Universidade Federal do Paraná

Tiago Gonçalves de Andrade

O Pequeno Teorema de Fermat

Curitiba

2019

Tiago Gonçalves de Andrade

O Pequeno Teorema de Fermat

Trabalho de conclusão apresentado ao curso de Licenciatura em Matemática da Universidade Federal do Paraná como requisito parcial à obtenção do grau de licenciado em Matemática.
Orientador: Prof. Dr. Aldemir José da Silva Pinto

Curitiba
2019

"A Matemática é a rainha das Ciências, e a Teoria dos Números é a rainha das matemáticas".

– K. F. Gauss

Agradecimentos

À minha família, pela paciência, por sempre acreditarem em mim, me incentivarem nos momentos de dificuldade, e pela educação de qualidade;

Aos meus amigos de graduação, futuros professores, que perante nosso objetivo fizeram desta parte importante da minha vida mais satisfatória e divertida. Em especial, a Adriano Aparecido da Silva que sempre esteve ao meu lado me apoiando;

Ao meu orientador Aldemir José da Silva Pinto, pelos ensinamentos, disponibilidade, e incentivo durante todo o percurso;

Agradeço também a instituição, por me dar a oportunidade e as ferramentas necessárias para adquirir este título;

Enfim, agradeço a todos que contribuíram de alguma forma para a realização deste trabalho.

Resumo

O objetivo deste trabalho é entender e demonstrar o Pequeno Teorema de Fermat. Para tal, trazemos uma fundamentação axiomática dos números inteiros e algumas propriedades complementares referentes aos mesmos, associando com a forma que esses elementos se relacionam uns com os outros. Com esse enfoque, analisamos ainda a relação desses elementos perante outras perspectivas, como a da divisibilidade e das congruências. Trazemos ainda outros resultados importantes para a Teoria dos Números, como o Princípio da Indução Completa, o Algoritmo da Divisão de Euclides, o Teorema de Bézout, o Teorema de Euclides, o Teorema Fundamental da Álgebra, dentre outros.

Palavras-chave: Teoria dos Números, Números primos, Pequeno Teorema de Fermat, Divisibilidade, Congruência.

Abstract

The objective of this work is to understand and demonstrate Fermat's Little Theorem. For this, we bring an axiomatic basis of the integers and some complementary properties referring to them, associating with the form that these elements relate to each other. With this approach, we analyze the relationship of these elements to other perspectives, such as divisibility and congruences.We also present other important results for Number Theory, such as the Principle of Complete Induction, Euclid's Division Algorithm, Bézout's Theorem, Euclid's Theorem, the Fundamental Algebra Theorem, among others.

Keywords: Numbers Theory, Prime Numbers, Fermat's Little Theorem, Divisibility, Congruence.

Sumário

Introdução

A Teoria dos Números é parte determinante dos esforços de matemáticos para o desenvolvimento da Matemática. Neste trabalho, iremos desenvolver diversos conceitos e resultados que nos servirão de base para que possamos provar e entender o Pequeno Teorema de Fermat.

Evidentemente o objeto de estudo dessa teoria são os números, em particular, os números inteiros. Para tal, concretizamos axiomaticamente o conjunto dos números inteiros ($\mathbb{Z}$) a fim de entendermos como os elementos desse conjunto se distribuem, se relacionam, quais resultados essas relações produzem e quais nos motiva a investigar. Partindo dessa ideia, o presente trabalho é dividido em três partes. A primeira delas se refere a fundamentar axiomaticamente esse conjunto, ou seja, através de axiomas (verdades evidentes) construirmos e provarmos outros resultados com relação a como podemos relacionar os elementos de $\mathbb{Z}$. Feito isso, definimos o conceito de *divisibilidade* como uma outra forma de relacionar dois números inteiros, e vemos como esses elementos se comportam agora com esse novo conceito. Sendo assim, provamos outros resultados que provém dessa definição, mas que ainda estão submetidos aos axiomas que vimos inicialmente.

Salientamos aqui que esse processo é parte fundamental de construir uma teoria sobre algo, de uma forma geral, pois, uma vez que partimos de verdades evidentes para provar teoremas, proposições, entre outros resultados, estes também passam a serem vistos como verdades que, apesar de muitas vezes não serem evidentes, servem de base para que possamos concluir outras coisas, e assim poder avançar cada vez mais em relação aos conhecimentos adquiridos.

Ainda falando sobre o conceito de divisibilidade, podemos definir o que é um "número primo", sendo este agora um novo conceito ao qual voltamos a investigar suas propriedades através dos conhecimentos que já obtivemos. Porém, o mais interessante deste é que, apesar de seu entendimento ser simples, encontrar um número primo não é tarefa muito fácil. Muitos matemáticos se dedicaram a desenvolver métodos para encontrá-los, e até então, grande parte dos números primos que conhecemos devemos aos esforços de Marin Mersenne, que apesar de não ter tido

a oportunidade em vida de conhecer os primos que conhecemos hoje, teve grande contribuição para que matemáticos posteriores a ele os encontrassem através de seu método.

Por fim, definimos o conceito de *congruência*, sendo este parte fundamental deste trabalho, pois é através do mesmo que demonstramos o Pequeno Teorema de Fermat.

Pensando na fundamentação e direcionamento dos estudos, para o desenvolvimento deste trabalho, utilizamos como base o livro [1]. Por meio deste seguimos uma sequência de estudo a fim de demonstrar o Pequeno Teorema de Fermat. Entretanto, no decorrer deste trabalho também buscamos inspiração em outras fontes como, por exemplo, o livro [2], para demonstrarmos o Teorema Fundamental da Aritmética, [3] para buscar curiosidades referentes aos números primos, e [4] para mostrar um resultado referente ao Binômio de Newton.

Capítulo 1

Uma breve introdução aos Números Inteiros ($\mathbb{Z}$)

O conjunto dos números inteiros ($\mathbb{Z}$) é um conjunto bem conhecido, onde estão bem definidas as operações de adição e multiplicação, além da relação de "menor ou igual"($\leq$). Mas, ele nem sempre foi tão aceito como hoje, devido a diversas interpretações em relação aos "números negativos". Com o aparecimento dos números complexos (em meados do séc.XVI), foi posta em cheque a origem dos números que era até então aceita, movendo os estudiosos da época a formular uma teoria ainda mais axiomática dos números.

O que faremos neste capítulo é abordar certos axiomas desse conjunto que fundamenta a teoria dos números como veremos a seguir.

1.1 Principais axiomas: uma fundamentação axiomática

Inicialmente vamos apresentar os principais postulados dos números inteiros, e em seguida, outras propriedades e relações que podem ser provadas a partir das primeiras.

Dessas propriedades básicas que veremos a seguir, quatro são referentes a adição, identificadas como A1, A2, A3 e A4; quatro referentes a multiplicação reconhecidas com M1, M2, M3 e M4; e uma outra que envolve ambas operações (AM). Dito isso, sejam α, β, $\gamma \in \mathbb{Z}$, temos que valem as seguintes afirmações:

A1. Associatividade: $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$; $\forall \alpha, \beta, \gamma \in \mathbb{Z}$.

A2. Existência do elemento neutro: $\exists x \in \mathbb{Z}$ tal que $\alpha + x = \alpha$, $\forall \alpha \in \mathbb{Z}$.

Notação: $x = 0$.

A3. Existência do oposto: $\forall \alpha \in \mathbb{Z}$, $\exists y \in \mathbb{Z}$ de tal modo que, $\alpha + y = 0$.

Notação: $y = -\alpha$.

A4. Comutatividade: $\forall \alpha \in \mathbb{Z}$ temos que $\alpha + \beta = \beta + \alpha$.

M1. Associatividade: $(\alpha.\beta).\gamma = \alpha.(\beta.\gamma)$; $\forall \alpha, \beta, \gamma \in \mathbb{Z}$.

M2. Existência do elemento neutro: $\exists p \in \mathbb{Z}$ tal que $\alpha.p = \alpha$, $\forall \alpha \in \mathbb{Z}$.

Notação: $p = 1$.

M3. Cancelativa: $\forall \alpha, \beta, \gamma \in \mathbb{Z}$ com $\alpha \neq 0$, podemos concluir que se $\alpha\beta = \alpha\gamma$, então $\beta = \gamma$.

M4. Comutatividade: $\alpha.\beta = \beta.\alpha$, $\forall \alpha, \beta \in \mathbb{Z}$.

AM. Distributividade: $\alpha.(\beta + \gamma) = \alpha.\beta + \alpha.\gamma$, $\forall \alpha, \beta, \gamma \in \mathbb{Z}$.

Essas propriedades caracterizam o conjunto dos números inteiros ($\mathbb{Z}$), e através delas podemos demonstrar muitas outras que são fundamentais para a teoria de números, como podemos ver no exemplo a seguir.

Exemplo 1. Seja $a, b, c \in \mathbb{Z}$. Se $a + b = a + c$, então $b = c$.

Temos que $a + b = a + c$, logo somando $(-a)$ na igualdade temos,

$\Rightarrow -a + (a + b) = -a + (a + c)$, por A1 temos,

$\Rightarrow (-a + a) + b = (-a + a) + c$, por A3 temos,

$\Rightarrow 0 + b = 0 + c$, e por A2 temos que,

$\Rightarrow b = c$, como gostaríamos.

Observação: É válido ressaltar aqui que esse exemplo é equivalente a propriedade cancelativa M3, porém para a adição.

Exemplo 2. Para todo $a \in \mathbb{Z}$ temos que $a.0 = 0$.

Temos como verdade absoluta que $0 + 0 = 0$, multiplicando por a temos,

$\Rightarrow a.(0 + 0) = a.0$, por AM temos,

$\Rightarrow a.0 + a.o = a.0$, por A2 temos,

$\Rightarrow a.o + a.o = a.o + 0$, pelo exemplo 1, concluímos que,

$a.o = 0$, como gostaríamos.

1.2 Outras propriedades e axiomas: uma complementação

Agora que vimos algumas propriedades sobre adição e multiplicação vamos tomar mais conhecimento sobre a relação de "menor ou igual" ($\leq$), e como os números (inteiros) se relacionam através dela. Para tanto, usaremos que "a menor que b" ($a < b$) é o mesmo que dizer que "$a \leq b$ e $a \neq b$".

P1. Reflexiva: Para todo $a \in \mathbb{Z}$, temos que $a \leq a$.

P2. Anti-Simétrica: Sejam $a, b \in \mathbb{Z}$. Se $a \leq b$ e $b \leq a$, então $a = b$.

P3. Transitiva: Para todo $a, b, c \in \mathbb{Z}$ temos que se $a \leq b$ e $b \leq c$, então $a \leq c$.

Essas três propriedades nos motiva a dizer que $\leq$ é uma relação de ordem dentro do conjunto dos inteiros, uma vez que uma relação é dita de ordem se ela é "reflexiva, anti-simétrica e transitiva".

P4. Tricotomia: Dados $a, b \in \mathbb{Z}$, então $a < b$, $b < a$ ou $a = b$.

Observação: Essa propriedade nos permite "colocar" todos os números inteiros em uma sequência, crescente ou decrescente.

P5. Princípio da Boa Ordem: Temos que para todo conjunto $A \subset \mathbb{Z}^+$ com $A \neq \varnothing$, $\exists a_0 \in A$ tal que $a_0 \leq a$, $\forall a \in A$.

Em outras palavras, o conjunto A é dito limitado inferiormente, mas, para entendermos melhor essa propriedade, precisamos ter em mente as seguintes definições.

Definição 1 (Os inteiros positivos)**.** *O conjunto* $\mathbb{Z}^+ = \{x \in \mathbb{Z} \mid x \geq 0\}$.

Definição 2 (Conjunto Limitado)**.** *Seja $A \subset \mathbb{Z}$, dizemos que A é um conjunto limitado inferiormente se $\exists k \in \mathbb{Z}$ tal que para todo $a \in A$ temos $k \leq a$, ou seja, A possui um elemento mínimo $a_0 \in \mathbb{Z}$ tal que $\forall a \in \mathbb{Z}$, $a_0 \leq a$. De forma análoga podemos definir um conjunto limitado superiormente.*

Proposição 1. *Sejam $a, b \in \mathbb{Z}$. Se $a.b = 0$, então $a = 0$ ou $b = 0$.*

Demonstração. Temos da proposição anterior que $0 = a.0$, $\forall a \in \mathbb{Z}$, logo, temos que $a.b = a.0$, nesse caso, se $a = 0$ já está provado, caso contrário, ou seja, se $a \neq 0$, podemos concluir que $b = 0$, pela propriedade M3 que mencionamos anteriormente. □

Essas proposições nos permitem trabalhar com mais facilidade e liberdade na teoria que está sendo desenvolvida aqui, como veremos na proposição a seguir.

Proposição 2 (Regra de sinais)**.** *Sejam $a, b \in \mathbb{Z}$, então valem:*

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

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

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

Demonstração. Note que para provar esses itens, basta mostrar que o elemento do segundo membro é, na verdade, o elemento oposto da adição do primeiro membro, vide propriedade A3, logo, basta verificar que a diferença entre eles é igual a zero.

(i) De fato,

$$\begin{aligned} -(-a) - a &= -a(-1+1), \text{ por AM,} \\ \Rightarrow -(-a) - a &= -a.0, \text{ por A3,} \\ \Rightarrow -(-a) - a &= 0, \text{ pelo exemplo 2.} \end{aligned}$$

Portanto, $-(-a) = a$.

(ii) Esse item vamos resolver por partes: $I) \rightarrow (-a)b = -(ab)$ e $II) \rightarrow -(ab) = a.(-b)$.

$$\begin{aligned} (I)\ (-a)b + (ab) &= (-a+a).b, \text{ por AM,} \\ \Rightarrow (-a)b + (ab) &= 0.b, \text{ por A3,} \\ \Rightarrow (-a)b + (ab) &= 0, \text{ pelo exemplo 2, logo,} \\ \Rightarrow (-a)b &= -(ab). \\ (II)\ a.(-b) + (ab) &= a(-b+b), \text{ por AM,} \\ \Rightarrow a.(-b) + (ab) &= a.0, \text{ por A3,} \\ \Rightarrow a.(-b) + (ab) &= 0, \text{ pelo exemplo 2, logo,} \\ \Rightarrow -(ab) &= a.(-b). \end{aligned}$$

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

(iii) De fato,

$$\begin{aligned} (-a)(-b) - (ab) &= (-a)(-b) + a(-b), \text{ por } (II), \\ \Rightarrow (-a)(-b) - (ab) &= (-a+a)(-b), \text{ por AM,} \end{aligned}$$

$$\Rightarrow (-a)(-b) - (ab) = 0.(-b), \text{ por A3},$$
$$\Rightarrow (-a)(-b) - (ab) = 0, \text{ pelo exemplo 2},$$

Portanto, $(-a)(-b) = (ab)$.

