UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS E TECNOLOGIA
DEPARTAMENTO DE MATEMÁTICA

Dyego Heverton Souza Vasconcelos

TÓPICOS DE TEORIA DOS NÚMEROS E DE CRIPTOGRAFIA RSA

Campina Grande- PB

2017

Dyego Heverton Souza Vasconcelos

TÓPICOS DE TEORIA DOS NÚMEROS E DE CRIPTOGRAFIA RSA

Monografia apresentada ao Departamento e Matemática, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do Curso de Licenciatura Plena em Matemática.

Área de concentração: Matemática Aplicada.

Orientadora: Prof. Dra. Maria Isabelle Silva

Campina Grande - PB

2017

V331t Vasconcelos, Dyego Heverton Souza.
Tópicos de Teoria dos números e de Criptografia RSA [manuscrito] : / Dyego Heverton Souza Vasconcelos. - 2017.
58 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências e Tecnologia, 2017.
"Orientação : Profa. Dra. Maria Isabelle Silva, Departamento de Matemática - CCT."

1. Teoria dos números. 2. Criptografia RSA. 3. Números primos.

21. ed. CDD 512.7

Dyego Heverton Souza Vasconcelos

TÓPICOS DE TEORIA DOS NÚMEROS E DE CRIPTOGRAFIA RSA

Monografia apresentada a Banca Examinadora da Universidade Estadual da Paraíba, como requisito parcial para obtenção do Curso de Licenciatura Plena em Matemática. **Área de concentração:** Matemática Aplicada.

Aprovada em 18 / 12 / 2017.

BANCA EXAMINADORA

Maria Isabelle Silva

Prof. Dra. Maria Isabelle Silva (Orientadora)
Departamento de Matemática - UEPB/CCT

Kátia Suzana Medeiros Graciano

Prof. Msc . Kátia Suzana Medeiros Graciano (Examinadora)
Departamento de Matemática - UEPB/CCT

Aníbal de Menezes Maciel

Prof. Dr. Aníbal de Menezes Maciel (Examinador)
Departamento de Matemática - UEPB/CCT

A minha família e todas as pessoas
que fizeram parte da graduação,
por todo o apoio, DEDICO.

Agradecimentos

A Deus por ter me concedido saúde e força para superar todas as dificuldades.

A esta Universidade, seu corpo docente, direção e administração que oportunizaram a janela que hoje vislumbro um horizonte superior com toda confiança no mérito e ética aqui presentes.

A minha orientadora e amiga Isabelle Silva pelo suporte e confiança em todo o tempo, pelas suas correções e incentivos.

Aos meus pais, Milton Vasconcelos Souto e Erizalda Ana Souza de Souto, pelo o amor e apoio incondicional.

A Manoel Paulo Filho e Josefa Maria de Macedo Almeida por todo o apoio no início dessa processo. Apoio que foi se extrema importância para a conclusão dessa etapa.

A todos que de forma direta e indireta fizeram parte de toda a minha caminhada.

Também é uma conquista de todos. Tenham o meu muitíssimo obrigado.

Resumo

Este trabalho é derivado de um estudo despertado durante a graduação, tendo como foco o estudo da Criptografia RSA. Para tal assunto tivemos como base a teoria dos números e a teoria dos grupos. Pois são os assuntos bases e os pré-requisitos para então entender e ter a capacidade de trabalhar com a Criptografia RSA. Essa importante ferramenta na troca de informações sigilosas está implementada no nosso cotidiano de forma coadjuvante que nem percebemos a sua utilização e os meios em que se encontram. Nem a menos nos perguntamos qual o método utilizados pelos os bancos, sites de compras e etc, de sistema que carregam nossos dados pessoais de forma segura. Onde a mensagem só consiga ser lida pelo o verdadeiro destinatário. Graças a essa fascinante ferramenta de codificação e decodificação de dados importante que temos, nos dias atuais, todas as facilidades que nos rodeiam. Portanto, tivemos como resultado o estudo e compreensão de todo o processo da criptografia RSA.

Palavras chaves: Teoria dos Números, Criptografia RSA e Números Primos.

Abstract

This paper is derived from a study awakened during graduation, focusing on the study of RSA Cryptography. For this subject we had as the basis of number theory and group theory. For these are the basic subjects and prerequisites to understand and have the ability to work with RSA Cryptography. This important tool in the exchange of confidential information is implemented in our daily life in an auxiliary way that we do not even perceive its use and the means in which they are. Nor do we even ask ourselves what methods are used by banks, shopping sites, etc. system that carry our personal data safely. Where the message can only be read by the true recipient. Thanks to this fascinating tool of codification and decoding of important data that we have, in the present day, all the facilities that surround us. Therefore, we have resulted in the study and understanding of the entire process of RSA Cryptography.

keywords: Number theory, Cryptoraphy RSA and Prime numbers.

Índice

Capítulo 1

Introdução

A criptografia é usada desde a antiguidade. Uma das primeiras utilizações foi o com o imperador romano César, que utilizava um tipo de cifra de substituição onde na mensagem cada letra era substituída por outra letra do alfabeto. Já na Segunda Guerra Mundial que obteve uma atuação e importância maior e foi responsável pelo o desenvolvimento computacional que temos hoje, os alemães utilizavam a famosa maquina Enigma que criptografava as mensagens. O termo criptografia é a junção de duas palavras de origem grega, *cryptos* e *grafia* que significa secreto e oculto, respectivamente.

Apesar de inicialmente ter sido usada, basicamente, para troca de informações e estratégias militares, atualmente, além desse tipo de uso, recebe uma enorme atenção de pesquisadores, quanto ao seu uso comercial, usada para proteger transmissões de dados entre computadores, como por exemplo, as comunicações via internet como transmissões bancárias. Tal o modo que o investimento de bancos, empresas privadas e governamentais aumentam seus investimentos em segurança a cada dia, onde processos criptográficos são necessários.

Dentre os vários processos criptograficos que existem, um dos mais importantes e seguro é o sistema RSA, que usa fortemente a Teoria dos Números. O sistema recebe esse nome devido aos seus criadores: Rivest, Shamir e Adleman.

A criptografia estuda os métodos para codificar uma mensagem de modo que só o seu destinatário legítimo consiga interpretá-la, lê-la.

Segundo Calvacante (2004), a criptografia é a ciência que estuda os métodos de se escrever uma mensagem em código. Trata-se de um conjunto de técnicas que permitem tornar inlegível uma mensagem originalmente escrita com clareza, de tal forma a permitir

que apenas o destinatário legítimo a decifre e compreenda.

Naturalmente, todo código vem acompanhado de duas receitas, dois passos: 1) uma para codificar uma mensagem; 2) para decodificar uma mensagem da qual esteja codificada.

Vale ressaltar, que há diferença entre os sentidos das palavras: decodificar e decifrar. Decodificar é o que o destinatário legítimo da mensagem codificada faz ao recebê-la, ou seja, ele conhece o código para decodificar. Decifrar é o que um usuário faz para ler uma mensagem codificada sem ser o destinatário legitimo, ou seja, consequentemente consegue "quebrar"o código.

Para a implementação do RSA, precisamos de dois parâmetros básicos: dois números primos que iremos chamar de p e q. Para codificar uma mensagem usando RSA, precisamos conhecer o produto de dois números primos que chamaremos de n, que é a chave pública do sistema. Já para decodificar a mensagens precisamos saber os números p e q, esses números são a chave de codificação que deve ser altamente restrita. Caso contrário o sistema é comprometido.

Então, se conhecemos $n = p \cdot q$ basta fatorar o número n e acharemos os números p e q. A ideia é simples, mas usando números (com 150 algarismos ou mais) a fatoração do número n demoraria cerca de milhares de anos para ser fatorado, então, a segurança do RSA depende da ineficiência dos métodos de fatoração que temos hoje em dia.

Dividido em cinco capítulos, o trabalho trata a criptografia como uma prática da teoria dos números. No primeiro capítulo, apresentamos alguns conceitos importantes de divisibilidade; o segundo capítulo traz uma exposição dos números primos; no terceiro abordamos os conceitos de aritmética necessários para o sistema RSA; o quarto capítulo trata dos métodos para encontrar os números primos e classifica-los; o último capítulo aborda o sistema RSA, a parte prática, apresentando o algoritmo que permite a sua aplicação e sua segurança.

Contudo, o objetivo do trabalho é empreender o estudo para compreender o funcionamento do sistema de Criptografia RSA

Capítulo 2

Conceitos Importantes

Inicialmente, trataremos de alguns conceitos de teoria números de extrema importância para entender o limiar do processo necessário para o sistema RSA. Dessa forma, abordaremos a parte de divisibilidade, como o algoritmo da divisão, que calcula o quociente e o resto da divisão de um inteiro por outro; implicando no algoritmo Euclidiano, que calcula o máximo divisor comum entre dois inteiros (mdc).

2.1 Divisibilidade

Definição 2.1. Dados os números $a, b \in \mathbb{Z}$, com $a \neq 0$, dizemos que a divide b, e escrevemos $a \mid b$, se existir um inteiro n tal que $b = an$, ou seja, $a \mid b \iff \exists n \in \mathbb{Z}; b = an$. Caso a não divida b, escrevemos $a \nmid b$

Quando a divide b, $a \mid b$, também dizemos que a é divisor de b, ou também, que b é múltiplo de a, $b = an$. Dessa forma, temos, por exemplo, que 9 é um divisor de 36 ou que 36 é um múltiplo de 9, já que, $9 \mid 36$, ou seja, $36 = 9 \cdot 4$.

De maneira análoga, temos que 11 não divisor de 45, já que não existe um número $n \in \mathbb{Z}$, tal que, $45 = 11n$. Assim $11 \nmid 45$.

Dessa forma, segue algumas propriedades fundamentais de divisibilidade.

Propriedades

1. $a \mid a$ para todo $a \in \mathbb{Z}$;

2. Se $a \mid b$ e $b \mid c$, então $a \mid c$, para todo $a, b \in \mathbb{Z}$;

3. Se $a \mid b$ e $c \mid d$, então $ac \mid bd$;

4. Se $a \mid b$, então $a \mid mb$, para todo $m \in \mathbb{Z}$;

5. Se $a \mid b$ e $a \mid c$, então $a \mid (bx + cy) \forall x, y \in \mathbb{Z}$;

6. Se $a \mid b$ e $b \mid a$, então $a = \pm b$.

2.2 Algoritmo da divisão

De uma forma simples o algoritmo é uma receita, um passo a passo, para resolver um determinado problema. Assim temos uma entrada e uma saída.

Teremos que ter uma sequencia de instruções que sempre possamos usa-la. Entretanto, tem que haver um tempo limite, um tempo limite, caso contrário se repetiria eternamente, situação a qual não queremos.

Primeiramente, queremos dividir um número por outro, uma divisão com resto. O trabalho é encontrar o quociente e o resto de uma divisão de dois números inteiros e positivos.

Por exemplo, se dividimos 2587 por 56 encontraremos o quociente 46 e o resto 11. Então o algoritmo terá a entrada o dividendo e o divisor, 2587 e 56, e por saída, o quociente e o resto, 46 e 11, respectivamente.

De uma maneira geral para o caso acima a entrada são dois números inteiros a e b, e a saída são dois inteiros q e r, ou seja,

$$a = b \cdot q + r \text{ e } 0 \leq r < b,$$

O algoritmo para encontrar q e r, a partir de a e b é extremamente simples

2.3 Teorema da divisão

Teorema 2.2 (Teorema da divisão)**.** *Sejam a e b inteiros positivos. Existem números inteiros q e r, onde q e r são únicos, tais que*

$$a = b \cdot q + r \ e \ 0 \leq r < b$$

Demonstração:

A primeira parte da demonstração, que diz que dados dois inteiros a e b existem q e r diso já sabemos e temos até como calcular pelo o algoritmo da divisão. Entretanto, temos que provas que esses valores são únicos.

Suponhamos que ao dividir o inteiros a pelo o inteiro b encontramos os inteiros q e r, e, q' e r'. De outra maneira,

$$a = b \cdot q + r \text{ e } 0 \leq r < b \ (1)$$

e que

$$a = b \cdot q' + r' \text{ e } 0 \leq r' < b \ (2)$$

Como r e r' são inteiros, então um deles é maior ou igual ao outro.

Suponhamos que $r \geq r'$

Subtraindo (1) e (2)

$$r - r' = (a - b \cdot q) - (a - b \cdot q') = b(q' - q)$$

Mas r e r' são inteiros menores que b. Como supomos que $r \geq r'$, temos que $0 \leq r - r' < b$.

$$0 \leq b(q' - q) < b$$

Como b é um inteiro positivo, ela pode se cancelado.

$$0 \leq q' - q < 1 \Rightarrow q' = q$$

Logo, concluímos que:

$$r = r'$$

Daí, r e q são números inteiros únicos.

