UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

EM REDE NACIONAL

AURÉLIO EUGÊNIO AGUIAR DE LIMA

CÓDIGOS DE BARRA E CRIPTOGRAFIA

FORTALEZA

2014

AURÉLIO EUGÊNIO AGUIAR DE LIMA

CÓDIGOS DE BARRA E CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Orientador: Prof. Dr. Marcelo Ferreira de Melo

FORTALEZA
2014

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca do Curso de Matemática

L696c Lima, Aurélio Eugênio Aguiar de
Códigos de barra e criptografia / Aurélio Eugênio Aguiar de Lima. – 2014.
77 f. : il., enc.; 31 cm

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2014.
Área de Concentração: Ensino de Matemática.
Orientação: Prof. Dr. Marcelo Ferreira de Melo.

1. Códigos de barra. 2. Criptografia de dados (Computação). I. Título.

CDD 005.82

AURÉLIO EUGÊNIO AGUIAR DE LIMA

CÓDIGOS DE BARRA E CRIPTOGRAFIA

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional, do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial para a obtenção do Título de Mestre em Matemática. Área de concentração: Ensino de Matemática.

Aprovada em: 26 / 04 / 2014.

BANCA EXAMINADORA

Prof. Dr. Marcelo Ferreira de Melo (Orientador)
Universidade Federal do Ceará (UFC)

Prof. Dr. Jonatan Floriano da Silva
Universidade Federal do Ceará (UFC)

Prof. Dr. Jobson de Queiroz Oliveira
Universidade Estadual do Ceará (UECE)

Antônio Gomes de Lima e Maria Madalena Aguiar de Lima, meus pais.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus pelo dom da vida, por sempre me dar forças nos momentos difíceis, por todas as maravilhas que fez em minha vida, por todos os sonhos realizados e também pelo dom de gostar de estudar matemática.

Agradeço a minha querida, adorada e amada esposa Lívia Helena pelo seu empenho, dedicação, carinho e amor ao longo desse tempo que estamos juntos.

Agradeço aos meus pais, o Sr Antônio Gomes de Lima e a Sra Maria Madalena Aguiar de Lima pela dedicação, acompanhamento, amparo, incentivo e amor. Além disso, sempre me ensinaram a ser justo e honesto, mostrando-me o caminho da verdade, do trabalho e da conquista.

Agradeço aos meus irmãos Regina, Rosimar, Nagélia, Mairton, Cristina, Sheila, Eugênia e Lucas pelo apoio, incentivo e harmonia sempre presente em nosso lar.

Agradeço a todos os sobrinhos que sempre me proporcionam grandes alegrias.

A meu amigo, companheiro do mestrado e do PAPMEM, o professor Bacelar da Silva, que despertou em mim o prazer de estudar matemática. Por ter abdicado grande parte de seus horários livres para me ajudar, me ensinando dicas importantíssimas ao longo do 2º Ano do Ensino Médio. Além disso, me incentivou a seguir a profissão na qual estou muito feliz e realizado.

Ao meu amigo Fabrício Figueredo, que por tantas vezes tirou minhas dúvidas, assim como me ensinou novos conteúdos. Ao Dayvit Keffen e ao Ruann Albert pela solidariedade e compromisso com a minha pessoa. A força de vontade e dedicação de vocês três, são fontes de inspiração de que é possível acreditar e realizar nossos sonhos.

Ao, meu amigo, professor Carlos Segundo pelos inúmeros conselhos e pelas sábias palavras que dirigiu a mim, na minha busca pelo melhor desempenho profissional.

Agradeço também ao programa PROFMAT pela oportunidade de crescimento profissional, assim como a CAPES pelo auxílio financeiro ao longo do curso.

Aos meus colegas do mestrado, pelas experiências vividas nas quais me serviram para meu crescimento profissional.

Aos meus professores da UFC, Marcelo Melo, Marcos Melo, Jonatan Floriano, Alberto Maia, Robério Rogério, Othon Dantas e José Afonso pelo valoroso ensino e aprendizado nas disciplinas por eles ministradas.

A banca examinadora pela valorosa contribuição, enriquecendo o trabalho.

Ao meu orientador, o professor Marcelo Melo, pela hospitalidade e pela paz que o senhor transmite, por sua disposição e pelas dicas valiosas que me ensinou tanto ao longo do curso, como nos encontros de orientação e também pelo comprometimento para com sua função.

“Felizes aqueles que conhecem o prazer que tem um bom problema de matemática.”

Aurélio Eugênio

RESUMO

Descreveremos o surgimento e o desenvolvimento dos códigos de barra. Explicaremos como funcionam os códigos UPC, EAN, ISBN e o QR Code. Enfatizaremos o EAN-13 – o mais usado atualmente –, mostrando em que casos e como esse código consegue detectar erros cometidos por falha humana. Além disso, faremos um estudo da criptografia, citando o código de César e o código de blocos. Faremos também um estudo mais detalhado da criptografia RSA, exemplificando a codificação e a decodificação.

Palavras-chave: Códigos de barra. Criptografia.

ABSTRACT

We will describe the emergence and development of the barcodes. We'll explain how the UPC, EAN, ISBN and QR codes work. We will emphasize the EAN-13 – the most currently used – showing where and how this code can detect errors committed by human error. In addition, we make a study of cryptography, quoting the code of Caesar and the code block. We will also do a more detailed study of RSA encryption, exemplifying encoding and decoding.

Keywords: Barcodes. Encryption.

LISTA DE TABELAS

SUMÁRIO

1 PRELIMINARES

1.1 Divisibilidade

Neste trabalho, será considerado o conjunto dos números naturais como sendo o seguinte conjunto $\mathbb{N}=\{0,1,2,3,...\}$ e $\mathbb{N}-\{0\}$ sendo denotado por $\mathbb{N}^*=\{1,2,3,...\}$.

Definição 1.1.1 Dados dois números naturais a e b com $a\neq 0$. Se existir $c\in\mathbb{N}$ tal que $b=a.c$, então dizemos que a divide b, e escrevemos por $a\,|\,b$. Podemos dizer ainda que a é divisor ou um fator de b ou, ainda, que b é múltiplo de a. Caso não exista $c\in\mathbb{N}$ tal que $b=a.c$, dizemos que a não divide b, e escrevemos $a\nmid b$.

Proposição 1.1.1 Sejam $a\in\mathbb{N}^*$ e $c\in\mathbb{N}$. Então $1\,|\,c$, $a\,|\,a$ e $a\,|\,0$.

Demonstração: De fato, todas são verdadeiras, já que $c=1.c$, $a=a.1$ e $0=a.0$.

■

Proposição 1.1.2 Sejam $a,b\in\mathbb{N}^*$ e $c\in\mathbb{N}$, se $a\,|\,b$ e $b\,|\,c$, então $a\,|\,c$.

Demonstração: $a\,|\,b\Rightarrow b=a.m$ com $m\in\mathbb{N}$. Do mesmo modo, $b\,|\,c\Rightarrow c=b.n$ com $n\in\mathbb{N}$. Ora, $c=b.n\Rightarrow c=a.m.n\Rightarrow c=a(m.n)$, isto nos diz que $a\,|\,c$.

■

Proposição 1.1.3 Se $a\,|\,b$ e $a\,|\,c$, então $a\,|\,b+c$.

Demonstração: De fato, $b=a.m$ e $c=a.n$, com $m,n\in\mathbb{N}$. Somando membro a membro teremos $b+c=a.m+a.n=a(m+n)$, logo $a\,|\,b+c$.

■

Proposição 1.1.4 Dados $a\in\mathbb{N}^*$ e $b,c,x,y\in\mathbb{N}$, se $a\,|\,b$ e $a\,|\,c$, então $a\,|\,(bx+cy)$.

Demonstração: $a \mid b \Rightarrow b = a.m$ com $m \in \mathbb{N}$. Do mesmo modo, $b \mid c \Rightarrow c = b.n$ com $n \in \mathbb{N}$. Logo, $bx + cy = a.m.x + a.n.y = a(mx + ny) \Rightarrow a \mid (bx + cy)$.

■

Proposição 1.1.5 Sejam $a, b \in \mathbb{N}^*$, se $a \mid b$ então $a \leq b$.

Demonstração: Como $a \mid b$, temos que $b = a.c$ com $c \in \mathbb{N}^*$, logo $c \geq 1$.

Portanto $a \leq a.c \Rightarrow a \leq b$.

■

Proposição 1.1.6 Sejam $a, b, n \in \mathbb{N}$, com $a \neq b$. Temos que $a - b \mid a^n - b^n$.

Demonstração: Usando o fato que $a^n - b^n = (a-b).(a^{n-1} + a^{n-2}b + ... + ab^{n-2} + b^{n-1})$, logo segue o resultado.

■

Proposição 1.1.7 Sejam $a, b, n \in \mathbb{N}$, com n ímpar, temos que $a + b \mid a^n + b^n$.

Demonstração: De fato, basta ver que $(-b)^n = -b^n$ para n ímpar, logo

$a^n + b^n = a^n - (-b)^n$

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

$= (a+b).(a^{n-1} - a^{n-2}b + \cdots - ab^{n-2} + b^{n-1})$. Logo, segue o resultado.

■

Exemplo 1.1.1 Mostre que se $7 \mid 10a+b$, então $7 \mid a-2b$.

Solução: Veja que $10a+b = 7(a+b)+3(a-2b)$

Como $7 \mid 10a+b \Rightarrow 7 \mid 7(a+b)+3(a-2b) \Rightarrow 7 \mid 3(a-2b)$ já que $7 \mid 7(a+b)$. Como

$7 \nmid 3 \Rightarrow 7 \mid a-2b$.

■

Exemplo 1.1.2 Mostre que $25 \mid 3^{18}+4^{18}$.

Solução: Veja que, $3^{18}+4^{18} = (3^2)^9+(4^2)^9 = 9^9+16^9$.

Pela proposição 1.1.7, temos que $9+16 \mid 9^9+16^9 \Rightarrow 25 \mid 3^{18}+4^{18}$.

■

Exemplo 1.1.3 Mostre que 165 divide a soma $S = 1^{99}+2^{99}+\cdots+163^{99}+164^{99}+165^{99}$.

Solução: Usando proposição 1.1.7, temos que $165 \mid 1^{99}+164^{99}$, $165 \mid 2^{99}+163^{99}$,...,$165 \mid 165^{99}$ de modo geral, $165 \mid a^{99}+(165-a)^{99}$, com $a \in \mathbb{N}$ e $1 \le a \le 165$. De fato, pela proposição 1.1.3, 165 divide a soma, logo $165 \mid 1^{99}+2^{99}+\cdots+163^{99}+164^{99}+165^{99}$.

■

Exemplo 1.1.4 Mostre que o número $1^n+8^n-3^n-6^n$ é múltiplo de 10 para todo natural.

