Márcio Alexandre dos Santos Silva

FRAÇÕES CONTÍNUAS: UMA APLICAÇÃO EM CRIPTOGRAFIA RSA

Itabaiana

Outubro de 2019

Márcio Alexandre dos Santos Silva

FRAÇÕES CONTÍNUAS: UMA APLICAÇÃO EM CRIPTOGRAFIA RSA

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Universidade Federal de Sergipe

Departamento de Matemática

Programa de Pós-Graduação

Orientador: Prof. Me. Samuel Brito Silva

Itabaiana

Outubro de 2019

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA PROFESSOR ALBERTO CARVALHO
UNIVERSIDADE FEDERAL DE SERGIPE

S586f Silva, Márcio Alexandre dos Santos.
Frações contínuas: uma aplicação em criptografia RSA / Márcio Alexandre dos Santos Silva; orientação: Samuel Brito Silva. – Itabaiana, 2019.
48 f.

Dissertação (Mestrado em Matemática) – Universidade Federal de Sergipe, 2019.

1. Matemática. 2. Frações. 3. Criptografia. I. Silva, Samuel Brito. II. Título.

CDU 511.13

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Frações Contínuas: Uma Aplicação em Criptografia RSA

por

Márcio Alexandre dos Santos Silva

Aprovada pela banca examinadora:

Samuel Brito Silva
Prof. Samuel Brito Silva - UFS
Orientador

Mateus Alegri
Prof. Mateus Alegri - UFS
Primeiro Examinador

Fábio Lima Santos
Prof. Fabio Lima Santos - UFS
Segundo Examinador

Itabaiana, 10 de Outubro de 2019

Dedico este trabalho a Deus, Naty, Louro, Dui,
... Edudim 2004.

Agradecimentos

Na oportunidade da conclusão do presente trabalho, desejo agradecer as seguintes pessoas e instituições:

Preimeiramente a Deus, porque sem ele não vamos a lugar nenhum;

aos meus pais, Maria da Natividade dos Santos e Lourival Bispo da Silva, pela força, apoio e colaboração;

ao Prof. Me. Samuel Brito Silva, meu orientador, pela dedicação, incentivo e paciência em acompanhar cada passo deste trabalho;

à Universidade Federal de Sergipe por ter me dado a oportunidade disso tudo acontecer. Foi na UFS que dei meus primeiros passos no ensino superior, foi aqui que tive a honra de ter trabalhado como Auxiliar em Administração por mais de seis anos;

às Escolas Santa Bárbara, Zumbi dos Palmares, Edvaldo Fernandes, Bolivar Santana e ao Colégio Estadual Severino Vieira por ter me dado a formação básica, por me ensinar o que é ser social e, principalmente, pelas alegrias da infância e adolescência;

aos colegas e professores do Profmat que estiveram comigo ao longo desta jornada, sempre me apoiando e ajudando;

finalmente, a todos que acreditaram e contribuíram de forma direta ou indiretamente para a realização deste trabalho.

Resumo

Apresentam-se, nesta dissertação, um estudo sobre a expansão de números reais em forma de frações contínuas simples e uma aplicação desta teoria ao sistema de criptografia RSA. No primeiro capítulo é discutido as definições, propriedades e reduzidas destas frações. Explanam-se ainda reduzidas como as melhores aproximações de um número para um dado denominador. Estabelecido este estudo preliminar, expõe-se, no segundo capítulo, o ataque à criptografia RSA desenvolvido, em 1990, por Wiener. Sendo assim, este trabalho tem como objetivo abordar este ataque através do estudo das frações contínuas simples.

Palavras-chaves: Frações Contínuas, reduzidas, Ataque de Wiener, Criptografia RSA.

Abstract

This dissertation presents a study on the expansion of real numbers in the form of simple continuous fractions and an application of this theory to the RSA cryptography system. In the first chapter the definitions, properties and reduced of these fractions are discussed. They are further explained as the best approximations of a number for a given denominator. Once this preliminary study is established, the second chapter presents the attack on RSA cryptography developed in 1990 by Wiener. Thus, this paper aims to address this attack by studying the simple continuous fractions.

Key-words:

Continued Fractions, reduced, Wiener's Attack, RSA Cryptosystem.

Sumário

1 INTRODUÇÃO 9

2 FRAÇÕES CONTÍNUAS SIMPLES 11
2.1 Frações Contínuas Finitas 12
2.2 Reduzidas 16
2.3 Soluções de Equações Diofantinas através de Frações Contínuas . . 23
2.4 Frações Contínuas Infinitas 24

3 ATAQUE DE WIENER 40
3.1 Criptografia RSA 40
3.2 Ataque de Wiener ao sistema de criptografia RSA 40

Referências Bibliográficas 48

1 Introdução

Sem dúvida alguma, a ideia de números irracionais não é das mais simples. O conceito de número natural é intuitivo, o de números inteiros acrescentam-se aos naturais apenas os sinais de mais ou menos e o de números racionais é dado como a divisão de inteiros por naturais não nulos. Entretanto quando se quer definir ou representar números irracionais a tarefa acaba ficando mais complicada, principalmente no que diz respeito a sua representação decimal. Apesar disso, podemos, devido a densidade de $\mathbb{Q}$ em $\mathbb{R}$, aproximá-los por racionais. Assim, dado um número real x qualquer sempre é possível aproximá-lo por meio de um número inteiro, ou seja, sendo $\alpha = \lfloor x \rfloor$, então a distância entre α e x é menor do que 1. A aproximação por racional é possível, pois considerando $0 < x - \alpha < 1$, existem inteiros $a_1, a_2, a_3, ..., a_n, ... \in [0, 1, 2, ..., 9]$ tais que

$$x - \alpha = 0, a_1 a_2 a_3 ... a_n ....$$

Dessa forma, sendo $r_n = 0.10^n + a_1.10^{n-1} + \cdot + a_{n-1}10 + a_n$ então $\dfrac{r_n}{10^n} = 0, a_1 a_2 a_3 ... a_n$, logo $\dfrac{r_n}{10^n} < x - \alpha < \dfrac{r_n}{10^n} + \dfrac{1}{10^n} = \dfrac{r_n + 1}{10^n}$. Podemos então aproximar x por $\left(\alpha + \dfrac{r_n}{10^n}\right)$ com erro menor do que $\dfrac{1}{10^n}$, tendo em vista que

$$\frac{r_n}{10^n} < x - \alpha < \frac{r_n + 1}{10^n}$$
$$0 < x - (\alpha + \frac{r_n}{10^n}) < \frac{1}{10^n}.$$

À medida que n cresce, temos uma ótima aproximação racional para x. Um bom exemplo é a aproximação $\dfrac{3141592}{1000000}$ para π, onde

$$\left|\pi - \frac{3141592}{1000000}\right| < \frac{1}{10^6}.$$

Contudo nem sempre as aproximações decimais são boas, pois, neste caso por exemplo, pode haver racionais com denominadores bem menores 10^6 mais próximos de π. A título de ilustração, temos o racional $\dfrac{355}{113}$ que é uma excelente aproximação para π, pois

$$\left|\pi - \frac{355}{113}\right| < \left|\pi - \frac{3141592}{1000000}\right|.$$

Sendo assim, o primeiro Capítulo deste trabalho tem como objetivo encontrar excelentes aproximações racionais para números reais. Para isso, apresentaremos os conceitos e propriedades de Frações Contínuas. Já o segundo, será destinado à aplicação desse estudo ao ataque à criptografia RSA. Este sistema, que foi desenvolvido por Rivest, Shamir

e Adleman, em 1978, é, definitivamente, o mais conhecido dos métodos de criptografia de chave pública segundo (COUTINHO, 2000).

Ele é baseado em duas chaves: pública e privada. A pública é utilizada para criptografar a informação, enquanto que a privada tem o papel de descriptografá-la. Para gerar a chave pública, o sistema escolhe dois números primos distintos p e q, realiza a multiplicação deles e obtém o módulo N. Assim, (N, e) é a chave pública, onde $e \in \mathbb{Z}$ tal que $1 < e < (p-1)(q-1)$, chamado de expoente público. Já a privada é dada por (p, q, d), onde d é o expoente privado tal que $ed \equiv 1(mod\ (p-1)(q-1))$.

A ideia por trás do RSA é relativamente simples, tendo em vista que para descobrir a chave privada basta encontrar os primos que deram origem ao módulo N. Entretanto, decompor N em fatores primos não é uma tafera muito fácil, caso N tenha mais que 10^{100} algarismos. Isso ocorre porque os métodos de fatoração conhecidos atualmente são ineficientes, e podem levar milhares de anos para encontrar os fatores primos de um número.

Por exemplo, se quiséssemos encontrar a decomposição de N em fatores primos, supondo p e q maiores do 10^{50}, então precisaríamos de aproximadamente 10^{50} divisões, pois N tem aproximadamente 10^{100} casas decimais. Supondo que um supercomputador realize 10^{10} divisões por segundo, ainda assim precisaríamos de 10^{40} segundos para decompor o módulo N, ou seja 3170979198376460000000000000000000 anos.

A utilização de primos extremamente grandes, no entanto, nem sempre é viável, justamente porque a comunicação entre os equipamentos pode ficar lenta. Com o intuito de minimizar o tempo gasto para criptografar e descriptografar, pode-se propor a diminuição do valor dos expoentes público e privado.

Em um sistema de autenticação feito por meio do uso de cartões inteligentes, por exemplo, pode-se acelerar a descriptografia RSA, utilizando um expoente privado d relativamente pequeno. Esta escolha é especialmente interessante, pois há uma grande diferença no poder de processamento entre o cartão e computador utilizado.

Apesar de alcançar o resultado desejado, esta medida compromete sobre maneira a segurança dessas operações, devido ao ataque desenvolvido por Wiener.

Michael J. Wiener descreveu, em 1990, um algoritmo de tempo polinomial para quebrar um sistema de criptografia RSA típico, isto é, p e q são do mesmo tamanho e $e < N$. Assim, ele mostrou que se o expoente privado d for menor do que $N^{\frac{1}{4}}$, onde N é o módulo RSA, então pode-se obter d analisando apenas a chave pública correspondente.

2 Frações Contínuas Simples

Este capítulo tem como objetivos apresentar o conceito de frações contínuas simples, definir reduzidas e listar algumas de suas propriedades básicas. Estes resultados serão extremamentes importantes para o bom entendimento de todo o trabalho.

Antes de mais nada, sabemos que dados $a, b \in \mathbb{Z}$ é possível, através do método de divisões sucessivas, determinar o *mdc*, denotado por (a, b), desses números da seguinte forma:

Exemplo 2.1. *Determine o mdc de* 121 *e* 34.

$$\begin{aligned} 121 &= 34.3 + 19 \\ 34 &= 19.1 + 15 \\ 19 &= 15.1 + 4 \\ 15 &= 4.3 + 3 \\ 4 &= 3.1 + 1 \\ 3 &= 1.3 + 0, \end{aligned}$$

como 1 *é o último resto não nulo das divisões sucessivas, logo* $(121, 34) = 1$.

Uma das consequências imediatas dessas igualdades é que se pode expressar a fração $\frac{121}{34}$ em função dos quocientes encontrados nas divisões sucessivas, ou seja,

$$\frac{121}{34} = 3 + \frac{19}{34} = 3 + \frac{1}{\frac{34}{19}} = 3 + \frac{1}{1 + \frac{15}{19}} = 3 + \frac{1}{1 + \frac{1}{\frac{19}{15}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{4}{15}}}$$

$$\frac{121}{34} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{\frac{15}{4}}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{3}{4}}}} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{\frac{4}{3}}}}}$$

$$\frac{121}{34} = 3 + \frac{1}{1 + \frac{1}{1 + \frac{1}{3 + \frac{1}{1 + \frac{1}{3}}}}}.$$

Diz-se que esta última expressão é a representação do número racional $\frac{121}{34}$ em termos de fração contínua, a qual pode ser representada de maneira simplificada por $[3; 1, 1, 3, 1, 3]$.

Apresentaremos a seguir a definição de frações contínuas.

Definição 2.2. *Sejam $a_0, a_1, a_2, a_3, ...$ números reais todos positivos, exceto possivelmente o a_0. Uma fração contínua é uma expressão do tipo*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots}}} = [a_0; a_1, a_2, a_3...],$$

onde os números $a_0, a_1, a_2, a_3, ...$ são chamados de quocientes parciais.