2.4 Algoritmo Euclidiano

O algoritmo euclidiano nos permite calcular o máximo divisor comum entre dois números inteiros quaisquer.

O máximo divisor comum entre dois números inteiros a e b é o maior número inteiros d que divide ou é o divisor de a e também de b, $d = mdc(a, b)$. Quando o $mdc(a, b) = 1$, os inteiros a e b são chamados de primos entre si.

Supondo que temos dois inteiros a e b e que $a \leq b$. Queremos realizar o cálculo do máximo divisor comum (mdc) entre a e b. O algoritmo euclidiano basear-se em dividir a por b encontrando um r_1. Se $r_1 \neq 0$, dividimos b por r_1, obtendo um r_2. Se $r_2 \neq 0$, dividimos r_1 por r_2, achando um r_3. E continua assim até o último resto que seja diferente de 0. O último resto será o máximo divisor comum (mdc).

Talvez você tenha se perguntado: por que o resultado dessas divisões é o máximo divisor comum? Entretanto, também temos que verificar que essas divisões simultâneas chegam sempre a um resto 0 (zero), caso contrário o algoritmo continuaria pela a eternidade.

Verificando que o algoritmo sempre pára.

$$\begin{aligned} a = b \cdot q_1 + r_1 \quad &\text{e} \quad 0 \leq r_1 < b \\ b = r_1 \cdot q_2 + r_2 \quad &\text{e} \quad 0 \leq r_2 < r_1 \\ r_1 = r_2 \cdot q_3 + r_3 \quad &\text{e} \quad 0 \leq r_3 < r_2 \\ \vdots \qquad &\qquad \vdots \end{aligned}$$

Observe a coluna da direita, a dos restos. A mesma mostra que o seguinte sempre é menor que o anterior, entretanto, todos são sempre maiores ou iguais a zero.

$$b > r_1 > r_2 > r_3 > ... \geq 0$$

Logo, como entre os números b e 0 exitem apenas uma quantidade finita de números inteiros, por isso essa sequência não pode continuar indefinidamente. Contudo, só pára se um dos restos for 0 (zero), por isso que é que o algoritmo sempre pára.

Como cada resto de uma divisão é sempre estritamente menor que o anterior, assim o maior resto possível de uma divisão é o resto anterior menos 1. Supondo que no extemos dos casos isso sempre aconteça, então teríamos que efetuar b divisões para chegar a o resto igual a 0. Concluímos que o máximo de divisões possíveis que podem acontecer é b.

Para a demonstração precisaremos de um lema.

Lema 2.3. *Sejam a e b inteiros positivos. Suponhamos que existam inteiros g e s, tais que, $a = b \cdot g + s$, então o $mdc(a, b)$=$mdc(b, s)$.*

Demonstração:

Resumi-se em mostrar que o último resto não nulo das divisões consecutivas é o máximo divisor comum. Aplicando o algoritmo a a e b, e supondo que o resto nulo é o n-éssimo, o que ocorre após n divisões, temos:

$$\begin{aligned} a &= b \cdot q_1 + r_1 \quad \text{e} \quad 0 \leq r - 1 < b \\ b &= r_1 \cdot q_2 + r_2 \quad \text{e} \quad 0 \leq r_2 < r_1 \\ r_1 &= r_2 \cdot q_3 + r_3 \quad \text{e} \quad 0 \leq r_3 < r_2 \\ &\vdots \qquad\qquad\qquad \vdots \\ r_{n-4} &= r_{n-3} \cdot q_{n-2} + r_{n-2} \quad \text{e} \quad 0 \leq r_{n-2} < r_{n-3} \\ r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1} \quad \text{e} \quad 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1} \cdot q_n \quad \text{e} \quad r_n = 0 \end{aligned}$$

Observe a coluna da esquerda. Em particular a última divisão que temos que r_{n-1} divide r_{n-2}. Logo, o maior divisor comum entre os dois números é o r_{n-1}. De outro modo, o $\text{mdc}(r_{n-2}, r_{n-1}) = r_{n-1}$.

Utilizando o lema, temos:

$$\begin{aligned} \text{mdc}(r_{n-3}, r_{n-2}) &= \text{mdc}(r_{n-2}, r_{n-1}) = r_{n-1} \\ \text{mdc}(r_{n-4}, r_{n-3}) &= \text{mdc}(r_{n-3}, r_{n-2}) = r_{n-1} \end{aligned}$$

Continuando a aplicar o lema coluna acima chegaremos que $\text{mdc}(a, b) = r_{n-1}$.

Agora falta demonstrar o lema para que não fique nenhuma falha na demonstração. O lema nos diz que assumindo que a, b, g e s estão relacionados por $a = bg + s$, então o $\text{mdc}(a, b) = \text{mdc}(b, s)$.

Suponhamos que

$$d_1 = \text{mdc}(a, b) \quad \text{e} \quad d_2 = \text{mdc}(b, s)$$

Para demonstrar o lema temos que mostrar que $d_1 = d_2$. Vamos realizar-la em duas partes: 1) mostrar que $d_1 \leq d_2$e 2) mostrar que $d_2 \leq d_1$.

1ª parte $d_1 \leq d_2$

Se $d_1 = \text{mdc}(a, b)$, então $d_1 | \ a$ (d_1 divide a) e $d_2 | \ b$ (d_2 divide b). Assim existem dois inteiros x e y onde

$$a = d_1 x \quad \text{e} \quad b = d_2 y$$

Substituindo a e b em $a = bq + s$

$$d_1x = d_1yg + s, \text{ ou seja,}$$
$$s = d_1x - d_1yg$$
$$s = d_1(x - yg).$$

Portanto, $d_1|s$. Como $d_1 = \text{mdc}(a, b)$, em particular $d_1|b$. Mas foi demonstrado que d_1 também divide s. Portanto, d_1 é o maior, ou máximo, divisor comum entre b e s. Entretanto, d_2 é o maior divisor de b e s. Logo $d_1 \leq d_2$.

2^{a} parte $d_2 \leq d_1$

A demonstração segue o mesmo raciocínio, ou seja, é análoga a 1^{a} parte $d_1 \leq d_2$.

Logo a interseção nos dar que $d_1 = d_2$. Que é o que queríamos demonstrar.

Capítulo 3

Números primos

A base para o sistema RSA são so números primos. Devido a sua particularidade aliada aos métodos da teoria dos números que temos toda a eficácia da criptografia algo trataremos no ultimo capítulo. Dessa forma, iremos nos atentar aos conceitos dos Números Primos tais como suas propriedades, escrevendo-os em formas polinomiais, fórmulas de Mersenne e Fermat e fórmulas fatoriais.

3.1 Propriedade fundamental dos primos

Teorema 3.1 (Propriedade fundamental dos primos.)**.** *Sejam p um número primo e a e b inteiros positivos. Se p divide o produto ab então p divide a ou p divide b.*

Para provarmos isso precisamos dc uma resultado auxiliar. Comecemos com um lema.

Lema 3.2. *Sejam a, b e c inteiros positivos e suponhamos que a e b são primos entre si. i) Se b divide o produto ac então b divide c. ii) Se a e b dividem c então o produto ab divide c.*

Demonstração do lema

Temos, por hipotese, que a e b são primos entre si, ou seja, mdc(a,b)=1. O algoritmo euclidiano estendido nos garante que existe α e β, tais que

$$\alpha \cdot a + \beta \cdot b = 1$$
$$\alpha \cdot ac + \beta \cdot bc = c$$

i) É que claro que a segunda parcela é divisível por b. Mas a primeira também é (por hipotese). Logo o lada esquerda é divisível por b. Portanto, c é divisível por b.

ii) Se a divide c, podemos escrever $c = at$, para algum t inteiro. Mas b também divide c. Como a e b são primos entre si, segue da afirmação (i) que b tem que dividir t. Assim teremos que $t = bk$, para algum inteiro k. Portanto

$$c = at = a(bk) = (ab)k$$

é divisível por ab, que é a afirmação (ii).

Demonstração do teorema

Utilizando o lema. Se por acaso p dividir a, estamos feitos. Então, digamos, que p não divida a. Neste ponto usamos o fato de p ser primo, para concluir que se p não divide a, então p e a são primos entre si. Isto ocorre porque qualquer divisor comum a p e a divide p; mas os únicos divisores de p são 1 e o próprio p. Portanto, se p não divide a, então, mdc(p,a)=1. Por isso podemos aplicar o lema: como p e a são primos entre si e como p divide ab temos que p divide b.

3.2 Fórmulas polinomiais

Teorema 3.3. *Dado um polinômio f(x) com coeficientes inteiros, existe uma infinidade de inteiros positivos m tais que f(m) é composto.*

Demonstração

Vamos demonstrar apenas quando o polinômio f tem grau 2. Este caso ocorre a mesma dificuldade no caso geral, sem que as ideias sejam ofuscadas pela notação.

Seja $f(x) = ax^2 + bx + c$, um polinômio cujos coeficientes a, b e c são inteiros. Cada que seja sempre positiva para valores muito grandes de x, consideremos $a > 0$. Se f é composto sempre que x for um inteiro positivo, não há nada a provar. Então, digamos que existe um inteiro positivo m tal que $f(m) = p$ é um número inteiro primo (positivo).

Seja agora h um inteiro positivo qualquer. Vamos calcular $f(m + hp)$. Queremos determinar

$$f(m + hp) = a(m + hp)^2 + b(m + hp) + c$$
$$f(m + hp) = a[m^2 + 2mhp + (hp)^2] + bm + bhp + c$$

$$f(m+hp) = am^2 + 2amhp + ah^2p^2 + bm + bhp + c$$

Expandindo o produto notável e colocando o termo p em evidência, temos

$$f(m+hp) = (am^2 + bm + c) + p(2amh + aph^2 + bh).$$

Observe que a expressão do primeiro parênteses é igual a $f(m)$, que é igaul a p, assim

$$f(m+hp) = p(1 + 2amh + aph^2 + bh) \tag{3.1}$$

Disto poderíamos concluir que $f(m+hp)$ é composto, já que é igual a p vezes um outro números inteiro, terminando a demonstração. Entretanto, para $f(m+hp)$ ser composto precisamos mostrar que a complicada expressão em parênteses não seja igual a 1. Ou seja

$$1 + 2amh + aph^2 + bh > 1$$

que é equivalente a

$$2amh + aph^2 + bh > 0.$$

Como h é positivo por hipótese, essa última desigualdade é verificada quando

$$2am + aph + b > 0,...$$

isto é, quando

$$h > \frac{-b - 2am}{ap}.$$

Note que $-b-2am$ pode ser um número positivo, baste que b seja negativo e menor que $-2am$.

Com isso, provamos que se $f(x) = ax^2 + bx + c$ é um polinômio com coeficientes inteiros ($a > 0$) e $f(m) = p$ é primo, então $f(m+hp)$ é composto sempre que $h = (-b - 2am)/ap$. Em particular existe uma infinidade de valores inteiros positivos que x pode assumir para que $f(x)$ seja composto.

3.3 Fórmulas exponenciais: números de Mersenne

Existem duas fórmulas exponencias de uma enorme importância na história. Ambas as fórmulas foram estudadas por Matemáticos do século XVII, tais fórmulas são

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

onde n é um inteiro não negativo. Os números da forma de $M(n)$ e $F(n)$ são conhecidos como os números de Mersenne e os números de Fermat, respectivamente.

Como muitos dos conhecimentos matemáticos, os núemros de Mersenne é mais uma questão que herdamos da Grécia. Na numerologia dos pitagóricos um número é considerado perfeito se é igual a metade da soma de todos os seus divisores positivos. Vejamos um exemplo, os divisores de 6 são 1,2,3,6. Somando estes números

$$1 + 2 + 3 + 6 = 12 = 2 \cdot 6.$$

Logo, temos que 6 é um número perfeito. Se compararmos por exemplo com os números primos temos que nenhum é um números perfeito. Já que se p é um número primo seus únicos divisores positivos são 1 e o próprio p e não podemos ter $1 + p = 2P$, a não ser que p seja 1, mas assim p não é um número primo.

Euclides já sabia que os números que são da forma $2^{n-1}(2^n - 1)$ são perfeitos quando $2^n - 1$ é primo. Portanto, para achar número perfeitos pares basta achar os primos de Mersenne.

Os números da forma $2^n - 1$ receberam este nome por causa de uma afirmação de Mersenne que teve um enorme repercussão nos séculos que os seguiram. Segundo Mersenne, os números da forma $2^n - 1$ seriam primos quando

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

e composto para os demais valores de n menores que 257, num total de 44 valores.

