UNIVERSIDADE ESTADUAL DA PARAÍBA
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UEPB

Congruências e Equações Diofantinas: Algumas Aplicações

Rivanildo Garcia da Silva

Trabalho de Conclusão de Curso

Orientador: Prof. Dr. Vandenberg Lopes Vieira

Campina Grande - PB
Dezembro/2018

UNIVERSIDADE ESTADUAL DA PARAÍBA
Programa de Pós-Graduação em Matemática
Mestrado Profissional - PROFMAT/CCT/UEPB

Teoria dos Números e Criptografia com Aplicações Básicas

por

Rivanildo Garcia da Silva †

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, na modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

---

†Bolsista CAPES

S586c Silva, Rivanildo Garcia da.
Congruências e Equações diofantinas [manuscrito] : algumas aplicações / Rivanildo Garcia da Silva. - 2018.
77 p.
Digitado.
Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa , 2019.
"Orientação : Prof. Dr. Vandeberg Lopes Vieira , Departamento de Matemática - CCT."
1. Equações diofantinas. 2. Teoria dos números. 3. Matemática - Resolução de problemas. I. Título
21. ed. CDD 512.94

Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

Congruências e Equações Diofantinas: Algumas Aplicações

por

Rivanildo Garcia da Silva

Trabalho de Conclusão de curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCT - UEPB, modalidade Mestrado Profissional, como requisito parcial para obtenção do título de Mestre.

Aprovado por:

Severino Horácio da Silva

Prof. Dr. Severino Horácio da Silva - UFCG

Aldo Trajano Lourêdo

Prof. Dr. Aldo Trajano Lourêdo - UEPB

Vandenberg Lopes Vieira

Prof. Dr. Vandenberg Lopes Vieira - UEPB
Orientador

Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Curso de Mestrado Profissional em Matemática em Rede Nacional

Dezembro/2018

Dedicatória

A toda minha família e em especial
aos meus pais por todo incentivo.

Agradecimentos

Primeiro agradeço a Deus, pela sua riquíssima misericórdia que tem para conosco, suas criaturas. Pelas muitas bênçãos e forças que tem dado para que eu possa superar as adversidades que surgiram ao longo desses anos de estudos.

Um agradecimento especial vai para minha família, minha esposa Geovania Franklin e meus filhos José Eudes e Maria Rita, que estiveram ao meu lado nos momentos de conquistas e principalmente nos momentos de dificuldades e angustias, me dando apoio e incentivando a seguir em frente. Esse agradecimento se estende também a familiares e amigos, que por algumas vezes não pude estar com eles por necessidade de tempo para se dedicar aos estudos.

Não posso deixar de agradecer a SBM, por ofertar o curso e me dar a oportunidade de ingressar nele para ampliar meus conhecimentos matemáticos. Meu muito obrigado, vai também para todos os professores e auxiliares que ministraram as disciplinas e com os quais tive a honra de estar adquirindo novos conhecimentos através das aulas lecionadas por cada um deles. Em especial, agradeço a meu orientador Vandeberg Vieira, que foi mais que um professor, sempre ensinando, apoiando e dando sugestões, na tentativa de explorar o melhor do aluno para desempenhar um bom trabalho.

Resumo

É notória as inúmeras contribuições das congruências lineares e equações diofantinas lineares quando se deseja estudar problemas relacionados à divisibilidade. Além das aplicações em problemas diofantinos, que são aqueles problemas que requerem solução de equação ou de sistema de equações com valores inteiros para as suas incógnitas, as congruências são uma forte ferramenta para se estabelecer resultados substanciais na Teoria dos Números, não apenas em sua parte elementar, mas também na Teoria Analítica, o ambiente onde se estuda com profundidade propriedades dos números primos. Neste trabalho, apresentamos resultados básicos sobre congruências e, portanto, das equações diofantinas, objetivando apresentar um texto que possa ser útil a todo estudante da graduação, como também do Mestrado Profissional em Matemática.

Palavras Chaves: Congruências, Equações Diofantinas, Resolução de Problemas.

Abstract

The innumerable contributions of Linear Congruences and Linear Diophantine Equations are well known when we study problems related to divisibility. In addiction to the applications in Diophantine problems, which are problems that require solution of equation or system of equations with integer values for their unknown results, the congruences are important tools to establish substantial results in the Number Theory, not only in its elementary part, but also in the Analytical Theory, area in which the properties of prime numbers are studied in a higher level. In this paper, we have presented basic results on congruences and, therefore, on Diophantine equations, in order to present a text that can be useful for all undergraduate students, as well as for the Professional Master in Mathematics.

Keywords: Congruences. Diophantine Equations. Problem Solving.

Sumário

Capítulo 1

Introdução

Os números estão entre as diversas coisas que fazem parte do nosso cotidiano; eles nos ajudam a planejarmos e resolvermos diversas situações práticas que vivenciamos a todo momento. O modelo de numeração que hoje nos parece tão organizado, é resultado de um longo processo de aperfeiçoamento ao decorrer dos tempos. Para chegar a essa sistematização dos números, que tanto usamos no nosso dia a dia, foram necessários muito estudo.

O conceito de *número* foi um dos primeiros conceitos matemáticos assimilados pelo homem na antiguidade, surgiu devido às necessidades do processo de contagem em algumas situações do cotidiano e serviu de base para a formulação do conjunto numérico que hoje denominamos de números naturais, constituído de um modelo matemático que permite a definição de operações matemáticas entre seus elementos. Os conceitos e as notações matemáticas foram sendo construídos pouco a pouco ao longo dos tempos, tendo origem na resolução de problemas, oriundos das necessidades diárias enfrentadas pelo homem. Esses conceitos foram sendo aperfeiçoados e se tornando cada vez mais fascinante a utilização deles nas resoluções dos problemas, desde os de natureza mais simples aos mais sofisticados.

Em [4], os autores apresentam algumas definições para a Matemática. Vejamos algumas delas:

"*A Matemática é a ciência exata que trata das quantidades e de suas medidas*";

"*Matemática é a arte de calcular*";

"*Matemática é a ciência dos números e das figuras*".

A tarefa de definir aquela que é considerada a rainha das ciências não é nada fácil. A Matemática não se restringe apenas na medição de quantidades e em fazer cálculos triviais. Ela também abrange outros elementos, tais como vetores, conjuntos, espaços vetoriais, transformações, entre outros. Quando sintetizamos a Matemática em poucas palavras, como nas supracitadas, estamos abrangendo alguns de seus muitos aspectos.

O matemático e filósofo grego, Pitágoras (570 a.C - 495 a.C), considerava os números como "a essência e o princípio da todas as coisas". Apesar de ser um matemático amador,

ele deu grandes contribuições à Matemática; seu resultado mais famoso, intitulado Teorema de Pitágoras, assegura que em um triângulo retângulo, o quadrado da medida da hipotenusa é igual à soma dos quadrados das medidas dos catetos.

Aspectos Históricos

Na história da Matemática, podemos apontar seis importantes etapas de acordo com fatos ocorridos que merecem destaques e que marcaram cada época.

1) Pré-história (até o século VI a.c.).

Nesse período, a Matemática não era uma ciência organizada. Os babilônios e os egípcios faziam uso dela apenas para atender suas necessidades práticas, tais como a agricultura e as atividades pastoris.

2) Época Clássica (séculos VI a.c. – VII d.c.)

Somente nos séculos VI e V a.c., os matemáticos gregos passaram a tratar a Matemática como uma ciência organizada. Diferentemente dos bárbaros e egípcios, os gregos não se preocupavam com a aplicação prática da Matemática; eles exploravam problemas relacionados a processos infinitos, tratavam de problemas de movimento e de continuidade.

Dentre os matemáticos da época, Pitágoras foi um dos que mais contribuíram para essa estruturação da Matemática como ciência. Outro matemático que merece destaque nessa época, na Grécia, é Euclides (século IV a. c.), cuja principal obra foi "*Os Elementos*", contribui bastante para o avanço dos estudos na área da Geometria. Depois de Euclides, outros matemáticos dessa época que deram grandes contribuições para a evolução da Geometria foram Arquimedes (287 a.c.-212 a.c) e Apolônio (02-98 da era cristã). Também merece destaque nesse período, o matemático grego Diofanto de Alexandria (século III d.c), considerado por muitos o "pai da Álgebra". Ele dedicou-se ao estudo de soluções para equações com coeficientes inteiros. É um dos matemáticos mais importante de todos os tempos na área da Teoria dos Números.

3) Época estacionária (séculos V II -XV)

É uma época de transição, em que na Grécia, a ciência sofreu um processo de decadência, devido à invasão dos árabes à cidade de Alexandria em dezembro de 641. Nesse episódio, muitas obras gregas foram destruídas. Os árabes também invadiram e conquistaram a Índia, e lá, encontraram outro tipo de cultura Matemática, com destaque para a Álgebra e para Aritmética.

Os hindus revolucionaram a "arte de calcular" com a introdução do zero no sistema de numeração. Foram os próprios árabes os responsáveis pela propagação da Matemática dos hindus pela Europa, fazendo com que essa ciência ganhasse espaço. Isto possibilitou que outros povos pudessem tomar conhecimento e usa-la cada vez mais.

4) Época do desenvolvimento (séculos XV-XVII)

O desenvolvimento da Álgebra foi consolidado na obra do matemático francês, François Viete (1540-1603), denominada "Álgebra Speciosa". Nessa obra, os símbolos alfabéticos têm uma significação geral, podendo designar números, segmentos de reta, etc.

Também nessa época, a Teoria dos Números ganhou destaque com Pierre de Fermat (1601-1665). Além de François e Fermat, outros matemáticos fizeram parte desse momento, Marin Mersenne (1588-1648) e Blaisel Pascal (1623-1622).

5) Época de revisão (XVII-XVIII)

Foi o momento em que houve uma retomada aos ideais gregos, do método axiomático. Fizeram parte dessa época os matemáticos Leonhard Euler (1707-1783), Joseph Louis Lagrange (1736-1813), Jonh Wilson (1741-1793), Adrien Louis Lagrange (1752-1833), Carl Friedrish Gauss (1777-1855) e Agostin Louis Cauchy (1777- 1857). É importante destacar que Euler é considerado até hoje o matemático mais prolífero de todos os tempos. A obra por ele deixada é extremamente volumosa. Entre suas contribuições mais conhecidas na Matemática moderna estão: a introdução da função gama, a analogia entre o cálculo infinitesimal e o cálculo das diferenças finitas, quando discutiu minunciosamente todos os aspectos formais do Cálculo Diferencial e Integral, da época. Foi o primeiro matemático a trabalhar com as funções seno e cosseno. Já Gauss é considerado o maior matemático de todos os tempos. Ele também é conhecido como o príncipe dos matemáticos. Ele desenvolveu trabalhos em álgebra, teoria dos números, equações diferenciais, teoria de funções elípticas, cartografia, pesquisou o campo magnético terrestre, participou do desenvolvimento do primeiro telégrafo elétrico, contribuiu para a física-matemática com trabalhos em eletromagnetismo e gravitação, além de inúmeros outros tópicos aos quais dedicou suas pesquisas. Dando importantes contribuições, não apenas à Matemática, mas também para outras ciências, como física e astronomia.

6) Época do desenvolvimento formal (século XVIII em diante)

Foram elaboradas cada vez mais teorias mais gerais e mais abstratas, fazendo com que a Matemática atingisse um notável desenvolvimento em suas diversas áreas de atuação. Dentre os que contribuíram muito para uma formalidade e universalização da Matemática, destacam-se Gauss, Cauchy e, além desses, também merecem destaque Peter Gustav Dirichlet (1805-1859), Friedrich Nelson Cole (1861-1927), Axel Thue (1863-1922), Charles de La Vallé e Poisson (1866-1962). Todos esses matemáticos deram grandes contribuições para o desenvolvimento matemático; muitos deles atuaram principalmente na área da Teoria dos Números, com estudos e demonstrações de resultados de alta complexidade.

A Importância da Teoria dos Números para a Matemática

Foi a partir da necessidade de contagem e de resolução de problemas do cotidiano do homem, na antiguidade, que a Matemática começou a ser utilizada de forma mais dinâmica e foi se estruturando até tornar-se uma das ciências que mais contribuíram para o desenvolvimento e avanço de outras ciências, como Física, Biologia, Economia, Engenharia e Informática. A Matemática é uma ciência multifacetada, que abrange diversas áreas de estudos, tais como Geometria, Análise, Topologia, Álgebra, Aritmética, e Teoria dos Números.

A Teoria dos Números é um ramo de destaque da Matemática Pura. Ela se dedica ao estudo dos números inteiros e suas generalizações. Uma parte desse estudo está relacionado com soluções de problemas que requerem solução de equações ou sistemas de equações com valores inteiros para suas incógnitas. Ela exige a capacidade de investigação e argumentação na busca por soluções dos problemas inerentes. Além das propriedades dos números inteiros, alguns desses problemas necessitam de conhecimentos de outras áreas da Matemática para serem resolvidos.

Gauss, que contribuiu significativamente para o desenvolvimento da Teoria dos Números, uma vez, disse: "a Matemática é a rainha das ciências e a Teoria dos Números é a rainha da Matemática". Por essa frase, daquele que é considerado o maior dos matemáticos de todos os tempos, podemos notar a grande importância que a Teoria dos Números tem dentro da Matemática.

Enfoque para o Ensino

Os Parâmetros Curriculares Nacionais são um documento que tem como proposta fazer a integração da base nacional comum do ensino básico em suas diversas áreas, em todo o país. Em [5], podemos observar que esse documento foi elaborado para auxiliar as equipes escolares na execução de seus trabalhos e servem de orientação para o planejamento de aulas e sobre tudo para o desenvolvimento do currículo da escola. As competências exigidas na área de Ciências da Natureza, Matemática e suas Tecnologias têm como desafio promover o aprofundamento dos saberes e superar as deficiências e as carências das disciplinas de biologia, química, física e matemática, que compõem essa área de ensino. De acordo com a referência [6], a Matemática ocupa uma posição singular nesse processo de interdisciplinaridade, sendo fundamental na formação dos alunos. Mas não é só nesse sentido que a Matemática tem utilidades, possivelmente, não existe nenhuma atividade da vida contemporânea, da música à informática, do comércio à meteorologia, da medicina à cartografia, das engenharias às comunicações, em que a Matemática não compareça de maneira insubstituível para codificar, ordenar, quantificar e interpretar compassos, taxas, dosagens, coordenadas e resolver problemas diversos. As formas de pensar dessa ciência possibilitam ir além da descrição da realidade e da elaboração de modelos.

Aritmética é, em geral, um componente curricular obrigatório em cursos de Licenciatura em Matemática. Sua ementa contém conteúdos que possibilitam ao aluno a aquisição

de conhecimentos ligados à aritmética dos números naturais e inteiros, os quais são requisitos necessários e exigidos daqueles que lecionarão na educação básica. O papel da Teoria dos Números na formação do professor de Matemática para atuar no Ensino Fundamental e Médio é, acima de tudo, agregar conhecimentos específicos de conteúdos a serem trabalhados pelo docente com seus alunos, possibilitando-o atender as necessidades pedagógicas exigidas na pratica do ensino.

Essa disciplina conecta os conteúdos estudados no ensino superior com aqueles que o professor do ensino básico precisa para ministrar suas aulas, possibilitando a esse professor maior segurança na transmissão de conhecimentos mais sofisticados do universo matemático, em suas aulas.

Na Teoria dos Números, um mesmo problema pode requerer em sua resolução a utilização simultânea de métodos de outras áreas da matemática, como álgebra, topologia, análise ou mesmo geometria. Assim, ela é um ramo da Matemática que faz uso com frequência, das demais áreas. Dessa forma, a Teoria dos Números ganha destaque e importância no processo de ensino, tornando-se um dos ramos mais populares da Matemática.

Neste trabalho, iremos considerar alguns resultados da Teoria dos Números, objetivando empregá-los na resolução de alguns problemas que envolvem congruências lineares e equações diofantinas lineares. Por isto, organizamos o trabalho na seguinte forma:

No Capítulo 2, apresentamos alguns resultados preliminares que serão usados ao longo do texto. Entre os quais destacamos aqueles relacionados à divisibilidade, sendo o Algoritmo da Divisão sua parte principal, máximo divisor comum entre dois inteiros.

No Capítulo 3, abordamos os números primos, com destaque especial ao Teorema Fundamental da Aritmética e o Crivo de Eratóstenes.

No Capítulo 4, destacamos alguns conceitos e resultados de congruências e equações diofantinas. Aproveitamos esse capítulo para apresentar os Teoremas de Fermat e de Euler, que são dois clássicos da Teoria das Congruências. Como não poderia deixar de ser, apresentamos o Teorema Chinês dos Restos, que é um resultado central para o estudo dos sistemas de congruências lineares.

Por fim, no Capítulo 5, consideramos algumas aplicações básicas das congruências lineares, como também das equações diofantinas com duas e três incógnitas. Essas aplicações constituem essencialmente de situações-problemas.

Capítulo 2

Preliminares

2.1 Divisibilidade

O conceito de *divisibilidade* sobre o conjunto dos números inteiros é um tópico básico e central, não apenas para a Teoria Elementar, como também para outros ramos da Teoria dos Números. Por isso, neste capítulo, iremos considerar esse conceito e apresentar suas principais propriedades, que são extremamente importantes para alcançarmos os objetivos em que o trabalho se insere. Apresentaremos também tópicos relacionados como máximo divisor comum e mínimo múltiplo comum, destacando resultados elementares, porém necessários para os capítulos posteriores. Entre os resultados aqui abordados, destacaremos de modo especial o Algoritmo da Divisão, que é algo emblemático na Teoria dos Números.

Sabe-se que dados dois inteiros arbitrários a e b, nem sempre o quociente a/b é um número inteiro, ou melhor, não existe um inteiro k de modo que $a = bk$. Isto nos conduz ao conceito de divisibilidade.

Definição 2.1.1 *Sejam a e b dois números inteiros com $b \neq 0$. Diremos que b **divide** a, e indicamos por $b \mid a$, se existir $k \in \mathbb{Z}$ tal que*

$$a = bk.$$

Escrevemos $b \nmid a$ para indicar o fato que b não divide a. Assim,

$$b \mid a \;\Leftrightarrow\; a = bk \;\text{ para algum }\; k \in \mathbb{Z}.$$

Exemplo 2.1.2 Temos que $-3 \mid 12$, pois $12 = (-3)\cdot(-4)$ e ainda que $15 \nmid -7$, pois não existe $k \in \mathbb{Z}$, tal que $-7 = 15 \cdot k$.

Além disso, $1 \mid a$, $a \mid a$ e $a \mid 0$, pois $a = 1 \cdot a$, $a = a \cdot 1$ e $0 = a \cdot 0$ para todo $a \in \mathbb{Z}$. $\triangle$

Lema 2.1.3 *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então existe $k \in \mathbb{Z}$ tal que $a = b \cdot k$. Logo,

$$|a| = |b \cdot k| = |b| \cdot |k| .$$

Segue que $k \neq 0$, já que $a \neq 0$, então $1 \leq |k|$. Assim, multiplicando $1 \leq |k|$ por $|b|$, obtemos que $|b| \leq |b| \cdot |k| = |a|$. □

Se b é um divisor de a, segue que $-b$ também o é, visto que se $a = bc$, então $a = (-b)(-c)$. Por isso, os divisores de um número sempre ocorrem em pares. Desse modo, a fim de determinar todos os divisores de um inteiro a, é suficiente encontrar todos os seus divisores positivos.

Para um número inteiro a, indicaremos seu conjunto de divisores positivos por D_a, e para $a \neq 0$, denotaremos seu conjunto de múltiplos positivos por M_a, ou seja,

$$D_a = \{n \in \mathbb{N} : n \mid a\} \quad \text{e} \quad M_a = \{n \in \mathbb{N} : a \mid n\}.$$

Observe que $D_a = D_{-a}$ e $M_a = M_{-a}$.

O conjunto D_a é sempre finito e contém pelo menos os números 1 e $|a|$. Por exemplo,

$$D_1 = \{1\}, \quad D_2 = \{1,2\}, \quad D_6 = \{1,2,3,6\}, \quad D_9 = \{1,3,9\}.$$

Já para cada inteiro não nulo a, o conjunto M_a é infinito e contém sempre $|a|$. Assim,

$$M_1 = \mathbb{N}, \quad M_2 = \{2,4,6,8,\ldots\}, \quad M_3 = \{3,6,9,12,\ldots\}.$$

Exemplo 2.1.4 Determinar todos os números inteiros n para os quais $n+1$ divide $n^3 - 3$.

Solução: Mostra-se que $n^3 - 3 = (n+1)(n^2 - n + 1) - 4$, de modo que

$$\frac{n^3 - 3}{n+1} = n^2 - n + 1 - \frac{4}{n+1}, \text{ com } n \neq -1.$$

Como $n^2 - n + 1 \in \mathbb{Z}$, segue que $n+1$ divide $n^3 - 3$ se, e somente se, $n+1$ divide 4. Visto que os divisores de 4 são ± 1 e ± 2 e ± 4 , devemos ter

$$n+1 = \pm 1, \quad n+1 = \pm 2 \text{ e } n+1 = \pm 4,$$

de onde obtemos $n = 0$, $n = -2$, $n = -3$, $n = 1$, $n = -5$ e $n = 3$. △

Exemplo 2.1.5 Dados inteiros a e b, mostrar que $a - b$ divide $a^n - b^n$ para todo $n \in \mathbb{N}$.

Solução: Provemos por meio de indução finita. Para $n = 1$, o resultado segue imediatamente. Por hipótese de indução, suponhamos que $a - b$ divide $a^n - b^n$, com $n \geq 1$. Notemos que, para $n+1$,

$$a^{n+1} - b^{n+1} = a \cdot a^n - b \cdot a^n + b \cdot a^n - b \cdot b^n = (a-b) \cdot a^n + b \cdot (a^n - b^n).$$

Já que $a-b$ divide ele mesmo e, por hipótese, $a-b$ divide a^n-b^n, segue da igualdade acima que $a-b$ divide $a^{n+1}-b^{n+1}$. Isto completa a indução e, com isto, segue a prova do resultado. $\triangle$

o resultado a seguir traduz o fato de o conjunto D_a ser sempre finito, desde que o inteiro a seja não nulo.

Lema 2.1.6 (Limitação) *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então por definição, existe $c \in \mathbb{Z}^*$ tal que $a = b \cdot c$ (c é diferente de zero, pois assim é o inteiro a). Logo,

$$|a| = |b \cdot c| = |b| \cdot |c| .$$

Como $c \neq 0$, segue que $1 \leq |c|$. Assim, multiplicando os lados desta desigualdade por $|b|$, obtemos $|b| \leq |b| \cdot |c| = |a|$. $\square$

Proposição 2.1.7 *Em $\mathbb{Z}$, valem as seguintes propriedades:*

(1) *Os únicos divisores de 1 são 1 e -1.*

(2) *Se $a \mid b$ e $b \mid a$, então $a = \pm b$.*

Demonstração: (1) Se b é um divisor de 1, então pelo Lema 2.1.6, $|b| \leq 1$. Assim, $0 < |b| \leq 1$. Como não existe inteiro entre 0 e 1, concluímos que $|b| = 1$, isto é, $b = \pm 1$.

