Propriedade 2.4 no segundo membro da igualdade, segue que, $x \cdot 0 + x \cdot 0 - x \cdot 0 = 0$. Novamente usando a Propriedade 2.4, agora no primeiro membro, temos:

$$x \cdot 0 + 0 = 0$$

Por fim, usando a Propriedade 2.3, obtemos

$$x \cdot 0 = 0$$

■

2.2 Ordenação dos Inteiros

Em $\mathbb{Z}$ também valem as seguintes propriedades:

Propriedade 2.6. *Fechamento de $\mathbb{N}$: O conjunto dos números Naturais é fechado para a adição e para a multiplicação, ou seja, para $x, y \in \mathbb{N}$, tem-se que $x + y \in \mathbb{N}$ e $xy \in \mathbb{N}$.*

Propriedade 2.7. *Tricotomia: Dados $x, y \in \mathbb{Z}$, uma, e somente uma, das possibilidades a seguir é verdadeira:*

1. $x = y$;
2. $y - x \in \mathbb{N}$;
3. $-(y - x) = (x - y) \in \mathbb{N}$.

Observação 2.3. *Diremos que x é menor do que y, em símbolos $x < y$, toda vez que a possibilidade 2 acima for satisfeita.*

De acordo com a Observação 2.3, a possibilidade 3, acima mencionada, é equivalente a escrever $y < x$ e lemos, y é menor do que x.

Propriedade 2.8. *A relação **menor do que** é transitiva:*

$$\forall x, y, z \in \mathbb{Z},\ x < y \ \textbf{e}\ y < z \Longrightarrow x < z.$$

Demonstração. Supondo $x < y$ e $y < z$, temos que $y - x \in \mathbb{N}$ e $z - y \in \mathbb{N}$. O conjunto dos números naturais é fechado em relação a adição, ou seja, a soma de dois números naturais resulta em outro número natural. Assim como $z - x = (y - x) + (z - y)$ sabemos que $y - x \in \mathbb{N}$ e $z - y \in \mathbb{N}$ logo $z - x \in \mathbb{N}$, o que nos dar $x < z$. ■

Propriedade 2.9. *A adição é compatível e cancelativa com respeito à relação **menor do que**:*

$$\forall x, y, z \in \mathbb{Z},\ x < y \Longleftrightarrow x + z < y + z.$$

Demonstração. Supondo $x < y$, $y - x \in \mathbb{N}$, como $y - x = (y + z) - (x + z)$ e sabemos que $y - x \in \mathbb{N}$ logo $x + z < y + z$.

Reciprocamente, supondo $x + z < y + z$ temos que $(y + z) - (x + z) \in \mathbb{N}$, mas $(y + z) - (x + z) = y - x \in \mathbb{N}$. Assim $x < y$.

■

Propriedade 2.10. *A multiplicação por elementos de $\mathbb{N}$ é compatível e cancelativa com respeito à relação **menor do que**:*

$$\forall x, y \in \mathbb{Z}, \forall z \in \mathbb{N}, x < y \Longleftrightarrow xz < yz.$$

Demonstração. Supondo que $x < y$. Então, $y - x \in \mathbb{N}$. Assim, como $\mathbb{N}$ é fechado em relação a multiplicação, seja $z \in \mathbb{N}$ temos:

$$yz - xz = (y - x)z \in \mathbb{N}$$

logo, $xz < yz$

Reciprocamente, supondo que $xz < yz$, com $c \in \mathbb{N}$. Pela tricotomia temos três possibilidades para analisar:

1. $x = y$. Mas isso resultaria em $xz = yz$ o que é falso;

2. $y < x$. Mas, pela primeira para da demonstração, isso resultaria em $yz < xz$, para $z \in \mathbb{N}$. O que é falso.

3. $x < y$ é a única possibilidade verdadeira.

■

Propriedade 2.11. *A multiplicação é compatível e cancelativa com respeito à igualdade:*

$$\forall x, y \in \mathbb{Z}, \forall z \in \mathbb{Z}\backslash\{0\},\ x = y \iff xz = yz.$$

Demonstração. A implicação $x = y \implies xz = yz$ decorre imediatamente do fato de a multiplicação estar bem definida nos inteiros. Vale também para $z = 0$.

Supondo agora que $xz = yz$. Temos duas possibilidades:

1. Caso $z > 0$. Se $x < y$, pela Propriedade 2.10, temos que $xz < yz$, o que é um absurdo. Se $y < x$, também pela Propriedade 2.10, $yz < xz$, o que é um absurdo. Portanto a única alternativa válida é $x = y$.

2. Caso $-z > 0$. Se $x < y$, usando o fato que, $d < f \iff -d > -f$, ou seja, $z < 0$. Assim $-zx < -zy$, se e somente se, $zy < zx$ o que é um absurdo. Se $y < x$ analogamente $-zy < -zx$ se e somente se, $zx < zy$ o que é um absurdo. Logo $x = y$ é a única possibilidade válida.

■

Observação 2.4. *Note que a relação $<$ não é uma relação de ordem, pois não é reflexiva, ou seja, $x < x$ é falso.*

Observação 2.5. *Diremos que x é menor ou igual do que y, ou que y é maior ou igual do que x, escrevendo $x \leq y$ ou $y \geq x$, se $x < y$ ou $x = y$.*

Na observação acima $x \leq y \iff y - x \in \mathbb{N} \cup \{0\}$. O que nos permite verificar com facilidade que essa nova relação é uma relação de ordem. Portanto possui as seguintes propriedades:

- É reflexiva: $\forall x \in \mathbb{Z}$, $x \leq x$;
- É antissimétrica: $\forall x, y \in \mathbb{Z}$, $x \leq y$ e $y \leq x \implies x = y$;
- É transitiva: $\forall x, y, z \in \mathbb{Z}$, $x \leq y$ e $y \leq z \implies x \leq z$.

Agora vamos definir o valor absoluto de um número inteiro.

Seja $x \in \mathbb{Z}$ definimos:

$$|x| = x, \text{ se } x \geq 0 \text{ ou } |x| = -x, \text{ se } x < 0$$

Observação 2.6. *Observe que* $\forall x \in \mathbb{Z}$*, tem-se que* $|x| \geq 0$ *e* $|x| = 0 \iff x = 0$*.*

Ao número inteiro $|x|$ chamaremos *módulo de x* ou *valor absoluto de x*.

Vamos agora enunciar as principais propriedades do valor absoluto.

$\forall x, y \in \mathbb{Z}$ *e* $a \in \mathbb{N}$ temos:

1. $|xy| = |x||y|$;
2. $|x| \leq a \iff -a \leq x \leq a$;
3. $-|x| \leq x \leq |x|$;
4. a desigualdade triangular

$$||x| - |y|| \leq |x \pm y| \leq |x| + |y|.$$

2.2.1 Principio da Boa Ordenação

Descrevemos até aqui algumas propriedades dos números inteiros e suas operações mas, tais propriedades não caracterizam os números inteiros, tendo em vista que os números racionais, os números reais, os racionais positivos e os números reais positivos possuem as propriedades citadas até aqui. Então se um conjunto possui essas propriedades não podemos garantir que é o conjunto dos números inteiros, pode ser os reais ou outro.

Descreveremos a seguir o *Princípio da Boa Ordenação*, que é uma propriedade exclusiva dos números inteiros.

Definição 2.1. *Diremos que um subconjunto* A *de* $\mathbb{Z}$ *é limitado inferiormente, se existir* $z \in \mathbb{Z}$ *tal que* $z \leq a$ *para todo* $a \in A$*. Diremos que* $x \in A$ *é um menor elemento de* A *se* $x \leq a$ *para todo* $a \in A$*.*

Observação 2.7. *O conjunto vazio, apesar de não possuir elementos, é limitado inferiormente, e qualquer número pode ser uma cota inferior do conjunto vazio.*

Observação 2.8. *Se um existir um menor elemento para* A*, ele é único. Isso vem do fato que se* a *e* b *são menores elemento de* A *então,* $a \leq b$ *e* $b \leq a$ *o que resultaria em* $a = b$*.*

Propriedade 2.12. *Princípio da Boa Ordenação: Se* A *é um subconjunto não vazio de* $\mathbb{Z}$ *e limitado inferiormente, então* A *possui um menor elemento.*

Observação 2.9. *Qualquer subconjunto de* $\mathbb{N}$ *é limitado inferiormente, por* 1*, assim todo subconjunto de* $\mathbb{N}$ *possui um menor elemento.*

A propriedade acima, juntamente com as anteriores, caracteriza os números inteiros, e com essas propriedades podemos deduzir qualquer propriedade dos números inteiros.

A seguir mostraremos alguns exemplos de propriedades do conjunto dos números inteiros que são demonstradas com o auxílio do *Princípio da Boa Ordenação*.

Exemplo 2.1. *O subconjunto* $A_1 = (0, 1)$ *dos números inteiros possui apenas dois elementos,* 0 *e* 1*, ou seja, não existe* $x \in A_1$ *tal que* $0 < x < 1$.

Demonstração. Supondo por absurdo que exista $x \in A_1$ tal que $0 < x < 1$, então o conjunto A_1=$\{x \in \mathbb{Z}; 0 < x < 1\} \subset \mathbb{Z}$ é não vazio e limitado inferiormente. Portanto, A_1 possui um menor elemento y, com $0 < y < 1$. Nesta última desigualdade, multiplicando por y, obtemos $0 < y^2 < y < 1$, logo $y^2 \in A_1$ e $y^2 < y$, o que é uma contradição, pois y é o menor elemento de A_1 portanto $A_1 = \emptyset$ e A possui apenas dois elementos. ■

Exemplo 2.2. *Dado um número inteiro* x *qualquer, não existe nenhum número inteiro* y *tal que* $x < y < x + 1$.

Demonstração. Supondo por absurdo que exista $y \in \mathbb{Z}$ tal que $x < y < x + 1$, subtraindo x nessa desigualdade temos, $0 < y - x < 1$, o que contradiz o Exemplo 2.1. ■

Exemplo 2.3. *Sejam* $x, y \in \mathbb{Z}$*. Se* $xy = 1$*, então* $x = y = \pm 1$.

Demonstração. Notemos inicialmente que $x \neq 0$ e $y \neq 0$, pois do contrário $xy = 0$. Assim, nos resta duas possibilidades, $x > 0$ ou $x < 0$.

Supondo $x > 0$. Como $xy = 1$, temos que $y > 0$. Segue-se do Exemplo 2.1 que $x \geq 1$ e $y \geq 1$. logo, $1 = xy \geq y \geq 1$, o que implica $y = 1$. Como $xy = 1$, temos que $x = 1$.

Para o caso em que $x < 0$ vamos adaptar o Exemplo 2.1 para o seguinte, não existe nenhum número inteiro x tal que $-1 < x < 0$.

Agora supondo $x < 0$. Como $xy = 1 > 0$, temos que $y < 0$. Segue da adaptação do Exemplo 2.1 que $x \leqslant -1$ e $y \leqslant -1$. Logo, $1 = xy \geqslant y \leq -1$, o que implica $y = -1$. Como $xy = 1$, temos que $x = -1$. ■

O conjunto dos números inteiros tem uma importante propriedade chamada propriedade Arquimediana, que enunciaremos a seguir.

Propriedade 2.13. *Propriedade Arquimediana: Sejam* $x, y \in \mathbb{Z}$*, com* $y \neq 0$*. Então existe* $a \in \mathbb{Z}$ *tal que* $ay > x$.

Demonstração. Como $|y| \neq 0$, do Exemplo 2.1, temos que $|y| \geq 1$ assim, multiplicando $|x|+1$ na desigualdade acima resulta em, $|y|(|x| + 1) \geq |x| + 1 \geq |x| \geq x$.

O resultado desejado segue-se tomando na desigualdade acima $a = |x| + 1$, se $y > 0$ e $a = -(|x| + 1)$, se $b < 0$.

■

Enunciaremos a seguir o **Princípio de Indução Matemática** que servirá como auxilio para importantes demonstrações que faremos mais no decorrer do texto.

Teorema 2.1. *Sejam X um subconjunto de* $\mathbb{Z}$ *e* $y \in \mathbb{Z}$ *tais que:*

1. $y \in X$
2. X *é fechado em relação à operação "adicionar 1" a seus elementos, ou seja,* $\forall a$, $a \in X \Longrightarrow a + 1 \in X$.

Então, $\{c \in \mathbb{Z}; c \geq y\} \subset X$

O teorema acima é de tal importância a que dar origem a outro teorema que nos auxilia na prova de teoremas importantes em matemática, o qual enunciaremos a seguir.

Teorema 2.2. *Seja* $x \in \mathbb{Z}$ *e seja* $P(n)$ *uma sentença aberta em n. Suponha que :*

1. $P(x)$ *é verdadeiro, e que*
2. $\forall n \geq x,\ P(n) \Longrightarrow P(n+1)$ *é verdadeiro.*

Então, $P(n)$ *é verdadeiro para todo* $n \geq x$

Demonstração. Consideremos o conjunto $S = \{n \in \mathbb{N}; P(n)$ é falso$\}$. Vamos mostrar que $S = \varnothing$, resultando que $P(n)$ é verdadeiro para todo $n \in \mathbb{N}$.

Suponhamos que $S \neq \varnothing$. Como S é um subconjunto não-vazio dos números naturais, existe $n_0 = \min S$, pelo Princípio da Boa Ordenação dos números naturais. Devido $P(x)$ ser verdadeiro, temos $x \notin S$, isto é, $n_0 > x$.

Como n_0 é o menor elemento de S, o número $n_0 - 1 \notin S$. Assim, $P(n_0 - 1)$ é verdadeiro, e pela hipótese indutiva, $P[(n_0 - 1) + 1] = P(n_0)$ é verdadeiro. Mas, $n_0 \in S$, pois é o menor elemento de S. Temos uma contradição: $n_0 \in S$ e $n_0 \notin S$.

Portanto, $S = \varnothing$, e com as hipóteses do problema, temos que $P(n)$ é verdadeiro para todo $n \geq x$.

■

A seguir mostraremos alguns exemplos que podem ser demonstrados com o auxílio do Principio de Indução Matemática.

Exemplo 2.4. *A soma dos primeiros* n *números naturais pode ser obtida pela fórmula* $S(n) = \dfrac{n(n+1)}{2}$.

Demonstração. Seja $P(n) = \{n \in \mathbb{N}; S(n) = \dfrac{n(n+1)}{2}\}$.

1. $P(1)$ é verdadeira, pois $P(1) = \dfrac{1(1+1)}{2} = \dfrac{2}{2} = 1$.

2. Agora supondo que $P(k)$ seja verdadeira, vamos provar que $P(k+1)$ é verdadeira, ou seja $P(k) \Longrightarrow P(k+1)$.

   Como $P(k)$ é válido então, $S(k) = \dfrac{k(k+1)}{2}$. Na igualdade anterior, ao somarmos a ambos membros $k+1$ obteremos $S(k) + (k+1) = \dfrac{k(k+1)}{2} + (k+1)$, o primeiro membro dessa igualdade corresponde a somar $(k+1)$ números inteiros, ou seja, $S(k+1)$, Assim $S(k+1) = \dfrac{k(k+1)}{2} + (k+1)$ aplicando as propriedades dos números inteiros chegamos a $S(k+1) = \dfrac{k(k+1)+2(k+1)}{2} = \dfrac{(k+1)(k+2)}{2}$. O que nos mostra que $P(k+1)$ é verdadeiro.

■

No decorrer do texto mostraremos algumas proposições que podem ser demonstradas usando o Princípio de Indução Matemática.

2.3 Divisibilidade

Definição 2.2. *Dados dois números inteiros a e b, diremos que a divide b, escrevendo $a \mid b$, quando existir $c \in \mathbb{Z}$ tal que $b = ca$. Nesse caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a ou que b é divisível por a.*

Proposição 2.2. *Sejam $x,\ y,\ z \in \mathbb{Z}$. Tem-se que:*

1. $1 \mid x$, $x \mid x$ *e* $x \mid 0$;
2. $0 \mid x \Longleftrightarrow x = 0$;
3. x *divide* y *se, e somente se,* $|x|$ *divide* $|y|$;
4. *se* $x \mid y$ *e* $y \mid z$, *então* $x \mid z$.

