Universidade Federal de Mato Grosso
Instituto de Ciências Exatas e da Terra
Departamento de Matemática

Aplicações da função de Euler

Anderson Marcos Piffer
Mestrado Profissional em Matemática: PROFMAT/SBM/UFMT

Orientador: **Prof. Dr. Martinho da Costa Araújo**

Trabalho financiado pela Capes

Cuiabá - MT

Abril de 2014

Aplicações da função de Euler

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Anderson Marcos Piffer e aprovada pela comissão julgadora.

Cuiabá, 11 de Abril de 2014.

Prof. Dr. Martinho da Costa Araújo
Orientador

Banca examinadora:

Prof. Dr. Martinho da Costa Araújo (UFMT)
Prof. Dr. Eduardo Fávaro(UFMT)
Prof. Dr. José de Arimatéia Fernandes (UFCG)

Dissertação apresentada ao curso de Mestrado Profissional em Matemática - PROFMAT da Universidade Federal de Mato Grosso, como requisito parcial para obtenção do título **de Mestre em Matemática**.

Dados Internacionais de Catalogação na Fonte.

P627a Piffer, Anderson Marcos.
aplicações da função de Euler / Anderson Marcos Piffer. -- 2014
52 f. ; 30 cm.

Orientador: Martinho da Costa Araújo.
Dissertação (mestrado profissional) - Universidade Federal de Mato Grosso, Instituto de Ciências Exatas e da Terra, Programa de Pós-Graduação em Matemática, Cuiabá, 2014.
Inclui bibliografia.

1. Criptografia R.S.A. 2. Dízimas Periódicas. 3. função de Euller. I. Título.

Ficha catalográfica elaborada automaticamente de acordo com os dados fornecidos pelo(a) autor(a).

Dissertação de Mestrado defendida em 11 Abril de 2014 e aprovada pela banca examinadora composta pelos Professores Doutores

Prof. Dr. Martinho da Costa Araújo

Prof. Dr. Eduardo Fávaro

Prof. Dr. José de Arimatéia Fernandes

Agradeço a Deus, por ter me guiado até aqui, a minha família pelo apoio em todas as horas, a meu filho Angelo, pelo qual tudo faz sentido, aos professores,em especial meu orientador, professor Martinho por toda a paciência e aos amigos Wilson e Giseli por toda ajuda prestada.

Resumo

Atualmente existe uma lacuna a ser preenchida pelos acadêmicos de Licenciatura em Matemática: O abismo existente entre as metodologias inovadoras propostas em disciplinas vinculadas a área de Educação Matemática e o método tradicional com o qual se desenvolvem assuntos trabalhados em outras carreiras universitárias. Muitos destes alunos, que ao longo do Ensino Fundamental e Médio, não tiveram a oportunidade de lidar com a Matemática de maneira contextualizada, continuam carentes desta experiência no curso superior.

Mesmo teoricamente conscientes da necessidade de inovar, muitos destes estudantes, quando professores, acabam por reproduzir com seus alunos aquilo que vivenciaram ao longo de praticamente toda a sua formação acadêmica. Por outro lado, nem sempre é fácil para o professor universitário abordar temas de Álgebra abstrata, entre outros, de uma maneira que desperte o espírito investigativo do estudante. Há uma tendência, em nossa cultura acadêmica, em apresentar os teoremas seguidos de demonstrações, as quais não são suficientes para esclarecer as motivações subjacentes, nem as implicações dos resultados mencionados. Entendemos que é necessário atuar nos diversos níveis de escolaridade, com o objetivo de tornar o ensino e a aprendizagem da matemática mais indagador e voltado para a reflexão. Neste contexto, estamos pesquisando metodologias nas quais os alunos sejam levados a investigar a aplicabilidade de alguns destes conceitos matemáticos mencionadas fazem parte do curso de Licenciatura em matemática. Apresentaremos neste trabalho os resultados que obtivemos envolvendo a investigação sobre o número de algarismos do período de dízimas periódicas e o tema bastante atual da Criptografia RSA.

Palavras chave: Criptografia R.S.A.; Dízimas periódicas; Função de Euler

Abstract

Currently there is a gap to be filled by the students in Mathematics: The gulf between the proposed innovative methodologies in disciplines related area of mathematics education and the traditional method with which to develop subjects worked in other university courses. Many of these students, who throughout the elementary and high school, have not had the opportunity to deal with mathematics in context, remain deprived of this experience in college.

Even theoretically aware of the need to innovate, many of these students when teachers end up playing with your students what they experienced over virtually the entire academic training. On the other hand, is not always easy for the professor to address topics of abstract algebra, among others, in a way that arouses the investigative spirit of the student. There is a tendency in our academic culture, to present the theorems followed by statements, which are not sufficient to explain the underlying motivations, nor the implications of the results mentioned. We believe it is necessary to act at different levels of education, with the goal of making the teaching and learning of mathematics and more inquisitive facing reflection. In this context, we are researching methodologies in which students are led to investigate the applicability of some of these mentioned mathematical concepts are part of the Degree in temática. Apresentaremos this paper the results we obtained involving Research the number of digits of the period of regular tithes and very current theme of RSA encryption. **Keywords:** RSA encryption; regular tithes; function

de Euler.

Sumário

Introdução

Baseado na dificuldade de trabalharmos com os algoritmos algébricos presentes na teoria dos números surgiu a pesquisa de algumas aplicações para estas teorias, inicialmente trabalharemos com a criptografia R.S.A, pois é um tema bastante atual, útil e emprega vários teoremas. A curiosidade de descobrir algo é inerente a todos nós, seres humanos. Durante muito tempo, líderes necessitavam de algum tipo de comunicação para troca de mensagens e uma grande preocupação era a de como não deixar que o inimigo descobrisse o conteúdo destas mensagens. Foram estas ameaças que geraram o desenvolvimento de métodos para esconder tais mensagens, os denominados códigos e cifras. Os principais métodos usados atualmente para a proteção de informação foram elaborados por matemáticos com conhecimento militar. Apesar da criptografia ser de suma importância aos militares, hoje o sistema criptográfico é amplamente usado no mundo civil, podemos citar como exemplo as transações bancárias e a troca de informação via internet. Com o aumento do uso da informática e de variados sistemas de comunicação a partir da década de 60, criou-se uma grande procura do setor privado buscando na criptografia uma maneira de proteger a informação digitada e fornecer esta informação com segurança. A Criptografia RSA trabalha com algoritmos computacionais utilizando a chave pública, este código foi emitido em 1978 por Ron L. Rivestt, Ade Shamir e Ton Adleman. As letras RSA correspondem as iniciais dos nomes dos inventores do código. A segurança deste método consiste em obter os fatores primos d e de um número dado. O RSA explora bem isso ao utilizar um número que é produto de dois primos muito grande. Vários matemáticos desenvolveram alguns métodos de fatoração a fim de descobrir estes dois números, quebrando para que pudessem quebrar a segurança do RSA, porém todos estes métodos foram em vão, tendo em vista que mesmo os recursos computacionais como os métodos de fatoração, se aumentarmos o número de dígitos da chave n, qualquer um dstes métodos seriam incapazes de descobri-la. A engenhosidade destes matemáticos pro-

duziu resultados relevantes ao estudo de fatoração, porém, como dito antes, nenhum deles é considerado satisfatório para ser executado em tempo hábil, portanto o tamanho do número deve ser suficientemente grande para garantir a segurança do RSA. O algoritmo RSA foi patenteado em 1983 nos Estados Unidos e atualmente é o mais utilizado nas transações comerciais. No que se refere às dízimas, surgiu a curiosidade de identificar o comportamento de sua expansão decimal usando as bases matemáticas da teoria dos números, para isto desejamos identificar a parte não periódica e a quantidade de algarismos da parte periódica, bem como a sua composição. Isto parece uma tarefa fácil e realmente é, quando tratamos de expansões relativamente pequenas, facilidade esta que não ocorrerá em alguns casos. Perguntas do tipo: Quando a expansão decimal de uma fração é finita? E nos casos em que esta expansão é infinita, qual o seu comportamento? Tais comportamentos deverão ser esclarecidos após a apresentação de alguns teoremas.
Para auxiliar nossos estudos, usamos algumas obras que trata destes assuntos, podemos citar aqui: [Coutinho, 2011] ; [Iezzi, 2004] ; [Lima, 2006a] ; [Lima, 2006b] [Lima, 1987] ; [Roosevelt] ; [Carneiro, 2003] ; [Hygino, 2003] ; [alvares, 2004] ; [Santos, 2011].

Capítulo 1

Bases Matemáticas

Para o estudo definiremos aqui $\mathbb{N} = \{1, 2, 3, 4, ...\}$

1.1 Divisibilidade

Dado dois números naturais a e b, com $a \neq 0$ dizemos que a divide b e denotamos por $a \mid b$ quando existir um $c \in \mathbb{N}$ tal que $b = a.c$. Neste caso dizemos que a ou é um divisor ou um fator de b, ou ainda que b é múltiplo de a.

Propriedades

1. Sejam a e $b \in \mathbb{N}^*$ e c pertencente a $\mathbb{N}$ temos:

   a) $1 \mid c$, $a \mid a$ e $a \mid 0$

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

2. Sejam $a, b, c, d \in \mathbb{N}$ com a e c diferentes de 0, se $a \mid b$ e $c \mid d$, então $a.c \mid b.d$

3. Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$, tais que $a \mid (b + c)$, Então $a \mid b$ se e somente se $a \mid c$.

4. Dados $a, b \in \mathbb{N}^*$, se $a \mid b$, então, $b \geq a$.

5. Sejam $a, b, n \in \mathbb{N}$, com $(a+b) \neq 0$, então $(a+b) \mid a^{2n+1} + b^{2n+1}$.

6. Sejam $a, b, n \in \mathbb{N}$, com $a \geq b > 0$, então $(a-b) \mid a^{2n} - b^{2n}$.

7. Sejam $a, b, c \in \mathbb{N}$, com $a \neq 0$ e $b \geq c$, tais que $a \mid (b-c)$, então $a \mid b$ se e somente se $a \mid c$.

   Demostrações em [Hefez, 2011]

1.2 Números primos

Um número natural maior do que 1 e que só é divisível por 1 e por ele mesmo é chamado de número primo. Caso, além disso, este número seja divisível por qualquer outro valor, ele será chamado de número composto. Indicaremos por $D(x)$ o conjunto dos divisores naturais do número x e $mdc(a, b)$ o máximo divisor comum entre a e b.

Exemplo 1.1 *:*
D (7) = { 1 , 7 } , logo 7 é primo
D (8) = { 1, 2, 4, 8 } , logo 8 é composto

Dados dois números primos m e n e um número qualquer a, decorre da definição acima os seguintes fatos:

1. Se $m \mid n$, então $m = n$

   Dem: Se $m \mid n$ e m e n são primos, então $n = 1$ ou $n = m$, mas como pela definição, todo número primo deve ser maior que 1, então que $m = n$.

