Felipe Lopes Castro

Criptografia RSA: uma abordagem para professores do ensino básico

Porto Alegre

2014

Felipe Lopes Castro

Criptografia RSA: uma abordagem para professores do ensino básico

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Universidade Federal do Rio Grande do Sul – UFRGS

Instituto de Matemática

Orientador: Alveri Alves Sant'Ana

Porto Alegre

2014

CIP - Catalogação na Publicação

Castro, Felipe Lopes
Criptografia RSA: uma abordagem para professores do ensino básico / Felipe Lopes Castro. -- 2014.
59 f.

Orientador: Alveri Alves Sant'Ana.

Trabalho de conclusão de curso (Graduação) -- Universidade Federal do Rio Grande do Sul, Instituto de Matemática, Licenciatura em Matemática, Porto Alegre, BR-RS, 2014.

1. Criptografia RSA. 2. Teoria dos Números. 3. Números Primos. 4. Divisibilidade. 5. Ensino Básico. I. Sant'Ana, Alveri Alves, orient. II. Título.

Elaborada pelo Sistema de Geração Automática de Ficha Catalográfica da UFRGS com os dados fornecidos pelo(a) autor(a).

Felipe Lopes Castro

Criptografia RSA: uma abordagem para professores do ensino básico

Trabalho de Conclusão de Curso apresentado ao Departamento de Matemática Pura e Aplicada do Instituto de Matemática da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Licenciado em Matemática.

Trabalho aprovado. Porto Alegre, 01 de Dezembro de 2014.

Alveri Alves Sant'Ana
Orientador

Professora
Luisa Rodriguez Doering

Professor
Eduardo Henrique de Mattos Brietzke

Porto Alegre
2014

Este trabalho eu dedico ao meu filho Henri
e a minha esposa Erica.

Agradecimentos

Agradeço à minha família pelo apoio e compreensão durante a minha graduação, sem os quais o presente momento não seria possível.

Agradeço ao Alveri, orientador neste trabalho, pelos frutíferos momentos de discussão, pela disposição em me orientar não somente neste trabalho mas na vida acadêmica, como um todo.

Agradeço à banca pelos comentários e sugestões com relação ao presente trabalho.

Agradeço ao projeto abnTeX2[1] e aos seus colaboradores, ao qual me incluo, pelo desenvolvimento e aperfeiçoamento dessa excelente ferramenta para a elaboração dos trabalhos acadêmicos dentro das normas da ABNT.

[1] O **abnTeX2**, evolução do abnTeX, é uma suíte para LaTeX que atende os requisitos das normas da ABNT (Associação Brasileira de Normas Técnicas) para elaboração de documentos técnicos e científicos brasileiros, como artigos científicos, relatórios técnicos, trabalhos acadêmicos como teses, dissertações, projetos de pesquisa e outros documentos do gênero. Página do projeto: ⟨code.google.com/p/abntex2/⟩

"Procure ser uma pessoa de valor, em vez de procurar ser uma pessoa de sucesso. O sucesso é consequência" (Albert Einstein)

Resumo

O objetivo deste trabalho é estudar o funcionamento do sistema de criptografia RSA, discutindo toda a matemática necessária para a sua plena compreensão, onde são demonstrados o Teorema de Fermat, o Teorema Chinês dos Restos e o Teorema de Euler, bem como são abordados as questões de dificuldade de se fatorar números inteiros e de gerar números primos.

O texto é dirigido aos professores da escola básica e serve de estímulo aos mesmos para introduzirem a aritmética modular como atividade de ensino em suas classes.

Palavras-chaves: Criptografia RSA, Teoria dos Números, Números Primos, Divisibilidade e Ensino Básico.

Abstract

The aim of this work is to study how works the RSA encryption system, discussing all mathematical subjects which are needed for its full understanding, where we present a proof of the following results: Fermat's Little Theorem, Chinese Remainder Theorem and the Euler's Theorem. Moreover, we discuss the difficulties of factorization methods and generating prime numbers.

The text is intended for basics school teachers and one of the purposes is to stimulate them to introduce modular arithmetic as a teaching activities in their classes.

Key-words: RSA cryptography, Number Theory, Prime Numbers, Divisibility and Basic School.

Lista de tabelas

Sumário

Introdução

A criptografia estuda os métodos de codificar uma mensagem de tal forma que apenas o destinatário consiga decodificá-la, gerando assim uma segurança na troca de mensagens. A criptografia foi sendo utilizada ao longo da história, desde os tempos antigos. Os gregos já utilizavam formas de criptografia, como o quadrado de Políbio, desde 200 a.C. O imperador romano Júlio César, utilizava da chamada Cifra de César para se comunicar com os seus generais. E muitas outras criptografias foram criadas ao longo da história.

Com o advento da computação e da internet, houve necessidade de uma melhoria nos métodos de criptografia, pois as técnicas existentes dependiam de uma prévia correspondência entre o remetente e o destinatário, o que se tornaria um grande problema. Este foi solucionado por Diffie e Hellman (1976), através da criação do sistema de criptografia com chave pública[2] (ou criptografia assimétrica), a qual é composta por duas chaves, uma inversa da outra, de forma que seja computacionalmente inviável a determinação de uma chave a partir da outra. Deste modo, uma das chaves é disponibilizada publicamente (chave pública) e a outra guardada em segredo (chave privada), sem que haja riscos à segurança do código.

Através desse sistema de criptografia com chave pública, se todos os usuários da internet disponibilizarem sua chave pública, então para enviar uma mensagem de forma secreta basta que utilizemos a chave pública do destinatário, assegurando que apenas ele será capaz de entender a mensagem.

A partir da criação do conceito de sistema de criptografia com chave pública, buscou-se um método de criptografia assimétrica que fosse computacionalmente interessante. Rivest, Shamir e Adleman (1978)[3] desenvolveram um método de criptografia, chamada criptografia RSA, utilizando a teoria dos números inteiros desenvolvida por grandes matemáticos como Fermat, Euler, Gauss. Na criptografia RSA a chave pública e a privada são compostas por dois números naturais cada (e, n) e (d, n), respectivamente, onde n é o produto de dois primos, e d, e satisfazem determinadas relações. Um fato interessante é que, para obter a chave privada a partir da pública basta que fatoremos o número natural n, assim parece ser fácil "quebrar"essa criptografia, porém veremos durante o texto que escolhendo os dois fatores primos de n de maneira conveniente tornamos a fatoração de n praticamente impossível.

---

[2] Através desse sistema de criptografia, pode-se garantir o sigilo da mensagem, bem como a autenticidade da mesma.

[3] R. Rivest, A. Shamir e L. Adleman trabalhavam no Massachussets Institute of Technology (MIT) quando desenvolveram tal método de criptografia, que recebeu o nome de criptografia RSA em homenagem a eles.

No primeiro capítulo do presente trabalho fazemos um apanhado de como a criptografia se desenvolveu ao longo da história. Conhecemos algumas formas de criptografia, desde métodos simples, como o quadrado de Políbio e a cifra de César, até métodos complexos, como a cifra de Vigenère, a qual usa uma técnica polialfabética para codificar uma mensagem e foi considerada indecifrável por mais de 300 anos. Para finalizar, falamos sobre a codificação e assinatura digital através de um sistema de criptografia com chave pública.

No segundo capítulo estudamos a criptografia RSA de fato, inicialmente nos preocupando em responder a seguinte pergunta: Como e Porque ela Funciona? Para responder tal questionamento desenvolvemos alguns conceitos matemáticos, como relação de equivalência, congruência entre números inteiros e aritmética modular, e provamos alguns resultados necessário, como o Pequeno Teorema de Fermat (2.2.7), o Teorema Chinês dos Restos (2.2.10) e o Teorema de Euler (2.2.16).

Após discutir como e porque a criptografia RSA funciona, procuramos entender o quão segura é essa criptografia, ou seja, o quão difícil pode ser fatorar um número inteiro. Deste modo, estudamos dois algoritmos para encontrar a fatoração de um número composto, o algoritmo simples e o de Fermat, e também estudamos o crivo de Eratóstenes, o qual determina todos os números primos menores que um inteiro qualquer. Por fim, discutimos alguns métodos existentes para gerar números primos "bons"[4]. Assim estudamos algumas fórmulas famosas para gerar números primos, como os números de Mersenne e os de Fermat, e estudamos alguns testes de composição e primalidade.

No terceiro capítulo criamos uma proposta de atividade de aperfeiçoamento de professores do ensino básico. Essa proposta é dividida em três etapas: inicialmente estudamos a história da criptografia, discutindo como podemos relacionar alguns métodos estudamos com conceitos matemáticos na sala de aula; na segunda etapa, estudamos a criptografia RSA e a matemática envolvida para a sua plena compreensão, discutindo alguns conteúdos de sala de aula, como divisibilidade e fatoração, e relacionando com a criptografia; e, por fim, estudamos alguns métodos para gerar primos, bem como alguns testes de composição e primalidade, e como podemos relacionar tais conhecimentos com a sala de aula, por exemplo utilizando o crivo de Eratóstenes.

Este trabalho está baseado no livro de Coutinho, e o mesmo é uma ótima referência para o aprofundamento das questões aqui discutidas. O livro de Coutinho também oferece uma referência bibliográfica mais completa para o caso de um maior interesse em criptografia.

[4] Para termos grande segurança na criptografia RSA devemos escolher dois números primos grandes o suficiente (com mais de 100 algarismos cada um) e razoavelmente "longe" um do outro (um dos primos tem que ter vários algarismos a mais que o outro).

1 História da Criptografia

Em grego *kryptós* significa escondido e *gráphein* significa escrita, assim criptografia é o estudo dos métodos para codificar uma mensagem de tal modo que apenas o destinatário seja capaz de decodificá-la. Assim, criptografar é o processo de codificar uma mensagem, enquanto que descriptografar é o processo em que o destinatário da mensagem decodifica a mesma afim de lê-la. Aqui precisamos ter cuidado com a palavra decifrar que, conforme Coutinho (1997, p. 2), refere-se a conseguir entender a mensagem original sem ser o destinatário da mesma, ou seja, decifrar significa "quebrar"a codificação. Neste contexto de decifrar uma mensagem surge a criptoanálise, que conforme a Wikipédia (2014a) "é a arte de tentar descobrir o texto cifrado e/ou a lógica utilizada em sua encriptação (chave)".

A criptografia é utilizada há muito tempo na comunicação, sendo que uma das primeiras formas utilizadas para criptografar uma mensagem foi desenvolvida pelo grego Políbio, 200 a.C. a 118 a.C., que consiste num dos primeiros métodos de transformar o alfabeto em números, seguindo uma tabela 5 x 5, chamada de quadrado de Políbio. Usando o alfabeto atual, com 26 letras, construímos o quadrado de Políbio como segue:

Tabela 1 – Quadrado de Políbio

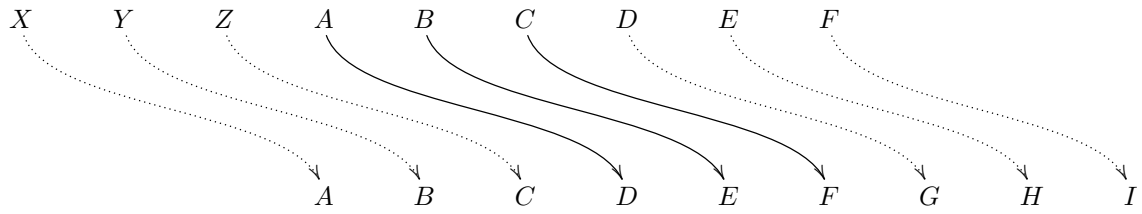
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I/J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Assim associamos a cada letra do alfabeto a sua posição na matriz, por exemplo a letra P é associada ao número 35. Note que, como esta é uma tabela 5 x 5, precisamos associar duas letras a mesma posição na tabela, no caso associamos I e J a mesma posição. Através dessa criptografia a mensagem "Hoje vai ter peixe no RU"seria criptografada como 233424155111244415423515245315333442 45 e quando descriptografada gera a mensagem "hoievaiterpeixenoru".

Outro método antigo de criptografia criado foi o da translação de letras do alfabeto, consistindo na substituição de uma letra do alfabeto por outra que se encontra um número fixo de posições adiante, como por exemplo, a "cifra de César", que foi uma criptografia usada pelo imperador Júlio César, 100 a.C. a 44 a.C., para mandar mensagens ao seu exército; esta criptografia consiste na translação das letras do alfabeto três posições, conforme a Tabela 2 a seguir.

Seguindo esse método a mensagem "UAU terá peixe no RU" seria criptografada por

Tabela 2 – Cifra de César



"XDX whud shlah qr UX"e seria descriptografada como "UAU tera peixe no RU". Apesar desse método ser fácil de decifrar, ele se mostrou muito eficiente para o seu propósito, sendo muito utilizado por César na comunicação com os seus generais.

Uma forma de "melhorar"essa criptografia é trocar as letras por números de modo não sequencial, parecido com o método utilizado por Políbio, por exemplo seguindo a Tabela 3 a seguir.

Tabela 3 – Substituição de letras por números

A	B	C	D	E	F	G	H	I	J	K	L	M
11	23	25	68	19	36	46	89	77	33	17	63	35

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
55	43	37	21	16	83	91	72	84	77	96	12	26

Deste modo a mensagem "Acabou o peixe, agora tem tatu"seria criptografada como 1125112343729943993719779619669911464316119991193599911191 72, onde os espaços foram substituídos por 99 e a vírgula por 66. E descriptografada como "acabou o peixe, agora tem tatu".

