UFES

SBM
Sociedade Brasileira de Matemática

PROFMAT

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO - UFES
SOCIEDADE BRASILEIRA DE MATEMÁTICA - SBM
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

KAYODÊ DAVID DE MELO SOUZA

CRIPTOGRAFIA RSA:

Um minicurso para o Ensino Médio

VITÓRIA - ESPÍRITO SANTO
DEZEMBRO DE 2020

KAYODÊ DAVID DE MELO SOUZA

CRIPTOGRAFIA RSA:
Um minicurso para o Ensino Médio

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFES como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Florêncio Ferreira Guimarães Filho

VITÓRIA - ESPÍRITO SANTO
DEZEMBRO DE 2020

CRIPTOGRAFIA RSA:
Um minicurso para o Ensino Médio

Kayodê David de Melo Souza

Dissertação de Mestrado apresentada à Comissão Acadêmica Institucional do PROFMAT-UFES como requisito parcial para obtenção do título de Mestre em Matemática, aprovada em 04 de Dezembro de 2020.

Banca Examinadora:

Prof. Dr. Florêncio Ferreira Guimarães Filho (Orientador)
UFES

Prof. Dr. Moacir Rosado Filho
UFES

Prof. Dr. Fidelis Zanetti de Castro
IFES

AGRADECIMENTOS

Agradeço primeiramente as pessoas que participaram ativamente na realização deste sublime trabalho: minha esposa Priscilla, meu amigo Vitor e minha amiga Aline. Sem a ajuda, incentivo e a paciência de vocês não seria possível.

Agradeço aos professor do PROFMAT-UFES, principalmente ao professor Florêncio, meu orientador, que cedeu seu tempo por diversas vezes ao longo do programa para transmitir seus conhecimentos mesmo em fins de semana e período de férias.

Agradeço a todos os meus colegas da turma 2017/1, pois o companheirismo prevaleceu tornando o ambiente de estudos agradável.

Desejo sinceramente manifestar essa gratidão retribuindo da mesma maneira em todo lugar em que eu for.

RESUMO

O presente trabalho refere-se a elaboração de uma sequência didática sobre Criptografia RSA e o seu funcionamento, apresentando uma contextualização do tema e sua importância objetivando estimular o interesse em aprender Matemática. Abordamos os principais conceitos da Teoria dos Números como divisibilidade, números primos e aritmética modular de modo que não seja necessário um pré-requisito para compreender o desenvolvimento deste trabalho. Apresentamos passo a passo o processo de encriptação e desencriptação de uma mensagem na internet fazendo a utilização de recursos digitais que facilitem o entendimento. A importância do tema e sua escolha se justificam pelo fato do RSA ser o método mais simples e extremamente eficiente utilizado nas operações cotidianas de usuário de internet como enviar e-mail, realizar transações bancárias ou efetuar compras on-line.

Palavras chave: Criptografia. Criptografia RSA. Teoria dos números. Internet.

ABSTRACT

The present text explores the creation of a teaching sequence about RSA Cryptography and its operations, showing a contextualization of the theme and its importance in the goal of stimulating the interest in learning math. We have covered main concepts from Number Theory as divisibility, prime numbers and modular arithmetic in a way that no pre-requisites are required in order to understand the development of this text. We present, step by step, the process of encrypting and decrypting a message on the internet while making use of digital resources to facilitate the understanding of the algorithm. The choice of the theme is justified by the fact that the RSA method is the simplest and extremely efficient, used in daily life operations on the internet like sending an email, making bank transfers and shopping online.
Keyowrds: Cryptography. RSA Cryptography. Number Theory. Internet.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O RSA é um sistema de criptografia onde a chave de encriptação é pública e diferente da chave de desencriptação. Ele é o sistema mais utilizado no mundo. É ele que garante a segurança das nossas compras na internet. Neste trabalho, buscamos uma forma de apresentá-lo ao aluno do ensino básico como amostra de uma aplicação da matemática no cotidiano de todos nós, que é um dos maiores anseios da geração estudantil atual.

Obviamente não estou dizendo que a matemática deva ser tratada somente dessa maneira. Existe um charme em conseguir encontrar a solução de um problema de matemática do tipo "demonstre" ou "prove que" que parece ser cada vez mais difícil de apresentar em uma sala de aula com 35 alunos, por exemplo.

Paralelamente, surgem no cenário da educação escolas de tempo integral que oferecem disciplinas eletivas. Ao mesmo tempo, Institutos Federais vêm oferecendo cada vez mais cursos que atendam seus alunos de maneira remota e, eventualmente, alunos (e professores) de outras redes (pública e privada).

> No ensino da Matemática, destacam-se dois aspectos básicos: um consiste em relacionar observações do mundo real com representações (esquemas, tabelas, figuras); outro consiste em relacionar essas representações com princípios e conceitos matemáticos. Nesse processo, a comunicação tem grande importância e deve ser estimulada, levando-se o aluno a falar e a escrever sobre Matemática. [...] O significado da Matemática para o aluno resulta das conexões que ele estabelece entre ela e as demais disciplinas, entre ela e seu cotidiano e das conexões que ele estabelece entre os diferentes temas matemáticos. (BRASIL, 2007, p.19).

Dessa forma, elaboramos uma sequência didática sobre criptografia RSA que possa ser oferecida como eletiva ou minicurso nas escolas de ensino básico. Sequencias didáticas, como o nome já diz, são etapas continuadas de um tema com o objetivo de ensinar um conteúdo.

A criptografia RSA é uma aplicação interessante do curso elementar de teoria dos números. Assim sendo, vamos abordar tópicos de Aritmética (disciplina obrigatória do PROFMAT) de modo que possamos compreender a matemática por trás da criptografia RSA.

Escolhi o tema, dentre todos oferecidos durante o programa de mestrado, por acreditar que seja o mais apropriado para ser encaixado em uma sequência didática para o ensino básico. É possível ministrar os conteúdos sem que o professor deixe um excesso de perguntas não respondidas (como acontece em minicursos sobre Cálculo).

É importante ressaltar que este trabalho versa sobre a matemática por trás da criptografia RSA, não iremos tratar de elementos da programação ou como encontrar informações escondidas na internet.

Ao longo deste trabalho, tentaremos sintetizar o máximo possível os conteúdos da teoria dos números sem deixar de demonstrar, exemplificar e propor exercícios que atendam as expectativas daqueles que gostam da matemática.

Afim de enriquecer este minicurso, utilizamos como base os livros da Sociedade Brasileira de Matemática (SBM), que também podem (e devem) ser utilizados como complemento deste trabalho em caso de aplicação do mesmo.

2 CRIPTOGRAFIA

A palavra *criptografia*, do grego *cryptus*, significa secreto, oculto. Ou seja, em essência significa "escrita oculta". Ao longo da história da civilização, os homens usavam códigos secretos para transmitir suas mensagens de modo que, em caso de interceptação, elas não pudessem ser interpretadas.

> Criptografia é um assunto tão antigo quanto a civilização humana. Ao longo da história, os homens inventaram códigos secretos na tentativa de transmitir mensagens que não poderiam ser inteligíveis por um interceptador. A história mostra que construir tais códigos é um problema muito difícil e que todos eventualmente sucumbem a uma análise inteligente. (ROUSSEAU, 2015, p 224.).

Ao falar de criptografia nos tempos atuais, lembramos imediatamente de Alan Turing, principalmente após a exibição do filme O Jogo da Imitação em 2014, que conta um pouco de sua história.

Em 1939, Turing ingressou voluntariamente em programa secreto britânico durante a Segunda Guerra Mundial. Acontece que, naquela época, os nazistas usavam uma máquina automatizada com criptografia chamada Enigma. Turing, que ao longo da sua vida sempre se mostrou interessado por criptografia, ingressou no programa desafiando-se a decodificar mensagens secretas nazistas. Turing criou outra máquina, capaz de testar rapidamente combinações para obter a chave de decifração das mensagens geradas pelo dispositivo alemão.

Figura 1 – O Jogo da Imitação: cinebiografia de Alan Turing

Fonte: https://pt.wikipedia.org/wiki/O_Jogo_da_Imitação.

Por diversas vezes, desde 2015, a justiça brasileira solicitou o bloqueio do aplicativo WhatsApp. Aparentemente a decisão foi tomada pois o aplicativo se recusou a dar informações (quebrando o sigilo dos usuários) sobre um inquérito policial. O que esqueceram de avisar a justiça brasileira é que o WhatsApp usa uma **criptografia de ponta a ponta**, ou seja, nem mesmo o aplicativo tem acesso as mensagens trocadas pelos usuários. A única maneira de se obter informações sobre o diálogo trocado entre os usuários é tendo acesso a um dos telefones.

Figura 2 – Bloqueio do WhatsApp em todo Brasil

Justiça determina bloqueio do WhatsApp em todo o Brasil por 48 horas

Justin Sullivan/Getty Images/AFP

Além de troca de mensagens, Whatsapp também permite chamadas telefônicas via internet

JULIO WIZIACK
DE SÃO PAULO

Fonte: http://gazetaweb.globo.com/portal/noticia.php?c=1016

O Governo do Espírito Santo anunciou no final de 2018 um investimento de 32 milhões de reais para interceptar mensagens de criminosos no WhatsApp. Com o que foi discutido acima, sabemos que não passou de uma jogada de marketing político, visto que, não é possível interceptar essas mensagens.

O fato é que, se por um lado a criptografia tem dificultado o trabalho das autoridades, também é ela que nos da segurança para conversar na internet e efetuar compras online.

3 CIFRAGEM DE CHAVE PÚBLICA

Quando desejamos realizar uma compra na internet, basta que informemos os dados do nosso cartão de crédito (número, validade e código de segurança) e a compra estará autorizada. Ou seja, qualquer pessoa com essas informações pode realizar a compra com o seu cartão. Evidentemente que, em caso de roubo, você imediatamente cancelaria seu cartão evitando problemas futuros. Porém, o que garante que seus dados chegarão a loja de maneira segura? Muita gente não confia em realizar compras na internet justamente por isso. Para realizar uma compra virtual, seu computador precisa enviar de maneira extremamente segura as informações até a loja de modo que, em caso de interceptação, essa mensagem não possa ser compreendida pelo interceptador. Entretanto o trabalho para codificar e manter a chave de decodificação segura seria desestimulador para qualquer comprador online

Foi então que Whitfield Driffie, um matemático e criptógrafo estadunidense, pioneiro em criptografia de chave pública, teve a ideia de um sistema com chaves assimétricas, sendo uma pública (para cifragem) e uma privada para decifrar as informações. A cifragem deveria ser um processo fácil de fazer usando a chave pública ao passo que a decifragem deveria ser quase impossível sem a chave secreta (que somente o remetente teria).

