Universidade Estadual da Paraíba
Campus I Campina Grande
Centro de Ciências e Tecnologia
Departamento de Matemática
Mestrado Profissional em Matemática em Rede Nacional

Raimundo João dos Santos Júnior

Números Perfeitos e Amigáveis

Campina Grande - PB
Março/2020

Raimundo João dos Santos Júnior

Números Perfeitos e Amigáveis

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.

Orientador: Prof. Dr. Vandenberg Lopes Vieira

Campina Grande - PB
Março/2020

S237n Santos Júnior, Raimundo João dos.
Números perfeitos e amigáveis [manuscrito] / Raimundo João dos Santos Júnior. - 2020.
68 p.
Digitado.
Dissertação (Mestrado em Profissional em Matemática em Rede Nacional) - Universidade Estadual da Paraíba, Pró-Reitoria de Pós-Graduação e Pesquisa , 2020.
"Orientação : Prof. Dr. Vandenberg Lopes Vieira , Departamento de Matemática - CCT."
1. História da Matemática. 2. Teoria dos números. 3. Números perfeitos. 4. Números amigáveis. I. Título
21. ed. CDD 512.7

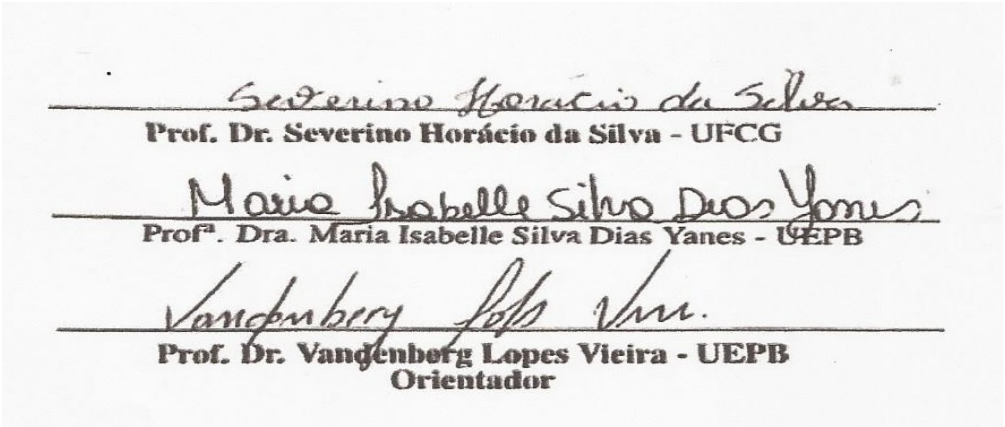
Elaborada por Giulianne M. Pereira - CRB - 15/714 BC/UEPB

Raimundo João dos Santos Júnior

Números Perfeitos e Amigáveis

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de Mestre.

Aprovada em: 06/03/2020



Dedicatória

Dedico este trabalho a minha família. Exemplos incontestáveis de dedicação e empenho. Sem o apoio dela eu nunca teria chegado até aqui.

Agradecimentos

Todas as pessoas que conhecemos ao longo da nossa vida nos deixam marcas. Sejam exemplos a serem seguidos ou posturas a serem repudiadas. De uma forma ou de outra aprendemos com todos. Dividirei os meus agradecimentos as diversas pessoas e grupos que me possibilitaram ser quem sou hoje.

Obrigado **Deus** pela dádiva da vida, por estar ao meu lado em todos os momentos que me senti sozinho, incapaz, insuficiente e triste; bem como os momentos de felicidade, paz, harmonia e amor. Sentir a tua presença em todos os momentos é nunca se afastar do verdadeiro amor.

Agradeço a minha **Família** por todo amor, carinho e proteção que me foram dados desde o meu nascimento até hoje. Agradeço ao meu pai **Raimundo** pelas diversas tardes em que, mesmo interrompendo seu trabalho, sempre me ajudava nos deveres de matemática, esse foi o começo do meu gosto e apreço pela ciência. Agradeço a minha mãe **Maria do Carmo** que sempre se esforçou ao máximo trabalhando de sol a sol, para nos dar uma vida confortável, a senhora é o meu maior exemplo do que é ser professor. Também agradeço ao meu irmão **Antônio Cassio**, um acadêmico brilhante desde a juventude, obrigado por todos os ensinamentos até hoje.

Agradeço aos diversos professores que conheci durante toda a minha vida, desde o ensino básico até a pós-graduação. Em especial agradeço aos professores **Shelliton Santiago, Tássio Tavares** e **Gelder Golçalves** que me impulsionaram a estudar matemática no Ensino Básico, tenho orgulho de ser colega de profissão desses homens.

Também agradeço a banca avaliadora desse trabalho pelas contribuições que certamente serão feitas. Um agradecimento especial ao professor **Vandenberg Lopes Vieira** por toda paciência e compreensão durante essa orientação.

Estendo meus agradecimentos também aos companheiros de curso **Maxwell Aires da Silva** e **Állisson Herinque Leite Cabral** pelas incontáveis horas de estudo em grupo. Obrigado por não me deixarem desistir e por acreditarem na minha capacidade mais do que eu mesmo em muitos momentos.

Gostaria também de agradecer a todos os meus alunos, eu leciono desde 2011 como professor de reforço e até hoje encontro neles um apoio e força para continuar trabalhando com foco e buscando a melhora a cada dia. Saber que posso desmistificar a matemática para eles e transmitir o amor que eu sinto através das minhas aulas me faz ser uma pessoa melhor.

Obrigado *Brotherhood, Barbarian Badgers* e *Associação Shibumi* por estarem lá sempre que eu precisei.

Por fim, agradeço Sociedade Brasileira de Matemática - SBM, pelo oferecimento deste Curso em Rede Nacional e à Universidade Estadual da Paraíba - UEPB, pelo oferecimento do programa em seus domínios.

Epígrafe

A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas. (Gauss)

Resumo

Os números perfeitos, bem como os números amigáveis, começaram a ser estudados pela escola pitágorica e até os dias atuais despertam a curiosidade de muitos teóricos dos números. Apesar de serem tópicos relativamente simples, no sentido de considerar conceitos elementares, como divisores e a função $\sigma(n)$ soma de divisores, ainda existem alguns problemas em aberto inerentes, e isto tem motivado cada vez mais estudiosos a desenvolverem técnicas mais substanciais a fim de encontrar uma solução satisfatória para cada desses problemas. Neste trabalho, consideramos algumas propriedades relativas a estes números, abordando, de forma especial, o teorema central que caracteriza os números perfeitos pares, uma estreita relação desses números com os primos de Mersenne. Consideramos, também, alguns problemas que são clássicos do assunto com suas respectivas soluções.

Palavras Chaves: História da Matemática. Teoria dos Números. Números Perfeitos. Números Amigáveis.

Abstract

The perfect numbers, as well as the friendly numbers, began to be studied by the pythagorean school and up to the current days they wake the curiosity of many theoreticians of the numbers. In spite of being relatively simple topics, in the sense of finding elementary concepts, like dividing and function $\sigma(n)$ a sum of divisors, there are still some problems when in it was opened inherent, and this has been causing more and more scholars to develop more substantial techniques in order to find a satisfactory solution for each of these problems. In this work, we consider some relative properties to these numbers, boarding, in a special form, the central theorem that characterizes the perfect equal numbers, a narrow relation of these numbers with the cousins of Mersenne. We consider, also, some problems that are classics of the subject with its respective solutions.

Keywords: History of Mathematics. Number's Theory. Perfect Numbers. Friendly Numbers.

Sumário

Capítulo 1

Introdução

Os números, como conhecemos hoje em dia, são utilizados em todas as áreas da Matemática, em outras ciências e também por toda a população em suas atividades diárias. Entretanto, seu conceito é mais amplo e era utilizado séculos antes do desenvolvimento da linguagem simbólica, até mesmo antes da linguagem escrita. Vejamos a seguir um pouco da origem e evolução, da representação e utilização, dos números ao longo do tempo.

1.1 Da Idade Antiga às Primeiras Civilizações

O homo sapiens (homem que sabe) começou a ocupar a terra por volta de 30.000 a.C; eles viviam em pequenas tribos nômades que obtinham alimento da caça e da coleta. As ideias matemáticas nesse período se resumiam apenas a compreender se o local era adequado para a tribo, no sentido da obtenção de recursos para a subsistência, para a criação de algumas ferramentas simples, principalmente para facilitar a própria caça, na preparação de alimentos e na ótica da medição do tempo.

Por volta de 3.000 a.C, a humanidade começou a abandonar a fase conhecida como Idade da Pedra[1], por meio da primeira reforma agrícola que ocorreu no globo terrestre. Os estudiosos creditam essa evolução às mulheres, que passavam a maior parte de seu tempo nos acampamentos sazonais das tribos, cuidando das crianças e guardando o assentamento. Com o passar do tempo, elas começaram a entender como tratar, tanto dos grãos para o plantio, como dos animais para a criação. Isso levou os humanos a deixarem gradativamente de ser nômades, de modo a se estabelecerem definitivamente em locais convenientes, como perto de rios, pois, facilitaria a obtenção de água, além da terra fértil a disposição.

Com essa nova postura adotada pela humanidade, os números foram ficando cada vez mais necessários, sejam para contagem de tempo que a plantação demorava para chegar a fase de colheita, como para verificar se a quantidade de animais da criação estava sofrendo

[1] A Idade da Pedra foi deixada para trás nas maiores partes do Oriente Médio, África e Ásia. Na América e em regiões mais isoladas do mundo, em relação a essas, demoraram alguns séculos a mais para ocorrer essa mudança.

alterações. Graças a ausência do simbolismo para representar os números, essas contagens eram feitas por meio de associação, em que, cada elemento a ser contado era relacionado a um nó em uma corda, uma marcação feita em madeira, pedra e até mesmo ossos. Atualmente, esse tipo de associação é chamada *relação biunívoca* e é um conceito básico utilizado em todos os campos da Matemática.

As primeiras cidades se formaram próximas a rios, como o Tigre e o Eufrates (no Oriente Médio) e o Nilo (na África), respectivamente. Com o estabelecimento delas, começaram a se desenvolver novas estruturas, físicas e sociais. Por exemplo, a criação de um sistema comercial, a construção de sistemas de irrigação e a evolução das construções urbanas. Essas novas características sociais necessitavam mais do que as ideias primitivas de contagem que existiam. Desse modo, foi necessária uma evolução do pensamento matemático, chegando a uma representação simbólica primitiva dos números; era o começo da Matemática simbólica, que é a que estudamos até os dias atuais.

As principais civilizações desta época foram a babilônica, a egípcia e a grega. Existiram outras, porém, suas formas de registros eram mais perecíveis e acabaram se perdendo ao longo dos séculos. A Matemática e o uso dos números foram se aprimorando cada vez mais nessas civilizações, como veremos a seguir.

1.2 Babilônia

No século XIX, foram escavadas inúmeras tábuas de argila na região da Mesopotâmia, Antiga Babilônia[2]. Nessas tábuas, os povos da Antiga Babilônia faziam os registros de suas atividades diárias e, muitas delas, foram identificadas como sendo puramente sobre Matemática. O sistema de numeração desenvolvido por este povo era composto de 60 dígitos, possuindo apenas dois símbolos distintos, um para representar as unidades e outro para as dezenas, conforme a Figura 1.1.

Os problemas que são tratados nessas tábuas são referentes ao dia a dia; neles estão expressos cálculos de operações envolvendo situações financeiras (multiplicação, divisão, juros simples e compostos, exponenciais) e problemas geométricos, relacionados à construção civil, aspectos da agricultura e criação de animais. Em tábuas um pouco menos antigas, existem resoluções de equações do segundo grau, até mesmo do terceiro e do quarto graus (biquadradas), além de aproximações bastante convincentes para números irracionais, como $17/12$, uma aproximação de $\sqrt{2}$.

Uma placa bastante intrigante é a Plimpton 322 (Figura 1.2) que, apesar de parcialmente danificada, nos revela algo muito interessante para a época. Composta por quatro colunas, a mais à direita é apenas para enumerar as linhas, e as outras três, salvo por

[2]O termo se refere a todos os povos que habitaram a região de 2100 A.c até por volta de 300 D.c. Para mais recomendamos a referência [1].

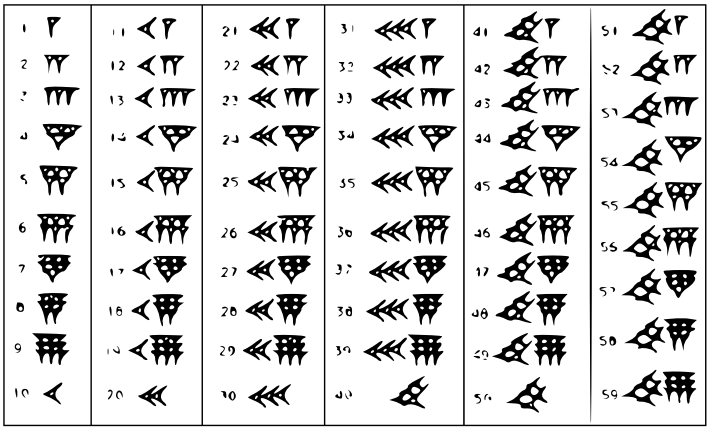


Figura 1.1: Sistema de Numeração Babilônico.

poucas exceções, formam ternos pitagóricos[3]. Para essas exceções, não sabemos ao certo se são realmente erros, ou incoerências no processo de tradução dos símbolos originais. Entretanto, é inegável que essa civilização conseguiu transcender a noção intuitiva de número, ao longo de alguns séculos de evolução social, para uma mais abstrata.

1.3 Egito

A região em que se localiza o Egito possibilitou a existência de uma sociedade bem diferente da babilônica, pois, graças ao ambiente desértico, o Egito era, de difícil acesso a outros povos, o que dificultava invasões e relações comerciais. Esse quadro possibilitou um poder continuado de dinastias da própria região. O resultado disso foi que a Matemática egípcia não se desenvolveu tal como a babilônica, principalmente pela falta de integração com outros povos.

Essa sociedade era prioritariamente teocêntrica[4], com os nobres teocráticos no poder e os escravos responsáveis pela manutenção dos sistemas sociais. Por exemplo, cuidavam das plantações, dos sistemas de irrigação e executavam as construções, como as notórias pirâmides do Egito. Semelhante ao conhecimento babilônico, os conhecimentos matemáticos eram unicamente relacionados com as questões necessárias para a sociedade, não existindo um estudo voltado à teoria da ciência.

Segundo Eves (2008), a Matemática egípcia foi estudada anteriormente à babilônica,

[3]Ternos pitagóricos são inteiros (x,y,z) tais que $x^2+y^2=z^2$.

[4]Teocentrismo é uma crença de que Deus/deuses são o centro de tudo.

Figura 1.2: Placa Plimpton 322.

pois seus escritos mantinham um mesmo tipo de escrita, graças a ausência da influência cultural de outros povos. Esses conhecimentos também ficaram preservados nas paredes das pirâmides e em papiros que, graças ao clima da região, resistiram bem ao tempo.

Documentos importantes sobre o conhecimento matemático dessa época são os papiros Moscou e o Rhind. O primeiro se encontra no Museu de Belas Artes de Moscou, e o segundo no Museu Britânico. O papiro Moscou é um compilado de problemas ainda mais antigos do que sua origem (aproximadamente 1850 a.C), enquanto o Rhind é um importante apanhando de técnicas operacionais utilizadas pelos egípcios em seu sistema de numeração.

Esses papiros começaram a ser traduzidos com a posse de um fragmento basáltico que continha escritos egípcios e gregos, fazendo a ponte entre as duas escritas. Diante disso, foi possível a tradução dos papiros egípcios, inclusive os papiros Moscou e Rhind. Para mais informações sobre o conhecimento operacional e problemas provindos dos papiros, e as situações históricas em que eles foram descobertos, sugerimos a leitura de [1].

