Universidade Estadual da Paraíba
Centro de Ciências e Tecnologia
Departamento de Matemática

Os Teoremas de Fermat, Euler e Wilson

JOSÉ CLÁUDIO DA SILVA TEODISTA

Trabalho de conclusão de curso

Trabalho de Conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para a obtenção do título de licenciado em Matemática.

23 de janeiro de 2013
Campina Grande – PB

JOSÉ CLÁUDIO DA SILVA TEODISTA

Os Teoremas de Fermat, Euler e Wilson

Trabalho de Conclusão de Curso apresentado na Universidade Estadual da Paraíba, como parte dos requisitos exigidos para a obtenção do título de licenciado em Matemática.

Orientador: Prof. Dr. Vandenberg Lopes Vieira

23 de janeiro de 2013
Campina Grande – PB

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL – UEPB

T314t Teodista, José Claudio da Silva.

Os Teoremas de Fermat, Euler e Wilson. [manuscrito] / José Claudio da Silva Teodista. – 2013.

58 f. : il. color.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2013.

"Orientação: Prof. Dr. Vandenberg Lopes Vieira, Departamento de Matemática".

1. Números inteiros. 2. Números primos. 3. Teoremas. I. Título.

21. ed. CDD 512

JOSÉ CLÁUDIO DA SILVA TEODISTA

OS TEOREMAS DE FERMAT, EULER E WILSON

Monografia apresentada no Curso de Licenciatura Plena em Matemática da Universidade Estadual da Paraíba, em cumprimento às exigências para obtenção do Título de Licenciado em Matemática.

BANCA EXAMINADORA

Prof. Dr. Vandenberg Lopes Vieira
Departamento de Matemática – CCT/UEPB
Orientador

Prof. Dr. Aldo Trajano Lourêdo
Departamento de Matemática – CCT/UEPB
Examinador

Prof. Msc. Fernando Luiz T. Silva
Departamento de Matemática – CCT/UEPB
Examinador

Campina Grande, 23 de Janeiro de 2013

Ao meu pai Cícero Teodista da Silva
(in memorian) e à minha Maria da
Conceição da Silva.

DEDICO

Agradecimentos

À força maior que rege todas as coisas existentes, que me deu saúde, coragem e disposição para que eu pudesse concluir essa importante etapa de minha vida – meu grande e generoso Deus – sem o qual nada seria possível.

À minha família, (irmãos: Claudenor, Jocélio, Tito, Selma, Simone; mãe: Conceição) e à minha querida noiva Flávia Shirley, que me aguentaram durante toda essa fase e me deram suporte emocional para que eu pudesse vencer as dificuldades. Ao meu pai Cícero Teodista, que sempre foi um exemplo, desde meu nascimento até o momento que Deus o convidou para o céu.

Aos meus colegas e amigos do curso: Dayse Medeiros, Eliane Dias, Josiel Custódio, Tiago Alves e Wesklemyr Lacerda, com os quais aprendi demais, nas conversas de corredores, nos grupos de estudos, nas discordâncias e com a história de vida de cada um. Vou levar um pouquinho de vocês comigo e espero ter deixado algo de mim com vocês. Às minhas colegas e amigas: Adeilma, Andrea, Eliane Lins e Jucileide que mesmo não tendo concluído o curso comigo, marcaram a mim pelo carisma, personalidade e uma generosidade que eu admiro muito.

Um agradecimento especial ao meu orientador, prof. Dr. Vandenberg Lopes, que generosamente se dispôs a orientar este trabalho. Sem esquecer os professores e ex-professores da uepb: Aldo Trajano, Ernesto, Fernando Luiz, Francisco de Sá, Núbia Martins, Pedro Lúcio e Orlando Almeida que são especiais por qualidades como competência, generosidade, humildade, etc. E de uma maneira geral, a todo o corpo docente da universidade.

Por fim, agradeço a todos que de maneira direta ou indireta contribuíram para a realização desse sonho.

Resumo

O objetivo principal deste trabalho é apresentar a demonstração dos teoremas de Euler, Fermat e Wilson, bem como, alguns exemplos que mostram suas aplicabilidades. Tais teoremas são de suma importância em Teoria dos Números, sendo base para relevantes resultados. Para tanto, foram apresentados alguns resultados prévios sobre os números tais como princípio de indução finita, máximo divisor e mínimo múltiplo comum e números primos. Foram abordados também o conceito de congruência e suas principais propriedades, as quais são úteis no contexto em que o trabalho se insere.

Palavras-chave: Números Inteiros, Congruências, Fermat, Euler, Wilson.

Abstract

The main objective of this paper is to present the proof of the theorems of Euler, Fermat and Wilson, as well as some examples that show their applicability. These theorems are of paramount importance in number theory, and basis for relevant results. Thus, we present some preliminary results about numbers such as the principle of finite induction, divisor and least common multiple and primes. We also addressed the concept of congruence and its main properties, which are useful in the context in which the work is located.

Keywords: Integer, congruences, Fermat, Euler, Wilson.

Sumário

Capítulo 1

Introdução

Em princípio, os números surgiram apenas com o intuito de contar. Talvez esse surgimento tenha se dado por volta de 4000 a.C., com aparecimento das primeiras cidades egípcias e sumérias, onde se desenvolveu o comércio, a agricultura e a criação de animais. Todavia, a concepção de número já existe desde a idade da pedra, onde há registros marcados em ossos e pinturas em cavernas. Porém, o avanço dessa área do conhecimento não se deteve apenas a contagem. Há tempo que o ser humano é incansável pela busca de métodos matemáticos que o ajudem a resolver problemas provenientes de muitos ramos da vida cotidiana e até mesmo problemas mais sofisticados, aplicados as demais ciências. O **papiro de Rhind** ou **papiro de Ahmes**, um documento egípcio, que data de cerca de 1650 a.C, já detalha a solução de 84 problemas ligados à aritmética, progressões, geometria, etc. Ou seja, já existia ali uma matemática bem mais complexa do que aquela que nascera apenas no intuito de contar coisas e objetos.

Uma coleção de livros muito famosa e uma das mais lidas do mundo é "*Os elementos*" de Euclides de Alexandria[1] (360 a.C. – 295 a.C.), esta é muito conhecida pelo conteúdo de geometria que aborda, tornando-se referência no ensino desse ramo da matemática até o início do século XX; contudo, se engana quem pensa que esta obra é exclusivamente sobre geometria. Dois volumes (II e V) de um total de treze volumes

[1]Foi um professor, matemático platônico e escritor possivelmente grego, muitas vezes referido como o "Pai da Geometria". Ele era ativo em Alexandria durante o reinado de Ptolomeu I (323 – 283 a.C.).

são dedicados ao estudo da álgebra e outro três volumes (VII, VIII e IX) são voltados à teoria dos números. Uma observação importante é que os gregos consideravam número como sendo os números naturais, pois os números inteiros negativos só foram aceitos muitos séculos depois. O primeiro uso dos números negativos que se tem notícia data de cerca 628 d.C. e é atribuído a um matemático que viveu na Índia Central chamado Brahmagupta (589 – 668), onde ele interpretou tais números como dívidas.

Talvez os números negativos tenham sido os mais polêmicos da história da matemática. Muitos matemáticos ao encontrarem soluções negativas de equações consideravam essas soluções como impossíveis ou absurdas. Por exemplo, Diofanto (cerca 325 – 409) ao calcular a solução de equações do tipo $3x + 20 = 5$, considerava o problema como absurdo. Tal situação perdurou por muitos séculos, prova disso é que Michael Stifel (1487–1567), em pleno século XVI, não aceitava que um número negativo pudesse ser solução de uma equação. No entanto, Leonard Euler (1707 – 1783) manipulava números negativos com naturalidade. Esse foi o dilema que passara a matemática, enquanto alguns aceitavam os números negativos, outros questionavam sua validade. Mas a partir do século XVIII esse cenário começou a mudar com a descoberta de uma interpretação geométrica para os números positivos e negativos, ou seja, número negativo era segmento de direção oposta ao positivo. Foi a partir daí que os matemáticos começam a enxergar as inúmeras aplicabilidades dos números negativos e sua importância para o desenvolvimento da matemática.

Um subconjunto dos números inteiros ($\mathbb{Z}$) que possue características bem interessantes é o conjunto dos números primos. **Pierre de Fermat** (1601 – 1665), um grande matemático francês, conjecturou que todo número da forma $2^{2^n} + 1$ é primo, em que n é um número natural qualquer. Mas, Euler, um século depois, mostrou que para $n = 5$, a fórmula é falha, pois $2^{2^5} = 4294967297$ é divisível por 641. Até os dias atuais não se base de uma fórmula que gere todos os números primos. Todavia, sabe-se que existem infinitos números primos, pois tal resultado foi provado por Euclides no volume IX de Os Elementos.

Fermat provou que a soma de um cubo jamais resulta outro cubo, ou seja, não

existem x, y e z inteiros não nulos (solução não trivial) tais que $x^3 + y^3 = z^3$. E generalizando seu teorema, propôs e garantiu ter demonstrado o caso geral, isto é, que a equação $x^n + y^n = z^n$ não possui solução inteira não trivial. Nota-se que tem um problema de fácil enunciado, porém desafiou matemáticos por mais de três séculos. Infelizmente ele faleceu sem publicar a demonstração de um dos mais célebres teoremas da história da matemática, conhecido mundialmente como O Último Teorema de Fermat. Tal teorema foi demonstrado, em 1995 por Andrew Wiles, um matemático britânico, que usou muito resultados que não eram conhecidos na época de Fermat, por esses motivos, fica uma dúvida no ar: será mesmo que o Matemático francês realmente havia demonstrado o belíssimo teorema? Ou seria uma maneira de desafiar os outros matemáticos da época? A resposta a essa pergunta, talvez, jamais teremos.

O trabalho está dividido da seguinte forma: no Capítulo 2 deste trabalho abordaremos os principais resultados relacionados aos números inteiros, bem como algumas das principais propriedades inerentes às operações de soma e adição. Enunciaremos e em muitos casos demonstraremos resultados importantes sobre *divisibilidade*, *máximo divisor comum*, *números primos* e outros inerentes. Dentro deste conjunto, daremos significativa importância a um subconjunto com características bastante especiais – os números primos.

No Capítulo 3, apresentaremos os principais resultados relacionados às congruências, de modo que se possa apresentar os resultados principais do trabalho, ou seja, o *Pequeno Teorema de Fermat*, o *Teorema de Eule*r e o *Teorema de Wilson*.

Capítulo 2

Números Inteiros

Entre os conjuntos numéricos, consideramos o conjunto dos números naturais, $\mathbb{N}$, o mais familiar. A denominação "natural" vem do fato, de eles, os naturais, surgirem atrelados em nossa experiência desde os estudos da infância. Não será feita aqui uma apresentação axiomática de $\mathbb{N}$. Indicamos a referência [2] para um estudo sobre $\mathbb{N}$, na qual axiomas e propriedades referentes às operações de adição e multiplicação são abordados.

Vamos considerar propriedades básicas e iniciais inerentes ao conjunto $\mathbb{N}$, mas estudadas em um ambiente mais amplo — o conjunto $\mathbb{Z}$ —, as quais formarão um ponto de partida para obtenção de outras propriedades menos elementares que serão consideradas ao longo do texto.

Existe um processo natural de construção do conjunto $\mathbb{Z}$, a partir do conjunto $\mathbb{N}$, tomando como base a relação de equivalência $\sim$ sobre $\mathbb{N} \times \mathbb{N}$ dada por

$$(a, b) \sim (c, d) \quad \Leftrightarrow \quad a + d = bc.$$

Considera-se então

$$\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim .$$

A partir de então, é possível verificar todas as propriedades iniciais apresentadas a seguir. Esse processo é apresentado em detalhes em um curso de introdução em teoria dos números.

Daremos a seguir uma breve fundamentação axiomática do conjunto dos números

inteiros. Para mais detalhes sugerimos a referência [2].

