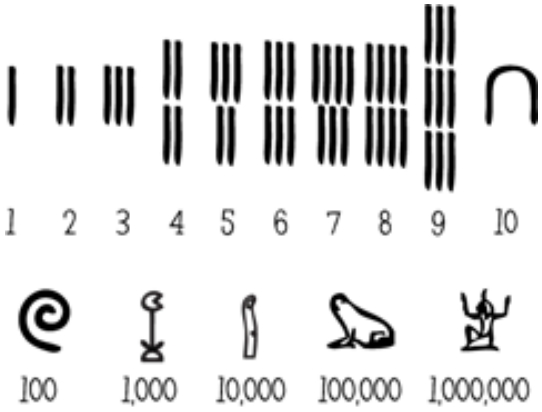
UFPR - Universidade Federal do Paraná
Setor de Ciências Exatas
Departamento de Matemática
CM122 - Fundamentos de Análise
Prof. Zeca Eidam

1 Introdução

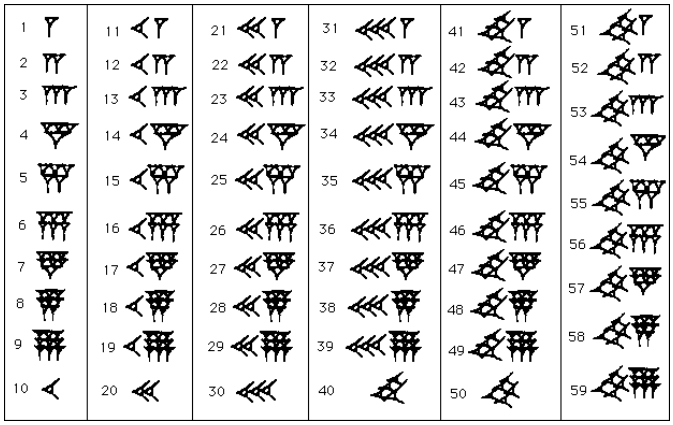
Este texto propõe-se introduzir de maneira informal os conjuntos numéricos e estudar diversas propriedades dos mesmos. Para isso, falaremos um pouco sobre o conceito de número.



Sistema de numeração egípcio

Os números estão por todo lugar. Não se sabe ao certo exatamente quando o homem começou a conceber o conceito de número. De qualquer forma, registros arqueológicos muito antigos comprovam que a numeração escrita é tão antiga quanto a própria escrita. Os sistemas de numeração mais antigos que temos notícia são os sistemas egípcio e sumério, ambos datando aproximadamente de 3500 a.C.

Embora seja muito interessante investigar os números do ponto de vista histórico e arqueológico, neste curso vamos estudá-los do ponto de vista matemático. À primeira vista, pode parecer ao estudante que, por serem conhecidos há tanto tempo por tantas pessoas de tantas raças, nacionalidades e épocas distintas, tudo o que se podia saber sobre os números já está contido em livros e artigos científicos, e ao aluno resta apenas o trabalho de aprender o que está nos textos.



Sistema de numeração sumério

Porém, acontece justamente o contrário: quanto mais a Ciência avança e conhece a respeito dos números, mais se mostra por fazer. E mais aplicações aparecem. Exemplo interessante deste fenômeno ocorre em uma ciência chamada Criptografia. A Criptografia, como o próprio nome diz, é o estudo de princípios e técnicas através das quais uma informação pode ser transmitida através de um código ilegível e decifrada apenas pelo seu legítimo destinatário. A Criptografia é bastante antiga e já está presente nos códigos utilizados pelo imperador romano Julio Cesar para enviar mensagens secretas aos generais de seus exércitos. Durante as duas grandes guerras do século XXI, por interesses militares, houve grande interessante na geração de códigos secretos para envio de mensagens codificadas. Você já deve estar se perguntando o que isto tem a ver com números... Pois bem, em 1976, três pesquisadores do MIT (Massachussets Institut of Technology) chamados Ronald Rivest, Adi Shamir e Leonard Adleman desenvolveram uma forma de criptografar mensagens de maneira relativamente simples utilizando para isso conceitos elementares de aritmética. Este método passou a ser chamado de criptografia RSA, em homenagem aos seus criadores. Para

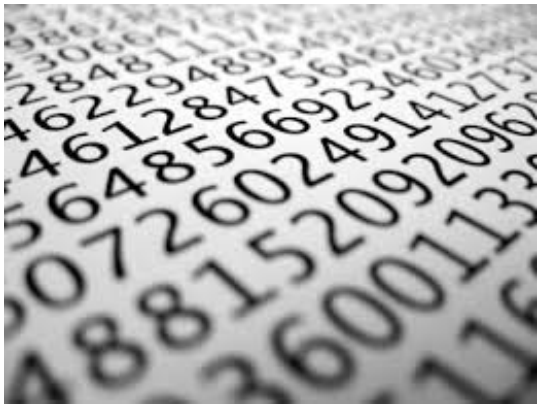
se ter uma idéia da segurança do processo, para um interceptador decifrar uma mensagem criptografada utilizando criptografia RSA, dependendo dos parâmetros utilizados, seriam necessários mais de 40 milhões de anos!