1.4 Grécia

A leste do mar Mediterrâneo se encontra uma das regiões na qual ocorreu a evolução social de mais alto grau de complexidade para a época. A Grécia, durante o período Helênico (800-336 a.C), foi o polo mundial da sociedade. As cidades-estado, cada qual com suas particularidades, impulsionaram um desenvolvimento ímpar na região, tanto social, como bélico e intelectual. Nessa sociedade, surgiram diversos pensadores importantes para toda

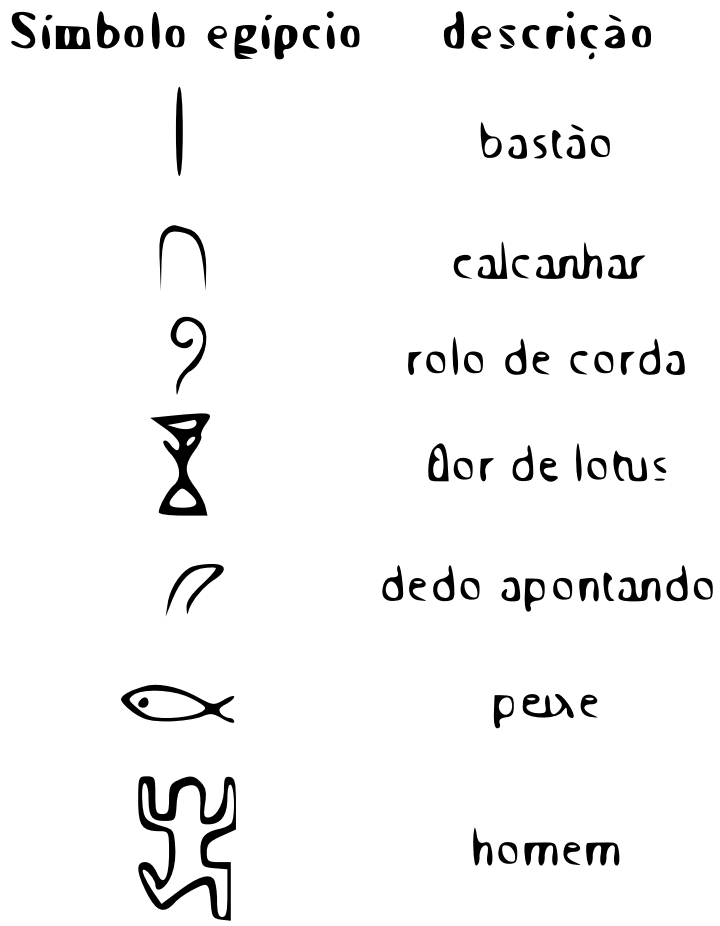


Figura 1.3: Símbolos do Sistema de Numeração Egípcio.

a humanidade, estudados até nos dias atuais, que fundamentaram os primeiros passos do conhecimento teórico e do raciocínio científico.

A evolução das cidades e do comércio trouxeram mudanças significativas para a sociedade, o que motivou as pessoas a pensarem mais e se questionarem acerca de suas decisões, principalmente com o objetivo de ascensão pessoal dentro da sociedade. Não bastava mais apenas encontrar soluções para os problemas, mas saber se essas soluções são únicas, se elas são as mais práticas, ou ainda, analisar em quais outros problemas elas também podem ser úteis.

Essa mudança de pensamento da sociedade levou a evoluções em todas as áreas do conhecimento cientifico. Nessa época, surgiram os primeiros estudos teóricos que atualmente constituem a *Teoria dos Números*. Os protagonistas principais desta área científica da Matemática, nesta época, foram: Euclides, Pitágoras e Diofanto.

Euclides (aproximadamente 350 A.c) escreveu uma das obras matemáticas consideradas mais importantes até a atualidade. Os *elementos* é um trabalho genial, composto por 13 livros, que condensa o conhecimento matemático da época de maneira sistemática. Três desses se dedicam aos números e suas propriedades, principalmente ao cálculo de máximo divisor comum, a determinação de primalidade e a demonstração da infinidade do conjunto dos primos (veremos no Capítulo 3 a demonstração da infinidade desse conjunto, originalmente encontrada na obra de Euclides).

Pitágoras (569-500 a.C) viajou o mundo e aprendeu as técnicas matemáticas dominadas por estudiosos de várias localidades. Após isso, Pitágoras se questionou se a matemática se resumia apenas a técnicas operatórias, ou se existia algo mais a ser descoberto. Partindo disso, começou a investigar padrões, propriedades numéricas e geométricas. Pitágoras foi fundador da famosa escola pitagórica, uma irmandade que buscava o conhecimento acima de tudo. A irmandade realizou diversos estudos, entre eles, sobre números primos, números perfeitos, e aplicações da matemática, como a teoria musical, por exemplo.

Um dos teoremas mais conhecidos da matemática, até os dias atuais, é creditado a Pitágoras. O famoso Teorema de Pitágoras trata da relação entre os lados inteiros de um triângulo retângulo, os inteiros que verificam a igualdade $x^2 + y^2 = z^2$. O número representado pela letra z é o maior lado do triângulo, chamado *hipotenusa.* Já x e y são chamados *catetos*. Para mais sobre Pitágoras, e seu tão famoso teorema, sugerimos a leitura de [2].

Diofanto (aproximadamente 250 d.C) foi um estudioso que até hoje tem parte de sua vida pessoal como um enigma. Seu foco de estudo eram problemas que admitiam apenas soluções inteiras, tanto que, esse tipo de problema é conhecido como problemas de Diofanto ou problemas Diofantinos.

Uma grande contribuição para os futuros matemáticos deixada por Diofanto foi a sua obra intitulada *Arithmetica*, que dispõe do conhecimento e dos estudos dele sobre números, suas propriedades e problemas. Essa obra, junto com o conhecimento científico da época, ficou esquecida durante a Idade Média, também conhecida como *Idade das Trevas*. Com o advento do *Renascimento Cultural*[5], a obra de Diofanto foi redescoberta, e ganhou a atenção de estudiosos dessa época, por exemplo, Pierre Fermat.

1.5 Fibonacci, Mersenne, Fermat e Euler

Durante o período da Idade Média, a sociedade não teve grandes avanços científicos. A Matemática era usada apenas para cálculos triviais e para o uso do calendário. Por volta do século XIII, alguns estudiosos se destacaram. Ressaltaremos um em especial.

Leonardo Fibonacci (1170-1240) era filho de comerciantes, por isso, teve sua vida

[5]Período pós Idade Média em que o conhecimento científico foi redescoberto pela sociedade.

dividida entre vários centros comerciais do mundo, o possibilitando ter contato com diversas técnicas de calcular, sistemas de numeração e instrumentos para realizar operações voltadas ao comércio.

Fibonacci ficou conhecido principalmente pela sua obra *Liber Abaci,* que apresenta o sistema indo-arábico para à grande massa europeia. A facilidade em realizar operações desse sistema, em relação aos sistemas de numeração utilizados até então, fez com que ele fosse adotado pela maioria da população, e é usado até os dias atuais em todo o mundo, com pequenas alterações. Fibonacci também ficou conhecido pelo problema da reprodução de coelhos, que deu luz à *sequência de Fibonacci*, que possui uma estreita relação com à *razão áurea*. A contribuição de Fibonacci foi imensa neste período de baixa produtividade Matemática, pois simplificou bastante processos operatórios massantes, o que auxiliou a releitura do conhecimento grego, que viria a ser redescoberto poucos séculos no futuro, por meio do Renascimento Cultural.

Durante o século XVI, na tensão do Renascimento Cultural, o religioso Marin Mersenne (1588-1648) defendia a ciência e o conhecimento, ao invés de tratá-los como uma heresia. Mersenne era um difusor de informações Matemáticas da época, relacionando conhecimentos de diferentes estudiosos, como Pierre Fermat e Blaise Pascal. Esse trabalho de correspondência, mesmo que indiretamente, motivou, no futuro, a reunião de matemáticos em congressos e outros eventos que até hoje tem essa finalidade, difundir conhecimento entre a sociedade matemática.

Pierre Fermat (1601-1665) foi um estudioso amador da matemática. Tinha outra ocupação, entretanto, a sua produção foi tão significativa que o fez ser conhecido como *O príncipe dos Amadores*. Ele estudava com uma cópia do livro escrito por Diofanto e usava as largas margens de suas páginas para fazer anotações que, após sua morte, foram publicados por seu filho. Fermat, enquanto estudioso, não se preocupava em documentar detalhadamente os seus feitos. Ele se correspondia com outros matemáticos de uma maneira voltada a desafiá-los, e não para compartilhar conhecimento. Tanto que, um problema levantado por Fermat demorou mais de três séculos para ser resolvido, o *Último Teorema de Fermat*. Outros problemas, em sua época, foram estudados por diversos matemáticos, mas, por diversas vezes eles não conseguiam resolvê-los. Para uma abordagem mais especifica sobre Fermat, sua história e, principalmente, seu ultimo teorema, recomendamos a leitura de [3].

Leonard Euler (1707-1783) teve sua vida sempre centrada nos estudos; primeiramente em teologia e depois, por influência da famosa família de matemáticos Bernoulli, em Matemática. Graças a essa relação com os Bernoulli, Euler teve excelente formação e logo começou a escrever diversos trabalhos sobre matemática, que ganharam muita visibilidade na época.

A matemática desse século (XVIII), após a influência de Isaac Newton, voltou-se a questões mais práticas, como por exemplo, à de resolver problemas da sociedade

contemporânea, de saneamento básico, de navegação, do comércio, dentre outros. O primeiro trabalho publicado de Euler foi sobre problemas envolvendo mastreação de navios. Outro problema prático, este que originou a *Teoria dos Grafos*, foi o da *Ponte de Königsberg* (cf. Figura 1.4). Ambos foram produzidos com o objetivo de resolver problemas sociais da época.

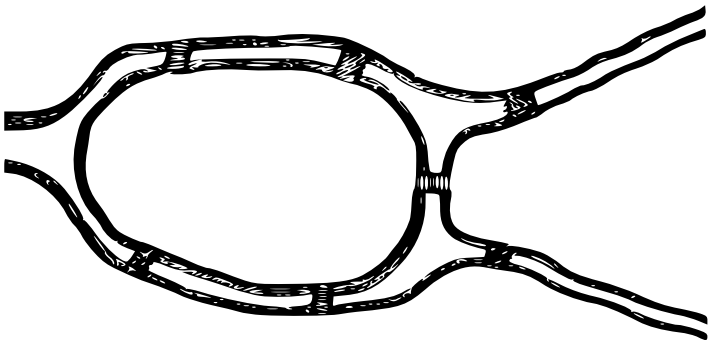


Figura 1.4: Ponte de Königsberg.

Ao longo dos anos, Euler perdeu a visão. Após isso, por incrível que pareça, intensificou seu trabalho. Seu poder de concentração e capacidade de memorização o auxiliaram nesse período. É comum para qualquer estudante de matemática, com um conhecimento básico, estudar algum dos resultados que são creditados a Euler.

Euler desenvolveu pesquisas em diversas áreas da matemática: Matemática Aplicada, Equações Diferenciais e Teoria dos Números, por exemplo. Até a atualidade, ele é considerado o matemático mais prolífero de todos, graças à quantidade e a qualidade do conhecimento desenvolvido por ele.

O Trabalho está dividido da seguinte maneira: no Capítulo 2, consideramos alguns resultados sobre divisibilidade e outros básicos inerentes, tais como o Algoritmo da Divisão e o Máximo Divisor Comum. No Capítulo 3, destacamos números primos, destacando resultados básicos; em especial, consideramos o Teorema Fundamental da Aritmética, o principal teorema da Teoria dos Números. Consideramos, também, as principais propriedades da relação de congruência módulo m, a base da aritmética modular. Por fim, no Capítulo 4, apresentamos resultados clássicos que versam sobre números perfeitos e amigáveis, entre os destacamos a caracterização dos números perfeitos pares e o método de Thabit para a obtenção de pares de números amigáveis. Aproveitamos este capítulo para, de forma adicional, solucionar alguns exemplos, propostos em livros-texto do componente Aritmética/MA14, obrigatório do Profmat.

Capítulo 2

Preliminares

Neste capítulo, vamos considerar alguns resultados iniciais que são necessários para o desenvolvimento do trabalho. Admitiremos que o leitor tenha conhecimentos básicos sobre as principais propriedades referentes às operações de adição e multiplicação usuais sobre o conjunto $\mathbb{Z}$ dos números inteiros,

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

como também sobre dois princípios matemáticos: o Princípio da Boa Ordenação - PBO, e o Princípio de Indução Finita - PIF. Lembremos que o conjunto $\mathbb{N}$ dos números naturais é formado por todos os inteiros positivos,

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Admitiremos, também, conhecimento das propriedades básicas da relação de ordem usual sobre $\mathbb{Z}$, " $\leq$ ", em que, dados a e b em $\mathbb{Z}$,

$$a \leq b \Leftrightarrow \ b = a + u,$$

sendo u um inteiro não negativo.

2.1 Divisibilidade

O conceito de divisibilidade é básico e de importância fundamental para a Teoria dos Números. Nesta seção, veremos as principais propriedades relativas a este conceito. No Capítulo 3, quanto ao estudo de congruências, abordaremos resultados mais substanciais sobre divisibilidade. No que segue, as letras a, b, c, etc. indicarão nesta seção sempre números inteiros, a menos que seja mencionado o contrário. Isso será feito para evitar repetições.

Definição 2.1.1 *Diremos que b* ***divide*** *a, em símbolos* $b \mid a$*, se existir um inteiro c tal que*

$$a = bc. \tag{2.1}$$

Neste caso, diremos também que a é **divisível** por b, que b é um **divisor** inteiro de a ou ainda que a é um **múltiplo** inteiro de b. Assim,

$$b \mid a \;\Leftrightarrow\; a = bc \quad \text{para algum} \quad c \in \mathbb{Z}.$$

O fato "b não divide a" será indicado por $b \nmid a$. Por exemplo, $3 \mid 9$, $-7 \mid 21$ e $5 \nmid 22$. Além disso, $1 \mid a$, $a \mid a$ e $a \mid 0$ para todo $a \in \mathbb{Z}$, pois

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

Quando $b \neq 0$, o inteiro c de (2.1) é único. Com efeito, se c' é outro inteiro e $a = bc'$, então $bc' = bc$, ou melhor, $b(c' - c) = 0$. Mas, como $b \neq 0$, então $c' - c = 0$, isto é, $c' = c$. Também, $0 \mid a$ se, e somente se, $a = 0$. Por isso, costuma-se excluir o caso em que o divisor é zero, e é o que faremos sempre.

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

Para um 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,

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

É claro 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 2.1.2 Determinar todos os números inteiros n para os quais $n+2$ divide n^3+1.

Solução: É fácil verificar que $n^3 + 1 = (n+2)(n^2 - 2n + 4) - 7$, de modo que

$$\frac{n^3+1}{n+2} = n^2 - 2n + 4 - \frac{7}{n+2}, \;\; \text{com} \;\; n \neq -2.$$

Como $n^2 - 2n + 4 \in \mathbb{N}$, $n+2$ divide n^3+1 se, e somente se, $n+2$ divide 7. Visto que os divisores de 7 são ± 1 e ± 7, devemos ter

$$n+2 = \pm 1, \quad n+2 = \pm 7,$$

de onde obtemos $n = -1$, $n = -3$, $n = 5$ e $n = -9$. △

Exemplo 2.1.3 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 sobre n. 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 $n+1$,

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

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

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

Lema 2.1.4 (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 $a = bc$ (c é diferente de zero, pois assim é o inteiro a). Logo,

$$|a| = |bc| = |b|\,|c|\,.$$

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

Proposição 2.1.5 *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 2.1.4, $|b| \leq 1$. 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, $a = \alpha b$ e $b = \beta a$, com $\alpha, \beta \in \mathbb{Z}$. Desse modo,

$$a = (\alpha\beta)a,$$

ou seja, $\alpha\beta = 1$ e, pelo item (1), $\alpha = \pm 1$, o que implica $a = \pm b$. □

No próximo teorema, apresentaremos outras propriedades elementares da divisibilidade.

Teorema 2.1.6 *A divisibilidade tem as 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 $a \mid (mb + nc)$, $\quad \forall\, m, n \in \mathbb{Z}$.*

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

(2) Sendo $b = a\alpha$ e $d = c\beta$, temos $bd = (ac)(\alpha\beta)$, isto é, $ac \mid bd$.

(3) Por hipótese, $b = a\alpha$ e $c = a\beta$. Logo, dados inteiros m e n, $mb = am\alpha$ e $nc = an\beta$, de modo que $mb + nc = a(m\alpha + n\beta)$. Assim, $a \mid (mb + nc)$. □

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 $x_1, x_2, \ldots, x_n$.

2.2 Algoritmo da Divisão

O Algoritmo da Divisão, ou Divisão Euclidiana, é um dos resultados mais básicos de toda a Teoria dos Números. Como já destacamos na seção anterior, nem sempre a divisão entre dois números inteiros resulta em um número inteiro, por exemplo, efetuando a divisão de $a = 12$ por $b = 5$, obtemos

$$12 = 5 \cdot 2 + 2.$$

De uma maneira informal, a igualdade anterior representa uma situação em que, dividindo igualmente 12 objetos entre 5 pessoas, cada uma possuirá 2 objetos, e ainda sobrarão 2 outros.