Demonstração. Para demonstrar 1) usaremos a Propriedade 2.3 dos números inteiros, $x = x \cdot 1$ e como a definição de divisibilidade exige a existência de um $c \in \mathbb{Z}$ tal que $x = c \cdot 1$, fazendo $c = x$ obtemos o desejado, logo $1 \mid x \ \forall\ x \ \in \mathbb{Z}$.

Usaremos ainda a Propriedade 2.3 , juntamente com a Propriedade 2.1 dos números inteiros para mostrar que $x \mid x$. Assim, $x = x \cdot 1 = 1 \cdot x$ e fazendo $c = 1$ concluímos pela definição de divisibilidade que $x \mid x \ \forall x \in \mathbb{Z}$.

Para $x \mid 0$, como $0 = 0 \cdot x$ e fazendo $c = 0$ obtemos o desejado.

2) $(\Longrightarrow)$

$$0 \mid x \Rightarrow x = 0$$

Se $0 \mid x$ temos, pela definição de divisibilidade, que $x = c \cdot 0$ para algum $c \in \mathbb{Z}$ e pela Proposição 2.1 concluímos que $x = 0$.

($\Longleftarrow$)

$x = 0 \Longrightarrow 0 \mid x$.

Se $x = 0$ basta mostrar que $0 \mid 0$, o que ja fizemos no item i) já que $x \mid 0$
$\forall x \in \mathbb{Z}$ então vale para $x = 0$.

3) $x \mid y \Longrightarrow |x|$ divide $|y|$.

Se $x \mid y$ então $\exists c \in \mathbb{Z}$ tal que $y = c \cdot x$, aplicando o módulo a ambos membros da igualdade obtemos $|y| = |c \cdot x| = |c||x|$, agora fazendo $|c| = d \in \mathbb{Z}$ (como $c \in \mathbb{Z}$ então $|c| \in \mathbb{Z}$) temos que $|y| = d|x|$, que pela definição de divisibilidade nos mostra que $|x|$ divide $|y|$.

Reciprocamente se $|x|$ divide $|y|$ então $\exists c \in \mathbb{Z}$ tal que $|y| = c|x|$. O que nos dar duas possibilidades:

1. $y = c \cdot |x|$ onde $y = c \cdot x$ ou $y = c(-x)$. Para $y = c \cdot x$, pela definição de divisibilidade $x \mid y$. Para $y = c(-x)$ podemos reescrever da seguinte forma $y = -cx$, onde $-c \in \mathbb{Z}$, o que resulta em $x \mid y$ pela definição de divisibilidade.

2. $-y = c|x| =$ onde $-y = cx$ ou $-y = c(-x)$. Para $-y = cx$ podemos reescrever da seguinte forma, $y = -cx$, onde $-c \in \mathbb{Z}$, e pela definição de divisibilidade $x \mid y$. Analogamente $-y = -cx$ pode ser escrito na forma $y = cx$, logo $x \mid y$.

4) Se $x \mid y$ e $y \mid z$ então existem $a, b \in \mathbb{Z}$ tais que

$$y = ax$$
e
$$z = by$$

Substituindo o valor de y na expressão de z, obtemos:

$$z = by = bax = (ba)x = cx, \text{ com } c \in \mathbb{Z}$$

Portanto $x \mid z$. ■

2.3.1 Algumas Proposições.

Observação 2.10. $\dfrac{b}{a}$ *só está definido quando* $a \neq 0$ *e* $a \mid b$.

Proposição 2.3. *Se* $x, y, z, w \in \mathbb{Z}$*, então*

$$x \mid y \; e \; z \mid w \Longrightarrow xz \mid yw.$$

Demonstração. Se $x \mid y$ e $z \mid w$ então existem $c, d \in \mathbb{Z}$ tais que: $y = cx$ e $w = dz$. Agora multiplicando y e w obtemos $yw = cdxz$ e fazendo $cd = k \in \mathbb{Z}$ obtemos $yw = kxz$, que pela definição de divisibilidade mostra que $xz \mid yw$.

■

É de fácil compreensão ver que a recíproca não é válida, pois seja $x = 3$, $y = 4$, $z = 2$, $w = 9$ temos que $xz \mid yw$ mas $x \nmid y$.

Proposição 2.4. *Sejam $a, b, c \in \mathbb{Z}$, tais que $a \mid (b \pm c)$. Então*

$$a \mid b \iff a \mid c.$$

Demonstração. Vamos iniciar a demonstração para $a \mid (b + c)$ então $a \mid b \iff a \mid c$.

Se $a \mid (b + c)$ então existe $\alpha \in \mathbb{Z}$ tal que $(b + c) = \alpha a$, por outro lado, se $a \mid b$ existe $\beta \in \mathbb{Z}$ tal que $b = \beta a$. Juntando essas duas informações temos, $\beta a + c = \alpha a$ assim $c = (\alpha - \beta)a$ com $(\alpha - \beta) \in \mathbb{Z}$, logo $a \mid c$.

Reciprocamente, se $a \mid c$ então existe $\gamma \in \mathbb{Z}$ tal que $c = \gamma a$ e como $a \mid (b+c)$ existe também $\theta \in \mathbb{Z}$ tal que $b + c = \theta a$. Juntando essas informações temos, $b + \gamma a = \theta a$, logo $b = (\theta - \gamma)a$ com $(\theta - \gamma) \in \mathbb{Z}$, portanto $a \mid b$.

Agora demonstraremos $a \mid (b - c)$ então $a \mid b \iff a \mid c$.

Como $a \mid (b - c)$ então existe $\alpha \in \mathbb{Z}$ tal que $b - c = \alpha a$. Analogamente, como $a \mid b$ existe $\beta \in \mathbb{Z}$ tal que $b = \beta a$. Assim $\beta a - c = \alpha a$ o que resulta em $\alpha a - \beta a = -c$ e $(\alpha - \beta)a = -c$, portando $a \mid -c$, logo $a \mid c$.

Reciprocamente se $a \mid c$, existe $\alpha \in \mathbb{Z}$ tal que $c = \alpha a$ e como $a \mid (b - c)$ existe também $\beta \in \mathbb{Z}$ tal que $b - c = \beta a$, assim $b - \alpha a = \beta a$ o que resulta em $b = \alpha a + \beta a$ de modo que $b = (\alpha + \beta)a$, como $(\alpha + \beta) \in \mathbb{Z}$. Portanto $a \mid b$. ■

Proposição 2.5. *Se $x, y, z \in \mathbb{Z}$ são tais que $x \mid y$ e $x \mid z$, então $x \mid (ay + bz)$ para todo $a, b \in \mathbb{Z}$.*

Demonstração. Se $x \mid y$ e $x \mid z$ então existem $\beta, \lambda \in \mathbb{Z}$ tais que $y = \beta x$ e $z = \lambda x$. Agora vamos escrever $ay+bz$ usando as igualdades acima, $ay+bz = a\beta x+b\lambda x$ que pode ser reescrito $ay + bz = x(a\beta + b\lambda)$. Portanto $x \mid (ay + bz)$.

■

Proposição 2.6. *Sejam $x, y \in \mathbb{Z}$ e $n \in \mathbb{N}$. Temos que $x - y$ divide $x^n - y^n$.*

Conforme prometido na discussão sobre indução, essa é uma proposição que pode ser provada por indução. É o que vamos fazer.

Demonstração. Vamos verificar para $n = 1$. É fácil ver que $x - y$ divide $x^1 - y^1 = x - y$, pois $a \mid a$ para todo $a \in \mathbb{Z}$;

Agora, supondo que $(x-y) \mid x^n-y^n$ é verdadeiro e escrevendo $x^{n+1}-y^{n+1} = xx^n-yy^n$. Ao somar e subtrair yx^n sem alterar a igualdade, obtemos, $x^{n+1}-y^{n+1} = xx^n-yx^n+yx^n-yy^n =$

$(x-y)x^n + y(x^n - y^n)$. Como $(x-y) \mid (x-y)$ e por hipótese $(x-y) \mid x^n - y^n$ e juntamente com a Proposição 2.5 $(x-y) \mid x^{n+1} - y^{n+1}$ o que estabelece o resultado para todo $n \in \mathbb{N}$.

■

Proposição 2.7. *Sejam $x, y \in \mathbb{Z}$ e $n \in \mathbb{N} \cup \{0\}$. Temos que $x+y$ divide $x^{2n+1} + y^{2n+1}$.*

Aqui temos outro exemplo de prova por indução.

Demonstração. Para $n = 0$ temos que $x^1 + y^1 = x + y$ e $x + y \mid x + y$ portanto é valido para $n = 0$;

Agora supondo que seja válido que $(x+y) \mid (x^{2n+1} + y^{2n+1})$. Escreveremos para $n+1$, $x^{2(n+1)+1} + y^{2(n+1)+1} = x^2 x^{2n+1} + y^2 y^{2n+1}$. Agora vamos somar e subtrair $y^2 x^{2n+1}$ sem alterar a igualdade e obtemos como resultado:

$$x^{2(n+1)+1} + y^{2(n+1)+1} = x^2 x^{2n+1} - y^2 x^{2n+1} + y^2 x^{2n+1} + y^2 y^{2n+1} = (x^2 - y^2)x^{2n+1} + y^2(x^{2n+1} + y^{2n+1}).$$

Como

$$(x+y) \mid (x^2 - y^2) = (x+y)(x-y)$$

e por hipótese

$$(x+y) \mid (x^{2n+1} + y^{2n+1})$$

e ainda usando a Proposição 2.5 , então a igualdade acima nos leva a,

$$(x+y) \mid (x^{2(n+1)+1} + y^{2(n+1)+1}),$$

o que nos mostra que é válido para $n+1$.

Assim,

$$(x+y) \mid (x^{2n+1} + y^{2n+1}).$$

■

Teorema 2.3. *Sejam $x, y \in \mathbb{Z}$ com $b \neq 0$. Existem dois únicos números inteiros q e r tais que*

$$x = yq + r, \text{ com } 0 \leq r < |y|.$$

Demonstração. Seja o conjunto $A = \{a = x - by; y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$.

Vamos mostrar que existem esses q e r.

Pela propriedade Arquimediana, existe $n \in \mathbb{Z}$ tal que $n(-y) > -x$, logo $x - ny > 0$, portanto A é não vazio. O conjunto A é limitado inferiormente por 0, logo, pelo Princípio da Boa Ordenação, temos que A possui um menor elemento r. Suponhamos então que $r = x - yq$. Sabemos que $r \geq 0$. Vamos mostrar que $r < |y|$. Suporemos agora por absurdo que $r \geq |y|$, então existe $\lambda \in \mathbb{N} \cup \{0\}$ tal que $r = |y| + \lambda$, logo $0 \leq \lambda < r$. Mas isso é uma contradição ao fato de r ser o menor elemento de A, pois $\lambda = x - (q \pm 1)y \in A$, com $\lambda < r$.

Mostraremos agora a unicidade.

Supondo por absurdo que existam $q, r, q_1, r_1 \in \mathbb{Z}$, com $0 \leq r < |y|$ e $0 \leq r_1 < |y|$ tais que, $x = yq + r = yq_1 + r_1$. Então temos, que $-|y| < -r \leq r_1 - r \leq r_1 < |y|$, logo $|r_1 - r| < |y|$. Por outro lado $y(q - q_1) = r_1 - r$, o que implica em $|y||q - q_1| = |r_1 - r| < |y|$, mas isso só é possível se $q = q_1$ e consequentemente $r = r_1$. ■

Observação 2.11. *Euclides trabalhava apenas com números naturais.*

Observação 2.12. *Ao número **q** na divisão Euclidiana chamaremos quociente e ao número **r** resto.*

Corolário 2.1. *Dados dois números inteiros x, y com $y > 0$, existe um único número inteiro n tal que*

$$ny \leq x < (n + 1)y.$$

Demonstração. Na definição de divisão Euclidiana, basta tomar $n = q$, pois pela divisão Euclidiana Existem $q, r \in \mathbb{Z}$ com $0 \leq r < y$ determinados de forma única e obtemos o desejado. ■

Exemplo 2.5. *O quociente e o resto da divisão de 30 por 7 são $q = 4$ e $r = 2$.*

Exemplo 2.6. *Mostraremos que o resto da divisão de 10^n por 9 é sempre 1, qualquer que seja n natural.*

Demonstração. De acordo com a Proposição 2.6 , $x - y \mid x^n - y^n$, assim fazendo $x = 10$ e $y = 1$ temos $(10 - 1) \mid 10^n - 1^n$, ou seja, $9 \mid 10^n - 1$. Portanto o resto da divisão de 10^n por 9 é 1. ■

Observação 2.13. *Esse exemplo pode também ser demonstrado usando indução.*

Definição 2.3. *Dizemos que x é par se o resto da divisão de x por 2 for 0. Nesse casso escrevemos $x = 2n + 0 = 2n$*

Definição 2.4. *Dizemos que x é ímpar se o resto da divisão de x por 2 for 1. Nesse caso escrevemos $x = 2n + 1$.*

Observação 2.14. *Conhecer essas formas de escrever o números pares e ímpares nos ajudam a resolver mais facilmente alguns problemas.*

Observação 2.15. *Os restos da divisão de um número inteiro x por 3 podem ser $0, 1, 2$. Assim podemos escrever um número inteiro de uma e somente uma das formas a seguir.*

$$3n, 3n + 1, 3n + 2$$

Observação 2.16. *Os restos da divisão de um número x por 4 podem ser $0, 1, 2, 3$. Assim podemos escrever um número inteiro de uma e somente uma das formas a seguir.*

$$4n, 4n + 1, 4n + 2, 4n + 3$$

Observação 2.17. *Conhecer como escrevemos números inteiros na divisão por números naturais é de grande importância na resolução de alguns problemas.*

2.3.2 Máximo divisor comum e algoritmo de Euclides

Definição 2.5. *Sejam $x, y \in \mathbb{Z}$, distintos ou não. Um número inteiro b é um divisor comum de x e y se $b \mid x$ e $b \mid y$.*

Exemplo 2.7. *Os números $\pm 1, \pm 2, \pm 4$ são divisores comuns de 4 e 16.*

Definição 2.6. *Um número $d \geq 0$ é o máximo divisor comum de x e y, denotaremos (x, y), se satisfazer as seguintes condições:*

- *d é um divisor comum de x e y;*
- *d é divisível por todo divisor comum de x e y.*

A segunda condição nos diz o seguinte:

Se c é um divisor comum de x e y, então $c \mid d$.

Exemplo 2.8. *O MDC de 8 e 20 é 4.*

Observe que os divisores comuns de 8 e 20 são $\{2,\ 4\}$. O maior é 4, observe também que 4 é divisível por todos os outros divisores comuns, neste caso so há o 2.

Observação 2.18. *O MDC de x e y é único.*

Lema 2.1 (Lema de Euclides)**.** *Sejam $x, y, a \in \mathbb{Z}$. Se existe $(x, y - ax)$, então, (x, y) existe e $(x, y) = (x, y - ax)$.*

Demonstração. Seja $d = (x, y - ax)$. Como $d \mid x$ e $d \mid (y - ax)$, segue que d divide $b = b - ax + ax$. Logo d é um divisor comum de a e b. Supondo agora que n seja um divisor comum de x e y. Logo, n é um divisor comum de $y - ax$ e, portanto, $n \mid d$. Assim $d = (x, y)$. ■

Algoritmo de Euclides

Dados $a, b \in \mathbb{N}$, podemos supor $b \leq a$. Se $b = 1$ ou $b = a$, ou ainda $b \mid a$, já vimos que $(a, b) = a$. Suponhamos, então, que $1 < b < a$ e que $b \nmid a$. Logo, pela divisão Euclidiana, podemos escrever

$$a = bq_1 + r_1 \text{ com } 0 < r_1 < b.$$

Temos duas possibilidades:

1. $r_1 \mid b$.

