Capítulo 7

Teoria dos números no ensino básico: uma proposta de texto didático

Me. Josemar Claudino Barbosa[1]
Dra. Barbara Costa da Silva[2]

Resumo: A Teoria dos Números é uma área da matemática de extrema importância, por suas aplicações e por trazer muitas técnicas para resolução de problemas. Este artigo aborda os temas mais clássicos da Teoria dos Números e que também pertence ao currículo do ensino fundamental, tais como divisibilidade, números primos, mdc e mmc. Além disso, também abordamos temas como equações diofantinas e congruência modular, apresentamos a resolução de alguns exemplos, frutos da aplicação dessa teoria, bem como a demonstração das proposições e teoremas expostos, sem abrir mão do rigor matemático.

Palavras-chave: Teoria dos Número; Congruências; Teorema de Euler.

[1]IFPE-Instituto Federal de Pernambuco, josemar.barbosa@pesqueira.ifpe.edu.br
[2]UFRPE-Universidade Federal Rural de Pernambuco, barbara.costasilva@ufrpe.br

7.1 Fundamentos teóricos e metodológicos

7.1.1 Divisibilidade

A Teoria dos Números é o ramo da matemática pura que estuda propriedades dos números inteiros, bem como a larga classe de problemas que surge no seu estudo. O termo aritmética (*arithmetiké*) vem do idioma grego e literalmente significa ciência dos números, sendo também usado para se referir à Teoria dos Números.

Um conceito muito importante no estudo da Teoria dos Números é chamado de divisibilidade. Mas, do que trata tal conceito? Vejamos a seguir.

Definição 1. *Sejam a e b inteiros com* $a \neq 0$*. Dizemos q*

43 errors36 warnings ue a é um divisor de b ou que b é um múltiplo de a, se existir um inteiro c tal que $b = a \cdot c$ *(indicamos* $a|b$*). Caso contrário, expressamos* $a \nmid b$*.*

Exemplo 1. $8|24$*, pois* $24 = 3.8$*.*

É fácil ver que $1|a$ para todo a inteiro, $a|a$ e $a|0$ para todo $a \neq 0$, $a \in \mathbb{Z}$. De fato, temos que $a = 1 \cdot a$, para todo $a \in \mathbb{Z}$ e que $0 = a \cdot 0$, para todo inteiro a, $a \neq 0$.

As propriedades a seguir serão de fundamental importância, pois se revelarão bastante úteis na resolução de vários exercícios. A princípio, tente verificar por meio de alguns números a veracidade de cada afirmação abaixo.

1. Sejam a, b e c inteiros, $a \neq 0$, $b \neq 0$. Se $a|b$ e $b|c$, então $a|c$.

2. Sejam a, b, c, e d inteiros, $a \neq 0$, $c \neq 0$. Se $a|b$ e $c|d$, então $ac|bd$.

3. Sejam a, b, m e n inteiros, com $a \neq 0$ e $n \neq 0$. Se $an|am$, então $n|m$.

4. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|(b+c)$, então $a|b$ se, e somente se, $a|c$.

5. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|(b-c)$, então $a|b$ se, e somente se, $a|c$.

6. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|b$ e $a|c$, então $a|(bx \pm cy)$ para quaisquer x, y inteiros.

7. Dados a, b com $a \neq 0$. Temos que se $a|b$, então $b \geq a$.

Vejamos agora as demonstrações de cada propriedade.

Demonstrações:

1. Ora, se $a|b$, então podemos escrever $b = am$, para algum $m \in \mathbb{Z}$. Por outro lado, como $b|c$, então podemos escrever $c = bn$, para algum $n \in \mathbb{Z}$. Portanto, teremos que $c = bn = a(mn)$, o que mostra que $a|c$.

2. Ora, se $a|b$ então podemos escrever $b = am$ para algum $m \in \mathbb{Z}$. Por outro lado, se $c|d$ então $d = cn$, para algum $n \in \mathbb{Z}$. Daí, temos que $b \cdot d = (ac)(mn)$, o que mostra que $ac|bd$.

3. De fato, como $an|am$, temos que existe k inteiro tal que $am = (an)k$. Ora, como $a \neq 0$, podemos dividir ambos os membros por a, o que vai resultar $m = nk$, o que mostra que $n|m$.

4. Como $a|(b+c)$, existe $k \in \mathbb{Z}$ tal que $b+c = ak$. Mais ainda, como $a|b$, temos que existe $r \in \mathbb{Z}$ tal que $b = ar$. A partir das duas igualdades, concluímos que

$$ar + c = ak,$$

Logo, temos que

$$c = ak - ar = a(k-r),$$

o que implica que $a|c$. Ficará como exercício para o leitor a demonstração da outra implicação.

5. A demonstração dessa propriedade também fica a cargo do leitor, pois tem uma demonstração análoga à propriedade anterior.

6. De fato, como $a|b$ e $a|c$, então existem inteiros m e n tais que $b = am$ e $c = an$. Daí, temos que
$bx \pm cy = (am)x \pm (an)y = a(mx) \pm a(ny) = a(mx \pm ny)$, para todo $x, y \in \mathbb{Z}$,

   portanto, concluí-se que $a|(bx \pm cy)$.

7. Essa última demonstração utiliza ideias análogas às anteriores, ficando, portanto, como exercício para o leitor.

Exemplo 2. *Prove que o número* $N = 5^{45362} - 7$ *não é divisível por* 5.

Solução 1. *Suponhamos que esse número fosse divisível por* 5. *Pela propriedade* 5 *acima, temos que se* $5|5^{45362} - 7$, *então* $5|7$, *o que não é verdade, mostrando assim que* $5 \not| 5^{45362} - 7$.

Exemplo 3. *Se a e b são dois números naturais e* $2a + b$ *é divisível por* 13, *mostre que* $93a + b$ *também é múltiplo de* 13.

Solução 2. *De fato, temos que* $93a + b = 91a + (2a + b)$. *Ora, como* $13|91a$, *pois* $91a = 13 \cdot (7a)$ *e, por hipótese,* $13|2a + b$, *concluímos que* $13|93a + b$.

Definição 2. *Chamamos de conjunto dos divisores naturais de um natural n dado, e indicamos por* $D(n)$, *os naturais de quem n é múltiplo.*

Exemplo 4. *Sendo* $n = 20$, *temos* $D(20) = \{1, 2, 4, 5, 10, 20\}$.

Se $D(n)$ tem exatamente dois elementos, isto é, $D(n) = \{1, n\}$, dizemos que n é um número primo. O número 7 possui apenas dois divisores, 1 e 7, portanto é um número primo.

7.1.2 Divisão Euclidiana

O algoritmo da divisão, apesar de sua simplicidade, é uma das ferramentas mais poderosas no estudo da Teoria dos Números. Apresentado pelo matemático Euclides, é bastante útil na resolução de muitos problemas. Vimos no tópico anterior que um número inteiro b é divisível por outro $a \neq 0$, se existir um inteiro c, tal que $b = a \cdot c$. Mas, quando b não é divisível por a, isto é,a ,/é o algoritmo da divisão que possibilitará as devidas representações desse processo. Vamos, então, ao enunciado desse importante resultado.

Teorema 1 (Algoritmo da divisão)**.** *Dados dois inteiros b e a, com* $a \neq 0$*, existem dois únicos inteiros q e r, tais que:*

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

Nesse caso, o número b é chamado de dividendo, a é chamado de divisor, q é chamado de quociente e r é chamado de resto da divisão.