2. Se m não divide a, então m e a são primos entre si, ou seja, $(m, a) = 1$

   Dem: se (m, a) = x, então $x \mid m$ e $x \mid a$, portanto $x = m$ ou $x = 1$, mas de fato $m \neq x$, já que m não divide a, logo $x = 1$.

1.3 A função ϕ de Euler

Seja $\mathbb{N} = \{1, 2, 3, 4, ...\}$, definimos como função ϕ de Euler o número de elementos do conjunto: $\{\ k \in \mathbb{N}\ \ /\ \ 1 \leq k \leq n\ \ \text{e}\ \ mdc(k, n) = 1\}$ com $n \in \mathbb{N}$.
Sendo assim indicaremos a função ϕ de Euler como:

$\phi(\text{n}) = |\{\ k \in \mathbb{N}\ \ /\ \ 1 \leq k \leq n\ \ \text{e}\ \ mdc(k, n) = 1\}\ |$

Eis seus primeiros valores:

n	1	2	3	4	5	6	7	8	9	10
$\phi(n)$	1	1	2	2	4	2	6	4	6	4

$\phi(1) = 1$, pois o único inteiro positivo menor ou igual a 1 é o próprio 1 e ainda se verifica $mdc(1, 1) = 1$. Agora, para qualquer $n \geq 2$, temos $n = mdc(n, n) \neq 1$, de forma que, a princípio, $\phi(n) < n$.

Exemplo 1.2 *:*
Calcular ϕ(9).
Vejamos o conjunto a seguir:

$$\{x \in \mathbb{N}/1 \leq x \leq 9\ e\ \ mdc(x, 9) = 1\ \} = \{1,\ 2,\ 4,\ 5,\ 7,\ 8\}$$

Note que o conjunto possui 6 *elementos.*
Logo, ϕ(9) = 6.

Este processo de montar o conjunto ϕ para um certo n e contar seu número de elementos é fácil apenas se este n for relativamente pequeno. Esta tarefa torna-se complicada com, por exemplo $n = 12960$.

Mas se n for primo, $\phi(n)$ simplesmente $= n - 1$, tendo em vista que todos os inteiros positivos menores que n são primos relativos com n.
Vejam na tabela que $\phi(2)$=1, $\phi(3)$=2, $\phi(5)$=4, $\phi(7)$=6.

A questão principal é a seguinte: Sendo n um inteiro positivo qualquer, como calcular $\phi(n)$? Podemos utilizar, então, a importante propriedade de que a função ϕ de Euler é uma função aritmética multiplicatica, ou seja, se a e b são inteiros positivos tais que $mdc(a, b) = 1$, então:
$\phi(ab)=\phi(a)\phi(b)$ Este fato não é evidente e precisa ser demonstrado. Para isto, nos apoiaremos no seguinte teorema auxiliar.

Lema 1.3.1 *:*
Dados os inteiros positivos k, a e b, com $mdc(a, b) = 1$, então os restos das divisões dos a inteiros k, $k + b$, $k + 2b$, ..., $k + (a - 1)b$ por a, são todos diferentes.

Demonstração: 1 *:*

Seja a desigualdade $0 \leq s, t < a$. Suponhamos, por absurdo, que $k+sb$ e $k+tb$ deixem o mesmo resto na divisão por a. Assim, $k+sb = aq+r$ e $k+tb = aq^{'}+r$. Então, que a divide o produto $(s-t)b$, pois

$$(k+sb)-(k+tb) = (aq+r)-(aq^{'}+r) \Rightarrow (s-t)b = a(q-q^{'}) \Rightarrow q-q^{'} = \frac{(s-t)b}{a}$$

Mas por hipótese, $mdc(a, b) = 1$, logo, a divide $(s-t)$, o que é impossível porque foi imposto que $0 \leq s, t < a$.

Concluímos, então, que os restos são todos diferentes.

Teorema 1.3.2 *:*

A função ϕ de Euler é uma função aritmética multiplicativa.

Demonstração: 2 *:*

O que queremos provar é que $\phi(ab) = \phi(a)\phi(b)$, desde que $mdc(a, b) = 1$.
Isto é:

Se $a = 1$ ou $b = 1$, o teorema é válido, pois $\phi(1.b) = \phi(b) = 1.\phi(b) = \phi(a).\phi(b)$ ou
$\phi(a.1) = \phi(a) = \phi(a).1 = \phi(a).\phi(b)$ ou
$\phi(1.1) = 1 = \phi(1).\phi(1)$. Sejam, então $a > 1$ e $b > 1$. Vamos agora dispor todos os inteiros 1,2,...,*ab em a linhas e b colunas, para daí tirar algumas conclusões.*

$0b+1$	$0b+2$	....	$0b+k$	.....	$1b$
$1b+1$	$1b+2$	....	$1b+k$	.....	$2b$
$2b+1$	$2b+2$	....	$2b+k$	.....	$3b$
.....	.....	....	.....	.....	.....
$(a-1)b+1$	$(a-1)b+1$	....	$(a-1)b+k$	.....	ab

Os inteiros da k-ésima coluna serão primos com b apenas se k for primo com b,pois, de modo inverso, b divide $q.b+k$, apenas se k for múltiplo de b.

Na primeira linha temos $\phi(b)$ inteiros que são primos com b. Assim, temos $\phi(b)$ colunas onde todos os inteiros são primos com b.

Suponhamos que a k-ésima coluna seja uma destas $\phi(b)$ colunas. Pelo lema 1.3.1*, os restos das divisões dos a inteiros desta coluna por a são* 1,2,...,$a-1$. *Logo, o número de inteiros da k-ésima coluna que são primos com a é $\phi(a)$.*

Portanto, em cada coluna (em um total de $\phi(b)$) de inteiros onde todos são primos com b, vamos ter $\phi(a)$ inteiros que são primos com a.

Logo, o número de inteiros da matriz acima, que são primos com a e b é $\phi(a).\phi(b)$. É claro que todo número que não tem fatores primos com a e b também não terão com o produto ab. Assim, $\phi(a).\phi(b)$ também é a quantidade de inteiros positivos menores que e primos com ab.
Conclusão: $\phi(ab)=\phi(a)\phi(b)$.

Assim temos a seguinte generalização:
Se os inteiros positivos $a,b,c,...,z$ são primos entre si, dois a dois, então:
$\phi(abc...z)=\phi(a).\phi(b).\phi(c)...\phi(z)$
Já sabemos que se $n = p$ é primo, então $\phi(\mathrm{p})=p-1$. Dado $\alpha \in \mathbb{N}$, com $\alpha \geq 1$, vamos demonstrar agora a fórmula para calcular $\phi(p^{\alpha})$.

Teorema 1.3.3 *:*

$\phi(p^\alpha)=p^\alpha$ - $p^{\alpha-1}$

Demonstração: 3 *:*

Os inteiros menores que p^α *e que são primos com* p^α *são, obviamente, aqueles números que não possuem o fator primo p. Os que possuem são da forma p,* $2p$*,...,*tp*, onde*

$$tp = p^\alpha \Rightarrow t = p^{\alpha-1}$$

Logo, se t indica a quantidade de inteiros menores que p^α *que não são primos com* p^α*, então a quantidade de inteiros que são menores que e primos com* p^α *são exatamente* p^α - $p^{\alpha-1}$*. Assim,* $\phi(p^\alpha)=p^\alpha$ - $p^{\alpha-1}$*.*

Agora, com a propriedade multiplicativa da função de Euler em conexão com o teorema anterior, estamos em condições de calcular $\phi\ (n)$ para qualque inteiro positivo n. Vejamos:

Exemplo 1.3 *:*

Calcular $\phi(5625000)$*.*

Primeiro passo. Fatorar $n = 5625000$*, ou seja* $n = 2^3.3^2.5^7$*.*

Segundo Passo. Calcular $\phi(p^\alpha)=p^\alpha$ - $p^{\alpha-1}$ *para cada potência da fatoração.*

$\phi(2^3)=2^3 - 2^2 = 8 - 4 = 4$

$\phi(3^2)=3^2 - 3^1 = 9 - 3 = 6$

$\phi(5^7)=5^7 - 5^6 = 78125 - 15625 = 62500$

Terceiro Passo: Aplica-se a propriedade multiplicativa de $\phi(n)$*.*

Assim temos:

$\phi(5625000)=\phi(2^3.3^2.5^7)=\phi(2^3).\phi(3^2).\phi(5^7)=4.6.62500 = 1500000$

Ou seja, existem 1500000 *inteiros positivos que são menores que e primos com* 5625000*.*

1.4 O pequeno teorema de Fermat

Teorema 1.4.1 *:*

Seja p um número primo e a pertencente aos inteiros, de modo que $mdc(p, a) = 1$ *Se p não divide a então* $a^{p-1} \equiv 1 \ mod \ p$.

Demonstração: 4 *:*

Seja o conjunto de valores a, $2a$, $3a$ *,...,* $(p-1)a$. *Sabemos que, pelo fato de que p não divide a e* $mdc(a, p) = 1$ *e, portanto, nenhum dos números deste conjunto é divisível por p. Além disso, se* $aj \equiv ak \ mod \ p$, *então* $j \equiv k \ mod \ p$, *ou seja, todos eles são congruentes módulo p e, portanto, podemos estabelecer uma relação biunívoca entre os* aj, $j = 1, 2, ..., p-1$ *e o conjunto* $1, 2, 3, ..., (p-1)$, *em termos de congruência, isto é, cada um dos termos do primeiro conjunto é congruente a um diferente do segundo.*
$a(2a)(3a)...(p-1)a \equiv 1.2.3...(p-1) \ mod \ p$
ou seja $a^{p-1}(p-1)! \equiv (p-1)! \ mod \ p$. *Da lei do cancelamento,*
e do fato de que $mdc((p-1)!, p) = 1$, *segue que*
$a^{p-1} \equiv 1 \ mod \ p$

Corolário 1 *:*

Se p é um número primo e a é um inteiro positivo,tal que $mdc(a, p) = 1$, *então,* $a^p \equiv a \ mod \ p$
Para esta situação existem duas conclusões:

1. *Se* $p \mid a$, *então* $p \mid a(a^{p-1} - 1)$, *ou seja,* $p \mid a^p - a$, *e portanto* $a^p \equiv a \ mod \ p$

2. *Se p não divide a , então pelo Pequeno Teorema de Fermat,* $a^{p-1} \equiv 1 \ mod \ p$, *daí multiplicando a congruência por a, temos:*
   $a^p \equiv a \ mod \ p$.

1.5 Teorema de Euler

O teorema de Euler visa generalizar o Pequeno Teorema de Fermat para quaisquer números inteiros, utilizando para isso a função ϕ de Euler. É interessante notar que para um número primo, o Teorema de Euler é exatamente o Pequeno Teorema de Fermat.

Teorema 1.5.1 *:*
Se m é um inteiro positivo e a é um inteiro com $mdc(a, m) = 1$, então $a^{\phi(m)} \equiv 1 \ mod \ m$.