(2) Por hipótese, $a = \lambda_1 b$ e $b = \lambda_2 a$, com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Desse modo,

$$a = (\lambda_1 \lambda_2) a,$$

ou seja, $\lambda_1 \lambda_2 = 1$ e, pelo item (1), $\lambda_1 = \pm 1$, o que implica $a = \pm b$. $\square$

No próximo teorema, apresentaremos outras propriedades elementares da divisibilidade.

Teorema 2.1.8 *A divisibilidade tem as seguintes propriedades:*

(1) *Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

(2) *Se $a \mid b$ e $c \mid d$, então $ac \mid bd$.*

(3) *Se $a \mid b$ e $a \mid c$, então $a \mid (bx+cy)$, $\quad \forall\, x, y \in \mathbb{Z}$.*

Demonstração: (1) Por hipótese, $b = a\lambda_1$ e $c = b\lambda_2$, com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Substituindo o valor de b em $c = b\lambda_2$, obtemos $c = a(\lambda_1 \lambda_2)$, ou seja, $a \mid c$.

(2) Sendo $b = ak_1$ e $d = ck_2$, temos $bd = (ac)(k_1 k_2)$, isto é, $ac \mid bd$.

(3) Por hipótese, temos que $b = ak_1$ e $c = ak_2$. Logo, dados inteiros x e y, $bx = axk_1$ e $cy = ayk_2$, de modo que $bx + cy = a(xk_1 + yk_2)$. Assim, $a \mid (bx + cy)$. □

A Propriedade (3) do teorema anterior pode ser generalizada da seguinte forma: se $a_1, a_2, \ldots, a_n$ são números inteiros divisíveis por a, então

$$a \mid (a_1x_1 + a_2x_2 + \cdots + a_nx_n),$$

para quaisquer inteiros $x_1, x_2, \ldots, x_n$.

Como consequência do Teorema 2.1.8, temos para quaisquer inteiros a, b e c, o seguinte:

- $a \mid b$ e $a \mid c \Rightarrow a \mid b + c$ e $a \mid b - c$.
- $a \mid b \Rightarrow a \mid bx$ para qualquer inteiro x.
- $a \mid b$ e $a \mid c \Rightarrow a \mid bx - cy$.

2.2 Divisão Euclidiana

A Divisão Euclidiana, também conhecida como Algoritmo da Divisão, é um dos resultados mais básicos e importantes da Teoria dos Números. Ela é muito familiar para estudantes não apenas de nível superior, mas também para os do ensino básico. Esse resultado é atribuído a Euclides, que o apresentou em seu livro Elementos (cf. [1]).

As primeiras introduções que abordam a divisão nas etapas iniciais de ensino sempre fazem referência a situações básicas como, por exemplo, dividir uma quantidade a de objetos para b pessoas. O resultado desta divisão resulta em q objetos para cada uma das pessoas e r objetos restantes, que pode ser igual a zero.

Conforme já destacamos, nem sempre se pode dividir um inteiro por outro de modo a se obter um número inteiro, ou seja, essa divisão nem sempre é exata. Por exemplo, tomando os inteiros $a = 21$, $b = 4$ e dividindo a por b, obtemos

$$21 = 4 \cdot 5 + 1.$$

Numa linguagem bem elementar, quando dividimos de forma igualitária vinte e um objetos entre quatro pessoas, de modo que cada uma receba sempre uma quantidade inteira desses objetos, cada uma delas receberá cinco objetos, e ainda sobrará um. De uma forma geral, temos:

Teorema 2.2.1 (Divisão Euclidiana) *Sejam $a, b \in \mathbb{Z}$, com $b > 0$, existem únicos $q, r \in \mathbb{Z}$ tais que*

$$a = b \cdot q + r, \quad com \quad 0 \leq r < b.$$

Demonstração: Há duas coisas a serem provadas: uma é a existência dos inteiros q e r nas condições exigidas, e a outra é a unicidade destes inteiros.

(**Existência**) Consideremos o conjunto

$$L = \{a - bq : q \in \mathbb{Z} \quad \text{e} \quad a - bq \geq 0\}.$$

Uma primeira coisa a ser verificada é que L é não vazio. De fato, já que $b \geq 1$, temos $|a| \cdot b \geq |a|$. Logo,

$$a - (-|a|) \cdot b = a + |a| \cdot b \geq a + |a| \geq 0.$$

Como $x = a - (-|a|) \cdot b$ é da forma $a - bq$, com $q = -|a|$, segue que $x \in L$. Sendo L limitado inferiormente (por zero, por exemplo) e não vazio, temos pelo Principio da Boa Ordenação-PBO que L possui menor elemento, digamos $r = \min L$. Como $r \in L$, $r \geq 0$ e

$$r = a - bq, \quad \text{com} \quad q \in \mathbb{Z}.$$

Asseguramos que $r < b$. De fato, se isto não ocorrer, então $r - b \geq 0$ e

$$r - b = a - bq - b = a - b(q+1).$$

Portanto, $r - b \in L$ e $r - b < r$, o que contraria a minimalidade de r. Esta contradição mostra que $r < b$. Por conseguinte, $a = qb + r$, com $q \in \mathbb{Z}$ e $0 \leq r < b$, o que prova a existência dos inteiros q e r.

(**Unicidade**) Para a unicidade, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

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

Assim, $bq + r = bq_1 + r_1$, o que implica

$$r - r_1 = b(q_1 - q),$$

ou seja, $b \mid (r - r_1)$. Como $|r - r_1| < b$, segue que $r - r_1 = 0$, isto é, $r = r_1$. Por isso, $q_1 = q$, uma vez que $b \neq 0$. □

Uma versão mais geral do Algoritmo da Divisão é obtida quando substituímos a condição $b > 0$ por $b \neq 0$, de acordo com o seguinte:

Corolário 2.2.2 (Algoritmo da Divisão - Versão Geral) *Dados inteiros a e b, com $b \neq 0$, existem únicos inteiros q e r tais que*

$$a = bq + r, \quad \textit{com} \quad 0 \leq r < |b|. \tag{2.1}$$

Os inteiros q e r dados em (2.1) são chamados **quociente** e **resto** da Divisão Euclidiana de a por b, respectivamente. Às vezes, r também é dito o **resto de a módulo b**. Quando $b > 0$, r é indicado por $r = a \bmod b$. Neste caso, dizemos que r **é igual a a reduzido módulo b**.

Algumas calculadoras e algumas linguagens de programação têm uma função frequentemente denotada por $\text{mod}(a, b)$, cujo valor é exatamente $r = a \bmod b$.

Exemplo 2.2.3 Temos que $2 = -10 \bmod -4$, pois $-10 = 3 \cdot (-4) + 2$, isto é, na divisão de -10 por 3 o quociente e o resto são respectivamente -4 e 2. $\triangle$

Como uma primeira aplicação da Divisão Euclidiana, notemos que se a é um inteiro qualquer, então ao efetuar sua divisão por $b = 2$, temos que os possíveis restos são $r = 0$ ou $r = 1$, ou seja,

$$a = 2q + r, \quad \text{com} \quad 0 \leq r \leq 1.$$

Quando $r = 0$, segue que a é da forma $a = 2q$. Um inteiro assim é chamado de **número par**. Se $r = 1$, então $a = 2q + 1$. Qualquer inteiro desta forma é chamado de **número ímpar**.

É claro que zero é um número par. Os números -8 e 10 também são pares, pois

$$8 = 2 \cdot (-4) \quad \text{e} \quad 10 = 2 \cdot 5,$$

enquanto -9 e 37 são ímpares, visto que

$$-9 = 2 \cdot (-5) + 1 \quad \text{e} \quad 37 = 2.18 + 1.$$

Dizemos que a e b têm a **mesma paridade** quando a e b são ambos pares ou ambos ímpares.

Se P e I denotam os conjuntos dos números pares e ímpares, respectivamente, então

$$P = \{2k : k \in \mathbb{Z}\} \quad \text{e} \quad I = \{2k + 1 : k \in \mathbb{Z}\}.$$

Podemos verificar que:

(1) $P \cap I = \emptyset$.

(2) Se $x, y \in P$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in P$.

(3) Se $x, y \in I$, então $x \pm y \in P \quad \text{e} \quad x \cdot y \in I$.

(4) Se $x \in P$ e $y \in I$, então $x \pm y \in I \quad \text{e} \quad x \cdot y \in P$.

No exemplo que segue, consideraremos algumas aplicações elementares do Algoritmo da Divisão. Lembremos que um inteiro a é um **quadrado perfeito** quando $a = q^2$, para algum inteiro q.

Exemplo 2.2.4 Mostrar que:

a) *Todo quadrado perfeito é da forma* $4k$ *ou* $4k + 1$.

b) *Todo inteiro ímpar é da forma* $4k + 1$ *ou* $4k + 3$.

c) *O quadrado de todo inteiro ímpar é da forma* $8k + 1$.

Solução: a) Se $a = 2q$, então $a^2 = 4q^2 = 4k$, com $k = q^2$; e se $a = 2q+1$, então $a^2 = 4(q^2+q)+1 = 4k+1$, em que $k = q^2+q$.

b) Dado um número inteiro a, temos pelo Algoritmo da Divisão que

$$a = 4q + r, \quad \text{com} \quad 0 \leq r < 4,$$

ou seja, a pode assumir as seguintes formas: $4q$, $4q+1$, $4q+2$ ou $4q+3$. Logo, se a é ímpar, então pelas considerações anteriores, concluímos que $a = 4q+1$ ou $4q+3$.

c) Sendo a ímpar, segue do item b) que $a = 4q+1$ ou $4q+3$. Se $a = 4q+1$, então

$$a^2 = 8(2q^2+q)+1 = 8k+1,$$

com $k = 2q^2+q$. Se $a = 4q+3$,

$$a^2 = 8(2q^2+3q+1)+1 = 8k+1,$$

em que $k = 2q^2+3q+1$. △

2.3 Máximo Divisor Comum

O conceito de *Máximo Divisor Comum* (mdc) está relacionado a resultados essenciais da Teoria dos Números. Neste trabalho, sua importância e utilidade estão nas aplicações elementares da resolução de problemas diversos.

Nas séries iniciais, quando fazemos o estudo de mdc, geralmente consideramos dois números naturais relativamente pequenos, com intuito de determinar seus divisores positivos, identificar os divisores comuns e verificar o maior entre eles. Há também, na maioria dos livros adotados nesse nível de ensino, um método prático que consiste na fatoração simultânea desses números por meio de divisões sucessivas por números primos, e considerando apenas os fatores primos comuns nesse processo; o resultado segue do produto destes. Por exemplo,

40, 72	2
20, 36	2
10, 18	2
5, 9	3
5, 3	3
5, 1	5
1, 1	

De modo que considerando o produto dos fatores comuns, temos que o máximo divisor comum de 40 e 72 é 8.

Numa linguagem mais técnica: tomemos a e b números inteiros, não ambos nulos, e consideremos

$$D_a = \{n \in \mathbb{N} : n \mid a\} \quad \text{e} \quad D_b = \{n \in \mathbb{N} : n \mid b\},$$

É claro que $D_a \cap D_b \neq \emptyset$, pois $1 \mid a$ e $1 \mid b$. Além disso, da acordo com o Lema 2.1.6 $D_a \cap D_b$ é um conjunto finito e, por isso, possui maior elemento, o qual é chamado **máximo divisor comum** dos números a e b.

Quando $a = b = 0$, o conjunto $D_a = D_b$ é infinito. É por isso que este caso não será considerado e convencionaremos que o máximo divisor comum entre eles é zero.

O que faremos aqui é essencialmente a mesma coisa, apenas com certo rigor e destacando propriedades relevantes relacionadas ao conteúdo que forma um dos pilares da Aritmética.

Definição 2.3.1 *Dados $a, b \in \mathbb{Z}$, com $a \neq 0$ ou $b \neq 0$, o inteiro positivo d é o **máximo divisor comum** (mdc) de a e b quando:*

(a) $d \mid a$ e $d \mid b$.

(b) Se $c \in \mathbb{Z}$, é um divisor comum de a e b, então c é um divisor de d.

Em outras palavras, o máximo divisor comum de a e b é um inteiro positivo que os divide e é divisível por todo divisor comum de a e b. Indicaremos este número por

$$d = mdc(a,b),$$

por familiaridade com a notação utilizada pela maioria dos livros didáticos do ensino básico, ou simplesmente $d = (a,b)$ por razão de praticidade. Notemos que:

$$mdc(a,b) = mdc(b,a)$$

Em alguns casos particulares, é imediato calcular o mdc. Por exemplo, se a é um número inteiro não nulo, temos claramente que:

(1) $mdc(a,0) = |a|$.

(2) $mdc(a,1) = 1$.

(3) $mdc(a,a) = |a|$.

Além disso, para todo $b \in \mathbb{Z}$, temos que a divide b se, e somente se, $|a|$ é o mdc entre a e b, ou seja,

$$a \mid b \;\Leftrightarrow\; mdc(a,b) = |a|.$$

Também, é imediato verificar que:

$$mdc(a,b) = mdc(-a,b) = mdc(a,-b) = mdc(-a,-b).$$

Assim, vamos assumir que a e b são sempre positivos.

O próximo teorema é fundamental para soluções de muitos problemas na Teoria dos Números, pois nos dá uma proveitosa identidade que relaciona os números a e b e seu mdc. Tal identidade é conhecida como identidade de **Bachet-Bézout** para os inteiros a e b. Esta denominação é pelo fato de o matemático francês Claude-Gaspard Bachet (1581-1638) ser o primeiro a provar este resultado, o qual foi posteriormente generalizado para polinômios pelo também matemático francês Étienne Bézout (1730-1783).

Teorema 2.3.2 (Bachet-Bézout) *Se $d = mdc(a,b)$, então existem inteiros x_0 e y_0 tais que*

$$d = ax_0 + by_0. \tag{2.2}$$

Demonstração: Consideremos o conjunto

$$W = \{ax + by : x, y \in \mathbb{Z} \quad \text{e} \quad ax + by > 0\}.$$

Notemos de início que W não é vazio, pois para $x = y = 1$,

$$a \cdot 1 + b \cdot 1 = a + b > 0 \;\Rightarrow\; a + b \in W.$$

Desse modo, pelo PBO, W possui menor elemento, digamos $\lambda = \min W$. Vamos mostrar que $\lambda = mdc(a,b)$. Como $\lambda \in W$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$\lambda = ax_0 + by_0. \tag{2.3}$$

Usando o Algoritmo da Divisão com os inteiros a e λ, temos

$$a = \lambda q + r, \quad \text{com} \quad 0 \leq r < \lambda. \tag{2.4}$$

Substituindo o valor de λ em (2.3) na igualdade de (2.4), segue que

$$\begin{aligned} r &= a - \lambda q &&= a - (ax_0 + by_0)q \\ &&&= a - aqx_0 - bqy_0, \end{aligned}$$

ou melhor,

$$r = a(1 - qx_0) + b(-qy_0).$$

Isto nos mostra que $r = au + bv$, com $u = 1 - qx_0$ e $v = -qy_0$. Por conseguinte, $r = 0$, pois do contrário, $r > 0$ e, assim, $r \in W$, o que contraria o fato de λ ser o mínimo de W, visto que $r < \lambda$. Portanto, $a = \lambda q$, ou seja, $\lambda \mid a$. Similarmente, prova-se que $\lambda \mid b$. Com isto, tem-se que $\lambda \mid d$, pois $d = mdc(a,b)$.

Sendo $d = mdc(a,b)$, $a = d\alpha$ e $b = d\beta$, com $\alpha, \beta \in \mathbb{Z}$. Logo, por (2.3), $\lambda = ax_0 + by_0$.

$$\lambda = (d\alpha)x_0 + (d\beta)y_0 = d(\alpha x_0 + \beta y_0),$$

ou seja, $d \mid \lambda$, e como $\lambda \mid d$, segue que $d = \lambda$. Logo, $d = ax_0 + by_0$. □

Pelo teorema anterior, se $d = mdc(a,b)$, então podemos escrevê-lo na forma

$$d = ax_0 + by_0,$$

com $x_0, y_0 \in \mathbb{Z}$. Por isso, dizemos que d é uma *combinação linear*[1] de a e b. Além disso, tal combinação não é única. Por exemplo,

$$\begin{aligned} mdc(6,10) &= 2 = 6\cdot 2 + 10\cdot(-1) \qquad (x_0 = 2 \text{ e } y_0 = -1) \\ &= 6\cdot(-3) + 10\cdot(2). \quad (x_0 = -3 \text{ e } y_0 = 2) \end{aligned}$$

Em geral, todos os pares de inteiros (x_0, y_0) que satisfazem a identidade $10x + 6y = 2$ são obtidos das expressões algébricas

$$x = 2 + 10k \quad \text{e} \quad y = -1 - 6k,$$

em que k percorre todos os inteiros. Nota-se que $6(2+10k) + 10(-1-6k) = 2$. Veremos isto em detalhes quando considerarmos equações diofantinas lineares.

2.3.1 Algoritmo de Euclides

Quando os inteiros $a > 0$ e $b > 0$ assumem valores "pequenos", o valor de $d = mdc(a,b)$ é determinado sem muitas dificuldades. Mas, como determiná-lo quando a e b são números muito grandes? Por exemplo, quanto vale $mdc(17588, 1875)$? Neste caso, não é conveniente descrever D_a e D_b e verificar o maior elemento do conjunto $D_a \cap D_b$. Isso seria tedioso e bem exaustivo! Veremos que o Lema 2.3.3 é um resultado extremamente importante, sendo base para a obtenção de um método bastante eficiente para se calcular $d = mdc(a,b)$ para quaisquer inteiros positivos a e b, o qual consiste em divisões sucessivas (o Algoritmo de Euclides).

Ao leitor interessado em analisar a prova que não for apresentada nesta seção, recomendamos as referências [2], [3], e [8].

Lema 2.3.3 (Euclides) *Se $a = bq + r$, então $mdc(a,b) = mdc(b,r)$.*

Demonstração: É suficiente mostrar que $D_a \cap D_b = D_b \cap D_r$, pois se estes conjuntos forem iguais, seus elementos máximos também serão iguais. Se $d \in D_a \cap D_b$, então $d \mid a$ e $d \mid b$. Assim, como $r = a - qb$, segue que $d \mid r$ e, por isso, $d \in D_b \cap D_r$. Desse modo, temos a inclusão $D_a \cap D_b \subset D_b \cap D_r$. Por outro lado, dado $d \in D_b \cap D_r$, temos $d \mid b$ e $d \mid r$. Daí, $d \mid bq + r = a$, isto é, $d \in D_a \cap D_b$. Isto acarreta a inclusão $D_b \cap D_r \subset D_a \cap D_b$. Por conseguinte, $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc(a,b) = mdc(b,r)$. □

Exemplo 2.3.4 Como $30 = 4\cdot 7 + 2$, $mdc(30,4) = mdc(4,2) = 2$ e $mdc(30,7) = mdc(7,2) = 1$. △

[1] Uma *combinação linear* de a e b é toda expressão da forma $ax + by$, em que x e y são inteiros.

Exemplo 2.3.5 Dado $n \in \mathbb{N}$, provar que $mdc(n+1, n^2+n+1) = 1$.

Solução: Para qualquer inteiro positivo n, vale a igualdade

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

Assim, do Lema de Euclides, $mdc(n^2+n+1, n+1) = mdc(n+1, 1) = 1$. △

É importante destacar que o resultado do lema anterior é válido mesmo que r não seja o resto da divisão de a por b.

A aplicação repetida do lema acima consiste no *Algoritmo de Euclides* (*Algoritmo da Divisão*) que cessa ao chegarmos ao resto zero no processo de divisões sucessivas e, consequentemente, o último resto não nulo é o mdc de a e b.

Exemplo 2.3.6 Calcular $mdc(72, 42)$.

Solução: Aplicando divisões sucessivas, temos:

$$\begin{aligned} 72 &= 42 \cdot 1 + 30, \\ 42 &= 30 \cdot 1 + 12, \\ 30 &= 12 \cdot 2 + 6, \\ 12 &= 6 \cdot 2 + 0. \end{aligned} \tag{2.5}$$

Logo,

$$mdc(72, 42) = mdc(42, 30) = mdc(30, 12) = mdc(12, 6) = 6.$$

△

Exemplo 2.3.7 Escrever o resultado do exemplo anterior na forma do Teorema 2.3.2.

Solução: Devemos encontrar x_0 e y_0 tais que $72 \cdot x_0 + 42 \cdot y_0 = 6$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (2.5), substituindo-os sucessivamente. Temos:

$$\begin{aligned} 6 = 30 \cdot 1 - 12 \cdot 2 &= 30 \cdot 1 - 2 \cdot (42 - 1 \cdot 30) \\ &= 30 \cdot 3 - 2 \cdot 42 \\ &= (72 \cdot 1 - 42 \cdot 1) \cdot 3 - 2 \cdot 42 \\ &= 72 \cdot 3 + 42 \cdot (-5). \end{aligned}$$

Portanto,

$$72 \cdot 3 + 42 \cdot (-5) = 6.$$

Por conseguinte, temos que $x_0 = 3$ e $y_0 = -5$. △

Definição 2.3.8 *Dois inteiros a e b são ditos* ***primos entre si*** *ou* ***relativamente primos*** *quando* $mdc(a,b) = 1$.

Nota-se que os inteiros a e b são primos entre si, se e somente se, existem inteiros x_0 e y_0 tais que

$$1 = ax_0 + by_0 \tag{2.6}$$

Por exemplo, 8 e 5 são primos entre si, pois $mdc(6,5) = 1$; Já 10 e 5 não são primos entre si , uma vez que $mdc(10,5) = 4$.

Exemplo 2.3.9 Para cada inteiro k, mostrar que os inteiros $2k+1$ e $9k+4$ são primos entre si.

Solução: Pelo Lema (2.3.3), temos

$$mdc(2k+1,9k+4) = mdc(9k+4,1) = mdc(1,4) = 1.$$

Portanto, $2k+1$ e $9k+4$ são primos entre si. A partir desta identidade algébrica, pode-se obter infinitos pares de inteiros $a = 2k+1$ e $b = 9k+4$ primos entre si. Assim, para $k = 1$, $mdc(3,13) = 1$, e para $k = 4$, $mdc(9,40) = 1$, e assim por diante. △

Corolário 2.3.10 *Sejam* $a,b,c \in \mathbb{Z}$. *Se* $a \mid bc$ *e* $mdc(a,b) = 1$, *então* $a \mid c$.

Demonstração: Por hipótese, $bc = ak$, com $k \in \mathbb{Z}$. Além disso, por (2.6), existem $x,y \in \mathbb{Z}$ tais que $1 = ax + by$. Multiplicando ambos os lados desta igualdade por c, obtemos

$$c = cax + cby = cax + aky = a(cx + ky).$$

Desse modo, $a \mid c$. □

Outra consequência importante é a seguinte:

Corolário 2.3.11 *Sejam* $a,b \in \mathbb{Z}$ *tais que* $mdc(a,b) = 1$. *Se* $a \mid c$ *e* $b \mid c$, *então* $ab \mid c$.

Encerraremos esta seção com alguns resultados adicionais sobre mdc.