   Nesse caso temos, $r_1 = (b, r_1)$ e, pelo Lema de Euclides temos que $r_1 = (b, r_1) = (b, a - q_1 b) = (b, a) = (a, b)$, e o algoritmo termina.

2. $r_1 \nmid b$.

   Em tal caso, podemos efetuar a divisão de b por r_1, obtendo $b = r_1q_2 + r_2$, com $0 < r_2 < r_1$. Novamente temos duas possibilidades:

   (a) $r_1 \mid r_2$. O que nos dar $r_2 = (r_1, r_2)$ e novamente pelo lema de Euclides, $r_2 = (r_1, r_2) = (r_1, b - q_2r_1) = (r_1, b) = (a - q_1b, b) = (a, b)$, e o algoritmo termina.

   (b) $r_2 \nmid r_1$. Então podemos efetuar a divisão de r_1 por r_2, obtendo $r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$.

Podemos continuar esse processo até que pare. E sempre vamos encontrar onde parar, pois se o processo não tivesse fim, teríamos uma sequência de números naturais $b > r_1 > r_2 > r_3 > \cdots$ que não possui um menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum n, temos $r_n \mid r_{n-1}$, o que implica que $(a, b) = r_n$.

Mostraremos a seguir o modo prático de aplicação do algoritmo acima.

Ao efetuarmos a divisão de de a por b, obtemos $a = bq_1 + r_1$ e colocamos os números envolvidos no diagrama a seguir:

	q_1	
a	b	
r_1		

Ao efetuarmos a divisão de b por r_1, obtemos $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama a seguir:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Ao prosseguirmos com as divisões sucessivas e pondo os números envolvido no diagrama obtemos:

	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			

2.3.3 Propriedades do mdc

Sejam $a, b \in \mathbb{Z}$. Definimos o conjunto $I(a, b) = \{ma + nb;\ m, n \in \mathbb{Z}\}$.

Observação 2.19. *Note que se a e b não são simultaneamente nulos, então $I(a, b) \cap \mathbb{N} \neq \emptyset$, pois $a^2 + b^2 = a \cdot a + b \cdot b \in I(a, b) \cap \mathbb{N}$*

Teorema 2.4. *Sejam $m, n \in \mathbb{Z}$, não ambos nulos. Se $d = minI(m, n) \cap \mathbb{N}$, então*

1. $d = (m, n)$;

2. $I(m, n) = d\mathbb{Z}$.

Não provaremos esse teorema aqui, uma demonstração pode ser encontrada em [3].

Propriedade 2.14. *Quaisquer que sejam $x, y \in \mathbb{Z}$, não ambos nulos, e $n \in \mathbb{N}$, tem-se que* $(nx, ny) = n(x, y)$.

Propriedade 2.15. *Dados $x, y \in \mathbb{Z}$, ambos não nulos, tem-se que* $(\frac{x}{(x,y)}, \frac{y}{(x,y)}) = 1$

Demonstração. Pela Propriedade 2.14 temos,

$$(x, y)(\frac{x}{(x, y)}, \frac{y}{(x, y)}) = ((x, y)\frac{x}{(x, y)}, (x, y)\frac{y}{(x, y)}) = (x, y)$$

■

Definição 2.7. *Dois números inteiros a e b serão ditos primos entre si, ou coprimos, se* $(a, b) = 1$*; ou seja, se o único divisor comum positivo de ambos é* 1.

Propriedade 2.16. *Dois números inteiros a e b são primos entre si se, e somente se, existem números inteiros x e y tais que* $ax + by = 1$.

Demonstração. Vamos supor inicialmente que a e b são primos entre si, então $(a, b) = 1$ e pelo Teorema 2.4 temos que existem $x, y \in \mathbb{Z}$ tais que $ax + by = (a, b) = 1$.

Reciprocamente, supondo que existem $x, y \in \mathbb{Z}$ tais que $ax + by = 1$. Se $d = (a, b)$, temos que $d \mid (xa + yb)$, ou seja, $d \mid 1$ e $d = 1$.

■

A propriedade a seguir é conhecida como *Lema de Gauss*

Propriedade 2.17. *Sejam x, y e z números inteiros. Se $x \mid yz$ e $(x, y) = 1$, então $x \mid z$.*

Demonstração. Se $x \mid yz$, então existe $n \in \mathbb{Z}$ tal que $yz = nx$.

Se $(x, y) = 1$, então pela Propriedade 2.16, existem $a, b \in \mathbb{Z}$ tais que

$$ax + by = 1$$

Agora vamos multiplicar ambos membros da igualdade acima por z e obteremos

$$z = axz + byz$$

Ao substituir yz por nx na igualdade acima obtemos

$$z = anx + bnx$$

$$z = x(na + nb)$$

ou seja, $z = kx,\ k \in \mathbb{Z}$, $k = na + nb$ e portanto $x \mid z$. ■

Corolário 2.2. *Dados $x, y, z \in \mathbb{Z}$, com x e y não nulos, temos que $y \mid x$ e $z \mid x \iff \frac{yz}{(y,z)} \mid x$*

Demonstração. Se $y \mid x$ e $z \mid x$, então existem $n\ e\ m \in \mathbb{Z}$ tais que $x = ny$ e $x = mz$, ou seja, $x = ny = mz$ para algum $n, m \in \mathbb{Z}$. Na igualdade $ny = mz$ vamos dividir ambos membros por (y, z), o que resulta em

$$n\frac{y}{(y,z)} = m\frac{z}{(y,z)}$$

pela Propriedade 2.15 temos que $(\frac{y}{(y,z)}, \frac{z}{(y,z)}) = 1$ então $\frac{y}{(y,z)} \mid m$ o que nos leva a concluir que

$$\frac{y}{(y,z)}z \mid mz \text{ e como } mz = x \text{ então } \frac{yz}{(y,z)} \mid x.$$

A recíproca é de fácil verificação, pois a expressão $\frac{yz}{(y,z)} \mid x$ implica que $\frac{yz}{(y,z)}n = x$

para algum $n \in \mathbb{Z}$ e portanto como todos os y, (y, z) e n são números inteiros, podemos

reescrever $\frac{yz}{(y,z)}n = x$ das seguintes formas:

1. $\frac{yz}{(y,z)}n = x$, $x = ky$, onde $k = \frac{zn}{(y,z)}$ com $k \in \mathbb{Z}$, ou seja, $y \mid x$
2. $\frac{yz}{(y,z)}n = x$, $k_1 z$, onde $k_1 = \frac{yn}{(y,z)}$ com $k_1 \in \mathbb{Z}$, ou seja, $z \mid x$.

■

Trataremos a seguir dos números primos, que são de grande importância na Aritmética e na matemática. Desde os tempos passados tem-se procurado mostrar, sem sucesso, uma fórmula que descreva todos os números primos, entre outros problemas que até hoje permanecem sem solução.

2.4 Números Primos

2.4.1 Teorema fundamental da Aritmética

Definição 2.8. *Um número natural n maior do que 1 que possui como divisores positivos apenas 1 e n , ou seja, 1 e ele mesmo é chamado de número primo.*

Definição 2.9. *Se $n > 1$ não é primo dizemos que n é composto.*

A proposição a seguir é conhecida como *Lema de Euclides*

Proposição 2.8. *Sejam $x, y, p \in \mathbb{Z}$, com p primo. Se $p \mid xy$, então $p \mid x$ ou $p \mid y$.*

Demonstração. Se $p \mid xy$ então $xy = np$ para algum $n \in \mathbb{Z}$, supondo que $p \nmid x$, então $(p, x) = 1$. Portanto pela Propriedade 2.17, $p \mid y$.

■

Corolário 2.3. *Se $p, p_1, p_2, \cdots, p_n$ são primos e, se $p \mid p_1 p_2 \cdots p_n$, então $p = p_j$ para algum $j = 1, 2, \cdots, n$.*

Demonstração. Vamos utilizar o resultado da Proposição 2.8 e indução matemática para provar o corolário.

Pela Proposição 2.8 se $p \mid p_1 p_2$, então $p \mid p_1$ ou $p \mid p_2$. Neste caso como p, p_1 e p_2 são primos tem-se que $p \mid p_1$ então $p = p_1$, analogamente se $p \mid p_2$, $p = p_2$. De modo geral se $p \mid p_j$, $p = p_j$.

Agora, seja $A = \{1, 2, \cdots, n \ ; \ p, p_1, \cdots, p_n \text{ são } primos \ e \ p \mid p_1 p_2 \cdots p_n \text{ então } p = p_j \text{ com } j = 1, 2, \cdots, n\}$.

Note que $1 \in A$, pois se $p \mid p_1$, como p_1 é primo então só pode ser divisível por 1 e por p_1, mas como p é primo $p \neq 1$, logo $p = p_1$;

Supondo agora que $k \in A$, vamos mostrar que $k + 1 \in A$.

Como $k \in A$ então $p \mid p_1 p_2 \cdots p_k$ e $p = p_j$ para algum $j = 1, 2, \cdots, k$. Vamos agora escrever para $n = k + 1$, $p_1 p_2 p_3, \cdots, p_k p_{k+1}$. Vamos usar aqui o resultado da Proposição 2.8 pois, para que p divida $p_1 p_2 p_3, \cdots, p_k p_{k+1}$ então $p \mid p_1 p_2 \cdots p_k$ ou $p \mid p_{k+1}$. Se $p \mid p_1 p_2 \cdots p_k$ por hipótese de indução $p = p_j$ para algum $j = 1, 2, \cdots, k$. Se $p \mid p_{k+1}$ então $p = p_{k+1}$, pois p e p_{k+1} são primos. O que prova o resultado.

■

A seguir apresentaremos o *Teorema Fundamental da Aritmética*.

Teorema 2.5. *Seja n um número natural maior do que 1. Temos duas possibilidades.*

1. *n é primo;*
2. *Ou n é composto, ou seja, pode ser escrito de maneira única, a não ser pela ordem dos fatores, como produto de números primos.*

Aqui não demonstraremos tal teorema, uma demonstração pode ser encontrada em [3] páginas 141-142.

Teorema 2.6. *Dado um número inteiro $n \neq 0, 1, -1$, existem primos $p_1 < \cdots < p_r$ e $\alpha_1, \alpha_2, \cdots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que*

$$n = \pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}.$$

Proposição 2.9. *Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ um número natural escrito na forma do teorema anterior. Se d é um divisor positivo de n, então*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$$

onde $0 \leq \beta_i \leq \alpha_i$*, para* $i = 1, 2, \cdots, r$.

Demonstração. Seja d um divisor positivo de n e seja p^β a potência de um primo que figura na decomposição de d em fatores primos. Como p^β divide algum $p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$ e, consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$. ■

Observação 2.20. *Se* $n \in \mathbb{Z}^*$ *e* p *é um número primo, denotaremos pro* $E_p(n)$ *o expoente da maior potência de* p *que divide* n.

Proposição 2.10. *Se* m *e* n *são dois números naturais, então*

$$m = n \Longleftrightarrow E_p(m) = E_p(n) \text{ para todo número primo } p.$$

Demonstração. De fato, se $m = n$, é claro 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 $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ e $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$, onde $\{p_1, \cdots, p_r\}$ e $\{q_1, \cdots, q_s\}$ são dois conjuntos cada um deles composto por números primos dois a dois distintos. Como

$$\{p; p \ \ primo \ e \ E_p(m) > 0\} = \{p_1, p_2, \cdots, p_r\}$$

e

$$\{p; p \ \ primo \ e \ E_p(n) > 0\} = \{q_1, q_2, \cdots, q_s\},$$

Segue-se que

$$\{p_1, \cdots, p_r\} = \{q_1, \cdots, q_s\}.$$

Assim, $r = s$ e, após reordenarmos os elementos $q_1, \cdots, q_r$, podemos supor $q_i = p_i$, para $i = 1, 2, \cdots, r$. Como $\alpha_i = E_{pi}(m) = E_{pi}(n) = \beta_i$, para $i = 1, 2, \cdots, r$, conclui-se que $n = m$. ■

Teorema 2.7. *Existem infinitos números primos.*

Demonstração. Vamos supor por absurdo, que exista um número finito de números primos, ou seja, que $\{p, p_1, \cdots, p_r\}$ é a lista de todos os números primos. Agora escreveremos um número natural x tal que $x = p_1 p_2 \cdots p_r$, tomemos agora o sucessor de $x = p_1 p_2, \cdots, p_r + 1$ é possível tomar o sucessor de x, pois $\mathbb{N}$ é ilimitado superiormente.

Pelo Teorema 2.5 o número x possui um fator primo p que, portanto dever ser um dos $\{p, p_1, \cdots, p_r\}$ e consequentemente divide o produto $p_1 p_2, \cdots, p_r$, mas como p é fator de x implica que $x \mid 1$, o que é um absurdo.

Portanto existem infinitos números primos. ■

Lema 2.2. *Se um número natural* $a > 1$ *não é divisível por nenhum número primo* p *tal que* $p^2 \leq a$*, então ele é primo.*

Demonstração. Suponhamos, por absurdo, que a não seja divisível por nenhum número primo p tal que $p^2 \leq a$ e que não seja primo. Seja q o menor número primo que divide a; então, $a = qn$, com $q \leq n$. Segue daí que $q^2 \leq qn = a$.

Logo, a é divisível por um número primo q tal que $q^2 \leq a$, absurdo. ■

2.5 Pequeno Teorema de Fermat

Vamos demonstrar primeiro um Lema importante que nos ajudará na demonstração do teorema de Fermat.

Lema 2.3. *Seja p um número primo. Os números $\binom{p}{i}$ onde $0 < i < p$, são todos divisíveis por p.*

Demonstração. O resultado vale para $i = 1$ de maneira óbvia. Então vamos supor $1 < i < p$. Nesse caso, $i! \mid p(p-1)\cdots(p-i+1)$. Como $(i!, p) = 1$, decorre que $i! \mid (p-1)\cdots(p-1+1)$, e o resultado segue, pois

$$\binom{p}{i} = p\frac{(p-1)\cdots(p-i+1)}{i!}.$$

■

Teorema 2.8. *Dado um número primo a, tem-se que a divide o número $p^a - p$, para todo $p \in \mathbb{Z}$*

Demonstração. Se $a = 2$ é fácil verificar pois, $p^2 - p = p(p-1)$ é par e portanto $2 \mid p^2 - p$.

Vamos supor que a seja ímpar, então precisamos mostrar o resultado para $p \geq 0$. Vamos usar indução sobre p.

Se $p = 0$, $a \mid 0$, o resultado é válido;

Supondo agora que seja válido para um p, vamos provar que vale para $p + 1$.

Se vale para p então, $a \mid p^a - p$. Agora escrevendo para $p + 1$ obtemos, $(p+1)^a - (p+1)$, que ao usarmos a fórmula do Binômio de Newton, chegamos ao seguinte

$$(p+1)^a - (p+1) = p^a - p + \binom{a}{1}p^{a-1} + \cdots + \binom{a}{a-1}p.$$

Por hipótese de indução $a \mid p^a - p$ e pelo Lema 2.3,

$$\binom{a}{1}p^{a-1} + \cdots + \binom{a}{a-1}p$$

é divisível por a, e chegamos ao resultado. ■

Corolário 2.4. *Se a é um número primo e se p é um número natural não divisível por a, então a divide $p^{a-1} - 1$.*

Demonstração. Temos pelo Pequeno Teorema de Fermat que $a \mid p^a - p$. Podemos reescrever $p^a - p = p(p^{a-1} - 1)$, mas como $(a, p) = 1$, pela Proposição 2.8, $a \mid p^{a-1} - 1$.

■

2.6 Números Especiais

2.6.1 Números de Fermat

Proposição 2.11. *Sejam x e n números naturais maiores do que 1. Se $x^n + 1$ é primo, então x é par e $n = 2^m$, com $m \in \mathbb{N}$.*

Demonstração. Suponhamos que $x^n + 1$ seja primo, onde $x > 1$ e $n > 1$. Logo, x tem que ser par, pois, caso contrário, $x^n + 1$ seria par e maior do que 2, e isso contraria o fato de ser primo.