Apesar desses métodos de criptografia aparentarem serem razoáveis, eles são relativamente simples de quebrar, principalmente se usarmos recursos computacionais. O grande problema dessa forma de criptografia é que a uma determinada letra se associa sempre o mesmo número, e em cada idioma existem algumas letras cuja frequência com a qual são usadas é maior[1]. Desse modo, identificando os padrões que aparecem com maior frequência podemos descobrir algumas letras, o que muitas vezes é o suficiente para entender a mensagem. Quanto maior a mensagem mais fácil de identificar as letras que se repetem e, portanto, mais fácil fica a tarefa decifrar a mensagem. Essa técnica de criptoanálise, onde se observa a frequência da repetição de algumas pequenas partes da mensagem, é chamada análise de frequência, e foi criada pelo filósofo árabe Al-Kindi no século IX, durante um estudo extensivo do Corão.

O surgimento da análise de frequência obrigou os métodos de criptografia a evoluírem, e não usarem mais substituições simples de letras. Assim surgiram algumas técnicas de criptografia, entre elas podemos citar: 1 - associação de letras que aparecem

[1] No Português, conforme Quaresma e Pinho (2007), as 10 letras usadas com maior frequência são, nessa ordem, A, E, O, S, R, I, D, N, M e U.

com maior frequência a mais de um simbolo, por exemplo a letra E poderia ser associada aos símbolos 19, 67 e 59; 2 - substituição polialfabética, onde se usam vários alfabetos para a codificação; 3 - substituição poligráfica, onde pares ou trincas de letras são cifradas como um símbolo diferente; e 4 - substituição mecânica, técnica utilizada pelo exército de Adolf Hitler durante a 2ª guerra mundial, que consiste na utilização de equipamento elétrico/mecânico para criptografar.

Durante a renascença, o monge alemão Johannes Trithemius desenvolveu uma das primeiras cifras polialfabéticas. Ele criou a chamada tábua de Trithemius, utilizando 26 vezes o alfabeto e criando a seguinte da tabela 26 x 26:

Tabela 4 – Tábua de Trithemius

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

Onde para criptografar uma mensagem inicia-se transformando a primeira letra da mensagem através da primeira linha da tabela, em seguida traduz-se a segunda letra da mensagem utilizando a segunda linha da tabela, a terceira letra é criptografada utilizando a terceira linha da tabela, e assim sucessivamente. Quando for usada a última linha da tabela para criptografar, reinicia-se o processo da primeira linha.

Nessa criptografia, a cada letra pode ser associada qualquer outra letra do alfabeto, dependendo da sua "posição"na mensagem. Uma grande vantagem é que essa forma de criptografia é imune a análise de frequência, portanto gera uma grande dificuldade de ser decifrada. Porém um grande problema na criptografia de Trithemius é que a primeira letra

permanece a mesma, portanto quando se sabe que esta é a criptografia usada fica fácil decifrar uma mensagem.

O francês Blaise de Vigenère aprimorou a criptografia de Trithemius, utilizando uma palavra-chave para executar a criptografia. Assim a mensagem é criptografada utilizando-se as linhas correspondentes as letras da palavra-chave, de forma repetida. Por exemplo, utilizando a palavra chave "ufrgs" a mensagem "matematica pura" seria criptografada da seguinte maneira: a letra M será cifrada com a linha que inicia com U, a letra A será cifrada com a linha que inicia com F, a letra T será criptografada utilizando a linha que inicia com a letra R, e assim sucessivamente, gerando a seguinte mensagem criptografada: "gfkkeuyzisjzig", conforme a Tabela 5.

Tabela 5 – Criptografia de Vigenère com palavra-chave

Chave	u	f	r	g	s	u	f	r	g	s	u	f	r	g
Msg Original	m	a	t	e	m	a	t	i	c	a	p	u	r	a
Msg Codificada	g	f	k	k	e	u	y	z	i	s	j	z	i	g

Em 1586 Vigenère publicou um livro intitulado "Traicté des Chiffres", onde ele descreve a chamada Criptografia de Vigenère que utiliza uma chave-automática. Este método funciona da seguinte forma: há uma letra inicial previamente combinada com o destinatário, essa letra inicial é a chave inicial que determina a linha que será usada para criptografar a primeira letra da mensagem. Após codificar a primeira letra, a letra resultante se torna a chave para criptografar a letra seguinte. Continuando este processo, sempre uma letra criptografada se torna automaticamente a chave da letra seguinte.

Utilizando a criptografia de chave automática de Vigenère, com chave inicial "K", a mensagem "A matemática é surpreendente" seria codificada da seguinte maneira:

Tabela 6 – Criptografia de Vigenère com chave automática

Chave	k	k	w	w	p	t	f	f	y	g	i	i	m	e	y	p	e	u	z	d	q	t	x	k	d
Mensagem Original	a	m	a	t	e	m	a	t	i	c	a	e	s	u	r	p	r	e	e	n	d	e	n	t	e
Mensagem Criptografada	k	w	w	p	t	f	f	y	g	i	i	m	e	y	p	e	u	z	d	q	t	x	k	d	h

Gerando a mensagem "kwwptffygiimeypeuzdqtxkdh", que quando decodificada geraria a mensagem "amatematicaesurpreendente".

A criptografia de Vigenère permaneceu imune aos métodos para decifrar mensagens conhecidos na época, chegando a ser chamada "le chiffre indéchiffrable"[2]. Apenas em meados do século XIX foram encontrados métodos para decifrá-la.

Após a cifra de Vigenère, algumas outras técnicas de criptografia foram desenvolvidas, porém ainda havia a necessidade do compartilhamento prévio da senha. Um grande problema da criptografia até o século XIX consistia em encontrar um modo seguro de

[2] Em tradução literal, seria: "a cifra indecifrável".

enviar a chave de criptografia ao destinatário, afim do mesmo ser capaz de descriptografar uma mensagem. Além disso, outros problemas existiam, por exemplo: quando se faz necessária a comunicação com mais de um destinatário, deve ser criada uma chave para cada destinatário, caso contrário todos poderiam ler as mensagens dos outros. Assim deveriam existir muitas chaves para haver uma comunicação segura. Por muito tempo a criptografia ficou sem resposta para esse problema.

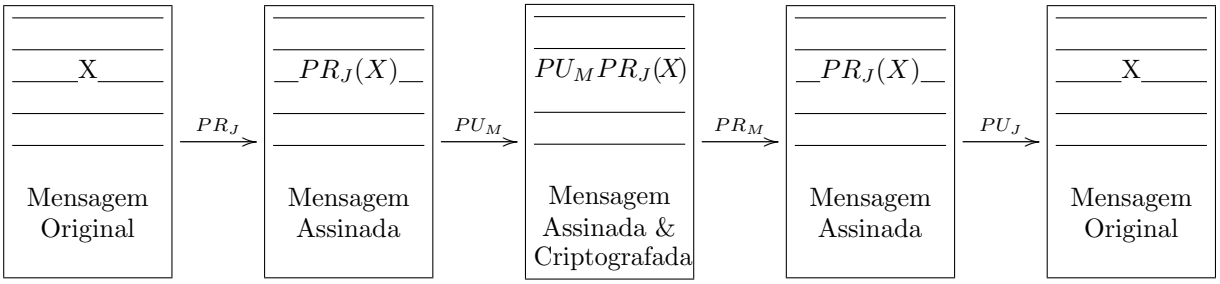
Diffie e Hellman (1976) solucionaram esse problema através da criação de duas chaves distintas, sendo uma delas disponibilizada publicamente (chave pública) e a outra mantida em posse do proprietário (chave privada), de forma que após codificada com a chave pública apenas com a chave privada se poderia decodificar[3]. Para o envio de uma mensagem deve-se proceder da seguinte maneira: primeiro precisamos da chave pública do destinatário, através dela codificamos a mensagem e enviamos ao destinatário. Assim o destinatário, usando a sua chave privada, é o único capaz de ler a mensagem. Essa forma de criptografia chama-se de criptografia assimétrica, ou criptografia de chave pública.

Porém há uma questão a se considerar com relação a criptografia assimétrica: visto que a chave pública fica à disposição de todos, então como podemos assegurar quem é o verdadeiro remetente da mensagem? A resposta a essa questão surge de maneira bem simples e interessante. Para nos certificarmos da identidade do remetente fazemos uso da assinatura digital, da seguinte maneira: o remetente da mensagem, utilizando a sua chave privada, criptografa a mensagem e a envia ao destinatário. Este usa a chave pública do remetente a fim de verificar a autenticidade da mesma. Porém, se o remetente apenas criptografar utilizando a sua chave privada, então todos poderão descriptografar a mensagem. Deste modo, o remetente primeiramente assina digitalmente a mensagem — criptografando a mesma através de sua chave privada —, em seguida o remetente criptografa a mensagem assinada, utilizando a chave pública do destinatário. Deste modo, apenas o destinatário será capaz de descriptografar a mensagem final e, através da chave pública do remetente, ter a certeza da autenticidade da mesma.

Vejamos através do seguinte exemplo: João e Maria querem trocar mensagens, para isto João possui a sua chave privada (PR_J) e a sua chave pública (PU_J) e Maria também possui sua chave privada (PR_M) e pública (PU_M). João deseja enviar uma mensagem "X"para Maria, para isto ele assina a mensagem gerando $PR_J(X)$. Em seguida ele utiliza a chave pública de Maria, gerando a mensagem criptografada final $PU_M PR_J(X)$. Maria ao receber a mensagem utiliza da sua chave privada, $PR_M(X)$, reobtendo a mensagem assinada por João. Finalmente, Maria utiliza a chave pública de João para obter a mensagem original a partir da mensagem assinada. Para ilustrar melhor o procedimento, vejamos a Tabela 7 a seguir

[3] Da mesma maneira, após cifrada uma mensagem utilizando a chave privada, apenas com a chave pública pode-se decifrar. Esta forma de cifrar uma mensagem utilizando a chave privada é utilizada para garantir a autenticidade da mensagem.

Tabela 7 – Criptografia Assimétrica e Assinatura Digital



Outra observação importante é a seguinte, como uma das chaves é de conhecimento público, então não deve ser possível obter a chave privada a partir da pública. Esse fato é de essencial importância para garantir o sigilo da informação. Como o nosso objetivo é estudar a criptografia RSA — que é uma criptografia com chaves assimétricas —, analisaremos o motivo de não conseguirmos a chave privada à partir da pública.

As duas formas de criptografia, simétrica e assimétrica, têm pontos positivos e negativos. A criptografia simétrica é fácil de ser utilizada, não requer muito processamento para codificação/decodificação, enquanto que a criptografia assimétrica é muito lenta, requer maior processamento para codificação/decodificação. A criptografia simétrica tem problemas de distribuição de chave, precisa de uma comunicação prévia para a troca da chave e uma chave diferente para cada destinatário distinto; enquanto que a assimétrica utiliza duas chaves, sendo que apenas uma é de conhecimento público.

Portanto podemos combinar as duas formas para gerarmos uma criptografia mista que tire proveito do melhor de cada uma destas duas formas de criptografia. Em geral, utiliza-se uma chave simétrica para criptografar a mensagem e uma chave assimétrica para criptografar a chave simétrica. Através desse método misto, temos a eficiência da criptografia simétrica, com a segurança da criptografia assimétrica.

2 Criptografia RSA

2.1 Como e Porque Funciona?

A criptografia RSA utiliza a teoria dos números para a codificação e decodificação de mensagens. Esta é uma criptografia que se utiliza de chaves assimétricas, ou seja, existem duas chaves distintas, uma pública e outra privada. A chave pública fica à disposição de qualquer pessoa e é utilizada para codificar uma mensagem e mandá-la para o proprietário da chave privada, que será a única pessoa capaz de decodificar a mensagem.

Basicamente, para realizarmos a criptografia de uma mensagem precisamos de dois números primos p e q, do produto deles $n = pq$, do valor da *função totiente*[1] de n, que no nosso caso é $\phi(n) = (p-1)(q-1)$ e de um número inteiro $e < \phi(n)$ de tal forma que o máximo divisor comum entre e e $\phi(n)$ seja 1, isto é, existe um número $d < \phi(n)$ de tal forma que $1 = k\phi(n) + de$. Com essas informações temos a chave de codificação (e, n) e a chave de decodificação (d, n).

Para efetuarmos a criptografia precisamos inicialmente fazer uma pré-codificação, que consiste na transformação do alfabeto utilizado na mensagem em números. Após feita essa transformação, separamos os números pré-codificados em blocos cujo valor numérico seja menor que n[2]. Finalizada a pré-codificação podemos executar a codificação da mensagem, da seguinte forma: dado um bloco b calculamos $C(b)$, que é o resto da divisão de b^e por n. Note que $C(b)$ é um número entre 0 e n, ou seja, um bloco. Assim, para descriptografarmos um bloco c calculamos $D(c)$, que é o resto da divisão de c^d por n. Deste modo, podemos codificar e decodificar qualquer mensagem formada por blocos de números positivos menores que n.

O seguinte exemplo aparece em Coutinho (1997, p. 179–181), se escolhermos $p = 11$ e $q = 13$. Temos que $n = 143$ e $\phi(n) = 120$, segue que podemos escolher $e = 7$ e $d = 103$. Portanto, temos a chave de codificação (chave pública) (7, 143) e a chave de decodificação (chave privada) (103, 143). Para procedermos a pré-codificação, utilizaremos a Tabela 8, codificando os espaços como 99.