2.1 Frações Contínuas Finitas

Definição 2.3. *Uma fração contínua é finita quando há um número finito de quocientes parciais*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \; + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}} = [a_0; a_1, a_2, ..., a_n],$$

onde $a_1, a_2, ..., a_n$ são todos positivos.

As frações contínuas são ditas simples, se os a_n, com $n \in \mathbb{N}$, são números inteiros. Como iremos utilizar apenas as frações contínuas simples, então a expressão "frações contínuas" deverá ser entendida como "frações contínuas simples".

A fração contínua do Exemplo 2.1 além de ser simples, também é finita, tendo em vista que tem uma quantidade finita de quocientes parciais.

Considere agora uma sequência finita de números inteiros. Por exemplo, dados os inteiros $2, 3, 8, 5$, a fração contínua representada por eles

$$[2; 3, 8, 5] = 2 + \cfrac{1}{3 + \cfrac{1}{8 + \cfrac{1}{5}}} = 2 + \cfrac{1}{3 + \cfrac{5}{41}} = 2 + \frac{41}{128} = \frac{297}{128}$$

expressa um número racional. Este fato vale de modo geral como mostra o resultado a seguir.

Teorema 2.4. *Toda fração contínua finita representa um número racional.*

Prova. *Demonstraremos por indução matemática. Considere os inteiros $a_0, a_1, ..., a_k$ todos positivos, exceto possivelmente o a_0.*

i) Para $k = 1$*, temos* $[a_0; a_1] = a_0 + \dfrac{1}{a_1} = \dfrac{a_0a_1 + 1}{a_1}$*. Assim* $[a_0; a_1]$ *representa um racional.*

ii) Supondo que para k *inteiros a fração contínua finita* $[a_0; a_1, ..., a_k]$ *representa um número racional então*

$$[a_0; a_1, ..., a_k, a_{k+1}] = a_0 + \frac{1}{[a_1; a_2, ..., a_k, a_{k+1}]}.$$

Como $[a_1; a_2, ..., a_k, a_{k+1}]$ *é racional, existem* r *e* s *inteiros positivos tais que* $\dfrac{r}{s} = [a_1; a_2, ..., a_k, a_{k+1}]$*, assim*

$$[a_0; a_1, ..., a_k, a_{k+1}] = a_0 + \frac{1}{\frac{r}{s}} = a_0 + \frac{s}{r} = \frac{a_0r + s}{r},$$

logo $[a_0; a_1, ..., a_k, a_{k+1}]$ *representa um número racional.*

□

A recíproca do Teorema acima é verdadeira. Uma vez que é garantia pelo Algoritmo de Euclides, pois o processo de divisões sucessivas sempre nos fornece um resto nulo, depois de uma quantidade finita de divisões.

Teorema 2.5. *Todo número racional pode ser escrito em forma de frações contínuas finita.*

Prova. *Com efeito, seja* r *um número racional, então existem* p *e* r_0 *inteiros, com* r_0 *positivo, tal que* $r = \dfrac{p}{r_0}$*. Pelo Algoritmo de Euclides, temos a sequência de equações*

$$\begin{aligned}
p &= r_0a_0 + r_1 && 0 < r_1 < r_0\\
r_0 &= r_1a_1 + r_2 && 0 < r_2 < r_1\\
r_1 &= r_2a_2 + r_3 && 0 < r_3 < r_2\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1}a_{n-1} + r_n && 0 < r_n < r_{n-1}\\
r_{n-1} &= r_na_n,
\end{aligned}$$

onde $a_0, a_1, a_2, ..., a_n$ *são todos inteiros positivos, exceto possivelmente o* a_0*. Podemos*

reescrevê-las da seguinte forma

$$\frac{p}{r_0} = a_0 + \frac{r_1}{r_0} = a_0 + \frac{1}{\frac{r_0}{r_1}} \qquad 0 < r_1 < r_0$$

$$\frac{r_0}{r_1} = a_1 + \frac{r_2}{r_1} = a_1 + \frac{1}{\frac{r_1}{r_2}} \qquad 0 < r_2 < r_1$$

$$\frac{r_1}{r_2} = a_2 + \frac{r_3}{r_2} = a_2 + \frac{1}{\frac{r_2}{r_3}} \qquad 0 < r_3 < r_2$$

$$\frac{r_2}{r_3} = a_3 + \frac{r_4}{r_3} = a_3 + \frac{1}{\frac{r_3}{r_4}} \qquad 0 < r_4 < r_3$$

$$\vdots \qquad \vdots$$

$$\frac{r_{n-2}}{r_{n-1}} = a_{n-1} + \frac{r_n}{r_{n-1}} = a_{n-1} + \frac{1}{\frac{r_{n-1}}{r_n}} \qquad 0 < r_n < r_{n-1}$$

$$\frac{r_{n-1}}{r_n} = a_n.$$

Portanto como $r = \dfrac{p}{r_0}$ *então*

$$r = a_0 + \frac{1}{\frac{r_0}{r_1}} = a_0 + \frac{1}{a_1 + \frac{1}{\frac{r_1}{r_2}}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{\frac{r_2}{r_3}}}}$$

prosseguindo dessa forma, teremos

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}} = [a_0; a_1, a_2, a_3, ..., a_n].$$

□

Exemplo 2.6. *Vamos expressar os racionais* $\dfrac{-364}{121}$ *e* $\dfrac{34}{121}$ *em termo de frações contínuas.*

Solução. *Sendo* $-329 = 121(-3) + 34$*, então podemos escrever*

$$\frac{-329}{121} = -3 + \frac{34}{121} = -3 + \frac{1}{\frac{121}{34}} = -3 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{3}}}}}},$$

logo $\dfrac{-329}{121} = [-3; 3, 1, 1, 3, 1, 3]$*. Já o racional* $\dfrac{34}{121}$*, podemos reescrevê-lo da seguintes forma*

$$\frac{34}{121} = 0 + \frac{34}{121} = 0 + \frac{1}{\frac{121}{34}} = 0 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \frac{1}{3}}}}}} = [0; 3, 1, 1, 3, 1, 3].$$

Pode-se inferir, a partir do exemplo acima, que no desenvolvimento da fração contínua somente o primeiro dos quocientes parciais pode assumir um valor negativo ou nulo.

Proposição 2.7. *Se* $\dfrac{p}{q} = [a_0; a_1, a_2, ..., a_n]$*, onde* $\dfrac{p}{q}$ *é um número racional positivo com* $q < p$*, então* $\dfrac{q}{p} = [0; a_0, a_1, a_2, ..., a_n]$*.*

Prova. *De fato, seja* $\dfrac{p}{q} = [a_0; a_1, a_2, ..., a_n]$*, logo*

$$\frac{p}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}.$$

Como

$$\frac{q}{p} = 0 + \frac{1}{\frac{p}{q}} = 0 + \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{n-1} + \frac{1}{a_n}}}}} = [0; a_0, a_1, a_2, ..., a_n].$$

□

Quando o quociente a_n for maior que 1, podemos substituí-lo por $(a_n - 1) + \frac{1}{1}$. Dessa forma, a quantidade de quocientes da fração contínua pode ser par ou ímpar. Podemos representar $\frac{51}{27}$ por $[1, 1, 8]$ ou $[1, 1, 7, 1]$. Generalizando, se $a_n > 1$, então $[a_0; a_1, a_2, a_3, ..., a_n] = [a_0; a_1, a_2, a_3, ..., a_n - 1, 1]$.

2.2 Reduzidas

Definição 2.8. *A fração contínua $[a_0; a_1, a_2, ..., a_k]$, onde k é um inteiro não negativo menor do que ou igual a n, é chamada de k-ésima reduzida da fração contínua $[a_0; a_1, a_2, ..., a_n, ...]$. A k-ésima reduzida é denotada por c_k.*

Teorema 2.9. *Sejam $a_0, a_1, a_2, ..., a_n$ números reais com $a_1, a_2, ..., a_n$ positivos. Sejam as sequências $p_0, p_1, p_2, ..., p_n$ e $q_0, q_1, q_2, ..., q_n$ definidas recursivamente por*

$$\begin{aligned} p_0 &= a_0 & q_0 &= 1 \\ p_1 &= a_0a_1 + 1 & q_1 &= a_1 \\ p_2 &= a_2p_1 + p_0 & q_2 &= a_2q_1 + q_0 \\ &\vdots & &\vdots \\ p_k &= a_kp_{k-1} + p_{k-2} & q_k &= a_kq_{k-1} + q_{k-2}, \end{aligned}$$

para $k = 2, 3, ..., n$. Então a k-ésima reduzida da fração contínua $[a_0; a_1, a_2, ..., a_{k-1}, a_k]$ é dada por $c_k = \frac{p_k}{q_k}$.

Prova. *Demonstraremos este teorema por indução matemática.*

i) Para $k = 0$ e $k = 1$, temos $c_0 = [a_0] = \frac{a_0}{1} = \frac{p_0}{q_0}$. Analogamente, $c_0 = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1} = \frac{p_1}{q_1}$ e $c_2 = [a_0; a_1, a_2] = a_0 + \frac{1}{a_1 + \frac{1}{a_2}}$ logo

$$c_2 = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0(a_1a_2 + 1) + a_2}{a_1a_2 + 1} = \frac{a_2(a_1a_0 + 1) + a_0}{a_2a_1 + 1} = \frac{a_2p_1 + p_0}{a_2q_1 + q_0} = \frac{p_2}{q_2}.$$

ii) Suponha que o teorema seja válido para um inteiro k, onde $2 \leq k < n$, assim

$$c_k = [a_0; a_1, a_2, ..., a_k] = \frac{p_k}{q_k} = \frac{a_kp_{k-1} + p_{k-2}}{a_kq_{k-1} + q_{k-2}}.$$

Seja $c_{k+1} = [a_0; a_1, a_2, ..., a_k, a_{k+1}]$ então é possível obter c_{k+1} a partir de c_k simplesmente pela substituição de a_k por $a_k + \frac{1}{a_{k+1}}$, e note que $p_{k-1}, q_{k-1}, p_{k-2}$ e q_{k-2}

dependem apenas dos $a_0, a_1, a_2, ..., a_{k-1}$*, neste caso, eles não serão alterados na substituição. Assim* $c_{k+1} = [a_0; a_1, a_2, ..., a_{k-1}, a_k + \frac{1}{a_{k+1}}]$*, isso resulta em*

$$\begin{aligned} c_{k+1} &= \frac{\left(a_k + \frac{1}{a_{k+1}}\right) p_{k-1} + p_{k-2}}{\left(a_k + \frac{1}{a_{k+1}}\right) q_{k-1} + q_{k-2}} \\ &= \frac{(a_k a_{k+1} + 1)p_{k-1} + a_{k+1}p_{k-2}}{(a_k a_{k+1} + 1)q_{k-1} + a_{k+1}q_{k-2}} \\ &= \frac{a_{k+1}(a_k p_{k-1} + p_{k-2}) + p_{k-1}}{a_{k+1}(a_k q_{k-1} + q_{k-2}) + q_{k-1}} \\ &= \frac{a_{k+1}p_k + p_{k-1}}{a_{k+1}q_k + q_{k-1}} \\ &= \frac{p_{k+1}}{q_{k+1}}. \end{aligned}$$

Portanto a demonstração por indução está concluída.