Se n tivesse um divisor primo a com $a \neq 2$, teríamos $n = ka$, $k \in \mathbb{N}$. Portanto, pela Proposição 2.7, $x^k + 1$ dividiria $(x^k)^a + 1 = x^n + 1$, mas isso contraria o fato de $x^n + 1$ ser primo. Logo $n = 2^m$. ■

Definição 2.10. *Os números de Fermat são os números da forma $F_a = 2^{2^a} + 1$, onde $a = 0, 1, 2, 3, \cdots$*

Observação 2.21. *Os números de Fermat primos são chamados de **primos de Fermat***

Propriedade 2.18. *Sejam x e n números naturais maiores do que 1. Se $x^n - 1$ é primo, então $x = 2$ e n é primo.*

Demonstração. Admitamos que $x^n - 1$ seja primo, com $x > 1$, $n > 1$.

Agora supondo, por absurdo, que $x > 2$. Logo, $x - 1 > 1$ e $x - 1 \mid x^n - 1$ de acordo com a Proposição 2.6. Portanto, $x^n - 1$ não é primo, o que é uma contradição, logo x precisa ser igual a 2.

Por outro lado, vamos agora supor, por absurdo, que n não é primo. Temos que $n = rs$ com $r > 1$ e $s > 1$. Como pela Proposição 2.6 $2^r - 1 \mid (2^r)^s - 1 = 2^n - 1$, segue-se $2^n - 1$ não é primo, o que é uma contradição. Logo, n é primo. ■

2.6.2 Números de Mersenne

Definição 2.11. *Os números de Mersenne são os números de forma $M_n = 2^n - 1$.*

Observação 2.22. *Os números de Mersenne que são primos são chamados primos de Mersenne.*

2.6.3 Números Perfeitos

Definição 2.12. *Vamos denotar a soma de todos os divisores positivos de um número natural a por $S(a)$.*

Observação 2.23. *Observe que de acordo com a definição acima a soma dos divisores positivos de 1 é denotada por $S(1) = 1$.*

Proposição 2.12. *Seja $a \in \mathbb{N}$, $S(a) = a + 1 \iff a$ é um número primo.*

Demonstração. É simples verificar tal resultado, pois a será primo se, e somente se, seus divisores são 1 e a. Logo, a soma de seus divisores será $a + 1$. ■

Proposição 2.13. *Seja $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ a decomposição de a em fatores primos. Então,*

$$S(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}.$$

Não demonstraremos essa proposição aqui, uma demonstração poderá ser encontrada em [3], página 170.

Corolário 2.5. *A função $S(n)$ é multiplicativa; isto é, se $(a, b) = 1$, então $S(ab) = S(a)S(b)$.*

Exemplo 2.9. *A seguir mostraremos como encontrar a soma dos divisores positivos de 6 usando o corolário acima.*

$$S(2) = \frac{2^2 - 1}{2 - 1} = 3$$

$$S(3) = \frac{3^2 - 1}{3 - 1} = 4$$

$$S(6) = S(2 \cdot 3) = \frac{2^2 - 1}{2 - 1}\frac{3^2 - 1}{3 - 1} = 3 \cdot 4 = 12$$

Exemplo 2.10. *Mostraremos agora como encontrar a soma dos divisores positivos de 21 já sabendo que $S(3) = 4$ conforme mostrado no exemplo anterior.*

$$S(7) = \frac{7^2 - 1}{7 - 1} = \frac{48}{6} = 8$$

$$S(21) = S(3 \cdot 7) = S(3) \cdot S(7) = 4 \cdot 8 = 32.$$

Observação 2.24. *Observe que de acordo com a Proposição 2.12, antes de fazermos os cálculos da soma dos divisores positivos de um número natural devemos reescrevê-lo na decomposição de números primos e observar o expoente para realizar os cálculos corretos.*

Exemplo 2.11. *Vamos calcular a soma dos divisores positivos de 50.*

Primeiro vamos reescrever 50, $50 = 10 \cdot 5 = 2 \cdot 5 \cdot 5 = 2 \cdot 5^2$. Agora efetuamos os cálculos conforme a Proposição 2.13 com $\alpha_1 = 1$ e $\alpha_2 = 2$.

$S(2) = 3$ e $S(5^2) = \dfrac{5^3 - 1}{5 - 1} = \dfrac{125 - 1}{4} = \dfrac{124}{4} = 31$. Portanto $S(50) = 3 \cdot 31 = 93$

Observação 2.25. *Temos que ser cuidadosos ao usar o Corolário 2.5 , pois se* $(a.b) \neq 1$ *ele não vale.*

No exemplo 2.11 concluímos que $S(50) = 93$. Mas se tomarmos uma outra decomposição de 50, 5×10 por exemplo, ao calcularmos $S(5) = 6$ e $S(10) = S(2) \cdot S(5) = 3 \cdot 6 = 18$. Ao aplicar o corolário em $S(5 \cdot 10) = S(2) \cdot S(10) = 6 \cdot 18 = 108 \neq 93$. Portanto o corolário não é verdadeiro se $(a, b) \neq 1$. Note que $(5, 10) = 5$.

Definição 2.13. *Um número natural* a *é dito perfeito se a soma de todos os divisores dele é o seu dobro, ou seja,* $S(a) = 2a$*. Ou se na soma de todos os divisores positivos de* a*, excluímos ele mesmo,* $S(a) = a$*.*

Exemplo 2.12. *O número* 6 *é um número perfeito.*

A soma dos divisores positivos de 6 é $S(6) = S(2 \cdot 3) = S(2) \cdot S(3) = 3 \cdot 4 = 12$, ou seja $S(6) = 2 \cdot 6$. Portanto 6 é um número perfeito.

2.7 Congruências

Aqui trataremos da realização de uma aritmética com restos da divisão Euclidiana por um número fixo. Tal assunto foi introduzido por Gauss em seu livro *Disquisitiones Arithmeticae*.

2.7.1 Aritmética dos Restos

Definição 2.14. *Seja* x *um número natural. Diremos que dois números inteiros* m *e* n *são congruentes módulo* x *se os restos de sua divisão euclidiana por* x *são iguais e escrevemos* $m \equiv n \mod x$.

Exemplo 2.13. *Vamos verificar se* 45 *e* 37 *são congruentes na divisão por 2.*

Demonstração. $45 = 2 \times 22 + 1$ e $37 = 2 \times 18 + 1$, ou seja 45 e 37 deixam resto 1 na divisão euclidiana por 2, logo $45 \equiv 37 \mod 2$. ■

Definição 2.15. *Diremos que* m *e* n *não são congruentes módulo* x*, ou que são incongruentes módulo* x*, quando* m *e* n *deixam restos diferentes na divisão por* x*. Quando isso ocorre a relação* $m \equiv n \mod x$ *é falsa e escrevemos* $m \not\equiv \mod n$*.*

Exemplo 2.14. *Vamos mostrar que* 45 *e* 37 *deixam restos diferentes na divisão por* 5*.*

Demonstração. $45 = 9 \times 5 + 0$ e $37 = 7 \times 5 + 2$, os restos das divisões por 5 são diferentes, logo $45 \not\equiv 37 \mod 5$. ■

Observação 2.26. *Como o resto da divisão de qualquer número inteiro por* 1 *é sempre* 0 *então a relação* $x \equiv y \mod 1$ *é sempre válida para todos* $x, y \in \mathbb{Z}$.

Observação 2.27. *A observação acima torna desinteressante trabalhar com os restos da divisão por* 1. *Assim daqui por diante vamos considerar sempre* $x > 1$ *na definição 2.14.*

A seguir enunciaremos uma proposição que nos permite concluir que a relação de congruência módulo um número inteiro x é uma relação de equivalência.

Proposição 2.14. *Sejam* $n \in \mathbb{N}$. *Para todos* $x, y, z \in \mathbb{Z}$, *tem-se que*

1. $x \equiv x \mod n$;
2. *se* $x \equiv y \mod n$, *então* $y \equiv x \mod n$;
3. *Se* $x \equiv y \mod n$ *e* $y \equiv z \mod n$, *então* $x \equiv z \mod n$.

Agora vamos enunciar e demonstrar uma proposição que nos permite verificar se dois números inteiros são congruentes módulo um número natural x sem que seja preciso efetuar a divisão de cada número por x e depois comparar os restos.

Proposição 2.15. *Suponha que* $m, n, x \in \mathbb{Z}$, *com* $x > 1$. *Temos que* $m \equiv n \mod x$ *se, e somente se,* $x \mid n - m$.

Demonstração. Suponhamos que $m \equiv n \mod x$. Dividindo m, n por x, pelo algoritmo de Euclides, existem $q, q_1, r, r_1 \in \mathbb{Z}$ tais que

$$m = qx + r \text{ e } n = q_1 x + r_1$$

Como $m \equiv n \mod x$, então $r = r_1$, de onde:

$$m - n = (q - q_1)x, \ (q - q_1) \in \mathbb{Z}$$

Logo, $x \mid (m - n)$.

Reciprocamente, com as mesmas notações da parte já demonstrada, supondo agora que $x \mid (m - n)$, teremos

$$m = qx + r \text{ e } n = q_1 x + r_1$$

com

$$m - n = (q - q_1)x + (r - r_1)$$

Como $x \mid (m - n)$ então $r - r_1 = 0$ o que implica em $r = r_1$.
Se $r = r_1$ então $m \equiv n \mod x$.

■

Observação 2.28. *Todo número inteiro é congruente módulo x ao seu resto pela divisão euclidiana por x e, portanto, é congruente módulo x a um dos números $0, 1, 2, \cdots, x-1$ e além disso, dois desses números distintos não são congruentes módulo x.*

A relação de congruência é uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, a seguir mostraremos uma proposição que mostra esse fato.

Proposição 2.16. *Sejam $m, n, o, p, x \in \mathbb{Z}$ com $x > 1$.*

1. *Se $m \equiv n \mod x$ e $o \equiv p \mod x$, então $m + o \equiv n + p \mod x$;*
2. *Se $m \equiv n \mod x$ e $o \equiv p \mod x$, então $mo \equiv np \mod x$.*

Demonstração. Supondo que $m \equiv n \mod x$ e $o \equiv p \mod x$, temos que $x \mid (m-n)$ e $x \mid (o-p)$.

1. Vamos observar que, pela Proposição 2.5, $x \mid (m-n)+(o-p)$ e portanto $x \mid (m+o)-(n+p)$, ou seja, $m + o \equiv n + p \mod x$;
2. Notemos que $mo - np = p(m-n) + m(o-p)$ e como $x \mid (m-n)$ e $x \mid (o-p)$ pela Proposição 2.5, $x \mid p(m-n) + m(o-p)$ o que é equivalente a dizer $x \mid mo - np$. Logo, $mo \equiv np \mod x$.

■

Corolário 2.6. *Para todos $x, n \in \mathbb{N}$, com $x > 1$, $m, o \in \mathbb{Z}$, se $m \equiv o \mod x$, então tem-se que $m^n \equiv o^n \mod x$.*

Demonstração. Vamos provar usando indução matemática.
Seja $P = \{m^n \equiv o^n \mod x; com\ n \in \mathbb{N}\ e\ m, o \in \mathbb{Z}\}$.

1. $1 \in P$? Vamos mostrar.

   Por hipótese do corolário $m \equiv o \mod x$, e para $n = 1$ $m^n \equiv o^n \mod x$ se torna em $m \equiv o \mod x$. Portanto $1 \in P$;

2. Agora supondo que um certo $k \in P$ vamos provar que $k + 1 \in P$.

   Se $k \in P$ então $m^k \equiv o^k \mod x$ e por hipótese do corolário $m \equiv o \mod x$. Agora de posse do resultado da Proposição 2.16 item 2, vamos multiplicar as congruências acima e obteremos o que segue,

$$m^k \equiv o^k \mod x \text{ e } m \equiv o \mod x$$

então

$$m^k m \equiv o^k o \mod x$$

e

$$m^{k+1} \equiv o^{k+1} \mod x.$$

O que prova que $k+1 \in P$, logo $m^n \equiv o^n \mod x$.

■

Observação 2.29. *Podemos reescrever o Pequeno Teorema de Fermat com a notação de congruência.*

Teorema 2.9. *O Pequeno Teorema de Fermat.*
Se p é um número primo e $a \in \mathbb{Z}$, então $a^p \equiv a \mod p$.
Também se $p \nmid a$, então $a^{p-1} \equiv 1 \mod p$.

Proposição 2.17. *Sejam $a, b, c, x \in \mathbb{Z}$, com $x > 1$. Tem-se que*

$$a + c \equiv b + c \mod x \iff a \equiv b \mod x.$$

Demonstração. Vamos começar com a implicação, $a + c \equiv b + c \mod x \implies a \equiv b \mod x$.

Se $a + c \equiv b + c \mod x$ então $x \mid (b + c) - (a + c)$, ou seja, $x \mid (b - a)$ o que nos mostra que $a \equiv b \mod x$.

Reciprocamente, se $a \equiv b \mod x$, a prova segue do item 1 da Proposição 2.15, pois como $c \equiv c \mod x$ temos que $a + c \equiv b + c \mod x$. ■

Proposição 2.18. *Sejam $a, b, c, x \in \mathbb{Z}$, com $x > 1$. Temos que*

$$ac \equiv bc \mod x \iff a \equiv b \mod \frac{x}{(c, x)}.$$

Demonstração. Como $\frac{x}{(c,x)}$ e $\frac{c}{(c,x)}$ são primos entre si, então

$$ac \equiv bc \mod x \iff x \mid (b-a)c \iff \frac{x}{(c,x)} \mid (b-a)\frac{c}{(c,x)} \iff \frac{x}{(c,x)} \mid b - a \iff$$

$$a \equiv b \mod \frac{x}{(c,x)}.$$

■

Corolário 2.7. *Sejam $a, b, c, x \in \mathbb{Z}$, com $x > 1$ e $(c, x) = 1$. Temos que*

$$ac \equiv bc \mod x \iff a \equiv b \mod x.$$

Proposição 2.19. *Sejam $m, n \in \mathbb{Z}$ e $x, y, x_1, x_2, \cdots, x_r$ inteiros maiores do que 1. Temos que*

1. *$m \equiv n \mod x$ e $y \mid x$, então $m \equiv n \mod y$;*
2. *$m \equiv n \mod x_i$, $\forall i = 1, 2, \cdots, r \iff m \equiv n \mod [x_1 \cdot x_2, \cdots, x_r]$;*
3. *Se $m \equiv n \mod x$, então $(m, x) = (n, x)$.*

Demonstração. 1. Se $m \equiv n \mod x$ então $x \mid n - m$, e como $y \mid x$ temos que $y \mid n - m$, portanto

$$m \equiv n \mod y.$$

2. Se $m \equiv n \mod x_i,\ i = 1, 2, \cdots, r$, então $x_i \mid n - m$, para todo i. Sendo $n - m$ um múltiplo de cada x_i, segue-se que $[x_1, x_2, \cdots, x_r] \mid n - m$, isso prova que

$$m \equiv n \mod [x_1, x_2, \cdots, x_r].$$

   A recíproca decorre do item 1, pois $[x_1, x_2, \cdots, x_r] \mid x_i$ para todo x_i.

3. Se $m \equiv n \mod x$, então $x \mid n - m$, portanto $n = m + tx$, com $t \in \mathbb{Z}$. Assim pelo Lema 2.1 segue que

$$(m, x) = (m + tx, x) = (n, x).$$

■

Observação 2.30. *A notação $[x_1, x_2, \cdots, x_r]$ refere-se ao mínimo múltiplo comum, que não tratamos no texto.*

Capítulo 3

Algumas aplicações

Neste capítulo trataremos de algumas aplicações de algumas das proposições e teoremas apresentados no texto até aqui.

Trataremos agora das aplicações do Máximo Divisor Comum.

3.1 Equações Diofantinas Lineares

Definição 3.1. *As Equações Diofantinas são as as equações do tipo* $aX+bY = c$*, com* $a, b, c \in \mathbb{Z}$*.*

Observação 3.1. *As equações da Definição 3.1 nem sempre possuem solução.*

Exemplo 3.1. *A equação* $2X + 4Y = 9$ *não possui solução, pois dado qualquer par de* (x_0, y_0) *com* $x_0 \in \mathbb{Z}$ *e* $y_0 \in \mathbb{Z}$ *a expressão* $2x_0 + 4y_o$ *será par para todo* $x_o, y_0 \in \mathbb{Z}$*, portanto nunca será igual a* 9*.*

Nas proposições a seguir mostraremos as condições em que uma equação Diofantina possui solução.

