Iniciação à Aritmética

Abramo Hefez

Texto já revisado pela nova ortografia.

Sobre o Autor

Abramo Hefez nasceu no Egito, mas é brasileiro por opção e carioca de coração. Cursou o *ginasial* e *científico* no Rio de Janeiro, graduou-se na PUC-Rio em Matemática e prosseguiu seus estudos na Universidade de Pisa, Itália e nos Estados Unidos, doutorando-se, em Geometria Algébrica no Massachusetts Institute of Technology. É Professor Titular no Instituto de Matemática da Universidade Federal Fluminense, onde exerce docência na graduação e na pós-graduação e desenvolve atividade de pesquisa.

Prefácio

O nosso objeto de estudo neste pequeno livro, aos alunos premiados que participam do Programa de Iniciação Científica da OBMEP, é o conjunto dos números inteiros e algumas de suas propriedades.

Os números inteiros são obtidos estendendo os números naturais e esses são os mais simples de todos os números, mas ao mesmo tempo muito ricos em problemas. Você verá ao longo do texto alguns desses problemas, muito fáceis de enunciar, mas ainda não resolvidos e com certeza se maravilhará de como, apesar do ser humano estar estudando os números naturais há vários milênios, eles ainda encerrem grandes mistérios a serem desvendados.

Nessas notas, além de possivelmente estar vendo pela primeira vez a noção de congruência, você revisitará as noções de múltiplo, de divisor, de número primo, de mínimo múltiplo comum e de máximo divisor comum, e estudará algumas de suas propriedades. Muito provavelmente você ainda não estudou esses conceitos com o grau de formalização que encontrará aqui, mas que ainda não representa o maior rigor possível, pois nos permitiremos fazer deduções por analogia e por indução empírica (isto é, estabelecer regras gerais através

da análise de um número finito de casos). Essas deduções podem se transformar em verdadeiras demonstrações utilizando-se o Princípio de Indução Matemática, que é assunto de um outro texto do autor, publicado nesta coleção e destinado aos alunos do nível III.

Este texto não existiria não fosse o desafio lançado por Suely Druck, Diretora Acadêmica da OBMEP, a quem agradeço calorosamente pela preciosa oportunidade de me dirigir aqui a vocês. Agradeço também ao colega Dinamérico Pombo por sua leitura cuidadosa do manuscrito original.

Finalmente, espero que você aprecie o material aqui apresentado e que faça de seu estudo uma atividade prazerosa. Bom divertimento!

Niterói, março de 2009.

O Autor

Sumário

Capítulo 1

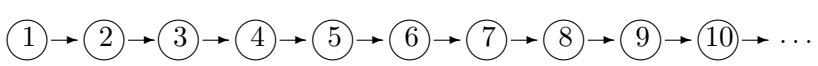
Os Números Naturais

1.1 Os Naturais

Os números naturais formam um conjunto cujos elementos são descritos de modo ordenado como segue:

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ \ldots$$

ou ainda, de modo mais sugestivo:



Essa descrição não é completa, pois só explicitamos alguns poucos de seus elementos, guardando o restante na nossa imaginação.

No entanto, todos nós sabemos perfeitamente do que estamos falando. Tudo começa com o número um, simbolizado por 1, que repre-

senta a *unidade*, e com uma lei, simbolizada pelas flechas, que a cada número, começando pelo 1, fornece o seu sucessor, isto é, o número que lhe segue.

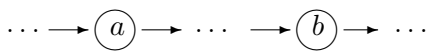
Sabemos também que esta sequência nunca termina; ou seja, os números naturais são em *quantidade infinita*.

Cada elemento desse conjunto tem de ser obviamente representado por um símbolo distinto. Como fazer isto de modo a poder memorizar todos esses símbolos? A resposta, muito engenhosa, é dada pela adoção de um sistema de numeração, que no nosso caso é o sistema decimal posicional, que será descrito no próximo capítulo. Assim, por exemplo, sabemos que nesse sistema sucedendo o 10 vem o 11 e sucedendo o 999 vem o 1 000 etc.

Os números naturais permitem contar objetos, inclusive subconjuntos do próprio conjunto dos naturais. Por exemplo, de 1 a n, inclusive, existem exatamente n números naturais.

1.2 Ordem

Quando um número a aparece na sequência, acima mencionada, *antes* do número b, ou seja, à *esquerda* de b, escrevemos $a < b$ e dizemos que a é *menor* do que b, ou ainda, escrevemos $b > a$ e dizemos que b é *maior* do que a.

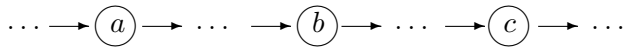


Por exemplo, $1 < 2$, $5 < 7$, $9 > 6$ etc.

Essa relação que ordena os números naturais tem claramente a

seguinte propriedade *transitiva*:

Se a aparece antes de b e b aparece antes de c, então a aparece antes de c.



Em símbolos:

Se $a < b$ e $b < c$, então $a < c$.

Escreveremos também $a \leq b$ para representar a situação:

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

Por exemplo, temos que $2 \leq 3$ e também que $2 \leq 2$.

A ordem nos naturais é *total*, o que significa que dados dois números naturais a e b temos verificada uma e apenas uma das três seguintes possibilidades (*tricotomia*):

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

Sejam dados dois números naturais a e b com $a < b$. Definimos os seguintes conjuntos:

$[a, b]$ o conjunto dos números naturais x tais que $a \leq x \leq b$,

(a, b) o conjunto dos números naturais x tais que $a < x < b$,

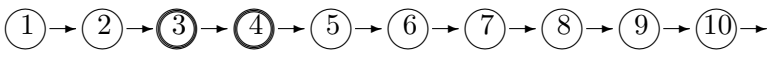
$(a, b]$ o conjunto dos números naturais x tais que $a < x \leq b$,

$[a, b)$ o conjunto dos números naturais x tais que $a \leq x < b$.

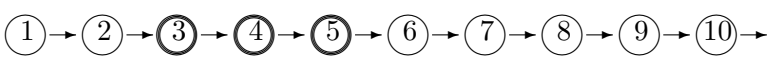
O primeiro e o segundo conjunto são chamados, respectivamente, de *intervalo fechado* e *intervalo aberto*. Os dois outros conjuntos são chamados indiferentemente de intervalos *semiabertos*, ou *semifechados*.

Exemplos:

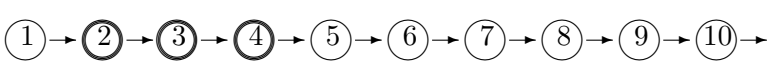
O intervalo $(2, 5) = \{3, 4\}$:



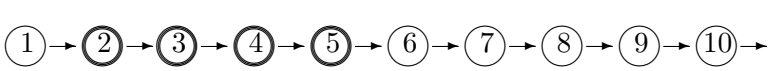
O intervalo $(2, 5] = \{3, 4, 5\}$:



O intervalo $[2, 5) = \{2, 3, 4\}$:



O intervalo $[2, 5] = \{2, 3, 4, 5\}$:



Problema 1.1. Determine os elementos dos seguintes intervalos:

$$(2, 3),\ \ (2, 3],\ \ [2, 3),\ \ [2, 3],\ \ (3, 7),\ \ (3, 7],\ \ [3, 7)\ \ \text{e}\ \ [3, 7].$$

Uma propriedade característica e fundamental do conjunto dos

números naturais, que não procuraremos justificar por parecer tão óbvia, é a seguinte:

Princípio da Boa Ordem. Todo subconjunto não vazio do conjunto dos números naturais possui um *menor elemento*.

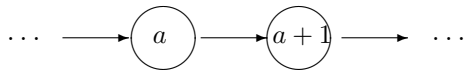
A afirmação acima significa que dado um subconjunto A de $\mathbb{N}$, não vazio, existe um elemento a de A tal que $a \leq b$, para todo elemento b de A.

Problema 1.2. Determine o menor elemento de cada um dos seguintes conjuntos: $[2, 8]$, $(2, 8]$, $(3, 5)$, $(3, 4)$, $[3, 7] \cap [2, 5]$, $[3, 7] \cup [2, 5]$.

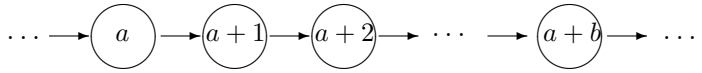
1.3 Adição

Vamos a seguir introduzir a operação básica nos naturais.

Seja dado um número natural a, o sucessor de a será também representado por $a + 1$:



Sejam dados dois números naturais a e b, quaisquer. Podemos deslocar a de b posições para a direita, obtendo um número que será denotado por $a+b$. Essa operação entre números naturais é chamada de *adição* e o número $a + b$ é chamado *soma* de a e b.



Por exemplo, dados $a = 2$ e $b = 3$, ao deslocarmos a de três posições para a direita, obtemos a sequência

$$2, \quad 2+1=3, \quad 3+1=4, \quad 4+1=5,$$

obtendo assim o número $2+3=5$.

Agora, suponha que deslocamos $b = 3$ de $a = 2$ posições para a direita, obtemos

$$3, \quad 3+1=4, \quad 3+2=5,$$

logo, também, $3+2=5$.

Portanto,

$$2+3=3+2=5.$$

Este fato não é uma mera coincidência, ocorre sempre!

Propriedade comutativa da adição. Quaisquer que sejam os números naturais a e b, temos que

$$\boxed{a+b=b+a.}$$

Esse fato, devido à nossa experiência com os números, nos parece óbvio, mas você teria alguma ideia de como mostrar que ao deslocar a para a direita de b posições alcança-se o mesmo número que deslocar b para a direita de a posições?

Vamos agora introduzir um símbolo para representar o não deslocamento de um número. Diremos que deslocamos um número a de

zero posições para a direita quando não o movemos do seu lugar. Escreveremos, neste caso,

$$a + 0 = a.$$

Vamos colocar o símbolo 0, chamado *zero*, à esquerda de todos os números naturais, obtendo o conjunto ordenado:

$$(0) \to (1) \to (2) \to (3) \to (4) \to (5) \to (6) \to (7) \to (8) \to (9) \to \cdots$$

Portanto, consideraremos $0 < a$, para todo número natural a.

Denotaremos o conjunto acima por $\mathbb{N}$, continuando a chamá-lo de conjunto (ampliado) dos números naturais.

Se deslocarmos agora 0 de 1 posição para a direita, obtemos o número 1, se o deslocarmos de 2 posições à direita, obtemos 2, se o deslocarmos de 3 posições à direita obtemos 3. Portanto, é intuitivo aceitar que se deslocarmos 0 de a posições à direita obtemos o número a. Finalmente, é claro que $0 + 0 = 0$, pois ao não deslocarmos o zero nos mantemos no zero. Portanto, para todo a no conjunto $\mathbb{N}$, temos que

$$\boxed{0 + a = a = a + 0.}$$

Assim, quaisquer que sejam a e b no conjunto $\mathbb{N}$ (incluindo agora o elemento 0), temos que $a + b = b + a$.

Podemos estender a soma para uma quantidade de números maior do que dois. Por exemplo, para somar três números a, b e c, podemos

proceder da seguinte forma: somamos inicialmente a e b, formando o número $(a+b)$, depois somamos esse novo número com c, obtendo o número $(a+b)+c$. Por exemplo dados $3, 5$ e 6, formaríamos $3+5=8$ e o somaríamos com 6 obtendo $(3+5)+6=8+6=14$.

Por outro lado, poderíamos somar a com $(b+c)$, obtendo o número $a+(b+c)$. No exemplo acima, isso nos daria $3+(5+6)=3+11=14$.

Acontece que a adição tem também a seguinte propriedade:

Propriedade associativa da adição. Quaisquer que sejam os números a, b e c de $\mathbb{N}$, tem-se

$$\boxed{(a+b)+c=a+(b+c).}$$

Problema 1.3. Utilizando as propriedades comutativa e associativa da adição, mostre que os 12 modos de somar três números a, b e c:

$(a+b)+c,\ a+(b+c),\ (a+c)+b,\ a+(c+b),\ (b+a)+c,\ b+(a+c),$

$(b+c)+a,\ b+(c+a),\ c+(b+a),(c+a)+b,\ c+(a+b),\ (c+b)+a,$

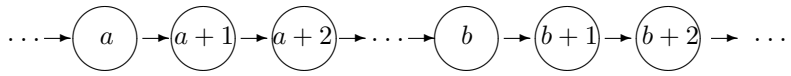
dão o mesmo resultado.

Adição e Ordem. Há uma relação de compatibilidade entre a ordem e a adição de números naturais, que é a seguinte:

Dados três números naturais a, b e c quaisquer,

$$\boxed{\text{se}\quad a<b,\quad \text{então}\ \ a+c<b+c.}$$

De fato, se a está à esquerda de b, então ao deslocarmos a e b simultaneamente de c posições à direita, não é difícil aceitar que $a+c$ se mantém à esquerda de $b+c$.



A propriedade acima admite uma recíproca, ou seja:

Dados três números naturais a, b e c, quaisquer,

$$\boxed{\text{se} \quad a+c<b+c, \quad \text{então} \quad a<b.}$$

Prova-se esta propriedade utilizando a tricotomia. De fato, suponhamos que $a+c<b+c$. Pela tricotomia, temos uma das três possibilidades:

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

A primeira possibilidade não pode ser verificada, pois se $b<a$, teríamos $b+c<a+c$, pela propriedade já provada, o que está em contradição com a nossa hipótese $a+c<b+c$.

A segunda possibilidade também não pode ser verificada, pois se $a=b$, teríamos $a+c=b+c$, o que também está em contradição com a nossa hipótese.

Só resta portanto a única possibilidade: $a<b$.

Você percebeu que utilizamos a tricotomia diversas vezes na prova acima?

Problema 1.4. Mostre que dados três números naturais a, b e c, quaisquer,

$$\boxed{\text{se} \quad a+c=b+c, \quad \text{então} \quad a=b.}$$

Problema 1.5. Usando a propriedade de compatibilidade da adição com a ordem e a transitividade da ordem, mostre que:

$$\boxed{\text{Se} \quad a<b \ \text{ e } \ c<d, \quad \text{então } a+c<b+d.}$$

Vale a recíproca dessa propriedade?

SUGESTÃO: Usando a compatibilidade da adição com a ordem, some c a ambos os lados da primeira desigualdade, some b a ambos os lados da segunda desigualdade. Finalmente, compare as novas desigualdades assim obtidas.

1.4 Subtração

Dados dois números naturais a e b tais que $a \leq b$, o número de deslocamentos para a direita partindo de a para atingir b será representado por $b-a$ e será chamado de *diferença* entre b e a.

Por exemplo, dados $a=3$ e $b=7$, é preciso deslocar 3 para a direita de 4 posições para alcançar 7, logo $7-3=4$.

Portanto, pela definição de $b-a$, temos que

$$a+(b-a)=b. \tag{1.1}$$

O número $b - a$ é também o quanto devemos deslocar b para a esquerda para alcançar a.

Devido à equação (1.1), o número $b-a$ pode ser interpretado como o quanto falta a a para atingir b.

Portanto, da equação (1.1) e do Problema 1.4, seque que se tivermos uma igualdade entre números naturais do tipo $a + c = b$, então $c = b - a$.

Problema 1.6. Tenho 50 reais, mas uma bicicleta custa 200 reais, quanto falta para eu poder comprar a bicicleta?

Problema 1.7. Mostre que se $c \leq a < b$, então $a - c < b - c$.

Note que $a - a = 0$, pois devemos deslocar a de zero para atingir a; ou seja não falta nada a a para atingir a.

Note também que $a - 0 = a$, pois devemos deslocar 0 de a para a direita para atingir a; ou seja, falta a a zero para atingir a.

Observe que, no contexto dos números naturais, só faz sentido formar a diferença $b - a$ quando $b \geq a$: caso contrário, isto é, se $b < a$,

$$\cdots \longrightarrow \textcircled{b} \longrightarrow \cdots \longrightarrow \textcircled{a} \longrightarrow \cdots$$

não há como deslocar b para a esquerda para alcançar a, ou o que é o mesmo, não há como deslocar a para a direita para atingir b.

Quando $a \leq b$, a diferença $b - a$, entre b e a, define uma operação sobre pares de números naturais (a, b), que chamaremos de *subtração*.

A subtração é a operação inversa da adição, pois ao deslocarmos a para a direita de b posições encontramos $a+b$, depois ao deslocarmos $a+b$ para a esquerda de b posições voltamos para a. Em símbolos:

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

Reciprocamente, se deslocarmos b para a esquerda de a posições encontramos $b-a$, depois ao deslocarmos $b-a$ para a direita de a posições encontramos b. Em símbolos:

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

Quando $b>a$, o número $b-a$ nos auxilia na contagem de quantos números inteiros maiores ou iguais a a e menores ou iguais a b existem. Para contar esses números considere a sequência:

$$a+0,\ a+1,\ a+2,\ a+3,\ldots,\ a+(b-a)=b,$$

cujo número de elementos é igual ao número de naturais entre 0 e $b-a$, inclusive, o que nos dá exatamente $b-a+1$ números.

Portanto,

se $a<b$, o intervalo $[a,b]$ possui $b-a+1$ elementos.

Problema 1.8. Quantos números naturais existem maiores ou iguais a 37 e menores ou iguais a 72?

Problema 1.9. Quantos números naturais existem em cada um dos intervalos $(32,75]$, $[32,75)$ e $(32,75)$?

Problema 1.10. Se $a < b$, quantos números naturais existem nos intervalos $(a, b]$, $[a, b)$ e (a, b)?

1.5 Múltiplos

Dado $a \in \mathbb{N}$, podemos considerar os múltiplos de a:

0 vezes a (nenhuma vez a), uma vez a, duas vezes a, três vezes a etc., obtendo assim a sequência:

$$0 \times a = 0, \quad 1 \times a = a, \quad 2 \times a = a + a, \quad 3 \times a = a + a + a, \quad \ldots$$

Por exemplo, 0 dúzias, uma dúzia, duas dúzias, três dúzias etc., são os múltiplos de 12.

Outro exemplo é dado pelos múltiplos de 2:

$$0, \quad 2, \quad 4, \quad 6, \quad 8, \quad 10, \quad \cdots$$

que são chamados de números pares. Um número que não é par é chamado de *ímpar*.

Problema 1.11. Os números ímpares são múltiplos de algum número fixado maior do que 1? Você seria capaz de justificar de modo convincente a sua resposta?

Problema 1.12. Liste os 10 primeiros múltiplos de 5.

Problema 1.13. Descubra quantos múltiplos de 7 existem entre 14 e 63, inclusive.

Solução: O modo mais direto de proceder é listar esses números para depois contá-los:

$$14, \quad 21, \quad 28, \quad 35, \quad 42, \quad 49, \quad 56, \quad 63.$$

Assim, concluímos que esses são 8 em número.

Problema 1.14. Descubra quantos múltiplos de 7 existem entre 14 e 7 000, inclusive.

Solução: Resolver o problema listando todos esses números, como na solução do Problema 1.13, seria muito trabalhoso. Podemos abordar o problema fazendo-o recair num caso já considerado e de fácil resolução:

$$\underline{2} \times 7 \ (= 14), \quad \underline{3} \times 7, \quad \underline{4} \times 7, \quad \ldots \quad , \quad \underline{1\,000} \times 7 \ (= 7\,000).$$

Agora é só contar quantos são os números de 2 a 1 000, que sabemos serem $1\,000 - 2 + 1 = 999$.

Note que o único múltiplo de 0 é apenas o 0. Todos os números são múltiplos de 1 e de si próprios. Note também que, pela definição de múltiplo, um múltiplo não nulo, isto é diferente de zero, de um número $a > 0$ é sempre maior ou igual do que a.

Assim, temos a seguinte propriedade importante:

Se $a \times b = 0$, então $a = 0$ ou $b = 0$.

Problema 1.15.

(a) Quantos múltiplos de 8 existem entre 32 e 8 000, inclusive?

(b) Quantos números pares existem entre 3 211 e 6 321?

(c) Quantas dúzias podemos formar com 180 laranjas? E com 220 laranjas?

(d) Quantas semanas formam 280 dias? E 360 dias?

Problema 1.16. Seja $c \neq 0$.

(a) Mostre que

$$0 < c < 2 \times c < 3 \times c < 4 \times c < 5 \times c.$$

Fica assim "bastante evidente", por analogia, ou por indução empírica, que se $a < b$, então $a \times c < b \times c$ (uma prova rigorosa disto pode ser dada usando Indução Matemática).

(b) Mostre que vale a recíproca da propriedade acima, isto é que se $a \times c < b \times c$, então $a < b$.

SUGESTÃO: Mostre que qualquer uma das opções, $a = b$ ou $b < a$, implica numa contradição, restando assim, por tricotomia (recorde que a ordem é total), a única possibilidade: $a < b$.