Solução: Basta mostrar que tal número é múltiplo de 2 e 5.

i) $1^n+8^n-3^n-6^n = (8^n-6^n)-(3^n-1^n) = 2(8^{n-1}+\cdots+6^{n-1})-2(3^{n-1}+\cdots+1)$

$= 2[(8^{n-1}+\cdots+6^{n-1})-(3^{n-1}+\cdots+1)]$, portanto é múltiplo de 2.

ii) $1^n+8^n-3^n-6^n = (8^n-3^n)-(6^n-1^n) = 5(8^{n-1}+\cdots+3^{n-1})-5(6^{n-1}+\cdots+1)$

$= 5[(8^{n-1}+\cdots+3^{n-1})-(6^{n-1}+\cdots+1)]$, portanto é múltiplo de 5. Logo o número é múltiplo de 10.

■

Exemplo 1.1.5 Mostre que:

i) $2^{1000} \mid 1001\times1002\times\cdots\times2000$.

ii) $2^{1001} \nmid 1001\times1002\times\cdots\times2000$.

Solução:

i) Veja que

$$1001\times1002\times\cdots\times2000=\frac{1\times2\times\cdots\times1999\times2000}{1\times2\times\cdots\times999\times1000}=\frac{(2\times4\times\cdots\times1998\times2000)(1\times3\times\cdots\times1997\times1999)}{1\times2\times\cdots\times999\times1000}$$

$$=\frac{2^{1000}(1\times2\times\cdots\times999\times1000)(1\times3\times\cdots\times1997\times1999)}{1\times2\times\cdots\times999\times1000}=2^{1000}(1\times3\times\cdots\times1997\times1999).$$

ii) Basta observar que 2^{1000} é a potência máxima de 2 que divide $2^{1000}(1\times3\times\cdots\times1997\times1999)$. Portanto, $2^{1001} \nmid 1001\times1002\times\cdots\times2000$.

■

1.2 Divisão euclidiana

Se um número natural a não divide o número natural b, Euclides, nos seus *Elementos*, utiliza o fato de que é sempre possível efetuar a divisão de b por a, com resto. Daremos a demonstração deste importante fato abaixo.

Teorema 1.2.1 (Divisão Euclidiana). Sejam a e b dois números naturais com $0<a<b$. Existem dois únicos números naturais q e r tais que $b=a.q+r$, com $0\le r<a$.

Demonstração: Supondo inicialmente que $b>a$ e considere, enquanto fizer sentido, os números do conjunto $S=\{b,\ b-a,\ b-2a,\ ...,\ b-n.a,\ ....\}$. Note que, esse conjunto é finito e todos os seus elementos são distintos. Portanto pelo Princípio da Boa Ordem o conjunto acima tem um menor elemento $r=b-q.a$. Agora, será mostrado que r tem a propriedade requerida, isto é, que $r<a$.

Se $a \mid b$, então $r = 0$, logo $0 = r < a$. Outra hipótese seria $a \nmid b$, então teríamos $r \neq a$, e, portanto, provaremos que não pode ocorrer $r > a$. De fato, se isto ocorresse, existiria um número natural $c < r$ tal que $r = c + a$. Isto implicaria na seguinte igualdade $c + a = b - qa \Rightarrow c = b - (q+1)a$, donde $c \in S$ e com $c < r$. Absurdo, já que r é o menor elemento de S.

Agora, vamos provar a unicidade. Supondo que $b = aq_1 + r_1$ e $b = a.q_2 + r_2$, com $0 \leq r_1 < a$ e $0 \leq r_2 < a$. Podemos supor, sem perda de generalidade, que $r_1 \leq r_2$. Deste modo, tem-se:

$r_1 \leq r_2 \Rightarrow 0 \leq r_1 - r_2 < a$. Por outro lado temos, $aq_1 + r_1 = aq_2 + r_2 \Rightarrow r_1 - r_2 = a(q_2 - q_1)$.

Logo, $0 \leq a(q_2 - q_1) < a \Rightarrow 0 \leq q_2 - q_1 < 1 \Rightarrow q_2 = q_1$, assim $r_2 = r_1$.

Portanto, q e r são únicos tais que $b = a.q + r$, com $0 \leq r < a$.

■

Os naturais q e r são respectivamente o ***quociente*** e o ***resto*** da divisão de b por a.

Corolário 1.2.1 Dados dois números a e b com $1 < a \leq b$, existe um único número natural n tal que $na \leq b < (n+1)a$. De fato,

$$q \leq \frac{b}{a} < q + 1 \Rightarrow q.a \leq b < (q+1).a \Rightarrow qa \leq b < qa + a \Rightarrow 0 \leq b - qa < a$$

por definição $r = b - qa \Rightarrow b = aq + r$. Basta tomar $n = q$.

■

A afirmação no corolário 1.2.1, feita sem demonstração, por Euclides nos *Elementos*, é o que lhe permitia deduzir a divisão euclidiana.

Teorema 1.2.2 (Teorema dos restos) Se b_1 e b_2 deixam restos r_1 e r_2 na divisão por a, respectivamente, então:

i) $b_1 + b_2$ deixa o mesmo resto que $r_1 + r_2$ na divisão por a.

ii) $b_1.b_2$ deixa o mesmo resto que $r_1.r_2$ na divisão por a.

Demonstração:

i) Por hipótese, temos que $b_1 = a.q_1 + r_1$, $b_2 = a.q_2 + r_2$ e supondo que $r_1 + r_2 = a.q + r$.

$b_1 + b_2 = a.q_1 + r_1 + a.q_2 + r_2 = a(q_1 + q_2) + r_1 + r_2 = a(q_1 + q_2 + q) + r$.

ii) Por hipótese, temos que $b_1 = a.q_1 + r_1$, $b_2 = a.q_2 + r_2$ e supondo que $r_1.r_2 = a.q + r$.

$b_1.b_2 = (aq_1 + r_1)(aq_2 + r_2) = a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 = a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + aq + r$

$= a(aq_1 q_2 + q_1 r_2 + q_2 r_1 + q) + r$.

■

Exemplo 1.2.1 Qual o resto que o número $2011 \times 2012 \times 2013 \times 2014$ deixa quando dividido por 5?

Solução: 2011 deixa resto 1 na divisão por 5, assim, 2012, 2013 e 2014 deixam restos 2, 3 e 4 respectivamente na divisão por 5. Pelo teorema 1.2.2, o resto procurado é o mesmo resto de $1 \times 2 \times 3 \times 4 = 24$ por 5. Portanto o resto é 4.

Exemplo 1.2.2 Qual o resto que o número 7^{2014} deixa quando dividido por 6.

Solução: Pelo teorema 1.2.2, 7^{2014} dividido por 6 deixa o mesmo resto que $1^{2014} = 1$. Logo, o resto procurado é 1.

Exemplo 1.2.3 Calcule o resto da divisão de 4^{2014} por 3.

Solução: Note que, $3 \mid 4^{2014} - 1$, pois $4^{2014} - 1 = 3(4^{2013} + 4^{2012} + \cdots + 4 + 1)$.

Isso significa que o resto procurado é 1.

Fixado um número natural $m \geq 2$, podemos escrever um número natural $n \in \mathbb{N}^*$ de modo único, da forma $n = mk + r$, onde $k, r \in \mathbb{N}$ e $r < m$. Por exemplo, todo número natural n pode ser escrito de uma, e somente uma, das seguintes formas: $2k$ ou $2k+1$. O número é chamado de par se for da seguinte forma: $2k$. Caso contrário, ele será chamado de ímpar, e terá a seguinte forma: $2k+1$. Os números naturais são classificados em pares e ímpares, desde Pitágoras, 500 anos antes de Cristo. Pode-se ainda escrever um número natural n apenas de um dos três modos: $3k$, $3k+1$ ou $3k+2$.

Exemplo 1.2.4 Mostre que $3 \mid n^3 + 2n$ para todo $n \in \mathbb{N}$.

Solução: Vamos dividir a solução em três casos.

i) Se n for da forma $3k$.

$(3k)^3 + 2(3k) = 27k^3 + 6k = 3(9k^3 + 2k)$, então $3 \mid n^3 + 2n$.

ii) Se n for da forma $3k+1$.

$(3k+1)^3 + 2(3k+1) = 27k^3 + 27k^2 + 9k + 1 + 6k + 2 = 3(9k^3 + 9k^2 + 5k + 1)$, então $3 \mid n^3 + 2n$.

iii) Se n for da forma $3k+2$.

$(3k+2)^3 + 2(3k+2) = 27k^3 + 54k^2 + 36k + 8 + 6k + 4 = 3(9k^3 + 18k^2 + 14k + 4)$, então $3 \mid n^3 + 2n$.

■

Outra solução: Note que, $n^3 + 2n = n^3 - n + 3n = n(n^2 - 1) + 3n = (n-1)n(n+1) + 3n$, logo $3 \mid (n-1)n(n+1)$, visto que, $n-1$, n, $n+1$ são naturais consecutivos, e um deles é múltiplo de 3, e $3 \mid 3n$. Portanto, $3 \mid n^3 + 2n$.

Exemplo 1.2.5 Um número m é dito um *quadrado* se existe $a \in \mathbb{N}$ tal que $m = a^2$. Mostre que todo quadrado é da forma $4n$ ou $4n+1$.

Solução: Todo número natural a se escreve na forma $4q+r$, com $r \in \{0,1,2,3\}$.

Pelo teorema 1.2.2, basta olhar para os restos dos números $0^2, 1^2, 2^2, 3^2$ na divisão por 4, desta forma, os possíveis restos são 0 ou 1.

Portanto todo quadrado é da forma $4n$ ou $4n+1$.

■

Exemplo 1.2.6 Mostre que o número escrito na base 10 da forma $\underset{n}{11...1}$ (com n algarismos iguais a 1) não pode ser quadrado para $n \geq 2$.

Solução: $\underset{n}{11...1} = 10^{n-1} + 10^{n-2} + \cdots + 10^2 + 10 + 1$

$= 10^2(10^{n-3} + 10^{n-4} + \cdots + 1) + 10 + 1$

$= 100(10^{n-3} + 10^{n-4} + \cdots + 1) + 8 + 3$

$= 4[25(10^{n-3} + 10^{n-4} + \cdots + 1) + 2] + 3$

$= 4n + 3$, com $n = 25(10^{n-3} + 10^{n-4} + \cdots + 1) + 2$.

Como $\underset{n}{11...1}$ é da forma $4n+3$, por isso não pode ser quadrado.

■

De modo geral, nenhum número do sistema decimal da forma $a = \underbrace{ddd...d}_{n}$, com n algarismos iguais a d, é quadrado perfeito para $n \geq 2$.

1.3 O algoritmo de Euclides

1.3.1 *Máximo divisor comum (MDC)*

Sejam a, b naturais ambos não nulos, $mdc(a,b)$ é o maior inteiro positivo d tal que $d \mid a$ e $d \mid b$. Supondo sem perda de generalidade $a \neq 0$. Se $d \mid a$ então $d = |d| \leq |a|$.

Proposição 1.3.1.1 Dados $a, b \in \mathbb{Z}$ não ambos nulos, então existe um único inteiro positivo d com as seguintes propriedades.