Observemos que todos o valores de n, ou os expoentes de $M(n)$, são números primos. Pois, se n for composto, então $M(n)$ também será composto. Vejamos, se $n = rs$ é composto então

$$M(n) = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1).$$

Portanto, se $r|n$, então $M(r)|M(n)$. Entretanto, a reciproca não é verdadeira. Em outra palavras, se n for primo não quer dizes que $M(n)$ é primo. De acordo com Mersenne $M(11)$ deve ser composto. Claro, pois

$$M(11) = 2^{11} - 1 = 2048 - 1 = 2047 = 23 \cdot 89.$$

Como era de costume da época Mersenne não nenhuma justificativa para estes resultados. Tempos mais tarde Pervusin e Seelhof descobriram um erro da lista em 1886. Descobriram que $M(61)$ é primo. Outros erros foram encontrados posteriormente, entre eles estão, $M(89)$ e $M(107)$ que são primos e os compostos $M(67)$ e $M(257)$.

3.4 Fórmulas exponenciais: números de Fermat

Fermat enviou uma carta a outro matemático amador o cavalheiro Frenicle, Fremat enumerou os números da forma $F(n) = 2^{2^n} + 1$ para os valores inteiros de n entre 0 e 6. Tais números são

$$3,\ 5,\ 17,\ 257,\ 65537,\ 4294967297 \text{ e } 18446744073709551617.$$

Depois conjecturou que todos os números da desta forma seriam primos. Impressionante que Fermat não tenha tentado aplicar um método semelhante ao que aplicou para fatorar os números de Mersenne ao último dos números acima, que chamamos de $F(5)$. Foi essencialmente isto que Euler fez quase cem anos mais tarde, obtendo assim o fator primo de $F(5)$.

Também é impressionante que Frenicle não tenha observado o erro de Fermat, já que ele também trabalhava com a fatoração de números de Mersenne.

Apesar de os números de Fermat serem uma rica fonte de números primos, pouco primos de Fermat são conhecidos. Até hoje não se conhecem números primos com $n \geq 5$. É claro que calcular com números de Fermat para valores muitos 'grandes' de n é mais difícil do que os números de Mersenne, já que a fórmula de Fermat é duplamente exponencial.

Assim, encontramos na fórmula de Mersenne uma ferramenta bem útil de produzir primos grandes.

3.5 Fórmulas Fatoriais

Suponhamos que p é um primo positivo. Construiremos uma função semelhante ao fatorial, só que apenas os primos são multiplicados. Vamos chama-la de p^*. Por definição

p^* significa o produto de todos os primos menores ou iguais a p. Por exemplo, $2^* = 2$, e $5^* = 2 \cdot 3 \cdot 5 = 30$. Observe que se $q < p$ são primos sucessivos, então

$$p^* = q^* \cdot p.$$

Estamos interessados nos números da forma p^*+1. Para entender porque observemos a tabela:

p	p^*	$p^* + 1$
2	2	3
3	6	7
5	30	31
7	210	211
11	2310	2311

Todos os números da terceira coluna são primos. Será mera coincidência? Mais ou menos. Paramos maliciosamente em $p = 11$ porque

$$13^* + 1 = 30031 = 59509$$

é composto.

Embora $p^* + 1$ nem seja primo, podemos mostrar que não tem nenhum fator primo menor do que ou igual a p. Usando redução ao absurdo. Digamos, então, que $p + 1$ é divisível por um primo $q \leq p$. Em outras palavras, existe um inteiro positivo r talque $p^* + 1 = q \cdot r$. É melhor escrever esta equação na forma

$$q \cdot r - p^* = 1.$$

Como $q \leq p$, então q é necessariamente um fator de p^*. Logo q divide ambas as parcelas da diferença. Portanto, q—1; isto é, $q = 1$. Mas isto não é possível porque q é primo.

Concluímos que mesmo quando $p^* + 1$ é composto, seu menor fator primo tem que ser maior que p. Em principio isto daria um algoritmo para achar $p^* + 1$. Digamos que conhecemos todos os primos até p. Calculamos então $p^* + 1$ e tentamos fatorá-lo. O problema esta em precisar fatorar $p^* + 1$. Mesmo para valores relativamente pequenos de p, este número é muito grande, de modo que fatorá-lo é impraticável.

Se por acaso $p^* + 1$ for primo, os problema se torna mais fácil. É geralmente mais econômico determinar se um número é primo do que tentar fatorá-lo.

No caso da fórmula fatorial nada disto é de muita ajuda já que $p^* + 1$ raramente é primo. Só são conhecidos 16 primos desta forma. O maior dos quais corresponde a p=24029. Por isso se estendida como maneira de construir primos, a fórmula é um desastre.

3.6 Infinidade de primos

Teorema 3.4. *Existem infinitos números primos.*

Demonstração

Fazendo uma redução ao absurdo. Digamos que há uma quantidade finita de primos, ou seja, exite um que é maior que todos os outros, vamos chama-lo de p. Entretanto, vimos que o número inteiro $p^* + 1$ não pode ter divisores primos $\leq p$. Mas estamos supondo que todos os primos são menores ou iguais a p. Disso concluir que $p^* + 1$ não possui fatores primos, o que contradiz o teorema da fatoração única. Logo existem infinitos números primos

Relembrando o teorema da fatoração única: Dado um inteiro positivo $n > 1$ podemos sempre escrevê-lo, de modo único, na forma

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

3.7 Crivo de Eratóstenes

O crivo de Eratóstenes determina todos os primos até um certo inteiro positivo n previamente escolhido. Para realizar o crivo no lápis e papel procedemos da seguinte maneira. Listamos os primos maiores que 3 até o número n. Comecemos a operar o crivo. O primeiro número da lista é o 3; riscamos os demais números da lista de 3 em 3. Assim riscaremos os múltiplos de 3 maiores que o próprio 3. Depois procuramos o menor número da lista que seja maior que 3, que é o 5. E riscamos os números de 5 em 5, ou os múltiplos de 5. E assim por diante até chegar no núemro n.

Vamos a um exemplo. Seja $n = 35$.

$$3\ 5\ 7\ 9\ 11\ 13\ 15\ 17\ 19\ 21\ 23\ 25\ 27\ 29\ 31\ 33\ 35$$

Vamos riscar os números múltiplos de 3. Maiores que ele próprio

$$3\ 5\ 7\ \not{9}\ 11\ 13\ \not{15}\ 17\ 19\ \not{21}\ 23\ 25\ \not{27}\ 29\ 31\ \not{33}\ 35$$

Em seguida procuramos o números da lista maior que o 3, neste caso o números 5 e riscamos os seus múltiplos.

$$3\ 5\ 7\ \not{9}\ 11\ 13\ \not{15}\ 17\ 19\ \not{21}\ 23\ \not{25}\ \not{27}\ 29\ 31\ \not{33}\ \not{35}$$

Ao final da terceira passagem do crivo, que seria com os múltiplos de 7, a lista continua a mesma acima. Na verdade nenhuma passagem posterior do crivo vai eliminar nenhum número desta lista. Logo os números primos ímpares positivo menores que 35 são os não foram eliminado, ou seja

$$3\ 5\ 7\ 11\ 13\ 17\ 19\ 23\ 29\ 31$$

Capítulo 4

Congruência - Aritmética modular

Uma ferramenta importante na Teoria dos números é a aritmética modular, ao qual envolve o conceito de congruência. De acordo com (Sá, 2010) uma congruência é uma relação entre dois números que ao ser dividido por um terceiro tem o mesmo resto da divisão. Foi o matemático Gauss o primeiro a perceber essa relação que introduziu uma notação específica para este fato e que denominou de **congruência**.

4.1 Relações de equivalência

Definição 4.1. Seja R uma relação de equivalência definida sobre o conjunto não vazio A. Dizemos que R é uma relação de equivalência se satisfaz as seguintes propriedades.

1. $x \in A \Longrightarrow xRx, \forall x.$
2. $x, y \in A \; e \; xRy \Longrightarrow yRx, \forall x, y.$
3. $x, y, z \in A \; e \; xRy \; e \; yRz \Longrightarrow xRz, \forall x, y, z.$

As subdivisões de um conjunto A produzidas por uma relação de equivalência R são chamadas classes de equivalência.

Seja A um conjunto e R uma relação de equivalência em A, se $x \in$ A então a classe de equivalência de x é o conjunto dos elementos de A que são equivalentes a x por R. Denotamos $\overline{x}$ a classe de equivalência de x em:

$$\overline{x} = \{y \in X : yRx\}$$

Por um único elemento de uma classe de equivalência podemos definir toda a classe, em simbolo

$$x \in X \quad e \quad y \in \overline{x} \quad \Rightarrow \quad \overline{x} = \overline{y}$$

$$x \in X \quad e \quad y \in \overline{x} \Longrightarrow \overline{x} = \overline{y}$$

Demonstração

Temos que provar que $\overline{x} \subseteq \overline{y}$ e $\overline{y} \subseteq \overline{x}$.

1. $\overline{x} \subseteq \overline{y}$

   Se $a \in \overline{x}$, temos aRx. Mas $yR\overline{x}$, portanto, yRx, por simetria xRy. Por transitividade, aRy, isto é, $aR\overline{y}$. Logo, $\overline{x} \subseteq \overline{y}$.

2. $\overline{y} \subseteq \overline{x}$

   Se $a \in \overline{y}$ então aRy, mas yRx, logo, aRx. Ou melhor $a \in \overline{x}$. Assim, $\overline{y} \subseteq \overline{x}$.

   Logo

$$\overline{x} = \overline{y}.$$

que é o que queríamos provar.

Agora consideremos o conjunto

$$A = \{(a, b) \in \mathbb{Z}x\mathbb{Z}^* : b \neq 0\}$$

define a seguinte relação:

$$(a, b)R(a', b') \Longleftrightarrow ab' = a'b.$$

verifiquemos A se é realmente uma relação de equivalência.

Prova:

1. Reflexiva

   $(a, b) \in A$; $ab \Rightarrow ab = ab$, portanto temos que, $(a, b)R(a, b)$.

2. Simetrica

   (a, b) e $(c, d) \in A$; $(a, b)R(c, d) \Longleftrightarrow ad = cb \Longleftrightarrow cb = ad \Longleftrightarrow (c, d)R(a, b)$.

3. Transitiva

   $(a, b), (c, d)$ e $(e, f) \in A$; queremos mostrar que $(a, b)R(c, d)$ e $(c, d)R(e, f) \Longrightarrow (a, b)R(e, f)$, ou melhor, que $af = eb$.

$(a,b)R(c,d) \iff ad = cb$

e $\{b,d \text{ e } f \neq 0\}$

$(c,d)R(e,f) \iff cf = ed$

$$\begin{array}{cc} ad = cd & ({}_xf) \\ f(ad) = f(cd) & \text{associar} \\ (fa)d = (fc)b & \text{comutar} \\ (af)d = (cf)b & \text{substituindo } (cf = ed) \\ (af)d = (ed)b & \text{associar} \\ (af)d = e(db) & \text{comutar} \\ (af)d = e(bd) & \text{associar} \\ (af)d = (eb)d & \text{Lei do cancelamento} \end{array}$$

Temos,

$$(af) = (eb),$$

ou seja,

$$(a,b)R(e,f).$$

4.2 Inteiros módulo n

Definição 4.2. Sejam dois inteiros a e b quaisquer e seja n um inteiro positivo. Dizemos que a é congruente a b módulo n se, e somente se, $n|a-b$.

a é congruente a b módulo n se, e somente se, existe um inteiro k, talque, $a-b = kn$.

Notação

$$a \equiv b(\text{mod } n) \Leftrightarrow n|a-b$$

ou seja

$$a \equiv b(\text{mod } n) \Leftrightarrow \exists k \in \mathbb{Z} : a-b = kn.$$

Exemplo 4.3. Para n=5 e n=7

$n = 5 \quad \longrightarrow \quad 10 \equiv 0(\text{mod } 5) \quad \text{e} \quad 14 \equiv 24(\text{mod } 5)$

$n = 7 \quad \longrightarrow \quad 10 \equiv 3(\text{mod } 7) \quad \text{e} \quad 14 \equiv 0(\text{mod } 7)$

Vamos verificar que a concruência módulo n é uma relação de equivalência, ou seja, deve atender as propriedades: reflexiva, simétrica e transitiva.

Prova:

i) Reflexiva

De fato, como $n|0$, ou seja, $n|a-a$, ou melhor, $a \equiv a(\text{mod } n)$.

ii) Simetrica

$a \equiv b(\text{mod } n) \quad \Leftrightarrow \quad a-b=kn$, para algum inteiro $k \quad \Leftrightarrow \quad -a+b=-kn \quad \Leftrightarrow$ $b-a=(-k)n \quad \Leftrightarrow \quad b \equiv a(\text{mod } n)$.

iii) Transitiva

$$\begin{array}{cc} a \equiv b(\text{mod } n) \text{ e } & b \equiv c(\text{mod } n) \\ a-b=kn & b-c=kn \\ n|a-b & n|b-c \end{array}$$

Como n divide $(a-b)$ e $(b-c)$, então n divide a soma

$$n|(a-b)+(b-c) \Leftrightarrow n|a-c$$

$$a \equiv c(\text{mod } n)$$

.