Teorema 2.2.1 *Sejam a e b inteiros, com $b > 0$. Então, existem únicos inteiros q e r tais que*

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

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 $|a|\, b \geq |a|$. Logo,

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

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

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*

$$a = bq + r, \quad com \quad 0 \leq r < |b|. \tag{2.2}$$

Demonstração: É suficiente considerar o caso $b < 0$. O teorema anterior nos mostra que existem únicos inteiros q_1 e r tais que

$$a = |b| q_1 + r, \quad \text{com} \quad 0 \leq r < |b|.$$

Como $|b| = -b$,

$$a = |b| q_1 + r = b(-q_1) + r,$$

de maneira que, tomando $q = -q_1$,

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

□

Os inteiros q e r dados em (2.2) são chamados **quociente** e **resto** da Divisão Euclidiana de a por b, respectivamente. Nota-se que, na Divisão Euclidiana, com $a = bq + r$,

$$r = 0 \iff b \mid a.$$

Além disso,

Observação 2.2.3 Temos os seguintes casos particulares:

(a) Se $a = 0$, então $q = r = 0$.

(b) Se $a > 0$ e $a < b$, então $q = 0$ e $r = a$.

Alguns Exemplos Básicos

Exemplo 2.2.4 Determinar o quociente e o resto da divisão de a por b quando:

(a) $a = 41$ e $b = 7$.

(b) $a = -10$ e $b = 6$.

(c) $a = -1243$ e $b = -4$.

Solução: a) Como $41 = 7 \cdot 5 + 6$ e $6 < 7$, $q = 5$ e $r = 6$.

b) Para este caso, vamos efetuar a divisão natural de 10 por 6. Após isso, manipularemos a expressão convenientemente. Já que $10 = 1 \cdot 6 + 4$, temos

$$\begin{aligned} -10 &= -1 \cdot 6 - 4 = -1 \cdot 6 - 4 - 6 + 6 \\ &= 6 \cdot (-2) + 2. \end{aligned}$$

Logo, $q = -2$ e $r = 2$.

c) Sendo $a = -1243$ e $b = -4$, efetuaremos a divisão de 1243 por 4 e usaremos artifício análogo ao do item b). Ora, uma vez que $1243 = 310 \cdot 4 + 3$,

$$\begin{aligned} -1243 &= 310 \cdot (-4) - 3 = 310 \cdot (-4) - 3 - 4 + 4 \\ &= -4 \cdot (310 + 1) + 1 \\ &= -4 \cdot 311 + 1. \end{aligned}$$

Assim, $q = 311$ e $r = 1$. △

Exemplo 2.2.5 Determinar o resto da divisão de 5^{101} por 4.

Solução: Pelo Exemplo 2.1.3, sabemos que para quaisquer $a, b \in \mathbb{Z}$, $(a-b)$ divide $(a^n - b^n)$ para todo $n \in \mathbb{N}$. Em particular, para $a = 5$, $b = 1$ e $n = 101$, segue que $(5-1)$ divide $(5^{101} - 1)$. Assim, existe um inteiro q tal que $5^{101} - 1 = 4q$, isto é, $5^{101} = 4q + 1$. Por isso, o resto é $r = 1$. △

Exemplo 2.2.6 Determinar todos os inteiros positivos que, quando divididos por 20, deixam resto igual ao quadrado do quociente.

Solução: Dado um inteiro $m > 0$ temos, pelo Algoritmo da Divisão, $m = 20q + r$, com $0 \leq r \leq 19$. A condição exige que $r = q^2$ e, com isto, $0 \leq q^2 \leq 19$, ou melhor, $1 \leq q \leq 4$, pois $q > 0$, visto que $m = q(20 + q) > 0$. Assim,

$$\begin{aligned} q = 1 &\Rightarrow m = 21 = 20 \cdot 1 + 1, \\ q = 2 &\Rightarrow m = 44 = 20 \cdot 2 + 2^2, \\ q = 3 &\Rightarrow m = 69 = 20 \cdot 3 + 3^2, \\ q = 4 &\Rightarrow m = 96 = 20 \cdot 4 + 4^2 \end{aligned}$$

são os inteiros desejados. △

2.3 Máximo Divisor Comum

O conceito de máximo divisor comum é imprescindível para se estabelecer resultados relevantes dos números inteiros. Essencialmente, suas propriedades são centrais quando se deseja investigar problemas mais substâncias sobre divisibilidade. Em uma linguagem mais técnica, para determinar o máximo divisor comum de dois inteiros a e b não nulos devemos considerar o seguinte

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

O maior elemento n em comum entre esses conjuntos é o mdc de a e b. É claro que $D_a \cap D_b \neq \varnothing$, pois, $1 \in D_a \cap D_b$. Como este conjunto é finito, ele possui um maior elemento, chamado *máximo divisor comum* (mdc) de a e b, em símbolos $mdc(a,b)$.

Por exemplo, para $a = 20$ e $b = 28$,

$$D_a = \{1,2,4,5,10,20\} \quad \text{e} \quad D_b = \{1,2,4,7,14,28\},$$

de modo que $D_a \cap D_b = \{1,2,4\}$. Por isso, $mdc(a,b) = 4$. De maneira mais formal:

Definição 2.3.1 *Dados $a,b \in \mathbb{Z}$ não nulos, dizemos que o inteiro positivo d é o mdc de a e b quando as seguintes condições são satisfeitas:*

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

(b) *Se c é um divisor de a e b, então $c \mid d$.*

Em outras palavras, o máximo divisor comum de a e b é um número natural que os divide e ainda é divisível por todo divisor comum de a e b.

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

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

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

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

Além disso, é imediato verificar que:

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

Isto porque $c \in D_a$ se, e somente se, $-c \in D_a$. Por isto, para o cálculo de $mdc(a,b)$, vamos sempre considerar a e b positivos.

A identidade de Bachet[1]-Bézout[2], apresentada no teorema a seguir, é uma das principais identidades da Teoria dos Números. Por meio dela, pode-se estabelecer importantes resultados. Aliás, ela é proveitosa não apenas para a Teoria dos Números em si, mas também para se estabelecer muitos resultados das Teorias de Grupos e Anéis (cf. [4]).

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

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

Demonstração: Consideremos o conjunto

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

Notemos, de início, que W é não 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

$$\lambda = ax_0 + by_0. \tag{2.4}$$

Usando o Algoritmo da Divisão, com os elementos a e λ,

$$a = \lambda q + r, \text{ com } 0 \leq r < \lambda. \tag{2.5}$$

Substituindo o valor de λ em (2.4) na igualdade (2.5), vem que

$$r = a - \lambda q = a - (ax_0 + by_0)q = a - aqx_0 - bqy_0.$$

Daí,

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

Isso 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 $\lambda \mid b$.

Sendo $d = mdc(a,b)$, então $a = d\lambda_1$ e $b = d\lambda_2$. Daí, por (2.4),

$$\lambda = (d\lambda_1)x_0 + (d\lambda_2)y_0 = d(\lambda_1 x_0 + \lambda_2 y_0),$$

ou seja, $d \mid \lambda$, e como $\lambda \mid d$, pois $d = mdc(a,b)$, $d = \lambda$. Logo, $d = ax_0 + by_0$. □

[1]Claude Gaspar Bachet (1581-1638) foi o primeiro a demonstrar o resultado. É creditado a ele, também, a tradução da obra *Arithmetica* do matemático Diofanto do grego para o latim.

[2]Étienne Bézout (1730-1783) foi responsável pela generalização do resultado para polinômios. Foi conhecido também pela produção de livros voltados ao ensino da Matemática.

O Teorema 2.3.2 assegura que, dados inteiros a e b, existe outro par de inteiros x e y tais que:

$$d = ax + by, \quad \text{com} \quad d = mdc(a,b).$$

Aliás, esse par de inteiros não é único. Com efeito, consideremos os inteiros $a = 8$ e $b = 12$. Assim,

$$\begin{aligned} mdc(8,12) &= 4 = 8\cdot(-1)+12\cdot 1 \qquad (x_0 = -1 \text{ e } y_0 = 1) \\ &= 8\cdot(11)+12\cdot(-7) \quad (x_0 = 11 \text{ e } y_0 = -7). \end{aligned}$$

A equação $12x + 8y = 4$ é um exemplo de uma Equação Diofantina nas incógnitas x e y. Mais geralmente, uma equação da forma $ax + by = c$, em que a,b e c são inteiros dados e x e y são as incógnitas, é chamada uma **equação diofantina**. Uma solução (inteira) para esta equação é um par de inteiros (x_0, y_0) tal que

$$ax_0 + by_0 = c. \tag{2.6}$$

Verifica-se que esta equação tem solução se, e somente se, $mdc(a,b)$ é igual a c. Além disso, se x_0 e y_0 formam uma solução, então $ax + by = c$ admite infinitas soluções, que são determinadas pelas expressões algébricas

$$x = x_0 - 8k \quad \text{e} \quad y = y_0 + 12k.$$

Por causa disto, a expressão algébrica em (2.6) é chamada **identidade de Bachet-Bézout** para os inteiros a e b. Como mencionamos, ela é fundamental para se estabelecer importantes resultados aritméticos. Para mais detalhes, sugerimos as referências [5] e [6].

Algoritmo de Euclides

No ensino básico, para se calcular o mdc de dois inteiros a e b, é comum considerar estes números relativamente pequenos, determinar seus divisores positivos e encontrar o maior dos divisores em comum. No entanto, quando a e b são "grandes", este processo já não é conveniente, do ponto de vista prático.

O Algoritmo de Euclides é até hoje o método mais eficiente de se calcular o *mdc* de dois inteiros. Ele consiste em divisões sucessivas. Para estabelecê-lo, faremos o uso do seguinte lema:

Lema 2.3.3 (Euclides) *Dados a e b inteiros positivos tais que $a = bq + r$, 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 máximos também serão. Se $d \in D_a \cap D_b$, então $d \mid a$ e $d \mid b$. Mas, como $r = a - qb$, $d \mid r$ e, por isso, $d \in D_b \cap D_r$. Por outro lado, se $d \in D_b \cap D_r$, então $d \mid D_b$ e

$d \mid D_r$, de modo que $d \mid bq + r = a$, isto é, $d \in D_a \cap D_b$. Logo, $D_a \cap D_b = D_b \cap D_r$ e, portanto, $mdc(a,b) = mdc(b,r)$. □

Usando de forma repetida o Lema 2.3.3, obtém-se uma forma prática para se calcular o mdc de quaisquer pares de inteiros a e b; essa forma é precisamente o Algoritmo de Euclides. Além disso, ele mostra como se obter uma combinação linear que envolve $d = mdc(a,b)$ e os inteiros a e b. Vejamos um exemplo concreto.

Exemplo 2.3.4 Determinar $d = mdc(202,28)$. Além disso, determinar inteiros x_0 e y_0 tais que $d = ax_0 + by_0$, em anuência com o Teorema 2.3.7.

Solução: Por meio de divisões sucessivas,

$$\begin{aligned} 202 &= 28 \cdot 7 + 6, \\ 28 &= 6 \cdot 4 + 4, \\ 6 &= 4 \cdot 1 + 2, \\ 4 &= 2 \cdot 2 + 0. \end{aligned} \tag{2.7}$$

Assim, do Lema 2.3.3,

$$mdc(202,28) = mdc(28,6) = mdc(6,4) = mdc(4,2) = mdc(2,0) = 2.$$

Determinemos inteiros x_0 e y_0 tais que $2 = 202x_0 + 28y_0$. Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades (2.7), substituindo-os sucessivamente. Fazendo isto, obtemos

$$\begin{aligned} 2 &= 6 + 4 \cdot (-1) \\ &= 6 + [28 + 6 \cdot (-4)](-1) \\ &= 6 + 28 \cdot (-1) + 6 \cdot 4 \\ &= 28 \cdot (-1) + 6 \cdot 5 \\ &= 28 \cdot (-1) + [202 + 28 \cdot (-7)] \cdot 5 \\ &= 28 \cdot (-1) + 202 \cdot 5 + 28 \cdot (-35) \\ &= 202 \cdot 5 + 28 \cdot (-36). \end{aligned}$$

Dessa forma, podemos considerar $x_0 = 5$ e $y_0 = -36$. △

Definição 2.3.5 *Dois inteiros a e b são ditos **primos entre si**, ou **relativamente primos**, quando $mdc(a,b) = 1$.*

Observa-se que, a e b são relativamente primos se, somente se, existem inteiros x e y para os quais

$$1 = ax + by.$$

Os inteiros 5 e 9 são primos entre si, pois $mdc(5,9) = 1$, Já 4 e 6 não são, uma vez que $mdc(4,6) = 2$.

Corolário 2.3.6 *Sejam a, b, c inteiros. Se $a \mid bc$ e $mdc(a,b) = 1$, então $a \mid c$.*

Demonstração: Por hipótese, $bc = ak$ com $k \in \mathbb{Z}$. Por outro lado, pela identidade de Bachet-Bézout, existem x e y inteiros tais que $1 = ax + by$. Multiplicando a ultima igualdade por c, obtemos

$$c = acx + bcy = acx + aky = a(cx + ky)$$

ou seja, $a \mid c$. □

As propriedades dadas no teorema que segue são úteis para o calculo do *mdc* quando os inteiros a e b tem um divisor em comum maior do que 1.

Teorema 2.3.7 *Sejam a, b, k e $n \in \mathbb{N}$. Então,*

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

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

Corolário 2.3.8 *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.*

Demonstração: Consideremos $d = mdc(a,b)$. Daí,

$$d = mdc\left(\frac{da}{d}, \frac{db}{d}\right) \Leftrightarrow d = d \cdot mdc\left(\frac{a}{d}, \frac{b}{d}\right) \Leftrightarrow 1 = mdc\left(\frac{a}{d}, \frac{b}{d}\right).$$

Por este motivo, a/d e b/d são primos entre si. Agora, suponhamos a/d e b/d primos entre si. Logo,

$$1 = mdc\left(\frac{a}{d}, \frac{b}{d}\right) = mdc(a,b)/d.$$

Daí, $d = mdc(a,b)$. □

O conceito de *Mínimo Múltiplo Comum* (*mmc*) é um paralelo importante do conceito de *mdc*. Para mais detalhes, sugerimos as referências [5] e [6].

Capítulo 3

Números Primos e Congruências

Este capítulo será dividido em duas partes. Na primeira, trataremos de alguns resultados básicos sobre números primos destacando, de modo especial, o Teorema Fundamental da Aritmética. Este é o principal resultado da Teoria dos Númeors, e um dos mais importantes de toda matemática. Na segunda, iremos considerar o conceito de *congruência*. Este conceito nos permite estabelecer propriedades substanciais da divisibilidade.

3.1 Números Primos

Os números primos começaram a ser estudados pela escola pitagórica e, até hoje, são objeto de estudo para muitos teóricos dos números. Uma quantidade considerável dos resultados sofisticados da Teoria dos Números deve-se a esses números. Alguns deles continua sem solução. Como, por exemplo,

(Conjectura de Goldbach) Em 1742, Christian Goldbach conjecturou que todo inteiro par maior do que 2 é soma de dois primos, não necessariamente distintos. Por exemplo,

$$4 = 2+2, \quad 6 = 3+3, \quad 22 = 3+19, \quad 100 = 29+71.$$

(Conjectura dos primos gêmeos) Existem infinitos pares de primos gêmeos, ou seja, pares de números da forma $(p, p+2)$, em que p e $p+2$ são primos, tais como

$$(3,5), \quad (5,7), \quad (11,13), \quad (17,19), \quad (29,31).$$

(Conjectura dos primos da forma n^2+1) Existem infinitos primos p da forma $p = n^2+1$, assim como

$$5 = 2^2+1, \quad 17 = 4^2+1, \quad 37 = 6^2+1.$$

(Conjectura dos primos de Mersenne) Existem infinitos primos de Mersenne, isto é, primos da forma $M_p = 2^p - 1$, com p primo. Por exemplo,

$$M_2 = 2^2-1 = 3, \quad M_3 = 2^3-1 = 7, \quad M_5 = 2^5-1 = 31.$$

(Conjectura dos números perfeitos) Existem infinitos números perfeitos (um número natural é perfeito se ele é igual a soma de seus divisores positivos, exceto ele próprio). Por exemplo, os números 6 e 28 são perfeitos, pois

$$6 = 1+2+3 \quad \text{e} \quad 28 = 1+2+4+7+14.$$

Outra conjectura relacionada afirma que não existe nenhum número perfeito ímpar. Os números perfeitos, objeto central deste trabalho, serão cosiderados no Capítulo 4.