> Os benefícios de sistemas de criptografia de chave pública são bastante claros. Para que duas pessoas se comuniquem usando um sistema de criptografia, ambas precisam saber os detalhes do sistema: é a troca de detalhes do sistema, onde o perigo de intersectação é maior. Entretanto, no caso de criptografia de chave pública, este perigo não existe: o sistema inteiro é público! Tal sistema é efetivamente a única abordagem que pode funcionar quando há milhões de usuários finais, quando são enviadas informações de cartões de crédito pela internet, por exemplo.(ROUSSEAU, 2015, p 225.)

Driffie não conseguiu implementar sua ideia na prática, mas a publicou para que outros pudessem resolver o problema.

4 O SISTEMA RSA

Ronald **R**ivest, Adi **S**hamir e Leonard **A**dleman, do Massachusetts Institute of Technology (MIT), foram os responsáveis pela implementação do primeiro sistema de criptografia com chave pública. O nome RSA é uma homenagem aos seus inventores. Esse sistema foi implementado em 1978 e hoje, 41 anos depois, ainda é um dos sistemas mais seguros do mundo.

O RSA é baseado em teoria dos números básica. Tais conexões serão estudadas nos capítulos seguintes.

Três propriedades simples, bastante conhecidas, garantem a eficiência do sistema.

*É difícil para um computador fatorar um número com cerca de 600 dígitos.

*É fácil para um computador construir primos com cerca de 600 dígitos.

*É fácil para um computador decidir se um número (mesmo com 600 dígitos) é primo.

De maneira resumida, o RSA funciona da seguinte maneira:

Escolhemos dois números primos p e q e calculamos o seu produto $n = p \cdot q$

Usamos n para codificar a mensagem (n pode ser tornado público);

Usamos p e q para decodificar a mensagem (esses precisam ser mantidos em segredo).

Ou seja, para quebrar um código criptografado basta decompor o número n em fatores primos.

Você pode questionar a eficiência do RSA devido a simplicidade do sistema. Porém, simples não significa fácil. Por exemplo, uma chave pública RSA tem cerca de 600 dígitos. Logo, para quebrar o código seria necessário encontrar um número primo de aproximadamente 300 dígitos.

Para você ter uma ideia, o computador no qual está sendo escrito este trabalho encontra um milhão de números primos a cada 2 segundos. Uau, que veloz, você pode pensar. Entretanto, com uma simples regra de 3, você concluiria que neste computador levaríamos cerca de $2 \cdot 10^{296}$ segundos. Se isso ainda não parece assustador, refaça os cálculos e veja que isso é o equivalente a aproximadamente 10^{291} anos.

Evidentemente que este computador não é nem cogitado como uma possível ameaça para o RSA, mas mesmo os computadores quânticos ainda não são uma ameaça para esse sistema.

5 ALGUNS TÓPICOS DA TEORIA DOS NÚMEROS

O algoritmo RSA é uma aplicação das propriedades dos números inteiros, que por sua vez é o objeto central da teoria dos números. Portanto, nos capítulos seguintes, apresentaremos algumas ferramentas que julgamos essenciais para compreender o funcionamento do RSA.

5.1 DIVISIBILIDADE

Sejam a e b números inteiros. Dizemos que a divide b se existir um inteiro k tal que $b = ak$. As frases "a é divisor de b", "b é divisível por a"e "b é múltiplo de a"têm o mesmo significado que a divide b.

Usaremos a notação $a \mid b$ para representar as frases ditas anteriormente. Em caso negativo usa-se $a \nmid b$.

Por exemplo, $7 \mid 35$ pois $35 = 7.5$. Por outro lado, $6 \nmid 35$, pois não existe um inteiro k tal que $35 = 6k$.

Proposição 5.1. *Sejam $a, b, c \in \mathbb{Z}$. Então*

(a) Se $a \mid b$ e $b \mid c$ então $a \mid c$

(b) Se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$

(c) Se $a \mid b$ e $c \mid d$ então $ac \mid bd$

Demonstração:

(a) Como $a \mid b$ então existe um inteiro k_1 tal que:

$$b = a \cdot k_1 \qquad (1)$$

Como $b \mid c$ então existe um inteiro k_2 tal que:

$$c = b \cdot k_2 \qquad (2)$$

Substituindo (1) em (2), obtemos

$$c = a \cdot k_1 \cdot k_2 = a \cdot k$$

Portanto, a divide c.

(b) Como $a \mid b$ e $a \mid c$ então existem inteiros k_1 e k_2 tais que $b = a \cdot k_1$ e $c = a \cdot k_2$. Logo

$$b + c = a \cdot k_1 + a \cdot k_2 = a \cdot (k_1 + k_2) =$$

Portanto $a \mid (b + c)$.

(c) Como $a \mid b$ e $c \mid d$ então existem inteiros k_1 e k_2 tais que $b = a \cdot k_1$ e $d = c \cdot k_2$. Logo

$$bd = (a \cdot k_1) \cdot (c \cdot k_2) = (ac) \cdot (k_1 k_2)$$

Portanto $ac \mid bd$.

(Divisão Euclidiana). Dados dois inteiros a e b, sendo a positivo, existem inteiros q e r, unicamente determinados, tais que

$$b = aq + r, \text{ com } 0 \leqslant r < a$$

Exemplo 5.1: O número N deixa resto 8 na divisão por 20. Qual é o resto da divisão de N por 5?

Solução: Segue pela divisão euclidiana que $N = 20q + 8$.

Como 20 é múltiplo de 5 e $8 = 5 + 3$, podemos reescrever N como

$$N = (5 \cdot 4)q + 5 + 3 = 5(4q + 1) + 3 = 5q_1 + 3$$

Portanto o resto da divisão de N por 5 é 3.

Exemplo 5.2: Encontre os inteiros $a \geq 1$ tal que $a + 2 \mid a^4 + 2$.

Solução: Basta observar que $a^4 + 2 = a^4 - 16 + 18 = (a^2 - 4)(a^2 + 4) + 18 = (a + 2)(a - 2)(a^2 + 4) + 18$. Portanto, basta encontrar todos os inteiros $a \geq 1$ tal que $a + 2 \mid 18$. Como $D_{18} = \{1, 2, 3, 6, 9, 18\}$, então $a = 1$, $a = 4$, $a = 7$ ou $a = 16$.

5.2 MÁXIMO DIVISOR COMUM

Este conceito, pouco utilizado após o 6º ano, é extremamente elegante e repleto de aplicações interessantes. Vale a pena tal conteúdo ser mais explorado pelos professores de matemática.

Definição: Sejam a e b inteiros diferentes de zero. O máximo divisor comum (mdc) de a e b é um número d positivo tal que:

(i) d é um divisor comum de a e b, ou seja, $d \mid a$ e $d \mid b$;

(ii) Se c é um divisor comum de a e b, então $c \mid d$.

O mdc de a e b, será denotado por (a, b).

No Ensino Fundamental define-se o mdc de dois números a e b como o maior elemento do conjunto dos divisores de a e b. Entretanto, essa definição não valida imediatamente a propriedade (ii), porém a unicidade é imediata pois se d e d' são números positivos que obedecem as condições i e ii então $d \mid d'$ e $d' \mid d$, portanto $d = d'$. Como (a, b) é o divisor comum de a e b, que é múltiplo de todos os divisores comuns de a e b, então (a, b) é o maior dos divisores comuns de a e b, já que (a, b) é múltiplo do maior dos divisores comuns de a e b. Assim, a definição de máximo divisor comum, adotada no Ensino Fundamental, como sendo o maior dos divisores comuns de a e b equivale à definição aqui adotada, no sentido de que ambas geram o mesmo número. Por outro lado, a definição dada acima nos condiciona a demonstrar que o mdc sempre existe, o que faremos mais à frente.

Um caso simples de existência é dado quando um divide o outro.

Proposição 5.2. *Sejam a e b inteiros positivos tal que $a \mid b$. Então (a, b) existe e $(a, b) = a$*

Demonstração: Basta analisar sob a ótica da definição de mdc, ou seja:

(i) $a \mid a$ e $a \mid b$

(ii) Se $c \mid a$ e $c \mid b$, então $c \mid a$.

Por exemplo, o mdc de 24 e 36, ou simplesmente $(24, 36)$ é $d = 12$, vejamos:

Os divisores de 24 são:

$$D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$$

Já os divisores de 36 são:

$$D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

Os divisores comuns de 24 e 36 são:

$$D_{24,36} = \{1, 2, 3, 4, 6, 12\}$$

Dentre os divisores comuns de 24 e 36, aquele que é divisível por todos os outros divisores é o 12, o maior deles.

Já o mdc entre 5 e 9, ou simplesmente $(5, 9)$ é 1, pois $D_{5,9} = \{1\}$.

Quando o mdc entre dois números a e b for igual a 1 diremos que eles são primos entre si.

Proposição 5.3. *Sejam $a, b, n \in \mathbb{Z}$. Se $(a, b - na)$ existe, então (a, b) existe e*

$$(a, b) = (a, b - na)$$

Demonstração: Seja $d = (a, b - na)$, logo $d \mid a$ e $d \mid (b - na)$. Pelo item (a) da proposição 5.1 temos que $d \mid na$. E pelo item (b) $d \mid (b - na + na) = b$. Portanto $d \mid a$ e $d \mid b$. Considere agora c um divisor comum de a e b. Então $c \mid (b - na)$. Como $c \mid a$ e $c \mid b - na$ pelo item (ii) da definição de mdc $c \mid d$. Portanto $d = (a, b)$

Exemplo 5.3: Mostre que para todo n natural, é irredutível a fração

$$\frac{21n + 4}{14n + 3}$$

Solução: Para que a fração seja irredutível devemos ter $(21n + 4, 14n + 3) = 1$. Usando a proposição 5.3 temos que $(21n + 4, 14n + 3) = (21n + 4 - 14n - 3, 14n + 3) = (7n + 1, 14n + 3) = (7n + 1, 14n + 3 - 2 \cdot (7n + 1)) = (7n + 1, 1) = 1$.