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

ii) Se $d' \mid a$ e $d' \mid b$ então $d' \mid d$

iii) Existem $x, y \in \mathbb{Z}$ tais que $d = ax + by$, esse d é o máximo divisor comum de a e b e escreve-se $d = mdc(a,b)$.

Prova:

Seja, por definição, $C = \{n \in \mathbb{N}^*, x, y \in \mathbb{Z} / n = ax + by\}$, observe que $C \neq \varnothing$, de fato, $|a| + |b| \in C$ e $C \subset \mathbb{N}$, pelo *Princípio da Boa Ordenação* C possui um menor elemento. Seja d o menor elemento do conjunto C.

iii) Temos que $d \in C$, logo existem $x_0, y_0 \in \mathbb{Z}$ tais que $d = ax_0 + by_0$.

i) Existem $q, r \in \mathbb{Z}$ com $0 \leq r < d$ tais que $a = qd + r = q(ax_0 + by_0) + r$

$$\Rightarrow r = a - q(ax_0 + by_0)$$

$$\Rightarrow r = a(1 - qx_0) + b(-qy_0)$$

Se $r > 0 \Rightarrow r \in C$, absurdo, já que $r < d$.

Portanto $r = 0$ assim $a = dq$, logo $d \mid a$.

Analogamente, $d \mid b$.

ii) Seja $d' \in \mathbb{Z}$ tal que $d' \mid a$ e $d' \mid b$. Temos então $d' \mid ax_0$ e $d' \mid by_0$

$\Rightarrow d' \mid ax_0 + by_0 = d$.

■

Note que $d' \mid a$ e $d' \mid b$, então $d' \mid d$, como vimos. Logo $d' < |d| = d$. Assim d justifica o nome e é o maior divisor comum de a e b.

(Propriedades do MDC) Considere $a, b, n \in \mathbb{N}$, $mdc(a,b) = d$ e $a < na < b$.

i) $mdc(0,a) = a$,

ii) $mdc(1,a) = 1$,

iii) $mdc(a,a) = a$,

iv) $a \mid b \Leftrightarrow mdc(a,b) = a$,

v) Se $k \neq 0$, $mdc(ka,kb) = kd$,

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

vii) Se $mdc(a,c) = 1$, então $mdc(a,bc) = d$,

viii) (Lema de Euclides) $mdc(a,b) = mdc(a, b - na)$.

As demonstrações das propriedades podem ser encontradas em [5]

Exemplo 1.3.1.1 Determinar o $mdc(4 \times 2014, 2 \times 2014 - 1)$.

Solução: Aplicando o Lema de Euclides sucessivas vezes teremos:

$mdc(4 \times 2014, 2 \times 2014 - 1) = mdc(4 \times 2014 - 2(2 \times 2014 - 1), 2 \times 2014 - 1)$

$= mdc(3, 2 \times 2014 - 1) = mdc(3, 2 \times 2014 - 1 - 3 \times 1342) = mdc(3,1) = 1$.

Exemplo 1.3.1.2 Mostre que, $mdc(n, n+1) = 1, \forall n \in \mathbb{N}$.

Solução: Seja $d = mdc(n, n+1)$, então $d \mid n$ e $d \mid n+1$, logo $d \mid 1$, portanto $d = 1$.

■

1.3.2 *Algoritmo de Euclides: uma ferramenta para descobrir o MDC*

A seguir, será apresentada uma receita prática e importantíssima para simplificar questões relacionadas com MDC. Essa ferramenta determinará o MDC de dois números naturais.

Sejam $a,b \in \mathbb{N}$, sem perda de generalidade, podemos supor que $a < b$.

$b = aq_1 + r_1$, com $0 < r_1 < a$,

$a = r_1q_2 + r_2$, com $0 < r_2 < r_1$,

$r_1 = r_2q_3 + r_3$, com $0 < r_3 < r_2$,

$\vdots$

$r_{n-2} = r_{n-1}q_n + r_n$, com $0 < r_n < r_{n-1}$,

$r_{n-1} = r_nq_{n+1}$.

Então $mdc(a,b) = r_n$

De fato,

$r_n \mid r_{n-1}$

$\Rightarrow r_n \mid r_{n-1}q_n + r_n = r_{n-2}$

$\Rightarrow r_n \mid r_{n-2}q_{n-1} + r_{n-1} = r_{n-3}$

$\vdots$

$\Rightarrow r_n \mid r_3q_4 + r_4 = r_2$

$\Rightarrow r_n \mid r_2q_3 + r_3 = r_1$

$\Rightarrow r_n \mid r_1q_2 + r_2 = a$

$\Rightarrow r_n \mid aq_1 + r_1 = b$ Assim $r_n \mid a$ e $r_n \mid b$.

Por outro lado,

$r_1 = b - aq_1$,

$r_2 = a - r_1 q_2 = a - q_2(b - aq_1) = a(1 + q_1 q_2) + b(-q_2)$

$\vdots$

De modo geral, para cada K, $\exists\ x_k, y_k \in \mathbb{Z}$ com $r_k = ax_k + by_k$,

assim $r_n = ax_n + by_n$. Se $d' \mid a$ e $d' \mid b$, temos então que $d' \mid ax_n$ e $d' \mid by_n$

$\Rightarrow d' \mid ax_n + by_n = r_n$.

$\Rightarrow r_n = mdc(a,b)$

Exemplo 1.3.2.1 Determinar o $mdc(45,12)$

Solução: Aplicando o algoritmo de Euclides, teremos:

$45 = 12.3 + 9$

$12 = 9.1 + 3$

$9 = 3.3$

Então $mdc(45,12) = 3$

Exemplo 1.3.2.2 No planeta W existem apenas dois tipos de notas de dinheiro: \$5 e \$78. É possível pagarmos exatamente \$4 por alguma mercadoria? E se as notas fossem \$3 e \$78?

Solução: 1º Caso: Aplicando o algoritmo de Euclides, teremos:

$78 = 5.25 + 3$

$25 = 3.8 + 1$

$3 = 1.3$, isto nos diz que $mdc(5,78) = 1$, podemos ainda escrever o mdc como combinação linear de 5 e 78. Dessa forma, teremos:

$1 = 78.2 + 5.(-31) \Rightarrow 4 = 78.8 + 5.(-124)$. Portanto, teríamos que dar oito notas de \$78 e receber de troco cento e vinte e quatro notas de \$5 para pagar a quantia de \$4.

2º Caso: Veja que $mdc(3,78) = 3$, deste modo não é possível pagar \$4 visto que o dinheiro pago e recebido (troco) sempre é múltiplo de 3.

Exemplo 1.3.2.3 Prove que, para todo $n \in \mathbb{N}$, é irredutível a fração $\frac{21n+4}{14n+3}$.

Solução: Basta mostrar que $mdc(21n+4, 14n+3) = 1, \forall n \in \mathbb{N}$.

Com efeito, aplicando o algoritmo de Euclides, teremos:

$21n + 4 = 1(14n + 3) + (7n + 1)$

$14n + 3 = 2(7n + 1) + 1$

$7n + 1 = 1(7n + 1)$

Portanto $mdc(21n+4, 14n+3) = 1$.

■

Exemplo 1.3.2.4 Mostre que, $mdc(2^{120} - 1, 2^{100} - 1) = 2^{20} - 1$.

Solução: Aplicando o algoritmo de Euclides, teremos:

$2^{120} - 1 = 2^{20}(2^{100} - 1) + 2^{20} - 1$

$2^{100} - 1 = (2^{20})^5 - 1 = (2^{20} - 1)[(2^{20})^4 + (2^{20})^3 + (2^{20})^2 + 2^{20} + 1]$

Portanto, $mdc(2^{120} - 1, 2^{100} - 1) = 2^{20} - 1$.

■

Exemplo 1.3.2.5 Determinar o máximo divisor comum de $\underbrace{111...111}_{100 vezes}$ e $\underbrace{111...111}_{60 vezes}$.

Solução: Podemos escrever os números na base decimal, ou seja,

$\underbrace{111...111}_{100 vezes} = 10^{99} + 10^{98} + \cdots + 1$ e $\underbrace{111...111}_{60 vezes} = 10^{59} + 10^{58} + \cdots + 1$.

Pelo algoritmo de Euclides,

$$\underbrace{111...111}_{100 vezes} = 10^{99} + 10^{98} + \cdots + 1 = (10^{59} + 10^{58} + \cdots + 1)10^{40} + 10^{39} + 10^{38} + \cdots + 1,$$

$$10^{59} + 10^{58} + \cdots + 1 = (10^{39} + 10^{38} + \cdots + 1)10^{20} + 10^{19} + 10^{18} + \cdots + 1,$$

$$10^{39} + 10^{38} + \cdots + 1 = (10^{19} + 10^{18} + \cdots + 1)10^{20} + 10^{19} + 10^{18} + \cdots + 1,$$

$$10^{19} + 10^{18} + \cdots + 1 = (10^{19} + 10^{18} + \cdots + 1).1 + 0.$$

Portanto, $mdc(\underbrace{111...111}_{100 vezes}, \underbrace{111...111}_{60 vezes}) = 10^{19} + 10^{18} + \cdots + 1 = \underbrace{111...111}_{20 vezes}$.

1.4 Números primos

Definição 1.4.1 Um inteiro $p \geq 2$ é *primo* se os únicos divisores positivos de p são 1 e p. Se um número $q \geq 2$ não é primo, então é dito *composto*. Dois números naturais a e b serão ditos *primos entre si,* ou *coprimos,* ou ainda, *relativamente primos* se $mdc(a,b) = 1$. Dizemos ainda que a fração $\frac{a}{b}$ é irredutível se a e b são relativamente primos. Por exemplo, os números $2,3,5,7,11,13,17,19$ são primos e os números $6,10,25,48,2014$ são compostos.

Proposição 1.4.1.1 Dados p e q primos e um $a \in \mathbb{Z}$ tem-se que:

i) Se $p \mid q$ então $p = q$.

ii) Se $p \nmid a$ então $mdc(a, p) = 1$.

Demonstração:

i) Os possíveis valores para p são 1 e q, já que q é primo. Mas p também é primo, logo segue que $p = q$.

ii) Seja $d = mdc(a, p)$, então $d \mid p$ e $d \mid a$ assim ou $d = 1$ ou $d = p$ já que p é primo. Como $p \nmid a$, tem-se que $d \neq p$. Portando, temos que, $d = 1$.

■

Proposição 1.4.1.2 Seja a, b e c inteiros positivos e suponhamos que a e b são primos entre si.

i) Se b divide o produto ac então b divide c.

ii) Se a e b dividem c então o produto ab divide c.

Demonstração:

i) Se $b \mid ac$ então existe d_1 inteiro tal que $bd_1 = ac$. Pela hipótese $mdc(a,b) = 1$, então existem x e y inteiros tais que $ax + by = 1$. Multiplicando a equação por c, teremos $acx + bcy = c$, assim $bd_1x + bcy = b(d_1x + cy) = c$, então $b \mid c$.

ii) Se $a \mid c$ então existe d_2 inteiro tal que $c = ad_2$, mas $b \mid c = ad_2$ daí $b \mid d_2$ já que $b \nmid a$. Deste modo podemos escrever $d_2 = bd_3$ para algum inteiro. Portanto $c = abd_3$, isso nos diz que $ab \mid c$.