□

A regra de sinais é muito importante e simples de entender, embora possa causar confusão aos estudantes pela maneira que é ensinada na escola, uma vez entendida, usamo-nas de olhos fechados na Matemática.

Exemplo 3. Seja $a \in \mathbb{Z}$, então temos que:
i) Se $a \leq 0$, então $-a \geq 0$.
ii) Se $a \geq 0$, então $-a \leq 0$.
iii) $a^2 \geq 0$, $\forall a \in \mathbb{Z}$. Ou, em outras palavras, "todo quadrado é não negativo".

Primeiramente podemos observar que esse exemplo nos diz na verdade que se $a \in \mathbb{Z}$ tal que $a \geq 0$, então seu oposto da soma é negativo, ou se $a \leq 0$, então o seu elemento oposto da soma é positivo.
(i) De fato, temos como hipótese que $a \leq 0$, somando $(-a)$ temos,

$$\Rightarrow (-a) + a \leq 0 + (-a), \text{ por A3 temos},$$
$$\Rightarrow 0 \leq 0 + (-a), \text{ por A2 temos},$$
$$\Rightarrow 0 \leq -a, \text{ ou seja, } -a \geq 0.$$

E note que mantemos o sinal de $(=)$ na desigualdade pois a pode assumir o valor 0.
(ii) A demonstração desse item é análoga ao i) desse exemplo, então vamos apenas aceitá-la para não ficar muito repetitiva a demonstração.
(iii) Sendo $a \in \mathbb{Z}$, temos que a pode assumir tanto valores negativos quanto positivos, então vamos analisar as duas possibilidades separadamente para facilitar nossos cálculos.

I) Se $a \geq 0$: Multiplicando essa desigualdade por a temos que $a.a \geq a.0$, pelo exemplo 2 já temos que $a^2 \geq 0$.

II) Se $a \leq 0$: Nesse caso, temos diretamente por (i) que $-a \geq 0$, então multiplicando por $(-a)$ a desigualdade temos que $(-a)(-a) \geq (-a).0$, e como vimos na proposição 2, temos que $(-a).(-a) = a.a = a^2$, logo já podemos concluir também que $a^2 \geq 0$.

Proposição 3. *Seja a um inteiro tal que $0 \leq a \leq 1$, então $a = 0$ ou $a = 1$. Em outras palavras, não existe nenhum número inteiro entre 0 e 1.*

Demonstração. Vamos supor por absurdo que exista um $a \in \mathbb{Z}$ tal que $0 \leq a \leq 1$, com isso, podemos definir o seguinte conjunto $S = \{a \in \mathbb{Z} |\ 0 < a < 1\}$, então, pela propriedade 5 (Princípio da Boa ordem), temos que $\exists m \in S$ tal que $0 < m$ e $m < 1$, mas como $0 < m$, temos que $0.m < m.m \Rightarrow 0 < m^2$, e da mesma forma temos $m.m < 1.m \Rightarrow m^2 < m$. Então, por transitividade, temos que $m^2 < m$ e ainda $m < 1$, logo $m^2 < 1$, ou seja, $m^2 \in S$ e $m^2 < m$. Contradição! Pois $m = minS$.

Portanto, não existe $a \in \mathbb{Z}$ tal que $0 \leq a \leq 1$. Então, $a = 0$ ou $a = 1$. □

Observação: Para a prova dessa proposição usamos propriedades que já foram observadas neste trabalho, porém, são verdades fáceis de serem vistas, então não as indicamos para tornar a leitura mais dinâmica.

Vejamos então uma proposição em forma de exemplo muito importante, e que nos permite dizer que não existe nenhum inteiro entre dois inteiros consecutivos, conceito esse que Giuseppe Peano se baseou para fundamentar axiomaticamente sua teoria.

Exemplo 4. Seja $a \in \mathbb{Z}$. Se $b \in \mathbb{Z}$ é tal que $a \leq b \leq a + 1$, então $b = a$ ou $b = a + 1$.

$$\begin{gathered}
\text{Temos que } a \leq b \leq a + 1, \text{ logo somando } (-a) \text{ temos,} \\
\Rightarrow a - a \leq b - a \leq (a + 1) - a, \text{ por A1, A2 e A3 temos,} \\
\Rightarrow 0 \leq b - a \leq 1, \text{ pela proposição anterior temos,} \\
\Rightarrow b - a = 0 \text{ ou } b - a = 1,
\end{gathered}$$

Portanto, $b = a$ ou $b = a + 1$.

1.3 O Princípio da Indução Completa

Nas ciências naturais, de uma forma geral, esse tipo de verificação que temos feito acontece de uma forma diferente, mas que também é aceita. Nesse âmbito, quando está sob investigação a validação de uma lei em relação a um fenômeno que foi observado diversas vezes, o simples fato de o mesmo ter sido observado muitas vezes já pode servir para validar o que está sendo proposto, nas ciências exatas não. Existem vários exemplos de situações dentro da Matemática que acontecem para um grande número de elementos, mas que no fim não valem para todos. Por exemplo, a expressão $\Phi(n) = n^2 - n + 41$ para valores de n dentro do conjunto dos inteiros,

entrega números primos (aqui assumimos que o leitor tenha algum entendimento sobre o que é um número primo, mas de qualquer forma, ele será definido mais à frente na seção 2.3 do trabalho). Para $n = 1$ temos que $\Phi(1) = 41$, da mesma forma $\Phi(2) = 43$, $\Phi(3) = 47$, e assim por diante, porém, quando chegamos à $n = 41$ a expressão falha, pois nesse caso temos $\Phi(41) = 41^2 - 41 + 41 = 41.41 + 0 = 41.41$, ou seja, resulta no produto de dois números inteiros, portanto para $n = 41$ não obtemos um número primo.

O Princípio da Indução Completa é um método bem interessante para provar teoremas, proposições que vem justamente para que possamos garantir a veracidade (ou não) de afirmações como a que acabamos de exemplificar.

Teorema 1. *Seja a um inteiro dado e S um conjunto de inteiros maiores ou iguais a a, que tem as seguintes propriedades:*
i) $a \in S$.
ii) Se um inteiro $k \geq a$ pertence a S, então $k + 1$ também pertence a S.
Então S é o conjunto de todos os inteiros maiores ou iguais a a.

Demonstração. Vamos supor por absurdo que S não é o conjunto de todos os inteiros maiores ou iguais a a, ou seja, deve existir pelo menos um elemento k maior a a tal que $k \notin S$. Isso nos permite definir um conjunto S' tal que os elementos desse conjunto auxiliar são todos os inteiros maiores ou iguais a a que não pertencem a S. Dessa forma, temos que S' é não vazio e limitado inferiormente por a, logo existe $m = minS'$. Ou seja, $a < m$, logo $a \leq m - 1 < m$. Como $m = minS'$, temos que $m - 1 \notin S'$, logo $m - 1 \in S$. Então, por $ii)$ temos que $(m - 1) + 1 \in S \Rightarrow m \in S$. Absurdo! Pois $m \in S'$.

Portanto, $S = \{x | x \geq a\}$. □

Corolário 1 (Princípio de Indução Completa - versão 1)**.** *Seja a um inteiro dado. Suponhamos que para cada $n \geq a$ está dada uma afirmação $A(n)$ de forma que:*
i) $A(a)$ é verdadeira.
ii) Se para um inteiro $k \geq a$, $A(k)$ é verdadeira, então $A(k + 1)$ também é verdadeira.
Então a afirmação $A(n)$ é verdadeira para todo $n \geq a$.

Demonstração. Como vimos no teorema anterior, basta tomar S como sendo o conjunto dos inteiros $n \geq a$ tais que $A(n)$ é verdadeira. Ou seja, como $a \geq a$, então $A(a) \in S$. Supondo que $k \geq a$, então $A(k)$ é verdadeira, logo como $k + 1 \geq a$, então $A(k + 1)$ também pertence a S.

Portanto, S contém todos os inteiros maiores ou iguais a a. □

O que podemos tirar desse teorema e do corolário é que, em situações que intuitivamente permitem esse tipo de demonstração, e as quais ela é útil, para provar a validade das mesmas, basta iniciarmos a nossa demonstração com 3 passos a seguir:

1º) Verificar que a mesma vale para um primeiro elemento (o primeiro que queremos mostrar que a propriedade vale). Normalmente o 0 ou o 1, mas isso não é nenhuma regra, dependerá do que queremos provar.

2º) Assumir que a propriedade vale para um $n = k$.

3º) Mostrar que a propriedade vale também para $n = k+1$, utilizando a hipótese de indução (aquilo que já sabemos e assumimos que é verdade).

É interessante observarmos que existe uma outra forma de tratarmos o Princípio da Indução Completa, equivalente a primeira, cuja demonstração é análoga a anterior e nos pouparemos em repeti-la, porém, a utilizaremos se nos parecer vantajoso.

Corolário 2 (Princípio da Indução Completa - versão 2)**.** *Seja a um inteiro dado. Suponhamos que para cada $n \in \mathbb{Z}$ onde $n \geq a$ está dada uma afirmação $A(n)$ de forma que:*
i) $A(a)$ é verdadeira.
ii) Se $A(m)$ é verdadeira para todo inteiro m tal que $a \leq m \leq k$, então $A(k+1)$ também é verdadeira.
Então, $A(n)$ é verdadeira para todo $n \geq a$.

Agora, vejamos alguns exemplos de como podemos aplicar esse conceito na teoria dos números. Exemplos esses que poderiam, eventualmente, serem demonstrados de alguma outra forma, mas que, com o Princípio da Indução Completa, são facilmente demonstráveis:

Exemplo 5. Sejam a e r dois números inteiros. A sequência $a_1 = a$, $a_2 = a + r$, $a_3 = a + 2r$,..., $a_n = a + (n-1).r$ diz-se uma Progressão Aritmética (PA) de razão r. Provaremos que a soma dos n primeiros termos de uma PA é: $a + (a + r) + ... + (a + (n-1)r) = \frac{n(2a+(n-1))r}{2}$.

Para tal demonstração, seguiremos os 3 passos que citamos anteriormente referentes ao Princípio de Indução.
1º) Para $n = 1$ temos:
$a_1 = \frac{1(2a+(1-1)r)}{2} = \frac{2a}{2} = a$. Logo, para $n = 1$ a premissa é verdadeira.
2º) Agora vamos supor que a afirmação é verdadeira para $n = k$, ou seja, $X_k = a + (a + r) + ... + (a + (k-1)r) = \frac{k(2a+(k-1))r}{2}$ e então mostrar que vale para $k + 1$.

3^o) Sendo assim, temos que $X_{k+1} = a+(a+r)+...+(a+(k-1)r)+(a+kr) = \frac{k(2a+(k-1)r)}{2}+(a+kr)$ pela hipótese, logo

$$\begin{aligned} X_{k+1} &= \frac{k(2a+(k-1)r)}{2}+(a+kr) \\ &= \frac{k(2a+(k-1)r)+2(a+kr)}{2} \\ &= \frac{2ak+(k-1)kr+2a+2kr}{2} \\ &= \frac{2a(k+1)+kr(k-1+2)}{2} \\ &= \frac{2a(k+1)+kr(k+1)}{2} \\ &= \frac{(k+1)(2a+kr)}{2}. \end{aligned}$$

Portanto, vale a nossa afirmação.

Exemplo 6. Vamos provar que para todo inteiro positivo n vale que:
$1^2+2^2+3^2+...+n^2 = \frac{n(2n+1)(n+1)}{6}$. Pelo Princípio da Indução temos que:
1^o) Para $n = 1$ temos: $1^2 = \frac{1(2.1+1)(1+1)}{6} = \frac{(2+1)2}{6} = \frac{3.2}{6} = 1$.
Então, para $n = 1$ vale a afirmação.
2^o) Vamos supor que a mesma vale para $n = k$, logo $x_k = 1^2+2^2+3^2+...+k^2 = \frac{k(2k+1)(k+1)}{6}$ e vamos mostrar que vale também para $k+1$, ou seja: 3^o) Desta forma, temos que:
$X_{k+1} = 1^2+2^2+3^2+...+k^2+(k+1)^2 = \frac{k(2k+1)(k+1)}{6}+(k+1)^2$, logo

$$\begin{aligned} X_{k+1} &= \frac{k(2k+1)(k+1)}{6}+(k+1)^2 \\ &= \frac{k(2k+1)(k+1)+6(k+1)^2}{6} \\ &= \frac{(2k^2+k)(k+1)+6(k+1)(k+1)}{6} \\ &= \frac{(k+1)(2k^2+k+6k+6)}{6} \\ &= \frac{(k+1)(2k^2+4k+3k+6)}{6} \\ &= \frac{(k+1)[2k(k+2)+3(k+2)]}{6} \\ &= \frac{(k+1)[(2k+3)(k+2)]}{6} \\ &= \frac{(k+1)[2(k+1)+1][(k+1)+1]}{6}. \end{aligned}$$

Portanto, a afirmação é verdadeira e vale que $1^2+2^2+3^2+...+n^2 = \frac{n(2n+1)(n+1)}{6}$.

Exemplo 7. Sejam a e r dois números inteiros com $r \neq 1$. A sequência $a_1 = a, a_2 = ar, a_3 = ar^2, ..., a_n = ar^{n-1}$ diz-se uma Progressão Geométrica (PG) de razão r. Vamos provar que a soma dos n primeiros termos de uma PG é: $S_n = \frac{r^n a - a}{r-1}$.