Assim a mensagem " Paraty é linda" seria pré-codificada como

$$25 - 102 - 7 - 102 - 93 - 49 - 91 - 49 - 92 - 118 - 23 - 13 - 10$$

e criptografada como

$$64 - 119 - 6 - 119 - 102 - 36 - 130 - 36 - 27 - 79 - 23 - 117 - 10.$$

[1] Função totiente, também chamada função de Euler, será estuda com mais detalhes na página 37.

[2] Para que a mensagem seja descriptografada de maneira correta, devemos ter dois cuidados: nenhum bloco pode iniciar com o algarismo 0; e após separada em blocos, a mensagem não pode ser reagrupada.

Tabela 8 – Pré-codificação

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Primeiramente vamos entender porque ela é segura. A criptografia RSA, como já vimos, é criada a partir de dois números primos p e q, sendo que para decifrá-la basta que determinemos tais primos. Como a chave pública contém o resultado do produto destes primos, logo para descobrir p e q basta conseguirmos fatorar esse número. Assim, tecnicamente, seria muito fácil quebrar a criptografia RSA. Mas essa criptografia se mostra eficiente em função das limitações computacionais existentes. Conforme Coutinho (1997, p. 4)

> *[. . .] decifrar o RSA é* teoricamente *muito simples: o obstáculo é de natureza tecnológica. Usando como chaves de codificação do RSA números muito grande (de 150 algarismos ou mais), fatorar n para achar p e q, com os métodos atuais levaria alguns milhares de anos. É disto que depende a segurança do RSA; da ineficiência dos métodos de fatoração atualmente conhecidos.*

Precisamos mostrar que a criptografia RSA funciona, ou seja, precisamos mostrar que quando descriptografarmos um texto criptografado este retorna a mensagem original, para verificarmos isso precisaremos estudar aritmética modular, mais especificamente precisamos do Teorema de Euler (2.2.16) que é uma generalização do Pequeno Teorema de Fermat (2.2.7). Além disso, conforme vimos, para podermos usar a criptografia RSA precisamos escolher primos grandes (com mais de 100 algarismos), portanto estudaremos métodos para determinar se um número é primo ou composto, também estudaremos métodos para fatorar um número inteiro, e também métodos para gerarmos números primos.

2.2 Aritmética Modular e o Teorema de Euler

Um dos aspectos mais importantes para a garantia da segurança da criptografia RSA é a inabilidade de fatorarmos um dado número inteiro muito grande. Para entendermos melhor essa dificuldade, vamos primeiro discutir a existência da fatoração de números inteiros como produto de primos.

Um dos primeiros fatos que devemos observar é que dados dois números inteiros sempre podemos efetuar a divisão euclidiana obtendo um quociente e um resto, conforme o Teorema a seguir:

Teorema 2.2.1 (Teorema de Divisão Euclidiana)**.** *Dados dois inteiros positivos a e b, existem únicos inteiros q e r satisfazendo*

$$a = b\,q + r,\ com\ 0 \leq r < b. \tag{2.1}$$

Do Teorema de Divisão Euclidiana obtemos a definição de divisor. Dizemos que b divide a (ou que b é divisor de a) se o resto da divisão de a por b for 0, e portanto existe um inteiro q tal que $a = b\,q$. Uma propriedade interessante relacionando dois números é a existência de divisores em comum entre eles. Dados dois números inteiros positivos a e b, definimos o *máximo divisor comum* entre a e b, $mdc(a, b)$, como o maior inteiro positivo que divide a e b simultaneamente[3]. Uma outra forma de definir o mdc é a seguinte: dizemos que d é o máximo divisor comum de a e b, se:

(1) d divide a;

(2) d divide b;

(3) se d' é outro inteiro que divide a e b, então d' divide d.

Dizemos que a e b são *relativamente primos* quando tivermos $mdc(a, b) = 1$.

Uma propriedade interessante do mdc entre dois números é a seguinte. Se $d = mdc(a, b)$, então existem inteiros α, β tais que

$$a\,\alpha + b\,\beta = d. \tag{2.2}$$

É simples ver que os inteiros α e β não são unicamente determinados. Por exemplo, $1 = mdc(2, 3)$ e $2 \times (-1) + 3 \times 1 = 1 = 2 \times 2 + 3 \times (-1)$. Uma observação pertinente aqui é que, se c é um inteiro positivo tal que existem α' e β' para os quais $c = a\,\alpha' + b\,\beta'$, então d divide c. Assim temos que o $mdc(a, b)$ é o menor inteiro positivo para o qual existam α e β satisfazendo a Equação 2.2. Portanto, quando podemos escrever 1 da forma $1 = a\alpha + b\beta$, podemos concluir que $mdc(a, b) = 1$.

Agora que já definimos a divisão entre inteiros e que já sabemos algumas propriedades do máximo divisor comum entre dois inteiros, estamos em busca da existência de uma fatoração como produto de primos. Primeiramente recordemos que um número inteiro $p \neq \pm 1$ é dito *primo* se os únicos divisores positivos de p são ele mesmo e 1. Como exemplo de primos temos 2, 3, -5, 7, etc. Os números inteiros distintos de $0, +1$ e -1 não primos são chamados de *compostos*. Note que, dado um primo p, todo inteiro ou é relativamente primo com p ou é múltiplo dele. Das definições de máximo divisor comum e de número primo, temos o seguinte teorema.

[3] Como 1 divide qualquer inteiro, segue que o $mdc(a, b)$ sempre existe.

Teorema 2.2.2 (Propriedade Fundamental dos Números Primos)**.** *Sejam a e b números inteiros e p um número primo. Se p divide ab então p divide a ou p divide b.*

Demonstração. Queremos mostrar que p divide a ou b. Então suponhamos que p não divide a nem b. Então pelo observado anteriormente, p é relativamente primo com a e b. Logo exitem inteiros a', b', p', p'' tais que

$$a\,a' + p\,p' = 1 \qquad \text{e} \qquad b\,b' + p\,p'' = 1.$$

Multiplicando essas duas igualdades obtemos que

$$\begin{aligned} 1 &= (a\,a' + p\,p')(b\,b' + p\,p'') \\ &= a\,b\,a'\,b' + p\,p''\,a\,a' + p\,p'\,b\,b' + p^2 p'\,p'' \\ &= a\,b\,a'\,b' + p(p''\,a\,a' + p'\,b\,b' + p\,p'\,p''). \end{aligned}$$

Portanto, $mdc(p, ab) = 1$, mas isso contradiz o fato de p dividir ab. Portanto a suposição de que p não divida a nem b é falsa, assim p divide a ou b. □

Essa propriedade é dita propriedade fundamental dos números primos pois ela caracteriza todos os números primos, ou seja, se um número inteiro p satisfaz essa propriedade, então esse número é primo. De fato, suponhamos que p satisfaça tal propriedade e seja $a \neq p$ um divisor positivo de p, ou seja, existe b inteiro tal que $p = a\,b$. Logo p divide $a\,b$ e, pela propriedade, p divide a ou p divide b. Deste modo p divide b, isto é, existe a' tal que $b = a'p$. Portanto, $p = ab = a\,a'p$ e, consequentemente, $a'a = 1$. Assim os únicos divisores positivos de p são 1 e ele mesmo, portanto p é primo.

Relembrados esses conceitos básicos, temos que todo inteiro se escreve como produto de primos. Agrupando os fatores primos iguais e ordenando, temos o seguinte resultado.

Teorema 2.2.3 (Teorema da Fatoração Única)**.** *Dado um número inteiro $n \geq 2$, podemos escrever n da seguinte maneira*

$$n = p_1^{n_1} \cdots p_k^{n_k}, \tag{2.3}$$

com $1 < p_1 < \cdots < p_k$ números primos e $n_1, \ldots, n_k$ inteiros positivos. Mais ainda, essa escrita é única.

Demonstração. A forma mais simples que podemos usar para determinar a decomposição de n como produto de primos é a seguinte: dividimos n por todos os números entre 2 e $n-1$, se em todas as divisões obtivermos restos não nulos, então n é primo e já está fatorado. Caso contrário, consideremos p_1 o menor inteiro entre 2 e $n-1$ que divide n. É fácil ver que esse menor número tem que ser primo e, como p_1 divide n, existe q_1' tal que $n = p_1 q_1'$. Como todo divisor de q_1' é divisor de n e p_1 é o menor divisor de n, então se q_1' tiver algum divisor este será maior ou igual a p_1. Deste modo, existe $n_1 > 0$ tal que $n = p_1^{n_1} q_1$, onde $mdc(q_1, p_1) = 1$.

Como $n = p_1^{n_1} q_1$, então pela Propriedade Fundamental dos Primos (2.2.2) todo primo distinto de p_1 que dividir n tem que dividir q_1. Portanto para achar os demais divisores de n, devemos procurar os divisores de q_1. Assim efetuamos as divisões de q_1 pelos números entre p_1 e $q_1 - 1$. Se q_1 não for primo então, analogamente ao feito anteriormente, existe um primo p_2 que divide q_1 e um inteiro $n_2 > 0$, tais que $q_1 = p_2^{n_2} q_2$ para algum $q_2 < q_1$ e, portanto, $n = p_1^{n_1} p_2^{n_2} q_2$. Repetindo esse processo obtemos uma sequência decrescente de números inteiros positivos $n > q_1 > q_2 > \cdots$, logo, pelo princípio da boa ordenação, essa sequência é finita, ou seja, existe k tal que $q_k = 1$. E portanto $n = p_1^{n_1} p_2^{n_2} p_k^{n_k}$. A unicidade da fatoração segue direto da Propriedade Fundamental dos Primos. □

Uma observação pertinente com relação a este procedimento é que, para concluir a primalidade de n basta dividirmos n pelos números entre 2 e $[\sqrt{n}]$, onde $[\sqrt{n}]$ é a parte inteira de $\sqrt{n}$. Pois se encontrarmos um menor p que divide n, então $p^2 \leq n$. Esse procedimento de fatoração de um número inteiro irá gerar um primeiro algoritmo simples de fatoração. Essa existência e unicidade da escrita de um número inteiro como produto de primos será importante para garantir a segurança da criptografia RSA.

Revisadas as propriedades básicas dos números inteiros, podemos introduzir a chamada aritmética modular. Esta estuda propriedades cíclicas que ocorrem nos números inteiros, essas propriedades cíclicas nos fornecem informações muito importantes sobre os números inteiros. A aritmética modular é uma ferramenta fascinante da matemática, como exemplos podemos citar o Pequeno Teorema de Fermat que veremos nesta seção. Apesar de não percebermos, as propriedades cíclicas estão presentes no nosso dia-a-dia.

> *Você já ouviu a frase: esses matemáticos são uns loucos, para eles 2 mais 2 nem sempre é quatro? Quem fala isso deveria pensar um pouco. Mesmo no dia a dia nem sempre as contas dão como resultado aquilo que reza a aritmética. Por exemplo, quando que 13 + 18 dá 7? Quando estamos falando de horas, claro. Se é 1 da tarde, então daqui a 18 horas serão 7 da manhã. Isso não é privilégio das horas; qualquer fenômeno cíclico vai produzir uma aritmética peculiar, semelhante a esta.*
> *(COUTINHO, 1997, p. 69)*

Aqui estamos interessados na aritmética modular das congruências entre os números inteiros, assim precisamos definir relação de equivalência entre números inteiros. Uma relação entre números inteiros é uma regra a qual se compara dois números inteiros, assim dizemos que m se relaciona com n — $m \sim n$ — se m é comparável com n segundo essa relação. Por exemplo, considere a seguinte relação em $\mathbb{Z}$: dados dois inteiros m, n dizemos que m se relaciona com n se $m - n$ é múltiplo de 2. Assim temos que $1024 \sim_2 6$ e $37 \sim_2 -3$, mas $-7 \not\sim_2 12$.

Definição 2.2.4. Uma relação $\sim$ em $\mathbb{Z}$ é dita uma *relação de equivalência*[4], se para todos

[4] A noção de relação de equivalência pode ser definida num contexto mais geral.

elementos $m, n, o \in \mathbb{Z}$ tivermos as seguintes propriedades:

Reflexividade $m \sim m$;

Simetria Se $m \sim n$, então $n \sim m$;

Transitividade Se $m \sim n$ e $n \sim o$, então $m \sim o$.

Retornando ao exemplo anterior, temos que a relação, $m \sim_2 n$ se $m - n$ é par, é uma relação de equivalência. De fato, claramente esta relação é reflexiva e simétrica, bastando verificarmos a transitividade. Assim, se $m \sim_2 n$ e $n \sim_2 o$, então $m - n = 2k$ e $n - o = 2k'$. Somando as duas equações temos que

$$2(k + k') = 2k + 2k' = (m - n) + (n - o) = m - n + n - o = m - o,$$

portanto $m \sim_2 o$. Essa relação de equivalência descrita é chamada relação de congruência módulo 2, e é o tipo de relação que estamos interessados em explorar.