Teorema 2.3.12 *Sejam*[2] a,b,k *e* n *inteiros positivos. Temos:*

(1) $mdc(ka,kb) = k \cdot mdc(a,b)$.

(2) *Se* $n \mid a$ *e* $n \mid b$, *então* $mdc\,(a/n,b/n) = mdc(a,b)/n$.

[2]Estamos considerando $a,b,k \in \mathbb{N}$, mas o resultado continua válido se $a,b,k \in \mathbb{Z}^*$. Neste caso, o item (1) se reescreve como $mdc(ka,kb) = |k| \cdot mdc(a,b)$.

Demonstração: (1) Sendo $d = mdc(a,b)$, segue que $d \mid a$ e $d \mid b$ e, desse modo, $kd \mid ka$ e $kd \mid kb$. Portanto, kd é um divisor comum de ka e kb. Consideremos agora $d_1 \in \mathbb{N}$ um divisor comum de ka e kb. Pela identidade de Bachet-Bézout, existem $x, y \in \mathbb{Z}$ tais que

$$d = ax + by.$$

Multiplicando ambos os lados desta igualdade por k e considerando que $d_1 \mid ka$ e $d_1 \mid kb$, obtemos

$$kd = kax + kby \;\Rightarrow\; d_1 \mid kd.$$

Logo, por definição, $mdc(ka,kb) = kd$, ou seja, $mdc(ka,kb) = k \cdot mdc(a,b)$.

(2) Se $n \mid a$ e $n \mid b$, então por definição, $n \mid d$. Agora, pelo item (1),

$$mdc(a,b) = mdc\left(\frac{an}{n}, \frac{bn}{n}\right) = n \cdot mdc\left(\frac{a}{n}, \frac{b}{n}\right),$$

ou melhor, $mdc\,(a/n, b/n) = mdc(a,b)/n$. □

Exemplo 2.3.13 Temos:

$$mdc(8,28) = mdc(4 \cdot 2, 7 \cdot 4) = 4 \cdot mdc(2,7) = 4 \cdot 1 = 4,$$

e $mdc(50/2, 28/2) = mdc(50,28)/2 = 1$. △

Corolário 2.3.14 *Seja d um divisor comum de a e b. Então, $d = mdc(a,b)$ se, e somente se, a/d e b/d são primos entre si.*

O conceito de máximo divisor comum pode ser estendido naturalmente e de forma semelhante para vários inteiros. Nas referências [2] e [8] tratam disso com detalhes.

2.4 Mínimo Múltiplo Comum

O conceito de *Mínimo Múltiplo Comum* (mmc) é bem semelhante ao conceito de mdc, e bastante familiar aos estudantes de ensino básico. A respeito de sua aplicação neste nível de ensino existem poucos e simples exemplos de situações práticas. Após o próximo teorema traremos um deles.

Sejam a e b dois inteiros não nulos, e tomemos os conjuntos

$$M_a = \{n \in \mathbb{N}; a \mid n\} \quad \text{e} \quad M_b = \{n \in \mathbb{N}; b \mid n\}.$$

Primeiramente, notemos que $|ab| \in M_a$ e $|ab| \in M_b$, de modo que $|ab| \in M_a \cap M_b$. Assim, o conjunto $M_a \cap M_b$ possui menor elemento, chamado de *Mínimo Múltiplo Comum* de a e b, que será indicado por $mmc(a,b)$ ou simplesmente por $[a,b]$.

Resumidamente, temos:

Definição 2.4.1 *Dados $a,b \in \mathbb{Z}$, com $a \neq 0$ e $b \neq 0$, o inteiro positivo m é o* ***mínimo múltiplo comum*** *de a e b, quando:*

(a) $a \mid m$ e $b \mid m$;

(b) Se $c \in \mathbb{Z}$ é um múltiplo comum de a e b, então m é um divisor de c.

Por exemplo,

$$mmc(3,4) = 12, \quad mmc(5,10) = 10 \quad \text{e} \quad mmc(6,-4) = 12.$$

É possível mostrar sem muitas dificuldades que, para quaisquer $a,b \in \mathbb{Z}^*$,

$$mmc(a,b) = mmc(-a,b) = mmc(a,-b) = mmc(-a,-b).$$

Por isso, para o cálculo do mmc, consideremos sempre $a > 0$ e $b > 0$.

O próximo teorema estabelece uma relação muito proveitosa entre o máximo divisor comum e o mínimo múltiplo comum de dois números inteiros. Além do mais é bastante prático no cálculo do mmc, diferentemente dos métodos conhecidos pela maioria dos alunos do ensino básico que por sua vez utiliza fatoração.

Teorema 2.4.2 *Para quaisquer $a,b \in \mathbb{Z}^*$, como $d = mdc(a,b)$ e $m = mmc(a,b)$, temos que*

$$m = \frac{|ab|}{d}.$$

Com efeito, do teorema anterior, o cálculo de $d = mdc(a,b)$, realizado de modo prático por meio do Algoritmo de Euclides, implica diretamente na determinação de $m = mmc(a,b)$. Para tanto, basta dividir o produto ab por d.

Exemplo 2.4.3 Calcular o $mmc(42,72)$.

Solução: Pelo o Algoritmo de Euclides, obtemos que $mdc(42,72) = 6$. Portanto,

$$mmc(42,72) = \frac{42 \cdot 72}{6} = 504$$

△

Exemplo 2.4.4 O soldado José trabalha de 3 em 3 dias e o sargento Joaquim de 4 em 4 dias. Sabendo-se que eles trabalharam juntos hoje, daqui a quantos dias eles voltarão a trabalhar juntos novamente?

Solução: Temos que $mdc(3,4) = 1$. Então pelo último teorema, temos que:

$$mmc(3,4) = \frac{3 \cdot 4}{1} = 12$$

Assim, o soldado José e o cabo Joaquim, voltarão a trabalhar juntos daqui a 12 dias. △

Uma consequência imediata do teorema anterior é o seguinte:

Corolário 2.4.5 *Dados $a,b \in \mathbb{Z}^*$, temos que*

$$mmc(a,b) = ab \iff mdc(a,b) = 1.$$

Capítulo 3

Números Primos

Os números primos têm sido objeto de estudo há mais de 2000 anos e recebe este nome devido aos gregos, seus precursores, que os chamavam de **primeiros**, traduzindo em latim *primus*. Possuem um dos conceitos mais importantes de toda a Matemática. Seus resultados são importantes não apenas para a Teoria dos Números, mas também para a Teoria dos Grupos Finitos. Por isso, eles desempenham um papel importante e estão associados a muitos problemas famosos. Alguns desses resultados ja foram provados, mas ainda existem uma quantidade considerável deles que continuam em aberto. Na referência [7], o leitor poderar verificar uma lista desses problemas.

3.1 Teorema Fundamental da Aritmética

O Teorema Fundamental da Aritmética (TFA) assegura que todo inteiro $a \in \mathbb{Z} - \{0, \pm 1\}$ pode ser escrito como produto finito de primos. Em outras palavras, os primos são suficientes para gerar todos os inteiros diferentes de 0 e ± 1. Isso mostra a importância desses números na Teoria dos Números.

Os números primos, com relação à divisibilidade, são os mais simples, conforme a seguinte:

Definição 3.1.1 *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ é **primo** quando seus únicos divisores positivos são 1 ou $|p|$. Caso contrário, dizemos que p é **composto**.*

Por exemplo, os números 2, -3, 5 e 13 são primos, enquanto $6 = 2 \cdot 3$, $15 = 3 \cdot 5$ e $18 = 2 \cdot 9$ são compostos.

Notemos que o número 2 é o único primo par. O número 1 não é primo nem composto.

Como p é primo se, e somente se, $-p$ é primo, vamos considerar apenas primos positivos, e o conjunto desses primos indicaremos por $\mathscr{P}$, ou seja,

$$\mathscr{P} = \{2, 3, 5, 7, 11, 13, 17, ...\}$$

Observamos que um número composto $a \in \mathbb{N}$ pode ser escrito na forma

$$a = b \cdot c, \quad \text{com} \quad 1 < b, c < a.$$

Neste caso, os números b e c são chamados **divisores próprios** de a.

Se a é um número composto e a divide o produto bc, então não necessariamente $a \mid b$ ou $a \mid c$. Por exemplo, $6 \mid 3 \cdot 4$, mas $6 \nmid 3$ e $6 \nmid 4$. O mesmo não ocorre se a é um número primo. De fato,

Nota-se que se p é primo, então para qualquer inteiro a,

$$mdc(a, p) = 1 \quad \text{ou} \quad mdc(a, p) = p.$$

Os números primos serão sempre indicados pelas letras p e q, a menos que seja mencionado o contrário.

Proposição 3.1.2 *Sejam a e b inteiros, e p um número primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Como p é primo, então $mdc(a, p) = 1$ ou $mdc(a, p) = p$. Assim, se $p \nmid a$, então $mdc(a, p) = 1$. Portanto, pelo corolário 2.3.10, segue que $p \mid b$. □

O resultado anterior pode ser estendido para um produto de n inteiros como veremos a seguir. Sua demonstração é facilmente desenvolvida usando indução sobre n.

Corolário 3.1.3 *Se p é primo e $p \mid a_1 a_2 \dots a_n$, então $p \mid a_i$ para algum $i = 1, \dots, n$. Em particular, se $p \mid q_1 q_2 \dots q_n$ e $q_1, q_2, \dots, q_n$ são primos, então $p = q_i$, para algum $i = 1, \dots, n$.*

Passemos agora ao Teorema Fundamental da Aritmética.

Teorema 3.1.4 (Teorema Fundamental da Aritmética - TFA) *Todo inteiro $a > 1$ ou é primo ou se escreve de maneira única (a menos da ordem dos fatores) como um produto de fatores primos.*

Demonstração: Há duas coisas a serem provadas: a primeira é a existência dos primos, e a segunda é a unicidade da fatoração.

(**Existência**) Tomemos o conjunto

$$M = \{a \in \mathbb{N} : a > 1 \ \text{ e } \ a \neq p_1 p_2 \dots p_n\}$$

para primos $p_1, p_2, \dots, p_n$. Se mostrarmos que $M = \emptyset$, então a existência dos números primos estará provada. Por absurdo, suponhamos que $M \neq \emptyset$. Logo, pelo PBO, M possui um menor elemento m. É claro que m não pode ser primo (por hipótese dos elementos do conjunto M) e, por isso, é composto. Assim, podemos escrevê-lo na forma

$$m = b \cdot c, \quad \text{com} \quad 1 < b, c < m.$$

Como $b < m$ e $c < m$, segue que $b \notin M$ e $c \notin M$, pois $m = \min M$. Assim, sendo $b > 1$ e $c > 1$, estes números são primos ou são produtos de primos. Logo, $m = b \cdot c$ é um produto de primos, o que é uma contradição. Desse modo, $M = \emptyset$.

(**Unicidade**) Suponhamos que

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \tag{3.1}$$

sendo $p_1, \dots, p_n, q_1, \dots, q_m$ todos primos. Daí,

$$p_1 \mid q_1 q_2 \dots q_m$$

e, pelo Corolário 3.1.3, $p_1 = q_j$ para algum $j = 1, \dots, m$. Sem perda de generalidade, digamos que $p_1 = q_1$. Pela lei do cancelamento, segue de (3.1) que

$$p_2 \dots p_n = q_2 \dots q_m.$$

Da mesma forma, temos $p_2 = q_j$ para algum $j = 2, \dots, m$. Assumindo que $p_2 = q_2$, obtemos

$$p_3 \dots p_n = q_3 \dots q_m.$$

Continuando com este processo, e assumindo que $n > m$, temos

$$1 = p_{m+1} \dots p_n,$$

o que é impossível. Similarmente, se $n < m$, então

$$1 = q_{n+1} \dots q_m,$$

o que também é uma impossibilidade. Portanto, $m = n$ e $q_i = p_i$ para cada $i = 1, \dots, n$. □

Os primos que surgem na fatoração de um dado inteiro $a > 1$ não são, necessariamente, distintos. Por exemplo, $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 = 2^2 \cdot 3 \cdot 5^2$. Por isso, agrupando os primos que, porventura, repetem-se na fatoração de a, podemos enunciar o Teorema 3.1.4 da seguinte forma:

Corolário 3.1.5 *Todo número natural $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}, \tag{3.2}$$

em que $p_1, p_2, \dots, p_k$ são primos distintos e $r_1, r_2, \dots, r_k$ são números naturais.

A representação de um inteiro $a > 1$ dada em (3.2) é a sua **fatoração** ou **decomposição canônica** em fatores primos.

Verifica-se que se $a = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$ é a fatoração canônica de a, então a é um quadrado perfeito se, e somente se, cada expoente r_i é par.

Exemplo 3.1.6 Mostrar que $\sqrt{2}$ é irracional.

Solução: Por absurdo, suponhamos que $\sqrt{2} \in \mathbb{Q}$. Dessa forma, $\sqrt{2} = a/b$, com a e b primos entre si. Elevando ao quadrado ambos os lados desta igualdade, obtemos

$$2 \cdot b^2 = a^2. \tag{3.3}$$

Como $a > 1$ e $b > 1$, os inteiros a^2 e b^2 têm em suas fatorações sempre um número par de primos (incluindo repetições). Assim, o lado esquerdo de (3.3) tem um número ímpar de primos, enquanto seu lado direito tem um número par de primos. Isso contradiz o TFA. Portanto, $\sqrt{2} \notin \mathbb{Q}$. △

Podemos resolver o exemplo anterior da seguinte forma: se $\sqrt{2} = a/b$, com $mdc(a,b) = 1$, então $2b^2 = a^2$, o que nos mostra que 2 divide a^2. Sendo 2 primo, segue da Proposição 3.1.2 que 2 divide a, ou seja, $a = 2k$. Substituindo este valor em $2b^2 = a^2$, obtemos que $b^2 = 2k^2$, ou seja, 2 também divide b. Por isso, $mdc(a,b) \neq 1$, o que é uma contradição.

Teorema 3.1.7 *Se $a = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n}$ é a fatoração canônica de $a > 1$, então um inteiro d é um divisor positivo de a se, e somente se,*

$$d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

em que $0 \leq s_i \leq r_i$ para cada $i = 1, \dots, n$.

Exemplo 3.1.8 De acordo com o teorema anterior, os divisores positivos de $a = 60 = 2^2 \cdot 3 \cdot 5$ são:

$$\begin{aligned}
&d_1 = 2^0 \cdot 3^0 \cdot 5^0 = 1, \quad && d_2 = 2^1 \cdot 3^0 \cdot 5^0 = 2, \quad && d_3 = 2^2 \cdot 3^0 \cdot 5^0 = 4,\\
&d_4 = 2^0 \cdot 3^1 \cdot 5^0 = 3, \quad && d_5 = 2^0 \cdot 3^0 \cdot 5^1 = 5, \quad && d_6 = 2^1 \cdot 3^1 \cdot 5^0 = 6,\\
&d_7 = 2^1 \cdot 3^0 \cdot 5^1 = 10, \quad && d_8 = 2^2 \cdot 3^1 \cdot 5^0 = 12, \quad && d_9 = 2^2 \cdot 3^0 \cdot 5^1 = 20\\
&d_{10} = 2^0 \cdot 3^1 \cdot 5^1 = 15, \quad && d_{11} = 2^1 \cdot 3^1 \cdot 5^1 = 30, \quad && d_{12} = 2^2 \cdot 3^1 \cdot 5^1 = 60.
\end{aligned}$$

Temos assim um total de $(2+1) \cdot (1+1) \cdot (1+1) = 12$ divisores. Mais adiante, veremos como se calcular de forma eficiente o número de divisores de um dado inteiro, desde que seja dada a sua fatoração canônica. △

Às vezes, quando um dado primo p_k não surge com expoente maior do que zero na fatoração de $a \in \mathbb{N}$, é conveniente escrever a na forma

$$a = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} p_k^0.$$

Isto nos permite concluir o seguinte: dados $a, b \in \mathbb{N}$, com $a > 1$ e $b > 1$, sempre é possível escrevê-los como

$$a = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} \quad \text{e} \quad b = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

sendo $p_1, \ldots, p_n$ primos distintos e $r_i, s_i \in \mathbb{N} \cup \{0\}$.

Por exemplo, para $a = 100 = 2^2 \cdot 5$ e $b = 42 = 2 \cdot 3 \cdot 7$, temos

$$a = 2^2 \cdot 3^0 \cdot 5 \cdot 7^0 \quad \text{e} \quad b = 2 \cdot 3 \cdot 5^0 \cdot 7.$$

Estas considerações nos são úteis para provar o resultado que segue. Cujos prova pode ser observada em [8].

Teorema 3.1.9 *Sejam* $a = p_1^{r_1} p_2^{r_2} \ldots p_n^{r_n}$ *e* $b = p_1^{s_1} p_2^{s_2} \ldots p_n^{s_n}$, *sendo* $p_1, \ldots, p_n$ *primos distintos e* $r_i, s_i \in \mathbb{N} \cup \{0\}$. *Então,*

$$mdc(a,b) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}, \quad com \quad \alpha_i = \min\{r_i, s_i\}, \quad 1 \leq i \leq n$$

e

$$mmc(a,b) = p_1^{\beta_1} p_2^{\beta_2} \ldots p_n^{\beta_n}, \quad com \quad \beta_i = \max\{r_i, s_i\}, \quad 1 \leq i \leq n,$$

em que $\min\{r_i, s_i\}$ *e* $\max\{r_i, s_i\}$ *indicam o mínimo e o máximo entre* r_i *e* s_i, *respectivamente.*

Exemplo 3.1.10 Sendo $a = 2^3 \cdot 3^2 \cdot 5 \cdot 7^0 \cdot 11^0 = 360$ e $b = 2^2 \cdot 3^3 \cdot 7^2 \cdot 11^2 = 640332$, temos

$$\begin{aligned} mdc(a,b) &= 2^2 \cdot 3^2 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 36, \\ mmc(a,b) &= 2^3 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 6403320. \end{aligned}$$

△

Exemplo 3.1.11 Determinar inteiros positivos a e b tais que $mdc(a,b) = 20$ e $mmc(a,b) = 480$.

Solução: Sejam $d = mdc(a,b) = 20$ e $m = mmc(a,b)$, é claro que $a = d = 20$ e $b = m = 480$ são tais que

$$mdc(a,b) = 20 \quad \text{e} \quad mmc(a,b) = 480.$$

Vamos determinar outros pares de inteiros, caso existam. Façamos $d = 20 = 2^2 \cdot 3^0 \cdot 5$ e $m = 480 = 2^5 \cdot 3 \cdot 5$. De acordo com o Teorema 3.1.9, os inteiros a e b satisfazendo as condições $mdc(a,b) = 2$ e $mmc(a,b) = 480$ se, e somente se,

$$a = 2^{r_1} \cdot 3^{r_2} \cdot 5^{r_3} \quad \text{e} \quad b = 2^{s_1} \cdot 3^{s_2} \cdot 5^{s_3},$$

em que

$$2 = \min\{r_1, s_1\}, \quad 0 = \min\{r_2, s_2\}, \quad 1 = \min\{r_3, s_3\}.$$

Logo,

$$\begin{aligned} r_1 \leq s_1 \quad &\Rightarrow \quad \min\{r_1, s_1\} = r_1 = 2, \\ s_1 \leq r_1 \quad &\Rightarrow \quad \min\{r_1, s_1\} = s_1 = 2. \end{aligned}$$

Da mesma forma, temos $r_2 = 0$ ou $s_2 = 0$, e $r_3 = 1$ ou $s_3 = 1$. Por outro lado,

$$5 = \max\{r_1, s_1\}, \quad 1 = \max\{r_2, s_2\}, \quad 1 = \max\{r_3, s_3\}.$$

Daí,

$$r_1 = 2 \Leftrightarrow s_1 = 5, \qquad r_2 = 0 \Leftrightarrow s_2 = 1$$

e $r_3 = s_3 = 1$. Na tabela abaixo, temos as possíveis combinações dos valores de r_i e s_i com os valores correspondentes de a e b.

Valores dos r_i's	Valores dos s_i's	Valores de a e b
$r_1 = 2,\ r_2 = 0,\ r_3 = 1$	$s_1 = 5, s_2 = 1, s_3 = 1$	$a = 20$ e $b = 480$
$r_1 = 2,\ r_2 = 1,\ r_3 = 1$	$s_1 = 5, s_2 = 0, s_3 = 1$	$a = 60$ e $b = 160$
$r_1 = 5,\ r_2 = 1,\ r_3 = 1$	$s_1 = 2, s_2 = 0, s_3 = 1$	$a = 480$ e $b = 20$
$r_1 = 5,\ r_2 = 0,\ r_3 = 1$	$s_1 = 2, s_2 = 1, s_3 = 1$	$a = 160$ e $b = 60$

Portanto, os inteiros positivos são $a = 20$ e $b = 480$, $a = 60$ e $b = 160$. △

É importante chamar a atenção para o seguinte: para se fazer uso do Teorema 3.1.9 de modo a calcular o mdc e o mmc entre dois inteiros, é necessário determinar a fatoração canônica de cada um deles. A dificuldade consiste exatamente nisso, pois fatorar um dado número como produto de potências de primos é, em geral, uma tarefa árdua. Nesta direção, o Algoritmo de Euclides é a forma mais eficaz.

3.2 O Crivo de Eratóstenes

De acordo com o Teorema Fundamental da Aritmética, os números primos são os principais números inteiros. Por isso uma questão central na Teoria dos Números é decidir quando um inteiro $a > 1$ é primo ou não. Gauss disse:

"*O problema de distinguir os números primos dos números compostos é de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e dos mais úteis em Aritmética.... A própria dignidade da ciência requer que todos os meios possíveis sejam explorados para a resolução de um problema tão elegante e tão famoso.*"

No Ensino Básico, um teste de primalidade costuma ser feito por meio de tentativas, através de divisões do número a ser verificado pela sequência crescente de primos positivos, isto é,

$$2, 3, 5, 7, \ldots,$$

e caso nenhuma divisão seja exata e o quociente obtido seja menor ou igual ao divisor primo, o processo cessa e garantimos que o número é primo. Caso alguma divisão seja exata, o número é composto.

Mas para fazer essa identificação, podemos usar um dos mais antigos método, o Crivo de Eratóstenes[1]. Esse método permite determinar todos os números primos existentes até um determinado número inteiro.

Teorema 3.2.1 *Se n um inteiro positivo composto, então n possui, necessariamente, um fator primo p, tal que $p \leq \sqrt{n}$. Ou seja, se n não possui divisores diferentes de* 1, *menores ou iguais a $\sqrt{n}$, então n é primo.*

Demonstração: Sendo n um inteiro composto, então

$$n = a \cdot b, \quad \text{com} \quad 1 < a, b < n.$$

Se $a > \sqrt{n}$ e $b > \sqrt{n}$, então

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n,$$

o que é impossível. Portanto, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, digamos que $1 < a \leq \sqrt{n}$. Pelo Teorema 3.1.4, existe um primo p tal que $p \mid a$, com $(p \leq a \leq \sqrt{n})$. Daí $p \mid a \cdot b$ e, por conseguinte, $p \mid n$. □

Dessa forma, o teorema anterior mostra que para verificar se um dado inteiro $n > 1$ é primo, é suficiente verificar sua divisibilidade pelos primos $p \leq \sqrt{n}$. No entanto, esse teste torna-se inviável na prática quando consideramos valores de n relativamente grandes. Do ponto de vista computacional, ainda não existe um algoritmo eficaz para testar a primalidade de um dado inteiro.