□

Exemplo 2.10. *Se* $c_k = \frac{p_k}{q_k}$ *é a k-ésima reduzida da fração contínua* $[a_0; a_1, a_2, ..., a_{k-1}, a_k]$ *e* $a_0 > 0$*, então*

$$\frac{p_k}{p_{k-1}} = [a_k; a_{k-1}, a_{k-2}, ..., a_1, a_0]$$

e

$$\frac{q_k}{q_{k-1}} = [a_k; a_{k-1}, a_{k-2}, ..., a_1].$$

Solução. *Sabemos que*

$$\begin{aligned} p_r &= a_r p_{r-1} + p_{r-2} \\ \frac{p_r}{p_{r-1}} &= a_r + \frac{p_{r-2}}{p_{r-1}} \\ \frac{p_r}{p_{r-1}} &= a_r + \frac{1}{\frac{p_{r-1}}{p_{r-2}}}, \end{aligned}$$

com r natural maior do que ou igual a 2*. Assim podemos escrever* $\frac{p_k}{p_{k-1}}$ *da seguinte forma*

$$\frac{p_k}{p_{k-1}} = a_k + \cfrac{1}{a_{k-1} + \cfrac{1}{a_{k-2} + \ddots + \cfrac{1}{a_2 + \cfrac{1}{\frac{p_1}{p_0}}}}},$$

onde $p_1 = a_1a_0 + 1$ *e* $p_0 = a_0$. *Logo*

$$\frac{p_k}{p_{k-1}} = a_k + \cfrac{1}{a_{k-1} + \cfrac{1}{a_{k-2} + \ddots + \cfrac{1}{a_2 + \cfrac{1}{a_1 + \cfrac{1}{a_0}}}}} = [a_k; a_{k-1}, a_{k-2}, ..., a_1, a_0].$$

De modo análogo $\frac{q_k}{q_{k-1}}$ *temos*

$$\frac{q_k}{q_{k-1}} = a_k + \cfrac{1}{a_{k-1} + \cfrac{1}{a_{k-2} + \ddots + \cfrac{1}{a_2 + \cfrac{1}{\cfrac{q_1}{q_0}}}}}.$$

Como $q_1 = a_1$ *e* $q_0 = 1$ *implica*

$$\frac{q_k}{q_{k-1}} = a_k + \cfrac{1}{a_{k-1} + \cfrac{1}{a_{k-2} + \ddots + \cfrac{1}{a_2 + \cfrac{1}{a_1}}}} = [a_k; a_{k-1}, a_{k-2}, ..., a_1].$$

Exemplo 2.11. *Se* $c_k = \frac{p_k}{q_k}$ *é a k-ésima reduzida da fração contínua* $[1; 2, 3, 4, ..., n, n+1]$, *então*

$$p_n = np_{n-1} + np_{n-2} + (n-1)p_{n-3} + \cdots + 3p_1 + 2p_0 + p_0 + 1$$

Prova. *Pela fração contínua, sabemos que* $p_0 = 1, p_1 = 3, a_k = (k+1)$ *e, pelo Teorema 2.9,* $p_k = a_kp_{k-1} + p_{k-2} \Rightarrow p_k = (k+1)p_{k-1} + p_{k-2}$, *logo* $p_k - p_{k-1} = kp_{k-1} + p_{k-2}$. *Para*

$k \geq 2$ *temos*

$$\begin{aligned}
\sum_{k=2}^{n}(p_k - p_{k-1}) &= \sum_{k=2}^{n}(kp_{k-1} + p_{k-2}) \\
p_n - p_1 &= \sum_{k=2}^{n} kp_{k-1} + \sum_{k=2}^{n} p_{k-2} \\
p_n - p_1 &= \left(np_{n-1} + \sum_{k=2}^{n-1} kp_{k-1}\right) + \left(\sum_{k=2}^{n-1} p_{k-1} + p_0\right) \\
p_n &= np_{n-1} + \sum_{k=2}^{n-1}(k+1)p_{k-1} + p_1 + p_0 \\
p_n &= np_{n-1} + np_{n-2} + \cdots + 4p_2 + 3p_1 + p_1 + p_0 \\
p_n &= np_{n-1} + np_{n-2} + \cdots + 4p_2 + 3p_1 + 3p_0 + p_0 \\
p_n &= np_{n-1} + np_{n-2} + \cdots + 4p_2 + 3p_1 + 2p_0 + p_0 + 1.
\end{aligned}$$

Teorema 2.12. *A relação $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$ se verifica para todo $k \geq 1$, onde p_k e q_k são, respectivamente, o numerador e denominador da k-ésima reduzida da fração contínua $[a_0; a_1, a_2, ..., a_{k-1}, a_k]$.*

Prova. *Este resultado será demostrado por indução matemática.*

i) Para $k = 1$, temos que $p_1q_0 - p_0q_1 = (a_0a_1 + 1).1 - a_0.a_1 = 1 = (-1)^0 = (-1)^{1-1}$.

ii) Supondo que $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$ é válido para algum k natural maior do que ou igual a 2, então

$$\begin{aligned}
p_{k+1}q_k - p_kq_{k+1} &= (a_{k+1}p_k + p_{k-1})q_k - p_k(a_{k+1}q_k + q_{k-1}) \\
&= a_{k+1}p_kq_k + p_{k-1}q_k - a_{k+1}p_kq_k - p_kq_{k-1} \\
&= p_{k-1}q_k - p_kq_{k-1} \\
&= -(p_kq_{k-1} - p_{k-1}q_k) \\
&= (-1)(-1)^{k-1} = (-1)^k.
\end{aligned}$$

Assim a relação é válida para todo inteiro positivo.

□

Corolário 2.13. *Para toda reduzida $c_k = \dfrac{p_k}{q_k}$ tem-se que $(p_k, q_k) = 1$.*

Prova. *Seja $d = (p_k, q_k)$, então $d \mid p_k$ e $d \mid q_k$, mas como $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$. Então $d \mid 1$ ou $d \mid -1$, logo $d = 1$.*

□

Exemplo 2.14. *Mostre que* $c_k = \dfrac{u_k}{u_{k+1}}$, *onde* c_k *é a n-ésima reduzida da fração contínua* $[0; 1, 1, 1, ...]$ *e* u_k *é um número de Fibonacci.*

Prova. *Com efeito, como todos os* $a_i = 1$ *para* $i \geq 1$ *então* $p_k = p_{k-1} + p_{k-2}$ *e* $q_k = q_{k-1} + q_{k-2}$, *sendo* $p_1 = 1$, $p_2 = 1$, $q_0 = 1$ *e* $q_1 = 1$. *Logo* $u_k = p_k$ *e* $u_{k+1} = q_k$, *resulta que*

$$c_k = \frac{p_k}{q_k} = \frac{u_k}{u_{k+1}}.$$

□

O resultado a seguir é consequência direta da demonstração do exemplo anterior.

Exemplo 2.15. *Sendo* u_k *o k-ésimo número de Fibonacci, temos que* $u_k^2 - u_{k+1}u_{k-1} = (-1)^{k-1}$ *para* $k \geq 2$.

Prova. *Considerando Teorema 2.12, temos que* $p_k q_{k-1} - p_{k-1}q_k = (-1)^{k-1}$, *para* $k \geq 2$. *Sendo* $u_k = p_k$ *e* $u_{k-1} = q_k$, *temos*

$$u_k u_k - u_{k-1}u_{k+1} = (-1)^{k-1}$$
$$u_k^2 - u_{k-1}u_{k+1} = (-1)^{k-1}.$$

□

Os quocientes das reduzidas das Frações Contínuas formam uma sequência crescente a partir do q_1, ou seja $q_0 \leq q_1$ e $q_{k-1} < q_k$ para todo inteiro k tal que $k \geq 2$. Este resultado é mostrado no Lema 2.16 que segue abaixo.

Lema 2.16. *Se* q_k *é o denominador da k-ésima reduzida da fração contínua* $[a_0; a_1, a_2, ..., a_n]$, *então* $q_{k-1} \leq q_k$, *para* $1 \leq k \leq n$. *A desigualdade é estrita para* $k > 1$.

Prova. *Usaremos novamente o princípio de indução matemática para demonstrar este resultado.*

i) Para $k = 1$, *temos que* $q_0 = 1 \leq a_1 = q_1$. *Sendo* $k = 2$ *temos* $q_2 = a_2 q_1 + q_0$, *com* a_2, q_1, q_0 *positivos, logo* $q_2 > a_2 q_1$ *o que resulta* $q_2 > q_1$.

ii) Supondo que seja verdadeiro para algum m inteiro tal que $1 \leq m < k$, *então como* $q_{m+1} = a_{m+1}q_m + q_{m-1}$ *temos* $q_{m+1} > a_{m+1}q_m > q_m$, *pois* $q_{m-1}, a_{m+1} \geq 1$.

Portanto o resultado é válido para todo inteiro $k \geq 1$.

□

Proposição 2.17. *Se* $c_k = \dfrac{p_k}{q_k}$ *é a k-ésima reduzida da fração contínua simples* $[a_0; a_1, a_2, ..., a_n]$, *então*

$$q_k \geq 2^{\frac{k-1}{2}},$$

para $2 \leq k \leq n$.

Prova. *Do Teorema 2.9, temos que* $q_k = a_k q_{k-1} + q_{k-2}$ *e, pelo Lema 2.16, sabemos que a sequência dos quocientes das reduzidas é não decrescente, ou seja* $q_{k-2} \leq q_{k-1}$, *para* $2 \leq k \leq n$. *Sendo* a_k *inteiro positivo, então* $a_k q_{k-2} \leq a_k q_{k-1}$ *implica que* $q_{k-2} \leq a_k q_{k-1}$.

Adicionando q_{k-2} *em ambos os lados da desigualdade, obtemos*

$$\begin{aligned} q_{k-2} + q_{k-2} &\leq a_k q_{k-1} + q_{k-2} \\ 2q_{k-2} &\leq a_k q_{k-1} + q_{k-2} \\ 2q_{k-2} &\leq q_k \\ 2 &\leq \frac{q_k}{q_{k-2}}. \end{aligned}$$

Portanto

$$\begin{aligned} \left(\frac{q_2}{q_0}\right) \cdot \left(\frac{q_3}{q_1}\right) \cdot \left(\frac{q_4}{q_2}\right) \cdot \cdots \cdot \left(\frac{q_{k-2}}{q_{k-4}}\right) \cdot \left(\frac{q_{k-1}}{q_{k-3}}\right) \cdot \left(\frac{q_k}{q_{k-2}}\right) &\geq 2^{k-1} \\ \left(\frac{q_k q_{k-1}}{q_0 q_1}\right) &\geq 2^{k-1} \end{aligned}$$

Sendo $q_0 = 1$, $q_1 = a_1 \geq 1$ *implica que* $\dfrac{1}{q_1} \leq 1$. *Dessa forma,*

$$\begin{aligned} q_k q_{k-1} \geq \frac{q_k q_{k-1}}{q_0 q_1} &\geq 2^{k-1} \\ q_k^2 \geq q_k q_{k-1} &\geq 2^{k-1} \\ q_k &\geq 2^{\frac{k-1}{2}}. \end{aligned}$$

Teorema 2.18. *As reduzidas de índices ímpares de uma fração contínua formam uma sequência estritamente decrescente, ao passo que as de índices pares formam uma sequência estritamente crescente.*

Prova. *Seja*

$$\begin{aligned} c_{k+2} - c_k &= (c_{k+2} - c_{k+1}) + (c_{k+1} - c_k) \\ &= \left(\frac{p_{k+2}}{q_{k+2}} - \frac{p_{k+1}}{q_{k+1}}\right) + \left(\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right) \\ &= \frac{p_{k+2}q_{k+1} - p_{k+1}q_{k+2}}{q_{k+1}q_{k+2}} + \frac{p_{k+1}q_k - p_kq_{k+1}}{q_{k+1}q_k} \\ &= \frac{(-1)^{k+1}}{q_{k+1}q_{k+2}} + \frac{(-1)^k}{q_{k+1}q_k} \\ &= (-1)^k\left(\frac{1}{q_{k+1}q_k} - \frac{1}{q_{k+1}q_{k+2}}\right) \\ &= (-1)^k\left(\frac{q_{k+2} - q_k}{q_{k+2}q_{k+1}q_k}\right). \end{aligned}$$

Pelo Lema 2.16, $q_{k+2} > q_{k+1}$ *e* $q_{k+1} > q_k$ *então* $q_{k+2} > q_k$*, para todo* $k > 1$*.*

Portanto $c_{k+2} - c_k < 0$*, se* k *é ímpar. Dessa forma, as reduzidas de índices ímpares determinam uma sequência estritamente decrescente, ou seja* $c_1 > c_3 > c_5 > \cdots$*.*

Por outro lado, se k *é par, então* $c_{k+2} - c_k > 0$ *e, assim, a sequência das reduzidas de ordem par é crescente.*

□

Teorema 2.19. *Qualquer reduzida de índice ímpar é maior do que qualquer reduzida de índice par.*

Prova. *De fato, pelo Teorema 2.12, temos que* $p_kq_{k-1} - p_{k-1}q_k = (-1)^{k-1}$*. Assim, sendo* $q_kq_{k-1} \neq 0$*, segue que*

$$\begin{aligned} \frac{p_kq_{k-1} - p_{k-1}q_k}{q_kq_{k-1}} &= \frac{(-1)^{k-1}}{q_kq_{k-1}} \\ \frac{p_k}{q_k} - \frac{p_{k-1}}{q_{k-1}} &= \frac{(-1)^{k-1}}{q_kq_{k-1}} \\ c_k - c_{k-1} &= \frac{(-1)^{k-1}}{q_kq_{k-1}}. \end{aligned}$$

Para $k = 2j$*, com* $j \in \mathbb{N}$*, temos que* $\dfrac{(-1)^{2j-1}}{q_{2j}q_{2j-1}} < 0$*, portanto* $c_{2j} - c_{2j-1} < 0$ *o que implica* $c_{2j} < c_{2j-1}$*. Seja* c_{2j} *a 2j-ésima reduzida de uma fração contínua, como*

$$c_{2j} < c_{2j+2r} < c_{2j+2r-1} < c_{2r-1},$$

com r *um inteiro positivo. Logo* $c_{2j} < c_{2r-1}$ *para* $j, r \in \mathbb{N}$*.*

□

2.3 Soluções de Equações Diofantinas através de Frações Contínuas

Seja $ax + by = c$ uma equação diofantina, com $a, b, c \in \mathbb{Z}$ e $(a, b) = 1$. Assim para encontrarmos um par X e Y que satisfaça a equação precisamos expandir o número racional $\frac{a}{b}$ em fração contínua. Considerando $\frac{a}{b} = [a_0; a_1, a_2, ..., a_n]$, então os dois últimos reduzidas são $c_{n-1} = \frac{p_{n-1}}{q_{n-1}}$ e $c_n = \frac{p_n}{q_n} = \frac{a}{b}$, pois $(p_n, q_n) = 1$.