Sobre o conjunto dos números inteiros

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

existem duas operações de adição " + " e multiplicação " · ", as operações *usuais* de adição e multiplicação, satisfazendo as seguintes propriedades:

($\mathcal{A}_1$) **Associatividade da adição**: dados $a, b, c \in \mathbb{Z}$

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

($\mathcal{A}_2$) **Comutatividade da adição**: dados $a, b \in \mathbb{Z}$

$$a + b = b + a.$$

($\mathcal{A}_3$) **Elemento neutro da adição**: existe um elemento em $\mathbb{Z}$ chamado zero, indicado por

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

($\mathcal{A}_4$) **Existência de inverso aditivo**: dado $a \in \mathbb{Z}$ existe um único elemento $-a \in \mathbb{Z}$, chamado de inverso aditivo de a, tal que

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

($\mathcal{M}_1$) **Associatividade da multiplicação**: dados $a, b, c \in \mathbb{Z}$

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

($\mathcal{M}_2$) **Comutatividade da multiplicação**: $a, b \in \mathbb{Z}$

$$a \cdot b = b \cdot a.$$

($\mathcal{M}_3$) **Existência de elemento neutro da multiplicação**: existe um único elemento em $\mathbb{Z}$, denotado por 1, tal que

$$a \cdot 1 = a, \quad \forall\ a \in \mathbb{Z}.$$

($\mathcal{M}_4$) **Distributividade da multiplicação sobre a adição**: dados $a, b, c \in \mathbb{Z}$

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

($\mathcal{M}_5$) **Lei do cancelamento da multiplicação**: dados $a, b, c \in \mathbb{Z}$, com $a \neq 0$, tem-se que

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

2.1 Algumas Propriedades Elementares

Os resultados que seguem podem ser deduzidos dos axiomas acima citados.

Proposição 2.1 *Sejam a, b e c inteiros quaisquer. Valem:*

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

(2) *Se $a + b = a + c$, então $b = c$.* **(propriedade cancelativa da adição)**

(3) *Se $a \cdot b = 0$, então $a = 0$ ou $b = 0$.* **(integridade de $\mathbb{Z}$)**

Demonstração: (1) Temos que

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

ou seja,

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

Como $a \cdot 0 \in \mathbb{Z}$, então existe $-(a \cdot 0) \in \mathbb{Z}$ tal que $-(a \cdot 0) + (a \cdot 0) = 0$. Logo, adicionando a ambos os membros da igualdade $a \cdot 0 + a \cdot 0 = a \cdot 0$, e usando a propriedade associativa da adição, obtemos

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

isto é,

$$0 + a \cdot 0 = 0 \;\; \Rightarrow \;\; a \cdot 0 = 0.$$

(2) Similar ao que foi feito na demonstração do item (1), vamos adicionar $-a$ a ambos os membros de $a+b=a+c$. Desse modo,

$$(-a)+(a+b)=(-a)+(a+c) \;\Rightarrow\; ((-a)+a)+b=((-a)+a)+c.$$

Portanto,

$$0+b=0+c \;\Rightarrow\; b=c.$$

(3) Pelo item (1), temos que $a\cdot 0=0$, e por hipótese, $a\cdot b=0$; por isso, $a\cdot b=a\cdot 0$. Se $a=0$, o resultado segue naturalmente. Caso contrário, usando a lei do cancelamento da multiplicação,

$$a\cdot b=a\cdot 0 \;\Rightarrow\; b=0.$$

■

A próxima proposição nos lembra algo que conhecemos desde o estudo básico sobre os inteiros. São resultados que envolvem as regras dos sinais.

Proposição 2.2 *Se a e b são inteiros quaisquer, então:*

(1) $-(-a)=a$.

(2) $(-a)\cdot(b)=-(a\cdot b)=a\cdot(-b)$.

(3) $(-a)\cdot(-b)=a\cdot b$.

Demonstração: (1) Notemos que por definição, se $a,b\in\mathbb{Z}$ e $a+b=0$, então $a=-b$. Por isso, como $a+(-a)=0$, segue imediato que

$$a=-(-a).$$

(2) Temos

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

ou seja,

$$(-a)\cdot(b)=-(a\cdot b).$$

Da mesma forma,

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

de modo que

$$a \cdot (-b) = -(a \cdot b).$$

Portanto,

$$(-a) \cdot (b) = -(a \cdot b) = a \cdot (-b).$$

(3) Usando inicialmente o item (2),

$$(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)).$$

Agora, pelo item (1), sabemos que $-(-a) = a$ para todo $a \in \mathbb{Z}$. Portanto,

$$(-a) \cdot (-b) = a \cdot b.$$

■

Sobre o conjunto $\mathbb{Z}$ também está definida uma relação "menor ou igual", simbolizada por " $\leq$ ". Há três importantes propriedades desta relação, que são:

Propriedade reflexiva: para todo inteiro a,

$$a \leq a.$$

Propriedade anti-simétrica: dados os inteiros a e b, se $a \leq b$ e $b \leq a$, então $a = b$.

Propriedade transitiva: dados os inteiros a, b e c, se $a \leq b$ e $b \leq c$, então $a \leq c$.

Com estas propriedades satisfeitas, diz-se então que a relação " $\leq$ " é uma *relação de ordem*[1].

Usa-se o símbolo $a < b$ (lê-se: a é *menor* que b) para indicar que $a \leq b$, mas $a \neq b$. Além disso, é comum usar os símbolos $b \geq a$ ou $b > a$ para indicar que $a \leq b$ ou $a < b$, respectivamente. Um número $a \in \mathbb{Z}$ é dito **positivo** quando $0 < a$; e é dito **negativo** se $a < 0$.

A relação " $\leq$ " permite comparar quaisquer dois elementos de $\mathbb{Z}$, ou seja,

[1]Este conceito pode ser considerado sobre um conjunto não vazio qualquer (cf. [**?**]).

Lei da Tricotomia: para quaisquer inteiros a e b, tem-se que

$$a < b, \quad a = b \quad \text{ou} \quad b < a.$$

Duas propriedades da relação " $\leq$ " que se relacionam com as operações de adição e multiplicação são as seguintes:

Compatibilidade com a adição: se $a, b, c \in \mathbb{Z}$, então

$$a \leq b \;\Rightarrow\; a + c \leq b + c.$$

Compatibilidade com a multiplicação: dados $a, b, c \in \mathbb{Z}$, se $0 \leq c$, então

$$a \leq b \;\Rightarrow\; ac \leq bc.$$

Definiremos posteriormente a potência não negativa de um inteiro $a \in \mathbb{Z}^*$. Para apresentar o teorema que segue, vamos adiantar um caso particular, considerando que $a \cdot a = a^2$.

Teorema 2.1 *Seja a um número inteiro. Temos que:*

(1) *Se $a \leq 0$, então $-a \geq 0$.*

(2) *Se $a \geq 0$, então $-a \leq 0$.*

(3) $a^2 \geq 0$. **(todo quadrado é não negativo)**

(4) $1 > 0$.

Demonstração: (1) Se $a \leq 0$, então somando $-a$ a ambos membros e usando a compatibilidade com a adição, obtemos

$$-a + a \leq -a + 0 = 0,$$

ou seja, $-a \geq 0$.

(2) É similar ao item (1).

(3) Se $a \geq 0$, então multiplicando ambos os lados desta desigualdade por a e por meio da compatibilidade com a multiplicação, segue que

$$a \cdot a \geq a \cdot 0 = 0 \;\Rightarrow\; a^2 \geq 0.$$

Agora, se $a < 0$, então pelo item (1), $-a > 0$ e, assim, $(-a)(-a) > 0$. Mas, pelo item (3) da Proposição 2.2, sabemos que $(-a)(-a) = aa = a^2$. Portanto, $a^2 \geq 0$.

(4) Como $1 = 1 \cdot 1$ e $1 \neq 0$, então pelo item (3), temos que $1 > 0$. ■

Os resultados a seguir são obtidos diretamente do Teorema 2.1.

Corolário 2.1 *Se a e b são inteiros quaisquer, valem:*

(1) *Se $a \leq b$, então $-a \geq -b$.*

(2) *Se $a \geq 0$ e $b \leq 0$, então $ab \leq 0$.*

(3) *Se $a \leq 0$ e $b \leq 0$, então $ab \geq 0$.*

Definição 2.1 *Consideremos um inteiro a. O **valor absoluto**[2] de a (ou **módulo** de a), em símbolos $|a|$, é definido como segue:*

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

Segue imediatamente da definição que $|a| \geq 0$, para todo $a \in \mathbb{Z}$, e que $|a| = 0$ se, somente se, $a = 0$. Por exemplo, $|5| = 5$ e $|-8| = 8$.

Proposição 2.3 *Para $a, b, c \in \mathbb{Z}$, valem as propriedades:*

(1) $|a \cdot b| = |a| \cdot |b|$.

(2) $-|a| \leq a \leq |a|$.

(3) $|a| \leq c \;\Leftrightarrow\; -c \leq a \leq c$.

(4) $|a + b| \leq |a| + |b|$. **(Desigualdade triangular)**

Demonstração: (1) Se $a \geq 0$ e $b \geq 0$, então $ab \geq 0$ (compatibilidade com a multiplicação). Assim,

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

[2]Esta definição se estende para qualquer número real x.

Se $a \geq 0$ e $b \leq 0$, então $ab \leq 0$. Logo,

$$|a \cdot b| = -(ab) = a(-b) = |a| \cdot |b| .$$

Os casos $a \leq 0$, $b \geq 0$ e $a \leq 0$, $b \leq 0$ são tratados de modo similar.

(2) O resultado desse item é obtido diretamente da definição.

(3) Suponhamos que $|a| \leq c$. Logo, pelo item (1) do Corolário 2.1, concluímos que $-|a| \geq -c$. Assim, do item (2), obtemos

$$-c \leq -|a| \leq a \leq |a| \leq c,$$

ou seja,

$$-c \leq a \leq c.$$

Reciprocamente, vamos supor que $-c \leq a \leq c$. Se $a \geq 0$, então

$$|a| = a \leq c.$$

Se $a < 0$, então

$$|a| = -a \leq c.$$

(4) Pelo item (2), temos que

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

Somando membro a membro estas desigualdades, segue que (compatibilidade com a adição)

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

Portanto, pelo item (3),

$$|a + b| \leq |a| + |b| .$$

■

A partir de agora, a hipótese básica inicial sobre os inteiros que destacamos é o Princípio da Boa Ordenação dado no Axioma 2.1. Trata-se de uma forte ferramenta usada em algumas demonstrações matemáticas. Esse axioma servirá como fundamento para uma série de resultados sobre os números inteiros.

Definição 2.2 *Seja X um subconjunto não vazio de $\mathbb{Z}$. Diz-se que X é* ***limitado inferiormente*** *quando existe um elemento $x_0 \in \mathbb{Z}$ tal que*

$$x_0 \leq x, \quad \forall\, x \in X.$$

Diz-se também que X é limitado inferiormente por x_0 e que este é um ***limitante inferior*** *de X.*

Exemplo 2.1 O conjunto $X_1 = \{1, 2, 3, 4\}$ é limitado inferiormente, pois $x_0 = 1$ é um limitante inferior de X_1. Em geral, todo subconjunto finito não vazio X de $\mathbb{Z}$ é limitado inferiormente. Já o conjunto $X_2 = \{\ldots, -2, -1, 0, 1, 2, \}$ não tem um limitante inferior.

♣

Nota-se que um limitante inferior de um conjunto X não necessariamente pertence a X.

Com esta definição, temos o axioma:

Axioma 2.1 (**Princípio da Boa Ordenação – PBO**). *Todo subconjunto não vazio X de $\mathbb{Z}$ limitado inferiormente possui um menor elemento (ou elemento mínimo).*

Para o conjunto dos naturais, o PBO se reduz à afirmação: *todo subconjunto não vazio X de $\mathbb{N}$ possui um menor elemento.*

Diferente de um limitante inferior, um elemento mínimo de um conjunto X, por definição, pertence a X.