■

Proposição 1.4.1.3 Seja p um número primo, a e b inteiros positivos. Se p divide ab então p divide a ou p divide p.

Demonstração: Se p divide a não há o que fazer. Supondo que p não divide a, então p e a são primos entre si já que qualquer divisor comum a p e a divide p, porém p é primo e seus únicos divisores são 1 e p. Assim tem-se que $mdc(p,a) = 1$ e usando a proposição 1.4.1.3 concluímos que $p \mid b$

■

Proposição 1.4.1.4 Seja n é um número natural tal que $n \geq 2$. Se d é o menor divisor maior que 1 de n, então d é primo.

Demonstração: Suponha que d é composto e ainda é o menor divisor de n. Assim, existe $a, q \in \mathbb{N}$ tal que $1 < a \leq q < d$ com $d = aq$ isso nos diz que $a \mid d$. Como $d \mid n$ então $a \mid n$, absurdo, já que d é o menor divisor de n.

■

Proposição 1.4.1.5 Todo número composto $a > 1$, admite um número primo p tal que $p^2 \leq a$.

Demonstração: Como a é composto então existe $p, q \in \mathbb{N}$ com $a = pq$, onde $1 < p \leq q < a$. Daí, $p \leq q \Rightarrow p^2 \leq pq = a$.

■

Exemplo 1.4.1 O número 101 é primo ou composto?

Solução: Inicialmente, veja que $101 > 10^2$. Se 101 é composto então existe um primo menor que 10 que é divisor de 101. Logo, os possíveis primos são 2, 3, 5 e 7, mas nenhum deste é divisor de 101. Portanto 101 é primo.

O crivo de Eratóstenes

Eratóstenes foi diretor da famosa biblioteca de Alexandria. No século III A.C., ele elaborou um método para determinar todos os primos e também os fatores primos dos números compostos menores que certo número n. Esse método é conhecido como o *Crivo de Eratóstenes.* Eis a descrição do crivo de Eratóstenes:

1º passo: escrevem-se a partir do número 2 todos os inteiros até n;

2º passo: elimina-se todos os múltiplos de 2, superiores a 2. Passa para 3 que é próximo número primo;

3º passo: elimina-se todos os múltiplos de 3, superiores a 3. Passa para 5 que é próximo número primo;

4º passo: elimina-se todos os múltiplos de 5, superiores a 5. Passa para 7 que é próximo número primo;

O processo continua, até chegar à última etapa, que é:

p-ésimo passo: elimina-se todos os múltiplos do menor inteiro p ainda não eliminado e que são maiores do que p.

Conclusão: Todos os números que não foram eliminados são os primos menores ou iguais a n.

Exemplo 1.4.2 Determinar todos os primos menores ou iguais a 101 usando o crivo de Eratóstenes.

Seguindo os passos mencionados acima, teremos:

2	**3**	4	**5**	6	**7**	8	9	10	**11**
12	**13**	14	15	16	**17**	18	**19**	20	21
22	**23**	24	25	26	27	28	**29**	30	**31**
32	33	34	35	36	**37**	38	39	40	**41**
42	**43**	44	45	46	**47**	48	49	50	51
52	**53**	54	55	56	57	58	**59**	60	**61**
62	63	64	65	66	**67**	68	69	70	**71**
72	**73**	74	75	76	77	78	**79**	80	81
82	**83**	84	85	86	87	88	**89**	90	91
92	93	94	95	96	**97**	98	99	100	**101**

Onde os números sublinhados são os que foram eliminados com o crivo de Eratóstenes.

Assim os números primos menores ou iguais a 101 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97 e 101.

Exemplo 1.4.3 Mostre que $n = 2^{100} - 25$ é composto.

Solução: Veja que $n = 2^{100} - 25 = (2^{50})^2 - 5^2 = (2^{50} + 5)(2^{50} - 5)$, logo é composto porque pode ser escrito como um produto.

■

Proposição 1.4.1 Dois números naturais a e b são *primos entre si* se, e somente se, existem números naturais m e n tais que $am-bn=1$.

Demonstração:

($\Rightarrow$) Suponha que a e b são primos entre si. Então $mdc(a,b)=1$ daí existe $x,y\in\mathbb{Z}$ tais que $ax+by=1$, basta fazer $x=m$ e $-y=n$.

($\Leftarrow$) Suponha que existem naturais m e n tais que $am-bn=1$. Se $d=mdc(a,b)$, então $d\,|\,am-bn$, o que mostra que $d\,|\,1$. Portanto $d=1$

■

Proposição 1.4.2 Sejam $a,b,p\in\mathbb{N}^*$, com p primo. Se $p\,|\,ab$ então $p\,|\,a$ ou $p\,|\,b$.

Demonstração: Basta mostrar que se, $p\,|\,ab$ e $p\nmid a$ então $p\,|\,b$. De fato, como $p\,|\,ab$, então existe $q\in\mathbb{N}$ tal que $ab=pq$. Se $p\nmid a$ então $mdc(p,a)=1$, pela proposição 1.4.1 existem $m,n\in\mathbb{N}$ tal que $pm-an=1$. Multiplicando ambos os membros por b temos que $b=bpm-ban=pbm-pqn=p(bm-qn)$ e, portanto $p\,|\,b$.

■

Exemplo 1.4.4 Mostre que, existe um bloco com 2014 números inteiros positivos consecutivos com nenhum número primo.

Solução: De fato, a sequência dada por $a_1,a_2,...,a_{2014}$ satisfaz a condição do enunciado, onde:

$$a_1=2015!+2=2\left(\frac{2015!}{2}+1\right)$$

$$a_2=2015!+3=3\left(\frac{2015!}{3}+1\right)$$

$$a_3=2015!+4=4\left(\frac{2015!}{4}+1\right)$$

$$\vdots$$

$$a_{2014}=2015!+2015=2015(2014!+1)$$

■

De modo geral podemos encontrar um bloco $a_1, a_2, ..., a_n$ com n inteiros consecutivos com nenhum primo. Basta pegar a sequência com a seguinte característica:

$a_1 = (n+1)!+2$, $a_2 = (n+1)!+3$, ... , $a_n = (n+1)!+(n+1)$

Teorema 1.4.1 (Teorema Fundamental da Aritmética) Todo número natural $n > 1$ pode ser escrito de maneira única – a menos da ordem dos fatores – como o produto de um número finito de primos, não necessariamente distintos.

Demonstração: Usaremos o segundo Princípio da Indução Finita.

1º passo: $n = 2$, nada temos a fazer já que 2 é primo

2º passo: por hipótese, suponha que todo número n, no intervalo, $2 \le n < m$ é escrito como um produto finito de primos.

3º passo: se m for primo, acaba por aqui. Se m não é primo, então existem a e b tais que $m = ab$, com $1 < a \le b < m$ sem perca de generalidade. Por hipótese de indução $a = p_1.p_2.....p_k$ e $b = q_1.q_2.....q_l$, com $k, l \ge 1$ e $p_1, p_2, \ldots, p_k, q_1, q_2, \ldots, q_l$ primos. Deste modo $m = ab = p_1.p_2.....p_k.q_1.q_2.....q_l$, que também é um produto finito de números primos.

■

Teorema 1.4.2 O conjunto dos números primos é infinito.

Demonstração: Suponha que a sequência $p_1 = 2$, $p_2 = 3, ..., p_n$ dos n números primos seja finita. Fazendo $P = p_1.p_2.....p_n + 1$ e seja p um número primo que divide P. Temos que $p \notin \{p_1, p_2, ..., p_n\}$, porque então ele dividiria a diferença $P - p_1.p_2.....p_n = 1$, o que é impossível. Assim p é um número primo que não pertence à sequência e, por consequência, $p_1, p_2, ..., p_n$ não podem formar o conjunto de todos os números primos.

■

1.5 Congruência

Definição 1.5.1 Dizemos que os inteiros a e b são congruentes módulo m se eles deixam o mesmo resto quando divididos por m. Sendo denotado por $a \equiv b \bmod m$. Em outras palavras $a \equiv b \bmod m \Leftrightarrow m \mid a-b \Leftrightarrow \frac{a-b}{m} \in \mathbb{Z}$. Quando a relação $a \equiv b \bmod m$ for falsa, diremos que a e b não são congruentes módulo m. Neste caso, escrevemos $a \not\equiv b \bmod m$.

Teorema 1.5.1 Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então:

i) $a+c \equiv b+d \bmod m$

ii) $a-c \equiv b-d \bmod m$

iii) $ka \equiv kb \bmod m$

iv) $ac \equiv bd \bmod m$

v) $a^k \equiv b^k \bmod m$

Demonstração: Inicialmente temos que $m \mid b-a$ e $m \mid d-c$

i) $m \mid (b-a)+(d-c) = (b+d)-(a+c) \Rightarrow a+c \equiv b+d \bmod m$

ii) $m \mid (b-a)-(d-c) = (b-d)-(a-c) \Rightarrow a-c \equiv b-d \bmod m$

iii) $m \mid b-a \Rightarrow m \mid kb-ka \Rightarrow ka \equiv kb \bmod m$

iv) $n \mid b(d-c)+c(b-a) = bd-bc+bc-ac = bd-ac \Rightarrow ac \equiv bd \bmod m$

v) Usaremos o Princípio da Indução Finita sobre k.

1º passo: $a \equiv b \bmod m$.

2º passo: Por hipótese $a^k \equiv b^k \bmod m$.

3º passo: $a^{k+1} = a.a^k \equiv b^k.b = b^{k+1} \bmod m$.

Portanto, $a^k \equiv b^k \bmod m$, $k \in \mathbb{N}$.

■

Exemplo 1.5.1 Calcule o resto da divisão de 4^{100} por 7

Solução: Veja que $4^3 \equiv 1 \bmod 7$

$\Rightarrow \left(4^3\right)^{33} \equiv 1^{33} \bmod 7 \Rightarrow 4^{99} \equiv 1 \bmod 7$

$\Rightarrow 4^{99} \times 4 \equiv 1 \times 4 \bmod 7 \Rightarrow 4^{100} \equiv 4 \bmod 7$, logo o resto procurado é 4.

Exemplo 1.5.2 Qual é o resto da divisão de $2^{70} + 3^{70}$ por 13?

Solução: inicialmente, note que, $2^{70} + 3^{70} = 4^{35} + 9^{35}$.

$\Rightarrow 4 + 9 = 13 \equiv 0 \bmod 13 \Rightarrow 9 \equiv -4 \bmod 13$

$\Rightarrow 9^{35} \equiv (-4)^{35} \bmod 13 \Rightarrow 4^{35} + 9^{35} \equiv 4^{35} - 4^{35} \bmod 13$

$\Rightarrow 4^{35} + 9^{35} \equiv 0 \bmod 13$. Isso nos diz que o resto é 0.

