SBM SOCIEDADE BRASILEIRA DE MATEMÁTICA

PROFESSOR DE MATEMÁTICA ONLINE
Revista eletrônica da Sociedade Brasileira de Matemática

2017, NÚMERO 1, VOLUME 5
ISSN 2319-023X

Implementações Aritméticas

Evilson Vieira
Universidade Federal de Sergipe - UFS
evilson@ufs.br

Resumo

Neste trabalho apresentamos uma implementação para execução manual do algoritmo estendido das divisões sucessivas de Euclides para a obtenção de soluções de equações diofantinas lineares de duas variáveis e, em particular, para o cálculo do inverso multiplicativo modular. Também apresentamos uma implementação para o cálculo manual da solução de um sistema de restos.

Palavras-chave: implementações aritméticas; inverso modular; sistema de restos.

1. Introdução

Quando efetuamos cálculos manuais sempre estamos executando alguns algoritmos previamente estudados, comprovados e documentados por matemáticos ao redor do mundo. Para executarmos tais algoritmos é necessário que usemos uma implementação desses algoritmos. Chamamos de implementação uma diagramação intuitiva associada a um algoritmo, que registra, de forma organizada, os passos do algoritmo e seus valores parciais. Uma boa implementação é aquela que além de tornar possível a execução do algoritmo:

- ◇ faz com que essa execução seja rápida;
- ◇ evita cálculos desnecessários;
- ◇ evita repetições desnecessárias de termos;
- ◇ facilita a detecção de erros de cálculo;

Como exemplo citamos uma implementação bem conhecida do cálculo do mdc (máximo divisor comum) de dois números inteiros positivos em que dispomos os valores parciais das divisões sucessivas de Euclides em uma estrutura matricial com três linhas conforme ilustramos a seguir:

Problema 1. *Dados os inteiros positivos* m, n*, encontrar* $\text{mdc}(m, n)$.

Solução: Convenientemente tomamos $m \geqslant n$. Usamos o algoritmo das divisões sucessivas de Euclides, registrando os quocientes e restos parciais na estrutura matricial abaixo:

	q_2	q_3	$\cdots$	q_{k-1}	q_k
d_1	d_2	d_3	$\cdots$	d_{k-1}	d_k
r_1	r_2	r_3	$\cdots$	(0)	

Colocamos $d_1 = m$ e $d_2 = n$ e, para cada $j = 1, 2, 3, \ldots, k$, fazemos, recursivamente:

$$\boxed{d_j = d_{j+1} \cdot q_{j+1} + r_j} \text{ e } \boxed{d_{j+2} = r_j}$$

ou seja, dividimos d_j por d_{j+1} e anotamos o quociente q_{j+1} na primeira linha e o resto r_j na terceira linha e, depois disso, copiamos o resto obtido para a segunda linha. Repetimos esse procedimento até obtermos um resto zero. Então, o último termo da segunda linha é o valor procurado, ou seja,

$$d_k = \text{mdc}(d_1, d_2).$$

Exemplo: Para $m = 487$ e $n = 305$ temos:

	1
487	305
182	

Pois $487 = 305 \cdot 1 + 182$;

	1	1
487	305	182
182	123	

Pois $305 = 182 \cdot 1 + 123$;
(note que 182 foi copiado da terceira para a segunda linha)

Continuamos até obter um resto zero:

	1	1	1	2	11	1	4
487	305	182	123	59	5	4	(1)
182	123	59	5	4	1	0	

E concluímos que $\text{mdc}(487, 305) = 1$.

Essa implementação aritmética é bem popular e ilustra o quanto é interessante ter uma diagramação organizada das etapas parciais de um algoritmo.

2. Resolvendo equações diofantinas lineares com duas variáveis

Nesta seção, o foco é resolver equações da forma

$$mx + ny = c, \tag{1}$$

onde $m, n \in \mathbb{Z}$, e queremos encontrar todos os pares de inteiros (x, y) que sejam soluções desta equação. É bem conhecido (veja Hefez (1993) ou Hefez (2006)) que, para essa equação ter solução, basta que $\text{mdc}(m, n) \mid c$. Consideraremos que tal afirmação é válida aqui em nosso problema.