Exemplo 5. *Note que* $13 = 5 \cdot 2 + 3$ *e isso significa dizer que, ao dividirmos* 13 *por* 5*, o quociente é* 2 *e o resto dessa divisão é* 3*.*

Exemplo 6. *Vejamos também que* $4 = 5 \cdot 0 + 4$*, ou seja, na divisão de* 4 *por* 5*, o quociente é* 0 *e o resto é* 4*.*

Exemplo 7. *Ao dividirmos* -19 *por* 5*, obteremos* $q = -4$ *e* $r = 1$*.*

Demonstração. Considere o número inteiro a, com $a \neq 0$. Podemos escrever o conjunto dos números inteiros da seguinte forma:

$$\mathbb{Z} = ... \cup \big[-2a, -a\big) \cup \big[-a, 0\big) \cup \big[0, a\big) \cup \big[a, 2a\big) \cup \big[2a, 3a\big) \cup ... \cup \big[qa, (q+1)a\big) \cup ...$$

Os subconjuntos descritos acima são disjuntos, ou seja, sendo b um inteiro qualquer, temos que b pertence a apenas um desses subconjuntos, sendo portanto único. Mais ainda, podemos escrever:

$$qa \leq b < (q+1)a = qa + a \Rightarrow 0 \leq \underbrace{b - qa}_{r} < a$$

Desta forma, r é únicamente determinado e

$$b = qa + r, \text{ com } 0 \leq r < a$$

□

Uma das importantes consequências do algoritmo da divisão é saber que, ao dividirmos um inteiro b por um inteiro a, $a \neq 0$, o resto r dessa divisão pertence ao conjunto $\{0, 1, 2, 3, ..., a-1\}$. Estudando o caso em que $a = 2$, temos que o resto r da divisão de b por a será 0 ou 1. Se $r = 0$, temos que $b = 2 \cdot q$, com q inteiro e, nesse caso, dizemos que b é um número par. Se $r = 1$, escrevemos $b = 2 \cdot q + 1$, com q inteiro e, nesse caso, dizemos que b é um número ímpar. Tal análise permite-nos generalizar e dizer que todo inteiro b pode ser expresso na forma $2 \cdot q$ ou $2 \cdot q + 1$, com $q \in \mathbb{Z}$. Analogamente, no caso em que $a = 3$, temos que b será da forma $3 \cdot q$, $3 \cdot q + 1$ ou $3 \cdot q + 2$, com q inteiro.

A seguir, estudaremos um importante resultado conhecido como lema dos restos.

Lema 1 (Lema dos restos)**.** *A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, respectivamente, na divisão por um inteiro a, $a \neq 0$.*

Demonstração. Sejam n_1 e $n_2 \in \mathbb{Z}$. Ao fazermos a divisão com resto desses dois números por a, teremos:

$$n_1 = aq_1 + r_1 \text{ e } n_2 = aq_2 + r_2$$

em que $0 \leq r_1, r_2 < a$. Daí, teremos:

$$\begin{aligned} n_1 n_2 &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 \\ &= aq + r_1 r_2 \end{aligned} \tag{7.1}$$

onde consideraremos $q \in \mathbb{Z}$ e $q = aq_1q_2 + q_1r_2 + q_2r_1$. Mais ainda, ao dividirmos r_1r_2 por a, teremos:

$$r_1 r_2 = ap + r, \quad p \in \mathbb{Z}, \quad 0 \leq r < a \tag{7.2}$$

Daí, de (7.1) e (7.2), concluí-se que

$$n_1 n_2 = aq + ap + r = a(p+q) + r,\ 0 \leq r < a$$

□

A demonstração para a soma é muito simples e tem procedimento análogo ao anterior, ficando, portanto, como exercício.

Exemplo 8. *Qual é o resto da divisão de* 3^{250} *por* 4*?*

Solução 3. *Note que, ao dividirmos* $3^2 = 9$ *por* 4*, o resto será* 1*. Como* $3^{250} = (3^2)^{125}$*, temos, pelo lema dos restos, que o resto da divisão de* 3^{250} *por* 4 *será igual ao produto* $\underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdots 1}_{125\, fatores} = 1$.

Exemplo 9. *Qual é o resto da divisão de* $3^{100} + 5^{45}$ *por* 2*?*

Solução 4. *Inicialmente, note que o resto da divisão de* 3 *por* 2*, é* 1*. Portanto, pelo lema do resto, temos que o resto da divisão de* 3^{100} *por* 2 *será igual a* $1^{100} = 1$*. Por outro lado, o resto da divisão de* 5 *por* 2 *também é igual a* 1*; sendo assim, o resto da divisão de* 5^{45} *por* 2 *será igual a* $1^{45} = 1$ *e, consequentemente, o resto da divisão de* 3^{100} + 5^{45} *por* 2 *será* $1 + 1 = 2$*. É claro que, cfomo o divisor é* 2*, o resto será, portanto, igual a* 0*!*

7.1.3 Números primos

Agora, vamos estudar um tema que há bastante tempo tem sido objeto de estudo de vários matemáticos: os números primos.

Definição 3. ***Número primo***. *Um número inteiro $p > 1$ é dito primo se possui apenas dois divisores positivos:* 1 *e p. São exemplos de números primos, os números* 5*,* 17*,* 19*,* 71*, etc. Quando um número inteiro positivo não é primo, ele é chamado de número composto.*

A aplicabilidade dos números primos no nosso cotidiano é vasta. Por exemplo, podemos citar o método de criptografia (conjunto de regras que visa codificar informações) RSA, um sistema criado pelos matemáticos Ron Rivest, Adi Shamir e Leonard Adleman na década de 70, que permite a segurança do uso de cartões de crédito, criando números primos de até 100 dígitos. Hoje em dia, já são usados números primos com 600 dígitos, objetivando uma maior segurança.

Teorema 2 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou pode ser escrito de forma única, como produto de números primos.*

Demonstração. Seja n um número inteiro tal que $n > 1$. Mais ainda, seja p_1 o menor entre os divisores de n diferentes de 1. Temos assim que p_1 é primo ou composto. Suponhamos que p_1 seja composto. Daí, existirá um inteiro d, $1 < d < p_1$, de forma que $d|p_1$. Ora, como $d|p_1$ e $p_1|n$, concluímos, pela propriedade 1 estudada na discussão sobre divisibilidade, que $d|n$. No entanto, essa conclusão vai contradizer a escolha de p_1. Logo, p_1 é primo. Mas, como $p_1|n$, existe $m_1 \in \mathbb{N}$, tal que $n = p_1 \cdot m_1$. Daí:

- Se $m_1 = 1$, temos $n = p_1$, portanto, n é primo.
- Se $m_1 > 1$, então podemos fazer o mesmo procedimento que fizemos para o valor de n, ou seja, teremos $m_1 = p_2 \cdot m_2$, com p_2 primo e, consequentemente, podemos escrever $n = p_1 \cdot p_2 \cdot m_2$, com $1 \leq m_2 < m_1$ e p_1, p_2 primos.
- Se tivermos $m_2 = 1$, teremos $n = p_1 \cdot p_2$ e, assim, terminaríamos a prova.
- Se $m_2 > 1$, de maneira análoga, podemos decompor m_2 assim como fizemos com m_1.