Pela relação 2.12, temos que $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$, mas $p_n = a$ e $q_n = b$ resulta que

$$aq_{n-1} - bp_{n-1} = (-1)^{n-1}.$$

i) Para n ímpar, $aq_{n-1} - bp_{n-1} = 1$ logo $x_0 = cq_{n-1}$ e $y_0 = -cp_{n-1}$ é uma solução particular. Dessa forma, $X = cq_{n-1} + bt$ e $Y = -cp_{n-1} - at$, com $t \in \mathbb{Z}$, é a solução da equação

ii) Para n par, temos que $aq_{n-1} - bp_{n-1} = -1 \Rightarrow -aq_{n-1} + bp_{n-1} = 1$. Portanto $x_0 = -cq_{n-1}$ e $y_0 = cp_{n-1}$ é uma solução particular. Assim $X = -cq_{n-1} + bt$ e $Y = cp_{n-1} - at$, com $t \in \mathbb{Z}$, é a solução da equação.

Exemplo 2.20. *Resolva a equação diofantina linear*

$$363x + 102y = 90$$

por meio das frações contínuas.

Solução. *Sabemos que o* $(363, 102) = 3$, *assim podemos simplificar a equação dividindo ambos os membros por* 3, *logo temos*

$$121x + 34y = 30.$$

Pelo Exemplo 2.1, temos $\frac{121}{34} = [3; 1, 1, 3, 1, 3]$ *portanto* $\frac{p_4}{q_4} = 3 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1}}}}$, *com isso* $p_4 = 32$ *e* $q_4 = 9$. *Como* $n = 5$ *é ímpar, resulta que*

$$121(9) - 34(32) = 1$$
$$121(9.30) - 34(32.30) = 30$$
$$121(270) + 34(-960) = 30.$$

Dessa forma, $x_0 = 270$ e $y_0 = -960$ é uma solução particular da equação diofantina, ao passo que

$$x = 270 + 34t \qquad\qquad y = -960 - 121t,$$

com $t \in \mathbb{Z}$, é a solução geral.

2.4 Frações Contínuas Infinitas

Para estudarmos as frações contínuas infinitas, precisaremos de um resultado da Análise matemática. Dessa forma, iremos apresentar o Teorema, sem, contudo, demonstrá-lo. O leitor interessado em compreender a demonstração do resultado que segue pode encontrá-lo em [11].

Teorema 2.21. *Toda sequência crescente (decrescente) limitada superiormente (inferiormente) é convergente.*

Com esse resultado podemos demonstrar o teorema que segue.

Teorema 2.22. *Sejam $a_0, a_1, a_2, ...$ uma sequência infinita de números inteiros, com $a_1, a_2, ...$ positivos e $c_k = [a_0; a_1, a_2, ..., a_k]$. Então a sequência das reduzidas c_k tende para o limite α, isto é*

$$\lim_{k\to\infty} c_k = \alpha.$$

Prova. *Pelo Teorema 2.18, sabemos que $c_0 < c_2 < c_4 < c_6 < \cdots$, ou seja as reduzidas de índices pares formam uma sequência crescente. Mas pelo Teorema 2.19, temos que qualquer reduzida de ordem par é menor do qualquer uma de ordem ímpar, em particular $c_{2k} < c_1$, para todo $k \in \mathbb{N}$. Dessa forma, a sequência formada pelas reduzidas de ordem par é crescente e limitada superiormente, logo, pelo teorema anterior, é convergente. Analogamente, a sequência das reduzidas de ordem ímpar é decrescente e limitada inferiormente, portanto $(c_{2k-1})_{k\in\mathbb{N}}$ é convergente.*

Suponha que $\lim_{k\to\infty} c_{2k} = L_1$ e que $\lim_{k\to\infty} c_{2k-1} = L_2$, assim

$$\begin{aligned}
L_2 - L_1 &= \lim_{k\to\infty} c_{2k-1} - \lim_{k\to\infty} c_{2k} \\
&= \lim_{k\to\infty} (c_{2k-1} - c_{2k}) \\
&= \lim_{k\to\infty} \left(\frac{p_{2k-1}}{q_{2k-1}} - \frac{p_{2k}}{q_{2k}} \right) \\
&= \lim_{k\to\infty} \left(\frac{p_{2k-1}q_{2k}}{q_{2k}q_{2k-1}} - \frac{p_{2k}q_{2k-1}}{q_{2k}q_{2k-1}} \right) \\
&= \lim_{k\to\infty} \frac{p_{2k-1}q_{2k} - p_{2k}q_{2k-1}}{q_{2k}q_{2k-1}} = \lim_{k\to\infty} \frac{(-1)^{2k}}{q_{2k}q_{2k-1}} = \lim_{k\to\infty} \frac{1}{q_{2k}q_{2k-1}}.
\end{aligned}$$

Sendo $\lim_{k\to\infty} \dfrac{1}{q_{2k}q_{2k-1}} = 0$ *pois* $q_k \geq 2^{\frac{k-1}{2}}$ *para* $k \in \mathbb{N}$, *implica que* $L_2 - L_1 = 0$, *logo* $L_2 = L_1 = \alpha$.

□

Corolário 2.23. *Se a sequência das reduzidas* $(c_n)_{n\in\mathbb{N}}$ *de* $[a_0; a_1, a_2, ...]$ *converge para* α, *então* α *pertence ao segmento de extremos* $\dfrac{p_n}{q_n}$ *e* $\dfrac{p_{n+1}}{q_{n+1}}$.

Prova. *Pelo Teorema 2.22, temos*

$$\lim_{k\to\infty} c_{2k} = \alpha \qquad\qquad \lim_{k\to\infty} c_{2k-1} = \alpha.$$

Sendo $(c_{2k})_{k\in\mathbb{N}}$ *crescente implica que* $c_{2k} < \alpha$, *para todo* k *natural. Por outro lado,* $\alpha < c_{2k-1}$, *pois* $(c_{2k-1})_{k\in\mathbb{N}}$ *é decrescente.*

i) Para n *par, implica* $c_n < \alpha < c_{n+1}$. *Logo* $\alpha \in (c_n; c_{n+1})$.

ii) Para n *ímpar, temos* $c_{n+1} < \alpha < c_n$. *Logo* $\alpha \in (c_{n+1}; c_n)$.

De toda forma, α *pertence ao segmento de extremos* $c_n = \dfrac{p_n}{q_n}$ *e* $c_{n+1} = \dfrac{p_{n+1}}{q_{n+1}}$.

□

Definição 2.24. *Se* $a_0, a_1, a_2, ...$ *é uma sequência infinita de numeros inteiros, com* $a_1, a_2, \cdots$ *positivos, então a fração contínua infinita* $[a_0; a_1, a_2, ...]$ *tem o valor*

$$\lim_{n\to\infty}[a_0; a_1, a_2, ...a_n].$$

Exemplo 2.25. *Vamos recorrer ao Exemplo 2.14 para ilustrarmos a definição acima. Pela definição de fração contínua infinita, sabemos* $[1; 1, 1, ...] = \lim_{n\to\infty}[1; 1, 1, ..., 1]$. *Como a n-ésima reduzida é dada por* $c_n = \dfrac{u_n}{u_{n+1}}$, *então sendo* $\alpha = [1; 1, 1, ...]$ *implica que*

$$\begin{aligned}
\alpha = \lim_{n\to\infty}[1; 1, 1, ..., 1] &= \lim_{n\to\infty} \frac{u_n}{u_{n-1}} \\
&= \lim_{n\to\infty} \frac{u_{n-1} + u_{n-2}}{u_{n-1}} \\
&= \lim_{n\to\infty} \left(1 + \frac{u_{n-2}}{u_{n-1}}\right) \\
&= 1 + \lim_{n\to\infty} \frac{u_{n-2}}{u_{n-1}} \\
&= 1 + \frac{1}{\lim_{n\to\infty} \dfrac{u_{n-1}}{u_{n-2}}} \\
&= 1 + \frac{1}{\alpha}
\end{aligned}$$

Como $\alpha = 1 + \frac{1}{\alpha}$, *então* $[1;1,1,...]$ *é a raiz positiva da equação do segundo grau* $\alpha^2 - \alpha - 1 = 0$. *Logo* $[1;1,1,...] = \frac{1+\sqrt{5}}{2}$.

Lema 2.26. *Se* $\alpha = [a_0; a_1, a_2, ...]$, *então* $0 < |\alpha - c_n| < \frac{1}{q_n q_{n+1}}$.

Prova. *Como* $\alpha = [a_0; a_1, a_2, ...]$ *então*

$$\alpha = \lim_{n\to\infty}[a_0; a_1, a_2, ..., a_n]$$
$$\alpha = \lim_{n\to\infty} c_n.$$

Assim, pelo Corolário 2.23, α *está estritamente entre* c_n *e* c_{n+1}, *assim* $|\alpha - c_n| > 0$ *e, além disso,*

$$|\alpha - c_n| < |c_{n+1} - c_n|$$
$$|\alpha - c_n| < \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right|$$
$$|\alpha - c_n| < \left|\frac{p_{n+1}q_n - p_n q_{n+1}}{q_n q_{n+1}}\right|$$
$$|\alpha - c_n| < \left|\frac{(-1)^n}{q_n q_{n+1}}\right|$$
$$|\alpha - c_n| < \frac{1}{q_n q_{n+1}},$$

logo $0 < |\alpha - c_n| < \frac{1}{q_n q_{n+1}}$.

□

Teorema 2.27. *Sejam* $a_0, a_1, a_2, ...$ *números inteiros, com* $a_1, a_2, ...$ *positivos. Então* $[a_0; a_1, a_2, ...]$ *é irracional.*

Prova. *Suponha, por absurdo, que* $\alpha = [a_0; a_1, a_2, ...]$ *é racional, assim existem* a, b *inteiros, com* b *positivo, tais que* $\alpha = \frac{a}{b}$. *Pelo Lema anterior, temos que* $0 < \left|\frac{a}{b} - c_n\right| < \frac{1}{q_n q_{n+1}}$,

logo

$$\begin{aligned}\left|\frac{a}{b}-\frac{p_n}{q_n}\right| &< \frac{1}{q_nq_{n+1}}\\ \left|\frac{aq_n-bp_n}{bq_n}\right| &< \frac{1}{q_nq_{n+1}}\\ \frac{|aq_n-bp_n|}{bq_n} &< \frac{1}{q_nq_{n+1}}\\ |aq_n-bp_n| &< \frac{b}{q_{n+1}},\end{aligned}$$

portanto $0 < |aq_n - bp_n| < \dfrac{b}{q_{n+1}}$. *Sabemos que* q_n *é inteiro e aumenta à medida que* n *cresce. Assim tomando um* n *suficientemente grande tal que* $b < q_{n+1}$, *então* $\dfrac{b}{q_{n+1}} < 1$. *Assim,*

$$0 < |aq_n - bp_n| < 1,$$

que é uma contradição, porque a, b, q_n, p_n *são inteiros, logo* $|aq_n - bp_n|$ *é um inteiro que estaria entre* 0 *e* 1. *Portanto* $\alpha = [a_0, a_1, a_2, ...]$ *é um irracional.*

□

Teorema 2.28. *Se* $[a_0; a_1, a_2, ...]$ *e* $[b_0; b_1, b_2, ...]$ *representam o mesmo número irracional, então* $a_n = b_n$ *para todo* $n \geq 0$.