Demonstração: 5 *:*

Para demonstrar o Teorema de Euler, vamos seguir o mesmo roteiro do Pequeno Teorema de Fermat. Primeiramente, se r_1, r_2, ... , $r_{\phi(m)}$ são todos os restos não-nulos possíveis na divisão por m, então ar_1, ar_2, ... , $ar_{\phi(m)}$ também são, com $mdc(a, m) = 1$. Ou seja, podemos fazer uma relação biunívoca entre os dois conjuntos, em congruência, e daí chegamos em:

$$ar_1.ar_2....ar_{\phi(m)} \equiv r_1.r_2....r_{\phi(m)} \ mod \ m$$

ou seja:

$a^{\phi(m)}.r_1.r_2...r_{\phi(m)} = r_1.r_2...r_{\phi(m)} \ mod \ m$

Aplicando o cancelamento temos:

$a^{\phi(m)} \equiv 1 \ mod \ m$

1.6 Teorema Fundamental da Aritmética

Dado um número $n > 1$, existem primos $p_1 < p_2 < ... < p_n \in \mathbb{N}^*$ univocadamente determinados tais que:

$$N = p_1^{a_1}.p_2^{a_2}.....p_n^{a_n}$$

1.7 Congruências Lineares

Sejam $a, b, n \in \mathbb{Z}$ com $n > 1$, dizemos que a é congruente a b módulo n, se $n \mid (a - b)$, neste caso por:
$a \equiv b \; mod \; n$

Propriedades

1. Reflexiva: $a \equiv a \; mod \; n$,
2. Simétrica: se $a \equiv b \; mod \; n$, então $b \equiv a \; mod \; n$,
3. Transitiva: Se $a \equiv b \; mod \; n$ e $b \equiv c \; mod \; n$, então $a \equiv c \; mod \; n$,
4. Se $a \equiv b \; mod \; n$ e $c \equiv d \; mod \; n$ então $(a + c) \equiv (b + d) \; mod \; n$ e $(a.c) \equiv (b + d) \; mod \; n$.

Capítulo 2

Descrição da Criptografia RSA

Para ajudar no entendimento do método, mostraremos inicialmente as regras e paralelamente decodificaremos a palavra PROFMAT. O método RSA é constituído de 3 etapas: Pré-codificação, codificação e decodificação que serão explicadas cada uma a seguir:

2.1 Pré-codificação

Inicialmente devemos considerar o nosso alfabeto representado por númeors inteiros, conforme a tabela a seguir:

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

No caso da mensagem ser formado por frases, o espaço entre duas palavras será substituído pelo numero 99. Desta forma a pré-codificação da palavra PROFMAT é:

25272415221029

Note que o motivo de fazer cada letra corresponder a um número de dois algarismos é que evita-se a ambigüidade. De fato, observe que se fizéssemos A corresponder a 1, B corresponder a 2 e assim por diante, então o número 12 por exemplo, poderia ser

interpretado como AB ou como a letra L, que é a décima segunda letra do alfabeto. Assim não conseguiríamos decidir qual é a escolha correta. Antes de continuar precisamos determinar os parâmetros do sistema RSA que usaremos. Estes parâmetros são dois números primos distintos que denotamos por P e Q onde $N = P.Q$

A titulo de ilustração escolheremos os parâmetros $P = 5$ e $Q = 11$ e conseqüentemente $N = 55$.

A última etapa do processo de pré codificação consiste em quebrar o número produzido na primeira etapa em blocos menores, onde cada bloco gerado deverá ser inferior a N, neste caso, a mensagem cujo conversão numérica foi feita anteriormente pode ser quebrado nos seguintes blocos:

$$25 - 27 - 24 - 15 - 22 - 10 - 29.$$

2.2 Critérios de escolha dos primos P e Q

É fato que os primos P e Q são de livre escolha, porém a questão de segurança do sistema RSA depende muito destas escolhas, é claro que se eles forem muitos pequenos, a mensagem será facilmente descoberta, mas não basta escolhermos P e Q grandes. Deste modo se P e Q forem grandes, mas $|P - Q|$ é pequeno, então é fácil fatorar $N = P.Q$.

Vejamos alguns exemplos:

Exemplo 2.1 *:*
Tomamos n=12987, vamos tentar determinar P e Q primos, tais que P.Q = 12987. Inicialmente tomamos x como parte inteira de $\sqrt{n}$, logo:

$$\sqrt{12987} \cong 113,96 \Rightarrow x^2 = 113^2 \Rightarrow x^2 = 12769 < 12987$$

No próximo passo adicionamos uma unidade por vez ao x, até que $\sqrt{x^2 - n}$ seja inteiro, ou x seja igual a $\dfrac{(n+1)}{2}$, vejamos a tabela abaixo:

x	$y = \sqrt{x^2 - n}$
114	$y = 3$

Portanto $x = 114$ *e* $y = 3$*, logo os valores de* P *e* Q *correspondente são dado por:*

$x + y = 114 + 3 = 117$

$x - y = 114 - 3 = 111$

Logo $P = 117$ *e* $Q = 111$

Exemplo 2.2 *:*

Tomamos agora $N = 1342127$*. Assim:*

$x^2 = 1158^2 = 1340964 < 1342127$.

Vamos aos testes:

x	$y = \sqrt{x^2 - n}$
159	$y = \sqrt{1159^2 - 1342127} \notin \mathbb{N}$
160	$y = \sqrt{1160^2 - 1342127} \notin \mathbb{N}$
161	$y = \sqrt{1611^2 - 1342127} \notin \mathbb{N}$
162	$y = \sqrt{1621^2 - 1342127} \notin \mathbb{N}$
163	$y = \sqrt{1163^2 - 1342127} \notin \mathbb{N}$
164	$y = \sqrt{1164^2 - 1342127}$ $y = 113$

Assim $x = 1164$ *e* $y = 113$

Logo $P = x + y = 1664 + 113 = 1227$ *e*

$Q = x - y = 1164 - 113 = 1051$

Note que no último exemplo temos $|P - Q| > |P - Q|$ do primeiro exemplo, por isso se torna mais difícil determinar P e Q. O método descrito nos exemplos acima é conhecido como algoritmo de Fermat e está devidamente demonstrado em [Coutinho, 2011]. A maneira de quebrar os blocos não é única, porém alguns cuidados devem ser tomados. É necessário que se evite que o bloco se inicie com zero, pois isto acarretaria em problemas na hora de decodificar .

Assim a etapa de pré-codificação está concluída .

2.3 Etapa codificadora

Para fazer a codificação usamos a função Φ de Euler e como $\phi(n) = (n - 1)$ e se n é primo e ainda esta é uma função multiplicativa temos: Para $n = 55$:

$\phi(55) = \phi(5).\phi(11) = (5 - 1).(11 - 1) = 4.10 = 40$

Para codificar a mensagem, usamos uma chave codificadora (n, e), onde n já foi previamente escolhido na etapa de pré-codificação e o valor e precisa seguir os parâmetros. $mdc(e, \phi(n)) = 1$ e $1 < e < \phi(n)$.
Neste caso podemos escolher $e = 3$ $mdc(3, 40) = 1$ e $1 < 3 < 40$.

Usando os valores de n e e, cada bloco b obtido na etapa de pré-codificação é transformado num bloco $C(b)$, onde $C(b)$ é igual ao resto da divisão de b^e por n. Usando as relações de congruência temos:

$$C(b) : b^e \equiv \text{x mod n},$$

onde $b \in \{25, 27, 24, 15, 22, 10, 29\}$

Voltando ao nosso exemplo da palavra PROFMAT, vamos codificar cada bloco $C(b)$:

$$C(25) : 25^3 \equiv \text{x } mod\ 55 \equiv 5\ mod\ 55, \text{ logo x=5}$$
$$C(27) : 27^3 \equiv \text{x } mod\ 55 \equiv 48\ mod\ 55, \text{ logo x=48}$$
$$C(24) : 24^3 \equiv \text{x } mod\ 55 \equiv 19\ mod\ 55, \text{ logo x=19}$$
$$C(15) : 15^3 \equiv \text{x } mod\ 55 \equiv 20\ mod\ 55, \text{ logo x=20}$$
$$C(22) : 22^3 \equiv \text{x } mod\ 55 \equiv 33\ mod\ 55, \text{ logo x=33}$$
$$C(10) : 10^3 \equiv \text{x } mod 55 \equiv 10\ mod\ 55, \text{ logo x=10}$$
$$C(29) : 29^3 \equiv \text{x } mod\ 55 \equiv 24\ mod\ 55, \text{ logo x=24}$$

Assim temos a mensagem codificada:

$$5 - 48 - 19 - 20 - 33 - 10 - 24$$

2.4 Decodificação

Para decodificar um bloco, precisamos calcular dois números: n e o inverso de e que vamos denotar por d. O par (n, d) é chamado de chave de decodificação, onde d é calculado pela relação de congruência a seguir:
$e.d \equiv 1\ mod\ \phi(n)$.

Seja a um bloco de mensagem codificada, então D(a) será a decodificação deste bloco. O modo de acharmos $D(a)$ é dado por: $D(a)$ é igual ao resto da divisão de a^d por n

Assim, usando as notações de congruência, temos:

$$D(a) = a^d \equiv \text{x } mod \text{ n}$$

Voltando ao exemplo PROFMAT, Vamos fazer a decodificação.

Inicialmente vamos achar o valor da chave d.

$ed \equiv 1 \ mod \ \phi(n)$

$3d \equiv 1 \ mod \ 40$

$3d - 1 \equiv 0 \ mod \ 40$

$40|3d - 40$ logo $d = 27$.