Exemplo 5.4: Mostre que $4k + 3$ e $5k + 4$ são primos entre si para todo inteiro k.

Solução: Usando a proposição 5.3 temos que $(5k+4, 4k+3) = (5k+4-4k-3, 4k+3) = (k + 1, 4k + 3) = (k + 1, 4k + 3 - 3 \cdot (k + 1)) = (k + 1, k) = (k + 1 - k, k) = (1, k) = 1$

5.3 O ALGORITMO DE EUCLIDES

Sejam a e b dois inteiros positivos com $a \geq b$. Divida b por a; chamamos de q_1 o quociente desta divisão e r_1 o resto, de forma que:

$$b = aq_1 + r_1, \qquad 0 \leq r_1 < b$$

Neste caso temos duas possibilidades:

1) Se $r_1 \mid a$, pela proposição 5.3 sabemos que $(a, b) = (a, r_1) = (a, b - aq_1) = r_1$

2) Se $r_1 \nmid a$ então podemos efetuar a divisão euclidiana de a por r_1

$$a = r_1q_2 + r_2 \qquad 0 \leq r_2 < r_1$$

Novamente temos duas possibilidades

1) Se $r_2 \mid r_1$, pela proposição 5.3

$$(a, b) = (a, r_1) = (r_1, a - r_1q_2) = (r_1, r_2) = r_2$$

2) Se $r_2 \nmid r_1$, podemos efetuar a divisão de r_1 por r_2.

Efetuando sucessivamente a divisão euclidiana obteremos

$$r_{n-1} = r_nq_{n+1} + r_{n+1}. \qquad 0 \leq r_{n+1} < r_n$$

O fato da sequência r_i ser estritamente decrescente garante que existe um inteiro n tal que $r_{n+1} = 0$, ou seja, $r_{n-1} = r_nq_{n+1}$, logo $r_n \mid r_{n-1}$ e ocorrerá a existência e portanto $r_n = (a, b)$

Proposição 5.4. *(Teorema de Bézout). Se $d = (a, b)$ então existem inteiros x e $y \in \mathbb{Z}$ tais que $d = ax + by$.*

Demonstração: Pelo Algoritmo de Euclides temos que $d = r_n$. Como $r_{n-2} = q_n r_{n-1} + r_n$,

$$r_n = r_{n-2} - q_n r_{n-1}$$

Podemos agora substituir $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$ e a equação acima torna-se

$$r_n = r_{n-2}(1 + q_{n-1} q_n) - q_n r_{n-3}$$

Continuando essas substituições repetidas vezes, chegaremos em $r_n = r_1 x_1 + r_2 y_2$, com x_1, y_1 inteiros.

Substituindo $r_2 = b - r_1 q_2$ obteremos

$$r_n = r_1(x_1 - q_2 y_1) + b y_1$$

Por fim, basta substituir $r_1 = a - b q_1$, obtendo finalmente

$$r_n = d = a(x_1 - q_2 y_1) + b(-q_1 x_1 + q_1 q_2 y_1 + y_1) = ax + by$$

Onde $x = x_1 - q_2 y_1$ e $y = -q x_1 + q_1 q_2 y_1 + y_1$

O Teorema de Bézout nos permite incluir propriedades importantes do mdc.

(iii) *Considere $a, b, n \in \mathbb{N}$. Temos que*

$$(na, nb) = n(a, b)$$

Sejam $d = (a, b)$ e $d' = (na, nb)$. Pelo Teorema de Bézout, existem $x, y \in \mathbb{Z}$ tais que $ax + by = d$. Multiplicando ambos os membros da última equação por n, teremos:

$$nax + nby = nd$$

Como $d' \mid na$ e $d' \mid nb$ então $d' \mid nd$.

Por outro lado, como $d \mid a$ e $d \mid b$ então $nd \mid na$ e $nd \mid nb$, logo $nd \mid d'$.

Se $d' \mid nd$ e $nd \mid d'$ então $nd = d'$.

(iv) *Dados a, $b \in \mathbb{Z}$, ambos não nulos, temos que:*

$$\left(\frac{a}{(a, b)}, \frac{b}{(a, b)} \right) = 1$$

Usando o item (iii) teremos

$$(a,b)\cdot\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=\left((a,b)\cdot\frac{a}{(a,b)},(a,b)\cdot\frac{b}{(a,b)}\right)=(a,b)$$

(v) *(Lema de Gauss) Considere* $a,b,c\in\mathbb{N}$. *Se* $c\mid ab$ *e* $(c,b)=1$ *então* $c\mid a$

Como $c\mid ab$, então existe $k\in\mathbb{Z}$ tal que $ab=ck$.

Além disso, pelo Teorema de Bézout, temos

$$cx+by=1$$

Multiplicando ambos os lados da equação por a teremos

$$acx+aby=a$$

Substituindo $ab=ck$ na equação acima obtemos

$$acx+cky=c(ax+ky)=a$$

Portanto, $c\mid a$.

5.3.1 MÍNIMO MÚLTIPLO COMUM

Para este trabalho nos basta conhecer a notação de mmc e seu significado. Portanto, iremos nos abster de nos aprofundar em suas propriedades.

Definição: Sejam a e b inteiros diferentes de zero. O mínimo múltiplo comum entre a e b é o inteiro positivo m tal que:

(i) m é um múltiplo comum de a e b, isto é, $a\mid m$ e $b\mid m$;

(ii) Se c é um múltiplo de a e b, então $m\mid c$.

O item (ii) nos dá que o m é o menor elemento do conjunto dos múltiplos de a e b e ele é único. Suponha que m e m' sejam mínimos múltiplos comum de a e b, então, pelo item (ii), $m\mid m'$ e $m'\mid m$. Como m e m' são inteiros positivos, temos $m=m'$.

Denotaremos o mínimo múltiplo comum de a e b por $[a,b]$.

Como $|ab|$ é múltiplo comum positivo de a e b, então existe o menor múltiplo comum positivo de a e b, digamos m_0. Então, $m_0>0$, m_0 é múltiplo comum de a e b, e se c é um múltiplo comum positivo de a e b, então m_0c. Como m_0 é múltiplo comum de a e b, então m_0 satisfaz a condição (i) da definição de $[a,b]$. Agora, seja c um múltiplo comum de a e b. Pelo Algoritmo da Divisão Euclidiana, existem inteiros q e r tais que $c=qm_0+r$ e $0r<m_0$. Como c e m_0 são múltiplos comuns de a e b, então $r=c-qm_0$ é múltiplo comum de a e b. Como $0\leq r<m_0$, r é múltiplo comum de a e b, e m_0 é o menor múltiplo comum positivo de a e b, então $r=0$ e, portanto, $c=qm_0$, sendo, portanto, m_0 divisor c.

Assim, m_0 satisfaz a condição (ii) da definição de $[a, b]$. Conclui-se, assim, que o menor múltiplo comum positivo de a e b é igual a $[a, b]$. Em particular, isso mostra a existência de $[a, b]$. Portanto, a definição do Ensino Fundamental para o mínimo múltiplo comum de a e b como sendo o menor múltiplo comum positivo de a e b equivale à definição aqui adotada, pois geram o mesmo número.

Por exemplo, $[4, 6] = 12$. Vejamos, os múltiplos de 4 são $\{0, \pm4, \pm8, \pm12, \pm16, \pm20, \pm24...\}$, os múltiplos de 6 são $\{0, \pm6, \pm12, \pm18, \pm24, \dots\}$. Os múltiplos comuns de 4 e 6 são $\{0, \pm12, \pm24, \dots\}$. De fato, 12 é o menor múltiplo comum positivo de 4 e 6, e é o múltiplo comum positivo de 4 e 6, que divide todos os múltiplos comuns de 4 e 6.

É fácil mostrar que $[a, b] = [-a, b] = [a, -b] = [-a - b]$, portanto vamos supor a e b sempre não negativos.

Proposição 5.5. *Dados a, b e c, inteiros não negativos. então*

$$[ca, cb] = c[a, b]$$

Demonstração: Observe que $c[a, b]$ é múltiplo de ca e cb, logo

$$[ca, cb] \leq c[a, b]$$

.

Por outro lado, $[ca, cb] = r \cdot ca = s \cdot cb$. Logo $\frac{[ca,cb]}{c} = ra = sb$ é múltiplo de a e b. Isso significa que

$$[a, b] \leq \frac{[ca, cb]}{c} \iff c[a, b] \leq [ca, cb]$$

.

Como $c[a, b] \leq [ca, cb] \leq c[a, b]$, então $[ca, cb] = c[a, b]$.

Proposição 5.6. *Dados dois números inteiros a e b, temos que*

$$[a, b] \cdot (a, b) = ab$$

Demonstração: Dividiremos em dois casos: $(a, b) = 1$ e $(a, b) > 1$.

Caso (a,b)=1: Pela definição mmc, sabemos que $b \mid [a, b]$ e $[a, b] = an$, com $n \in \mathbb{N}$, logo $b \mid an$. Como $(a, b) = 1$, temos que $b \mid n$, portanto $b \leq n$. Como estamos supontando a e b não negativos, podemos multiplicar ambos os membros da última desigualdade por a e obter

$$ab \leq an = [a, b]$$

.

Por outro lado, pela definição de mmc, vale que

$$[a, b] \leq ab$$

.

Se $ab \leq [a,b] \leq ab$, então $ab = [a,b]$. Como $(a,b) = 1$. podemos concluir que $ab = [a,b] \cdot 1 = [a,b] \cdot (a,b)$.

Caso (a,b)>1: Sabemos que $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$. Usando o resultado do caso anterior, vale que

$$\frac{a}{(a,b)} \cdot \frac{b}{(a,b)} = \left[\frac{a}{(a,b)}, \frac{b}{(a,b)}\right] \cdot \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$$

.