Suponhamos que conheçamos duas soluções distintas da equação (1), digamos (x_0, y_0) e (x_1, y_1), nesse caso temos:

$$\begin{cases} mx_0 + ny_0 = c \\ mx_1 + ny_1 = c. \end{cases}$$

Subtraindo-se os membros esquerdo e direito dessas duas equações, obtemos:

$$m(x_1 - x_0) + n(y_1 - y_0) = 0.$$

Portanto, o par de inteiros $(x_1 - x_0, y_1 - y_0)$ é solução da equação diofantina linear

$$mx + ny = 0. \tag{2}$$

Seja $d = \text{mdc}(m, n)$. Escrevamos $m = dm_1$ e $n = dn_1$, dessa forma, $\text{mdc}(m_1, n_1) = 1$. Assim, (2) torna-se

$$\begin{aligned} ny &= -mx \\ dn_1 y &= -dm_1 x \\ n_1 y &= -m_1 x. \end{aligned} \tag{3}$$

Seja (x, y) uma solução de (3). Como $\text{mdc}(m_1, n_1) = 1$, concluímos que $n_1 \mid x$, então podemos escrever $x = n_1 t$, para algum inteiro t. Substituido-se essa igualdade em (3), temos

$$\begin{aligned} n_1 y &= -m_1 n_1 t \\ y &= -m_1 t. \end{aligned} \tag{4}$$

Então, as soluções de (2) são os pares da forma $(x, y) = (n_1 t, -m_1 t)$, ou seja, $(x, y) = \left(\frac{n}{d}t, -\frac{m}{d}t\right)$, onde t percorre todos os números inteiros. De acordo com tais resultados, se (x_0, y_0) é uma solução particular de (1) então, o conjunto de todas as soluções de (1) é dado por

$$\left\{ \left(x_0 + \frac{n}{\text{mdc}(m,n)}t,\, y_0 - \frac{m}{\text{mdc}(m,n)}t \right) ;\, t \in \mathbb{Z} \right\}.$$

Exemplo: $(3, 4)$ é uma solução particular da equação $5x - 3y = 3$. Portanto o conjunto solução dessa equação é $\{(3 + 3t,\, 4 + 5t) ;\, t \in \mathbb{Z}\}$.

Dessa forma, resolver uma equação diofantina linear de duas variáveis reduz-se à determinação de uma solução particular (x_0, y_0).

Na verdade, basta que saibamos resolver o Problema 2 abaixo:

Problema 2. *Dados os inteiros positivos m, n, encontrar inteiros r e s tais que*

$$r \cdot m + s \cdot n = d, \tag{5}$$

onde $d = \text{mdc}(m, n)$.

De fato, considere a equação (1), onde $d \mid c$, se tivermos uma solução (r, s) do Problema 2, então o par $\left(\frac{c}{d}r, \frac{c}{d}s\right)$ é uma solução de (1), pois:

$$\frac{c}{d}rm + \frac{c}{d}sn = \frac{c}{d}(rm + sn) = \frac{c}{d}d = c.$$

É bem conhecido que o Problema 2 sempre tem solução (veja Teorema de Bachet-Bézout em Martinez (2010)). Esta solução é obtida executando-se o algoritmo estendido das divisões sucessivas de Euclides. Na seção seguinte propomos uma implementação para a execução deste algoritmo.

3. Implementação do Algoritmo Estendido de Euclides

Nosso foco agora é propor uma implementação para resolver o Problema 2. Primeiramente propomos enxugar a implementação do cálculo do mdc mencionado na Introdução. Note que a terceira linha pode ser ignorada devido ao fato de que todos os seus termos são copiados para a segunda linha. Podemos, então, deixar a implementação apenas com as duas primeiras linhas:

	q_2	q_3	$\cdots$	q_{k-1}	q_k	
d_1	d_2	d_3	$\cdots$	d_{k-1}	(d_k)	0

Onde $d_1 = m$ e $d_2 = n$ e para cada $j = 1, 2, 3, \ldots, k$, fazemos, recursivamente:

$$\boxed{d_j = d_{j+1} \cdot q_{j+1} + d_{j+2}} \tag{6}$$

até que o último termo da segunda linha seja zero. Então o penúltimo termo da segunda linha é o valor procurado, ou seja,

$$d_k = \text{mdc}(d_1, d_2)$$

Exemplo: Para $m = 487$ e $n = 305$ temos:

	1	
487	305	182

	1	1	
487	305	182	123

	1	1	1	2	11	1	4	
487	305	182	123	59	5	4	(1)	0

E concluímos que $\text{mdc}(487, 305) = 1$.

