UM POUCO DA TEORIA DOS NÚMEROS: DA ANTIGUIDADE ATÉ OS DIAS ATUAIS

Cristiana Abud da Silva Fusco
PUC-SP
cfusco@pucsp.br

Sônia Pitta Coelho
PUC-SP
sonicoe@terra.com.br

RESUMO

Esse artigo faz uma retrospectiva histórica da origem do conceito de número focando os números inteiros positivos que são tratados na Teoria dos Números. Apresenta também uma discussão sobre números primos incluindo os números primos de Fermat, além de descrever o método do Crivo de Eratóstenes. O texto destaca, ainda, que não existem fórmulas de geração de primos. O método de criptografia RSA, utilizado na codificação de mensagens enviadas por computador, é descrito após discussões sobre a origem da criptografia.

PALAVRAS-CHAVE: Teoria dos Números; números primos; criptografia; método RSA

1. O CONCEITO DE NÚMERO ENTRE OS GREGOS

O estudo da geometria parece ter sucedido o estudo da aritmética mesmo entre os antigos gregos, e a afirmação atribuída a Pitágoras de que tudo é número parece corroborar essa crença. Acredita-se que, enquanto os gregos eram especialmente dotados para a geometria, os babilônios antigos dedicaram-se com especial talento à aritmética. Além das inquestionáveis descobertas conhecidas, os gregos geometrizaram alguns dos resultados que chegaram a eles da Babilônia e do Egito e assim criaram um tipo de álgebra geométrica, no contexto da qual teriam resolvido algumas equações quadráticas, resolução esta que chegou até nós e é bastante popular em livros de história da matemática elementar.

Os gregos antigos foram os primeiros a discutir o conceito de número, e um paradigma importante da matemática grega - pelo menos desde os tempos de Platão (429-348 A. C.) até Diofanto (segunda metade do século III) - é o seguinte: o conceito de número era restrito aos números inteiros positivos; ou seja, para os gregos, o conceito de número referia-se a magnitudes descontínuas, fato que teve importantes consequências na História da Matemática.

A definição: “Um número é uma ‘multidão’ de unidades” aparece no início do Livro VII dos Elementos de Euclides. Mesmo a separação dos inteiros positivos em duas categorias de números, pares e ímpares, aparece pela primeira vez explicitamente na literatura grega; embora a antiga tabela egípcia para a redução de frações da forma 2/n, em que n é sempre um número ímpar - mencionada no papiro de Rhind (1700 A. C.) - pareça implicar que estes últimos eram conscientes dessa classificação dos inteiros. Restringir a atenção aos inteiros positivos - apesar de que as frações comuns foram usadas extensivamente pelos matemáticos pré-gregos - a ponto de limitar o conceito de número a eles parece ter sido uma postura principalmente filosófica, que acabou por retardar o progresso da matemática grega, principalmente no que diz respeito à álgebra. Sabemos o quanto o tratamento de temas algébricos foi simplificado pelo uso modernamente difundido dos números negativos e complexos; em contrapartida, a matemática grega foi prejudicada por séculos por não estender aos negativos o conceito de número.

Diofanto (por volta do século III) foi aparentemente o primeiro matemático grego que fez uso de racionais como números – e não como relação entre grandezas. Foi apenas no período em que ele viveu que frações racionais que não são equivalentes a números inteiros foram vistas na Grécia como números.

Por outro lado, merece menção o fato de que os primeiros resultados teóricos sobre número inteiros (positivos) – assunto conhecido como Teoria dos Números - encontram-se na matemática grega.

2. NÚMEROS PRIMOS

Pitágoras (570-500 A. C.) fundou na atual Itália uma escola, conhecida como Ordem Pitagórica, para transmitir suas ideias às classes privilegiadas, que eram iniciadas nos mais profundos segredos numéricos da Ordem. Os assim chamados pitagóricos devotaram considerável atenção aos números primos; muitos problemas de teoria dos números formulados por eles - aos quais proeminentes matemáticos dedicaram atenção desde aquela época - ainda não tiveram solução satisfatória.