Exemplo 3.2.2 Para o número $n = 101$, temos que $\sqrt{101} \leq 11$ e os primos menores ou iguais a 10 são $2, 3, 5, 7$ e 11. Como nenhum destes primos divide 101, concluímos que $n = 101$ é primo. △

Resumidamente, o método de Eratóstenes fundamenta-se em construir uma tabela e excluir todos os números compostos menores que um dado número inteiro $n > 1$, de forma sistemática. Assim, deve-se:

(1) Escrever todos os números inteiros entre 2 e n.

(2) Para todo primo $p \leq n$, risca-se todos os múltiplos de p maiores do que p.

(3) Os números restantes são todos os primos menores que n.

Observação 3.2.3 O Teorema 3.2.1 diminui o número de verificações dos múltiplos de primos no passo (2) do algoritmo descrito acima.

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

Tabela 3.1: Crivo de Eratóstenes - Números Primos entre 2 e 50.

Vejamos, por exemplo, como determinar todos os primos menores que 50, utilizando o Crivo de Eratóstenes. Inicialmente, escrevemos todos os números inteiros entre 2 e 50. Em seguida excluímos todos os múltiplos de 2, 3, 5 e 7 pois estes são os primos menores ou iguais a $\sqrt{50} \geq 7$. Como mostra a Tabela 3.1.

Logo, os primos entre 2 e 50 são todos aqueles que não foram descartados pelo processo realizado, ou seja,

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47.$$

Destacaremos agora um resultado muito significativo sobre os números primos. Euclides (cerca de 300 a.C.) provou a infinidade dos números primos, em seu livro *Os Elementos.* De acordo com relatos históricos, sua demonstração foi a primeira a ser estabelecida utilizando o método de redução ao absurdo.

Teorema 3.2.4 (Euclides) *O conjunto $\mathscr{P}$ dos números primos é infinito.*

Demonstração: Suponhamos por absurdo que $\mathscr{P}$ é um conjunto finito, e sejam $p_1, p_2, \ldots, p_n$ todos os primos. Consideremos $a \in \mathbb{N}$ dado pelo produto dos p_i's somado ao número 1, isto é,

$$a = p_1 p_2 \cdots p_n + 1.$$

Como $a > 1$, segue do TFA que existe um primo p que divide a. Sendo $p_1, p_2, \ldots, p_n$ os únicos primos, então $p = p_i$ para algum $i = 1, \ldots, n$, digamos que $p = p_1$. Segue da hipótese que $p \mid (pp_2 \cdots p_n + 1) = a$. É claro que $p \mid (pp_2 \cdots p_n)$, assim temos que $p \mid 1$, que é uma contradição. Logo, $\mathscr{P}$ é infinito. □

[1]Devido ao matemático grego Eratóstenes, que viveu por volta de 230 a.C.

Capítulo 4

Congruências e Equações Diofantinas Lineares

O conceito de congruência e sua notação que usamos atualmente foi introduzido por Gauss, quando tinha apenas 24 anos de idade, por meio da obra *Disquisitiones Arithmeticae* (Investigações Aritméticas) em 1801.

A Teoria das Congruências ou Aritmética dos Restos, ocupa um lugar de destaque na Teoria dos Números. Suas propriedades são fortes ferramentas para se estudar divisibilidade sobre $\mathbb{Z}$ com mais profundidade.

Apresentaremos os resultados básicos sobre congruências e equações diofantinas lineares. Algumas aplicações mais substanciais serão abordadas no capítulo seguinte, onde trataremos de alguns problemas práticos.

4.1 Propriedades Básicas das Congruências

Sejam m um número natural e a e b inteiros quaisquer. Dizemos que a é **congruente** a b **módulo** m, em símbolos

$$a \equiv b \pmod{m},$$

quando m divide $a-b$. O número m é chamado o **módulo** da congruência.

Exemplo 4.1.1 Temos que

$$4 \equiv 1 \pmod{3}, \quad 16 \equiv -4 \pmod{5}, \quad -7 \equiv 5 \pmod{2},$$

pois, $3 \mid (4-1)$, $5 \mid (16+4)$ e $2 \mid (-7-5)$. △

Se m não dividir $a-b$, então diremos que a **não é congruente** a b **módulo** m ou que a é **incongruente** a b **módulo** m. Neste caso, escreveremos

$$a \not\equiv b \pmod{m}.$$

Assim, $5 \not\equiv 1 \pmod 3$ e $8 \not\equiv 24 \pmod 5$, já que $3 \nmid (5-1)$ e $5 \nmid (8-24)$.

Gauss usou o símbolo " $\equiv$ " para indicar a congruência devido à analogia com a igualdade algébrica. Nota-se que $a \equiv b \pmod m$ significa afirmar que existe um inteiro k tal que

$$a = b + km.$$

Na definição anterior, é possível considerar o módulo $m < 0$ ou $m = 0$. Mas, atentemos para o seguinte: para quaisquer inteiros a e b, $a \equiv b \pmod m$ se, e somente se, $a \equiv b \pmod{(-m)}$, pois

$$a = b + km \;\Leftrightarrow\; a = b + (-k)(-m).$$

Também, $a \equiv b \pmod 0$ se, e somente se, 0 divide $a - b$, ou seja, se, e somente se, $a = b$, visto que 0 divide apenas ele próprio. Por outro lado, para $m = 1$, temos que $a \equiv b \pmod 1$ sempre se verifica, pois 1 divide qualquer inteiro. É em decorrência disto que se costuma desconsiderar estes casos, e é o que faremos, isto é, na congruência $a \equiv b \pmod m$, m indicará sempre um inteiro maior ou igual a 2.

Chamamos a atenção do leitor para não confundir o uso de "mod" na congruência $a \equiv b \pmod m$ com o uso em $r = a \bmod m$. Apesar de os dois casos terem certa relação, eles têm significados diferentes. O primeiro significa que m divide $a - b$, e no segundo, temos que r é o resto da divisão de a por m, ou seja, $a = mq + r$, com $0 \leq r < m$. Por exemplo, $12 \equiv 39 \pmod 9$, mas não é verdade que $12 = 39 \bmod 9$. No entanto, se $a \equiv b \pmod m$ e $0 \leq b < m$, então $b = a \bmod m$.

Outra forma de caracterizar a noção de congruência em termos de restos sobre a divisão por m é dada pela seguinte:

Proposição 4.1.2 *Dados a e b inteiros, temos que* $a \equiv b \pmod m$ *se, e somente se, a e b têm o mesmo resto quando divididos por m.*

Demonstração: Se $a \equiv b \pmod m$, então $a = b + km$, com $k \in \mathbb{Z}$. Pelo Algoritmo da Divisão,

$$b = qm + r, \quad \text{com} \quad 0 \leq r < m.$$

Assim,

$$a = b + km = qm + r + km = (q + k)m + r,$$

ou seja, r também é o resto da divisão de a por m.
Reciprocamente, suponhamos que

$$a = q_1 m + r \quad \text{e} \quad b = q_2 m + r,$$

em que $0 \leq r < m$. Logo,

$$a - b = (q_1 - q_2)m,$$

de modo que $m \mid a - b$, isto é, $a \equiv b \pmod m$. □

Por exemplo, como $15 \equiv -9 \pmod{4}$, então 15 e -9 têm o mesmo resto quando divididos por 4. Observa-se que

$$15 = 4 \cdot 3 + 3 \quad \text{e} \quad -9 = 4 \cdot (-3) + 3.$$

Exemplo 4.1.3 (O calendário: congruência módulo 7) Consideremos o mês de outubro do ano de 2017, cujos dias estão descritos abaixo:

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	18	20	21
22	23	24	25	26	27	28
29	30	31				

Em cada uma das colunas referentes aos dias da semana, encontram-se números naturais que são congruentes entre si módulo 7. No domingo, os inteiros congruentes a 1 módulo 7; na segunda os inteiros congruentes a 2 módulo 7, e assim por diante. Agora, vamos supor que não dispomos de um calendário em si, mas apenas do primeiro número de cada coluna e seu respectivo dia, e determinemos o dia da semana que corresponde o dia 26 de outubro de 2017. Para isto, basta determinarmos o inteiro r, com $8 \leq r \leq 31$, congruente a 26 módulo 7. Ora, como

$$26 = 7 \cdot 3 + 5,$$

ou seja, $26 \equiv 5 = r \pmod{7}$, e 5 corresponde a quinta-feira, concluímos que o dia 26 de outubro de 2017 também refere-se a uma quinta-feira. $\triangle$

O conceito de congruência módulo m estabelece uma relação sobre o conjunto dos números inteiros, a *relação de congruência módulo m*, que indicaremos por

$$\equiv \pmod{m} \quad \text{ou} \quad \equiv_m .$$

Essa relação tem muitas propriedades em comum com a relação de igualdade entre inteiros. De início, temos:

Proposição 4.1.4 *Dados a, b e c inteiros quaisquer, temos que as seguintes propriedades são satisfeitas:*

(1) ($\equiv_m$ **é reflexiva**) $a \equiv a \pmod{m}$.

(2) ($\equiv_m$ **é simétrica**) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$.

(3) ($\equiv_m$ **é transitiva**) $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$.

Demonstração: (1) Para qualquer inteiro a, segue que $a-a=0=0\cdot m$, ou seja, $a\equiv a\ (\mathrm{mod}\, m)$.

(2) Se $a\equiv b\ (\mathrm{mod}\, m)$, então $a-b=mk$, com $k\in\mathbb{Z}$. Logo, $b-a=m(-k)$ e $-k\in\mathbb{Z}$, isto é, $b\equiv a\ (\mathrm{mod}\, m)$.

(3) Assumindo que $a\equiv b\ (\mathrm{mod}\, m)$ e $b\equiv c\ (\mathrm{mod}\, m)$, existem $k_1,k_2\in\mathbb{Z}$ tais que

$$a-b=mk_1 \quad \text{e} \quad b-c=mk_2.$$

Somando membro a membro estas duas igualdades, obtemos $a-c=mk_3$, com $k_3=k_1+k_2\in\mathbb{Z}$, ou seja, $a\equiv c\ (\mathrm{mod}\, m)$. □

Os resultados da proposição anterior nos mostram que " $\equiv_m$ " é uma relação de equivalência sobre $\mathbb{Z}$, (cf. [9]) algo que é extremamente importante. Este fato tem uma estreita relação com o conjunto finito $\mathbb{Z}_m$, que é na realidade o conjunto quociente de $\mathbb{Z}$ pela relação " $\equiv_m$ ". Por meio do Algoritmo da Divisão, mostra-se que $\mathbb{Z}_m$ tem exatamente m classes de equivalência, chamadas classes de equivalência módulo m. Especificamente,

$$\mathbb{Z}_m=\{\overline{0},\ \overline{1},\ldots,\overline{m-1}\}.$$

Este conjunto dotado com as operações de adição e multiplicação usuais, isto é,

$$\overline{a}\oplus\overline{b}=\overline{a+b} \quad \text{e} \quad \overline{a}\odot\overline{b}=\overline{a\cdot b},\ \text{com}\ a.b\in\mathbb{Z}.$$

torna-se uma das principais estruturas algébricas (cf. [9]).

Ademais, é bastante significante o fato de a relação de congruência módulo m ser compatível com as operações de adição e multiplicação de inteiros, no seguinte sentido:

Teorema 4.1.5 *Dados a, b, c e d inteiros quaisquer, temos que as seguintes propriedades são satisfeitas:*

(1) *Se $a\equiv b\ (\mathrm{mod}\, m)$ e $c\equiv d\ (\mathrm{mod}\, m)$, então*

$$(a+c)\equiv(b+d)\ (\mathrm{mod}\, m) \quad e \quad ac\equiv bd\ (\mathrm{mod}\, m).$$

(2) *Se $a\equiv b\ (\mathrm{mod}\, m)$, então*

$$(a+c)\equiv(b+c)\ (\mathrm{mod}\, m) \quad e \quad ac\equiv bc\ (\mathrm{mod}\, m).$$

(3) *Se $a\equiv b\ (\mathrm{mod}\, m)$, então $a^k\equiv b^k\ (\mathrm{mod}\, m)$ para qualquer $k\in\mathbb{N}$.*

(4) *Se $(a+c)\equiv(b+c)\ (\mathrm{mod}\, m)$, então $a\equiv b\ (\mathrm{mod}\, m)$.*

Demonstração: (1) Sendo $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, temos

$$a = b + k_1 m \quad \text{e} \quad c = d + k_2 m.$$

Somando membro a membro estas duas igualdades, obtemos que

$$a + c = b + d + (k_1 + k_2)m,$$

isto é, $(a+c) \equiv (b+d) \pmod{m}$. Agora, multiplicando membro a membro as mesmas igualdades,

$$ac = (b + k_1 m)(d + k_2 m) = bd + k_3 m,$$

em que $k_3 = bk_2 + dk_1 + k_1 k_2 m$. Portanto, $ac \equiv bd \pmod{m}$.

(2) Se $a \equiv b \pmod{m}$, então como $c \equiv c \pmod{m}$, segue do item (1) que

$$(a+c) \equiv (b+c) \pmod{m} \quad \text{e} \quad ac \equiv bc \pmod{m}.$$

(3) Vamos provar por indução que $a^k \equiv b^k \pmod{m}$ para todo inteiro $k \geq 1$. Já que por hipótese, $a \equiv b \pmod{m}$, o resultado é válido para $k = 1$. Suponhamos por hipótese de indução que $a^k \equiv b^k \pmod{m}$ para $k \geq 1$. Como $a \equiv b \pmod{m}$, então multiplicando membro a membro estas duas congruências, segue do item (1) que $a^{k+1} \equiv b^{k+1} \pmod{m}$. Portanto, pelo Principio de Indução Finita $a^k \equiv b^k \pmod{m}$ para todo $k \geq 1$.

(4) Por hipótese, $(a+c) \equiv (b+c) \pmod{m}$. Somando membro a membro esta congruência com $-c \equiv -c \pmod{m}$, obtemos do item (1) que $a \equiv b \pmod{m}$. □

A congruência pode ser vista como uma forma generalizada da igualdade, no sentido dos resultados do teorema anterior. Ou seja, com relação à adição e à multiplicação, a congruência nos faz lembrar da forma com que obtemos $a+c = b+d$, $a+c = b+c$ e $ac = bd$, desde que $a = b$ e $c = d$.

Exemplos

Antes de descrevermos mais propriedades, vamos apresentar alguns exemplos que nos dão uma ideia de como as propriedades da congruência auxiliam na efetivação de certos tipos de cálculos.

Exemplo 4.1.6 Mostrar que $10^k \equiv 1 \pmod{11}$ ou $10^k \equiv -1 \pmod{11}$, conforme $k \in \mathbb{N}$ é par ou ímpar, respectivamente.

Solução: Como $10 \equiv -1 \pmod{11}$, então $10^k \equiv (-1)^k \pmod{11}$ para todo $k \in \mathbb{N}$. Por outro lado, visto que

$$(-1)^k = \begin{cases} 1 & \text{se } k \text{ é par,} \\ -1 & \text{se } k \text{ é ímpar,} \end{cases}$$

temos o resultado. △

Exemplo 4.1.7 Determinar o dígito das unidades de 2^{70} escrito na base 15.

Solução: O problema é equivalente a determinar um inteiro r tal que

$$2^{70} \equiv r \pmod{15},$$

com $0 \leq r \leq 14$. É claro que não é conveniente desenvolver a potência 2^{70} e, após isso, dividir o resultado por 15. Este de fato não é o melhor caminho. Ao contrário disso, é apropriado encontrar uma congruência base ou inicial de modo que, a partir dela, possamos usar as propriedades necessárias da congruência, chegando ao resultado desejado. Um bom ponto de partida é a congruência

$$2^4 \equiv 1 \pmod{15}.$$

Elevando ambos os membros desta congruência a 17 (o quociente da divisão de 70 por 4), segue do item (3) do Teorema 4.1.5 que

$$(2^4)^{17} \equiv 1^{17} \pmod{15} \;\Rightarrow\; 2^{68} \equiv 1 \pmod{15}.$$

Agora, usando o item (2) do mesmo teorema e multiplicando os membros da última congruência por $c = 4 = 2^2$, obtemos que $2^{70} \equiv 4 \pmod{15}$. Assim, o dígito das unidades é $r = 4$. △

As congruências iniciais ideais para resolver um problema análogo ao anterior são congruências da forma

$$a^k \equiv 1 \pmod{m} \quad \text{ou} \quad a^k \equiv -1 \pmod{m},$$

em que k é um inteiro positivo, pois $1^n = 1$ e $(-1)^n = \pm 1$ para $n \in \mathbb{N}$. Ocorre que às vezes isso não é possível ou não é fácil de se obter sem o uso de resultados especiais tais como o Pequeno Teorema de Fermat e o Teorema de Euler, que serão considerados mais adiante. Neste caso, devemos lançar mão de outras congruências, conforme faremos no exemplo que segue.

Exemplo 4.1.8 Calcular o dígito das unidades do número 9^{9^9} escrito na base 11.

Solução: O dígito das unidades de 9^{9^9} é o resto r da divisão de 9^{9^9} por 11. Sob a congruência módulo 11, temos

$$9 \equiv 9, \quad 9^2 \equiv 4, \quad 9^3 \equiv 3, \quad 9^4 \equiv 5, \quad 9^5 \equiv 1$$

e, a partir desta última congruência, os resultados se repetem ciclicamente módulo 5. Este fato nos permite calcular com facilidades o resto r. Senão vejamos. Considerando agora a congruência módulo 5, temos $9^2 \equiv 1 \pmod{5}$ e, por isso, $9^9 \equiv 4 \pmod{5}$. Assim, $9^9 = 4 + 5k$ para algum $k \in \mathbb{N}$. Logo, $9^{9^9} = 9^{4+5k}$, e como $9^5 \equiv 1 \pmod{11}$, segue sob a congruência módulo 11 que

$$9^{9^9} = 9^{4+5k} = 9^4 \cdot 9^{5k} \equiv 9^4 \equiv 5 \pmod{11}.$$

Portanto, o resto r é igual a 5. △

Exemplo 4.1.9 Determinar a maior potência de 2 que divide $3^{50}-1$.

Solução: Temos que 2 divide $3^{50}-1$, pois 3 é ímpar e, assim, $3^{50}-1$ é par. Para cada inteiro positivo r, obtemos

$$2^r \mid 3^{50}-1 \;\Leftrightarrow\; 3^{50} \equiv 1 \pmod{2^r}.$$

Já sabemos que esta congruência é válida para $r=1$. Analisemos, a congruência acima para outros valores de r. Para $r=2$, temos $3^2 \equiv 1 \pmod 4$, de modo que $(3^2)^{25} \equiv 1 \pmod 4$, ou seja, $3^{50} \equiv 1 \pmod 4$. Temos também:

$$\begin{aligned} 3^2 \equiv 1 \pmod 8 &\;\Rightarrow\; 3^{50} \equiv 1 \pmod 8, \\ 3^4 \equiv 1 \pmod{16} &\;\Rightarrow\; 3^{50} \equiv 9 \pmod{16}. \end{aligned}$$

Logo, 2^4 não divide $3^{50}-1$. Portanto, a maior potência de 2 que divide $3^{50}-1$ é 2^3. △

Outra forma de resolver o exemplo anterior é fatorando $3^{50}-1$ com base na seguinte identidade:

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

Em particular,

$$3^{50}-1 = (3^2)^{25}-1 = (3^2-1)(3^{2\cdot 24}+3^{2\cdot 23}+3^{2\cdot 22}+\cdots+3^{2\cdot 1}+1).$$

Notemos que na soma $3^{2\cdot 24}+3^{2\cdot 23}+3^{2\cdot 22}+\cdots+3^{2\cdot 1}+1$ existem 25 parcelas. Como todas elas são ímpares, segue que esta soma é ímpar e, por isso, não é divisível por 2. Por fim, como $3^2-1=2^3$, concluímos que a maior potência de 2 que divide $3^{50}-1$ é 2^3.

Lei do Cancelamento

É importante ressaltar que, em geral, a lei do cancelamento não é válida para congruência, isto é, se $ac \equiv bc \pmod m$, então não necessariamente se tem $a \equiv b \pmod m$. Por exemplo,

$$4\cdot 8 \equiv 4\cdot 5 \pmod 6$$

e, no entanto, $8 \not\equiv 5 \pmod 6$.

Essa lei tem consequências importantes, conforme poderemos comprovar ao longo do texto, e só se verifica sob certa condição.

Teorema 4.1.10 *Sejam a, b e c inteiros quaisquer. Então,*

$$ac \equiv bc \pmod m \;\Leftrightarrow\; a \equiv b \pmod{m/d},$$

em que $d = mdc(c,m)$.

Demonstração: Se $ac \equiv bc \pmod{m}$, então

$$ac - bc = c(a-b) = km, \quad \text{com} \quad k \in \mathbb{Z}. \tag{4.1}$$

Sendo $d = mdc(c,m)$, $m = dr$ e $c = ds$, em que r e s são primos entre si, pois $mdc(r,s) = mdc(m/d, c/d) = 1$. Substituindo os valores de m e c em (4.1), obtemos

$$ds(a-b) = kdr \;\Rightarrow\; s(a-b) = kr \;\Rightarrow\; r \mid s(a-b),$$

de modo que $r \mid (a-b)$, pois $mdc(r,s) = 1$. Logo, $a \equiv b \pmod{r}$, ou melhor, $a \equiv b \pmod{m/d}$.

Reciprocamente, sejam $c = d\lambda_1$ e $m = d\lambda_2$. Como $a \equiv b \pmod{m/d}$, isto é, $a \equiv b \pmod{\lambda_2}$, temos $a - b = k\lambda_2$, com $k \in \mathbb{Z}$. Portanto,

$$c(a-b) = (d\lambda_1) \cdot (k\lambda_2) = mk\lambda_1,$$

ou seja, $ac \equiv bc \pmod{m}$. □

Corolário 4.1.11 (Lei do Cancelamento) *Consideremos $ac \equiv bc \pmod{m}$. Se $mdc(c,m) = 1$, então $a \equiv b \pmod{m}$.*

Demonstração: Se $ac \equiv bc \pmod{m}$, com $d = mdc(c,m) = 1$, então pelo teorema anterior, $a \equiv b \pmod{m/d}$, isto é, $a \equiv b \pmod{m}$. □

Exemplo 4.1.12 Como $5 \cdot 102 \equiv 5 \cdot 14 \pmod{8}$ e $mdc(5,8) = 1$, segue do corolário anterior que $102 \equiv 14 \pmod{8}$. △

Exemplo 4.1.13 Determinar todos os inteiros x tais que $5(x^2 - 3) \equiv 20 \pmod{9}$.