1.6 Multiplicação

Tomar múltiplos define uma operação nos números naturais, $a \times b$, que se lê *a vezes b*, representando o múltiplo a vezes b de b. Assim,

$$a \times b = \begin{cases} 0, & \text{se } a = 0, \\ b, & \text{se } a = 1, \\ \underbrace{b + b + \cdots + b}_{a \text{ parcelas}}, & \text{se } a > 1. \end{cases}$$

O número $a \times b$ será chamado o produto de a por b e será também denotado por ab, quando não houver risco de confusão.

Exemplos: $2 \times 3 = 3 + 3 = 6$, $3 \times 2 = 2 + 2 + 2 = 6$, $5 \times 2 = 2 + 2 + 2 + 2 + 2 = 10$, $2 \times 5 = 5 + 5 = 10$ etc.

Dos exemplos acima temos que

$$2 \times 3 = 6 = 3 \times 2 \text{ e } 5 \times 2 = 10 = 2 \times 5.$$

De novo, isto não é mera coincidência, pois ocorre sempre. Vamos admitir que a multiplicação possua a seguinte propriedade:

Propriedade comutativa da multiplicação. Quaisquer que sejam os números naturais a e b, temos que

$$\boxed{a \times b = b \times a.}$$

De modo semelhante à adição, a multiplicação também possui a seguinte propriedade:

Propriedade associativa da multiplicação. Quaisquer que sejam os números naturais a, b e c, temos que

$$\boxed{a \times (b \times c) = (a \times b) \times c.}$$

Problema 1.17. Mostre que ser múltiplo é uma relação transitiva, isto é, se c é múltiplo de b e b é múltiplo de a, então c é múltiplo de a.

Recorde que definimos a multiplicação nos números naturais através da noção de múltiplo, que em última análise se reduz a ir somando, sucessivamente, a cópias de um mesmo número b. É portanto natural esperar que as operações de adição e de multiplicação tenham uma forte relação. Uma dessas relações se dá através da propriedade distributiva que passamos a discutir.

Propriedade distributiva da multiplicação com relação à adição. Considere dois múltiplos de um mesmo número natural, por exemplo 6×12 e 3×12, somando esses números obtemos

$$\begin{aligned} 6 \times 12 + 3 \times 12 &= 6 \times 12 + (1 \times 12 + 2 \times 12) \\ &= (6 \times 12 + 1 \times 12) + 2 \times 12 \\ &= 7 \times 12 + (1 \times 12 + 1 \times 12) \\ &= (7 \times 12 + 1 \times 12) + 1 \times 12 \\ &= 8 \times 12 + 1 \times 12 \\ &= 9 \times 12 = (6 + 3) \times 12. \end{aligned}$$

Um procedimento como o acima, mais um argumento de indução

que não queremos explicitar agora, permitiria mostrar que, em geral, dados números naturais a, b e c, tem-se que

$$\boxed{(a+b) \times c = a \times c + b \times c.}$$

Problema 1.18. Mostre que

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

Problema 1.19. Mostre que a soma de dois múltiplos de um mesmo número é múltiplo desse número.

Propriedade distributiva da multiplicação com relação à subtração. Podemos agora mostrar que se $a < b$, então

$$\boxed{c \times (b-a) = c \times b - c \times a.}$$

De fato, temos que

$$c \times a + c \times (b-a) = c \times [a + (b-a)] = c \times b.$$

Assim, pela definição da subtração, temos que

$$c \times (b-a) = c \times b - c \times a.$$

Problema 1.20. Mostre que a diferença de dois múltiplos de um mesmo número, quando faz sentido, é múltiplo desse número.

Problema 1.21. Sejam dados números naturais a, b e c tais que a é múltiplo de c. Mostre que $a + b$ é múltiplo de c se, e somente se, b é múltiplo de c.

Multiplicação e Ordem. A relação entre a adição e a ordem se reflete numa relação entre a multiplicação e a ordem que já tivemos oportunidade de abordar no Problema 1.16:

Se $a < b$ e $c > 0$, então $c \times a < c \times b$.

Problema 1.22. Mostre que o menor elemento do conjunto dos múltiplos não nulos de um número natural $a > 0$ é o próprio a.

1.7 Múltiplos Comuns

Um conceito importante é o de múltiplo comum de dois números.

Por exemplo, considere a sequência dos múltiplos de 3:

$$0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27,\ 30,\ 33,\ 36,\ 39,\ 42,\ 45, \ldots$$

e a sequência dos múltiplos de 5:

$$0,\ 5,\ 10,\ 15,\ 20,\ 25,\ 30,\ 35,\ 40,\ 45, \ldots$$

Assim, a sequência dos números que são simultaneamente múltiplos de 3 e de 5 é:

$$0,\ 15,\ 30,\ 45, \ldots$$

Você saberia continuar a sequência acima? Aparentemente, trata-se da sequência dos múltiplos de 15, ou seja, os múltiplos do menor múltiplo comum não nulo de 3 e de 5, que é 15.

Isso é absolutamente correto e é um resultado geral que provaremos a seu tempo.

Problema 1.23. Determine os dois primeiros múltiplos comuns de 4 e 14. Como você continuaria esta sequência?

Se a e b são números naturais não nulos, sabemos por definição que o número $a \times b$ é um múltiplo não nulo de b. Por outro lado, pela propriedade comutativa da multiplicação, tem-se que ele é também um múltiplo de a. Assim, o conjunto dos múltiplos comuns de a e b, além de conter o número 0, contém também o número $a \times b \neq 0$.

Definição. O menor múltiplo comum não nulo de dois números naturais não nulos a e b é denotado por $\text{mmc}(a, b)$ e será chamado de *mínimo múltiplo comum*[1] de a e b (ou abreviadamente mmc).

Problema 1.24. Ache o mmc dos seguintes pares de números:

3 e 4; 6 e 11; 6 e 8; 3 e 9.

Voce percebeu que algumas vezes $\text{mmc}(a, b) = a \times b$ e outras vezes não? Qual será a razão? Desvendaremos mais este mistério no Capítulo 3.

[1]Este número existe em função da observação acima e do Princípio da Boa Ordem.

1.8 Potenciação

Dados dois números naturais $a \neq 0$ e n qualquer, definimos a operação de potenciação como segue:

$$a^n = \begin{cases} 1, & \text{se } n = 0, \\ a, & \text{se } n = 1, \\ \underbrace{a \times a \times \cdots \times a}_{n \text{ fatores}}, & \text{se } n > 1. \end{cases}$$

Define-se também $0^n = 0$, para todo $n \neq 0$.

Exemplo: $2^0 = 1$, $2^1 = 2$, $2^2 = 2 \times 2 = 4$, $2^3 = 8$, $0^2 = 0$ etc.

Observação. *Fica de fora* 0^0*, que não é definido.*

Problema 1.25. Convença-se de que a potenciação possui as seguintes propriedades:

(a) $1^n = 1$; (b) $a^n a^m = a^{n+m}$;

(c) $(a^n)^m = a^{nm}$; (d) $a^n b^n = (ab)^n$.

Existem também fórmulas para escrever a potência de uma soma. Por exemplo,

$$(a+b)^2 = a^2 + 2ab + b^2,$$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3,$$

$$(a+b)^4 = a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.$$

Em geral, $(a+b)^n$ se escreve como a soma dos produtos de potências $a^i b^j$, onde $i+j=n$, multiplicados por certos números naturais. Esta fórmula geral que não apresentaremos aqui é chamada de *fórmula do binômio de Newton*. Para maiores informações sobre esta fórmula, veja o texto sobre indução do autor, já citado anteriormente e listado na bibliografia no final do livro.

Problema 1.26. Desenvolva $(a+b)^5$.

Capítulo 2

Representação dos Naturais

2.1 O Sistema Decimal

Os números naturais foram representados ao longo da história de vários modos distintos. O modo universalmente utilizado na atualidade é a representação decimal posicional. Esse sistema, variante do sistema sexagesimal utilizado pelos babilônios há cerca de 1 700 anos antes de Cristo, foi desenvolvido na China e na Índia. Nesse sistema, todo número natural é representado por uma sequência formada pelos algarismos

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9.$$

Por serem 10 esses algarismos, o sistema é chamado de decimal. O sistema é também dito posicional, pois cada algarismo, além de seu valor intrínseco, possui um peso que lhe é atribuído em função de sua posição dentro da sequência. Esse peso é uma potência de 10 e varia

do seguinte modo:

O algarismo da extrema direita tem peso $10^0 = 1$; o seguinte, sempre da direita para a esquerda, tem peso $10^1 = 10$; o seguinte tem peso $10^2 = 100$; o seguinte tem peso $10^3 = 1\,000$ etc.

Assim, o número 1 458, no sistema decimal representa o número

$$1 \times 10^3 + 4 \times 10^2 + 5 \times 10 + 8.$$

Os zeros à esquerda em um número são irrelevantes, pois por exemplo,

$$0231 = 0 \times 10^3 + 2 \times 10^2 + 3 \times 10 + 1 = 2 \times 10^2 + 3 \times 10 + 1 = 231.$$

Cada algarismo de um número possui uma *ordem*, contada da direita para a esquerda. Assim, no exemplo acima, o 8 é de primeira ordem, o 5 de segunda ordem, o 4 de terceira ordem e o 1 de quarta ordem.

Cada três ordens, também contadas da direita para a esquerda, constituem uma classe. As classes são usualmente separadas por um ponto. A seguir, damos os nomes das primeiras classes e ordens:

Classe das Unidades	unidades	$1^{\underline{a}}$ ordem
	dezenas	$2^{\underline{a}}$ ordem
	centenas	$3^{\underline{a}}$ ordem
Classe do Milhar	unidades de milhar	$4^{\underline{a}}$ ordem
	dezenas de milhar	$5^{\underline{a}}$ ordem
	centenas de milhar	$6^{\underline{a}}$ ordem

$$\text{Classe do Milhão} \begin{cases} \text{unidades de milhão} & 7^{\underline{a}} \text{ ordem} \\ \text{dezenas de milhão} & 8^{\underline{a}} \text{ ordem} \\ \text{centenas de milhão} & 9^{\underline{a}} \text{ ordem} \end{cases}$$

Problema 2.1. Determine a soma de todos os múltiplos de 6 que se escrevem no sistema decimal com dois algarismos.

Problema 2.2. Fixe três algarismos distintos e diferentes de zero. Forme os seis números com dois algarismos distintos tomados dentre os algarismos fixados. Mostre que a soma desses números é igual a 22 vezes a soma dos três algarismos fixados.

Problema 2.3. Nos tempos de seus avós não existiam as calculadoras eletrônicas e por isso eram ensinadas várias regras de cálculo mental. Uma delas era a seguinte:

Seja a um número natural cujo algarismo da unidade é 5, ou seja, $a = 10q + 5$, com q um número natural. Mostre que $a^2 = 100q(q + 1) + 25$. Com isto, ache uma regra para calcular mentalmente o quadrado de a. Aplique a sua regra para calcular os quadrados dos números; 15, 25, 35, 45, 55, 65, 75, 85, 95, 105 e 205.

Problema 2.4. Qual é o menor número de dois algarismos? E qual é o maior? Quantos são os números de dois algarismos? Quantos algarismos precisa-se para escrevê-los?

Problema 2.5. Quantos algarismos são usados para numerar um livro de 300 páginas? Quantas vezes usa-se cada algarismo?

Curiosidade. Existe uma fórmula interessante para descrever o número $Q(x)$ de algarismos necessários para escrever todos os números

naturais de 0 a x, no sistema decimal:

$$Q(x) = n(x+1) - (10^{n-1} + \cdots + 10),$$

onde n é o número de algarismos de x (cf. *Revista do Professor de Matemática*, n. 5, p. 32).

Utilize esta fórmula para conferir a sua resposta ao Problema 2.5.

2.2 Critérios de Multiplicidade de 2, 5 e 10

Critérios de multiplicidade são alguma regras práticas para decidir se um dado número é múltiplo de algum outro prefixado.

A seguir, veremos alguns desses critérios.

Seja dado um número n escrito no sistema decimal como

$$n = n_r \cdots n_1 n_0 = n_r 10^r + \cdots + n_1 10 + n_0.$$

Podemos então escrever

$$n = (n_r 10^{r-1} + \cdots + n_1)10 + n_0,$$

onde n_0 é o algarismo das unidades de n.

Reciprocamente, se n é da forma $n = 10m + n_0$, onde n_0 é um dos algarismos de 0 a 9, então n_0 é o algarismo das unidades de n.

Problema 2.6. Mostre que o algarismo das unidades de um quadrado perfeito, isto é, um número da forma a^2, onde a é um número natural,

só pode ser 0, 1, 4, 5, 6 ou 9.

Critério de multiplicidade de 2.

Inicialmente, consideremos a tabela:

$$\begin{array}{ll} 2\times 0 = 0 & 2\times 5 = 10 = 10+0 \\ 2\times 1 = 2 & 2\times 6 = 12 = 10+2 \\ 2\times 2 = 4 & 2\times 7 = 14 = 10+4 \\ 2\times 3 = 6 & 2\times 8 = 16 = 10+6 \\ 2\times 4 = 8 & 2\times 9 = 18 = 10+8 \end{array}$$

Note que todo número acima é um múltiplo de 10 somado com um dos números: 0, 2, 4, 6, ou 8.

Suponha agora que um dado número natural n seja par, ou seja, $n = 2m$, onde m é um número natural. Escrevendo m da forma $m'10 + m_0$, onde m_0 é o algarismo das unidades de m, temos

$$n = 2(m'10 + m_0) = 2m'10 + 2m_0.$$

Sendo $2m_0$ um dos números da tabela, temos que ele é um múltiplo de 10 somado com um dos números: 0, 2, 4, 6, ou 8. Logo, $n = 2m'10 + 2m_0$ é um múltiplo de 10 somado com um dos números: 0, 2, 4, 6, ou 8, e, portanto, o seu algarismo das unidades é 0, 2, 4, 6, ou 8.

Problema 2.7. Mostre a recíproca do que provamos acima, ou seja, mostre que é par um número cujo algarismo das unidades é um dos algarismos 0, 2, 4, 6 ou 8.

Juntando essas informações temos o seguinte resultado:

Teorema (Critério de Multiplicidade de 2)

Um número é múltiplo de 2 *se, e somente se, o seu algarismo das unidades é par.*

Critério de multiplicidade de 5 e de 10.

Seja n um número natural escrito na forma $n = 10m + n_0$, onde n_0 é o algarismo das unidades de n. Como $10m$ é múltiplo de 5 e de 10, temos que n é múltiplo de 5 ou de 10 se, e somente se, n_0 é múltiplo de 5 ou de 10, respectivamente (cf. Problema 1.21). Isto ocorre se, e somente se, $n_0 = 0$ ou $n_0 = 5$, no primeiro caso; e $n_0 = 0$, no segundo. Assim, provamos o seguinte resultado:

Teorema (Critério de Multiplicidade de 5 ou de 10)

Um número é múltiplo de 5 *se, e somente se, o seu algarismo das unidades for* 0 *ou* 5. *Um número é múltiplo de* 10 *se, e somente se, o seu algarismo das unidades for* 0.

Problema 2.8. Determine se é múltiplo de 2, de 5 ou de 10 cada número a seguir:

$$17,\ 22,\ 25,\ 28,\ 30,\ 35\,420,\ 523\,475.$$

Problema 2.9. Com a informação de que 100 é múltiplo de 4 e de 25, você seria capaz de achar um critério de multiplicidade de 4 ou de 25?

SUGESTÃO: Note que um número $n = n_r \cdots n_2 n_1 n_0$ pode ser escrito na forma $n = n_r \cdots n_2 \times 100 + n_1 n_0$.

Problema 2.10. Com a informação de que 1 000 é múltiplo de 8 (respectivamente de 125), você seria capaz de achar um critério de multiplicidade de 8? (respectivamente de 125?)

SUGESTÃO: Note que um número $n = n_r \cdots n_3 n_2 n_1 n_0$ pode ser escrito na forma $n = n_r \cdots n_3 \times 1\,000 + n_2 n_1 n_0$.

2.3 Critérios de Multiplicidade de 9 e de 3

Inicialmente note os seguintes fatos:

$10 - 1 = 9 = 1 \times 9$,

$10^2 - 1 = 100 - 1 = 99 = 11 \times 9$,

$10^3 - 1 = 1.000 - 1 = 999 = 111 \times 9$,

$10^4 - 1 = 10\,000 - 1 = 9\,999 = 1\,111 \times 9$.

Em geral, para n um número natural não nulo, temos

$$10^n - 1 = \underbrace{11\cdots1}_{\text{n vezes}} \times 9.$$

Portanto, todos os números da forma $10^n - 1$ são múltiplos de 9 e também de 3, já que 9 é múltiplo de 3.

Seja dado agora um número n escrito no sistema decimal como

$$n = n_r \cdots n_1 n_0 = n_r 10^r + \cdots + n_1 10 + n_0.$$

Subtraiamos a soma $n_r + \cdots + n_1 + n_0$, dos algarismos que compõem

o número n, de ambos os lados da igualdade acima:

$$\begin{aligned} n-(n_r+\cdots+n_1+n_0) &= n_r10^r-n_r+\cdots+n_110-n_1+n_0-n_0 \\ &= (10^r-1)n_r+\cdots+(10-1)n_1. \end{aligned}$$

Note agora que a última expressão é sempre múltiplo de 9 (logo, de 3). Portanto, pelo Problema 1.21, temos que n é múltiplo de 9 ou de 3 se, e somente se, o número $n_r+\cdots+n_1+n_0$ é múltiplo de 9 ou de 3. Assim, obtemos o seguinte resultado:

Teorema (Critério de Multiplicidade de 9 ou de 3)

Um número $n=n_r\cdots n_1n_0$ é múltiplo de 9 *ou de* 3 *se, e somente se, o número $n_r+\cdots+n_1+n_0$ for múltiplo de* 9 *ou de* 3*, respectivamente.*

O teorema acima reduz o problema de saber se um dado número é múltiplo de 9 ou de 3 ao problema de saber se um outro número obtido a partir desse é múltiplo de 9 ou de 3. O que ganhamos com isto? Bem, o número $n_r+\cdots+n_1+n_0$ é consideravelmente menor do que n e se ele ainda for grande podemos aplicar o teorema a ele obtendo um número ainda menor e assim, sucessivamente, até encontrar um número para o qual seja fácil decidir se é múltiplo de 9 ou de 3.

Por exemplo, dado o número 257 985 921, somando os seus algarismos obtemos $2+5+7+9+8+5+9+2+1=48$. Repetindo o mesmo procedimento para o número 48, obtemos $4+8=12$, o qual é múltiplo de 3 mas não de 9. Logo, o número dado inicialmente é múltiplo de 3, mas não múltiplo de 9.

Problema 2.11. Determine se é múltiplo de 3 ou de 9 cada um dos

números a seguir:

$$108,\ 111,\ 225,\ 328,\ 930,\ 35\,424,\ 523\,476.$$

2.4 Números Primos

Os números primos são números especiais que desempenham um papel importante dentro da teoria e entre outras coisas os seus produtos representam todos os números naturais, como veremos ainda nesta seção.

Definição. Um número natural diferente de 0 e de 1 e que é apenas múltiplo de 1 e de si próprio é chamado de *número primo*. Um número diferente de 0 e de 1 que não é primo é chamado de *número composto*.

Por exemplo, 2, 3, 5 e 7 são números primos, enquanto 4, 6 e 8 são números compostos, por serem múltiplos de 2.

Mais geralmente, todo número par maior do que 2 não é primo, ou seja, é composto (justifique).

Note que a definição acima não classifica os números 0 e 1 nem como primos nem como compostos. Exceto esses dois números, todo número natural ou é primo ou é composto.

Problema 2.12. Diga quais dos seguintes números são primos e quais são compostos:

$$9, 10, 11, 12, 13, 15, 17, 21, 23, 47, 49.$$

Certamente, os números compostos são em número infinito, pois

já os números pares diferentes de 2 são em número infinito (justifique).

Uma pergunta que surge espontaneamente é a seguinte: Quantos são os números primos?

Euclides de Alexandria, em 300 a.C., ou seja, há mais de 2 300 anos, mostrou que existem infinitos números primos.

Como terá Euclides feito isto? Será que ele exibiu todos os números primos? Seria isto possível? Veremos na próxima seção como ele realizou esta façanha.

Determinar se um dado número é primo ou composto pode ser uma tarefa muito árdua. Para se ter uma ideia da dificuldade, você saberia dizer se o número 241 é primo?