Multiplicando ambos os membros da última igualdade por $(a,b)^2$ teremos:

$$(a,b)^2 \cdot \frac{a}{(a,b)}\frac{b}{(a,b)} = (a,b)\left[\frac{a}{(a,b)}, \frac{b}{(a,b)}\right] \cdot (a,b)\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right)$$

$$ab = [a,b] \cdot (a,b)$$

.

Exemplo 5.5: Resolva o sistema de equações

$$\begin{cases} (x,y) = 6 \\ [x,y] = 60 \end{cases}$$

Solução: Usando a proposição 5.6 teremos $xy = [x,y] \cdot (x,y) = 6 \cdot 60 = 360$. Como x e y são múltiplos de 6 e divisores de 60, as possíveis soluções são: $x, y, \in \{6, 12, 30, 60\}$.

Portanto, as possíveis soluções que satisfazem a condição $xy = 360$ são $x = 6$ e $y = 60$; $x = 12$ e $y = 30$; $x = 30$ e $y = 12$ ou $x = 60$ e $y = 6$.

5.4 EQUAÇÕES DIOFANTINAS

Por diversas vezes nos deparamos com problemas cuja solução é um par ordenado de uma equação do tipo

$$ax + by = c$$

Esse conceito é trabalho no ensino básico em temas como: equações do primeiro grau com duas incógnitas, sistemas de equações do primeiro grau, função polinomial do primeiro grau, etc..

Entretanto, por diversas vezes, nossas soluções se restringem ao conjunto dos números inteiros em equações com coeficientes inteiros. Ou seja, quando a, b e c são números inteiros, chamamos essas equações de *Equações Diofantinas* em homenagem a Diofanto da Alexandrina (aprox. 300d.C).

Para tanto, precisamos estabelecer condições tais que esse tipo de equação admita solução inteira. Apresentamos essas condições a seguir.

Proposição 5.7. *A equação $ax + by = c$ com $a, b, c \in Z$, com $a \neq 0$ e $b \neq 0$, tem solução se, e somente se, $d \mid c$, onde $d = (a, b)$*

Demonstração:

(Ida) Considere que o par (x_0, y_0) é uma solução da equação $ax + by = c$. Logo, $ax_0 + by_0 = c$. Por outro lado, como $d = (a, b)$ podemos escrever $a = dk_1$ e $b = dk_2$ e assim obtemos:

$$dk_1x_0 + dk_2y_0 = d(k_1y_0 + k_2y_0) = c$$

Portanto $d \mid c$

(Volta) Suponha agora que $d \mid c$, ou seja $c = dk$. Usando que $d = (a, b)$ podemos escrever d como $d = ax_0 + by_0$ (Teorema de Bézout). Multiplicando ambos os lados da última igualdade po k obtemos

$$ax_0k + by_0k = dk = c$$

Logo, o par (kx_0, ky_0) é solução da equação diofantina $ax + by = c$

Proposição 5.8. *Seja (x_0, y_0) uma solução da equação $ax + by = c$, onde $(a, b) = 1$. Então, as soluções x e y em Z da equação são*

$$x = x_0 + tb, \qquad y = y_0 - ta; \qquad t \in Z$$

Demonstração: Sendo (x, y) uma outra solução qualquer além de (x_0, y_0) podemos escrever

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

que pode ser reescrita como

$$a(x - x_0) = b(y_0 - y)$$

Como $(a, b) = 1$ segue que $b \mid (x - x_0)$ e $a \mid (y_0 - y)$, portanto

$$x - x_0 = tb, \qquad y_0 - y = ta, \qquad t \in Z$$

O que prova que as soluções são do tipo exibido na proposição.

Vale ressaltar que em algumas situações buscamos soluções naturais. Não iremos falar de tais condições, pois encontrar tais soluções torna-se relativamente fácil com as proposições acima.

Os exemplos a seguir são para efeito de ilustração.

Exemplo 5.6: Resolva a equação dioafntina $8x - 13y = 23$

Solução: Um estratégia apropriada é escrever $(8, 13) = 1$ como combinação linear de inteiros e depois multiplicar a igualdade por 23.

Perceba que não precisamos de uma solução específica, precisamos apenas de UMA solução qualquer para encontrar as demais.

É fácil perceber que $40 - 39 = 8 \cdot 5 - 13 \cdot 3 = 1$. Multiplicando ambos os lados da igualdade por 23 obteremos

$$8 \cdot (115) - 13 \cdot (69) = 23$$

Portanto as soluções $8x - 13y = 23$ são do tipo

$$x = 115 - 13t, \qquad y = 69 - 8t, \qquad t \in Z$$

Exemplo 5.7: A secretaria de educação de certo município dispõe de 5000 reais para compra de livros: o livro Tipo A custa 26 reais a unidade, e o livro Tipo B custa 24 reais a unidade. Existem quantas possibilidades para a compra desses dois tipos de livros, gastando todo valor disponível?

Solução: Basta supor que serão comprados x livros do Tipo A e y livros do Tipo B, nos fornecendo assim a equação

$$26x + 24y = 5000$$

podemos dividir ambos os lados da equação por 2 para obter

$$13x + 12y = 2500$$

Como $13 \cdot 1 + 12 \cdot (-1) = 1$, temos que $13 \cdot (2500) + 12 \cdot (-2500) = 2500$.

Portanto as soluções de $13x + 12y = 2500$ são do tipo

$$x = 2500 + 12t, \qquad y = -2500 - 13t, \qquad t \in Z$$

O problema nos restringe a soluções naturais, portando queremos

$$2500 + 12t \geq 0$$

e

$$-2500 - 13t \geq 0$$

Ou seja, $-208 \leq t \leq -192$

Assim, total de possibilidades são $-192 - (-208) = 16$.

Exemplo 5.8: Um grupo de 30 pessoas entre homens, mulheres e crianças foram a um banque e, juntos, gastaram 30 patacas. Cada homem pagou 2 patacas, cada mulher

meia pataca e cada criança um décimo de pataca. Quantos homens, quantas mulheres e quantas crianças havia no grupo?

Solução: Temos o sistema

$$\begin{cases} h+m+c=30 \\ 2h+0.5m+0.1c=30 \end{cases} \Longrightarrow \begin{cases} h+m+c=30 \\ 20h+5m+c=300 \end{cases}$$

Subtraindo a primeira equação da segunda equação obteremos a equação diofantina

$$19h+4m=270$$

. Como $(19,4)=1$ a equação possui solução. Pelo Teorema de Bézout, podemos escrever $(19,4)=1$ como

$$19\cdot(-1)+4\cdot(5)=1$$

Multiplicando ambos os membros da equação acima por 270 teremos

$$19\cdot(-270)+4\cdot(1350)=270$$

Como buscamos soluções naturais, podemos reescrever a equação acima como

$$19\cdot(2)+4\cdot(58)=270$$

Portanto a solução geral é dada por

$$\begin{cases} h=2+4t \\ m=58-19t \end{cases}, t\in\mathbb{N}$$

Devemos ter $0\leq t\leq 3$. Portanto as possíveis soluções para a quantidade de homens e mulheres são: $h=\{2,6,10,14\}$ e $m=\{1,20,39,58$. O único par que satisfaz as condições iniciais é $h=14$ e $m=1$. Consequentemente $c=15$.

5.5 NÚMEROS PRIMOS

O estudo dos números primos é um dos conceitos mais importante da matemática. Não raro, ao longo da história, diversos problemas envolvendo números primos desafiaram gênios como Fermat, Euler e Gauss.

Para termos uma ideia da importância dos números primos, existem cientistas que voltam suas pesquisas para descobertas desses números e, recentemente, um novo número primo foi descoberto conforme matéria publicada pela revista Exame em janeiro de 2019.

Como os números primos são a base do sistema de criptografia RSA, falaremos a seguir sobre suas propriedades.

Figura 3 – A descoberta do maior número primo


CIÊNCIA

Por que a descoberta do maior número primo da história importa?

Pesquisadores descobriram um número primo de 24.862.048 dígitos — e a criptografia agradece

Por **Gustavo Gusmão**
20 jan 2019, 07h01

Fonte: https://exame.com/ciencia/por-que-a-descoberta-do-maior-numero-primo-da-historia-importa/

Definição: *Um número natural maior do que* 1 *é chamado de primo se ele possui como divisores* 1 *e ele próprio; caso contrário, é dito composto.*

Da definição acima surgem alguns fatos.

(i) Se p e q são números primos e $p \mid q$, então $p = q$

(ii) Se p é um número primo e a um número inteiro qualquer, se $p \nmid a$, então $(p, a) = 1$

Os fatos mencionados acima são relativamente fáceis de concluir e a verificação deixaremos a cargo do leitor.

Proposição 5.9. *Seja n>1 um número inteiro. Então o menor divisor de n diferente de 1 é um número primo.*

Demonstração: Seja p o menor divisor de n diferente de 1. Se p é composto, então existe $1 < q < p$ tal que $q \mid p$. Por outro lado, como $q \mid p$ e $p \mid n$, então $q \mid n$. Absurdo, já que p é o menor divisor de n. Logo p é primo.

Outra proposição importante sobre os números inteiros é o Lema de Euclides, enunciado a seguir.

Proposição 5.10. *(Lema de Euclides). Sejam $a, b, p \in \mathbb{Z}$, com p primo. Se $p \mid ab$ então $p \mid a$ ou $p \mid b$*

Demonstração: Suponha que $p \nmid a$. Isso significa que $(p, a) = 1$, logo

$$px + ay = 1$$

Multiplicando ambos os membros por b teremos

$$pbx + aby = b$$

Mas, por hipótese, $ab = pk$, então

$$pbx + aby = pbx + pky = b$$

$$p \cdot (bx + ky) = p \cdot k' = b$$

O que mostra que $p \mid b$.

Exemplo 5.9: Encontre o menor número natural $k > 2008$, tal que $1+2+3+...+k$ seja múltiplo de 13.

Solução: Sabemos que

$$1 + 2 + 3... + k = \frac{k \cdot (k+1)}{2}$$

.

Para que essa soma seja múltiplo de 13 devemos ter k ou $k+1$ múltiplo de 13 pois 13 é primo. Para que k seja o menor possível, devemos ter $k+1$ múltiplo de 13. O menor múltiplo de 13 maior que 2008 é 2015. Logo, $k + 1 = 2015$ e, portanto, $k = 2014$.