Para $n = 1$ temos: $S_1 = \frac{r^1 a - a}{r-1} = \frac{ra-a}{r-1} = \frac{(r-1)a}{r-1} = a$. Logo a afirmação vale para $n = 1$.
Agora, vamos assumir que vale também para $n = k$ e vamos provar que vale para $k+1$, ou seja:

$$\begin{aligned} a + (ar) + (ar^2) + ... + (ar^{k-1}) + (ar^k) &= \frac{r^k a - a}{r-1} + r^k a \\ &= \frac{r^k a - a + (r-1)(r^k a)}{r-1} \\ &= \frac{r^k a - a + r^{k+1} a - r^k a}{r-1} \\ &= \frac{r^{k+1} a - a}{r-1}. \end{aligned}$$

Exemplo 8. Provar que $\frac{1}{1.2} + \frac{1}{2.3} + ... + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

Para $n = 1$ temos: $\frac{1}{1(1+1)} = \frac{1}{1.2} = \frac{1}{2}$. Logo, a afirmação vale para $n = 1$.
Agora vamos assumir que vale também para $n = k$ e, por fim, provar que vale para $k+1$, ou seja:

$$\begin{aligned} \frac{1}{1.2} + \frac{1}{2.3} + ... + \frac{1}{k(k+1)} + \frac{1}{(k+1)(k+2)} &= \frac{k}{k+1} + \frac{1}{(k+1)(k+2)} \\ &= \frac{k(k+1)(k+2) + (k+1)}{(k+1)^2(k+2)} \\ &= \frac{(k+1)[k(k+2)+1]}{(k+1)^2(k+2)} \\ &= \frac{k(k+2)+1}{(k+1)(k+2)} \\ &= \frac{k^2 + 2k + 1}{(k+1)(k+2)} \\ &= \frac{(k+1)^2}{(k+1)(k+2)} \\ &= \frac{k+1}{k+2} \\ &= \frac{k+1}{(k+1)+1}. \end{aligned}$$

Desta forma, a nossa afirmação confere com o que desejávamos.

Por fim, para encerrar este capítulo, iremos mostrar um resultado importante no âmbito da Matemática, e da ciência de uma forma geral, que demonstraremos através do Princípio da Indução, o *Teorema do Binômio de Newton*. Mas antes, precisamos ter em mente uma definição.

Definição 3. *O número de combinações de n elementos tomados k a k é dado por:*
$\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

Teorema 2 (Binômio de Newton)**.** *Sejam $a, b \in \mathbb{Z}$ e $n \in \mathbb{Z}^+$. Então temos que:*
$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{n-2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n$.

Demonstração. Pelo Princípio da Indução sobre n temos que:
1º) Para $n = 1$: $(a+b)^1 = \binom{1}{0}a + \binom{1}{1}b = a + b$. Logo, a afirmação é verdadeira para $n = 1$.
2º) Suponhamos que a afirmação seja verdadeira para um $n = k$, ou seja, $(a+b)^k = \binom{k}{0}a^k + \binom{k}{1}a^{k-1}b + \cdots + \binom{k}{k-1}ab^{k-1} + \binom{k}{k}b^k$.
3º) Neste terceiro passo, vamos mostrar que a afirmação vale para $k+1$. Logo,
$(a+b)^{k+1} = (a+b)(a+b)^k = a(a+b)^k + b(a+b)^k$, mas pela hipótese de indução temos que:
(I) $a(a+b)^k = \binom{k}{0}a^{k+1} + \binom{k}{1}a^kb + \cdots + \binom{k}{k-1}a^2b^{k-1} + \binom{k}{k}ab^k$, e
(II) $b(a+b)^k = \binom{k}{0}a^kb + \binom{k}{1}a^{k-1}b^2 + \cdots + \binom{k}{k-1}ab^k + \binom{k}{k}b^{k+1}$.
Então, somando (I) e (II) temos que:
(III) $(a+b)^{k+1} = \binom{k}{0}a^{k+1} + \left[\binom{k}{1} + \binom{k}{0}\right]a^kb + \cdots + \left[\binom{k}{k} + \binom{k}{k-1}\right]ab^k + \binom{k}{k}b^{k+1}$, mas note que $\binom{k}{1} + \binom{k}{0} = \binom{k+1}{1}$, e $\binom{k}{k} + \binom{k}{k-1} = \binom{k+1}{k}$ pois, pela definição anterior, temos que:

(i) $\binom{k}{1} + \binom{k}{0} = \frac{k!}{1!(k-1)!} + \frac{k!}{k!} = \frac{k.(k-1)!}{(k-1)!} + 1 = k + 1 = \binom{k+1}{1}\left(= \frac{(k+1)!}{k!} = \frac{(k+1)k!}{k!} = k+1\right)$, e

(ii) $\binom{k}{k} + \binom{k}{k-1} = \frac{k!}{k!} + \frac{k!}{(k-1)!} = 1 + \frac{k(k-1)!}{(k-1)!} = k + 1 = \binom{k+1}{k}\left(= \frac{(k+1)!}{k!} = \frac{(k+1)k!}{k!} = k+1\right)$.

Logo, substituindo os resultados de (i) e (ii) em (III), temos que:

$$(a+b)^{k+1} = \binom{k}{0}a^{k+1} + \binom{k+1}{1}a^kb + \cdots + \binom{k+1}{k}ab^k + \binom{k}{k}b^{k+1}$$

Mas é evidente que $\binom{k}{0} = \binom{k+1}{0}$ e $\binom{k}{k} = \binom{k+1}{k+1}$, portanto:

$$(a+b)^{k+1} = \binom{k+1}{0}a^{k+1} + \binom{k+1}{1}a^kb + \cdots + \binom{k+1}{k}ab^k + \binom{k+1}{k+1}b^{k+1}.$$

□

Feito isso, vejamos uma forma interessante em que podemos aplicar esse teorema.

Exemplo 9. Temos que $2^n = (1+1)^n$, logo, pelo teorema do binômio que acabamos de ver,

obtemos que:

$$\begin{aligned}(1+1)^n &= \sum_{i=0}^{n} \binom{n}{i} 1^{n-i}.1^i \\ &\overset{(*)}{=} \sum_{i=0}^{n} \binom{n}{i} \\ &= \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n-1} + \binom{n}{n}.\end{aligned}$$

Note vale a igualdade (*) só vale pois $1^{n-i} = 1$ e $1^i = 1$ também, independente de que sejam n e i.

Capítulo 2

A Divisibilidade e os Números Primos

Neste capítulo veremos importantes resultados dentro da Teoria dos Números como o Algoritmo da Divisão, Máximo Divisor Comum e Mínimo Múltiplo Comum, o Algoritmo de Euclides e o Teorema Fundamental da Aritmética. Resultados esses que provém do conceito de *divisibilidade,* que elucidaremos a seguir. Por fim, provaremos outro importante teorema que nos mostra que o conjunto dos números primos é infinito. Antes de mais nada, vamos conhecer um pouco mais sobre a história dos números primos.

Os números primos de uma forma geral, são conhecidos a mais de 2.300 anos e sua definição é extremamente simples de entender diga-se de passagem, porém, encontrar um número primo nunca foi tarefa fácil, diversos matemáticos se inclinaram a desenvolver métodos para encontrá-los e talvez o mais famoso deles creditado a Marin Mersenne, onde o mesmo afirma que $2^n - 1$ com $n \in \mathbb{N}$ resulta em um número primo. Esse método não é de todo perfeito, pois existem *números de Mersenne* que não são primos, como por exemplo $2^4 - 1 = 16 - 1 = 15$ (número composto), entretanto, o maior primo encontrado até hoje (junho de 2019) foi obtido através deste método, sendo ele igual a $2^{82.589.933} - 1$ com mais de 24 milhões de algarismos, encontrado em 7 de dezembro de 2018. Esse fato nos faz pensar em algo que nos intriga, o quão grande é o conjunto dos números primos?

Essa é uma pergunta fácil de responder e a dimensão dos números não é mais algo que nos inquieta graças a Euclides, que demonstra em uma das suas obras de *Os Elementos*, mais precisamente no Livro 9 (aprox. 300 anos a.C.), que "o conjunto dos números primos é infinito", em uma das demonstrações mais belas da Matemática e que abordaremos nesse capítulo. Desde então, muitos estudiosos e matemáticos dedicaram-se a estudar esse conjunto de número tão enigmático, e através disso nos mostraram diversas aplicações às quais o conceito de primalidade

se aplica, e umas das mais interessantes está relacionada com a Criptografia, porém, esta não é de nosso interesse, colocamos este fato aqui como curiosidade para que intrigue o leitor a buscar mais conhecimento sobre esses números.

2.1 O Algoritmo de Euclides

Definição 4. *Sejam a e b números inteiros com $b \neq 0$. Dizemos que "b divide a" se existe $c \in \mathbb{Z}$ tal que $a = bc$.*

Notação: Em $(b \setminus a)$ lê-se "b divide a".

Sendo assim, a primeira observação que fazemos é em relação a unicidade desse elemento c, pois se existisse outro $c^* \in \mathbb{Z}$ tal que $a = b.c^*$, teremos que $bc = bc^*$, e como $b \neq 0$, temos pela propriedade M3 (Cancelativa) que $c = c^*$.

Note também que se não exigimos que $b \neq 0$, teríamos que $0 \setminus a$ se, e somente se, $a = 0$, e nesse caso teremos que c não é único, pois a igualdade $0 = 0.c$ vale para qualquer valor de c, como provamos na (Proposição 1). Dito isso, daqui em diante vamos sempre assumir que os divisores são diferente de zero.

Por fim, devemos lembrar também que dizer que "b divide a" é equivalente a dizer que "b é um divisor de a", ou ainda que "a é um múltiplo de b".

Proposição 4. *Se $b \setminus a$ com $a \neq 0$, então $|b| \leq |a|$.*

Demonstração. Se $b \setminus a$ temos, por definição, que $a = bc$ para algum $c \in \mathbb{Z}$, então, aplicando o módulo temos $|a| = |b||c|$, mas como $1 \leq |c|$ pois $c \in \mathbb{Z}*$, multiplicando $|b|$ nessa desigualdade teremos que $|b| \leq |b||c| = |a|$. □

Corolário 3. *Sejam $a, b \in \mathbb{Z}^*$, então valem:*

i) Os únicos divisores de 1 são 1 e -1.

ii) Se $a \setminus b$ e $b \setminus a$, então $a = \pm b$.

Demonstração. i) Seja b um divisor de 1, então temos que $1 = bc$ para algum $c \in \mathbb{Z}$, mas, pela proposição anterior, temos que $|b| \leq |1| = 1$ e $|b| \geq 0$ (pois b é inteiro), logo $0 \leq |b| \leq 1$, e como não existem inteiros entre 0 e 1 (como vimos no capítulo anterior) e $b \neq 0$, temos que $|b| = 1$, ou seja, $b = 1$ ou $b = -1$.

ii) Se $a \setminus b$ temos que $b = ac$, com $c \in \mathbb{Z}$. Se $b \setminus a$ temos que $a = bc^*$, com $c^* \in \mathbb{Z}$. Logo, $\Rightarrow b = (bc^*)c$, por A5 temos,

$\Rightarrow b = b(c^*c)$, por M3 temos,

$\Rightarrow 1 = c^*c$, ou seja, por $i)$ temos $c^* = \pm 1$ e por consequência obtemos que $a = \pm b$. □

Proposição 5. *Sejam $a, b, c, d \in \mathbb{Z}$ quaisquer, temos que valem os seguintes itens:*

i) $a \setminus a$.

ii) Se $a \setminus b$ e $b \setminus c$, então $a \setminus c$.

iii) Se $a \setminus b$ e $c \setminus d$, então $ac \setminus bd$.

iv) Se $a \setminus b$ e $a \setminus c$, então $a \setminus (b + c)$.

v) Se $a \setminus b$, então para todo $m \in \mathbb{Z}$ temos que $a \setminus mb$.

vi) Se $a \setminus b$ e $a \setminus c$, então para todos $m, n \in \mathbb{Z}$ temos que $a \setminus (mb + nc)$.

Demonstração. (i) Temos por definição que se $a \setminus a$, então $a = ac$, para algum $c \in \mathbb{Z}$, mas como $a \neq 0$, temos por M3 que $c = 1$, ou seja, existe $c \in \mathbb{Z}$ tal que a afirmação seja verdade.

(ii) Da mesma forma, temos por definição que se $a \setminus b$ e $b \setminus c$, então $b = ae$ e $c = bf$, para algum $e, f \in \mathbb{Z}$, respectivamente. Logo, $c = (ae)f$, e por A5 temos que $c = (ae)f \Rightarrow c = a(ef)$, e como $ef \in \mathbb{Z}$, temos que $a \setminus c$.

(iii) Se $a \setminus b$, então $b = ak$, para algum $k \in \mathbb{Z}$. E, da mesma forma, se $c \setminus d$, então $d = ch$, para algum $h \in \mathbb{Z}$. Logo, $bd = (ak)(ch)$, e por M1 e M4 temos que $bd = ac(kh)$, e como $kh \in \mathbb{Z}$, podemos concluir que $ac \setminus bd$.

(iv) Se $a \setminus b$, então $b = ak$, $k \in \mathbb{Z}$. Assim como se $a \setminus c$, então $c = ak'$, para algum $k' \in \mathbb{Z}$. Logo, $(b + c) = (ak) + (ak')$, e por distributividade temos que $(b + c) = a(k + k')$, novamente como $(k + k') \in \mathbb{Z}$, concluímos que $a \setminus (b + c)$.

(v) Se $a \setminus b$, então $b = ak$, para algum $k \in \mathbb{Z}$. Logo, multiplicando ambas as partes por algum $m \in \mathbb{Z}$ temos que: $bm = (ak)m$

$\Rightarrow bm = a(km)$, por M1, e como $km \in \mathbb{Z}$, temos que $a \setminus bm$.

(vi) Se $a \setminus b$, então $b = ak$ com $k \in \mathbb{Z}$. Se $a \setminus c$, então $c = ah$ com $h \in \mathbb{Z}$. Mas, como vimos no item anterior, temos que nessas condições também valem que $bm = a(km)$ e $cn = a(hn)$, com $m, n \in \mathbb{Z}$. Logo, temos que $bm + cn = a(km) + a(hn)$, e por distributividade temos $bm + cn = a(km + hn)$, e como $(km + hn) \in \mathbb{Z}$ podemos concluir que $a \setminus (bm + cn)$. □

Lema 1. *Sejam $a, b \in \mathbb{Z}$ tais que $a \geq 0$ e $b > 0$. Então temos que existem $q, r \in \mathbb{Z}$ tais que $a = bq + r$, com $0 \leq r < b$.*

Demonstração. Seja $S = \{a - bx / x \in \mathbb{Z}, a - bx \geq 0\}$. Note que este conjunto S é não vazio, pois, para $x = 0$, temos $a \geq 0 \in S$. Então, pelo Princípio da Boa Ordem, temos que existe $r = minS$,

ou seja, $r = a - bq$ para algum $q \in \mathbb{Z}$, ou, em outras palavras, $a = bq + r$.