Dando continuidade a esse procedimento, obtemos números primos $p_1, p_2, p_3, ..., p_i$ e uma sequência de números naturais $m_1 > m_2 > m_3 > ... > m_i \geq 1$, de forma que, sempre que $m_i > 1$, podemos continuar a decomposição de n. Ora, como entre 1 e n existe uma quantidade finita de números naturais, haverá, na decomposição de n, um último passo, no qual teremos $m_j = 1$ e, portanto:

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_j, \text{ com } p_1, p_2, p_3, ..., p_j \text{ primos.}$$

□

Exemplo 10. *Notemos que* $18 = 3 \cdot 3 \cdot 2 = 3^2 \cdot 2$, $40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$ *e* $800 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 2^4 \cdot 3 \cdot 5^2 \cdot 7$

Uma importante consequência do Teorema Fundamental da Aritmética está no fato de descobrirmos a quantidade de divisores positivos de um número natural n. Representando por $d(n)$ o número de divisores positivos de n, e sendo $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde $p_1, p_2, \cdots, p_k$ são primos e $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$, então:

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

De fato, todos os divisores de n serão da forma $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, com $r_1 \in \{0, 1, ..., \alpha_1\}$, que é um conjunto que possui, obviamente, $\alpha_1 + 1$ elementos. Por outro lado, temos que $r_2 \in \{0, 1, ..., \alpha_2\}$, que por sua vez, possui $\alpha_2 + 1$ elementos e assim por diante. Portanto, é fácil ver, pelo Princípio Multiplicativo, que o número de divisores positivos, $d(n)$, do natural n será dado pela expressão vista anteriormente.

Exemplo 11. *Encontrar o número de divisores positivos do número* 80.

Solução 5. *Temos que* $80 = 2^4 \cdot 5$. *Daí, é fácil ver que* $D(80) = (4+1) \cdot (1+1) = 5 \cdot 2 = 10$.

Teorema 3. *O conjunto dos números primos é infinito.*

Demonstração. Suponhamos que exista um primo p_n tal que p_n seja o maior número primo. Seja $n \in \mathbb{N}$ tal que $n = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$, onde $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. Logo, como $n > 1$, pelo Teorema Fundamental da Aritmética, existe pelo menos algum primo p, tal que $p|n$. No entanto, como $p_1, p_2, p_3, p_4, ..., p_n$ são, por hipótese, os únicos primos, concluímos que $p|p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_n$. Daí, pela propriedade 4 estudada na discussão sobre divisibilidade, temos que $p|1$, o que é absurdo, pois o único inteiro positivo divisor de 1 é ele mesmo. Portanto, qualquer que seja o primo p_n, existirá sempre um outro primo p_m tal que $p_m > p_n$, a partir do que concluímos que a quantidade de primos é infinita. □

Dando prosseguimento, veremos uma proposição que servirá para estudarmos um importante procedimento, conhecido como Crivo de Eratóstenes, procedimento esse utilizado para descobrir se um número positivo inteiro é primo.

Proposição 1. *Seja n um número natural maior que 1. Se n é um número composto, temos então que o menor divisor, diferente de* 1*, de n é* $\leq \sqrt{n}$*, isto é, se os divisores de n, diferentes de* 1*, forem maiores que* $\sqrt{n}$*, então n é primo.*

Demonstração. Com efeito, seja p o menor divisor de n, diferente de 1. Temos então que $n = pq$, com $q \geq p$. Se multiplicarmos cada membro da desigualdade por p, o resultado será:

$$n = pq \geq p^2,$$

daí, segue que $\sqrt{n} \geq p$. □

O crivo de Eratóstenes - Trata-se de um algoritmo criado pelo matemático grego Eratóstenes (285 - 194 a.C) cujo objetivo é encontrar, até determinado número n inteiro positivo dado, quais são os números primos menores ou iguais a ele. De acordo com esse algoritmo, inicialmente lista-se numa tabela todos os inteiros positivos ordenadamente, a partir de 2, até o n, isto é,

$$2, 3, 4, , 5, 6, 7, 8, 9, ..., n$$

Após isso, marca-se com um X o primeiro número primo da tabela, no caso o 2 e em seguida circula-se todos os múltiplos de 2 da tabela por serem todos eles compostos. O primeiro número que não foi circulado, após o 2, foi o 3, que é próximo número primo da tabela. Daí, o procedimento prossegue , ou seja, marca-se com um X o número 3 e circula-se todos os múltiplos de 3 da tabela. O processo será repetido até que o primeiro número não circulado na tabela seja maior que $\sqrt{n}$, devido à **Proposição 1**. A partir daí, todos os números restantes são os primos menores ou iguais a n.

Um dos problemas mais famosos relacionados aos números primos e que ainda não foi provado, sendo portanto ainda uma conjectura, é chamado de Conjectura de Goldbach. Em 1742, o matemático Christian Goldbach enviou uma carta para outro matemático, cujo nome era Leonhard Euler. Nessa carta, Goldbach afirmava que todo número natural par, maior ou igual a 4, podia ser expresso como a soma de dois números primos. Vejamos alguns exemplos:

$$4 = 2+2,\ 22 = 19+3,\ 70 = 59+11.$$

Outro importante matemático, Pierre de Fermat $(1601-1665)$, fascinado pela beleza dos números primos, tentou criar uma fórmula através da qual pudéssemos encontrar qualquer número primo. Tal busca levou Fermat a conjecturar que são primos todos os números F_n, da forma:

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

sendo n um inteiro não-negativo.

Fermat conseguiu verificar a veracidade de tal conjectura para os seguintes casos:

$n = 0 \Rightarrow F_o = 2^{2^0}+1 = 3$
$n = 1 \Rightarrow F_1 = 2^{2^1}+1 = 5$
$n = 2 \Rightarrow F_2 = 2^{2^2}+1 = 17$
$n = 3 \Rightarrow F_3 = 2^{2^3}+1 = 257$
$n = 4 \Rightarrow F_4 = 2^{2^4}+1 = 65537$

O números acima são chamados de Primos de Fermat. O problema é que a partir de $n \geq 5$, Fermat conjecturou que todos os próximos números seriam primos. Porém, outro grande matemático citado anteriormente, Leonhard Euler $(1707-1783)$, mostrou que, para o caso $n = 5$, o número obtido é composto. De fato,

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641.6700417,$$

que é, consequentemente, um número composto.

7.1.4 Máximo divisor comum - MDC

Considere todos os divisores positivos dos números 36 e 42:

$$D(36) = \{1,2,3,4,6,9,12,18,36\} \text{ e } D(42) = \{1,2,3,6,7,14,21,42\}$$

Note que o maior número que é divisor de 36 e 42, ao mesmo tempo, é 6. Dizemos que 6 é o máximo divisor comum de 36 e 42 e escrevemos $(32,42) = 6$.

Definição 4. *Sejam $a,b \in \mathbb{Z}$ com pelo menos um deles diferente de zero. O máximo divisor comum de a e b (MDC) é um inteiro positivo d tal que d é o maior dentre os divisores positivos comuns de a e b. Escrevemos $(a,b) = d$. Se $(a,b) = 1$, dizemos que a e b são primos entre si.*

É fácil ver que, sendo $a \in \mathbb{Z}$, temos que $(a,0) = |a|$,$(a,1) = 1$ e que $(a,a) = |a|$. As proposições a seguir são de grande importância na teoria dos números, em especial para o cálculo do MDC de números inteiros.

Proposição 2. *Sejam a e b dois inteiros, com pelo menos um deles diferente de zero. As seguintes afirmações são válidas:*

(i) Se a é múltiplo de b, então $(a,b) = |b|, b \neq 0$.

(ii) Se $a = bq + c$, com $c \neq 0$, então o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e c e temos, em particular, que $(a,b) = (b,c)$.

Demonstração. Inicialmente, demonstraremos (i). De fato, se um inteiro pertence ao conjunto dos divisores comuns dos números a e b, então, em particular, ele também é divisor de b. Mas, como b|a, segue que todo divisor de b também é divisor de a. Daí, o conjunto dos divisores comuns de a e b é, portanto, igual ao conjunto dos divisores de b. No entanto, como o maior inteiro que divide b é ele mesmo, concluímos que (a,b) = b.