Por essa razão, os números primos sempre ocuparam e ainda ocupam uma posição de destaque na Matemática. Há excelentes referências que se dedicam ao estudo específico dos primos, entre as quais, destacamos [7].

O Teorema Fundamental da Aritmética, TFA, revela-nos o motivo pelo qual os números primos são tão importantes. Ele assegura que todo inteiro $a \in \mathbb{Z} - \{0, \pm 1\}$ pode ser escrito como um produto de números primos. Em outras palavras, os primos são suficientes para gerar todos os inteiros diferentes de 0 e ± 1.

Definição 3.1.1 *Um inteiro $p > 1$ é chamado **primo** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, dizemos que p é **composto**.*

Noat-se que $a \in \mathbb{Z}$ é composto se, e somente se,

$$a = bc, \quad \text{com} \quad b, c \in \mathbb{Z} \quad \text{e} \quad 1 < |b|, |c| < |a|.$$

Nestas condições, b e c são chamados **divisores próprios** de a. Também se p é primo então, para qualquer inteiro a,

$$mdc(a, p) = 1 \quad \text{ou} \quad mdc(a, p) = p. \tag{3.1}$$

Por exemplo, 3, 5 e 17 são primos, enquanto $6 = 2 \cdot 3$, $8 = 2 \cdot 4$ e $15 = 3 \cdot 4$ são compostos. Importante ressaltar que 2 é o único primo par.

Exemplo 3.1.2 Mostrar que todo inteiro positivo $n > 11$ é a soma de dois números compostos.

Solução: Seja n um inteiro, com $n > 11$. Se n é par, $n = 2k$, com $k \geq 6$. Assim, $n-6 = 2(k-3)$, e como $k \geq 6$, $n-6$ é composto e $n = 2(k-3)+6$. Se n é ímpar, $n = 2k+1$, com $k \geq 6$ e, por isso, $n-9 = 2(k-4)$, que é composto e $n = 2(k-4)+9$. Por exemplo, $n = 48 = 2 \cdot 21 + 6$ ($k = 24$); e $n = 105 = 2 \cdot 48 + 9$ ($k = 52$). △

Exemplo 3.1.3 Sejam a e n inteiros positivos maiores do que 1. Mostrar que se $a^n - 1$ é primo, então $a = 2$ e n é primo.

Solução: Suponhamos $a^n - 1$ primo, com $a > 1$ e $n > 1$. Por absurdo, admitamos $a > 2$. Daí, $1 < a-1 < a^n - 1$. Por outro lado, do Exemplo **??**, $a-1$ divide $a^n - 1$, ou seja, $a^n - 1$ não é primo, uma contradição. Por isso, $a = 2$.

Para a segunda parte, vamos supor, também por absurdo, n composto. Logo, podemos escrevê-lo na forma $n = rs$, em que $1 < r, s < n$. Daí, usando mais uma vez o Exemplo **??**, segue que $2^r - 1$ divide $2^{rs} - 1 = 2^n - 1$, com

$$1 < 2^r - 1 < 2^n - 1,$$

isto é, $2^n - 1$ não é primo, o que também é uma contradição. Por conseguinte, n é primo. $\triangle$

Propriedades Básicas dos Primos

Importante destacar algumas propriedades elementares dos primos. Comecemos com a seguinte:

Proposição 3.1.4 (Euclides) *Sejam $a, b \in \mathbb{Z}$ e p um número primo. Se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Como p é primo, $mdc(a,p) = 1$ ou $mdc(a,p) = p$, conforme observado em (3.1). Se $p \nmid a$, então $mdc(a,p) = 1$. Portanto, pelo Corolário 2.3.6, segue que $p \mid b$. $\square$

Na realidade, tem-se o seguinte: um inteiro $p > 1$ é primo se, e somente se, toda vez que p dividir um produto de dois números, dividirá ao menos um deles. De uma forma geral,

Corolário 3.1.5 *Se p é primo e $p \mid a_1 a_2 \ldots a_n$, então $p \mid a_i$ para algum $i = 1, \ldots, n$.*

Demonstração: Provemos por indução sobre n (o número de fatores). Para $n = 1$ o resultado segue imediatamente. Suponhamos, por hipótese de indução, que o resultado seja válido para $n \geq 1$. Logo, para $a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{Z}$, temos

$$\begin{aligned} p \mid a_1 a_2 \ldots a_n a_{n+1} &\Rightarrow p \mid (a_1 a_2 \ldots a_n) a_{n+1} \\ &\Rightarrow p \mid (a_1 a_2 \ldots a_n) \text{ ou } p \mid a_{n+1}. \end{aligned}$$

Se $p \mid a_{n+1}$, temos o resultado. Se $p \mid (a_1 a_2 \ldots a_n)$, então por hipótese de indução, $p \mid a_i$ para algum $i = 1, \ldots, n$. $\square$

Corolário 3.1.6 *Se $p, q_1, q_2, \ldots, q_r$ são números primos e $p \mid q_1 q_2 \ldots q_r$, então $p = q_i$ para algum $i = 1, 2, \ldots, r$.*

Demonstração: Se $p \mid q_1 q_2 \ldots q_r$, então do Corolário 3.1.5, $p \mid q_i$ para algum $i = 1, 2, \ldots, r$. Como q_i é primo, seus únicos divisores positivos são 1 e q_i. Logo, $p = q_i$, pois $p > 1$. $\square$

Exemplo 3.1.7 Mostrar que $p = 3$ é o único primo que satisfaz o seguinte: se p e $p^2 + 8$ são ambos primos, então $p^3 + 4$ também é primo.

Solução: O primo $p = 3$ é tal que $3^2 + 8 = 17$ e $3^3 + 4 = 31$. Seja $p > 3$ primo. Pelo Algoritmo da Divisão, $p = 6k+1$ ou $p = 6k+5$. Daí,

$$\begin{aligned} p &= 6k+1 \;\Rightarrow\; p^2+8 = 3\left(12k^2+4k+3\right), \\ p &= 6k+5 \;\Rightarrow\; p^2+8 = 3\left(12k^2+20k+11\right). \end{aligned}$$

Portanto, para $p > 3$, p^2+8 não é primo. △

Passemos agora ao principal resultado desta seção, o Teorema Fundamental da Aritmética, um dos pilares da Teoria dos Números. Como já destacamos, este teorema afirma que todo inteiro maior do que um é um produto de primos.

Teorema 3.1.8 (Fundamental da Aritmética – TFA) *Todo número natural*[1] $a > 1$ *pode ser escrito de forma única, a menos da ordem dos fatores, como um produto de primos. Especificamente,*

$$a = p_1 p_2 \dots p_n,$$

em que $p_1, p_2, \dots, p_n$ *são 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 e, por isso, é composto. Assim, podemos escrevê-lo na forma

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

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, $m = bc$ é um produto de primos, uma contradição. Desse modo, $M = \emptyset$.

(**Unicidade**) Suponhamos

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m, \tag{3.2}$$

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

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

[1] A fatoração de $a > 1$ implica diretamente na fatoração de $-a$.

e, pelo Corolário 3.1.6, $p_1 = q_j$ para algum $j = 1, \ldots, m$. Sem perda de generalidade, digamos que $p_1 = q_1$. Pela lei do cancelamento, segue de (3.2) que

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

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

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

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

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

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

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

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

Os primos que surgem na fatoração de um dado inteiro $a > 1$ não são, necessariamente, distintos. Por exemplo, $500 = 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^2 \cdot 5^2$. Por isso, agrupando os primos que, porventura, repetem-se na fatoração de a, podemos enunciar o Teorema 3.1.8 da seguinte forma:

Corolário 3.1.9 *Todo número natural $a > 1$ pode ser escrito de modo único, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}, \tag{3.3}$$

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

A representação de um inteiro $a > 1$ dada em (3.3) é a sua **fatoração** ou **decomposição canônica** em fatores primos.

Teorema 3.1.10 *O conjunto P dos números primos é infinito.*

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

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

Como $a > 1$, existe um primo p que divide a, ou seja, $a = pk$, conforme o Teorema 3.1.8. Já que por hipótese $p_1, p_2, \ldots, p_n$ são os únicos primos, temos $p = p_i$ para algum $i = 1, \ldots, n$, digamos $p = p_1$. Assim,

$$pk = p p_2 \ldots p_n + 1,$$

isto é, $p \mid 1$, uma contradição. Portanto, P é infinito. □

O próximo exemplo é um clássico e representou uma evolução considerável para a abstração da Matemática. Desde a escola pitagórica, existiam indícios da existência de números que não podiam ser representados em forma de fração, os chamados *números irracionais*. Os pitagóricos não tinham nenhuma afeição por tais números. Euler resolveu o exercício a seguir, e mostrou por meio dele a existência desses números.

Exemplo 3.1.11 Mostrar que $\sqrt{2}$ é irracional.

Solução: Por absurdo, suponhamos que $\sqrt{2} \in \mathbb{Q}$. Assim, por definição, existem inteiros positivos a e b, primos entre si, tais que

$$\sqrt{2} = \frac{a}{b}.$$

Multiplicando a igualdade por b e depois elevando ambos os membros ao quadrado, obtemos

$$2b^2 = a^2. \tag{3.4}$$

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 (3.4) tem um número ímpar de primos, enquanto seu lado direito tem um número par de primos. Isso contradiz o TFA. Portanto, $\sqrt{2} \notin \mathbb{Q}$. △

Teorema 3.1.12 *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 $i = 1, 2, \dots, n$.

Demonstração: Se $d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}$, com $0 \leq s_i \leq r_i$, então $r_i = s_i + k_i$ para cada $i = 1, \dots, n$. Desse modo,

$$\begin{aligned} a = p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} &= p_1^{(s_1+k_1)} p_2^{(s_2+k_2)} \dots p_n^{(s_n+k_n)} \\ &= \left(p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}\right) \left(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}\right) \\ &= d \cdot p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}, \end{aligned}$$

isto é, $d \mid a$.

Reciprocamente, suponhamos que $d \mid a$, ou seja, $a = dc$ para algum inteiro c. De acordo com o TFA, tomemos

$$c = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n} \quad \text{e} \quad d = p_1^{s_1} p_2^{s_2} \dots p_n^{s_n},$$

em que $0 \leq s_i$ e $0 \leq k_i$ para $i = 1, \dots, n$. Assim, sendo $a = dc$, temos

$$p_1^{r_1} p_2^{r_2} \dots p_n^{r_n} = \left(p_1^{s_1} p_2^{s_2} \dots p_n^{s_n}\right) \left(p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}\right) = p_1^{(s_1+k_1)} p_2^{(s_2+k_2)} \dots p_n^{(s_n+k_n)}.$$

Pelo TFA, devemos necessariamente ter

$$r_i = s_i + k_i, \quad i = 1, \ldots, n.$$

Ademais, como $0 \leq k_i$, temos $s_i \leq r_i$ para cada $i = 1, \ldots, n$. □

Exemplo 3.1.13 Use o Teorema anterior para determinar todos os divisores positivos de 12.

Solução: Dado que $12 = 2^2 \cdot 3$ é a decomposição canônica de 12, então seus divisores positivos são:

$$d_1 = 2^0 \cdot 3^0 = 1, \ d_2 = 2^1 \cdot 3^0 = 2, \ d_3 = 2^0 \cdot 3^1 = 3,$$
$$d_4 = 2^2 \cdot 3^0 = 4, \ d_5 = 2^1 \cdot 3^1 = 6, \ d_6 = 2^2 \cdot 3^1 = 12.$$

Concluímos que a quantidade de divisores positivos de 12 é dada por $(2+1) \cdot (1+1) = 6$.△

No Capítulo 4, iremos considerar duas funções aritméticas,

$$\tau(n) \quad \text{e} \quad \sigma(n),$$

relacionadas a divisores positivos de um número natural n. A função $\tau(n)$ descreve a quantidade desses divisores, enquanto $\sigma(n)$ a soma deles. É importante destacarmos que para fazer uso do Teorema 3.1.12 precisamos determinar a forma canônica dos números em questão. A dificuldade se constitui justamente nisto, pois, decompor um número dado em fatores primos nem sempre é tarefa fácil. Neste sentido, o Algoritmo de Euclides é uma ferramenta mais adequada.

3.2 O Crivo de Eratóstenes

Há, de fato, uma questão central a cerca dos números primos: como decidir a respeito da primalidade de um dado inteiro positivo? No ensino básico, essa questão é tratada de forma bastante simples.

Mesmo com o avanço tecnológico, com computadores cada vez mais sofisticados, não existe um algoritmo eficiente, do ponto de vista computacional, para decidir quando um inteiro é primo. O Teorema que segue é um teste bastante básico e, a partir dele, obtém-se um método para determinar todos os primos entre 1 e um dado inteiro $n > 0$, chamado **Crivo de Eratóstenes**.

Teorema 3.2.1 *Se n é 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 número composto, então

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

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

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

que é impossível. Portanto, $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$, digamos que $1 < a \leq \sqrt{n}$. Pelo TFA, existe um primo p, tal que $p \mid a$. Daí, $p \mid a \cdot b$ e, dessa forma, $p \mid n$. □

É claro que, a dificuldade de aplicação do Teorema anterior cresce de acordo com o valor de n.

Exemplo 3.2.2 Verificar se $n = 1023$ é um número primo, utilizando o Teorema 3.2.1.

Solução: Os primos que são menores, ou iguais, a $31 \leq \sqrt{1023}$ são:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31.$$

Como $3 \mid 1023$, concluímos que este é um número composto. △

O método de Eratóstenes, para listar todos os números primos entre 2 e um dado inteiro n, baseia-se nos seguintes passos:

(1) Escrever todos os números naturais de 2 até n.

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

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

Determinemos todos os primos entre 2 e 100.

Passo 1:

	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
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Passo 2: Como $\sqrt{100} = 10$, os primos menores ou iguais a 10 são:

$$2, 3, 5, 7.$$

Passo 3: Excluindo da tabela do passo 1 todos os múltiplos próprios dos primos descritos no passo 2, então, os números que restarem são precisamente os primos entre 2 e 100. Fazendo isto, obtemos os seguintes primos:

	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

3.3 Congruências

O conceito de *congruência* é um dos mais importantes da Teoria dos Números. Ele é a base da Aritmética Modular e, por meio dele, estabelecemos resultados substanciais sobre divisibilidade.

O conceito e a notação de congruência, utilizados até os dias atuais, devem-se a Gauss, que os introduziu em seu famoso livro *Disquisitiones Arithmeticae (Investigações Aritméticas)* publicado em 1801, quando ele tinha apenas 24 anos de idade.

Nesta seção, vamos abordar propriedades básicas das congruências e, após isso, destacaremos resultados importantes: o Pequeno Teorema de Fermat e o Teorema de Euler. Estes teoremas não dão duas congruências básicas importantes e seus resultados são usados com muita frequência na Aritmética Modular.

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

$$a \equiv_m b,$$

quando m divide $a-b$. O número m é chamado o **módulo** da congruência. Se m não dividir $a-b$, diremos que a é incongruente a b módulo m. Neste caso, escreveremos

$$a \not\equiv_m b.$$

Por exemplo, $5 \equiv_3 2$, $-9 \equiv_4 -1$ e $3 \not\equiv_2 2$, pois, $3 \mid (5-2)$, $4 \mid [-9-(-4)]$ e $2 \nmid (3-2)$.

Em termos algébricos, a congruência $a \equiv_m b$ significar que existe um $k \in \mathbb{Z}$ tal que

$$a = b + km.$$

Proposição 3.3.1 *Dados a e b inteiros, $a \equiv \ _m b$ se, e somente se, a e b têm o mesmo resto quando divididos por m.*

Demonstração: Se $a \equiv_m b$, então $a = b + km$ para algum $k \in \mathbb{Z}$. 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

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

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

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

de modo que, $m \mid (a - b)$, isto é, $a \equiv_m b$. □

Como já mostramos anteriormente, $13 \equiv_3 25$. Então, 13 e 25 possuem o mesmo resto ao serem divididos por 3. De fato,

$$13 = 4 \cdot 3 + 1 \quad \text{e} \quad 25 = 8 \cdot 3 + 1.$$

Exemplo 3.3.2 (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. △

A relação de congruência possui algumas propriedades semelhantes às da igualdade. Na realidade, a igualdade é uma relação de congruência com módulo $m = 0$.

Proposição 3.3.3 *Se a, b e c são inteiros quaisquer, então, 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, temos $a - a = 0 = 0 \cdot m$, ou seja, $a \equiv a \pmod{m}$.