Prova. *A prova será feita por indução.*

i) Devemos mostrar primeiramente que $a_0 = b_0$. *De fato, supondo que* $[a_0; a_1, a_2, ...] = \alpha = [b_0; b_1, b_2, ...]$ *e que* c_n *e* c'_n *as* n*-ésimas reduzidas de cada uma das frações contínuas infinitas, então* $c_0 < \alpha < c_1$ *e* $c'_0 < \alpha < c'_1$. *Mais precisamente, temos*

$$a_0 < \alpha < a_0 + \frac{1}{a_1} \qquad\qquad b_0 < \alpha < b_0 + \frac{1}{b_1}.$$

Sendo a_1 *e* b_1 *inteiros positivos, então* $\dfrac{1}{a_1} \leq 1$ *e* $\dfrac{1}{b_1} \leq 1$. *Assim*

$$\begin{aligned} a_0 < \alpha < a_0 + 1 \qquad & e \qquad b_0 < \alpha < b_0 + 1\\ a_0 = \lfloor \alpha \rfloor \qquad & \qquad b_0 = \lfloor \alpha \rfloor,\end{aligned}$$

onde $\lfloor \alpha \rfloor$ *é a parte inteira do irracional* α. *Dessa forma* $a_0 = b_0$.

ii) Supondo que $a_k = b_k$ para todo $k \leq n$, então devemos mostrar que $a_{n+1} = b_{n+1}$. Pois bem, como

$$\begin{aligned}
[a_0; a_1, a_2, ...] &= \lim_{n\to\infty}[a_0; a_1, a_2, ..., a_n] \\
&= \lim_{n\to\infty}\left(a_0 + \frac{1}{[a_1; a_2, a_3, ..., a_n]}\right) \\
&= a_0 + \lim_{n\to\infty}\left(\frac{1}{[a_1; a_2, a_3, ..., a_n]}\right) \\
&= a_0 + \frac{1}{\lim_{n\to\infty}[a_1; a_2, a_3, ..., a_n]} \\
&= a_0 + \frac{1}{[a_1; a_2, a_3, ...]}
\end{aligned}$$

e, de forma análoga,

$$[b_0; b_1, b_2, ...] = b_0 + \frac{1}{[b_1; b_2, b_3, ...]},$$

então sendo $a_0 = b_0$ implica $[a_1; a_2, a_3, ...] = [b_1; b_2, b_3, ...]$. Procedendo da mesma forma e tendo $a_0 = b_0, a_1 = b_1, ..., a_n = b_n$ resulta

$$[a_{n+1}; a_{n+2}, a_{n+3}, ...] = [b_{n+1}; b_{n+2}, b_{n+3}, ...] = \beta.$$

Logo

$$\begin{aligned}
a_{n+1} < \beta < a_{n+1} + 1 \qquad & \qquad b_{n+1} < \beta < b_{n+1} + 1 \\
a_{n+1} = \lfloor\beta\rfloor \qquad & \qquad b_{n+1} = \lfloor\beta\rfloor,
\end{aligned}$$

portanto $a_{n+1} = b_{n+1}$. Dessa forma $a_n = b_n$ para todo $n \in \mathbb{N}$.

□

Teorema 2.29. *Seja $\alpha = x_0$ um número irracional. Se x_{n+1} é definido recursivamente como $x_{n+1} = \dfrac{1}{x_n - \lfloor x_n\rfloor}$, com $a_n = \lfloor x_n\rfloor$, então α é o valor da fração contínua infinita $[a_0; a_1, a_2, ...]$.*

Prova. *De fato, como $x_{n+1} = \dfrac{1}{x_n - \lfloor x_n\rfloor}$ implica que $x_n = \lfloor x_n\rfloor + \dfrac{1}{x_{n+1}} = a_n + \dfrac{1}{x_{n+1}}$,*

para $n \geq 0$. *Portanto*

$$\begin{aligned}
\alpha &= a_0 + \frac{1}{x_1} \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{x_2}} \\
&\vdots \\
&= a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots \; + \cfrac{1}{a_n + \cfrac{1}{x_{n+1}}}}} = [a_0; a_1, a_2, ..., a_n, x_{n+1}],
\end{aligned}$$

logo $\alpha = [a_0; a_1, a_2, ..., a_n, x_{n+1}]$.

Assim, como x_0 *é irracional, implica que* x_{n+1} *é irracional, para todo* $n \geq 0$. *Provaremos esse fato por indução sobre* n.

i) Pois bem, para $n = 0$, $x_1 = \dfrac{1}{x_0 - \lfloor x_0 \rfloor}$. *Sendo* $x_0 - \lfloor x_0 \rfloor$ *irracional, então* x_1 *também será.*

ii) Supondo que x_n *é um número irracional, para algum* n *natural. Então* $x_n - \lfloor x_n \rfloor$ *é irracional, logo* $\dfrac{1}{x_n - \lfloor x_n \rfloor}$ *é irracional. Assim* x_{n+1} *é um número irracional, para todo* $n \geq 0$.

Como $x_n - \lfloor x_n \rfloor < 1$ *então* $1 < \dfrac{1}{x_n - \lfloor x_n \rfloor} = x_{n+1}$, *para* $n \geq 0$. *Sendo* $a_{n+1} = \lfloor x_{n+1} \rfloor$, *logo* $a_{n+1} \geq 1$. *Assim os inteiros* a_{n+1} *são todos maiores ou iguais a* 1, *exceto possivelmente o* a_0.

Considerando a fração contínua infinita $[a_0; a_1, a_2, ..., a_n, ...]$, *verificam-se que as* $(n+1)$ *primeiras reduzidas são iguais às de* $[a_0; a_1, a_2, ..., a_n, x_{n+1}]$. *Como* $\alpha = [a_0; a_1, a_2, ..., a_n, x_{n+1}]$ *então, pelo Teorema 2.9,* $\alpha = \dfrac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}}$. *Sendo* c_n *a* n*-ésima reduzida de* $[a_0; a_1, a_2, ..., a_n, ...]$, *então*

$$\begin{aligned}
\alpha - c_n =& \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} \\
\alpha - c_n =& \frac{x_{n+1}p_nq_n + p_{n-1}q_n - p_nx_{n+1}q_n - p_nq_{n-1}}{q_n(x_{n+1}q_n + q_{n-1})} \\
\alpha - c_n =& \frac{-(-p_{n-1}q_n + p_nq_{n-1})}{q_n(x_{n+1}q_n + q_{n-1})} \\
\alpha - c_n =& \frac{(-1)^n}{q_n(x_{n+1}q_n + q_{n-1})}.
\end{aligned}$$

Sabendo que $x_{n+1} > a_{n+1}$*, temos que*

$$|\alpha - c_n| = \frac{1}{q_n(x_{n+1}q_n + q_{n-1})} < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} < \frac{1}{q_nq_{n+1}}.$$

Assim

$$\alpha = \lim_{n\to\infty} c_n = [a_0; a_1, a_2, a_3, ...].$$

□

Exemplo 2.30. *Para ilustrarmos o algoritmo anterior, iremos expandir* $\sqrt{5}$ *em termo de frações contínuas. Como* $x_{n+1} = \dfrac{1}{x_n - \lfloor x_n \rfloor}$*, com* $a_n = \lfloor x_n \rfloor$*, então* $a_0 = \lfloor \sqrt{5} \rfloor = 2$*.*

$$\begin{aligned}
x_0 &= \sqrt{5} && a_0 = 2 \\
x_1 &= \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 && a_1 = 4 \\
x_2 &= \frac{1}{(\sqrt{5} + 2) - 4} = \frac{1}{\sqrt{5} - 2} = \sqrt{5} + 2 && a_2 = 4
\end{aligned}$$

Como $x_2 = x_1$ *implica que* $\lfloor x_2 \rfloor = \lfloor x_1 \rfloor$*, assim*

$$x_3 = \frac{1}{x_2 - \lfloor x_2 \rfloor} = \frac{1}{x_1 - \lfloor x_1 \rfloor} = x_2 = x_1,$$

logo $x_1 = x_2 = x_3 = x_4 = \cdots$ *e, portanto,* $a_1 = a_2 = a_3 = a_4 = \cdots$*. Assim podemos representar* $\sqrt{5}$ *por* $[2; 4, 4, ...]$

Dizemos, neste caso, que a expansão de $\sqrt{5}$ em termo de fração contínua é infinita e periódica.

Proposição 2.31. *Sejam $\alpha = x_0$ um número irracional e x_{n+1} definido recursivamente como no Teorema 2.29, assim*

$$\alpha - \frac{p_n}{q_n} = \frac{(-1)^n}{(x_{n+1} + y_{n+1}){q_n}^2},$$

com $y_{n+1} = \dfrac{q_{n-1}}{q_n}$ e $a_n = \lfloor x_n \rfloor$.

Prova. *Como na demonstração do Teorema 2.29 $\alpha = [a_0; a_1, a_2, ..., a_n, x_{n+1}]$, então*

$$\alpha = \frac{(x_{n+1})p_n + p_{n-1}}{(x_{n+1})q_n + q_{n-1}}.$$

Dessa forma,

$$\begin{aligned}
\alpha - \frac{p_n}{q_n} =& \frac{(x_{n+1})p_n + p_{n-1}}{(x_{n+1})q_n + q_{n-1}} - \frac{p_n}{q_n} \\
=& \frac{x_{n+1}p_nq_n + p_{n-1}q_n - x_{n+1}p_nq_n - p_nq_{n-1}}{(x_{n+1}q_n + q_{n-1})q_n} \\
=& \frac{p_{n-1}q_n - p_nq_{n-1}}{(x_{n+1}q_n + q_{n-1})q_n} \\
=& \frac{(-1)^n}{(x_{n+1}q_n + q_{n-1})q_n} \\
=& \frac{(-1)^n}{\left(x_{n+1} + \dfrac{q_{n-1}}{q_n}\right){q_n}^2} = \frac{(-1)^n}{(x_{n+1} + y_{n+1})\,{q_n}^2}.
\end{aligned}$$

□

Uma das consequências imediatas desta proposição é o seguinte teorema.

Teorema 2.32. *Sejam $\alpha = [a_0; a_1, a_2, ...]$ um número irracional e $\dfrac{p_n}{q_n}$ a n-ésima reduzida desta expansão, então*

$$\frac{1}{(a_{n+1} + 2){q_n}^2} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{a_{n+1}{q_n}^2},$$

onde $y_{n+1} = \dfrac{q_{n-1}}{q_n}$, $x_0 = \alpha$ e $a_n = \lfloor x_n \rfloor$.