Para provarmos (ii), utilizaremos a propriedade 4 estudada no tópico de Divisibilidade. Baseados nela, temos que todo divisor comum de a e b também é divisor de c e, portanto, divisor de b e c. Por outro lado, todo divisor comum de b e c também é divisor de a e, assim, também é um divisor de a. Logo, os divisores comuns dos inteiros a e b também são os mesmos que os divisores comuns dos inteiros b e c o que resulta que $(a,b) = (b,c)$.

□

Exemplo 12. *Sejam* $a = 15$ *e* $b = 5$. *De* (i), *temos que* $(15,5) = 5$

Exemplo 13. *Sendo* $a = 28$ *e* $b = 8$, *temos* $28 = 3 \cdot 8 + 4$. *Logo, por* (ii), *concluímos que* $(28,8) = (8,4) = 4$.

Teorema 4 (Algoritmo de Euclides)**.** *Dados dois inteiros positivos a e b, considere as divisões sucessivas, para obtermos:*

$$\begin{array}{rcrcrcl}
a &=& bq &+& r, & & 0<r<b \\
b &=& rq_1 &+& r_1, & & 0<r_1<r \\
r &=& r_1q_2 &+& r_2, & & 0<r_2<r_1 \\
r_1 &=& r_2q_3 &+& r_3, & & 0<r_3<r_2 \\
\vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
r_k &=& r_{k+1}q_{k+2} &+& r_{k+2}, & & 0<r_{k+2}<r_{k+1} \\
r_{k+1} &=& r_{k+2}q_{k+3} & & & &
\end{array}$$

até algum r_{k+2} *dividir* r_{k+1}. *Assim, temos que* $(a,b) = r_{k+2}$, *que é o último resto não-nulo das divisões sucessivas anteriores.*

Demonstração. É fácil ver que processo de divisões sucessivas descritos acima é finito. De fato, pelo algoritmo da divisão, temos que $b > r_0 > r_1 >$

$r_2 > ...$, e, se essa sequência de restos não fosse finita, em algum momento teríamos um resto negativo, o que é absurdo. Mais ainda, analisando as igualdades de cima para baixo, como também utilizando a **Proposição 2**, concluímos que:

$$(a,b) = (b,r_0) = (r_0,r_1) = \cdots = (r_{k+1},r_{k+2}) = r_{k+2}$$

□

Exemplo 14. *Calcular* $(1320,35)$.

Solução 6. *Baseados no algoritmo de Euclides, tal cálculo será realizado da seguinte forma:*

1320	35	35	25	25	10	10	5
25	37	10	1	5	2	0	2

Ou seja,

$$\begin{aligned} 1320 &= 35 \cdot 37 + 25 \\ 35 &= 25 \cdot 1 + 10 \\ 25 &= 10 \cdot 2 + 5 \\ 10 &= 5 \cdot 2 \end{aligned}$$

A partir dos resultados acima, temos que $(1320,35) = (35,25) = (25,10) = (10,5) = (5,0) = 5$. *Daí,* $(1320,35) = 5$. *Esse método é chamado de divisões sucessivas. Uma forma de representarmos as divisões sucessivas é usando uma grade conforme ilustrada abaixo para o cálculo de* $(1320,35)$. *Utilizando esse mecanismo,* $(1320,35)$ *será o último resto, no caso, igual a* 5.

Exemplo 15. *Vejamos outro exemplo. Calculemos* $(60,42)$. *Utilizando o método descrito acima, temos:*

	37	1	2	2
1320	35	25	10	5
25	10	5	0	

	1	2	3
60	42	18	6
18	6	0	

Portanto, $(60,42) = 6$. *Note que, a partir desses dados, podemos escrever:*

$$18 = 60 - 42 \cdot 1 \tag{7.1}$$
$$6 = 42 - 18 \cdot 2 \tag{7.2}$$

Substituindo (7.1) *em* $(7,2)$*, teremos:*

$$\begin{aligned} 6 &= 42 - (60 - 42 \cdot 1) \cdot 2 \\ 6 &= 42 - 60 \cdot 2 + 42 \cdot 2 \\ 6 &= 42 \cdot 3 - 60 \cdot 2 \\ 6 &= 60 \cdot (-2) + 42 \cdot 3. \end{aligned}$$

Nesse último exemplo, o fato $(60,42) = 60 \cdot (-2) + 42 \cdot 3$ será generalizado a seguir.

Teorema 5 (Teorema de Bachet-Bézout)**.** *Seja* $d = (a,b)$*. Então, existem inteiros* x *e* y *de forma que:*

$$d = ax + by.$$

Demonstração. Com efeito, considere o conjunto $C = \{ax + by, \text{com } x,y \in \mathbb{Z}\}$ e $n = ax_0 + by_0$ o menor elemento de C. Suponhamos, por absurdo, que $n \nmid a$. Pelo algoritmo da divisão, temos que $a = nq + r$, com $0 < r < n$. Daí, $r = a - nq$.

Substituindo o valor de n nessa última equação, teremos $r = a - (ax_0 + by_0)q = a - ax_0q - by_0q = a(1 - x_0q) + b(-y_0q)$, ou seja, $r \in C$. Mas, como $r < n$, esse fato contraria a hipótese de n ser o menor elemento de C. Portanto, $n|a$. De forma análoga, podemos provar que $n|b$. Sendo assim, n é divisor comum de a e b. Agora, resta-nos mostrar que $n = d$. De fato, como $d|a$ e $d|b$, podemos escrever $a = dq_1$ e $b = dq_2$. Como $n = ax_0 + by_0$, temos então, $n = (dq_1)x_0 + (dq_2)y_0$, mais ainda, $n = d(q_1x_0 + q_2y_0)$, e daí concluímos que $d|n$. Como $d = (a,b)$, segue que $d = n$. □

Uma consequência importante desse Teorema é a proposição abaixo.

Proposição 3. *Dados a,b inteiros com pelo menos um deles diferente de zero, se existirem inteiros r,s tais que $1 = ra + sb$, então $(a,b) = 1$.*

Demonstração. De fato, sendo $d = (a,b)$, temos que $d|ra$ e $d|sb$, portanto $d|(ra + sb)$. Daí, temos que $d|1$. Logo, $d = 1$. □

Uma outra proposição importante é a que veremos a seguir.

Proposição 4. *Dados a, b e c inteiros não nulos, então $(a,b,c) = \big((a,b),c\big)$.*

Demonstração. Com efeito, sejam $(a,b) = d$, $(a,b,c) = d_1$, $\big((a,b),c\big) = d_2$. Daí, temos que $d_2|c$ e $d_2|d$. Mas, como $d|a$ e $d|b$, concluímos que d_2 divide a,b e c. Portanto, $d_2 \leq d_1$. No entanto, como d_1 divide a,b e c, temos que, em particular, $d_1|a$ e $d_1|b$, logo $d_1|d$. Daí, segue que d_1 divide d e c, donde seque que $d_1|d_2$ e, portanto, $d_1 \leq d_2$. Enfim, $d_1 = d_2$, como queríamos mostrar. □

Exemplo 16. *Calcular* $(24,18,12)$.

Solução 7. *Deixaremos a solução a cargo do leitor.*

Proposição 5. *Sejam $b_1,b_2,b_3,...,b_n$ inteiros com pelo menos um diferente de zero, temos que $(b_1,b_2,b_3,...,b_n)$ será o produto de todas as potências p^s, tal que p pertence ao conjunto de todos os primos que dividem simultaneamente $b_1,b_2,b_3,...,b_n$, e s é o menor expoente de p de forma que p^s divide, ao mesmo tempo, $b_1,b_2,b_3,...,b_n$.*

Exemplo 17. *Calcular* $(24, 18, 12)$.