Os Elementos de Euclides contêm uma prova de que existem infinitos números primos. O enunciado está formulado no livro IX, de uma forma estranha para nós modernos: “Os primos são mais (em número) do que qualquer quantidade determinada a priori de primos”. Esse fato

provavelmente tinha sido provado antes dos tempos de Euclides mas não se sabe quem o fez primeiro. Aceita-se que seja uma contribuição grega ao conhecimento, pois não existe evidência de que os matemáticos pré-gregos estivessem interessados em questões de exclusivo interesse teórico. Deve-se notar que esta contribuição dos gregos é uma das provas mais antigas da existência – que, ao contrário do que podem pensar nossos contemporâneos, não é de modo algum evidente – de um número infinito de elementos num conjunto dado.
Também figura no livro IX o enunciado e uma prova parcial do Teorema Fundamental da Aritmética, que afirma: todo número natural maior que 1 é produto de números primos. Outro resultado que figura neste mesmo livro é o conhecido algoritmo Euclidiano para calcular o máximo divisor comum de dois inteiros.

O livro do grego Nikomachos (100 d.C), Arithmetiké, é, depois dos Elementos, o mais antigo livro de Teoria dos Números que chegou até nossos dias. Este foi a base do primeiro livro sobre a Teoria dos Números escrito em latim: De Institutione Arithmetica, do romano Boethius (500 d.C). Neste livro é que aparece, pela primeira vez, a denominação numerus primus como tradução da tradicional Protós arithmói, preservada a partir de Euclides por Nikomachos.

O livro de Boethius foi, durante seiscentos anos, a única fonte de estudos da Teoria dos Números na idade Média. Por volta de 1200, iniciou-se o renascimento científico e matemático do Mundo Cristão, com o afluxo das obras árabes e a tradução das obras gregas. Nesta época, surge um dos mais influentes livros da História da Matemática: o Liber Abbaci, de Fibonacci, escrito em 1202. Este livro introduziu os algarismos arábicos na Europa Ocidental. Como Fibonacci tinha estudado entre os muçulmanos do Norte da África, preferiu adotar primus ao invés do incomposto preferido pelos árabes, consagrando desta forma em definitivo a denominação número primo em toda a Europa.

O método mais antigo para achar primos menores que um número dado é o chamado Crivo de Eratósthenes (276-194 A.C.). Esse método era provavelmente conhecido antes de Eratósthenes, mas atribui-se sua origem à matemática grega. Embora o método não envolva muita matemática, é o único relacionado ao assunto que nos foi transmitido desde a antiguidade.

Suponhamos que desejamos determinar todos os números primos (positivos) menores que 100. Escrevemos então a sequência dos números até 100. Em seguida riscamos todos os múltiplos de 2, a menos do próprio 2. Depois, riscamos todos os múltiplos de 3, a menos do

próprio 3. Passamos em seguida aos múltiplos de 5 (sempre mantendo o próprio 5), uma vez que os múltiplos de 4 já foram riscados. Os números que não são cancelados são obviamente os primos menores que 100. Abaixo, mostramos esse Crivo de Eratóstenes. Os números que estão sobre fundo branco são primos.

Números primos positivos menores que 100

1	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	

Para determinar quando um número n é primo, costumava-se dividi-lo por todo número primo menor que a raiz quadrada de n, e nenhum método melhor parece ter sido descoberto até o século XVII. Veremos mais adiante como a situação muda com o advento dos computadores.

3. OUTRAS INSPIRAÇÕES PARA A TEORIA DOS NÚMEROS

Alguns problemas de Geometria revelaram-se uma forte motivação para levantar questões em Teoria dos Números Inteiros. Uma delas é a construção de polígonos regulares.

Euclides construiu, em seus Elementos, polígonos regulares de 3, 4, 5 e 15 lados. É fácil construir um polígono regular tendo o dobro de lados de um outro polígono regular já construído. Assim, o método de Euclides mostrou como construir polígonos regulares que têm um número de lados igual a uma das expressões: 3.2^n, 4.2^n, 5.2^n, 15.2^n. Os menores números maiores que 2 que não são dados por essas expressões são 7, 9, 11, 13 e 24. Esforços para encontrar métodos de construir por meio de régua e compasso polígonos tendo um número de lados igual a um desses números excepcionais falharam, e os dois mil anos após Euclides não geraram aumento no número de polígonos regulares que podem ser construídos de uma dada maneira nem uma teoria exibindo a real natureza da dificuldade.

Foi Gauss (1777-1855) quem, com apenas 19 anos, forneceu uma resposta definitiva para a questão: quais são os polígonos regulares tendo um dado número primo ímpar de lados que podem ser inscritos num círculo por meio de régua e compasso? A resposta: são os primos ímpares da forma $2^{2n}+1$. Contudo, essa resposta, como é comum em matemática, levantou outras questões mais difíceis. Entre elas, citamos: a determinação de todos os valores de naturais n para os quais um número da forma $2^{2^n}+1$ é um número primo.