Existem alguns conjuntos de números que desempenham um papel fundamental não só na Matemática, como na vida cotidiana. O mais elementar deles é o chamado *conjunto dos números naturais*, denotado pelo símbolo $\mathbb{N}$. É compreendido pelos números

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

A importância deste conjunto é justificada pelo fato de que é nele que somos inseridos pela primeira vez que falamos de número. O conceito de número foi desenvolvido pela necessidade de contagem e o conjunto dos números naturais é o ambiente natural para isto. Durante a maior parte deste curso, estaremos trabalhando neste conjunto.

2 Sistemas de numeração

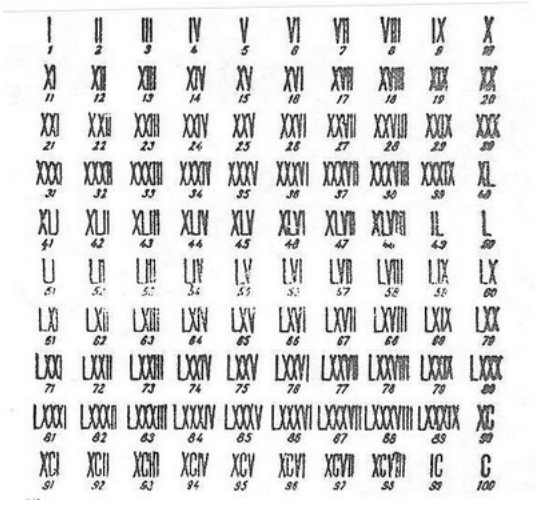


O primeiro problema encontrado pelo homem ao trabalhar com números é o problema de *representação*. Nas tabelas anteriores, vemos as soluções encontradas pelos sumérios e egípcios para denotar os números. O sistema de numeração romano utilizado até hoje tem suas bases nos sistemas grego e hebraico, os quais atribuíam valores numéricos às letras.

Evidentemente, ao utilizarmos determinado sistema de numeração, estamos não somente interessados em registrar quantias, mas também em operar com estas. Neste segundo quesito, todos os sistemas apresentados anteriormente deixam a desejar. O leitor pode comprovar rapidamente a veracidade desta afirmação fazendo os cálculos abaixo:

$$\begin{aligned} \text{XXXVII} \times \text{MCXIX} &= \\ \text{DLXXVI} \div \text{XVI} &= \end{aligned}$$

Utilizar o sistema romano ou qualquer dos outros apresentados para realizar as operações cotidianas seria um verdadeiro desastre! Isso explica em parte o *sucesso* do sistema de numeração posicional de base 10, o qual passamos a descrever.



O sistema posicional de base 10 teve sua origem na Índia, muito provavelmente no final do século V e foi introduzido na Europa em torno do século VII d.C. pelo árabe Mohammed Ben Mussa Al Khawarismi. Nos trabalhos de Aryabhata, um destacado matemático e astrônomo indiano do século V, aparece a célebre expressão *de lugar para*

lugar, cada um vale dez vezes o seu precedente, dando a entender o uso do princípio da posição. Com bastante certeza, a escolha da base 10 está ligada ao fato de termos dez dedos nas mãos para utilizarmos nos cálculos...

Aryabhata

Ao escrever um número no sistema decimal, por exemplo, 1977, estamos pensando no número obtido como resultado da expressão

$$1.10^3 + 9.10^2 + 7.10^1 + 7.10^0.$$

Genericamente, se $x_0, x_1, \ldots, x_m$ são algarismos pertencentes ao conjunto $\{0,1,2,3,4,5,6,7,8,9\}$, então o número

$$x_m.10^m + x_{m-1}.10^{m-1} + \ldots + x_1.10^1 + x_0.10^0$$

pode ser representado simplesmente como

$$x_m x_{m-1} \ldots x_1 x_0.$$

Não é muito difícil verificar que qualquer número natural pode ser representado de uma única maneira através de uma soma do tipo acima. O leitor pode deduzir facilmente as conhecidas regras para soma e produto já conhecidas.

A popularidade deste sistema de numeração deve-se muito ao fato que as operações cotidianas podem ser facilmente sistematizadas de forma que até mesmo as crianças podem realizá-las!

Convencido de que a escolha da base 10 é uma simples convenção que auxilia muito nos cálculos, você pode estar se perguntando se poderíamos considerar uma base qualquer. A resposta é *sim*!

Dados um número natural $b > 1$ (chamado *base*) e $x_0, x_1, \ldots, x_m$ algarismos pertencentes ao conjunto $\{0,1,2,\ldots,b-1\}$ o número

$$x_m.b^m + x_{m-1}.b^{m-1} + \ldots + x_1.b^1 + x_0.b^0$$

será denotado por $(x_m x_{m-1} \ldots x_1 x_0)_b$ ou $x_m x_{m-1} \ldots x_1 x_0$, quando não houver perigo de confusão. De maneira inteiramente análoga ao que já fizemos para a base 10, podemos mostrar que qualquer número natural pode ser escrito de maneira única como uma soma do tipo anterior.

Uma base de particular interesse na computação é a base 2. Neste caso, todo número natural corresponde a uma única sequência de dígitos 0 ou 1. Por exemplo, como então o número 19 escrito na base 2 é 10011. Observamos que um número relativamente pequeno pode necessitar de muitos algarismos para ser representado na base 2. As regras de soma e multiplicação na base 2 são muito simples e baseadas na igualdade $(1)_2 + (1)_2 = (10)_2$, que pode assumir um aspecto pitoresco se eliminarmos a referência à base 2 e escrevermos simplesmente $1 + 1 = 10$...