Note que, nos casos em que $\text{mdc}(m, n) = 1$, podemos encerrar a etapa das divisões sucessivas no momento em que obtivermos o primeiro resto igual a 1, pois já sabemos que o próximo resto será zero.

Após executada esta primeira parte do algoritmo, adicionamos uma nova linha à estrutura inical, com elementos a_j:

	q_2	q_3	$\cdots$	q_{k-1}	q_k	
d_1	d_2	d_3	$\cdots$	d_{k-1}	(d_k)	0
a_1	a_2	a_3	$\cdots$	a_{k-1}	a_k	

de forma que, para cada posição j tenhamos:

$$a_j \cdot d_{j+1} + a_{j+1} \cdot d_j = d_k \tag{7}$$

$\cdots$	q_j	q_{j+1}	$\cdots$	q_k	
$\cdots$	d_j	d_{j+1}	$\cdots$	(d_k)	0
$\cdots$	a_j	a_{j+1}	$\cdots$	a_k	

As setas duplas cruzadas indicam os pares de inteiros a serem multiplicados, de forma que a soma desses produtos seja d_k. Observe que, substituindo d_{j+1} na equação (7) usando (6), obtemos uma expressão para a_{j-1} que depende, apenas, de q_j, a_j e a_{j+1}:

$$\begin{aligned} a_j \cdot (d_{j-1} - d_j \cdot q_j) + a_{j+1} \cdot d_j &= d_k \\ a_j \cdot d_{j-1} - a_j \cdot d_j \cdot q_j + a_{j+1} \cdot d_j &= d_k \\ \underbrace{(a_{j+1} - q_j \cdot a_j)}_{a_{j-1}} \cdot d_j + a_j \cdot d_{j-1} &= d_k \end{aligned} \tag{8}$$

$\cdots$	q_{j-1}	q_j	q_{j+1}	$\cdots$
$\cdots$	d_{j-1}	d_j	d_{j+1}	$\cdots$
$\cdots$	a_{j-1}	a_j	a_{j+1}	$\cdots$

Ou seja, cada termo da terceira linha pode ser obtido a partir dos dois termos posteriores, então a terceira linha precisa ser preenchida da direita para a esquerda. Observemos que os candidatos mais simples para as duas últimas posições, a_k e a_{k-1}, para que satisfaçam a equação (7), são $\boxed{a_k = 0}$ e $\boxed{a_{k-1} = 1}$. Portanto, podemos iniciar o preenchimento da terceira linha começando com 0 e 1:

	q_2	q_3	$\cdots$	q_{k-1}	q_k	
d_1	d_2	d_3	$\cdots$	d_{k-1}	(d_k)	0
				1	0	

Veja que:

$$1 \cdot d_k + 0 \cdot d_{k-1} = d_k$$

Terminamos o preenchimento usando a recorrência obtida na equação (8):

$$a_{j-1} = a_{j+1} - q_j \cdot a_j.$$

No final da recorrência obteremos os valores a_1 e a_2 que satisfazem à equação

$$a_1 \cdot d_2 + a_2 \cdot d_1 = d_k$$

que era nosso objetivo.

Exemplo: Para $m = 487$ e $n = 305$, a implementação fica da seguinte forma:

	1	1	1	2	11	1	4	
487	305	182	123	59	5	4	(1)	0
99	**−62**	37	−25	12	−1	1	0	

E temos os valores $r = -62$ e $s = 99$, que satisfazem à equação que queríamos:

$$(\mathbf{-62}) \cdot 487 + \mathbf{99} \cdot 305 = 1$$

3.1. O inverso multiplicativo modular

Quando $\text{mdc}(m, n) = 1$, os valores r e s obtidos podem ser interpretados como inverso multiplicativo de m módulo n e inverso multiplicativo n módulo m, respectivamente. De fato, se tivermos:

$$r \cdot m + s \cdot n = 1$$

Então:

$$\boxed{r \cdot m \equiv 1 \pmod{n}} \text{ e } \boxed{s \cdot n \equiv 1 \pmod{m}}$$

Denotaremos por $m^{-1}_{(n)}$ o inverso multiplicativo de m módulo n.