Exemplo 1.5.3 Encontre o último dígito do número 1989^{1989}.

Solução: Basta encontra o resto na divisão por 10. Assim,

$1989 \equiv -1 \bmod 10 \Rightarrow 1989^{1989} \equiv (-1)^{1989} \bmod 10$

$\Rightarrow 1989^{1989} \equiv -1 \bmod 10$. Portanto o resto da divisão é 9.

Exemplo 1.5.4 Mostre para todo $n \in \mathbb{N}$ $37 \mid 300\ldots07$ (com $3n$ zeros)

Solução: Temos que $300\ldots07 = 300\ldots00 + 7 = 3 \times 100\ldots00 + 7 = 30 \times 10^{3n} + 7$.

Note que, $1000 = 10^3 \equiv 1 \bmod 37$, daí

$\left(10^3\right)^n = 10^{3n} \equiv 1 \bmod 37 \Rightarrow 30 \times 10^{3n} + 7 \equiv 30 + 7 = 37 \equiv 0 \bmod 37$.

■

Exemplo 1.5.5 Prove que $n^2 + 1$ não é divisível por 3 para nenhum n inteiro.

Solução: Podemos ter três situações:

1ª situação: $n \equiv 0 \bmod 3 \Rightarrow n^2 + 1 \equiv 1 \bmod 3$.

2ª situação: $n \equiv 1 \bmod 3 \Rightarrow n^2 \equiv 1 \bmod 3 \Rightarrow n^2 + 1 \equiv 2 \bmod 3$.

3ª situação: $n \equiv 2 \bmod 3 \Rightarrow n^2 \equiv 1 \bmod 3 \Rightarrow n^2 + 1 \equiv 2 \bmod 3$.

Portanto, 3 não divide $n^2 + 1$.

■

Exemplo 1.5.6 Prove que 24 divide $p^2 - 1$ para todo p primo maior que 3.

Solução: Note que, p é ímpar, assim podemos escrever $p = 2k + 1 \Rightarrow p^2 = 4k^2 + 4k + 1 \Rightarrow p^2 - 1 = 4k(k+1)$, desta forma $p^2 - 1$ é sempre múltiplo de 8, já que $k(k+1)$ é múltiplo de 2.

Veja também que $p \equiv 1 \bmod 3$ ou $p \equiv 2 \bmod 3$.

Se $p \equiv 1 \bmod 3 \Rightarrow p^2 \equiv 1 \bmod 3$, isto nos diz que $p^2 - 1$ é múltiplo de 3. Por outro lado, se $p \equiv 2 \bmod 3 \Rightarrow p^2 \equiv 4 = 1 \bmod 3$, isto nos diz que $p^2 - 1$ é múltiplo de 3.

Portanto, $24 \mid p^2 - 1$.

■

Teorema 1.5.2 (Pequeno Teorema de Fermat). Se p é primo e a é inteiro positivo, então $a^p \equiv a \bmod p$.

Demonstração: Basta mostrar que $p \mid a^p - a$. Supondo que, se queira colocar p pedras numa pulseira, de modo, que a pulseira não tenha todas as pedras da mesma cor. Supondo

ainda que se tenha a cores disponíveis. Deste modo, têm-se a maneiras para escolher a cor da primeira pedra, a maneiras para escolher a cor da segunda pedra, seguindo o raciocínio, têm-se a maneiras para escolher a cor da p-ésima pedra. Devemos retirar todas as pulseiras que têm todas as pedras com a mesma cor, isto é, a pulseiras. Em seguida, devemos dividir por p devido as p rotações possíveis, já que p é primo. Assim $\frac{a^p - a}{p}$ é o número de pulseiras diferentes. Deste modo $\frac{a^p - a}{p} \in \mathbb{N}$, assim $p \mid a^p - a$.

■

Em particular, se $mdc(a, p) = 1$, então $p \mid a^{p-1} - 1$, logo $a^{p-1} \equiv 1 \bmod p$.

Exemplo 1.5.7 Prove que $n^7 \equiv n \bmod 42, \forall n \in \mathbb{N}$.

Prova: Como $42 = 2.3.7$ então basta mostrar que $2 \mid n^7 - n$, $3 \mid n^7 - n$ e $7 \mid n^7 - n$. Aplicando o Pequeno Teorema de Fermat

$2 \mid n^2 - n \Rightarrow 2 \mid (n^2 - n)(n^5 + n^4 + n^3 + n^2 + n + 1) = n^7 - n$,

$3 \mid n^3 - n \Rightarrow 3 \mid (n^3 - n)(n^4 + n^2 + 1) = n^7 - n$, e

$7 \mid n^7 - n$. Assim $42 = 2 \times 3 \times 7 \mid n^7 - n, \forall n \in \mathbb{N}$.

■

Exemplo 1.5.8 Prove que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um inteiro para todo inteiro.

Prova: Veja que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5 + 5n^3 + 7n}{15}$, basta mostra que $3 \mid 3n^5 + 5n^3 + 7n$ e $5 \mid 3n^5 + 5n^3 + 7n, \forall n \in \mathbb{Z}$. Pelo Pequeno Teorema de Fermat

$3 \mid n^3 - n \Rightarrow 3 \mid 5n^3 - 5n \Rightarrow 3 \mid 3n^5 + 5n^3 - 5n + 12n = 3n^5 + 5n^3 + 7n$, e

$5 \mid n^5 - n \Rightarrow 5 \mid 3n^5 - 3n \Rightarrow 3 \mid 3n^5 - 3n + 5n^3 + 10n = 3n^5 + 5n^3 + 7n$.

■

Exemplo 1.5.9 Determine todos os números primos $p \in \mathbb{N}$ tais que $p \mid 3^p + 7$.

Solução: Pelo Pequeno Teorema de Fermat temos que $3^p \equiv 3 \bmod p$, daí $3^p + 7 \equiv 10 \bmod p$. Portanto $p \mid 3^p + 7$ se, e somente se $p \mid 10$. Como p é primo, então $p = 2$ ou $p = 5$.

Exemplo 1.5.10 Ache o resto da divisão de $1^5 + 2^5 + \cdots + 183^5$ por 5.

Solução: Pelo Pequeno Teorema de Fermat temos que $n^5 \equiv n \bmod 5$. Portanto

$1^5 \equiv 1 \bmod 5$, $2^5 \equiv 2 \bmod 5$, $3^5 \equiv 3 \bmod 5$, ..., $183^5 \equiv 183 \bmod 5$, assim

$1^5 + 2^5 + 3^5 \cdots + 183^5 \equiv 1 + 2 + 3 + \cdots + 183 \bmod 5$.

$$1 + 2 + 3 + \cdots + 183 = \frac{(1+183)183}{2} = 92 \times 183 \equiv 2 \times 3 = 6 \equiv 1 \bmod 5.$$

O resto procurado da divisão de $1^5 + 2^5 + \cdots + 183^5$ por 5 é 1.

Teorema 1.5.3 (Teorema Chinês dos Restos) Dado o seguinte sistema de congruências

$$\begin{aligned} x &\equiv c_1 \bmod n_1 \\ x &\equiv c_2 \bmod n_2 \\ &\cdots \\ x &\equiv c_r \bmod n_r \end{aligned}$$

com $mdc(n_i, n_j) = 1$, para todo par n_i, n_j com $i \neq j$, possui uma única solução módulo $N = n_1 n_2 \cdots n_r$. Tal solução é obtida da seguinte maneira: $x = N_1 y_1 c_1 + N_2 y_2 c_2 \cdots + N_r y_r c_r$,

onde $N_i = N/n_i$ e y_i é solução de $N_i y \equiv 1 \bmod n_i$, para todo $i = 1, 2, \ldots, r$. Além disso, se x' é outra solução do mesmo sistema, então $x \equiv x' \bmod n_i$, $\forall i$, $i = 1, 2, \ldots, r$. Os detalhes da demonstração encontram-se em [5, Cap. 11].

O sistema de congruências pode ser interpretado da seguinte maneira: como achar um número que deixa restos específicos quando divididos por uma série de números dados.

Exemplo 1.5.11 O professor pede a um aluno que escolha um número menor do que 1001 e que diga os restos na divisão por 7, 11 e 13. O aluno então diz que o número escolhido deixa resto 2 na divisão por 3, deixa resto 3 na divisão por 7 e resto 5 na divisão por 13. Qual foi o número escolhido pelo aluno?

Solução: O problema é equivalente ao seguinte sistema de congruências:

$$\begin{matrix} x \equiv 2 \bmod 7 \\ x \equiv 3 \bmod 11 \\ x \equiv 5 \bmod 13 \end{matrix} \text{ assim, } \begin{cases} c_1 = 2 \\ c_2 = 3 \\ c_3 = 5 \end{cases}, \begin{cases} N_1 = 11 \times 13 = 143 \\ N_2 = 7 \times 13 = 91 \\ N_3 = 7 \times 11 = 77 \end{cases} \text{ e } \begin{cases} 143y_1 \equiv 3y_1 \equiv 1 \bmod 7 \Rightarrow y_1 = 5 \\ 91y_2 \equiv 3y_2 \equiv 1 \bmod 11 \Rightarrow y_2 = 4 \\ 77y_3 \equiv 12y_3 \equiv 1 \bmod 11 \Rightarrow y_3 = 12 \end{cases}$$

Logo,

$$x = N_1 y_1 c_1 + N_2 y_2 c_2 + N_3 y_3 c_3$$

$$x = 143 \times 5 \times 2 + 91 \times 4 \times 3 + 77 \times 12 \times 5$$

$$x = 1430 + 1092 + 4620$$

$$x = 7142 .$$

Deste modo $7142 \equiv 135 \bmod 1001$, assim a solução geral do sistema de congruências é dado por $x = 135 + 1001k$, com $k \in \mathbb{Z}$. Portanto o número escolhido pelo aluno é 135.

2 CÓDIGOS DE BARRA

Quase todos os dias nós perdemos tempo em filas de supermercados, farmácias, bancos e no comércio em geral; Agora, imagine ir a um supermercado para fazer suas compras e enfrentar as grandes filas sem a rapidez dos códigos de barra, tendo que esperar o operador de caixa digitar cada produto, um a um, seria uma tarefa muito difícil. Imagine também o funcionário desta empresa recebendo mercadorias e digitando uma a uma no estoque, ou colocando manualmente as etiquetas em todos os produtos da loja. Sabemos que, hoje em dia, tudo isso é mais simples, porém, há pouco tempo, vivíamos na época em que as coisas eram assim. Então foi desenvolvido o código de barra para dar conta de tudo isso. Essa

tecnologia mudou a vida dos comerciantes, e foi muito mais além dos mercados e do comércio em geral.

O código de barra revolucionou a forma de identificar e armazenar dados no mundo inteiro. Hoje, basta você passar o produto no *scanner* e já sabe o preço, de onde veio, e quantos existem no estoque, portanto, ficou muito mais fácil encontrar um produto na loja. O código de barra facilitou a vida de muita gente, de quem trabalha no comércio, na indústria, e até mesmo do cliente, afinal, economiza tempo e evita erros.