Solução: Temos que

$$5(x^2-3) \equiv 20 \pmod{9} \;\Leftrightarrow\; 5(x^2-3) \equiv 5 \cdot 4 \pmod{9}.$$

Já que $mdc(5,9) = 1$, então pela Lei do Cancelamento, podemos cancelar o fator 5 da última congruência. Fazendo isto, obtemos $x^2 - 3 \equiv 4 \pmod{9}$, ou melhor,

$$x^2 \equiv 7 \pmod{9}.$$

Por outro lado, sabemos que o conjunto $\{0,1,2,\ldots,8\}$ é um sistema completo de resíduos módulo 9. Por isso, vamos analisar módulo 9 os quadrados dos inteiros x deste conjunto. Temos

x	0	1	2	3	4	5	6	7	8
$x^2 \bmod 9$	0	1	4	0	7	7	0	4	1

Logo, $x_1 = 4$ e $x_2 = 5$ são soluções da equação. Disto segue que a solução geral da equação é $x = 4 + 9k$ ou $x = 5 + 9k$, com $k \in \mathbb{Z}$. △

4.2 Os Teoremas de Fermat e Euler

Os teoremas de Fermat e de Euler fornecem duas importantes congruências básicas da forma $a^k \equiv 1 \pmod{m}$, sendo k um número natural. Uma congruência deste tipo implica certas facilidades na aritmética modular. Algumas aplicações relativas a esses teoremas serão apresentadas no Capítulo 5.

O Teorema de Fermat

O Grande Teorema de Fermat, também chamado de *O Último Teorema de Fermat,* afirma que para qualquer número natural $n > 2$, não existem inteiros positivos x, y e z tais que

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

O teorema que iremos considerar nesta seção é o *Pequeno Teorema*, que tem uma demonstração relativamente fácil, tendo sido provado por Fermat em 1640. Esse resultado estabelece uma congruência base importante com aplicações relevantes em outros resultados da Teoria dos Números.

Teorema 4.2.1 (O Pequeno Teorema de Fermat) *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então,*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demonstração: Consideremos os primeiros $p-1$ múltiplos de a, ou seja,

$$a, 2a, 3a, \ldots, (p-1)a. \tag{4.2}$$

Observemos primeiramente que estes números são dois a dois incongruentes módulo p. De fato, se

$$ak_1 \equiv ak_2 \pmod{p},$$

com $1 \leq k_1 < k_2 \leq p-1$, então conforme o Corolário 4.1.11, podemos cancelar o fator a desta congruência, pois $mdc(a,p) = 1$. Fazendo isto, obtemos $k_1 \equiv k_2 \pmod{p}$, isto é, $p \mid (k_2 - k_1)$, o que é impossível. Além disso, se $1 \leq r \leq p-1$ e $p \mid ra$, então $p \mid a$ ou $p \mid r$, o que também não é possível, pois p é primo. Portanto, $ra \not\equiv 0 \pmod{p}$ para todo $r = 1, \ldots, p-1$.

De acordo com o Algoritmo da Divisão, cada inteiro k, com $p \nmid k$, é congruente módulo p a um, e somente um, número da sequência

$$1, 2, 3, \ldots, p-1. \tag{4.3}$$

Portanto, cada inteiro de (4.2) é equivalente a um número de (4.3) numa determinada ordem, digamos

$$\begin{aligned} a &\equiv b_1 \pmod{p}, \\ 2a &\equiv b_2 \pmod{p}, \\ &\vdots \\ (p-1)a &\equiv b_{p-1} \pmod{p}, \end{aligned}$$

em que $b_i \in \{1,2,\ldots,p-1\}$ para $i = 1,2,\ldots,p-1$. Multiplicando membro a membro estas congruências, temos que

$$a \cdot 2a \cdots (p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

isto é,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Como $mdc((p-1)!, p) = 1$, podemos cancelar $(p-1)!$ desta última congruência, de modo que

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

O resultado anterior implica que para um inteiro a qualquer, divisível por p ou não, $a^p \equiv a \pmod{p}$. Com efeito,

Corolário 4.2.2 *Se p é primo, então*

$$a^p \equiv a \pmod{p}$$

para qualquer inteiro a.

Demonstração: Se $p \nmid a$, então pelo teorema anterior, $a^{p-1} \equiv 1 \pmod{p}$. Assim, multiplicando esta congruência por a, segue que $a^p \equiv a \pmod{p}$. Se $p \mid a$, então $p \mid a^p$ e, por isso, $p \mid a^p - a$, ou seja, $a^p \equiv a \pmod{p}$. □

Teorema de Euler

Vamos agora apresentar o Teorema de Euler que é uma generalização do Teorema de Fermat, no sentido de considerar congruências módulo m, em que m pode ser primo ou não. Começaremos definindo a função ϕ de Euler, que é parte central desse teorema.

Definição 4.2.3 (Função ϕ de Euler) *Para cada inteiro $n \geq 1$, indiquemos por $\phi(n)$ o número de inteiros positivos menores ou iguais a n que são relativamente primos com n. A função ϕ assim definida é chamada **função ϕ de Euler**.*

Para cada $n \in \mathbb{N}$, considerando

$$A_n = \{m \in \mathbb{N} : 1 \leq m \leq n \text{ e } mdc(m,n) = 1\},$$

segue que

$$\phi(n) = car(A_n),$$

em que $car(A_n)$ indica a cardinalidade de A_n. Temos

$$\phi(1) = 1, \quad \phi(2) = 1, \quad \phi(3) = 2, \quad \phi(4) = 2, \quad \phi(5) = 4.$$

Para um inteiro um pouco maior, digamos $n = 20$, os inteiros positivos menores do que 20 e primos com 20 são 1, 3, 7, 9, 11, 13, 17, 19 e, por isso, $\phi(20) = 8$. Nota-se que $\phi(4) \cdot \phi(5) = 2 \cdot 4 = 8$, isto é,

$$\phi(20) = \phi(2^2 \cdot 5) = \phi(2^2) \cdot \phi(5).$$

Esta propriedade *multiplicativa* é válida para quaisquer m e n, com $mdc(m,n) = 1$. De início, temos que $\phi(n) \leq n - 1$ para $n > 1$, e

$$\phi(n) = n - 1 \quad \Leftrightarrow \quad n \text{ é primo.}$$

O que vamos estabelecer é uma fórmula que nos permitirá calcular $\phi(n)$ a partir da fatoração de n em potências de primos. Nesta direção, o resultado que segue é central.

Teorema 4.2.4 *Se p é primo e $k \geq 1$, então*

$$\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p).$$

Demonstração: Primeiramente, é claro que $mdc(n, p^k) = 1$ se, e somente se, $p \nmid n$. Agora, entre 1 e p^k existem p^{k-1} números que são divisíveis por p, que são

$$p, 2p, 3p, \ldots, (p^{k-1})p,$$

pois $p\lambda \leq p^k$ se, e somente se, $\lambda = 1, 2, \ldots, p^{k-1}$. Desse modo, o conjunto $\{1, 2, \ldots, p^k\}$ contém exatamente $p^k - p^{k-1}$ números que são relativamente primos com p^k. Daí, por definição, $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$. □

Por exemplo,

$$\phi(2^4) = 2^4 - 2^3 = 8, \quad \phi(3^3) = 3^3 - 3^2 = 18.$$

Lema 4.2.5 *Dados inteiros a, b e c, temos que*

$$mdc(a, bc) = 1 \quad \Leftrightarrow \quad mdc(a,b) = 1 \text{ e } mdc(a,c) = 1.$$

De uma forma geral, dados inteiros $a, a_1, a_2, \ldots, a_n$, temos que

$$mdc(a, a_1 a_2 \ldots a_n) = 1 \;\Leftrightarrow\; mdc(a, a_i) = 1 \tag{4.4}$$

para $i = 1, \ldots, n$. Diante disto, prova-se que a função ϕ é multiplicativa. A prova desse resultados não será apresentada aqui, pois ela é relativamente longa e um tanto quanto técnica. Ao leitor interessado em verificar com detalhes a prova deste resultado, sugerimos a referência [8].

Teorema 4.2.6 (A função ϕ é multiplicativa) *Se m e n são números naturais tais que $mdc(m,n) = 1$, então*

$$\phi(mn) = \phi(m)\phi(n).$$

De um modo geral, temos o seguinte resultado:

Corolário 4.2.7 *Se $m_1, m_2, \ldots, m_k$ são inteiros positivos primos aos pares, ou seja, $mdc(m_i, m_j) = 1$ se $i \neq j$, então*

$$\phi(m_1 m_2 \ldots m_k) = \phi(m_1)\phi(m_2)\ldots\phi(m_k).$$

Demonstração: Se $k = 2$, então pelo teorema anterior o resultado segue imediatamente. Por hipótese de indução, suponhamos que o resultado é válido para $k \geq 2$ e sejam $m_1, m_2, \ldots, m_k, m_{k+1}$ inteiros primos aos pares. Logo, por (4.4), temos $mdc(m_1 m_2 \ldots m_k, m_{k+1}) = 1$ e, assim,

$$\begin{aligned}
\phi(m_1 m_2 \ldots m_k m_{k+1}) &= \phi((m_1 m_2 \ldots m_k) m_{k+1}) \\
&= \phi(m_1 m_2 \ldots m_k)\phi(m_{k+1}) \\
&= \phi(m_1)\phi(m_2)\ldots\phi(m_k)\phi(m_{k+1}),
\end{aligned}$$

o que prova o resultado. □

Agora, já podemos provar o resultado que generaliza o Teorema 4.2.4.

Teorema 4.2.8 *Se $n > 1$ e $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$ é a fatoração canônica de n, então*

$$\begin{aligned}
\phi(n) &= \left(p_1^{k_1} - p_1^{k_1 - 1}\right)\left(p_2^{k_2} - p_2^{k_2 - 1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r - 1}\right) \\
&= n(1 - 1/p_1)(1 - 1/p_2)\cdots(1 - 1/p_r).
\end{aligned}$$

Demonstração: Já que ϕ é multiplicativa e $mdc(p_i^{k_i}, p_j^{k_j}) = 1$ para $i \neq j$, temos do Corolário 4.2.7 que

$$\phi(n) = \phi(p_1^{k_1})\phi(p_2^{k_2})\ldots\phi(p_r^{k_r}).$$

Pelo Teorema 4.2.4,

$$\phi(p_i^{k_i}) = p_i^{k_i} - p_i^{k_i - 1} = p_i^{k_i}(1 - 1/p_i)$$

para cada $i = 1, \ldots, r$. Portanto,

$$\begin{aligned}\phi(n) &= \left(p_1^{k_1} - p_1^{k_1-1}\right)\left(p_2^{k_2} - p_2^{k_2-1}\right)\cdots\left(p_r^{k_r} - p_r^{k_r-1}\right)\\ &= p_1^{k_1}p_2^{k_2}\ldots p_r^{k_r}(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r)\\ &= n(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r),\end{aligned}$$

o que completa a prova. □

Uma vez que $p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i-1}(p_i-1)$, a fórmula para $\phi(n)$ do teorema anterior pode ser reescrita como

$$\phi(n) = p_1^{k_1-1}\cdot p_2^{k_2-1}\ldots p_r^{k_r-1}(p_1-1)(p_2-1)\cdots(p_r-1). \tag{4.5}$$

Exemplo 4.2.9 Calcular $\phi(1008)$.

Solução: Como $1008 = 2^4\cdot 3^2\cdot 7$, temos

$$\begin{aligned}\phi(1008) = \phi(2^4\cdot 3^2\cdot 7) &= \phi(2^4)\phi(3^2)\phi(7)\\ &= (2^4-2^3)(3^2-3)(7-1)\\ &= 8\cdot 6\cdot 6\\ &= 288.\end{aligned}$$

Usando a igualdade $\phi(n) = n(1-1/p_1)(1-1/p_2)(1-1/p_3)$, com $n = 1008$, $p_1 = 2$, $p_2 = 3$ e $p_3 = 7$, segue que

$$\begin{aligned}\phi(1008) &= 1008\,(1-1/2)\,(1-1/3)\,(1-1/7)\\ &= 1008\,(1/2)\,(2/3)\,(6/7)\\ &= 288.\end{aligned}$$

△

Consideremos um caso particular. Para $m = 9$, o número de inteiros menores que 9 e que são primos com 9 é dado por $\phi(9)$. Sendo $\phi(9) = 6$, temos 6 inteiros satisfazendo está condição, que são:

$$a_1 = 1,\ a_2 = 2,\ a_3 = 4,\ a_4 = 5,\ a_5 = 7,\ a_6 = 8.$$

Assim, para $a = 5$, temos

$$\begin{aligned}&5\cdot 1 \equiv 5\ (\mathrm{mod}9),\quad 5\cdot 2 \equiv 1\ (\mathrm{mod}9),\\ &5\cdot 4 \equiv 2\ (\mathrm{mod}9),\quad 5\cdot 5 \equiv 7\ (\mathrm{mod}9),\\ &5\cdot 7 \equiv 8\ (\mathrm{mod}9),\quad 5\cdot 8 \equiv 4\ (\mathrm{mod}9).\end{aligned}$$

Multiplicando membro a membro estas seis congruências, obtemos que

$$5^6(1\cdot 2\cdot 4\cdot 5\cdot 7\cdot 8) \equiv (1\cdot 2\cdot 4\cdot 5\cdot 7\cdot 8)\ (\mathrm{mod}9).$$

Como $mdc(1\cdot 2\cdot 4\cdot 5\cdot 7\cdot 8,9)=1$, temos $5^6\equiv 1\ (\mathrm{mod}9)$, isto é,

$$5^{\phi(9)}\equiv 1\ (\mathrm{mod}9).$$

É exatamente isto que mostra o Teorema de Euler para o caso geral.

Teorema 4.2.10 (Euler) *Sejam a e m inteiros, com $m\geq 1$ e $mdc(a,m)=1$. Então,*

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

Demonstração: O caso $m=1$ é imediato, pois $\phi(1)=1$. Por isso, vamos considerar $m>1$. Sejam $a_1,a_2,\ldots,a_{\phi(m)}$ os inteiros positivos menores do que m que são relativamente primos com m. Visto que $mdc(a,m)=1$, temos que $aa_1,aa_2,\ldots,aa_{\phi(m)}$ são congruentes módulo m a $a_1,a_2,\ldots,a_{\phi(m)}$, em alguma ordem. Desse modo,

$$\begin{aligned} a\cdot a_1 &\equiv b_1\ (\mathrm{mod}m),\\ a\cdot a_2 &\equiv b_2\ (\mathrm{mod}m),\\ &\vdots\\ a\cdot a_{\phi(m)} &\equiv b_{\phi(m)}\ (\mathrm{mod}m), \end{aligned}$$

em que $b_1,b_2,\ldots,b_{\phi(m)}$ são os inteiros $a_1,a_2,\ldots,a_{\phi(m)}$, não necessariamente nesta ordem. Multiplicando membro a membro estas congruências, temos

$$(aa_1)(aa_2)\ldots(aa_{\phi(m)})\equiv b_1b_2\ldots b_{\phi(m)}\ (\mathrm{mod}m),$$

ou seja,

$$a^{\phi(m)}(a_1a_2\ldots a_{\phi(m)})\equiv a_1a_2\ldots a_{\phi(m)}\ (\mathrm{mod}m).$$

Como $mdc(a_i,m)=1$ para todo $i=1,\ldots,\phi(m)$, segue em decorrência do Lema 4.2.5 que $mdc(a_1a_2\ldots a_{\phi(m)},m)=1$. Por isso, podemos cancelar o fator $a_1a_2\ldots a_{\phi(m)}$ da última congruência e, assim, $a^{\phi(m)}\equiv 1\ (\mathrm{mod}m)$. □

Nota-se que se $m=p$ é primo, então $\phi(p)=p-1$. Desse modo, para $a\in\mathbb{Z}$, com $mdc(a,p)=1$, obtemos do Teorema de Euler que

$$a^{p-1}\equiv 1\ (\mathrm{mod}p),$$

ou seja, o Teorema de Fermat é um caso particular do Teorema de Euler.

4.3 Congruências Lineares

Nesta seção, estudaremos congruências lineares, que são um tipo especial de congruência. Veremos que se uma congruência linear tiver uma solução inteira (ou simplesmente, uma solução), então ela terá infinitas delas. Apresentaremos um resultado que caracteriza todas as congruências lineares que têm solução. Por outro lado, veremos que as soluções de uma congruência linear são obtidas a partir de uma solução inicial e com um parâmetro inteiro.

Definição 4.3.1 *Sejam a e b inteiros, com $a \neq 0$. Uma congruência da forma*

$$ax \equiv b \pmod{m}$$

é chamada ***congruência linear****, onde x é uma incógnita.*

Por exemplo, $x_0 = 2$ é uma solução da congruência linear $8x \equiv 7 \pmod{3}$, pois $8 \cdot 2 = 16 \equiv 7 \pmod{3}$. Enquanto, a congruência linear $4x \equiv 3 \pmod{2}$ não tem solução inteira, pois se existisse uma solução $x_0 \in \mathbb{Z}$, teríamos

$$4x_0 - 3 = 2q \Rightarrow 3 = 2(2x_0 - q) \Rightarrow 2 \mid 3,$$

o que é uma contradição.

Objetivamente, temos que determinar todas soluções inteiras (se existirem) de $ax \equiv b \pmod{m}$, isto é, todos os inteiros x_0 para os quais

$$ax_0 \equiv b \pmod{m}.$$

Um caso particular importante da congruência linear definida anteriormente é

$$ax \equiv 1 \pmod{m}.$$

Neste caso, se x_0 é uma solução desta congruência, então dizemos que a é **invertível** módulo m, e que x_0 é um **inverso** de a módulo m. Por exemplo, na congruência

$$19x \equiv 1 \pmod{5},$$

o número 19 é invertível, pois $x_0 = 4$ é uma solução desta congruência, de modo que este é um inverso de 19.

Vimos que nem sempre uma congruência linear tem solução inteira. Por outro lado, uma congruência linear pode ter infinitas soluções. Inicialmente, observamos que se x_0 é uma solução de $ax \equiv b \pmod{m}$ e $x_0 \equiv y_0 \pmod{m}$, então y_0 também é solução desta congruência.

Por exemplo, $x_0 = 2$ é uma solução de $8x \equiv 7 \pmod{3}$. Por outro lado, toda solução é da forma

$$x = 2 + 3k, \quad \text{com} \quad k \in \mathbb{Z},$$

como veremos adiante, de modo geral, nos passos apresentados para resolver uma congruência linear.

Os próximos resultados estabelecerão quando uma congruência linear tem solução e também o conjunto de todas as soluções.

Teorema 4.3.2 *A congruência linear $ax \equiv b \pmod{m}$ tem solução inteira se, e somente se, $d \mid b$, com $d = mdc(a,m)$.*

Demonstração: Inicialmente, tomemos $d = mdc(a,m)$ e suponhamos que x_0 seja uma solução de $ax \equiv b \pmod{m}$. Logo, existe $k \in \mathbb{Z}$, tal que, $ax_0 - b = km$, isto é, $b = ax_0 - km$. Daí, como $d \mid a$ e $d \mid m$, então $d \mid b$.

Reciprocamente, supondo que $d \mid b$ com $d = mdc(a,m)$, então pela identidade de Bachet-Bézout existem inteiros r e s tais que

$$d = a \cdot r + s \cdot m.$$

Como $d \mid b$, então existe $t \in \mathbb{Z}$, tal que $b = dt$, logo usando o valor de d, obtemos

$$b = (ar + sm)t = art + smt,$$

isto é, $a(rt) \equiv b \pmod{m}$. Portanto, $x_0 = rt$ é uma solução de $ax \equiv b \pmod{m}$. □

Por exemplo, a congruência $6x \equiv 5 \pmod{2}$ não tem solução inteira, pois $mdc(6,2) = 2$ e $2 \nmid 5$.

A solução geral de uma congruência linear fica estabelecida com o seguinte:

Teorema 4.3.3 *Se x_0 é uma solução da congruência linear $ax \equiv b \pmod{m}$, então todas as soluções desta congruência são da forma*

$$x = x_0 + (m/d)k, \quad com \quad k \in \mathbb{Z},$$

com $d = mdc(a,m)$.

Demonstração: Inicialmente, vamos provar que para cada inteiro k, $x = x_0 + (m/d)k$, com $d = mdc(a,m)$, é uma solução de $ax \equiv b \pmod{m}$. Como $ax_0 \equiv b \pmod{m}$, ou seja, $ax_0 = b + \lambda m$, com $\lambda \in \mathbb{Z}$, temos

$$ax = a(x_0 + (m/d)k) = ax_0 + a(m/d)k = b + m(\lambda + ak/d).$$

Portanto, $ax \equiv b \pmod{m}$, pois $ak/d \in \mathbb{Z}$.

Agora, seja $x_1 \in \mathbb{Z}$ tal que $ax_1 \equiv b \pmod{m}$. Sendo $ax_0 \equiv b \pmod{m}$, segue por transitividade que $ax_1 \equiv ax_0 \pmod{m}$. Assim, pelo Teorema 4.1.10, $x_0 \equiv x_1 \pmod{m/d}$, ou seja,

$$x_1 = x_0 + \frac{m}{d}k, \quad \text{com} \quad k \in \mathbb{Z}.$$

□Particularmente,

Corolário 4.3.4 *Temos que $ax \equiv 1 \pmod{m}$ tem solução se, e somente se, $mdc(a,m) = 1$. Neste caso, a solução geral é dada por*

$$x = x_0 + km, \quad com \quad k \in \mathbb{Z},$$

com x_0 uma solução inicial.

Note que um inteiro a é invertível módulo m se, e somente se, $mdc(a,m) = 1$, como pode ser observado facilmente do corolário anterior.

Quanto ao número de soluções incongruentes de uma congruência linear a proposição seguinte caracteriza esse fato.

Proposição 4.3.5 *Consideremos a congruência* $ax \equiv b \pmod{m}$*, em que* $d = mdc(a,m)$*. Se* $d \mid b$*, então esta congruência possui* d *soluções incongruentes módulo* m*, dadas por*

$$x_0, \quad x_0 + \frac{m}{d}, \quad x_0 + \frac{2m}{d}, \ldots, \quad x_0 + \frac{(d-1)m}{d}, \tag{4.6}$$

com x_0 *é uma solução particular.*

Demonstração: Pelo Teorema 4.3.3, para cada inteiro k,

$$x = x_0 + \frac{m}{d}k$$

é solução de $ax \equiv b \pmod{m}$. O que devemos mostrar é que

$$\left(x_0 + \frac{m}{d}k_1\right) \not\equiv \left(x_0 + \frac{m}{d}k_2\right) \pmod{m},$$

com $0 \leq k_1 < k_2 \leq d-1$. De fato, nestas condições, se

$$\left(x_0 + \frac{m}{d}k_1\right) \equiv \left(x_0 + \frac{m}{d}k_2\right) \pmod{m},$$

então

$$\frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \pmod{m},$$

e pelo Teorema 4.1.10,

$$k_1 \equiv k_2 \pmod{m/d_1},$$

sendo $d_1 = mdc(m/d, m)$. Como $m = (m/d)d$, temos $d_1 = m/d$ e, com isto,

$$\frac{m}{d_1} = \frac{m}{m/d} = d.$$

Portanto, $k_1 \equiv k_2 \pmod{d}$, ou seja, $d \mid k_2 - k_1$, o que é uma contradição, já que $0 < k_2 - k_1 < d-1$. Por conseguinte, as soluções são duas a duas incongruentes módulo m.