As relações de equivalência servem para agrupar números inteiros que possuem uma propriedade em comum. Assim consideremos a classe de equivalência do elemento m dada por

$$\overline{m} = \{n \in \mathbb{Z} \mid m \sim n\}$$

e consideremos o conjunto formado por essas classes de equivalência $\mathbb{Z}_\sim = \{\overline{m} \mid m \in \mathbb{Z}\}$. Algumas observações pertinentes devem ser feitas para que possamos compreender melhor as classes de equivalência. Primeiramente, qualquer elemento da classe pode ser um representante da classe, ou seja, se m é um inteiro tal que $m \in \overline{n}$, então $\overline{m} = \overline{n}$. Também temos que duas classes distintas não possuem elemento em comum.

Agora vamos nos fixar às relações de congruência entre os inteiros. Conforme vimos, a relação de congruência módulo 2 — $m \sim_2 n$ se e só se $m - n$ é múltiplo de 2 — é uma relação de equivalência em $\mathbb{Z}$, denotaremos o conjunto das classes de equivalência módulo 2 por $\mathbb{Z}_2$. É fácil ver que, dado m um inteiro, $m \sim_2 r$, onde r é o resto da divisão de m por 2. Como na divisão por 2 só podemos obter resto 0 ou 1, podemos concluir que $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$.

Essa relação de congruência pode ser estendida para outro inteiro n qualquer. Assim temos a seguinte generalização : fixado n inteiro positivo, considero a relação $a \sim_n b$ se $a - b$ é múltiplo de n. Essa relação é chamada de congruência módulo n, portanto diremos que a é congruente a b módulo n, se $a - b$ é múltiplo de n, e denotaremos por

$$a \equiv b \pmod{n}.$$

É fácil ver, pelo mesmo argumento do resto na divisão, que

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\},$$

onde $\overline{a} = \{b \in \mathbb{Z} \mid b - a = k\,n\} = \{a + k\,n \mid k \in \mathbb{Z}\}$. Uma forma interessante de enxergar essas classes de equivalência módulo n, é a seguinte

> *Como devemos imaginar $\mathbb{Z}_n$? Em geral pensamos em $\mathbb{Z}$ como sendo o conjunto dos pontos marcados ao longo da reta, de uma em uma unidade. Imagine agora que enrolamos essa reta em uma circunferência, colando o ponto n ao ponto 0. Como a reta é infinita, continuamos a enrolá-la na circunferência. Dessa maneira os pontos que são múltiplos de n coincidem todos com o zero. A imagem correspondente a $\mathbb{Z}_n$ é, portanto, a de uma circunferência, onde estão marcados n pontos equidistantes. Cada ponto corresponde a uma das classes de equivalência de $\mathbb{Z}_n$.*
> *(COUTINHO, 1997, p. 74)*

Por exemplo, tomando $n = 5$ temos que as classes de equivalência módulo 5 são dadas por

$$\begin{aligned}
\overline{0} &= \{\ldots,\ -10,\ -5,\ 0,\ 5,\ 10, \ldots\} \\
\overline{1} &= \{\ldots,\ -9,\ -4,\ 1,\ 6,\ 11, \ldots\} \\
\overline{2} &= \{\ldots,\ -8,\ -3,\ 2,\ 7,\ 12, \ldots\} \\
\overline{3} &= \{\ldots,\ -7,\ -2,\ 3,\ 8,\ 13, \ldots\} \\
\overline{4} &= \{\ldots,\ -6,\ -1,\ 4,\ 9,\ 14, \ldots\}.
\end{aligned}$$

Agora vamos definir as operações de soma e de multiplicação em $\mathbb{Z}_n$, e as definimos da forma natural:

$$\overline{a} \oplus \overline{b} = \overline{a + b} \tag{2.4}$$

$$\overline{a} \odot \overline{b} = \overline{a \cdot b} \tag{2.5}$$

Quando definimos uma aplicação cujos elementos do domínio são classes de equivalência, devemos ter uma atenção especial com relação à boa definição da mesma. Como uma classe pode ter vários representantes, então para que uma tal função esteja bem definida devemos mostrar que, independente do representante da classe, o resultado da operação é sempre a mesma classe. É fácil ver que, no nosso caso, as operações de soma e multiplicação estão bem definidas e que temos as seguintes propriedades.

Proposição 2.2.5. *Seja n um número inteiro. Então em $\mathbb{Z}_n$ são válidas as seguintes propriedades:*

(1) $\overline{0}$ *é o elemento neutro da soma;*

(2) $-(\overline{a}) = \overline{-a}$*;*

(3) $\overline{1}$ *é o elemento neutro da multiplicação;*

(4) $\overline{a^b} = (\overline{a})^b$.

Quando trabalhamos com relações de equivalência, ganhamos algumas propriedades interessantes e, eventualmente, perdemos outras. Uma propriedade que ganhamos quando estamos trabalhando em congruência módulo n, é a possibilidade de existir um inverso de uma classe. Sabemos que os únicos inteiros invertíveis são ± 1, porém é fácil ver que $\overline{2}$ é invertível em $\mathbb{Z}_5$, pois $\overline{2}\,\overline{3} = \overline{6} = \overline{1}$. Esta propriedade não vale em qualquer congruência, por exemplo, podemos observar que $\overline{4}$ não tem inverso, módulo 6.

Portanto podemos pensar em quais situações uma determinada classe é invertível, módulo n. Deste modo, relembrando a Equação 2.2 e as observações feitas acerca da mesma, temos o seguinte teorema.

Teorema 2.2.6 (Teorema de Inversão)**.** *Sejam a e n números inteiros. Então a classe $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se e somente se, a e n são relativamente primos.*

Uma propriedade importante a ser investigada é a existência de inversos em $\mathbb{Z}_n$, isto será importante para a criptografia RSA. Denotaremos por $\mathcal{U}(n)$ o subconjunto de $\mathbb{Z}_n$ formado pelas classes invertíveis e estaremos interessados em sua cardinalidade. Note que $\mathcal{U}(n)$ é fechado para o produto, para isto basta verificar que se a tem inverso α, módulo n, e se b tem inverso β, módulo n, então o inverso de $a\,b$, módulo n, é $\beta\,\alpha$. Do teorema acima concluímos que, *um número inteiro p é primo se e somente se toda classe não nula tem inverso, módulo p.*

Feitas as primeiras definições e mostradas as primeiras relações na aritmética modular, podemos estudar alguns resultados de Fermat, um dos grandes matemáticos da teoria dos números. Fermat demonstrou um resultado muito importante dentro da teoria dos números, o chamado Pequeno Teorema de Fermat, e este resultado nos permite trabalhar, de modo simples, com o cálculo de grandes potências de um número inteiro. Esse resultado pode ser escrito da seguinte maneira.

Teorema 2.2.7 (Pequeno Teorema de Fermat)**.** *Sejam a um número inteiro e p um número primo, então*

$$a^p \equiv a \pmod{p}.$$

Conforme já observamos, todas as classes não nulas são invertíveis módulo um primo p. Assim podemos modificar o Pequeno Teorema de Fermat, para o caso em que $a \not\equiv 0 \pmod{p}$. Relembre do Teorema de Inversão que a classe de a é invertível, módulo p, quando $mdc(a, p) = 1$. Assim temos o segundo Teorema de Fermat, que é uma modificação do Pequeno.

Teorema 2.2.8 (Teorema de Fermat II)**.** *Sejam p um número primo e a um inteiro tal que $mdc(a, p) = 1$. Então temos que*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Decorre então deste resultado que o inverso de uma classe $\overline{a}$ em $\mathbb{Z}_p$ é a sua $(p-2)$-ésima potência. Existem várias demonstrações para o Teorema de Fermat, uma delas utiliza de indução matemática. Como não pretendemos nos estender nestas notas e estudar o método de indução matemática finita, apresentaremos aqui uma ideia da demonstração seguindo os passos feitos por Euler.

Idéia da demonstração. Vamos proceder por passos. Como $mdc(a,p) = 1$, temos que $\overline{a} \in \mathcal{U}(p)$. Considere o seguinte subconjunto de $\mathcal{U}(p)$

$$\mathcal{X} = \{\overline{a}, \overline{2a}, \ldots, \overline{(p-1)a}\}$$

Passo 1- Note que os elementos de $\mathcal{X}$ são todos distintos, logo $\mathcal{X} = \mathcal{U}(p)$.

Passo 2- Multiplique todos os elementos de $\mathcal{X}$ e $\mathcal{U}(p)$.

Passo 3- Note que, do passo anterior, obtemos a seguinte igualdade

$$a^{p-1}\,(p-1)! \equiv (p-1)! \pmod{p}$$

Passo 4- Note que $(p-1)!$ é invertível, módulo p. Portanto, multiplicando a igualdade do Passo 3 pelo inverso de $(p-1)!$, módulo p, obtemos o desejado. □

Este resultado mostra-se bastante útil para o cálculo de grandes potências, por exemplo se precisarmos determinar o valor de 2^{6765}, módulo 11. Observando que $6765 = 10 \cdot 676 + 5$, temos que

$$\begin{aligned} 2^{6765} &= 2^{10\times 676+5} \\ &= (2^{10})^{676}\ 2^5 \\ &\equiv 1^{676}\ 32 \qquad \pmod{11} \\ &\equiv 32 \qquad \pmod{11} \\ &\equiv -1 \qquad \pmod{11} \end{aligned}$$

Outra propriedade interessante que obtemos na aritmética modular, e que não é válida na aritmética dos inteiros, é a seguinte.

Proposição 2.2.9. *Sejam p um número primo e a, b inteiros. Então*

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

A demonstração da Proposição 2.2.9 decorre da expansão de $(a+b)^p$ via binômio de Newton, observando que todos os coeficiente binomiais dessa expansão, com exceção do primeiro e do último, têm coeficiente múltiplo de p, ou seja, p divide $\binom{p}{i}$, para i distinto de 1 ou p [5].

[5] Note que essa propriedade não é válida se p não for primo, por exemplo: 4 não divide $\binom{4}{2}$.

Agora veremos um interessante resultado de aritmética modular, o chamado Teorema Chinês dos Restos, que nos diz sobre a solubilidade de um sistema de congruências.

Teorema 2.2.10 (Teorema Chinês dos Restos)**.** *Sejam $n_1, \ldots, n_k$ números inteiros dois a dois primos entre si. Então o sistema de congruências*

$$\begin{array}{rcll} x & \equiv & a_1 & (\text{mod } n_1) \\ x & \equiv & a_2 & (\text{mod } n_2) \\ \vdots & & \vdots & \vdots \\ x & \equiv & a_k & (\text{mod } n_k) \end{array}$$

tem uma única solução em $\mathbb{Z}_{n_1 \cdots n_k}$.

A demonstração deste Teorema é bastante trabalhosa, assim demonstraremos o caso em que temos apenas duas congruências. A prova do caso geral pode ser obtida a partir desta, por indução.

Ideia da demonstração. Considere o seguinte sistema de congruências

$$\begin{array}{rcll} x & \equiv & a & (\text{mod } m) \\ x & \equiv & b & (\text{mod } n), \end{array}$$

com m, n inteiros relativamente primos. Da primeira congruência obtemos que $x = a + m\,y$, para qualquer y inteiro. Substituindo na segunda congruência, temos que $m\,y \equiv b - a \pmod{n}$, logo $m\,y = b - a + n\,z$, para qualquer inteiro z. Como $m\,n$ são relativamente primos, então existem m', n' tais que

$$m\ m' + n\ n' = 1.$$

Deste modo, $m\,m'\,y = m'\,b - m'\,a + m'\,n\,z$, logo $y = m'\,b - m'\,a + k\,n$, para todo k inteiro. Como $x = a + m\,y$, segue que $x = a + m\,m'\,b - m\,m'\,a + k\,m\,n = (1 - m\,m')a + m\,m'\,b + k\,m\,n$. Portanto $x = a\,n\,n' + b\,m\,m' + k\,m\,n$, onde k é qualquer inteiro, é uma solução para o sistema acima.

A unicidade de x em $\mathbb{Z}_{mn}$ decorre do fato que, se y satisfaz as duas congruências, então m e n dividem $x - y$. Como m e n são primos entre si e ambos dividem $x - y$, logo $m\,n$ divide $x - y$, portanto $x \equiv y \pmod{m\,n}$. □

Observação 2.2.11. Sejam a, m, n inteiros, com $mdc(m, n) = 1$. Então $x \equiv a \pmod{m\,n}$ se e somente se

$$\begin{array}{rcll} x & \equiv & a & (\text{mod } m) \\ x & \equiv & a & (\text{mod } n). \end{array}$$

De fato, supondo válidas as duas congruências acima temos que existem m', n' inteiros tais que

$$m'm = x - a = n'n.$$

Como m e n são primos entre si, segue que todo primo p que dividir m não pode dividir n. Assim todo primo p que dividir m tem que dividir n' e, mais ainda, toda potência p^k que dividir m tem que dividir n'. Portanto m divide n', isto é, existe k' tal que $n' = k'm$. Deste modo, $x - a = n'n = k\,m\,n$ e, consequentemente, $x \equiv a \pmod{m\,n}$. A recíproca é imediata.