Solução 8. *Notemos que* $24 = 2^3 \cdot 3$, $18 = 2 \cdot 3^2$ *e* $6 = 2 \cdot 3$. *Note que os primos* 2 *e* 3 *dividem simultaneamente* 24, 18 *e* 6. *Mais ainda, o menor expoente de tanto do* 2 *quanto do* 3, *é* 1. *Portanto,* $(24, 18, 6) = 2^1 \cdot 3^1 = 6$.

Proposição 6. *Sejam a e b inteiros não nulos. Se* $a|bc$ *e* $(a,b) = 1$, *então* $a|c$.

Demonstração. De fato, pela Proposição 5, podemos escrever $ra + sb = 1$, com r, s inteiros. Multiplicando cada membro dessa igualdade por c, teremos:

$$a(rc) + s(bc) = c$$

Como $a|a(rc)$ e $a|s(bc)$, segue, pela propriedade 4 da divisibilidade, que $a|c$.

□

7.1.5 Menor múltiplo comum - MMC

Suponhamos que, no alto de uma torre de uma emissora de televisão, duas luzes piscam com frequências diferentes. A primeira pisca 15 vezes por minuto e a segunda pisca 10 vezes por minuto. Se num certo instante as luzes piscam simultaneamente, após quantos segundos elas voltarão a piscar simultaneamente? Para resolvermos esse problema de uma maneira muito prática, estudaremos o conceito de MMC (menor múltiplo comum).

Definição 5. *Sejam a e b inteiros não nulos. Chamamos de menor múltiplo comum de a e b, e indicamos por* $[a,b]$, *o inteiro positivo m tal que m é o menor número que é divisível por a e b ao mesmo tempo.*

Exemplo 18. $M(24) = \{24, 48, 72, 96, 120, 144, ...\}$ *e*
$M(30) = \{30, 60, 90, 120, 150, ...\}$.

Notemos que 120 é o menor número da lista que é divisível ao mesmo tempo por 24 e 30, ou seja, é o menor número inteiro positivo que é múltiplo ao mesmo tempo de 24 e 30. Portanto, $[24,30] = 120$.

Um método bastante prático para o cálculo do mmc de dois inteiros dados será visto a seguir, utilizando a decomposição em fatores primos, assim como foi feito para o MDC. Para utilizar esse método, considere $b_1, b_2, b_3, ..., b_n$ inteiros não nulos. Decompondo em fatores primos cada número desse, temos que $[b_2, b_3, ..., b_n]$ será o produto de todos os fatores primos, comuns e não-comuns a eles, cada um elevado ao maior expoente que aparece "acompanhando" cada um dos fatores primos. É claro que se algum b_i, $i \in \{1,2,3,...,n\}$ é negativo, basta decompor $|b_i|$.

Exemplo 19. *Calcular* $[18,24,30]$. *Temos que* $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$ *e* $30 = 2 \cdot 3 \cdot 5$. *Daí,* $[18,24,30] = 2^3 \cdot 3^2 \cdot 5 = 360$.

Esse resultado também poderia ser obtido através do método que consiste em colocar os três números um ao lado do outro, separados por vírgulas e com uma barra vertical a sua direita, assim realizando as divisões sucessivas. Abaixo de cada número, colocamos o quociente da divisão de cada um deles pelo menor primo que divide pelo menos um deles. Se algum deles não for divisível por esse primo, ele é repetido na linha seguinte. O procedimento termina quando todos os quocientes forem iguais a 1. O MMC será o resultado do produto dos fatores primos.

18,	24,	30	2
9,	12,	15	2
9,	6,	15	2
9	3,	15	3
3,	1,	5	3
1,	1,	5	5
1,	1,	1	

Agora, vejamos uma situação bastante interessante. Já vimos anteriormente que $[24,30] = 120$. É trivial encontrarmos que $(24,30) = 6$. Efetuando $[24,30] \cdot (24,30)$, teremos:

$$[24,30] \cdot (24,30) = 120 \cdot 6 = 24 \cdot 30$$

Será que isso sempre será verdade? Veremos mais adiante um teorema importante que generaliza esse fato. Mas, antes, estudaremos dois lemas que fundamentarão a prova desse teorema.

Lema 2. *Sejam a e b inteiros não nulos e $(a,b) = d$. Sendo $a = dm_1$ e $b = dm_2$, então $(m_1, m_2) = 1$.*

Demonstração. Suponhamos que $(m_1, m_2) = k$, tal que $k > 1$. Sendo assim, teremos:

- $m_1 = k \cdot n_1 \Rightarrow a = d \cdot kn_1 \Rightarrow d \cdot k | a$
- $m_2 = k \cdot n_2 \Rightarrow b = d \cdot kn_2 \Rightarrow d \cdot k | b$

Daí, concluímos que $d \cdot k$ é um divisor comum de a e b. Logo, como por hipótese $k > 1$, teremos $d \cdot k > d$, o que é absurdo, pois d é o maior divisor comum de a e b. Portanto, $(m_1, m_2) = 1$.

□

Lema 3. *Sejam a e b inteiros não nulos e $[a,b] = m$. Sendo $m = ak_1$ e $m = bk_2$, então $(k_1, k_2) = 1$.*

Demonstração. Suponhamos que $(k_1, k_2) = l$, tal que $l > 1$. Sendo assim, teremos:

- $k_1 = l \cdot r_1 \Rightarrow m = a \cdot l \cdot r_1$
- $k_2 = l \cdot r_2 \Rightarrow m = b \cdot l \cdot r_2$

Das duas igualdades acima, concluímos que

$$a \cdot l \cdot r_1 = b \cdot l \cdot r_2 \Rightarrow a \cdot r_1 = b \cdot r_2$$

Se $m_1 = a \cdot r_1 = b \cdot r_2$, temos $m_1 < m$. Como m_1 é um múltiplo comum de a e b e menor que m, chegamos a um absurdo, pois $[a,b] = m$. Portanto, $(k_1, k_2) = 1$. □

Agora, vejamos o seguinte teorema:

Teorema 6. *Sejam a e b inteiros não nulos. Então* $(a,b)\cdot[a,b] = a\cdot b$.

Demonstração. Seja $(a,b) = d$. Então:

- $a = d\cdot h_1$
- $b = d\cdot h_2$

Daí, pelo **Lema 2**, temos que $(h_1,h_2) = 1$. Sejam também $[a,b] = m$. Temos que:

- $m = a\cdot\alpha_1$ e
- $m = b\cdot\alpha_2$

Sendo assim, pelo **Lema 3**, temos $(\alpha_1,\alpha_2) = 1$. Podemos escrever, então:

- $m = a\cdot\alpha_1 = d\cdot h_1\cdot\alpha_1$
- $m = b\cdot\alpha_2 = d\cdot h_2\cdot\alpha_2$

Daí, temos que $d\cdot h_1\cdot\alpha_1 = d\cdot h_2\cdot\alpha_2 \Rightarrow h_1\cdot\alpha_1 = h_2\cdot\alpha_2$. Portanto, $h_1|h_2\cdot\alpha_2$. Mas, como $(h_1,h_2) = 1$, só nos resta concluir que $h_1|\alpha_2$. Analogamente, temos $h_2|h_1\cdot\alpha_1$. No entanto, como já foi visto antes, $(h_1,h_2) = 1$. Concluímos que $h_2|\alpha_1$. Utilizando a mesma argumentação, chegaremos a conclusão que $\alpha_2|h_1$ e que $\alpha_1|h_2$ e, consequentemente:

- $h_1 = \alpha_2$; e que
- $h_2 = \alpha_1$

Por fim, teremos:

$$a\cdot b = d\cdot h_1\cdot d\cdot h_2 = d^2\cdot\alpha_1\cdot\alpha_2 = d^2\frac{m}{a}\cdot\frac{m}{b} = \frac{d^2\cdot m^2}{a\cdot b} \Rightarrow a^2\cdot b^2 = d^2\cdot m^2$$

Ou seja, $ab = dm$, como queríamos demonstrar. □

Observação: uma importante consequência desse fato é que, sendo a e b inteiros não nulos e primos entre si, ou seja, $(a,b) = 1$, teremos: q

$$(a,b) \cdot [a,b] = a \cdot b \Rightarrow [a,b] = a \cdot b$$

.