2.1 Desenvolvimento dos códigos de barra

O primeiro código foi patenteado em 1952 por Bernard Silver e Norman Joseph Woodland. O código consistia em várias circunferências concêntricas de cores pretas e brancas e de espessuras diferentes, mas naquela época ainda não existia leitura a laser. Apenas nos anos 70, que George Laurer e dois amigos, que trabalhavam na IBM, desenvolveram o código de barra como conhecemos hoje. O UPC, sigla em inglês para "*Universal Product Code*", que, em português, significa Código de Produto Universal. O código de barra é formado por colunas verticais que podem ser brancas ou pretas. O laser identifica se a coluna reflete alguma luz ou nenhuma. Colunas que refletem luz são representados por 0, já as colunas que não refletem luz são representados por 1. Os números em baixo da barra são divididos em quatro seções e não são lidos pelo *scanner*, entretanto podem ser lidos pelas pessoas, caso necessário. Vejamos o que eles representam: os dois ou três primeiros dígitos representam o país de origem do produto, no caso do Brasil, são três dígitos (789), isto é, todos os produtos fabricados no Brasil começam com esses dígitos e nesta ordem. Logo em seguida, vem a numeração do fabricante, que pode ser quatro ou cinco dígitos, depois vem a numeração do produto, sendo este representado por cinco dígitos, e, por fim, o último número é o dígito de controle, também chamado de dígito verificador, que serve para confirmar se a leitora ótica identificou o código de barra corretamente. Esse dígito de verificação não é escolhido aleatoriamente, muito pelo contrário, ele está bem definido com a escolha dos números que o antecedem, veremos esse fato com detalhes adiante. A tabela 1, disponível em *http://www.barcodeisland.com/ean13.phtml* mostra alguns países e seus dígitos iniciais de identificação.

Tabela 1 – Dígitos iniciais de cada país.

País	Dígitos iniciais
Argentina	779
China	690-692
Espanha	84
França	30-37
Portugal	560

Quando vamos ao supermercado, percebemos inúmeras vezes, que o operador de caixa passa o código de barra em qualquer sentido, isto é, da esquerda para a direita, da direita para a esquerda, e até de cabeça para baixo. E se por algum motivo a leitora ótica não conseguir ler o código de barra, então o que vemos é o operador de caixa digitar o número que está logo abaixo. Você também já viu algumas vezes que se o operador de caixa errar a digitação, a máquina identifica o erro e avisa com o sinal sonoro. Isso evita que o cliente pague por um produto que não estará levando.

Em 1973, o código UPC foi adotado nos Estados Unidos e no Canadá. Inicialmente, o código consistia numa sequência numérica de 12 dígitos; logo depois, vieram novas versões para o UPC, porém com algumas pequenas modificações, tivemos, por exemplo, o UPC-E que continha apenas 8 dígitos. Ainda na década de setenta, mais precisamente em 1976, com a missão de expandir o sistema para uso mundial, Laurer aprimorou seu trabalho. Ele, baseado no UPC-A, criou um novo código adicionando um novo dígito. O novo código, agora com 13 dígitos, foi chamado de EAN (European Article Numbering system). Com esse novo dígito, o código permitiu também identificar o país de origem de cada produto. Vários países adotaram o EAN, porém com outro nome. Por exemplo, no Japão o sistema é conhecido como JAN (Japanese Article Numbering system)

2.2 Como funciona o código de barra

Cada número que aparece abaixo do código de barra corresponde a exatamente quatro barras, duas brancas e duas pretas intercaladas, e mais ainda, essas quatro barras juntas ocupam sempre a mesma área. Vejamos um exemplo: as quatro barras que correspondem ao algarismo 1 ocupam a mesma área que as quatro barras que correspondem ao algarismo 3,

que, por sua vez, ocupam a mesma área das quatro barras referentes a qualquer outro algarismo pertencente ao código da figura 2.1.

Figura 2.1 – Código UPC.

Inicialmente, note que as barras têm espessuras diferentes. Essas espessuras são classificadas como: fina, média, grossa ou muito grossa. Utilizamos 0 (zero) e 1 (um) para representar a cor. A espessura da barra é representada pela quantidade de 0 (zeros) ou 1 (uns). Se a barra for de cor branca representaremos por 0, e da seguinte maneira, 0 para a barra fina, 00 para a barra média, 000 para a barra grossa e 0000 para a barra muito grossa. A barra de cor preta é representada por 1. De modo análogo, teremos 1 para representar a barra fina, 11 para a barra média, 111 para a barra grossa e 1111 para a barra muito grossa.

Agora, representaremos o código de barra da figura 2.1 como sequência de zeros e uns, sem considerar as três barras iniciais (101), cinco centrais (01010) e três finais (101), uma vez que servem apenas de limites, portanto, não serão contadas. Começaremos com o algarismo 1, veja que ele está representado por uma coluna branca média (00), uma coluna preta média (11), outra coluna branca média (00) e uma coluna preta fina (1), assim, o algarismo 1 está representado por 0011001. O próximo será o algarismo 3: a primeira coluna é branca fina (0), a segunda coluna é preta muito grossa (1111), a terceira coluna é branca fina (0), e a quarta e última coluna é preta fina (1), portanto, o algarismo 3 tem essa representação 0111101. Do mesmo modo, o algarismo 5 é representado por 0110001, porém o algarismo 5 que está após as barras centrais tem esta representação 1001110 e o algarismo 1 que também está após as barras centrais tem representação dada por 1100110. Veja que o mesmo dígito é codificado de maneira diferente quando estão em lados diferentes do código de barra, isto é, à direita ou à esquerda das barras centrais.

2.2.1 *Aprendendo a escrever com barra*

A tabela 2 identificará a correspondência dos dígitos com as barras.

Tabela 2 – Correspondência dos dígitos do código UPC.

Dígito	Do lado esquerdo	Do lado direito
0	0001101	1110010
1	0011001	1100110
2	0010011	1101100
3	0111101	1000010
4	0100011	1011100
5	0110001	1001110
6	0101111	1010000
7	0111011	1000100
8	0110111	1001000
9	0001011	1110100

Perceba que a codificação de um número à esquerda é dado pela codificação do mesmo número à direita trocando cada 0 por 1 e cada 1 por 0. Veja, que cada número à esquerda, possui uma quantidade ímpar de dígitos iguais a 1, enquanto cada número à direita possui uma quantidade par de dígitos iguais 1. Portanto, assim que o operador de caixa passar o produto na leitora, automaticamente a máquina leitora verifica a paridade de uns, isto é, se cada número tem em sua representação uma quantidade ímpar ou par de dígitos iguais a 1. Daí, ela sabe de que lado o operador está passando o produto, se é da esquerda para direita ou da direita para a esquerda, e logo faz a leitura sem cometer erros.

Exemplo 2.2.1.1 Representar cada número do código de barra, da figura 2.2 como sequência de sete números entre zeros e uns.

Figura 2.2 – Código UPC.

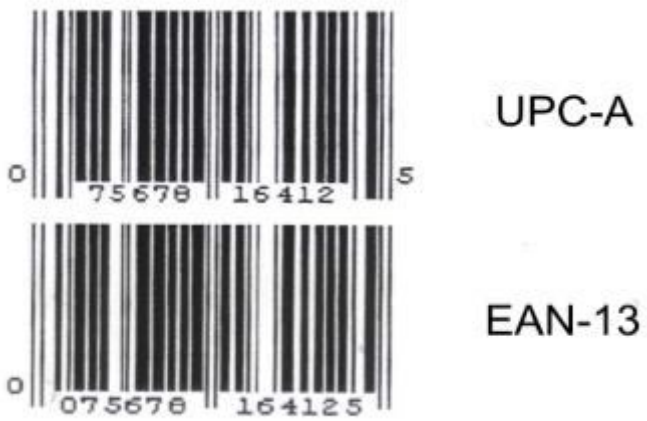
Solução: Primeiramente precisamos identificar quais são os números que estão à esquerda e à direita das barras centrais:

Lado esquerdo: $127035 \Rightarrow 0011001-0010011-0111011-0001101-0111101-0110001$.

Lado direito: $240760 \Rightarrow 1101100-1011100-1110010-1000100-1010000-1110010$.

Na elaboração no EAN, viu-se a necessidade de adicionar um novo dígito, de modo que o novo número indicasse também a origem do produto fabricado. Esse dígito foi escolhido de tal maneira que a mesma leitora pudesse ler o código UPC e o código EAN.

Figura 2.3 – Códigos UPC-A e EAN-13.



Observando as barras dos códigos da figura 2.3, vê-se facilmente que eles são idênticos, porém quando se olha para os números que estão logo abaixo das barras, percebe-se que o EAN-13 é exatamente o código UPC-A acrescentado de um novo dígito, portanto, este novo dígito não é representado através de barras. Estados Unidos e Canadá acrescentaram o dígito 0 ao antigo UPC. Adiante será explicado o motivo do dígito escolhido no UPC-A ser 0. Entretanto, o dígito acrescentado ao código dos outros países, inclusive o Brasil, foi escolhido de tal maneira que dependesse das paridades dos dígitos à esquerda das barras centrais e,

dessa maneira, não seria necessário mudar o tamanho do código de barra. Para que a máquina leitora continuasse a reconhecer o lado, o qual o produto estaria sendo lido, não foi modificada a codificação do lado direito, contudo, a codificação do lado esquerdo passou a variar de acordo com o primeiro dígito. Agora, um dígito qualquer, estando do lado esquerdo, pode ser representado por uma quantidade par ou ímpar de uns, como era antes, de acordo com a tabela 2.

Tabela 3 – Correspondência dos dígitos do código EAN-13.

Dígito	Lado esquerdo ímpar	Lado esquerdo par	Do lado direito
0	0001101	0100111	1110010
1	0011001	0110011	1100110
2	0010011	0011011	1101100
3	0111101	0100001	1000010
4	0100011	0011101	1011100
5	0110001	0111001	1001110
6	0101111	0000101	1010000
7	0111011	0010001	1000100
8	0110111	0001001	1001000
9	0001011	0010111	1110100

Ressaltando que cada algarismo do código de barra corresponde a uma sequência de sete dígitos, entre uns e zeros. Ao iniciar a leitura do lado esquerdo, a máquina analisará a paridade de uns, dos seguintes casos:

1º caso: se a quantidade de uns for ímpar, então segue a tabela 1, que está novamente presente na coluna *lado esquerdo ímpar* da tabela 2.

2º caso: se a quantidade de uns for par, então cada dígito terá uma nova representação, conforme a coluna *lado esquerdo par* da tabela 2. Note que, esta coluna é equivalente ao inverso da coluna *lado direito* da tabela 2.

De acordo com a sequência de paridades encontradas no lado esquerdo do código, determina-se o dígito inicial de acordo com a tabela 3.

Tabela 4 – Critérios para a escolha do primeiro dígito.