O conjunto que nos interessa é p conjunto quociente $\mathbb{Z}$ pela a relação de congruência módulo n.

Notação: $\mathbb{Z}_n$ − conjunto dos inteiros módulos n.

Elementos de $\mathbb{Z}_n$. As classe de equivalência da congruência módulo n são os subconjuntos de $\mathbb{Z}$.

Seja

$$\overline{a}=\{x \in \mathbb{Z}/xRa\}$$

$$\overline{a}=\{x \in \mathbb{Z}/x \equiv a(\text{mod } n)\}$$

$$\overline{a}=\{x \in \mathbb{Z}/n|x-a\}$$

$$\overline{a}=\{x \in \mathbb{Z}/x-a=nk; k \in \mathbb{Z}\}$$

$$\overline{a}=\{x \in \mathbb{Z}/x=a+nk; k \in \mathbb{Z}\}$$

$$\overline{a}=\{a+nk/k \in \mathbb{Z}\}.$$

Em particular $\overline{0}$ é o conjunto dos múltiplos de n. Se $a \in \mathbb{Z}$, então podemos dividi-lo por n, obtendo q e r inteiros, tais que

$$a = qn + r \qquad\qquad 0 \leq r \leq n-1.$$

Logo $a - r = qn \iff a \equiv r (\text{mod } n)$.

Um inteiro qualquer é congruente módulo n a um inteiros no intervalo de 0 a $n-1$. Assim, o conjunto quociente $\mathbb{Z}_n$ é formado pelas classes $\overline{0}, \overline{1}, \cdots, \overline{n-1}$, onde duas dessa classes não podemos ser iguais.

Resumindo

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \cdots, \overline{n-1}\right\} \text{ Forma reduzida.}$$

4.3 Aritmética modular

Para operar uma soma com elemento de $\mathbb{Z}_n$ precisamos entender que difere um pouco da soma casual. Vamos imaginar que temos um "relógio de n horas, com um ponteiro". Imaginemos que as classes de $\overline{0}$ a $\overline{n-1}$ estão dispostas ao longo da circunferência, em intervalos iguais, no sentido horário. Tomando isto temos uma *máquina de calcular* para operar em $\mathbb{Z}_n$.

Vejamos como funciona a maquina. Por exemplo, para somar duas classes $\overline{a}$ e $\overline{b}$, colocamos o ponteiro na classe a e depois o movemos b unidades no sentido horário. O resultado da soma é classe ao qual o ponteiro se localiza depois de movido. Por exemplo, para somar $\overline{5}$ e $\overline{4}$ em $\mathbb{Z}_8$, colocamos o ponteiro em $\overline{5}$ e o movemos quatro casas, no sentido horário. Quando movemos três casas estamos de volta ao $\overline{0}$, continuamos mais um casa e o ponteiro fica apontado para $\overline{1}$. Logo $\overline{5} + \overline{4} = \overline{1}$ em $\mathbb{Z}_8$.

Entretanto, é máquina de calcular não é muito prática para valores de n muito 'grandes'. Então precisamos descrever esta mesma operação de uma forma mais prática, ou seja, de modo matemático. Sejam $\overline{a}$ e $\overline{b}$ as classes de $\mathbb{Z}_n$ que desejamos somar. A fórmula para a operação é a seguinte

$$\overline{a} + \overline{b} = \overline{a+b}.$$

De acordo com a fórmula para somar $\overline{5}$ a $\overline{4}$ somamos os inteiros 5 e 4, obtendo o

resultado 9; logo $\overline{5}+\overline{4}=\overline{9}$. O resultado deu parece que deu diferente da soma do relógio. Mas, como $9-1=8$, temos que 1 e 9 estão na mesma classe de equivalência módulo 8, já que 9 dividido por 8 deixa resto 1, $9=8\cdot 1+1$.; isto é $\overline{9}=\overline{1}$.

Agora, quem nos garante que escolhendo elementos distintos da cada classe não obtemos um resultado diferente? Somamos os as classes $\overline{5}$ e $\overline{4}$ usando o elemento 5 da primeira e o elemento 4 da segunda. Mas $\overline{13}=\overline{5}$ e $\overline{12}=\overline{4}$, já que, $13=8\cdot 1+5$ e $12=8\cdot 1+4$, respectivamente. o que aconteceria de se somássemos as classes $\overline{13}$ e $\overline{12}$? O resultado da soma tem que igual a 1. De acordo com a fórmula

$$\overline{13}+\overline{12}=\overline{13+12}=\overline{25}.$$

Temos que $25=8\cdot 3+1$, ou seja, $\overline{25}=\overline{1}$.

Temos que qualquer que sejam os representantes das classes escolhidos para efetuar a soma de duas classes, o resultado sempre é a mesma classes. Verifiquemos. Em $\mathbb{Z}_n$, temos $\overline{a}$ e $\overline{b}$, onde $\overline{a}=\overline{a'}$ e $\overline{b}=\overline{b'}$. Queremos verificar que $\overline{a+b}=\overline{a'+b'}$. Mas $a=a'$ que equivale a $a-a'=kn$, para algum inteiro k; o mesmo acontece para $b-b'$. Somando os dois múltiplo de n teremos um múltiplo de n, logo

$$(a-a')+(b-b')=(a+b)-(a'+b')$$

é múltiplo de n. Portanto, $(a+b)=(a'+b')$.

A forma para multiplicar as classes $\overline{a}$ e $\overline{b}\in\mathbb{Z}_n$ é

$$\overline{a}\cdot\overline{b}=\overline{a\cdot b}.$$

Digamos que $\overline{a}=\overline{a'}$ e $\overline{b}=\overline{b'}$, e queremos mostrar que $\overline{ab}=\overline{a'b'}$. Como $a=a'$ é múltiplo de n, então $a=a'+kn$, para algum inteiro k. Também temos $b=b'$ e $b=b'+rn$, para algum inteiro r. Multiplicando

$$ab=(a'+kn)(b'+rn)=a'b'+a'rn+b'kn+krn^2=a'b'+(a'r+b'k+krn)n.$$

Logo $ab-a'b'$ é um múltiplo de n. Portanto, $\overline{ab}=\overline{a'b'}$, que é o que queríamos provar.

Com isso temos algumas propriedades muito semelhantes às operações em $\mathbb{Z}$. Sejam $\overline{a},\overline{b}$ e $\overline{c}$ elemento de $\mathbb{Z}_n$. Temos as seguinte propriedades com respeito a adição:

i) $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$

ii) $\overline{a}+\overline{b}=\overline{b}+\overline{a}$

iii) $\overline{a}+\overline{0}=\overline{a}$

iv) $\overline{a}+\overline{-a}=\overline{0}$

e as seguintes propriedades com respeito a multiplicação:

v) $(\overline{a}\cdot\overline{b})\cdot\overline{c}=\overline{a}\cdot(\overline{b}\cdot\overline{c})$

vi) $\overline{a}\cdot\overline{b}=\overline{b}\cdot\overline{a}$

vii) $\overline{a}\cdot\overline{1}=\overline{a}$

Ainda há uma propriedade que relaciona as duas operações, a *distributividade*:

$$\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.$$

Até então, pode-se pensar que por uma pequena diferença nas definições, as operações de $\mathbb{Z}_n$, são como as operações de $\mathbb{Z}$. Mas aqui temos um exemplo que quebra isso.

Exemplo 4.4. Multipliquemos os elementos $\overline{2}$ e $\overline{3}$ pertencentes a $\mathbb{Z}_6$.

As classes $\overline{2}$ e $\overline{3}$ são, evidentemente, diferentes da classe $\overline{0}$. Entretanto

$$\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}.$$

4.4 Critérios de divisibilidade

Para cerificar se um número é divisível por 3 é bem simples. Basta soma os algarismos do número se o resultado for divisível por 3 então o números original também é divisível. Vamos provar isto usando congruência módulo 3.

Prova: Utilizando congruência módulo 3.

Seja a um número inteiro, e que a seja

$$a=a_n a_{n-1}\cdots a_1 a_0$$

onde a_0 é o algorismo da unidades, a_1 o da dezenas e assim por diante. Em outras palavras,

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0.$$

Temos que $10 \equiv 1 \pmod 3$. Logo qualquer potência de 10 é congruente a 1 módulo 3. Assim,

$$a \equiv a_n + a_{n-1} + \cdots + a_1 + a_0 \pmod 3.$$

Se o segundo termo acima é divisível por 3, então

$$a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 3.$$

Concluindo,

$$a \equiv 0 \pmod 3$$

Portanto, $3|a$ se, e somente se, $3|a_n + a_{n-1} + \cdots + a_1 + a_0$.

Oberserve que o cálculo acima também funciona para o número 9. Se substituimos 3 por 9, temos $10 \equiv 1 \pmod 9$. Então $9|a \Leftrightarrow 9|a_n + a_{n-a} + \cdots + a_1 + a_0$.

Vejamos o que obtemos para 11. Seja,

$$a = a_n 10^n + a_{n-1} 10^{n-1} \cdots a_1 + a_0.$$

onde

$$a_n, a_{n-1}, \cdots, a_1 + a_0 \text{ são os algarismos de } a.$$

Observe que

$$10 \equiv (-1) \pmod{11}, \text{portanto,}$$

$$10^k \equiv (-1)^k \pmod{11}.$$

que é igual a 1 ou -1 dependendo da paridade de k. Assim

$$a = a_n(-1)^n + a_{n-1}(-1)^{n-1} + \cdots + a_2 - a_1 + a_0 \pmod{11}.$$

Logo temos que, 11 divide a se, e somente se, 11 divide a soma alternada dos algarismo de a.

Exemplo 4.5. Verifiquemos se 11 divide 3443?

Temos que $3 - 4 + 4 - 3 = 0$, como $11|0$, então $11|3443$.

4.5 Potências

Vejamos como calcular o resto de uma divisão de uma potência por um número qualquer.

Exemplo 4.6. Quanto é o resto da divisão de 10^{135} por 7?

Temos que, $10^6 \equiv 1 \pmod 7$,

$$6|135 \Rightarrow 135 = 6 \cdot 22 + 3, \text{logo}$$

$$10^{135} \equiv (10^6)^{22} + 10^3 \pmod 7$$

$$(10^6)^{22} + 10^3 \equiv (1)^{22} \cdot 10^3 \pmod 7$$

$$(1)^{22} \cdot 10^3 \equiv 6 \pmod 7.$$

Logo o resto da divisão é 6.

Nem sempre é tão fácil.

Exemplo 4.7. Qual o resto da divisão de 3^{64} por 31, ou melhor, $31|3^{64}$?

Ao invés de tentar descobrir uma potência de 3 cujo o resto da divisão por 31 da 1, usamos que

$$64 = 3 \cdot 21 + 1.$$

Obtemos então a seguinte congruência módulo 31.

$$3^{64} \equiv (3^3)^{21} \cdot 3 \equiv (-4)^{21} \cdot 3 \equiv -(2)^{42} \cdot 3,$$

não chegamos onde queriamos. Mas temos $2^5 \equiv 1 \pmod{31}$, então usaremos que $42 = 8 \cdot 5 + 2$, assim

$$3^{64} \equiv -(2)^{42} \cdot 3 \equiv -(2^5)^8 \cdot 2^2 \cdot 3 \equiv -12 \pmod{31}.$$

Como $-12 \equiv 19 \pmod{31} \Rightarrow\ -12 = 31(-1) + 19$. Então o resto da divisão de 3^{64} por 31 é 19.

Agora vejamos qual é o menor expoente r talque $3^r \equiv 1 \pmod{31}$

Temos $31|3^r - 1 \Rightarrow 3^r - 1 = 31q$, para algum inteiro q. $3^r - 1 = 31q \Rightarrow 3^r = 31q + 1$. Logo se $r = 0$, então, $31|3^0 - 1 \Rightarrow 31|1 - 1 \Rightarrow 31|0$, ou seja, $1 = 31q + 1 \therefore q = 0$

Então o menor valor de r é 0(zero), para que $3^r \equiv 1 \pmod{31}$.

4.6 Equações Diofantinas

Equações de várias incógnitas com coeficientes inteiros denominam-se equações diofantinas. Por exemplo, $3x - 2y = 1$, $x^3 + y^3 = z^3$ e $x^3 - 117y^3 = 5$.

Como as equações têm várias variáveis, pode haver infinitas soluções. Por exemplo, $x = 1 + 2k$ e $y = 1 + 3k, \forall k \in \mathbb{Z}$, satifaz a equação $3x - 2y = 1$

Verfiquemos se $x = 1 + 2k$ e $y = 1 + 3k$ é solução da equação $3x - 2y = 1$.