Resta-nos mostrar que qualquer solução $x = x_0 + (m/d)k$ de $ax \equiv b \pmod{m}$ é congruente módulo m a uma das d soluções dadas em (4.6). Pelo Algoritmo da Divisão, temos que $k = dq + r$, com $0 \leq r \leq d-1$. Assim,

$$\begin{aligned} x \;=\; x_0 + (m/d)k \;&=\; x_0 + (m/d)(dq + r) \\ &=\; x_0 + mq + r(m/d) \\ &\equiv\; x_0 + r(m/d) \pmod{m}, \end{aligned}$$

em que $x_0 + r(m/d)$ é uma das soluções em (4.6). □

Em particular, quando o $mdc(a,m) = 1$, obtemos o seguinte:

Corolário 4.3.6 *Se $mdc(a,m) = 1$, então a congruência linear $ax \equiv b \pmod{m}$ tem única solução módulo m.*

Em síntese, fazendo uso dos resultados obtidos anteriormente, podemos resolver uma congruência linear $ax \equiv b \pmod{m}$, com $d = mdc(a,m)$ e $d \mid b$, seguindo os seguintes passos:

(1) De acordo com a Identidade de Bachet-Bézout, obtemos inteiros r e s tais que

$$d = a \cdot r + m \cdot s.$$

(2) Se $b = dt$, então $x_0 = rt$ é uma solução de $ax \equiv b \pmod{m}$, de modo que sua solução geral é dada por

$$x = x_0 + k\frac{m}{d}, \text{ com } k \in \mathbb{Z}.$$

Além disso,

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + \frac{2m}{d},\ldots,\ x_0 + \frac{(d-1)m}{d}$$

são as soluções de $ax \equiv b \pmod{m}$ duas a duas incongruentes módulo m.

Exemplo 4.3.7 Resolver as seguintes congruências lineares:

a) $6x \equiv 21 \pmod{8}$.

b) $3x \equiv 6 \pmod{12}$.

Solução: a) Como $mdc(8,6) = 2$ e $2 \nmid 21$, então, pelo Teorema 4.3.2 a congruência não tem solução inteira.

b) Como $mdc(3,12) = 3$ e $3 \mid 6$, então a congruência tem solução inteira. Daí, procedendo de maneira análoga ao Exemplo 2.3.7, temos

$$3 \cdot 5 + 12 \cdot (-1) = 3,$$

isto é, $r = 5$. Daí, como $b = 6 = 3 \cdot 2$, segue que $t = 2$. Logo, $x_0 = rt = 5 \cdot 2 = 10$ é uma solução particular de $3x \equiv 6 \pmod{12}$. A solução geral é dada por $x = 10 + (12/3)k$, ou seja,

$$x = 10 + 4k, \text{ com } k \in \mathbb{Z}.$$

Dessa forma, temos $d = 3$ soluções incongruentes módulo 12, que são

$$10,\ 10 + \frac{12}{3},\ 10 + 2 \cdot \frac{12}{3},$$

ou melhor, 10, 14 e 18. △

A fim de estabelecer alguns resultados relevantes da Teoria dos Números por meio de congruências, é importante decidir quando uma congruência linear tem solução inteira.

Proposição 4.3.8 *Um inteiro a é invertível módulo m se, e somente se, $mdc(a,m) = 1$. Ademais, quaisquer dois inversos de a módulo m são congruentes*[1] *módulo m.*

Demonstração: Se a é invertível módulo m, então existe um inteiro b tal que $ab \equiv 1 \pmod{m}$. Logo, existe $c \in \mathbb{Z}$, com $ab = 1 + cm$, ou seja, $ab + (-c)m = 1$. Logo, de (2.6), obtemos $mdc(a,m) = 1$.

Para a recíproca, se $mdc(a,m) = 1$, então pela identidade de Bachet-Bézout, existem inteiros x e y tais que $ax + my = 1$, isto é, $ax \equiv 1 \pmod{m}$, o que mostra que a é invertível módulo m.

Finalmente, se x_0 e y_0 são inversos de a módulo m, então $ax_0 \equiv 1 \pmod{m}$ e $ay_0 \equiv 1 \pmod{m}$, ou seja, $ax_0 \equiv ay_0 \pmod{m}$. Já que $mdc(a,m) = 1$, segue do Corolário 4.1.11 que $x_0 \equiv y_0 \pmod{m}$. □

Exemplo 4.3.9 Temos que 4 e 8 são invertíveis módulo 9, cujos inversos módulo 9 são 7 e 8, respectivamente, pois $4 \cdot 7 \equiv 1 \pmod{9}$ e $8 \cdot 8 \equiv 1 \pmod{9}$. △

Vale ressaltar que se x_0 é uma solução de $ax \equiv b \pmod{m}$ e $x_0 \equiv y_0 \pmod{m}$, então y_0 também é solução. De fato, como $ax_0 \equiv b \pmod{m}$ e $ax_0 \equiv ay_0 \pmod{m}$, segue por transitividade que $ay_0 \equiv b \pmod{m}$. Isto nos mostra que se uma congruência linear $ax \equiv b \pmod{m}$ tem uma solução x_0, então para cada inteiro k,

$$x = x_0 + km$$

também é solução, ou melhor, $ax \equiv b \pmod{m}$ tem infinitas soluções. Por exemplo, $x_0 = 1$ é uma solução de $8x \equiv 14 \pmod{6}$, de modo que

$$x = 1 + 6k$$

é solução para todo $k \in \mathbb{Z}$, isto é, esta expressão gera infinitas soluções, mas não gera todas elas. Com efeito, $y_0 = 4$ é uma solução de $8x \equiv 14 \pmod{6}$, mas é claro que não existe um inteiro k, com $4 = 1 + 6k$.

4.3.1 Sistemas de Congruências Lineares

Uma vez que já consideramos a solução de uma única congruência linear, surge naturalmente, assim como ocorre com sistemas de equações lineares, o problema que consiste em resolver simultaneamente um sistema de duas ou mais congruências lineares, por exemplo, um sistema da forma

$$\begin{cases} x \equiv 25 \pmod{6}, \\ x \equiv 4 \pmod{15}. \end{cases}$$

[1] Em outras palavras, o inverso de a é único módulo m.

Resolvê-lo é determinar todos os inteiros x que satisfazem ambas as congruências. Vamos fazer isto usando o método de substituição, semelhante ao usado para resolver um sistema de equações lineares.

Da primeira congruência, obtemos que $x = 25 + 6y$, com $y \in \mathbb{Z}$. Aqui usamos y ao invés de k, pois precisamos resolver outra congruência em y. De fato, para que x seja solução do sistema, ele deve satisfazer também a segunda congruência. Assim, devemos substituir o valor de $x = 25 + 6y$ em $x \equiv 4 \pmod{15}$. Fazendo isto, temos

$$25 + 6y \equiv 4 \pmod{15},$$

ou melhor, $6y \equiv -21 \pmod{15}$. Como $mdc(6,15) = 3$ e $3 \mid -21$, esta congruência tem solução inteira. Resolvendo-a da mesma forma que fizemos anteriormente, obtemos

$$y = 9 + 5k.$$

Substituindo o valor de y em $x = 25 + 6y$, segue que

$$x = 25 + 6(9 + 5k) = 79 + 30k,$$

isto é, a solução geral do sistema é $x = 79 + 30k$ ou, se preferirmos, $x = 19 + 30k$, sendo k um inteiro arbitrário, pois $79 \equiv 19 \pmod{30}$.

Se a congruência $6y \equiv -21 \pmod{15}$ não tivesse solução, então o sistema dado também não teria solução. Além disso, se este tivesse mais uma congruência, então para não causar confusão, seria conveniente escrever $x = 19 + 30z$ ao invés de $x = 19 + 30k$ (para dar uma conotação de incógnita), e após isso substituir este valor na terceira congruência, resolvendo-a em z e fazendo a substituição necessária para se obter uma expressão algébrica final para x. O procedimento é análogo para um sistema com n congruências.

4.3.2 O Teorema Chinês dos Restos

O problema que conduz a um sistema de congruências lineares é um tanto quanto antigo. O matemático chinês Sun-Tsu que viveu no primeiro século da nossa era, propôs em seu livro intitulado *Suan-Ching* (*Aritmética*) o seguinte problema: determinar um número que deixa restos 2, 3 e 2 quando dividido por 3, 5 e 7, respectivamente. Em termos de congruências, este problema consiste em resolver o seguinte sistema:

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

Sun-Tsu, encontrou $x = 23$ como solução para o problema. É bem provável que ele não tivesse conhecimento de um método de resolução geral para congruências lineares e também não soubesse que o problema tem uma infinidade de soluções módulo 23.

No capítulo seguinte resolveremos esse problema usando um método que apresentaremos mais adiante (o Teorema chinês dos restos).

De um modo geral, vamos estudar sistemas de congruências da forma

$$\begin{cases} a_1x \equiv b_1 \pmod{m_1}, \\ a_2x \equiv b_2 \pmod{m_2}, \\ \quad \vdots \\ a_kx \equiv b_k \pmod{m_k}. \end{cases} \tag{4.7}$$

Naturalmente, para que este sistema tenha solução, é necessário que cada uma das k congruências tenha solução, ou seja, que $d_i \mid b_i$, em que $d_i = mdc(a_i, m_i)$ para cada $i = 1, \ldots, k$, conforme o Teorema 4.3.2. Entretanto, esta condição não é suficiente. Por exemplo, o sistema formado pelas congruências $x \equiv 6 \pmod{4}$ e $x \equiv 5 \pmod{2}$ não tem solução embora cada uma tenha solução.

Vamos começar com o lema seguinte que nos mostra como obter um sistema equivalente ao dado em (4.7), mas com os coeficientes iguais a 1 (os inteiros a_i em $a_ix \equiv b_i \pmod{m_i}$). Ressaltamos que dois sistemas de congruências lineares são **equivalentes** quando possuem as mesmas soluções. Da mesma forma, duas congruências lineares são **equivalentes** quando têm as mesmas soluções.

Lema 4.3.10 *A congruência linear $ax \equiv b \pmod{m}$, em que $d = mdc(a,m)$, com $d \mid b$, é equivalente a*

$$x \equiv rb_1 \pmod{n},$$

sendo $b = b_1d$, $d = a \cdot r + s \cdot m$ e $m = nd$.

Demonstração: Considerando $a = a_1d$, $b = b_1d$ e $m = nd$, vem que

$$ax \equiv b \pmod{m} \iff a_1dx \equiv b_1d \pmod{nd}.$$

Pelo Teorema 4.1.10,

$$a_1x \equiv b_1 \pmod{n}. \tag{4.8}$$

Sendo $d = a \cdot r + s \cdot m$, segue que $d = a_1d \cdot r + s \cdot nd$, ou seja, $1 = a_1 \cdot r + s \cdot n$. Logo,

$$ra_1 \equiv 1 \pmod{n}.$$

Multiplicando a congruência de (4.8) por r, temos

$$ra_1x \equiv rb_1 \pmod{n},$$

e como $a_1r \equiv 1 \pmod{n}$, segue que $x \equiv a_1rx \pmod{n}$, isto é,

$$x \equiv rb_1 \pmod{n},$$

o que prova a primeira parte.

Reciprocamente, se $x \equiv rb_1 \pmod{n}$, então como $ra_1 \equiv 1 \pmod{n}$, segue que $xra_1 \equiv rb_1 \pmod{n}$. Por outro lado, visto que $1 = a_1 \cdot r + s \cdot n$, temos que $mdc(r,n) = 1$. Portanto, podemos cancelar o fator r da última congruência de modo a obter $xa_1 \equiv b_1 \pmod{n}$, ou seja, $x(a/d) \equiv b/d \pmod{m/d}$, da qual obtemos $ax \equiv b \pmod{m}$. □

A vantagem de se considerar uma congruência da forma $x \equiv b \pmod{m}$ é que sua solução geral é obtida de forma direta, $x = b + km$, com $k \in \mathbb{Z}$.

Exemplo 4.3.11 Determinar a congruência linear da forma $x \equiv c \pmod{n}$ equivalente à congruência $6x \equiv 10 \pmod{4}$.

Solução: Temos que $mdc(6,4) = 2$, $b_1 = b/2 = 10/2 = 5$, $n = m/2 = 4/2 = 2$. Como $2 = 6 \cdot 1 - 1 \cdot 4$, $r = 1$. Assim, $6x \equiv 10 \pmod{4}$ é equivalente a $x \equiv rb_1 \pmod{n}$, ou seja, $x \equiv 5 \pmod{2}$, cuja solução geral é $x = 5 + 2k$, com $k \in \mathbb{Z}$. △

De acordo com o lema anterior, o sistema dado em (4.7) é equivalente ao sistema

$$\begin{cases} x \equiv c_1 \pmod{n_1}, \\ x \equiv c_2 \pmod{n_2}, \\ \quad \vdots \\ x \equiv c_k \pmod{n_k}, \end{cases} \tag{4.9}$$

o qual será resolvido por meio do teorema a seguir com uma hipótese adicional, cujo título faz lembrar a origem desse problema.

Teorema 4.3.12 (Teorema Chinês dos Restos) *Sejam $n_1, n_2, \ldots, n_k$ números naturais tais que $mdc(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares dado em* (4.9) *possui uma solução, que é única módulo $n = n_1 n_2 \ldots n_k$.*

Demonstração: Sendo $n = n_1 n_2 \ldots n_k$, então

$$N_i = \frac{n}{n_i} = n_1 n_2 \ldots n_{i-1} n_{i+1} \ldots n_k,$$

ou seja, N_i é o produto de todos os inteiros $n_1, n_2, \ldots, n_k$ excluindo n_i. Já que $mdc(n_i, n_j) = 1$ para $i \neq j$, temos $mdc(N_i, n_i) = 1$. Assim, pela identidade de Bachet-Bézout, existem inteiros r_i e s_i tais que

$$r_i N_i + s_i n_i = 1 \tag{4.10}$$

para cada $i = 1, \ldots, k$. A partir disto, vamos provar que o inteiro

$$x_0 = \sum_{i=1}^{k} c_i r_i N_i = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k$$

é uma solução do sistema dado. Inicialmente, se $i \neq j$, então $N_j \equiv 0 \pmod{n_i}$, pois $n_i \mid N_j$. Logo, $c_j r_j N_j \equiv 0 \pmod{n_i}$, de modo que

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \cdots + c_k r_k N_k \equiv c_i r_i N_i \pmod{n_i}.$$

Por outro lado, de (4.10), temos que $r_i N_i \equiv 1 \pmod{n_i}$ para cada $i = 1, \ldots, k$. Daí, $c_i r_i N_i \equiv c_i \pmod{n_i}$ e, por transitividade, $x_0 \equiv c_i \pmod{n_i}$ para todo i. Isto mostra que x_0 é uma solução do sistema. Por fim, se y_0 é outra solução, então

$$y_0 \equiv c_i \pmod{n_i}$$

para cada $i = 1, \ldots, k$. Desse modo, $x_0 \equiv y_0 \pmod{n_i}$, isto é, $n_i \mid x_0 - y_0$. Já que $mdc(n_i, n_j) = 1$, com $i \neq j$, segue do Corolário 2.3.11 que $n = n_1 n_2 \ldots n_k$ divide $x_0 - y_0$, ou seja, $x_0 \equiv y_0 \pmod{n}$, o que prova a unicidade de solução módulo n. Por isso, a solução geral do sistema é

$$x = x_0 + kn, \quad k \in \mathbb{Z}.$$

□

4.4 Equações Diofantinas Lineares

Chama-se *equação diofantina* a toda equação polinomial com coeficientes inteiros, independente da quantidade de incógnitas. Essa nomenclatura é uma homenagem ao matemático grego Diofanto que viveu na cidade de Alexandria no século III. Ele é considerado o pai da Álgebra e da Teoria dos Números, e talvez mais conhecido como o escritor do livro *Aritmética*.

Foram os matemáticos italianos do século XVI quem apresentaram os trabalhos de Diofanto para a Europa, onde foram bem-recebidos e onde eles estimularam o estudo da Álgebra. Diofanto foi o primeiro a estudar de forma sistemática as soluções inteiras de algumas equações polinomiais, considerando uma abordagem algébrica.

Muito pouco se sabe sobre a vida pessoal de Diofanto. No que concerne à idade que ele tinha quando morreu, conta-se que sobre seu túmulo havia escrito um enigma que continha pistas para se calcular seu tempo de vida. É o seguinte:

> *"Aqui jaz o matemático que passou um sexto de sua vida como criança. Depois, por um doze avos da sua vida passou como rapaz. Depois viveu um sétimo da sua vida antes de se casar. Cinco anos após nasceu seu filho, com quem conviveu metade da sua vida. Após a morte de seu filho, sofreu mais 4 anos antes de morrer".*

Vamos estabelecer uma equação (diofantina em uma incógnita) baseada nos dados do enigma acima, de modo a calcular o tempo de vida de Diofanto.

Seja x a idade de Diofanto quando de sua morte. Assim, $x/6$ de sua vida ele passou como criança; $x/12$ ele passou como rapaz; $x/7$ foi o tempo antes de se casar; 5 anos após seu filho nasceu; $x/2$ foi o tempo de vida de seu filho; e finalmente, sofreu mais 4 anos antes de morrer. Desse modo, x é igual a seguinte soma:

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4,$$

ou melhor, $x = (25/28)x + 9$, da qual obtemos $x = 84$. Portanto, Diofanto teria morrido com 84 anos.

Definição 4.4.1 *Uma **equação diofantina** é qualquer equação polinomial com coeficientes inteiros com uma ou mais incógnitas.*

Assim, uma equação da forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

é chamada uma **equação diofantina linear**, em que $a_1, \ldots, a_n$ são inteiros dados, chamados **coeficientes**, b que também é um inteiro dado, é chamado **termo constante** e $x_1, \ldots, x_n$ são as **incógnitas**.

De acordo com as definições anteriores, as equações

$$x^2 + y^2 = z^2, \quad xy + 4y = xy \quad e \quad x - y^3 = -8$$

são exemplos de equações diofantinas não lineares.

Inicialmente, focaremos nosso estudo no caso mais simples de equações diofantinas lineares com duas incógnitas – equações da forma

$$ax + by = c.$$

Uma **solução inteira** desta equação é um par de inteiros x_0 e y_0 tais que

$$ax_0 + by_0 = c.$$

É importante responder as seguintes questões:

a) Em quais condições a equação $ax + by = c$ admite solução?

b) Caso admita, quantas existem e como determiná-las?

Quando $a = 0$ ou $b = 0$, obtemos casos triviais, os quais não serão, por razões óbvias, considerados. Observemos também que resolver $ax + by = c$ em valores reais equivale geometricamente a traçar uma reta no plano. Isso é algo muito fácil de se fazer. Por isso, focaliza-se as soluções inteiras ou racionais, em nosso caso, apenas as inteiras.

Vamos responder as questões acima. De início, a equação $ax + by = c$ nos conduz à congruência linear

$$ax \equiv c \pmod{|b|},$$

a qual nos dá um ponto de partida.

Teorema 4.4.2 *A equação diofantina $ax+by=c$ tem solução inteira se, e somente se, $d \mid c$, com $d = mdc(a,b)$. Além disso, se x_0 e y_0 é uma solução particular desta equação, então sua solução geral é dada por*

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

em que k é um inteiro.

Demonstração: Como $ax+by=c$ tem solução se, e somente se, a congruência linear $ax \equiv c \pmod{|b|}$ tem solução, segue do Teorema 4.3.2 que $ax+by=c$ tem solução se, e somente se, $d \mid c$, com $d = mdc(a,b)$. Isto prova a primeira parte. Para a segunda, notemos primeiramente que sendo x_0 e y_0 uma solução particular de $ax+by=c$, então para cada inteiro k,

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

também é solução, pois $ax_0+by_0=c$ e, assim,

$$\begin{aligned} ax'+by' &= a[x_0+(b/d)k]+b[y_0-(a/d)k] \\ &= (ax_0+by_0)+(ab/d-ab/d)k, \end{aligned}$$

ou seja, $ax'+by'=c$. Agora, suponhamos que x' e y' seja outra solução de $ax+by=c$. Logo,

$$ax'+by' = c = ax_0+by_0,$$

ou melhor,

$$a(x'-x_0) = b(y_0-y'). \tag{4.11}$$

Sendo $d = mdc(a,b)$, então $a=dr$ e $b=ds$, em que $mdc(r,s)=1$. Substituindo estes valores em (4.11) e cancelando o fator comum d, temos

$$r(x'-x_0) = s(y_0-y'). \tag{4.12}$$

Isto nos mostra que $r \mid s(y_0-y')$. Como $mdc(r,s)=1$, segue do Corolário 2.3.10 que $r \mid (y_0-y')$, ou seja, $y_0-y'=kr$ para algum inteiro k. Substituindo esta expressão em (4.12), obtemos $x'-x_0=ks$. Portanto,

$$\begin{aligned} x' &= x_0+ks &&= x_0+(b/d)k, \\ y' &= y_0-kr &&= y_0-(a/d)k. \end{aligned}$$

□

Nas condições do teorema anterior, uma equação diofantina $ax+by=c$ possui infinitas soluções e, para determiná-las, faz-se necessário apenas encontrar uma solução particular x_0 e y_0, a qual pode ser obtida por meio de uma combinação linear dos inteiros a e b para $d = mdc(a,b)$. Vejamos então. Pelo Algoritmo de Euclides, obtemos inteiros r e s tais que

$$d = ar+bs.$$

Fazendo $c = dt$ e multiplicando a igualdade acima por t, temos

$$c = dt = a(rt) + b(st),$$

ou seja, $x_0 = rt$ e $y_0 = st$ é uma solução de $ax + by = c$.