Proposição 3.1. *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. Pelo Teorema 2.4, temos que $I(a, b) = \{ma + yb;\ m, n \in \mathbb{Z}\} = (a, b)\mathbb{Z}$.

Como a equação é da forma $aX + bY = c$, é claro ela possuirá solução se, e somente se, $c = ma + nb$, o que equivale a dizer $c \in I(a, b)$ e ainda equivalente a $c \in (a, b)\mathbb{Z}$, que, por sua vez, é equivalente a $(a, b) \mid c$. ■

Observação 3.2. *Tomemos agora a equação* $aX+bY = c$*, vamos então dividir ambos membros por* (a, b)*, e obteremos a equação* $mX + nY = c_1$*, onde* $m = \dfrac{a}{(a, b)}$*,* $n = \dfrac{b}{(a, b)}$ *e* $c_1 = \dfrac{c}{(a, b)}$*.*

Vamos observar que pela Propriedade 2.15 $(m, n) = 1$ *e, portanto, podemos nos restringir às equações do tipo*

$$aX + bY = c, \textit{ com } (a, b) = 1$$

que sempre têm soluções.

A Proposição a seguir mostra como encontrar todas a soluções de uma equação Diofantina como na Observação 3.2 a partir de uma solução particular qualquer (x_0, y_0).

Proposição 3.2. *Seja (x_0, y_0) uma solução da equação $aX + bY = c$, onde $(a, b) = 1$. Então, as soluções x, y em $\mathbb{Z}$ da equação são da forma*

$$x = x_0 + tb,\ \ y = y_0 - ta;\ \ t \in \mathbb{Z}.$$

Demonstração. Seja (x, y) uma solução de $aX + bY = c$, logo

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

Consequentemente,

$$a(x - x_0) = b(y_0 - y).$$

Como $(a, b) = 1$, segue-se que $b \mid (x - x_0)$. Logo,

$$x - x_0 = tb,\ \ t \in \mathbb{Z}, \text{ ou seja, } x = x_0 + tb.$$

Agora, na expressão $a(x - x_0) = b(y - y_0)$ vamos substituir $x - x_0 = tb$, e obteremos o seguinte

$$a(tb) = b(y - y_0)$$

o que equivale a dizer que $y_0 - y = ta$, ou seja, $y = y_0 - ta$.

Portanto as soluções são da forma como enunciado.

Reciprocamente, se (x, y) são da forma como enunciado, então

$$ax + by = a(x_0 + tb) + b(y_0 - ta) = ax_0 + by_0 = c$$

Portanto (x, y) é solução.

■

3.2 Congruências Lineares e Classes Residuais

Trataremos nesta seção da resolução de congruências e sistemas de congruências lineares.

3.2.1 Resolução de Congruências Lineares

Vamos tratar dos seguintes tipos de congruências e suas resoluções.

$$mX \equiv n \mod x, \text{ onde } m, n, x \in \mathbb{Z}, \text{ com } x > 1,$$

ou seja, vamos determinar, caso existam, os números y tais que $my \equiv n \mod x$.

Observação 3.3. *As soluções das congruências do tipo acima podem existir ou não, a seguir vamos determinar um critério para determinar se exite solução.*

Proposição 3.3. *Dados $m, n, x \in \mathbb{Z}$, com $x > 1$, a congruência*

$$mX \equiv n \mod x$$

possui solução se, e somente se, $(m, x) \mid n$.

Demonstração. Suponhamos que a congruência $mX \equiv n \mod x$ tenha uma solução a. Logo temos, que $x \mid ma - n$, o que é equivalente a dizer, que existe $k \in \mathbb{Z}$ tal que $ma - n = kx$. Portanto a equação $mX - xY = n$ possui solução, tendo em vista o exposto na Proposição 3.1 isso implica em $(m, x) \mid n$.

Reciprocamente, suponha que $(m, x) \mid n$. Logo, em virtude da Proposição 3.1 e da Observação 3.1 a equação $mX - xY = n$ admite uma solução (x, y). Portanto, $mX = n + xY$, e consequentemente, x é solução da congruência pois, $ax \equiv n \mod x$. ■

Teorema 3.1. *Sejam $m, n, x \in \mathbb{Z}$, com $x > 1$ e $d = (m, x) \mid n$. Se y_0 é uma solução da congruência $mX \equiv n \mod x$, então*

$$y_0, y_0 + \tfrac{x}{d}, y_0 + 2\tfrac{x}{d}, \cdots, y_0 + (d-1)\tfrac{x}{d},$$

formam um sistema completo de soluções da congruências, duas a duas incongruentes módulo x.

Uma demonstração pode ser encontrada em [3].

Corolário 3.1. *Se $(m, x) = 1$, então a congruência $mX \equiv n \mod x$, com $x > 1$ e $n \in \mathbb{Z}$, possui uma única solução módulo x.*

A congruência $mX \equiv 1 \mod x$, com $(m, x) = 1$, admite uma única solução módulo x. Chamaremos tal solução de *inverso multiplicativo módulo x*.

Corolário 3.2. *Sejam $x > 1$ e R_1 um conjunto reduzido de resíduos módulo x. Se $n \in \mathbb{Z}$, então para todo $y \in R_1$, a congruência $yX \equiv n \mod x$ possui uma única solução em R_1.*

Demonstração. De fato, como $y \in R_1$, temos que $(y, x) = 1$, logo a congruência tem uma única solução módulo x. Toda solução em $\mathbb{Z}$ é tal que $(a, x) = 1$, logo, tem um único representante módulo m no conjunto R_1. ■

Observação 3.4. *Toda congruência* $mX \equiv n \mod x$ *que possui solução é equivalente a uma congruência da forma*

$$X \equiv c \mod y$$

onde $c, y \in \mathbb{Z}$ *e* $y > 1$.

Demonstração. Observe que a congruência $mX \equiv n \mod x$ possui solução, então $d = (m, x) \mid n$. Pondo $m_1 = \frac{m}{d}$, $n_1 = \frac{n}{d}$, $x_1 = \frac{x}{d}$, temos a congruência acima é equivalente a

$$m_1 X \equiv n_1 \mod x_1, \text{ com } (m_1, x_1) = 1,$$

que por sua vez é equivalente à congruência

$$X \equiv c \mod y \text{ onde } c = m_2 n_1,$$

sendo m_2 o inverso multiplicativo de m_1 módulo x_1.

■

Teorema 3.2. *Sejam* $x > 1$ *um número natural não quadrado e* $n \in \mathbb{Z}$*, com* $(n, x) = 1$*. A congruência* $nX \equiv Y \mod x$ *possui uma solução* $(a, b) \in \mathbb{Z}^2$ *tal que* $0 < |a| < \sqrt{x}$ *e* $0 < |b| < \sqrt{x}$.

Uma demonstração pode ser encontrada em [3].

3.2.2 Teorema Chinês dos Restos

Teorema 3.3. *Sejam* $m_1, m_2, m_3, \cdots, m_r$ *inteiros positivos primos entre si dois a dois, ou seja,* $(m_i, m_j) = 1 \quad \forall \quad i \neq j$*. Então o sistema de congruências lineares*

$$X \equiv c_i \mod m_i \text{ onde } m_i = 1, 2, \cdots, r$$

possui uma única solução módulo $M = m_1 \cdot m_2 \cdots m_r$ *. As soluções são*

$$x = M_1 y_1 c_1 + \cdots + M_r y_r c_r + tM,$$

onde $t \in \mathbb{Z}$, $M_i = \frac{M}{m_i}$ *e* y_i *é solução de* $M_i Y \equiv 1 \mod m_i \ i = 1, 2, \cdots, r$.

Uma demonstração pode ser encontrada em [5].

3.2.3 Classes Residuais

Definição 3.2. *O conjunto* $\overline{x} = \{a \in \mathbb{Z};\ a \equiv x \mod m,\ com\ m > 1\}$ *é chamado classe residual módulo* m *.*

Observação 3.5. *Dado um* $m > 1$ *podemos repartir o conjunto* $\mathbb{Z}$ *dos números inteiros em subconjuntos, onde cada um deles possui como elementos os números inteiros que possuem o mesmo resto quado divididos por* m*. Assim temos a seguinte partição de* $\mathbb{Z}$*:*

$$\begin{gathered}\overline{0} = \{x \in \mathbb{Z}\ ;\ x \equiv 0 \mod m\},\\ \overline{1} = \{x \in \mathbb{Z}\ ;\ x \equiv 1 \mod m\},\\ \vdots\\ \overline{m-1} = \{x \in \mathbb{Z}\ ;\ x \equiv m-1 \mod m\}.\end{gathered}$$

Na Observação 3.5 paramos em $\overline{m-1}$, pois $\overline{m} = \overline{0}$, $\overline{m+1} = \overline{1}, \cdots$

Observação 3.6. *O conjunto de todas as classes residuais módulo* m *será representado por* $\mathbb{Z}_m$*. Assim,*

$$\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1}\}$$

Exemplo 3.2. *Seja* $m = 2$*. Então*

$$\begin{aligned}\overline{0} &= \{x \in \mathbb{Z}\ ;\ x \equiv 0 \mod 2\} = \{x \in \mathbb{Z};\ x \textit{ é par }\}\ \textit{e,}\\ \overline{1} &= \{x \in \mathbb{Z}\ ;\ x \equiv 1 \mod 2\} = \{x \in \mathbb{Z};\ x \textit{ é ímpar }\}\end{aligned}$$

Temos portanto que $\overline{a} = \overline{0}$ se, e somente se, a é par.

Analogamente, $\overline{a} = \overline{1}$ se, e somente se, a é ímpar.

3.3 Resolução de Exercícios

Exercício 3.1. *(ENQ 2012/2)* a*) Mostre que nenhum número natural da forma* $4n + 3$ *pode ser escrito como um quadrado ou a soma de dois quadrados de números naturais.*

b*) Mostre que nenhum número* a *da forma* $11\cdots11$*(*n *dígitos iguais a* 1*, com* $n > 1$*) é um quadrado ou a soma de dois quadrados de números naturais.*

Demonstração. a) Supondo por absurdo que existam $n, x, y \in \mathbb{N}$ tais que, $n^2 = 4k + 3$, com $k \in \mathbb{N}$ ou $x^2 + y^2 = 4k_1 + 3$, com $k_1 \in \mathbb{N}$. Então $n^2 \equiv 3 \mod 4$ ou $x^2 + y^2 \equiv 3 \mod 4$.

Por outro lado, seja $a \in \mathbb{N}$, pela classes Residuais $a \equiv 0 \mod 4$, $a \equiv 1 \mod 4$, $a \equiv 2 \mod 4$ ou $a \equiv 3 \mod 4$.

Se $a \equiv 0 \mod 4$, então $a^2 \equiv 0 \mod 4$;

Se $a \equiv 1 \mod 4$, então $a^2 \equiv 1 \mod 4$;

Se $a \equiv 2 \mod 4$, então $a^2 \equiv 0 \mod 4$;

Se $a \equiv 3 \mod 4$, então $a^2 \equiv 1 \mod 4$.

Assim, $n^2 \not\equiv 3 \mod 4$ e $x^2 + y^2 \not\equiv 3 \mod 4$, o que é uma contradição. Logo não existe $n^2 = 4k + 3$.

b Para $a = 11$, temos que $a = 4 \cdot 2 + 3$, ou seja, $a = 4k + 3$ e pelo item $a)$ a não é um quadrado nem a soma de dois quadrados de números naturais.

Agora vamos escrever a para $n \geq 2$.

$$a = 100b + 11, \text{ com } b \geq 0.$$

Temos que $a = 4 \cdot 25b + 11 = 4 \cdot 25b + 8 + 3 = 4(25b + 2) + 3 = 4k + 3$. Portanto pelo item $a)$ obtemos o desejado.

■

Exercício 3.2. *(ENQ 2012/3) Mostre que, para todo $n \in \mathbb{N}$, é inteiro o número $\frac{1}{7}n^7 + \frac{1}{5}n^5 + \frac{23}{35}n$.*

Demonstração. Vamos inicialmente somar e subtrair $2n$ a essa expressão, obtendo assim

$$\frac{1}{7}n^7 + \frac{1}{5}n^5 + \tfrac{23}{35}n + 2n - 2n$$

que podemos reagrupar da seguinte forma

$$\frac{1}{7}n^7 - n + \frac{1}{5}n^5 - n + \frac{23}{35}n + 2n =$$

$$\frac{5n^7 - 35n + 7n^5 - 35n + 23n + 70n}{35} =$$

$$\frac{5n^7 - n - 30n + 7n^5 - 7n - 28n + 23n + 70n}{35} =$$

$$\frac{5(n^7 - n) + 7(n^5 - n) + 35n}{35} = \frac{n^7 - n}{7} + \frac{n^5 - n}{5} + n.$$

Ja sabemos que $n \in \mathbb{N}$, nos resta mostrar que $\dfrac{n^7 - n}{7}$ e $\dfrac{n^5 - n}{5}$ são inteiros. E de fato são pelo Teorema 2.8. Logo $\frac{1}{7}n^7 + \frac{1}{5}n^5 + \frac{23}{35}n$ é inteiro.

■

Exercício 3.3. *(ENQ 2012/3) Um número m é dito um quadrado se existe $a \in \mathbb{N}$ tal que $m = a^2$.*

$a)$ Mostre que o algarismo das unidades (na base 10) de um quadrado só pode ser um dos seguintes $0, 1, 4, 5, 6$ ou 9.

$b)$ Mostre que todo quadrado é da forma $4n$ ou $4n + 1$.

$c)$ Mostre que nenhum número que (escrito na base 10) tem a forma $m = dd \cdots dd$ (todos os algarismos iguais), com $m > 10$ e $d \in \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, é um quadrado.

Demonstração. $a)$ Para encontrarmos o algarismo das unidades de um número natural, devemos dividi-lo por 10. Assim pelas classes residuais os restos possíveis são, considerando um a natural:

- $a \equiv 0 \mod 10$, e portanto $a^2 \equiv 0 \mod 10$;

- $a \equiv 1 \mod 10$, e portanto $a^2 \equiv 1 \mod 10$;
- $a \equiv 2 \mod 10$, e portanto $a^2 \equiv 4 \mod 10$;
- $a \equiv 3 \mod 10$, e portanto $a^2 \equiv 9 \mod 10$;
- $a \equiv 4 \mod 10$, e portanto $a^2 \equiv 6 \mod 10$;
- $a \equiv 5 \mod 10$, e portanto $a^2 \equiv 5 \mod 10$;
- $a \equiv 6 \mod 10$, e portanto $a^2 \equiv 6 \mod 10$;
- $a \equiv 7 \mod 10$, e portanto $a^2 \equiv 9 \mod 10$;
- $a \equiv 8 \mod 10$, e portanto $a^2 \equiv 4 \mod 10$;
- $a \equiv 9 \mod 10$, e portanto $a^2 \equiv 1 \mod 10$;

Assim, o algarismo das unidades de um quadrado so pode ser um dos $0, 1, 4, 5, 6$ ou 9.

$b)$ Pelas classes residuais, se $a \in \mathbb{N}$, então:

- $a \equiv 0 \mod 4$, $a^2 \equiv 0 \mod 4$;
- $a \equiv 1 \mod 4$, $a^2 \equiv 1 \mod 4$;
- $a \equiv 2 \mod 4$, $a^2 \equiv 0 \mod 4$;
- $a \equiv 3 \mod 4$, $a^2 \equiv 1 \mod 4$;

Assim, todo quadrado é da forma $4n$ ou $4n + 1$.

$c)$ Pelo item $a)$ o algarismo das unidades de um quadrado não podem ser $2, 3, 7$ ou 8. Assim se $d \in \{2, 3, 7, 8\}$, m não é um quadrado.