A julgar pelo passado, o desenvolvimento da matemática aponta para um crescimento contínuo desse tema, pois a solução de problemas que permaneceram longo tempo em aberto chama atenção para outros problemas mais difíceis.

Curiosamente, esses primos foram estudados cerca de 150 anos antes por um grande matemático amador, Pierre de Fermat (1601-1665), considerado o maior matemático francês do século XVII e um dos fundadores da moderna Teoria dos Números. Fermat conjeturou que um número da forma $F_n= 2^{2^n}+1$ é primo para todo inteiro não-negativo n. Por causa disso, esses números são chamados números de Fermat. Em 1640, Fermat anunciou que $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$ e $F_4=65537$ eram números primos e conjeturou que F_n era primo para todo natural n. A conjetura se revelou incorreta em 1732 quando Euler mostrou que F_5 é divisível por 641. Os únicos números de Fermat conhecidos que são primos são aqueles acima, anunciados pelo próprio Fermat.

Gauss tinha justificadamente tanto orgulho de sua descoberta, que o pedestal de sua estátua em Gottingen tem o formato de um polígono regular de 17 lados. É surpreendente que os números primos tenham tido um papel de destaque para resolver um problema de construção geométrica que desafiava os matemáticos desde a antiguidade.

Descrevemos outra questão geométrica que levou a importantes desdobramentos em Teoria dos Números. Os números 3, 4, 5 têm a curiosa propriedade de serem as medidas dos três lados de um triângulo retângulo (o que pode ser facilmente verificado pela recíproca do teorema de Pitágoras, já que $3^2+4^2= 5^2$). Ternas de números com essa propriedade são chamadas ternas pitagóricas, ou números pitagóricos. Na Babilônia antiga, pelo menos quatro dessas ternas eram conhecidas: 3, 4, 5; 8, 15, 17; 5, 12, 13; 20, 21, 29. Um número maior de tais ternas era já conhecido na matemática hindu, na qual se incluíam algumas ternas nas quais figuravam números irracionais. Também entre os egípcios algumas ternas pitagóricas eram conhecidas. Mas nenhuma prova do assim chamado Teorema Pitagórico foi encontrada na literatura desses povos.

Os gregos antigos eram fascinados pela questão de encontrar triângulos retângulos tendo medidas inteiras para seus lados. Desta forma, os pitagóricos acabaram descobrindo que os lados de um tal triângulo tinham uma certa relação algébrica, que foi reformulada por Platão. Em seus Elementos, Euclides deu uma fórmula mais geral que incluía todos os casos já citados acima[1].

4. COMPUTAÇÃO E TEORIA DOS NÚMEROS

4.1 Polinômios e os primos

Um problema estreitamente relacionado com o Crivo de Eratóstenes é a exibição de muitos números primos, não necessariamente todos os menores que um natural dado. Desde os tempos de Euclides, procuram-se fórmulas de gerar números primos. Durante muito tempo, as fórmulas pesquisadas eram diferentes tipos de polinômios. Neste campo de pesquisa, os computadores mostraram-se ferramentas potentíssimas. Por exemplo, o computador Maniac II

---

[1] Para enunciar o chamado Teorema Pitagórico e a resposta dada por Euclides, precisamos de uma definição: uma terna pitagórica (a, b, c) é dita primitiva se o único fator inteiro positivo comum aos termos a, b, c é 1. Assim, a terna (3, 4, 5) é primitiva, assim como todas as outras ternas conhecidas pelos antigos citadas acima.
Eis o enunciado do Teorema Pitagórico: Todas as ternas pitagóricas são dadas parametricamente por:

$$a=2uv,\ b=u^2-v^2,\ c=u^2+v^2,$$

em que u e v são naturais primos entre si, um é par e o outro é ímpar e u>v.
Por exemplo, para u=2 e v=1, obtemos a=2, b=3 e c=5. Para u=3 e v=2, obtemos a=12, b=5 e c=13.
O leitor pode verificar que fazendo u e v variar obtêm-se as demais ternas conhecidas na antiguidade.

mostrou que o polinômio n^2 +n+ 41, gera primos 47,5 % das vezes, para números naturais abaixo de 10 milhões - um número bastante respeitável tendo em vista a simplicidade da "fórmula". Para os polinômios do tipo $x^2 + x + q$, com q inteiro, o melhor resultado possível é obtido pelo polinômio em que q=41, que citamos acima. No caso dos polinômios cúbicos, o recordista é $2x^3 - 489x^2 + 39847x - 1084553$, que assume 267 valores primos para $0 \leq x \leq 500$ (gera primos 53,4 % das vezes).