Muito mais difícil é decidir se o número 4 294 967 297 é primo ou composto. O matemático francês Pierre de Fermat (1601-1655) afirmou que esse número é primo, enquanto o matemático suíço Leonhard Euler (1707-1783) afirmou que é composto. Qual deles estava com a razão? Daremos a resposta na Seção 4.5.

A tarefa de decidir se um número é primo ou múltiplo de outro pode ser ligeiramente auxiliada com critérios de multiplicidade, como os que vimos nas Seções 2.2 e 2.3.

2.5 O Crivo de Eratóstenes

Um método muito antigo para se obter de modo sistemático números primos é o chamado *Crivo de Eratóstenes*,[1] devido ao matemático grego Eratóstenes.

A eficiência do método é baseada na observação bem simples a seguir.

Se um número natural $a > 1$ é composto, então ele é múltiplo de algum número primo p tal que $p^2 \leq a$. Equivalentemente, é primo todo número a que não é múltiplo de nenhum número primo p tal que $p^2 < a$.

De fato, se a é composto e p é o menor número primo do qual a é múltiplo, então $a = p \times b$, onde p e b são menores do que a. De todo modo, sendo b primo ou composto, ele será múltiplo de um número primo q. Como a é múltiplo de b e b é múltiplo de q, pela transitividade da relação de ser múltiplo (Problema 1.17), temos que a é também múltiplo de q e sendo p o menor primo do qual a é múltiplo, temos $p \leq q$. Logo, $p^2 \leq p \times q \leq a$.

Por exemplo, para mostrar que o número $221 (= 13 \times 17)$, é composto, bastaria testar se ele é múltiplo de algum dos números primos $p = 2, 3, 5, 7, 11$ ou 13, já que o próximo primo 17 é tal que $17^2 = 289 > 221$.

Para se obter os números primos até uma certa ordem n, escreva os números de 2 até n em uma tabela.

[1] A palavra crivo significa peneira. O método consiste em peneirar os números naturais em um intervalo $[2, n]$, jogando fora os números que não são primos.

O primeiro desses números, o 2, é primo, pois não é múltiplo de nenhum número anterior. Risque todos os demais múltiplos de 2 na tabela, pois esses não são primos.

O primeiro número não riscado nessa nova tabela é o 3 que é primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque todos os demais múltiplos de 3 na tabela, pois esses não são primos.

O primeiro número maior que 3 e não riscado na tabela é o 5 que é um número primo, pois não é múltiplo de nenhum número anterior diferente de 1. Risque os demais múltiplos de 5 na tabela.

O primeiro número maior do que 5 e que não foi riscado é o 7, que é primo. Risque os demais múltiplos de 7 na tabela.

Ao término desse procedimento, os números não riscados são todos os primos menores ou iguais a n.

Note que o procedimento termina assim que atingirmos um número primo p tal que $p^2 \geq n$, pois, pela observação que fizemos acima, já teríamos riscado todos os números compostos menores ou iguais a n.

Exibimos a seguir o resultado do crivo para $n = 250$. Note que, neste caso, o procedimento termina tão logo cheguemos ao número primo $p = 17$.

	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36
37	38	39	40	41	42	43	44	45	46	47	48
49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72
73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96
97	98	99	100	101	102	103	104	105	106	107	108
109	110	111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130	131	132
133	134	135	136	137	138	139	140	141	142	143	144
145	146	147	148	149	150	151	152	153	154	155	156
157	158	159	160	161	162	163	164	165	166	167	168
169	170	171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190	191	192
193	194	195	196	197	198	199	200	201	202	203	204
205	206	207	208	209	210	211	212	213	214	215	216
217	218	219	220	221	222	223	224	225	226	227	228
229	230	231	232	233	234	235	236	237	238	239	240
241	242	243	244	245	246	247	248	249	250		

Consultando a tabela acima temos que o número 241 é primo, respondendo à pergunta que formulamos anteriormente.

Da tabela acima, extraímos todos os números primos até 250:

2	3	5	7	11	13	17	19	23	29
31	37	41	43	47	53	59	61	67	71
73	79	83	89	97	101	103	107	109	113
127	131	137	139	149	151	157	163	167	173
179	181	191	193	197	199	211	223	227	229
233	239	241							

Note que a diferença de dois números primos consecutivos, excetuando 2 e 3 (que diferem de 1) é de no mínimo 2 (justifique).

Dois primos consecutivos são chamados *primos gêmeos* se eles diferem de 2.

Assim, consultando a tabela dos primos acima, os seguintes são pares de primos gêmeos:

$(3,5),\ (5,7),\ (11,13),\ (17,19),(29,31),\ (41,43),\ (59,61),\ (71,73),$

$(101,103),\ (107,109),\ (137,139),\ (149,151),\ (179,181),\ (191,193),$

$(197,199),\ (227,229),\ (239,241).$

O que é surpreendente é que até o presente momento os matemáticos ainda não saibam dizer se os pares de primos gêmeos formam um conjunto finito ou infinito.

Três primos consecutivos serão chamados *primos trigêmeos* se a diferença entre cada dois primos consecutivos da terna é 2.

Por exemplo, $(3,5,7)$ é uma terna de primos trigêmeos. Você seria capaz de exibir outra terna de primos trigêmeos?

Ao contrário dos pares de primos gêmeos, vamos mais adiante ver que será muito fácil responder à questão da finitude ou não dessas

ternas.

Outro problema muito simples de ser enunciado, mas que ainda não tem resposta, é a chamada *Conjectura de Goldbach.*[2]

O matemático prussiano[3] Christian Goldbach, numa carta de 7 de junho de 1742 endereçada a Leonhard Euler, o maior matemático da época e um dos maiores matemáticos de todos os tempos, propôs que se provasse que todo número maior do que 5 é a soma de três primos.

Por exemplo, $6 = 2 + 2 + 2$, $7 = 3 + 2 + 2$, $8 = 3 + 3 + 2$, $9 = 5 + 2 + 2$, $10 = 5 + 3 + 2$, $11 = 5 + 3 + 3 = 7 + 2 + 2$, $12 = 5 + 5 + 2 = 3 + 7 + 2$ etc.

Euler respondeu que acreditava nessa conjectura, porém não sabia demonstrá-la, mas que ela era equivalente a mostrar que todo número par maior ou igual do que 4 era soma de dois números primos.

Por exemplo, $4 = 2+2$, $6 = 3+3$, $8 = 5+3$, $10 = 3+7 = 5+5$, $12 = 5 + 7$ etc.

Pois bem, esta conjectura, até o presente momento, não foi provada, nem desmentida.

Problema 2.13. Teste a Conjectura de Goldbach e a versão de Euler para os números de 14 a 40. Você acredita que esta conjectura seja verdadeira?

[2] O termo conjectura numa linguagem mais coloquial significa *palpite, chute.*

[3] A Prússia tem uma história muito rica dentro do contexto europeu dos séculos 18, 19 e 20, marcado por guerras intermináveis. No tempo de Goldbach a Prússia era um reino muito pobre, mas que posteriormente tornou-se um potente império chegando a ocupar grande parte da Europa do Norte. Para saber mais consulte o seu professor de História.

Um outro problema proposto em 1845 pelo matemático francês Joseph Bertrand (1822-1900) foi que, dado um número natural $n > 3$, sempre existe um número primo p no intervalo $(n, 2n-2)$. Cinco anos depois, o matemático russo Pafnuti Chebyshev (1821-1894) provou de modo surpreendentemente elementar, mas não o suficiente para que o façamos aqui, que a afirmação era verdadeira.

Problema 2.14. Usando a nossa tabela de primos, verifique o Postulado de Bertrand para $n \leq 125$.

Há uma conjectura semelhante ao Postulado de Bertrand, proposta anteriormente pelo matemático francês Adrien-Marie Legendre (1752-1833), mas que ainda não foi provada nem desmentida, que é a seguinte:

Dado um número natural n sempre existe um número primo no intervalo $(n^2, (n+1)^2)$.

Problema 2.15. Usando a nossa tabela de primos, verifique a Conjectura de Legendre para $n \leq 15$.

2.6 Teorema Fundamental da Aritmética

O método do Crivo de Eratóstenes nos mostra que dado um número natural a, existe um número primo p_0 tal que ou $a = p_0$, ou a é um múltiplo não trivial de p_0; isto é, $a = p_0 a_1$, com $1 < a_1 < a$.

Se a segunda possibilidade é verificada, segue que existe um número primo p_1, tal que ou $a_1 = p_1$, ou $a_1 = p_1 a_2$, onde

$1 < a_2 < a_1 < a$. Assim,

$$a = p_0 p_1, \quad \text{ou} \quad a = p_0 p_1 a_2.$$

Continuando a argumentação para a_2, temos $a = p_0 p_1 p_2$, ou $a = p_0 p_1 p_2 a_3$, para algum primo p_2 e $1 < a_3 < a_2 < a_1 < a$.

Note que desigualdades como a acima não podem continuar indefinidamente (justifique). Logo, para algum r, o número a_r é um primo p_r, obtendo desse modo uma decomposição de a em fatores primos:

$$a = p_1 p_2 \cdots p_r.$$

Obtemos, assim, o seguinte resultado que se encontra no livro *Os Elementos* de Euclides de Alexandria.

Proposição (Euclides)

Todo número natural $a > 1$, ou é primo, ou se escreve como produto de números primos.

Prova-se com um pouco mais de trabalho, que faremos na Seção 3.9, que esta escrita é única a menos da ordem dos fatores. Com esta informação adicional, o resultado de Euclides pode ser reformulado do seguinte modo:

Teorema Fundamental da Aritmética

Dado um número natural $a \geq 2$, existem um número $r > 0$, números primos $p_1 < \cdots < p_r$ e números naturais não nulos $n_1, \ldots, n_r$ tais que

$$a = p_1^{n_1} \cdots p_r^{n_r} ;$$

além disso, esta escrita é única.[4]

Problema 2.16. Decomponha em produtos de primos os seguintes números: 4, 6, 8, 28, 36, 84, 320 e 2 597.

SUGESTÃO: Para o número 2 597, note que se esse número é composto há certamente um número primo $p < 51$ que o divide, pois $51^2 > 2\,597$ (veja a observação que fizemos ao descrevermos o Crivo de Eratóstenes).

Vamos aproveitar que já temos os ingredientes para dar a demonstração de Euclides de que existem infinitos números primos.

Suponha por absurdo que os números primos sejam em número finito e seja a o produto de todos eles. O número $a+1$ não seria primo pois ele seria maior do que qualquer número primo. Logo, $a+1$ sendo composto, ele seria múltiplo de algum número primo q. Mas sendo a também múltiplo de q, teríamos, pelo Problema 1.21, que 1 seria múltiplo do número primo q, o que é um absurdo.

E foi assim que o astuto Euclides provou que existem infinitos números primos, sem ter o trabalho de exibi-los todos. O método utilizado na prova acima é chamado de *redução ao absurdo* e consiste em negar a afirmação que se quer provar e mostrar que isto leva a uma contradição. Assim, mostra-se que a negação da afirmação é falsa e, portanto, a própria afirmação é verdadeira.

[4]Observe que ordenamos os primos que intervêm na fatoração de a por ordem crescente, daí a unicidade da escrita. Esta parte do teorema não se encontra nos *Elementos* de Euclides, apesar daquela obra conter todos os ingredientes para prová-la. A prova completa foi dada por Gauss mais de dois séculos depois e acredita-se que Euclides não a fez por falta de notações adequadas.

Os números primos se distribuem dentro de $\mathbb{N}$ de modo bastante irregular. Já vimos que existem primos consecutivos cuja diferença é 2: são os primos gêmeos. Por outro lado, dado um número n arbitrário, existem dois primos consecutivos cuja diferença é maior do que n.

De fato, dado n, considere o número $a = 1 \times 2 \times 3 \times \cdots \times n$. Assim,

$$a+2,\ a+3,\ a+4,\ \ldots,\ a+n,$$

são inteiros consecutivos todos compostos, pois $a+2$ é múltiplo de 2, $a+3$ é múltiplo de 3, ..., $a+n$ é múltiplo de n. Sejam p o maior primo menor do que $a+2$ e q o menor primo maior do que $a+n$ (que existe pois os primos são infinitos); logo p e q são dois primos consecutivos, com $q - p > n$.

Alguns dos problemas mais profundos ainda por resolver estão relacionados com a distribuição dos números primos dentro da sequência dos números naturais.

Capítulo 3

Os Inteiros e suas Propriedades

3.1 Os Inteiros

Dados dois números naturais a e b, até o momento, o número $b - a$ só foi definido quando $b \geq a$. Como remediar esta situação? O jeito que os matemáticos encontraram para que seja sempre definido o número $b - a$ foi o de ampliar o conjunto dos números naturais formando um novo conjunto $\mathbb{Z}$ chamado de *conjunto dos números inteiros*, cujos elementos são dados ordenadamente como segue:

$$\cdots \to (-3) \to (-2) \to (-1) \to (0) \to (1) \to (2) \to (3) \to \cdots$$

Os números à esquerda do zero são chamados de *números negativos* e os à direita são chamados de *números positivos*. Os pares

de números 1 e -1, 2 e -2, 3 e -3 etc., são chamados de *números simétricos*. O elemento 0, que não é nem positivo, nem negativo, é o seu próprio simétrico.

Em $\mathbb{Z}$ temos uma relação de ordem que estende a relação de ordem de $\mathbb{N}$, onde declaramos $a < b$ quando a se encontra à esquerda de b. Esta relação continua transitiva e total (i.e., satisfazendo à tricotomia). Os intervalos em $\mathbb{Z}$ são definidos de modo análogo aos intervalos de $\mathbb{N}$.

Representando por $-a$ o simétrico de a, seja ele positivo, negativo ou nulo, temos sempre que

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

No conjunto $\mathbb{Z}$, temos definida a adição como segue:

Para todo número inteiro a, definimos $a+b$ como sendo o número obtido pelo deslocamento de a para a direita de b posições, se $b \geq 0$ ou de $-b$ posições para a esquerda se $b < 0$. A adição no conjunto $\mathbb{Z}$ continua tendo as propriedades comutativa e associativa e é compatível com a relação de ordem.

Definimos a diferença $b - a$ como sendo o número obtido deslocando b para a esquerda a posições, se $a > 0$; e deslocando b para a direita $-a$ posições, se $a < 0$. Isto define uma operação em $\mathbb{Z}$, sem restrições, chamada de *subtração*. Assim, temos que a subtração é a operação inversa da adição e

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

Problema 3.1. Mostre que em $\mathbb{Z}$ continua valendo a propriedade do Problema 1.4.

Problema 3.2. Mostre que em $\mathbb{Z}$ continua valendo que $(b-a)+a = b$ e que $(a+b)-b = a$.

Problema 3.3. Mostre com exemplos que a subtração não é uma operação nem comutativa nem associativa.

Problema 3.4. Mostre que em $\mathbb{Z}$ um intervalo $[a, b]$, onde $a \leq b$, tem $b - a + 1$ elementos.

A multiplicação nos inteiros é definida como segue: Se $a, b \geq 0$, sabemos o que é $a \times b$. Definimos

$$(-a) \times b = a \times (-b) = -(a \times b),$$

e

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

Assim, $a \times b$ está definido para quaisquer inteiros a e b. A multiplicação em $\mathbb{Z}$ continua sendo comutativa, associativa e distributiva com relação à adição e à subtração.

Tem-se também que se $a \times b = 0$, com a e b inteiros, então $a = 0$ ou $b = 0$.

Problema 3.5. Mostre que se $a \times c = b \times c$, com $c \neq 0$, então $a = b$.

A multiplicação também continua compatível com a ordem, no seguinte sentido:

Se $a < b$ e $c > 0$, então $c \times a < c \times b$.

Problema 3.6. Mostre com um exemplo que em $\mathbb{Z}$ não vale a propriedade:

Se $a < b$, então $a \times c < b \times c$, qualquer que seja c.

Nem a sua recíproca:

Se $a \times c < b \times c$, então $a < b$, qualquer que seja c.

3.2 Múltiplos Inteiros de um Número

Dado um inteiro a, consideremos o conjunto dos múltiplos inteiros de a:

$$a\mathbb{Z} = \{a \times d;\ d \in \mathbb{Z}\}.$$

Problema 3.7. Mostre que os múltiplos inteiros de um elemento a possuem as seguintes propriedades:

(i) 0 é múltiplo de a.

(ii) Se m é um múltiplo de a, então $-m$ é múltiplo de a.

(iii) Um múltiplo de um múltiplo de a é um múltiplo de a.

(iv) Se m e m' são múltiplos de a, então $m+m'$ e $m-m'$ são também múltiplos de a.

(v) Se m e m' são múltiplos de a, então $e \times m + f \times m'$ é múltiplo de a, quaisquer que sejam os inteiros e e f (note que (iv) é um caso particular da presente propriedade).

(vi) Se $m + m'$ ou $m - m'$ é múltiplo de a e m é múltiplo de a, então m' é múltiplo de a.

O mesmo resultado vale para os múltiplos comuns de dois inteiros a e b. De fato, o seguinte problema lida com esta situação.

Problema 3.8. Mostre que os múltiplos inteiros comuns de dois elementos a e b possuem as seguintes propriedades:

(i) 0 é múltiplo comum de a e b.

(ii) Se m é um múltiplo comum de a e b, então $-m$ é múltiplo comum de a e b.

(iii) Um múltiplo de um múltiplo comum de a e b é um múltiplo comum de a e b.

(iv) Se m e m' são múltiplos comuns de a e b, então $m + m'$ e $m - m'$ são também múltiplos comuns de a e b.

(v) Se m e m' são múltiplos comuns de a e b, então $e \times m + f \times m'$ é múltiplo comum de a e b, quaisquer que sejam os inteiros e e f (note que (iv) é um caso particular da presente propriedade).

(vi) Se $m + m'$ ou $m - m'$ é múltiplo comum de a e b e m é múltiplo comum de a e b, então m' é múltiplo comum de a e b.

Vimos que dois números naturais a e b possuem sempre um mmc que é um número natural. Se um dos números a ou b é nulo e o outro

é um inteiro qualquer, então esses números só admitem o zero como múltiplo comum (justifique), que será chamado do mínimo múltiplo comum (mmc) de a e b. Se a e b são ambos não nulos, mesmo que não sejam ambos positivos, então define-se o mínimo múltiplo comum (mmc) de a e b como sendo o menor múltiplo comum positivo; ou seja, o menor elemento positivo do conjunto

$$a\mathbb{Z} \cap b\mathbb{Z}.$$

Problema 3.9. Suponha que os números 216 e 144 sejam múltiplos comuns de um determinado par de números a e b. Mostre que $\text{mmc}(a, b) \leq 72$.

SUGESTÃO: Utilize a propriedade (iv) do Problema 3.8.

3.3 Divisores

Nesta seção olharemos a noção de múltiplo sob outro ponto de vista.

Definição. Diremos que um número inteiro d é um *divisor* de outro inteiro a, se a é múltiplo de d; ou seja, se $a = d \times c$, para algum inteiro c.

Quando a é múltiplo de d dizemos também que a é *divisível* por d ou que d *divide* a.

Representaremos o fato de um número d ser divisor de um número a, ou d dividir a, pelo símbolo $d \mid a$. Caso d não divida a, escrevemos $d \nmid a$.

Assim, por exemplo, temos que

$$1 \mid 6, \quad 2 \mid 6, \quad 3 \mid 6, \quad 6 \mid 6, \quad -6 \mid 6, \quad -3 \mid 6, \quad -2 \mid 6, \quad -1 \mid 6.$$

Além disso, se $d \notin \{-6, -3, -2, -1, 1, 2, 3, 6\}$, então $d \nmid 6$.

Temos também que $1 \mid a$ e $d \mid 0$, para todo d, inclusive quando $d = 0$, pois 0 é múltiplo de qualquer número[1].

Note também que se $d \mid a$, então $-d \mid a$, $d \mid -a$ e $-d \mid -a$

Note que se a e d são números naturais, com $a \neq 0$, e se $d \mid a$, então $d \leq a$. De fato, sendo a um múltiplo natural não nulo do número natural d, sabemos que $a \geq d$.

Problema 3.10. Mostre que das duas propriedades acima segue que, se a é um inteiro não nulo, os divisores de a são em número finito.

Problema 3.11. Mostre que se a e b são números naturais não nulos, então $a \mid b$ e $b \mid a$ se, e somente se, $a = b$.

Os critérios de multiplicidade podem ser reenunciados como critérios de divisibilidade.

Por exemplo, dado um número $n = n_r \ldots n_1 n_0$ na sua representação decimal, temos o resultado:

n é divisível por 2 (*ou seja múltiplo de* 2) *se e somente se n_0 é um número par.*

[1] Isto absolutamente não quer dizer que podemos dividir zero por zero, pois como $0 = c \times 0$ para todo c, o "quociente" de 0 por 0 poderia ser qualquer número, logo não estaria bem definido.