Vamos supor que $ax + by = c$ admita solução e seja $d = mdc(a,b)$. Dividindo ambos os lados desta equação por d, obtemos

$$\left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y = \left(\frac{c}{d}\right), \tag{4.13}$$

com $mdc(a/d, b/d) = 1$. Assim, se x_0 e y_0 é uma solução desta equação, então

$$\left(\frac{a}{d}\right)x_0 + \left(\frac{b}{d}\right)y_0 = \left(\frac{c}{d}\right),$$

de modo que $ax_0 + by_0 = c$, isto é, x_0 e y_0 é solução de $ax + by = c$. Reciprocamente, se $ax_0 + by_0 = c$, então $(a/d)x_0 + (b/d)y_0 = c/d$ e, assim, x_0 e y_0 é solução de (4.13). Portanto, as equações consideradas são equivalentes, ou seja, têm as mesmas soluções. □

Teorema 4.4.3 *A equação diofantina $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ tem solução inteira se, e somente se, $d \mid b$, com $d = mdc(a_1, a_2, \cdots, a_n)$.*

Demonstração: Consideremos $(x'_1, x'_2, \ldots, x'_n)$ uma solução de equação apresentada nesse Teorema, então

$$a_1x'_1 + a_2x'_2 + \cdots + a_nx'_n = b. \tag{4.14}$$

Seja $d = mdc(a_1, a_2, \cdots, a_n) \Rightarrow d \mid a_i$ com $i = 1, 2, \cdots, n$. Dessa forma, existem inteiros $k_1, k_2, \cdots k_n$ tais que $a_i = d \cdot k_i$.
Agora em (4.14) temos:

$$(d \cdot k_1) \cdot x'_1 + (d \cdot k_2) \cdot x'_2 + \cdots + (d \cdot k_n) \cdot x'_n = b.$$

Logo,

$$d \cdot (k_1 \cdot x'_1 + k_2 \cdot x'_2 + \cdots + k_n \cdot x'_n) = b \Rightarrow d \mid b.$$

Agora suponhamos que $d = mdc(a_1, a_2, \cdots, a_n)$ e que $d \mid b$, então:

$$b = d \cdot t; \ t \in \mathbb{Z}. \tag{4.15}$$

Pela identidade de Bachet-Bézout, existem inteiros $k_1, k_2, \cdots k_n$ tais que tal que:

$$a_1 \cdot k_1 + a_2 \cdot k_2 + \cdots + a_n \cdot k_n = d.$$

Assim em (4.15) teremos:

$$b = (a_1 \cdot k_1 + a_2 \cdot k_2 + \cdots + a_n \cdot k_n) \cdot t.$$

Dessa forma:

$$a_1 \cdot (k_1 \cdot t) + a_2 \cdot (k_2 \cdot t) + \cdots + a_n \cdot (k_n \cdot t) = b.$$

Na equação acima, considerando $k_i \cdot t = x_i'$ teremos:

$$a_1 \cdot x_1' + a_2 \cdot x_2' + \cdots + a_n \cdot x_n' = b.$$

Mostrando que $(x_1', x_2', \cdots, x_n')$ é uma solução inteira para a equação apresentada no Teorema.□

Exemplo 4.4.4 Resolver a equação diofantina

$$52x + 72y = 40.$$

Solução: Como $mdc(52,72) = 4$ e $4 \mid 40$, a equação admite solução. Pelo que foi observado, a equação inicial é equivalente à equação

$$13x + 18y = 10,$$

em que $mdc(13,18) = 1$. Devemos determinar inteiros r e s tais que

$$13 \cdot r + 18 \cdot s = 1.$$

Temos

$$\begin{aligned} 18 &= 13 \cdot 1 + 5, \\ 13 &= 5 \cdot 2 + 3, \\ 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1. \end{aligned}$$

Assim,

$$\begin{aligned} 1 = 3 - 2 = 3 - (5-3) &= 2 \cdot 3 - 5 \\ &= 2 \cdot (13 - 5 \cdot 2) - 5 \\ &= 2 \cdot 13 - 5 \cdot 5 \\ &= 2 \cdot 13 - 5 \cdot (18 - 13) \\ &= 7 \cdot 13 - 5 \cdot 18. \end{aligned}$$

Logo, $r = 7$ e $s = -5$. Multiplicando ambos os lados de $1 = 13 \cdot 7 + 18 \cdot (-5)$ por 10, segue que

$$10 = 13 \cdot 70 + 18 \cdot (-50),$$

isto é, $x_0 = 70$ e $y_0 = -50$ é uma solução de $13x + 18y = 10$. Por conseguinte, a solução geral desta equação é dada por

$$x = 70 + 18k \quad \text{e} \quad y = -50 - 13k,$$

em que $k \in \mathbb{Z}$. $\triangle$

Em muitas situações, apenas as soluções não negativa de uma equação diofantina são de interesse, ou seja, soluções x e y, com $x \geq 0$ e $y \geq 0$. Neste caso, essas soluções são determinadas pelo parâmetro k. Veremos isto no próximo capítulo.

Capítulo 5

Algumas Aplicações

Uma vez que já consideramos no capítulo anterior o conceito de congruência módulo m, bem como as suas principais propriedades, iremos agora apresentar algumas aplicações dos resultados obtidos por meio dessas propriedades. Essas aplicações consistirão de duas partes, conforme descritas a seguir.

A primeira parte será constituída de problemas elementares que, essencialmente, trazenos situações do cotidiano. Alguns deles foram retirados de banco de dados de provas do Programa de Mestrado Profissional Em Matemática em Rede Nacional - PROFMAT, e outros foram selecionados dos livros textos que serviram de base para a elaboração do capítulo, como por exemplo, as referências [2] e [8]. Com isto, atingimos duas coisas essenciais. A primeira delas é contemplar os conteúdos ministrados em um componente da grade curricular obrigatória do PROFMAT. Especificamente, o componente intitulado Aritmética-MA14, que cobre os conteúdos de um curso inicial em Teoria Elementar dos Números. A outra coisa é destacar a aplicabilidade de conceitos que são usados para resolver problemas um pouco familiares aos leitores, mesmo que esses não sejam estudantes de Matemática.

Já a segunda parte deste será usada para apresentar algumas aplicações mais substanciais, mesmo que seja em nível elementar. Basicamente, a ideia é destacar, questões relacionadas à Aritmética Modular.

5.1 Parte I

Comecemos destacando algumas aplicações que envolvem equações diofantinas lineares com duas incógnitas.

Exemplo 5.1.1 Uma pessoa recebeu 91 reais em notas de 2 e de 5 reais.

a) Qual é o número máximo de notas que ela pode ter recebido?

b) O número de notas recebidas de 2 reais pode ser igual ao número de notas de 5 reais?

Solução: a) Indiquemos por x a quantidade de notas de 2 reais e por y a de notas de 5 reais. Assim, o problema nos conduz à equação diofantina

$$2x+5y=91.$$

Como $mdc(2,5)=1$ e $1 \mid 91$, a equação acima possui solução. Determinemos uma solução inicial. De acordo com Algoritmos de Euclides, obtemos

$$2\cdot(-2)+5\cdot 1=1.$$

Multiplicando ambos os membros desta igualdade por 91, vem que

$$2\cdot(-182)+5\cdot 91=91.$$

Desse modo, $x_0=-182$ e $y_0=91$ é uma solução para a equação. Por conseguinte, do Teorema 4.4.2, sua solução geral é dada por

$$x=-182+5t \quad \text{e} \quad y=91-2t, \tag{5.1}$$

em que $t\in\mathbb{Z}$. Portanto a pessoa receberá:

$$x+y=(-182+5t)+(91-2t) \;\Rightarrow\; x+y=-91+3t.$$

De acordo com a natureza do problema, apenas as soluções positivas, isto é, $x>0$ e $y>0$, são de interesse. Estas condições implicam $37\leq t\leq 45$. O número máximo de notas resultará quando t assumir seu valor máximo e a quantidade mínima quando t tiver assumido o valor mínimo. Para $t=45$,

$$x+y=-91+3\cdot 45 \;\Rightarrow\; x+y=44,$$

e para $t=37$,

$$x+y=-91+3\cdot 37 \;\Rightarrow\; x+y=20.$$

Portanto, o número máximo de notas recebidas é 44 e o número mínimo é igual a 20.

b) Para que o número de notas de 2 reais recebidas seja igual ao número de notas de 5 reais, devemos ter $x=y$, ou melhor,

$$-182+5t=91-2t \;\Rightarrow\; t=39.$$

Substituindo este valor em (5.1), obtemos

$$x=-182+5\cdot 39 \quad \text{e} \quad y=91-2\cdot 39 \;\Rightarrow\; x=13 \quad \text{e} \quad y=13.$$

Logo, é possível que o número de notas de 2 reais seja igual ao número de notas de 5 reais.$\triangle$

Exemplo 5.1.2 Numa criação de coelhos e galinhas, contam-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo-se que a diferença entre esses dois números é a menor possível?

Solução: Sejam x o número de galinhas e y o número de coelhos. Daí, obtemos a equação diofantina

$$2x+4y=400 \;\Rightarrow\; x+2y=200.$$

Esta equação tem solução, pois $mdc(1,2)=1$. Como

$$1=2\cdot 1-1\cdot 1 \;\Rightarrow\; 1\cdot(-1)+2\cdot 1=1,$$

segue que

$$1\cdot(-200)+2\cdot 200=200.$$

Portanto $x_0=-200$ e $y_0=200$ é uma solução inteira da equação. Visto que as demais soluções são da forma

$$x=x_0+bt \quad \text{e} \quad y=y_0-at,$$

Então

$$x=-200+2t \quad \text{e} \quad y=200-t,$$

com $t\in\mathbb{Z}$. Pelas condições do problema, devemos ter $x>0$, $y>0$, isto é,

$$-200+2t>0 \quad \text{e} \quad 200-t>0 \;\Rightarrow\; 100<t<200.$$

Disto segue que

$$y-x=(200-t)-(-200+2t) \;\Rightarrow\; y-x=400-3t.$$

Analisemos se $y-x=1$ conduz ao valor inteiro para t. Isto será feito, pois desejamos que a diferença entre a quantidade de animais seja a menor possível. Temos:

$$400-3t=1 \;\Rightarrow\; t=133.$$

Assim,

$$x=-200+2\cdot 133 \;\Rightarrow\; x=66 \quad \text{e} \quad y=200-133 \;\Rightarrow\; y=67.$$

Desse modo, existem 66 galinhas e 67 coelhos. △

Exemplo 5.1.3 Ao entrar em um bosque, alguns viajantes avistaram 37 montes de maças. Após serem retiradas 17 frutas, o restante foi dividido igualmente entre 79 pessoas. Qual a parte de cada pessoa?.

Solução: Sejam x o número de maças em cada monte e y o número de maças que cada pessoa recebeu, temos a seguinte equação diofantina:

$$37x-17=79y \;\Rightarrow\; 37x-79y=17. \tag{5.2}$$

Como $mdc(37,79)=1$, e 1 divide 17, logo a equação acima possui solução. Agora, pelo Algoritmo de Euclides temos que:

$$37\cdot(-32)-79\cdot(-15)=1.$$

Multiplicando ambos os membros da última igualdade acima por 17, temos:

$$37 \cdot (-544) - 79 \cdot (-255) = 17$$

Assim, $x_0 = -544$ e $y_0 = -255$ é uma solução particular para a equação em (5.2), cujas demais soluções, de acordo com (4.4.2) são da forma:

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

assim,

$$x = -544 - 79t \quad \text{e} \quad y = -255 - 37t,$$

com $t \in \mathbb{Z}$. Pela natureza do problema, devemos ter $x > 0$ e $y > 0$, que acarreta $t \leq 7$. Para $t = -7$, temos

$$\begin{aligned} x &= -544 - 79 \cdot (-7) \Rightarrow x = 9, \\ y &= -255 - 37 \cdot (-7) \Rightarrow y = 4. \end{aligned}$$

Da mesma forma, para $t = -8$, obtemos que $x = 88$ e $y = 41$. Todas as soluções positivas são obtidas quando fazemos t percorrer os inteiros $t = -9, -10, -11, \ldots$. △

Exemplo 5.1.4 Um parque de diversões cobra R$ 1,00 para a entrada de crianças e R$ 3,00 a de adulto. Para que a arrecadação de um dia seja R$ 200,00, qual o maior número de pessoas entre crianças e adultos que poderia frequentar o parque nesse dia? Quantas são as crianças e quantos são os adultos?

Solução: Sejam x a quantidade de crianças e y a quantidade de adultos. Daí, obtemos a equação

$$x + 3y = 200,$$

que tem solução, pois $mdc(1,3) = 1$. Verifica-se que a solução geral desta equação é

$$x = -400 + 3t \quad \text{e} \quad y = 200 - t,$$

em que $t \in \mathbb{Z}$. Devido às condições iniciais do problema, temos $x > 0$ e $y > 0$. Desse modo, $133 < t < 200$.

Para que o número de pessoas seja o máximo possível, devemos fazer a variável t assumir seu valor máximo no intervalo acima, pois assim teremos o maior número de crianças possível. Isso ocorre quando $t = 199$. Considerando este valor nas equações acima, obtemos

$$x = -400 + 3 \cdot 199 \Rightarrow x = 197 \quad \text{e} \quad y = 200 - 199 \Rightarrow y = 1.$$

Ou seja, o número máximo de pessoas é 198, sendo 197 crianças e 1 adulto. △

No próximo exemplo, temos uma situação que nos conduz a uma equação que, de acordo com a Definição 4.4.1, não é diofantina. No entanto, podemos fazer manipulações algébricas de forma a tornar seus coeficientes inteiros e obter tal equação.

Exemplo 5.1.5 Um lava jato lava carros oferecendo dois tipos de serviços: lavagem simples com o custo de R$ 24,00 e a completa por R$ 36,00. Certo dia, o gerente resolveu fazer uma promoção, dando 20% de desconto na lavagem simples e 10% de desconto na completa. No dia da promoção, o faturamento foi de R$ 810,00. Qual foi o menor número de clientes que foram atendidos?

Solução: Sejam x e y as quantidades de lavagens simples e completas respectivamente. Então a expressão que determina o faturamento do dia é dado pela equação

$$0,8 \cdot 24x + 0,9 \cdot 36y = 810 \;\Rightarrow\; 19,2x + 32,4y = 810.$$

Representando os coeficientes da equação acima na forma de fração, temos

$$\frac{192}{10}x + \frac{324}{10}y = 810.$$

Este problema pode ser resolvido multiplicando ambos os membros da última equação por 10. Fazendo isto, obtemos a equação diofantina

$$192x + 324y = 8100.$$

Dividindo ambos os membros desta equação por $12 = mdc(192,324)$, segue que

$$16x + 27y = 675, \tag{5.3}$$

Pelo Algoritmo de Euclides, obtemos

$$16 \cdot (-5) + 27 \cdot 3 = 1$$

Multiplicando esta igualdade por 675, vem que

$$16 \cdot (-3375) + 27 \cdot 2025 = 675.$$

Assim, $x_0 = -3375$ e $y_0 = 2025$ é uma solução particular de (5.3). As demais soluções são da forma

$$x = -3375 + 27t \quad \text{e} \quad y = 2025 - 16t,$$

com $t \in \mathbb{Z}$. Pelas condições iniciais $x \geq 0, y \geq 0$, por isso $125 \leq t \leq 126$, p/ $t = 125$

$$x = -3375 + 27 \cdot (125) \;\Rightarrow\; x = 0 \quad \text{e} \quad y = 2025 - 16 \cdot (125) \;\Rightarrow\; y = 25.$$

Totalizando 25 clientes. Agora, com $t = 126$,

$$x = -3375 + 27 \cdot (126) \;\Rightarrow\; x = 27 \quad \text{e} \quad y = 2025 - 16 \cdot (126) \;\Rightarrow\; y = 9.$$

Totalizando 36 clientes. Logo, 25 foi o menor número de clientes atendidos nesse dia da promoção. △

Exemplo 5.1.6 A quantidade de R$ 50000,00 foi dividido para um grupo de 40 pessoas. Esse grupo era formado por homens, mulheres e crianças. Supondo que cada homem recebeu R$500,00, cada mulher recebeu R$1 500,00 e cada criança recebeu R$ 100,00. Determine a quantidade de homens, mulheres e crianças que havia no grupo.

Solução: Sejam x, y, e z o número de homens, mulheres e crianças respectivamente. Logo,

$$x+y+z=40. \tag{5.4}$$

Por outro lado,

$$500x+1500y+100z=50000 \;\Rightarrow\; 5x+15y+z=500, \tag{5.5}$$

ou seja, obtemos uma equação diofantina com três incógnitas. Mas podemos usar a equação (5.4) de modo a reduzi-la a uma com duas incógnitas. Senão vejamos. De (5.4), temos $z=40-x-y$. Substituindo esta expressão em (5.5), segue que

$$2x+7y=230. \tag{5.6}$$

Como $mdc(2,7)=1$, esta equação tem solução, e sua solução geral é

$$x=-690+7t \quad \text{e} \quad y=230-2t, \tag{5.7}$$

em que $t\in\mathbb{Z}$. Mas pelas condições iniciais, $x,y>0$, de modo que $99\leq t\leq 114$. Observemos que se $t=99$, então

$$x=3 \quad \text{e} \quad y=32,$$

que é a solução mínimal. Logo, a equação em (5.7) é equivalente a

$$x=3+7t \quad \text{e} \quad y=32-2t. \tag{5.8}$$

Agora, substituindo (5.8) em (5.4), temos:

$$(3+7t)+(32-2t)+z=40 \;\Rightarrow\; z=5-5t. \tag{5.9}$$

Sendo por hipótese $z>0$, $t<1$ e, com isto, $t=0$. Portanto, substituindo o valor de $t=0$ em (5.9) e (5.8), temos $x=3$, $y=32$ e $z=5$. Que corresponde ao número de homens, mulheres e crianças, respectivamente. △

Equações Diofantinas Lineares com Três Incógnitas

Às vezes, um dado problema nos conduz a uma equação diofantina linear com três incógnitas que, pela natureza do problema, não pode ser reduzido a uma com duas incógnitas, como foi feito no problema do exemplo anterior.

Vamos a seguir estabelecer um método de solução para uma equação diofnatina da forma

$$a_1x+a_2y+a_3z=b, \tag{5.10}$$

em que x, y e z são as incógnitas. No capítulo anterior, vimos as condições necessária e suficiente para que a equação acima possua solução inteira.

A questão agora é determinar todas as soluções da equação anterior. Isto será feito seguindo os seguintes passos:

(1) Primeiramente, tomaremos uma equação diofantina da forma

$$a_1x+a_2y=t, \quad a_2y+a_3z=t \quad \text{ou} \quad a_1x+a_3z=t.$$

(2) A partir de uma solução da equação anterior, faremos as substituições necessárias, de modo a obter uma equação linear com duas incógnitas. Resolvendo essa equação, obteremos a solução geral da equação original.

Vamos tornar isto mais claro. Tomemos a equação

$$a_1x+a_2y+a_3z=b, \tag{5.11}$$

com $d \mid b$, em que $d=mdc(a_1,a_2,a_3)$. Consideremos também

$$a_1x+a_2y=t,$$

ou seja,

$$t+a_3z=b,$$

uma equação linear nas incógnitas t e z. Já que $mdc(1,a_3)=1$, esta equação tem solução inteira. Além disso, de acordo com o Teorema 4.4.2, sua solução geral é dada por

$$t=t_0+a_3k \quad \text{e} \quad z=z_0-k, \ \text{com} \ k\in\mathbb{Z},$$

sendo (t_0,z_0) uma solução particular. Logo,

$$a_1x+a_2y=t_0+a_3k. \tag{5.12}$$

Esta equação tem uma solução x_0 e y_0. Daí, sua solução geral é

$$x=x_0+\frac{a_2}{d_1}\lambda \quad \text{e} \quad y=y_0-\frac{a_1}{d_1}\lambda, \quad \text{com} \quad d_1=mdc(a_1,a_2), \ \lambda\in\mathbb{Z}.$$

Portanto, a solução geral da equação (5.11) é dada por

$$x=x_0+\frac{a_2}{d_1}\lambda, \quad y=y_0-\frac{a_1}{d_1}\lambda, \quad z=z_0-k,$$

para $\lambda,k\in\mathbb{Z}$.

Exemplo 5.1.7 Um avicultor comprou cem animais por um custo de R$ 4 000,00. Os preços desses animais foram os seguintes: perus R$ 120,00 cada um, patos R$ 50,00 cada um e galinhas R$ 25,00 cada uma. Se o avicultor obteve ao menos um animal de cada espécie, qual a quantidade comprada de cada uma dela?

Solução: Sejam x, y e z a quantidade de perus, patos e galinhas respectivamente, formaremos a seguinte equação:

$$120x + 50y + 25z = 4000 \;\Rightarrow\; 24x + 10y + 5z = 800. \tag{5.13}$$

Temos $mdc(24, 10, 5) = 1$ e como 1 divide 800, segue que a equação acima possui solução. Nesta equação, vamos considerar

$$24x + 5z = \lambda. \tag{5.14}$$

Dessa forma em (5.13) temos:

$$\lambda + 10y = 800. \tag{5.15}$$

Nesta última equação admitindo-se $y_0 = 1 \;\Rightarrow\; \lambda_0 = 790$. Então toda solução de (5.15) é da forma:

$$\lambda = 790 + 10t \quad \text{e} \quad y = 1 - t, \tag{5.16}$$

Com $t \in \mathbb{Z}$. Agora, substituindo (5.16) em (5.14) encontraremos a seguinte equação:

$$24x + 5z = 790 + 10t. \tag{5.17}$$

Sendo $mdc(24, 5) = 1$. Por meio do Algoritmo de Euclides, chegaremos a seguinte identidade:

$$24 \cdot (-1) + 5 \cdot 5 = 1,$$

e assim

$$24 \cdot (-790 - 10t) + 5 \cdot (3950 + 50t) = 790 + 10t.$$

A igualdade acima nos mostra que

$$x = -790 - 10t \quad \text{e} \quad z = 3950 + 50t$$

é uma solução particular em t de (5.17). Portanto, sua solução geral é

$$x = -790 - 10t + 5k \quad \text{e} \quad z = 3950 + 50t - 24k,$$

em que $k \in \mathbb{Z}$. Por essa última expressão e por (5.16), as solução de (5.13) são dadas por

$$x = -790 - 10t + 5k; \quad y = 1 - t \quad \text{e} \quad z = 3950 + 50t - 24k. \tag{5.18}$$

Pelas condições iniciais do problema, temos que

$$x + y + z = 100 \;\Rightarrow\; 39t - 19k = -3061. \tag{5.19}$$

Isto é, a soma das incógnitas da equação (5.13) é uma equação diofantina de incógnitas t e k. Para resolvê-la, observemos que $mdc(39,19) = 1$ e, pelo Algoritmo de Euclides,

$$39 \cdot 1 - 19 \cdot 2 = 1.$$

Dessa maneira,

$$39 \cdot (-3061) - 19 \cdot (-6122) = -3061.$$

Mostrando que $t_0 = -3061$ e $k_0 = -6122$ é uma solução particular de (5.19). Suas demais soluções são da forma

$$t = -3061 + 19\alpha \quad \text{e} \quad k = -6122 + 39\alpha, \tag{5.20}$$

com $\alpha \in \mathbb{Z}$. Agora, podemos substituir (5.20) em (5.18), vem que

$$x = -790 + 5\alpha, \quad y = 3062 - 19\alpha, \quad \text{e} \quad z = -2172 + 14\alpha.$$

Por hipótese, x, y e z devem ser positivos. Esta condição implica $159 \leq \alpha \leq 161$. Com isto, teremos três soluções para o problema:

$$x = 5, \quad y = 41 \quad \text{e} \quad z = 54,$$

$$x = 10, \quad y = 22 \quad \text{e} \quad z = 68, \quad \text{ou}$$

$$x = 15, \quad y = 3 \quad \text{e} \quad z = 82,$$

em que x, y e z são as quantidade de perus, patos e galinhas, respectivamente. △

Vejamos agora algumas aplicações da Aritmética Modular.

Exemplo 5.1.8 Determine o resto da divisão de 2^{2002} por 101.

Solução: Como 101 é um número primo, segue do Teorema de Fermat que:

$$2^{100} \equiv 1 \pmod{101}.$$

Pelas propriedades das congruências,

$$(2^{100})^{20} \equiv 1^{20} \pmod{101},$$

ou seja,

$$2^{2000} \equiv 1 \pmod{101}, \tag{5.21}$$

notemos que

$$2^2 \equiv 4 \pmod{101}. \tag{5.22}$$

Quando fazendo o produto de (5.21) por (5.22), determinamos a seguinte congruência:

$$2^{2000} \cdot 2^2 \equiv 1 \cdot 4 \pmod{101}.$$

Dessa forma,

$$2^{2002} \equiv 4 \pmod{101}.$$

Portanto, o resto é igual a 4. △

Exemplo 5.1.9 Um grupo teatral fez uma apresentação cultural, vendendo os ingressos com preço único de R$ 5,00. Sabendo-se que o valor arrecadado foi menor que R$ 10 000,00 e que esse valor foi dividido igualmente entre os 23 componentes desse grupo, restando R$ 7,00. Determine o público máximo presente nesse espetáculo.