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

(3) Assumindo que $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, 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, $a \equiv c \pmod{m}$. □

A última proposição mostra que a congruência é uma relação de equivalência sobre $\mathbb{Z}$. Este fato tem uma forte ligação com o conjunto finito $\mathbb{Z}_m$, o conjunto quociente de $\mathbb{Z}$ pela relação de congruência módulo m. Este conjunto possui exatamente m elementos, chamados classes de equivalência módulo m. Especificamente,

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

O conjunto $\mathbb{Z}_m$ é, de fato, um dos mais importantes conjuntos finitos, tanto na Teoria dos Números quanto em Estruturas Algébricas, principalmente quando munido de suas operações usuais de adição e multipicação de classes de restos. Para mais detalhes, sugerimos a referência [4].

Teorema 3.3.4 *Sejam a, b, c e d inteiros quaisquer. Então, as seguintes propriedades são satisfeitas:*

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

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

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

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

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

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

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

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

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) Por hipótese, $a \equiv b \pmod{m}$, e como $c \equiv c \pmod{m}$, temos, do item (1),

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

(3) Provemos 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, $a^k \equiv b^k \pmod{m}$ para $k \geq 1$. Assim, multiplicando membro a membro esta congruência com $a \equiv b \pmod{m}$, que nos foi dada por hipótese, temos $a^{k+1} \equiv b^{k+1} \pmod{m}$, conforme o item (1). Portanto, $a^k \equiv b^k \pmod{m}$ 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), $a \equiv b \pmod{m}$. □

Os exemplos que seguem não dão uma ideia como as propriedades das congruências auxiliam em questões de divisibilidade.

Exemplo 3.3.5 Determinar um critério de divisibilidade por 11.

Solução: Sejam a um inteiro positivo e

$$a = a_r a_{r-1} \ldots a_1 a_0$$

sua representação decimal. Vamos usar congruência $10 \equiv_{11} -1$ como ponto de partida para definir outras congruências, uma para cada digito de a. Pelo item (3) do Teorema 3.3.4,

$$(10)^{2k} \equiv_{11} (-1)^{2k} \;\Leftrightarrow\; 10^{2k} \equiv_{11} -1$$

para cada $k \in \mathbb{Z}$. Multiplicando membro a membro, $10 \equiv_{11} -1$ e $10^{2k} \equiv_{11} -1$, obtemos

$$10^{2k+1} \equiv_{11} -1.$$

Pela reflexividade da relação de congruência, $a_0 \equiv_{11} a_0$. Para os outros dígitos de a, utilizaremos as congruências obtidas. Pelo item (2) do Teorema 3.3.4,

$$\begin{array}{rcrcrcr} 10 & \equiv_{11} & -1 & \Leftrightarrow & a_1 10 & \equiv_{11} & -a_1 \\ 10^2 & \equiv_{11} & 1 & \Leftrightarrow & a_2 10^2 & \equiv_{11} & a_2 \\ 10^3 & \equiv_{11} & -1 & \Leftrightarrow & a_3 10^3 & \equiv_{11} & -a_3 \\ 10^4 & \equiv_{11} & 1 & \Leftrightarrow & a_4 10^4 & \equiv_{11} & a_4 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array}$$

Somando membro a membro as congruências acima, vem que

$$a \equiv_{11} (a_0 - a_1 + a_2 - a_3 + \ldots a_r).$$

Por este motivo, a é divisível por 11 se, e somente se, $S_P - S_I$ é divisível por 11, em que

$$S_P = r_0 + r_2 + r_4 + r_6 + \cdots \quad \text{(a soma dos dígitos de índice par)}$$

e

$$S_I = r_1 + r_3 + r_5 + r_7 + \cdots \quad \text{(a soma dos dígitos de índice ímpar)}.$$

△

Exemplo 3.3.6 Provar, usando congruências, que $11^{n+2} + 12^{2n+1}$ é divisível por 133, para qualquer número natural n.

Solução: Notemos que

$$121 \equiv_{133} -12.$$

Pelo o item (3) do Teorema 3.3.4, temos

$$121 \cdot 11^n \equiv_{133} -12 \cdot 11^n. \tag{3.5}$$

Também,

$$144 \equiv_{133} 11.$$

Dos itens (3) e (2) do Teorema 3.3.4,

$$12 \cdot 144^n \equiv_{133} 12 \cdot 11^n. \tag{3.6}$$

Somando (3.5) e (3.6), obtemos

$$11^{n+2} + 12^{2n+1} \equiv_{133} -12 \cdot 11^n + 12 \cdot 11^n \;\Leftrightarrow\; 11^{n+2} + 12^{2n+1} \equiv_{133} 0.$$

Ou seja, $11^{n+2} + 12^{2n+1}$ é divisível por 133. △

Na maioria dos problemas que envolvem congruências, é ideal, para simplificar os cálculos, determinarmos uma congruência base na forma $a^k \equiv_m 1$ ou $a^k \equiv_m -1$, para k e m naturais. Entretanto, às vezes isto não é possível ou não é fácil de se determinar. Nesta direção, as congruências dadas pelos Teoremas de Fermat e Euler são, quando possíveis de serem aplicadas, duas congruências iniciais que implicam bastante facilidade no trato algébrico.

A lei do cancelamento para congruêncis, dada a seguir, é um resultados aplicado a resolução de sistema de congruências.

Teorema 3.3.7 *Sejam a, b e c inteiros quaisquer. Então,*

$$ac \equiv_m bc \Leftrightarrow a \equiv_{m/d} b,$$

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

Demonstração: Se $ac \equiv_m bc$, então

$$ac - bc = c(a-b) = km, \quad \text{com} \quad k \in \mathbb{Z}. \tag{3.7}$$

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 (3.7), obtemos

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

de modo que $r \mid (a-b)$. Logo, $a \equiv_r b$, ou ainda, $a \equiv_{m/d} b$.

Reciprocamente, sejam $c = d\lambda_1$ e $m = d\lambda_2$. Como $a \equiv_{m/d} b$, isto é, $a \equiv_{\lambda_2} b$, 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, $ac \equiv_m bc$. □

Corolário 3.3.8 *Consideremos* $ac \equiv_m bc$. *Se* $mdc(c,m) = 1$, *então* $a \equiv_m b$.

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

O Pequeno Teorema de Fermat e o Teorema de Euler

Vejamos agora os dois principais resultados desta parte preliminar. Destaquemos, em primeiro lugar, o Pequeno Teorema de Fermat, ou simplesmente o Teorema de Fermat. Como é sabido, Fermat ficou conhecido por enunciar o resultado até hoje mais enigmático da Matemática, o *Último Teorema de Fermat*. Este resultado assegura que não existem inteiros positivos x, y e z tais que

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

em que n é um número natural maior do que 2.

Em 1993, o matemático inglês Andrew Wiles anunciou que tinha demonstrado o último teorema, apresentando um material com mais de 200 páginas contendo sua demonstração. Após isso, os maiores especialistas da área passaram cerca de dois anos analisando cuidadosamente o texto. Só depois disso, sua prova foi de fato confirmada.

Em sua demonstração, Wiles fez uso de conceitos e técnicas extremamente sofisticados e que, por justa razão, constitui-se numa das mais complexas demonstrações. São poucos matemáticos capazes de entendê-la em toda a sua essência. Para mais detalhes, recomendamos a referência [3].

O teorema que iremos considerar aqui tem um prova bastante simples. Senão vejamos.

Teorema 3.3.9 *Sejam p um número primo e a um inteiro, tal que $p \nmid a$. Então,*

$$a^{p-1} \equiv_p 1.$$

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

$$a, 2a, 3a, \ldots, (p-1)a. \tag{3.8}$$

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

$$ak_1 \equiv_p ak_2,$$

com $1 \leq k_1 < k_2 \leq p-1$, então, conforme o Corolário 3.3.8, podemos cancelar o fator a desta congruência, pois $mdc(a,p) = 1$ por hipótese. Fazendo isto, $k_1 \equiv_p k_2$, o que é impossível, visto que $k_1 \neq k_2$. 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, $ra \not\equiv_p 0$ 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

$$1, 2, \ldots, p-1. \tag{3.9}$$

Portanto, cada inteiro em (3.8) equivale a um número em (3.9), numa determinada ordem, digamos

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

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

$$a \cdot 2a \ldots (p-1)a \equiv_p 1 \cdot 2 \ldots (p-1),$$

isto é,

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

Visto que $mdc((p-1)!, p) = 1$, então, pela Lei do Cancelamento, $a^{p-1} \equiv_p 1$. □

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

Corolário 3.3.10 *Se p é primo, então*

$$a^p \equiv_p a$$

para qualquer inteiro a.

Demonstração: Se $p \nmid a$, então, pelo Teorema 3.3.9, $a^{p-1} \equiv_p 1$. Daí, multiplicando por a, obtemos $a^p \equiv_p a$. Se $p \mid a$, então $p \mid a^p$ e, por isso, $p \mid a^p - a$, ou seja, $a^p \equiv_p a$ para todo $a \in \mathbb{Z}$. □

Exemplo 3.3.11 Determine o resto da divisão de 237^{28} por 13.

Solução: Podemos fazer uso do Teorema de Fermat, com $p = 13$ e $a = 237$, já que 13 é primo e $mdc(13, 237) = 1$. Isto nos dá uma congruência base inicial. Com efeito, por Fermat, $237^{12} \equiv_{13} 1$. Dessa maneira,

$$237^{24} \equiv_{13} 1.$$

Por outro lado, visto que $237 \equiv_{13} 3$, então,

$$237^4 \equiv_{13} 3^4 \equiv_{13} 81 \equiv_{13} 3.$$

Multiplicando, membro a membro, $237^{24} \equiv_{13} 1$ e $237^4 \equiv_{13} 3$, obtemos

$$237^{28} \equiv_{13} 3,$$

ou seja, o resto da divisão de 237^{28} por 13 é 3. △

O Teorema de Euler é, em linhas gerais, uma generalização do Teorema de Fermat, pois o módulo m da congruência é um inteiro positivo qualquer, primo ou não. Antes de enunciá-lo, devemos, em primeiro lugar, considerar a função φ de Euler, parte central desse teorema.

Definição 3.3.12 (Função φ de Euler) *Para cada inteiro $n \geq 1$, indiquemos por $\varphi(n)$ 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 $n \in \mathbb{N}$, consideremos

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

em que $car(A_n)$ indica a cardinalidade de A_n. Sendo assim, $\varphi(n) = car(A_n)$. Por exemplo,

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

Para um inteiro um pouco maior, digamos $n = 18$, os inteiros positivos menores do que 18 e que são relativamente primos com ele são 1, 5, 7, 11, 13 e 17 e, com isto, $\varphi(18) = 6$. Além disso,

$$\varphi(18) = \varphi(2 \cdot 9) = \varphi(2) \cdot \varphi(9).$$

Esta propriedade multiplicativa é válida para quaisquer m e n inteiros, tal que, $mdc(m,n) = 1$. De início, temos $\varphi(n) \leq n - 1$, para $n \geq 1$, e ainda

$$\varphi(n) = n - 1 \Leftrightarrow n \text{ primo.}$$

O objetivo é descrever uma fórmula para se calcula $\varphi(n)$ a partir da decomposição canônica de n. Em primeiro lugar,

Teorema 3.3.13 *Se p é primo e $k \geq 1$, então*

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

Demonstração: Notemos que $mdc(n, p^k) = 1$ se, e somente se, $p \nmid n$. Por outro lado, entre 1 e p^k existem p^{k-1} inteiros que são divisíveis por p,

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

De fato, $p\lambda \leq p^k$ se, e somente se, $\lambda = 1, 2, \ldots, p^{k-1}$. Desse modo, o conjunto $\{1, 2, \ldots, p^k\}$ possui $p^k - p^{k-1}$ inteiros relativamente primos com p^k. Daí, por definição, $\varphi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$. □

Por exemplo,

$$\varphi(25) = \varphi(5^2) = 5^2 - 5 = 20 \quad \text{e} \quad \varphi(32) = \varphi(2^5) = 2^5 - 2^4 = 16.$$

A prova da propriedade multiplicativa da função φ não será apresentada aqui. Para este fim, recomendamos as referências [5] e [6]

Teorema 3.3.14 (A função φ é multiplicativa) *Se m e n são números naturais tais que $mdc(m,n) = 1$, então,*

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

De uma maneira geral, por indução finita, mostra-se o seguinte:

Corolário 3.3.15 *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*

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

À luz dos resultados anteriores, podemos provar o seguinte:

Teorema 3.3.16 *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*

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1})\ldots(p_r^{k_r} - p_r^{k_r-1}) = n(1-1/p_1)\ldots(1-1/p_r).$$

Demonstração: Já que φ é multiplicativa e $mdc(p_i^{k_i}, p_j^{k_j}) = 1$, para $i \neq j$, então, do Corolário 3.3.15,

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

Pelo Teorema 3.3.14,

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

para cada $i = 1, 2, \ldots, r$. Portanto,

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

o que completa a prova □

Sabendo que, $p_i^{k_i} - p_i^{k_i-1} = p_i^{k_i-1}(p_i - 1)$, podemos reescrever a fórmula do teorema anterior da seguinte forma

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \cdots p_r^{k_r-1}(p_1-1)(p_2-1)\cdots(p_r-1).$$

Exemplo 3.3.17 Calcular $\varphi(250)$.

Solução: Como $250 = 2 \cdot 5^3$, $p_1 = 2$, e $p_3 = 5$. Desse modo,

$$\begin{aligned}
\varphi(250) &= 250(1-1/2)(1-1/5) \\
&= 250(1/2)(4/5) \\
&= 100.
\end{aligned}$$

△

Teorema 3.3.18 (Euler) *Sejam a e m inteiros, com* $m \geq 1$ *e* $mdc(a, m) = 1$*. Então,*

$$a^{\varphi(m)} \equiv_m 1.$$

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

$$\begin{aligned} a \cdot a_1 &\equiv_m b_1, \\ a \cdot a_2 &\equiv_m b_{2,} \\ \vdots \quad & \quad \vdots \quad \vdots \\ a \cdot a_{\varphi(m)} &\equiv_m b_{\varphi(m),} \end{aligned}$$

em que, $b_1, b_{2,} \ldots, b_{\varphi(m)}$ são os inteiros $a_1, a_2, \ldots a_{\varphi(m)}$, não necessariamente nesta ordem. Multiplicando membro a membro essas congruências, obtemos

$$(aa_1)(aa_2)\cdots(aa_{\varphi(m)}) \equiv_m b_1 b_2 \cdots b_{\varphi(m)},$$

ou seja,

$$a^{\varphi(m)}(a_1 a_2 \cdots a_{\varphi(m)}) \equiv_m a_1 a_2 \cdots a_{\varphi(m)}. \tag{3.10}$$

Uma vez que $mdc(a_i, m) = 1$, para todo $i = 1, 2, \ldots, \varphi(m)$, então $mdc(a_1, a_2, \ldots a_{\varphi(m)}, m) = 1$. Por isso, podemos cancelar o fator $a_1, a_2, \ldots a_{\varphi(m)}$ em (3.10). Fazendo isto, obtemos $a^{\varphi(m)} \equiv_m 1$. □

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

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

ou seja, o Teorema de Fermat é uma consequência do Teorema de Euler.

Capítulo 4

Números Perfeitos

Os números perfeitos, bem como os números amigáveis, começaram a ser estudados pela escola pitágorica e até os dias atuais despertam a curiosidade de muitos teóricos dos números. Apesar de serem tópicos relativamente simples, no sentido de considerar conceitos elementares, como divisores e a função $\sigma(n)$ soma de divisores, ainda existem alguns problemas em aberto sobre eles. Assim como ocorre com os números primos.

É bem verdade que, tanto números perfeitos quanto os números amigáveis, estão diretamente relacionados à função $\sigma(n)$. No entanto, para que se possa somar os divisores positivos de n, faz-se necessários contá-los. É aí que lançamos mão da função $\tau(n)$, a função número de divisores positivos de n. Em resumo, $\tau(n)$ relaciona inteiro n com a quantidade de seus divisores, e $\sigma(n)$ com a soma desses divisores.

Neste capítulo, iremos considerar a nossa contribuição ao trabalho. Essencialmente, ela consiste na descrição e solução de alguns problemas que envolvem números perfeitos, e também números amigáveis. Alguns desses problemas são em nível médio e outros são clássicos do assunto.

4.1 As funções $\tau(n)$ e $\sigma(n)$

Nesta seção, iremos considerar duas funções aritméticas importantes, que desempenharão um papel central para os objetivos em que o trabalho se insere, as funções $\tau(n)$ e $\sigma(n)$. Como já ressaltamos acima, elas estabelecem importantes relações entre um dado inteiro positivo e seus divisores. Apenas lembramos qualquer função $f : \mathbb{N} \to \mathbb{R}$ (ou $\mathbb{C}$) diz-se uma **função aritmética**.