Problema 3.12. Enuncie critérios de divisibilidade por 3, 4, 5, 8, 9 e 10.

Utilizando a noção de divisor, podemos também redefinir a noção de número primo como sendo um número $p > 1$ que só possui 1 e o próprio p como divisores positivos.

A divisibilidade possui várias propriedades importantes decorrentes das propriedades dos múltiplos e cuja utilização vai nos facilitar a vida.

A relação de divisibilidade é transitiva, ou seja, se $a \mid b$ e $b \mid c$, então $a \mid c$.

De fato, isto é o mesmo que a transitividade da relação de ser múltiplo (veja Problema 1.17).

Problema 3.13. Mostre as seguintes propriedades importantes da divisibilidade:

(a) Se $d \mid a$ e $d \mid b$, então $d \mid (b + a)$ e $d \mid (b - a)$.

(b) Se $d \mid (b + a)$ ou $d \mid (b - a)$ e $d \mid a$, então $d \mid b$.

(c) Conclua que d é um divisor comum de a e de b se e somente se d é um divisor comum de a e de $b - a$.

Definição. Dados dois números inteiros a e b não simultaneamente nulos, o maior divisor comum de a e b será chamado de *máximo divisor comum* de a e b e denotado por $\text{mdc}(a, b)$.

Note que

$$\text{mdc}(a, b) = \text{mdc}(b, a).$$

Problema 3.14.

(a) Mostre que $\text{mdc}(0,0)$ não existe.

(b) Mostre que

$$\text{mdc}(0,b) = \begin{cases} b, & \text{se } b > 0 \\ -b, & \text{se } b < 0. \end{cases}$$

(c) Mostre que se $a \neq 0$ ou $b \neq 0$, então

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

O problema de determinar o mdc de dois números é bem simples quando os números são pequenos, pois neste caso podemos listar todos os divisores comuns desses números e escolher o maior deles, que será o seu mdc.

Por exemplo, para calcular $\text{mdc}(12,18)$, determinamos os divisores de 12, que são:

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4, \pm 6,\ \pm 12;$$

e os divisores de 18, que são:

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 6,\ \pm 9, \pm 18.$$

Tomando o maior divisor comum, obtemos: $\text{mdc}(12,18) = 6$.

No entanto, quando um dos dois números for grande, esse método fica impraticável, pois achar os divisores de um número grande é muito complicado. O que fazer então? Euclides, três séculos antes de Cristo, nos dá uma solução para este problema descrevendo um algoritmo

muito eficiente para fazer este cálculo. O Algoritmo de Euclides, como é conhecido o método por ele desenvolvido, será descrito no próximo capítulo e repousa numa generalização da propriedade do Problema 3.13(c) que recordamos abaixo:

Um número d é divisor comum de a e b, não ambos nulos, se, e somente se, ele é um divisor comum de a e $b - a$.

Tomando o máximo divisor comum, obtemos a seguinte identidade:

$$\text{mdc}(a, b) = \text{mdc}(a, b - a),$$

que permite ir reduzindo sucessivamente o cálculo do mdc de dois números ao cálculo do mdc de números cada vez menores.

Como exemplo de aplicação, vejamos como isto vai permitir o cálculo de $\text{mdc}(3\,264, 1\,234)$:

$$\begin{aligned}
&\text{mdc}(3\,264, 1\,234) = \text{mdc}(1\,234, 3\,264 - 1\,234) = \\
&\text{mdc}(1\,234, 2\,030) = \text{mdc}(1\,234, 2\,030 - 1\,234) = \\
&\text{mdc}(1\,234, 796) = \text{mdc}(796, 1\,234 - 796) = \\
&\text{mdc}(796, 438) = \text{mdc}(796 - 438, 438) = \\
&\text{mdc}(358, 438) = \text{mdc}(358, 438 - 358) = \\
&\text{mdc}(358, 80) = \text{mdc}(358 - 80, 80) = \\
&\text{mdc}(278, 80) = \text{mdc}(198, 80) = \\
&\text{mdc}(118, 80) = \text{mdc}(38, 80) = \\
&\text{mdc}(38, 42) = \text{mdc}(38, 4) = \\
&\text{mdc}(34, 4) = \text{mdc}(30, 4) = \\
&\text{mdc}(26, 4) = \text{mdc}(22, 4) = \\
&\text{mdc}(18, 4) = \text{mdc}(14, 4) = \\
&\text{mdc}(10, 4) = \text{mdc}(6, 4) = 2
\end{aligned}$$

As contas anteriores serão abreviadas de modo drástico com o algoritmo de Euclides para o cálculo do mdc que iremos apresentar na Seção 3.8.

Problema 3.15. Sejam a e b dois números com um divisor comum d. Mostre que d divide $a \times n + b \times m$, quaisquer que sejam os números inteiros n e m.

Dois números inteiros, não ambos nulos, serão ditos *primos entre si* se não forem múltiplos de um mesmo número diferente de 1 e de -1.

Portanto, dois inteiros a e b, não ambos nulos, são primos entre si se os únicos divisores comuns de a e b são 1 e -1, o que equivale a dizer que $\text{mdc}(a, b) = 1$.

Exemplos de pares de inteiros primos entre si são: 2 e 3; 4 e 15; 9 e 7. Não são primos entre si os pares: 2 e 4; 3 e 6; 9 e 12.

Dois números primos distintos são sempre primos entre si.

Dois números consecutivos são sempre primos entre si. De fato, podemos escrever os dois números na forma n e $n + 1$, logo

$$\text{mdc}(n, n + 1) = \text{mdc}(n, n + 1 - n) = \text{mdc}(n, 1) = 1.$$

Problema 3.16.

(a) Mostre que dois números inteiros da forma n e $2n + 1$ são sempre primos entre si.

(b) Mostre que se n é um número ímpar, então $\text{mdc}(n, 2n + 2) = 1$.

(c) Mostre que se n é um número par, então $\text{mdc}(n, 2n+2) = 2$.

Problema 3.17. Sejam a e b dois números naturais não ambos nulos e seja $d = \text{mdc}(a, b)$. Se a' e b' são os dois números naturais tais que $a = a' \times d$ e $b = b' \times d$, mostre que $\text{mdc}(a', b') = 1$.

3.4 Algoritmo da Divisão

Uma das propriedades mais importantes dos números naturais é a possibilidade de dividir um número por outro com resto pequeno. Essa é a chamada *divisão euclidiana*.

Sejam dados dois números naturais a e b, com $a > 0$ e b qualquer. Queremos comparar o número natural b com os múltiplos do número a. Para isto, considere todos os intervalos da forma $[na, (n+1)a)$, para n um número natural qualquer. Isto nos dá uma partição de $\mathbb{N}$, ou seja,

$$\mathbb{N} = [0, a) \cup [a, 2a) \cup [2a, 3a) \cup \cdots \cup [na, (n+1)\,a) \cup \cdots$$

e os intervalos acima são dois a dois sem elementos em comum.

Portanto, o número b estará em um e apenas um dos intervalos acima. Digamos que b pertença ao intervalo

$$[qa, (q+1)\,a).$$

Logo, existem dois números naturais q e r, unicamente determi-

nados, tais que

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

O número b é chamado *dividendo*, o número a *divisor*, os números q e r são chamados, respectivamente, *quociente* e *resto* da divisão de b por a.

Note que dados dois números naturais a e b, nem sempre b é múltiplo de a, este será o caso se, e somente se, $r = 0$.

Como determinar os números q e r na divisão euclidiana?

Caso b < a Como $b = 0 \times a + b$, temos que $q = 0$ e $r = b$.

Caso b = a Neste caso, tomamos $q = 1$ e $r = 0$.

Caso b > a Podemos considerar a sequência:

$$b - a,\ b - 2a, \ldots,\ b - na,$$

até encontrar um número natural q tal que $b - (q + 1)a < 0$, com $b - qa \geq 0$. Assim, obtemos $b = qa + r$, onde $r = b - qa$ e, portanto, $0 \leq r < a$.

Por exemplo, para dividir o número 54 por 13, determinamos os resultados da subtração de 54 pelos múltiplos de 13:

$$54 - 13 = 41,$$
$$54 - 2 \times 13 = 28,$$
$$54 - 3 \times 13 = 15,$$
$$54 - 4 \times 13 = 2$$
$$54 - 5 \times 13 = -11 < 0.$$

Assim, a divisão euclidiana de 54 por 13 se expressa como:

$$54 = 4 \times 13 + 2.$$

Problema 3.18. Efetue a divisão euclidiana nos seguintes casos:

(a) de 43 por 3 (b) de 43 por 5 (c) de 233 por 4

(d) de 1 453 por 10, por 100, por 1 000 e por 10 000.

Problema 3.19. Mostre o chamado *Algoritmo da Divisão Euclidiana* nos inteiros:

Dados inteiros a e b, com $a > 0$, existe um único par de inteiros q e r tal que

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

SUGESTÃO: Considere os intervalos da forma $[na, (n+1)\ a)$, com n em $\mathbb{Z}$.

Problema 3.20. Efetue a divisão euclidiana nos seguintes casos:

(a) de -43 por 3 (b) de -43 por 5 (c) de -233 por 4

(d) de $-1\,453$ por 10, por 100, por 1 000 e por 10 000.

Pelo Problema 3.19, se $a > 0$, os possíveis restos da divisão de um

número qualquer por a são os números $0, 1, \ldots, a-1$.

Por exemplo, os possíveis restos da divisão de um número inteiro por 2 são $r = 0$ ou $r = 1$.

Se um dado número quando divido por 2 deixa resto $r = 0$, ele é divisível por 2, ou seja, ele é par.

Se, ao contrário, esse número deixa resto 1 quando dividido por 2, ele é ímpar.

Assim, um número é par se é da forma $2q$ e é ímpar se é da forma $2q + 1$, para algum inteiro q.

Problema 3.21. Mostre que dentre dois inteiros consecutivos um deles é par e o outro ímpar.

Problema 3.22. Mostre que um número n escrito no sistema decimal como $n_r \ldots n_1 n_0$ deixa resto n_0 quando dividido por 10. Como se relacionam os restos da divisão de n por 2 ou 5 com os restos da divisão de n_0 por 2 ou 5?

Um número quando dividido por 3 pode deixar restos $r = 0$, $r = 1$ ou $r = 2$.

Problema 3.23. Mostre que de três inteiros consecutivos um e apenas um deles é múltiplo de 3.

Solução: Suponha que os três inteiros consecutivos sejam a, $a + 1$ e $a + 2$. Temos as seguintes possibilidades: a deixa resto 0, 1 ou 2 quando dividido por 3.

1) Suponha que a deixe resto 0 quando dividido por 3, ou seja, $a = 3q$. Logo, $a + 1 = 3q + 1$ e $a + 2 = 3q + 2$. Assim, um e apenas um dos

três números é múltiplo de 3, a saber, a.

2) Suponha que a deixe resto 1 quando dividido por 3, ou seja, $a = 3q + 1$. Logo, $a + 1 = 3q + 2$ e $a + 2 = 3q + 3 = 3(q + 1)$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 2$.

3) Suponha que a deixe resto 2 quando dividido por 3, ou seja, $a = 3q+2$. Logo, $a+1 = 3q+3 = 3(q+1)$ e $a+2 = 3q+4 = 3(q+1)+1$. Assim, um e apenas um dos três números é múltiplo de 3, a saber, $a + 1$.

Problema 3.24. Mostre que dados três números a, $a + 2$ e $a + 4$, um e apenas um deles é múltiplo de 3. Usando este fato, mostre que a única terna de primos trigêmeos é $(3, 5, 7)$.

Problema 3.25. Mostre que dados três números $2a$, $2(a + 1)$ e $2(a + 2)$, um e apenas um deles é múltiplo de 3.

Problema 3.26.

(a) Mostre que a soma de três inteiros consecutivos é sempre múltiplo de 3.

(b) Dados três inteiros consecutivos, mostre que um deles é múltiplo de 3 e a soma dos outros dois também.

Dividir por $a > 0$ é agrupar em conjuntos com a elementos. Por exemplo, para saber quantas dúzias de ovos temos no quintal, temos que dividir o número de ovos por 12, a divisão podendo ser exata ou não. Se tivermos 36 ovos, teremos 3 dúzias exatas, mas se tivermos 38 ovos, teremos ainda 3 dúzias de ovos e sobrariam 2 ovos.

Problema 3.27. Uma fábrica produz chicletes que são embalados em pacotes de cinco unidades cada. Quantos pacotes serão produzidos com 3 257 unidades?

3.5 Par ou Ímpar?

Nesta seção veremos, em um caso bem simples, como lidar com os restos da divisão de números inteiros por um número natural dado, introduzindo uma nova aritmética chamada *aritmética residual* ou *aritmética modular*.

A soma de dois números pares é par. De fato, os dois números podem ser escritos na forma $2a$ e $2b$, cuja soma é $2(a+b)$, logo par.

A soma de dois números ímpares é par. De fato, os números são da forma $2a+1$ e $2b+1$, cuja soma é $2(a+b+1)$, logo par.

A soma de um número par com um número ímpar é ímpar. De fato, um dos números é da forma $2a$ e o outro $2b+1$, cuja soma é $2(a+b)+1$, logo ímpar.

A paridade, isto é, a qualidade de ser par ou ímpar, da soma de dois números só depende da paridade de cada um dos números e não dos números em si.

O produto de dois números pares é par. De fato, os números sendo da forma $2a$ e $2b$, temos que o seu produto é $4ab$ e, portanto, múltiplo de 4, logo par.

O produto de um número par por um número ímpar é par. De fato, um número da forma $2a$ e um número da forma $2b+1$ têm um produto igual a $2a(2b+1)$, que é par.

O produto de dois números ímpares é ímpar. De fato, sendo os números da forma $2a+1$ e $2b+1$, o seu produto é $2(2ab+a+b)+1$, logo ímpar.

Novamente, como no caso da soma, temos que a paridade do produto de dois números só depende da paridade desses números e não dos números em si.

Assim, podemos decidir a paridade de uma expressão complexa envolvendo produtos e somas de inteiros do modo a seguir.

Atribuindo o símbolo $\overline{0}$ aos números pares e o símbolo $\overline{1}$ aos números ímpares, as observações acima nos fornecem as seguintes tabelas que regem a paridade das somas e produtos dos números inteiros.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\times$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Por exemplo, se quisermos saber a paridade do número $20^{10} \times 11^{200} + 21^{19}$ não será necessário desenvolver as contas indicadas para saber se o resultado final é par ou ímpar. O que fazemos é substituir na expressão acima o número 20 por $\overline{0}$, por ser par; e os números 11 e 21 por $\overline{1}$, por serem ímpares. Obtemos, assim, a expressão

$$\overline{0}^{10} \times \overline{1}^{200} + \overline{1}^{19},$$

que operada segundo as tabelas acima nos dá $\overline{1}$ como resultado. Portanto, o número dado é ímpar.[2]

[2]Tente explicar por que não substituímos os expoentes 10, 200 e 19 pelos símbolos $\overline{0}$ e $\overline{1}$, segundo a sua paridade.

O método acima pode ser generalizado para controlar os restos da divisão dos números inteiros por qualquer número natural fixado m. Veremos na próxima seção mais um caso especial, o caso $m = 3$. No próximo capítulo analisaremos o caso geral. Esse método foi idealizado pelo matemático alemão Carl Friedrich Gauss (1777-1855), considerado o maior matemático de todos os tempos, quando tinha perto de 17 anos.

Problema 3.28. Mostre que o dobro de um número ímpar é par mas nunca múltiplo de 4.

Problema 3.29. Determine a paridade do seguinte número:

$$(123\,275 + 346\,231)^{234} + (3\,451 + 4\,532)^{542}.$$

Problema 3.30. Mostre que para todos a inteiro e n natural não nulos, os números a e a^n têm mesma paridade.

Problema 3.31. Dado um número inteiro a e dados dois números naturais n e m, não nulos, mostre que são sempre pares os números $a^n + a^m$ e $a^n - a^m$.

Problema 3.32. Qual é a paridade da soma dos números naturais de um a 10? E de seu produto?

3.6 Zero, Um ou Dois?

Nesta seção analisaremos a aritmética dos restos da divisão por 3.

Vamos organizar os números inteiros numa tabela como segue:

⋮	⋮	⋮
−9	−8	−7
−6	−5	−4
−3	−2	−1
0	1	2
3	4	5
6	7	8
9	10	11
⋮	⋮	⋮

Note que os números da primeira coluna são os múltiplos de 3, ou seja, os números que deixam resto nulo quando divididos por 3. Os números da segunda e da terceira coluna são, respectivamente, aqueles que deixam resto 1 e 2 quando divididos por 3.

Fazendo uma análise semelhante àquela feita na seção anterior, nota-se que o resto da divisão por 3 da soma ou do produto de dois números só depende da coluna ocupada por esses números, ou seja só depende dos restos da divisão desses números por 3 e não dos números em si.

Assim, atribuindo o símbolo $\overline{0}$ aos números da primeira coluna (que são os múltiplos de 3) e os símbolos $\overline{1}$ e $\overline{2}$, respectivamente, aos números que ocupam a segunda e terceira coluna (que são os números que deixam restos 1 e 2, quando divididos por 3), obtemos as seguintes tabelas que regem os restos da divisão por 3 das somas e produtos dos números naturais:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Problema 3.33. Usando as tabelas acima, ache o resto da divisão por 3 do número $4^{100} + 32^{30}$.

3.7 Mínimo Múltiplo Comum

Sabemos que todo múltiplo do mmc de dois inteiros é um múltiplo comum desses inteiros (Problema 3.8(iii)). Mostraremos no próximo resultado que vale a recíproca desse fato.

Teorema 3.1. *Todo múltiplo comum de dois inteiros a e b é múltiplo de* $\text{mmc}(a, b)$.

Demonstração. Seja $m = \text{mmc}(a, b)$. Suponha que m' seja um múltiplo comum de a e b. Se $m' = 0$, nada temos a provar, pois 0 é múltiplo de qualquer inteiro, inclusive de m. Suponha que $m' \neq 0$, logo $a \neq 0$ e $b \neq 0$, o que mostra que $m = \text{mmc}(a, b) > 0$. Pelo algoritmo da divisão euclidiana, podemos escrever

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

Logo, $r = m' - mq$ e, sendo m' e mq múltiplos comuns de a e b, segue do Problema 3.8(iv) que r é múltiplo de comum de a e b. Mas então $r = 0$, pois caso contrário teríamos um múltiplo comum r de a e b, tal que $0 < r < m$, contradizendo a definição de mmc. □

O Teorema acima nos fornece a seguinte relação:

$$a\mathbb{Z} \cap b\mathbb{Z} = \text{mmc}(a, b)\mathbb{Z}.$$

Problema 3.34. Mostre que um número é múltiplo de 6 se, e somente se, ele é simultaneamente múltiplo de 2 e de 3.

Problema 3.35. Baseado no problema anterior, dê um critério de multiplicidade de 6, conhecendo os critérios de multiplicidade de 2 e de 3.

Problema 3.36. Sendo n um número inteiro qualquer, mostre que o número $n(n+1)(2n+1)$ é sempre múltiplo de 6.

Problema 3.37. Utilizando os critérios de multiplicidade de 3 e de 4, enuncie um critério de multiplicidade de 12.

Problema 3.38. Enuncie critérios de multiplicidade de 15, de 20 e de 45.

Dados três números inteiros a, b e c, não nulos, podemos nos perguntar como calcular o seu mínimo múltiplo comum $mmc(a, b, c)$, ou seja, o menor elemento positivo do conjunto dos múltiplos comuns de a, b e c.

Portanto, queremos determinar o menor elemento positivo do conjunto

$$a\mathbb{Z} \cap b\mathbb{Z} \cap c\mathbb{Z} = (a\mathbb{Z} \cap b\mathbb{Z}) \cap c\mathbb{Z} = \text{mmc}(a, b)\mathbb{Z} \cap c\mathbb{Z}.$$

Isto nos mostra que

$$\text{mmc}(a, b, c) = \text{mmc}\left(\text{mmc}(a, b), c\right).$$

Assim, para calcular o mmc de três números recai-se no cálculo de dois mmc de dois números.

Problema 3.39. Calcule $\text{mmc}(4, 6, 9)$.

Você deve ter notado que calcular o mmc de dois números é ainda uma tarefa muito trabalhosa, pois o que aprendemos até o momento foi escrever ordenadamente os múltiplos de cada um dos números até encontrarmos o menor múltiplo comum positivo. Com este método, é praticamente impossível calcular o mmc de dois números quando um deles for bastante grande. Na próxima seção finalizaremos um método muito mais eficiente para se determinar o mmc, baseado no Algoritmo do mdc de Euclides e no teorema a seguir.