Prova. *De fato, sabemos da proposição anterior que $\alpha - \dfrac{p_n}{q_n} = \dfrac{(-1)^n}{(x_{n+1} + y_{n+1}){q_n}^2}$, com $y_{n+1} = \dfrac{q_{n-1}}{q_n}$, logo*

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{(x_{n+1} + y_{n+1}){q_n}^2}.$$

Sendo crescente a sequência dos denominadores das reduzidas, então $q_{n-1} < q_n$*, ou seja* $\frac{q_{n-1}}{q_n} < 1$*. Assim*

$$0 < y_{n+1} < 1. \tag{2.1}$$

Como $a_n = \lfloor x_n \rfloor$*, implica*

$$a_{n+1} < x_{n+1} < a_{n+1} + 1. \tag{2.2}$$

De (2.1) e (2.2), temos

$$a_{n+1} < x_{n+1} + y_{n+1} < a_{n+1} + 2$$
$$\frac{1}{a_{n+1}+2} < \frac{1}{x_{n+1}+y_{n+1}} < \frac{1}{a_{n+1}},$$

multiplicando todos os membros das desigualdades por $\frac{1}{{q_n}^2}$*, obtemos*

$$\frac{1}{(a_{n+1}+2){q_n}^2} < \frac{1}{(x_{n+1}+y_{n+1}){q_n}^2} < \frac{1}{(a_{n+1}){q_n}^2},$$

o que implica

$$\frac{1}{(a_{n+1}+2){q_n}^2} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{(a_{n+1}){q_n}^2}.$$

□

Teorema 2.33. *Se* $\alpha = [a_0; a_1, a_2, ...]$ *e* $\frac{p_n}{q_n}$ *é a n-ésima reduzida para* $n \geq 1$*, então*

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2{q_n}^2} \qquad ou \qquad \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| < \frac{1}{2{q_{n+1}}^2}.$$

Prova. *Suponha, por absurdo, que*

$$\left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{2{q_n}^2} \qquad e \qquad \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2{q_{n+1}}^2}.$$

Como α *pertence ao intervalo de extremos* $\frac{p_n}{q_n}$ *e* $\frac{p_{n+1}}{q_{n+1}}$*, assim*

$$\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|(\frac{p_{n+1}}{q_{n+1}} - \alpha) + (\alpha - \frac{p_n}{q_n})\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \alpha\right| + \left|\alpha - \frac{p_n}{q_n}\right|,$$

porque $\left(\frac{p_{n+1}}{q_{n+1}} - \alpha\right)$ *e* $\left(\alpha - \frac{p_n}{q_n}\right)$ *possuem o mesmo sinal. Pelo Teorema 2.12 temos* $|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}| = \frac{1}{q_n q_{n+1}}$*, logo*

$$\frac{1}{q_n q_{n+1}} = \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \left|\frac{p_{n+1}}{q_{n+1}} - \alpha\right| + \left|\alpha - \frac{p_n}{q_n}\right| \geq \frac{1}{2{q_{n+1}}^2} + \frac{1}{2{q_n}^2},$$

dessa desigualdade, temos

$$\frac{{q_n}^2 - 2q_nq_{n+1} + {q_{n+1}}^2}{2{q_n}^2{q_{n+1}}^2} \leq 0$$
$$(q_n - q_{n+1})^2 \leq 0 \Rightarrow q_n = q_{n+1},$$

que é uma contradição.

□

As reduzidas c_n das frações contínuas infinitas da expansão de um número irracional α são boas aproximações racionais para α. Elas são os racionais mais próximos de α, dentre todos aqueles que têm denominador menor ou igual a q_n.

Este fato será demonstrado no Teorema 2.35, antes, porém, necessitamos do Lema 2.34, que segue abaixo.

Lema 2.34. *Seja* $\frac{p_n}{q_n}$ *a n-ésima reduzida da fração contínua que representa o número irracional* α. *Se a e b são inteiros, com* $1 \leq b < q_{n+1}$, *então*

$$|q_n\alpha - p_n| \leq |b\alpha - a|.$$

Prova. *Considere o seguinte sistema de equações nas variáveis* ϕ *e* β :

$$p_n\phi + p_{n+1}\beta = a$$
$$q_n\phi + q_{n+1}\beta = b.$$

Sendo D o determinante da matriz dos coeficientes do sistema, temos que $D = p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1} \neq 0$, *logo o sistema admite solução única*

$$\phi = (-1)^{n+1}(aq_{n+1} - bp_{n+1})$$
$$\beta = (-1)^{n+1}(bp_n - aq_n).$$

É evidente que $\phi \neq 0$, *pois caso contrário* $aq_{n+1} = bp_{n+1}$ *e como* $(p_{n+1}, q_{n+1}) = 1$ *implica que* $q_{n+1} \mid b$ *que é um absurdo, tendo em vista que* $1 \leq b < q_{n+1}$.

Passaremos a analisar agora os casos em que β *é maior, menor ou igual a zero.*

i) Para $\beta = 0$, *temos* $p_n\phi = a$ *e* $q_n\phi = b$, *logo* $|b\alpha - a| = |q_n\phi\alpha - p_n\phi| = |\phi||q_n\alpha - p_n|$. *Como* $\phi \neq 0$ *implica* $1 \leq |\phi|$, *assim*

$$|q_n\alpha - p_n| \leq |\phi||q_n\alpha - p_n| = |b\alpha - a|.$$

ii) *Para $\beta > 0$, temos $b < q_{n+1}\beta$, pois $b < q_{n+1}$ por hipótese. Sabemos que $q_n\phi + q_{n+1}\beta = b$, então $q_n\phi + b < b$. Logo $q_n\phi < 0$, portanto $\phi < 0$.*

iii) *Se $\beta < 0$, então, como sabemos que $q_n\phi + q_{n+1}\beta = b$, implica $q_n\phi = b - q_{n+1}\beta > 0$. Assim $q_n\phi > 0$, logo $\phi > 0$.*

Caso $\beta = 0$ verificamos que o Lema é satisfeito. Sendo β não nulo, constatamos, a partir de (ii) e (iii), que ϕ e β têm sinais contrários.

Além disso, podemos inferir também que $q_n\alpha - p_n$ e $q_{n+1}\alpha - p_{n+1}$ têm sinais opostos. Com efeito, como α se encontra entre as reduzidas consecutivas $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$, então $\frac{p_n}{q_n} < \alpha < \frac{p_{n+1}}{q_{n+1}}$. Assim $\frac{p_n}{q_n} < \alpha$, ou seja $0 < q_n\alpha - p_n$. Analogamente, $\alpha < \frac{p_{n+1}}{q_{n+1}}$ então $q_{n+1}\alpha - p_{n+1} < 0$.

Sendo assim, os números

$$\phi(q_n\alpha - p_n) \qquad e \qquad \beta(q_{n+1}\alpha - p_{n+1})$$

têm o mesmo sinal.

Podemos concluir que

$$\begin{aligned} |b\alpha - a| &= |(q_n\phi + q_{n+1}\beta)\alpha - (p_n\phi + p_{n+1}\beta)| \\ &= |q_n\phi\alpha + q_{n+1}\beta\alpha - (p_n\phi + p_{n+1}\beta)| \\ &= |(q_n\phi\alpha - p_n\phi) + (q_{n+1}\beta\alpha - p_{n+1}\beta)| \\ &= |\phi||q_n\alpha - p_n| + |\beta||q_{n+1}\alpha - p_{n+1}| \\ &\geq |\phi||q_n\alpha - p_n| \geq |q_n\alpha - p_n|. \end{aligned}$$

□

Teorema 2.35. *Se $1 \leq b \leq q_n$, então o número racional $\frac{a}{b}$ satisfaz*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leq \left|\alpha - \frac{a}{b}\right|,$$

onde $\frac{p_n}{q_n}$ representa a n-ésima reduzada da fração contínua de α.

Prova. *Suponha que $\left|\alpha - \frac{p_n}{q_n}\right| > \left|\alpha - \frac{a}{b}\right|$. Então como*

$$|q_n\alpha - p_n| = q_n|\alpha - \frac{p_n}{q_n}| > b|\alpha - \frac{a}{b}| = |b\alpha - a|,$$

logo $|q_n\alpha - p_n| > |b\alpha - a|$ que é um absurdo, conforme Lema anterior.

□

Exemplo 2.36. *Como* $\sqrt{5} = [2; 4, 4, 4, ...]$ *então as quatro primeiras reduzidas são* $c_0 = 2, c_1 = \frac{9}{4}, c_2 = \frac{38}{17}$ *e* $c_3 = \frac{161}{72}$. *Podemos concluir, a partir do teorema anterior, que* $\frac{9}{4}$ *é a melhor aproximação racional de* $\sqrt{5}$ *com denominador menor ou igual a 4. Da mesma forma,* $\frac{161}{72}$ *é a melhor aproximal racional de* $\sqrt{5}$ *com denominador menor ou igual a 72.*

Apresentaremos a seguir um resultado que garante que qualquer aproximação racional suficientemente próxima de um irracional arbitrário α é uma das reduzidas da fração contínua infinita que representa este α.

Teorema 2.37. *Seja* α *um número irracional arbitrário. Se o racional irredutível* $\frac{a}{b}$, *com* $b \geq 1$, *satisfaz*

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

então $\frac{a}{b}$ *é uma das reduzidas da fração contínua infinita que representa* α.

Prova. *Suponha que* $\frac{a}{b}$ *não é uma das reduzidas de* α, *logo* $\frac{a}{b} \neq \frac{p_n}{q_n}$, *a qual podemos reescrever da seguinte forma* $aq_n - bp_n \neq 0$. *Sabemos que a sequência dos denominadores das reduzidas de* α *é crescente, sendo assim existe um único* $n \in \mathbb{N}$ *tal que* b *está entre* q_n *e* q_{n+1}, *ou seja*

$$q_n \leq b < q_{n+1}.$$

A partir do Lema 2.34 para este n, *obtemos*

$$|q_n\alpha - p_n| \leq |b\alpha - a| = b\left|\alpha - \frac{a}{b}\right|.$$

Dessa última desigualdade e considerando $\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2}$, *temos*

$$|q_n\alpha - p_n| < \frac{1}{2b}$$
$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2bq_n}.$$

Como $aq_n - bp_n$ *é um inteiro não nulo, então* $|aq_n - bp_n| \geq 1$. *Dividindo ambos os*

membros por bq_n a desigualdade não se altera, porque b e q_n são ambos positivos. Assim

$$\begin{aligned}\frac{1}{bq_n} \leq \frac{|aq_n - bp_n|}{bq_n} &= \left|\frac{aq_n}{bq_n} - \frac{bp_n}{bq_n}\right| = \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \\ &\leq \left|\frac{a}{b} - \frac{p_n}{q_n}\right| = \left|\frac{a}{b} - \alpha + \alpha - \frac{p_n}{q_n}\right| \\ &\leq \left|\left(\frac{a}{b} - \alpha\right) + \left(\alpha - \frac{p_n}{q_n}\right)\right| \\ &\leq \left|\frac{a}{b} - \alpha\right| + \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{2b^2} + \frac{1}{2bq_n}\end{aligned}$$

logo $\dfrac{1}{bq_n} < \dfrac{1}{2b^2} + \dfrac{1}{2bq_n}$ *o que resulta*

$$\begin{aligned}\frac{1}{bq_n} - \frac{1}{2bq_n} &< \frac{1}{2b^2} \\ \frac{1}{2bq_n} &< \frac{1}{2b^2} \\ \frac{1}{q_n} &< \frac{1}{b}\end{aligned}$$

portanto $b < q_n$, que é uma contradição.

□

Teorema 2.38. *Para todo α irracional e todo inteiro $n \geq 1$, temos*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2},$$

para pelo menos um racional $\dfrac{p}{q} \in \left\{\dfrac{p_{n-1}}{q_{n-1}}, \dfrac{p_n}{q_n}, \dfrac{p_{n+1}}{q_{n+1}}\right\}$.

Prova. *Pela Proposição 2.31, temos*

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{(x_{n+1} + y_{n+1}){q_n}^2},$$

com $y_{n+1} = \dfrac{q_{n-1}}{q_n}$, *para algum α irracional. Assim, supondo que o Teorema seja falso, temos que* $\left|\alpha - \dfrac{p_n}{q_n}\right| \geq \dfrac{1}{\sqrt{5}{q_n}^2}$, *para $n \geq 1$. Podemos reescrever esta última desigualdade da seguinte forma*

$$\begin{aligned}\frac{1}{(x_{n+1} + y_{n+1}){q_n}^2} &\geq \frac{1}{\sqrt{5}{q_n}^2} \\ x_{n+1} + y_{n+1} &\leq \sqrt{5}.\end{aligned}$$

Desse jeito,

$$x_{n-1} + y_{n-1} \leq \sqrt{5}, \qquad x_n + y_n \leq \sqrt{5}, \qquad x_{n+1} + y_{n+1} \leq \sqrt{5}.$$

Por outro lado, sabemos que $y_{n+1} = \dfrac{q_{n-1}}{q_n}$ *e que* $q_n = a_n q_{n-1} + q_{n-2}$*, então*

$$\begin{aligned} y_{n+1} &= \frac{q_{n-1}}{a_n q_{n-1} + q_{n-2}} \\ &= \frac{1}{\dfrac{a_n q_{n-1} + q_{n-2}}{q_{n-1}}} \\ &= \frac{1}{a_n + \dfrac{q_{n-2}}{q_{n-1}}} \\ &= \frac{1}{a_n + y_n}, \end{aligned}$$

logo

$$y_{n+1} = \frac{1}{a_n + y_n}. \tag{2.3}$$

Como $x_k + y_k \leq \sqrt{5}$*, para* $k \in \{n, n+1, n+2\}$*, então* $x_k < 3$ *e* $a_k = \lfloor x_k \rfloor \leq 2$*. Sendo* $1 < x_k$ *resulta que* $1 \leq a_k \leq 2$*.*