No nosso exemplo temos $487^{-1}_{(305)} = -62$ e $305^{-1}_{(487)} = 99$. A seguir fazemos uso de um problema para ilustrar a aplicação do dispositivo:

Problema 3. *Qual o menor inteiro positivo cujo produto com* 305 *deixa resto* 43 *quando dividido por* 487*?*

Solução:

$$\begin{aligned}
305x &\equiv 43 && \pmod{487} \\
(\underbrace{305^{-1}_{(487)} \cdot 305}_{\equiv 1})x &\equiv 305^{-1}_{(487)} \cdot 43 && \pmod{487} \\
x &\equiv 99 \cdot 43 && \pmod{487} \\
x &\equiv 361 && \pmod{487}.
\end{aligned}$$

4. Resolvendo um sistema de restos

Nosso problema agora é resolver o sistema de restos:

$$\begin{cases}
x \equiv a_1 \pmod{m_1} \\
x \equiv a_2 \pmod{m_2} \\
x \equiv a_3 \pmod{m_3} \\
\vdots \quad \vdots \quad \vdots \\
x \equiv a_k \pmod{m_k},
\end{cases} \tag{9}$$

onde $\text{mdc}(m_i, m_j) = 1$, para $i \neq j$.

É bem conhecido (veja Teorema Chinês do Resto em Hefez (1993), Hefez (2006) ou Martinez (2010)) que esse sistema tem solução, e que essa solução é dada por:

$$x \equiv M_1 b_1 + M_2 b_2 + M_3 b_3 + \cdots + M_k b_k \pmod{M}, \tag{10}$$

onde

$$\begin{cases} M = m_1 m_2 m_3 \cdots m_k \\ M_j = \dfrac{M}{m_j}\ ,\ j \in \{1, 2, 3, \ldots, k\} \\ M_j b_j \equiv a_j \pmod{m_j}\ ,\ j \in \{1, 2, 3, \ldots, k\}. \end{cases}$$

O valor de M e os valores $\{M_1, M_2, M_3, \ldots, M_k\}$ são obtidos sem dificuldade. Para obter os valores $\{b_1, b_2, b_3, \ldots, b_k\}$, fazemos:

$$\begin{aligned} M_j b_j &\equiv a_j && \pmod{m_j} \\ (\underbrace{M_{j(m_j)}^{-1} M_j}_{\equiv 1}) b_j &\equiv M_{j(m_j)}^{-1} a_j && \pmod{m_j} \\ b_j &\equiv M_{j(m_j)}^{-1} a_j && \pmod{m_j}, \end{aligned} \tag{11}$$

onde $M_{j(m_j)}^{-1}$ pode ser calculado da seguinte forma:

$$\begin{aligned} M_{j(m_j)}^{-1} &\equiv \left(\prod_{i \neq j} m_i \right)_{(m_j)}^{-1} && \pmod{m_j} \\ &\equiv \prod_{i \neq j} m_{i(m_j)}^{-1} && \pmod{m_j}. \end{aligned} \tag{12}$$

E, assim, temos a solução do sistema (9).

4.1. A implementação do algoritmo

Apresentamos, agora, a implementação proposta para o cálculo da solução do sistema (9).

Primeiramente, ordenamos as equações do sistema de forma que $m_1 > m_2 > m_3 > \cdots > m_k$ e montamos uma tabela com os termos $c_{(i,j)} = m_{i(m_j)}^{-1}$, para $i \neq j$.

	$c_{(1,2)}$	$c_{(1,3)}$	$\cdots$	$c_{(1,k)}$
$c_{(2,1)}$		$c_{(2,3)}$	$\cdots$	$c_{(2,k)}$
$c_{(3,1)}$	$c_{(3,2)}$		$\cdots$	$c_{(3,k)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$	$c_{(k,2)}$	$c_{(k,3)}$	$\cdots$	

Note que deixamos vazias as células $c_{(j,j)}$, ou seja, as células da diagonal.