Problema 3.40. Sejam a, b, d e m quatro inteiros positivos tais que $a \times b = m \times d$. Mostre que m é um múltiplo comum de a e b se, e somente se, d é um divisor comum de a e b.

Teorema 3.2. *Sejam a e b dois inteiros positivos. Tem-se a seguinte identidade:*

$$\text{mmc}(a, b) \times \text{mdc}(a, b) = a \times b.$$

Demonstração. Como a é um múltiplo de $\text{mdc}(a, b)$, segue que $a \times b$ é múltiplo de $\text{mdc}(a, b)$. Logo, $a \times b = m \times \text{mdc}(a, b)$, para algum inteiro positivo m. Pelo Problema 3.40, temos que m é um múltiplo

comum de a e b e, consequentemente, pelo Teorema 3.1 temos que $m = \text{mmc}(a, b) \times c$, para algum c positivo. Assim,

$$a \times b = \text{mmc}(a, b) \times (c \times \text{mdc}(a, b)). \tag{3.1}$$

Novamente, pelo Problema 3.40, segue que $c \times \text{mdc}(a, b)$ é um divisor comum de a e b, logo sendo o mdc o maior dentre esses divisores, segue que

$$c \times \text{mdc}(a, b) \leq \text{mdc}(a, b). \tag{3.2}$$

Como $c \geq 1$, temos que

$$\text{mdc}(a, b) \leq c \times \text{mdc}(a, b),$$

o que juntamente com a desigualdade (3.2) implica que $c = 1$. Agora, o resultado segue da equação (3.1). □

Podemos agora esclarecer o mistério a que nos referimos na Seção 1.7:

O mmc de dois números é igual ao seu produto se, e somente se, os dois números são primos entre si.

Problema 3.41. Seja n um número natural não nulo. Calcule $\text{mmc}(n, 2n + 1)$.

Problema 3.42. Suponha que n seja um número natural divisível por a e por b. Sabendo que $\text{mdc}(a, b) = 1$, mostre que n é divisível por $a \times b$.

3.8 Algoritmo do mdc de Euclides

O Lema de Euclides: *Dados inteiros a e b, os divisores comuns de a e b são os mesmos que os divisores comuns de a e $b - c \times a$, para todo número inteiro c fixado.*

Demonstração. Se d é um divisor comum de a e b, é claro que d é divisor comum de a e de $b - c \times a$.

Reciprocamente, suponha que d seja divisor comum de a e de $b - c \times a$. Logo, d é divisor comum de $b - c \times a$ e de $c \times a$ e, portanto, pelo Problema 3.13(c), tem-se que d é divisor de b. Assim, d é divisor comum de a e b. □

Esta simples observação, que generaliza a relação do Problema 3.13(c), vai nos dar um modo prático para calcular o mdc de dois números, mais eficiente do que o utilizado na Seção 3.3.

O Lema de Euclides nos diz que os divisores de comuns de a e b são os mesmos divisores comuns de a e $b - a \times c$, logo tomando o maior divisor comum em ambos os casos, obtemos a fórmula:

$$\text{mdc}(a, b) = \text{mdc}(a, b - a \times c),$$

o que permite ir diminuindo passo a passo a complexidade do problema, até torná-lo trivial.

Algoritmo de Euclides para o cálculo do mdc

Nada melhor do que um exemplo para entender o método.

Vamos calcular $\text{mdc}(a, b)$, onde $a = 162$ e $b = 372$.

Pelo Lema de Euclides, sabemos que o mdc de a e b é o mesmo que o de a e de b menos um múltiplo qualquer de a. Otimizamos os cálculos ao tomarmos o menor dos números da forma b menos um múltiplo de a e isto é realizado pelo algoritmo da divisão:

$$372 = 162 \times 2 + 48.$$

Assim,

$$\text{mdc}(372, 162) = \text{mdc}(372 - 162 \times 2, 162) = \text{mdc}(48, 162).$$

Apliquemos o mesmo argumento ao par $a_1 = 48$ e $b_1 = 162$:

$$162 = 48 \times 3 + 18.$$

Assim,

$$\begin{aligned} \text{mdc}(372, 162) &= \text{mdc}(162, 48) \\ &= \text{mdc}(162 - 48 \times 3, 48) \\ &= \text{mdc}(18, 48). \end{aligned}$$

Apliquemos novamente o mesmo argumento ao par $a_2 = 18$ e $b_2 = 48$:

$$48 = 18 \times 2 + 12.$$

Assim,

$$\text{mdc}(372, 162) = \text{mdc}(48, 18) = \text{mdc}(48 - 18 \times 2, 18) = \text{mdc}(12, 18).$$

Novamente, o mesmo argumento para o par $a_3 = 18$ e $b_3 = 12$ nos dá:

$$18 = 12 \times 1 + 6.$$

Assim,

$$\text{mdc}(372, 162) = \text{mdc}(18, 12) = \text{mdc}(18 - 12 \times 1, 12) = \text{mdc}(6, 12).$$

Finalmente, obtemos

$$\text{mdc}(372, 162) = \text{mdc}(12, 6) = \text{mdc}(12 - 6 \times 2, 6) = \text{mdc}(0, 6) = 6.$$

Logo,

$$\boxed{\text{mdc}(372, 162) = 6.}$$

O procedimento acima pode ser sistematizado como segue:

	2	3	2	1	2
372	162	48	18	12	6=mdc
48	18	12	6	0	

O Algoritmo de Euclides usado de trás para frente nos dá uma informação adicional fundamental.

Das igualdades acima podemos escrever:

$\textcircled{6} = 18 - 12 \times 1$

$12 = 48 - 18 \times 2$

$18 = 162 - 48 \times 3$

$48 = 372 - 162 \times 2$

Donde,

$$\begin{aligned} \textcircled{6} = 18 - 12 \times 1 &= 18 - (48 - 18 \times 2) \\ &= 18 \times 3 - 48 \\ &= (162 - 48 \times 3) \times 3 - 48 \\ &= 162 \times 3 - 48 \times 10 \\ &= 162 - (372 - 162 \times 2) \times 10 \\ &= 162 \times 23 - 372 \times 10. \end{aligned}$$

Assim, podemos escrever:

$$\textcircled{6} = \text{mdc}(372, 162) = 162 \times 23 + 372 \times (-10).$$

Este método sempre se aplica conduzindo ao seguinte importante resultado:

Teorema 3.3 (Relação de Bézout)**.** *Dados inteiros a e b, quaisquer, mas não ambos nulos, existem dois inteiros n e m tais que*

$$\text{mdc}(a, b) = a \times n + b \times m.$$

Problema 3.43. Determine $\text{mdc}(a, b)$, $\text{mmc}(a, b)$ e inteiros n e m tais que $\text{mdc}(a, b) = a \times n + b \times m$ para os seguintes pares de números a e b.

(a) $a = 728$ e $b = 1\,496$ (b) $a = 108$ e $b = 294$.

3.9 Aplicações da Relação de Bézout

Esta seção pode ser omitida sem prejuízo na primeira leitura, exceto a Proposição 3.3 que será utilizada na Seção 3.10.

Uma propriedade notável do máximo divisor comum que decorre da Relação de Bézout é a seguinte:

Se d é um divisor comum de dois números a e b, não simultaneamente nulos, então d divide $\text{mdc}(a, b)$.

De fato, sendo d um divisor de a e de b, temos que d é um divisor de todo número da forma $a \times n + b \times m$, logo, em particular, de $\text{mdc}(a, b)$.

Definindo

$$a\mathbb{Z} + b\mathbb{Z} = \{a \times n + b \times m;\ n, m \in \mathbb{Z}\},$$

temos o seguinte resultado:

Proposição 3.1. *Dados dois inteiros a e b, não ambos nulos, o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$ é* $\text{mdc}(a, b)$.

Demonstração. De fato, ponhamos $d = \text{mdc}(a, b)$. Como $d \mid a$ e $d \mid b$, temos que d divide todo elemento de $a\mathbb{Z} + b\mathbb{Z}$, logo d é menor ou igual do que qualquer elemento positivo de $a\mathbb{Z} + b\mathbb{Z}$. Pela Relação de Bézout, temos que $d \in a\mathbb{Z} + b\mathbb{Z}$, logo d é o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$. □

Daí decorre um importante critério para que dois números sejam primos entre si.

Proposição 3.2. *Dois números inteiros a e b são primos entre si se, e somente se, existem inteiros m e n tais que $a \times n + b \times m = 1$.*

Demonstração. Suponhamos que a e b sejam primos entre si, isto é, $\text{mdc}(a, b) = 1$. Como, pela Relação de Bézout, existem inteiros n e m tais que $a \times n + b \times m = \text{mdc}(a, b)$, segue que $a \times n + b \times m = 1$.

Reciprocamente, se existem n e m tais que $a \times n + b \times m = 1$, segue que 1 é o menor elemento positivo do conjunto $a\mathbb{Z} + b\mathbb{Z}$, logo ele é o mdc de a e b. Portanto, a e b são primos entre si. □

Problema 3.44. Sejam a e b dois números naturais não ambos nulos e c um terceiro número natural não nulo. Mostre que

$$\text{mdc}(c \times a, c \times b) = c \times \text{mdc}(a, b).$$

Problema 3.45. Sejam a, b e c três números naturais não nulos. Mostre que

$$\text{mmc}(c \times a, c \times b) = c \times \text{mmc}(a, b).$$

Outra propriedade fundamental que decorre da Relação de Bézout é o resultado a seguir:

Proposição 3.3. *Sejam a, b e c três inteiros tais que a divide $b \times c$ e a e b são primos entre si, então a divide c.*

Demonstração. Como $a \mid b \times c$, então existe um inteiro e tal que $b \times c = a \times e$. Como a e b são primos entre si, então existem inteiros n e m tais que $a \times n + b \times m = 1$. Multiplicando esta última

igualdade por c obtemos

$$a \times n \times c + b \times m \times c = c.$$

Substituindo aí $b \times c$ por $a \times e$, temos que

$$c = a \times n \times c + a \times e \times m = a \times (n \times c + e \times m),$$

mostrando que $a \mid c$. □

A série de problemas a seguir nos permitirá deduzir a unicidade referida no Teorema Fundamental da Aritmética.

Problema 3.46. Sejam a um número inteiro qualquer e p um número primo. Mostre que uma das seguintes possibilidades acontece: $p \mid a$ ou $\text{mdc}(a, p) = 1$.

Problema 3.47. Sejam a e b dois inteiros e p um número primo. Mostre que se $p \mid a \times b$, então $p \mid a$ ou $p \mid b$.

Problema 3.48. Sejam p, p_1 e p_2 três números primos. Mostre que se $p \mid p_1 \times p_2$, então $p = p_1$ ou $p = p_2$.

A propriedade acima pode se generalizar como segue:

Se $p, p_1, p_2, \ldots, p_r$ são números primos e se $p \mid p_1 \times p_2 \times \cdots \times p_r$, então para algum índice i tem-se que $p = p_i$.

Problema 3.49. Mostre que se $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ são duas coleções de números primos e se

$$p_1 \times \cdots \times p_r = q_1 \times \cdots \times q_s,$$

então $r = s$ e reordenando $q_1, \ldots q_r$, se necessário, tem-se que $p_1 = q_1, \ \ldots, \ p_r = q_r$.

Este último problema é a prova da unicidade da escrita como produto de primos de qualquer número natural maior do que 1, contida no enunciado do Teorema Fundamental da Aritmética.

Seja n um número natural escrito na sua decomposição em fatores primos como

$$n = p_1^{a_1} \times \cdots \times p_r^{a_r},$$

e seja n' um divisor positivo de n. Logo na decomposição de n' em fatores primos só podem aparecer os fatores primos $p_1, \ldots, p_r$, com expoentes $b_1, \ldots, b_r$, respectivamente, satisfazendo

$$0 \leq b_1 \leq a_1, \quad \ldots, \quad 0 \leq b_r \leq a_r. \tag{3.3}$$

Note que permitimos que alguns dos b_i sejam nulos, pois o correspondente primo p_i pode não constar da fatoração de n'.

Por exemplo, os divisores positivos de $60 = 2^2 \times 3 \times 5$ são:

$$\begin{array}{lll} 2^0 \times 3^0 \times 5^0 = 1, & 2^0 \times 3^1 \times 5^0 = 3, & 2^0 \times 3^0 \times 5^1 = 5 \\ 2^0 \times 3^1 \times 5^1 = 15, & 2^1 \times 3^0 \times 5^0 = 2, & 2^1 \times 3^1 \times 5^0 = 6, \\ 2^1 \times 3^0 \times 5^1 = 10, & 2^1 \times 3^1 \times 5^1 = 30, & 2^2 \times 3^0 \times 5^0 = 4, \\ 2^2 \times 3^1 \times 5^0 = 12, & 2^2 \times 3^0 \times 5^1 = 20, & 2^2 \times 3^1 \times 5^1 = 60. \end{array}$$

O número de divisores de $n = p_1^{a_1} \times \cdots \times p_r^{a_r}$ é exatamente o número de números inteiros $b_1, \ldots, b_r$ satisfazendo às desigualdades

(3.3), logo esse número é

$$(a_1 + 1) \times \cdots \times (a_r + 1).$$

Problema 3.50. Ache os divisores positivos de 40 e de 120. Quais são todos os divisores?

Problema 3.51. Quantos divisores positivos tem o número $6^3 \times 25$?

É fácil determinar o mdc e o mmc de dois números decompostos em fatores primos.Por exemplo, se

$$a = 2^3 \times 3^5 \times 7^3 \times 17 \text{ e } b = 3^4 \times 7^5 \times 19,$$

temos que $\text{mdc}(a, b) = 2^0 \times 3^4 \times 7^3$, enquanto

$$mmc(a, b) = 2^3 \times 3^5 \times 7^5 \times 17 \times 19.$$

Os números a e b acima podem ser representados como produtos de potências dos mesmos primos, com o artifício de introduzir fatores extras da forma p^0 $(= 1)$ para certos números primos p. Mais precisamente, podemos escrever

$$a = 2^3 \times 3^5 \times 7^3 \times 17 \times 19^0 \text{ e } b = 2^0 \times 3^4 \times 7^5 \times 17^0 \times 19.$$

Problema 3.52. Ache o mdc e mmc dos números $a = 1\,080$ e $b = 210$.

Problema 3.53. Dados $a = p_1^{a_1} \times \cdots \times p_r^{a_r}$ e $b = p_1^{b_1} \times \cdots \times p_r^{b_r}$ dois números decompostos em fatores primos, escritos ambos como produtos de potências dos mesmos primos, onde $a_1 \geq 0, \ldots, a_r \geq 0$ e

$b_1 \geq 0, \ldots, b_r \geq 0$, mostre que

$$\text{mdc}(a,b) = p_1^{c_1} \times \cdots \times p_r^{c_r} \quad \text{e} \quad \text{mmc}(a,b) = p_1^{d_1} \times \cdots \times p_r^{d_r},$$

onde

$$c_i = \min\{a_i, b_i\} \ \text{ e } \ d_i = \max\{a_i, b_i\}, \quad i = 1, \ldots, r.$$

Mostre como obter disto uma nova prova da igualdade

$$\text{mdc}(a,b)\text{mmc}(c,b) = ab.$$

O leitor não deve se iludir sobre a facilidade em calcular o mdc e o mmc com o método acima, pois para utilizá-lo é necessário que os dois números estejam decompostos em fatores primos. Se os dois números são grandes e não são dados na forma fatorada, é muito trabalhoso fatorá-los para calcular o mdc ou o mmc, sendo, nesse caso, muito mais eficiente o Algoritmo de Euclides.

3.10 Equações Diofantinas Lineares

A resolução de muitos problemas de aritmética depende da resolução de equações do tipo $ax + by = c$, onde a, b e c são números inteiros dados e x e y são incógnitas a serem determinadas em $\mathbb{Z}$. Um exemplo típico de um problema modelado por este tipo de equação é o seguinte:

Problema 3.54. De quantos modos podemos comprar selos de cinco e de três reais, de modo a gastar cinquenta reais?

Dada uma equação, as perguntas naturais que se colocam são as seguintes:

1) Quais são as condições para que a equação possua solução?

2) Quantas são as soluções?

3) Como calcular as soluções, caso existam?

Daremos a seguir respostas a essas perguntas no caso das equações em questão.

A primeira pergunta admite a resposta a seguir.

Teorema 3.4. *A equação diofantina* $ax + by = c$ *admite solução se, e somente se,* $\text{mdc}(a, b)$ *divide* c*.*

Demonstração. Suponha que a equação admita uma solução x_0, y_0. Então vale a igualdade $ax_0 + by_0 = c$. Como $\text{mdc}(a, b)$ divide a e divide b, segue que ele divide $ax_0 + by_0$, logo divide c.

Reciprocamente, suponha que $\text{mdc}(a, b)$ divida c, ou seja $c = \text{mdc}(a, b) \times d$, para algum inteiro d. Por outro lado, sabemos que existem inteiros n e m tais que

$$\text{mdc}(a, b) = a \times n + b \times m.$$

Multiplicando ambos os lados da igualdade acima por d, obtemos

$$c = \text{mdc}(a, b) \times d = a \times (n \times d) + b \times (m \times d).$$

Logo, a equação diofantina $ax + by = c$ admite pelo menos a

solução

$$x = n \times d \quad \text{e} \quad y = m \times d.$$

□

Problema 3.55. Diga quais são as equações diofantinas a seguir que possuem pelo menos uma solução:

(a) $3x + 5y = 223$ (b) $5x + 15y = 33$ (c) $2x + 16y = 2\,354$

(d) $3x + 12y = 312$ (e) $23x + 150y = 12\,354$ f) $7x + 14y = 77$

Problema 3.56. Mostre que se a e b são números inteiros tais que $\text{mdc}(a, b) = 1$, então toda equação diofantina $ax + by = c$ possui solução, independentemente do valor de c.

Problema 3.57. Para quais valores de c, onde c é inteiro, a equação $30x + 42y = c$ admite soluções inteiras?

Se a equação $ax + by = c$ admite uma solução, então o número $d = \text{mdc}(a, b)$ divide c e, portanto, temos que $a = a' \times d$, $b = b' \times d$ e $c = c' \times d$, onde $\text{mdc}(a', b') = 1$ (Problema 3.17).

Assim, é imediato verificar que x_0, y_0 é uma solução da equação $ax + by = c$ se, e somente se, é solução da equação $a'x + b'y = c'$, onde agora $\text{mdc}(a', b') = 1$.

Portanto, toda equação diofantina linear que possui solução é equivalente a uma equação reduzida, ou seja, da forma

$$ax + by = c, \quad \text{com} \quad \text{mdc}(a, b) = 1.$$

O próximo resultado nos dará uma fórmula para resolver a equação diofantina linear $ax + by = c$, onde $\text{mdc}(a, b) = 1$, conhecida uma solução particular x_0 e y_0 da equação.

Teorema 3.5. *Seja x_0 e y_0 uma solução particular, arbitrariamente dada, da equação $ax + by = c$, onde $\text{mdc}(a, b) = 1$. Então as soluções da equação são da forma $x = x_0 + tb$ e $y = y_0 - ta$, para t variando em $\mathbb{Z}$.*

Demonstração. Se x, y é uma solução qualquer da equação, temos que

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

donde

$$a(x - x_0) = b(y_0 - y). \tag{3.4}$$

Daí segue que $a \mid b(y_0 - y)$ e $b \mid a(x - x_0)$. Como $\text{mdc}(a, b) = 1$, da Proposição 3.3 segue que $a \mid (y_0 - y)$ e $b \mid (x - x_0)$. Assim,

$$y_0 - y = ta \quad \text{e} \quad x - x_0 = sb, \tag{3.5}$$

para alguns inteiros t e s. Substituindo esse valores em (3.4), obtemos

$$asb = bta,$$

o que implica que $s = t$. Logo, de (3.5), temos que a solução é dada por $x = x_0 + tb$ e $y = y_0 - ta$.

Reciprocamente, se $x = x_0 + bt$ e $y = y_0 - at$, substituindo esses valores na equação $ax + by = c$, obtemos

$$a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 + abt - bat = ax_0 + by_0 = c.$$

□

Por exemplo, a equação $3x + 5y = 50$ admite a solução particular $x_0 = 0$ e $y_0 = 10$. Assim, a solução geral dessa equação é dada por $x = 0 + 5t$ e $y = 10 - 3t$. Se estivermos à procura de soluções não negativas então deveríamos ter $10 - 3t \geq 0$, o que implica que $t = 0, 1, 2$ ou 3. Assim, o Problema 3.54 admite as seguintes soluções:

(a) 10 selos de 5 reais.

(b) 5 selos de 3 reais e 7 selos de 5 reais.

(c) 10 selos de 3 reais e 4 selos de 5 reais.