Outras bases importantes para a computação são as base 8 e 16, as quais são bases para os sistemas de numeração octal e hexadecimal, respectivamente. Veja mais informações em Sistema Octal e Sistema Hexadecimal.

3 Axiomatização dos naturais

Na seção anterior, aprendemos sobre a representação dos números naturais. Nesta seção, iremos estudar um pouco mais a fundo as propriedades intrínsecas do conjunto dos números naturais.

Embora questões teóricas envolvendo os números naturais tenham surgido no começo do século XIX, o primeiro matemático a formular de maneira consistente a construção dos números naturais foi o italiano Giuseppe Peano (1858-1932) por volta de 1880. Falando de maneira bastante genérica, Peano encontrou uma maneira de descrever os números naturais sem falar exatamente o que eles são, mas dizendo exatamente como se comportam. Esta filosofia de trabalho foi profundamente influencial em todos os ramos da matemática que estavam se desenvolvendo na mesma época e foi utilizada também para descrever o conjunto dos números reais.

Os chamados *axiomas de Peano* são os seguintes:

1. Existe um conjunto (chamado $\mathbb{N}$) e uma função $S : \mathbb{N} \to \mathbb{N}$ chamada de *função sucessor*;
2. A função S é *injetora*, isto é, se $S(m) = S(n)$ então $m = n$;
3. Existe um elemento em $\mathbb{N}$ chamado 1 tal que $S(n) \neq 1$ para todo $n \in \mathbb{N}$;

Além destes axiomas, temos também o *Axioma da Indução*:

- Se uma propriedade $P(n)$ é verificada para $n = 1$ e sempre que $P(n)$ é verdadeira então $P(S(n))$ também é verdadeira, então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Giuseppe Peano

As 4 propriedades acima caracterizam completamente o conjunto dos números naturais e todas as operações podem ser descritas em termos da função sucessor. Você poderá encontrar mais detalhes em

A axiomática de Peano nos fornece uma maneira matematicamente rigorosa de provar afirmações a respeito de números naturais. Vamos mostrar um exemplo simples de como isso é feito. Considere, para cada número natural n, a soma

$$\Sigma(n) = 1 + 2 + 3 + \ldots + n\,.$$

Não é muito difícil de verificar que $\Sigma(n) = \dfrac{n(n+1)}{2}$. Esta fórmula, aliás, tem uma história interessante que pode ser consultada em (ver historinha de Gauss).

Vamos agora partir de outro ponto. Suponha agora que alguém que não conheça a discussão do parágrafo anterior apresente a questão seguinte: *É verdade que* $\Sigma(n) = \dfrac{n(n+1)}{2}$ para todo $n \in \mathbb{N}$? Podemos testar alguns valores e verificar que a fórmula é verdadeira, mas por mais tempo e disposição que tenhamos, nunca conseguiremos testar a veracidade da fórmula para *todos os números naturais!*

Nesta situação, para provar a que a afirmação é verdadeira, devemos utilizar o Axioma (ou Princípio) da Indução. Evidentemente, a fórmula é verdadeira para $n = 1$. Além disso, se a fórmula é verificada para um certo número natural n, então

$$\Sigma(n+1) = 1 + 2 + 3 + \ldots + n + (n+1) = \Sigma(n) + n + 1 = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)((n+1)+1)}{2},$$

o que comprova que a fórmula também é verificada para $n+1$. Portanto, pelo Princípio da Indução, segue que a fórmula é verificada para todo n natural.

4 Divisibilidade, Divisão Euclidiana e Congruências

Dados $a, b \in \mathbb{N}$, dizemos que *a divide b* se existe $c \in \mathbb{N}$ tal que $b = ac$. Este fato é denotado por $a|b$. Por exemplo, $2|2014$, $4|32$, $10|1000$, mas não é verdade que $8|18$ e $11|20$; neste caso, escrevemos $8 \nmid 18$ e $11 \nmid 20$. Quando a divide b, dizemos que b é um múltiplo de a.

Vamos enunciar algumas propriedades elementares da relação de divisibilidade, cuja prova é muito simples e será deixada como exercício.

Proposição 1 Sejam $a, b, c \in \mathbb{N}$. As seguintes afirmações são verdadeiras:

1. $1|a$;
2. $a|a$;
3. Se $a|b$ e $b|c$ então $a|c$;
4. Se $a|b$ e $a|c$ e $b > c$ então $a|(b \pm c)$.

Existem relações de divisibilidade para certas expressões especiais que são muito úteis e serão descritas no teorema a seguir.

Teorema 2 Sejam $a, b, n \in \mathbb{N}$. As afirmações abaixo são verdadeiras:

1. $a + b|a^{2n+1} + b^{2n+1}$;
2. Se $a > b$ então $a - b|a^n - b^n$ e $a + b|a^{2n} - b^{2n}$.

Dados $a < b$ naturais, mesmo quando a não divide b, é possível escrever b como soma de um múltiplo de a mais um resto r que não excede a. Este é o conteúdo do próximo teorema, chamado de *algoritmo da divisão*.