Proposição 2.4 *Na condição do Axioma 2.1, o elemento mínimo $x_0 \in X$ é único.*

Demonstração: Se x_0 e y_0 são elementos mínimos de X, então $x_0 \leq y_0$ e $y_0 \leq x_0$. Mas, isto em $\mathbb{Z}$ implica em $x_0 = y_0$, poia a relação " $\leq$ " é anti-simétrica. ■

Indicaremos o elemento mínimo x_0 de X por

$$x_0 = \min X.$$

Como aplicação inicial do PBO, temos:

Proposição 2.5 *Seja a um número inteiro. Se $a > 0$, então $a \geq 1$.*

Demonstração: Provaremos a afirmação por absurdo. Assim, suponhamos que exista $m \in \mathbb{Z}$ com $0 < m < 1$. Desse modo, o conjunto $X = \{m \in \mathbb{Z} : 0 < m < 1\} \subset \mathbb{Z}$ é não vazio e limitado inferiormente e, pelo PBO, X possui um menor elemento x_0. Como $x_0 \in X$, segue que $0 < x_0 < 1$; multiplicando estas desigualdades por x_0, obtemos

$$0 < x_0 < 1 \;\Rightarrow\; 0 < x_0^2 < x_0 < 1,$$

ou seja, $0 < x_0^2 < 1$, o que implica que $x_0^2 \in X$ e $x_0^2 < x_0$, contrariando a minimalidade de x_0. ■

Corolário 2.2 *Seja a e b inteiros quaisquer. Se $a > b$, então $a \geq b + 1$.*

Demonstração: Como $a - b > 0$, então pela proposição anterior, $a - b \geq 1$, ou seja, $a \geq b + 1$. ■

2.2 Indução finita (ou matemática)

A partir do Princípio da Boa Ordenação, pode-se considerar o princípio da indução finita ou princípio da indução matemática em suas duas formas. É um resultado utilizado em muitas demonstrações (demonstrações por indução) referentes a resultados válidos em conjuntos infinitos de inteiros.

No que segue, $P(n)$ é uma sentença aberta que depende da variável n sobre um subconjunto não vazio de $\mathbb{Z}$ limitado inferiormente, ou seja, uma sentença que contém n de maneira que toda vez que se substitui n por $a \in \mathbb{Z}$, se obtém uma sentença $P(a)$ que é, sem ambiguidade, verdadeira ou falsa.

Teorema 2.2 (Indução Finita – 1ª Forma). *Seja $P(n)$ uma sentença sobre o conjunto $\{n \in \mathbb{Z} : n \geq n_0\}$, em que $n_0 \in \mathbb{Z}$, tal que:*

(1) *$P(n_0)$ é verdadeira.*

(2) *Se $P(n)$ é verdadeira para $n \geq n_0$, então $P(n+1)$ também é verdadeira.*

Logo, $P(n)$ é verdadeira para todo $n \geq n_0$.

Demonstração: Vamos considerar o seguinte conjunto

$$X = \{n \in \mathbb{Z} : n \geq n_0 \text{ e } P(n) \text{ é falsa}\}.$$

Suponhamos por absurdo que $X \neq \emptyset$. Como X é limitado inferiormente (por n_0, por exemplo), então pelo PBO, existe $m_0 \in X$ (elemento mínimo) tal que

$$m_0 \leq n, \quad \forall\ n \in X.$$

Como $m_0 \in X$, temos que $m_0 \geq n_0$ e $P(m_0)$ é falsa. Logo, $m_0 \neq n_0$, pois, por hipótese, $P(n_0)$ é verdadeira. Por conseguinte, $m_0 > n_0$ e, pelo Corolário 2.2, $m_0 - 1 \geq n_0$. Sendo m_0 o menor elemento de X, segue que $m_0 - 1 \notin X$. Portanto, $P(m_0 - 1)$ é verdadeira; mas pela condição (2),

$$P(m_0 - 1 + 1) = P(m_0)$$

é verdadeira e, assim, $m_0 \notin X$, o que é uma contradição. Logo, $X = \emptyset$ e, portanto, $P(n)$ é verdadeira para todo $n \geq n_0$. ■

Exemplo 2.2 Mostrar usando indução matemática que

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}, \quad \forall\ n \geq 1.$$

Solução: Seja $P(n)$ a seguinte sentença sobre $\mathbb{N}$,

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

Como $1 = \frac{1(1+1)}{2}$, temos que $P(n_0 = 1)$ é verdadeira. Assim, por hipótese de indução, vamos supor que $P(n)$ seja verdadeira, e provemos que $P(n+1)$ também o é, ou seja,

$$P(n) \ \Rightarrow \ P(n+1).$$

Para $n+1$, usando a hipótese de que $1+2+\cdots+n=\frac{n(n+1)}{2}$,

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

o que prova que $P(n+1)$ é verdadeira. Consequentemente, $P(n)$ é verdadeira para todo $n \geq 1$. ♣

Exemplo 2.3 *Mostrar usando indução finita que*

$$2^n \leq n!, \quad \forall\ n \geq 4.$$

Solução: Como $2^4 = 16 \leq 4!$, então a afirmação é válida para $n_0 = 4$. Suponhamos agora que $p(n) : 2^n \leq n!$ é válida $\forall\ n \geq 4$. Logo

$$2^n \leq n! \Rightarrow 2^{(n+1)} \leq 2n!$$

Ora, como $n \geq 4$, então $2 \leq n+1$. Logo,

$$2^{(n+1)} \leq 2n! \leq (n+1)n! \Rightarrow 2^{(n+1)} \leq (n+1)n! = (n+1)!$$

Com isso, provamos que $p(n+1)$ é válida, o que implica que,

$$2^n \leq n!, \quad \forall\ n \geq 4.$$

♣

O princípio de indução finita é uma importante ferramenta matemática que pode ser utilizada para demonstrar muitos resultados em praticamente todos os ramos dessa ciência. Veremos a seguir a prova de um resultado da geometria plana.

Exemplo 2.4 Mostrar que a soma dos ângulos internos de um polígono convexo de n lados é

$$s_n = (n-2)\cdot 180^\circ, \quad n \geq 3.$$

Solução: Para $n = 3$, temos que o polígono é um triângulo e sabemos da geometria euclidiana que a soma dos ângulos de um triângulo é 180°, ou seja,

$$s_3 = (3-2) \cdot 180^\circ = 180^\circ$$

Agora, suponhamos que a afirmação é válida para $n \geq 3$, isto é, $s_n = (n-2) \cdot 180^\circ$ e consideremos o polígono convexo $a_0a_1 \ldots a_n$ que possui $n+1$ lados. Podemos traçar outro polígono através deste suprimindo-se o vértice a_1 de modo a obter o polígono $a_1a_2 \ldots a_n$ que contém n lados, cuja soma dos ângulos internos é por hipótese

$$s_n = (n-2) \cdot 180^\circ.$$

Como a soma dos ângulos internos do polígono original (s_{n+1}) é a soma dos ângulos do triângulo $a_0a_1a_2$ com a soma dos ângulos internos do polígono s_n, temos que

$$s_{n+1} = s_n + 180^\circ = (n-2) \cdot 180^\circ + 180^\circ = (n-1) \cdot 180^\circ,$$

o que finaliza a prova ♣

Os casos apresentados acima se referem a sentenças com apenas uma variável. Adiante trataremos de sentenças com duas variáveis, onde uma prova por indução consiste em fixar uma variável e usar indução sobre a outra.

Definição 2.3 *Dado $a \in \mathbb{Z}^*$ e $m \in \mathbb{N} \cup \{0\}$, define-se a potência não negativa de a da seguinte forma:*

$$a^m = \begin{cases} 1 & se \quad m = 0, \\ a^{m-1} \cdot a & se \quad m \geq 1. \end{cases}$$

É claro que por definição, dado $a \in \mathbb{Z}^*$ e $m \in \mathbb{N} \cup \{0\}$, então

$$a^m = a \cdot a \cdots a \quad (m \text{ vezes}).$$

Proposição 2.6 *Seja $a \in \mathbb{Z}^*$. Então,*

(1) $a^n \cdot a^m = a^{m+n}, \quad \forall\ m, n \in \mathbb{N}.$

(2) $(a^n)^m = a^{m \cdot n}, \quad \forall\ m, n \in \mathbb{N}.$

Demonstração: Vamos demonstrar apenas a propriedade (1), fixando m e usando indução sobre n. Por definição de a^{m+1}, temos para $n = 1$,

$$a^1 \cdot a^m = a \cdot a^m = a^m \cdot a = a^{m-1+1} \cdot a = a^{m+1}.$$

Agora, suponhamos que o resultado seja válido para n, isto é, $a^n \cdot a^m = a^{n+m}$. Assim, para $n + 1$, obtemos

$$\begin{aligned} a^{n+1} \cdot a^m &= a^n \cdot a \cdot a^m && (\text{pois } a^n \cdot a = a^{(n+1)-1} \cdot a = a^{n+1}) \\ &= a^n \cdot a^m \cdot a \\ &= a^{n+m} \cdot a && (\text{fazendo uso da hipótese}) \\ &= a^{(n+m+1)-1} \cdot a \\ &= a^{n+m+1}. \end{aligned}$$

Logo, $a^n \cdot a^m = a^{n+m}$ para todos $m, n \in \mathbb{N}$. ■

2.3 Divisibilidade em $\mathbb{Z}$

Nesta seção apresentamos os principais resultados referente à divisibilidade. Tais resultados são de suma importância para que se possa compreender os focos principais deste trabalho que são os teoremas de Fermat, Euler e Wilson. Apresentaremos o algoritmo da divisão, uma importante ferramenta no estudo de teoria dos números. De uma forma geral, consideramos as principais propriedades de divisibilidade.

Definição 2.4 *Sejam $a, b \in \mathbb{Z}$. Diz que b **divide** a ou que b é **divisor** de a (ou ainda que a é **múltiplo** de b) e denotamos por $b \mid a$, quando existe $c \in \mathbb{Z}$ tal que*

$$a = b \cdot c. \tag{2.1}$$

O caso em que b não divide a será indicado por:

$$b \nmid a.$$

Exemplo 2.5 *Tem-se que $3 \mid 6$, pois, $6 = 3 \cdot 2$. E, por outro lado, $4 \nmid 7$, pois não existe $c \in \mathbb{Z}$ tal que $7 = 4 \cdot c$.*

Notemos que, $1 \mid a, \quad \forall\, a \in \mathbb{Z}$, pois $a = 1 \cdot a$.

Um número $a \in \mathbb{Z}$ chama-se **par** quando $2 \mid a$. Em particular, concordamos que zero é par. O número a é dito **ímpar** quando ele não é par, isto é, se a não é divisível por 2. Por exemplo, os números -4 e 14 são pares; enquanto 9 e 25 são ímpares. Diz-se que a e b têm a **mesma paridade** quando a e b são ambos pares ou são ambos ímpares.

Observa-se que para $b \neq 0$, então o inteiro c que figura em (2.1) é único. Além disso, $a \mid 0$ 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.