(d) 15 selos de 3 reais e um selo de 5 reais.

O único verdadeiro trabalho que se tem para resolver uma equação diofantina linear $ax + by = c$ é calcular $\text{mdc}(a, b)$ para verificar se divide ou não c e descobrir uma solução particular x_0, y_0. O primeiro problema se resolve utilizando o algoritmo de Euclides para o cálculo do mdc. Quanto ao segundo, o de determinar uma solução particular da equação, procede-se por inspeção se a e b são números pequenos. Caso a ou b seja grande, podemos usar o algoritmo de Euclides de trás para a frente para determinar inteiros n e m tais que

$$an + bm = \text{mdc}(a, b) = 1,$$

e depois multiplicar ambos os membros da equação acima por c, ob-

tendo

$$a(nc) + b(mc) = c,$$

dando-nos a solução particular $x_0 = nc$ e $y_0 = mc$.

Problema 3.58. De que maneiras podemos comprar selos de cinco e de sete reais, de modo a gastar cem reais?

Problema 3.59. Se um macaco sobe uma escada de dois em dois degraus, sobra um degrau; se ele sobe de três em três degraus, sobram dois degraus. Quantos degraus a escada possui, sabendo que o número de degraus é múltiplo de sete e está compreendido entre 40 e 100.

Problema 3.60. Mostre que nenhum número pode deixar resto 5 quando dividido por 12 e resto 4 quando dividido por 15.

Problema 3.61. Ache todos os números naturais que quando divididos por 18 deixam resto 4 e quando divididos por 14 deixam resto 6.

Capítulo 4

A Aritmética dos Restos

4.1 Congruências

Vamos agora introduzir a grande ideia de Gauss de desenvolver uma aritmética dos restos da divisão por um certo número fixado, o que já foi explorado nas Seções 2.2 e 2.3.

Definição. Seja dado um número inteiro m maior do que 1. Diremos que dois números inteiros a e b são *congruentes módulo* m se a e b possuírem mesmo resto quando divididos por m. Neste caso, simbolizaremos esta situação como segue:

$$a \equiv b \mod m.$$

Quando a e b não são congruentes módulo m, escreve-se

$$a \not\equiv b \mod m.$$

Exemplos:

1) $15 \equiv 8 \bmod 7$, pois o restos das divisões de 15 e de 8 por 7 são os mesmos (iguais a 1).

2) $27 \equiv 32 \bmod 5$, pois os restos das divisões de 27 e 32 por 5 são os mesmos (iguais a 2).

3) $31 \not\equiv 29 \bmod 3$, pois o resto da divisão de 31 por 3 é 1, enquanto o resto da divisão de 29 por 3 é 2.

Para mostrar que $a \equiv b \bmod m$ não é necessário efetuar a divisão de a e de b por m, como mostrado a seguir.

Proposição 4.1. *Tem-se que* $a \equiv b \mod m$ *se e somente se* m *divide* $b - a$.

Demonstração. De fato, pelo algoritmo da divisão, podemos escrever

$$a = mq_1 + r_1 \quad \text{e} \quad b = mq_2 + r_2,$$

onde $0 \leq r_1 < m$ e $0 \leq r_2 < m$. Sem perda de generalidade, podemos supor que $r_1 \leq r_2$ (se o contrário ocorrer, basta trocar os papéis de r_1 e r_2). Assim, podemos escrever

$$b - a = m(q_2 - q_1) + r_2 - r_1.$$

Logo, m divide $b - a$ se, e somente se, m divide $r_2 - r_1$. Por ser $0 \leq r_2 - r_1 < m$, segue que m divide $b - a$ se e somente se $r_2 - r_1 = 0$, ou seja, se e somente se $r_2 = r_1$. □

Problema 4.1. Verifique se são verdadeiras ou falsas as seguintes afirmações:

$35 \equiv 27 \bmod 4$; $72 \equiv 32 \bmod 5$; $83 \equiv 72 \bmod 5$; $78 \equiv 33 \bmod 9$.

Problema 4.2. Se $a \equiv b \bmod 4$, mostre que $a \equiv b \bmod 2$.

Problema 4.3. Mostre que $10^n \equiv 1 \bmod 9$, para todo número natural n.

SUGESTÃO: Veja o início da Seção 2.3.

Problema 4.4. Dados a, b e c inteiros quaisquer e m um inteiro maior do que 1, mostre as seguintes afirmações:

(a) $a \equiv a \bmod m$.

(b) Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$.

(c) Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$.

Pela definição, as congruências módulo m tem tudo a ver com os restos da divisão por m. A seguir exploramos mais a fundo esta relação.

Segue-se, da definição de congruência módulo m e das propriedades do problema acima, o seguinte fato:

Todo número inteiro a é congruente módulo m a um e somente um dos números $0, 1, \ldots, m-1$.

De fato, os possíveis restos da divisão de a por m são precisamente os números $0, 1, \ldots, m-1$, cujos restos da divisão por m são eles próprios, logo dois a dois não congruentes módulo m.

Problema 4.5. Sejam a um número inteiro qualquer e m um inteiro maior do que 1. Suponha que r seja um número inteiro tal que $0 \leq r < m$ e $a \equiv r \bmod m$. Mostre que r é o resto da divisão de a por m.

SUGESTÃO: Utilize a unicidade da escrita no Algoritmo da Divisão.

4.2 Critérios de Multiplicidade e Restos

É fácil determinar o resto da divisão de um inteiro n por 2, pois esse é 0 ou 1, dependendo de n ser par ou ímpar.

Para facilitar a determinação do resto da divisão de um inteiro n por 3 ou por 9, podemos utilizar os conhecimentos já adquiridos, evitando o trabalho de efetuar a divisão em questão.

De fato, sabemos da Seção 2.3 que se $n_r \dots n_1 n_0$ é a escrita de n no sistema decimal, então

$$n - (n_r + \cdots + n_1 + n_0) = (10^r - 1)n_r + \cdots + (10 - 1)n_1.$$

Como o segundo membro da igualdade acima é divisível por 3 e por 9, o mesmo ocorre com o primeiro membro, logo

$$n \equiv (n_r + \cdots + n_1 + n_0) \bmod 3; \text{ e } \bmod 9.$$

Assim, pela definição de congruência, temos os seguintes fatos:

O resto da divisão por 3 (*respectivamente por* 9) *de um número* $n = n_r \dots n_1 n_0$*, escrito no sistema decimal, é igual ao resto da divisão por* 3 (*respectivamente por* 9) *do número* $n_r + \cdots + n_1 + n_0$.

Problema 4.6. Determine os restos da divisão por 3 e por 9 dos números: 3 254, 12 736, 54 827, 33 875 435, 57 612 510.

Da Seção 2.2 também sabemos que todo número n é da forma $n = n_0 + 10m$, onde n_0 é o algarismo das unidades de n. Assim, $n \equiv n_0 \bmod 5$ e $n \equiv n_0 \bmod 10$. Isto acarreta que:

Os restos da divisão de n por 5 e por 10 são, respectivamente, os restos da divisão de n_0 por 5 e por 10.

Problema 4.7. Determine os restos da divisão por 5 e por 10 dos números: 3 254, 12 736, 54 827, 33 875 435, 57 612 510.

Problema 4.8. Descreva critérios semelhantes aos estabelecidos acima para determinar os restos da divisão de um número por $4, 8, 25$ e 125.

Problema 4.9. Determine os restos da divisão por 4, 8, 25 e 125 dos números: 3 254, 12 736, 54 827, 33 875 435, 57 612 510.

As congruências possuem propriedades operatórias notáveis que exploraremos a seguir.

4.3 Congruências e Somas

Proposição 4.2. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja m um inteiro maior do que 1. Se $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então $a_1 \pm a_2 \equiv b_1 \pm b_2 \bmod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então

m divide $b_1 - a_1$ e divide $b_2 - a_2$. Logo

$$m \text{ divide } (b_1 - a_1) \pm (b_2 - a_2) = (b_1 \pm b_2) - (a_1 \pm a_2),$$

mostrando que $b_1 \pm b_2 \equiv a_1 \pm a_2 \bmod m$. □

Conclui-se que as congruências de mesmo módulo somam-se e subtraem-se membro a membro tal qual as igualdades.

Problema 4.10. Suponha que $a \equiv b \bmod m$. Mostre que

$$a \pm c \equiv b \pm c \bmod m,$$

qualquer que seja o inteiro c.

Problema 4.11. Suponha que $a \pm c \equiv b \pm c \bmod m$, mostre que $a \equiv b \bmod m$.

Considere agora dois inteiros a e b cujos restos na divisão por m sejam respectivamente r_1 e r_2.

Então temos que

$$a \equiv r_1 \bmod m \quad \text{e} \quad b \equiv r_2 \bmod m.$$

Assim,

$$a + b \equiv r_1 + r_2 \bmod m.$$

Seja r o resto da divisão de $r_1 + r_2$ por m; logo

$$a + b \equiv r_1 + r_2 \equiv r \bmod m, \quad \text{com } 0 \leq r < m.$$

Logo, pelo Problema 4.5, o resto da divisão de $a + b$ por m é o número r.

Assim, acabamos de verificar o seguinte fato:

O resto da divisão da soma $a + b$ de dois números a e b por um outro número $m > 1$ depende apenas dos restos da divisão de a e de b por m e não desses números em si.

Esse fato generaliza o que foi dito nas Seções 3.5 e 3.6, onde os casos $m = 2$ e $m = 3$ foram analisados.

Problema 4.12. Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine os restos da divisão de $a + b$, $a - b$ e de $b - a$ por 7

SUGESTÃO: Para o último resto, observe que $-4 \equiv 3 \bmod 7$.

Problema 4.13. Sem efetuar as somas e subtrações indicadas, determine os restos da divisão por $2, 3, 4, 5, 8, 9, 10, 25$ e 125 do número $3\,534\,785 + 87\,538 - 9\,535\,832$.

4.4 Congruências e Produtos

Proposição 4.3. *Sejam a_1, a_2, b_1, b_2 inteiros quaisquer e seja m um inteiro maior do que 1. Se $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então $a_1 \times a_2 \equiv b_1 \times b_2 \bmod m$.*

Demonstração. De fato, como $a_1 \equiv b_1 \bmod m$ e $a_2 \equiv b_2 \bmod m$, então

m divide $a_1 - b_1$ e $a_2 - b_2$. Por outro lado, como

$$a_1 \times a_2 - b_1 \times b_2 = a_1 \times (a_2 - b_2) + b_2 \times (a_1 - b_1),$$

segue que m divide $a_1 \times a_2 - b_1 \times b_2$, o que prova o resultado. □

Conclui-se que as congruências de mesmo módulo multiplicam-se membro a membro tal qual as igualdades.

Problema 4.14. Suponha que $a \equiv b \bmod m$. Mostre que

$$a \times c \equiv b \times c \bmod m,$$

qualquer que seja o inteiro c.

Repetidas aplicações da Proposição 4.3 fornecem o seguinte resultado:

Se $a \equiv b \bmod m$, então $a^n \equiv b^n \bmod m$, para todo n natural.

Sejam a e b dois inteiros cujos restos da divisão por m sejam respectivamente r_1 e r_2.

Então temos que

$$a \equiv r_1 \bmod m \quad \text{e} \quad b \equiv r_2 \bmod m.$$

Assim,

$$a \times b \equiv r_1 \times r_2 \bmod m.$$

Seja r o resto da divisão de $r_1 \times r_2$ por m; logo

$$a \times b \equiv r_1 \times r_2 \equiv r \bmod m, \quad \text{com} \quad 0 \leq r < m.$$

Logo, pelo Problema 4.5, o resto da divisão de $a \times b$ por m é o número r.

Assim, acabamos de verificar que, como no caso da adição, vale também seguinte fato para a multiplicação:

O resto da divisão do produto $a \times b$ de dois números a e b por um outro número $m > 1$ depende apenas dos restos da divisão de a e de b por m e não desses números em si.

Isso também generaliza para a multiplicação o que foi dito nas Seções 3.5 e 3.6, onde os casos $m = 2$ e $m = 3$ foram analisados.

Problema 4.15. Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine o resto da divisão de $a \times b$ por 7.

Problema 4.16. Sem efetuar as multiplicações indicadas, determine os restos da divisão por $2, 3, 4, 5, 8, 9, 10, 25$ e 125 do número $5\,327\,834^3 \times 3\,842\,536^2 \times 9\,369\,270\,001^{20}$.

Note que $2 \times 3 \equiv 2 \times 6 \bmod 6$, mas no entanto $3 \not\equiv 6 \bmod 6$. Portanto, no caso das congruências não vale um cancelamento análogo ao caso da igualdade.

Problema 4.17. Sejam a, b, c e m números inteiros e com $m > 1$. Mostre que se $a \times c \equiv b \times c \bmod m$ e se $\text{mdc}(c, m) = 1$, então $a \equiv b \bmod m$.

SUGESTÃO: Utilize a Proposição 3.3.

4.5 Algumas Aplicações

1. Um critério de divisibilidade por 6

Observe inicialmente que

$10 \equiv 4 \bmod 6$,

$10^2 \equiv 4^2 \equiv 4 \bmod 6$,

$10^3 \equiv 10^2 \times 10 \equiv 4 \times 4 \equiv 4 \bmod 6$,

$10^4 \equiv 10^3 \times 10 \equiv 4 \times 4 \equiv 4 \bmod 6$.

Você tem ainda alguma dúvida de que $10^i \equiv 4 \bmod 6$, para todo número natural $i > 0$?

Assim, se um número natural n é escrito no sistema decimal como $n_r \ldots n_1 n_0$, temos que

$$n = n_0 + 10n_1 + 10^2 n_2 + \cdots + 10^r n_r \equiv n_0 + 4n_1 + 4n_2 + \cdots + 4n_r \bmod 6.$$

Com isto, temos que o resto da divisão de n por 6 é igual ao resto da divisão de $n_0 + 4n_1 + 4n_2 + \cdots + 4n_r$ por 6.

Logo, provamos que:

Um número $n = n_r \ldots n_1 n_0$ *é divisível por* 6 *se e somente se* $n_0 + 4n_1 + 4n_2 + \cdots + 4n_r$ *é divisível por* 6.

Problema 4.18. Ache o resto da divisão por 6 do número 3 215 529.

2. Um critério de divisibilidade por 7, 11 e 13

Note que $7 \times 11 \times 13 = 1\,001$. Logo,

$$1\,000 \equiv -1 \bmod 7, \quad 1\,000 \equiv -1 \bmod 11 \text{ e } 1\,000 \equiv -1 \bmod 13.$$

Assim, módulo 7, 11 e 13, temos que

$10^3 \equiv -1$,

$10^6 \equiv (-1)^2 \equiv 1$,

$10^9 \equiv (-1)^3 \equiv -1$,

$10^{12} \equiv (-1)^4 \equiv 1$,

etc.

Escrevendo um número n na representação decimal como $n_r \ldots n_2 n_1 n_0$, temos, módulo 7, 11 ou 13, que

$$\begin{aligned} n &= n_0 n_1 n_2 + n_3 n_4 n_5 \times 10^3 + n_6 n_7 n_8 \times 10^6 + \cdots \\ &\equiv n_0 n_1 n_2 - n_3 n_4 n_5 + n_6 n_7 n_8 - \cdots . \end{aligned}$$

Assim, o resto da divisão de n por 7,11 ou 13 é igual ao resto da divisão de $n_0 n_1 n_2 - n_3 n_4 n_5 + n_6 n_7 n_8 - \cdots$ por 7, 11 ou 13, respectivamente.

Desse modo, obtemos o seguinte critério de divisibilidade por 7, 11 ou 13:

O número $n_r \ldots n_2 n_1 n_0$ é divisível por 7, 11 *ou* 13 *se, e somente se, o número $n_0 n_1 n_2 - n_3 n_4 n_5 + n_6 n_7 n_8 - \cdots$ é divisível por* 7, 11 *ou* 13, *respectivamente.*

Problema 4.19. Ache o resto da divisão por 7, 11 e 13 do número 3 215 529.

Problema 4.20. Mostre que $10^i \equiv (-1)^i \bmod 11$, para todo natural i. Deduza este outro critério de divisibilidade por 11:

Um número $n_r \dots n_2 n_1 n_0$ é divisível por 11 *se, e somente se, o número $n_0 - n_1 + n_2 - \cdots$ é divisível por* 11.

3. Os restos da divisão das potências de 2 por 7

Observe que

$$2^1 \equiv 2 \bmod 7,$$

$$2^2 \equiv 4 \bmod 7,$$

$$2^3 \equiv 1 \bmod 7.$$

Dado um número inteiro n, pelo algoritmo da divisão, podemos escrevê-lo na forma $n = 3q + r$, onde $r = 0, 1$ ou 2.

Assim,

$$2^n = 2^{3q+r} = (2^3)^q \times 2^r \equiv 2^r \bmod 7.$$

Por exemplo, se $n = 132 = 3 \times 44$, então $2^{132} \equiv 1 \bmod 7$, pois $r = 0$.

Se $n = 133 = 3 \times 44 + 1$, então $2^{133} \equiv 2 \bmod 7$, pois $r = 1$.

Se $n = 134 = 3 \times 44 + 2$, então $2^{134} \equiv 4 \bmod 7$, pois $r = 2$.

Problema 4.21. Ache o resto da divisão por 7 dos seguintes números: $2^{5\,345}$, $2^{3\,765\,839}$, $2^{10^{10}}$.

Problema 4.22. Sabendo que $2^4 = 16 \equiv -1 \bmod 17$, ache o resto da divisão de 2^{30} por 17.

Problema 4.23. Determine o resto da divisão de 2^{325} por 17.

4. A equação diofantina $x^3 - 117y^3 = 5$

Esta equação possui uma história curiosa que é relatada no livro de S. Collier citado na bibliografia.

Vamos mostrar que esta equação não possui soluções inteiras. De fato, suponhamos, por absurdo, que x_0, y_0 seja uma solução inteira da equação. Então

$$x_0^3 \equiv 5 \bmod 9, \tag{4.1}$$

já que $117 \equiv 0 \bmod 9$.

Mas, sendo x_0 congruente a $0, 1, 2, 3, 4, 5, 6, 7$ ou 8 módulo 9, segue por contas elementares que x_0^3 é congruente a $0, 1$ ou 8, módulo 9. Logo, a congruência (4.1) não possui solução, o que fornece uma contradição.

Problema 4.24. Mostre que a equação diofantina

$$x^2 + y^2 + z^2 = 8w + 7$$

não possui soluções x, y, z, w inteiros.

SUGESTÃO: Reduza a equação módulo 8 e mostre que

$$x_0^2 + y_0^2 + z_0^2 \equiv 7 \bmod 8$$

nunca ocorre.

5. Os números da forma $3^{6n} - 2^{6n}$ são divisíveis por 35

Temos que

$$3^6 = 3^3 \times 3^3 \equiv (-1) \times (-1) \equiv 1 \bmod 7,$$
$$2^6 = 2^3 \times 2^3 \equiv 1 \times 1 \equiv 1 \bmod 7.$$

Por outro lado,

$$3^6 = 3^3 \times 3^3 \equiv 2 \times 2 \equiv -1 \bmod 5,$$
$$2^6 = 2^3 \times 2^3 \equiv 3 \times 3 \equiv -1 \bmod 5.$$

Logo, $3^{6n} - 2^{6n} \equiv 0 \bmod 7$ e $3^{6n} - 2^{6n} \equiv 0 \bmod 5$.

Assim, $3^{6n} - 2^{6n}$ é divisível por 5 e por 7 e como $\text{mdc}(5, 7) = 1$, segue, do Problema 3.42, que $3^{6n} - 2^{6n}$ é divisível por 35.

Problema 4.25. Mostre que todo número da forma $19^{8n} - 1$ é divisível por 17.

Problema 4.26. Mostre que todo número da forma $13^{3n} + 17^{3n}$ é divisível por 45, quando n é ímpar.

6. Euler tinha razão, Fermat estava enganado!

Na Seção 2.4 nos perguntamos se o número 4 294 967 297 era primo ou composto?

De fato, esse número corresponde a $n = 5$ dos chamados números de Fermat que são da forma:

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

Fermat afirmou que esses números, para qualquer valor natural de n, eram primos e dava como exemplos $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65\,537$, que são efetivamente primos.

No entanto, o número $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$ era muito grande para se poder verificar se era primo ou não.

Euler, estudando a forma dos divisores de um número do tipo de F_n, chegou à conclusão de que se F_5 fosse composto, ele deveria ser divisível pelo primo 641.