Definição 4.1.1 *Dado um número natural n, denotemos por $\tau(n)$ o número de divisores positivos de n, e por $\sigma(n)$ a soma desses divisores.*

Nota-se, de início, que τ e σ são funções de $\mathbb{N}$ em $\mathbb{N}$. Por exemplo,

$$\tau(1) = 1, \quad \tau(2) = 2, \quad \tau(3) = 2 \quad \tau(4) = 3 \quad \tau(10) = 4$$

e

$$\sigma(1) = 1, \quad \sigma(2) = 3, \quad \sigma(3) = 4, \quad \sigma(4) = 7, \quad \sigma(10) = 18.$$

Intuitivamente, percebe-se que, à medida que o valor de n aumenta, aumenta também a dificuldade de se determinar os valores $\tau(n)$ e $\sigma(n)$; isto também se inclui o caso de identificar se n é ou não primo. Dessa maneira, é necessário estabelecer fórmulas para se calcular os valores destas funções para qualquer inteiro positivo n. É exatamente isso que trataremos no teorema seguinte. Mas, antes disso, notemos que, por definição,

$$\tau(n) = 2 \;\Leftrightarrow\; n \text{ é primo}$$

e

$$\sigma(n) = n + 1 \;\Leftrightarrow\; n \text{ é primo.}$$

Uma Propriedade Especial

Vejamos um resultado central relacionado às funções $\tau(n)$ e $\sigma(n)$, o qual traduz o fato de ambas serem *multiplicativas*.

Teorema 4.1.2 *Se $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ é a fatoração canônica de $n > 1$, então*

$$\tau(n) = (r_1 + 1)(r_2 + 1) \cdots (r_k + 1)$$

e

$$\sigma(n) = \left(\frac{p_1^{r_1+1} - 1}{p_1 - 1} \right) \left(\frac{p_2^{r_2+1} - 1}{p_2 - 1} \right) \cdots \left(\frac{p_k^{r_k+1} - 1}{p_k - 1} \right).$$

Demonstração: De acordo com o Teorema 3.1.12, os divisores positivos de n são precisamente da forma

$$d = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k},$$

em que $0 \leq s_i \leq r_i$ para cada $i = 1, 2, \ldots, k$. Como existem $r_1 + 1$ escolhas para o expoente s_1, $r_2 + 1$ escolhas para o expoente s_2,..., $r_n + 1$ escolhas para o expoente s_n, pela análise combinatória, existem

$$(r_1 + 1)(r_2 + 1) \cdots (r_k + 1)$$

divisores possíveis de n, ou seja,

$$\tau(n) = (r_1 + 1)(r_2 + 1) \cdots (r_k + 1).$$

Vamos analisar agora a função $\sigma(n)$. Notemos que, no produto

$$(1 + p_1 + p_1^2 + \cdots + p_1^{r_1})(1 + p_2 + p_2^2 + \cdots + p_2^{r_2}) \cdots (1 + p_n + p_n^2 + \cdots + p_k^{r_k}),$$

cada divisor positivo de n aparece apenas uma única vez, como um termo, na expansão desse produto. Por conseguinte,

$$\sigma(n) = (1 + p_1 + p_1^2 + \cdots + p_1^{r_1})(1 + p_2 + p_2^2 + \cdots + p_2^{r_2}) \cdots (1 + p_k + p_k^2 + \cdots + p_k^{r_k}).$$

Agora, para cada r_i, $1 + p_i + p_i^2 + \cdots + p_i^{r_i}$ representa a soma dos $r_i + 1$ termos de uma progressão geométrica com primeiro termo $a_1 = 1$ e razão $q = p_i$. Desse modo,

$$1 + p_i + p_i^2 + \cdots + p_i^{r_i} = \frac{p_i^{r_i+1} - 1}{p_i - 1}.$$

Portanto,

$$\sigma(n) = \left(\frac{p_1^{r_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{r_2+1} - 1}{p_2 - 1}\right)\cdots\left(\frac{p_k^{r_k+1} - 1}{p_k - 1}\right).$$

□

Verifica-se que, em particular, se p é primo e r é um inteiro não negativo, então

$$\tau(p^r) = (r+1) \quad \text{e} \quad \sigma(p^r) = \left(\frac{p^{r+1} - 1}{p - 1}\right).$$

Para $n = 280 = 2^3 \cdot 5 \cdot 7$, temos $p_1 = 2$ e $r_1 = 3$, $p_2 = 5$ e $r_2 = 1$, $p_3 = 7$ e $r_3 = 1$. Logo, pelo Teorema 4.1.2,

$$\tau(280) = (3+1)(1+1)(1+1) = 16$$

e

$$\sigma(280) = \left(\frac{2^4 - 1}{2 - 1}\right)\left(\frac{5^2 - 1}{5 - 1}\right)\left(\frac{7^2 - 1}{7 - 1}\right) = 720.$$

△

Exemplo 4.1.3 Mostrar que um número natural n é um quadrado perfeito se, e somente se, $\tau(n)$ é ímpar.

Solução: Como $1 = 1^2$ e $\tau(1) = 1$ é ímpar, o resultado é válido para $n = 1$. Consideremos $n > 1$ e seja

$$n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$$

sua fatoração canônica. Se n é um quadrado perfeito, então conforme observamos logo após o Corolário 3.1.9, existe $\alpha_i \in \mathbb{N}$ tal que $r_i = 2\alpha_i$, com $i = 1, \ldots, k$. Assim, pelo Teorema 4.1.2,

$$\begin{aligned} \tau(n) &= (r_1 + 1)(r_2 + 1)\cdots(r_k + 1) \\ &= (2\alpha_1 + 1)(2\alpha_2 + 1)\cdots(2\alpha_k + 1), \end{aligned}$$

que é um número ímpar, pois é um produto de números ímpares.

Reciprocamente, se $\tau(n)$ é ímpar, então, cada fator $r_i + 1$ de

$$\tau(n) = (r_1 + 1)(r_2 + 1)\cdots(r_k + 1)$$

é, necessariamente, ímpar, ou seja, $r_i = 2\beta_i$ para cada $i = 1, \ldots, k$. Portanto,

$$\begin{aligned} n = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k} &= p_1^{2\beta_1} p_2^{2\beta_2} \ldots p_k^{2\beta_k} \\ &= \left(p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}\right)^2, \end{aligned}$$

isto é, n é um quadrado perfeito. △

Exemplo 4.1.4 Determinar todos os inteiros positivos n tais que $\tau(n) = 6$.

Solução: Já que $6 = 1 \cdot 6 = 2 \cdot 3$, o inteiro n deve ter no máximo dois divisores primos distintos, digamos p e q. Assim, $n = p^\alpha q^\beta$, com $\tau(n) = (\alpha+1)(\beta+1) = 6$. Logo,

$$\alpha+1 = 1 \quad \text{e} \quad \beta+1 = 6, \quad \text{ou} \quad \alpha+1 = 2 \quad \text{e} \quad \beta+1 = 3,$$

ou seja, $\alpha = 0$ e $\beta = 5$, ou $\alpha = 1$ e $\beta = 2$. Portanto, os inteiros que satisfazem a condição dada são da forma $n = q^5$ ou $n = pq^2$. Por exemplo, para $n = 2^5$ e $m = 3 \cdot 7^2$, temos $\tau(n) = 6$ e $\tau(m) = 6$. △

Uma Propriedade Especial

Vejamos um resultado central relacionado às funções $\tau(n)$ e $\sigma(n)$, o qual traduz o fato de ambas serem *multiplicativas*.

Teorema 4.1.5 *As funções $\tau(n)$ e $\sigma(n)$ são multiplicativas, ou seja,*

$$\tau(m \cdot n) = \tau(m) \cdot \tau(n) \quad e \quad \sigma(m \cdot n) = \sigma(m) \cdot \sigma(n),$$

sempre que $mdc(m,n) = 1$.

Demonstração: Se $m = 1$ ou $n = 1$, então o resultado segue. Por isso, vamos considerar que $m > 1$ e $n > 1$. Sejam

$$m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r} \quad \text{e} \quad n = q_1^{t_1} q_2^{t_2} \dots q_s^{ts}$$

as fatorações canônicas de m e n. Como $mdc(m,n) = 1$, então $p_i \neq q_j$ para $1 \leq i \leq r$ e $1 \leq j \leq s$. Logo, a fatoração canônica de $m \cdot n$ é

$$m \cdot n = p_1^{k_1} \dots p_r^{k_r} q_1^{t_1} \dots q_s^{ts}.$$

Pelo Teorema 4.1.2,

$$\begin{aligned} \tau(m \cdot n) &= [(k_1+1)\cdots(k_r+1)][(t_1+1)\cdots(t_s+1)] \\ &= \tau(m) \cdot \tau(n). \end{aligned}$$

Da mesma forma, para a função $\sigma(n)$,

$$\begin{aligned} \sigma(m \cdot n) &= \left[\left(\frac{p_1^{k_1+1}-1}{p_1-1}\right) \cdots \left(\frac{p_r^{k_r+1}-1}{p_r-1}\right)\right] \left[\left(\frac{q_1^{t_1+1}-1}{q_1-1}\right) \cdots \left(\frac{q_s^{ts+1}-1}{q_s-1}\right)\right] \\ &= \sigma(m) \cdot \sigma(n). \end{aligned}$$

□

Exemplo 4.1.6 Para $m = 14$ e $n = 45$, $mdc(14,45) = 1$, $14 = 2 \cdot 7$ e $45 = 3^2 \cdot 5$. Logo, pelo Teorema 4.1.5

$$\tau(14 \cdot 45) = \tau(14) \cdot \tau(45) = (2+1)(1+1)^3 = 24$$

e

$$\begin{aligned} \sigma(14 \cdot 45) &= \sigma(14) \cdot \sigma(45) \\ &= \left(\frac{2^{1+1}-1}{2-1}\right)\left(\frac{7^{1+1}-1}{7-1}\right)\left(\frac{3^{2+1}-1}{3-1}\right)\left(\frac{5^{1+1}-1}{5-1}\right) \\ &= 1872. \end{aligned}$$

△

4.2 Números Perfeitos e o Teorema de Euclides-Euler

Os pitágoricos também são responsáveis pela descoberta dos dois primeiros números perfeitos, os números 6 e 28. Do ponto de vista filosófico, que os pitágoricos buscavam encontrar nos números e em suas propriedades, esses dois números estão associados a coisas muito importantes. O número 6 representa, na teória criacionista, quantos dias Deus levou para criar todo o universo, enquanto o número 28 tem relação com a quantidade de dias que a lua leva para orbitar a terra. Eles são chamados perfeitos, pois os divisores positivos de 6 são 1, 2, 3 e 6. Somando estes números, excluindo 6, temos

$$6 = 1+2+3.$$

Da mesma forma, os divisores positivos de 28 são 1, 2, 4, 7, 14 e 28, e

$$28 = 1+2+4+7+14.$$

De uma maneira geral:

Definição 4.2.1 *Um número natural $n > 1$ é chamado **perfeito** quando n for igual a soma de seus divisores positivos, excluindo ele próprio.*

Em termos da função $\sigma(n)$, a soma dos divisores positivos de n, cada um deles menor do que n, é dada por $\sigma(n) - n$. Desse modo, um número n é perfeito se, e somente se, $\sigma(n) - n = n$, ou melhor,

$$\sigma(n) = 2n.$$

Por exemplo, como

$$\sigma(18) = \sum_{d|18} 1+2+3+6+9+18 = 39 \neq 2 \cdot 18,$$

18 não é perfeito. Além dos números perfeitos $P_1 = 6$ e $P_2 = 28$,

$$P_3 = 496 = \sum_{d \in A} d,$$

com $A = \{1,2,4,8,16,31,62,124,248\}$, e

$$P_4 = 8128 = \sum_{d \in B} d,$$

em que

$$B = \{1,2,4,8,16,32,64,127,254,508,1016,2032,4064\},$$

são perfeitos. O Teorema 4.2.4 nos fornece um método prático para a obtenção de P_3 e P_4.

Os números P_1, P_2, P_3 e P_4 têm $1,2,3$ e 4 dígitos, respectivamente. Por isso, conjecturou-se que:

(1) O n-ésimo número perfeito P_n contém exatamente n dígitos.

(2) Os números perfeitos pares terminam, alternadamente, em 6 e 8.

O Teorema *de Euclides-Euler* assegura que essas afirmações são falsas. Esse teorema resolve uma questão antiga acerca dos números perfeitos, que é determinar uma forma geral para eles. Entretando, antes de apresentá-lo, devemos considerar o conceito de *número de Mersenne*.

Os números de Mersenne são inteiros que foram estudados com bastante afinco por Marin Mersenne, e até hoje são objeto de pesquisa para muitos teóricos dos números. Isto se deve por dois motivos: a relação com os números perfeitos pares; e por serem os maiores primos já descobertos. Este último motivo tem implicações importantes na Criptografia, por exemplo. Ao leitor interessando algumas aplicações de primos relativamente grandes, sugerimos a referência [8].

Definição 4.2.2 *Dado um número natural n,*

$$M_n = 2^n - 1$$

é chamado o n-ésimo ***número de Mersenne****. Se M_n for primo, então M_n é chamado* ***primo de Mersenne****.*

O resultado a seguir nos traz uma conclusão básica, porém muito importante acerca desses primos.

Proposição 4.2.3 *Se M_p é primo, então p é necessariamente primo.*

Demonstração: Se p é composto, digamos $p = ab$, em que $1 < a, b < p$, então

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

Como M_p é primo, $2^a - 1 = 2^{ab} - 1$ ou $2^a - 1 = 1$. Destas igualdades, obtemos $b = 1$ ou $a = 1$, uma contradição.Assim, p é primo. □

É importante ressalatra que a recíproca do teorema naterior não é válida. De fato, $p = 11$ é primo, mas

$$M_{11} = 2^{11} - 1 = 23 \cdot 89$$

não o é. Atualmente, com a utilização de computadores sofisticados, tornou-se bem mais fácil determinar primos de Mersenne. Os maiores números primos conhecidos são de Mersenne. Até o presente momento, $M_{82589933}$ é o maior primo (também de Mersenne), com mais de 24 milhões de dígitos, descoberto no final de 2018 por P. Laroche e outros. No site

`http://primes.utm.edu/largest.html`

o leitor poderá acompanhar a lista atual dos maiores primos já descobertos.

O problema de determinar uma forma geral para os números perfeitos foi parcialmente resolvido por Euclides no nono livro de sua obra *Elementos*. Ele mostrou que se a soma

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^{k-1} = 2^k - 1 = p$$

é um número primo, então $2^{k-1}(2^k - 1)$ é um número perfeito (nota-se que $2^k - 1$ é o k-ésimo número de Mersenne). Mais de dois mil anos depois, Euler provou a recíproca do resultado. Por este motivo, um número par é perfeito se, e somente se, é da forma $2^{k-1}(2^k - 1)$. É isto que iremos provar no próximo teorema.

Teorema 4.2.4 (Caracterização dos Números Perfeitos Pares) *Se $2^p - 1$ é um primo, com p primo, então*

$$n = 2^{p-1}(2^p - 1)$$

é um número perfeito, e todo número perfeito par pode ser expresso dessa forma.

Demonstração: Para verificar a primeira parte do resultado, consideremos $p = M_k = 2^k - 1$ e tomemos $n = 2^{k-1}p$. Visto que $mdc(2^{k-1}, p) = 1$, então, pelo Teorema 4.1.5,

$$\sigma(n) = \sigma(2^{k-1})\sigma(p).$$

Desse modo, do Teorema 4.1.2,

$$\sigma(n) = (2^k - 1)(p + 1) = p2^k = 2n.$$

Portanto, n é perfeito.

Reciprocamente, seja n um número perfeito par. Em primeiro lugar, podemos escrevê-lo na forma

$$n = 2^{k-1}m,$$

em que m é um inteiro ímpar e $k \geq 2$. Como $mdc(2^{k-1}, m) = 1$,

$$\sigma(n) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m).$$

Visto que n é perfeito, então $\sigma(n) = 2n = 2(2^{k-1}m)$, ou seja, $\sigma(n) = 2^k m$, de modo que

$$2^k m = (2^k - 1)\sigma(m) \tag{4.1}$$

e, por isso, $(2^k - 1) \mid 2^k m$. Uma vez que 2^k e $2^k - 1$ são relativamente primos, $(2^k - 1)$ divide m, digamos

$$m = (2^k - 1)\lambda.$$

Substituindo este valor em (4.1), obtemos

$$\sigma(m) = 2^k \lambda.$$

Já que m e λ são divisores de m, com $\lambda < m$,

$$2^k \lambda = \sigma(m) \geq m + \lambda = 2^k \lambda,$$

ou seja, $\sigma(m) = m + \lambda$. Isso nos mostra que m tem apenas dois divisores positivos, a saber, λ e o próprio m. Assim, m deve ser necessariamente primo, ou seja, $\lambda = 1$. Logo, $m = 2^k - 1$ e, por conseguinte,

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

com $m = 2^k - 1$ primo (de Mersenne). Isso completa a prova. □

Exemplo 4.2.5 Sem fazer uso da função σ, explicar por que $n = 23464$ e $m = 812340$ não são números perfeitos.