Como consequência do segundo Teorema de Fermat, conseguimos calcular grandes potências de números, módulo um número primo. Agora vejamos que, com essa nova ferramenta, Teorema Chinês dos Restos, conseguimos determinar grandes potências de números, módulo alguns números compostos. Por exemplo, suponhamos que queremos determinar o valor de 2^{6754} módulo $1155\,(= 3 \times 5 \times 7 \times 11)$. Usando o Teorema de Fermat, para cada um desses primos da fatoração de 1155, obtemos o seguinte

$$\begin{aligned} 2^{6754} &\equiv 1 \pmod 3 \\ 2^{6754} &\equiv 4 \pmod 5 \\ 2^{6754} &\equiv 2 \pmod 7 \\ 2^{6754} &\equiv 5 \pmod{11} \end{aligned}$$

Assim temos que, para encontrar o valor de 2^{6754}, módulo $3 \times 5 \times 7 \times 11$, precisamos encontrar a solução do sistema

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 2 \pmod 7 \\ x &\equiv 5 \pmod{11} \end{aligned}$$

Pelo Teorema Chinês dos Restos, temos que o sistema acima possui única solução em $\mathbb{Z}_{1155}$. Note que da primeira equação temos $x = 1 + 3k$, então a segunda equação se torna $1 + 3k \equiv 4 \pmod 5$. Como 3 é invertível, módulo 5, obtemos que a segunda equação se torna $k \equiv 1 \pmod 5$ e então obtemos que $x = 4 + 15l$. Substituindo esta última igualidade na terceira equação obtemos que $l \equiv 5 \pmod 7$ e, logo, $x = 79 + 105m$. Por fim, substituindo esta igualdade na última equação obtemos que $m \equiv 6 \pmod{11}$ e, consequentemente, $x = 709 + 1155n$. Portanto concluímos que $2^{6754} \equiv 709 \pmod{1155}$. Apesar deste método parecer ser complicado, seria muito mais difícil calcular 2^{6754} para depois dividir por 1155.

Dado um número inteiro n, consideremos $\mathcal{U}(n)$ o conjunto das classes invertíveis de $\mathbb{Z}_n$. Conforme já vimos, este conjunto é fechado para produto e inversos e, claramente, contém a classe $\overline{1}$. Estamos interessados em estudar propriedades de $\mathcal{U}(n)$, para isso definimos a *função de Euler ou função totiente* dada por

$$\begin{aligned} \phi\colon \mathbb{Z} &\longrightarrow \mathbb{Z} \\ n &\longmapsto |\mathcal{U}(n)|, \end{aligned} \tag{2.6}$$

onde $|\mathcal{U}(n)|$ denota a cardinalidade do conjunto $\mathcal{U}(n)$.

Queremos determinar o valor de $\phi(n)$ para qualquer inteiro n, então comecemos estudando os casos mais simples. Se p é primo, então para todo $1 \leq a < p$ sabemos que $mdc(a, p) = 1$, portanto $\phi(p) = p - 1$. Agora vejamos qual o valor da função de Euler aplicada a uma potência de um número primo. Para determinarmos o valor de $\phi(p^k)$ precisamos encontrar todos os inteiros $0 \leq a < p^k$, com $1 = mdc(a, p^k)$. Como p é primo, então ou $mdc(a, p^k) = 1$ ou p divide a, então é mais fácil contar os casos em que p divide a. Assim temos que p divide a se e somente se $a = p\,b$, com $0 \leq b < p^{k-1}$. Portanto $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p - 1)$.

Para determinarmos o valor de $\phi(n)$ para um n qualquer precisamos de um resultado auxiliar, que decorre do Teorema Chinês dos Restos.

Dados m e n inteiros relativamente primos, então, do Teorema Chinês dos Restos e da Observação 2.2.11, temos que para cada $x \in \{0, \ldots, mn - 1\}$ existem únicos $a \in \{0, \ldots, m - 1\}$ e $b \in \{0, \ldots, n - 1\}$ tais que $\overline{x}$ é solução de

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

em $\mathbb{Z}_{mn}$. Assim temos uma correspondência biunívoca entre $\mathbb{Z}_{mn}$ e $\mathbb{Z}_m \times \mathbb{Z}_n$, denotaremos essa correspondência por $\overline{x} \leftrightarrow (\overline{a}, \overline{b})$.

Portanto, para provarmos o resultado a seguir, basta observarmos que $\overline{x} \in \mathcal{U}(mn)$ se e somente se $\overline{a} \in \mathcal{U}(m)$ e $\overline{b} \in \mathcal{U}(n)$, onde $\overline{x} \leftrightarrow (\overline{a}, \overline{b})$.

Teorema 2.2.12. *Sejam m e n inteiros primos entre si. Então*

$$\phi(mn) = \phi(m)\phi(n).$$

Note que como consequência do Teorema 2.2.12, temos os seguintes corolários.

Corolário 2.2.13. *Seja n um número inteiro, cuja fatoração em primos é $n = p_1^{n_1} \cdots p_k^{n_k}$, com $p_1 < \cdots p_k$. Então*

$$\phi(n) = \phi(p_1^{n_1}) \cdots \phi(p_k^{n_k}) = p_1^{n_1 - 1} \cdots p_k^{n_k - 1}(p_1 - 1) \cdots (p_k - 1) \tag{2.7}$$

Corolário 2.2.14. *Se $n = pq$, com p e q primos, então $\phi(n) = (p - 1)(q - 1)$.*

Observação 2.2.15. Se m e n são inteiros relativamente primos, então, pelo observado antes do Teorema 2.2.12, se x é um número inteiro que satisfaz as equações

$$\begin{aligned} x &\equiv 1 \pmod{m} \\ x &\equiv 1 \pmod{n}, \end{aligned}$$

então $\overline{x} = \overline{1}$ em $\mathbb{Z}_{mn}$, isto é $x \equiv 1 \pmod{mn}$.

Feitas todas as colocações acima, podemos estender o segundo Teorema de Fermat da seguinte maneira.

Teorema 2.2.16 (Teorema de Euler)**.** *Sejam a e n inteiros relativamente primos. Então*

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Para demonstrar o Teorema de Euler, seguindo como feito em Coutinho (1997, Cap. 8), seria necessário introduzir o conceito de Grupo e provar o Teorema de Lagrange. Porém podemos demonstrar o mesmo de outra forma, por passos, similar à demonstração do segundo Teorema de Fermat (2.2.8).

Idéia da Demonstração. Denote $\mathcal{U}(p)$ por $\{\overline{u_1}, \overline{u_2}, \ldots, \overline{u_{\phi(n)}}\}$, então

Passo 1- Considere o seguinte subconjunto de $\mathcal{U}(p)$

$$\mathcal{X} = \{\overline{a\,u_1}, \overline{a\,u_2}, \ldots, \overline{a\,u_{\phi(n)}}\};$$

Passo 2- Note que $\mathcal{X} = \mathcal{U}(p)$;

Passo 3- Do Passo 2, multiplicando os elementos de $\mathcal{X}$ e $\mathcal{U}(p)$ obtemos a seguinte igualdade em $\mathbb{Z}_n$

$$\prod_{i=1}^{\phi(n)} \overline{u_i} = \prod_{i=1}^{\phi(n)} \overline{a\,u_i} \quad \left(= \overline{a}^{\phi(n)} \prod_{i=1}^{\phi(n)} \overline{u_i} \right);$$

Passo 4- Como $\prod \overline{u_i}$ é invertível em $\mathbb{Z}_n$, assim, multiplicando o seu inverso nos dois lados igualdade do Passo 3, obtemos o desejado. □

Agora vejamos uma importante observação acerca da função de Euler.

Observação 2.2.17. Sejam a, p, q inteiros, com p, q primos distintos e $n = p\,q$, então, para todo k inteiro positivo

$$a^{\phi(n)\,k+1} \equiv a \pmod{n}.$$

De fato, conforme a Observação 2.2.11 $a^{\phi(n)\,k+1} \equiv a \pmod{n}$ se e somente se

$$a^{\phi(n)\,k+1} \equiv a \pmod{p} \tag{2.8}$$

$$a^{\phi(n)\,k+1} \equiv a \pmod{q}. \tag{2.9}$$

Se p não divide a, então pelo segundo Teorema de Fermat (2.2.8) temos que $a^{p-1} \equiv 1 \pmod{p}$, logo $1 \equiv (a^{p-1})^{(q-1)\,k} \equiv a^{\phi(n)\,k} \pmod{p}$. Portanto $a^{\phi(n)\,k+1} \equiv a \pmod{p}$.

Se p divide a, logo $a \equiv 0 \pmod{p}$. Portanto $a^{\phi(n)\,k+1} \equiv a \pmod{p}$. Assim obtemos que a Equação 2.8 é verdadeira, para todo a, k inteiro positivo. Analogamente, se mostra que a Equação 2.9 é verdadeira, obtendo o desejado.

Voltemos agora a criptografia RSA. Conforme já vimos, para criptografar uma mensagem escolhemos p e q primos e consideremos $n = p\,q$. Em seguida escolhemos $1 < e < \phi(n)$ relativamente primo com $\phi(n)$. Assim, existe único $1 < d < \phi(n)$ tal que $d\,e \equiv 1 \pmod{\phi(n)}$, ou seja, $d\,e = \phi(n)\,k + 1$, para algum k inteiro.

Então definimos as aplicações de codificação e decodificação do seguinte modo

$$\begin{array}{rcl} C : \mathbb{Z}_n & \to & \mathbb{Z}_n \\ \overline{m} & \mapsto & \overline{m}^{\,e} \end{array} \qquad \text{e} \qquad \begin{array}{rcl} D : \mathbb{Z}_n & \to & \mathbb{Z}_n \\ \overline{m} & \mapsto & \overline{m}^{\,d}. \end{array}$$

Agora precisamos ver que quando codificarmos e decodificarmos um bloco — cujo valor numérico é menor que n — este retornará à original. De fato, seja m un número inteiro positivo menor que n, então temos que

$$D(C(\overline{m})) = (\overline{m}^e)^d = \overline{m}^{ed} = \overline{m}^{\phi(n)\,k+1} = \overline{m}$$

em $\mathbb{Z}_n$, onde a última igualdade segue da Observação 2.2.17. Como $m < n$, então reobtemos o mesmo valor m.

2.3 Gerando Primos

Conforme já foi descrito, a segurança dessa criptografia depende da escolha dos primos p e q de forma que dificultem a fatoração de $n = p\,q$. Assim devemos conseguir gerar primos suficientemente grandes. Nesta seção veremos alguns métodos que surgiram para tentar gerar números primos, assim perceberemos o quão difícil pode ser gerar um número primo. Na sequência estudaremos o crivo de Eratóstenes, com o qual será possível gerar todos os primos menores que um n fixado. Além disso, estudaremos o algoritmo de Fermat que se mostra bastante eficiente para encontrar fatores primos próximos à raiz quadrada do número a ser fatorado. Por fim estudaremos os números pseudoprimos, números de Carmichael e os pseudoprimos fortes, bem como os testes de primalidade de Miller e de Lucas.

2.3.1 Fórmulas Para Gerar Primos

Ao longo da história, muito buscou-se fórmulas para gerar números primos, ou seja, funções $f\colon \mathbb{Z} \to \mathbb{Z}$ tais que para cada valor inteiro n tenha-se um número primo $f(n)$. Uma primeira forma que fora pensada, é a possibilidade de se gerar números primos através de uma função polinomial com coeficientes inteiros. Porém mostrou-se que para todo polinômio com coeficientes inteiros $f(x)$ existem infinitos valores inteiros para n de forma que $f(n)$ seja composto. Para detalhes da demonstração desse fato consultar Coutinho (1997, p. 54) ou ainda Ribenboim (1989, Cap. 3, Sec. II).

Por exemplo, considerando a função $f(n) = n^2 + 1$ observamos que $f(n)$ é ímpar se e somente se n é par. Deste modo, se $n \neq 1$ então $f(n)$ só pode ser primo de n for par. Calculando o valor de $f(n)$, obtemos que para $n = 2, 4, 6$ $f(n)$ é primo, porém isso não gera uma regra geral, haja vista que $f(8) = 65$ é composto.

Duas fórmulas exponenciais tiveram especial importância histórica que são

$$M(n) = 2^n - 1 \text{ e } F(n) = 2^{2^n} + 1.$$

Os números da forma $M(n)$ são chamados *números de Mersenne* e os números da forma $F(n)$ são chamados *números de Fermat*. Conforme Coutinho (1997, p. 56) "ambas [as fórmulas] foram intensamente estudadas pelos matemáticos do século XVII, sobretudo Fermat".

Os números de Mersenne já eram estudados desde os gregos, mas receberam esse nome em homenagem a seguinte conjectura de Mersenne: *os números da forma* $M(n) = 2^n - 1$ *são primos para*

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 \text{ } e \text{ } 257,$$

e composto para os demais 44 números primos menores que 257.

Primeiramente, é fácil ver que se n é composto, então $M(n)$ é composto. De fato, se $n = ab$, então

$$M(n) = 2^n - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^b + 1).$$

Assim só faz sentido tentar determinar a primalidade dos números de Mersenne da forma $M(p)$, onde p é primo positivo. Poderíamos nos perguntar se a recíproca é verdadeira, ou seja, se todo número da forma $M(p)$ é primo. Porém isto não é verdade, pois, conforme conjecturou Mersenne, $M(11)$ é composto ($M(11) = 2047 = 23 \times 89$). A conjectura de Mersenne foi provada ser falsa apenas em 1886 por Pervusin e Seelhof, que mostraram que $M(61)$ é primo. Posteriormente foi provado que $M(89)$ e $M(107)$ também são primos e que $M(67)$ e $M(257)$ são compostos.

Apesar de os números de Mersenne $M(p)$ não serem todos primos, eles são importantes por vários motivos, entre eles, a criação de números perfeitos e a geração de primos com muitos algarismos.