Assim $1 < a_k + y_k < 3$*, pois* y_k *é um número racional entre zero e um. Dessa última desigualdade, resulta que* $\dfrac{1}{3} < \dfrac{1}{a_k + y_k} = y_{k+1}$*, isso nos mostra que*

$$\frac{1}{3} < y_{n+1}, \qquad \frac{1}{3} < y_{n+2}, \qquad \frac{1}{3} < y_{n+3}.$$

Supondo, por absurdo, que $a_{n+1} = 2$*, temos* $a_{n+1} + y_{n+1} > 2 + \dfrac{1}{3} > \sqrt{5}$ *que é claramente impossível, tendo em vista que* $x_{n+1} + y_{n+1} \leq \sqrt{5}$*. Analogamente, se* $a_{n+2} = 2$ *então nos conduz ao absurdo* $2 + \dfrac{1}{3} < a_{n+2} + y_{n+2}$*, assim* $a_{n+1} = a_{n+2} = 1$*.*

Considerando $x_{n+2} = \dfrac{1}{b}$*,* $y_{n+1} = c$ *e sabendo que* $x_{n+2} = \dfrac{1}{x_{n+1} - a_{n+1}}$*, com* $a_{n+1} = 1$*, temos* $\dfrac{1}{b} = \dfrac{1}{x_{n+1} - 1} \Rightarrow x_{n+1} = b + 1$*.*

Da mesma forma, temos que $x_{n+1} = \dfrac{1}{x_n - a_n}$ *o que resulta* $b + 1 = \dfrac{1}{x_n - a_n}$*, a qual podemos reescrever da seguinte forma*

$$x_n - a_n = \frac{1}{b+1}. \tag{2.4}$$

Para determinarmos y_n *e* y_{n+2}*, usaremos a relação de recorrência em (2.3). Assim* $y_{n+2} = \dfrac{1}{1+c}$*, pois* $y_{n+1} = c$ *e* $a_{n+1} = 1$*. Analogamente, como* $y_{n+1} = \dfrac{1}{a_n + y_n}$*, então*

$a_n + y_n = \dfrac{1}{y_{n+1}}$ *o que resulta em*

$$a_n + y_n = \frac{1}{c} \tag{2.5}$$

De (2.4) e (2.5), temos

$$\begin{aligned}(x_n - a_n) + (a_n + y_n) &= \frac{1}{1+b} + \frac{1}{c}\\ x_n + y_n &= \frac{1}{1+b} + \frac{1}{c}\\ \frac{1}{1+b} + \frac{1}{c} &\leq \sqrt{5}.\end{aligned}$$

Além disso, como $x_{n+1} = 1 + b$ *e* $y_{n+1} = c$ *implica*

$$\begin{aligned}x_{n+1} + y_{n+1} &= (1+b) + c\\ (1+b) + c &\leq \sqrt{5}\end{aligned}$$

e como $x_{n+2} = \dfrac{1}{b}$ *e* $y_{n+2} = \dfrac{1}{1+c}$, *temos*

$$\begin{aligned}x_{n+2} + y_{n+2} &= \frac{1}{b} + \frac{1}{1+c}\\ \frac{1}{b} + \frac{1}{1+c} &\leq \sqrt{5}.\end{aligned}$$

Sabendo que $(1+b) + c \leq \sqrt{5}$ *então* $1 + b \leq \sqrt{5} - c$, *logo*

$$\frac{1}{\sqrt{5}-c} \leq \frac{1}{1+b}.$$

Ao somarmos $\dfrac{1}{c}$ *em ambos os membros da desigualdade, obtemos*

$$\begin{aligned}\frac{1}{\sqrt{5}-c} + \frac{1}{c} &\leq \frac{1}{1+b} + \frac{1}{c}\\ \frac{c + \sqrt{5} - c}{(\sqrt{5}-c)c} &\leq \frac{1}{1+b} + \frac{1}{c} \leq \sqrt{5}\\ \frac{\sqrt{5}}{(\sqrt{5}-c)c} &\leq \sqrt{5}.\\ 1 &\leq (\sqrt{5}-c)c\\ 0 &\leq -c^2 + \sqrt{5}c - 1\end{aligned}$$

Determinaremos agora para quais valores de c a função quadrática $f(c) = -c^2 + \sqrt{5}c - 1$ *assume valores não negativos. Sendo* $c^2 - \sqrt{5}c + 1 = 0$, *implica que a função f é não negativa para*

$$\frac{\sqrt{5}-1}{2} \leq c \leq \frac{\sqrt{5}+1}{2}.$$

Por outro lado, podemos também reorganizar a desigualdade $(1+b)+c \leq \sqrt{5}$ *como segue*

$$\begin{aligned} b &\leq \sqrt{5} - c - 1 \\ \frac{1}{\sqrt{5}-c-1} &\leq \frac{1}{b}. \end{aligned}$$

Somando $\dfrac{1}{1+c}$ *em ambos os membros da desigualdade, temos*

$$\begin{aligned} \frac{1}{\sqrt{5}-c-1} + \frac{1}{1+c} &\leq \frac{1}{b} + \frac{1}{1+c} \\ \frac{1+c+\sqrt{5}-c-1}{(\sqrt{5}-c-1)(1+c)} &\leq \frac{1}{b} + \frac{1}{1+c} \leq \sqrt{5} \\ \frac{\sqrt{5}}{(\sqrt{5}-c-1)(1+c)} &\leq \sqrt{5} \\ 1 &\leq (\sqrt{5}-c-1)(1+c) \\ 0 &\leq -c^2 + c(\sqrt{5}-2) + \sqrt{5} - 2 \end{aligned}$$

Semelhantemente, determinaremos para quais valores de c a função quadrática $f(c) = -c^2 + c(\sqrt{5}-2) + \sqrt{5} - 2$ *assume valores não negativos. Assim f é não negativa para* $\dfrac{\sqrt{5}-3}{2} \leq c \leq \dfrac{\sqrt{5}-1}{2}$.

Como o único valor de c que satisfaz as duas inequações é $\dfrac{\sqrt{5}-1}{2}$, *assim* $c \in \mathbb{R} - \mathbb{Q}$ *que é obviamente um absurdo, pois* $c = y_{n+1} = \dfrac{q_{n-1}}{q_n} \in \mathbb{Q}$.

□

3 Ataque de Wiener

3.1 Criptografia RSA

Mostraremos na próxima seção o ataque à Criptografia RSA desenvolvido por Wiener. Basicamente este ataque fatora, em um tempo polinomial, o módulo RSA, desde que o expoente privado d seja suficientemente pequeno.

Sabemos que neste sistema criptografia, o módulo N é dado por $N = pq$, onde p e q são primos grandes distintos, e que $\phi(N) = (p-1)(q-1)$, com ϕ a função de Euler.

Assim, a chave pública é dada por (N, e), ao passo que a privada é dada por (p, q, d), onde $ed \equiv 1(mod\ \phi(N))$, com $e, d \in \mathbb{N}$ satisfazendo $1 < e, d < \phi(N)$.

Para se codificar uma mensagem m - supondo $m < N$, se não for, pode-se enviar em blocos - usa-se a função de criptografia

$$E(m) \equiv m^e (mod\ N).$$

De posse da mensagem cripitografada m^e, pode-se, com a função de descriptografia, recuperar a mensagem m, ou seja

$$D(m^e) \equiv (m^e)^d \equiv m^{ed} \equiv m(mod\ N).$$

3.2 Ataque de Wiener ao sistema de criptografia RSA

Sejam $N = pq$, onde p e q são primos ímpares, a o menor natural tal que $p < q < ap$ e e com $ed \equiv 1(mod\ \phi(N))$, sendo $1 < e, d < \phi(N)$. Podemos reescrever esta congruência da seguinte forma

$$\phi(N) = \frac{ed-1}{k}, k \in \mathbb{N}. \tag{3.1}$$

A ideia principal do ataque de Wiener é mostrar que para certas restrições de d permitem que a fração $\frac{k}{d}$ possa ser uma das reduzidas de $\frac{e}{N}$.

Para determinarmos uma restrição para d, precisaremos dos três Lemas seguintes.

Lema 3.1. *Seja $N = pq$ onde p e q são primos distintos tais que $p < q < ap$ para alguns $a \in \mathbb{N}$. Então $N - (a+1)\sqrt{N} < \phi(N) < N$.*

Prova. *Primeiro vamos mostrar que $N > \phi(N)$. De fato, como p e q são primos distintos, com $p < q$, então $2 \leq p < q$ o que implica $1 < p + q$. Dessa forma,*

$$\begin{aligned} p + q &> 1 \\ 0 &> 1 - p - q \\ pq &> pq + 1 - p - q \\ N &> p(q-1) - (q-1) \\ N &> (p-1)(q-1) \\ N &> \phi(N) \end{aligned}$$

Agora provaremos que $N - (a+1)\sqrt{N} < \phi(N)$.

Sendo $p < q$ ambos primos então $pp < pq$. Assim $p^2 < N$, logo

$$p < \sqrt{N}. \tag{3.2}$$

Além disso, como $a \in \mathbb{N}$ então $\dfrac{1}{a+1} > 0$, logo

$$p > p - \frac{1}{a+1}. \tag{3.3}$$

Das desigualdades (3.2) e (3.3), temos que

$$\sqrt{N} > p > p - \frac{1}{a+1}.$$

Esta afirmação implica

$$\begin{aligned} (a+1)\sqrt{N} &> p(a+1) - 1 \\ (a+1)\sqrt{N} &> pa + p - 1 > q + p - 1 \\ -(a+1)\sqrt{N} &< 1 - p - q \\ N - (a+1)\sqrt{N} &< N + 1 - p - q \\ N - (a+1)\sqrt{N} &< pq + 1 - p - q \\ N - (a+1)\sqrt{N} &< (p-1)(q-1) \\ N - (a+1)\sqrt{N} &< \phi(N), \end{aligned}$$

portanto $N - (a+1)\sqrt{N} < \phi(N) < N$.

□

Iremos apresentar um resultado que será importante para obtermos uma restrição de d para a qual a fração $\dfrac{k}{d}$ será uma das reduzidas de $\dfrac{e}{N}$.

Lema 3.2. *Seja (N, e) a chave pública, com $N = pq$ tal que $p < q < ap$ para alguns $a \in \mathbb{N}$. Além disso, sejam k e d definidos a partir de (3.1). Então*

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{k(a+1)}{d\sqrt{N}}.$$

Prova. *Mostraremos, primeiro, que* $\left(\frac{k}{d} - \frac{e}{N}\right) < \frac{k(a+1)}{d\sqrt{N}}$.

Assim, pelo Lema 3.1, $N - (a+1)\sqrt{N} < \phi(N) < N$, *logo, para* $k \in \mathbb{N}$, $k(N - (a+1)\sqrt{N}) < k\phi(N)$. *Sendo* $\phi(N) = \frac{ed-1}{k}$, *com* $k \in \mathbb{N}$, *temos que* $k\phi(N) = ed - 1$. *Portanto*

$$\begin{aligned} k(N - (a+1)\sqrt{N}) &< ed - 1 \\ kN - k(a+1)\sqrt{N} &< ed - 1 \\ kN - ed &< k(a+1)\sqrt{N} - 1 \\ \frac{kN - ed}{dN} &< \frac{k(a+1)\sqrt{N} - 1}{dN} \end{aligned}$$

pois $dN \neq 0$. *Dessa forma,*

$$\begin{aligned} \frac{k}{d} - \frac{e}{N} &< \frac{k(a+1)}{d\sqrt{N}} - \frac{1}{dN} \\ \frac{k}{d} - \frac{e}{N} &< \frac{k(a+1)}{d\sqrt{N}}. \end{aligned}$$

Agora, vamos mostrar que $-\frac{k(a+1)}{d\sqrt{N}} < \left(\frac{k}{d} - \frac{e}{N}\right)$. *Sabemos, pelo Lema 3.1, que* $\phi(N) < N$, *assim*

$$k\phi(N) < kN.$$

Além disso, sabemos que $k\phi(N) = ed - 1$ *o que implica* $k\phi(N) + 2 = ed + 1$. *Por hipótese,* $p < q < ap$ *com* p, q *primos distintos e* $a \in \mathbb{N}$, *assim* $a > 1$, *logo* $a + 1 > 2$.