Agora, só nos resta provar que $r < b$. Então vamos supor por absurdo que $r \geq b$, nessas condições teríamos que: $a - bq \geq b \Rightarrow a - bq - b \geq 0 \Rightarrow a - b(q+1) \geq 0$, logo, $a - b(q+1)$ também pertenceria a S, mas $a - b(q+1) = a - bq - b = r - b \leq r = minS$, uma contradição. Logo, $r < b$. □

Este lema é na verdade uma parte importante da demonstração de um teorema conhecido como "Algoritmo da divisão", desenvolvido por Euclides, e que veremos a seguir, mas nessas condições já podemos dizer que se $r = 0$, então teríamos que $b \setminus a$ por definição.

Teorema 3 (Algoritmo da Divisão)**.** *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$. Então existem $q, r \in \mathbb{Z}$, únicos, tais que $a = bq + r$, com $0 \leq r < |b|$.*

Demonstração. Para provar esse teorema, vamos dividi-lo em 4 partes:

- Se $b > 0$ e $a \geq 0$: Este caso está contemplado no lema anterior e não iremos repeti-lo aqui.
- Se $b > 0$ e $a \leq 0$: Temos que se $a \leq 0$, então $|a| \geq 0$. Assim voltamos no caso anterior, logo, existem $q', r' \in \mathbb{Z}$ tais que: $|a| = bq' + r'$ com $0 \leq r' < b$. Então temos que:
  Se $r' = 0$, temos $|a| = bq$, em outras palavras, $-|a| = -bq \Rightarrow a = b(-q)$, que satisfaz o teorema. (Note que aqui usamos o fato de que se $a \leq 0$, então $-|a| = a$).
  Se $r' > 0$, temos $-|a| = a = b(-q') - r' \Rightarrow a = b(-q') + b - b - r' = b(-q' - 1) + (-r' + b)$.
  Mas como $-r' + b > 0$ pois $r' \geq 0$ e $b > 0$, temos que $-r' + b > 0 \Rightarrow -r' > -b \Rightarrow r' < b$.
  Logo, $q = -q' - 1$ e $r = -r' + b$ satisfazem o teorema.
- Se $b < 0$ e $a > 0$: Se $b < 0$, então $|b| = -b$, logo $a = |b|q' + r'$, com $0 \leq r' < |b| = -b$, isso implica que $a = (-b)q' + r' = b(-q') + r'$, que satisfaz o teorema.
- Se $b < 0$ e $a < 0$: Nessas condições, temos que $|a| > 0$ e $|b| > 0$, ou seja, $-a > 0$ e $-b > 0$. Logo, $|a| = |b|q' + r' \Rightarrow -a = -bq' + r'$, com $0 \leq r < |b| = -b$, que, pelo lema anterior, satisfaz o teorema.

Agora que analisamos todas as possibilidades, só nos resta mostrar que essa solução é única. Então sejam $q, q', r, r' \in \mathbb{Z}$ tais que $qb + r = q'b + r' \Rightarrow qb - q'b = r' - r \Rightarrow (q - q')b = r' - r$, mas como $r' < |b| \Rightarrow r' - r < |b|$, logo $(q - q')b < |b|$, e aplicando o módulo nessa desigualdade obtemos que $0 \leq |q - q'||b| < |b|$, utilizando a propriedade cancelativa temos que $0 \leq |q - q'| < 1$, ou seja, $|q - q'| = 0$, pois não existem inteiros entre 0 e 1, logo $q = q'$. E, por fim, substituindo

esse resultado na seguinte igualdade, obtemos: $(q-q')b = r'-r \Rightarrow 0.b = r'-r \Rightarrow 0 = r'-r \Rightarrow r' = r$. $\square$

Observação: Note que aqui utilizamos o fato de que $|ab| = |a||b|$*, para todos* $a, b \in \mathbb{Z}$.

Ainda sobre esse teorema, definimos que os inteiros q e r são chamados de quociente e resto da divisão de a por b, respectivamente. E, com esse raciocínio, podemos provar coisas interessantes dentro da teoria dos números. Vejamos o seguinte número, por exemplo: $x = 5123$. Podemos reescrever x da seguinte forma: $x = 5.10^3 + 1.10^2 + 2.10 = 7$, pois $x = 5000 + 100 + 20 + 3$. Isso se deve porque a nossa base numérica se escreve em função de 10 algarismos $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Mas, com o teorema que veremos a seguir, poderíamos escrever os números em bases numéricas diferentes utilizando apenas a teoria desenvolvida nas páginas precedentes à essa. (ver o exemplo 10).

Notação: Em $(5123)_{10}$*, lê-se "5123 na base 10".*

Teorema 4. *Seja* $b \geq 2$ *um número inteiro. Todo* $a \in \mathbb{Z}^+$ *pode ser escrito de modo único na forma* $a = r_n b^n + r_{n-1} b^{n-1} + ... + r_1 b + r_0$ *com* $n \geq 0$, $r_n \neq 0$ *e, para cada índice* i *com* $0 \leq i \leq n$, *tem-se que* $0 \leq r_i < b$.

Demonstração. Primeiramente vamos mostrar que a, de fato, pode ser escrito dessa forma (I). Feito isso, mostraremos que essa forma é única (II).

(I). Para tanto, vamos efetuar a divisão de a por b e obtemos, pelo teorema anterior, que existem $q_0, r_0 \in \mathbb{Z}$ tais que:
$a = bq_0 + r_0$, com $0 \leq r_0 < b$; agora dividindo q_0 por b temos:
$q_0 = bq_1 + r_1$, com $0 \leq r_1 < b$; agora dividindo q_1 por b temos:
$q_1 = bq_2 + r_2$, com $0 \leq r_2 < b$; e note que repetindo esse processo, em um certo momento, o quociente se anulará. Vamos supor que o primeiro quociente que se anule seja o n-ésimo, logo,

$$\begin{aligned}
(i)\ a &= bq_0 + r_0,\ 0 \leq r_0 < b,\\
(ii)\ q_0 &= bq_1 + r_1,\ 0 \leq r_1 < b,\\
(iii)\ q_1 &= bq_2 + r_2,\ 0 \leq r_2 < b,\\
&\vdots\\
(i_{n-1})\ q_{n-2} &= bq_{n-1} + r_{n-1},\ 0 \leq r_{n-1} < b,\\
(i_n)\ q_{n-1} &= bq_n + r_n = b.0 + r_n,\ 0 < r_n < b.
\end{aligned}$$

Agora, substituindo (i_n) em (i_{n-1}) sucessivamente, obtemos:

Substituindo (ii) em (i),

$a = b(bq_1 + r_1) + r_0 \Rightarrow a = b^2q_1 + br_1 + r_0$

Substituindo (iii) nessa nova expressão temos,

$a = b^2(bq_2 + r_2) + br_1 + r_0 \Rightarrow a = b^3q_2 + b^2r_2 + br_1 + r_0$

Continuando esse processo teremos,

$a = b^{n-1}(bq_{n-1} + r_{n-1}) + b^{n-2}r_{n-2} + \cdots + b^2r_2 + br_1 + r_0 = b^nq_{n-1} + b^{n-1}r_{n-1} + b^{n-2}r_{n-2} + \cdots + b^2r_2 + br_1 + r_0$, mas em (i_n) temos que $q_{n-1} = r_n$, logo,

$\Rightarrow a = r_nb^n + r_{n-1}b^{n-1} + ... + r_1b + r_0$.

Portanto, é possível escrever a na forma que enunciamos. Agora, vamos mostrar que essa forma é única.

(II). Vamos supor então que $a = r_nb^n + r_{n-1}b^{n-1} + ... + r_1b + r_0 = r'_mb^m + r'_{m-1}b^{m-1} + ... + r'_1b + r'_0$, logo, colocando b em evidência, temos:

$\Rightarrow b(r_nb^{n-1} + r_{n-1}b^{n-2} + ... + r_1) + r_0 = b(r'_mb^{m-1} + r'_{m-1}b^{m-2} + ... + r'_1) + r'_0$, e por cancelamento temos que:

$\Rightarrow r_nb^{n-1} + r_{n-1}b^{n-2} + ... + r_1 + r_0 = r'_mb^{m-1} + r'_{m-1}b^{m-2} + ... + r'_1 + r'_0$, e como $0 \leq r_o, r'_0 < b$ (e da unicidade do quociente que provamos no teorema anterior) temos que $r_o = r'_0$, logo, colocando b em evidência novamente e repetindo esse processo teremos:

$\Rightarrow a = r_nb^{n-2} + r_{n-1}b^{n-3} + ... + r_2 + r_1 + r_0 = r'_mb^{m-2} + r'_{m-1}b^{m-3} + ... + r'_2 + r'_1 + r'_0$, da mesma forma, aqui teremos que $r_1 = r'_1$ e $r_2 = r'_2$. Novamente repetindo o processo de colocar b em evidência até b^{n-n} e b^{m-m}, teremos que:

$$r_o = r'_0,\ r_1 = r'_1,\ r_2 = r'_2,\ \ldots,\ r_n = r'_m.$$

Portanto, essa forma de escrever a é única. □

Para encerrar essa seção, vejamos alguns exemplos de como podemos utilizar esse teorema, de formas diferentes.

Exemplo 10. Aqui voltamos a questão que discutimos em relação ao Algoritmo de Euclides, vamos escrever 218 em uma base numérica diferentes da usual, na base 2.

Para mostrarmos isso basta seguir os mesmo passos do teorema anterior, ou seja, efetuar a

divisão euclidiana repetidamente entre o quociente e o divisor 2, logo,

$$\begin{aligned} 218 &= 2.109 + 0 \\ 109 &= 2.54 + 1 \\ 54 &= 2.27 + 0 \\ 27 &= 2.13 + 1 \\ 13 &= 2.6 + 1 \\ 6 &= 2.3 + 0 \\ 3 &= 2.1 + 1 \\ 1 &= 2.0 + 1. \end{aligned}$$

Portanto, $218 = (11011010)_2$.

Note que para verificarmos que $218 = (11011010)_2$ de fato, basta ver que:
$(2^7).1 + (2^6).1 + (2^5).0 + (2^4).1 + (2^3)1 + (2^2).0 + (2^1).1 + (2^0).0 = 128 + 64 + 16 + 8 + 2 = 218$.

Exemplo 11 (Critérios de Divisibilidade)**.** Seja $b \in \mathbb{Z}^+$ tal que $b = r_n 10^n + r_{n-1}10^{n-1} + r_{n-2}b^{n-2} \cdots + r_2 10^2 + r_1 10 + r_0$ (b se escreve dessa forma na base 10). Vamos mostrar que:
a) $2 \setminus b$ se, e somente se, $2 \setminus r_0$.
b) $3 \setminus b$ se, e somente se, $3 \setminus (r_0 + r_1 + \ldots r_n)$.

(a) Temos que se $2 \setminus b \Leftrightarrow 2 \setminus r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$, logo,

$$\begin{aligned} 2 \setminus b &\Leftrightarrow 2 \setminus r_n(2.5)^n + r_{n-1}(2.5)^{n-1} + \cdots + r_1(2.5) + r_0 \\ &\Leftrightarrow 2 \setminus r_n 2^n 5^n + r_{n-1}2^{n-1}5^{n-1} + \cdots + r_1 2.5 + r_0 \\ (*) &\Leftrightarrow 2 \setminus r_0. \end{aligned}$$

Note que só podemos concluir a implicação (*) pois, como 2 divide todo o produto $r_n 2^n 5^n + r_{n-1}2^{n-1}5^{n-1} + \cdots + r_1 2.5$, devemos concluir que 2 divide também r_0.

(b) Temos que se $3 \setminus b \Leftrightarrow 3 \setminus r_n 10^n + r_{n-1}10^{n-1} + \cdots + r_1 10 + r_0$, logo,

$3 \setminus b \Leftrightarrow 3 \setminus r_n(9+1)^n + r_{n-1}(9+1)^{n-1} + \cdots + r_1(9+1) + r_0$, mas, note que, pelo binômio de newton que provamos ainda no primeiro capítulo, vem que:
(i) $(9+1)^n = 9^n + \binom{n}{1}9^{n-1} + \cdots + \binom{n}{n-1}9 + 1$, logo,
$r_n(9+1)^n = r_n(3^2)^n + r_n\binom{n}{1}(3^2)^{n-1} + \cdots + r_n\binom{n}{n-1}(3^2) + r_n$, e isso nos mostra que, para que 3

divida a primeira parte da expressão de b, 3 deve dividir r_n.
(ii) $(9+1)^{n-1} = 9^{n-1} + \binom{n-1}{1}9^{n-2} + \cdots + \binom{n-1}{n-2}9 + 1$, logo,
$r_{n-1}(9+1)^{n-1} = r_{n-1}(3^2)^{n-1} + r_{n-1}\binom{n-1}{1}(3^2)^{n-2} + \cdots + r_{n-1}\binom{n-1}{n-2}(3^2) + r_{n-1}$, e da mesma forma vem que, para que 3 divida essa segunda parte da expressão de b, 3 deve dividir r_{n-1}.

$\vdots$

(i_{n-1}) $10 = 9+1$, logo, $r_1 10 = r_1(9+1) = r_1(3^2) + r_1$, ou seja, para que 3 divida essa penúltima parte da expressão de b, 3 deve dividir r_1.
(i_n) $3 \setminus r_0$.

Portanto, isso mostra que $3 \setminus b$ se, e somente se, $3 \setminus r_n + r_{n-1} + \cdots + r_1 + r_0$.

Agora, note que com a demonstração dos itens a) e b) provamos também que $5 \setminus b$ se, e somente se, $5 \setminus r_0$, e provamos ainda que $9 \setminus b$ se, e somente se, $9 \setminus r_n + r_{n-1} + \cdots + r_1 + r_0$, respectivamente.

2.2 Ideais, Máximo Divisor Comum e Mínimo Múltiplo Comum

O conceito de *ideal* que veremos inicialmente aqui é importante na Matemática pois permitiu simplificar certas questões da Teoria dos Números que, durante muito tempo, foram questionadas e estudadas.

Definição 5 (Ideal)**.** *Seja J um conjunto não vazio de números inteiros. Dizemos que J é um ideal de $\mathbb{Z}$ se:*
i) Dados $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J$,
ii) Dado $\alpha \in J$ e $a \in \mathbb{Z} \Rightarrow \alpha a \in J$.

Definição 6. *Dado um $m \in \mathbb{Z}$ qualquer, temos que $m\mathbb{Z}$ é o conjunto de todos os múltiplos de m.*
Notação: $m\mathbb{Z} = \{mx | x \in \mathbb{Z}\}$.