Um número é dito perfeito se a soma dos seus divisores positivos próprios (excluído ele mesmo) resulta nele. Por exemplo, o número 6 é o menor número perfeito, pois os seus divisores positivos próprios são 1, 2 e 3, cuja soma resulta em $1 + 2 + 3 = 6$. O próximo número perfeito é 28 e o 3º número perfeito é 496. Um fato muito interessante já era descrito pelos gregos, se um número de Mersenne $2^n - 1$ é primo então $2^{n-1}(2^n - 1)$ é um número perfeito. Conforme Wikipédia (2014b)

> *O IX Livro dos Elementos de Euclides contém a definição de números perfeitos e a seguinte proposição: 'Se tantos números quantos se queira começando a partir da unidade forem dispostos continuamente numa proporção duplicada até que a soma de todos resulte num número primo, e se a soma multiplicada pelo último origina algum número, então o produto será um número perfeito'.*

Também pode-se provar que todo número perfeito par é dessa forma. Já foi mostrado, veja Ochem e Rao (2012), que se um número ímpar é perfeito, então este tem que ter, pelo menos, 1500 casas decimais, ou seja, números perfeitos ímpares, se existirem, são maiores que 10^{1500}. Portanto conjecturou-se que não existem números perfeitos ímpares. Note que nenhum número primo é perfeito.

Existe registro de 48 números de Mersenne[6] que são primos, sendo que o maior existente $2^{57.885.161}-1$ tem 17.425.170 algarismos e gera o número perfeito $2^{57.885.160}(2^{57.885.161}-1)$ que tem 34 milhões de algarismos[7].

Os números de Fermat $F(n) = 2^{2^n}+1$ tem história semelhante, sendo que o próprio Fermat listou os mesmos para n entre 0 e 6. Que são

$$3, 5, 17, 257, 56637, 4294967297 \text{ e } 18446744073709551617.$$

Fermat conjecturou que todos os números $F(n)$ seriam primos, porém ele não percebera que um dos números que ele mesmo listará era composto. Quase um século depois, Euler fatorou $F(5)$ da seguinte maneira

$$F(5) = 4294967297 = 641 \times 6700417$$

Mais geralmente, para $5 \leq n \leq 32$, mostrou-se que $F(n)$ é composto. Não se conhece primos de Fermat além dos listados por ele.

2.3.2 Fatoração e Testes de Composição

Inicialmente temos o método de fatoração decorrente do Teorema da Fatoração Única (2.2.3). Este método para determinação da primalidade de um número inteiro n consiste na divisão sistemática desse número por 2, 3, 4, 5, ..., $[\sqrt{n}]$, onde $[\sqrt{n}]$ é a parte inteira de $\sqrt{n}$ [8]. Se em algum dos passos obtivermos como resto 0, então o número em questão é composto e, mais ainda, obtivemos uma fatoração para o mesmo. Deste modo, para determinar se 239 é um número primo, utilizando esse método, procedemos da seguinte maneira: resolvemos sequencialmente a divisão de 239 por 2, 3, 4, ..., 15. Como todas as divisões resultam em restos não nulos, segue que 239 é um número primo.

[6] Os últimos 14 números primos de Mersenne encontrados formam encontrados através the um software do GIMPS (Great Internet Mersenne Prime Search)

[7] Este número é tão grande, que um arquivo de texto, disponível em ⟨www.mersenne.org⟩, com esse número tem 32MB de tamanho.

[8] Podemos melhorar esse teste efetuando a divisão de n apenas pelos primos menores ou iguais a $[\sqrt{n}]$.

Note que o método descrito acima não apenas determina se um número é primo ou composto, como também encontra um fator para o mesmo (quando existir). Portanto esse método parece ser muito interessante para o propósito, porém quando o número o qual pretende-se determinar a primalidade é muito grande esse método torna-se inviável. Se tivermos um número primo n com mais de 100 algarismos[9], isto é, $n \geq 10^{100}$, logo $\sqrt{n} \geq 10^{50}$ e, portanto, será necessário efetuar mais de 10^{50} divisões. Supondo que um computador consiga fazer 10^{10} divisões por segundo — o que é bem além da capacidade de um computador atualmente —, levaríamos 10^{40} segundos para realizar essas divisões, ou seja, 3 x 10^{32} anos para descobrir que n é primo.

Mas isto não significa que esse método seja inútil, o mesmo é bastante eficiente quando o número tem um divisor relativamente pequeno, pois, usando os dados do exemplo anterior, em 1 hora conseguiríamos testar se o número tem algum divisor menor que 36 bilhões.

Outra forma para determinar a primalidade de um número é usando o algoritmo de Fermat, como descrito a seguir. Visto que todo número par distinto de 2 é composto, podemos supor, sem perda de generalidade, que n é impar. Se $n = a\,b$, então a e b são ímpares. Deste modo, tomando $x = {}^{(a+b)}/_{2}$ e $y = {}^{(a-b)}/_{2}$ temos que $n = x^2 - y^2$. Assim temos que n é composto se e somente se existem números inteiros x e y tais que $n = x^2 - y^2$, neste caso $n = (x-y)(x+y)$. Como $a, b > 1$, assim temos que $b(a-1) > a-1$, somando $b+1$ na desigualdade acima e como $n = ab$, obtemos que $a + b = (a-1) + (b+1) < (ab-b) + (b+1) = n+1$. Portanto, $\frac{(a+b)}{2} < \frac{(n+1)}{2}$.

Então atribuímos valores para x entre $[\sqrt{n}]$ e $\frac{n+1}{2}$ e calculamos $y = \sqrt{x^2 - n}$ afim de determinar uma fatoração de n. Deste modo, se encontrarmos algum valor de x tal que $\sqrt{x^2 - n}$ seja inteiro, concluiremos que n é um número composto e, mais ainda, teremos a seguinte fatoração para n

$$(x - \sqrt{x^2 - n})(x + \sqrt{x^2 - n}).$$

Por exemplo, se $n = 1342127$ então $[\sqrt{1342127}] = 1158$ e n não é quadrado perfeito. Logo tomando $x = 1159$ e aumentando de um em um, calculamos os valores de $\sqrt{x^2 - n}$ para encontrar uma fatoração de n. Se formos incrementando o valor de x e chegarmos a $x = 671064$ sem obter que $\sqrt{x^2 - n}$ é inteiro, então obteremos que n é primo. Porém, no nosso caso, obtemos um valor de x para o qual $\sqrt{x^2 - n}$ é inteiro, conforme a Tabela 9, obtendo que 1342127 é composto. Deste modo $x = 1164$ e $y = 113$, satisfazem $n = x^2 - y^2$. Portanto, 1342127 é decomposto como

$$13421217 = (1164 - 113)(1164 + 113) = 1051 \times 1277.$$

[9] Para uma maior segurança da criptografia RSA, é necessário que se utilize números primos com mais de 100 algarismos.

Tabela 9 – Fermat

x	$\sqrt{x^2 - n}$
1159	33,97
1160	58,93
1161	76,11
1162	90,09
1163	102,18
1164	113

Note que, usando o método anterior, teríamos que efetuar 1050 divisões para encontrar essa fatoração, portanto o método de Fermat se mostra bastante interessante quando usado para números que possuam fatores próximos de sua raiz quadrada.

Esses dois métodos descritos acima são formas de determinar a primalidade e, caso exista, exibir uma fatoração para números inteiros. Esse procedimento é importante para conseguir fatorar um número e quebrar a criptografia. Conforme vimos, a segurança da criptografia RSA está intimamente ligada a escolha de "bons"números primos, números com 100 algarismos ou mais. Assim, precisamos de métodos para gerar números primos gigantes. Então vamos discutir alguns métodos "ingênuos", que surgiram ao longo da história, para a criação de primos. Começaremos por estudar o Crivo de Eratóstenes, que foi o primeiro método criado para determinar números primos.

Crivo de Eratóstenes

O Crivo foi desenvolvido pelo matemático grego Eratóstenes de Cirene (276 a.C. à 194 a.C.). Através deste método obtemos uma lista contendo todos os primos entre 2 e um número qualquer n, da seguinte maneira. Primeiramente escrevemos a lista completa de 2 a n, em seguida riscamos todos os múltiplos de 2 da lista (4, 6, 8, 10, 12, ...). Dessa maneira o primeiro número não riscado após o 2, no caso 3, é um número primo. Então riscamos todos os múltiplos de 3 da lista (6, 9, 12, 15, ...). O primeiro número não riscado após o 3, no caso o 5, é um número primo, assim riscamos os múltiplos de 5 (10, 15, 20, ...). Repetimos esse procedimento, até que tenhamos riscado todos os números compostos menores ou iguais a n.

Alguns pontos interessantes devem ser observados para que possamos melhorar o crivo. Note que, se um número da lista é composto então um de seus fatores precisa ser menor ou igual a $\sqrt{n}$. Deste modo, quando chegarmos a um primo $p > \sqrt{n}$ todos os números compostos já estarão riscados, portanto podemos parar o crivo. Como pode ser facilmente percebido, alguns números são riscados várias vezes e, infelizmente, não podemos evitar isso. Porém podemos melhorar o crivo, evitando fazer alguns riscos desnecessários. Quando chegarmos um número primo p e formos riscar os seus múltiplos, como todos os múltiplos dos primos menores que ele já foram riscados logo todos os múltiplos de p menores que p^2 já foram retirados da lista, portanto podemos riscar os múltiplos de p começando por p^2.

Por exemplo, vamos determinar os primos entre 2 e 100. Assim escrevemos a lista com todos os números de 2 a 100, conforme a Tabela 10.

Tabela 10 – Crivo de Eratóstenes

	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

Iniciamos riscando os múltiplos de 2 (4, 6, 8, ..., 98, 100). Em seguida riscamos os múltiplos de 3 iniciando, conforme a observação anterior, a partir de $9 = 3^2$, assim riscamos $(9, 12, 15, \ldots, 99)$. Na sequência, riscamos os múltiplos de 5, iniciando por 25, que são $(25, 30, 35, \ldots, 100)$. Por fim riscamos os múltiplos de 7 iniciando por 49, que são $(49, 56, 63, 70, 77, 84, 91, 98)$. Quando chegarmos a um primo maior que $\sqrt{n}$, então todos os números compostos já estarão riscados. No nosso caso, como o próximo número primo é 11 e este é maior que $\sqrt{100} = 10$, podemos parar o processo aqui. Assim obtemos a Tabela 11, onde todos os números compostos estão riscados. Portanto determinamos todos os primos menores que 100, à saber: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89 e 97.

Tabela 11 – Crivo de Eratóstenes

	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~~

Note que esse crivo não é útil para criar primos muito grandes, afinal ele determina todos os primos menores ou iguais a um dado número. Portanto, se o intuito é encontrar um número primo grande, por exemplo com mais de 100 algarismos, então este crivo não é eficiente. Porém, mostra-se útil para listar números primos até um valor n fixado.

Como não existem métodos eficientes para gerar primos gigantes, atacaremos esse problema por um outro caminho, estudando formas de, dado um número inteiro positivo e ímpar, garantir que esse número seja primo (testes de primalidade). Ou então, estudaremos formas de garantir que um tal número seja composto (testes de composição). Para esse fim utilizaremos da aritmética modular estudada, mais especificamente, utilizaremos os Teoremas de Fermat para criar os testes de composição/primalidade.

Agora que temos mais ferramentas matemáticas em nosso poder, podemos discutir métodos para verificar quando um determinado número é composto. Para esse fim vamos discutir a existência dos números chamados pseudoprimos, os números de Carmichael e os pseudoprimos fortes. Também vamos discutir sobre alguns testes de primalidade existentes, como o teste de Lucas e o teste de Miller.

O Pequeno Teorema de Fermat (2.2.7) nos diz que quando p é primo, então $a^p \equiv a \pmod{p}$, para qualquer a inteiro. Note que, dado um inteiro n, se existir um número inteiro a tal que $a^n \not\equiv a \pmod{n}$, então temos que n é obrigatoriamente composto. Deste resultado obtemos uma forma de garantir que um dado número é composto, gerando assim o seguinte teste.

Teste 2.3.1. Seja n um número ímpar. Se existir $1 < a < n-1$ tal que $a^{n-1} \not\equiv 1 \pmod{n}$, então n é composto.

Observação 2.3.2. A recíproca do teste acima é verdadeira, isto é, se n é composto então existe $1 < a < n-1$ tal que $a^{n-1} \not\equiv 1 \pmod{n}$.

De fato, se n tem um divisor próprio $1 < a < n-1$, então $mdc(a, n) \neq 1$ e, pelo Teorema 2.2.6, $a^k \not\equiv 1 \pmod{n}$, para qualquer $k > 0$.

Note que com este teste, determinamos que n é composto sem exibir uma fatoração para o mesmo. A partir desse teste, nasce uma questão natural: podemos afirmar que um número inteiro n é primo se encontrarmos $1 < a < n-1$ de tal forma que $a^{n-1} \equiv 1 \pmod{n}$? Alguns matemáticos achavam que sim, como por exemplo Leibniz. Porém a resposta para essa pergunta é não, por exemplo $2^{340} \equiv 1 \pmod{341}$, porém $341 = 11 \cdot 13$ é composto.