Exemplo 5.10: Se p é um número primo maior do que 3, então $p^2 + 2$ é múltiplo de 3.

Solução: Como $p > 3$, então p deixa resto 1 ou resto 2 na divisão por 3. Isto é, $p = 3n + 1$ ou $p = 3n + 2$ com $n \in \mathbb{N}$.

Se $p = 3n + 1$ então

$$p^2 + 2 = (3n + 1)^2 + 2 = 9n^2 + 6n + 1 + 2 = 3 \cdot (3n^2 + 2n + 1) = 3k$$

.

Se $p = 3n + 2$ então

$$p^2 + 2 = (3n + 2)^2 + 2 = 9n^2 + 12n + 4 + 2 = 3 \cdot (3n^2 + 4n + 2) = 3k'$$

.

Portanto, $p^2 + 2$ é múltiplo de 3 para todo $p > 3$.

5.5.1 SOBRE A DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Ao longo dos nossos estudos conhecemos alguns números primos, dentre eles $\{2, 3, 5, 7, 11, 13, 17, ...\}$. Mas será que existe uma lei matemática que descreva todos? Até o momento, não. Lendas urbanas dizem inclusive que, se por ventura, for possível descrever todos os números primos nosso sistema financeiro viria abaixo. Evidentemente que conhecemos algumas leis matemáticas que fornecem números primos, como *"Os primos de Fermat"* e também *"Os primos de Mersenne"*, por exemplo. A única certeza que temos é que os números primos são infinitos. Essa afirmação foi enunciada como teorema por Euclides no Livro IX de *Os Elementos*.

> Os números primos além de belos e desafiadores do ponto de vista matemático, são extremamente importantes para as atividades usuais do nosso dia a dia. Por exemplo, nenhuma transação bancária ou pela internet estaria segura sem o uso de números primos muito grandes. Apesar deles serem abundantes, não existe nenhum método razoável de produção de números primos, mesmo tendo em mãos a alta tecnologia de hoje em dia. (OLIVEIRA e CORCHO, 2012, p.127).

Proposição 5.11. *(Teorema de Euclides). Existem infinitos números primos.*

Demonstração: Suponha que exista uma quantidade finita de números primos $p_1, p_2, ..., p_k$.

Considere o número $n = p_1 p_2 \cdots p_k + 1$. Seja q o menor divisor primo de n. Se $q = p_i$, para algum $1 \leq i \leq k$, como $q \mid n$ então $q \mid 1$, o que é impossível. Logo, temos uma contradição a hipótese de termos uma quantidade finita de primos.

Existem muitas curiosidades acerca dos números primos. Uma delas é a *Conjectura de GoldBach* que afirma que todo número natural maior que 3 pode ser escrito como a soma de dois números primos.

Também não podemos deixar de mencionar aquele que talvez seja o mais importante problema em aberto da Teoria dos números: a Hipótese de Riemann. Em 2015 um professor nigeriano disse ter resolvido tal problema, porém não passou de um engano. Recentemente o matemático britânico Michael Atiyah afirmou ter resolvido a Hipótese de Riemann. Vale ressaltar que a Hipótese de Riemann é um dos sete problemas do milênio, proposto pelo Clay Mathematics Institute of Cambridge (CMI) com premiação de 1 milhão de dólares, cada. O CMI ainda não se pronunciou sobre a solução de Atiyah.

5.6 ARITMÉTICA MODULAR

Nesta seção trataremos de um dos assuntos mais extensos e importantes da Teoria dos números. Sempre na tentativa de sintetizar este trabalho, trataremos apenas dos tópicos necessários e suficientes para que possamos compreender o funcionamento da Criptografia RSA, tema central deste trabalho.

Diremos que um número inteiro a e um número inteiro b são congruentes módulo n se, efetuada a divisão euclidiana, deixam o mesmo resto na divisão por n. Denotaremos essa congruência como

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

Por exemplo, $35 \equiv 23 \pmod 4$ pois ambos deixam resto 3 na divisão por 4.

Decorre da definição de congruência a seguinte proposição.

Proposição 5.12. *Se* $a \equiv b \pmod{n}$*, então* $n \mid (b-a)$

Demonstração: Como $a \equiv b \pmod{n}$, segue que:

$$a = nq_1 + r \quad (1) \qquad b = nq_2 + r \quad (2)$$

Subtraindo (1) de (2) obtemos

$$b - a = n(q_1 - q_2) = nk \qquad k \in Z$$

e portanto $n \mid (b-a)$

Proposição 5.13. *Sejam* $a, b, c, d, n \in \mathbb{Z}$*, com* $n > 1$*.*

i) Se $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$*, então* $a + c \equiv b + d \pmod{n}$*.*

ii) se $a \equiv b \pmod{n}$ *e* $c \equiv d \pmod{n}$*, então* $ac \equiv bd \pmod{n}$*.*

Demonstração: Da proposição 5.8 temos que $n \mid (b-a)$ e $n \mid (d-c)$.

i) Como $n \mid (b-a)$ e $n \mid (d-c)$ então $n \mid (b-a)+(d-c)$, portanto $n \mid (a+c)-(b+d)$.

ii) Basta observar que $bd = d(b-a) + a(d-c)$ e concluir que $n \mid bd - ac$

Proposição 5.14. *Sejam* $a, b \in \mathbb{Z}$ *e* $n_1, n_2, ...n_r$ *inteiros maiores do que 1. Se* $a \equiv b \pmod{n_i}$*,* $\forall \in \{1, 2, ...r\}$ *então* $a \equiv b \pmod{[n_1, n_2, ...n_r]}$

Demonstração: Basta observa que se $a \equiv b \pmod{n_i}$ então $n_i \mid (b-a)$, ou seja, $b - a$ é múltiplo de cada n_i, portanto $b - a$ é múltiplo de $[n_1, n_2, ...n_r]$, ou seja, $[n_1, n_2, ...n_r] \mid (b-a)$, logo $a \equiv b \pmod{[n_1, n_2, ..., n_r]}$.

Exemplo 5.11: Quem é o menor múltiplo de 11 que deixa resto 1 na divisão por 2, 3 e 4?

Solução: Temos que $11X \equiv 12$, $11X \equiv 1 \pmod{3}$ e $11X \equiv 1 \pmod{4}$. A proposição 5.12 nos dá que $11X \equiv 1 \pmod{[2,3,4]}$, ou seja $11X \equiv 1 \pmod{12}$.

A última congruência nos dá a equação diofantina $11X - 12Y = 1$, que nos leva a $11 \cdot (11) - 12 \cdot (10) = 1$. Logo $11 \cdot 11 = 121 \equiv 1 \pmod{12}$. O número que procuramos é o 121.

Exemplo 5.12: Determine o resto da divisão de $2^9 \cdot 3^8 \cdot 5^{13}$ por 7.

Solução: Perceba que $2^3 = 8 \equiv 1 \pmod{7}$. Logo $2^9 = 2^3 \cdot 2^3 \cdot 2^3 \equiv 1 \cdot 1 \cdot 1 \equiv 1 \pmod{7}$.

$3^2 = 9 \equiv 2 \pmod{7}$. Logo, $3^8 = (3^2)^4 \equiv 2^4 \equiv 16 \equiv 2 \pmod{7}$.

Por fim, $5^2 = 25 \equiv 4 \pmod 7$. Logo, $5^{13} = (5^2)^6 \cdot 5 \equiv 4^6 \cdot 5 \pmod 7$. Por outro lado, $4^3 = 64 \equiv 1 \pmod 7$, então $4^6 \cdot 5 \equiv (4^3)^2 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \pmod 7$.

Assim, $2^9 \cdot 3^8 \cdot 5^{13} \equiv 1 \cdot 25 \equiv 10 \equiv 3 \pmod 7$.

Portanto o resto da divisão de $2^9 \cdot 3^8 \cdot 5^{13}$ por 7 é 3.

Exemplo 5.13: Mostre que

$$7 \mid 3^{2n+1} + 2^{n+2}$$

Solução: Observe que

$$3^{2n+1} = (3^2)^n \cdot 3 = 9^n \cdot 3 \equiv 3 \cdot 2^n \pmod 7$$

e

$$2^{n+2} = 2^2 \cdot 2^n = 4 \cdot 2^n$$

.

Portanto,

$$3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \cdot 2^n \equiv 0 \pmod 7$$

.

5.7 TEOREMA DE EULER

Antes de apresentar o teorema de Euler, é do nosso interesse a proposição seguinte.

Proposição 5.15. *Sejam a e n inteiros com $a < n$. Se $(a, n) = 1$, existe um único inteiro $x \in \{1, 2, ..., n-1\}$ tal que $ax \equiv 1 \pmod n$.*

Demonstração: Como $(a, n) = 1$, existem inteiros x e y tais que $ax - ny = 1$. Logo $ax - 1 = ny$ que nos diz que $n \mid ax - 1$. Portanto, $ax \equiv 1 \pmod n$.

Suponha agora que exista uma segunda solução $x' \in \{1, 2, ...n-1\}$ com $ax' \equiv 1 \pmod n$. Então $a(x - x') \equiv 0 \pmod n$ e portanto $n \mid a(x - x')$. Como $(a, n) = 1$, então $n \mid x - x'$. Mas $x - x' \in \{-(n-1), ..., n-1\}$, deixando $x - x' = 0$ como a única possibilidade.

5.7.1 A FUNÇÃO FI DE EULER

A função fi de Euler a qual denotaremos por $\varphi(n)$ é a quantidade de números inteiros em $\{1, 2, ...n-1\}$ relativamente primos com n para $n > 1$. Além disso, definimos $\varphi(1) = 1$ e, se p é um número primo, então $\varphi(p) = p - 1$

Proposição 5.16. *Sejam p e q números primos. Então,*

$$\varphi(pq) = (p-1)(q-1)$$

Demonstração: Queremos saber quantos inteiros pertencentes ao conjunto $\{1, 2, ...pq-1\}$ são relativamente primos com pq. Basta observar que existem $(q-1)$ múltiplos de p e $(p-1)$ múltiplos de q no conjunto $\{1, 2, ..., pq-1\}$. Portanto o número de inteiros em $\{1, 2, ..., pq-1\}$ relativamente primos com pq é

$$(pq-1) - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

Proposição 5.17. *(Teorema de Euler). Se m e n são inteiros com $m > 1$ e $(m, n) = 1$, então*

$$m^{\varphi(n)} \equiv 1 \pmod{n}$$

Fermat provou que $m^{n-1} \equiv 1 \pmod{n}$ quando n é primo. Este resultado ficou conhecido como Pequeno Teorema de Fermat.