Teorema 5. *Se J é um ideal de $\mathbb{Z}$, então temos que $J = \{0\}$ ou existe $m \in \mathbb{Z}$ tal que $J = m\mathbb{Z}$.*

Demonstração. Temos que se J é um ideal de $\mathbb{Z}$, então, por definição de ideal, temos que:
i) $\alpha, \beta \in J \Rightarrow \alpha + \beta \in J$,
ii) $\alpha \in J$, $a \in \mathbb{Z} \Rightarrow \alpha a \in \mathbb{Z}$.

Com isso, temos que se $J = \{0\}$ é trivial.

Agora, para concluirmos que $J = m\mathbb{Z}$, basta mostrarmos que $m\mathbb{Z} \subset J$ e $J \subset m\mathbb{Z}$.

Mas, se $J \neq \{0\}$, temos que deve existir um $m \in J$. Nesse caso, $\pm m, \pm 2m, \pm 3m, \ldots, \pm zm \in J$, pois $\pm 2m = \pm(m+m) \in J, \pm 3m = \pm(m+2m) \in J, \ldots, \pm zm = \pm(m+(z-1)m)$, ou seja, $m\mathbb{Z} \subset J$.

Por outro lado, seja $m = minJ^+$ e $a \in J$, efetuando a divisão de a por m, temos que existem $q, r \in \mathbb{Z}$ tais que: $a = mq + r$, com $0 \leq r < m$.
$\Rightarrow a - mq = r$, mas como $a, mq \in J$, temos que $r \in J^+$; mas $r < m = minJ^+$. Absurdo! Logo, $r = 0$ e $J \subset m\mathbb{Z}$.

Portanto, $J = m\mathbb{Z}$.

□

Agora, voltando a discutir o conceito divisibilidade que definimos anteriormente, podemos perceber que um número inteiro a qualquer possui vários divisores b, e isso nos permite definir um conjunto D dos "divisores de a". Além disso, se tomarmos dois inteiros x e y diferentes, se eles não forem primos entre si, eles possuem divisores em comum, dito isso, conseguimos definir um máximo divisor comum d entre x e y. Vejamos:

Definição 7 (Máximo Divisor Comum)**.** *Chama-se o máximo divisor comum (MDC) de a e b o maior de seus divisores comuns, ou seja, $mdc(a,b) = maxD(a,b)$.*

Note que esta definição não nos diz ao certo "quem" é o máximo divisor comum de a e b, mas, para isso, basta observarmos a próxima definição.

Definição 8. *Sejam $a, b \in \mathbb{Z}$. Dizemos que $d \in \mathbb{Z}$ é o máximo divisor comum de a e b se, e somente se, d verifica:*
i) $d \setminus a$ e $d \setminus b$.
ii) Se $d' \setminus a$ e $d' \setminus b$, então $d' \setminus d$.
Notação: $d = mdc(a,b)$.

Com essa definição de Máximo Divisor Comum, fica mais fácil identificarmos quem é, de fato, o MDC entre dois números inteiros a e b. E, da mesma forma, facilita a interpretação e a demonstração de outros resultados, como veremos a seguir.

Teorema 6 (Teorema de Bézout)**.** *Sejam $a, b \in \mathbb{Z}$ e $d = mdc(a,b)$. Então, existem $r, s \in \mathbb{Z}$ tais que $d = ra + sb$.*

Demonstração. Vamos considerar o conjunto $J = \{xa+yb|\ x, y \in \mathbb{Z}\}$. Mostraremos que $J = d\mathbb{Z}$, e para isso, veremos que J é um ideal de $\mathbb{Z}$ utilizando o teorema anterior para concluir isso.

Então, sejam $g, h \in J$. Logo, como $g, h \in J$, temos que $g = x_1a + y_1b$ e $h = x_2a + y_2b$. Dessa forma, temos que $g + h = (x_1 + x_2)a + (y_2 + y_2)b \in J$.

Com o mesmo raciocínio, temos que se $\alpha \in \mathbb{Z}$, então $\alpha g \in J$, pois $\alpha g = \alpha x_1 a + \alpha y_1 b$
$\Rightarrow \alpha g = (\alpha x_1)a + (\alpha y_1)b \in J$. Logo, J é um ideal de $\mathbb{Z}$. E, pelo teorema anterior, temos que existe $n \in \mathbb{Z}$ tal que $J = n\mathbb{Z}$.

Agora, vamos mostrar que $n = d\ \big(= mdc(a, b)\big)$. Temos que $n \in J$, então $n = ar + bs$. E como $a = 1.a + 0.b$ e $b = 0.a + 1.b$, temos também que $a, b \in J$, logo $n \setminus a$ e $n \setminus b$ (pois $J = n\mathbb{Z}$), ou seja, $n \in D(a, b)$. Seja então $d' \in D(a.b)$, logo $d' \setminus a$ e $d' \setminus b$, então $d' \setminus (ar + bs)$ como vimos no capítulo anterior, logo $d' \setminus n$. Portanto, $|d'| \leq |n| = n$. Com isso, vemos que $n = d$. □

Proposição 6. *Sejam $a, b, c, d \in \mathbb{Z}$, com $d = mdc(a, b)$ e $c \neq 0$. Então temos que:*
i) $mdc(ac, bc) = d|c|$.
ii) Se $c \setminus a$ e $c \setminus b$, então $mdc(a/c, b/c) = d/|c|$.

Demonstração. (i) Temos que se $d = mdc(a, b)$, então, por definição, $d \setminus a$ e $d \setminus b$, ou seja, existem $q, r \in \mathbb{Z}$ tais que $a = dq$ e $b = dr$, respectivamente. Logo, multiplicando por c temos,
$ac = (dq)c \Rightarrow ac = (dc)q$, e $bc = (dr)c \Rightarrow bc = (dc)r$. Portanto $dc \in D(ac, bc)$. Para concluirmos o que se pede em $i)$, só nos resta mostrar que dc é o maior dos divisores de a e b. Mas, do Teorema de Bézout, temos que existem $s, t \in \mathbb{Z}$ tais que:
$d = as + bt \Rightarrow d|c| = (as)|c| + (bt)|c|$, logo $d|c| = (a|c|)s + (b|c|)t$. E, dessa forma, se algum $d' \in \mathbb{Z}$ divide ac e bc, assim como no teorema de Bézout, teremos que $d' \setminus d|c|$. Portanto, $mdc(ac.bc) = d|c|$.
(ii) Do item anterior temos que $d|c| = mdc(ac, bc)$, e, pela hipótese, temos que $d = mdc(a, b)$. Logo, $d = mdc\big(\frac{ac}{c}, \frac{bc}{c}\big) = mdc\big(\frac{a}{c}, \frac{b}{c}\big).|c|$, chamando $mdc\big(\frac{a}{c}, \frac{b}{c}\big) = D$, temos que:
$d = |c|.D \Rightarrow D = d/|c|$. □

Teorema 7 (Teorema de Euclides)**.** *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \setminus bc$. Se a e b são relativamente primos, ou seja, se $mdc(a, b) = 1$, então $a \setminus c$.*

Demonstração. Se $a \setminus bc$, então $bc = ak$, para algum $k \in \mathbb{Z}$. Mas, se $mdc(a, b) = 1$, então, pela proposição anterior, vemos que $mdc(ac, bc) = |c|$. Mas $bc = ak$, logo $mdc(ac, bc) = mdc(ac, ak) = |c|$, ou seja, $mdc(c, k)|a| = |c|$. Vamos chamar $mdc(c, k) = p \in \mathbb{Z}$, logo, temos que:
$p.|a| = |c|$. Então, por definição, obtemos que $a \setminus c$. □

Com esse conceito de números *relativamente primos* que vimos no teorema anterior, podemos provar outro resultado interessante, e que certamente será útil para nós nessas páginas a seguir, mesmo que implicitamente.

Proposição 7. *Sejam $a, b \in \mathbb{Z}$ relativamente primos, e seja também um inteiro c tal que $a \setminus c$ e $b \setminus c$. Então, $ab \setminus c$.*

Demonstração. Se $a \setminus c$, então $c = al$, $l \in \mathbb{Z} - (I)$, e se $b \setminus c$, então $c = bk$, $k \in \mathbb{Z} - (II)$. Ou seja, $al = bk$, mas a e b são relativamente primos, logo $a \setminus k \Rightarrow k = ap$, $p \in \mathbb{Z}$. Logo, voltando em (II), temos: $c = b(ap) \Rightarrow c = (ab)p$.

Portanto, $ab \setminus c$. □

Visto que a tarefa de encontrar o Máximo Divisor Comum entre dois números pode ser demasiadamente complicada com a teoria que vimos até aqui, vejamos um resultado importante, decorrente do Algoritmo de Euclides, e que nos ajudará a encontrar com mais facilidade esse número.

Lema 2. *Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, e sejam q, r o quociente e o resto da divisão de a por b, respectivamente. Então, $D(a, b) = D(b, r)$; e teremos também que $mdc(a, b) = mdc(b, r)$.*

Demonstração. Nessas condições, temos que $a = bq + r$, com $1 \leq r < b$. Então, seja $\alpha \in D(a, b)$, logo $\alpha \setminus a$ e $\alpha \setminus b$, assim, $\alpha \setminus a - bq$, ou seja, $\alpha \setminus r$. Então, $D(a, b) \subseteq D(b, r)$. Mas como $r = a - bq$, temos analogamente que $D(b, r) \subseteq D(a, b)$.

Portanto, $D(a, b) = D(b, r)$. E $mdc(a, b) = mdc(b, r)$. □

Vejamos então como podemos aplicar isso na prática.

Exemplo 12. Usando o Algoritmo de Euclides para obter r e s tais que:
i) $mdc(56, 72) = 56r + 72s$.
ii) $mdc(24, 138) = 24r + 138s$.
iii) $mdc(119, 272) = 119r + 272s$.

Resolvendo *i)*: Sabemos que o $mdc(72, 56) = 8$, pois, fazendo a divisão euclidiana de 72 por 56, obtemos que $72 = 56.1 + 16$ (I). Agora, dividindo 56 por 16 temos que $56 = 16.3 + 8$ (II). E, da mesma forma, temos que $16 = 8.2 + 0$. Ou seja, pelo lema que acabamos de ver, temos que $mdc(72, 56) = mdc(56, 16) = mdc(16, 8) = 8$.

Temos também, pelo Teorema de Bézout, que existem esses $r, s \in \mathbb{Z}$. tais que $8 = 56r + 72s$. Temos em (II) que $8 = 56 + 16.(-3)$, e em (I) que $16 = 72 - 56$, logo, substituindo (I) em (II) temos:

$$\begin{aligned} 8 &= 56 + (72 - 56)(-3) \\ \Rightarrow 8 &= 56 + 72(-3) + 56.3 \\ \Rightarrow 8 &= 56.4 + 72(-3). \end{aligned}$$

Portanto, para $r = 4$ e $s = -3$ temos que vale a igualdade.

Resolvendo *ii*): Da mesma forma do exercício anterior temos que $mdc(138, 24) = 6$, pois, $138 = 24.5 + 18$ (I), e, fazendo a divisão de 24 po 18 obtemos que $24 = 18.1 + 6$ (II), assim como $18 = 6.3 + 0$. Logo, $mdc(138, 24) = \cdots = mdc(18, 6) = 6$. Agora, pelo Teorema de Bézout, sabemos que $6 = 24r + 138s$. Vamos encontrar quem são r e s.

Temos em (II) que $6 = 24 - 18$, e em (I) temos que $18 = 138 + 24(-5)$, logo, substituindo (I) em (II) temos:

$$\begin{aligned} 6 &= 24 - (138 + 24(-5)) \\ \Rightarrow 6 &= 24 + 138(-1) + 24.5 \\ \Rightarrow 6 &= 24.6 + 138(-1). \end{aligned}$$

Portanto, para $r = 6$ e $s = -1$ temos que vale a igualdade.

Resolvendo *iii*): Analogamente descobrimos que $mdc(272, 119) = 17$, visto que $272 = 119.2 + 34$ (I), assim como, $119 = 34.3 + 17$ (II) e $34 = 17.2 + 0$. Logo, $mdc(272, 119) = mdc(34, 17) = 17$. Por fim, temos pelo Teorema de Bézout que, $17 = 119r + 272s$.

Temos em (II) que $17 = 119 + 34(-3)$ e em (I) vem que $34 = 272 + 119(-2)$, logo, substituindo (I) em (II) temos,

$$\begin{aligned} 17 &= 119 + (272 + 119(-2))(-3) \\ \Rightarrow 17 &= 119 + 272(-3) + 119.6 \\ \Rightarrow 17 &= 119.7 + 272(-3). \end{aligned}$$

Portanto, para $r = 7$ e $s = -3$ temos que vale a igualdade.

Agora, discutiremos algumas coisas em relação ao Mínimo Múltiplo Comum (MMC) entre dois números. Mas, antes disso, precisamos ter em mente o que significa dizer que um número é "múltiplo" um do outro.

Definição 9. *Sejam $a, b, c \in \mathbb{Z}$. Dizemos que c é "múltiplo" de a e de b se, e somente se, $a \setminus c$ e $b \setminus c$.*

Definição 10 (Mínimo Múltiplo Comum)**.** *Um número $m \in \mathbb{Z}$ é dito "mínimo múltiplo comum entre a e b" se ele for o menor dos múltiplos de a e b, ou seja, se $m = minM^+(a, b)$. Onde $M^+(a, b)$ é o conjunto dos múltiplos positivos de a e b.*

Notação: $m = mmc(a, b)$.

Aqui novamente percebemos que essa definição não nos mostram "quem" é esse mínimo múltiplo comum entre a e b. Para tal, vejamos o seguinte teorema.

Teorema 8. *Sejam $a, b \in \mathbb{Z}$ e $m \in \mathbb{Z}^+$. Então, $m = mmc(a, b)$ se, e somente se, m verifica que:*
i) $a \setminus m$, $b \setminus m$,
ii) Se $a \setminus m'$ e $b \setminus m'$, então $m \setminus m'$.