Teorema 3 Dados $a < b$ naturais, existem únicos q, r naturais tais que

$$b = aq + r$$

e $0 \leq r < a$.

Este resultado aparece implicitamente nos *Elementos* de Euclides, obra datada do século III a.C.

Uma consequência importante do algoritmo da divisão é que, dados $j, n \in \mathbb{N}$ tais que $0 \leq j \in \mathbb{N}$, podemos considerar o conjunto formado pelos naturais cujo resto na divisão por n é j. Este conjunto é chamado de *classe residual módulo n*. Evidentemente, um número não pode pertencer simultaneamente a dois desses conjuntos e a reunião de todos eles é o conjunto de todos os naturais. A família das classes residuais módulo n forma o que se chama *partição do conjunto* $\mathbb{N}$. Quando $a, b \in \mathbb{N}$ têm o mesmo resto na divisão por n (ou seja, quando a e b pertencem à mesma classe residual módulo n), escrevemos

$$a \equiv b \mod n.$$

Euclides

A expressão acima é lida como *a é congruente (ou congruo) a b módulo n*. Se $b \geq a$, vemos que $a \equiv b \mod n$ se e só se $n|b-a$. A relação de congruência e notação acima foi introduzida e estudada pelo famoso matemático alemão *Karl Friedrich Gauss* em seu trabalho *Disquitiones Aritmeticae*.

Grande parte do interesse na relação de congruência provém do fato que esta é uma relação muito bem comportada em relação às operações usuais, como veremos no próximo teorema.

Teorema 4 Sejam $a, a', b, b' \in \mathbb{N}$ tais que $a \equiv a' \mod n$ e $b \equiv b' \mod n$. Então:

① $a+b \equiv a'+b' \mod n$;

② $aa' \equiv bb' \mod n$;

③ $a^k \equiv a'^k \mod n$ para todo $k \in \mathbb{N}$

5 Os números inteiros

A diferença $b-a$ entre $a, b \in \mathbb{N}$ somente é definida quando $b \geq a$. Para podermos definir a diferença entre dois naturais quaisquer, é preciso *aumentar* o conjunto dos números naturais de forma a incluir os números da forma $b-a$, com $b < a$.

A maneira rigorosa de fazer isto é observar que duas diferenças $b-a$ e $d-c$ definem o mesmo inteiro se e somente se $b+c = a+d$. Sendo assim, dizemos que dois pares de naturais (a,b) e (c,d) são equivalentes se $b+c = a+d$. Esta é uma relação de equivalência e o conjunto das classes de equivalência é, por definição, o conjunto $\mathbb{Z}$ dos números inteiros. Assim, por definição, $-1 = [(1,2)] = [(12,13)] = [(1977,1978)]$, $-6 = [(4,10)] = [(43,49)]$, e assim por diante.

As operações sobre $\mathbb{Z}$ são definidas em termos de classes de equivalência. Por exemplo, definimos a soma e o produto de dois inteiros como $[(a,b)] + [(c,d)] = [(a+c, b+d)]$ e $[(a,b)].[(c,d)] = [(ac+bd, ad+bc)]$. Não é difícil verificar que estas operações são bem-definidas (independem dos representantes utilizados) e são associativas e comutativas. Vemos que $0 = [(1,1)]$ é o elemento neutro da adição e $1 = [(2,1)]$ é o elemento neutro da multiplicação.

Fica associado a cada natural n, o inteiro $[(n+1,1)]$, sendo assim, podemos pensar que todo natural é também um inteiro. Definimos $-n = [(1,n+1)]$; não é difícil verificar que $n+(-n) = 0$ e $-n = (-1).n$. Além disso, cada inteiro ou é da forma n ou é da forma $-n$, para n natural. Vemos também que $(m+n).p = mp+np$, para todos m, n, p inteiros (Propriedade distributiva).

Os resultados válidos para os naturais valem com as devidas adaptações para os inteiros. As noções de divisibilidade também são naturalmente traduzidas para o ambiente dos inteiros.

6 MDC e MMC

Dados $a, b \in \mathbb{Z}$ o *MDC (máximo divisor comum)* entre a e b é o maior divisor comum entre a e b. Este inteiro é denotado por (a,b). O *MMMC (mínimo múltiplo comum)* entre a e b é menor múltiplo comum positivo entre a e b e é denotado por $[a,b]$.

O método *pedestre* para calcular o mdc entre dois inteiros positivos, digamos 24 e 18, é escrever os divisores positivos de ambos (1,2,3,4,6,8,12,24 e 1,2,3,6,12,18) e tomar o maior deles (12). Isso funciona bem para números pequenos, pois neste caso, os divisores são facilmente calculados. Seria bem mais trabalhoso utilizar este método para calcular o mdc entre 12794 e 798, por exemplo. Felizmente, para resolver esta situação, temos à disposição um lema muito simples devido a Euclides.

Lema 5 (Euclides) Para quaisquer $a, b, n \in \mathbb{Z}$, os divisores comuns de a e b são os mesmos que os divisores comuns de a e $b - na$. Em particular, $(a, b) = (a, b - na)$.

A justificativa para a afirmação acima decorre do fato que c divide simultaneamente a e b se e somente se c divide simultaneamente a e $b - na$.