Em seguida vamos decodificar cada bloco , lembrando que a mensagem codificada foi:

$$5 - 48 - 19 - 20 - 33 - 10 - 24$$

$D(5)$

$D(5) = 5^{27} \equiv \text{x } mod \ 55 \Rightarrow 125^9 \equiv \text{x } mod \ 55 \Rightarrow 15^9 \equiv \text{x } mod \ 55 \Rightarrow 15.(15^2)^4 \equiv \text{x } mod \ 55$

$15.(225)^4 \equiv \text{x } mod \ 55 \Rightarrow 15.5^4 \equiv \text{x } mod \ 55 \Rightarrow 15.625 \equiv \text{x } mod \ 55 \Rightarrow 15.20 \equiv \text{x } mod \ 55$

$300 \equiv \text{x } mod \ 55$

Logo $x = 25$

$D(48)$

$D(48) = 48^{27} \equiv \text{x } mod \ 55$

$48^{27} \equiv \text{x } mod \ 5 \Rightarrow 3^{27} \equiv \text{x } mod \ 5 \Rightarrow 3^4 \equiv 1 \ mod \ 5 \Rightarrow (3^4)^6.3^3 \equiv 1^3.3^3 \ mod \ 5$

$3^{27} \equiv 27 \ mod \ 5 \Rightarrow 3^{27} \equiv 2 \ mod \ 5 \Rightarrow 48^{27} \equiv 2 \ mod \ 5$

$48^{27} \equiv \text{x } mod \ 11 \Rightarrow 4^{27} \equiv \text{x } mod \ 11 \Rightarrow 4^{10} \equiv 1 \ mod \ 11 \Rightarrow (4^{10})^2.4^7 \equiv 1^2.4^7 \ mod \ 11$

$4^{27} \equiv 4^2.4^2.4^2.4 \ mod \ 11 \Rightarrow 4^{27} \equiv 5.5.5.4 \ mod \ 11 \Rightarrow 4^{27} \equiv 500 \ mod \ 11$

$4^{27} \equiv 5 \ mod \ 11 \Rightarrow 48^{27} \equiv 5 \ mod \ 11$

Assim basta resolvermos o sistema:

$$\begin{cases} x \equiv 2 \quad mod \ 5 \\ x \equiv 5 \quad mod \ 11 \end{cases}$$

Resolvendo o sistema temos:

$$x = 27$$

$D(19)$

$D(19) = 19^{27} \equiv \text{x} \ mod \ 55 \Rightarrow 19.(19^2)^{13} \equiv \text{x} \ mod \ 55 \Rightarrow 19.361^{13} \equiv \text{x} \ mod \ 55$

$19.31^{13} \equiv \text{x} \ mod \ 55 \Rightarrow 19.31.(31^2) \equiv \text{x} \ mod \ 55 \rightarrow 589.961^6 \equiv \text{x} \ mod \ 55$

$589.26^6 \equiv \text{x} \ mod \ 55 \Rightarrow 39.(26^2)^3 \equiv \text{x} \ mod \ 55 \Rightarrow 39.676^3 \equiv \text{x} \ mod \ 55$

$39.16^3 \equiv \text{x} \ mod \ 55 \rightarrow 39.26 \equiv \text{x} \ mod \ 55 \Rightarrow 1014 \equiv \text{x} \ mod \ 55$

Logo $x = 24$

$D(20)$

$D(20) = 20^{27} \equiv \text{x} \ mod \ 55$

$20^{27} \equiv \text{x} \ mod \ 5 \Rightarrow 20^{27} \equiv 0 \ mod \ 5$

$20^{27} \equiv \text{x} \ mod \ 11 \Rightarrow 9^{27} \equiv \text{x} \ mod \ 11 \Rightarrow 9^{10} \equiv 1 \ mod \ 11 \Rightarrow (9^{10})^2.9^7 \equiv 1^2.9^7 \ mod \ 11$

$9^{27} \equiv 9^2.9^2.9^2.9 \ mod \ 11 \Rightarrow 9^{27} \equiv 4.4.4.9 \ mod \ 11 \Rightarrow 9^{27} \equiv 576 \ mod \ 11$

$9^{27} \equiv 4 \ mod \ 11 \Rightarrow 20^{27} \equiv 4 \ mod \ 11$

$$\begin{cases} x \equiv 0 \quad mod \ 5 \\ x \equiv 4 \quad mod \ 11 \end{cases}$$

Resolvendo o sistema temos:

Logo $x = 15$

$D(33)$

$D(33) = 33^{27} \equiv \text{x} \ mod \ 55$

$33^{27} \equiv \text{x } mod\ 5 \Rightarrow 3^4 \equiv 1\ mod\ 5 \Rightarrow (3^4)^6.3^3 \equiv 3^3\ mod\ 5 \Rightarrow 3^{27} \equiv 27\ mod\ 5$

$3^{27} \equiv 2\ mod\ 5 \Rightarrow 33^{27} \equiv 2\ mod\ 5$

$33^{27} \equiv \text{x } mod\ 11 \Rightarrow 33 \equiv 0\ mod\ 11 \Rightarrow 33^7 \equiv 0\ mod\ 11$

Agora basta resolvermos o sistema a seguir:

$$\begin{cases} x \equiv 2 \quad mod\ 5 \\ x \equiv 0 \quad mod\ 11 \end{cases}$$

Resolvendo o sistema temos:

$$x = 22$$

$D(10)$

$D(10) = 10^{27} \equiv \text{x } mod\ 55$

$10^{27} \equiv \text{x } mod\ 5 \Rightarrow 10 \equiv 0\ mod\ 5 \Rightarrow 10^{27} \equiv 0\ mod\ 5 \Rightarrow x \equiv 0\ mod\ 5$

$x \equiv 10\ mod\ 11 \Rightarrow 10^{27} \equiv \text{x } mod\ 11 \Rightarrow 10^{10} \equiv 1\ mod\ 11 \Rightarrow 10^7.(10^{10})^2 \equiv 10^7\ mod\ 11$

$10^{27} \equiv 10^2.10^2.10^2.10\ mod\ 11$

$10^{27} \equiv 1.1.1.10\ mod\ 11$

$10^{27} \equiv 10\ mod\ 11$

Agora basta resolvermos o sistema a seguir:

$$\begin{cases} x \equiv 0 \quad mod\ 5 \\ x \equiv 10 \quad mod\ 11 \end{cases}$$

Resolvendo o sistema temos:

$$x = 10$$

$D(24)$

$D(24) = 24^{27} \equiv \text{x } mod\ 55$

$24^{27} \equiv \text{x } mod\ 5 \Rightarrow 4^{27} \equiv \text{x } mod\ 5 \Rightarrow 4^4 \equiv 1\ mod\ 5$

$(4^4)^6.4^3 \equiv 4^3\ mod\ 5 \Rightarrow 4^{27} \equiv 64\ mod\ 5 \Rightarrow 24^{27} \equiv 4\ mod\ 5$

$24^{27} \equiv \text{x } mod\ 11 \Rightarrow 2^{27} \equiv \text{x } mod\ 11 \Rightarrow 2^{10} \equiv 1\ mod\ 11$

$(2^{10})^2.2^7 \equiv 2^7\ mod\ 11 \Rightarrow 2^{27} \equiv 128\ mod\ 11 \rightarrow 24^{27} \equiv 7\ mod\ 11$

$$\begin{cases} x \equiv 4 \mod 5 \\ x \equiv 7 \mod 11 \end{cases}$$

Resolvendo o sistema temos:

$$x = 29$$

Assim temos:

$$D(5)D(48)D(19)D(20)D(33)D(10)D(24)$$
$$25272415221029.$$

Quebrando o bloco em dois dígitos temos:

$$25 - 27 - 24 - 15 - 22 - 10 - 29$$

que é a mensagem inicial: PROFMAT

Vejamos outro exemplo:

Exemplo 2.3 *:*

Descreva as três etapas da criptografia RSA com a palavra arco-íris.

Tomamos como referência a palavra ARCO IRIS e usando a tabela dada anteriormente, temos:

102712249918271828

Escolhendo P *e* Q *como* 11 *e* 17 *temos:*

$N = P.Q \Rightarrow N = 11.17 \Rightarrow n = 187$

Quebrando a sequência numérica em blocos menores do que 187, temos a seguinte pré-codificação:

$$102 - 71 - 2 - 24 - 9 - 91 - 82 - 7 - 182 - 8$$

Agora iniciando o processo de codificação temos: $\phi(n) = \phi(11.17) = \phi(11).\phi(17) = (11-1).(17-1) = 10.16 = 160$

Escolhendo um e, tal que $mdc(e, \phi(187)) = 1$ *Como* $\phi(187) = 160$ *e* $(3, 160) = 1$ *podemos*

escolher $e = 3$.

Desta forma temos:

$$C(102) : 102^3 \equiv x \ mod \ 187, \ logo \ x = 170$$

$C(71) : 71^3 \equiv x \ mod \ 187, \ logo \ x = 180$

$C(2) : 2^3 \equiv x \ mod \ 187, \ logo \ x = 8$

$C(24) : 24^3 \equiv x \ mod \ 187, \ logo \ x = 173$

$C(9) : 9^3 \equiv x \ mod \ 187, \ logo \ x = 168$

$C(91) : 91^3 \equiv x \ mod \ 187, \ logo \ x = 148$

$C(82) : 82^3 \equiv x \ mod \ 187, \ logo \ x = 92$

$C(7) : 7^3 \equiv x \ mod \ 187, \ logo \ x = 156$

$C(182) : 182^3 \equiv x \ mod \ 187, \ logo \ x = 62$

$C(8) : 8^3 \equiv x \ mod \ 187, \ logo \ x = 138$

Assim a mensagem codificada é:

$$170 - 180 - 8 - 173 - 168 - 148 - 92 - 156 - 62 - 138$$

Para iniciar a decodificação temos que determinar o parâmetro d de tal modo que: $ed \equiv 1 \ mod \ \phi(n)$.

$3d \equiv 1 \ mod \ 160$

$3d - 1 \equiv 0 \ mod \ 160$, *ou seja:*

$160|3d - 1$, *logo d=104, pois 3.107-1= 320 e* $160|320$ *em seguida vamos decodificar cada bloco:*

$170 - 180 - 8 - 173 - 168 - 148 - 92 - 156 - 62 - 138$

$D(170)$

$D(170) = 170^{170} \equiv x \ mod \ 187$

$170^{107} \equiv x \ mod \ 11 \Rightarrow 5^{107} \equiv x \ mod \ 11 \Rightarrow 5^{10} \equiv 1 \ mod \ 11$

$(5^{10})^{10}.5^7 \equiv 5^7 \ mod \ 11 \Rightarrow 5^{107} \equiv 5^2.5^2.5^2.5 \ mod \ 11 \Rightarrow 5^{107} \equiv 3.3.3.5 \ mod \ 11$

$5^{107} \equiv 3 \ mod \ 11 \rightarrow 170^{107} \equiv 3 \ mod \ 11$

$170^{107} \equiv x \ mod \ 17 \rightarrow 170 \equiv 0 \ mod \ 17 \Rightarrow 170^{107} \equiv 0 \ mod \ 17$

No sistema temos:

$$\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 0 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 102$

$D(180)$

$D(180) = 180^{107} \equiv x \ mod \ 187$

$180^{107} \equiv x \ mod \ 11 \Rightarrow 4^{107} \equiv x \ mod \ 11 \Rightarrow 4^{107} \equiv 1 \ mod \ 11$

$4^{107} \equiv 4^{7} mod \ 11 \Rightarrow 4^{107} \equiv 4^2.4^2.4^2.4 \ mod \ 11 \Rightarrow 4^{107} \equiv 5.5.5.4 \ mod \ 11$

$4^{107} \equiv 5 \ mod \ 11 \Rightarrow 180^{107} \equiv 5 \ mod \ 11$

$180^{107} \equiv x \ mod \ 17 \Rightarrow 10^{107} \equiv x \ mod \ 17 \rightarrow 10^{107} \equiv x \ mod \ 17$

$10^{16} \equiv 1 \ mod \ 17 \Rightarrow (10^{10})^6.10^{11} \equiv 10^{11} \ mod \ 17 \Rightarrow 10^{107} \equiv 10.((10)^2)^5 \ mod \ 17$

$10^{107} \equiv 10.100^5 \ mod \ 17 \Rightarrow 10^{107} \equiv 10.15^5 \ mod \ 17 \Rightarrow 10^{107} \equiv 10.15.(15^2)^2 \ mod \ 17$