Proposição 2.7 *Se $b \mid a$ e $a \neq 0$, então $|b| \leq |a|$.*

Demonstração: Se $b \mid a$, então existe $c \in \mathbb{Z}$ tal que $a = b{\cdot}c$. Logo, $|a| = |b \cdot c| = |b|{\cdot}|c|$. Como $c \neq 0$, então $|c| \geq 1$. Assim, multiplicando esta desigualdade por $|b|$, obtemos

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

■

Proposição 2.8 *Em $\mathbb{Z}$ valem as seguintes propriedades:*

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

(2) *Dados $a, b \in \mathbb{Z}$, se $a \mid b$ e $b \mid a$, então, $a = \pm b$.*

Demonstração: (1) Tomemos $b \in \mathbb{Z}$ um divisor de 1, ou seja, $a \mid 1$. Pela proposição 2.7, temos que $|b| \leq 1$. Assim,

$$0 < |b| \leq 1 \Rightarrow |b| = 1 \Rightarrow b = \pm 1.$$

(2) Por hipótese,

$$b = \lambda_1 \cdot a \quad \text{e} \quad a = \lambda_2 \cdot b, \quad \text{com } \lambda_1, \lambda_2 \in \mathbb{Z}.$$

Substituindo o valor de $a = \lambda_1 \cdot b$ em $b = \lambda_1 \cdot a$, obtemos que:

$$b = \lambda_1 \cdot (b \cdot \lambda_2) \Rightarrow b = \lambda_1 \cdot \lambda_2 \cdot b \Rightarrow 1 = \lambda_1 \cdot \lambda_2,$$

pois, $b \neq 0$. Ou seja,

$$1 = \lambda_1 \cdot \lambda_2 \Rightarrow \lambda_1 | 1 \Rightarrow \lambda_1 = \pm 1,$$

Logo,

$$b = \pm 1 \cdot a = \pm a \Rightarrow b = \pm a.$$

■

Na próxima proposição encontram-se outras propriedades elementares da divisibilidade.

Proposição 2.9 *Sobre os números inteiros valem as seguintes:*

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

(2) *Se* $a \mid b$, *então* $ax \mid bx$,

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

Demonstração: Faremos apenas as demonstrações (1) e (3).

(1) Temos que:

$$b = a \cdot \lambda_1 \quad \text{e} \quad c = b \cdot \lambda_2, \quad \text{com } \lambda_1,\ \lambda_2 \in \mathbb{Z}.$$

Logo,

$$c = b \cdot \lambda_2 = a \cdot \lambda \cdot \lambda_2 \Rightarrow a \cdot (\lambda_1 \cdot \lambda_2).$$

Portanto, $a \mid c$.

(3) Temos:

$$b = \beta_1 \cdot a \quad \text{e} \quad c = \beta_2 \cdot b, \quad \text{com } \beta_1,\ \beta_2 \in \mathbb{Z}.$$

Agora, para x, $y \in \mathbb{Z}$,

$$b \cdot x = (\beta_1 \cdot x) \quad \text{e} \quad c \cdot y = (\beta_2 \cdot y).$$

Somando membro a membro as duas últimas igualdades, obtemos:

$$b \cdot x + c \cdot y = (\beta_1 \cdot x + \beta_2 \cdot y) \cdot a,$$

ou seja, $a \mid bx + cy$, pois $\beta_1 \cdot x + \beta_2 \cdot y \in \mathbb{Z}$. ■

2.4 Algoritmo da divisão

O algoritmo da divisão (ou divisão euclidiana), que consideramos um dos mais familiares resultados dos inteiros, cujo resultado é base para muitas propriedades algébricas relevantes em $\mathbb{Z}$, será demonstrado tendo ponto de partida o seguinte lema:

Lema 2.1 (Propriedade Arquimediana) . *Consideremos dois inteiros a e b com $b \neq 0$. Então, existe $n \in \mathbb{Z}$ tal que $nb \geq a$.*

Teorema 2.3 (Algoritmo da Divisão) *Sejam $a, b \in \mathbb{Z}$, com $b \neq 0$. Então, existe únicos $q, r \in \mathbb{Z}$, tais que*

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

Demonstração: Consideremos o conjunto

$$S = \{a - bk : k \in \mathbb{Z}\}.$$

Pelo Lema 2.1, existe um inteiro n_0 tal que

$$-a \leq n_0(-b) \;\Rightarrow\; a \geq n_0 b \;\Rightarrow\; a - n_0 b \geq 0.$$

Desse modo, o conjunto L dado por

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

é não vazio, pois $x = a - n_0 b \in L$. Como L é limitado inferiormente, segue pelo PBO que L possui menor elemento, digamos r. Como $r \in L$, então $r \geq 0$ e

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

Mostremos agora que $r < |b|$. Suponhamos por absurdo que $r \geq |b|$. Se $b > 0$, então $|b| = b$; logo, $r - b \geq 0$ e

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

Daí, $r - b \in L$ e $r - b < r$, o que contradiz a minimalidade de r. Se $b < 0$, então $|b| = -b$; assim, $r + b \geq 0$ e

$$r + b = a - b \cdot (q - 1),$$

ou seja, $r + b \in L$ e $r + b < r$, o que é uma contradição. Desse modo, $a = qb + r$ com $q \in \mathbb{Z}$ e $0 \leq r < |b|$, o que prova a existência dos inteiros q e r. Para mostrarmos a unicidade desses inteiros, consideremos $q_1, r_1 \in \mathbb{Z}$ tais que

$$a = qb + r \quad \text{e} \quad a = q_1 b + r_1$$

com

$$0 \leq r < |b| \quad \text{e} \quad 0 \leq r_1 < |b|\,.$$

Assim,

$$qb + r = q_1 b + r_1 \;\; \Rightarrow \;\; r - r_1 = b(q_1 - q),$$

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

Os números q e r em (2.2) se chamam, respectivamente, **quociente** e **resto** da divisão de a por b.

Observação 2.1 No Teorema 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 $r = a$.

Exemplo 2.6 Determinar o quociente e resto da divisão de a por b quando:

a) $a = 41 \quad \text{e} \quad b = 7$.

b) $a = -10 \quad \text{e} \quad b = 6$.

c) $a = -1243 \quad \text{e} \quad b = -4$.

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

b) Para o caso em que $a = -10 < 0$ e $b = 6$, vamos efetuar a divisão natural de 10 por 6. Após isso, manipulamos a expressão convenientemente. Assim,

$$10 = 1 \cdot 6 + 4 \;\Rightarrow\; -10 = -1 \cdot 6 - 4.$$

Como $-10 = -1 \cdot 6 - 4 = -1 \cdot 6 - 4 + 6 - 6$, obtemos

$$\begin{aligned} 10 = 1 \cdot 6 + 4 \;&\Rightarrow\; -10 = -1 \cdot 6 - 4 \\ &\Rightarrow\; -10 = -1 \cdot 6 - 4 + 6 - 6 \\ &\Rightarrow\; -10 = 6 \cdot (-1 - 1) + 2 \\ &\Rightarrow\; -10 = 6 \cdot (-2) + 2 \\ &\Rightarrow\; q = -2 \quad \text{e} \quad r = 2. \end{aligned}$$

c) Sendo $a = -1243$ e $b = -4$, efetuamos a divisão de 1243 por 4 e usamos artifício análogo ao do caso 2. Temos:

$$\begin{aligned} 1243 = 310 \cdot 4 + 3 \;&\Rightarrow\; -1243 = 310 \cdot (-4) - 3 \\ &\Rightarrow\; -1243 = 310 \cdot (-4) - 3 + 4 - 4 \\ &\Rightarrow\; -1243 = -4 \cdot (310 + 1) + 1 \\ &\Rightarrow\; -1243 = -4 \cdot 311 + 1 \\ &\Rightarrow\; q = 311 \quad \text{e} \quad r = 1. \end{aligned}$$

♣

Exemplo 2.7 *Mostrar que:*

(a) $a \in \mathbb{Z}$ *é par* $\Leftrightarrow \;\; a = 2k, \quad k \in \mathbb{Z}$.

(b) $a \in \mathbb{Z}$ *é ímpar* $\Leftrightarrow \;\; a = 2k + 1, \quad k \in \mathbb{Z}$.

(c) *A soma de dois números ímpares é par.*

(d) *A soma de dois números pares é par.*

(e) *A soma de um número par com um número ímpar é ímpar.*

(f) *O produto de dois números pares é par.*

(g) *O produto de dois números ímpares é ímpar.*

Solução: Só daremos a solução de (c) e (e).

(c) Sejam α e β dois números ímpares, digamos $\alpha = 2q_1 + 1$ e $\beta = 2q_2 + 1$. Assim,

$$\alpha + \beta = 2(q_1 + q_2) + 2 = 2(q_1 + q_2 + 1),$$

ou seja, $\alpha + \beta$ é um número par.

(e) Se α e β são par e ímpar, respctivamente, então $\alpha = 2k_1$ e $\beta = 2k_2 + 1$, de modo que

$$\alpha + \beta = 2k_1 + 2k_2 + 1 = 2 \cdot (k_1 + k_2) + 1,$$

isto é, $\alpha + \beta$ é ímpar. ♣

2.5 Máximo Divisor Comum – MDC

Dada uma quantidade finita de números inteiros, é evidente que cada um desses números possui divisores, e além disso, tais números possuem em comum um ou mais divisores (pelos menos o número um é divisor comum). Nesta seção, estudaremos maneiras de encontrarmos o maior desses divisores, o qual chamaremos de **máximo divisor comum**. Os resultados referentes a máximo divisor comum são imprescindíveis no estudo dos números inteiros. Eles serão usados na seção de congruências, inclusive da demosntração do teorema de Euler.

Definição 2.5 *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$ ou $b \neq 0$. Diz-se que $d \in \mathbb{N}$ é* ***máximo divisor comum*** *(mdc) entre a e b quando as seguintes condições são satisfeitas:*

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

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

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

Observação 2.2 *Se $a = b = 0$, vamos acordar que o máximo divisor comum de a e b é 0.*

Em alguns casos particulares, é imediato verificar a existência do mdc. Por exemplo, se a é um número inteiro não nulo, tem-se claramente que:

(a) $|a|$ é um mdc de $b = 0$ e a.

(b) O número 1 é um mdc de 1 e a.

(c) $|a|$ é um mdc entre a e ele próprio.

Além disso, para todo $b \in \mathbb{Z}$, temos que

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

Nosso objetivo é provar que o natural d na condição acima existe e é único.

Lema 2.2 *Se os inteiros a e b têm um máximo divisor comum, então ele é único.*

Demonstração: Se d_1 e d_2 são máximos divisores comuns de a e b, então, por definição,

$$d_1 = \lambda_1 d_2 \quad \text{e} \quad d_2 = \lambda_2 d_1, \quad \text{com} \quad \lambda_1, \lambda_2 \in \mathbb{N}.$$

Substituindo o valor de $d_2 = \lambda_2 d_1$ em $d_1 = \lambda_1 d_2$, obtemos pela Proposição **??** que $d_1 = (\lambda_1 \lambda_2)\, d_1$, ou seja,

$$1 = \lambda_1 \lambda_2 \;\Rightarrow\; \lambda_1 = \lambda_2 = 1.$$

Por conseguinte, $d_1 = d_2$. ♣

Dados dois inteiros a e b ambos não nulos, vamos indicar por $mdc(a, b)$ o máximo divisor comum entre eles, quando este existir. Temos,

$$mdc(a, b) = mdc(-a, b) = mdc(-a, -b) = mdc(a, -b). \tag{2.3}$$

Além disso, se $a = 0$ e $b \neq 0$, então, como observado anteriormente, $mdc(0, b) = |b|$. Por isso, vamos assumir que a e b são sempre positivos.

O próximo teorema além de garantir a existência de mdc de dois inteiros, mostra que $mdc(a, b)$ é uma combinação muito proveitosa de a e b. Esta combinação não é única, por exemplo,

$$\begin{aligned} mdc(18, 4) &= 2 = 1 \cdot \mathbf{18} + (-4) \cdot \mathbf{4} \\ &= -1 \cdot \mathbf{18} + 5 \cdot \mathbf{4}. \end{aligned}$$

Teorema 2.4 (Existência de mdc) *Para quaisquer números naturais*[3] *a e b, existe $d = mdc(a, b)$. Além disso, existem $x_0, y_0 \in \mathbb{Z}$ tais que*

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

Demonstração: Consideremos o conjunto

$$X = \{ax + by : x, y \in \mathbb{Z}\}.$$

Obviamente, existem em X elementos que são estritamente positivos. Por exemplo, para $x = y = 1$, obtemos $a \cdot 1 + b \cdot 1 = a + b > 0$ e $a + b \in X$. Seja W o subconjunto de X constituído pelos elementos de X estritamente positivos. Desse modo, pelo PBO, W possui menor elemento $d \in W$. Vamos mostrar que $d = mdc(a, b)$; como $d \in W$, existem $x_0, y_0 \in \mathbb{Z}$ tais que

$$d = ax_0 + by_0. \tag{2.5}$$

Usando o algoritmo da divisão com os elementos a e d, temos

$$a = dq + r, \quad \text{com} \quad 0 \leq r < d. \tag{2.6}$$

Substituindo o valor de d em (2.5) em (2.6), segue que

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

[3] Já estamos usando as igualdades em (2.3) e o fato de $mdc(0, b) = |b|$ com $b \neq 0$.