Isso nos permite reduzir o *tamanho* de nosso problema! De fato, como $12794 = 16.798 + 26$ então $(12794, 798) = (12794 - 16.798, 798) = (26, 798)$. Como $798 = 30.26 + 18$, aplicamos novamente o lema de Euclides, obtendo $(26, 798) = (26, 798 - 30.26) = (26, 18) = 2$. Logo,

$$(12794, 798) = 2\,.$$

O mmc entre dois inteiros possui uma propriedade importante: se c é um múltiplo comum de a e b, então, não só $[a, b]$ é menor que c como também $[a, b]$ divide c. De fato, pondo $m = [a, b]$, podemos escrever, pelo algoritmo de Euclides, $c = mq + r$, com $0 \leq r < m$. Como a, b dividem c e m, então, pela última igualdade, a e b dividem r. Portanto, r também é um múltiplo comum de a e b. Como $r < m$, isso nos obriga a termos $r = 0$, e portanto, m divide c. Esta argumentação prova o resultado abaixo.

Proposição 6 O mmc entre dois inteiros a e b divide todos os múltiplos comuns de a e b.

A proposição a seguir fornece uma interessante relação entre o mdc e o mmc de dois inteiros.

Proposição 7 Se $a, b \in \mathbb{N}$ então $(a, b)[a, b] = ab$.

7 Números primos

Nesta seção, falaremos um pouco sobre os números primos. Estes números são extremamente importantes e estão associados a um grande número de problemas famosos e de grande relevância para a matemática.

Definição 8 Um número natural maior que 1 é dito *primo* se for divisível somente por 1 e por si próprio.

Um número natural $n > 1$ que não é primo pode ser escrito como $n = n_1 \cdot n_2$ com $1 < n_1, n_2 < n$ e por isso é chamado de *composto*. Assim, exemplos de números primos são $2, 3, 5, 7, 11, 13, 17, \ldots$ e $4, 6, 8, 9, 10, 12, 14, \ldots$ são compostos.

Na proposição abaixo são enunciadas propriedades importantes dos números primos.

Proposição 9 Sejam $a, b \in \mathbb{N}$ quaisquer e $p, q \in \mathbb{N}$ primos. São verdadeiras as afirmações abaixo:

1. Se $p|q$ então $p = q$.
2. Se $p \nmid a$ então $(p, a) = 1$.
3. Se $p|ab$ então $p|a$ ou $p|b$.
4. Se p divide um produto de números primos então p deve ser igual a um deles.

Observamos que quando um número é composto, pode ser reduzido sucessivamente até ser escrito como produto de primos. Veja isto nos exemplos abaixo:

① $24 = 2 \cdot 12 = 2 \cdot 2 \cdot 6 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$

② $784 = 2 \cdot 392 = 2 \cdot 2 \cdot 196 = \ldots = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 7 = 2^4 \cdot 3^2 \cdot 7$

③ $13981323125 = \ldots = 5^4 \cdot 7^5 \cdot 11^3$

A pergunta é: *Isso pode ser feito para qualquer número natural?* É claro que para responder esta pergunta, não podemos testar os números naturais um por um; é preciso utilizar o *Princípio de Indução finita*. Vejamos como isto pode ser feito.

Evidentemente, como 2 é primo, se escreve como produto de primos. Além disso, se todos os números menores que um certo inteiro $n > 2$ são primos então, ou n é primo (e a afirmação está provada) ou n é composto, digamos $n = n_1 \cdot n_2$, com $1 < n_1, n_2 < n$. Como, por hipótese indutiva, n_1, n_2 se escrevem como produto de primos, segue que n é um produto de primos. Um instante de reflexão utilizando o ítem (4) da proposição (9) mostra que esta fatoração é essencialmente única a menos da ordem dos fatores. Sendo assim, está provado o *Teorema Fundamental da Aritmética*.

Teorema 10 Todo número natural maior que 1 se escreve de forma única (a menos da ordem dos fatores) como produto de números primos.

Assim, os números primos podem ser vistos como os pequenos *tijolos* a partir dos quais todos os outros inteiros são construídos. Uma questão que surge naturalmente é saber *quantos* destes números existem. A resposta é dada na proposição abaixo, devida a Euclides. A demonstração utiliza o método chamado de *redução ao absurdo* e é a primeira situação em que se tem notícia do uso deste método.

Proposição 11 Existem infinitos números primos.

Prova. Se fato, caso os primos fossem em quantidade finita, poderíamos enumerá-los como $p_1, p_2, \ldots, p_n$. Sendo assim, consideremos o número

$$N = p_1 \cdot \ldots \cdot p_n + 1 \,.$$

Se p é um divisor primo de N, então p deve ser um dos $p_j's$, e portanto, $p|1$, o que é um absurdo. ∎

Como consequência do Teorema Fundamental da Aritmética acima, podemos escrever cada número inteiro $n > 1$ de forma única como

$$n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k} \,,$$

onde $p_1, \ldots, p_k$ são primos distintos e $\alpha_1, \ldots, \alpha_k$ são unicamente determinados. Esta decomposição é bastante útil para fazermos contas, como veremos abaixo.