Executando-se a implementação do cálculo do inverso multiplicativo modular para os pares (m_1, m_2), (m_1, m_3), ..., (m_1, m_k), obtemos a primeira coluna e primeira linha da tabela, conforme ilustrado abaixo:

	$c_{(1,2)}$	$c_{(1,3)}$	$\cdots$	$c_{(1,k)}$
$c_{(2,1)}$			$\cdots$	
$c_{(3,1)}$			$\cdots$	
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$			$\cdots$	

	$\#$	$\cdots$
m_1	m_2	$\cdots$
$c_{(2,1)}$	$c_{(1,2)}$	$\cdots$

	$\#$	$\cdots$
m_1	m_3	$\cdots$
$c_{(3,1)}$	$c_{(1,3)}$	$\cdots$

$\vdots$

	$\#$	$\cdots$
m_1	m_k	$\cdots$
$c_{(k,1)}$	$c_{(1,k)}$	$\cdots$

Executando-se a implementação do cálculo do inverso multiplicativo modular para os pares (m_2, m_3), (m_2, m_4), ..., (m_2, m_k), completamos a segunda coluna e segunda linha da tabela. E assim por diante (os símbolos "#" representam valores que aparecem na implementação mas que não serão úteis na montagem da tabela).

Feito isso, preenchemos as células vazias com os termos $\{a_1, a_2, a_3, \ldots, a_k\}$ do sistema de restos, de forma que o termo a_j ocupe a célula (j, j). Por fim, acrescentamos uma linha extra à tabela onde colocaremos os valores $\{b_1, b_2, b_3, \ldots, b_k\}$.

a_1	$c_{(1,2)}$	$c_{(1,3)}$	$\cdots$	$c_{(1,k)}$
$c_{(2,1)}$	a_2	$c_{(2,3)}$	$\cdots$	$c_{(2,k)}$
$c_{(3,1)}$	$c_{(3,2)}$	a_3	$\cdots$	$c_{(3,k)}$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
$c_{(k,1)}$	$c_{(k,2)}$	$c_{(k,3)}$	$\cdots$	a_k
b_1	b_2	b_3	$\cdots$	b_k

Das equações (11) e (12) concluimos que cada b_j é o produto de todos os elementos da coluna j da tabela, módulo m_j, ou seja:

$$\begin{cases} b_1 \equiv a_1 c_{(2,1)} c_{(3,1)} \cdots c_{(k,1)} & (\text{mod } m_1) \\ b_2 \equiv c_{(1,2)} a_2 c_{(3,2)} \cdots c_{(k,2)} & (\text{mod } m_2) \\ b_3 \equiv c_{(1,3)} c_{(2,3)} a_3 \cdots c_{(k,3)} & (\text{mod } m_3) \\ \vdots \quad \vdots \qquad \ddots \qquad \vdots \\ b_k \equiv c_{(1,k)} c_{(2,k)} c_{(3,k)} \cdots a_k & (\text{mod } m_k). \end{cases}$$

E, finalmente, podemos escrever a solução:

$$x \equiv M_1b_1 + M_2b_2 + M_3b_3 + \cdots + M_kb_k \pmod{M}. \tag{13}$$

Em geral, buscamos a menor solução não negativa do sistema, ou seja, queremos que $0 \leqslant x < M$. Para isso, basta escolher os b_js, convenientemente, de forma que:

$$\begin{aligned} 0 &\leqslant M_1b_1 + M_2b_2 + M_3b_3 + \cdots + M_kb_k < M \\ 0 &\leqslant \frac{M_1b_1}{M} + \frac{M_2b_2}{M} + \frac{M_3b_3}{M} + \cdots + \frac{M_kb_k}{M} < 1 \\ 0 &\leqslant \frac{b_1}{m_1} + \frac{b_2}{m_2} + \frac{b_3}{m_3} + \cdots + \frac{b_k}{m_k} < 1. \end{aligned}$$

Cabe observar que escolha dos b_j s dessa forma não é única.

Para fins de organização, é interessante escrever a solução (13) como:

$$x \equiv [b_1m_2m_3\cdots m_k] + [m_1b_2m_3\cdots m_k] + [m_1m_2b_3\cdots m_k] + \cdots + [m_1m_2m_3\cdots b_k] \pmod{M}.$$

ou seja, a j-ésima parcela é obtida substituindo-se m_j por b_j.