A demonstração deste teorema requer ferramentas que não foram utilizadas ao longo do trabalho, por isso não iremos fazê-lo. Entretanto, ele é necessário para o funcionamento do método RSA, por isso ele foi enunciado aqui.

Exemplo 5.14: Sejam p e q números primos distintos. Mostre que

$$pq \mid p^{q-1} + q^{p-1} - 1$$

.

Solução: Pelo pequeno teorema de Fermat, $p \mid q^{p-1} - 1$ e além disso $p \mid p^{q-1}$, logo $p \mid q^{p-1} + p^{q-1} - 1$. Analogamente, $q \mid p^{q-1} - 1$ e $q \mid q^{p-1}$, logo $q \mid p^{q-1} + q^{p-1} - 1$. Portanto, como $(p, q) = 1$, então $pq \mid p^{q-1} + q^{p-1} - 1$.

Exemplo 5.15: Ache o resto da divisão de $1^5 + 2^5 + ... + 183^5$ por 5.

Solução: Vimos acima $m^{n-1} \equiv 1 \pmod{n}$ quando n é primo e $(m.n) = 1$. Por outro lado, se multiplicarmos ambos os membros da congruência por m, teremos $m^n \equiv m \pmod{n}$. Este último resultado é valido mesmo que $(m, n) \neq 1$, já que teríamos $n \mid m^n - m$.

Utilizando este resultado perceba que

$$1^5 + 2^5 + ... + 183^5 \equiv 1 + 2 + ... + 183 \pmod{5}$$

. Como

$$1 + 2 + ... + 183 = \frac{184 \cdot 183}{2} = 92 \cdot 183$$

então

$$1^5 + 2^5 + ... + 183^5 \equiv 1 + 2 + ... + 183 \equiv 92 \cdot 183 \equiv 2 \cdot 3 \equiv 1 \pmod{5}$$

Ou seja, o resto da divisão de $1^5 + 2^5 + ...183^5$ por 5 é 1.

Exemplo 5.16: Mostre que $a^7 \equiv a \pmod{21}$.

Solução: Temos, pelo pequeno teorema de Fermat, que $a^7 \equiv a \pmod{7}$. De modo análogo temos

$$a^3 \equiv a \pmod{3}$$
$$a^5 = a^3 \cdot a^2 \equiv a \cdot a^2 = a^3 \equiv a \pmod{3}$$
$$a^5 \cdot a^2 \equiv a \cdot a^2 = a^3 \equiv a \pmod{3}$$

Ou seja, $a^7 \equiv a \pmod{3}$. Logo, $a^7 \equiv a \pmod{[3,7]}$. Portanto $a^7 \equiv a \pmod{21}$.

5.8 TEOREMA CHINÊS DOS RESTOS

Na antiguidade, os generais chineses costumavam contar suas tropas perdidas após a guerra da seguinte forma: ordenavam que as tropas formassem várias colunas com um determinado tamanho e depois contavam quantas sobravam, e faziam isto para vários tamanhos diferentes. Por exemplo, um general chinês possuía 1200 tropas antes da guerra. Após a guerra, ele alinhou as tropas de 5 em 5 de forma que sobraram 3 tropas (1). Quando alinhou de 6 em 6, também sobraram 3 tropas (2). Quando alinhou de 7 em 7, sobrou 1 tropa (3). E quando alinhou de 11 em 11, não sobrou nenhuma tropa (4). Quantas tropas o general tinha?

Podemos escrever as sentenças (1), (2), (3) e (4) como um sistema de congruência, ou seja, o número X de tropas que o general possui agora é tal que:

$$X \equiv 3 \pmod{5} \qquad (1)$$

$$X \equiv 3 \pmod{6} \qquad (2)$$

$$X \equiv 1 \pmod{7} \qquad (3)$$

$$X \equiv 0 \pmod{11} \qquad (4)$$

A solução deste problema, embora trabalhosa, não é difícil. Usaremos a mesma ideia da teoria de sistemas de equações para resolver o problema do general.

A congruência (4) nos fornece $X = 11k$ (5). Substituindo essa igualdade em (1), (2) e (3) obteremos:

$$11k \equiv 3 \pmod{5} \Longrightarrow k \equiv 3 \pmod{5} \qquad (6)$$

$$11k \equiv 3 \pmod{6} \Longrightarrow k \equiv 3 \pmod{6} \qquad (7)$$

$$11k \equiv 1 \pmod{7} \Longrightarrow k \equiv 2 \pmod{7} \qquad (8)$$

De maneira similar, a partir de (8) obtemos $k = 7r + 2$ (9). Substituindo (9) em (6) e (7) teremos.

$$7r + 2 \equiv 3 \pmod 5 \Longrightarrow r \equiv 3 \pmod 5 \qquad (10)$$

$$7r + 2 \equiv 3 \pmod 6 \Longrightarrow r \equiv 1 \pmod 6 \qquad (11)$$

A congruência (10) nos leva a $r = 5s + 3$ (12). Substituindo r em função de s em (11) teremos

$$5s + 3 \equiv 1 \pmod 6 \Longrightarrow s \equiv 2 \pmod 6 \qquad (13)$$

Por fim, de (13) podemos escrever $s = 6t + 2$ (14) e podemos voltar substituindo (14) em (12), (12) em (9) e (9) em (5) para obter X em função de t. Teremos então

$$r = 5 \cdot (6t + 2) + 3 \Longrightarrow r = 30t + 13$$

$$k = 7 \cdot (30t + 13) + 2 \Longrightarrow k = 210t + 93$$

$$X = 11 \cdot (210t + 93) \longrightarrow X = 2310t + 1023$$

Como queremos $0 < X < 1200$, basta substituir $t = 0$ para concluir que $X = 1023$

Evidente que a solução encontrada acima não é o Teorema Chinês dos Restos. O teorema em questão tem o objetivo de facilitar a descoberta da solução de um sistema de congruência, afinal se fossem 5, 10 ou mais congruências como faríamos?

> Problemas antigos da astronomia, ligados aos movimentos periódicos dos corpos celestes, deram origem ao hoje conhecido como Teorema Chinês de Restos. O nome veio do fato dos problemas terem sido originários dos antigos matemáticos chineses. Há registros de problemas relacionados ao tema propostos no século terceiro depois de Cristo. (MEIRA, et. al., 2016)

Proposição 5.18. *(Teorema Chinês dos Restos). Sejam $n_1, n_2, ...n_r$ números inteiros positivos tais que cada par $(n_i, n_j) = 1$ com $i \neq j$. O sistema*

$$\begin{cases} X \equiv a_1 \pmod{n_1} \\ X \equiv a_2 \pmod{n_2} \\ \qquad ... \\ X \equiv a_r \pmod{n_r} \end{cases}$$

Possui uma única solução módulo $N = n_1 n_2 \cdots n_r$ e ela é do tipo

$$x = N_1 y_1 a_1 + ... + N_r y_r a_r + tN$$

onde $t \in \mathbb{Z}$, $N_i = \frac{N}{n_i}$ e y_i é solução da congruência $N_i Y \equiv 1 \pmod{n_i}$, $i = 1, ..., r$

Demonstração: Como $n_i \mid N_j$, se $i \neq j$ e $N_i y_i \equiv 1 \pmod{n}$, então

$$x = N_1 y_1 a_1 + N_2 y_2 a_2 + ... + N_r y_r a_r \equiv N_i y_i a_i \pmod{n_i}$$

Isso mostra que x é solução do sistema.

Suponhamos agora que x' seja uma outra solução do sistema. Então

$$x \equiv x' \pmod{n_i}, \forall i, i = 1, 2..., r$$

. Como $(n_i, n_j) = 1$, para todo $i \neq j$, segue que $[n_1, n_2, ..., n_r] = [n_1 n_2 ... n_r] = N$ e portanto, $x \equiv x' \pmod{N}$.

Vamos usar o Teorema Chinês dos Restos para resolver o problema do general.

Como o mdc entre cada par de números do conjunto $\{5, 6, 7, 11\}$ é igual a 1, então o sistema de congruências possui solução.

Temos $N = 5 \cdot 6 \cdot 7 \cdot 11 = 2310$, $N_1 = 462$, $N_2 = 385$, $N_3 = 330$ e $N_4 = 210$. Além disso $y_1 = 3$, $y_2 = 1$, $y_3 = 1$ e $y_4 = 1$ são, respectivamente, soluções das congruências $462y_1 \equiv 1 \pmod{5}$, $385y_2 \equiv 1 \pmod{6}$, $330y_3 \equiv 1 \pmod{7}$ e $210y_4 \equiv 1 \pmod{11}$. Portanto, a solução módulo $N = 2310$ é

$$X = 462 \cdot 3 \cdot 3 + 385 \cdot 1 \cdot 3 + 330 \cdot 1 \cdot 1 + 210 \cdot 1 \cdot 0 + 2310t = 5643 + 2310t$$

ou seja

$$X \equiv 5643 \equiv 1023 \pmod{2310}$$

logo $X = 1023 + 2310t$. Lembrando que queremos $0 < X < 1200$. logo $X = 1023$ é a solução do sistema.

Exemplo 5.17: Dispondo de uma quantia em reais maior do que 1000 e menor do que 2000. Se distribuirmos essa quantia entre 11 pessoas, sobra 1 real; se a distribuirmos entre 10 pessoas, sobram 2 reais e se a distribuirmos entre 9 pessoas sobram 4 reais. De quantos reais dispomos?

Solução: Queremos encontrar uma quantia X, tal que $1000 < X < 2000$ e seja solução do sistema

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{10} \\ x \equiv 4 \pmod{9} \end{cases}$$

Como $(11, 10) = (11, 9) = (10, 9) = 1$, podemos utilizar o teorema chinês dos restos para encontrar a solução do sistema.