$10^{107} \equiv 150.225^2 \ mod \ 17 \Rightarrow 10^{107} \equiv 14.4^2 \ mod \ 17 \Rightarrow 10^{107} \equiv 224 \ mod \ 17$

$10^{107} \equiv 3 \ mod \ 17 \equiv 108^{107} \equiv 3 \ mod \ 17$

Assim:

$$\begin{cases} x \equiv 5 \mod 11 \\ x \equiv 3 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 71$

$D(8)$

$D(8) = 8^{107} \equiv 187$

$8^{107} \equiv x \ mod \ 11 \Rightarrow 8^{107} \equiv 1 \ mod \ 11 \Rightarrow 8^{107} \equiv 8^7 \ mod \ 11$

$8^{107} \equiv 8^2.8^2.8^2.8 \ mod \ 11 \Rightarrow 8^{107} \equiv 9.9.9.8 \ mod \ 11 \Rightarrow 8^{107} \equiv 2 \ mod \ 11$

$8^{107} \equiv x \ mod \ 17 \Rightarrow 8^{16} \equiv 1 \ mod \ 17 \Rightarrow (8^{16})^{16}.8^{11} \equiv 8^{11} \ mod \ 17$

$8^{107} \equiv 8^2.8 \ mod \ 17 \Rightarrow 8^{107} \equiv 13^5.8 \ mod \ 17 \Rightarrow 8^{107} \equiv 2 \ mod \ 17$

Assim:

$$\begin{cases} x \equiv 2 \mod 11 \\ x \equiv 2 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 2$

$D(173)$

$D(173) = 173^{107} \equiv x \mod 187$

$173^{107} \equiv x \mod 11 \Rightarrow 8^{107} \equiv x \mod 11 \Rightarrow 8^{107} \equiv 8^7 \mod 11$

$8^{107} \equiv 9.9.9.8 \mod 11 \Rightarrow 8^{107} \equiv 2 \mod 11 \Rightarrow 173^{107} \equiv 2 \mod 11$

$173^{107} \equiv x \mod 17 \Rightarrow 3^{107} \equiv x \mod 17 \Rightarrow 3^{16} \equiv 1 \mod 17$

$(3^{16})^6.3^{11} \equiv 3^{11} \mod 17 \Rightarrow 3^{107} \equiv 3^3.3^3.3^3.3^2 \mod 17$

$3^{107} \equiv 10.10.10.9 \mod 17$

$3^{107} \equiv 7 \mod 17 \equiv 173^{107} \equiv 7 \mod 17$

Assim:

$$\begin{cases} x \equiv 2 \mod 11 \\ x \equiv 7 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 24$

$D(168)$

$D(168) = 168^{107} \equiv x \mod 187$

$168^{107} \equiv x \mod 11 \Rightarrow 3^{107} \equiv x \mod 11 \Rightarrow 3^{107} \equiv 1 \mod 11$

$3^{107} \equiv 3^7 \mod 11 \Rightarrow 3^{107} \equiv 3^3.3^3.3 \mod 11 \Rightarrow 3^{107} \equiv 5.5.3 \mod 11$

$3^{107} \equiv 9 \mod 11 \equiv 168^{107} \equiv 9 \mod 11$

$168^{107} \equiv x \mod 17 \Rightarrow 15^{107} \equiv x \mod 17 \Rightarrow 15^{107} \equiv x \mod 17 \Rightarrow 15^{16} \equiv 1 \mod 17$

$(15^{16})^3.15^{11} \equiv 15^{11} \mod 17 \Rightarrow 15^{107} \equiv (15^2)^5.15 \mod 17$

$15^{107} \equiv 4^5.15 \mod 17 \Rightarrow 15^{107} \equiv 9 \mod 17$

Assim:

$$\begin{cases} x \equiv 9 \mod 11 \\ x \equiv 9 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 9$

$D(148)$

$D(148) = 148^{107} \equiv x \mod 187$

$148^{107} \equiv x \mod 11 \Rightarrow 5^{107} \equiv x \mod 11 \Rightarrow 5^{107} \equiv 1 \mod 11$

$5107 \equiv 5^7 \mod 11 \Rightarrow 5^{107} \equiv 5^2.5^2.5^2.5 \mod 11 \Rightarrow 5^{107} \equiv 3.3.3.5 \mod 11$

$5^{107} \equiv 3 \mod 11 \equiv 148^{107} \equiv 3 \mod 11$

$148^{107} \equiv x \mod 17 \rightarrow 12^{107} \equiv x \mod 17 \Rightarrow 12^{16} \equiv 1 \mod 17$

$(12^{16})^6.12^{11} \equiv 12^{11} \mod 17 \Rightarrow 12^{107} \equiv (12^{12})^5 \mod 17$

$12^{107} \equiv (12^8)^5 \mod 17 \Rightarrow 12^{107} \equiv 12.9 \mod 17$

$12^{107} \equiv 6 \mod 17 \equiv 148^{107} \equiv 6 \mod 17$

Assim:

$$\begin{cases} x \equiv 3 \mod 11 \\ x \equiv 6 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 91$

$D(92)$

$D(92) = 92^{107} \equiv x \mod 187$

$92^{107} \equiv x \mod 11 \Rightarrow 4^{107} \equiv 1 \mod 11 \Rightarrow 4^{107} \equiv 4^7 \mod 11$

$4^{107} \equiv 5 \mod 11 \equiv 92^{107} \equiv 5 \mod 11$

$92^{107} \equiv x \mod 17 \Rightarrow 7^{107} \equiv x \mod 17 \Rightarrow 7^{16} \equiv 1 \mod 17$

$(7^{16})^6.7^{11} \equiv 7^{11} \mod 17 \Rightarrow 7^{107} \equiv (7^2)^5.7 \mod 17$

$7^{107} \equiv (15^5).7 \mod 17 \Rightarrow 7^{107} \equiv 14 \mod 17 \Rightarrow 92^{107} \equiv 14 \mod 17$

$$\begin{cases} x \equiv 5 \mod 11 \\ x \equiv 14 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 82$

$D(156)$

$D(156) = 156^{107} \equiv x \ mod \ 187$

$156^{107} \equiv x \ mod \ 11 \Rightarrow 2^{107} \equiv x \ mod \ 11 \Rightarrow 2^{10} \equiv 1 \ mod \ 11$

$2^{107} \equiv 2^7 \ mod \ 11 \Rightarrow 2^{107} \equiv 128 \ mod \ 11 \Rightarrow 2^{107} \equiv 7 \ mod \ 11$

$156^{107} \equiv 7 \ mod \ 11$

$156^{107} \equiv x \ mod \ 17 \Rightarrow 3^{107} \equiv x \ mod \ 17 \Rightarrow 3^{16} \equiv 1 \ mod \ 17$

$(3^{16})^6.3^{11} \equiv 3^{11} \ mod \ 17 \Rightarrow 3^{107} \equiv 3^2.(3^3)^3 \ mod \ 17 \Rightarrow 3^{107} \equiv 9.10^3 \ mod \ 17$

$3^{107} \equiv 7 \ mod \ 17 \Rightarrow 156^{107} \equiv 7 \ mod \ 17$

Logo:

$$\begin{cases} x \equiv 7 \mod 11 \\ x \equiv 7 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 7$

$D(138)$

$D(138) = 138^{(}107) \equiv x \ mod \ 187$

$138^{107} \equiv x \ mod \ 11 \Rightarrow 6^{107} \equiv x \ mod \ 11 \rightarrow 6^{107} \equiv 1 \ mod \ 11$

$6^{107} \equiv 6^7 \ mod \ 11 \Rightarrow 6^{107} \equiv 6.(6^2)^3 \ mod \ 11 \Rightarrow 6^{107} \equiv 6.(3^3) \ mod \ 11$

$6^{107} \equiv 8 \ mod \ 11 \equiv 138^{107} \equiv 8 \ mod \ 11$

$138^{107} \equiv x \ mod \ 17 \Rightarrow 2^{107} \equiv x \ mod \ 17 \Rightarrow 2^{16} \equiv 1 \ mod \ 17$

$(2^{16})^6.2^{11} \equiv 2^{11} \ mod \ 17 \Rightarrow 2^{107} \equiv 2^{11} \ mod \ 17 \Rightarrow 2^{17} \equiv 8 \ mod \ 17$

$138^{107} \equiv 8 \ mod \ 17$

$$\begin{cases} x \equiv 8 \mod 11 \\ x \equiv 8 \mod 17 \end{cases}$$

Resolvendo o sistema temos $x = 8$

Assim após a etapa da decodificação, temos:

$$D(170)D(180)D(8)D(173)D(168)D(148)D(92)D(156)D(62)D(138) = 102712249918271828$$

Quebrando em bloco de dois digito, temos: $10-27-12-24-99-18-27-18-28$*, voltando à tabela inicial temos a seguinte mensagem ARCO IRIS, que é a mensagem inicial.*

2.5 Porque o RSA funciona

Salientamos que a Criptografia RSA usa chave pública, isto é, a chave $(n; e)$ é revelada. Conhecendo ϕ(n) e e, é fácil descobrir o parâmetro d, necessário para a decodificação, usando-se o algoritmo estendido de Euclides. No entanto, descobrir ϕ(n) revelou-se equivalente a fatorar n, um problema potencialmente difícil. Em nossos exemplos, escolhemos n pequenos, especialmente fácil de decompor em fatores primos, a fim de ilustrar o funcionamento do método. Para quem cria a chave codificadora, é possível escolher primos P e Q muito grandes e tais que não existam métodos eficientes para fatorar n de modo a descobrir estes primos. Certamente existem métodos para fatorar n, porém, para primos sabiamente escolhidos, com a tecnologia atual, o processo demandaria milhares de anos. A tabela a seguir mostra o número de operações necessárias para fatorar n e o tempo requerido em cada operação em um microssegundo para cada quantidade de dígitos decimais do número n.

Dígitos	Número de operações	Tempo
50	$1,4.10^{10}$	$3,9$ horas
70	9.10^{12}	104 dias
100	$2,3.10^{15}$	74 anos
200	$1,2.10^{23}$	$3,8.10^{9}$ anos
300	$1,5.10^{29}$	$4,9.10^{15}$ anos
500	$1,3.10^{39}$	$4,2.10^{25}$ anos

O método General Number Field Sieve (GNFS) estudado por Shamir e Arjem Lenstra. Este é uma extensão do método chamado Special Number Field Sieve (SNFS).

Ele é o algoritmo mais eficiente conhecido atualmente para fatorar números com um número de dígitos maior do que 100.

Algoritmos "turbinados"e o uso de computadores super-velozes fariam a fatoração provavelmente mais rápida, mas não significativamente menor, para números muito grandes. A título de ilustração, considere que o bloco C a ser codificado tenha 100 casas decimais e que e tenha 50 casas decimais. Dessa forma, para cifrar o bloco haveria um cálculo da ordem de:

$$C^e = [10^{100}]^{(10)^{50}}$$

É importante observar que um número dessa grandeza não poderia ser armazenado em qualquer computador. No entanto, é possível obter o módulo deste número, evitando a explosão de memória. Outro problema que surge no método RSA é a necessidade de gerar números primos grandes aleatoriamente. Diante disso, acredita-se que quebrar o RSA e fatorar n sejam problemas equivalentes.