Dígito inicial	1º	2º	3º	4º	5º	6º
0	ímpar	Ímpar	ímpar	ímpar	ímpar	ímpar
1	ímpar	Ímpar	par	ímpar	par	par
2	ímpar	Ímpar	par	par	ímpar	par
3	ímpar	Ímpar	par	par	par	ímpar
4	ímpar	Par	ímpar	ímpar	par	par
5	ímpar	Par	par	ímpar	ímpar	par
6	ímpar	Par	par	par	ímpar	ímpar
7	ímpar	Par	ímpar	par	ímpar	par
8	ímpar	Par	ímpar	par	par	ímpar
9	ímpar	Par	par	ímpar	par	ímpar

Exemplo 2.2.1.2 Verificar que o código de barra da figura 2.4 segue a tabela 3.

Figura 2.4 – Código EAN-13.

Solução: Como a sequência inicia-se com o dígito 7, então este não está representado nas barras e é o dígito que está implícito através das paridades dos seis números compreendidos entre as barras iniciais e as barras centrais. Portanto, a sequência de paridades definida para os algarismos do lado esquerdo da barra, de acordo com a tabela 3, será a seguinte: ímpar, par, ímpar, par, ímpar, par.

Seguindo a sequência descrita acima e analisando a tabela 2, isso nos diz que: a paridade do 8 é ímpar, então $8 \mapsto 0110111$; a paridade do 9 é par, então $9 \mapsto 0010111$; a paridade do 8 é ímpar, então $8 \mapsto 0110111$; a paridade do 3 é par $3 \mapsto 0100001$; a paridade do 5 é ímpar, então $5 \mapsto 0110001$; e para finalizar o lado esquerdo teremos, a paridade 7 é par, então $7 \mapsto 0010001$. Do lado direito não foi alterado a codificação, logo, a paridade é

sempre par. Seguindo a tabela 2, teremos: $4 \mapsto 1011100$; $1 \mapsto 1110010$; $7 \mapsto 1000100$; $8 \mapsto 1001000$; $9 \mapsto 1110100$ e por último $2 \mapsto 1101100$.

2.2.2 *Detecção de erros*

Agora, veremos o que acontece quando o operador de caixa digita erroneamente a sequência numérica que está logo abaixo do código de barra. Com toda certeza, já vimos isso acontecer pelo menos uma vez. Mas será que o computador sempre avisa que o operador errou? É o que será analisado a seguir.

Já sabemos que no código EAN-13, os doze primeiros dígitos são fixos e distribuídos da seguinte maneira: os dois ou três primeiros dígitos indicam o país de origem – vale lembrar que o Brasil é 789 –, os dígitos seguintes até as barras centrais indicam a empresa, os cinco primeiros dígitos após as barras centrais são o código do produto – é a empresa fabricante quem os determina – e o último é o dígito verificador, ele é escolhido automaticamente e de maneira única, com a determinação dos doze dígitos iniciais.

Trataremos os treze números do código como um vetor $\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13})$, onde a_{13} é o dígito verificador. O sistema EAN-13 utiliza o vetor $\beta = (1,3,1,3,1,3,1,3,1,3,1,3,1)$, esse vetor é fixo, o que é denominado vetor de pesos. Calculamos o *produto escalar* dos vetores:

$$\alpha.\beta = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$\Rightarrow \alpha.\beta = a_1 + 3a_2 + a_3 + 3a_4 + a_5 + 3a_6 + a_7 + 3a_8 + a_9 + 3a_{10} + a_{11} + 3a_{12} + a_{13}$$

$$\Rightarrow \alpha.\beta = (a_1 + a_3 + a_5 + a_7 + a_9 + a_{11} + a_{13}) + 3(a_2 + a_4 + a_6 + a_8 + a_{10} + a_{12}).$$

Agora, escolheremos o dígito de verificação de modo que o produto escalar seja divisível por 10, usando a linguagem e congruências, isto significa que $\alpha.\beta \equiv 0 mod 10$.

Exemplo 2.2.2.1 Vamos ver como foi determinado o dígito verificador do código de barra da figura 2.4.

Solução: Sabemos que os doze primeiros dígitos são o país de origem, o fabricante, e o código dado pelo fabricante ao produto. São eles: 789835741789. Então,

$\alpha = (7,8,9,8,3,5,7,4,1,7,8,9,a_{13})$ e $\beta = (1,3,1,3,1,3,1,3,1,3,1,3,1)$

Fazendo $\alpha.\beta \equiv 0 \bmod 10$,

$\Rightarrow (7,8,9,8,3,5,7,4,1,7,8,9,a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1) \equiv 0 \bmod 10$

$\Rightarrow 1.7+3.8+1.9+3.8+1.3+3.5+1.7+3.4+1.1+3.7+1.8+3.9+1.a_{13} \equiv 0 \bmod 10$

$\Rightarrow (7+9+3+7+1+8+a_{13})+3(8+8+5+4+7+9) \equiv 0 \bmod 10$

$\Rightarrow 35+a_{13}+123 \equiv 0 \bmod 10$

$\Rightarrow a_{13}+158 \equiv 0 \bmod 10$

$\Rightarrow a_{13} = 2$.

O código UPC possuía doze dígitos, assim como o EAN trabalha módulo 10, e também possui seu vetor de pesos que era $\theta_1 = (3,1,3,1,3,1,3,1,3,1,3,1)$. Mas com a elaboração do EAN, o código UPC ganhou mais um dígito, passando a conter treze dígitos, os quais representaremos por $\mu = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13})$, onde a_{13} é o dígito verificador; com isso, seu vetor de pesos também ganhou mais uma coordenada, passando a ser $\theta_2 = (1,3,1,3,1,3,1,3,1,3,1,3,1)$, isto é, tem as mesmas coordenadas de β.

Nos Estados Unidos e Canadá, foi acrescentado o dígito 0 no início, com isso, o valor do produto escalar não se altera. Daí, a escolha do 0 para ser o primeiro dígito no código UPC-A. Tal resultado proporcionou que uma mesma máquina leitora pudesse ler o código UPC e EAN.

Exemplo 2.2.2.2 Um determinado produto deve ser identificado no sistema UPC pelo número 789490001152. Determine seu dígito verificador.

Solução: Temos que $\mu.\theta_2 \equiv 0 \bmod 10$

$\Rightarrow (7,8,9,4,9,0,0,0,1,1,5,2,a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1) \equiv 0 \bmod 10$

$\Rightarrow (7+9+9+0+1+5+a_{13})+3(8+4+0+0+1+2) \equiv 0 \bmod 10$

$\Rightarrow 31+a_{13}+3.15\equiv 0 \bmod 10$

$\Rightarrow a_{13}+76\equiv 0 \bmod 10$

$\Rightarrow a_{13}=4$

Exemplo 2.2.2.3 Vamos definir um sistema de detecção de erros da seguinte maneira: a cada número de doze dígitos $a_1a_2...a_{12}$, vamos assinalar um dígito de verificação a_{13} de modo que $\sum_{i=1}^{13} a_i \equiv 0 \bmod 10$.

(i) Determinar o dígito de verificação que se deve ser adicionado ao número 723443501297.

Solução: $7+2+3+4+4+3+5+0+1+2+9+7+a_{12}\equiv 0 \bmod 10$

$\Rightarrow 47+a_{12}\equiv 0 \bmod 10$

$\Rightarrow a_{12}=3$

(ii) Mostre que toda vez que apenas um dígito é alterado na digitação, este sistema é capaz de detectar o erro.

Solução: Seja o número $a_1a_2...a_i...a_{12}$, e a_{13} é o dígito de verificação, então $a_1+a_2+...+a_i+...+a_{12}+a_{13}\equiv 0 \bmod 10$. Seja b_i o dígito que substitui a_i na digitação, sem perda de generalidade, podemos escrever $b_i=a_i+c$, onde b_i,a_i,c são dígitos.

Suponha que $a_1+a_2+...+b_i+...+a_{12}+a_{13}\equiv 0 \bmod 10$

$\Rightarrow a_1+a_2+...+(a_i+c)+...+a_{12}+a_{13}\equiv 0 \bmod 10$

$\Rightarrow a_1+a_2+...+a_i+..+a_{12}+a_{13}+c\equiv 0 \bmod 10$

$\Rightarrow c\equiv 0 \bmod 10$

$\Rightarrow 10 \mid c$. Absurdo, já temos que $c<10$.

Logo, o sistema detecta o erro.

■

(*iii*) Mostre que este sistema não é capaz de detectar qualquer erro de transposição.

Solução: Seja o número $a_1a_2...a_j...a_i...a_{12}$, com o erro de transposição, e a_{13} é o dígito de verificação.

Veja que

$$a_1+a_2+...+a_j+...+a_i+...+a_{12}+a_{13}=a_1+a_2+...+a_i+...+a_j+...+a_{12}+a_{13}\equiv 0 \bmod 10.$$

■

Teorema 2.2.2.1 Uma transposição adjacente é detectada pelo EAN-13 e pelo UPC se, e somente se, $|a_i-a_{i+1}|\neq 5$.

Demonstração: Seja o vetor que representa o código $\alpha=(a_1,a_2,...,a_i,a_{i+1},...,a_{12},a_{13})$, sem perda de generalidade, podemos supor que i é par. Então,

$$\alpha.\beta\equiv 0 \bmod 10$$

$$\Rightarrow (a_1,a_2,...,a_i,a_{i+1},...,a_{12},a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1)\equiv 0 \bmod 10$$

$$\Rightarrow a_1+3a_2+...+3a_i+a_{i+1}+...+3a_{12}+a_{13}\equiv 0 \bmod 10. \qquad (i)$$

Este vetor indica como o operador digitou o código $\alpha'=(a_1,a_2,...,a_{i+1},a_i,...,a_{12},a_{13})$, e de modo análogo fazemos $\alpha'.\beta$

$$\Rightarrow \alpha'.\beta=(a_1,a_2,...,a_{i+1},a_i,...,a_{12},a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$\Rightarrow \alpha'.\beta=a_1+3a_2+...+3a_{i+1}+a_i+...+3a_{12}+a_{13}. \qquad (ii)$$

Temos $(i)-(ii)\equiv 0 \bmod 10$

$$\Leftrightarrow (a_1+3a_2+...+3a_i+a_{i+1}+...+3a_{12}+a_{13})-(a_1+3a_2+...+3a_{i+1}+a_i+...+3a_{12}+a_{13})\equiv 0 \bmod 10$$

$$\Leftrightarrow 2(a_i-a_{i+1})\equiv 0 \bmod 10$$

$\Leftrightarrow |a_i - a_{i+1}| = 5$, com $|a_i - a_{i+1}| \leq 9$

Se temos $|a_i - a_{i+1}| \neq 5$ o erro será detectado.

Para i ímpar o procedimento é análogo.

■

Para exemplificar, veremos dois casos de digitação errada como aplicação do teorema 2.1. Certo produto recebeu o seguinte código EAN 7896102514025.