Proposição 12 Sejam $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ e $n = p_1^{\beta_1} \cdot \ldots \cdot p_k^{\beta_k}$ naturais. Então

$$(m, n) = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k} \text{ e } [m, n] = p_1^{b_1} \cdot \ldots \cdot p_k^{b_k} \,,$$

onde $a_j = \min\{\alpha_j, \beta_j\}$ e $b_j = \max\{\alpha_j, \beta_j\}$, para $j = 1, \ldots, k$. Além disso, os divisores de m são todos da forma

$$d = p_1^{c_1} \cdot \ldots \cdot p_k^{c_k} \,,$$

onde $0 \leq c_j \leq \alpha_j$ para $j = 1, \ldots, k$.

Este é o método utilizado usualmente em sala de aula para cálculo de MDC e MMC. A grande fragilidade deste método é que nem sempre é fácil escrever a decomposição em fatores primos de números maiores. A segunda afirmação da proposição acima mostra que a quantidade de divisores de um inteiro $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ é dada por

$$d(n) = (\alpha_1 + 1) \cdot \ldots \cdot (\alpha_k + 1) .$$

Uma questão que surge naturalmente é saber *quantos* primos existem. A resposta é dada na proposição abaixo, devida a Euclides. A demonstração utiliza o método chamado de *redução ao absurdo* e é a primeira situação em que se tem notícia do uso deste método.

Proposição 13 Existem infinitos números primos.

Prova. Se fato, caso os primos fossem em quantidade finita, poderíamos enumerá-los como $p_1, p_2, \ldots, p_n$. Sendo assim, consideremos o número

$$N = p_1 \cdot \ldots \cdot p_n + 1 .$$

Se p é um divisor primo de N, então p deve ser um dos $p_j's$, e portanto, $p|1$, o que é um absurdo. ∎

Erastóstenes de Cirene

Uma maneira simples de determinar se números relativamente pequenos são primos é o chamado *Crivo de Erastóstenes*. Este foi um matemático grego que viveu entre 276 a.C. e 194 a.C. responsável por façanhas impressionantes para sua época. Por exemplo, ele foi o primeiro a calcular com precisão a circunferência da Terra, utilizando para isto uma idéia geométrica bem simples e obtendo um valor muito próximo do real. Veja mais informações sobre Erastóstenes aqui.

Para ilustrar a construção, vamos escrever todos os números inteiros de 2 a 180 em uma tabela e determinar quais são primos. Vamos riscar todos os que não são primos, começando pelos múltiplos de 2.

	~~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~~

Agora, eliminamos os múltiplos de 3, 5 e 7:

	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

Se continuarmos eliminando os múltiplos dos primos 11, 13, etc, evidentemente sobrarão somente os primos na tabela. A pergunta é: *Será que precisamos fazer isso com todos os primos até 160?* A resposta é **NÃO!** Observe que se $n \in \mathbb{N}$ é um número composto e p é o *menor* primo que divide n, então $n = pm$ para algum $m > 1$. Como m é um produto de primos $\geq p$, temos que $m \geq p$ e portanto, $p^2 = p \cdot p \leq p \cdot m = n$. Isto significa que o menor primo que divide n é sempre $\leq \sqrt{n}$. Em particular, se $n \in \mathbb{N}$ não é divisível por nenhum primo $\leq \sqrt{n}$, então n é primo. Isto significa que basta eliminarmos na tabela acima apenas os múltiplos de 2,3,5,7 e 11 (pois $12 < \sqrt{160} < 13$). A tabela fica assim:

	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

A argumentação anterior prova o resultado abaixo.

Proposição 14 (Crivo de Erastóstenes) Um número $n \in \mathbb{N}$ é primo se e só se não é divisível por nenhum primo $p \leq \sqrt{n}$.

A palavra *crivo* é utilizada acima como sinônimo da palavra *teste*, dando a idéia de que se um número $n \in \mathbb{N}$ passar pelo teste (i.e., se ele não for divisível por nenhum primo $\leq \sqrt{n}$) então n é primo. Este método funciona bem para determinar primos relativamente pequenos, pois parte do pressuposto que já conhecemos todos os primos menores que $\sqrt{n}$. Para determinar primos grandes, ele é definitivamente inviável, dada a assombrosa quantidade de cálculos necessários. Existem vários outros critérios para determinar se um número é primo, veja, por exemplo, o Critério de Lucas e o Critério de Lucas-Lehmer.

Uma propriedade especial dos números primos é o fato que, se p é primo e $a \in \mathbb{N}$ então

$$a^p \equiv a \mod p.$$

Como corolário, observamos que se p é primo e não divide a então $a^{p-1} \equiv 1 \mod p$. Este resultado é chamado de *Pequeno Teorema de Fermat* em homenagem ao matemático francês Pierre de Fermat (1601-1665), a quem é devida a sua descoberta. Vamos ilustrar com um exemplo o uso do Teorema de Fermat.

Pierre de Fermat

Exemplo 15 Vamos mostrar que

$$a^{11} \equiv a \mod 66$$

para todo $a \in \mathbb{N}$. De fato, pelo Pequeno Teorema de Fermat, $11|a^{11} - a$ para todo $a \in \mathbb{N}$. Evidentemente, $a^{11} - a$ é sempre par, portanto, $2|a^{11} - a$. Agora, observemos a tabela abaixo de restos módulo 3:

$a \mod 3$	$a^{11} - a$	$a^{11} - a \mod 3$
0	0	0
1	0	0
2	2046	0

Assim, em qualquer circunstância, $3|a^{11} - a$. Portanto, como 2,3 e 11 são primos entre si, segue que $66 = 2 \cdot 3 \cdot 11$ divide $a^{11} - a$.