Na verdade, pode-se demonstrar que não existe polinômio de coeficientes inteiros em uma variável apenas, e de grau arbitrário, que gere somente números primos. Este resultado aparece frequentemente nos textos universitários de Teoria dos Números. É importante registrar que o teorema citado é para polinômios de uma variável. Em 1971, o matemático Matiyasevic produziu um polinômio em várias variáveis com coeficientes inteiros, cujos valores percorrem todos os primos positivos e inteiros negativos. Este polinômio é de grau 37 e tem 24 variáveis. Mais tarde, outros polinômios foram obtidos, mas à medida que o grau diminuía, as variáveis aumentavam. O melhor resultado é constituído por um polinômio de grau 5 mas com 42 variáveis, obtido em 1976 por Jones, Sato, Wada e Wiens.

Atualmente os computadores, usando algoritmos sofisticados e processadores cada vez mais velozes, criam tabelas extensas de números primos. Todavia, antes do advento da computação, as tabelas eram construídas manualmente, sempre usando o crivo de Eratóstenes ou variantes dele, como foi o caso da tabela publicada em 1914 por Derick Norman Lehemer, que continha os números primos menores do que 10 milhões. Entretanto, o método de Eratóstenes exige um tempo que cresce exponencialmente com o tamanho do natural que é o limite superior da tabela. Com a necessidade de produzir muitos primos de grande magnitude – nascida da era da codificação de mensagens -, a pesquisa para encontrar algoritmos que gerem tais primos em tempo razoável tornou-se área de grande relevância em matemática computacional.

Em 2002, um cientista hindu da área de computação e dois estudantes seus (ainda não formados) surpreenderam a comunidade matemática ao exibir um algoritmo determinístico para decidir se um número é primo em tempo razoável. A prova, de surpreendente simplicidade, foi apresentada em 13 linhas e publicada em 2004 no Annals of Mathematics 160 (2). A seguinte citação de Gauss (Disquisitiones Arithmeticae, 1801) abre o artigo: "O problema de distinguir números primos de compostos e fatorar os últimos em primos é sabidamente um dos mais importantes e úteis em aritmética. Atraiu o empenho e a sabedoria

de geômetras antigos e modernos a um ponto tal que seria supérfluo discutir extensamente a questão (...) Além disso, a dignidade da ciência mesma parece requerer que todo método possível seja explorado para a solução de um problema tão elegante e celebrado." (tradução das autoras a partir da citação)

4.2 Um pouco da origem da criptografia

Outra grande renovação que ocorreu na Teoria dos Números foi quando se tornou necessário, com o uso difundido dos computadores, codificar as mensagens enviadas por linha telefônica, principalmente no contexto bancário e comercial. Surgiram, então, os diversos métodos de criptografia. Consideramos oportuno esclarecer um pouco as origens dos métodos de criptografia para posteriormente descrevermos um dos métodos atuais de chave pública utilizado na codificação e decodificação de mensagens enviadas por computador.

A palavra criptografia vem do grego *kriptós* (escondido, oculto) e de *gráphein* (escrita). Podemos definir criptografia como a arte ou ciência de escrever mensagens ocultas ou codificadas. Consiste no estudo dos princípios ou técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível de forma que possa ser conhecida apenas por seu destinatário. O uso da criptografia teve e tem aplicações diversas: assuntos ligados à guerra para que o inimigo não descubra as estratégias do emissor da mensagem; assuntos amorosos para que segredos não sejam descobertos; assuntos diplomáticos para que facções rivais não estraguem os planos de acordos; troca de e-mails nos dias atuais.

Na arte de decifrar códigos secretos, a criptografia está ligada a criptoanálise: a arte de descobrir o texto cifrado. Todo código vem acompanhado de duas receitas: uma para codificar uma mensagem e outra para decodificar a mensagem codificada. Decodificar é o que um usuário legítimo do código faz quando recebe uma mensagem codificada e deseja lê-la. Já decifrar significa ler uma mensagem codificada sem ser um usuário legítimo. Portanto, para decifrar é preciso "quebrar o código".