Daí,

$$r = a(1 - qx_0) + b(-qy_0) \;\Rightarrow\; r \in W.$$

Mas, sendo $r < d$, então, pela minimalidade de d, devemos necessariamente ter $r = 0$, isto é, $a = dq$, o que mostra que $d \mid a$. Similarmente, prova-se que d também divide b. Agora, se $c \in \mathbb{Z}$ é tal que $c \mid a$ e $c \mid b$, então $a = c\lambda_1$ e $b = c\lambda_2$ com $\lambda_1, \lambda_2 \in \mathbb{Z}$. Como $d = ax_0 + by_0$,

$$d = (c\lambda_1)x_0 + (c\lambda_2)y_0 = c(\lambda_1 x_0 + \lambda_2 y_0) \;\Rightarrow\; c \mid b.$$

Portanto, $d = mdc(a, b)$. ■

A expressão em (2.4) é conhecida como **identidade de Bézout** para os elementos a e b.

Algoritmo de Euclides sobre $\mathbb{Z}$

Quando os inteiros $a > 0$ e $b > 0$ são "pequenos", então determina-se $d = mdc(a, b)$ sem muitas dificuldades. Mas, como determinar d quando a e b são números consideravelmente grandes? Por exemplo, quanto vale $mdc(594, 382)$? Não é razoável determinar os divisores positivos de $a = 594$ e $b = 382$ e verificar o maior entre os divisores comuns. Isso seria tedioso!

O Lema 2.3 mostra que o algoritmo da divisão poder ser usado para calcular $d = mdc(a, b)$, quaisquer que sejam os inteiros a e b. O mesmo implicará em um método (o algoritmo de Euclides) para determinar d, o qual consiste em divisões sucessivas.

Lema 2.3 *Sejam a e b inteiros, $b \neq 0$, e q e r o quociente e resto da divisão de a por b, respectivamente, ou seja,*

$$a = b \cdot q + r, \quad com \quad 0 \leq r < |b|\,. \tag{2.7}$$

Então, $mdc(a, b) = mdc(b, r)$.

Demonstração: Por (2.7), todo divisor de b e r é também divisor de a. Por outro lado, se $d \in \mathbb{N}$ é tal que $d \mid a$ e $d \mid b$, então, como $r = a - qb$, segue que $d \mid r$. Isto é suficiente para que se tenha $mdc(a, b) = mdc(b, r)$. ■

Portanto, pelo Lema 2.3, o problema de determinar $mdc(a, b)$ reduz-se a calcular $mdc(b, r)$.

Consideremos os inteiros a e b, com $a > b > 0$. Pela divisão euclidiana, temos que

$$a = b \cdot q_1 + r_1, \quad \text{com} \quad 0 \leq r_1 < b.$$

De acordo com o lema anterior, sabemos que $mdc(a, b) = mdc(b, r_1)$. Temos dois casos a considerar:

1. Se $r_1 = 0$, então

$$mdc(a, b) = mdc(b, r_1) = mdc(b, 0) = b.$$

2. Se $r_1 \neq 0$, então efetuando a divisão de b por r_1, obtemos

$$b = r_1 \cdot q_2 + r_2, \quad \text{com} \quad 0 \leq r_2 < r_1.$$

Da mesma forma,

3. Se $r_2 = 0$, segue que

$$mdc(a, b) = mdc(b, r_1) = mdc(r_1, r_2) = mdc(r_1, 0) = r_1.$$

4. Se $r_2 \neq 0$, então efetuando a divisão de r_1 por r_2, temos que

$$r_1 = r_2 \cdot q_3 + r_3, \quad \text{com} \quad 0 \leq r_3 < r_2.$$

Mais uma vez, procedendo como acima, obtemos

$$mdc(a, b) = mdc(b, r_1,) = mdc(r_1, r_2) = mdc(r_2, r_3),$$

e assim sucessivamente.

Assim, deve existir um índice n tal que $r_n \neq 0$ e $r_{n+1} = 0$, pois caso contrário, obteríamos uma sequência infinita $b, r_1, r_2, \ldots$ de modo que

$$b > r_1 > r_2 > \cdots > 0,$$

o que não é possível. Por isso,

$$mdc(a,b) = mdc(b,r_1) = mdc(r_1,r_2) = \cdots = mdc(r_n,r_{n+1}) = mdc(r_n,0) = r_n.$$

Portanto, o último resto não nulo r_n é o mdc de a e b.

O método apresentado acima para o cálculo de $mdc(a,b) = r_n$ chama-se **Algoritmo de Euclides**.

Exemplo 2.8 Calcule $d = mdc(1020, 284)$. Além disso, determinar x_0 e $y_0 \in \mathbb{Z}$ tais que

$$d = 1020x_0 + 284y_0.$$

Solução: Como $1020 > 284$, vamos usar o algoritmo da divisão, dividindo $a = 1020$ por $b = 284$. Assim,

$$\begin{cases} 1020 = 284 \cdot 3 + 168 \Rightarrow mdc(1020,284) = mdc(284,168), \\ 284 = 168 \cdot 1 + 116 \Rightarrow mdc(284,168) = mdc(168,116), \\ 168 = 116 \cdot 1 + 52 \Rightarrow mdc(168,116) = mdc(116,52), \\ 116 = 52 \cdot 2 + 12 \Rightarrow mdc(116,52) = mdc(52,12), \\ 52 = 12 \cdot 4 + 4 \Rightarrow mdc(52,12) = mdc(12,4), \\ 12 = 4 \cdot 3 + 0 \Rightarrow mdc(12,4) = mdc(4,0) = 4 \end{cases} \tag{2.8}$$

Portanto, $mdc(1020, 284) = 4$. Vamos encontrar $x_0, y_0 \in \mathbb{Z}$ tais que

$$4 = 1020 \cdot x_0 + 284 \cdot y_0.$$

Isso consistirá em isolar os restos não nulos das divisões de baixo para cima das igualdades em (2.8), substituindo-os sucessivamente. Logo,

$$\begin{aligned} 4 \;=\; 52 - 4\cdot 12 \;&=\; 52 - 4\cdot(116 - 2\cdot 52) \\ &=\; 9\cdot 52 - 4\cdot 116 \\ &=\; 9\cdot(168 - 1\cdot 116) - 4\cdot 116 \\ &=\; 9\cdot 168 - 13\cdot 116 \\ &=\; 9\cdot 168 - 13\cdot(284 - 1\cdot 168) \\ &=\; 22\cdot 168 - 13\cdot 284 \\ &=\; 22\cdot(1020 - 3\cdot 284) - 13\cdot 284 \\ &=\; 22\cdot 1020 - 79\cdot 284. \end{aligned}$$

Assim, $4 = 22\cdot 1020 - 79\cdot 284$. Por conseguinte, podemos escolher $x_0 = 22$ e $y_0 = -79$.♣

Se $a, b, c \in \mathbb{Z}$, então se verifica facilmente que $mdc(a, b, c) = mdc(d_1, c)$, em que $d_1 = mdc(a, b)$. Em geral, se a_1, a_2,..., $a_n \in \mathbb{Z}$ (todos não nulos), então

$$d = mdc(a_1, a_2, \ldots, a_n) = mdc(d_1, a_3, \ldots, a_n).$$

em que $d_1 = mdc(a_1, a_2)$. Além disso, existem $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ tais que

$$d_1 = a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_2$$

Exemplo 2.9 *Calcular* $d_2 = mdc(404, 228, 142)$ *e determinar* $x_1, x_2, x_3 \in \mathbb{Z}$ *para os quais* $d = 404x_1 + 228x_2 + 142x_3$.

Solução: Vamos considerar $a = 404$ e $b = 228$. Similar ao que foi feito no exemplo anterior, encontra-se $d_1 = mdc(404, 228) = 4$ e

$$4 = 39 \cdot 228 - 22 \cdot 404. \tag{2.9}$$

Agora,

$$142 \;=\; 35 \cdot 4 + 2 \;\Rightarrow\; mdc(142, 4) = mdc(4, 2) = 2,$$

ou seja, $mdc(142, 4) = 2$. Dessa forma, $d_2 = mdc(404, 228, 142) = 2$ e, usando a igualdade em (2.9), obtemos

$$\begin{aligned} 2 &= 142 - 35 \cdot 4 = 142 - 35 \cdot (39 \cdot 228 - 22 \cdot 404) \\ &= 142 - 1365 \cdot 228 + 770 \cdot 404, \end{aligned}$$

ou seja, $2 = 770 \cdot 404 - 1365 \cdot 228 + 1 \cdot 142$. Portanto, $x_0 = 770$, $y_0 = -1365$ e $z_0 = 1$.♣

Quando $mdc(a, b) = 1$, diz-se que a e b são **primos entre si**, ou **relativamente primos**.

Proposição 2.10 *Se $a, b \in \mathbb{Z}$, então a e b são primos entre si se, e somente se, existem $x, y \in \mathbb{Z}$ tais que*

$$ax + by = 1.$$

Demonstração: Suponhamos que $mdc(a, b) = 1$. Pela identidade de Bezout, existem $x, y \in \mathbb{Z}$, tais que

$$1 = ax + by.$$

Reciprocamente, suponhamos que existam $x, y \in \mathbb{Z}$ tais que

$$1 = ax + by. \tag{2.10}$$

Consideremos

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

Assim,

$$a = d \cdot \lambda_1 \quad \text{e} \quad b = d \cdot \lambda_2, \quad \lambda_1, \lambda_2 \in \mathbb{Z}.$$

Substituindo os valores de a e b em (2.10), obtemos:

$$1 = d \cdot \lambda 1 \cdot x + d \cdot \lambda_2 \cdot y = d \cdot (\lambda_1 \cdot x + \lambda_2 \cdot y),$$

ou seja, $d \mid 1$ e, com isso, $d = 1$. ■

Corolário 2.3 *Sejam $a, b, c \in \mathbb{Z}$ com $mdc(a, b) = 1$. Se $a \mid b$ e $b \mid c$, então*

$$a \cdot b \mid c.$$

Demonstração: Por hipótese, $mdc(a,b) = 1$. Também, $c = \lambda_1 \cdot a$ e $c = \lambda_2 \cdot b$. Logo,

$$c \cdot b = \lambda_1 \cdot a \cdot b \quad \text{e} \quad c \cdot a = \lambda_2 \cdot b \cdot a$$

Pela identidade de Bezout, temos:

$$1 = ax + by, \quad x, y \in \mathbb{Z}.$$

Multiplicando ambos os membros da última igualdade por c, temos:

$$c = a \cdot c \cdot x + b \cdot c \cdot y = (\lambda_1 \cdot b \cdot a) \cdot x + (\lambda_2 \cdot a \cdot b) \cdot y = (a \cdot b) \cdot (\lambda_1 \cdot x + \lambda_2 \cdot y)$$

Fazendo, $\lambda_3 = \lambda_1 \cdot x + \lambda_2 \cdot y \in \mathbb{Z}$, obtemos que

$$c = (a \cdot b) \cdot \lambda_3 \Rightarrow (a \cdot b) \mid c.$$

■

2.6 Mínimo Múltiplo Comum – MMC

Dada uma quantidade finita de números inteiros, é obvio que tais números possuem múltiplos, e mais, esses números vão possuir múltiplos comuns, o menor desses múltiplos chamaremos **mínimo múltiplo comum**. Por exemplo os múltiplos do número 5 são $5, 10, 15, 20, 25$,..., os múltiplos do número 10 são $10, 20, 30, 40, 50, ...$, logo o mínimo múltiplo comum de 5 e 10 é o número 10. Nesta seção estudaremos alguns resultados importantes acerca de mínimo múltiplo comum (mmc). Tal conceito assemelha-se com o conceito de máximo divisor comum entre eles.