Euler, um exímio calculista, mostrou que 641 divide F_5 com uma verificação semelhante a que segue:[1]

Observemos inicialmente que $641 = 5 \times 2^7 + 1$, logo

$$5 \times 2^7 \equiv -1 \bmod 641.$$

Elevando à quarta potência ambos os membros da congruência acima, obtemos

$$5^4 \times 2^{28} \equiv 1 \bmod 641. \tag{4.2}$$

Por outro lado, da igualdade $641 = 5^4 + 2^4$ (verifique!), obtemos que

$$5^4 \equiv -2^4 \bmod 641. \tag{4.3}$$

[1] Fizemos uma adaptação do argumento de Euler, pois no seu tempo ainda não existia a noção de congruência.

Juntando (4.2) e (4.3), obtemos que $-2^{32} \equiv 1 \bmod 641$, o que implica $F_5 = 2^{32} + 1 \equiv 0 \bmod 641$, donde 641 divide F_5. Portanto, F_5 não é primo.

4.6 Aritmética Modular

A Aritmética Modular foi introduzida por Gauss no seu livro *Disquisitiones Aritmeticae* publicado em 1801.

Fixado um número inteiro $m > 1$, vamos associar a um número inteiro a qualquer o símbolo $\overline{a}$ representando o resto da sua divisão por m, tal qual fizemos nas Seções 3.5 e 3.6, nos casos $m = 2$ e $m = 3$.

Portanto, dados dois números a e b tem-se que $\overline{a} = \overline{b}$ se, e somente se, os restos da divisão de a e de b por m são iguais, ou seja,

$$\overline{a} = \overline{b} \text{ se, e somente se, } a \equiv b \bmod m.$$

Sendo todos os possíveis restos da divisão por m os números $0, 1, 2, \ldots, m-1$, temos qualquer $\overline{a}$ é igual a um dos seguintes: $\overline{0}, \overline{1}, \ldots, \overline{m-1}$.

Nas Seções 4.3 e 4.4 observamos que os restos da divisão da soma e do produto de dois números não dependem dos números em si, mas apenas dos restos da divisão desses números. Sendo assim, para achar $\overline{(a+b)}$ e $\overline{(a \times b)}$ só precisamos saber como operar aditivamente e multiplicativamente com os símbolos $\overline{a}$ e $\overline{b}$, que são justamente elementos da forma $\overline{0}, \overline{1}, \ldots, \overline{m-1}$, a exemplo do que fizemos nas seções 3.5 e 3.6, nos casos $m = 2$ e $m = 3$.

Aritmética módulo m = 4

Para efeito de ilustração, tomemos o caso $m = 4$. Neste caso, temos apenas os símbolos $\overline{0}$, $\overline{1}$, $\overline{2}$ e $\overline{3}$ a considerar.

Pede-se ao leitor verificar as seguintes tabelas:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note que diferentemente da aritmética dos números inteiros, surge um novo fenômeno: $\overline{2} \neq \overline{0}$ e, no entanto, $\overline{2} \times \overline{2} = \overline{0}$.

Problema 4.27. Mostre que se $i = 0, 1, 2, 3$, então $\overline{-i} = \overline{4 - i}$.

Problema 4.28. Determine o resto da divisão por 4 do número: $45\,769\,834^{532} \times 63\,876^{1\,654} + 87\,987\,545^{1\,345\,874} - 95\,973\,434$

Aritmética módulo m = 5

Analisaremos agora o caso $m = 5$. Neste caso, temos apenas os símbolos $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ e $\overline{4}$ a considerar.

Pede-se ao leitor verificar as seguintes tabelas:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Note que aqui volta a valer a regra: se $\overline{a} \neq \overline{0}$ e $\overline{b} \neq \overline{0}$, então $\overline{a} \times \overline{b} \neq \overline{0}$.

Problema 4.29. Mostre que se $i = 0, 1, 2, 3, 4$, então $\overline{-i} = \overline{5 - i}$.

Problema 4.30. Determine o resto da divisão por 5 do número:

$$45\,769\,834^{532} \times 63\,876^{1\,654} + 87\,987\,545^{1\,345\,874} - 95\,973\,434$$

Problema 4.31. Determine as tabelas da adição e da multiplicação para $m = 6$ e para $m = 7$. Que diferenças você nota entre os dois casos?

Capítulo 5

Problemas Suplementares

Apresentaremos neste capítulo uma lista de problemas mais desafiadores do que aqueles que se encontram no texto, cujo objetivo se restringia a complementá-lo, além de testar a compreensão do leitor nos conceitos apresentados.

Nos dois primeiros capítulos apresentamos a linguagem básica e os resultados fundamentais, sem os quais não seria possível enunciar, muito menos resolver, problemas mais elaborados. Os problemas propostos a seguir dizem respeito ao material exposto nos Capítulos 3 e 4. Os problemas marcados com asterisco têm um grau de dificuldade maior que os demais.

Antes porém de iniciar os problemas propriamente ditos, relacionamos a seguir algumas identidades muito úteis na resolução de alguns dos problemas.

Expressões do tipo $a^n - 1$, com n qualquer

$$\begin{aligned}
a^2 - 1 &= (a-1)(a+1) \\
a^3 - 1 &= (a-1)(a^2+a+1) \\
a^4 - 1 &= (a-1)(a^3+a^2+a+1) \\
a^5 - 1 &= (a-1)(a^4+a^3+a^2+a+1)
\end{aligned}$$

Em geral,

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

Expressões do tipo $a^m - 1$, com m par

$$\begin{aligned}
a^2 - 1 &= (a+1)(a-1) \\
a^4 - 1 &= (a+1)(a^3-a^2+a-1) \\
a^6 - 1 &= (a+1)(a^5-a^4+a^3-a^2+a-1)
\end{aligned}$$

Em geral,

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

Expressões do tipo $a^m + 1$, com m ímpar

$$\begin{aligned}
a^3 + 1 &= (a+1)(a^2-a+1) \\
a^5 + 1 &= (a+1)(a^4-a^3+a^2-a+1) \\
a^7 + 1 &= (a+1)(a^6-a^5+a^4-a^3+a^2-a+1)
\end{aligned}$$

Em geral,

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

Problemas sobre o Capítulo 3

S-3.1 Mostre que todo número inteiro não nulo a se escreve de modo único na forma $a = 2^r b$, onde $r \in \mathbb{N}$ e b é um número ímpar. O número 2^r é a maior potência de 2 que divide a. Generalize esta propriedade para um primo p qualquer no lugar de 2.

S-3.2

(a) Quantos múltiplos de 5 existem no intervalo $[1, 120]$? e no intervalo $[1, 174]$?

(b) Quantos múltiplos de 7 existem em cada um dos intervalos $[70, 342]$ e $[72, 342]$?

S-3.3 Dados $0 < a \leq n < m$, mostre que no intervalo $[1, n]$ existem q múltiplos de a, onde q é o quociente da divisão de n por q. Quantos são os múltiplos de a no intervalo $[n, m]$? (Na última situação, divida a análise em dois casos: n múltiplo de a e o contrário.)

S-3.4 Mostre que dados m inteiros consecutivos um, e apenas um, deles é múltiplo de m.

S-3.5 Com quantos zeros termina o número $2 \times 3 \times 4 \times \cdots \times 120$? E o número $2 \times 3 \times 4 \times \cdots \times 174$?

S-3.6 Mostre que o produto de quatro números inteiros consecutivos, quaisquer, é sempre múltiplo de 24.

S-3.7

(a) Mostre que se n é ímpar, então $n^2 - 1$ é múltiplo de 8.

(b) Mostre que se n é ímpar, então $n(n^2-1)$ é múltiplo de 24.

(c) Mostre que se n não é múltiplo de 2 nem de 3, então n^2-1 é múltiplo de 24. Mostre que o mesmo vale para n^2+23.

S-3.8

(a) Mostre que se um número a não é divisível por 3, então o resto da divisão de a^2 por 3 é 1.

(b) A partir desse dado, mostre que se um inteiro da forma a^2+b^2 é múltiplo de 3, então a e b são ambos múltiplos de 3.

S-3.9 Mostre que se $n>1$, então o número n^4+4 é composto.

S-3.10

(a) Mostre que o único número primo da forma n^3+1 é 2.

(b) Mostre que o único número primo da forma n^3-1 é 7.

S-3.11* Mostre que, dado $n>2$, entre n e $2\times 3\times\cdots\times n$ existe sempre um número primo. (Note que esta afirmação é bem mais fraca do que o Postulado de Bertrand.)

S-3.12

(a) Ache o menor inteiro positivo n tal que o número $4n^2+1$ seja divisível por 65.

(b) Mostre que existem infinitos múltiplos de 65 da forma $4n^2+1$.

(c) Mostre que se um dado número divide um número da forma $4n^2 + 1$, ele dividirá uma infinidade desses números.

(d) Para este último resultado, existe algo de especial nos números da forma $4n^2 + 1$?Teste o seu resultado para números da forma $an^2 + bn + c$, onde $a, b, c \in \mathbb{Z}$, com a e b não simultaneamente nulos.

(e) Mostre que existem infinitos múltiplos de 7 da forma $8n^2+3n+4$.

S-3.13

(a) Sejam dados os dois números $a = 10c + r$ e $b = c - 2r$, com $c, r \in \mathbb{Z}$. Mostre que a é múltiplo de 7 se, e somente se, b é múltiplo de 7.

(b) Deduza o seguinte critério de multiplicidade de 7:

O número $n = a_r \cdots a_1 a_0$ é múltiplo de 7 se, e somente se, o número $a_r \cdots a_1 - 2a_0$ é múltiplo de 7.

(c) Utilize repetidas vezes o critério acima para verificar se 2 368 é ou não múltiplo de 7.

Um número inteiro n é dito *um quadrado* se existe $a \in \mathbb{Z}$ tal que $n = a^2$. Dizemos que n é *uma potência m-ésima* quando $n = a^m$.

S-3.14

(a) Mostre que o algarismo das unidades de um quadrado só pode ser um dos seguintes: 0, 1, 4, 5, 6 e 9.

(b) Mostre que nenhum dos números 22, 222, 2 222, ..., ou 33, 333, 3 333, ..., ou 77, 777, 7 777, ..., ou ainda 88, 888, 8 888, ... pode ser um quadrado.

S-3.15

(a) Mostre que todo quadrado ímpar é da forma $4n + 1$.

(b) Mostre que nenhum número na sequência $11, 111, 1\,111, 11\,111$ etc., é um quadrado.

(c) Mostre que nenhum número na sequência $44, 444, 4\,444, 44\,444$ etc., é um quadrado.

(d) Mostre que nenhum número na sequência $99, 999, 9\,999, 99\,999$ etc., é um quadrado.

(e) Mostre que nenhum número na sequência $55, 555, 5\,555, 55\,555$ etc., é um quadrado.

S-3.16

(a) Mostre que nenhum número da forma $4n + 2$ é um quadrado.

(b) Mostre que nenhum dos números 66, 666, 6 666, ... é um quadrado.

S-3.17

(a) Mostre que a soma de quatro inteiros consecutivos nunca é um quadrado.

(b) Mostre que a soma dos quadrados de quatro inteiros consecutivos nunca é um quadrado. Faça o mesmo para a soma dos quadrados de três inteiros consecutivos.

S-3.18

(a) Mostre que todo quadrado é da forma $8n$, $8n+1$ ou $8n+4$.

(b) Mostre que nenhum número na sequência 3, 11, 19, 27 etc., é um quadrado.

S-3.19 Mostre que numa sequência de inteiros da forma

$$a, \quad a+d, \quad a+2d, \quad a+3d, \quad \ldots$$

se existir algum número que é quadrado, existirão infinitos números que são quadrados.

S-3.20*

(a) Mostre que todo número inteiro ímpar pode ser representado como diferença de dois quadrados.

(b) Mostre que se $p = 1$ ou se $p > 2$ é um número primo, então p se escreve de modo único como diferença de dois quadrados de números naturais.

(c) Mostre que todo número da forma $4^k n$, onde n é ímpar se escreve como diferença de dois quadrados.

(d) Mostre que se um número par é diferença de dois quadrados, então ele é múltiplo de 4.

S-3.21 Mostre que todo cubo é diferença de dois quadrados, ou seja, dado $a \in \mathbb{Z}$, existem $x, y \in \mathbb{Z}$ tais que $a^3 = x^2 - y^2$.

S-3.22* Ache os números n para os quais o número $n(n+14)$ seja um quadrado.

Um número inteiro $m \neq 0$ é dito *livre de quadrados*, quando não houver nenhum número $a \neq \pm 1$ tal que a^2 divide m.

Diremos que $m \neq 0$ é *livre de cubos* quando não houver nenhum número $a \neq \pm 1$ tal que a^3 divide m.

S-3.23

(a) Mostre que m é livre de quadrados se, e somente se, a decomposição de m em fatores primos é da forma $\pm p_1 \cdots p_r$, onde $p_1, \ldots, p_r$ são primos distintos.

(b) Mostre que m é livre de cubos se, e somente se, a decomposição de m em fatores primos é da forma $\pm p_1^{n_1} \cdots p_r^{n_r}$, onde $p_1, \ldots, p_r$ são primos distintos e $n_i \leq 2$, para todo $i = 1, \ldots, r$.

S-3.24 Qual é o maior número de inteiros positivos consecutivos livres de quadrados? E livres de cubos? Generalize.

S-3.25 Mostre que 5 é o único número primo que pertence a dois pares distintos de primos gêmeos.

S-3.26 Mostre que se n é composto, então n divide o produto

$$1 \times 2 \times 3 \times \cdots \times (n-1).$$

S-3.27 Dados dois inteiros a e b distintos, mostre que existem infinitos números n para os quais $\text{mdc}(a+n, b+n) = 1$.

S-3.28 Calcule $\text{mdc}(n+1, n^2+1)$, para $n \in \mathbb{Z}$.

S-3.29 Mostre que se a e b são dois números naturais tais que $\text{mdc}(a,b) = \text{mmc}(a,b)$, então $a = b$.

S-3.30 Resolva o seguinte sistema de equações:

$$\begin{cases} \text{mdc}(x,y) = 6 \\ \text{mmc}(x,y) = 60 \end{cases}$$

S-3.31 Observe que $\text{mdc}(x,y)$ divide $\text{mmc}(x,y)$, quaisquer que sejam $x, y \in \mathbb{Z}$, não nulos.

Mostre que se no seguinte sistema:

$$\begin{cases} \text{mdc}(x,y) = d \\ \text{mmc}(x,y) = m \end{cases}$$

$d \nmid m$, ele não admite solução. Mostre que se $d \mid m$, o sistema sempre admite solução.

S-3.32 Observe que $[\text{mdc}(x,y)]^2$ divide xy, quaisquer que sejam $x, y \in \mathbb{Z}$, não nulos.

Mostre que se o seguinte sistema:

$$\begin{cases} \text{mdc}(x, y) = d \\ xy = m \end{cases}$$

é tal que $d^2 \nmid m$, ele não admite solução. Mostre que se $d^2 \mid m$, o sistema sempre admite solução.

S-3.33

(a) Ache os números primos da forma $a^2 - 1$.

(b) Existem primos da forma $a^3 - 1$? E $a^4 - 1$?

(c) Mostre que se $a > 2$ e $n > 1$, então $a^n - 1$ é composto.

(d) Mostre que se n é composto, então $2^n - 1$ é composto.

Portanto, se $2^n - 1$ é primo, então n é primo. Números primos da forma $2^p - 1$, onde p é primo são chamados *primos de Mersenne*.

S-3.34

(a) Mostre que todo cubo que é também um quadrado é da forma $5n$, $5n+1$ ou $5n+4$ (ou seja, nunca é da forma $5n+2$ ou $5n+3$).

(b) Mostre que todo cubo que é também um quadrado é da forma $7n$, $7n + 1$.

S-3.35

(a) Mostre que todo primo maior do que 3 é da forma $3n + 1$ ou $3n + 2$.

(b) Mostre que qualquer número da forma $3n + 2$ tem um fator primo da mesma forma.

(c*) Mostre que existem infinitos primos da forma $3n + 2$.

(d) Existem infinitos primos da forma $3n + 1$, mas a prova disso é mais sutil.

S-3.36

(a) Mostre que todo primo maior do que 3 é da forma $4n + 1$ ou $4n + 3$.

(b) Mostre que qualquer número da forma $4n + 3$ tem um fator primo da mesma forma.

(c*) Mostre que existem infinitos primos da forma $4n + 3$.

(d) Existem infinitos primos da forma $4n + 1$, mas a prova disso é um pouco mais sutil (veja *Elementos de Aritmética*, Proposição 8.1.4).

S-3.37 Mostre que todo número primo da forma $3k + 1$ é da forma $6n + 1$.

S-3.38

(a) Mostre que todo primo maior do que 3 é da forma $6n + 1$ ou $6n - 1$.

(b) Mostre que qualquer número da forma $6n - 1$ tem um fator primo da mesma forma.

(c*) Mostre que existem infinitos primos da forma $6n-1$.

(d) Mostre que existem infinitos primos da forma $6n+1$ (Utilize os Problemas S-3.37 e S-3.35 (d)).

As propriedades enunciadas nos Problemas S-3.35 (c) e (d), S-3.36 (c) e (d) e S-3.38 (c) e (d) são casos particulares de um teorema profundo e de difícil demonstração do matemático Alemão Lejeune-Dirichlet (1805-1859), que afirma que se a e b são dois números primos entre si, então há infinitos números primos da forma $an+b$.

S-3.39 Verifique caso a caso que p divide 2^p-2 para p primo e $p \leq 7$.

S-3.40

(a) Mostre que em geral p divide a^p-a, para todo $a \in \mathbb{Z}$ e para todo p primo $p \leq 7$.

(b) Verifique que se p não divide a, com p nas condições de (a), então p divide $a^{p-1}-1$, para todo $a \in \mathbb{Z}$.

(c) Ache o resto da divisão por 7 do número $1^6+2^6+3^6+\cdots+15^6$.

(d) Mostre que se a e b são primos com 7, então b^6-a^6 é múltiplo de 7. Em particular, 23^6-18^6 é múltiplo de 7.

Os problemas S-3.39 e S-3.40 são casos particulares de um resultado geral chamado *Pequeno Teorema de Fermat*, cujo enunciado é:

Para todo primo p e todo inteiro a tem-se que p divide a^p-a. Além disso, se p não divide a, então p divide $a^{p-1}-1$.

Para uma prova, consulte o livro *Elementos de Aritmética*, Teorema 7.3.1 e o seu corolário.

S-3.41

(a) Mostre que 30 divide $n^5 - n$.

(b) Mostre que n^5 e n têm sempre o mesmo algarismo das unidades.

(c) Mostre que o número $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ é um inteiro para todo inteiro n.

S-3.42 Mostre que 42 divide $n^7 - n$.

S-3.43 Utilizando o Pequeno Teorema de Fermat, enunciado acima, mostre que se p um número primo, com $p \neq 2, 5$, então p divide infinitos elementos da sequência $9, 99, 999, 9999, \ldots$ Mostre também que p divide infinitos elementos da sequência $1, 11, 111, 1111, \ldots$

S-3.44 Quantos divisores positivos tem um número primo p? E p^n? E $p^n \times q^m$, com p e q primos distintos?

S-3.45 Ache o menor número natural que possui exatamente seis divisores positivos. Faça o mesmo para 15 divisores e para 100 divisores.

S-3.46 Mostre que se $\text{mdc}(a, c) = 1$ e $\text{mdc}(b, c) = 1$, então $\text{mdc}(ab, c) = 1$.

S-3.47 Mostre que

(a) $\text{mdc}(a^2, b^2) = [\text{mdc}(a, b)]^2$. (b) $\text{mmc}(a^2, b^2) = [\text{mmc}(a, b)]^2$.

(c) Generalize.

S-3.48 Sejam a e b inteiros e n um número natural. Mostre que se $a \times b$ é uma potência n-ésima e $\text{mdc}(a, b) = 1$, então a e b são potências n-ésimas.

S-3.49 (Esse é um problema proposto no século 16) Um total de 41 pessoas entre homens, mulheres e crianças foram a um banquete e juntos gastaram 40 *patacas*. Cada homem pagou 4 *patacas*, cada mulher 3 *patacas* e cada criança um terço de *pataca*. Quantos homens, quantas mulheres e quantas crianças havia no banquete?

S-3.50 (Proposto por Euler) Um grupo de homens e mulheres gastaram numa taberna 1 000 *patacas*. Cada homem pagou 19 *patacas* e cada mulher 13. Quantos eram os homens e quantas eram as mulheres?

S-3.51 (Proposto por Euler) Uma pessoa comprou cavalos e bois. Foram pagos 31 *escudos* por cavalo e 20 por boi e sabe-se que todos os bois custaram 7 *escudos* a mais do que todos os cavalos. Quantos cavalos e quantos bois foram comprados?