Definição 2.3.3 (Pseudoprimo)**.** Sejam n um número inteiro positivo ímpar e $1 < a < n-1$ um número inteiro. Então n é dito *pseudoprimo para a base a* se

$$a^{n-1} \equiv 1 \pmod{n}.$$

Apesar de um número n que satisfaça $2^{n-1} \equiv 1 \pmod{n}$ não necessitar ser primo, conforme Coutinho (1997, p. 106) " [. . .] entre 1 e um milhão existem 78498 números primos, mas apenas 245 pseudoprimos para a base 2", portanto há uma grande probabilidade de que um número que satisfaça $2^{n-1} \equiv 1 \pmod{n}$ seja primo.

Pela Observação 2.3.2, se $mdc(a, n) \neq 1$, então n não é pseudoprimo para a base a. Entretanto, podemos nos perguntar: existe algum número que seja pseudoprimo para toda base que seja prima com ele? A resposta a esta pergunta é sim. A seguir faremos algumas considerações utilizando o Pequeno Teorema de Fermat (2.2.7), e mostraremos uma classe de números compostos que respondem positivamente à questão acima.

Do Pequeno Teorema de Fermat temos que, para um primo p, $a^p \equiv a \pmod{p}$. Inspirado por esse resultado, definimos os números de Carmichael.

Definição 2.3.4 (Número de Carmichael)**.** Dizemos que um número positivo ímpar composto n é um *número de Carmichael* se, para todo inteiro a a seguinte congruência valer

$$a^n \equiv a \pmod{n}.$$

Mais ainda, podemos supor, sem perda de generalidade, que $1 < a < n - 1$.

Dados dois números inteiros a e n, sabemos que se a e n são primos entre si, então existe inteiro a' tal que $aa' \equiv 1 \pmod{n}$. Assim, se n é um número de Carmichael e a é primo com n, então $a^{n-1} \equiv 1 \pmod{n}$. Portanto, um número de Carmichael é pseudoprimo para toda base relativamente prima a ele.

Os números de Carmichael receberam esse nome pois o primeiro matemático a dar um exemplo de um tal número foi Carmichael em um artigo publicado em 1912

Teste de Miller

Para entendermos o Teste de Miller precisamos fazer as seguintes observações.

Se p é um primo ímpar ($p \neq 2$), então $p - 1 = 2^k q$, com q ímpar. Do segundo Teorema de Fermat (2.2.8), se $1 < a < p - 1$, temos

$$1 \equiv a^{p-1} \equiv a^{2^k q} \pmod{p}.$$

Desse modo, seja j o menor inteiro não-negativo tal que

$$1 \equiv a^{2^j q} \pmod{p}. \tag{2.10}$$

Agora temos duas situações, $j = 0$ ou $j > 0$.

• Se $j = 0$, então da igualdade acima obtemos que

$$1 \equiv a^q \pmod{p}.$$

• Se $j > 0$, então $a^{2^j q} - 1 = (a^{2^{j-1} q})^2 - 1 = (a^{2^{j-1} q} - 1)(a^{2^{j-1} q} + 1)$. Da equação (2.10), temos que p divide $a^{2^j q} - 1 = (a^{2^{j-1} q} - 1)(a^{2^{j-1} q} + 1)$. Pela minimalidade de j, segue que p divide $a^{2^{j-1} q} + 1$, ou seja,

$$a^{2^{j-1} q} \equiv -1 \pmod{p}.$$

Resumindo

Se p é primo ímpar, então $p-1 = 2^k q$, com q ímpar. Assim, para todo $1 < a < p-1$, temos que

$$a^q \equiv 1 \pmod{p} \qquad \text{ou} \qquad a^{2^j q} \equiv -1 \pmod{p},$$

para algum $0 < j \leq k - 1$.

Teste 2.3.5 (Teste de Miller)**.** Seja $n > 2$ ímpar ($n - 1 = 2^k q$, com q ímpar). Se existir $0 < a < n - 1$ tal que

$$a^q \not\equiv 1 \pmod{p} \qquad \text{e} \qquad a^{2^j q} \not\equiv -1 \pmod{p},$$

para todo $0 < j \leq k - 1$, então n é composto.

Definição 2.3.6 (Pseudoprimo Forte)**.** Seja $n > 2$ um número ímpar composto. Se existir $0 < a < n - 1$ tal que

$$a^q \equiv 1 \pmod{n} \qquad \text{ou} \qquad a^{2^j q} \equiv -1 \pmod{n},$$

para algum $0 < j \leq k - 1$, então n é dito *Pseudoprimo Forte para a base a.*

Note que se n é pseudoprimo forte para a base a, então n é pseudoprimo para a. Para qualquer base a existem infinitos inteiros pseudoprimos fortes para essa base[10]. Os menores inteiros pseudoprimos fortes para as 4 primeiras bases primas estão descritos na Tabela 12.

Tabela 12 – Pseudoprimos fortes

Pseudoprimo Forte	Base
$2047 = 23 \times 89$	2
$121 = 11 \times 11$	3
$781 = 11 \times 71$	5
$25 = 5 \times 5$	7

Fonte: Dados retirados do site ⟨primes.utm.edu⟩

Aplicando o Teste de Miller podemos afirmar que um determinado número é composto, porém quando o resultado é inconclusivo para uma base a podemos ter que o número é primo ou pseudoprimo forte para essa base. Para diminuirmos a chance de errarmos sobre a primalidade via o Teste de Miller, podemos aplicá-lo a mais de uma base. Assim poderemos ter uma confiabilidade maior sobre a primalidade de número, até mesmo podendo ter a certeza sobre a sua primalidade. Conforme Pomerance, Selfridge e Wagstaff Jr. (1980) e Jaeschke (1993), podemos afirmar a primalidade de um inteiro n a partir do Teste de Miller[11] nos seguintes casos:

Tabela 13 – Pseudoprimos Fortes

n menor que	Inconclusivo no teste de Miller para as bases
1.373.653	2 e 3
25.326.001	2, 3 e 5
118.670.087.467	2, 3, 5 e 7
2.152.302.898.747	2, 3, 5, 7, 11
3.474.749.660.383	2, 3, 5, 7, 11 e 13
341.550.071.728.321	2, 3, 5, 7, 11, 13 e 17

Nota: A primeira linha da tabela nos diz que, se $n < 1.373.653$ e for inconclusivo no teste de Miller para as bases 2 e 3, então n é primo.

Portanto, se n é menor que 2 trilhões e satisfaz as igualdades de pseudoprimo forte para as bases 2, 3, 5, 7 e 11, então n é primo.

[10] Demonstração para este fato pode ser encontrada em Pomerance, Selfridge e Wagstaff Jr. (1980)

[11] O teste de Miller nos afirma que, sob certas hipóteses, um número inteiro é composto. Porém, conforme Pomerance, Selfridge e Wagstaff Jr. (1980) e Jaeschke (1993) podemos afirmar a sua primalidade

2.3.3 Testes de Primalidade

Na subseção anterior, estudamos alguns testes para determinar se um número inteiro n é composto. Porém, como esses testes não são determinísticos, não conseguimos uma resposta sobre a primalidade. Conforme vimos, se compusermos os testes para mais de uma base, conseguiremos afirmar sobre a primalidade, porém estaremos limitados superiormente. Nesta subseção estudaremos alguns testes de primalidade, ou seja, testes que nos afirmam com certeza que n é primo.

Teste de Lucas

Teste 2.3.7 (Teste de Lucas)**.** Seja n inteiro positivo ímpar. Se existir $1 < a < n$ tal que

$$a^{n-1} \equiv 1 \pmod{n} \qquad \text{e} \qquad a^{(n-1)/p} \not\equiv 1 \pmod{n},$$

para todo p primo que dividir $n-1$, então n é primo.

A demonstração deste resultado, envolve o emprego do Teorema de Lagrange, e portanto não será feita aqui.

Note que para utilizarmos esse Teste, precisamos conhecer todos os primos da fatoração de $n-1$, e isso acaba tornando esse teste praticamente inaplicável. O Teste de Lucas se mostra razoável, quando $n-1$ tiver fatores primos pequenos.

Uma pequena modificação pode ser feita no Teste de Lucas, escolhendo uma base para cada divisor de $n-1$, tornando esse teste um pouco mais viável. Porém ainda necessitamos conhecer todos os fatores primos de $n-1$. Então o Teste de Lucas pode ser reescrito da seguinte maneira.

Teste 2.3.8 (Teste de Lucas modificado)**.** Seja $n > 0$ inteiro tal que

$$n - 1 = p_1^{k_1} \cdots p_l^{k_l},$$

onde $p_1 < \cdots < p_l$ são primos. Se para cada $i \in \{1, \ldots, l\}$, existirem $1 < a_i \leq n-1$ tais que

$$a_i^{n-1} \equiv 1 \pmod{n} \qquad \text{e} \qquad a_i^{(n-1)/p_i} \not\equiv 1 \pmod{n},$$

então n é primo.

Esses métodos exibidos não são determinísticos, ou seja, com nenhum deles obtemos que, sob certas condições, n é primo ou, caso contrário, n é composto. Por exemplo, no Teste de Miller obtemos que, se n satisfizer certas condições, então n é composto ou, caso contrário, nada pode-se afirmar. Após o desenvolvimento da criptografia RSA, muito procurou-se um teste de primalidade determinístico, que pudesse ser realizado em "tempo razoável". Finalmente, Agrawal, Kayal e Saxena (2004) desenvolveram um método, chamado Algoritmo AKS, que determina se um dado inteiro é primo ou composto. Uma

característica muito interessante deste método é que o tempo para realizar o teste em um inteiro n é proporcional ao número de algarismos de n, a partir de uma regra polinomial[12]. A existência de tal teste de primalidade determinístico não compromete a segurança da criptografia RSA, haja visto que esse algoritmo apenas determina a primalidade, não determinando uma fatoração de um número quando composto.

[12] Dizemos assim que o algoritmo é executado em *tempo polinomial*.

3 Proposta de Atividade

Conforme vimos ao longo do trabalho, a criptografia é de grande importância para a comunicação de forma segura. A criptografia RSA utiliza fortemente a teoria dos números inteiros, através da matemática modular e da fatoração como produto de primos, deste modo esta é uma interessante aplicação da matemática no cotidiano.

Este capítulo tem por objetivo desenvolver uma proposta de atividade, com relação a criptografia RSA, voltada para o aperfeiçoamento de professores do ensino básico. Pretendemos mostrar como esse assunto está relacionado com diversos aspectos matemáticos relevantes e apresentar uma proposta de atividade para estimular o professor do ensino básico a criar novas atividades envolvendo criptografia. Assim desenvolvemos a seguinte proposta.

Tema Criptografia RSA e a teoria dos números inteiros.

Objetivos Estudar o desenvolvimento da criptografia ao longo da história, estudar a criptografia RSA, os princípios básicos de aritmética modular (Pequeno Teorema de Fermat, Teorema Chinês dos Restos e Teorema de Euler), bem como alguns métodos de determinação de primalidade/composição de números inteiros. Discutir formas de relacionar alguns conteúdos em matemática com a criptografia.

Conteúdos Relacionados Divisibilidade, fatoração, potenciação e relações de congruência entre números inteiros. Números primos e aritmética modular.

Carga Horária 6 horas/aula.

Recursos Utilizados Quadro e giz, caderno, lápis e borracha.

Metodologia Atividade a ser realizada em 3 etapas, sendo cada etapa desenvolvida da seguinte maneira: inicialmente faz-se um estudo teórico acerca do tema e, em seguida, uma discussão sobre formas de aplicação desse conhecimento em sala de aula.

1ª Etapa - Desenvolvimento Histórico da Criptografia

Utilizaremos como base o Capítulo 1 para o desenvolvimento do Histórico da Criptografia. Assim, introduziremos inicialmente o conceito de criptografia, que é o estudo dos métodos para codificar uma mensagem de tal modo que apenas o destinatário seja capaz de decodificá-la.

Mostrar o Quadrado de Políbio, vide Tabela 1, que foi uma das primeiras formas de transformar o alfabeto em números, neste caso através de uma tabela 5×5. Escrever uma mensagem pequena e criptografá-la através do quadrado de Políbio. Por exemplo, criptografar a mensagem

A matemática é linda

através do Quadrado de Políbio, presente na Tabela 1, obtendo a seguinte mensagem codificada

11 321144153211442413 11 15 3124331411.

Em seguida, estudar a cifra de César, que consiste da translação das letras do alfabeto 3 "unidades", conforme a Tabela 2. Esta cifra, apesar de ser extremamente simples, foi muito utilizada pelo imperador Júlio César na comunicação com os seus generais.

Mostrar que essa cifra pode ser modificada, variando a posição da letra um número diferente de posições. Usar a cifra de César para codificar a mensagem

apesar de simples, a cifra de César mostra-se eficaz.

obtendo a mensagem

dshvdu gh vlpohv, d fliud gh Fhvdu prvwud-vh hilfdc.

Em seguida falar sobre a análise de frequência, estudada pelo árabe Al-Kindi. Explicar que, para cada idioma, existem letras que ocorrem com frequência maior que outras. No português, as letras que repetem com maior frequência são A, O e E, nessa ordem. Retornar às codificações anteriores e verificar se as mesmas são suscetíveis à análise de frequência.

Falar sobre a cifra de Vigenère, que foi um dos primeiros métodos de criptografia polialfabética. Mostrar que esta forma de codificação é imune à análise de frequência. Traduzir a palavra "Criptografia", utilizando como chave automática a letra D, obtendo a mensagem

Fwetmagyydll.

Explicar sobre a criação da criptografia com chave pública (criptografia assimétrica), explicando a maneira de criptografar e assinar digitalmente uma mensagem, conforme a Tabela 7. Comentar brevemente que a criptografia RSA é o método mais utilizado atualmente para a criptografia por chave pública.