Definição 2.6 *Sejam a e b inteiros ambos não nulos. Um número $m \in \mathbb{N}$ é dito* ***mínimo múltiplo comum*** *(mmc) de a e b quando as seguintes condições são satisfeitas:*

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

(b) *Se $c \in \mathbb{N}$ é tal que $a \mid c \quad e \quad b \mid c$, então $m \mid c$.*

O mínimo múltiplo comum de a e b é denotado por $mmc(a, b)$.

Teorema 2.5 *Sejam $a, b \in \mathbb{Z}_+^*$ e $d = mdc(a, b)$. Então, existe mínimo múltiplo comum de a e b. Além disso, se $m = mmc(a, b)$, tem-se que*

$$m = \frac{a \cdot b}{d}.$$

Demonstração: Consideremos $m = \frac{ab}{d}$ e provemos que $m = mmc(a, b)$. Como $d \mid a$ e $d \mid b$, então $a = d\lambda_1$ e $b = d\lambda_2$ com $\lambda_1, \lambda_2 \in \mathbb{N}$. Assim,

$$m = \frac{ab}{d} = \frac{\lambda_1 db}{d} = \lambda_1 b \;\Rightarrow\; b \mid m.$$

Da mesma forma, tem-se que $a \mid m$. Tomemos agora m_1 outro múltiplo comum de a e b, isto é, $m_1 = a\alpha_1$ e $m_1 = b\alpha_2$, com $\alpha_1, \alpha_2 \in \mathbb{N}$. Pela identidade de Bézout, existem inteiros x e y tais que

$$d = ax + by.$$

Logo,

$$\begin{aligned} \frac{m_1}{m} &= \frac{m_1 d}{md} \\ &= \frac{m_1 ax + m_1 by}{ab} \\ &= \frac{ab\alpha_2 x + ab\alpha_1 y}{ab} \\ &= \alpha_2 x + \alpha_1 y \in \mathbb{Z}, \end{aligned}$$

ou seja, $m \mid m_1$. Isso mostra que o mínimo múltiplo comum m entre a e b existe e que $m = \frac{ab}{d}$. ■

Exemplo 2.10 Calcular $mmc(224, 30)$.

Solução: Calculemos primeiramente $d = mdc(224, 30)$. Assim, aplicando o algoritmo de Euclides com $a = 224$ e $b = 30$, concluímos que $mdc(a, b) = 2$. Assim,

$$m = mmc(224, 30) = \frac{224 \cdot 30}{2} = 3360.$$

♣

Assim como foi feito para máximo divisor comum, pode-se calcular o mínimo múltiplo comum para vários inteiros. Se $a_1, a_2, \ldots, a_n$ são inteiros não nulos, então $mmc(a_1, a_2, \ldots, a_n)$ é calculado em $n-1$ passos através da sequências de números

$$m_1 = mmc(a_1, a_2), \quad m_2 = mmc(m_1, a_3), \ldots, m_{n-1} = mmc(m_{n-2}, a_n)$$

e m_{n-1} é o mínimo múltiplo comum entre $a_1, a_2, \ldots, a_n$.

Exemplo 2.11 Calcular $mmc(6, 14, 22, 36)$.

Solução: Temos que:

$$\begin{array}{rcl} mdc(6,14) = 2 & \Rightarrow & m_1 = mmc(6,14) = 42. \\ mdc(42,22) = 2 & \Rightarrow & m_2 = mmc(42,22) = 462. \\ mdc(462,36) = 6 & \Rightarrow & m_3 = mmc(462,36) = 2772. \end{array}$$

Portanto, $mmc(6, 14, 22, 36) = 2772$. ♣

2.7 Números Primos

Uma classe muito importante de inteiros é a classe dos números primos. Do ponto de vista de divisibilidade, esses números são os mais simples e, além disso, conforme o Teorema Fundamental da Aritmética, todo inteiro $a \in \mathbb{Z} - \{0, \pm 1\}$ pode ser escrito como produto de primos. Em outras palavras, os primos são suficientes para gerar todos os inteiros diferentes de 0 e ± 1. Isso mostra a importância deles na teoria dos números.

Os números primos sempre foram cercados de mistérios. Para se ter uma ideia, ainda não se conhece uma fórmula matemática simples que gere todos eles. Alguns matemáticos, a exemplo de Fermat, até que tentaram estabelecer essa relação, mas sem muito êxito, pois não conseguiram generalizar e provar suas teses.

Nesta seção, apresentaremos alguns resultados sobre os números primos, destacando de forma especial o Teorema Fundamental da Aritmética.

Definição 2.7 *Um número $p \in \mathbb{Z} - \{0, \pm 1\}$ diz-se **primo** quando seus únicos divisores positivos são 1 e $|p|$. Caso contrário, p é dito **composto**.*

Por exemplo, -3, 5 e 13 são primos, enquanto 9, 8 e 12 são compostos.

Observa-se que $a \in \mathbb{Z}$ composto significa dizer que

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

Além disso, p é primo se, e somente se, $-p$ é primo. Por isso, vamos considerar apenas primos positivos.

De uma maneira geral, chamaremos de **divisores triviais** de a os números 1 e a.

Proposição 2.11 *Sejam p um primo e $a, b \in \mathbb{Z}$. Então,*

(1) *Se $p \nmid a$, então $mdc(p, a) = 1$.*

(2) *Se $p \mid a \cdot b$, então $p \mid a$ ou $p \mid b$.*

Demonstração: (1) Se $p \nmid a$, então o único divisor comum de p e a é 1, pois, os únicos divisores de p são 1 e p. Logo, $mdc(p, a) = 1$.

(2) Por hipótese, temos $p \mid a \cdot b$. Se $p \mid a$, não há o que provar. Caso contrário, ou seja, se $p \nmid a$, então segue do item (1) que $mdc(p, a) = 1$. Pela identidade de Bézout, sabemos que

$$1 = ax + py, \quad \text{com} \quad x, y \in \mathbb{Z}.$$

Multiplicando ambos os membros desta igualdade por b, obtemos

$$b = abx + pby.$$

Mas, como $p \mid a \cdot b$, então $p \mid b$. ■

Por indução, para $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ e p primo,

$$p \mid a_1 a_2 \cdots a_n \;\Rightarrow\; p \mid a_i$$

para algum $i = 1, \ldots, n$. De fato, para $n = 1$, o resultado é imediato. Agora, suponhamos, por hipótese de indução, que o resultado seja válido para $n \geq 1$. Desse modo, para $a_1, a_2, \ldots, a_n, a_{n+1} \in \mathbb{Z}$, temos

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

Logo, por hipótese, $p \mid a_i$ para algum $i = 1, \ldots, n+1$.

Teorema 2.6 *Se $a > 1$, então existe um primo p tal que $p \mid a$.*

Demonstração: Consideremos o conjunto

$$W = \{a \in N : a > 1 \quad \text{e} \quad p \nmid a \quad \forall\ p \text{ primo}\}.$$

Se $W \neq \emptyset$, então pelo PBO, existe $d \in W$ com $d = \min W$. Como $d \mid d$, então d não pode ser primo. Por isso, $d = bc$ com $1 < b, c < n$. Desse modo, $b \notin W$, pois $d = \min W$. Por conseguinte, como $b > 1$, então deve existir um número primo p tal que $p \mid b$. Mas, como $b \mid p$, então $p \mid d$, isto é, $d \notin W$, o que é impossível. Essa contradição mostra que existe um primo p, com $p \mid a$. ■

Teorema 2.7 (Teorema Fundamental da Aritmética – TFA) *Todo número natural*[4] *$a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, como produto de primos.*

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

(**Existência**) Consideremos o conjunto

$$M = \{n \in \mathbb{N} : n \neq p_1 p_2 \cdots p_n\} \subset \mathbb{N},$$

para primos $p_1, p_2, \ldots, p_n$. Ou seja, M é constituído por todos os naturais que não são produtos de primos. Se mostrarmos que $M = \emptyset$, então a existência dos números primos estará provada. Suponhamos por absurdo que $M \neq \emptyset$; logo, pelo PBO, M possui um menor elemento $m \in M$. Dessa forma, m não pode ser primo e, por conseguinte, é composto. Assim, podemos escrevê-lo como

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

Como $a < m$ e $b < m$, então $a \notin M$ e $b \notin M$, pois $m = \min M$. Portanto, a e b são primos ou são produtos de primos. Logo, $m = a \cdot b$ é um produto de primos, o que é uma contradição.

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

(**Unicidade**) Suponhamos agora que

$$a = p_1 \cdot p_2 \cdots p_n = q_1 \cdot q_2 \cdots q_m,$$

sendo $p_1, \ldots, p_n, q_1, \ldots, q_m$ são primos. Assim, por (**??**), temos que

$$p_1 \mid q_j$$

para algum $j = 1, \ldots, m$. Sem perda de generalidade, podemos supor que $p_1 \mid q_1$. Mas, como q_1 também é primo, então $p_1 = q_1$. Desse modo, pela lei do cancelamento, segue que

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

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

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

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

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

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

$$1 = p_{n+1} \cdots p_m,$$

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

Como os primos que surgem na fatoração de um dado $a \in \mathbb{N}$, $a > 1$, não são necessariamente distintos, temos:

Corolário 2.4 *Todo número natural $a > 1$ pode ser escrito de forma única, a menos da ordem dos fatores, na forma*

$$a = p_1^{r_1} \cdot p_2^{r_2} \ldots p_n^{r_n},$$

em que $p_1 < p_2 < \cdots < p_n$ são números primos e $r_i \in \mathbb{N}$, para cada $i = 1, \ldots, n$. ■

Às vezes, se um dado primo p_k não surge com expoente maior do que zero na fatoração de $a \in \mathbb{N}$, $a > 1$, é conveniente escrever a na forma

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

Por isso, de uma forma geral, podemos considerar $r_i \in \mathbb{N} \cup \{0\}$, para cada $i = 1, \ldots, n$. Por este motivo, dados $a, b \in \mathbb{N}$, com $a > 1$ e $b > 1$, sempre é possível escrevê-los como

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

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

Por exemplo, $a = 300 = 2^2 \times 3 \times 5^2$ e $b = 154 = 2 \times 7 \times 11$. Portanto,

$$a = 2^2 \cdot 3 \cdot 5^2 \cdot 7^0 \cdot 11^0 \quad \text{e} \quad b = 2 \cdot 3^0 \cdot 5^0 \cdot 7 \times 11.$$

Teorema 2.8 *Se $n > 1$ é composto, então n possui, necessariamente, um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração: Sendo n um número composto, então

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

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

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

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

Em outras palavras, o Teorema 2.8 nos mostra que, para verificarmos se um dado número $n > 1$ é primo, é suficiente verificarmos a divisibilidade de n pelos primos $p \leq \sqrt{n}$.

Exemplo 2.12 Para o número $n = 103$, temos que $\sqrt{103} \leq 10$ e os primos menores ou iguais a 10 são $2, 3, 5$ e 7. Como nenhum destes primos divide n, concluímos que n é primo. ♣

Capítulo 3

Os Teoremas de Euler, Fermat e Wilson

É muito frequente em matemática nos defrontarmos com problemas que envolvem números inteiros demasiadamente grandes, tais números são quase impossíveis de serem manipulados fazendo uso apenas das operações básicas da aritmética (adição, subtração, multiplicação e divisão). Por exemplo, encontrar o resto da divisão de 2^{50} por 7 utilizando apenas as operações básicas não é uma tarefa tão fácil.