O primeiro uso documentado da criptografia foi no Egito, em torno de 1900 a.C., quando um escriba usou hieróglifos fora do padrão numa inscrição. Entre 660 a.C. e 500 a.C., os hebreus utilizavam a cifra de substituição simples, em que os caracteres são trocados um a um por outros. Com esse processo escreveram o Livro de Jeremias. Na Grécia Antiga, encontramos os primeiros estrategistas que já se preocupavam em encaminhar mensagens de

forma segura. Um exemplo de criptografia foi usado por Júlio César, imperador de Roma, que participou do primeiro triunvirato junto com Pompeu e Crasso em 60 a. C. e foi assassinado no senado em 44 a.C. A chave utilizada por Júlio César para enviar mensagens era muito simples: desloca-se o alfabeto 3 letras. Tal método foi denominado "Codificador de Júlio César" ou "Cifra de César", e consiste numa das técnicas mais clássicas de criptografia. Eis a troca de letras utilizada:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Houve época em que soldados tinham mensagens escritas em seu couro cabeludo como estratégia para transpassar uma informação pelas linhas inimigas, quando chegavam ao seu destino raspavam a cabeça revelando a mensagem.

Modernamente, em 1918, Arthur Scherbius desenvolveu uma máquina de criptografia chamada Enigma que foi amplamente utilizada pela marinha de guerra alemã em 1926 como a principal forma de comunicação. Em 1928, o exército alemão construiu uma versão elétrico-mecânica conhecida como "Enigma G", que tinha como garantidor de segurança a troca periódica mensal de suas chaves. A máquina funcionava inicialmente com três rotores e posteriormente com oito rotores. Ela se parecia com uma máquina de escrever, mas quando o usuário pressionava uma tecla, o rotor da esquerda avançava uma posição, provocando a rotação dos demais rotores à direita, sendo que esse movimento dos rotores gerava diferentes combinações de encriptação. A decodificação de mensagens elaboradas a partir das máquinas "Enigma" era muito difícil, pois era necessário ter outra máquina dessas e saber qual a chave utilizada para a codificação.

Alguns dizem que a criptografia moderna começou com Claud Shannon, possivelmente o pai da criptografia matemática. Em 1948, ele desenvolveu a teoria Matemática da Comunicação. Em 1949, Shannon publicou um artigo com Warren Weaver: *Communication Theory of Secrecy Systems.* Esse artigo, juntamente com outros trabalhos seus, deu origem à área de Teoria da Informação estabelecendo uma base teórica sólida para a criptografia e para a criptoanálise. A partir daí, quase todo trabalho realizado em criptografia se tornou secreto, realizado em organizações governamentais especializadas como, por exemplo, a *National Security Agency* (NSA) nos Estados Unidos. A NSA é a agência de segurança americana com funções relacionadas a inteligência de sinais incluindo

interceptação e criptoanálise, e também é um dos órgãos dedicados a proteger as comunicações.

O ano de 1976 testemunhou dois grandes marcos da criptografia para o público. Primeiramente, a publicação do *Data Encryption Standard (DES),* um algoritmo aberto de criptografia simétrica, o primeiro algoritmo de criptografia disponibilizado abertamente ao mercado. O segundo marco foi a publicação do artigo de Whitfield Diffie e Martin Hellman, *New directions in cryptography,* dando início à pesquisa de sistemas de criptografia de chave pública. Este algoritmo, que ficou conhecido como "Algoritmo de Diffie-Hellman para troca de chaves", levou ao imediato surgimento de pesquisas neste campo e uma delas culminou com a criação do algoritmo RSA.

4.3 O método de criptografia RSA

Um dos métodos de criptografia de chave pública bastante conhecido é o R.S.A. Ele foi inventado em 1978 por pesquisadores que trabalhavam no *Massachussets Institute of Technology* (M.I.T.). As letras R.S.A. correspondem às iniciais dos criadores do método: R. L. Rivest, A. Shamir e L. Adleman. Existem outros códigos de chave pública, mas o RSA é um dos mais utilizados em aplicações comerciais. Este método é utilizado, por exemplo, no Netscape, um dos mais populares softwares de navegação da Internet.