Temos que para uma equação do tipo $ax + by = c$ ter solução $d = \text{mdc}(a, b)$ tem que dividi c. Assim temos que $\text{mdc}(3, -2)$

$$3 = -2(-1) + 1$$

$$-2 = -1(2) + 0,$$

tem que o último resto não nulo é 1, então o $\text{mdc}(3, -2) = 1$ e como $d|c$, ou melhor, $1|1$. Assim a equação tem solução.

Agora, encontremos os valores de x e y. Primero encotremos x_0 e y_0 que satisfaça

$$1 = 3x_0 + 2y_0$$

neste casso, temos

$$1 = 3(1) + 2(-1),$$

ou seja,

$$x_0 = 1 \text{ e } y_0 = 1$$

Então encontramos uma solução da equação. Agora generalizemos e encontremos a

solução geral. Temos que a solução geral a da forma

$$x = x_0 + (\frac{b}{d})k \quad \text{e} \quad y = y_0 - (\frac{a}{d})k,$$

assim a solução geral é

$$x = 1 + 2k \quad \text{e} \quad y = 1 + 3k$$

que é a solução que queriamos encontrar.

Vamos centrar o foco em relação a equação $x^3 - 117y^3 = 5$ já que D.J. Lewis afirmou que essa equação tem no máximo 18 soluções. Dois depois dessa afirmação provaram que essa equação não possui nenhuma solução inteira. Entretanto, os métodos utilizados não são normalmente estudados em um curso de graduação em matemática. Contudo existe uma maneira muito fácil de verificar se isso é verdade, atravéz de congruência módulo 9.

Prova:

Suponhamos que $x^3 - 117y^3 = 5$ tem solução inteira. Isto é, $\exists x_0, y_0$ tais que

$$x_0^3 - 117y_0^3 = 5 \qquad \text{(Relação entre números inteiros).}$$

Logo, podemos reduzi-la módulo 9. Como $117 = 9 \cdot 13 + 0$, ou seja, $9|117$. Obtemos

$$x_0^3 \equiv x_0^3 - 117y_0^3 \equiv 5 \pmod 9.$$

Assim, se a equação tem solução inteira x_0 *e* y_0, então, $x_0^3 \equiv 5 \pmod 9$. Mas será que isso é possível? Basta calcular o cubo módulo 9 de cada um dos elementos das classes distintas módulo 9 para ver se algum deles é congruente a 5.

classes módulo 9: $\overline{0}$ $\overline{1}$ $\overline{2}$ $\overline{3}$ $\overline{4}$ $\overline{5}$ $\overline{6}$ $\overline{7}$ $\overline{8}$

cubos módulo 9: $\overline{0}$ $\overline{1}$ $\overline{8}$ $\overline{0}$ $\overline{1}$ $\overline{8}$ $\overline{0}$ $\overline{1}$ $\overline{8}$

Logo, o cubo de qualquer inteiro é congruente módulo 9 a 0,1 ou 8. Em particular $x_0^3 \equiv 5 \pmod 9$ não tem solução. Portanto, a equação $x^3 - 117y^3 = 5$ não tem soluções inteiras.

4.7 Divisão modular

Sejam $a, b \in \mathbb{R}$. Quando dividimos a por b é equivalente a multiplicar a por $1/b$. $1/b = b'$, onde, b' é o inverso de b. Então $b \cdot (1/b) = 1 = b \cdot b'$, isso para $b \neq 0$. Assim, o número real n só tem inverso se $n \neq 0$.

Transpondo para o $\mathbb{Z}_n$. Digamos que $\overline{a} \in \mathbb{Z}_n$. Diremos que a classe $\overline{a'} \in \mathbb{Z}_n$ é o inverso de $\overline{a}$ se, e somente se, $\overline{a} \cdot \overline{a'} = \overline{1} \in \mathbb{Z}_n$. Se $\overline{a} = \overline{0}$, $\overline{a}$ não tem inverso. Entretanto, em $\mathbb{Z}_n$ pode haver outros elementos sem inverso além de $\overline{0}$.

Teorema 4.8 (Teorema de Inversão)**.** *A classe $\overline{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, a e n são primos entre si.*

Demonstração:

($\Rightarrow$) Suponhamos que $\overline{a} \in \mathbb{Z}_n$ tem inverso $\overline{a'}$. A equação $\overline{a} \cdot \overline{a'} = 1$ corresponde dizer que $n|aa' - 1$. Isto é

$$aa' + kn = 1, \quad \text{para algum inteiro } k.$$

Isto implica que o mdc(a, n)=1. Concluímos que se $\overline{a}$ tem inverso. o mdc(a, n)=1.

($\Leftarrow$) Agora, suponhamos que $a \in \mathbb{Z}$ e mdc(a, n)=1.

Aplicando o algoritmo euclidiano estendido aos números a e n para obter inteiros a' e y_0 tais que

$$aa' + ny_0 = 1$$

é equivalente a

$$\overline{a} \cdot \overline{a'} = \overline{1} \ \text{ em } \ \mathbb{Z}_n.$$

Logo a classe $\overline{a'}$ é o inverso de $a \in \mathbb{Z}_n$. Concluímos que se mdc(a, n)=1, então $\overline{a}$ tem inverso em $\mathbb{Z}_n$.

O conjunto dos elementos de $\mathbb{Z}_n$ que têm inverso é importante e vamos denotá-lo por U(n). De tal modo que

$$U(n) = \{\overline{a} \in \mathbb{Z}_n / \text{mdc}(a, n) = 1\}.$$

É fácil calcular U(p) para p primo, já que o mdc(a,p)=1 para qualquer $a \in \mathbb{Z}$ o que quer dizer que p não divide a. Se p dividi a, então $\overline{a} = \overline{0}$.

Quando p é primo todas as classes diferente de $\overline{0}$ tem inverso. Mas o que acontece

quando n é um número composto é ilustrado nos seguintes exemplos:

$$U(4) = \{\overline{1}, \overline{3}\} \qquad \text{e} \qquad U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}.$$

Propriedade:

Se $\overline{a}, \overline{b} \in \mathbb{Z}_n$ tem inverso, então $\overline{a} \cdot \overline{b}$ também tem inverso em $\mathbb{Z}_n$.

Prova

Digamos que $\overline{a}$ tem inverso $\overline{a'}$ e $\overline{b}$ tem inverso $\overline{b'}$; $\overline{a}, \overline{b} \in \mathbb{Z}_n$. Temos

$$(\overline{a} \cdot \overline{b})(\overline{a'} \cdot \overline{b'}) = (\overline{a} \cdot \overline{a'}) \cdot (\overline{b} \cdot \overline{b'}) = \overline{1} \cdot \overline{1} = \overline{1}.$$

Agora, vamos executar divisões em $\mathbb{Z}_n$.

Se queremos dividir $\overline{a}$ por $\overline{b}$ precisamos saber se $b \in U(n)$. Se $b \notin U(n)$, então $\overline{a} \nmid \overline{b}$. Se não estiver a divisão não é possível. Se estiver, digamos que $\overline{b'}$ é o inverso de $\overline{b}$ e dividimos $\overline{a}$ por $\overline{b}$.

Exemplo 4.9. Calcule $\overline{2} \mid \overline{3}$ em $\mathbb{Z}_8$.

Como o mdc(3,8)=1, então $\overline{3}$ tem inverso em $\mathbb{Z}_8$.

$$\overline{3} \cdot x = \overline{1}$$

$$\overline{3} \cdot \overline{3} = \overline{9} = \overline{1},$$

assim, o inverso de $\overline{3}$ é o próprio $\overline{3}$ em $\mathbb{Z}_8$.

Então,

$$\overline{2} \equiv \overline{3} \pmod 8$$

$$\overline{2} \cdot \overline{3} \equiv \overline{3} \cdot \overline{3} \pmod 8$$

$$\overline{6} \equiv \overline{1} \pmod 8.$$

Portanto,

$$\overline{2} \mid \overline{3} = \overline{6} \ \text{ em } \ \mathbb{Z}_8$$

Entretanto, $\overline{2}$ não tem inverso em $\mathbb{Z}_8$, mas isso não tem importância já que $\overline{2}$ é o dividendo.

Usando o que foi estudado, vamos resolver congruências lineares em $\mathbb{Z}_n$. Uma congruência linear é do tipo

$$ax \equiv b \pmod{n}, \qquad a, b \in \mathbb{Z}.$$

Para resolver precisamos encontrar o "x", ou seja, dividir tudo por a para deixar o lado esquerdo livre, só com o "x". Ou seja, $\overline{a'}$ é o inverso de $\overline{a} \in \mathbb{Z}_n$. Multiplicando a equação com a', temos

$$aa'x \equiv a'b \pmod{n},$$

como $aa' = 1$,

$$x \equiv a'b \text{ (mdod } n)$$

Exemplo 4.10. Resolva: $7x \equiv 3 \pmod{15}$

Como $15 + 7x = 1 \Rightarrow 15 + 7(-2) = 1$, então o inverso de 7 e $\overline{-2} = \overline{13}$ em $\mathbb{Z}_15$. Multiplicando a congruência por 13, temos

$$x \equiv 13 \cdot 3 \equiv 39 \equiv 9 \pmod{15}. \qquad \text{(Solução)}$$

Concluímos que se o $\text{mdc}(a, n) = 1$, então a congruência linear $ax \equiv b \pmod{n}$ tem uma, e só uma, solução em $\mathbb{Z}_n$. Caso que pode não ocorrer se o $\text{mdc}(a, n) \neq 1$. Por exemplo, a equação $2x \equiv 1 \pmod{8}$ não tem solução.

Capítulo 5

Mersenne e Fermat

A fórmula mais inesgotável de produzir primos ‘’grandes” é através das fórmulas exponenciais. As mais importantes e antigas são as associadas aos nomes Mersenne e Fremat matemáticos do século XVII. São essas fórmulas que abordaremos nesse capitulo e a qual usamos para encontrar os números primos utilizados nas chaves de codificação e decodificação do sistema RSA.

5.1 Números de Mersenne

Seja o n-éssimo número de Mersenne

$$M(n) = 2^n - 1$$

com $n \in \mathbb{Z}_+$. Se n for composto, $M(n)$ também será composto. Seja, $n = rs$, então

$$2^n - 1 = (2^r)^s - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots + 2^r + 1).$$

Assim, $M(r)$ é fator de $M(n) = M(rs)$. Facilmente, $M(s)$ também é uma faotr de $M(n)$.

Portanto, para obter primos entre os números de Mersenne devemos procurar entre $M(p)$, com p primo. Entretanto, fato de p ser primo não é suficiente para garanti que $M(p)$ seja primo.

Vamos descrever um método, devido a Fermat, que permite encontrar fatores para números de Mersenne não muito ‘grandes’, de maneira eficiente. Para descrever o método precisamos de um resultado complementar ao teorema de lagrange. Seja o seguinte lema.

Lema 5.1 (Lema Chave)**.** *Digamos que G é um grupo finito munido de uma operação $*$ e seja $a \in G$. Um inteiro positivo t satisfaz $a^t = e$ se, e somente se, t é divisível pela a ordem de a.*

Demonstração

($\Leftarrow$)Chamaremos a ordem de a de s. Se s divide t, então, $t = sr$, para alguns inteiro r positivo, assim

$$a^t = (a^s)^r = e^r = e.$$

($\Rightarrow$)Suponhamos que $a^t = e$, como a ordem é o menor inteiro positivo, s, tal que $a^s = e$, então $s \leq t$. Dividindo t por s,

$$t = sq + r, \qquad 0 \leq r < s.$$

Assim

$$e = a^t = a^{sq+r} = (a^s)^q * a^r = e^q * a^r = e * a^r = a^r.$$

Como $r < s$ isto so pode acontecer se $r = 0$, ou teríamos uma contradição ao fato de s ser a ordem de a.

□

Voltando aos números de Mersenne. Digamos que $p \neq 2$ é um número primo e que q é um fator de $M(P) = 2^-1$. Então

$2^p - 1 = qz$, para alguns inteiro z;

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

Podemos ler essa equação como uma identidade do grupo $\mathrm{U}(q) = \mathbb{Z}_q \ \{\overline{0}\}$ a saber

$$\overline{2}^p = \overline{1}.$$

Teorema 5.2 (Método de Fermat)**.** *Seja $p \neq 2$ um primo e q um fator primo de M(p). Então q=1+2rp, para algum inteiro positivo r.*

Pelo o lema, a ordem de $\overline{2}$ deve dividir p. Mas como p é primo, então $\overline{2}$ tem ordem 1 ou p. Como $p \neq 2$, por hipótese $\overline{2}$ tem ordem p.