Após essa contextualização histórica, questionar os professores sobre quais os conhecimentos matemáticos envolvidos nas criptografia descritas anteriormente. Fazer uma lista com os conhecimentos envolvidos, incluindo por exemplo:

1- Dados em formato de tabela, extração, inserção e interpretação de dados em tabelas. Pode-se criar uma atividade envolvendo a interpretação de dados em tabela, extração de informações e organização de dados em tabelas.

2- Proporção/porcentagem através do estudo da frequência na língua portuguesa. Poderiam ser feitas análises de frequência utilizando textos encontrados em jornais, fazendo a contagem da ocorrência das letras de nosso alfabeto e trabalhando as proporções e porcentagens envolvidas.

Após elencar os conhecimentos relacionados com as criptografias descritas, pedir para os professores criarem práticas envolvendo esses conhecimentos, sempre auxiliando durante essas construções.

2ª Etapa - Criptografia RSA: Como e porquê funciona

Nessa etapa, pretende-se introduzir a criptografia RSA, explicar como se criptografa uma mensagem através dela, bem como desenvolver a matemática necessária para entender porque ela funciona. Para isso usaremos como base o Capítulo 2, mais especificamente utilizaremos as Seções 2.1 e 2.2.

Iniciaremos explicando como funciona a criptografia RSA, da seguinte maneira.

Sejam p e q dois números primos e considere $n = p\,q$ e $\phi(n) = (p-1)(q-1)$. Agora encontramos e inteiro positivo menor que $\phi(n)$, tal que o máximo divisor comum entre e e $\phi(n)$ seja 1. Seja d[1] inteiro positivo menor que $\phi(n)$ tal que

$$d\,e = \phi(n)\,k + 1,$$

para algum k inteiro. Assim obtemos duas chaves, a chave pública (e, n) e a chave privada (d, n).

Primeiramente devemos fazer a pré-codificação, que consiste na transformação do alfabeto em números inteiros positivos colocados lado a lado e, em seguida, dividimos os números em blocos, de tal forma que os blocos sejam menores que n. Para tal devemos ter o cuidado de não permitir blocos iniciando com 0.

Após a pré-codificação, efetuamos a criptografia de fato. Dado um bloco b, calculamos $C(b)$ que é o resto da divisão de b^e por n. Para descriptografar, dado um bloco (criptografado) b calculamos $D(b)$, que é o resto da divisão de b^d por n. Deste modo, reobtemos a mensagem pré-codificada, bastando decodificá-la. Vejamos este método criptográfico no seguinte exemplo:

Consideremos $p = 13$ e $q = 23$, obtendo assim $n = 299$ e $\phi(n) = 264$. Escolhemos $e = 5$ e obtemos $d = 53$, que satisfaz $5 = 264 + 1$. Desta forma temos a chave pública $(5, 299)$ e a chave privada $(53, 299)$. Se desejamos criptografar a palavra "matemática", devemos primeiro efetuar a pré-criptografia. Para tanto, utilizemos o quadro de Políbio da Tabela 1. Assim obtemos a mensagem

$$32 - 114 - 41 - 53 - 211 - 77 - 24 - 13 - 11,$$

já separada em blocos. Agora, para efetuar a criptografia de um bloco b devemos calcular o resto da divisão de b^5 por 299. Assim obtemos a seguinte mensagem criptografada

$$54 - 160 - 279 - 40 - 35 - 246 - 254 - 234 - 189.$$

[1] A existência desse inteiro d satisfazendo tal condição será justificada mais adiante.

Agora vamos fazer a descriptografia, para comprovarmos que recuperamos a mensagem original. Para tal, utilizemos a chave privada $(53, 299)$, obtendo

$$32 - 114 - 41 - 53 - 211 - 77 - 24 - 13 - 11,$$

que decodificando através do Quadro de Políbio reobtemos a palavra "matematica".

Após fazer esse exemplo, inicia-se o desenvolvimento da matemática necessária para responder a seguinte questão: *Porque a criptografia RSA funciona?* Para responder a essa questão, desenvolvemos o Teorema da Fatoração Única, mostrando que todo número inteiro se fatora de maneira única com produto de primos. Construímos as relações de congruência módulo um número inteiro e mostramos os Teoremas de Fermat. Descrevemos a solução de um sistema de congruências

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}, \end{aligned}$$

onde m e n são números inteiros relativamente primos. Definimos a *função de Euler* que a cada inteiro n associa o número de inteiros entre 1 e $n-1$ relativamente primos com ele. Essa função será muito importante para a criptografia RSA. A partir da função de Euler, provamos o Teorema de Euler.

Após o desenvolvimento dos requisitos teóricos para a compreensão total da criptografia RSA, questionaremos os professores sobre os conteúdos que estão relacionados a Criptografia RSA e a sobre uma forma como pode-se utilizá-los em atividades na sala de aula.

Aqui podemos elencar alguns tópicos como:

1- Critérios de divisibilidade de números inteiros.

2- Cálculo do máximo divisor comum através da equação (2.2).

Após discutidos alguns tópicos escolher um deles e desenvolver, com o auxílio dos professores, um plano de ensino.

3ª Etapa - Gerando Números Primos

Para garantirmos a segurança da criptografia RSA, precisamos assegurar que os dois primos p e q escolhidos sejam "bons"de tal forma que impossibilite a fatoração de $n = p\,q$. Para termos certeza da impossibilidade de n ser fatorado, devemos estar atentos aos seguintes quesitos: os números primos p e q devem ser muito grandes, o que para os métodos computacionais atuais significa que eles precisam ter mais de 100 algarismos; esses números primos devem estar "longe"o suficiente um do outro, isto é, deve haver uma diferença de, pelo menos, 5 algarismos entre eles. Isto se faz necessário para evitar uma fatoração pelo método de Fermat.

Assim, para implementar a criptografia RSA devemos ser capazes de gerar primos satisfazendo os quesitos acima. Inicialmente introduziremos os primeiros métodos para

tentar criar números primos, como o método simples de procurar um fator através da divisão sucessiva por todos os números primos entre 2 e a raiz quadrada do número. Depois descreveremos o algoritmo de Fermat, que permite encontrar fatores próximos a raiz quadrada de um inteiro. Em seguida, explicaremos o Crivo de Eratóstenes com o qual se encontra todos os números primos menores que um inteiro fixado.

Após discutir essas primeiras formas de encontrar números primos, vamos estudar os testes de composição e de primalidade que são formas de determinar se um dado número inteiro é composto ou primo, respectivamente. Uma ressalva com relação a esses testes é que eles, apesar de determinarem a primalidade ou composição de um número, não encontram uma fatoração, caso exista.

Introduziremos o teste simples de composição (2.3.1), decorrente do Pequeno Teorema de Fermat, explicando que existem números compostos, chamados pseudoprimos, que não são detectados por esse teste.

Explicaremos o teste de composição de Miller, exibindo alguns números compostos, chamados pseudoprimos fortes, que não são detectados por este teste.

Por fim, explicaremos o teste de primalidade de Lucas, que determina se um dado número é primo. Ao final da exposição teórica, faremos um breve comentário sobre o algoritmo AKS, que é um teste determinístico — determina precisamente se um inteiro é primo ou composto — que é executado em um tempo computacionalmente razoável.

Após a discussão sobre os testes de composição e primalidade, promover uma interação entre os professores afim dos mesmos discutirem métodos de trabalhar com números primos em sala de aula. Proporemos tópicos para serem trabalhados, como por exemplo

1- Números Primos e o teste simples de composição. Compreensão e aplicação deste teste para determinação da fatoração de um número. Neste tópico podemos trabalhar de maneira extensiva conteúdos como divisibilidade/multiplicidade, fatoração e decomposição.

2- Números Primos e o Crivo de Eratóstenes. Neste tópico poderíamos trabalhar a construção do Crivo de Eratóstenes com os alunos, aplicando o crivo para determinar os números primos menores que 100 ou 200, por exemplo. Assim poderíamos trabalhar fortemente com os conceitos de múltiplo, divisor e número primo.

Avaliação

Esta ocorrerá durante todo o processo, acompanhando a participação e o envolvimento dos professores com os tópicos sugeridos, bem como as sugestões de atividades propostas pelos mesmos.

4 Considerações Finais

A criptografia é importante para a comunicação de forma segura, sendo historicamente utilizada desde os gregos. As técnicas de criptografia evoluíram ao longo dos séculos, porém apenas com o surgimento da computação e da internet fez-se necessária uma mudança maior no modo de criptografar. Dessa necessidade surgiu o sistema de criptografia com chave pública e, posteriormente, foi desenvolvida a criptografia RSA, que é a criptografia assimétrica mais utilizada no mundo.

A criptografia RSA está apoiada na teoria dos números inteiros, que foi desenvolvida por grandes matemáticos como Fermat e Euler. E a segurança desse método está intimamente ligada ao fato de não existir algoritmo de fatoração eficiente.

No estudo dos métodos de criptografia, em especial a criptografia RSA, fica clara a relação destes com vários tópicos da escola básica. Portanto mostra-se muito interessante fazer uma atividade de aperfeiçoamento com os professores, afim de agregar novos conhecimentos para os mesmos e estimular a discussão sobre outras formas de desenvolver determinados conteúdos.

A realização deste trabalho mostrou-se muito interessante, haja visto que este era um tópico que sempre tive vontade de explorar. Trabalhar na criptografia RSA, me fez revisar conteúdos fantásticos como a aritmética modular, os Teoremas de Fermat e de Euler. Eu gostaria de ter desenvolvido o algoritmo AKS, que é um algoritmo determinístico de primalidade com tempo polinomial, porém para isto necessitaríamos desenvolver muitos outros conceitos em matemática, como por exemplo: anéis, ideais, grupos, subgrupos, entre outros.

Através de uma proposta como esta, podemos incentivar o professor de matemática da escola básica a proporem atividades, tanto em classe, como elemento motivador da aprendizagem, quanto em extra-classe, para alunos que demonstrem maior curiosidade em explorar os conceitos discutidos em sala de aula. É possível aprofundar os conceitos de divisibilidade, fatoração em primos, aritmética modular, etc, com alunos da escola básica e, neste sentido, a criptografia se mostra adequada como elemento motivador, visto que atualmente quase todas as pessoas usam ferramentas digitais para troca de mensagens sigilosas e, portanto, a criptografia está presente no dia a dia das pessoas.

Referências

AGRAWAL, M.; KAYAL, N.; SAXENA, N. Primes is in P. *Ann. of Math. (2)*, v. 160, n. 2, p. 781–793, 2004. ISSN 0003-486X. Disponível em: ⟨dx.doi.org/10.4007/annals.2004.160.781⟩. Citado na página 49.

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. Rio de Janeiro: IMPA/SBM, 1997. 195 p. (Série de Computação e Matemática, 2). ISBN 85-244-0124-9. Citado 9 vezes nas páginas 21, 27, 28, 31, 33, 39, 40, 41 e 46.

DIFFIE, W.; HELLMAN, M. E. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22, n. 6, p. 644–654, 1976. ISSN 0018-9448. Citado 2 vezes nas páginas 19 e 25.

JAESCHKE, G. On strong pseudoprimes to several bases. *Math. Comp.*, v. 61, n. 204, p. 915–926, 1993. ISSN 0025-5718. Disponível em: ⟨dx.doi.org/10.2307/2153262⟩. Citado na página 48.

OCHEM, P.; RAO, M. Odd perfect numbers are greater than 10^{1500}. *Math. Comp.*, v. 81, n. 279, p. 1869–1877, 2012. ISSN 0025-5718. Disponível em: ⟨http://dx.doi.org/10.1090/S0025-5718-2012-02563-4⟩. Citado na página 42.

POMERANCE, C.; SELFRIDGE, J. L.; WAGSTAFF JR., S. S. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.*, v. 35, n. 151, p. 1003–1026, 1980. ISSN 0025-5718. Disponível em: ⟨dx.doi.org/10.2307/2006210⟩. Citado na página 48.

QUARESMA, P.; PINHO, A. Análise de frequências da língua portuguesa. In: *Conferência Ibero-Americana InterTIC 2007*. Porto, Portugal: IASK, 2007. p. 267–272. Citado na página 22.

RIBENBOIM, P. *The book of prime number records*. Second. Springer-Verlag, New York, 1989. xxiv+479 p. ISBN 0-387-97042-8. Disponível em: ⟨dx.doi.org/10.1007/978-1-4684-0507-1⟩. Citado na página 40.

RIVEST, R. L.; SHAMIR, A.; ADLEMAN, L. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, v. 21, n. 2, p. 120–126, 1978. ISSN 0001-0782. Disponível em: ⟨dx.doi.org/10.1145/359340.359342⟩. Citado na página 19.

WIKIPÉDIA. *Criptoanálise — Wikipédia, a enciclopédia livre*. 2014. Acessado em 14-novembro-2014. Disponível em: ⟨pt.wikipedia.org/w/index.php?title=Criptoan%C3%A1lise&oldid=40174471⟩. Citado na página 21.

WIKIPÉDIA. *Número perfeito — Wikipédia, a enciclopédia livre*. 2014. Acessado em 14-novembro-2014. Disponível em: ⟨pt.wikipedia.org/w/index.php?title=N%C3%BAmero_perfeito&oldid=38801838⟩. Citado na página 41.