4.2. Um exemplo ilustrativo

Vamos resolver o sistema de restos: $\begin{cases} x \equiv 7 \pmod{17} \\ x \equiv 12 \pmod{15} \\ x \equiv 4 \pmod{11} \\ x \equiv 5 \pmod{7} \end{cases}$

	1	7	
17	15	2	1
8	−7	1	0

	1	2	1	
15	11	4	3	1
−4	3	−1	1	0

	1	1	1	
11	7	4	3	1
−3	2	−1	1	0

	1	1	1	
17	11	6	5	1
−3	2	−1	1	0

	2	
15	7	1
−2	1	0

	2	2	
17	7	3	1
5	−2	1	0

Preenchemos a diagonal da matriz com os valores fornecidos no problema.

	−7	2	−2
8			
−3			
5			

	−7	2	−2
8		3	1
−3	−4		
5	−2		

	−7	2	−2
8		3	1
−3	−4		2
5	−2	−3	

7	−7	2	−2
8	12	3	1
−3	−4	4	2
5	−2	−3	5

Substituiremos o 12 por -3 na segunda coluna, visto que é módulo 15. Usar valores o mais próximos de zero quanto pudermos pode simplificar os cálculos. Os valores obtidos na implementação do inverso multiplicativo modular já estão o mais próximo de zero possível. Agora calculamos os valores $\{b_1, b_2, b_3, b_4\}$ colocando-os na linha extra da matriz. Cada b_j é o produto dos termos da coluna j módulo m_j.

$$\begin{cases} b_1 \equiv 7 \cdot 8 \cdot (-3) \cdot 5 \equiv \mathbf{-7} & (\text{mod } 17) \\ b_2 \equiv (-7) \cdot (-3) \cdot (-4) \cdot (-2) \equiv \mathbf{3} & (\text{mod } 15) \\ b_3 \equiv 2 \cdot 3 \cdot 4 \cdot (-3) \equiv \mathbf{5} & (\text{mod } 11) \\ b_4 \equiv (-2) \cdot 1 \cdot 2 \cdot 5 \equiv \mathbf{1} & (\text{mod } 7) \end{cases}$$

7	-7	2	-2
8	-3	3	1
-3	-4	4	2
5	-2	-3	5
$\mathbf{-7}$	**3**	**5**	**1**

E então temos a solução:

$$x \equiv [(\mathbf{-7}) \cdot 15 \cdot 11 \cdot 7] + [17 \cdot \mathbf{3} \cdot 11 \cdot 7] + [17 \cdot 15 \cdot \mathbf{5} \cdot 7] + [17 \cdot 15 \cdot 11 \cdot \mathbf{1}] \pmod{17 \cdot 15 \cdot 11 \cdot 7}$$

$$x \equiv 7572 \pmod{19635}$$

Note que

$$\frac{-7}{17} + \frac{3}{15} + \frac{5}{11} + \frac{1}{7} > \frac{3}{15} + \frac{1}{7} > 0$$

$$\frac{-7}{17} + \frac{3}{15} + \frac{5}{11} + \frac{1}{7} < \frac{5}{11} + \frac{1}{7} < \frac{1}{2} + \frac{1}{2} = 1$$

Note, também, que poderíamos ter escolhido $b_1 = 10$ e $b_3 = -6$, pois $0 < \frac{10}{17} + \frac{3}{15} + \frac{-6}{11} + \frac{1}{7} < 1$.

Para fugir dessa desigualdade podemos escolher os b_j s o mais próximos de zero que pudermos. Mas, ocasionalmente, será necessário somar algum múltiplo de M (positivo ou negativo) ao resultado final para obtermos a menor solução não negativa.

Observe que todas as etapas intermediárias ficam bem diagramadas e organizadas favorecendo uma menor possibilidade de erro. E se houver erros, a diagramação facilita sua detecção.

5. Referências

Hefez, Abramo. *Curso de Álgebra*, vol. 1. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 1993.

Hefez, Abramo.*Elementos de Aritmética*. 2^a ed. Rio de Janeiro-RJ: Sociedade Brasileira de Matemática, 2006.

Martinez, Fabio Brochero; et alli. *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2010.