Pelo o terma de Fermat

$$\overline{2}^{q-1} = \overline{1}, \qquad \mathrm{U}(q).$$

Pelo o lema a ordem de 2 divide $q-1$. Então existe um k inteiro, tal que, $q-1=kp$. Sendo mais preciso, $M(P)=2^p-1$ é um número ímpar, assim todo fator de $M(p)$ é ímpar. Em particular,q é ímpar. Portanto, $q-1$ é par. Como p também é impar, concluímos que k tem que ser par. Assim, $q-1=2rp$, para algum r inteiro. Assim, provamos o resultado.

Vamos usar esse método para encontrar um fator de $M(11)=2047$. Pelo método, temos que qualquer fator primo de $M(11)$ é da forma, $q=1+22r$. Agora é atribuir valores a r e ir testando a cada caso para observar se temos um fator primo ou não. Mas podemos estimar quantos valores de r será necessário testar no pior dos casos para acharmos um fator primo.

Temos que se $M(p)$ for composto, então tem um fator menor ou igual a $\sqrt{M(P)}$. Logo

$$\sqrt{M(p)} \geqq = 1+2rp.$$

Temos que

$$\sqrt{M(p)} < 2^{p/2},$$

assim,

$$2^{p/2} > \sqrt{M(p)} \geq 1+2rp$$
$$2^{p/2} > 1+2rp$$
$$r > \frac{2^{p/2}-1}{2p}.$$

Portanto, quando $p=11$, isto dá $r<2$. Não poderia ser melhor, só temos que tentar $r=1$. Fazendo $r=1$, temos $q=23$, que é fator de 2047. Um outro fator primo é $89=1+44\cdot 2$. Não usando o método teríamos que tentar achar um fator primo entre os números menores que $\sqrt{M(p)}$, que neste caso seria $\left[\sqrt{M(11)}\right] = \left[\sqrt{2047}\right]$ =45. Assim. teríamos que testar todos os primos ímpares até 45, que são 13 primos.

5.2 Números de Fermat

Consideremos números da forma 2^n+1. Desejamos saber quando estes números podem ser primos. Suponhamos que $p=2^+1$ é primo. Assim, temos

$$\overline{2}^n = -\overline{1} \quad \text{em} \quad \mathrm{U}(p). \tag{5.1}$$

Portanto,

$$\overline{2}^{2n} = \overline{1} \quad \text{em} \quad \mathrm{U}(p).$$

Logo, temos que a ordem de $\overline{2}$ divide $2n$. Calculemos exatamente. Pela a equação (8.1) a ordem de $\overline{2}$ não pode ser n, nem um divisor de n¿ Mas como a ordem divide $2n$, então é múltiplo de 2. Digamos que a ordem seja $2r$, onde r é um inteiro positivo que divide n.

Assim,

$$\overline{2}^{2n} = \overline{1} \quad \text{em} \quad \mathrm{U}(p).$$
$$\overline{0} = \overline{2}^{2r} - \overline{1} = (\overline{2}^{r} - \overline{1})(\overline{2}^{r} + \overline{1})$$

em $\mathbb{Z}_p$. Como a nossa suposição é que p seja primo, podemos concluir que

$$2^r \equiv 1 \ (\mathrm{mod}\ p) \quad \text{ou} \quad 2^r \equiv -1 \ (\mathrm{mod}\ p) >$$

Ou seja, p divide $2^r + 1$ ou $2^r - 1$. Mas, temos que $p = 2^n + 1$ e $n > r$, onde temos uma contradição. Logo, $n = r$ e a ordem de $\overline{2}$ em U(p)$\in 2n$.

Como $p - 1 = 2^n$, temos pelo o teorema de Fermat que

$$\overline{2}^{2n} = \overline{1} \quad \text{em} \quad \mathrm{U}(p).$$

Logo a ordem de $\overline{2}$, que é $2n$, divide 2^n. Assim, em particular, concluímos que n é uma potência de 2, ou seja, $2^n + 1$ só é primo quando n é uma potência de 2. Por isso, o nosso interesse será apenas nos números da forma $2^{2^k} + 1$. Estes são os números de Fermat, denotados por F(k).

Em uma carta enviada ao cavaleiro Frenicle, Fermat sugeriu que todos os números dessa forma seriam sempre primos. De fato, F(k) é primo para $0 \leq k \leq 4$. Para valores maiores F(s) é composto, que foi demonstrado pelo o Matemático L. Euler em 1730. O método adotado por Euler copia o método inventado por Fermat para achar fatores de números de Mersenne. Vejamos o método.

Teorema 5.3 (Método de Euler)**.** *Se q é um fator primo de* F*(k) então existe um número inteiro positivo r tal que $q = 1 + 2^{k+1}r$.*

Demonstração

Digamos que q é um fator primo de F(k). Então,

$$\overline{2}^{2^k} = -\overline{1} \quad \text{em} \quad \text{U}(q). \tag{5.2}$$

Segue que a ordem de $\overline{2}$ divide 2^{k+1}, e a equação (8.2) nos diz que a ordem não pode ser uma potência menor que 2^{k+1}. Portanto, a ordem de $\overline{2}$ em U(q) é, exatamente, 2^{k+1}. Mas, pelo o teorema de Fermat, a ordem de $\overline{2}$ divide $q-1$, desse modo, $q-1 = 2^{k+1}r$.

□

Vamos determinar um fator de F(5)=$2^{2^5}+1 = 2^{32}+1$. Pelo o método de Euler um fator primo de F(5) tem que ter a forma $q = 1+64r$, $\forall r \in \mathbb{Z}$. A divisibilidade por q para valores de r são os quais

$$q < \sqrt{2^{32}+1} \leq 66000.$$

Isto nos dá $r < 1031$, um número muito grande. Temos que o menor valor de r para que $q$seja primo é 3, que dá $q = 193$. Fazendo a conta

$$2^{32} \equiv (2^8)^4 \equiv 63^4 \equiv 108 \pmod{193}.$$

Portanto, 193 não é fator de F(5). Para $r = 4$, temos $q = 257$ que é primo. Mas,

$$2^{32} \equiv 1 \pmod{257},$$

temos que 257 também não é fator de F(5).

O próximo valor de r que produz um primo é $r = 7$, onde $q = 449$. Mas,

$$2^{32} \equiv (2^{16})^2 \equiv 431^2 \equiv 324 \pmod{449};$$

logo 449 não é fator. O próximo valor é $r = 9$, onde $q = 577$. Neste caso,

$$2^{32} \equiv 287 \pmod{577}.$$

De modo que 577 também não fator de F(5).

Finalmente, quando $r = 10$, temos $q = 641$, que é fator de F(5). A nossa sorte é que o fator é pequeno e por isso temos como encontrá-lo usando o método de Euler e uma máquina de calcular. Mas, como F(r) cresce muito rápido. já que é duplamente exponencial. temos geralmente que testar um número tão grande de valores para r afim de encontrar um fator que o método se torna rapidamente inútil.

5.3 Fermat, novamente

O maior número de Fermat que se conhece é F(23471); o fator é $5 \cdot 2^{23473+1}$. Este é o maior número de Fermat que se sabe ser composto. O método utilizado para fatorar esse número foi o método inventado por Euler. Vamos entender como.

Comecemos inventando um número que posso ser fator de um número de Fermat. Basta escolher um inteiro ímpar k e um inteiro qualquer n e construir o número $q = k \cdot 2^n + 1$. De acordo com o método de Euler esse número pode ser um divisor de F(m), desde que $m \leq n - 1$. Dizer que q divide F(m) equivale afirmar a seguinte congruência

$$2^{2m} \equiv -1 \pmod{q}.$$

Como são números muito grandes precisamos de uma maneira mais eficiente de calcular essas congruências. Como só entram em jogo potências de 2, isto por ser feito com certa facilidade. A observação é:

$$(2^{2^i})^2 = 2^{2^{i+1}}.$$

Inicializamos $r = 2^{2^5}$ e $i = 5$. O programa substitui r pelo o resto de r^2 por q e incrementa i de 1. Se $r = q - 1$, então q divide F(i). Se não, então repetimos o processo até que $i = n - 1$. Observe que q não pode dividir F(i) quando $i \geq n$, como vimos na seção 2. Este método (com algumas melhorias) foi usado recentemente para achar fatores para F(15), F(25), F(27) e F(147).

5.4 O teste de Lucas-Lehmer

O principal ingrediente desse teste é a sequência de inteiros $S_0, S_1, S_2, \cdots$, definida recursivamente por

$$S_0 = 4 \qquad \text{e} \qquad S_{k+1} = S_k^2 - 2.$$

Mostraremos que os inteiros dessa sequência podem ser escritos como potências de números racionais. Seja

$$\omega = 2 + \sqrt{3} \qquad \text{e} \qquad \varpi = 2 - \sqrt{3}.$$

Provando por indução em n que

$$\omega^{2n} + \varpi^{2n} = S_n. \tag{5.3}$$

Prova:

É claro que $\omega + \varpi = S_0$.

$$\omega + \varpi = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4 = S_0.$$

Suponha, então que, $\omega^{2n-1} + \varpi^{2n-1} = S_{n-1}$. Elevando ambos os membros ao quadrado, obtemos

$$\omega^{2n} + 2(\omega\varpi)^{2n-1} + \varpi^{2n} = S_{n-1}^2.$$

Como $\omega\varpi = 1$, temos que

$$\omega^{2n} + \varpi^{2n} = S_{n-1}^2 - 2,$$

que é igual a S_n por definição.

□

Teorema 5.4 (Teste de Lucas-Lehmer)**.** *Seja p um primo positivo. O número de Mersenne M(p) é primo se, e somente se,* $S_{p-2} \equiv 0 \ (mod\ M(p))$.

Vamos demonstrar apenas que a condição é necessária, já que a demonstração também é suficiente está além do objetivo do estudo.

Assim, considere o subconjunto $\mathbb{Z}[\sqrt{3}]$ constituído pelo o número da forma $a + b\sqrt{3}$, $a, b \in \mathbb{Z}$. Esses números são reais de podem ser somados e multiplicados.

Seja agora, q um inteiro primo, e escreva

$$\mathrm{I}(q) = \left\{ q\alpha : \alpha \in \mathbb{Z}[\sqrt{3}] \right\}$$

É claro que $0 = 0q \in \mathrm{I}(q)$. Como $q\alpha + q\beta = q(\alpha + \beta)$, concluímos que a soma de dois números pertencentes a $\mathrm{I}(q)$ está em $\mathrm{I}(q)$. Além disso, para cada $\alpha \in \mathbb{Z}[\sqrt{3}]$, tanto, $q\alpha$, quanto $-q\alpha \in \mathrm{I}(q)$. Assim

$$\mathrm{I}(q) < \mathbb{Z}[\sqrt{3}], \text{ também é aditivo.}$$

Dessa forma a relação de congruência módulo $\mathrm{I}(q)$ é uma relação de equivalência pertencente a $\mathbb{Z}[\sqrt{3}]$. Lembrando que se $\alpha, \beta \in \mathbb{Z}[\sqrt{3}]$, então, $\alpha \equiv \beta \ (\mathrm{mod}\ \mathrm{I}(q))$ quando $\alpha - \beta \in \mathrm{I}(q)$.

Agora, se $\alpha \in \mathbb{Z}[\sqrt{3}]$, então $\alpha = a_1 + a_2\sqrt{3}$, onde $a+1, a_2 \in \mathbb{Z}$. Dividindo a_1 e a_2 por q, obtemos $a_1 = qb_1 + r_1$ e $a_2 = qb_2 + r_2$, com $0 \leq r_1, r_2 \leq q$. Escrevendo $\rho = r_1 + r_2\sqrt{3}$, temos que

$$\alpha - \rho = a_1 + a_2\sqrt{3} - r_1 - r_2\sqrt{3}$$
$$\alpha - \rho = qb_1 + qb_2\sqrt{3}$$
$$\alpha - \rho = q(b_1 + b_2\sqrt{3}).$$

Portanto, $\alpha \equiv \rho \pmod{\mathrm{I}(q)}$. O número ρ é chamado de formula reduzida de α módulo $\mathrm{I}(q)$. Como o resto de uma divisão é única, cada elemento $\mathbb{Z}[\sqrt{3}]$ te uma, e apenas uma, forma reduzida. E ainda, duas classes representadas por elementos cujas as formas reduzidas sejam diferentes também devem ser distintas. Desse modo o conjunto $\mathbb{Z}[\sqrt{3}]$, das classes de equivalência módulo $\mathrm{I}(q)$, tem q^2 elementos.