Vamos prova então para $d \in \{1, 4, 5, 6, 9\}$.

- se $m = 11 \cdots 11$, provamos no item $b)$ do Exercício 3.1.
- se $m = 44 \cdots 44 = 4.(11 \cdots 11)$ ou $m = 99 \cdots 99 = 9(11 \cdots 11)$, não são quadrados, pois do contrário $(11 \cdots 11)$ seria um quadrado.
- se $m = 55 \cdots 55 = 100y + 55 = 4(25y) + 52 + 3 = 4(25y + 13) + 3 = 4k + 3$, e portanto não é um quadrado pelo item $b)$.
- se $m = 66 \cdots 66 = 100b + 66 = 4(25b) + 64 + 2 = 4(25b + 16) + 2 = 4k + 2$ que, novamente pelo item $b)$ não é um quadrado.

■

Exercício 3.4. *Prove que, para todo $n \in \mathbb{N}$, o número $n^3 + 5n$ é um múltiplo de 6.*

Demonstração. Para que $n^3 + 5n$ seja múltiplo de 6, ele precisa ser divisível por 2 e 3 simultaneamente.

Vamos somar e subtrair n na expressão e obtemos

$$n^3 + 5n + n - n = n^3 - n + 6n$$

Visto que $6n$ é múltiplo de 6, nos resta provar que $n^3 - n$ é divisível por 6.

$i)$ Vamos mostrar primeiro que $n^3 - n$ é divisível por 3. Que segue imediatamente do Teorema 2.8, pois 3 é primo.

$ii)$ Agora para mostrar que $n^3 - n$ é divisível por 2 vamos reescrever-lo da seguinte forma $n^3 - n = n(n^2 - 1)$. Temos dois casos a considerar:

1. n é divisível por 2. Nesse caso não há o que fazer, pois $2 \mid n$ e portanto $2 \mid n^3 - n$.

2. n não é divisível por 2. Então pelo Corolário 2.4 $2 \mid n^2 - 1$. Logo $2 \mid n^3 - n$.

Como $n^3 - n$ é divisível por 2 e 3 ao mesmo tempo, é um múltiplo de 6.

■

Exercício 3.5. *(ENQ2013/1) Uma sequência* (a_n) *é tal que* $a_1 = 1$ *e* $a_{n+1} = \dfrac{a_1 + a_2 + \cdots + a_n}{n+1}$ $\forall n \geq 1$. *Mostre que os valores de* (a_n)*, para* $n \geq 2$*, são todos iguais.*

Demonstração. Vamos usar indução para mostrar que $(a_n) = \dfrac{1}{2}$ para $n \geq 2$.

1. Para $n = 2$ temos que $a_2 = \dfrac{a_1}{2} = \dfrac{1}{2}$. É válido para $n = 2$.

2. Supondo agora que $a_j = \dfrac{1}{2}$, para $j = 1, 2, \cdots, n$, mostraremos que $a_{j+1} = \dfrac{1}{2}$. Já sabemos que $a_2 = \dfrac{1}{2}, a_3 = \dfrac{1}{2}, \cdots, a_n = \dfrac{1}{2}$, por hipótese de indução. Vamos agora escrever $a_{n+1} = \dfrac{a_1 + a_2 + \cdots + a_n}{n+1}$, pela definição da sequência. Assim $a_{n+1} = \dfrac{1 + \frac{1}{2} + \cdots + \frac{1}{2}}{n+1} = \dfrac{1 + (n-1)\frac{1}{2}}{n+1}$, ou seja, $a_{n+1} = \dfrac{1 + \frac{1}{2}n - \frac{1}{2}}{n+1} = \dfrac{\frac{1}{2}n + \frac{1}{2}}{n+1} = \dfrac{1}{2}$. Portanto pelo principio da indução finita $a_n = \dfrac{1}{2}$ $\forall\, n \geq 2$.

■

Exercício 3.6. *(ENQ2013/1) Seja* $n \in \mathbb{N}$ *e considere os conjuntos:*

$$A = \{d \in \mathbb{N}; d \mid n\} \text{ e } B = \{\frac{n}{c}; c \in A\}.$$

Denotemos por $S(n)$ a soma dos divisores de n e por $S^*(n)$ a soma dos seus inversos.

a) Mostre que $A = B$ e com isto conclua que $S^*(n) = \dfrac{S(n)}{n}$.

b) Mostre que n é um número perfeito se, e somente se, $S^*(n) = 2$.

Demonstração. $a)$ Temos que $x \in A \iff x = \dfrac{d}{n} \iff n = xc$, para algum $c \in A \iff x = \dfrac{n}{c}$, para algum $c \in A \iff x \in B$. Portanto $A = B$.

Seja $A = \{d_1, d_2, ..., d_r\};\ d_i \neq d_j$ para $i \neq j$, logo $S(n) = \sum_{x \in A} x = \sum_{x \in B} x = \dfrac{n}{d_1} + \dfrac{n}{d_2} + \cdots + \dfrac{n}{d_r} = n(\dfrac{1}{d_1} + \frac{1}{d_2} + \cdots + \dfrac{1}{d_r}) = nS^*(n)$, daí segue-se que $S^*(n) = \dfrac{S(n)}{n}$.

$b)$ Por definição sabemos que n é perfeito se $S(n) = 2n$. Usando o item $a)$ obtemos o desejado, pois $S^*(n) = \dfrac{S(n)}{n} = \dfrac{2n}{n} = 2$. ■

Exercício 3.7. *(ENQ 2013/1) Mostre que se p é primo, $p > 3$, então p^2 deixa resto 1 na divisão por 24.*

Demonstração. Com $p > 3$ é primo, então $p = 3q + r$, com $r = 1$ ou $r = 2$. Vamos analisar as duas possibilidades.

$i)$ se $r = 1$, $p = 3q + 1$ e como $p - 1$ é par então $q = 2k$ para algum $k \in \mathbb{N}$. Assim, $p^2 = (3.2k + 1)^2 = 36k^2 + 12k + 1 = 12k(3k + 1) + 1$, mas ou k é par ou $3k + 1$ é par, em ambos casos podemos escrever $12.2m + 1 = 24k.m + 1 = 24k_1 + 1$, como queríamos demonstrar.

$ii)$ se $r = 2$, $p = 3q + 2$ e, sendo p ímpar, temos que q é ímpar, ou seja, $q = 2k + 1$ para algum $k \in \mathbb{N}$. Substituindo temos que $p^2 = (3q + 2)^2 = [3(2k + 1) + 2]^2 = (6k + 5)^2 = 36k^2 + 60k + 25 = 12k(3k + 5) + 25 = 12k(3k + 5) + 24 + 1 = 12(3k + 5 + 2) + 1$. Mas ou k é par ou $3k + 7$ é par, logo $p^2 = 24m + 1$, com $m \in \mathbb{N}$, ou seja, p^2 deixa resto 1 na divisão por 24. ■

Exercício 3.8. *(ENQ 2013/2) Determine todos os inteiros X que são soluções da congruência*

$$X^{49} + X^{14} + X^{12} - 2X \equiv 0 \mod 7.$$

Demonstração. Se $X \equiv 0 \mod 7$, é óbvio que X é solução da congruência.

Agora supondo que X não é divisível por 7, vamos procurar as soluções possíveis.

Pelo Teorema 2.9 temos que $X^6 \equiv 1 \mod 7$ e $X^7 \equiv X \mod 7$. Agora utilizando a Proposição 2.16 temos que

$$x^{49} \equiv (X^7)^7 \equiv X^7 \equiv X \mod 7$$

Como $X^7 \equiv X \mod 7$ então

$$X^{14} \equiv (X^7)^2 \equiv X^2 \mod 7$$

E ainda, como $X^6 \equiv 1 \mod 7$

$$X^{12} \equiv (X^6)^2 \equiv 1^2 \mod 7 \equiv 1 \mod 7.$$

Agora vamos substituir na congruência.

$X^{49} + X^{14} + X^{12} - 2X \equiv X + X^2 + 1 - 2X \equiv (X^2 - X + 1) \mod 7$.

Temos o seguinte, para o resto da divisão por 7, as possibilidades são $0, 1, 2, 3, 4, 5, 6$. Vamos então analisar cada caso, excetuando o caso em que $X \equiv 0 \mod 7$, pois ja é solução.

- $X \equiv 1$ então $X^2 - X + 1 \equiv 1 \mod 7$;
- $X \equiv 2$, então $X^2 - x + 1 \equiv 3 \mod 7$;
- $X \equiv 3$, então $X^2 - x + 1 \equiv 0 \mod 7$;
- $X \equiv 4$, então $X^2 - x + 1 \equiv 6 \mod 7$;
- $X \equiv 5$, então $X^2 - x + 1 \equiv 0 \mod 7$;
- $X \equiv 6$, então $X^2 - x + 1 \equiv 3 \mod 7$.

Assim, as soluções são $X \equiv 0$, $X \equiv 3$ e $X \equiv 5$, ou seja,

$$S = \{X : X = 7k;\ k \in \mathbb{Z}\} \cup \{X : X = 7k + 3;\ k \in \mathbb{Z}\} \cup \{X : X = 7k + 5;\ k \in \mathbb{Z}\}.$$

■

Exercício 3.9. *Prove por indução em n que* $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

Demonstração. Seja $P(n) = 1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

$i)$ $P(1)$ é verdadeira, pois $P(1) = 1 = \dfrac{1(1+1)}{2}$;

$ii)$ Supondo agora que seja válido para $n = k$, provaremos para $n = k + 1$.

Se $P(k)$ é verdadeiro, então $1 + 2 + \cdots + k = \dfrac{k(k+1)}{2}$. Vamos então escrever $P(k+1) = 1 + 2 + \cdots + k + k + 1$ usando a hipótese de indução temos que

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

O que prova o resultado. ■

Exercício 3.10. *(ENQ 2013/2) Encontre o menor valor de k, $k > 2008$, tal que $1 + 2 + \cdots + k$ seja múltiplo de 13. Justifique sua resposta.*

Demonstração. No exercício anterior provamos que $1 + 2 + \cdots + k = \frac{k(k+1)}{2}$. Vamos usar esse resultado aqui.

Como 13 é primo, então ou k é múltiplo de 13 ou $k + 1$ é múltiplo de 13. Como queremos o menor valor de k para que a soma seja múltiplo de 13, então $k + 1$ será o múltiplo de 13, pois caso k seja o múltiplo não teremos o menor valor de k.

Como $k > 2008$, $k + 1 > 2009$ e o primeiro múltiplo de 13 maior que 2009 é 2015. Logo, $k + 1 = 2015$ e $k = 20014$. ■

Exercício 3.11. *(ENQ 2014/1) O máximo divisor comum de dois números positivos é* 20*. Para se chegar a esse resultado pelo processo de divisões sucessivas, os quocientes encontrados foram, pela ordem,* $1, 5, 3, 3, 1$ *e* 3*. Encontre os dois números.*

Demonstração. Pelo método das divisões sucessivas temos que:

- $a = b \cdot 1 + r, 0 < r < b$;
- $b = r \cdot 5 + r_1,\ 0 < r_1 < r$;
- $r = r_1 \cdot 3 + r_2, 0 < r_2 < r_1$;
- $r_1 = r_2 \cdot 3 + r_3, 0 < r_3 < r_2$;
- $r_2 = r_3 \cdot 1 + r_4, 0 < r_4 < r_3$;
- $r_3 = r_4 \cdot 3$.

Como $r_4 = (a, b) = 20$, temos que $r_3 = 60$;
Como $r_3 = 60$, $r_4 = 20$, temos que $r_2 = 80$;
Como $r_2 = 80$, $r_3 = 60$, temos que $r_1 = 300$;
Como $r_1 = 300$, $r_2 = 80$, temos que $r = 980$;
Como $r = 980$, $r_1 = 300$, temos que $b = 5200$;
Como $b = 5200$, $r = 980$, temos que $a = 6180$.

■

Exercício 3.12. *(ENQ 2014/1) Para todo* n *inteiro positivo, seja*

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

Prove, por indução em n *que* $n + H_1 + \cdots + H_{n-1} = nH_n$ *para todo* $n \geq 2$*.*

Demonstração. Seja $P(n) = n + H_1 + H_2 + \cdots + H_{n-1} = nH_n, \forall\ n \geq 2$.
$i)$ $P(2)$ é verdadeira pois, $P(2) = 2 + H_1 = 2 + 1 = 3 = 2 \cdot \frac{3}{2} = 2(1 + \frac{1}{2}) = 2H_2$.
$ii)$ Supondo agora que $P(k)$ é verdadeira, vamos provar para $P(k + 1)$.
Vamos escrever $P(k + 1) = (k + 1) + H_1 + H_2 + \cdots + H_{k-1} + H_{(k+1)-1}$.
Reagrupando e usando a hipótese de indução obtemos,

$$(k + H_1 + \cdots + H_{k-1}) + H_k + 1 = kH_k + H_k + 1 = (k + 1)(H_k + \frac{1}{k+1}) = (k + 1)H_{k+1}.$$

Como queríamos mostrar.

■

Exercício 3.13. *(ENQ 2014/1) Mostre que* $a^7 \equiv a \mod 21$*, para todo inteiro* a*.*

Demonstração. Seja a um inteiro qualquer, segue pelas classes residuais que, $a \equiv 0 \mod 3$, $a \equiv 1 \mod 3$ ou $a \equiv 2 \mod 3$.

- se $a \equiv 0 \mod 3$ então $a^7 \equiv 0 \mod 3$, ou seja, $a^7 \equiv a \mod 3$;
- $a \equiv 1 \mod 3$ então $a^7 \equiv 1 \mod 3$, ou seja, $a^7 \equiv a \mod 3$;
- $a \equiv 2 \mod 3$ então $a^5 \equiv 2^5 \equiv 32 \equiv 2 \mod 3$ e como $a^2 \equiv 1 \mod 3$ temos que $a^7 \equiv a^5 \mod 3$, ou seja, $a^7 \equiv a \mod 3$.

Em todas a possibilidades $a^7 \equiv a \mod 3$.

Agora pelo Teorema 2.9 $a^7 \equiv a \mod 7$. Assim pela Proposição 2.19, como $a^7 \equiv a \mod 3$ e $a^7 \equiv a \mod 7$, então temos que $a^7 \equiv a \mod [3, 7]$ e obtemos $a^7 \equiv a \mod 21$, como queríamos demonstrar. ■

Exercício 3.14. *(ENQ 2014/2) Sejam* a, b, p *inteiros, com* p *primo. Demonstre que :* a*) Se* p *não divide* a*, então* $(p, a) = 1$.

b*) Se* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração. a) Supondo que $p \nmid a$ e seja $d = (p, a)$. Segue que de $d \mid p$ e $d \mid a$. Como p é primo então $d = p$ ou $d = 1$, mas como $p \nmid a$ logo $d \neq p$, assim $d = 1$.

b) Supondo que $p \mid ab$ e $p \nmid a$. Segue que $(a, p) = 1$ e portanto existem r e s inteiros tais que $ra + sp = 1$. Multiplicando a última equação por b temos

$$rab + spb = b$$

Mas como $p \mid ab$ e $p \mid p$, então $p \mid b$. ■

Exercício 3.15. *(ENQ 2014/2) Em uma cesta contendo ovos, na contagem de dois em dois, de três em três, de quatro em quatro, e de cinco em cinco, sobram* $1, 2, 3$ *e* 4 *ovos, respectivamente. Qual é a menor quantidade de ovos que a cesta pode ter?*

Demonstração. O problema nos dar o seguinte sistema de congruências.

- $x \equiv 1 \mod 2$
- $x \equiv 2 \mod 3$
- $x \equiv 3 \mod 4$
- $x \equiv 4 \mod 5$

Como $(3, 4) = (3, 5) = (4, 5) = 1$, consideremos o sistema formado pelas 3 últimas congruências e usaremos o Teorema 3.3 para resolver.