Temos $a_1 = 1$, $a_2 = 2$ e $a_3 = 4$. $N = 11 \cdot 10 \cdot 9 = 990$. $N_1 = 90$, $N_2 = 99$ e $N_3 = 110$. Além disso, temos $y_1 = 6$, $y_2 = 9$ e $y_3 = 5$ soluções, respectivamente, das congruências $90y_1 \equiv 1 \pmod{11}$, $99y_2 \equiv 1 \pmod{10}$ e $110y_3 \equiv 1 \pmod{9}$.

Logo, $x \equiv 90 \cdot 6 \cdot 1 + 99 \cdot 9 \cdot 2 + 110 \cdot 5 \cdot 4 \equiv 4522 \equiv 562 \pmod{990}$.

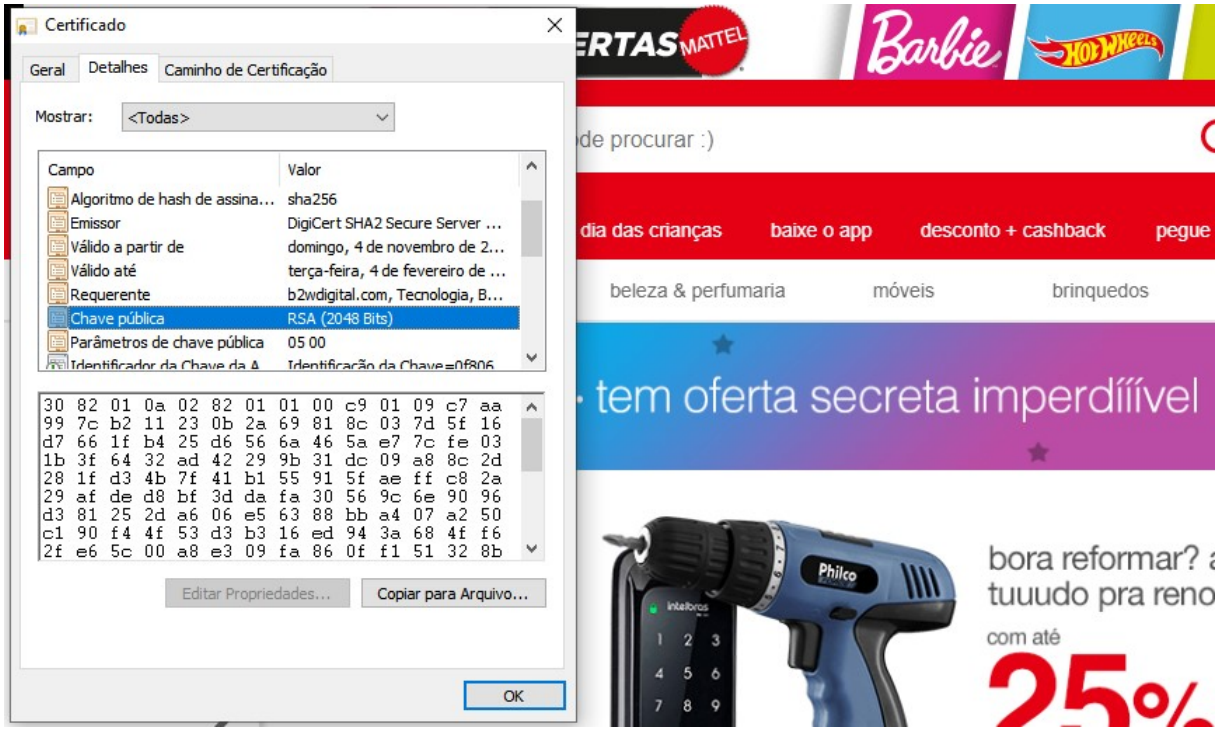
Ou seja, $x = 562 + 990t$, com $t \in \mathbb{Z}$. A única solução natural, tal que $1000 < X < 2000$ é obtida quando $t = 1$. Portanto, $X = 562 + 990 \cdot 1 = 1552$.

6 O MÉTODO RSA

O sistema de criptografia RSA é estabelecido pelo receptor (pessoa, loja online, bancos, etc) que deseja receber uma mensagem de maneira segura. Apresentaremos os 6 passos que constituem o funcionamento do método RSA extraído do livro Mathématiques et Technologie, traduzido pela SBM e que serviu de inspiração para a realização deste trabalho.

Passo 1. O receptor escolhe dois primos grande p e q (atualmente com cerca de 300 dígitos cada) e calcula $n = pq$. O número n é a "chave pública"(veja figura), que terá então, aproximadamente 600 dígitos. Lembre-se que lojas virtuais, bancos, etc. atualizam seu código de tempo em tempo tornando impossível (mesmo para um computador quântico) fatorar n em uma quantidade de tempo razoável.

Figura 4 – RSA de uma loja online



Fonte: https://www.americanas.com.br/

Passo 2. O receptor calcula $\varphi(n) = (p-1)(q-1)$ (função de Euler). Note que esta fórmula requer conhecimento sobre p e q. Logo, calcular $\varphi(n)$ sem conhecer p e q pode ser tão difícil quanto fatorar n.

Passo 3: escolhendo a chave de encriptação. O receptor escolhe $e \in \{1, 2, ..., n-1\}$ relativamente primo com $\varphi(n)$. O número e é a chave de encriptação. Este número é público e é usado pelo emissor para codificar a mensagem seguindo instruções publicadas

pelo receptor.

Passo 4: Construindo a chave de desencriptação. Existe $d \in \{1, 2, ...n-1\}$ tal que $ed \equiv 1 \pmod{\varphi(n)}$. A existência de d foi provada na **proposição 5.11**. O inteiro d (chave de desencriptação) é a chave privada e deve permanecer secreta. Esta chave permite ao receptor desencriptar suas mensagens recebidas.

Passo 5: Encriptando uma mensagem. Para enviar uma mensagem que consiste em um inteiro $m \in \{1, 2..., n-1\}$, o emissor calcula o resto da divisão a por n, ou seja, $m^e \equiv a \pmod{\varphi(n)}$. O inteiro a é a mensagem encriptada e já pode ser enviada ao receptor. É fácil calcular a mesmo que m, e e n sejam muito grandes. Utilizaremos o Excel para realizar esses cálculos, tornando possível sua aplicação no Ensino Médio.

Passo 6: Desencriptando uma mensagem. Ao receber a mensagem encriptada a, para desencriptá-la, basta o receptor calcular o resto da divisão de a^d por n. Mostraremos na proposição que isso sempre levará precisamente à mensagem original m.

Vamos fazer dois exemplos, um com números pequenos, "feito a mão", e outro com números muito grande com auxílio do computador.

Exemplo 6.1: Vamos supor que desejamos enviar a mensagem $m = 37$.

Passo 1: Seja $p = 7$ e $q = 13$ nossos números primos escolhidos. Então $n = 7 \cdot 13 = 91$.

Passo 2: Calcular $\varphi(n) = (p-1)(q-1)$. Logo, $\phi(n) = 6 \cdot 12 = 72$.

Passo 3: Escolher e, tal que $(e, \varphi(n)) = 1$. Vamos escolher $e = 5$. Perceba que $(5, 72) = 1$.

Passo 4: Encontrar a chave de desencriptação d tal que $ed \equiv 1 \pmod{\varphi(n)}$. vamos escrever a congruência como $5d - 72Y = 1$, observe que $5 \cdot 29 - 72 \cdot 2 = 1$, logo $5 \cdot 29 \equiv 1 \pmod{72}$. Portanto, nossa chave de desencriptação é $d = 29$.

Passo 5: Encriptar a mensagem encontrando o resto da divisão de $m^e = 37^5$ por 91.

$$37^2 = 1369 \equiv 4 \pmod{91}$$

então

$$37^5 = (37^2)^2 \cdot 37 \equiv 4^2 \cdot 37 \equiv 16 \cdot 37 \equiv 592 \equiv 46 \pmod{91}$$

. Portanto nossa mensagem encriptada é $a = 46$.

Passo 6: Recuperar a mensagem original calculando o resto da divisão de $a^d = 46^{29}$ por 91.

$$46^2 = 2116 \equiv 23 \pmod{91}.$$

então

$$46^{29} = (46^2)^{14} \cdot 46 \equiv 23^{14} \cdot 46 \pmod{91}.$$

temos que

$$23^2 = 529 \equiv 74 \pmod{91}.$$

então

$$23^{14} \cdot 46 = (23^2)^7 \cdot 46 \equiv 74^7 \cdot 46 \pmod{91}.$$

Por outro lado

$$74^2 = 5476 \equiv 16 \pmod{91}.$$

então

$$74^7 \cdot 46 = (74^2)^3 \cdot 74 \cdot 46 \equiv 16^3 \cdot 74 \cdot 46 \equiv 4096 \cdot 3404 \equiv 1 \cdot 37 \equiv 37 \pmod{91}$$

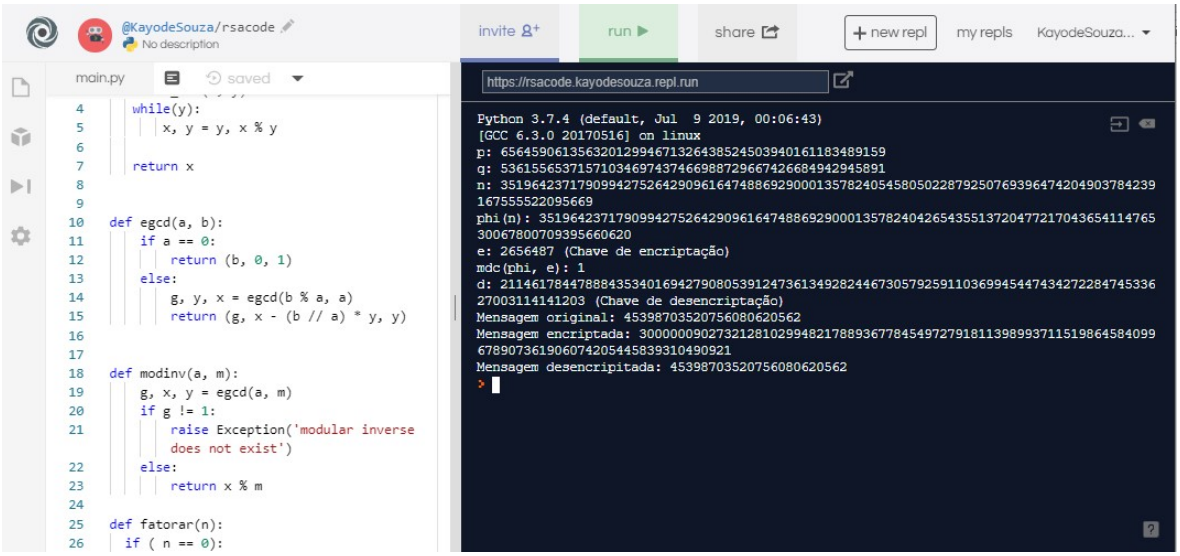
.