Demonstração. ($\Rightarrow$) Para mostrarmos que se $m = mmc(a, b)$, então m verifica $i)$ e $ii)$, basta mostrarmos que $M(a, b)$ é um ideal de $\mathbb{Z}$. Mas note que se $\alpha, \beta \in M(a, b)$, então $a \setminus \alpha$ e $a \setminus \beta$, logo $a \setminus \alpha + \beta$ (análogo para b). E, com um raciocínio semelhante a esse, concluímos que $a \setminus \alpha c$, para $c \in \mathbb{Z}$ (o mesmo vale para b). Portanto, $M(a, b)$ é um ideal de $\mathbb{Z}$. Com isso, podemos concluir pelo Princípio da Boa Ordem, pela própria definição de MMC e pelo teorema 5 desse capítulo, que $M(a, b) = m\mathbb{Z}$. Logo, se $m' \in M(a, b) \Rightarrow m' \in m\mathbb{Z}$. Mas $m = mmc(a, b)$, então $m \setminus m'$.

($\Leftarrow$) Para verificarmos que vale também a volta é mais simples, pois se m verifica $i)$, então $m \in M^+(a, b)$. E, se m verifica $ii)$ teremos que $m = minM^+(a, b)$.
Portanto, $m = mmc(a, b)$. □

Teorema 9. *Sejam $a, b, d, m \in \mathbb{Z}$ onde $d = mdc(a, b)$ e $m = mmc(a, b)$. Então, $md = |ab|$.*

Demonstração. Segue que se $d = mdc(a, b)$, então $a = dk$ e $b = dl$, com $k, l \in \mathbb{Z}$. E, da mesma forma, se $m = mmc(a, b)$, então $m = ax$ e $m = by$, com $x, y \in \mathbb{Z}$.

Queremos mostrar que $md = ab$, ou que $m = \frac{ab}{d}$. E, para isso, basta verificarmos que se $\alpha = \frac{ab}{d}$, então $\alpha = m$. Ou seja, α verifica as condições do teorema anterior.

Vimos que $a = dk$ e $b = dl$, para algum $k, l \in \mathbb{Z}$. Logo, $\alpha = \frac{ab}{d} = \frac{(dk)b}{d} = bk$ e, analogamente, $\alpha = al$. Portanto, $a \setminus \alpha$ e $b \setminus \alpha$.

Agora, vejamos que se $a \setminus \alpha'$ e $b \setminus \alpha'$, então $\alpha \setminus \alpha'$.

Se $a \setminus \alpha'$ e $b \setminus \alpha'$, então $\alpha' = ap$ e $\alpha' = bq$, com $p, q \in \mathbb{Z}$. Logo, $\alpha' = (dk)p$, e como $b \setminus \alpha'$ temos que $dl \setminus dkp$, ou seja, $l \setminus kp$. Mas, como $mdc(k, l) = 1$, temos que $l \setminus p$. Logo, $p = lz$, com $z \in \mathbb{Z}$. Assim, temos que $\alpha' = (dk)lz = alz$, mas $l = \frac{a}{d}$, portanto, $\alpha' = \frac{abz}{d} \Rightarrow \alpha' = \alpha z$, com $z \in \mathbb{Z}$. Portanto, $\alpha \setminus \alpha'$ e concluímos que $\alpha = m$. □

2.3 Teorema Fundamental da Aritmética e a infinitude dos primos

O Teorema Fundamental da Aritmética diz que "todo número inteiro pode ser decomposto em produto de números primos, e essa decomposição é única". Mas, antes de prová-lo, vejamos algumas propriedades e relações dos números primos que nos ajudarão nessa tarefa. Sendo assim, iremos assumir que um número inteiro positivo p é dito **primo** se seus únicos divisores são 1 e o próprio p.

Proposição 8. *Sejam $a, b \in \mathbb{Z}$ e p um número primo:*
i) Se $p \nmid a$, então $mdc(p, a) = 1$.
ii) Se $p \setminus ab$, então $p \setminus a$ ou $p \setminus b$.

Demonstração. i) Se $p \nmid a$, então não existe $h \in \mathbb{Z}$ tal que $a = ph$, mas, todo número inteiro tem 1 como divisor, logo $mdc(p, a) = 1$.
ii) Se $p \setminus ab$, então $ab = pk$, com $k \in \mathbb{Z}$. Se $p \setminus a$, não precisamos fazer nada, mas, se $p \nmid a$, então pelo item *i)* temos que $mdc(a, p) = 1$, logo, pelo teorema 7, temos que $p \setminus b$. □

Corolário 4. *Se p primo divide um produto $a_1a_2a_3 \dots a_n$, então $p \setminus a_k$ apara algum k, $1 \leq k \leq n$.*

Demonstração. Temos por definição que se $p \setminus a_1a_2a_3 \dots a_n$, então $a_1a_2a_3 \dots a_n = pl$, $l \in \mathbb{Z}$. Utilizando a proposição anterior temos que:

Se $p \setminus a_1$, então o corolário está provado. Se $p \nmid a_1$, então $p \setminus a_2a_3 \dots a_n$. Nesse caso, novamente temos que se $p \setminus a_2$, então está provado, mas, se $p \nmid a_2$, então $p \setminus a_3a_4 \dots a_n$. Esse raciocínio sucede por todo o produto $a_1a_2a_3 \dots a_n$, e com isso podemos concluir que vale o corolário. □

Teorema 10. *Seja p um inteiro tal que $p \neq -1, 0, 1$. Então, podemos dizer que p é primo se, e somente se, toda vez que p divide um produto de dois números, p divide pelo menos um dos fatores.*

Demonstração. ($\Rightarrow$) Essa implicação está provada no item *ii)* da proposição anterior e, para que não fique repetitivo esse texto, não iremos repeti-la.
($\Leftarrow$) Nesse caso, temos que $p \setminus ab$, com $a, b \in \mathbb{Z}$, onde $p \setminus a$ ou $p \setminus b$, mas com p não primo. Sendo assim, $|p|$ pode ser escrito como $|p| = ab$ com $1 < a < |p|$ e $1 < b < |p|$ (a e b divisores próprios). Nesse caso, se $p \setminus a$ teríamos que $a = p.k \Rightarrow |a| = |p||k| \Rightarrow \frac{|a|}{|k|} = |p|$, ou seja, de $1 < a < |p|$ teríamos que $|a| < |p| = \frac{|a|}{|k|} \Rightarrow |a| < \frac{|a|}{|k|} \Rightarrow |k| < 1$, uma contradição. E o mesmo acontece com $1 < b < |p|$. Logo, $p \setminus ab$ mas $p \not\setminus a$ e $p \not\setminus b$. Absurdo!

Portanto, p é primo.

□

Teorema 11. *Todo $a \in \mathbb{Z}$ tal que $a > 1$ pode ser escrito como produto de números primos, ou seja, existem $p_1 \leq p_2 \leq p_3 \cdots \leq p_n$ tais que $a = p_1 p_2 p_3 \dots p_n$, e essa decomposição é única.*

Demonstração. Primeiramente iremos provar que existe essa decomposição, fazendo indução sobre n. Feito isso, mostraremos que ela é única.

(i) Existência:

1º) Para $a = 2$ temos que o teorema é verdadeiro, visto que 2 já é um número primo.

2º) Vamos supor que o teorema é verdadeiro para todo inteiro b, tal que $1 < b < a$. Dito isso, vamos mostrar que, nessas condições, o teorema também vale para a.(Princípio de Indução Completa-2ª versão)

3º) Como $1 < b < a$, temos que a pode ser escrito como $a = bc$, onde $1 < c < a$, ou seja, b e c são divisores próprios de a com $b, c \in \mathbb{Z}$. Logo, pela própria hipótese de indução, temos que $b = p_1 p_2 \dots p_k$ e $c = q_1 q_2 \dots q_l$.

Portanto, $a = p_1 p_2 \dots p_k q_1 q_2 \dots q_l$. E isso prova a existência.

(ii) Agora, vamos mostrar que essa decomposição é única. Então, seja $a = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$, vamos mostrar que $r = s$.

Por indução sobre r temos que:

1º) Para $r = 1$, temos que $p_1 = q_1 q_2 \dots q_s$, mas, como p_1 é primo, teremos que $s = 1$, logo $p_1 = q_1$, e vemos que vale para $r = 1$.

2º) Vamos supor então que $r > 1$, e que para $r - 1$ o teorema é verdadeiro.

3^o) De $a = p_1p_2 \dots p_r = q_1q_2 \dots q_s$ temos que p_1 é um divisor de $q_1q_2 \dots q_s$, logo $p_1 \setminus q_j$ para algum $1 \leq j \leq s$, como vimos no corolário anterior. Podemos supor então que $p_1 \setminus q_1$, logo $p_1 = \pm q_1$, pois p_1 e q_1 são primos. Consideremos então o número inteiro $a' = a/p_1$; temos $a' \neq 0$, $a' \neq \pm 1$ e $a' = p_2p_3 \dots p_r = (\pm q_2)q_3 \dots q_s$, então como $a' < a$, pela hipótese de indução, temos que $r - 1 = s - 1$, logo, $r = s$. E, usando uma notação conveniente poderíamos dizer que $p_2 = \pm q_2$, $p_3 = \pm q_3, \dots$, $p_r = \pm q_s$.

Portanto, essa decomposição é única e vale que $a = p_1p_2p_3 \dots p_n$. □

Feito tudo isso, podemos finalmente demonstrar um dos resultados mais importantes desse capítulo, ao qual já está basicamente provado, só nos resta juntar as peças.

Teorema 12 (Teorema Fundamental da Aritmética)**.** *Seja $a \in \mathbb{Z}$ tal que $a \neq 0, 1, -1$. Então, existem primos positivos $p_1 \leq p_2 \leq p_3 \cdots \leq p_n$ e inteiros positivos $n_1, n_2, \dots, n_r$ tais que $a = Ep_1^{n_1} \dots p_r^{n_r}$, em que $E = \pm 1$ conforme a seja positivo ou negativo. Além disso, essa decomposição é única.*

Demonstração. Dado a nas condições do teorema, temos que podemos reescrevê-lo da seguinte forma: $a = E|a|$, onde $E = 1$ ou $E = -1$, dependendo de quem for a.

Como $|a| > 1$ para todo a nessas condições, temos pelo teorema anterior que existem $p_1 \leq p_2 \leq p_3 \cdots \leq p_i$, tais que $|a| = p_1p_2 \dots p_i$, logo:
$a = Ep_1p_2 \dots p_i$.

Agora, agrupando os primos eventualmente repetidos, podemos reescrever $a = Ep_1^{n_1} \dots p_r^{n_r}$. E, note que a unicidade dessa decomposição segue diretamente do teorema anterior. □

Lema 3. *Sejam $a = p_1^{n_1} \dots p_r^{n_r}$ e $d = p_1^{m_1} \dots p_r^{m_r}$ inteiros positivos, onde $p_1, p_2, \dots, p_r$ são primos positivos e $n_i, m_i, 1 \leq i \leq r$ são inteiros não negativos. Então, $d \setminus a$ se, e somente se, $m_i \leq n_i, 1 \leq i \leq r$.*

Demonstração. ($\Rightarrow$) Temos que se $d \setminus a$, então existe $c \in \mathbb{Z}$, por definição, tal que $a = dc$, ou seja, $p_1^{n_1} \dots p_r^{n_r} = (p_1^{m_1} \dots p_r^{m_r})c$, logo c é da forma $c = p_1^{t_1} \dots p_r^{t_r}$, com isso temos que:
$p_1^{n_1} \dots p_r^{n_r} = (p_1^{m_1} \dots p_r^{m_r})(p_1^{t_1} \dots p_r^{t_r}) \Rightarrow p_1^{n_1} \dots p_r^{n_r} = p_1^{m_1+t_1} \dots p_r^{m_r+t_r}$
$\Rightarrow n_1n_2 \dots n_r = (m_1 + t_1)(m_2 + t_2) \dots (m_r + t_r)$
$\Rightarrow n_i = m_i + t_i$.

Logo, $n_i \geq m_i$.
($\Leftarrow$) Se $m_i \leq n_i$, então temos que $n_i = m_i + t_i$, com $t_i \in \mathbb{Z}$. Logo,

$a = p_1^{n_1} \dots p_r^{n_r} = p_1^{m_1+t_1} \dots p_r^{m_r+t_r} = (p_1^{m_1} \dots p_r^{m_r})(p_1^{t_1} \dots p_r^{t_r}) = dc.$

Portanto, $d \setminus a$. □

Teorema 13. *Sejam* $a = p_1^{n_1} \dots p_r^{n_r}$ *e* $b = p_1^{m_1} \dots p_r^{m_r}$ *inteiros nas mesmas condições do lema anterior. Então valem,*

(i) $d = mdc(a, b) = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, *em que* $\alpha_i = min(n_i, m_i),\ 1 \leq i \leq r$.

(ii) $m = mmc(a, b) = p_1^{\beta_1} \dots p_r^{\beta_r}$, *em que* $\beta_i = max(n_i, m_i),\ 1 \leq i \leq r$.

Demonstração. Provando (i): Para provarmos que vale (i), basta mostrar que d verifica as condições de ser máximo divisor comum (definição 8), ou seja, que d divide a e b, e verificar que se tivermos um d' tal que $d' \setminus a$ e $d' \setminus b$, então $d' \setminus d$.

Seja $d = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, onde $\alpha_i = min(n_i, m_i),\ 1 \leq i \leq r$. Nessas condições temos que $d \setminus a$ e $d \setminus b$, pelo lema anterior, pois $\alpha_i \leq n_i$ e $\alpha_i \leq m_i$, para todo $q \leq i \leq r$.

Consideremos agora um d' tal que $d' \setminus a$ e $d' \setminus b$, com $d' = p_1^{s_1} \dots p_r^{s_r}$, onde $s_1, \dots, s_r$ são inteiros não negativos. Então, do lema anterior, vem que $s_i \leq n_i$ e $s_i \leq m_i$, $1 \leq i \leq r$, logo temos que $d' \setminus d$, pois $\alpha_i = min(n_i, m_i)$, ou seja, $s_i \leq \alpha_i$.

Provando (ii): Para provarmos que vale (ii), basta mostrar que m verifica as propriedades de ser mínimo múltiplo comum (teorema 8). Então, seja $m = p_1^{\beta_1} \dots p_r^{\beta_r}$, onde $\beta_i = max(n_i, m_i), 1 \leq i \leq r$. Nessas condições temos que $a \setminus m$ e $b \setminus m$, pelo lema anterior, pois $n_i \leq \beta_i$ e $m_i \leq \beta_i$, para todo $1 \leq i \leq r$.