A classe de equivalência de $\alpha \in \mathbb{Z}[\sqrt{3}]$ módulo $\mathrm{I}(q)$ denotaremos por $\widetilde{\alpha}$. Definimos a multiplicação em $\mathbb{Z}[\sqrt{3}]$ por

$$\widetilde{\alpha}\widetilde{\beta} = \widetilde{\alpha\beta}.$$

A demonstração que esta definição é válida independente da escolha dos representantes segue de perto a demonstração para a aritmética modular. Se $\alpha = a_1 + a_2\sqrt{3}$ e $\beta = b_1 + b_2\sqrt{3}$, assim $\widetilde{\alpha}\widetilde{\beta}$ está representada por

$$\widetilde{\alpha}\widetilde{\beta} = (a_1b_1 + 3a_2b_2) + (a_1b_2 + a_2b_1)\sqrt{3}.$$

Apesar de ser fácil verificar que esta multiplicação é associativa, comutativa e tem $\widetilde{1}$ como elemento neutro, temos que $\mathbb{Z}[\sqrt{3}]$ não é grupo com respeito a operação de multiplicação; por exemplo $\widetilde{0}$ não tem inverso em $\mathbb{Z}_q[\sqrt{3}]$. Contornando essa dificuldade, consideremos $\mathrm{V}(q)$ como os elementos inversíveis de $\mathbb{Z}_q[\sqrt{3}]$. Este conjunto é um grupo, porque o produto de elementos inversíveis em $\mathbb{Z}_q[\sqrt{3}]$ tem como resultado elementos inversíveis. A demonstração é a mesma para o $\mathrm{U}(q)$.

Como $\mathrm{V}(q) \subset \mathbb{Z}_q[\sqrt{3}] \setminus \left\{\widetilde{0}\right\}$, temos que a ordem de $\mathrm{V}(q)$ é necessariamente menor que q^2. Além disso, como $\omega\varpi = 1$ concluímos que, ω e ϖ pertencem a $\mathrm{V}(q)$. Com isso estamos preparados para a demonstrar o teste de Lucas-Lehmer.

Demonstração do teste de Lucas-Lehmer

Suponha que para algum primo p, o número de Mersenne $\mathrm{M}(p)$ divide S_{p-2}. Pela a equação (8.3) existe um r inteiro, tal que

$$\omega^{2^{p-2}} + \varpi^{2^{p-2}} = rM(p).$$

Multiplicando a equação por $\omega^{2^{p-2}}$, e que $\omega\varpi = 1$, temos

$$\omega^{2^{p-2}} + 1 = rM(p)\omega^{2^{p-2}}. \tag{5.4}$$

Suponha agora que $\mathrm{M}(p)$ é composto e que q é o menor fator primo e vamos tentar chegar numa contradição. Como q divide $\mathrm{M}(p)$, obtemos por (8.4) que

$$\widetilde{\omega}^{2^{p-1}} = -\widetilde{1},$$

Segue disto, e do lema-chave, que a ordem de $\widetilde{\omega}$ tem que dividir 2^p. Mas a equação (8.4) também nos diz que esta ordem não pode ser uma potência de 2 menor que 2^p. Portanto, a ordem de $\widetilde{\omega}$ em $\mathrm{V}(q)$ é 2^p.

Entretanto, pelo o teorema de Lagrange, a ordem de $\widetilde{\omega}$ divide a ordem de $\mathrm{V}(q)$. Como $\mathrm{V}(q)$ tem ordem menor ou igual a $q^2 - 1$, concluímos que $2^p < q^2 - 1$. Contundo, q é o menor divisor primo $\mathrm{M}(p)$, de modo que $q^2 \leq \mathrm{M}(p)$. Assim,

$$2^p \leq q^2 - 1 < 2^p - 1$$

que é a contradição que desejávamos. Com isso, se $\mathrm{M}(p)$ divide S_{p-2} então $\mathrm{M}(p)$ é primo. Isto mostra que a condição é necessária.

□

Capítulo 6

Criptografia RSA

Chegamos no capítulo onde entenderemos o funcionamento do método RSA. Para isso precisamos seguir todos os passos necessários para aplicação do sistema. Primeiramente, temos a pré-codificação, que é a parte onde convertemos a mensagem a ser codificada em uma sequência numérica; após temos a codificação e decodificação da mensagem, onde começamos a trabalha com os números primos; em seguida provamos que os sistema funciona independente da mensagem a ser codificada ou decodificada; demonstramos, a parte mais importante do sistema, a sua segurança e o porque, se realizado de forma correta, o método é totalmente seguro, explicando o porquê é o mais usado. contudo, toda a segurança depende da escolha certa dos números primos para a criação das chaves, pública n e privada p e q, assim mostramos como escolher-los; por último, e não menos relevante, a importância da legitimidade da mensagem ao qual será codificada, algo que só o destinatário verdadeiro precisa saber, dessa forma, concluímos com a assinatura da mensagem codificada.

6.1 Pré-codificação

A primeira coisa a fazer é converter a mensagem em uma sequência de números. Para simplificar, suponhamos que a mensagem contenha apenas palavras, nenhum número. Assim a mensagem é constituída pelas as letras e espaços que compõem a frase. Esta é a pré-codificação para distinguir do processo de codificação.

Na pré-codificação usamos a seguinte tabela para converter as letras em números.

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

O espaço entre duas palavras será representado pelo o número 99. Por exemplo, usando (Coutinho, 2013), a frase *Paraty é linda* fica convertida no número

$$25102710293499149921182313 10.$$

Fazemos cada letra corresponder a um número de dois algarismos para evitar uma ambiguidade. O que ocorreria caso atribuíssemos a A o 1, ao B 0 2 e dessa forma em diante. Assim, se estivesse o número 12 poderia ser AB ou L, que é a décima segunda letra do nosso alfabeto.

Precisamos determinar os parâmetros do sistema RSA que iremos usar. Esses parâmetros são dois números primos distintos, que denotaremos por p e q. Ponha $n = pq$. A última parte do processo de pré-codificação consiste em quebrar em blocos o extenso número produzido. Cada bloco dever ser números menores que n. Por exemplo, seja $p = 11$ e $q = 13$, então $n = 143$. Assim a mensagem pode ser quebrada nos blocos:

$$25 \text{ —}102 \text{ —}7 \text{ —}102 \text{ —}93 \text{ —}49 \text{ —}91 \text{ —}49 \text{ —}92 \text{ —}118 \text{ —}23 \text{ —}13 \text{ —}10.$$

Podemos escolher os blocos de maneiras diferentes, mas com o cuidado de nenhum bloco iniciar com o número 0, porque isto traria problemas para decodificar. Por isso não escolhemos os blocos

$$25 \text{ - } 102 \text{ - } 71 \text{ - } 029 \text{ - } \cdots$$

Observe que os blocos em que a mensagem foi quebrada não corresponde com nenhuma unidade linguística - seja palavra, número ou qualquer outra coisa. Isto é ótimo, porque torna a decodificação impossível por contagem de frequência.

6.2 Codificando e decodificando

Para iniciar a codificação precisamos do número n que é o produto dos dois números primos, e um inteiro positivo e que seja inversível módulo $\phi(n)$, ou seja, que o mdc$(e, \phi(n))$=1. Conhecendo p e q é fácil calcular $\phi(n)$. Já que

$$\phi(n) = (p-1)(q-1).$$

Chamaremos o par (e, n) de *chave de codificação* do sistema RSA que estamos usando. Depois da pré-codificação temos uma sequência de blocos. Codificaremos cada blocos separado e a mensagem codificada será a sequência de blocos codificados. Os blocos já codificados não poderão ser reunidos para formar um extenso número. Já se isso for feio se tornará impossível decodificar a mensagem.

Então, temos que a nossa chave de codificação é $(e.n)$. Temos que saber como codificar um bloco b. Sendo b um bloco menor do que n. Denotando o bloco codificado por $\mathbf{C}$(b). A forma para calcular $\mathbf{C}$(b) é:

$$\mathbf{C}(\text{b}) = \text{resto da divisão de } b^e \text{ por } n.$$

Em termos de aritmética modular, $\mathbf{C}$(b) é a forma reduzida de b^e módulo n.

Vejamos o que acontece utilizando o nosso exemplo. Temos $p = 11$ e $q = 13$, assim $n = 143$ e $\phi(n) = 120$. Precisamos escolher o inteiro e. Neste exemplo o menor valor possível é $e = 7$, onde é o menor primo, tal que, mdc(120,7)=1. Desse modo, o bloco 102 da nossa mensagem anterior é codificado como o resto da divisão de 102^7 divido por 143. Fazendo as contas e calculando a forma reduzida de 102^7, temos

$$102^7 \equiv (-41)^7 \equiv -41^7 \equiv -81 \cdot 138 \equiv -24 \equiv 119 \pmod{143}.$$

Assim $\mathbf{C}$(102)=119. Prosseguindo da mesma maneira com os outros blocos, a nossa mensagem codificada fica da forma

$$64 \text{ —}119 \text{ —}6 \text{ —}119 \text{ —}102 \text{ —}36 \text{ —}130 \text{ —}36 \text{ —}27 \text{ —}79 \text{ —}23 \text{ —}117 \text{ —}10.$$

Agora vejamos como decodificar um bloco da nossa mensagem codificada. Precisamos de dois números, o n e o inverso de e em $\phi(n)$, que denotaremos por d. o par (n, d) será a nossa *chave de decodificação.*, Sendo a o nosso bloco codificado, então $\mathbf{D}(a)$ será o nosso resultado do processo. A forma de como $\mathbf{D}(a)$ é

$$\mathbf{D}(a) = \text{resto da divisão de } a^d \text{ por } n.$$

Em terno de aritmética modular, $\mathbf{D}(a)$ é a forma reduzida de a^d módulo n.

Temos que é fácil calcular d conhecendo os números e e $\phi(n)$, pois basta nos aplicarmos o algoritmo euclidiano estendido. É claro que se b é um bloco da mensagem original, esperamos que quando $\mathbf{D}(\mathbf{C}(\text{b}))$=b, ou se não o código é inútil.

Voltando ao exemplo que estamos usando, temos que $n = 143$ e $e = 7$. Agora apliquemos o algoritmo euclidiano estendido para calcularmos d. Dividindo $\phi(143)$=120 por 7, temos

$$120 = 7 \cdot 17 + 1, \quad \text{donde} \quad 1 = 120 + (-17) \cdot 7.$$

Assim, o inverso de 7 módulo 143 é -17. Como usaremos o d com expoente precisamos que ele seja positivo. Portanto, d=120-17=103, é o menor inteiro positivo congruente a -17 módulo 120. Agora decodifiquemos o bloco 119 da mensagem codificada. Para isso calculemos a forma reduzida de 119^{103} módulo 143. Usando um sistema de computação algébrica, temos que $119^{103} \equiv 102 \pmod{143}$.

6.3 Por que funciona?

Como vimos esse método só será útil se, decodificando um bloco codificado conseguimos o bloco correspondente da mensagem original. Digamos que temos um sistema RSA de parâmetros p e q, com $n = pq$. Sabemos que para codificar precisamos de n e um inteiro e e para decodificar de n e d, que é o inverso de e. Precisamos verificar de b é um inteiro e $1 \leq b \leq n-1$ e $\mathbf{D}(\mathbf{C}(\text{b}))$=b. O que precisamos provar é que $\mathbf{D}(\mathbf{C}(b)) \equiv b \pmod{n}$. É suficiente porque tanto $\mathbf{D}(\mathbf{C}(\text{b}))$ quanto b estão no intervalo de 1 a $n-1$, logo só podem ser congruentes módulo n se foram iguais. Por isso que b tem que ser menor que n e que não podemos juntas os blocos depois de codificados.

Indo aos os cálculos. Por definição de $\mathbf{D}$ e $\mathbf{C}$ temos que

$$\mathbf{D}(\mathbf{C}(b)) \equiv (b^e)^d \equiv b^{ed} \pmod{n}. \tag{6.1}$$

Contudo, d é o inverso de e módulo $\phi(n)$, logo $ed = 1 + k\phi(n)$, para algum k inteiro. Como e e d são inteiros maiores que 2 e $\phi(n) > 0$, assim $k > 0$. Substituindo em (9.1)

$$b^{ed} \equiv b^{1+k\phi(n)} \equiv (b^{\phi(n)})^k b \pmod{n}.$$

Pelo o teorema de Euler, temos $b^{\phi}(n) \equiv 1 \pmod{n}$, resta apenas que $b^{ed} \equiv b \pmod{n}$. Portanto

$$\mathbf{D}(\mathbf{C}(b)) \equiv b \pmod{n}.$$

Entretanto, isso é um pouco errado. Porque só podemos usar o teorema de Euler para dizer que $b^{\phi}(n) \equiv 1 \pmod{n}$ quando o mdc$(b, n{=}1,)$ o que nem sempre é verdade.