7.1.6 Equações diofantinas

Suponhamos a seguinte situação: Pedro deseja comprar selos de 5 reais e de 3 reais e, para isso, quer gastar exatamente 50 reais. De quantas maneiras ele pode fazer essa compra?

Para resolvermos o problema acima, chamemos de x e y a quantidade de selos de 5 reais e 3 reais, respectivamente. Então, chegaremos a seguinte equação:

$$5x + 3y = 50 \,,$$

na qual devemos encontrar x e y inteiros positivos.

A equação encontrada é um exemplo do que chamamos de equação diofantina e será objeto de estudo nessa aula. O nome diofantina é uma homenagem ao matemático grego Diofanto (214 - 299) considerado por muitos como o "pai da Álgebra". Sua obra *Arithmetica*, que foi escrita por volta de 250 d.C, já traz referências a esses tipos de equações e como resolvê-las.

Definição 6 (Equação Diofantina)**.** *Chamamos de Equação Diofantina, toda equação da forma:*

$$ax + by = c, \;\; com \;\; a,b,c \in \mathbb{Z} \;\; e \; a,b \neq 0$$

Na equação $5x + 3y = 50$, temos $a = 5$, $b = 3$ e $c = 50$. Vejamos mais exemplos de equações diofantinas:

- $3x + y = 100$
- $4x + 6y = 9$

Proposição 7. *A equação diofantina*

$$ax+by=c, \ \ com \ \ a,b,c\in\mathbb{Z} \ \ e \ a,b\neq 0$$

possui solução se, e somente se, $(a,b)=d|c$. *Mais ainda, se o par* (x_0,y_0) *é uma solução dessa equação, temos que o conjunto dessa equação será formada por todos os pares de inteiros* (x,y) *da forma:*

$$x=x_0+t\frac{b}{d} \quad e \quad y=y_0-t\frac{a}{d}, \quad emque \quad t\in\mathbb{Z}$$

Demonstração. Suponhamos, por hipótese, que o par (x_0,y_0) seja uma solução da equação. Logo, teremos $ax_0+by_0=c$. Mas, como $d|a$ e $d|b$, temos que $d|c$, pela propriedade 6 estudada na seção de divisibilidade.

Da mesma forma, se $d|c$, existe $q\in\mathbb{Z}$ de forma que $c=qd$. No entanto, pelo Teorema de Bézout, existem dois inteiros x_0 e y_0 tais que $ax_0+by_0=d$. Daí, multiplicando os dois membros dessa última igualdade por q, teremos:

$$aqx_0+bqy_0=dq=c$$

Portanto, o par (x_1,y_1), com $x_1=x_0q$ e $y_1=y_0q$ é solução da equação difantina inicial.

Agora, considerando a solução (x_0,y_0) e seja o par (x,y) uma outra solução da equação difantina. Sendo assim, $ax_0+by_0=ax+by$. Então:

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

e, dividindo essa última igualdade por d, teremos:

$$\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$$

mas, como $(\frac{a}{d},\frac{b}{d})=1$, pelo lema 2 concluímos que $\frac{a}{d}|(y_0-y)$ e $(\frac{b}{d}|(x-x_0)$. Portanto, existe $t\in\mathbb{Z}$ tal que:

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

□

Em termos de solução de uma equação diofantina, só existem duas possibilidades: ou ela não possui soluções ou possui infinitas soluções.

Exemplo 20. *Resolver a equação* $15x + 10y = 20$.

Solução 9. *Inicialmente, observemos que* $(15, 10) = 5$ *e que* $5|20$. *Logo, é garantido que essa equação possui solução. Vamos encontrar uma particular e, assim, encontrar a solução geral. Utilizando o algoritmo de Euclides para calcular* $(15, 10)$, *encontraremos as seguintes igualdades:*

$$\begin{aligned} 15 &= 10 \cdot 1 + 5, \\ 10 &= 5 \cdot 2 + 0. \end{aligned}$$

Daí, temos que $5 = 15 \cdot 1 - 10 \cdot 1$. *Multiplicando essa igualdade por* 4, *teremos,* $20 = 15 \cdot 4 + 10 \cdot (-4)$. *Portanto,* $x_0 = 4$ *e* $y_0 = -4$ *são soluções particulares dessa equação e a solução geral dessa equação será:*

$$x = 4 + t\frac{10}{5} = 4 + 2t \quad e \quad y = -4 - \frac{15}{5}t = -4 - 3t$$

Para $t = 2$, *por exemplo, teremos* $x = 4 + 2 \cdot 2 = 8$ *e* $y = -4 - 3 \cdot 2 = -10$. *De fato,* $15 \cdot 8 + 10 \cdot (-10) = 120 - 100 = 20$.

Exemplo 21. *Resolver a equação* $5x + 3y = 50$.

Solução 10. *Pelo algoritmo de Euclides, temos:*

$$\begin{aligned} 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 1 + 1. \end{aligned} \tag{7.3}$$

Da primeira e segunda igualdade, temos

$$1 = 3 - 2 \cdot 1 \;\; e \;\; 2 = 5 - 3 \cdot 1$$

Usando essas duas últimas, vamos obter:

$$\begin{aligned} 1 &= 3-2\cdot 1 \\ &= 3-(5-3\cdot 1)\cdot 1 \\ &= 5\cdot(-1)+3\cdot(2) \end{aligned} \tag{7.4}$$

mas, multiplicando por 50 essa última igualdade, teremos

$$5\cdot(-50)+3\cdot(100)=50$$

e daí, temos $x_0=-50$ *e* $y_0=100$*, soluções particulares dessa equação, donde concluímos que a solução geral será, para* $t\in\mathbb{Z}$*:*

$$x=-50+3t \quad e \quad y=100-5t$$

.

Essa equação desse último exemplo é referente ao problema exposto no início desse tópico. Pela natureza do problema, as soluções devem ser naturais. Deixaremos a cargo do leitor encontrá-las.

7.1.7 Congruências

O estudo da aritmética modular introduz o conceito de congruências, linguagem que foi desenvolvida por Karl Friedrich Gauss no início do século XIX e faz parte da Teoria dos Números.

Definição 7 (**Aritmética Modular**)**.** *A aritmética modular é um sistema em que as operações entre números inteiros são feitas em módulo, um outro inteiro n, positivo e diferente de zero. Para isso, definimos que um inteiro a é congruente a outro inteiro b módulo m,* $m\in\mathbb{Z}$*,* $m>1$*, se a divisão de a e b por m deixam o mesmo resto. Indica-se* $a\equiv b\ (mod\ m)$*. Por exemplo,* $9\equiv 5\ (mod\ 4)$*, pois ambos deixam restos* 1 *na divisão por* 4*. Temos também que* $15\equiv 2\ (mod\ 13)$*.*

Proposição 8. *$a \equiv b \ (mod\ n) \Leftrightarrow a - b$ é divisível por m.*

Demonstração. De fato, se a e b deixam o mesmo resto na divisão por m, temos

$$a = mq_1 + r_1 \quad e \quad b = mq_2 + r_2, \ com \ \ 0 \leq r_1 < m \ \ e \ \ 0 \leq r_2 < m$$

mas como, por hipótese, $r_1 = r_2$, temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2)$, donde concluímos que $m|(a-b)$.