Consideremos agora um m' tal que $a \setminus m'$ e $b \setminus m'$, com $m' = p_1^{\theta_1} \dots p_r^{\theta_r}$, onde $\theta_1, \dots, \theta_r$ são inteiros não negativos. Então, do lema anterior, vem que $n_i \leq \theta_i$ e $m_i \leq \theta_i$, logo temos que $m \setminus m'$, pois $\beta_i = max(n_i, m_i)$, ou seja, $\beta_i \leq \theta_i$.

□

Vamos discutir agora um dos teoremas mais importantes em relação aos números primos, que, curiosamente, é de fácil entendimento.

Sabemos, pelo menos intuitivamente, que o conjunto dos números naturais $\mathbb{N}$, assim como, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, são infinitos, ou seja, existem incontáveis números dentro desses conjuntos, mas, o que podemos dizer em relação ao conjunto dos números primos, ao qual definiremos como sendo o conjunto $\mathbb{P}$?

Teorema 14. *O conjunto dos números primos* ($\mathbb{P}$) *é infinito.*

Demonstração. Vamos supor que o conjunto $\mathbb{P}$ seja finito, e tal que $\mathbb{P} = \{p_1, p_2, p_3, \ldots, p_n\}$. Sendo assim, consideremos então o número $\rho = p_1 p_2 \ldots p_n + 1$. De acordo com o teorema 11 que vimos anteriormente, temos que esse número ρ admite um divisor primo p_i, onde $p_i \in \mathbb{P}$. Mas, como $p_i \setminus p_1 p_2 \ldots p_n$, então p_i dividiria também $1 = \rho - p_1 p_2 \ldots p_n$, o que é um absurdo!

Portanto o conjunto dos número primos $\mathbb{P}$ é infinito.

□

Note que esse teorema é importante pois ele deixa explícito que o conjuntos dos números primos também é infinito, assim como os que mencionamos anteriormente. Mas, mesmo sabendo que o conjunto $\mathbb{P}$ é infinito, muitas questões referentes aos números primos ainda permanecem sob investigação. Um exemplo disso é que, diferentemente dos conjuntos já citados, não sabe-se ainda como estão distribuídos os número primos dentro de $\mathbb{P}$. O que significa dizer isso? Intuitivamente conhecemos "todos" os números inteiros, por exemplo, basta pensarmos no maior número inteiro que nos vem a mente e somar mais um, e fazendo isso sucessivamente conseguimos caracterizar e distribuir os elementos do conjunto $\mathbb{Z}$, porém, o mesmo não podemos fazer com relação ao conjunto dos números primos. No momento em que este trabalho está sendo construído, o maior número primo encontrado possui mais de 20 milhões de algarismos, mas não sabemos de imediato qual é o seu "sucessor".

Mesmo o conjunto dos números primos não sendo "completamente" conhecido, isso não impede que os estudiosos façam conjecturas em relação a ele, algumas delas foram provadas, outras desmentidas, mas o que podemos perceber disso tudo é que o conjunto dos números primos ainda é um incógnita para a comunidade. Há muito para descobrir.

Capítulo 3

Congruências e o "Teorema de Fermat"

3.1 Congruências

Definição 11. *(Congruência módulo m) Seja $m \neq 0$ um inteiro fixado. Dizemos que $a, b \in \mathbb{Z}$ são congruentes módulo m se o mesmo divide a diferença entre a e b. Em outras palavras, $a - b = dk$ para algum $k \in \mathbb{Z}$.*
Notação: $a \equiv b \pmod{m}$.

Antes de mais nada, devemos observar que vamos nos restringir apenas as situações em que $m > 0$, visto que para o contrário segue de uma forma bem parecida.

Dito isso, num primeiro momento, essa definição pode nos parecer estranha, sendo assim, vamos tentar ver o que há "por trás" dela para esclarecer um pouco mais o seu conceito e suas futuras aplicações.

Sendo assim, note que, nas mesmas condições da definição acima, podemos dizer que $a \equiv b \pmod{m}$ se, e somente se, eles tem como resto o mesmo inteiro quando dividimos por m, pois, pelo algoritmo de Euclides, temos que:

(I) $\frac{a}{m} \Rightarrow a = mq_1 + r_1$, $0 \leq r_1 < m$.

(II) $\frac{b}{m} \Rightarrow b = mq_2 + r_2$, $0 \leq r_2 < m$.

Logo, fazendo $(I) - (II)$ temos que: $a - b = (mq_1 + r_1) - (mq_2 - r_2)$, com $0 \leq |(r_1 - r_2)| < m$.
$\Rightarrow a - b = m(q_1 - q_2) + (r_1 - r_2)$.

Mas, para que a seja congruente a b módulo m, nessas condições, devemos ter que $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

Portanto, podemos dizer que $a \equiv b \pmod{m} \Leftrightarrow r_1 = r_2$.

Agora que pudemos entender um pouco melhor do que se tratam as congruências, vejamos algumas consequências desse tratamento com a divisão euclidiana.

Proposição 9. *Sejam $m > 0$ um inteiro fixo e sejam também $a, b, c, d \in \mathbb{Z}$ arbitrários. Então, valem as seguintes propriedades:*

i) $a \equiv a \pmod{m}$.

ii) Se $a \equiv b \pmod{m}$, *então* $b \equiv a \pmod{m}$.

iii) Se $a \equiv b \pmod{m}$ *e* $b \equiv c \pmod{m}$, *então* $a \equiv c \pmod{m}$.

iv) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $a + c \equiv b + d \pmod{m}$.

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

vi) Se $a \equiv b \pmod{m}$ *e* $c \equiv d \pmod{m}$, *então* $ac \equiv bd \pmod{m}$.

vii) Se $a \equiv b \pmod{m}$, *então* $a^n \equiv b^n \pmod{m}$, *para todo* $n \in \mathbb{Z}^+$.

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

Demonstração. O item *i)* não precisaremos provar pois é trivial, uma vez que, $a \equiv a \pmod{m} \Leftrightarrow m \setminus (a - a) \Rightarrow m \setminus 0$.

ii) Se $a \equiv b \pmod{m}$, então $a - b = mk$, para algum $k \in \mathbb{Z}$; multiplicando essa igualdade por (-1) temos que $b - a = m(-k)$.

Logo, $m \setminus (b - a) \Rightarrow b \equiv a \pmod{m}$.

iii) Temos que se $a \equiv b \pmod{m}$ e $b \equiv c \pmod{m}$, então $a - b = mk_1 \Rightarrow b = a - mk_1$ e $b - c = mk_2 \Rightarrow b = c + mk_2$, para algum $k_1, k_2 \in \mathbb{Z}$, respectivamente. Logo, $a - mk_1 = c + mk_2$, disso obtemos $a - c = mk_1 + mk_2 = m(k_1 + k_2)$.

Portanto, como $(k_1 + k_2) \in \mathbb{Z}$, temos que $a \equiv c \pmod{m}$.

iv) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a - b = mk_1$ e $c - d = mk_2$, com $k_1, k_2 \in \mathbb{Z}$. Logo, somando ambas desigualdades, temos que $(a - b) + (c - d) = mk_1 + mk_2$, e disso obtemos que $(a + c) - (b + d) = m(k_1 + k_2)$.

Portanto, $a + c \equiv b + d \pmod{m}$.

v) Se $a \equiv b \pmod{m}$, então $a - b = mk$ para algum $k \in \mathbb{Z}$, e disso temos que $a = b + mk$. Sendo assim, somando c nessa igualdade temos que $a + c = (b + c) + mk$, logo $(a + c) - (b + c) = mk$.

Portanto, $a + c \equiv b + c \pmod{m}$.

vi) Se $a \equiv b \pmod{m}$ e $c \equiv d \pmod{m}$, então $a = b + mk_1$ e $c = d + mk_2$, respectivamente, com $k_1, k_2 \in \mathbb{Z}$. Logo, multiplicando essas igualdades obtemos:

$ac = (b + mk_1)(d + mk_2) = bd + bmk_2 + dmk_1 + mk_1mk_2 \Rightarrow ac - bd = m(bk_2 + dk_1 + mk_1k_2)$.

Portanto, como $(bk_2 + dk_1 + mk_1k_2) \in \mathbb{Z}$, temos que $ac \equiv bd \pmod{m}$.

vii) Neste caso, usaremos o Princípio de Indução Completa para provar essa parte da proposição.

1º) Para $n = 1$ sabemos que é verdade pela própria hipótese.

2º) Suponhamos que a afirmação seja verdadeira para $n = k$.

3º) Assumindo como verdade que se $a \equiv b \pmod{m}$, então $a^k \equiv b^k \pmod{m}$, vamos mostrar que vale também para $k + 1$. Sendo assim, como já sabemos pela própria hipótese que $a \equiv b \pmod{m}$, utilizando *vi*) temos que: $a^k a \equiv b^k b \pmod{m} \Rightarrow a^{k+1} \equiv b^{k+1} \pmod{m}$.

viii) Se $a + c \equiv b + c \pmod{m}$, então $(a + c) - (b + c) = mk$, com $k \in \mathbb{Z}$. Mas, isso é equivalente a dizer que $a + c - b - c = a - b = mk$.

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

□

Depois de ver todas essas propriedades das congruências uma propriedade que ajudaria bastante nos nossos cálculos seria pensar em que se $ac \equiv bc \pmod{m}$, então $a \equiv b \pmod{m}$. Mas será que isso vale sempre? Vejamos:

Se $ac \equiv bc \pmod{m}$, então, por definição, temos que $m \setminus ac - bc$, logo, $m \setminus (a - b)c$. Sendo assim, para que possamos concluir que $a \equiv b \pmod{m}$ devemos ter que $mdc(m, c) = 1$ pois, nesse caso, pelo teorema de Euclides, teríamos que $m \setminus (a - b)$, que é rigorosamente o que desejávamos.

Proposição 10. *Seja m um inteiro fixo e a, b, c inteiros arbitrários. Se $mdc(c, m) = 1$, então $ac \equiv bc \pmod{m}$ implica que $a \equiv b \pmod{m}$.*

Como acabamos de verificar, temos que, nessas condições, essa proposição é verificada. Dito tudo isso, vejamos uma situação interessante em que podemos aplicar esse conceito de congruência.

Exemplo 13. Vamos determinar qual o resto da divisão de 5^{60} por 26.

Observamos inicialmente que realizar essa tarefa sem a Teoria das Congruências é deveras trabalhoso, visto que 5^{60} é um número demasiadamente grande. Agora, pelo Algoritmo de Euclides, temos que $5^{60} = 26q + r$, com $0 \leq r < 26$. Logo, com a teoria que vimos até agora, podemos concluir que a nossa tarefa se resume a encontrar r tal que $5^{60} \equiv r \pmod{26}$. Pensando em utilizar alguma das propriedades que provamos nesse tópico, podemos observar que:

$5^2 \equiv -1 \pmod{26}$, logo, como vimos em *vii*) da proposição anterior, temos que:

$(5^2)^{30} \equiv (-1)^{30} \pmod{26}$, para $n = 30$. Com isso, podemos concluir que $5^{60} \equiv 1 \pmod{26}$. Portanto, o resto da divisão de 5^{60} por 26 é 1.

Uma outra situação interessante a qual pode-se discutir esse conceito está relacionada com o Teorema de Bézout que provamos no capítulo anterior.

Lembrando: O Teorema de Bézout diz que dados $a, b \in \mathbb{Z}$ e $d = mdc(a, b)$, então existem inteiros r e s tais que $d = ra + sb$.

Mas o que não sabemos é, "será que r e s são únicos?". Para isso, vejamos:

Exemplo 14 (Equações Diofantinas Lineares)**.** Equações do tipo $ax + by = c$ com $a, b, c \in \mathbb{Z}$, onde $a, b \neq 0$, são chamadas de *Equações Diofantinas Lineares.*

Proposição 11. *Dados a, b, c nas condições do exemplo acima, e dado $d = mdc(a, b)$, temos que a equação diofantina $ax + by = c$ tem solução se, e somente se, $d \setminus c$.*

Demonstração. ($\Rightarrow$) Vamos considerar o seguinte conjunto $J = \{ax + by |\ x, y \in \mathbb{Z}\}$.

Dessa forma, temos que J é um ideal de $\mathbb{Z}$ (da mesma forma que vimos na demonstração do Teorema de Bézout); e como $d = mdc(a, b)$ temos ainda, do teorema que antecede ao de Bézout, que $J = d\mathbb{Z}$.

Isso já basta para provar a proposição pois, se $ax + by = c$, como $ax + by \in J$, temos que $ax + by = dk$, com $k \in \mathbb{Z}$, ou seja, $ax + by = dk = c \Rightarrow d \setminus c$.

($\Leftarrow$) Agora, se $d \setminus c$, então temos que $c = dp$, com $p \in \mathbb{Z}$, logo $dp = ax + by$, com $x, y \in \mathbb{Z}$. $\square$

Mas note que ao provarmos que $ax + by = c$ tem solução se, e somente se, $d \setminus c$, estamos na verdade mostrando que essa equação tem solução se $c \equiv 0 \pmod{d}$, pois são duas verdades equivalentes. Entretanto, observe também que ainda não discutimos se r e s são únicos, então vejamos o seguinte teorema.

Teorema 15. *Sejam $a, b, c \in \mathbb{Z}$ tais que $d = mdc(a, b)$ divide c. Pelo Teorema de Bézout, escrevendo d na forma $d = ra + sb$ com $r, s \in \mathbb{Z}$, temos que $x_0 = \frac{rc}{d}$, $y_0 = \frac{sc}{d}$ é uma solução da equação $ax + by = c$. Toda outra solução é da forma: $x = \frac{rc+bt}{d}$, $y = \frac{sc-at}{d}$, com $t \in \mathbb{Z}$.*

E, reciprocamente, para todo $t \in \mathbb{Z}$ os valores de x e y dados pelas fórmulas acima são soluções da equação.

Demonstração. Para tanto, vejamos se a solução apresentada é, de fato, uma solução para $d = ra + sb$, logo, multiplicando por $\frac{c}{d}$ teremos que: $\frac{rca}{d} + \frac{scb}{d} = \frac{dc}{d} = c$, ou seja, $x_0 = \frac{rc}{d}$ e $y_0 = \frac{sc}{d}$ são de fato soluções. Agora, devemos provar que todo par de inteiros $x = \frac{rc+bt}{d}$ e $y = \frac{sc-at}{d}$ são solução da equação $ax + by = c$, para isso, observe que $x = \frac{rc+bt}{d} = x_0 + \frac{bt}{d}$ e $y = \frac{sc-at}{d} = y_0 - \frac{at}{d}$.