Fermat, no século XV, conjecturou que todo número da forma $2^{2^n}+1$, com $n \in \mathbb{N}$, é sempre primo, o que se constata facilmente para $n = 0, 1, 2, 3$ e 4. Mas, para $n = 5$, por exemplo, tem-se que $2^{2^5}+1 = 2^{32}+1$, que já é um número relativamente grande para que se possa concluir se o mesmo possui ou não divisores diferentes de 1 e dele próprio, utilizando as operações básicas, muito embora Euler tenha mostrado que para $n = 5$, a fórmula não é mais válida.

O conceito de congruência é uma forte ferramenta em teoria dos números, em particular, é importante para o trato de problemas como o destacado acima.

3.1 Congruências

O conceito de congruência é de grande importância na Teoria dos Números, na Álgebra, e suas aplicações. Muitos problemas e estudos podem ser reduzidos à aritmética modular, e nesse ambiente eles são tratados em um conjunto finito.

Definição 3.1 *Sejam a e $b \in \mathbb{Z}$ e n inteiro positivo. Dizemos que a e b são* ***congruente módulo*** *n quando $n \mid (a-b)$. Caso contrário, ou seja, se $n \nmid (a-b)$, dizemos que a e b são* ***incongruentes*** *módulo n.*

Usaremos a notação $a \equiv b (\mathrm{mod}\, n)$ para denotar que a é congruente a b módulo n, e sua negação por $a \not\equiv b (\mathrm{mod}\, n)$.

Exemplo 3.1 *Temos que,* $15 \equiv 5 (\mathrm{mod}\, 5)$*, pois* $5 \mid (15-5)$*. Também,* $10 \not\equiv 3 (\mathrm{mod}\, 4)$*, pois* $4 \nmid (10-3)$*.*

Proposição 3.1 *Se a e b são números inteiros e n inteiro positivo, temos que $a \equiv b (\mathrm{mod}\, n)$, se e somente se, existir um inteiro λ tal que*

$$a = b + \lambda \cdot n.$$

Demonstração: Se $a \equiv b (\mathrm{mod}\, n)$, então $n \mid (a-b)$, donde segue da definição de divisibilidade que existe $\lambda \in \mathbb{Z}$ tal que

$$\lambda \cdot n = a - b \Leftrightarrow a = b + \lambda \cdot n.$$

Reciprocamente, suponhamos que existe $\lambda \in \mathbb{Z}$ com $a = b + \lambda \cdot n$, temos

$$\lambda \cdot n = a - b \Rightarrow n \mid (a-b) \Rightarrow a \equiv b (\mathrm{mod}\, n).$$

■

Proposição 3.2 *Sejam a, b, c e d inteiros quaisquer e n natural fixo. Então, são válidas as seguintes sentenças.*

(1) $a \equiv a (\mathrm{mod}\, n)$.

(2) Se $a \equiv b (\mathrm{mod}\, n)$, então $b \equiv a (\mathrm{mod}\, n)$.

(3) Se $a \equiv b (\mathrm{mod}\, n)$ e $b \equiv c (\mathrm{mod}\, n)$, então $a \equiv c (\mathrm{mod}\, n)$.

(4) Se $a \equiv b (\mathrm{mod}\, n)$ e $c \equiv d (\mathrm{mod}\, n)$, então $a + c \equiv b + d (\mathrm{mod}\, n)$ e $ac \equiv bd (\mathrm{mod}\, n)$.

(5) Ser $a \equiv b(\mathrm{mod}\, n)$, então $a + c \equiv b + c(\mathrm{mod}\, n)$.

(6) Se $a \equiv b(\mathrm{mod}\, n)$, então $a^k \equiv b^k(\mathrm{mod}\, n), \quad \forall\ k \in \mathbb{N}$.

(7) Se $a + c \equiv b + c(\mathrm{mod}\, n)$, então $a \equiv b(\mathrm{mod}\, n)$.

(8) Se $mdc(c, n) = 1$, então $ac \equiv bc(\mathrm{mod}\, n) \Leftrightarrow a \equiv b(\mathrm{mod}\, n)$.

Demonstração: Vamos demonstrar apenas (4) e (6).

(4) Por hipótese, temos que $a = b + \lambda_1 \cdot n$ e $c = d + \lambda_2 \cdot n$. Assim,

$$a + b = (b + d) + (\lambda_1 + \lambda_2) \cdot n \Rightarrow a + c \equiv b + d(\mathrm{mod}\, n).$$

Também,

$$ac = (b + \lambda_1 \cdot n) \cdot (d + \lambda_2 \cdot n) = bd + (b\lambda_2 + d\lambda_1 + \lambda_1\lambda_2 n) \cdot n.$$

Por isso, $ac \equiv bd(\mathrm{mod}\, n)$.

(6) Sabe-se que para qualquer $k \in \mathbb{N}$,

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

Desse modo, se $a \equiv b(\mathrm{mod}\, n)$, então $a - b$ é múltiplo de n e, portanto, $a^k - b^k$ também o é, ou seja, $a^k \equiv b^k(\mathrm{mod}\, n)$. ■

Os resultados da proposição anterior têm muitas aplicações aritméticas, em particular, é importante para o cálculo do resto da divisão de um número relativamente grande por outro. O exemplo a seguir ilustra isso.

Exemplo 3.2 *Determine o resto da divisão de* 2^{50} *por* 7.

Solução: Como $2^3 \equiv 1(\mathrm{mod}\, 7)$, então usando o item (6) da Proposição 3.2, segue que

$$(2^3)^{16} \equiv 1^{16}(\mathrm{mod}\, 7) \Rightarrow 2^{48} \equiv 1(\mathrm{mod}\, 7).$$

Agora, pelos itens (1) e (4) da mesma proposição,

$$2^{48} \cdot 2^2 \equiv 1 \cdot 2^2(\mathrm{mod}\, 7) \Rightarrow 2^{50} \equiv 4(\mathrm{mod}\, 7).$$

Como $0 \leq 4 < 7$, então o resto da divisão de 2^{50} por 7 é igual a 4. ♣

Como já foi citado no início, Fermat conjecturou que todo número da forma

$$F_n = 2^{2^n} + 1$$

é sempre primo. Ele estava certo para $n = 0, 1, 2, 3$ e 4, pois

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 3, \\ F_1 &= 2^{2^1} + 1 = 5, \\ F_2 &= 2^{2^2} + 1 = 17, \\ F_3 &= 2^{2^3} + 1 = 257 \\ F_4 &= 2^{2^4} + 1 = 65537. \end{aligned}$$

Para $n = 5$, temos que $F_5 = 2^{32} + 1 = 4294967296$. Como saber se esse número relativamente grande possui outros divisores, além dos triviais? Euler mostrou que F_5 é divisível por 641. Vejamos como podemos constatar isso utilizando congruências. Temos que $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$. Daí, $2^4 = 641 - 5^4$. Por outro lado,

$$641 \equiv 0 (\mathrm{mod}\, 641),$$

ou seja,

$$641 - 5^4 \equiv -5^4 (\mathrm{mod}\, 641),$$

donde segue que

$$(641 - 5^4)2^{28} \equiv -5^4 \cdot 2^{28} (\mathrm{mod}\, 641).$$

Além disso,

$$\begin{aligned} 2^{2^5} = 2^{32} &= 2^4 \cdot 2^{28} \\ &= (641 - 5^4)2^{28} \\ &\equiv -5^4 \cdot 2^{28} (\mathrm{mod}\, 641) \\ &= -(5 \cdot 2^7)^4 \\ &= -(641 - 1)^4 \\ &\equiv -1 (\mathrm{mod}\, 641). \end{aligned}$$

Isso significa que 641 divide $2^{2^5} + 1$.

Os números da forma $F_n = 2^{2^n} + 1$, com $n \geq 0$, são chamados Números de Fermat. Atualmente, só se conhece cinco Números de Fermat que são primos, os mesmos que o próprio Fermat conhecia. Além disso, sabe-se que F_n não é primo para $5 \leq n \leq 16$.

A partir das aplicações acima, pode-se perceber a importância do uso das congruências na resolução de alguns problemas envolvendo números inteiros relativamente grandes. Essa ferramenta ganha ainda mais destaque quando entra combinada com os teoremas de Fermat, Euler e Wilson.

3.1.1 O Pequeno Teorema de Fermat

O teorema que segue é fortemente usado em teoria dos números. Apesar de levar o nome de Fermat, a demonstração do mesmo foi publicada por Euler. O leitor deve ficar atento para não confundir esse resultado com o Último Teorema de Fermat, o qual mencionamos no início.

Teorema 3.1 (Pequeno Teorema de Fermat) *Se p é um número primo e a é um número inteiro tal que $p \nmid a$, então $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.*

Demonstração: Vamos considerar o conjunto de números inteiros

$$A = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

Uma primeira coisa a se observar é que os elementos de A são dois a dois incongruentes entre si módulo p. De fato, dados $\alpha, \beta \in A$, digamos $\alpha = \lambda_1 a$ e $\beta = \lambda_2 a$, com $\lambda_1, \lambda_2 \in \{1, 2, \ldots, (p-1\}$, temos que se $\alpha \equiv \beta (\mathrm{mod}\, p)$, então $p \mid (\lambda_1 - \lambda_2)a$. Mas como p é primo e $p \nmid a$, então $p \mid (\lambda_1 - \lambda_2)$, o que não é possível, pois $|(\lambda_1 - \lambda_2| < p$. Isso mostra que α e β são incongruentes módulo p. Por outro lado, mostra-se que nenhum elemento de A é congruente a zero módulo p. Sendo assim, temos que cada elemento de A é congruente a apenas um, e somente um elemento do conjunto

$$B = \{1, 2, 3, \ldots, p-1\},$$

Sem perda de generalidade, podemos supor que

$$\begin{array}{rcll} a & \equiv & 1 & (\mathrm{mod}\, p), \\ 2a & \equiv & 2 & (\mathrm{mod}\, p), \\ 3a & \equiv & 3 & (\mathrm{mod}\, p), \\ \vdots & \vdots & \vdots & \vdots \\ (p-1)a & \equiv & (p-1) & (\mathrm{mod}\, p). \end{array}$$

Multiplicando membro a membro as congruências acima, obtemos pelo item (6) Proposição 3.2 que

$$a \cdot (2a) \cdot (3a) \cdots (p-1) \cdot a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\mathrm{mod}\, p),$$

ou seja,

$$a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) (\mathrm{mod}\, p),$$

de modo que

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

Assim, como $mdc((p-1)!, p) = 1$, então

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

■

Corolário 3.1 *Se p é uma número primo e a é um número inteiro qualquer, então* $a^p \equiv a (\mathrm{mod}\, p)$.

Demonstração: Se $p \nmid a$, então do teorema anterior, temos que

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

Assim,

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

Por outro lado, se $p \mid a$, então é claro que $p \mid a^p$ e, por conseguinte, $p \mid a^p - a$, ou seja, $a^p \equiv a (\mathrm{mod}\, p)$. ■

Exemplo 3.3 *Mostrar que $2^{70} + 3^{70}$ é divisível por* 13.