Vamos provar agora a outra implicação. Com efeito, temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$. Mas, como $m|(a-b)$ e $m|m(q_1 - q_2)$, concluímos que $m|(r_1 - r_2)$. No entanto, notemos que $-m < r_1 - r_2 < m$. Porém, como $r_1 - r_2$ é um múltiplo de m e, entre $-m$ e m, o único múltiplo de m é 0, concluímos que $r_1 - r_2 = 0$, o que resulta $r_1 = r_2$.

□

As propriedades abaixo serão importantes na resolução de vários exercícios. Sejam a, b, c e m inteiros, $m > 1$ e $n \in \mathbb{N}$, então:

1. $a \equiv a \ (mod\ m)$. (Reflexividade)
2. Se $a \equiv b \ (mod\ m)$, então $b \equiv a \ (mod\ m)$. (Comutatividade)
3. Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$. (Transitividade)
4. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$.
5. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$.
6. Se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$, $c \in \mathbb{N}$.
7. $a + c \equiv b + c \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m)$.

8. Se $ac \equiv bc \ (mod\ m)$ e $(c,m) = 1$, então $a \equiv b \ (mod\ m)$.

9. Se $a \equiv b \ (mod\ m_i), i = 1,2,...,r$, então $a \equiv b \ (mod\ [m_1, m_2, ..., m_r])$.

Demonstração. Vejamos a demonstração de cada uma dessas propriedades:

1 De fato, $m|(a-a)$ para todo $a \in \mathbb{Z}$.

2 Com efeito, se $m|(a-b)$, então $m|(b-a)$.

3 De fato, se $m|(a-b)$ e $m|(b-c)$, então $m|(a-b)+(b-c)$. Daí, $m|(a-c)$, donde concluímos que $a \equiv c \ (mod\ m)$.

4 De fato, se $m|(a-b)$ e $m|(c-d)$, então $m|(a-b)+(c-d) = (a+c)-(b+d)$, o que mostra que $a+c \equiv b+d \ (mod\ m)$.

5 Basta notar que $ac - bd = a(c-d) + d(a-b)$. Portanto, $m|(ac-bd)$. Daí, $ac \equiv bd \ (mod\ m)$.

6 Com efeito, utilizando a propriedade 5 "n"vezes, temos:

$$\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n\,fatores} \equiv \underbrace{b \cdot b \cdot b \cdot b \cdots b}_{n\,fatores} \ (mod\ m),$$

o que mostra que $a^n \equiv b^n \ (mod\ m)$.

7 De fato, se $a+c \equiv b+c \ (mod\ m)$, então $m|(a+c)-(b+c) = (a-b)$, o que mostra que $a \equiv b \ (mod\ m)$.
Por outro lado, sendo $a \equiv b \ (mod\ m)$, temos que $c \equiv c \ (mod\ m)$ e, da propriedade 4, temos que $a+c \equiv b+c \ (mod\ m)$, como queríamos demonstrar.

8 Com efeito, se $ac \equiv bc \ (mod\ m)$, então $m|(ac-bc) = c(a-b)$. No entanto, sendo m e c primos entre si, temos que $m|(a-b)$, o que mostra que $a \equiv b \ (mod\ m)$.

9 Com efeito, como $a \equiv b \ (mod\ m_i), i = 1,2,...,r$, então $m_i|(a-b)$, para todo i. Sendo assim, $(a-b)$ é um múltiplo de cada m_i, donde segue que $[m_1, m_2, ..., m_r]|(a-b)$, como queríamos demonstrar.

□

Exemplo 22. *Qual é o resto da divisão de* $50^{20} + 35^{35}$ *por* 3*?*

Solução 11. *Utilizando as propriedades das congruências estudadas, tal cálculo será bastante simples. Para isso, notemos que* $50 \equiv -1 \ (mod\ 3)$. *Portanto,* $50^{20} \equiv (-1)^{20} \equiv 1 \ (mod\ 3)$. *Temos também que* $35 \equiv -1 \ (mod\ 3)$ *e, portanto,* $35^{35} \equiv (-1)^{35} \equiv -1 \ (mod\ 3)$. *Mas, como* $0 \equiv 3 \ (mod\ 3)$, *utilizando a propriedade 4, teremos* $35^{35} + 0 \equiv -1 + 3 \ (mod\ 3)$, *resultando, portanto, a partir daí, que* $35^{35} \equiv 2 \ (mod\ 3)$. *Mais uma vez, utilizando a propriedade 4, temos que* $50^{20} + 35^{35} \equiv 1 + 2 \equiv 0 \ (mod\ 3)$, *mostrando que o resto da divisão de* $50^{20} + 35^{35}$ *por* 3 *é* 0.

Proposição 9. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Temos que* $(a-b)|(a^n - b^n)$.

Demonstração. De fato, em particular, sendo $m = a - b$, temos $a \equiv b \ (mod\ m)$, pois é claro que $a - b|a - b$. Da propriedade 6, temos $a^n \equiv b^n \ (mod\ m)$, o que prova a proposição. □

Proposição 10. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Então,* $(a+b)|(a^{2n+1} + b^{2n+1})$.

Demonstração. Com efeito, considerando em particular $m = a + b$, temos $a \equiv -b \ (mod\ m)$. Como, para todo $n \in \mathbb{N}$, temos que $2n+1$ é um número ímpar, é fácil ver que $a^{2n+1} \equiv -b^{2n+1} \ (mod\ m)$, o que prova a proposição. □

Proposição 11. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Então, temos que* $(a+b)|(a^{2n} - b^{2n})$.

Demonstração. Mais uma vez, considerando $m = a + b$, verificando que $a \equiv -b \ (mod\ m)$ e que, para todo $n \in \mathbb{N}$, o número $2n$ é par, facilmente observa-se que $a^{2n} \equiv b^{2n} \ (mod\ m)$, como queríamos demonstrar. □

Exemplo 23. *Mostrar que, para todo* $n \in \mathbb{N}$, $11|(10^{2n+1} + 1)$.

Solução 12. *De fato, pela propriedade* 6, $11 = (10+1)|(10^{2n+1} + 1^{2n+1}) = 10^{2n+1} + 1$, *como queríamos demonstrar.*

Definição 8. *Um inteiro a é dito inversível módulo m se existir um outro inteiro* a' *tal que*

$$a \cdot a' \equiv 1 (mod\ m)$$

Por exemplo, 2 *e* 4 *são inversíveis módulo* 7*, pois* $2 \cdot 4 = 8 \cdot \equiv 1\ (mod\ 7)$.

Proposição 12. *Se um inteiro a é inversível módulo m, então* $(a,m) = 1$.

Demonstração. De fato, como por hipótese a é inversível módulo m, temos que:

$$a \cdot a' \equiv 1\ (mod\ m) \Rightarrow aa' = mk + 1 \Rightarrow aa' - mk = 1$$

daí, pelo teorema de Bezout, temos que $(a,m) = 1$. □

7.1.8 Teorema de Euler e Fermat

Definição 9. *Seja* $m \in \mathbb{N}^*$. *Seja* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ *a decomposição de m em fatores. Definimos:*

$$\varphi(m) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_n^{\alpha_n - 1}(p_1 - 1)(p_2 - 1) \cdots (p_n - 1).$$

onde

$$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N},$$

é chamada de função phi de Euler .

Exemplo 24. *Calcular* $\varphi(20)$.

Solução 13. *Como* $20 = 2^2 \cdot 5$*, então* $\varphi(2^2 \cdot 5) = 2^{2-1} \cdot 5^{1-1}(2-1)(5-1) = 8$.

Exemplo 25. *Encontrar* $\varphi(36)$.