- $x \equiv 2 \mod 3$
- $x \equiv 3 \mod 4$
- $x \equiv 4 \mod 5$

Assim, $c_1 = 2$, $c_2 = 3$ e $c_3 = 4$. E ainda,

$$M = 3 \cdot 4 \cdot 5 = 60$$
$$M_1 = 4 \cdot 5 = 20$$
$$M_2 = 3 \cdot 5 = 15$$
$$M_3 = 3 \cdot 4 = 12$$

Agora montamos as seguintes congruências.

$20y_1 \equiv 1 \mod 3$, por inspeção $y_1 = 2$

$15y_2 \equiv 1 \mod 4$, por inspeção $y_2 = 3$

$12y_1 \equiv 1 \mod 5$, por inspeção $y_3 = 3$.

Montaremos agora as soluções de acordo com o Teorema 3.3.

$$M_1y_1c_1 + M_2y_2c_2 + M_3y_3c_3 = 20 \cdot 2 \cdot 2 + 15 \cdot 3 \cdot 3 + 12 \cdot 3 \cdot 4 = 359$$

As soluções do sistema são dadas por

$$x = 359 + 60t, \text{ com } t \in \mathbb{Z}.$$

Como estamos contando ovos, o número de ovos é um número positivo, logo,

$$359 + 60t > 0, \text{ ou seja, } t > -5,9$$

O próximo inteiro maior que $-5,9$ é -5.

Para $t = -5$, $x = 59$. Como 59 é solução da congruência $x \equiv 1 \mod 2$, então 59 é a solução procurada. ■

Exercício 3.16. *(ENQ 2015/1) Sejam a, b e c inteiros tais que $a^3 + b^3 + c^3$ é divisível por 9. Mostre que pelo menos um dos inteiros a, b ou c é múltiplo de 3.*

Demonstração. Se um número n não é divisível por 3, então pelas classes residuais, n é da forma $3k + 1$ ou $3k + 2$ e n^3 é da forma $n^3 = (3k + 1)^3 = 27k^3 + 3 \cdot 9k^2 + 9k + 1 = 9k_1 + 1$ ou $n^3 = (3k + 2)^3 = 27k^3 + 27 \cdot 2k^2 + 36k + 8 = 9k_2 + 8$.

Considerando todas as possibilidades para a soma de dois cubos temos:

$i)$ $9k_1 + 1 + 9k_2 + 1 + 9k_3 + 1 = 9k + 3$

$ii)$ $9k_1 + 1 + 9k_2 + 1 + 9k_3 + 8 = 9k + 1$

$iii)$ $9k_1 + 1 + 9k_2 + 8 + 9k_3 + 8 = 9k + 8$

$iv)$ $9k_1 + 8 + 9k_2 + 8 + 9k_3 + 8 = 9k + 6$

Portanto, $a^3 + b^3 + c^3$ não é divisível por 9. Logo pelo menos um dos a, b, c é divisível por 3. ■

Exercício 3.17. *(ENQ 2015/2) Determine TODOS os valores possíveis para os algarismos* x, y, z *e* t *de modo que os números abaixo, representados na base* 10*, tenham a propriedade mencionada:*

$a)$ $3x90586y$ *é divisível por* 60*;*

$b)$ $72z41t$ *é divisível por* 99*.*

Demonstração. $a)$ $3x90586y$ é divisível por $60 = 2^2 \cdot 3 \cdot 5$ se, e somente se, é divisível simultaneamente por $4, 3$ e 5.

$i)$ $3x90586y$ é divisível por 5 se, e somente se, $y = 0$ ou $y = 5$.

$ii)$ $3x90586y$ é divisível por 4 se, e somente se, $6y$ é divisível por 4. Pelo item anterior, $y = 0$, pois 65 não é divisível por 4.

$iii)$ $3x905860$ é divisível por 3 se, e somente se, $3 + x + 9 + 0 + 5 + 8 + 6 + 0 - 31 + x$ é divisível por 3. Assim, os possíveis valores para x são $2, 5$ e 8.

Logo, 32905860, 35905860 e 38905860 são os números procurados.

$b)$ $72z41t$ é divisível por $99 = 9 \cdot 11$ se, e somente se, é divisível simultaneamente por 9 e 11.

$i)$ $72z41t$ é divisível por 9 se, e somente se, $7 + 2 + z + 4 + 1 + t = 14 + z + t$ é divisível por 9, então $z + t = 4$ ou $z + t = 13$.

$ii)$ $72z41t$ é divisível por 11 se, e somente se, $t - 1 + 4 - z + 2 - 7 = t - z - 2$ é divisível por 11. Então $t - z = -9$ ou $t - z = 2$.

De posse desses resultados, montamos os seguintes sistemas de equações.

- $z + t = 4$
- $t - z = -9$

Que não possui solução inteira.

- $z + t = 4$
- $t - z = 2$

Cuja solução é $z = 1$ e $t = 3$

- $z + 1 = 13$
- $t - z = -9$

As soluções são $z = 11$ e $t = 2$, mas não nos serve pois z deve possuir um único algarismo.

- $z + t = 13$
- $t - z = 2$

Não possui solução inteira.

Assim o número procurado é 721413.

■

Exercício 3.18. *(ENQ 2015/2)*

$a)$ *Calcule o resto da divisão de* 28^{237} *por* 13*;*

$b)$ *Determine o algarismo das unidades do número* $7^{7^{1000}}$.

Demonstração. $a)$ Como $28 = 2 \cdot 13 + 2$ temos que $28 \equiv 2 \mod 13$, e obtemos,

$$28^2 \equiv 2^2 \equiv 4 \mod 13$$
$$28^2 \cdot 28 = 28^3 \equiv 2 \cdot 4 \equiv 8 \mod 13$$
$$28^2 \cdot 28^2 = 28^4 \equiv 2^2 \cdot 2^2 \equiv 16 \equiv 3 \mod 13$$
$$28^6 \equiv 2^6 \equiv 64 \equiv -1 \mod 13.$$

Por outro lado, $237 = 6 \cdot 39 + 3$ o que resulta em

$$28^{237} \equiv 28^{6 \cdot 39 + 3} \equiv (28^6)^{39} \cdot 28^3 \equiv -1 \cdot 8 \equiv -8 \equiv 5 \mod 13.$$

Portanto, o resto procurado é 5.

$b)$ Para encontrar o algarismo das unidades de um número precisamos efetuar a divisão do mesmo por 10, assim buscamos

$$\frac{7^{7^{1000}}}{10}$$

Vamos escrever 7 na congruência módulo 10.

$$7 \equiv -3 \mod 10$$
$$7^2 \equiv 9 \mod 10$$
$$7^4 \equiv 9^2 \equiv 1 \mod 10$$
$$7^{4q} \equiv (7^4)^q \equiv 1 \mod 10, \text{ para todo } q \in \mathbb{N}.$$

Por outro lado, vamos escrever 7 na congruência módulo 4.

$$7 \equiv -1 \mod 4$$
$$7^{1000} \equiv 1 \mod 4$$

ou seja,

$$7^{1000} = 4q + 1$$

Logo,

$$7^{7^{1000}} \equiv 7^{4q+1} \equiv 7^{4q} \cdot 7 \equiv 1 \cdot 7 \mod 10.$$

Portanto, o algarismo das unidades procurado é 7.

■

Exercício 3.19. *(ENQ 2015/2) Prove a desigualdade de Bernoulli:*

$$x \in \mathbb{R},\, x \geq -1 \textit{ então } (1+x)^n \geq 1 + nx \;\; \forall n \geq 1.$$

Demonstração. Seja $P(n) = (1+x)^n \geq 1 + nx$.

$i)$ $P(1) = (1+x) \geq 1 + 1 \cdot x$, logo $P(1)$ é verdadeira.

$ii)$ Agora supondo que $P(k)$ seja verdadeira, provaremos para $P(k+1)$.

Se (k) é verdadeira então, $(1+x)^k \geq 1 + kx$. Sabemos que $(1+x) \geq 0$, visto que $x \geq -1$. Assim podemos multiplicar $(1+x)$ a ambos membros da desigualdade $P(k)$ sem alterar o resultado. E obtemos,

$$\begin{gathered}(1+x)^k.(1+x) \geq (1+kx)(1+x) \\ (1+x)^{k+1} \geq 1 + x + kx + kx^2 \\ (1+x)^{k+1} \geq 1 + (k+1)x + kx^2\end{gathered}$$

Visto que $kx^2 \geq 0$, pois $k \geq 1$ e $x^2 \geq 1$, Assim

$$(1+x)^{k+1} \geq 1 + (k+1)x$$

Como queríamos provar.

■

Exercício 3.20. *(ENQ2016/1) Se p é um número primo, mostre que $2^{(p+1)^3} \equiv 256 \mod p$.*

Demonstração. Se p é primo então pelo Teorema 2.9 $2^p \equiv 2 \mod p$.

Tendo em vista que $(p+1)^3 = p^3 + 3p^2 + 3p + 1$, vamos fazer as seguintes congruências.

- $2^p \equiv 2 \mod p$;
- $2^{p^2} = (2^p)^p \equiv 2^p \equiv 2 \mod p$;
- $2^{p^3} = (2^{p^2})^p \equiv 2^p \equiv 2 \mod p$;
- $2^{3p^2} = (2^{p^2})^3 \equiv 2^3 \equiv 8 \mod p$;
- $2^{3p} = (2^p)^3 \equiv 2^3 \equiv 8 \mod p$;

Portanto,

$$2^{(p+1)^3} = 2^{p^3} \cdot 2^{3p^2} \cdot 2^{3p} \cdot 2^1 \equiv 2 \cdot 8 \cdot 8 \cdot 2 \equiv 256 \mod p.$$

■

Exercício 3.21. *(ENQ 2016/1)*

$a)$ *Seja x_0, y_0 uma solução da equação diofantina $aX + bY = c$, onde a, b são inteiros não nulos e $(a,b) = 1$. Prove que as soluções x, y em $\mathbb{Z}$ da equação são $x = x_0 + tb$ e $y = y_0 - ta$, com $t \in \mathbb{Z}$.*

$b)$ *Encontre todas as soluções em $\mathbb{N} \cup \{0\}$ da equação $7X + 19Y = 781$.*

Demonstração. Para o item $a)$ Ver Proposição 3.2

$b)$ De acordo com a Proposição 3.2 as soluções são da forma

$$x = x_0 + tb \text{ e } y = y_0 - ta, \text{ com } t \in \mathbb{Z} \text{ e } x_0, y_0 \text{ uma solução particular.}$$

Como $x_0 = 3$ e $y_0 = 40$, satisfazem a equação, pois

$$7 \cdot 3 + 19 \cdot 40 = 781$$

Assim, $x = 3 + 19t$ e $y = 40 - 7t$.

Para encontrarmos todas as soluções em $\mathbb{N} \cup \{0\}$, queremos que $x \geq 0$ e $y \geq 0$. O que resulta nas seguintes inequações,

- $3 + 19t \geq 0$
- $40 - 7t \geq 0$

A primeira inequação tem como solução $t \geq \dfrac{-3}{19}$, ou seja, $t \geq -0,15$, cujo inteiro mais próximo que satisfaz é 0.

A segunda inequação tem como solução $t \leq \frac{40}{7}$, ou seja, $t \leq 5,7$, cujo inteiro mais próximo que satisfaz é 5.

Portanto os valores de t que satisfazem a equação são $0, 1, 2, 3, 4$ e 5.

Substituindo o valor de t encontramos como solução

$$(3, 40); (22, 33); (41, 26); (60, 19); (79, 12); (98, 5).$$

■

Exercício 3.22. *(ENQ 2016/1) A sequência (a_n) satisfaz as seguintes condições:*

$i)$ $a_1 = \dfrac{1}{2}$

$ii)$ $\displaystyle\sum_{i=1}^{n} = n^2 a_n$, *para* $n \geq 2$.

$a)$ *Determine a_2, a_3 e a_4;*

$b)$ *Conjecture uma expressão para o termo geral a_n em função de n.*

$c)$ *Prove, por indução em n, a fórmula obtida no item b).*

Demonstração. $a)$ Pela definição da sequência é possível encontrar a_2 usando a condição $ii)$, pois $\displaystyle\sum_{i=1}^{2} = a_1 + a_2 = 2^2 a_2$. Como $a_1 = \dfrac{1}{2}$, temos que

$$\frac{1}{2} + a_2 = 4a_2,$$

resolvendo encontramos $a_2 = \dfrac{1}{6}$.

Analogamente, Como $a_2 = \dfrac{1}{6}$, $a_1 = \dfrac{1}{2}$ e $\displaystyle\sum_{i=1}^{3} = a_1 + a_2 + a_3 = 3^2 a_3,\ \dfrac{1}{2} + \dfrac{1}{6} + a_3 = 9a_3,$ resolvendo encontramos $a_3 = \dfrac{1}{12}$.

Do mesmo modo, $\displaystyle\sum_{i=1}^{4}(a_1 + a_2 + a_3 + a_4) = 4^2 a_4$ substituindo os valores que ja possuímos encontramos $a_4 = \dfrac{1}{20}$.

$b)$ Analisando os dados do item $a)$ podemos fazer a seguinte conjectura para o termo geral de a_n.

$$a_n = \frac{1}{n(n+1)}, \forall n \geq 1.$$

$c)$ Vamos provar a expressão conjecturada no item $b)$

Seja $a(n) = \dfrac{1}{n(n+1)}\ \forall n \geq 1.$

$i)$ $a(1) = \dfrac{1}{1(1+1)} = \dfrac{1}{2}$, então é válido para $n = 1$.

$ii)$ Agora supondo que $a(k)$ seja válido, ou seja, $a_k = \dfrac{1}{k(k+1)}$ provaremos para $a(k+1)$.

Pela definição da sequência $a_1 + a_2 + \cdots + a_k = k^2 a_k$ e $a_1 + a_2 + \cdots + a_k + a_{k+1} = (k+1)^2 a_{k+1}$.

Assim,

$$\begin{gathered}
k^2 a_k + a_{k+1} = (k+1)^2 a_{k+1} \\
k^2 a_k = (k+1)^2 a_{k+1} - a_{k+1} \\
k^2 a_k = (k^2 + 2k + 1) a_{k+1} + a_{k+1} \\
k^2 a_k = (k^2 + 2k + 1 - 1) a_{k+1} \\
k^2 a_k = (k^2 + 2k) a_{k+1} \\
a_{k+1} = \tfrac{k^2 a_k}{k(k+2)} = \dfrac{k a_k}{k+2}
\end{gathered}$$

Agora por hipótese de indução $a_k = \dfrac{1}{k(k+1)}$, logo

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

Como queríamos demonstrar.

■

Exercício 3.23. *(ENQ 2016/2) A secretaria de educação de um município recebeu um certa quantidade de livros para distribuir entre as escolas do município. Sabe-se que a quantidade é superior a* 1000 *e inferior a* 2000*, que se dividi-los entre sete escolas sobram* 4*, entre* 9 *sobram* 2 *e entre* 13 *sobram* 6*. Encontre a quantidade de livros.*

Demonstração. Seja L a quantidade de livros o problema nos dar o seguinte sistema de congruências,

- $L \equiv 4 \mod 7$
- $L \equiv 3 \mod 9$
- $L \equiv 6 \mod 13$

E como $(7,9);(9,13);(7,13) = 1$, o sistema admite solução.
Portanto pelo Teorema 3.3 as soluções são dadas por

$$L \equiv 117y_1 \cdot 4 + 91y_2 \cdot 2 + 63y_3 \cdot 6 \mod 819.$$

Pois,

- $M = 7 \cdot 9 \cdot 13 = 819$;
- $m_1 = 117$ e $c_1 = 4$;
- $m_2 = 91$ e $c_2 = 2$;
- $m_3 = 63$ e $c_3 = 6$

Vamos agora encontrar, y_1, y_2, y_3
Escreveremos as seguintes congruências

- $117y_1 \equiv 1 \mod 7$
- $91y_2 \equiv 1 \mod 9$
- $63y_3 \equiv 1 \mod 13$

Obtemos como solução, $y_1 = 3$, $y_2 = 1$ e $y_3 = 6$ pois,

$$117 \cdot 3 = 351 \equiv 1 \mod 7$$
e
$$91 \cdot 1 = 91 \equiv 1 \mod 9$$
e ainda
$$63 \cdot 6 = 378 \equiv 1 \mod 13$$

Portanto,

$$L \equiv 117 \cdot 3 \cdot 4 + 91 \cdot 2 \cdot 1 + 63 \cdot 6 \cdot 6 \mod 819$$
$$L \equiv 3854 \equiv 578 \mod 819$$

Obtemos então $L = 578t + 819$, como $1000 < L < 2000$, então $t = 1$ e $L = 1397$.