Para que o método RSA possa ser implementado precisamos de dois parâmetros básicos: dois números primos distintos de grande magnitude que chamaremos de **p** e ***q*.** Mas a primeira fase do processo de codificação de uma mensagem inicia-se com a pré-codificação. As letras são convertidas em números segundo uma tabela que pode se iniciar com o número 10 correspondendo à letra A e terminar no número 35 correspondendo a letra Z. Convenciona-se que o espaço entre as palavras será substituído pelo número 99. Após a conversão numérica, a mensagem pode ser quebrada em blocos obedecendo a certas regras. Passando-se à etapa de codificação, precisamos conhecer uma chave denominada pública ou de codificação que é formada por dois números: **n,** que é o produto dos primos **p** e **q** mencionados acima**,** e **e**. Esse número **e** deve ser um inteiro positivo inversível módulo $\Phi(\mathbf{n})$, ou seja, mdc (**e**, $\Phi(\mathbf{n})$)=1. Quando se conhecem p e q é fácil calcular $\Phi(\mathbf{n})$ uma vez que $\Phi(\mathbf{n})=(p-1)(q-1)$. O par (**n,e**) é denominado então, chave de codificação do sistema RSA. Cada bloco b será codificado obtendo-se a forma reduzida de $\mathbf{b}^{\mathbf{e}}$ módulo **n**, isto é, C(**b**) = resto da divisão de $\mathbf{b}^{\mathbf{e}}$ por **n**. Ou

seja, utilizamos conhecimentos da aritmética modular, isto é, de congruências: C(b)≡ $\mathbf{b^e}$ **(modn)**

Para o processo de decodificação, é necessária a chave de decodificação, conhecida apenas pela empresa ou pessoa que irá decodificar a mensagem. A chave de decodificação também é denominada como chave privada e é formada pelo par (n,d). O número **d** é o inverso de **e** módulo Φ(n). Se chamarmos de **a** um bloco da mensagem codificada, então D(**a**) será o resultado do processo de decodificação que é obtido da seguinte forma: D(**a**) = resto da divisão de $\mathbf{a^d}$ por **n.** Em termos de aritmética modular, D(**a**) é a forma reduzida de $\mathbf{a^d}$ módulo **n.** Para decodificar a mensagem deve-se encontrar a forma reduzida de todos os blocos codificados, utilizando-se a chave **(n,d)**, e separá-los de dois em dois algarismos. Finalmente, faz-se a correspondência desses blocos de dois algarismos com as letras da tabela, obtendo-se assim a mensagem enviada.

Calcular **d** é fácil, desde que Φ(**n**) e **e** sejam conhecidos, pois basta aplicar o algoritmo euclidiano estendido. No entanto, para calcularmos Φ(**n**) é necessário conhecermos os dois fatores primos de **n**: **p** e **q.** Torna-se difícil "descobrir" os números **p** e **q**, pois são números primos da ordem de 100 ou mais algarismos: Dessa forma, para o cálculo de **d** é fundamental a utilização do algoritmo euclidiano estendido, que emprega fortemente recursos de Teoria dos Números.

Com o advento dos computadores toda uma teoria de Ciência da Computação foi elaborada, englobando não só métodos de criptografia para segurança na rede, mas também assuntos de programação. Essa teoria permanece em constante construção, pois as inovações tecnológicas são constantes. Com esse exemplo do método de criptografia RSA constatamos que a matemática, em especial a Teoria dos Números, desempenha um papel fundamental na área de computação. Definições, conceitos, teoremas e proposições matemáticas que vêm da antiguidade adquirem uma vasta gama de aplicações em questões concretas do mundo da computação passando a ter um papel fundamental no avanço de tecnologias.

Referências

BUNT, L. N. H.; JONES, P. S.; BEDIENT, J. D. **The Historical Roots of Elementary Mathematics.** New York: Dover, 1988.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2000. (Série Computação e Matemática)

EVES, H. **Introdução à história da matemática**. Tradução de Higyno H. Domingues. Campinas, SP: Editora da UNICAMP, 2004.

GONÇALVES, A. **Introdução à álgebra**. 5.ed. Rio de Janeiro: IMPA, 2006.
MANINDRA, A.; NEERAJ, K.; NITIN, S. Primes is in P, **Annals of Mathematics**, Princeton, NJ, v.160, n.2, p.781-793, 2004.

MILIES, C. P. F.; COELHO, S. P. **Números**: uma introdução à matemática. 3.ed. São Paulo: Editora da Universidade de São Paulo, 2003.

SHOKRANIAN, S. **Criptografia para iniciantes.** 2.ed**.** Rio de Janeiro: Ciência Moderna, 2012.

SINGH, S. **O livro dos códigos**. Tradução de Jorge Calife. Rio de Janeiro: Record, 2001
————O último teorema de Fermat. 10.ed. Rio de Janeiro: Ed. Record, 2004.

STRUIK, D. J. **História concisa das matemáticas**. Lisboa: Gradiva, 1992.