Solução: Visto que ambos os números são pares, então, pelo Teorema 4.2.6, eles só seriam perfeitos se seus últimos digitos fossem iguais a 6 ou a 8, o que não ocorre. Portanto, tais números não são perfeitos. △

De acordo com o resultado anterior, a cada primo de Mersenne M_p, existe um número perfeito par associado e vice-versa. Como existem até o momento 51 primos de Mersenne, os números perfeitos (pares) conhecidos são os relacionados a esses primos. Por exemplo, para $M_5 = 31$, obtemos o número perfeito $P_3 = 2^4(2^5 - 1) = 496$. Notemos que

$$\sigma(496) = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 + 496 = 992 = 2 \cdot 496.$$

Como ainda não se sabe se o conjunto dos primos de Mersenne é finito ou não, então o problema sobre a infinidade dos números perfeitos é outro problema em aberto da Teoria dos Números.

Calculemos os números perfeitos P_5 e P_6. Temos:

$$P_5 = 2^{12}(2^{13} - 1) = 4096 \cdot 8191 = 33550336$$

e

$$P_6 = 2^{16}(2^{17} - 1) = 65536 \cdot 131071 = 8589869056.$$

Assim, P_5 não possui 5 dígitos e, assim, o n-ésimo número perfeito não possui n dígitos. Daí, a primeira conjectura mencionada acima não se verifica. Por outro lado, uma vez que o dígito das unidades de P_6 é 6, a segunda conjectura também não verdadeira. No entanto, resultado a seguir, um clássico do assunto, assegura o seguinte:

Teorema 4.2.6 *Se n é um número perfeito par, então o último dígito de n é* 6 *ou* 8*, ou seja, $n \equiv_{10} 6$ ou $n \equiv_{10} 8$.*

Demonstração: Seja n um número perfeito par. Pelo Teorema 4.2.4,

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

em que $2^k - 1$ é primo. Pela Proposição 4.2.3, o expoente k também é primo. Se $k = 2$, $n = 2 \cdot 3 = 6$, ou seja, o resultado é válido. Vamos supor $k > 2$. Pelo Algoritmo da Divisão,

$$k = 4m + 1 \quad \text{ou} \quad k = 4m + 3.$$

Se $k = 4m + 1$, então

$$\begin{aligned} n = 2^{4m}(2^{4m+1} - 1) &= 2^{8m+1} - 2^{4m} \\ &= 2 \cdot 2^{8m} - 16^m \\ &= 2 \cdot \left(2^4\right)^{2m} - 16^m \\ &= 2 \cdot (16)^{2m} - 16^m. \end{aligned}$$

É fácil mostrar, usando indução finita, que $16^t \equiv_{10} 6$ para todo inteiro $t \geq 1$. Usando este fato, obtemos $2 \cdot 16^t \equiv_{10} 12$. Por esta razão,

$$n = 2 \cdot (16)^{2m} - 16^m \equiv_{10} 12 - 6 \equiv_{10} 6.$$

Se $k = 4m + 3$, então

$$\begin{aligned} n = 2^{4m+2}(2^{4m+3} - 1) &= 2^{8m+5} - 2^{4m+2} \\ &= 2 \cdot 2^{8m+4} - 2^2 \cdot 2^{4m} \\ &= 2 \cdot 16^{(2m+1)} - 4 \cdot 16^m, \end{aligned}$$

de modo que

$$n \equiv_{10} 2 \cdot 6 - 4 \cdot 6 \equiv_{10} -12 \equiv_{10} 8.$$

Portanto, todo número perfeito par tem seu último dígito igual a 6 ou 8. □

Dois Resultados Relacionados a Números Perfeitos Ímpares

Ainda não se conhece nenhum número perfeito ímpar e não se tem nenhuma comprovação sobre a existência ou não de tais números. Mas, se um perfeito ímpar existir, já se sabe que ele deve ter mais de 300 dígitos e atender condições muito específicas. Por isso, conjectura-se que não existe nenhum número perfeito ímpar.

Vamos considerar dois resultados sobre números perfeitos ímpares, cujas provas não serão aqui apresentadas.

Teorema 4.2.7 (Euler) *Se n é um número perfeito ímpar, então*

$$n = p_1^{k_1} p_2^{2k_2} \cdots p_r^{2k_r},$$

em que p_i's são primos ímpares distintos e $p_1 \equiv_4 k_1 \equiv_4 1$.

Por conseguinte,

Corolário 4.2.8 *Se n é um número perfeito ímpar, então n é da forma*

$$n = p^k m^2,$$

com p primo, $p \nmid m$, e $p \equiv_4 k \equiv_4 1$. Em particular, $n \equiv_4 1$.

4.3 Números Amigáveis

Dois números naturais m e n são ditos **amigáveis** quando cada um deles é igual a soma de todos os divisores positivos do outro, exceto o próprio número, ou seja, quando

$$m = \sigma(n) - n \quad \text{e} \quad n = \sigma(m) - m.$$

Logo,

$$m = \sigma(n) - \sigma(m) + m,$$

isto é, $\sigma(m) = \sigma(n)$. Daí, $m+n = 2\sigma(n) - (n+m)$, ou melhor, $\sigma(n) = m+n$. Por isso, m e n são amigáveis se, e somente se,

$$\sigma(m) = \sigma(n) = m+n.$$

Neste caso, dizemos também que (m,n) é um **par de números amigáveis**.

Por exemplo, os números $m = 220$ e $n = 284$ são amigáveis (o menor par entre os amigáveis, no sentido de m e n serem os menores possíveis). De fato,

$$\sigma(220) = \sigma(2^2 \cdot 5 \cdot 11) = (2^3 - 1) \cdot 6 \cdot 12 = 504$$

e

$$\sigma(284) = \sigma(2^2 \cdot 71) = (2^3 - 1) \cdot 72 = 504.$$

Assim,

$$\sigma(220) = \sigma(284) = 504 = 220 + 284 = m + n.$$

A descoberta deste par de números é atribuída a Pitágoras. Um outro par de números amigáveis é composto pelos números 1184 e 1210 e outro por 17296 e 18416. A descoberto desse último par é atribuída a Fermat. Entretanto, alguns historiadores afirmam que este par foi descoberto primeiramente por Ibn al-Banna[1] e por Kamaladdin Farsi no século XIV.

De acordo com relatos históricos, Thabit[2] foi o primeiro a descrever um método para a construção de pares de números amigáveis. Seu método consiste em considerar números x, y e z dados por

$$x = t + 2^n, \quad y = t - 2^{n-1}, \quad z = (2^{n+1} + 2^{n-2})2^{n+1} - 1,$$

com $n \geq 2$ e $t = 1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

Eliminando o parâmetro t de x e y, e simplificando as expressões, obtemos

$$x = 3 \cdot 2^n - 1, \quad y = 3 \cdot 2^{n-1} - 1, \quad z = 9 \cdot 2^{2n-1} - 1.$$

Thabit mostrou que se x, y e z são todos primos, então

$$m = 2^n \cdot x \cdot y \quad \text{e} \quad n = 2^n \cdot z$$

são amigáveis, conforme o seguinte:

Teorema 4.3.1 *Nas condições anteriores,*

$$m = 2^n \cdot x \cdot y \quad e \quad n = 2^n \cdot z$$

são amigáveis.

Demonstração: Como $x = 3 \cdot 2^n - 1$, $y = 3 \cdot 2^{n-1} - 1$ e $z = 9 \cdot 2^{2n-1} - 1$ são primos,

$$\sigma(x) = x + 1 = 3 \cdot 2^n, \quad \sigma(y) = y + 1 = 3 \cdot 2^{n-1}, \quad \sigma(z) = 9 \cdot 2^{2n-1}.$$

Assim,

$$\begin{aligned} \sigma(m) &= \sigma(2^n \cdot x \cdot y) \\ &= \sigma(2^n)\sigma(x)\sigma(y) \\ &= (2^{n+1} - 1)(3 \cdot 2^n)(3 \cdot 2^{n-1}) \\ &= 9 \cdot 2^{2n-1}(2^{n+1} - 1) \end{aligned}$$

[1] Ibn al Banna (1256-1321) foi educado no Marrocos, tendo contato com o grande conhecimento matemático árabe que vinha em constante desenvolvimento nos últimos 400 anos. Estudou geometria em geral e os *Elementos* de Euclides, em particular. Lecionou todos os ramos da matemática e escreveu diversas obras nas áreas de aritmética, algébra, geometria e astronomia.

[2] Thabit Ibn Qurra (824-901) é um famoso matemático árabe, além de médico, filósofo e linguista, que vivei no século IX. Além de ser responsável por uma das melhores traduções dos *Elementos* de Euclides também produziu diversos trabalhos sobre astronomia e cônicas, e ainda foi o primeiro a descrever um método para obtenção de um par de números amigáveis.

e

$$\begin{aligned}\sigma(n) &= \sigma(2^n \cdot z)\\ &= \sigma(2^n)\sigma(z)\\ &= (2^{n+1}-1)(9\cdot 2^{2n-1})\\ &= 9\cdot 2^{2n-1}(2^{n+1}-1).\end{aligned}$$

Logo, $\sigma(m) = \sigma(n)$. Além disso,

$$\begin{aligned}m+n &= 2^n\cdot(3\cdot 2^n-1)(3\cdot 2^{n-1}-1)+2^n(9\cdot 2^{2n-1}-1)\\ &= 2^n[(3\cdot 2^n-1)(3\cdot 2^{n-1}-1)+(9\cdot 2^{2n-1}-1)]\\ &= 2^n[9\cdot 2^{2n-1}-3\cdot 2^n-3\cdot 2^{n-1}+9\cdot 2^{2n-1}]\\ &= 2^n[9\cdot 2^{2n-1}-3\cdot 2\cdot 2^{n-1}-3\cdot 2^{n-1}+9\cdot 2^{2n-1}]\\ &= 2^n[18\cdot 2^{2n-1}-9\cdot 2^{n-1}]\\ &= 2^n[9\cdot 2^{n-1}(2^{n+1}-1)]\\ &= 2^n[9\cdot 2^{n-1}(2\cdot 2^n-1)]\\ &= 9\cdot 2^{2n-1}(2^{n+1}-1).\end{aligned}$$

Portanto, $\sigma(m) = \sigma(n) = m+n$, ou seja, m e n são amigáveis. □

Notemos que, para o expoente $n = 2$, temos $x = 11$, $y = 5$ e $z = 71$, que são todos primos. Assim,

$$m = 2^2\cdot 11\cdot 5 = 220 \quad \text{e} \quad n = 2^2\cdot 71 = 284$$

são amigáveis, conforme já tinhamos observado.

O próximo par de números amigáveis, determinado por esse método, é obtido quando o expoente $n = 4$. Para este, temos

$$\begin{aligned}x &= 3\cdot 2^4-1 = 47,\\ y &= 3\cdot 2^3-1 = 23,\\ z &= 9\cdot 2^7-1 = 1151.\end{aligned}$$

Como x, y e z são primos. Então, $m = 2^4\cdot 47\cdot 23 = 17296$ e $n = 2^4\cdot 1151 = 18416$ são um par de números amigáveis.

À medida que o valor de n aumenta, os valores de x, y e z também aumentam e, neste ponto, a tarefa de decidir sobre a primalidade destes números se torna mais árdua.

Baseado no trabalho de Thabit, Euler desenvolveu alguns métodos que geram números amigáveis, descobrindo 59 pares desses números. Desde então, muitos pares de amigáveis foram determinados, a maioria deles com o auxílio dos métodos estabelecidos por Euler.

O próximo teorema apresentará o método de Euler para determinação de números amigáveis, esse resultado generaliza o Teorema 4.3.1. Sua prova é similar à do Teorema de Thabit.

Teorema 4.3.2 (Euler) *Sejam n e r números naturais tais que $1 \leq r < n$, e tomemos $g = 2^{n-r} + 1$. Se*

$$\begin{aligned} x &= 2^n \cdot g - 1, \\ y &= 2^r \cdot g - 1, \\ z &= 2^{n+r} \cdot g^2 - 1 \end{aligned}$$

são todos primos, então $m = 2^n \cdot x \cdot y$ e $k = 2^n \cdot z$ são amigáveis.

Embora não se saiba se existe ou não um número infinito de pares amigáveis, existem alguns métodos que podem ser usados para gerar novos pares a partir de pares conhecidos. O seguinte método é um dos mais bem sucedidos e foi estabelecido por Riele[3]

Teorema 4.3.3 (Riele) *Sejam $m = a \cdot u$ e $n = a \cdot p$ um par de números amigáveis conhecido, com $mdc(a,u) = mdc(a,p) = 1$, sendo p primo. Se existir um par de primos (r,s), com $p < r < s$ e $mdc(a,rs) = 1$, satisfazendo*

$$(r-p)(s-p) = \frac{\sigma(a)}{a}\sigma(u)^2,$$

e se existir um terceiro primo q, com $mdc(au,q) = 1$ e

$$q = r + s + u,$$

então $m_1 = a \cdot u \cdot q$ e $n_1 = a \cdot r \cdot s$ são números amigáveis.

4.4 Problemas Adicionais

Finalizaremos nosso trabalho com alguns problemas relacionados a números perfeitos e números amigáveis, alguns, dentre os quais, com destaque especial, devido à sua importância dentro do contexto. Uns são problemas propostos nos livros-texto, e outros são clássicos do assunto. É importante ressaltar que tais problemas são específicos e tópicos de estudo da disciplina Aritmética/MA14, componente obrigatório do Curso de Mestrado Profissional em Matemática/Profmat. Sendo assim, a elaboração de um conjunto de problemas, com as respectivas soluções, atende aos requisitos do programa de mestrado e, além disso, consiste em nossa contribuição ao trabalho de conclusão de curso.

Exemplo 4.4.1 Mostrar cada uma das seguintes afirmações:

(a) *Se p é primo e $n = p^k$, com $k \in \mathbb{N}$, então n não é perfeito.*

(b) *O produto de dois primos ímpares p e q não é um número perfeito.*

[3]Herman J. J. Riele é um centista sênior do Centro de Matemática e Ciência da Computação (CWI), em Amsterdã. Possui contribuições importantes na área da Teoria dos Números Computacional.

Solução: (a) Suponhamos, por absurdo, que n é um número perfeito. Logo,

$$\sigma(n) = 2p^k.$$

Como $\sigma(n) = \sigma(p^k) = (p^k - 1)(p-1)$, temos

$$\frac{p^k - 1}{p-1} = 2p^k.$$

Desta igualdade, segue que p^k divide 1, uma contradição. Por isso, $n = p^k$ não é perfeito.

(b) Por absurdo, assumamos pq perfeito, com p e q primos, ou seja, $\sigma(pq) = 2pq$. Por outro lado, $\sigma(pq) = 1 + p + q + pq$, isto é,

$$2pq = 1 + p + q + pq.$$

Desse modo, $(p-1)(q-1) = 2$, uma contradição, já que $(p-1)(q-1) > 2$. △

Exemplo 4.4.2 Sejam n um número perfeito e $p > 2$ um primo, com $n = pa$ e $mdc(a, p) = 1$. Mostrar que $\sigma(a) \mid n$.

Solução: Como $n = pa$ e $mdc(a, p) = 1$,

$$\sigma(n) = \sigma(p) \cdot \sigma(a).$$

Por outro lado, já que n é perfeito, $\sigma(n) = 2n$. Daí, $2n = (p+1)\sigma(a)$, ou seja,

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

Uma vez que $p+1$ é par, então $(p+1)/2$ é um número inteiro. Por conseguinte, $\sigma(a) \mid n$.△

Exemplo 4.4.3 Se n é um número perfeito par, provar que $\sum_{d|n} 1/d = 2$.

Solução: Sejam $1, d_1, d_2, \ldots, d_k, n$ os divisores positivos de n. Logo,

$$\sigma(n) = 1 + d_1 + d_2 + \cdots + d_k + n.$$

Visto que, por hipótese, n é perfeito, então $\sigma(n) = 2n$ e, com isto,

$$\frac{1}{n} + \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} + 1 = 2,$$

ou melhor, $\sum_{d|n} 1/d = 2$. △

Exemplo 4.4.4 Mostrar que se d é um divisor próprio de um número perfeito, então d não pode ser perfeito.