S-3.52

(a) Dados a e b inteiros fixados, quando é que os números da forma $ax + by$, com $x, y \in \mathbb{Z}$ representam todos os inteiros?

(b) Quais são os números representados por $2x + 3y$?

(c) Quais são os números representados por $6x + 9y$?

S-3.53 Em um certo país, as cédulas são de \$4 e \$7. Quais das afirmações a seguir são verdadeiras? Com elas é possível pagar, sem troco, qualquer quantia inteira

(a) a partir de \$11, inclusive.

(b) a partir de \$18, inclusive.

(c) ímpar, a partir de \$7, inclusive.

(d) que seja \$1 maior do que um múltiplo de \$3.

(e) que seja \$1 menor do que um múltiplo de \$3.

S-3.54 Em um quintal onde são criados coelhos e galinhas contaram-se 400 pés. Quantas são as galinhas e quantos são os coelhos, sabendo que diferença entre esses dois números é a menor possível.

S-3.55 Vimos no Problema S-3.16 que um quadrado nunca é da forma $4n+2$. Usando este fato, mostre que a equação $x^2+y^2=z^2$ não admite nenhuma solução em x, y e z, com x e y ímpares.

S-3.56 Mostre que a equação $x^2+y^2=z^2$ não admite nenhuma solução em x, y e z, com x e y ambos primos com 3.

S-3.57 Mostre que se m e n são números inteiros, então $x=2mn$, $y=m^2-n^2$ e $z=m^2+n^2$ são soluções da equação pitagórica $x^2+y^2=z^2$.

Problemas sobre o Capítulo 4

S-4.1

(a) Mostre que os restos da divisão de n inteiros consecutivos são os números $1, 2, \ldots, n$ em alguma ordem.

(b) Utilizando a fórmula:

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

conclua que a soma de n inteiros consecutivos quando dividida por n deixa resto zero se n é ímpar e metade de n, se n é par.

(c) Ache os restos da divisão de $2\,356 + 2\,357 + 2\,358 + 2\,359 + 2\,360$ por 5 e de $32\,141 + 32\,142 + \cdots + 32\,149 + 32\,150 + 32\,151 + 32\,152$ por 12.

S-4.2 Mostre que, para todo $n \in \mathbb{N}$,

(a) 7 divide $3^{2n+1} + 2^{n+2}$.

(b) 9 divide $10^n + 3 \times 4^{n+2} + 5$.

(c) 24 divide $2 \times 7^n + 3 \times 5^n - 5$.

(d) 35 divide $3^{6n} - 2^{6n}$.

(e) 64 divide $7^{2n} + 16n - 1$.

S-4.3 Sabendo que $7^4 = 2\,401$, ache os últimos dois dígitos de $7^{99\,999}$.

S-4.4 Ache o resto da divisão de $2^{1\,000\,000}$ por 77.

S-4.5 Mostre que $143^6 + 91^{10} + 77^{12} - 1$ é múltiplo de 1 001.

S-4.6 Mostre que $2\,222^{5\,555} + 5\,555^{2\,222}$ é múltiplo de 7.

S-4.7 Mostre que 19 nunca divide um número da forma $4n^2 + 4$.

S-4.8 Quais são os dois últimos algarismos na representação no sistema decimal do número 3^{400}? E do número 2^{400}?

S-4.9 Qual é o algarismo da unidade na representação decimal do número 9^{9^9}? E do número 7^{7^7}?

S-4.10 Ache os algarismos das centenas e das unidades na representação decimal dos números $7^{999\,999}$ e $7^{7^{1\,000}}$.

S-4.11 Ache o resto da divisão

(a) de 5^{60} por 26. (b) de 3^{100} por 34 (c) de $2^{1\,000\,000}$ por 77.

S-4.12 Determine os restos da divisão por 4 dos números:

(a) $1 + 2 + 2^2 + 2^3 + \cdots + 2^{100}$ (b) $1^5 + 2^5 + 3^5 + \cdots + 20^5$.

S-4.13 Mostre que a congruência $x^2 + 1 \equiv 0 \bmod 7$ não possui soluções. Conclua que a equação $x^2 - 6x - 77 = 7y$ não admite soluções inteiras.

S-4.14 Mostre que a equação $x^2 - 13y^2 = 275$ não admite soluções inteiras.

S-4.15 Mostre que se um número da forma $7n - 5$ é múltiplo de 5, então o número $12n^2 + 19n - 19$ é múltiplo de 25.

S-4.16 Mostre que se um número da forma $2n + 1$ é múltiplo de 3, então o número $28n^2 - 13n - 5$ é múltiplo de 9.

S-4.17 Mostre que valem as seguintes congruências:

(a) $n^{13} \equiv n \bmod p$, para $p = 2, 3, 5, 7$ e 13, e para todo $n \in \mathbb{Z}$.

(b) Se $\text{mdc}(n, p) = 1$, mostre que $n^{12} \equiv 1 \bmod p$, para $p = 2, 3, 5, 7$ e 13.

Partes do problema acima são casos particulares do Pequeno Teorema de Fermat, que pode ser reenunciado como segue:

Para todo primo p e todo inteiro a tem-se que $a^p \equiv a \bmod p$. Além disso, se p não divide a, então $a^{p-1} \equiv 1 \bmod p$.

S-4.18 Resolva a congruência $3x \equiv 5 \bmod 11$.

S-4.19 Determine os inteiros que deixam restos 1, 2 e 3, quando divididos respectivamente por 3, 4 e 5.

S-4.20 Mostre que nenhum número da forma $4n + 3$ pode ser escrito como soma de dois quadrados.

Soluções e Respostas

Problemas do Capítulo 1

1.1 $\emptyset$, $\{3\}$, $\{2\}$, $\{2,3\}$, $\{4,5,6\}$, $\{4,5,6,7\}$, $\{3,4,5,6\}$ e $\{3,4,5,6,7\}$.

1.2 2, 3, 4, não tem, 3 e 2.

1.3 Por causa da comutatividade da adição pode-se separar essas 12 expressões em três grupos:

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

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

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

Portanto, novamente, pela comutatividade da adição, temos

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

e, consequentemente, os 12 números listados acima são iguais.

1.6 Faltam $200-50=150$ reais.

1.7 Pela tricotomia, temos três possibilidades:

$$a - c > b - c, a - c = b - c \text{ ou } a - c < b - c.$$

Somando c a ambos os lados da primeira e da segunda possibilidade obtemos uma contradição, logo só resta a terceira possibilidade.

1.8 São $72 - 37 + 1 = 36$ números.

1.9 São $75 - 32 = 43$ números, tanto no intervalo $(32, 75]$, quanto no intervalo $[32, 75)$ e $75 - 32 - 1 = 42$ números no intervalo $(32, 35)$.

1.10 $b - a$ nos dois primeiros casos e $b - a - 1$ no último.

1.11 Não são. Se fossem, teríamos $1 = la$, com $a > 1$, o que não é possível.

1.12 $5, 10, 15, 20, 25, 30, 35, 40, 45, 50$.

1.15

(a) Considerando a sequência $32 = 8 \times 4, 8 \times 5, \ldots, 8 \times 1\,000$, segue que o número de múltiplos de 8 é $1\,000 - 4 + 1 = 997$.

(b) Considerando a sequência $1\,606 \times 2, \ldots, 3\,160 \times 2$, segue que o número de números pares é $3\,160 - 1\,606 + 1 = 1\,555$.

(c) 15 e 18 dúzias, respectivamente.

(d) 40 e 51 semanas, respectivamente.

1.23 $28, 56, 84, \ldots$

1.24 12, 66, 24 e 9.

1.26 $(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$.

Problemas do Capítulo 2

2.1 Os números são

$$2 \times 6,\ 3 \times 6,\ \ldots,\ 16 \times 6,$$

cuja soma é

$$(2 + 3 + \cdots + 16) \times 6 = 135 \times 6 = 810.$$

2.2 Se os algarismos são a, b e c, os seis números são $ab = 10a + b$, $ba = 10b + a$, $ac = 10a + c$, $ca = 10c + a$, $bc = 10b + c$ e $cb = 10c + b$, logo a sua soma é

$$10a+b+10b+a+10a+c+10c+a+10b+c+10c+b = 22(a+b+c).$$

2.4 10; 99; $99 - 10 + 1 = 90$; $2 \times 90 = 180$.

2.5 São necessários 792 algarismos. Ao confrontar com a fórmula $Q(x)$ não se esqueça que não existe página 0.

2.6 Seja n_0, onde $0 \leq n_0 \leq 9$, o algarismo das unidades de a. Escreva a na forma $10m + n_0$, e o eleve ao quadrado.

2.16 $4 = 2^2$, $6 = 2 \times 3$, $8 = 2^3$, $36 = 2^2 \times 3^2$, $84 = 2^2 \times 3 \times 7$, $320 = 2^6 \times 5$ e $2.597 = 7^2 \times 53$.

Problemas do Capítulo 3

3.9 Pela propriedade sugerida, tem-se que $216 - 144 = 72$ é um múltiplo comum, logo $\text{mmc}(a, b) \leq 72$.

3.16

(a) $\text{mdc}(n, 2n+1) = \text{mdc}(n, 2n+1-2n) = \text{mdc}(n, 1) = 1$.

(b) e (c) $\text{mdc}(n, 2n+2) = \text{mdc}(n, 2n+2-2n) = \text{mdc}(n, 2)$, que é 1 ou 2 segundo se n é ímpar ou par.

3.17 Se $\text{mdc}(a', b') = d' > 1$, então $a = a''d'd$ e $b = b''d'd$, logo dd' seria um divisor comum de a e b maior do que d, absurdo.

3.18 $43 = 3 \times 14 + 1$, $43 = 5 \times 8 + 3$, $233 = 4 \times 58 + 1$, $1\,453 = 10 \times 145 + 3$, $1\,453 = 100 \times 14 + 53$, $1\,453 = 1\,000 \times 1 + 453$ e $1\,453 = 10\,000 \times 0 + 1\,453$.

3.20 $-43 = 3(-15) + 2$, $-43 = 5(-9) + 2$ $-233 = 4(-59) + 3$, $-1\,453 = 10 \times (-146) + 7$, $-1\,453 = 100(-15) + 47$, $-1\,453 = 1\,000(-2) + 547$, $-1\,453 = 10\,000(-1) + 8\,547$.

3.24 Um número a é da forma $3q + i$, onde $i = 0, 1, 2$. Agora analise cada caso separadamente. Se $a, a+2$ e $a+4$ são primos trigêmeos, um deles é divisível por 3 e sendo um número primo, ele é igual a 3. Analisando as três possibilidades conclui-se que $a = 3$ e, portanto, $3, 5$ e 7 é a única terna de primos trigêmeos.

3.25 e **3.26** Escreva a na forma $3q + i$, $i = 0, 1, 2$.

3.27 $3\,257 = 5 \times 651 + 2$. Logo são produzidos 651 pacotes de chicletes.

3.28 Escrevamos o número ímpar na forma $2n + 1$, logo

$$2(2n + 1) = 4n + 2,$$

que não é múltiplo de 4.

3.29 A paridade é determinada por

$$(\overline{1} + \overline{1})^{234} + (\overline{1} + \overline{0})^{542} = \overline{0}^{234} + \overline{1}^{542} = \overline{1},$$

logo é ímpar.

3.33 O resto da divisão por 3 se calcula como segue:

$$\overline{1}^{100} + (\overline{2}^2)^{15} = \overline{1} + \overline{1}^{15} = \overline{1} + \overline{1} = \overline{2}.$$

Portanto, o resto é 2.

3.34 Um múltiplo de 6 é obviamente múltiplo de 2 e de 3. Reciprocamente, todo múltiplo de 2 e de 3 é múltiplo do mmc desses números que é 6.

3.35 Um número é múltiplo de 6 se, e somente se, o seu algarismo das unidades é par e a soma de seus algarismos é múltiplo de 3.

3.36 Podemos escrever

$$\begin{aligned} n(n+1)(2n+1) &= n(n+1)(n-1+n+2) \\ &= (n-1)n(n+1) + n(n+1)(n+2). \end{aligned}$$

Agora note que cada parcela na última linha é múltiplo de 2 e de 3, donde o resultado segue levando em conta o Problema 3.34.

3.39 $\text{mmc}(4,6,9) = \text{mmc}(\text{mmc}(4,6),9) = \text{mmc}(12,9) = 36$.

3.40 Se m é múltiplo comum de a e b, temos $m = r \times a$ e $m = s \times b$. Logo, $a \times b = r \times a \times d$ e $a \times b = s \times b \times d$. Assim, temos que $b = r \times d$ e $a = s \times d$, mostrando que d é divisor comum de a e b.

Reciprocamente, se d é divisor comum de a e b temos que $b = r \times d$ e $a = s \times d$. Logo de $a \times b = m \times d$, obtemos $s \times b = m$ e $r \times a = m$. Concluímos assim que m é múltiplo comum de a e b.

3.41 Como $\text{mdc}(n, 2n+1) = 1$, segue que $\text{mmc}(n, 2n+1) = n(2n+1)$.

3.42 Sendo n múltiplo de a e de b, ele é múltiplo de seu mmc. Por outro lado, sendo $\text{mdc}(a,b) = 1$, temos que $\text{mmc}(a,b) = a \times b$, logo n é múltiplo de $a \times b$, logo divisível por ele.

3.43

(a) $8 = 728 \times 37 + 1\,496 \times (-1)$.

(b) $6 = 108 \times (-15) + 294 \times 7$.

3.44 Denotemos por $\min A$ o menor elemento de um conjunto de números naturais A. Sabemos da Proposição 3.1 que

$$\text{mdc}(a,b) = \min\{x \in a\mathbb{Z} + b\mathbb{Z};\ x > 0\}.$$

Portanto,

$$\begin{aligned} \mathrm{mdc}(ca, cb) &= \min\{x \in ac\mathbb{Z} + bc\mathbb{Z};\ x > 0\} \\ &= c\min\{x \in a\mathbb{Z} + b\mathbb{Z};\ x > 0\} \\ &= c \times \mathrm{mdc}(a, b). \end{aligned}$$

3.45 O resultado segue da fórmula do Teorema 3.2:

$$\mathrm{mdc}(a, b) \times \mathrm{mmc}(a, b) = a \times b,$$

e do Problema 3.44.

3.46 Como p é primo, os seus únicos divisores são ± 1 e $\pm p$. Logo $\mathrm{mdc}(a, p) = 1$ ou $\mathrm{mdc}(a, p) = p$. Na segunda possibilidade teremos $p \mid a$.

3.47 Do exercício anterior, temos que $p \mid a$ ou $\mathrm{mdc}(a, p) = 1$. No primeiro caso, nada temos a provar. No segundo caso, como $p \mid a \times b$, segue da Proposição 3.3 que $p \mid b$.

3.48 Sendo p primo, se $p \mid p_1 \times p_2$, pelo problema anterior, $p \mid p_1$ ou $p \mid p_2$. Como p_1 e p_2 são primos, isto acarreta que $p = p_1$ ou $p = p_2$.

3.49 Suponhamos que $p_1 \times \cdots \times p_r = q_1 \times \cdots \times q_s$. Portanto, p_1 divide $q_1 \times \cdots q_s$, logo p_1 é igual a um dos q_i, que após reordenamento podemos supor ser q_1. Assim, $p_1 \times \cdots \times p_r = p_1 \times \cdots \times q_s$, logo $p_2 \times \cdots \times p_r = q_2 \times \cdots \times q_s$. Continuando desse modo, se $r = s$, a demonstração está completa. Suponhamos $s > r$ (o outro caso é semelhante) temos que $1 = q_{r+1} \times \cdots \times q_s$, o que não é possível.

3.50 $1, 2, 4, 8,\quad 5, 10, 20, 40$ e $1, 2, 4, 8,\quad 5, 10, 20, 40,\quad 3, 6, 12, 24,$ $15, 30, 60, 120$.

3.51 Tem 48 divisores.

3.52 Sendo $1\,080 = 2^3 \times 3^3 \times 5 \times 7^0$ e $210 = 2 \times 3 \times 5 \times 7$, temos que $\text{mdc}(1\,080, 210) = 2 \times 3 \times 5$ e $\text{mmc}(1\,080, 210) = 2^3 \times 3^3 \times 5 \times 7$.

3.55 (a) tem solução (b) não tem solução (c) tem solução (d) tem solução (e) tem solução (f) tem solução.

3.56 $\text{mdc}(a, b) = 1$ divide qualquer número c.

3.57 Quando c for múltiplo de $\text{mdc}(30, 42) = 6$.

3.58 A equação a ser resolvida é $5x + 7y = 100$, que possui solução pois 5 e 7 são primos entre si. Uma solução particular é dada por $x_0 = 20$ e $y_0 = 0$. Logo a solução geral é da forma: $x = 20 - 7t$ e $y = 5t$, com t número natural e $20 - 7t \geq 0$ para que as soluções sejam não negativas. Assim obtemos as seguintes possibilidades: $x = 20, y = 0$; $x = 13, y = 5$ e $x = 6, y = 10$.

3.59 Se D é o número de degraus, temos $D = 2x + 1$ e $D = 3y + 2$. Assim, temos que $2x - 3y = 1$, da qual uma solução particular é $x_0 = 2$ e $y_0 = 1$. Portanto, $x = 2 + 3t$ e $y = 1 + 2t$. Por outro lado, $40 \leq D \leq 100$ e é múltiplo de 7. Isto implica que $6 \leq t \leq 15$, e para que D seja múltiplo de 7, é preciso que $t = 12$, ou seja, $D = 77$.

3.60 O problema conduz à equação $15x - 12y = 1$, que não possui soluções, pois $\text{mdc}(15, 12) = 3$ não divide 1.

3.61 Temos $n = 18x + 4$ e $n = 14y + 6$, o que nos conduz à equação

$9x - 7y = 1$. Uma solução particular é $x_0 = -3$ e $y_0 = -4$. Assim, $x = -3 + 7t$, logo $n = 18(-3 + 7t) + 4$, que é natual quando $t \geq 1$. Logo os números são da forma $n = 126t - 50$, onde $t \geq 1$.

Problemas do Capítulo 4

4.3 Já vimos que $10^n - 1 = 99\cdots9$, logo 9 divide $10^n - 1$, donde segue o resultado.

4.6 3 254 deixa resto 2 e 5, quando dividido por 3 e 9, respectivamente. 12 736 deixa resto 1, quando dividido por 3 e 9. 54 827 deixa resto 2 e 8, quando dividido por 3 e 9, respectivamente. 33 875 435 deixa resto 2, quando dividido por 3 e 9. 57 612 510 deixa resto 0, quando dividido por 3 e 9.

4.7 3 254 deixa resto 4 quando dividido por 5 e 10. 12 736 deixa resto 1 e 6, quando dividido por 5 e 10, respectivamente. 54 827 deixa resto 2 e 7, quando dividido por 5 e 10, respectivamente. 33 875 435 deixa resto 0 e 5, quando dividido por 5 e 10, respectivamente. 57 612 510 deixa resto 0 quando dividido por 5 e 10.

4.12 1, 4 e 3.

4.15 O resto é 5.

4.18 O resto é 3.

4.19 O resto da divisão por 7 é 2. O resto da divisão por 11 é 9 e o resto da divisão por 13 é 5.

4.21 Os restos da divisão por 3 de 5 345, 3 765 839 e 10^{10} são,

respectivamente, 2, 2 e 1, logo $2^{5\,345} \equiv 2^2 \bmod 7$, $2^{3\,765\,839} \equiv 2^2 \bmod 7$ e $2^{10^{10}} \equiv 2 \bmod 7$.

4.22 Temos que $30 = 4 \times 7 + 2$, logo

$$2^{30} = (2^4)^7 \times 2^2 \equiv (-1)^7 \times 4 \equiv 3 \bmod 17.$$

Logo o resto da divisão é 3.

4.23 Temos que $325 = 4 \times 81 + 1$, logo $2^{325} \equiv -2 \equiv 15 \bmod 17$.

4.25 $19 \equiv 2 \bmod 17$, logo $19^{4n} = (19^4)^{2n} \equiv (-1)^{2n} = 1 \bmod 17$. Assim, $19^{4n} - 1$ é divisível por 17.

4.26 Observe que se tem

$$13^3 = 2\,197 \equiv 37 \equiv -8 \bmod 45,$$

e que

$$17^3 = 4\,913 \equiv 8 \bmod 45,$$

dos quais o resultado segue.

4.28 O resto é 3.

4.30 O resto é 2.

Para Aprender Mais

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA, [s.d.]. (Série de Computação e Matemática.)

HEFEZ, A. *Elementos de Aritmética*. [S.l.: s.n., s.d.] (Série Textos Universitários, Sociedade Brasileira de Matemática.)

HEFEZ, A. *Indução Matemática*. Em http://www.obmep.org.br