Partindo para outra estratégia. Calcularemos a forma reduzida de b^{ed} módulo p e módulo q, já que são primos distintos. Como tanto faz qual módulo usemos, portanto, achemos a forma reduzida de b^{ed} módulo p. Como

$$ed = 1 + k\phi(n) = 1 + k(p-1)(q-1),$$

logo

$$b^{ed} \equiv b \cdot (b^{p-1})^{k(q-1)} \pmod{p}.$$

Usando Fermat precisamos supor que p não dividi b. Assumindo isso , então $b^{p-1} \equiv 1 \pmod{p}$ por Fermat, e temos que $b^{ed} \equiv b \pmod{p}$.

Parece que enfrentamos o mesmo problema quando usamos Euler. Mas por p ser primo nos permite tratar facilmente o caso em que p divide b. Nesse caso, $b \equiv 0 \pmod{p}$ a congruência é rapidamente verificada. Assim $b^{ed} \equiv b \pmod{p}$ vale para qualquer valor de b. Não podemos usar um argumento semelhante direto para n porque o mdc$(n, b) \neq 1$ não nos garante que $b \equiv 0 \pmod{n}$, pois n é composto.

Vimos que $b^{ed} \equiv b \pmod{p}$ vale para qualquer p. Análogo, temos $b^{ed} \equiv b \pmod{q}$. De outro modo, $b^{ed} - b$ é divisível por p e q. Temos também que mdc$(p, q){=}1$, donde pq divide $b^{ed} - b$, pelo o lema (2.2) da página 13. Como $n = pq$, concluímos que $b^{ed} \equiv b \pmod{n}$, para qualquer inteiro b. Agora falta mostrar a segurança.

6.4 Porque o RSA é seguro?

Lembrando que o RSA é um método de chave pública. Sendo p e q os parâmetros do sistema e $n = pq$. A chave de codificação é a chave pública do sistema, ou seja, o par (n, e) é acessível a qualquer usuário. Todo segura estão na dificuldade de achar d só conhecendo n e e.

Sabemos encontrar d aplicando o algoritmo euclidiano estendido a $\phi(n)$ e e. Mas só sabemos encontrar $\phi(n)$ se soubemos fatorar n para encontrar p e q. Portanto só podemos quebrar o sistema se fatoramos n, mas se n for muito grande não se conhece nenhum algoritmo rápido para fatorar n. E é nisso onde está toda a segurança do sistema.

Agora imagine que fosse possível chegar a d sem fatorar n. Por exemplo, o que aconteceria se inventasse um algoritmo que conseguisse chegar a $\phi(n)$ a partir de n e e? Nisso teria um algoritmo rápido de fatoração; porque? Estamos supondo que $n = pq$ e $\phi(n) = (p-1)(q-1)$ são nossos conhecidos. Queremos determinar p e q. Mas

$$\phi(n) = (p-1)(q-1) = pq - (p+q) + 1 = n - (p+q) + 1,$$

de maneira que $p + q = n - \phi(n)$ é conhecido. Assim

$$(p+q)^2 - 4n = (p^2 + q^2 + 2pq) - 4pq = (p-q)^2;$$

logo

$$p - q = \sqrt{(p+q)^2 - 4n}$$

também é conhecido. Mas conhecendo $p+q$ e $p-q$ calculamos p e q, assim, fatoramos n.

6.5 Escolhendo primos

É claro que se os primos escolhidos p e q forem pequenos fica fácil de quebrar o sistema. Mas não é só escolher primos grandes. De fato, se p e q são grandes, mas $|p-q|$ for pequeno fica fácil fatorar $n = pq$ usando o algoritmo de Fermat. Por outro lado se os primos forem bem escolhidos, o sistema tem se mostrado muito seguro. Assim temos uma receita para escolher bons primos.

Suponhamos que queremos implementar o RSA com uma chave pública (n, e), com n inteiro de aproximadamente r algarismos. Para construir n escolha p entre $\frac{4r}{10}$ e $\frac{45r}{100}$ algarismos, em seguida escolha q próximo de $\frac{10^r}{p}$. e recomendado uma chave para uso pessoal de 768 bits.Quer dize que n tem aproximadamente 231 algarismos. Para temos um n a repeito precisaremos de dois primos de 104 e 127 algarismos. Vejamos que a diferença entre os dois primos ainda é grande e impraticável de fatorar por Fermat. Também precisamos ter certeza que $p+1$, $q+1$, $p-1$ e $q-1$ não possuem fatores primos pequenos, se não torna-se um presa para os algoritmos conhecidos.

Precisamos de um resultado sobre a distribuição dos primos. Lembrando que $\pi(x)$ representa os primos positivos menores ou iguais a x. de acordo com o teorema dos números primos, se x é muito grande, então $\pi(x)$ é aproximadamente igual a $\frac{x}{\log x}$, onde o log é o logaritmo de base e. Consideremos x um numero muito grade e ε um inteiro

positivo. Queremos uma aproximação dos primos entre x e $x+\varepsilon$, ou seja, para $\pi(x+\varepsilon)-\pi(x)$. Pelo o teorema dos números primos e das propriedades de logaritmo que $\pi(x+\varepsilon)-\pi(x)$ é praticamente igual a

$$\frac{x+\varepsilon}{\log x+\log(1+x^{-1}\varepsilon)}-\frac{x}{\log x}. \tag{6.2}$$

Suponhamos que $x^{-1}\varepsilon$ é pequeno, assim podemos substitui-lo por po 0 e temos uma aproximação razoável de $\pi(x+\varepsilon)-\pi(x)$. Portanto o número de primos entre x e $x+\varepsilon$ é igual a $\frac{x}{\log x}$. Quando maior for o nosso x menor será $x^{-1}\varepsilon$ e como consequência a aproximação será melhor.

Suponhamos que queremos achar um primo próximo de um inteiro x. Concretizando, digamos que x é da ordem de 10^{127}. Procuraremos este primo no intervalo de x até $x+10^4$. Seria bom sabermos quantos primos devemos esperar que haja, no pior dos casos, para acharmos o que queremos. Como $x^{-1}\varepsilon$ é da forma 10^{-123} então é bem pequeno. Logo usando a fórmula (9.2) temos que o intervalo deve conter aproximadamente

$$\left[\frac{10^4}{\log(qo^{127})}\right]=34$$

primos. para verificar se m inteiro ímpar é primo seguimos uma estratégia. Estratégia essas que consiste de três etapas:

1. Verifique se n é divisível por um primo menor que 5000.

2. Supondo que n não é divisível por nenhum desse primos, aplique o teste Miller a n usando como bases os primos 10 primos.

3. Supondo que o teste de Miller teve como saída inconclusivo para todas as outras etapas, aplique o teste de primalidade a n.

Adaptemos esta estratégia para encontrar um primo o intervalo de x a $x+10^4$. Elimine do intervalo os inteiros ímpares que são divisíveis por primo menores que $5\cdot 10^3$. Depois, aplique (2) e (3) aos números que sobraram, até que um primo seja encontrado.

Para sabemos o trabalho que será necessário, podemos tentar descobrir quantos inteiros sobraram depois da eliminação daqueles que são divisíveis pelo os primos menores que $5\cdot 10^3$. Seja m um inteiro positivo. Se $x\leq km\leq x+10^4$, então

$$\left[\frac{x}{m}\leq k\leq\frac{x+10^4}{m}\right].$$

Assim temos

$$\left[\frac{x+10^4}{m} - \frac{x}{m}\right]$$

múltiplos de m no intervalo de x a $x+10^4$. Onde é aproximadamente igual a $\left[\frac{10^4}{m}\right]$, que é o número múltiplos de m menores que 10^4. Isto que dizer que o número de inteiros múltiplos de primos positivos menores que $5 \cdot 10^3$ no intervalo de $[x, x+10^4]$ e $[0, 10^4]$ é praticamente o mesmo. Calculemos o últimos desse número. Note que um número composto de 10^4 tem que se múltiplo de um primo menor que $\sqrt{10^4} = 100$. Assim, um inteiro no intervalo de $[0, 10^4]$ é múltiplo de um primo menor que $5 \cdot 10^3$ se é composto, ou se é ele próprio um primo menor que $5 \cdot 10^3$. Levando em conta que 2 é o único primo par, temos que o número de inteiros compostos e ímpares menores que 10^4 é $5000 - \pi(10^4) + 1$. Dessa forma, o número total de inteiros ímpares no intervalo de x a $x+10^4$ depois de todas as eliminações é

$$5000 - (5000 - (\pi(10^4) - 1)) - (\pi(5 \cdot 10^3) - 1) = 560.$$

Assim esperamos encontrar uma média de 34 primos de um total de 560 inteiros.

6.6 Assinaturas

Imaginemos que uma empresa fazer transações bancárias através de computadores, via rede telefônica. Por questões de segurança tanto o banco quanto a empresa vão exigir que as mensagens seja codificada antes de enviá-las. Mas só isso não basta. Afinal se o RSA está sendo usado a chave de codifica é público. Então, por exemplo, um *hacker* pode simplesmente mandar uma mensagem para o banco pedido que eles transfiram o saldo bancário da empresa para uma outra conta. Por isso o banco precisa garantir que a mensagem teve um origem e usuário autorizado da empresa. Assim, a mensagem teve ter uma assinatura digital.

Para mandar ma mensagem assinada no sistema RSA não é nada difícil. Vamos chamar $\mathbf{C}_e$ e $\mathbf{D}_e$ as funções de codificação e decodificação da empresa, respectivamente; e chamaremos $\mathbf{C}_b$ e $\mathbf{D}_b$ das mesmas funções, so com respeito ao banco. Seja a o bloco da mensagem que a empresa quer enviar ao banco. De acordo com o que foi estudado, a empesa deveria codificar a como $\mathbf{C}_b(a)$ e enviá-la ao banco pela a linha telefônica. Para mandar a mensagem codificada ao invés de enviar $\mathbf{C}_b(a)$ enviamos $\mathbf{C}_b(\mathbf{D}_e(a))$. Primeiro

aplicamos a função decodificação da empresa a a e depois a função codificação do banco ao bloco.

Tendo recebido o bloco $\mathbf{C}_b(\mathbf{D}_e(a))$, o banco aplica a sua função de decodificação para obter $\mathbf{D}_e(a)$, e a este último bloco aplica a função de codificação da empresa, já que essa é uma chave pública; e por isso o banco a conhece.

Por que isto é suficiente para saber que a mensagem a autorizada? O banco aplica aos blocos da mensagem recebida as funções $\mathbf{C}_e\mathbf{D}_b$. Se a mensagem resultante depois de aplicada as funções fizer sentido, isto que dizer que a mensagem enviada foi codificada aplicando aos blocos da mensagem original as funções $\mathbf{C}_b\mathbf{D}_e$. Lembrando que $\mathbf{D}_e$ só é conhecida da empresa. Então se a mensagem fizer sentido só pode ter origem na empresa. Como a probabilidade de que a mensagem produzida sem usar $\mathbf{D}_e$ seja decodificada pelo o banco e faça sentido é praticamente zero. Assim o banco estar seguro de que a mensagem é legítima.

Conclusão

Após todo o processo de estudo e a percepção da amplitude que a Criptografia abrange na atualidade, fica até difícil vê que esse sistema trabalha de uma maneira, a primeira vista, simples. Mas, quando nos aprofundamos na compreensão do processo de codificação e decodificação que entendemos o prestígio que o sistema possui. Podemos enxergar a grandiosidade de todos os benefícios proporcionados com a aplicação do sistema de criptografia RSA e o quão seguro ele se torna pela a ineficiência dos algoritmos conhecidos. A princípio vemos a sua maior segurança como a sua maior fraqueza, mas ao estudarmos conseguimos, sem dúvidas, compreender que o sistema é algo impressionante e atraente para os interessados no tema. Trazendo a compreensão desse extraordinários sistema, o que foi obtido como resultado, a compreensão de todo o processo de criptografia RSA.

Bibliografia

ALENCAR FILHO, Edgard de. **TEORIA ELEMENTAR DOS NÚMEROS** 1ª Ed —São Paulo: Nobel, 1981.

CAVALCANTE, A.L.B. Matemática II. Notas de Aula. Brasília: Editora UPIS, 2004.

COUTINHO, S. C. **NÚMEROS INTEIROS CRIPTOGRAFIA RSA.** 2ª Ed —Rio de Janeiro: IMPA, 2013.

IEZZI, G. **FUNDAMENTOS DE MATEMÁTICA ELEMENTAR**. 3ª Ed —São Paulos: Atual Ed., 1977.

SÁ, Ilydio Pereira. **ARITMÉTICA MODULAR E SUAS APLICAÇÕES**. Rio de Janeiro: UERJ, 2010.

SOUZA, Lana Priscila.**CRIPTOGRAFIA RSA: A TEORIA DOS NÚMEROS POSTA EM PRÁTICA**. 2015. 75f. Dissertação (Mestrado em Matemática) —Universidade Federa do Ceará, UFC, Fortaleza, 2015.