Sendo $N = pq > 1$ *logo* $\sqrt{N} > 1$. *Portanto, para* $k \in \mathbb{N}$, *implica que*

$$2 \leq 2k < k(a+1)\sqrt{N}. \tag{3.4}$$

Considerando

$$k\phi(N) < kN, \tag{3.5}$$

temos, a partir de (3.4) e (3.5), que

$$\begin{aligned} k\phi(N) + 2 &< kN + k(a+1)\sqrt{N} \\ ed + 1 &< kN + k(a+1)\sqrt{N} \\ 1 - k(a+1)\sqrt{N} &< kN - ed \\ \frac{1}{dN} - \frac{k(a+1)}{d\sqrt{N}} &< \frac{k}{d} - \frac{e}{N} \\ -\frac{k(a+1)}{d\sqrt{N}} &< \frac{k}{d} - \frac{e}{N}. \end{aligned}$$

Portanto

$$\left|\frac{k}{d} - \frac{e}{N}\right| < \frac{k(a+1)}{d\sqrt{N}}.$$

□

Lema 3.3. *Sejam k e d definidos a partir de (3.1). Então $k < d$.*

Prova. *Com efeito, sendo $1 < e, d < \phi(N)$ e $k \in \mathbb{N}$ então $ke < k\phi(N)$ logo $ke - 1 < k\phi(N)$. Sabemos de (3.1) que*

$$k\phi(N) = ed - 1,$$

assim $ke - 1 < ed - 1$ o que mostra que $ke < ed$, portanto $k < d$.

□

Com os Lemas 3.1, 3.2 e 3.3 estabelecidos, mostraremos agora que $\frac{k}{d}$ é uma reduzida de $\frac{e}{N}$, para certos valores de d. Para isso, recorreremos ao Teorema 2.37.

Teorema 3.4. *Temos $\frac{k}{d}$ como reduzida de $\frac{e}{N}$, desde que*

$$d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}.$$

Prova. *Sabemos, a partir do Teorema 2.37, que a fração irredutível $\frac{k}{d}$ é uma das reduzidas de $\frac{e}{N}$ se*

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{2d^2}.$$

Sendo (N, e) a chave pública, com $N = pq$ e $p < q < ap$ para alguns $a \in \mathbb{N}$, então, pelo Lema 3.2, temos

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{(a+1)k}{d\sqrt{N}}.$$

Assim para $\frac{(a+1)k}{d\sqrt{N}} < \frac{1}{2d^2}$ *implica que* $\frac{k}{d}$ *é uma das reduzidas de* $\frac{e}{N}$.

Podemos reescrever $\frac{(a+1)k}{d\sqrt{N}} < \frac{1}{2d^2}$ *da seguinte forma*

$$2dk(a+1) < \sqrt{N}.$$

Sendo $k < d$, *pelo Lema 3.4, e* $a \in \mathbb{N}$, *temos*

$$2dk < 2d^2$$
$$2dk(a+1) < 2d^2(a+1).$$

Sendo assim, maximizaremos d *deixando* $2d^2(a+1) \leq \sqrt{N}$, *que produz*

$$d^2 \leq \frac{\sqrt{N}}{2(a+1)}$$
$$d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}.$$

□

A partir do Teorema anterior, podemos observar que o valor máximo de d depende de a e, além disso, à medida que a aumenta o valor de d diminui, onde d é o valor que garante que $\frac{k}{d}$ é uma reduzida de $\frac{e}{N}$.

A partir deste momento, iremos determinar $\frac{k}{d}$ através da fatoração de N, ou seja supondo que $N = x^2 - y^2 = (x-y)(x+y)$, com $x, y \in \mathbb{N}$.

Como $N = pq$ implica $p = x - y$ e $q = x + y$ ou $1 = x - y$ e $N = x + y$. Logo

$$x = \frac{p+q}{2} \qquad y = \frac{q-p}{2}$$

ou

$$x = \frac{N+1}{2} \qquad y = \frac{N-1}{2}.$$

Veremos como utilizar essas informações no ataque de Wiener para determinarmos a chave privada (p, q, d).

Assumindo que $N = x^2 - y^2$ e que d é o maior denominador das reduzidas de $\frac{e}{N}$ tal que $d \leq \frac{\sqrt[4]{N}}{\sqrt{2(a+1)}}$, então testaremos sequencialmente cada uma das reduzidas. Seja

$\frac{k'}{d'}$ a reduzida de $\frac{e}{N}$ que está sendo testada. Para cada reduzida $\frac{k'}{d'}$, sejam $\phi'(N), x'$ e y' definidos da seguintes forma:

$$\begin{aligned}\phi'(N) &= \frac{ed'-1}{k'}\\ x' &= \frac{N-\phi'(N)+1}{2}\\ y' &= \sqrt{(x')^2-N}.\end{aligned}$$

O Teorema a seguir mostra como determinar a chave privada (p, q, d) a partir de x' e y'.

Teorema 3.5. *Seja* $\frac{k'}{d'}$ *uma reduzida de* $\frac{e}{N}$. *Se* $x', y' \in \mathbb{N}$, *definidos como*

$$\begin{aligned}x' &= \frac{N-\phi'(N)+1}{2}\\ y' &= \sqrt{(x')^2-N},\end{aligned}$$

então a chave privada $(p, q, d) = (x'-y', x'+y', d')$.

Prova. *Sendo* x' *e* y' *números naturais, então como* $y' = \sqrt{(x')^2-N}$ *resulta que*

$$\begin{aligned}N &= (x')^2-(y')^2\\ N &= (x'-y')(x'+y').\end{aligned}$$

Obviamente $x'-y' \neq 1$. *De fato, supondo* $1 = x'-y'$ *então* $N = x'+y'$, *assim temos* $x' = \frac{N+1}{2}$. *Como* $x' = \frac{N-\phi'(N)+1}{2}$ *e* $\phi'(N) = \frac{ed'-1}{k'}$ *implica*

$$\begin{aligned}x' &= \frac{N+1}{2} - \frac{\phi'(N)}{2}\\ \frac{N+1}{2} &= \frac{N+1}{2} - \frac{\phi'(N)}{2}\\ \phi'(N) &= 0.\end{aligned}$$

Assim $\frac{ed'-1}{k'} = 0$, *logo* $ed'-1 = 0 \Rightarrow ed' = 1$, *que é um absurdo pois e é um número natural maior do que* 1.

Dessa forma, como $N = pq$, *com* $p < q$, *implica* $p = x'-y'$ *e* $q = x'+y'$. *Logo*

$$x' = \frac{p+q}{2} \qquad\qquad y' = \frac{q-p}{2}.$$

Sendo $x' = \dfrac{N - \phi'(N) + 1}{2}$ *resulta*

$$\begin{aligned} 2x' &= N - \phi'(N) + 1 \\ \phi'(N) &= N - 2x' + 1 \\ \phi'(N) &= N - (p+q) + 1 \\ \phi'(N) &= pq - (p+q) + 1 \\ \phi'(N) &= (p-1)(q-1) = \phi(N). \end{aligned}$$

Como $\phi'(N)k' = ed' - 1$ *e que* $\phi(N)k = ed - 1$*, então*

$$\phi'(N) \mid (ed' - 1) \qquad\qquad \phi(N) \mid (ed - 1).$$

Sendo $\phi'(N) = \phi(N)$*, temos*

$$\begin{aligned} \phi(N) \mid (ed-1) \qquad\qquad & \phi(N) \mid (ed'-1) \\ \phi(N) \mid (ed-1) - (ed'-1) \Rightarrow \qquad\qquad & \phi(N) \mid e(d-d'). \end{aligned}$$

Dessa forma, temos $\phi(N) \mid (d - d')$ *porque* $\phi(N) \nmid e$*, pois* $1 < e < \phi(N)$*.*

Sendo a sequência dos denominadores das reduzidas crescente então $d' \leq d$*, pois estamos testando as reduzidas sequencialmente. Assim como* $1 < d < \phi(N)$ *segue que* $d' = d$*, pois se* $d' < d$ *resultaria no absurdo de* $\phi(N)$ *dividir um número natural menor do que ele. Portanto* $p = x' - y', q = x' + y'$ *e* $d = d'$*.*

□

Exemplo 3.6. *Sejam* $N = 6932927$ *e* $e = 2186443$*. Use o ataque de Wiener para determinar a chave privada* (p, q, d)*.*

Solução. *Sabemos que* $d \leq \dfrac{\sqrt[4]{N}}{\sqrt{2(a+1)}}$*, implica* $d \leq \dfrac{\sqrt[4]{N}}{\sqrt{6}}$*, pois* $a \geq 2$*. Portanto testaremos, sequencialmente, todos os denominadores* d' *das reduzidas de* $\dfrac{e}{N}$ *que sejam menores do que ou iguais a* 20*.*

Como a sétima reduzida de $\dfrac{e}{N}$ *é dada por* $c_7 = [0; 3, 5, 1, 5, 1, 3, 2]$ *assim* $c_1 = \dfrac{1}{3}, c_2 = \dfrac{5}{16}, c_3 = \dfrac{6}{19}$ *e* $c_4 = \dfrac{35}{111}$*.*

Sendo $\phi'(N), x'$ *e* y' *definidos como seguem*

$$\begin{aligned} \phi'(N) &= \frac{ed' - 1}{k'} \\ x' &= \frac{N - \phi'(N) + 1}{2} \\ y' &= \sqrt{(x')^2 - N}, \end{aligned}$$

i) *Para* $c_1 = \frac{1}{3}$, *temos* $d' = 3$ *e* $k' = 1$. *Assim* $\phi'(N) = \frac{2186443 \cdot 3 - 1}{1} = 6559328$, *logo* $x' = \frac{6932927 - 6559328 + 1}{2} = 186800$ *e* $y' = \sqrt{(186800)^2 - 6932927} = 186781,44$ *dessa forma o teste falha, pois* $y' \notin \mathbb{N}$.

ii) *Para* $c_2 = \frac{5}{16}$, *temos* $d' = 16$ *e* $k' = 5$. *Assim* $\phi'(N) = \frac{2186443 \cdot 16 - 1}{5} = 6996617,4$, *logo* $x' = \frac{6932927 - 6996617,4 + 1}{2} = -31844,7$. *O teste falha, pois* $x' \notin \mathbb{N}$.

iii) *Para* $c_3 = \frac{6}{19}$, *temos* $d' = 19$ *e* $k' = 6$. *Assim* $\phi'(N) = \frac{2186443 \cdot 19 - 1}{6} = 6923736$, *logo* $x' = \frac{6932927 - 6923736 + 1}{2} = 4596$ *e* $y' = \sqrt{(4596)^2 - 6932927} = 3767$ *dessa forma o teste é válido, tendo em vista que* $x', y' \in \mathbb{N}$.

Sendo $x' = 4596$ *e* $y' = 3767$, *temos que* $p = x' - y' = 829$ *e* $q = x' + y' = 8363$. *Com isso a chave privada é dada por* $(829, 8363, 19)$.

Referências Bibliográficas

[1] ROSEN, Kenneth H. **Elementary Number Theory and Its Applications,** 6th ed. Pearson, 2011.

[2] BURTON, David M. **Elementary Number Theory**, 6th ed., Mc Graw Hill, New York, 2007.

[3] MOREIRA, Carlos Gustavo T. de A. **Frações Contínuas, Representações de Números e Aproximações Diofantinas**. 1º Coloquio da Região Sudeste. São João del-Rei, 2011.

[4] SANTOS, José Plínio de Oliveira. **Introducão à Teoria dos Números**. 3ed. Rio de Janeiro, RJ: IMPA, 2017.

[5] BARBEDO, Inês. **O Sistema Criptográfico RSA:** Ataques e Variantes, 2003.

[6] DUJELLA, Andrej. **Continued fractions and RSA with small secret exponent**, Tatra Mt. Math. Publ. 29 (2004).

[7] COUTINHO, S. C. **Números Inteiros e Criptografia RSA**, 2ed. Rio de Janeiro, RJ: IMPA, 2005.

[8] SMART, Nigel. **Cryptography:**An Introduction, McGraw-Hill, London, 2002.

[9] WIENER, M. J. **Cryptanalysis of short RSA secret exponents**, IEEE Trans. Inform. Theory 36 (1990), 553–558

[10] KAUFER, Aaron H. **Applications of Continued Fractions in Cryptography and Diophantine Equations**, 2009.

[11] LIMA, Elon Lages. **Análise Real, Vol. 1**, Instituto de Matemática Pura e Aplicada, Rio de Janeiro, 2006.