Então, substituindo na equação, temos que:
$a(x_0 + \frac{bt}{d}) + b(y_0 - \frac{at}{d}) = ax_0 + by_0 = c$, logo, o par x, y dado é solução da equação.

Agora, seja x', y' uma solução da equação, iremos mostrar que existe $t \in \mathbb{Z}$ tal que $x' = x_0 + \frac{bt}{d}$ e $y' = y_0 - \frac{at}{d}$.

Sendo assim, temos que, como x', y' são solução da equação, então $ax' + by' = c = ax_0 + by_0$, logo $a(x' - x_0) = b(y_0 - y')$ (*).

Temos também que $d = mdc(a, b)$, logo $a = a_1 d$ e $b = b_1 d$, com $a_1, b_1 \in \mathbb{Z}$. Dessa forma, temos que $mdc(a_1, b_1) = mdc(a/d, b/d) = d/d = 1$, sendo assim, dividindo por d a expressão (*) temos que: $\frac{a(x'-x_0)}{d} = \frac{b(y_0-y')}{d} \Rightarrow a_1(x' - x_0) = b_1(y_0 - y')$ (**). E, com isso, podemos concluir que $b_1 \backslash (x' - x_0)$, pois $mdc(a_1, b_1) = 1$, portanto, existe $t \in \mathbb{Z}$ tal que $x' - x_0 = b_1 t \Rightarrow x' = x_0 + \frac{bt}{d}$. Mas como $x' - x_0 = b_1 t$, substituindo em (**), temos que:
$a_1 b_1 t = b_1(y_0 - y') \Rightarrow a_1 t = y_0 - y'$, logo $\frac{at}{d} = y' - y_0 \Rightarrow y' = y_0 - \frac{at}{d}$. □

Feito tudo isso em relação as equações diofantinas, podemos concluir que existem infinitos resultados para r e s tais que $d = ra + sb$, basta que consideremos a equação $ax + by = d$, dessa forma, pelo teorema que acabamos de ver, temos que $x = r + \frac{bt}{d}$ e $y = s - \frac{at}{d}$ são soluções dessa equação, com $t \in \mathbb{Z}$, ou seja, possui infinitas soluções.

3.2 Resolução de congruências lineares

O que faremos nessa seção é, de certa forma relacionar a teoria das congruências com as equações diofantinas. Sendo assim, estudaremos o problema de resolver equações da forma $ax \equiv b \pmod{m}$, com $a, b, m \in \mathbb{Z}$ dados e $m > 0$.

Dessa forma, verificamos que se x é uma solução dessa equação, então m divide a diferença entre ax e b, em outras palavras, deve existir $y \in \mathbb{Z}$ tal que $ax = b - my$, logo $ax + my = b$. Sem demora, vemos que o nosso problema se resume a discutir as soluções da equação diofantina $ax + my = b$, reciprocamente.

Teorema 16. *A congruência $ax \equiv b \pmod{m}$ tem solução se, e somente se, $d = mdc(a, m)$ divide b.*

Demonstração. Podemos observar inicialmente que se $ax \equiv b \pmod{m}$ tem solução, então existe $y \in \mathbb{Z}$ tal que $ax - b = my$, mas note que isso é equivalente a dizer que $ax + my = b$, ou seja, uma equação diofantina, e como acabamos de ver, esta só tem solução se $d = mdc(a, m)$ divide

b. Sabemos também que esta tem infinitas soluções, mas como estamos falando de congruências, veremos que esta possui m soluções, e as outras serão congruentes módulo m às anteriores.

Como acabamos de ver, as soluções dessa equação diofantina são da forma $x = x_0 + \frac{mt}{d}$, $y = y_0 - \frac{at}{d}$, com $t \in \mathbb{Z}$, onde $x_0 = \frac{rb}{d} = rb_1$ e $y_0 = \frac{sb}{d} = sb_1$, pois $b = b_1 d$, e $r, s, b_1 \in \mathbb{Z}$. Com isso, temos que todas as soluções da congruência $ax \equiv b \pmod{m}$ são da forma $x = rb_1 + \frac{mt}{d}$, com $t \in \mathbb{Z}$. Logo, atribuindo a t os valores $\{0, 1, 2, 3, \ldots, d-1\}$ obtemos todas as soluções $S = \{x_0 = rb_1, x_1 = x_0 + \frac{m}{d}, x_2 = x_0 + \frac{2m}{d}, \ldots, x_{d-1} = x_0 + \frac{m(d-1)}{d}\}$. O que faremos então é mostrar que qualquer outra solução obtida é congruente módulo m à alguma dessas.

De fato, se $x = x_0 + \frac{mt}{d}$ é dada por algum outro valor de t que não está presente em S, dividindo t por d podemos escrever $t = qd + r'$, onde $0 \leq r' \leq d-1$, logo, $x = x_0 + \frac{m(qd+r')}{d} \Rightarrow x = x_0 + mq + \frac{mr'}{d}$, ou seja, $x \equiv x_0 + \frac{mr'}{d} \pmod{m}$. Mas, como $0 \leq r' \leq d-1$, temos que esse $x \in S$. Portanto, vemos que as outras soluções são congruentes a alguma que está presente em S.

Provaremos também que estas soluções de S não são congruentes entre si módulo m. Sendo assim, vamos supor que $x_h = x_0 + \frac{hm}{d}$ e $x_k = x_0 + \frac{km}{d}$ são congruentes módulo m, onde $0 \leq h \leq k \leq d-1$. Logo, o que teríamos então é que:

$$\begin{aligned} x_0 + \frac{hm}{d} &\equiv x_0 + \frac{km}{d} \pmod{m} \\ \Rightarrow \frac{hm}{d} &\equiv \frac{km}{d} \pmod{m} \end{aligned}$$

Logo, $m \backslash \frac{(h-k)m}{d}$, mas temos que $0 \leq h-k < d$, então $0 \leq \frac{(h-k)m}{d} < \frac{md}{d} = m \Rightarrow 0 \leq \frac{(h-k)m}{d} < m$.

Portanto, como $m \backslash \frac{(h-k)m}{d}$ e $\frac{(h-k)m}{d} < m$, temos que $h - k = 0 \Rightarrow h = k$. □

Sendo assim, poderíamos reescrever esse teorema de tal forma.

Teorema 17. *Sejam $a, m \in \mathbb{Z}$, $d = mdc(a, m)$ e b um múltiplo de d. Escrevendo $d = ra + sm$, com $r, s \in \mathbb{Z}$ e $b = b_1 d$, a congruência $ax \equiv b \pmod{m}$ tem d soluções não congruentes, duas a duas módulo m, sendo elas $S = \{x_0 = rb_1, x_1 = x_0 + \frac{m}{d}, x_2 = x_0 + \frac{2m}{d}, \ldots, x_{d-1} = x_0 + \frac{m(d-1)}{d}\}$. Toda outra solução é congruente a uma dessas módulo m.*

Corolário 5. *Se a e m são inteiros relativamente primos, então a congruência $ax \equiv b \pmod{m}$ sempre tem solução.*

Escrevendo $1 = ra + sm$, temos pelo teorema que acabamos de ver que $x = rb$ é uma solução, e é única módulo m.

Agora, vejamos um exemplo.

Exemplo 15. Consideremos a congruência $-3x \equiv 18 \pmod{15}$.

Temos que $mdc(-3, 15) = 3$, logo, escrevendo $3 = (-3)r + (15)s$ vem que $r = 4$ (e $s = 1$). Temos também que como $d \backslash 18$, então $18 = 3b_1$, logo $b_1 = 6$. Sendo assim, uma solução particular será $x_0 = rb_1 = 4.6 = 24$, então $x_1 = rb_1 + \frac{m}{d} = 24 + \frac{15}{3} = 29$, $x_2 = 24 + 2.5 = 34$.

Portanto, as soluções dessa equação são $S = \{24, 29, 34\}$, todas as outras são congruentes a uma dessas módulo 15.

Proposição 12. *Sejam a e m inteiros e b um múltiplo de $d = mdc(a, m)$. Escrevendo $a = a_1 d$, $b = b_1 d$, $m = nd$ e escrevendo d na forma $d = ra + sm$, temos que a congruência $ax \equiv b \pmod{m}$ é equivalente a $x \equiv rb_1 \pmod{n}$.*

Demonstração. Para provarmos essa proposição temos que verificar que vale a dupla implicação (equivalência), ou seja, que nessas condições, $ax \equiv b \pmod{m} \Leftrightarrow x \equiv rb_1 \pmod{n}$.

($\Rightarrow$) Temos que $ax \equiv b \pmod{m}$, porém, pela hipótese $a = a_1 d$, $b = b_1 d$ e $m = nd$, logo essa congruência pode ser reescrita como: $a_1 dx \equiv b_1 d \pmod{nd}$, e disso temos que $a_1 x \equiv b_1 \pmod{n}$, e como $r \equiv r \pmod{n}$, temos também que $ra_1 x \equiv rb_1 \pmod{n}$ **(1)**.

Agora, voltando em $d = ra + sm$ temos que $d = ra_1 d + snd \Rightarrow 1 = ra_1 + sn$, ou seja, $ra_1 \equiv 1 \pmod{n}$, e como $x \equiv x \pmod{n}$, temos também que $ra_1 x \equiv x \pmod{n}$ **(2)**.

Portanto, de **(1)** e **(2)** obtemos que $x \equiv rb_1 \pmod{n}$.

($\Leftarrow$) Temos que $x \equiv rb_1 \pmod{n}$ **(3)**. Agora, como $d = ra + sm$, dividindo por d obtemos que $1 = r\frac{a}{d} + s\frac{m}{d} \Rightarrow 1 = ra_1 + sn$, sendo assim temos que $ra_1 \equiv 1 \pmod{n}$ **(4)**. Portanto, multiplicando **(3)** por **(4)** temos: $ra_1 x \equiv rb_1 \pmod{n}$, e como $mdc(r, n) = 1$, temos que $a_1 x \equiv b_1 \pmod{n}$, ou seja, $a_1 x - b_1 = nk$ com $k \in \mathbb{Z}$, mas $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$ e $n = \frac{m}{d}$, logo, essa igualdade se reescreve como $ax - b = mk$.

Portanto, $ax \equiv b \pmod{m}$ como gostaríamos.

□

Exemplo 16. Consideremos a congruência $6x \equiv 14 \pmod{4}$.

Temos que $mdc(6, 4) = 2$, logo, escrevendo $2 = 6r + 4s$ temos $r = 1$ (e $s = -1$). Como $2 = mdc(4, 6)$, também temos que $14 = 2b_1$ e $4 = 2.n$, logo $b_1 = \frac{b}{d} = \frac{14}{2} = 7$ e $n = \frac{m}{d} = \frac{4}{2} = 2$, com isso temos que a equação dada é equivalente a $x \equiv rb_1 \pmod{n} \Rightarrow x \equiv 1.7 \pmod{2}$. E as

soluções são $x_0 = rb_1 = 7.1 = 7$, $x_1 = 7 + 2 = 9$, toda outra solução é congruente a uma dessas módulo 4.

3.3 O Pequeno Teorema de Fermat

Finalmente, agora que conhecemos conceitos importantíssimos para a Teoria dos Números, e para entender a seguinte indagação de Fermat, podemos enunciar e demonstrar esse teorema tão prestigioso para a mesma através do conceito de congruências que acabamos de ver.

Teorema 18. *Sejam p um número primo e a um inteiro tal que $p \nmid a$. Então, nessas condições, temos que $a^{p-1} \equiv 1 \pmod{p}$.*

Antes de demonstrar este teorema podemos observar que o mesmo pode ser visto numa versão diferente, mas equivalente a esta, onde nessas mesmas condições teríamos que $a^p \equiv a \pmod{p}$.

Pode não parecer evidente, mas se $a^p \equiv a \pmod{p} \Rightarrow aa^{p-1} \equiv a \pmod{p}$, e como $p \nmid a$, isso implicaria que $a^{p-1} \equiv 1 \pmod{p}$, como vemos através da proposição 10, podemos concluir esta última implicação que iremos demonstrar agora.

Demonstração. Para tal demonstração consideremos os conjuntos $X = \{1, 2, 3, \ldots, p-1\}$ e $aX = \{a, 2a, 3a, \ldots, (p-1)a\}$. A primeira coisa que precisamos observar é que nenhum elemento de aX é congruente entre si módulo p pois, caso fosse, teríamos que $ax \equiv ay \pmod{p}$ com $1 \leq x, y \leq (p-1)$, e como $p \nmid a$, ou seja, $mdc(a, p) = 1$, teríamos que $x \equiv y \pmod{p}$, fato esse que sabemos que não acontece pois os elementos $x, y \in X$, logo, não são congruentes entre si módulo p.

Outra coisa que devemos observar é que nenhum elemento de X é congruente a 0 módulo p pois, caso fosse, teríamos que $p \setminus ax$ com $x \in X$, mas como já sabemos que $p \nmid a$, teríamos que $p \setminus x$, porém isso não acontece também.

Então, podemos concluir que os elementos de X são congruentes aos de aX módulo p numa ordem conveniente, ou seja, temos que:

$$\begin{aligned} a &\equiv x_1 \pmod{p} \\ 2a &\equiv x_2 \pmod{p} \\ &\vdots \\ (p-1)a &\equiv x_{p-1} \pmod{p}, \end{aligned}$$

onde $x_i \in X$ com $i = 1, 2, 3, \ldots, (p-1)$. Disso, multiplicando essas congruências, temos que:

$a.2a.3a \ldots (p-1)a \equiv 1.2.3 \ldots (p-1) \pmod{p} \Rightarrow (p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$, e como $mdc(p, (p-1)!) = 1$, podemos concluir que $a^{p-1} \equiv 1 \pmod{p}$.

E com isso finalizamos a demonstração desse teorema. □

Referências Bibliográficas

[1] F. C. P. Milies, S. P. Coelho; *Números: Uma Introdução à Matemática* -3.ed. 1. reimpr.- São Paulo: Editora da Universidade de São Paulo, 2003. - (Acadêmica; 20).

[2] L. H. J. Monteiro; *Elementos de Álgebra*, 1969, Livros Técnicos e Científicos Editora, Rio de Janeiro.

[3] C. Caldwell; The Prime Pages.
Disponível em: $https://primes.utm.edu/notes/by_year.html$.
Acesso em 24 de junho de 2019.

[4] A. Hefez; *Elementos de aritmética* -2.ed. Rio de Janeiro: SBM, 2011.