Solução: Para resolver esse problema, devemos encontrar o maior múltiplo de 5 e menor que 10000, que ao ser dividido por 23 deixa resto 7. Com isso temos a seguinte congruência:

$$5x \equiv 7 \pmod{23}. \tag{5.23}$$

Esta congruência linear tem soluções inteiras, pois $mdc(5,23) = 1$. Pelo Teorema 4.3.3, sua soluçao geral é dada por

$$x = x_0 + (m/d)k,$$

em que $k \in \mathbb{Z}$ e x_0 é uma solução particular. É fácil ver que $x_0 = 6$ é uma solução desta cogruência. Por isso, sua solução geral é

$$x = 6 + 23k, \tag{5.24}$$

com $k \in \mathbb{Z}$. Pelas condições iniciais, o valor arrecadado é menor que R$ 10 000,00. Assim, devemos ter

$$5(6+23k) < 10000 \;\Rightarrow\; k \leq 86.$$

Como desejamos saber qual o público máximo, k deve assumir seu valor máximo. Substituindo $k = 86$ em (5.24), obtemos $x = 1984$. Portanto, 1984 pessoas é o público máximo nesse espetáculo. △

Exemplo 5.1.10 De acordo com o problema proposto por Sun-Tsu, enunciado no capítulo anterior, temos o seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases} \tag{5.25}$$

Solução: Como $mdc(3,5) = mdc(5,7) = mdc(3,7) = 1$, podemos aplicar o Teorema chinês dos restos para determinar as soluções desse problema clássico. De acordo com o Teorema, essas soluções são dadas pela expressão:

$$x = x_0 + kn, \quad k \in \mathbb{Z}, \tag{5.26}$$

em que

$$x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + c_3 r_3 N_3 \quad \text{e} \quad n = n_1 \cdot n_2 \cdot n_3. \tag{5.27}$$

No sistema em (5.25), temos:

$$c_1 = 2; \quad n_1 = 3; \quad c_2 = 3; \quad n_2 = 5; \quad c_3 = 2 \quad \text{e} \quad n_3 = 7.$$

Sejam

$$n = 3\cdot 5\cdot 7; \quad \text{e} \quad N_i = \frac{n}{n_i}; \quad i = 1,2,3.$$

Daí,

$$N_1 = \frac{3\cdot 5\cdot 7}{3} = 35; \quad N_2 = \frac{3\cdot 5\cdot 7}{5} = 21 \quad \text{e} \quad N_3 = \frac{3\cdot 5\cdot 7}{7} = 15.$$

Agora devemos encontrar os inteiros r_i, com $i = 1,2,3$, tais que

$$N_i r_i \equiv 1 \pmod{n_i}.$$

Ora,

$$\begin{aligned} 35r_1 &\equiv 1(\mathrm{mod}\,3) \Rightarrow 2r_1 \equiv 1(\mathrm{mod}\,3) \Rightarrow r_1 = 5, \\ 21r_2 &\equiv 1(\mathrm{mod}\,5) \Rightarrow r_2 \equiv 1(\mathrm{mod}\,5) \Rightarrow r_2 = 1, \\ 15r_3 &\equiv 1(\mathrm{mod}\,7) \Rightarrow r_3 \equiv 1(\mathrm{mod}\,7) \Rightarrow r_3 = 1. \end{aligned}$$

Agora, de acordo com (5.27), vem que

$$x_0 = 2\cdot 5\cdot 35 + 3\cdot 1\cdot 21 + 2\cdot 1\cdot 15 = 443.$$

Mas, visto que $n = 3\cdot 5\cdot 7 = 105$, temos $443 = 105\cdot 4 + 23$, ou seja

$$443 \equiv 23 \pmod{105}.$$

Dessa forma, de (5.26) $x = 23 + 105k$, com $k \in \mathbb{Z}$. Quando fazemos $k = 0$, obtemos $x = 23$, que é a solução apontada por Sun-Tsu. △

5.2 Parte II

Nesta segunda parte, iremos considerar problemas mais substaciais, menos elementares, que envolvem questões de divisibilidade mais avançadas.

Exemplo 5.2.1 Mostrar que 5 divide $222^{333} + 333^{222} - 1$.

Solução: A princípio não temos um resultado que nos conduza a uma congruência da forma

$$222^k \equiv 1 \pmod{5} \quad \text{ou} \quad 222^k \equiv -1 \pmod{5}.$$

Busquemos, pois, outro caminho. Como $222 = 5\cdot 44 + 2$, ou seja, $222 \equiv 2 \pmod{5}$, segue pelo item (3) do Teorema 4.1.5 que

$$222^{333} \equiv 2^{333} \pmod{5}. \tag{5.28}$$

Sendo $2^2 \equiv -1 \pmod{5}$, então pelo mesmo item,

$$(2^2)^{166} \equiv 1 \pmod{5} \Rightarrow 2^{332} \equiv 1 \pmod{5},$$

e como $222 \equiv 2 \pmod 5$, segue do item (2) que

$$2^{333} \equiv 2 \pmod 5. \tag{5.29}$$

Logo, de (5.28) e (5.29),

$$222^{333} \equiv 2^{333} \equiv 2 \pmod 5. \tag{5.30}$$

Vamos analisar agora 333^{222} módulo 5. Considerando que $333 \equiv 3 \pmod 5$, obtemos

$$333^{222} \equiv 3^{222} \pmod 5.$$

Por outro lado, $3^2 \equiv -1 \pmod 5$ implica $(3^2)^{111} \equiv -1 \pmod 5$, isto é,

$$333^{222} \equiv 3^{222} \equiv -1 \pmod 5. \tag{5.31}$$

Usando o item (1) do Teorema 4.1.5, obtemos de (5.30) e (5.31),

$$2^{333} + 3^{222} \equiv 1 \pmod 5,$$

o que mostra o resultado. △

Exemplo 5.2.2 *Mostre que* $1^n + 2^n + 3^n + 4^n \equiv 0 \pmod 5$ *se, e somente se,* $n \not\equiv 0 \pmod 4$.

Solução: Conideremos inicialmente que $1^n + 2^n + 3^n + 4^n \equiv 0 \pmod 5$. Sendo $\phi(5) = 4$, segue do Teorema de Euler que

$$2^4 \equiv 1 \pmod 5, \quad 3^4 \equiv 1 \pmod 5 \quad \text{e} \quad 4^4 \equiv 1 \pmod 5. \tag{5.32}$$

Façamos $n = 4k + r$, com $0 \leq r \leq 4$. Por absurdo, suponhamos que $r = 0$, ou melhor, $n = 4k$. Disto segue que

$$2^n \equiv 1 \pmod 5, \quad 3^n \equiv 1 \pmod 5 \quad \text{e} \quad 4^n \equiv 1 \pmod 5.$$

Por isso, visto que $1^n \equiv 1 \pmod 5$, temos

$$1^n + 2^n + 3^n + 4^n \equiv 4 \pmod 5,$$

de modo que, por transitividade, $4 \equiv 0 \pmod 5$, o que é uma contradição. Isto prova a primeira parte.

Reciprocamente, vamos supor que $n \not\equiv 0 \pmod 4$. Disto segue que $n = 4k + 1$, $n = 4k + 2$ ou $n = 4k + 3$. Se $n = 4k + 1$, então, considerando as congruências em (5.32), obtemos módulo 5 as congruências:

$$2^n \equiv 2, \quad 3^n \equiv 3, \quad 4^n \equiv 4.$$

Portanto,

$$1^n + 2^n + 3^n + 4^n \equiv 10 \equiv 0 \pmod 5.$$

Da mesma forma, para $n = 4k + 2$ e $n = 4k + 3$, obtemos respectivamente que

$$1^n + 2^n + 3^n + 4^n \equiv 30 \equiv 0 \pmod 5 \text{ e } 1^n + 2^n + 3^n + 4^n \equiv 120 \equiv 0 \pmod 5.$$

Isto conclui a prova. △

Exemplo 5.2.3 Consideremos a sequência de números naturais com termo geral dado por

$$a_n = 4^n - 3^n$$

para todo $n \geq 1$. Determinar a quantidade de múltiplos de 5 no conjunto

$$\{a_n : 1 \leq n \leq 502\}.$$

Solução: Pelo Teorema de Fermat, temos $4^4 \equiv 1 \pmod 5$ e $3^4 \equiv 1 \pmod 5$. Disto segue que $4^4 - 3^4 \equiv 0 \pmod 5$. Por outro lado, para cada inteiro $n \geq 1$, temos pelo Algoritmo da Divisão

$$n = 4q + r, \quad r = 0, 1, 2, 3.$$

Daí,

$$4^n = 4^{4q} \cdot 4^r \equiv 4^r \pmod 5.$$

Da mesma forma, tem-se $3^n \equiv 4^r \pmod 5$. Assim, para $r = 1, 2, 3$, obtemos

$$\begin{aligned} a_1 &= 4^1 - 3^1 \equiv 1 \pmod 5, \\ a_2 &= 4^2 - 3^2 \equiv 2 \pmod 5, \\ a_3 &= 4^3 - 3^3 \equiv 2 \pmod 5. \end{aligned}$$

Disto e da congruência $4^4 - 3^4 \equiv 0 \pmod 5$, concluímos que a_n é múltiplo de 5 se, e somente se, n é múltiplo de 4. Por fim, sendo $502 = 4 \cdot 125 + 2$, temos que, entre 1 e 502, existem 125 múltiplos de 4. Por conseguinte, existem 125 múltiplos de 5 no conjunto $\{a_n : 1 \leq n \leq 502\}$. △

Exemplo 5.2.4 Se p é um primo ímpar e

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b},$$

em que a e b são inteiros primos entre si, mostrar que $p \mid a$. Ademais, se $p \geq 5$, $p^2 \mid a$.

Solução: Como p é ímpar, segue que na soma

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

existe um número par de parcelas. Além disso, podemos somar duas a duas dessas parcelas afim de obtermos um padrão dessas somas. Senão vejamos. Temos

$$\begin{aligned} \frac{1}{1} + \frac{1}{p-1} &= \frac{p}{1 \cdot (p-1)}, \\ \frac{1}{2} + \frac{1}{p-2} &= \frac{p}{2 \cdot (p-2)}, \\ \frac{1}{3} + \frac{1}{p-3} &= \frac{p}{3 \cdot (p-3)}, \\ &\vdots \\ \frac{1}{(p-1)/2} + \frac{1}{(p+1)/2} &= \frac{p}{(p-1)/2 \cdot (p+1)/2}. \end{aligned}$$

Já que existem $(p-1)/2$ desses pares, segue que

$$\frac{a}{b} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \sum_{k=1}^{(p-1)/2} \frac{p}{k \cdot (p-k)}.$$

Daí,

$$p \mid a(p-1)(p-2)\ldots\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)!.$$

Como p não divide $(p-k)$ para cada $k = 1, \ldots, (p-1)/2$, e nem divide $((p-1)/2)!$, concluímos que $p \mid a$. Isto prova a primeira parte. Vejamos agora a segunda.

Seja $p \geq 5$ e consideremos o polinômio

$$f(x) = (x-1)(x-2)\ldots(x-(p-1)).$$

Mostra-se que os coeficientes de $f(x)$ são múltiplos de p, excluindo o coeficiente líder e o termo independente. Façamos

$$f(x) = x^{p-1} + \sum_{i=0}^{p-2} a_i x^i.$$

Como $p \geq 5$, temos $p \mid a_2$ e, por isso,

$$f(p) \equiv (a_0 + a_1 p) \pmod{p^3}.$$

Verifica-se que $f(x) = (-1)^{p-1} \cdot f(p-x)$ e $p-1$ é par. Por conseguinte, $f(x) = f(p-x)$ e, desse modo,

$$a_0 = f(0) = f(p) \equiv (a_0 + a_1 p) \pmod{p^3},$$

ou seja,

$$a_1 p \equiv 0 \pmod{p^3},$$

de maneira que $p^2 \mid a_1$, isto é, $a_1 = p^2 k$ para algum inteiro k. Por outro lado, é fácil verificar que a soma $1 + 1/2 + 1/3 + \cdots + 1/(p-1)$ é exatamente igual a $a_1/(p-1)! = a/b$. Daí,

$$a(p-1)! = a_1 b = p^2 k b \;\Rightarrow\; p^2 \mid a(p-1)!.$$

Já que p é primo e não divide $(p-1)!$, concluímos que $p^2 \mid a$. △

O próximo exemplo que retrata uma propriedade interessante da função $\tau(n)$ em que $\tau(n)$ indica a quantidade de divisores positivos de n. Para tanto, lançaremos mão do seguinte fato: se $n = a \cdot b$, com $1 < a, b < n$, então

$$a \leq \sqrt{n} \quad \text{ou} \quad b \leq \sqrt{n}. \tag{5.33}$$

Exemplo 5.2.5 Para qualquer inteiro $n \geq 1$, mostrar que $\tau(n) \leq 2\sqrt{n}$, em que $\tau(n)$ indica a quantidade de divisores positivos de n.

Solução: Seja d um divisor positivo qualquer de $n \geq 1$. De acordo com (5.33), $d \leq \sqrt{n}$ ou $n/d \leq \sqrt{n}$. Sejam $d_1, d_2, \ldots, d_k$ todos os divisores positivos de n, com $d_1 < d_2 < \cdots < d_k$. Nestas condições, temos que $d_1 = 1$ e $d_k = n$. Como d_i é um divisor de n, n/d_i também o é. Isto significa que n/d_i deve ser um dos d_i's. Vamos emparelhar os divisores d_i e d_j de modo que $n = d_i d_j$, ou seja, $d_j = n/d_i$. É claro que, para cada $i = 1, \ldots, k$, $d_i \leq d_j$ ou $d_j \leq d_i$. Consideremos dois casos separadamente.

(1) Se k é par, então existem $k/2$ pares de divisores (d_i, d_j), com $d_i \neq d_j$ e $n = d_i d_j$. Para cada um desses pares, vamos supor, sem perda de generalidade, que $d_i < d_j$. Entre os divisores d_i's, seja d_s o maior deles[1]. Já que existem únicos $k/2$ pares nas condições descritas, devemos certamente ter $k/2 \leq d_s$. Desse modo, como $\tau(n) = k$ e $d_s \leq \sqrt{n}$, obtemos

$$\frac{\tau(n)}{2} \leq d_s \leq \sqrt{n},$$

ou seja, $\tau(n) \leq 2\sqrt{n}$.

(2) Se k é ímpar, então existem $(k+1)/2$ pares de divisores (d_i, d_j), com $n = d_i d_j$. Entre esses pares, existe um único par da forma (d_r, d_r), em que $n = d_r d_r$. Para os demais pares, num total de $(k-1)/2$, vamos supor, assim como no primeiro caso, que $d_i < d_j$. Da mesma forma, seja d_s o maior entre os divisores[2] d_i's. Isto implica $d_s < d_r$. De fato, se $d_r \leq d_s$, seja d_j o divisor associado a d_s. Assim, por construção, $d_s < d_j$ e $d_s d_j = n$. Daí, $d_r < d_s$ e $d_r < d_j$, de maneira que

$$n = d_r d_r \leq d_s d_r \quad \text{e} \quad d_s d_r < d_s d_j = n,$$

isto é, $n < n$, o que é uma contradição. Portanto, $d_s < d_r$.

Assim como no primeiro caso, $(k-1)/2 \leq d_s$ e $\tau(n) = k$. Logo, já que $d_r^2 = n$, ou melhor, $d_r = \sqrt{n}$,

$$\frac{\tau(n) - 1}{2} \leq d_s < d_r = \sqrt{n},$$

o que implica $\tau(n) - 1 < 2\sqrt{n}$ e, por conseguinte, $\tau(n) \leq 2\sqrt{n}$. Portanto, para ambos os casos, temos sempre $\tau(n) \leq 2\sqrt{n}$. △

Exemplo 5.2.6 Sejam p e q primos distintos tais que $a^p \equiv a \pmod{q}$ e $a^q \equiv a \pmod{p}$. Então, $a^{pq} \equiv a \pmod{pq}$.

Solução: Do Corolário 4.2.2,

$$(a^q)^p \equiv a^q \pmod{p}.$$

[1]Por exemplo, se $n = 12$, $D_{12} = \{1,2,3,4,6,12\}$. Daí, existem três pares de divisores (d_i, d_j), com $d_i < d_j$ e $12 = d_i d_j$. O conjunto dos d_i's é $\{1,2,3\}$; disto segue que $d_s = 3$.

[2]Por exemplo, se $n = 36$, $D_{36} = \{1,2,3,4,6,9,12,18,36\}$, ou seja, $k = 9$. Existem $5 = (9+1)/2$ pares de divisores, dentre os quais, quatro são da forma (d_i, d_j), com $d_i < d_j$, que são $(1,36)$, $(2,18)$, $(3,12)$ e $(4,9)$ e, neste caso, $d_s = 4$; há também um único par da forma (d_r, d_r), que é o par $(6,6)$.

Como $a^q \equiv a \pmod{p}$, segue por transitividade que $a^{pq} \equiv a \pmod{p}$, ou seja, $p \mid a^{pq} - a$. Da mesma forma, $q \mid a^{pq} - a$. Mas, sendo $mdc(p,q) = 1$, temos que $pq \mid a^{pq} - a$, isto é, $a^{pq} \equiv a \pmod{pq}$. △

Por exemplo, vamos considerar $a = 2$ e os primos $p = 11$ e $q = 31$. Uma vez que $2^{10} = 1024 = 31 \cdot 33 + 1$, temos $2^{10} \equiv 1 \pmod{31}$, de modo que

$$2^{11} \equiv 2 \pmod{31}. \tag{5.34}$$

Também, $2^{10} = 1024 = 11 \cdot 93 + 1$ e, assim, $2^{10} \equiv 1 \pmod{11}$. Logo,

$$2^{31} \equiv 2 \pmod{11}. \tag{5.35}$$

Portanto, pelo exemplo anterior, com $a = 2$, obtemos de (5.34) e (5.35) que

$$2^{11 \cdot 31} \equiv 2 \pmod{11 \cdot 31},$$

ou melhor, $2^{341} \equiv 2 \pmod{341}$. Mais ainda, já que $mdc(2,341) = 1$, podemos cancelar o fator 2 desta congruência, de modo a obter

$$2^{340} \equiv 1 \pmod{341}.$$

Considerando que 341 não é primo, a última congruência nos mostra que a recíproca do Teorema de Fermat não é válida.

O fato $341 \mid 2^{341} - 2$ contraria uma conjectura feita por matemáticos chineses mais de 25 séculos atrás que afirmava que n é primo se, e somente se, $n \mid 2^n - 2$. Algo semelhante ocorre com outros números composto, o que nos conduz a seguinte:

Definição 5.2.7 (Pseudoprimo) *Um número composto n é chamado **pseudoprimo** quando $n \mid 2^n - 2$.*

Existem infinitos pseudoprimos, sendo que os quatro menores são 341, 561, 645 e 1105. Especificamente, uma família infinita de pseudoprimos é obtida do seguinte:

Teorema 5.2.8 *Se $p > 3$ é primo, então*

$$n = (2^{2p} - 1)/3 = (2^p - 1)(2^p + 1)/3$$

é um pseudoprimo.

Demonstração: Pelo Corolário 4.2.2, segue que $2^p \equiv 2 \pmod{p}$. Assim,

$$2^p - 1 \equiv 1 \pmod{p} \quad \text{e} \quad 2^p + 1 \equiv 3 \pmod{p},$$

e já que $3 \mid 2^p + 1$, pois $2^p + 1 = 3(2^{p-1} - 2^{p-2} + \cdots + 1)$, concluímos que $(2^p + 1)/3 \equiv 1 \pmod{p}$. Sendo $2^p - 1$ e $2^p + 1$ ímpares, temos

$$2^p - 1 = 1 + pk_1 \quad \text{e} \quad 2^p + 1 = 3 + pk_2,$$

em que k_1 e k_2 são pares, com $6 \mid k_2$, digamos $k_1 = 2\theta_1$ e $k_2 = 6\theta_2$. Desse modo,

$$\begin{aligned} n &= (2^p-1)(2^p+1)/3 &&= (1+pk_1)(3+pk_2)/3 \\ &&&= (1+2p\theta_1)(3+6p\theta_2)/3, \end{aligned}$$

ou seja, $n = 1+2pk$, com $k \in \mathbb{Z}$. Visto que $n = (2^{2p}-1)/3$, obtemos

$$2^{2p} \equiv 1 \pmod{n} \;\Rightarrow\; 2^{2pk} \equiv 1 \pmod{n},$$

de modo que $2^{2pk+1} \equiv 2 \pmod{n}$, ou melhor, $2^n \equiv 2 \pmod{n}$. □

Por exemplo,

$$\begin{aligned} p &= 5 \;\Rightarrow\; n &&= (2^{2p}-1)/3 &&= 341, \\ p &= 7 \;\Rightarrow\; n &&= (2^{2p}-1)/3 &&= 5461, \\ p &= 11 \;\Rightarrow\; n &&= (2^{2p}-1)/3 &&= 1398101 \end{aligned}$$

são todos pseudoprimos. Nota-se que 561, 645 e 1105 não pertencem à família dos pseudoprimos obtidos por $n = (2^{2p}-1)/3$.

Referências Bibliográficas

[1] EUCLIDES. *Os elementos/Euclides*; tradução e introdução de Irineu Bicudo. UNESP, São Paulo, 2009.

[2] FILHO, E. A. *Teoria Elementar dos Números.* São Paulo, 1981.

[3] HEFEZ, A. *Elementos de Aritmética.* 2^a ed. Rio de Janeiro, SBM, 2011.

[4] OLIVEIRA, A. M; SILVA, Agostinho. *Biblioteca da Matemática Moderna.* 2^a ed. LISA:livros irradiantes s.a. , 2011.

[5] MINISTERIO DA EDUCAÇÃO. *Parâmetros Curriculares Nacionais.* Ciências da Natureza, Matemática e suas Tecnologias. Disponivel em: <http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf> Acesso em 31 de outubro de 2018.

[6] MINISTERIO DA EDUCAÇÃO. *Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais.* Ciências da Natureza, Matemática e suas Tecnologias. Disponivel em: <http://portal.mec.gov.br/seb/arquivos/pdf/CienciasNatureza.pdf>. Acesso em 31 de outubro de 2018.

[7] RIBENBOIM, P. *Números Primos: Velhos Mistérios e Novos Recordes*. IMPA, CMU, Rio de Janeiro, 2012.

[8] VIEIRA, V. L. *Um Curso Básico em Teoria dos Núneros.* Editora da Universidade Estadual da Paraíba (Co-edição: Livraria da Física), Campina Grande/São Paulo, 2015.

[9] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura.* 2^a ed. Editora da Universidade Estadual da Paraíba (Co-edição: Livraria da Física), Campina Grande/São Paulo, 2015.