8 Potências, Raízes e Números Reais

Do ponto de vista prático, podemos pensar na multiplicação como uma adição generalizada, observando que dados $m, n \in \mathbb{N}$,

$$mn = \underbrace{m + m + ... + m}_{n \text{ vezes}}.$$

Desta forma, não só a notação é mais compacta, mas os cálculos tornam-se mais simples. A potenciação pode ser tratada de maneira análoga, basta observar que

$$m^n = \underbrace{m.m.....m}_{n \text{ vezes}}.$$

Por exemplo, $2^7 = 128$, $3^3 = 27$, $5^2 = 25$, $9^4 = 6561$. Do ponto de vista prático, é razoável pensar se é possível *desfazer* a operação de potenciação. A resposta é *sim* para alguns casos: o único número cuja sétima potência é 128 é 2; o único número cujo cubo é 27 é 3. Por outro lado, tanto 5 quanto -5 têm quadrado igual a 25 e 9 e -9 têm quarta potência igual a 6561. Vamos estudar um pouco a operação inversa da potenciação de expoente n.

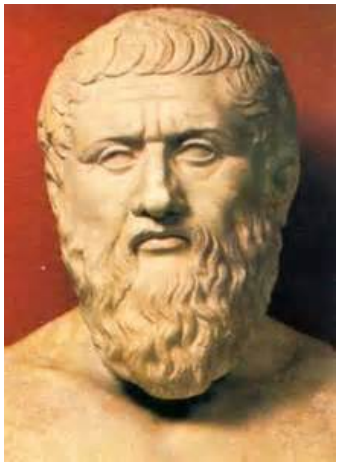
Definição 16 Dado $n > 1$ natural, um número x é dito *raiz n-ésima de a* se $x^n = a$. Escrevemos $x = \sqrt[n]{a}$ quando não houver perigo de ambiguidade. Quando $n = 2$, escrevemos somente $\sqrt{a}$ ao invés de $\sqrt[2]{a}$.

Vemos que $\sqrt[7]{128} = 2$ e $\sqrt[3]{27} = 3$. Uma pergunta surge de forma natural: *Que tipo de número podemos colocar dentro da raiz e que tipo de número obtemos como resultado?* Por exemplo, podemos colocar qualquer natural dentro da raiz? A resposta é: *depende*. Se quisermos obter como resposta um número natural b, podemos somente números naturais da forma b^n. Mas isso já é pedir demais... Na prática, raízes quadradas, cúbicas e outras aparecem com muita frequência na resolução de problemas variados e não podemos nos dar ao luxo de trabalhar somente com raízes inteiras.

Um conjunto muito importante de números já conhecido desde a Antiguidade pelos gregos e egípcios é o conjunto dos *números racionais*. Estes são as razões (quocientes) entre inteiros e surgem de maneira muito natural na resolução de qualquer problema simples envolvendo multiplicação de inteiros. De forma mais precisa, o conjunto dos números racionais, denotado pela letra $\mathbb{Q}$, é formado por todas as razões da forma $\frac{m}{n}$, onde $m, n \in \mathbb{Z}$ e $n \neq 0$. Assim, $\frac{1}{2} \in \mathbb{Q}$, $-\frac{19}{5} \in \mathbb{Q}$, $\frac{1977}{2014} \in \mathbb{Q}$, etc. As operações de soma e divisão de números racionais são definidas da maneira habitual.

Os filósofos da Escola Pitagórica (Século V a.C.) criam que os números naturais e suas razões (quocientes) descreviam o Universo. Esta idéia foi profundamente influencial sobre o pensamento filosófico da época. Para os pitagóricos, era totalmente inconcebível que algum fenômeno natural produzisse uma quantidade que não pudesse ser expressa por meio de uma razão entre números naturais. Este raciocínio provém, em parte, da idéia que o todo é constituído por uma quantidade finita de partes indivisíveis. Um partidário desta idéia foi o filósofo pré-socrático *Zeno de Eleia* (490-430 a.C.). Você pode encontrar mais informações sobre Zeno aqui.

Vamos agora discutir alguns problemas historicamente importantes cujas tentativas de soluções influenciaram profundamente o pensamento matemático e o conceito de número.



Zeno de Eleia

⚹ A Constante Pitagórica

Hippasus de Metapontum

Hippasus de Metapontum, membro da Escola Pitagórica, nasceu em torno do ano 500 a.C. em Metapontum, cidade grega da Magna Grécia situada no Golfo de Tarento, ao sul da atual Itália. Embora as evidências sejam obscuras, Hippasus é tido como o primeiro a provar a existência de números irracionais. Ele observou que a diagonal de um quadrado de lado 1 deveria ser um número d tal que $d^2 = 2$ (ou seja, $d = \sqrt{2}$) e este número não pode ser expresso como quociente de dois inteiros. Este número d é chamado de *constante pitagórica*. A descoberta e a divulgação de uma quantidade que não podia ser expressa como quociente de dois inteiros chocou os membros da Escola Pitagórica, que teriam afogado Hippasus no mar por ter divulgado o fato.