■

Exercício 3.24. *(ENQ 2016/2) Mostre que, para todo número natural $n \geq 1$, o resto da divisão do polinômio $x^{2n} + x + 1$ por $x + 2$.*

Demonstração. Vamos provar usando indução em n.

$i)$ Para $n = 1$, $x^2 + x + 1$ e ao efetuarmos a divisão obtemos

$$x^2 + x + 1 = (x^2 - 1) + (x + 2)$$

Portanto é válido para $n = 1$.

$ii)$ Supondo que seja válido para $n = k$, provaremos para $n = k + 1$.

Se vale para $n = k$, então

$$x^{2k} + x + 1 = q(x)(x^2 - 1) + (x + 2)$$

Vamos escrever a expressão para $n = k + 1$

$$x^{2(k+1)} + x + 1 = x^{2k+2} + x + 1 = x^2 x^{2k} + x + 1$$

Como por hipótese de indução, $x^{2k} + x + 1 = q(x)(x^2 - 1) + (x + 2)$, então

$$x^{2k} = q(x)(x^2 - 1) + (x + 2) - x - 1 = q(x)(x^2 - 1) + 1$$

Agora substituindo x^{2k} na expressão de $n = k + 1$, obtemos

$$x^{2(k+1)} + x + 1 = x^{2k+2} + x + 1 = x^2[q(x)(x^2 - 1) + 1)] + x + 1$$
$$x^2[q(x)(x^2 - 1) + 1)] + x + 1 = x^2 q(x)(x^2 - 1) + x^2 + x + 1$$

Mas, $x^2 + x + 1 = (x^2 - 1) + (x + 2)$, por $i)$

Assim,

$$x^2 q(x)(x^2 - 1) + x^2 + x + 1 = x^2 q(x)(x^2 - 1) + (x^2 - 1) + (x + 2)$$
$$x^2 q(x)(x^2 - 1) + (x^2 - 1) + (x + 2) = (x^2 - 1)(x^2 q(x) + 1) + x + 2$$
$$(x^2 - 1)(x^2 q(x) + 1) + x + 2 = (x^2 - 1)q_1(x) + (x + 2)$$

Portanto é válido para $n = k + 1$.

■

Exercício 3.25. *(ENQ 2016/2) Dados $a, n \in \mathbb{N}$, com $a > 2$ ímpar, mostre que*

$a)$ se $\dfrac{a^n - 1}{2}$ é par então a é da forma $4k + 1$ ou n é par.

$b)$ se a é da forma $4k + 1$ ou n é par, então $\dfrac{a^n - 1}{2}$ é par.

Demonstração. $a)$ Supondo que $\dfrac{a^n - 1}{2}$ é par e que não é da forma $4k + 1$.

Temos que $\dfrac{a^n - 1}{2} = 2k$, com k inteiro. Logo, $a^n = 4k + 1$, ou seja, $a^n \equiv 1 \mod 4$.

Como a é ímpar, $a = 4k + 3$ o que nos dar, $a \equiv 3 \equiv -1 \mod 4$. Assim,

$$a^n \equiv (-1)^n \mod 4$$

Portanto, se n é impar, contradiz o fato de $a^n \equiv 1 \mod 4$, logo n é par.

$b)$ Suponhamos que a é da forma $4k+1$. Temos então que $a \equiv 1 \mod 4$, daí $a^n \equiv 1 \mod 4$, portanto

$$a^n - 1 \equiv 0 \mod 4$$
$$d^{\frac{a^n-1}{2}} \equiv 0 \mod 2$$

Temos portanto que $\dfrac{a^n-1}{2} = 2k$, para algum $k \in \mathbb{Z}$.

Suponhamos agora que n é par. Como a é ímpar temos que $a \equiv 1 \mod 4$ ou $a \equiv 3 \mod 4$ que é equivalente a $a \equiv -1 \mod 4$, ou seja, $a^n \equiv 1 \mod 4$.

Nos dois casos $a^n \equiv 1 \mod 4$, logo $\dfrac{a^n-1}{2}$ é par. ■

Exercício 3.26. *(ENQ 2017/1)*

$a)$ *Prove que um número inteiro positivo n possui uma quantidade ímpar de divisores se, e somente se, é um quadrado perfeito.*

$b)$ *Sejam a e b números inteiros positivos com $(a,b) = 1$. Prove que, se ab é um quadrado perfeito, então a e b são quadrados perfeitos.*

Demonstração. $a)$ Pelo Teorema 2.6 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde $p_1 < p_2 < \cdots < p_k$ são números primos e $\alpha_1, \alpha_2, \cdots, \alpha_k$ são números inteiros positivos.

A quantidade de divisores de n é dada por

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

$i)$ Se n tem número ímpar de divisores, então todos os fatores de $d(n)$ são números ímpares, ou seja, $\alpha_1, \alpha_2, \cdots, \alpha_k$ são números pares.

Portanto,

$$n = (p_1^{\frac{\alpha_1}{2}} \cdot p_2^{\frac{\alpha_2}{2}} \cdots p_k^{\frac{\alpha_k}{2}})^2$$

Que é um quadrado perfeito.

$ii)$ Reciprocamente, se n é um quadrado perfeito, então $n = c^2$, para algum $c \in \mathbb{Z}$. Isto implica que todos os α_i são números pares e então $d(n)$ é ímpar, por ser o produto de ímpares.

$b)$ Sejam $a = a_1^{\beta_1} a_2^{\beta_2} \cdots a_k^{\beta_k}$ e $b = b_1^{\lambda_1} b_2^{\lambda_2} \cdots b_t^{\lambda_t}$ a decomposição destes números em fatores primos distintos, pois como $(a,b) = 1$, eles não tem fator primo em comum.

Ao efetuar o produto de a e b obtemos,

$$ab = a_1^{\beta_1} a_2^{\beta_2} \cdots a_k^{\beta_k} b_1^{\lambda_1} b_2^{\lambda_2} \cdots b_t^{\lambda_t}$$

Que é a decomposição de ab em fatores primos.

Como ab é um quadrado perfeito, pelo item $a)$, a quantidade de divisores de ab é ímpar, isto é,

$$d(ab) = (\beta_1 + 1)(\beta_2 + 1) \cdots (\beta_k + 1)(\lambda_1 + 1)(\lambda_2 + 1) \cdots (\lambda_t + 1)$$

é ímpar.

E pelo item $a)$ $d(a)$ é ímpar e $d(b)$ é ímpar, ou seja, a e b são quadrados perfeitos.

■

Exercício 3.27. *(ENQ 2017/1) Sejam a, b, m números inteiros, com $m > 1$ e tais que $(a, m) = 1$. Prove que a congruência $ax \equiv 1 \mod m$ possui solução. Além disso, mostre que se $x_1, x_2 \in \mathbb{Z}$ são soluções da congruência, então $x_1 \equiv x_2 \mod m$.*

Demonstração. Supondo que $(a, m) = 1$. Segue que existem inteiros r e s tais que $ar+ms = 1$. Daí temos que

$$ar \equiv 1 \mod m$$

Portanto r é solução da congruência.

Supondo agora que x_1 e x_2 são soluções da congruência, então

$$ax_1 \equiv 1 \mod m$$
e
$$ax_2 \equiv 1 \mod m$$

ou seja,

$$ax_1 \equiv ax_2 \mod m$$

e como $(a, m) = 1$ então temos

$$x_1 \equiv x_2 \mod m$$

■

Exercício 3.28. *(ENQ 2017/2) Sejam a, b números inteiros e p um número primo. Prove que:*

$a)$ se $p \mid a^p - b^p$, então $p \mid a - b$.

$b)$ se $p \mid a^p - b^p$, então $p^2 \mid a^p - b^p$.

Demonstração. $a)$ Supondo que $p \mid a^p - b^p$. Como p é primo, pelo Pequeno Teorema de Fermat temos, $p \mid a^p - a$ e $p \mid b^p - b$, assim $p \mid a^p - b^p - (a - b)$. Como $p \mid a^p - b^p$, concluímos que $p \mid a - b$.

$b)$ Suponha que $p \mid a^p - b^p$, usando o item $a)$ sabemos que $p \mid a - b$, ou seja, $a \equiv b \mod p$. Então temos que

$$a^n \equiv b^n \mod p, \ \forall\, n \in \mathbb{N}$$

Daí,

$$a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} \equiv b^{p-1} + b^{p-2}b + \cdots + bb^{p-2} + b^{p-1} \equiv pb^{p-1} \equiv 0 \mod p.$$

Como

$$a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1})$$

Sabemos que $p \mid a-b$, pelo item $a)$ e $p \mid a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}$

Assim,

$$a - b = kp \text{ e } a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1} = \alpha p, \text{ com } k, \alpha \in \mathbb{Z}.$$

ou seja, $a^p - b^p = (a-b)(a^{p-1} + a^{p-2}b + \cdots + ab^{p-2} + b^{p-1}) = k\ \alpha\ p^2$

Como

$$p \mid a^p - b^p = k\ \alpha\ p^2$$

logo,

$$p^2 \mid a^p - b^p.$$

■

Exercício 3.29. *Mostre que para todo n natural $6 \mid n^3 + 11n$.*

Demonstração. Para que n^3+11n seja divisível por 6 devemos mostrar que n^3+11n é divisível por 2 e por 3.

$i)$ Seja $n^3 + 11n = n(n^2 + 11)$ temos duas possibilidades para n.

- n é par, nesse caso $n^3 + 11n = n(n^2 + 11)$ é divisível por 2;
- n é ímpar, ou seja, $n = 2k + 1$, com $k \in \mathbb{Z}$. Vamos substituir a expressão de n em $n(n^2 + 11)$.

$$n(n^2 + 11) = (2k+1)[(2k+1)^2 + 11] = (2k+1)(4k^2 + 4k + 1 + 11)$$

ou seja,

$$n(n^2 + 11) = (2k+1)(4k^2 + 4k + 12)$$

como $2 \mid 4k^2 + 4k + 12$, então $2 \mid n^3 + 11n$.

$ii)$ Vamos mostrar que $n^3 + 11n$ é divisível por 3.

Pelo Teorema 2.8 temos que $3 \mid n^3 - n$. Assim reescrevendo $n^3 + 11n = n^3 + n + 10n$, somando e subtraindo n, obtemos

$$n^3 + 11n = n^3 - n + 12n$$

Como $3 \mid n^3 - n$ e $3 \mid 12n$, logo $3 \mid n^3 + 11n$.

Por $i)$ e $ii)$ temos que $6 \mid n^3 + 11n$. ■

Exercício 3.30. *Mostre que, se um inteiro é um quadrado e um cubo, então é da forma $7k$ ou $7k + 1$.*

Demonstração. Usando as classes residuais temos que n é da forma

$$7k, 7k+1, 7k+2, 7k+3, 7k+4, 7k+5 \; ou \; 7k+6$$

Vamos então analisar cada caso, e verificar a forma dos quadrados e cubos.

- se $n = 7k$ então, $n^2 = 49k^2 = 7k_1$ e $n^3 = 343k^3 = 7k_2$;
- se $n = 7k+1$ então $n^2 = 49k^2+14k+1 = k(49k+14)+1 = 7k(7k+2)+1 = 7k_3+1$ e $n^3 = (7k+1)^3 = 343k^3 + 3 \cdot 49k^2 + 3 \cdot 7k + 1 = 7k_4 + 1$;
- se $n = 7k+2$ então, $n^2 = (7k+2)^2 = 49k^2 + 28k + 4 = 7k(7k+4) + 4 = 7k_4 + 4$ e $n^3 = (7k+2)^3 = 343k^3 + 34 \cdot 9k^2 \cdot 2 + 3 \cdot 7k \cdot 8 + 8 = 7k_5 + 1$

  Como $7k_4 + 4 \neq 7k_5 + 1$, $n = 7k + 2$ não é um quadrado e um cubo.
- se $n = 7k+3$ então $n^2 = (7k+3)^2 = 49k^2 + 2 \cdot 7k \cdot 3 + 9 = 49k^2 + 42k + 9 = 7k_6 + 2$ e $n^3 = (7k+3)^3 = 343k^3 + 3 \cdot 49k^2 \cdot 3 + 3 \cdot 7k \cdot 9 + 27 = 343k^3 + 493k^2 + 7 \cdot 27k + 27 = 7k_7$

  Como $7k_6 + 2 \neq 7k_7$, $n = 7k + 3$ não é um quadrado e um cubo.
- se $n = 7k+4$ então $n^2 = (7k+4)^2 = 49k^2 + 14 \cdot 4k + 16 = 7k_8 + 2$ e $n^3 = (7k+4)^3 = 343k^3 + 3 \cdot 49k^2 \cdot 4 + 3 \cdot 7k \cdot 16 + 64 = 7k_9 + 1$

  Como $7k_8 + 2 \neq 7k_9 + 1$, $n = 7k + 4$ não é um quadrado e um cubo.
- se $7k + 5$ então $n^2 = (7k + 5)^2 = 49k^2 + 2 \cdot 7k \cdot 5 + 25 = 7k_{10} + 3$ e $n^3 = (7k + 5)^3 = 343k^3 + 3 \cdot 49k^2 \cdot 5 + 3 \cdot 7k \cdot 25 + 125 = 7k_{11} + 6$

  Como $7k_{10} + 3 \neq 7k_{11} + 6$, $n = 7k + 5$ não é um quadrado e um cubo.
- se $n = 7k+6$ então $n^2 = (7k+6)^2 = 49k^2 + 2 \cdot 7k \cdot 6 + 36 = 7k_{12} + 1$ e $n^3 = (7k+6)^3 = 343k^3 + 3 \cdot 49k^3 \cdot 6 + 3 \cdot 7k \cdot 36 + 216 = 7k_{13} + 6$

  Como $7k_{12} + 1 \neq 7k_{13} + 6$, $n = 7k + 4$ não é um quadrado e um cubo.

Portanto, para n ser um quadrado e um cubo ele deverá ter a forma $7k$ ou $7k + 1$. ■

Considerações Finais

Neste trabalho apresentamos um pouco de história da Aritmética discorrendo sobre alguns do principais matemáticos da área e suas contribuições. Tal abordagem será de grande ajuda aos leitores que buscam em um só lugar o conhecimento histórico sobre Aritmética e seus grandes precursores.

Apresentamos também algumas Proposições, Propriedades, Lemas, Teoremas e Definições que se mostraram ser grande ferramenta em resolução de problemas. Tais ferramentas foram usadas na solução dos problemas apresentados no Capítulo 3 que foram resolvidos de forma relativamente fácil com o auxílio dos recursos citados.

Os assuntos abordados servirão como base bibliográfica para alunos do PROFMAT que buscam aperfeiçoamento para o Exame Nacional de Qualificação, pois aqui resolvemos todas as questões de Exames anteriores que envolvem aritmética até o ano de 2017. Serve como auxílio na formação do futuro professor de matemática e para complementar o conhecimento dos que ja trabalham algum tempo na Educação Básica e superior ensinando teoria dos números.

Referências Bibliográficas

[1] BOYER, C. , História da Matemática, 1976. Tradução de Helena Castro, 2012.

[2] Roque, Tatiana, Tópicos de História da Matemática - Coleção PROFMAT 2012.

[3] Hefez, Abramo , Aritmética - Coleção PROFMAT 2014.

[4] Iezzi, Gelson, 3ª Série do Ensino Médio, 1990.

[5] Santos, Audemir dos, Teorema Chinês dos Restos e Aplicações, 2017.

[6] Domingues, Hygino H., A mulher e a Matemática.

[7] Ferreira, Francisco de Assis, A Prova dos Noves, Divisibilidade e Congruência, 2017.