Solução: Do Teorema de Fermat com $p = 13$ e $a = 2$, temos que $2^{12} \equiv 1 (\mathrm{mod}\, 13)$. Por isso, $(2^{12})^5 \equiv 1^5 (\mathrm{mod}\, 13)$, isto é,

$$2^{60} \equiv 1 (\mathrm{mod}\, 13).$$

Agora,

$$2^5 \equiv 6 (\mathrm{mod}\, 13) \Rightarrow 2^{10} \equiv 36 (\mathrm{mod}\, 13).$$

Assim, $2^{60} \cdot 2^{10} \equiv 1 \cdot 36 (\mathrm{mod}\, 13)$, de modo que

$$2^{70} \equiv 36 (\mathrm{mod}\, 13). \tag{3.1}$$

Da mesma forma, com $a = 3$ temos $3^{12} \equiv 1 (\mathrm{mod}\, 13)$, de onde obtemos

$$(3^{12})^5 \equiv 1^5 (\mathrm{mod}\, 13) \Rightarrow 3^{60} \equiv 1 (\mathrm{mod}\, 13).$$

Além disso,

$$3^3 \equiv 1 (\mathrm{mod}\, 13) \Rightarrow 3^9 \equiv 1 (\mathrm{mod}\, 13) \Rightarrow 3^{10} \equiv 3 (\mathrm{mod}\, 13).$$

Logo, $3^{10} \cdot 3^{60} \equiv 3 \cdot 1 (\mathrm{mod}\, 13)$, isto é,

$$\Rightarrow 3^{70} \equiv 3 (\mathrm{mod}\, 13). \tag{3.2}$$

Somando membro a membro as congruências de (3.1) e (3.2),

$$2^{70} + 3^{70} \equiv 36 + 3 (\mathrm{mod}\, 13) \Rightarrow 2^{70} + 3^{70} \equiv 39 (\mathrm{mod}\, 13).$$

Como $39 \equiv 0 (\mathrm{mod}\, 13)$, então por transitividade,

$$2^{70} + 3^{70} \equiv 0 (\mathrm{mod}\, 13).$$

♣

3.1.2 O Teorema de Euler

Euler foi um grande matemático suíço do século XVIII, nascido na cidade da Basiléia. Ele viveu os últimos dezessete anos de sua vida com total deficiência visual devido o excesso de estudos, mas mesmo assim não parou de produzir seus artigos, sendo o matemático que mais publicou artigos, sendo considerado até hoje o mais prolífero entre todos os matemáticos.

Esta seção será dedicada ao teorema de Euler. Antes, começaremos com alguns resultados necessários à sua demonstração.

Definição 3.2 *A função $\varphi : \mathbb{N} \to \mathbb{N}$ dada por $\varphi(1) = 1$ e $\varphi(n) = s$, em que s é o número de inteiros positivos m com $1 \leq m < n$ e $mdc(m, n) = 1$, chama-se* ***função de Euler****.*

Exemplo 3.4 *Temos que* $\varphi(8) = 4$*, pois* $1, 3, 5$ *e* 7 *são menores do que* 8 *e relativamente primos com ele. Similarmente,* $\varphi(15) = 8$ ♣

Observação 3.1 *É fácil ver que se* $n = p$ *é um número primo, então* $\phi(p) = p - 1$.

Definição 3.3 *Um* ***sistema reduzido de resíduos módulo*** n *é um conjunto de* $\phi(n)$ *números inteiros do conjunto* $R = \{r_1, r_2, \ldots, r_{\phi(n)}\}$*, tais que cada elemento de* R *é relativamente primo com* n*, e se* $i \neq j$*, então* $r_i \not\equiv r_j (\mathrm{mod}\, n)$.

Exemplo 3.5 *O conjunto* $R = \{1, 2, 3, 4\}$ *é um sistema reduzido de resíduos módulo* 5*. Já o conjunto* $R' = \{1, 5\}$ *é um sistema reduzido de resíduos módulo* 6.

Exemplo 3.6 *mama colocar um contra exemplo.*

Teorema 3.2 *Seja* $a > 0 \in \mathbb{Z}$ *tal que* $mdc(a, n) = 1$*. Se* $R_1 = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ *é um sistema reduzido de resíduos módulo* n*, então* $R_2 = \{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}\}$ *também é um sistema reduzido de resíduos módulo* n.

Demonstração: Primeiramente, nota-se que $R_2 = \{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}\}$ possui exatamente $\phi(n)$ elementos. Por isso, basta mostrar que estes elementos são relativamente primos com n e que são dois a dois incongruentes módulo n.

Como $mdc(a, n) = 1$ e $mdc(r_i, n) = 1$, então $mdc(a \cdot r_i, n) = 1$. Por outro lado, vamos supor que $i \neq j$. Como por hipótese, $mdc(a, n) = 1$, então se $a \cdot r_i \equiv a \cdot r_j (\mathrm{mod}\, n)$, temos que $r_i \equiv r_j (\mathrm{mod}\, n)$, o que implica em $i = j$, pois $R_1 = \{r_1, r_2, \ldots, r_{\phi(n)}\}$ é um sistema reduzido de resíduos módulo n. Assim, $i \neq j$ e $i = j$, o que é uma contradição. Portanto, $a \cdot r_i \not\equiv a \cdot r_j (\mathrm{mod}\, n)$. Isso finaliza a demonstração. ■

Teorema 3.3 (Teorema de Euler) *Sejam* $a, n \in \mathbb{Z}$*, com* $n \geq 1$*, tais que* $mdc(a, n) = 1$*. Então* $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$.

Demonstração: Pelo Teorema 3.2 temos que os elementos de

$$R_1 = \{a \cdot r_1, a \cdot r_2, \ldots, a \cdot r_{\phi(n)}\}$$

constituem um sistema reduzido de resíduos módulo n se $mdc(a, n) = 1$ e R_1 constituir um sistema reduzido de resíduos módulo n. Ou seja, $a \cdot r_i$ é congruente a um, e apenas um, dos r_j, com $1 \leq j \leq \phi(n)$, e portanto, o produto dos $a \cdot r_i$ deve ser congruente ao produto dos r_j módulo n, isto é,

$$(a \cdot r_1) \cdot (a \cdot r_2) \cdot \ldots \cdot (a \cdot r_{\phi(n)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} (\mathrm{mod}\, n),$$

Ou seja,

$$a^{\phi(n)} \cdot (r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)}) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} (\mathrm{mod}\, n). \tag{3.3}$$

Faça,

$$r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(n)} = \prod_{i=1}^{\phi(n)} r_i.$$

Como,

$$mdc(\prod_{i=1}^{\phi(n)} r_i, n) = 1.$$

Podemos fazer o cancelamento em (3.3), obtendo:

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

■

O leitor deve ter notado, que o Teorema de Euler é na verdade uma generalização do Pequeno Teorema de Fermat, uma vez que, se $n = p$ é um número primo, tem-se $\phi(p) = p - 1$.

Exemplo 3.7 *Mostre que* $7 \cdot 5^{20} \equiv -1 (\mathrm{mod}\, 8)$.

Solução: Usando o teorema de Euler, temos que:

$$5^4 \equiv 1(\mathrm{mod}\, 8) \Rightarrow 7 \cdot 5^{20} \equiv 7 \cdot 1(\mathrm{mod}\, 8) \Rightarrow 7 \cdot 5^{20} \equiv 7(\mathrm{mod}\, 8).$$

Por outro lado,

$$7 \equiv 15(\mathrm{mod}\, 8) \quad e \quad 15 \equiv -1(\mathrm{mod}\, 8).$$

Donde seguem por transitividade, que:

$$7 \cdot 5^{20} \equiv -1(\mathrm{mod}\, 8).$$

♣

3.1.3 O Teorema de Wilson

John Wilson (1741 – 1793) conjecturou que se p é um número primo, então p divide $(p-1)!+1$, ou, equivalentemente, que a divisão de $(p-1)!$ por p deixa resto -1. Tal enunciado se encontra no livro Medidationes algebraicae, publicado em 1770 por Eduard Waring (1734–1798), no entanto, o resultado ainda não havia sido provado. A prova foi dada em 1771 por Legendre. Veja a segui como o resultado pode ser escrito e provado utilizando as notações e os resultados de congruências. Mas antes anunciremos dois lemas importantes na demonstração do teorema de Wilson.

Lema 3.1 *Seja $p > 0$ um número primo. Para cada $a \in C = \{1, 2, \ldots, p-1\}$ existe um número $b \in C$ tal que $ab \equiv 1 (\mathrm{mod}\, p)$.*

(falta)

Lema 3.2 *Seja p um número primo. Os únicos elementos do conjunto*

$$C = \{1, 2, \ldots, p-1\}$$

que satisfazem a equação $x^2 \equiv 1 (\mathrm{mod}\, p)$ são 1 e $p-1$.

Demonstração: Tomemos $a \in C$ de modo que $a^2 \equiv 1 (\mathrm{mod}\, p)$, isto é,

$$p \mid (a^2 - 1) \Rightarrow p \mid (a-1) \cdot (a+1).$$

Como p é um número, então

$$p \mid (a-1) \quad \text{ou} \quad p \mid (a+1),$$

Como $a \in C$, temos que

$$1 \leq a \leq p-1 \Rightarrow 2 \leq a+1 \leq p.$$

Donde segue que $p = a+1$, o que implica que $a = p-1$.

Analogamente, considerando que $p \mid a-1$, e como $a - 1 \leq p$, para todo $a \in C$, só nos resta a possibilidade de $a - 1 = 0$, o que implica $a = 1$, finalizando assim a demonstração. ■

Teorema 3.4 ***(Teorema de Wilson)*** *Se p é um número primo, então*

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

Demonstração: Se $p = 2$ ou $p = 3$, temos a validade do teorema. De fato:

$$(2-1)! \equiv 1 (\mathrm{mod}\, 2) \quad \text{e} \quad (2-1)! \equiv 1 (\mathrm{mod}\, 2).$$

Supondo agora $p > 3$. E consideremos o conjunto

$$C = \{2, 3, \ldots, (p-2)\}.$$

De acordo com os lemas 3.1 e 3.2, podemos tomar os pares $a_1, a_2 \in C$, tais que $a_1 \neq a_2$ e $a_1 \cdot a_2 \equiv 1 (\mathrm{mod}\, p)$.

Consequentemente, efetuando o produto dos elementos desse conjunto, temos que:

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 (\mathrm{mod}\, p).$$

Por outro lado, é fácil ver que

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

Utilizando as propriedades de congruências, obtemos:

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (-1) (\mathrm{mod}\, p).$$

Finalizando a demonstração, temos

$$(p-1)! \equiv -1 (\mathrm{mod}\, p).$$

■

Exemplo 3.8 *Mostrar que a divisão de* $15!$ *por* 17 *deixa resto* 1*.*

Solução: Pelo Teorema de Wilson sabemos que

$$16! \equiv -1 (\mathrm{mod}\, 17) \Rightarrow 16 \cdot 15! \equiv -1 (\mathrm{mod}\, 17),$$

Por outro lado,

$$-1 \equiv 16 (\mathrm{mod}\, 17),$$

Por transitividade,

$$16 \cdot 15! \equiv 16 (\mathrm{mod}\, 17),$$

Como $mdc(16, 17) = 1$, temos

$$15! \equiv 1 (\mathrm{mod}\, 17).$$

Logo, o resto da divisão de 15! por 17 é igual a 1. ♣

Bibliografia

[1] BOYER, Carl B., *A história da Matemática*, tradução Elza F. Gomide, 2ª ed. São Paulo: Edgard Blucher, 1996.

[2] MILIES, C. P. e COELHO, S. P. – *Números: Uma Introdução à Matemática* (3ª edição), Edusp, 2001.

[3] DOMINGUES, Hygino H., IEZZI, Gelson. *Álgebra Moderna*. 4ª Ed. São Paulo: Atual, 2003.

[4] MILIES, Francisco César Polcino, COELHO, Sônia Pinto. *Números: Uma Introdução à Matemática*. 3ª ed. São Paulo: Editora da Universidade de São Paulo, 2006.

[5] RIBENBOIM, Paulo. *Números Primos: Velhos Mistérios e Novos Recordes*. Coleção Matemática Universitária 1ª ed. Rio de Janeiro: IMPA, 2012.

[6] SANTOS, José Plínio de Oliveira. *Introdução à Teoria dos Números*. 3ª ed. Coleção Matemática Universitária, Rio de Janeiro: IMPA, 2005.