Muito antes disto, os babilônios utilizavam a aproximação

$$1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} = \frac{30547}{21600} = 1.41421\overline{296}.$$

para $\sqrt{2}$, a qual foi encontrada em um fragmento de argila de 1600 a.C.! Outra aproximação interessante é dada no texto indiano *Sulbasutras (800 a.C.)* da seguinte forma: *aumente o lado pela sua terça parte e esta terça parte pela sua quarta parte menos a trigésima quarta parte deste quarto.* Em linguagem moderna, isto quer dizer

$$1+\frac{1}{3}+\frac{1}{3\cdot 4}-\frac{1}{3\cdot 4\cdot 34}=\frac{577}{408}=1.414\overline{2156862745098039}.$$

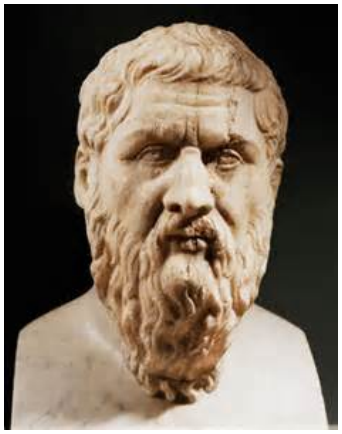
⚹ O problema da duplicação do cubo

Os pitagóricos já sabiam como, dado um quadrado, construir outro quadrado cuja área é o dobro da área do quadrado dado. Basta construir o novo quadrado tendo como lado a diagonal do quadrado dado. Provavelmente, os gregos tenham então transposto tal problema para as sólidos:

Dado um cubo, construir um novo cubo cujo volume seja o dobro do volume do cubo dado.

Este problema, que possui uma história muito interessante, é chamado de *Problema da Duplicação do Cubo* ou *Problema Deliano*, em referência a cidade grega de Delos (Atenas). Diz a lenda que os cidadãos de Delos consultaram o oráculo de Delfos, a fim de saber como derrotar uma praga enviada pelo deus Apolo. O oráculo respondeu que se devia dobrar o tamanho do altar a Apolo, que era um cubo regular. Os delianos estranharam a resposta e consultaram Platão, que foi capaz de interpretar o oráculo como o problema matemático de dobrar o volume de um cubo dado. A explicação de Platão para o conselho de Apolo era que os cidadãos de Delos deviam para estudar geometria a fim de acalmar suas paixões...

De acordo com Plutarco, Platão passou o problema para Eudoxus, Archytas e Menaechmus, que o resolveram utilizando meios mecânicos. Estes, receberam uma repreensão de Platão por não terem resolvido o problema usando somente geometria pura. Tanto é que o problema é referido nos *Diálogos* de Platão em 350 a.C. como ainda não resolvido. Outra versão da história é que os três encontraram soluções, mas estas eram muito abstratas para serem de valor prático.



Platão

Um desenvolvimento significativo na busca de uma solução para o problema foi feito por Hipócrates de Chios, que mostrou ser o problema equivalente a encontrar duas médias proporcionais entre dois segmentos, tendo um deles o dobro do comprimento do outro. Em linguagem um pouco mais contemporânea, isto significa que dados segmentos de comprimentos a e $2a$, a duplicação do cubo é equivalente a encontrar segmentos de comprimentos r e s tais que

$$\frac{a}{r}=\frac{r}{s}=\frac{s}{2a}.$$

Em particular, $r=a\cdot\sqrt[3]{2}$, como desejado. Somente muito tempo depois, em 1837, o matemático francês Pierre Laurent Wantzel mostrou que o número $\sqrt[3]{2}$ *não* pode ser construído utilizando somente régua (sem marcas) e compasso.

Neste ponto, podemos fazer um questionamento razoável: *Já que raízes podem não ser números racionais, será mesmo que elas existem? Será razoável admití-las?* A resposta é *sim*! Os antigos babilônios utilizavam há muito tempo um método empírico para extração de raízes quadradas, que pode

ser descrito como segue. Dado um número $a > 1$, para encontrar um número b tal que $b^2 = a$, considere a sequência de números $x_1, x_2, x_3, \ldots$ definida da seguinte forma: $x_1 = a$ e, admitindo x_n definido, definimos

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{a}{x_n}\right).$$

Pois bem, pode-se mostrar que a sequência acima se *aproxima*, com o grau de precisão que desejarmos, do número b procurado.

Sendo assim, percebemos que um ambiente numérico adequado para trabalharmos com liberdade deve, de alguma maneira, incluir as nuances e sutilezas tratadas acima. Este ambiente existe e é o conjunto dos *números reais* denotado usualmente pela letra $\mathbb{R}$. As questões teóricas envolvendo a existência e a construção dos números reais sempre permearam a matemática através dos séculos, mas ficaram mais evidentes a partir da segunda metade do século XIX quando matemáticos brilhantes como Karl Weierstrass, Augustin Cauchy, Richard Dedekind, Georg Cantor, entre outros, perceberam a necessidade de estabelecer bases matemáticas sólidas para o desenvolvimento do Cálculo e da Análise Matemática.