Capítulo 3

O que a função ϕ de Euler tem a ver com as dízimas

As frações podem ser representadas por números decimais onde sua expansão pode ser finita, ou após a parte inteira pode ocorrer repetições de algarismos, podendo ser logo após a vírgula ou ainda após algumas casas decimais, estes números são denominados dízimas periódica e são classificadas de acordo com os algarismos que aparecem em sua parte decimal. Vejamos a tabela a seguir:

$\frac{1}{2} = 0,5$	$\frac{1}{14} = 0,0\overline{718345}$	$\frac{1}{26} = 0,0\overline{384615}$
$\frac{1}{3} = 0,\overline{3}$	$\frac{1}{15} = 0,0\overline{6}$	$\frac{1}{27} = 0,\overline{037}$
$\frac{1}{4} = 0,25$	$\frac{1}{16} = 0,0625$	$\frac{1}{28} = 0,03\overline{571428}$
$\frac{1}{5} = 0,2$	$\frac{1}{17} = 0,\overline{0588235294117647}$	$\frac{1}{29} = 0,\overline{0344827586206896551724137931}$
$\frac{1}{6} = 0,1\overline{6}$	$\frac{1}{18} = 0,0\overline{5}$	$\frac{1}{30} = 0,033$
$\frac{1}{7} = 0,\overline{142857}$	$\frac{1}{19} = 0,\overline{052631578947368421}$	$\frac{1}{31} = 0,\overline{032258064516129}$
$\frac{1}{8} = 0,125$	$\frac{1}{20} = 0,05$	$\frac{1}{32} = 0,03125$
$\frac{1}{9} = 0,\overline{1}$	$\frac{1}{21} = 0,\overline{047619}$	$\frac{1}{33} = 0,\overline{03}$
$\frac{1}{10} = 0,1$	$\frac{1}{22} = 0,0\overline{45}$	$\frac{1}{34} = 0,0\overline{2941176470588235}$
$\frac{1}{11} = 0,\overline{09}$	$\frac{1}{23} = 0,\overline{0434782608695652173913}$	$\frac{1}{35} = 0,0\overline{285714}$
$\frac{1}{12} = 0,08\overline{3}$	$\frac{1}{24} = 0,041\overline{6}$	$\frac{1}{36} = 0,02\overline{7}$
$\frac{1}{13} = 0,\overline{076923}$	$\frac{1}{25} = 0,04$	$\frac{1}{37} = 0,\overline{027}$

Na representação da dízima periódica podemos escrever o período apenas uma vez, com um traço na parte superior, isto indica que aquele conjunto de algarismos repete-se infinitas vezes.

Exemplo 3.1 *:*

$$\frac{1}{7} = 0,\overline{142857}$$

$$\frac{1}{36} = 0,02\overline{7}$$

Note que o período da dízima periódica pode apresentar-se logo após a vírgula ou após alguns algarismos, estes dois fatos serão usados para a classificação de uma dízima periódica. Quando o período da dízima periódica vier logo após a vírgula, classificaremos como dízima periódica simples. Quando existir valores entre a vírgula e o início do período, a dízima periódica é classificada como composta. Neste caso os algarismos entre a vírgula e o período são chamados de parte não periódica. Vejamos no exemplo:

Exemplo 3.2 *:*

$\frac{1}{3} = 0,\overline{3} \rightarrow$ *Dízima periódica simples*

$\frac{1}{6} = 0,1\overline{6} \rightarrow$ *Dízima periódica composta*

3.1 Geratriz de uma dízima periódica

A geratriz de uma dízima periódica é a fração de valor igual aquela dízima periódica.

$\frac{7}{9} = 0,777... = 0,\overline{7}$

$\frac{12}{90} = 0,1333... = 0,1\overline{3}$

3.2 Determinando a fração geratriz de uma dízima periódica

De um modo geral, existem alguns métodos para determinar a fração geratriz, mas todos eles são decorrentes do estudo de séries numéricas.
Vejamos:

$$S = a + ar + ar^2 + ar^3 + \cdots = \sum_{i=0}^{\infty} ar^i = \frac{a}{1-r} \ \forall \ a \in \mathbb{R} \text{ e } \forall \mid \text{r} \mid < 1$$

sendo a o primeiro elemento da série e r a razão

Exemplo 3.3 *:*

Vamos definir a fração geratriz da expansão decimal $0,\overline{3}$

$0,\overline{3} = 0,33333333 = 0,3 + 0,03 + 0,003 + \cdots$

Deste modo Temos a = 0,3 e r = 0,1, logo

logo:

$$S = \frac{0,3}{1-0,1} = \frac{0,3}{0,9} = \frac{1}{3} \ .$$

Portanto: $0,\overline{3} = \frac{1}{3}$

Porém, no estudo de dízimas no ensino básico, são aplicadas algumas convenções para determinarmos a fração geratriz de uma dízima, mas todas elas como ja foi dito anteriormente são decorrentes do estudo de séries.
Vejamos dois casos:

1. Se a dízima periódica for simples o numerador da fração passa a ser o período da dízima e o denominador, tanto noves quantos forem os algarismos do período. Assim temos:

$$0,444... = \frac{4}{9}$$

$$0,151515... = \frac{15}{99}$$

Vale ressaltar que se a dízima periódica for maior que 1, temos que trabalhar apenas com a parte decimal e em seguida adicionarmos a parte inteira à fração encontrada determinando a fração geratriz.

Vejamos:

Exemplo 3.4 *:*
$2,151515... = 2 + 0,151515 = 2 + \frac{15}{99} = \frac{213}{99}$

2. Se a dízima periódica for composta, ela será do tipo $\frac{n}{m}$, onde n parte não periódica seguida do período, menos parte não periódica e m tanto noves quartos forem o período seguidos de tantos zeros quantos forem a parte não periódica.
   Vejamos:

Exemplo 3.5 *:*

$0,125252...$

Parte periódica = 25 e parte não periódica = 1, assim temos:
$\frac{n}{m} = \frac{125-1}{990} = \frac{124}{990} = \frac{62}{495} = 0,1252525252$

Exemplo 3.6 *:*

$0,047777777$

Parte periódica = 7 e parte não periódica = 04, assim temos:
$\frac{n}{m} = \frac{47-4}{900} = \frac{43}{900}$

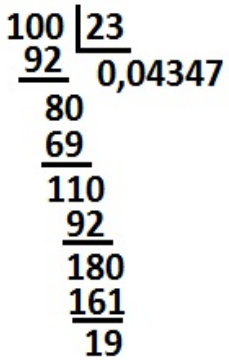
Do mesmo modo que no caso 1, se a dízima periódica for maior que 1, vamos achar a fração usando a parte decimal e em seguida devemos somar a parte inteira, determinando assim a fração geratriz. Vejamos:

Exemplo 3.7 *:*
$3,4171717... = 3 + 0,4171717... = 3 + \frac{417-4}{990} = \frac{3383}{990}.$

3.3 As dízimas periódicas e o uso da calculadora

Agora para fazermos o processo contrário, achar a dízima periódica gerada pela fração geratriz basta dividirmos o numerador pelo denominador e pronto, eis a dízima periódica. Mas ai é que mora o perigo, as dízimas periódicas pode ter seu período muito longo, geralmente quando fazemos a divisão manual pelo método convencional, trabalhamos poucas casas decimais e já chegamos a alguma conclusão, algumas delas erradas. Até mesmo na calculadora podemos cometer este erro, ja que a maioria delas trabalham com poucas casas decimais e algumas dízimas podem ter seu período tão grade ou tão distante da vírgula que seus visores não tem a capacidade de fazer tal visualização, induzindo assim o operador ao erro.

Exemplo 3.8 *:*
Tomamos como base a fração $\frac{1}{23}$*, manualmente temos:*



Somente um aluno muito dedicado faria uma divisão manual com tantas casas decimais para ter certeza que $\frac{1}{23}$ *= 0,04347, ou seja, não tem período de repetições dos dígitos, mas para ter certeza vejamos o que a calculadora nos diz:*

Na calculadora científica (que é um pouco melhor do que as comuns) temos: $\frac{1}{23} = 0,04347826$*, assim está comprovado que* $\frac{1}{23}$ *realmente não gera uma dízima periódica. Pois é ai que esta o perigo. Em uma análise mais detalhada podemos notar que:*

$\frac{1}{23} = 0,043478260869565217391304347 8$*, assim:*

$$\frac{1}{23} = 0,\overline{0434782608695652173913}$$

Uma dizíma periódica com 22 algarismos no período, portanto, tanto o aluno insistente quanto a calculadora estavam errados, pois $\frac{1}{23}$ é uma fração geratriz, portanto um número racional, mas aí surge a seguinte pergunta: Como determinar então o período da dízima quando este for muito grande, já que nem a calculadora faz isso? Vejamos então um algoritmo, usando a calculadora simples, que permite encontrar quantas casas decimais quisermos em uma divisão do tipo $\frac{1}{n}$ com n pertencente aos naturais.

Uma calculadora simples pode ter em seu visor 8 dígitos, o que nos permite uma expansão decimal de 7 casas nas divisões do tipo $\frac{1}{n}$, com n pertencente aos naturais. Assim, basta calcularmos os restos das divisões de $10^0, 10^7, 10^{14}, 10^{21}, 10^{28}$... sempre por n.

Vejamos outro caso:

Exemplo 3.9 *:*
Vamos determinar a expansão decimal de $\frac{1}{17}$ *usando uma calculadora comum:*

Vejamos:

- $10^0 \equiv x \ mod \ 17 \rightarrow 1 \equiv 1 \ mod \ 17$

  $\frac{1}{17}$ *na calculadora* $\rightarrow 0,0588235$

- $10^7 \equiv x \ mod \ 17 \rightarrow 10^7 \equiv 5 \ mod \ 17$

  $\frac{5}{17}$ *na calculadora* $\rightarrow 0,2941176$

- $10^{14} \equiv x \ mod \ 17 \rightarrow (10^7)^2 \equiv x \ mod \ 17 \rightarrow 5^2 \equiv x \ mod \ 17$
  $25 \equiv x \ mod \ 17 \rightarrow 10^{14} \equiv 8 \ mod \ 17$

$\frac{8}{17}$ *na calculadora* $\rightarrow 0,4705882$

Note que os dígitos começaram a se repetir, assim:

$\frac{1}{17} = 0,058823529411764705882$ ou simplesmente:

$\frac{1}{17} = 0,\overline{0588235294117647}$

Dada a fração ordinária irredutível $\frac{a}{b}$, a pergunta que se faz é a seguinta: Quando a expansão decimal de $\frac{a}{b}$ é finita ou infinita?
Para responder estas perguntas, optamos pelos seguintes teoremas:

Teorema 3.3.1 *:*
Se b tem outros fatores primos diferentes de 2 ou de 5, então a expansão decimal de $\frac{a}{b}$ *é infinita, caso contrário, a expansão decimal de* $\frac{a}{b}$ *é finita.*

A prova segue do lema a seguir:

Lema 3.3.2 *:*
Seja $\frac{a}{b}$ *uma fração ordinária irredutível, então temos as seguintes afirmações:*

1. *Toda expansão decimal finita pode ser representada pela fração* $\frac{a}{b}$*, onde b tem fatores primos diferentes de 2 ou 5.*

2. *Dada a fração* $\frac{a}{b}$*, onde b não tem fatores primos diferentes de 2 ou de 5, então existe uma expansão decimal finita de* $\frac{a}{b}$*.*

Demonstração: 6 .