Portanto, o resto da divisão de 46^{29} por 91 é 37, que é a nossa mensagem original m.

Exemplo 6.2: Vamos construir um sistema a base de um sistema de criptografia para uma loja que deseja receber números de cartões de crédito de seus clientes. Um cartão de crédito possui 23 dígitos (número + data de validade + código de segurança). Este número será a nossa mensagem original m, descrita no passo 5.

Evidentemente que não é possível realizar os cálculos descritos nos passos 1 à 6 em uma calculadora comum ou mesmo no excel. Portanto utilizaremos as ferramentas da linguagem de programação phyton através do site "repl.it". Os comandos não são difíceis, descreveremos cada passo a seguir de forma que possa ser de fácil execução para cada aluno.

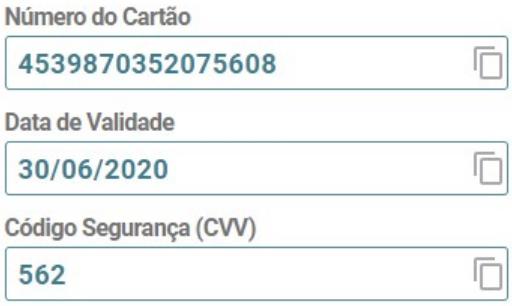
Figura 5 – Execução dos comandos no site repl.it



Fonte: https://repl.it/@KayodeSouza/rsacode

Suponha que o cliente deseje enviar os dados de um cartão de crédito como os descritos na figura 6.

Figura 6 – cartão de crédito que será enviado a loja



Fonte: https://www.4devs.com.br/gerador_de_numero_cartao_credito

Nossa mensagem original será $m = 45398703520756080620562$. O primeiro passo é determinar dois números primos p e q. Utilizaremos o site *bigprimes.org* para gerar esses números, com 50 dígitos cada, conforme conforme a figura 7.

Fonte: https://bigprimes.org/

A partir de p e q obtemos $n = pq$

$$p = 65645906135632012994671326438524503940161183489159$$

$$q = 53615565371571034697437466988729667426684942945891$$

$$n = 351964237179099427526429096164748869290001357824054580502$$

$$287925076939647420490378423916755552209566 9$$

O segundo passo consiste em calcular $\varphi(n) = (p-1)(q-1)$. Obtemos então $\varphi(n) = 351964237179099427526429096164748869290001357824042654355137204$

772170436541147653006780070939566062O

No terceiro passo escolhemos a chave de encriptação $e \in \{1, 2, ..., n-1\}$ relativamente primo com $\varphi(n)$. Neste exemplo escolhemos $e = 2656487$. Com o auxílio do software confirmamos $(\varphi(n), e) = 1$.

No quarto passo obtemos d, nossa chave de desencriptação, de modo que $ed \equiv 1 \pmod{\varphi(n)}$. Com o auxílio do software obtemos

$$d = 211461784478884353401694279080539124736134928244673057925911036994 5$$

$$44743427228474533627003114141203$$

O penúltimo passo é encriptar a nossa mensagem m obtemos a mensagem encriptada a tal que $m^e \equiv a \pmod{n}$. Obtemos, com auxílio do software

$$a = 300000090273212810299482178893677845497279181139899371151986 4$$

$$584099678907361906074205445839310490921$$

Por fim nos basta verificar, como descrito no passo 6, que $a^d \equiv m \pmod{n}$ fazendo com que a loja receba o número de cartão de crédito do cliente.

Deixo a cargo do leitor verificar que, embora seja extremamente simples realizar os cálculos necessários para encriptar uma mensagem, também é extremamente difícil realizar, com o mesmo software, a fatoração de n, o que pode dar uma noção do quão seguro é o método RSA.

Proposição 6.1. *Encriptação e desencriptação RSA são inversas uma da outra: se encriptarmos uma mensagem m como a, onde $m^e \equiv a \pmod{n}$, a desencriptação leva à mensagem original m. Isto é. $a^d \equiv m \pmod{n}$*

Demonstração: Como $m^e \equiv a \pmod{n}$ e $n = pq$ é divisível por p, então $m^e \equiv a \pmod{p}$. Portanto vamos mostrar que $a^d \equiv m \pmod{p}$ nos dois casos: p não divide m e P divide m. Como $ed \equiv 1 \pmod{\varphi(n)}$, então $ed = k(p-1)(q-1)+1$ para algum k inteiro.

$$a^d \equiv (m^e)^d = m^{ed} = m^{k(p-1)(q-1)+1} = (m^{p-1})^{k(q-1)} \cdot m \pmod{p}$$

No caso em que p não divide m, pelo pequeno teorema de Fermat $m^{p-1} \equiv 1 \pmod{p}$, então

$$a^d \equiv (m^{p-1})^{k(q-1)} \cdot m \equiv 1 \cdot m = m \pmod{p}$$

.

De maneira análoga também obtemos

$$a^d \equiv m \pmod{q}$$

Ou seja $p \mid (a^d - m)$ e $q \mid (a^d - m)$ logo $pq = n \mid (a^d - m)$ e portanto

$$a^d \equiv m \pmod{n}$$

.

No caso em que p divide m, então $m \equiv 0 \pmod{p}$. Como $m \equiv 0 \pmod{p}$ e $m^e \equiv a \pmod{p}$, tem-se $a \equiv m^e \equiv 0^e = 0 \pmod{p}$. Como $a \equiv 0 \pmod{p}$, então $a^d \equiv 0^d = 0 \pmod{p}$. Como $m \equiv 0 \pmod{p}$ e $a^d \equiv 0 \pmod{p}$, então $a^d \equiv m \pmod{p}$.

Assim, em qualquer um dos dois possíveis casos, tem-se $a^d \equiv m \pmod{p}$.

A proposição 6.1 amarra os passos finais da criptografia RSA, garantindo a volta do simples, porém eficaz, processo de segurança.

7 CONSIDERAÇÕES FINAIS

O presente trabalho teve por objetivo apresentar uma sequência didática que possa ser usada como minicurso ou disciplina eletiva para alunos do Ensino Médio da rede pública de ensino. Ao longo de todo o trabalho, tentamos apresentar os conteúdos sem dependência de pré-requisitos para o aluno participar do referente minicurso, bastando apenas o interesse e gosto pela matemática.

Primeiramente, apresentamos as noções e notações de divisibilidade e máximo divisor comum. Não poderíamos deixar de falar da importância e utilidade dos números primos, pois eles são a essência do RSA. Chegamos então em aritmética modular, algo totalmente desconhecido para o aluno do ensino básico, mas que é simples de compreender e de utilizar. Para efeito de curiosidade, deixamos aqui a sugestão de utilizar congruência para estabelecer critérios de divisibilidade.

O leitor pode questionar que algumas demonstrações não foram realizadas, é verdade. Por isso, mais uma vez, enfatizamos que o objetivo é de sintetizar o conteúdo, apresentando apenas os tópicos indispensáveis ao aluno para que possa compreender o funcionamento da criptografia RSA. No capítulo 6 adaptamos um problema do livro Matemática e Atualidade, utilizando ferramentas tecnológicas para gerar números primos e efetuar cálculos tornando mais real possível o estudo do tema, visto que, na época em que o referente livro foi escrito utilizava-se exemplos com números de poucos dígitos para facilitar os cálculos, sendo no entanto, uma ilustração nem tanto apropriada para o funcionamento do RSA.

Aproveito para disponibilizar o passo a passo da construção dos cálculos no link:

https://repl.it/@KayodeSouza/rsacode

Também aproveitamos para inserir tópicos da Teoria dos Números que julgamos interessante como Equações Diofantinas e o Teorema Chinês dos Restos.

Faço questão de ressaltar que o objetivo não é agradar o exigente aluno do tempo atual que incisivamente ataca a matemática querendo simplicidade e facilidade. Para essa questão lembro da frase de um querido professor: "A Matemática não é difícil, mas ela é exigente". Torna-se então impossível aprender Matemática estando indisposto a se dedicar a ela. Oferecemos este trabalho como uma opção ao amante da Matemática que tem curiosidade em ver suas aplicações.

REFERÊNCIAS

ROUSSEAU, C. **Matemática e Atualidade: Vol. 1**. Rio de Janeiro: SBM, 2015.

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2016.

OLIVEIRA, K.; FERNÁNDEZ, A. **Iniciação à Matemática: um curso com problemas e soluções**. 2. ed. Maceió: SBM, 2012.

COUTINHO S. C. **Criptografia**.Programa de Iniciação Científica da OBMEP. 1. ed. Rio de Janeiro: IMPA, 2010.

ALVES, A. **Criptografia e Segurança RSA: contextualização e aplicação**. 2019. 58f. Dissertação de Mestrado - Universidade Federal do Maranhão, São Luís, 2019.

MEIRA, Y. et al.**Teorema Chinês do Resto**. 2016. 9f. Universidade Estadual de Campinas, São Paulo: 2019.

BRASIL. **Parametros Curriculares Nacionais**. Ministério da Educação. Secretária de Educação Fundamental. Brasília: MEC/SEF, 1998. 152p.

POR QUE A DESCOBERTA DO MAIOR NÚMERO PRIMO DA HISTÓRIA IMPORTA? Disponível em: <https://exame.abril.com.br/ciencia/por-que-a-descoberta-do-maior-numero-primo-da-historia-importa/>. Acesso em: 20 mar. 2019.

O GENERAL E O TEOREMA CHINÊS DOS RESTOS. Disponível em: <http://legauss.blogspot.com/2009/06/o-general-e-o-teorema-chines-dos-restos.html>. Acesso em: 15 mai. 2019.