Solução: Suponhamos, por absurdo, que d é um número perfeito. Por hipótese, d é divisor próprio de n. Sendo $1, d_1, d_2, \ldots, d, \ldots, d_k, n$ os divisores positivos de n, então, do Exemplo 4.4.3,

$$1 + \frac{1}{d_1} + \cdots + \frac{1}{d_k} + \frac{1}{n} = 2.$$

Mas, como d é perfeito e todo divisor de d é, necessariemente, um divisor de n, então o lado direto da soma acima é maior do que 2, uma contradição. Portanto, d não é um número perfeito. △

Para o exemplo que segue, recordemos do conceito de número triangular. Um número natural a é chamado **número triangular** se a é igual a soma de inteiros consecutivos, começando com 1, ou seja, se existe $n \in \mathbb{N}$, com

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

Os inteiros 1, 3 e 6 são triangulares, pois

$$1 = 1, \quad 3 = 1 + 2 \quad \text{e} \quad 6 = 1 + 2 + 3.$$

Já 5 e 7 não são, pois $1 + 2 + k = 5$ implica $k = 2$, e $1 + 2 + 3 + r = 7$ acarreta $r = 1$.

Exemplo 4.4.5 Provar que todo número perfeito par é triangular.

Solução: Se n é perfeito (par), então, do Teorema 4.2.4, $n = 2^{k-1}(2^k - 1)$, em que $2^k - 1$ é primo e $k > 2$. Dessa forma, pondo $a = 2^k - 1$, obtemos

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

ou seja, n é um número triangular. △

Exemplo 4.4.6 Um número n é chamado k-**perfeito** quando $\sigma(n) = kn$, com $k \geq 3$. Mostrar que:

(a) $n = 2^9 \cdot 3 \cdot 11$ não é 3-perfeito e $m = 2^5 \cdot 3^3 \cdot 5 \cdot 7$ é 4-perfeito.

(b) Se n é 3-perfeito e $3 \nmid n$, então $3n$ é 4-perfeito.

(c) $n = 120$ e $m = 672$ são os únicos 3-perfeitos da forma $2^k \cdot 3 \cdot p$, em que p é um primo ímpar.

Solução: (a) Queremos provar que $\sigma(n) = 3n$. Com efeito,

$$\begin{aligned} \sigma(n) &= \sigma(2^9) \cdot \sigma(3) \cdot \sigma(11) \\ &= (2^{10} - 1) \cdot 4 \cdot 12 \\ &= 1023 \cdot 4 \cdot 12 \\ &= 49104 \\ &\neq 3n \end{aligned}$$

Assim, n não é um número 3-perfeito. Agora, verifiquemos que m é um número 4-perfeito. De fato,

$$\begin{aligned}\sigma(m) &= \sigma(2^5)\cdot\sigma(3^3)\cdot\sigma(5)\cdot\sigma(7)\\ &= (2^6-1)\cdot\tfrac{(3^4-1)}{(3-1)}\cdot 6\cdot 8\\ &= 63\cdot 40\cdot 6\cdot 8\\ &= 120960.\end{aligned}$$

Por outro lado,

$$4m = 2^7\cdot 3^3\cdot 5\cdot 7 = 128\cdot 27\cdot 35 = 120960.$$

Por isso, m é um número 4-perfeito.

(b) Como n é 3-perfeito, $\sigma(n) = 3n$. Por hipótese $3 \nmid n$ e, com isto,

$$\begin{aligned}\sigma(3n) &= \sigma(3)\cdot\sigma(n)\\ &= 4\cdot\sigma(n)\\ &= 4\cdot(3n).\end{aligned}$$

Concluímos assim que $3n$ é 4-perfeito.

(c) Tomemos $n = 2^k\cdot 3\cdot p$ e verifiquemos para quais valores de k e p o número n é 3-perfeito. Façamos, pois, $\sigma(n) = 3n$. Calculando $\sigma(n)$, temos

$$\begin{aligned}\sigma(n) &= \sigma(2^k)\cdot\sigma(3)\cdot\sigma(p)\\ &= (2^{k+1}-1)\cdot(3+1)\cdot(p+1)\\ &= (2^{k+1}\cdot 3+2^{k+1}-3-1)\cdot(p+1)\\ &= 2^{k+1}\cdot 3\cdot p+2^{k+1}\cdot 3+2^{k+1}\cdot p+2^{k+1}-3p-3-p-1\\ &= 2n+2\cdot 2^k\cdot(3+p+1)-(4p+4).\end{aligned}$$

Da igualdade $\sigma(n) = 3n$, vem que

$$2^k = \frac{4p+4}{8-p}.$$

Por isso, $p < 8$, e já que $p > 3$, obtemos $p = 5$ ou $p = 7$.

Para $p = 5$, temos $2^k = 8$, ou melhor, $k = 3$. Dessa forma $n = 2^3\cdot 3\cdot 5 = 120$. Já para $p = 7$, $2^k = 32$, isto é, $k = 5$ e $n = 2^5\cdot 3\cdot 7 = 672$. Por essa razão, os números 3-perfeitos da forma $2^k\cdot 3\cdot p$ são 120 e 672. △

Exemplo 4.4.7 Se n é um número perfeito ímpar, mostrar que n tem pelo menos três divisores primos distintos.

Solução: Por contradição, assumamos que n tem no máximo dois divisores primos distintos. Assim, de acordo com o Teorema 4.2.7, $n = p^k q^{2\alpha}$, com $p \equiv k \equiv 1 \pmod 4$. Visto que n é

perfeito, então $\sigma(n) = 2n$. Daí,

$$2 = \frac{\sigma(n)}{n} = \frac{p^k q^{2\alpha}(1-1/p)(1-1/q)}{p^k q^{2\alpha}} = \left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right),$$

ou seja,

$$2 = \left(\tfrac{p-1}{p}\right)\left(\tfrac{q-1}{q}\right).$$

Uma vez que $(p-1)/p < p/(p-1)$ e $(q-1)/q < q/(q-1)$, temos

$$2 < \left(\tfrac{p}{p-1}\right)\left(\tfrac{q}{q-1}\right).$$

Agora, $p \equiv 1 \pmod 4$, isto é $p = 4a+1$ para algum inteiro positivo a. Quanto ao primo q, há duas possibilidades: $p \equiv 1 \pmod 4$ ou $p \equiv 3 \pmod 4$. Consideremos, primeiramente, $q = 4b+1$, em que b é um inteiro positivo. Com isto,

$$2 < \left(\tfrac{4a+1}{4a}\right)\left(\tfrac{4b+1}{4b}\right) = \tfrac{1}{16ab} + \tfrac{1}{4a} + \tfrac{1}{4b} + 1 < 2,$$

uma contradição. Por outro lado, se $q = 4b+3$, então

$$2 < \left(\tfrac{4a+1}{4a}\right)\left(\tfrac{4b+3}{4b+2}\right) = \tfrac{3}{4(2a+4ab)} + \tfrac{3a}{2a+4ab} + \tfrac{b}{2a+4ab} + \tfrac{4ab}{2a+4ab} < 2,$$

outra contradição, e esta contradição prova que n tem pelo menos três divisores primos distintos. △

Para a solução do exercício seguinte, vamos lançar mão do seguinte resultadoSendo d um divisor de n, n/d também o é. Por isso, se $d_1, d_2, \ldots, d_k$ são todos os divisores positivos de n, então

$$\{d_1, d_2, \ldots, d_k\} = \{n/d_1, n/d_2, \ldots, n/d_k\}.$$

Desse modo, considerando λ a soma dos inversos de $d_1, d_2, \ldots, d_k$, ou seja, $\lambda = 1/d_1 + 1/d_2 + \cdots + 1/d_k$, temos

$$\begin{aligned} n\lambda &= n/d_1 + n/d_2 + \cdots + n/d_k \\ &= d_1 + d_2 + \cdots + d_k \\ &= \sigma(n). \end{aligned}$$

Logo, $\lambda = \sigma(n)/n$, isto é,

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}. \tag{4.2}$$

Exemplo 4.4.8 Se m e n são números amigáveis, mostrar que

$$\left(\textstyle\sum_{d|m} 1/d\right)^{-1} + \left(\textstyle\sum_{d|n} 1/d\right)^{-1} = 1.$$

Solução: Visto que m e n são números amigáveis, então, por definição,

$$\sigma(n) = \sigma(m) = n + m.$$

Desse modo, de (4.2),

$$\left(\sum_{d|m} 1/d\right)^{-1} + \left(\sum_{d|n} 1/d\right)^{-1} = \frac{n}{\sigma(n)} + \frac{m}{\sigma(m)} = \frac{n}{\sigma(n)} + \frac{m}{\sigma(n)} = \frac{n+m}{\sigma(n)} = \frac{\sigma(n)}{\sigma(n)} = 1.$$

Isto conclui a solução. △

Exemplo 4.4.9 Use o método de Thabit a fim de mostrar que $n = 2^7 \cdot 191 \cdot 383$ e $m = 2^7 \cdot 73727$ são amigáveis.

Solução: Vamos utilizar o método de Thabit, com

$$\begin{aligned} x &= 3 \cdot 2^7 - 1 = 383, \\ y &= 3 \cdot 2^6 - 1 = 191 \end{aligned}$$

e $z = 9 \cdot 2^{13} - 1 = 73727$. Usando o crivo de Eratóstenes, verifica-se, sem dificuldade, que x, y e z são todos primos. Dessa forma, pelo Teorema 4.3.1, os números

$$\begin{aligned} n &= 2^7 \cdot 191 \cdot 583 = 9363584 \\ m &= 2^7 \cdot 73727 = 9437056. \end{aligned}$$

formam um par de números amigáveis. △

Exemplo 4.4.10 Provar o Teorema 4.3.2, ou seja, tomemos n e r números naturais tais que $1 \leq r < n$, e $g = 2^{n-r} + 1$. Se

$$\begin{aligned} x &= 2^n \cdot g - 1, \\ y &= 2^r \cdot g - 1, \\ z &= 2^{n+r} \cdot g^2 - 1 \end{aligned}$$

são todos primos, então $m = 2^n \cdot x \cdot y$ e $k = 2^n \cdot z$ são amigáveis.

Solução: Sejam n e r números naturais tais que $1 \leq r < n$, e tomemos $g = 2^{n-r} + 1$. Se

$$\begin{aligned} x &= 2^n \cdot g - 1, \\ y &= 2^r \cdot g - 1, \\ z &= 2^{n+r} \cdot g^2 - 1 \end{aligned}$$

são todos primos, então $m = 2^n \cdot x \cdot y$ e $k = 2^n \cdot z$ são amigáveis. Primeiramente, devemos verificar se $\sigma(m) = \sigma(k)$, em que $m = 2^n \cdot x \cdot y$ e $k = 2^n \cdot z$. Calculando $\sigma(m)$ e $\sigma(k)$, temos

$$\begin{aligned} \sigma(m) = \sigma(2^n \cdot x \cdot y) &= \sigma(2^n) \cdot \sigma(x) \cdot \sigma(y) \qquad \text{(por hipótese } x, y \text{ são primos)} \\ &= (2^{n+1} - 1) \cdot (2^n \cdot g) \cdot (2^r \cdot g) \\ &= (2^{n+1} - 1) \cdot (2^{n+r} \cdot g^2) \\ &\quad 2^{2n+r+1} \cdot g^2 - 2^{n+r} \cdot g^2, \end{aligned}$$

e

$$\begin{aligned}\sigma(k) &= \sigma(2^n \cdot z) &= \sigma(2^n)\cdot\sigma(z) && \text{(por hipótese } z \text{ é primo)}\\ &&= (2^{n+1}-1)\cdot(2^{n+r}\cdot g^2)\\ &&= 2^{2n+r+1}\cdot g^2 - 2^{n+r}\cdot g^2.\end{aligned}$$

Portanto, $\sigma(m) = \sigma(k)$. Para garantir que esse números são amigáveis, precisamos mostrar que $\sigma(m) = \sigma(k) = m+k$. Calculando $m+k$, obtemos

$$\begin{aligned}m+k &= 2^n\cdot x\cdot y + 2^n\cdot z &= 2^n\cdot[(2^n\cdot g-1)\cdot(2^r\cdot g-1)+2^{n+r}\cdot g^2-1]\\ &&2^n\cdot(2^{n+r}\cdot g^2 - 2^n\cdot g - 2^r\cdot g + 1 + 2^{n+r}\cdot g^2 - 1)\\ &&2^n\cdot(2^{n+r+1}\cdot g^2 - 2^n\cdot g - 2^r\cdot g)\\ &&2^{2n+r+1}\cdot g^2 - 2^{2n}\cdot g - 2^{n+r}\cdot g.\end{aligned}$$

Como $g = 2^{n-r}+1$,

$$m+k = 2^{4n-r+1} + 2^{3n+2} + 2^{2n+r+1} - 2^{3n-r} - 2^{2n+1} - 2^{n+r}.$$

Por isso, $\sigma(m) = \sigma(k) = m+k$ e, assim, m e k formam um par de números amigáveis. △

Um número natural n diz-se **abundante** se $\sigma(n) > 2n$, e diz-se **deficiente** se $\sigma(n) < 2n$.

Exemplo 4.4.11 Mostrar que existem infinitos números abundantes, bem como infinitos números deficientes.

Solução: Visto que todo primo é deficiente, então, existem infinitos números deficientes. Para os números abundantes, consideremos $n = 2^k\cdot 3$, em que $k > 1$. Daí,

$$\begin{aligned}\sigma(n) &= \sigma(2^k)\cdot\sigma(3)\\ &= (2^{k+1}-1)\cdot(3+1)\\ &= 2\cdot 2^k\cdot 3 + 2^{k+1} - 3 - 1\\ &= 2n + 2^{k+1} - 4.\end{aligned}$$

Como $k > 1$, temos $2^{k+1} - 4 > 0$, ou seja, $\sigma(n) > 2n$. Isto conclui a solução. △

Exemplo 4.4.12 Mostrar que:

(a) Qualquer número perfeito ímpar n pode ser representado na forma $n = pa^2$, em que p é primo.

(b) Se $n = pa^2$ é um número perfeito ímpar, então $n \equiv_8 p$.

Solução: (a) Como n é perfeito ímpar, então $n = p^k m^2$, em que $p \nmid m$ e $p \equiv_4 k \equiv_4 1$. Ou seja, $k-1 = 4\alpha$, com $\alpha \in \mathbb{Z}$. Logo,

$$\begin{aligned} n &= p^{4\alpha+1} m^2 \\ &= p(p^{2\alpha})^2 m^2 \\ &= pa^2, \end{aligned}$$

em que $a = p^{2\alpha} m$.

(b) Sendo $n = pa^2$ um número perfeito ímpar, então, a é necessariamente ímpar, ou seja, $a = 2r+1$. Visto que o quadrado de qualquer inteiro ímpar é congruente a 1 módulo 8, temos $a^2 \equiv_8 1$. Assim, $pa^2 \equiv_8 p$, ou seja, $n \equiv_8 p$. $\triangle$

Referências Bibliográficas

[1] EVES, H. *Introdução à História da Matemática*, (3ª edição), Editora da Unicamp, Campinas, 2008.

[2] MARQUES, S. C. *A descoberta do Teorema de Pitágoras* (1ª edição). Livraria da Física, São Paulo, 2011.

[3] SING, S. *O Último Teorema de Fermat: a história que confundiu as mais brilhantes mentes do mundo durante 358 anos* (3ª edição). BestBolso, Rio de Janeiro, 2018.

[4] VIEIRA, V. L. *Álgebra Abstrata para Licenciatura* (2ª edição). Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2015.

[5] VIEIRA, V. L. – *Um Curso Básico em Teoria dos Números*, Editora da Universidade Estadual da Paraíba (coedição: Editora Livraria da Física), Campina Grande/São Paulo, 2019.

[6] HEFEZ, A. ARITMÉTICA (2ª edição). *Sociedade Brasileira de Matemática*, Rio de Janeiro, 2016.

[7] RIBENBOIM, P. *Números Primos: Velhos Mistérios e Novos Recordes*. IMPA, CMU, Rio de Janeiro, 2012.

[8] COUTINHO, S. C. *Números inteiros e Criptografia RSA* (2ª edição). IMPA, Rio de Janeiro, 2014.

[9] Connor, J.J O'. al-Marrakushi ibn Al-Banna. *MacTutor History of Mathematics archive*, Escócia, 1999. Disponível em: <http://mathshistory.st-andrews.ac.uk/Biographies/Al-Banna.html>. Acesso em: 09 de Fevereiro de 2020.