Solução 14. *Ora,* $\varphi(36) = \varphi(2^2 \cdot 3^2) = 2^{2-1} \cdot 3^{2-1}(2-1)(3-1) = 12$.

Note que se se p é primo, então $\varphi(p) = p-1$. De fato, pela definição vista, $\varphi(p) = p^{1-1} \cdot (p-1) = p-1$. Por exemplo, $\varphi(23) = 23-1 = 22$.

Teorema 7 (Teorema de Euler)**.** *Sejam $m, a \in \mathbb{N}$ com $m > 1$ e $(a,m) = 1$. Então,*

$$a^{\varphi(m)} \equiv 1 \ (mod\ m)$$

A demonstração desse teorema não será realizada nesse artigo, mas sugerimos aos leitores que a pesquisem.

Exemplo 26. *Qual é o resto da divisão de 5^{61} por 33?*

Solução 15. *Ora, como $(5,33) = 1$, e $\varphi(33) = 3^0 \cdot 11^0(3-1)(11-1) = 20$, pelo Teorema de Euler, $5^{20} \equiv 1 \ (mod\ 33)$. Daí, $5^{61} = 5^{60+1} \equiv (5^{20})^3 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \ (mod\ 33)$, o que mostra que o resto dessa divisão é 5.*

Uma consequência desse Teorema será vista a seguir.

Teorema 8 (Teorema de Fermat)**.** *Seja p um número primo e $a \in \mathbb{Z}$ com $(a,p) = 1$. Então:*

$$a^p \equiv a \ (mod\ p)$$

Demonstração. Como p é primo, $\varphi(p) = p-1$ e, mais ainda, como $p \nmid a$, pelo Teorema de Euler, teremos:

$$a^{\varphi(p)} \equiv 1 \ (mod\ p) \Rightarrow a^{p-1} \equiv 1 \ (mod\ p).$$

Como $a \equiv a \ (mod\ p)$, utilizando as propriedades das congruências, temos:

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

□

Observação: Sendo p primo, $a \in \mathbb{Z}$ com $(a,p) = 1$, concluímos, na demonstração anterior, que

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

Esse resultado é conhecido como **Pequeno Teorema de Fermat**.

Exemplo 27. *Quais são os dois últimos algarismos do número* 3^{121} *?*

Solução 16. *É claro que para descobrirmos esses dois algarismos, precisamos dividir* 3^{121} *por* 100*. Como* $(3,100) = 1$*, uma boa estratégia é utilizarmos o Teorema de Euler. Com um simples cálculo, descobrimos que* $\varphi(100) = 40$ *e, portanto,* $3^{40} \equiv 1 \ (mod \ 100)$*. Daí:*

$$3^{121} = 3^{40 \cdot 3+1} \equiv (3^{40})^3 \cdot 3 \equiv 3 \ (mod \ 100)$$

Porém, fazendo os devidos cálculos, também poderíamos descobrir que o menor inteiro n tal que $3^n \equiv 1 \ (mod \ 100)$ é $n = 20$, ou seja, $3^{20} \equiv 1 \ (mod \ 100)$ (fica a cargo de leitor fazer tal verificação). Dizemos, nesse caso, que 20 é a ordem de 3 com relação a 100. Em notação, $\text{ord}_{100}(3) = 20$. De maneira geral, temos:

Definição 10. *Sejam* $a, m \in \mathbb{N}^*$*, com* $m > 1$ *e* $(a,m) = 1$*. Definimos como a ordem de a com relação a m como sendo o número natural tal que:*

$$ord_m(a) = min\{i \in \mathbb{N}^*; a^i \equiv 1 \ (mod \ m)\}$$

Proposição 13. *Se* $k = ord_m(a)$*, então* $k | \varphi(m)$*.*

Demonstração. De fato, pela divisão euclidiana, podemos escrever:

$$\varphi(m) = kq + r, \text{ com } 0 \leq r < k.$$

daí, supondo, por absurdo, que $r \neq 0$, teremos:

$$1 \equiv a^{\varphi(m)} \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv a^r \ (mod \ m)$$

mas isso é um absurdo, pois supomos $0 < r < k$ e k é o menor expoente não nulo i tal que $a^i \equiv 1 \ (mod \ m)$. □

Exemplo 28. *Mostre que* $18 | 5^{1000} + 5$.

Solução 17. *Inicialmente, notemos que* $(5,8) = 1$. *Daí, podemos utilizar o Teorema de Euler. Temos então que* $\varphi(18) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 6 = 6$. *Portanto,* $5^6 \equiv 1 \ (mod\ 18)$. *No entanto, como* $1000 = 6 \cdot 166 + 4$, *segue que* $5^{1000} \equiv (5^{166})^6 \cdot 5^4 \equiv 1 \cdot 625 \equiv 13 \ (mod\ 18)$. *Portanto,* $5^{100} + 5 \equiv 13 + 5 \equiv 0 \ (mod\ 18)$, *como queríamos mostrar.*

Exemplo 29. *Qual é o resto da divisão de* 4^{110} *por* 23*?*

Solução 18. *Note que* $(4,23) = 1$. *Como* 23 *é primo, pelo Pequeno Teorema de Fermat, temos*

$$4^{23-1} = 4^{22} \equiv 1 \ (mod\ 23) \Rightarrow (4^{22})^5 \equiv 1^5 \ (mod\ 23) \Rightarrow 4^{110} \equiv 1 \ (mod\ 23).$$

Portanto, o resto divisão de 4^{110} *por* 23 *é* 1.

7.2 Considerações finais

Este artigo, acreditamos, contribui com o estudo, conhecimento e aprofundamento de tópicos básicos da Teoria dos Números. A linguagem utilizada é bastante acessível, inclusive para alunos do ensino básico. É importante destacar que esse trabalho foi fundamentado na dissertação de Josemar Claudino Barbosa, sob a orientação da Dra. Bárbara Costa da Silva, cujo título é "Teoria dos Números no Ensino Básico: Um estudo de caso no 2º ano do Ensino Médio". Será possível acessá-lo nas referências bibliográficas desse artigo.

7.3 Referências bibliográficas

BARBOSA, Josemar Claudino. .**Teoria dos números no ensino básico: um estudo de caso no 2º ano do ensino médio**.2017. 130f. Dissertação. Mestrado Profissional em Matemática. Universidade Federal Rural de Pernambuco, Recife.

BISPO, Dinguiston dos Santos.**Equações Diofantinas Lineares e suas**

Aplicações.2013.76 f. Monografia (Licenciatrua em Matemática). Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista.

COSTA, Eduardo S..**Equações Diofantinas Lineares e o Professor do Ensino Médio**. 2007. 119f. Dissertação. Mestrado Acadêmico em Educação Matemática. Pontifícia Universidade Católica de São Paulo, São Paulo.

COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

DIAS, Cristina Helena Bovo Batista.**Números Primos e Divisibilidade: Estudo de Propriedades**. 2013.49f. Dissertação (Mestrado Profissinal em Matemática). Universidade Estadual Paulista, São Paulo.

FOMIM, Dmitri. **Círculos Matemáticos.** Rio de Janeiro: IMPA, 2012.

FONSECA, Rubens.**Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.

noindent HEFEZ, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.

MOREIRA, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números.** Rio de Janeiro: SBM, 2012.

MOREIRA, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª.**1ª ed. Rio de Janeiro: SBM, 2003.

OLIVEIRA, Maycon Costa de.**Aritmética: Criptografia e outras aplicações de Congruências**.2013.74 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Mato Grosso do Sul, Campo Grande.

TAO, Terence.**Como resolver problemas matemáticos - Uma perspectiva pessoal**. Rio de Janeiro: SBM, 2013.