1. *Considere a representação decimal* $\frac{1}{b}$ *com k dígitos, ou seja,* $\frac{1}{b}$ *= 0,* $d_1d_2d_3...d_k$ *de outra forma podemos escrever:*

$$\frac{1}{b} = \frac{d_1}{10} + \frac{d_2}{10^2} + \frac{d_3}{10^3} + ... + \frac{d_k}{10^k}$$

$$\frac{1}{b} = \frac{1}{10^k}(d_1 10^{k-1} + d_2 10^{k-2} + d_3 10^{k-3} + d_k)$$

Agora tomamos $M = d_1 10^{k-1} + d_2 10^{k-2} + d_3 10^{k-3} + d_k$ *obtemos:*

$$\frac{1}{b} = \frac{M}{10^k} \Rightarrow Mb = 10^k \Rightarrow b \mid 10^k$$

Como os únicos divisores primos de 10^k *são o* 2 *e o* 5*, segue que os únicos divisores de* b *são também* 2 *e o* 5

2. *Agora, consideramos a fração ordinária irredutível* $\frac{a}{b}$*, onde* b *não tem fatores primos diferentes de* 2 *e de* 5.
   Logo podemos escrever:
   $b = 2^i \ . \ 5^j$ *com* i *e* j *inteiros* ≥ 0 .
   Seja $K = max:\{i, j\}$*, logo*

$$10^k.\frac{a}{b} = 2^k \ . \ 5^k.a.\frac{1}{2^i.5^j} = a.2^{k-i} \ . \ 5^{k-j}$$

tomamos agora $M = 2^{k-i} \ . \ 5^{k-j}$*, desta forma temos que* M *é um número inteiro, então:*

$$10^k \ . \ \frac{a}{b} = a.M, \text{ ou seja:}$$

$$\frac{10^k}{b} = M, \text{ o que significa que } M < 10^k, \text{ assim podemos escrever:}$$

$$M = a_{k-1}.10^{k-1} + a_{k-2}.10^{k-2} + ... + a_2.10^2 + a_1.10^1 + a_0$$
$$M = a_{k-1} \ . \ a_{k-2}.....a_2.a_1.a_0$$

Seja $K = max:\{i, j\}$*, logo*
$10^k.\frac{a}{b} = 2^k \ . \ 5^k.a.\frac{a}{2^i.5^j} = a.2^{k-i} \ . \ 5^{k-j}$*, desta forma temos que:*

$M = 2^{k-i} \ . \ 5^{k-j}$, *desta forma temos que* M *é um número inteiro, então:*

$\frac{1}{b} = \frac{M}{10^k}$, *o que significa que* $M < 10^k$.

Assim podemos escrever:
$M = a_{k-1}.10^{k-1} + a_{k-2}.10^{k-2} + ... + a_2.10^2 + a_1.10^1 + a_0$
$M = a_{k-1} \ . \ a_{k-2}.....a_2.a_1.a_0$
Como $K = max:\{i, j\}$, *pelo menos* $K - i = 0$ *ou* $k - j = 0$.
Para $K - i = 0$, *temos que* $M = 5^{k-j}$, *ou seja,* $M \not| 10$, *assim* $a_0 \neq 0$
Portanto:

$\frac{1}{b} = \frac{M}{10^k} = 0,a_{k-1} \ . \ a_{k-2}.....a_2.a_1.a_0$, *com* $a_0 \neq 0$.

Uma parte importante que deve ser mencionada é o comportamento sobre o comprimento da parte que se repete, ou seja, a parte periódica da expansão decimal. Para isso, vamos voltar nossas atenções para as expansões decimais da forma $\frac{1}{b}$.

Teorema 3.3.3 *:*
O comprimento de qualquer expansão decimal de $\frac{1}{b}$ *é no máximo* $b - 1$.

Demonstração: 7 .

Sejam $\alpha \geq 0$ *e* $\beta \geq 0$, *inteiros, então:*

- *Se* $b = 2^{\alpha}.5^{\beta}$, *então* $\frac{1}{b}$ *tem uma expansão decimal finita*

- *Se* $b \neq 2^{\alpha}.5^{\beta}$, *então* $b \neq 10^k$, *para algum inteiro* $k \geq 0$

Agora, seja t *um inteiro tal que* $10^{t-1} < b < 10^t$
Pelo algoritmo da divisão temos:

$$(1)\begin{cases} 10^{t-1} = & d_1 b + r_1 & 0 < r_1 < b \\ 10r_1 = & d_2 b + r_2 & 0 < r_2 < b \\ 10r_3 = & d_3 b + r_3 & 0 < r_3 < b \\ . & . & . \\ . & . & . \\ . & . & . \\ 10r_{k-1} = & d_k b + r_k & 0 \leq r_k < b \\ 10k = & d_{k+1} b + r_{k+1} & 0 \leq r_{k+1} < b \\ . & . & . \\ . & . & . \\ . & . & . \end{cases}$$

e assim por diante.

Note que:

$d_k\ b = 10r_{k-1}$ - $r_k \leq r_{k-1}$, *e como*

$r_{k-1} < b$, *temos que:*

$d_k\ b \leq 10r_{k-1} < 10b$

Para $k = 1$, *temos:*

$d_1\ b = 10^{t+1}$ - $r_1 < 10^{t+1} = 10^t 10 < 10b$

Dividindo $10r_k = d_{k+1}b + r_{k+1}$ *por* $10b$, *temos:*

$$\frac{r_k}{b} = \frac{d_{k+1}}{10} + \frac{r_{k+1}}{10b} \text{ (2)}$$

dividindo agora $10^{t+1} = d_1 b + r_1$ *por* $10^{t+1}b$, *obtemos*

$$\frac{1}{b} = \frac{d_1}{10^{t+1}} + \frac{r_1}{b10^{t+1}} \text{ (3)}$$

Substituindo agora (2) em (3), temos:

$$\frac{1}{b} = \frac{d_1}{10^{t+1}} + \frac{d_2}{10^{t+2}} + \frac{r_2}{b10^{t+2}}$$

$$\frac{1}{b} = \frac{d_1}{10^{t+1}} + \frac{d_2}{10^{t+2}} + \frac{d_3}{10^{t+3}} + \frac{r_3}{b10^{t+3}}$$

.

.

.

$$\frac{1}{b} = \frac{d_1}{10^{t+1}} + \frac{d_2}{10^{t+2}} + \frac{d_3}{10^{t+3}} + ... + \frac{d_k}{10^{t+k}} + ...$$

Onde d_1, d_2, d_3, ..., d_k, são os dígitos da expansão decimal de $\frac{1}{b}$.

Agora, se $r_k = 0$ para algum k, então:

$$\frac{1}{b} = \frac{d_1}{10^{t+1}} + \frac{d_2}{10^{t+2}} + \frac{d_3}{10^{t+3}} + ... + \frac{d_k}{10^{t+k}}$$

Ou seja, a expansão decimal de $\frac{1}{b}$ seria finita, o que contraria a hipótese de que $b \neq 10^k$

Agora se $r_k \neq 0$, para todo k.
então, cada resto r_1, r_2, r_3, ..., pode assumir um dos (b-1) valores: $1, 2, 3, 4, ..., (b-1)$.
Pelo princípio das gavetas, entre os $b-1$ inteiros r_1, r_2, r_3, ... r_b, existem dois deles que são iguais, digamos que para algum j e k, com $k < j$, pelas equações (1):

$$d_j + 1 = d_k + 1$$
$$d_j + 2 = d_k + 2$$
$$d_j + 3 = d_k + 3$$

.

.

.

Ou seja, a expansão decimal se repete com um período menor ou igual a $b-1$.

Consideramos a expansões decimais de $\frac{1}{b}$, com $mdc(b, 10) = 1$, o comprimento do período é determinado pelas soluções r da equação $10^r \equiv 1$ *mod* b. Mais precisamente:

Teorema 3.3.4 *:*
Se $M.D.C(b, 10) = 1$ e r é a menor solução inteira da equação $10^r \equiv 1$ mod b, então a expansão decimal de $\frac{1}{b}$ terá um período igual a r dígitos.

Demonstração: 8 .

Por hipótese, temos que $10^r \equiv 1 \mod b$

Então:

10^r*-1 =* kb *para algum inteiro* k*. Obviamente* $k < 10^r$*, logo podemos escrever este* k *na base 10*

Desta forma temos:

$k = d_{r-1}10^{r-1} + d_{r-2}10^{r-2} + ... + d_2 10^2 + d_1 10 + d_0$

$k = d_{r-1} \ . \ d_{r-2}...d_1.d_0$*, onde* $0 \leq d_k < 9$*, para cada* $k = 0, 1, 2, 3, ..., r-1$ *Mas:*

$$\frac{1}{b} = \frac{k}{10^r - 1} = \frac{k}{10^r(1 - 10^{-r})}$$

$$\frac{1}{b} = \frac{d_{r-1}.d_{r-2}...d_1.d_0}{10^r} \ . \ \frac{1}{1 - 10^{-r}}$$

$$\frac{1}{b} = (\ 0,\ d_{r-1} \ . \ d_{r-2}...d_1.d_0) + (1 + \frac{1}{10^r} + \frac{1}{10^{2r}} + \frac{1}{10^{3r}} + ...)$$

$$\frac{1}{b} = (\ 0,\ d_{r-1} \ . \ d_{r-2}...d_1.d_0) \ .(\underbrace{0,00...0}_{r-zeros} d_{r-1} \ . \ d_{r-2}...d_1.d_0) + (\underbrace{0,00...0}_{2r-zeros} d_{r-1} \ . \ d_{r-2}...d_1.d_0)$$
$$+ (\underbrace{0,00...0}_{3r-zeros} d_{r-1} \ . \ d_{r-2}...d_1.d_0) + ...$$

$$\frac{1}{b} = 0,\ d_{r-1} \ . \ d_{r-2}...d_1.d_0 \ d_{r-1} \ . \ d_{r-2}...d_1.d_0 \ d_{r-1} \ . \ d_{r-2}...d_1.d_0$$

$$\frac{1}{b} = 0, \overline{d_{r-1}.d_{r-2}...d_1.d_0}$$

Logo, o período de $\frac{1}{b}$ *é no máximo* r *dígitos.*

Agora, suponha que o períod de $\frac{1}{b}$ *é* s*, isto é:*

$\frac{1}{b} = 0, \overline{l_{s-1}.l_{s-2}...l_1.l_0}$*, onde* l_i *para* $i = 0, 1, 2, ..., s-1$ *são inteiros com* $0 \leq l_i < 10$

Por definição de período de uma expansão decimal, sabemos que $s \leq r$*.*
Mas $\frac{1}{b} = (\ 0,l_{s-1} \ . \ l_{s-2}...l_1.l_0)\ (1 + \frac{1}{10^s} + \frac{1}{10^{2s}} + \frac{1}{10^{3s}}...)$*, logo*

$$\frac{1}{b} = \frac{l_{s-1}.l_{s-2}...l_1.l_0}{10^s} \ . \ \frac{1}{1 - 10^{-s}}$$

$b(l_{s-1}\ .\ l_{s-2}...l_1.l_0) = \dfrac{1}{1-10^{-s}}$

$b|\ 10^s - 1$,
Ou seja, $10^s \equiv$ *1 mod b e como* $10^r \equiv$ *1 mod b segue que* $r \geq s$

portanto $r = s$

Observação 1 *:*
O inteiro r é chamado a ordem de 10 *módulo b. E escrevemos;* $r = ord_b^{10}$

Observação 2 *:*
Quando $r = \phi(b)$*, com b primo, dizemos que* 10 *é uma raiz primitiva módulo b.*

O teorema 3.2.3 também pode ser usado para encontrar o período da expansão decimal de qualquer fração irredutível $\dfrac{a}{b}$ cuja expansão é infinita.
Se $b = 2^{\alpha}.5^{\beta}$, então a expansão decimal é finita. Se $b \neq 2^{\alpha}.5^{\beta}$, então escolhemos b na forma $b = m_0.2^{\alpha}.5^{\beta}$, com $m_0 > 1$ e $mdc(10, m_0) = 1$.

Teorema 3.3.5 *:*
Se $b = m_0.2^{\alpha}.5^{\beta}$*, com* $m_0 > 1$*,* $mdc(10, m_0) = 1$ *e* $mdc(a, b) = 1$*, então o período da expanção decimal de* $\dfrac{a}{b}$ *é o menor inteiro r tal que* $10^r \equiv$ *1 mod* m_0*. Além disso, o comprimento da parte não periódica da expansão decimal de* $\dfrac{a}{b}$ *é dada por M, onde* $M =$ *max:*$\{\alpha, \beta\}$.

Demonstração: 9 *:*
A demonstração deste teorema segue dos teoremas anterioriores.

Exemplo 3.10 *:*

Determine o período de expansão decimal de $\dfrac{1}{33}$ *e sua expansão decimal.*

Como $M.D.C(33, 10) = 1$ *e r a maior solução inteira para a equação* $10^r \equiv$ *1 mod*

33

segue que $\phi(33) = \phi(3).\phi(11) \rightarrow \phi(33) = 2.10 \rightarrow \phi(33) = 20$

Assim temos que $r \mid \phi(33)$ *portanto* $r \in \{2, 4, 10, 20\}$.

Vamos aos testes:

$\underline{r = 2}$

Neste caso temos: $10^2 \equiv 1 \bmod 33$.

Note que ja conseguimos o resultado desejado, pois $10^2 \equiv 1 \bmod 33 \rightarrow 10^2 - 1 = 33.k$, *para algum* k, *onde este* k *possui dois dígitos.*

Logo k=03 Assim temos que

$$\frac{1}{33} = \frac{k}{10^2 - 1} = \frac{03}{10^2 - 1} = \frac{03}{10^2(1 - 10^{-2})}$$

Desmembrando a fração temos: $\frac{1}{33} = \frac{03}{10^2} . \frac{1}{(1 - 10^{-2})}$

$$\frac{1}{33} = 0,03.(1 + 10^{-2} + 10^{-4} + 10^{-6} + ...) \rightarrow 0,03 + 0,0003 + 0,000003 + 0,00000003 + ...$$

Desta forma segue que $\frac{1}{33}$ = 0,030303030303...

Ou Simplesmente $\frac{1}{33} = 0,\overline{03}$.

Exemplo 3.11 *:*

Determine o período e o comprimento da parte não periódica, bem como a expansão decimal de $\frac{18}{2800}$.

$$\frac{18}{2800} = \frac{2.3^2}{2^4.5^2.7} = \frac{3^2}{2^3.5^2.7}$$

Vamos responder ao primeiro questionamento, o comprimento da parte não periódica da expansão.

$M = max:\{\alpha, \beta\} \rightarrow M = max:\{3,2\} \rightarrow M = 3$

Assim temos que o comprimento da parte não periódica da expansão decimal de $\frac{18}{2800}$ *é 3*

Agora vamos definir o período da expansão decimal, r .

Sabemos que r é o menor inteiro tal que $10^r \equiv 1 \bmod 7$ *e ainda* $r \mid \phi(7)$

Como $\phi(7) = 6$, $r \in \{2, 3, 6\}$. *Vamos aos testes:*

$\underline{r = 2}$

Neste caso temos que $10^2 \equiv 1 \bmod 7$, *o que é uma afirmação falsa, pois* $10^2 - 1 \neq 7.k$ *para algum k inteiro*

portanto $r \neq 2$

$\underline{r = 3}$

Neste caso temos que $10^3 \equiv 1 \bmod 7$, *o que é uma afirmação falsa, pois* $10^3 - 1 \neq 7.k$ *para algum k inteiro*

portanto $r \neq 3$

$\underline{r = 6}$

Neste caso temos que $10^6 \equiv 1 \bmod 7$, *vejamos:* $10^6 \equiv 1 \bmod 7 \rightarrow 3^6 \equiv 1 \bmod 7$

$3^6 \equiv 1 \bmod 7 \rightarrow 9^3 \equiv 1 \bmod 7 \rightarrow 2^3 \equiv 1 \bmod 7 \rightarrow 8 \equiv 1 \bmod 7$

o que é uma afirmação verdadeira, logo $r = 6$

Assim temos que o comprimento do período da expansão decimal $\frac{18}{2800}$ *é de 6 dígitos.*

O último questionamento a ser respondido é sobre a expansão decimal, neste caso temos:

$$\frac{18}{2800} = \frac{3^2}{2^3.5^2.7} = \frac{3^2.5}{2^3.5^3.7} = \frac{9}{10^3.7} = \frac{1}{10^3}.\frac{45}{7}$$

$$\frac{18}{2800} = \frac{1}{10^3}.6 + \frac{3}{7} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{3}{7}$$

Mas $10^6 \equiv 1 \bmod 7 \iff 10^6 - 1 = 7.k$ *para algum k inteiro*

.

Logo $k = \frac{10^6 - 1}{7} \rightarrow k = 142857$, *sendo assim,* $3.k = \frac{3}{7}.(10^6 - 1)$, *portanto,* $\frac{3}{7} = \frac{3.k}{10^6 - 1} \rightarrow 3.k = 428571$

Assim temos que $\frac{18}{2800} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{3k}{10^6 - 1} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{428571}{10^6 - 1}$

$$\frac{18}{2800} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{428571}{10^6.[1 - 10^{-6}]}$$

$$\frac{18}{2800} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{428571}{10^6} \cdot \frac{1}{[1-10^{-6}]}$$

$$\frac{18}{2800} = \frac{6}{10^3} + \frac{1}{10^3} \cdot \frac{428571}{10^6} \cdot (1 + 10^{-6} + 10^{-12} + 10^{-18} + ...)$$

$$\frac{18}{2800} = 0,006 + \frac{1}{10^3} \cdot (0,428571).(1 + 10^{-6} + 10^{-12} + 10^{-18} + ...)$$

$$\frac{18}{2800} = 0,006 + 0,000428571 + 0,000000428571 + 0,000000000428571 + ...$$

$$\frac{18}{2800} = 0,006\overline{428571}$$

Considerações finais

Com os resultados encontrados, podemos exemplificar com maior clareza a utilização de algumas das ferramentas algébricas. Conseguimos com o estudo da criptografia R.S.A usar a maioria dos conteúdos estudados na disciplina de Aritmética neste mestrado, porém não foi encontrado grandes contribuições para o tema, tendo em vista a existência de vários materiais onde o tema ja é apresentado, entretanto, do modo abordado neste material mostramos a criptografia de uma maneira mais didática, de modo que podemos expor o assunto em uma sala de ensino médio e comprovamos também matematicamente a sua eficiência.

No estudo das dízimas, a pesquisa se mostrou mais inovadora, pois apresentou alguns resultados relevantes ao tema. Demonstramos alguns fatos importantes para o assunto, dentre eles mostramos que qualquer fração do tipo $\frac{1}{b}$, com b primo, apresenta parte periódica no máximo igual a $(b-1)$, e que caso este período não seja $(b-1)$, será um de seus divisores. De um modo geral, qualquer fração do tipo $\frac{1}{n}$ terá seu período no máximo igual a $\phi(n)$, caso contrário este período terá uma quantidade de casas igual a um de seus divisores.

Como profissional me vejo hoje muito mais capaz e humano para desenvolver minha função, aprendi que o fato de eu ser o professor da turma não me torna o centro das atenções, vi que não importa o tanto que acredito saber, mas que sim, sempre existe algo importante para aprender, seja isso com um professor, com um colega de trabalho au até mesmo com um aluno.

Referências Bibliográficas

Edson Ribeiro alvares. *Revista do professor de matemática, volume 53*, volume 53. SBM, Rio de Janeiro, 2004.

José Paulo Carneiro. *Revista do professor de matemática, volume 52 - dízimas periódicas e o uso da calculadora*, volume 52. SBM, Rio de Janeiro, 2003.

S.C. Coutinho. *números inteiros e criptografia RSA*. 2. IMPA, Rio de Janeiro, 2011.

Abramo Hefez. *Elementos de aritmética*. 2. SBM, Rio de Janeiro, 2011.

H. Domingues Hygino. *Revista do professor de matemática, volume 52 - O pequeno teorema de Fermat*, volume 52. SBM, Rio de Janeiro, 2003.

Samuel Iezzi, Gelson end Hazzann. *Fundamentos da matemática elementar*, volume 4 of *7*. Atual, São Paulo, 2004.

Elon Lima. *Revista do professor de matemática, volume 10 - Voltando a falar sobre dízimas*, volume 10. SBM, Rio de Janeiro, 1987.

Paulo Cezar Pinto end Vagner Eduardo end Morgado Augusto César Lima, Elon end Carvalho. *A matemática do ensino médio*, volume 1 of *9*. SBM, Rio de Janeiro, 2006a.

Paulo Cezar Pinto end Vagner Eduardo end Morgado Augusto César Lima, Elon end Carvalho. *A matemática do ensino médio*, volume 2 of *9*. SBM, Rio de Janeiro, 2006b.

José Dias Roosevelt. *Revista do professor de matemática, volume 14 - dízimas periódicas e a calculadora*, volume 14 of *1990*. SBM, Rio de Janeiro.

José Plínio de Oliveira Santos. *Introdução a teoria dos números*. 3. IMPA, Rio de Janeiro, 2011.