1º Caso: Suponha que o operador de caixa tenha digitado na seguinte ordem, 78<u>69</u>102514025 vejamos o que acontece ao calcular o produto escalar:

$(7,8,6,9,1,0,2,5,1,4,0,2,5).(1,3,1,3,1,3,1,3,1,3,1,3,1)$

$\Rightarrow (7+6+1+2+1+0+5)+3(8+9+0+5+4+2)$

$\Rightarrow 96 \not\equiv 0 \bmod 10$. O sistema detectaria o erro.

2º Caso: suponha, agora, que a sequência digitada é 789<u>16</u>02514025, e novamente, calculamos o produto escalar:

$(7,8,9,1,6,0,2,5,1,4,0,2,5).(1,3,1,3,1,3,1,3,1,3,1,3,1)$

$\Rightarrow (7+9+6+2+1+0+5)+3(8+1+0+5+4+2)$

$\Rightarrow 90 \equiv 0 \bmod 10$. O sistema não detectaria o erro.

Exemplo 2.2.2.4 Mostre que no código EAN-13 e no UPC podem ocorrer 90 erros de transposição adjacente e que o código é capaz de detectar todos eles, exceto quando os pares de números adjacentes são: 05, 16, 27, 38, 49, 50, 61, 72, 83, 94.

Solução: Inicialmente, observa-se que não faz sentido trocar os dígitos se eles forem iguais, logo, os dígitos serão distintos, isto é, $a_i \neq a_{i+1}$. De fato, seja $\alpha = (a_1, a_2, ..., a_i, a_{i+1}, ..., a_{12}, a_{13})$ o vetor que representa determinado produto, podemos escolher o dígito a_i de 10 maneiras, o dígito a_{i+1} de 9 maneiras, e, pelo *Princípio Fundamental da Contagem*, teremos 90

possibilidades. Pelo teorema 2.1 tais erros de transposição adjacente cometido com 05, 16, 27, 38, 49, 50, 61, 72, 83, 94 o sistema não detectaria o erro, pois a sua diferença em módulo é 5.

■

Teorema 2.2.2.2 Um erro de transposição não adjacente da forma $...a_i a_{i+1} a_{i+2}... \rightarrow ...a_{i+2} a_{i+1} a_i...$ não é detectado pelo sistema EAN-13.

Demonstração: Seja o vetor que representa o código $\alpha = (a_1, a_2, ..., a_i, a_{i+1}, a_{i+2}, ..., a_{12}, a_{13})$, sem perda de generalidade, podemos supor que i é par. Então,

$\alpha.\beta \equiv 0 \bmod 10$

$\Rightarrow (a_1, a_2, ..., a_i, a_{i+1}, a_{i+2}..., a_{12}, a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1) \equiv 0 \bmod 10$

$\Rightarrow a_1 + 3a_2 + ... + 3a_i + a_{i+1} + 3a_{i+2} + ... + 3a_{12} + a_{13} \equiv 0 \bmod 10.$

Esse vetor indica como o operador digitou o código $\alpha' = (a_1, a_2, ..., a_{i+2}, a_{i+1}, a_i, ..., a_{12}, a_{13})$, e de modo análogo fazemos o produto escalar $\alpha'.\beta$

$\Rightarrow (a_1, a_2, ..., a_{i+2,} a_{i+1}, a_i, ..., a_{12}, a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1)$

$\Rightarrow a_1 + 3a_2 + ... + 3a_{i+2} + a_{i+1} + 3a_i + ... + 3a_{12} + a_{13} =$

$= a_1 + 3a_2 + ... + 3a_i + a_{i+1} + 3a_{i+2} + ... + 3a_{12} + a_{13} \equiv 0 \bmod 10.$

Portanto, o erro não será detectado.

O procedimento é análogo para i ímpar

■

Teorema 2.2.2.3 Um erro de digitação em que dois dígitos não adjacentes a_i e a_j são trocados, não podem ser detectados pelo sistema EAN-13 se a diferença entre i e j for par.

Demonstração: Veja que no produto escalar de $\alpha = (a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}, a_{13})$ por $\beta = (1,3,1,3,1,3,1,3,1,3,1,3,1)$, os números que têm índice ímpar aparecem multiplicados por 1. Por outro lado, os números que

têm índice par aparecem multiplicados por 3. Se trocarmos os números que têm índices ímpares, os números continuariam a ser multiplicados por 1, e se trocarmos os números que têm índices pares, eles continuariam a ser multiplicados por 3. Portanto, quando a diferença entre i e j for par o erro não é detectado.

■

Teorema 2.2.2.4 Um erro de digitação em que dois dígitos não adjacentes a_i e a_j são trocados, se a diferença $i-j$ é ímpar, então o erro é detectado pelo sistema EAN-13 se, e somente se $|a_i - a_j| \neq 5$.

Demonstração: Se certo produto está identificado no sistema EAN-13 pelo vetor $\alpha = (a_1, a_2, ..., a_i, ..., a_j, ..., a_{12}, a_{13})$. Então, $\alpha.\beta \equiv 0 \bmod 10$, sem perda de generalidade, podemos supor que i é par.

$$\Rightarrow (a_1, a_2, ..., a_i, ..., a_j, ..., a_{12}, a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1) \equiv 0 \bmod 10$$

$$\Rightarrow a_1 + 3a_2 + ... + 3a_i + ... + a_j + ... + 3a_{12} + a_{13} \equiv 0 \bmod 10. \qquad (i)$$

Este vetor indica o produto anterior com a transposição $\alpha' = (a_1, a_2, ..., a_j, ..., a_i, ..., a_{12}, a_{13})$, e de modo análogo façamos $\alpha'.\beta$

$$\Rightarrow \alpha'.\beta = (a_1, a_2, ..., a_j, ..., a_i, ..., a_{12}, a_{13}).(1,3,1,3,1,3,1,3,1,3,1,3,1)$$

$$\Rightarrow \alpha'.\beta = a_1 + 3a_2 + ... + 3a_j + ... + a_i + ... + 3a_{12} + a_{13}. \quad (ii)$$

Temos $(i) - (ii) \equiv 0 \bmod 10$

$$\Leftrightarrow (a_1 + 3a_2 + ... + 3a_i + ... + a_j + ... + 3a_{12} + a_{13}) - (a_1 + 3a_2 + ... + 3a_j + ... + a_i + ... + 3a_{12} + a_{13}) \equiv 0 \bmod 10$$

$$\Leftrightarrow 2(a_i - a_j) \equiv 0 \bmod 10$$

$$\Leftrightarrow |a_i - a_j| = 5, \text{ com } |a_i - a_j| \leq 9$$

Se, $|a_i - a_j| \neq 5$ o erro será detectado.

O processo é análogo quando i for ímpar.

■

A seguir temos a tabela dos erros que mais acontecem.

Tabela 5 – Erros e suas frequências relativas segundo, Verhoeff.

Tipo de erro		Frequência relativa %
Erro único	$a \mapsto b$	79
Transposição adjacente	$ab \mapsto ba$	10.2
Transposição alterna	$abc \mapsto cba$	0.8
Erro gêmeo	$aa \mapsto bb$	0.6
Erro gêmeo alternado	$aba \mapsto cbc$	0.3
Outros		9.1

2.3 O sistema ISBN

O sistema ISBN (International Standard Book Number) foi criado em 1969 para a identificação de livros no mundo inteiro. Isso proporcionou uma linguagem única entre os livros, de modo que, para comprar um livro americano, por exemplo, não seria necessário falar inglês, muito menos saber o nome do autor. Bastaria somente a identificação ISBN do livro e nada mais.

De 1969 até 2006, inclusive, o ISBN era composto por dez dígitos ou por nove dígitos e uma letra, os quais eram conhecidos como ISBN-10. Já a partir no início do ano de 2007, o código passou a ter três dígitos a mais, ficando assim com treze dígitos e, logo, reconhecido como ISBN-13.

Calcula-se o dígito de verificação do ISBN-13 de modo semelhante ao código EAN-13. O dígito de verificação do ISBN-10 é o décimo número contado da esquerda para a direita.

Vejamos agora como é calculado o tal dígito. O ISBN-10 trabalha módulo 11 e o vetor de pesos utilizados é $\beta = (10,9,8,7,6,5,4,3,2,1)$. Assim, o dígito verificador, denominado por a_{10}, é dado de tal maneira que $\alpha.\beta = 0 \bmod 11$. Escolhendo o dígito desse modo, podemos

observar que $a_{10} \in \{0,1,2,3,4,5,6,7,8,9,10\}$. Surge então um inconveniente, a_{10} é um dígito, não podendo assumir valor 10. Por convenção, quando o dígito verificador for 10, será representado por x.

Exemplo 2.3.1 Ache o dígito verificador de um livro em que os nove primeiros dígitos do ISBN-10 são: 85-7056-463.

Solução: $\alpha = (8,5,7,0,5,6,4,6,3,a_{10})$ e $\beta = (10,9,8,7,6,5,4,3,2,1)$,

Temos $\alpha.\beta \equiv 0 \bmod 11$

$\Rightarrow (8,5,7,0,5,6,4,6,3,a_{10}).(10,9,8,7,6,5,4,3,2,1) \equiv 0 \bmod 11$

$\Rightarrow 10.8+9.5+8.7+7.0+6.5+5.6+4.4+3.6+2.3+a_{10} \equiv 0 \bmod 11$

$\Rightarrow 281+a_{10} \equiv 0 \bmod 11$

$\Rightarrow a_{10} = 5$.

Exemplo 2.3.2 Sabendo que os nove primeiros dígitos de um livro no ISBN-10 são: 85-7056-046. Encontre o dígito verificador.

Solução: $\alpha = (8,5,7,0,5,6,0,4,6,a_{10})$ e $\beta = (10,9,8,7,6,5,4,3,2,1)$

Temos $\alpha.\beta \equiv 0 \bmod 11$

$\Rightarrow (8,5,7,0,5,6,0,4,6,a_{10}).(10,9,8,7,6,5,4,3,2,1) \equiv 0 \bmod 11$

$\Rightarrow 10.8+9.5+8.7+7.0+6.5+5.6+4.0+3.4+2.6+a_{10} \equiv 0 \bmod 11$

$\Rightarrow 265+a_{10} \equiv 0 \bmod 11$

$\Rightarrow a_{10} = 10$

$\Rightarrow a_{10} = x$

Teorema 2.3.1 Se na leitura do sistema ISBN-10 acontece um erro singular, então esse erro será detectado.

Demonstração: Seja $\alpha = (a_1, a_2, ..., a_i, ..., a_9, a_{10})$ o código certo do produto no ISBN-10, e $\alpha' = (a_1, a_2, ..., b_i, ..., a_9, a_{10})$ o código após o erro singular, podemos escrever sem perda de generalidade, que $b_i = a_i + c$, onde b_i, a_i, c são dígitos. Sabemos que $(a_1, a_2, ..., a_i, ..., a_9, a_{10}).(10, 9, ..., 2, 1) \equiv 0 \bmod 11$

Usando a contra positiva, suponha que $(a_1, a_2, ..., b_i, ..., a_9, a_{10}).(10, 9, ..., 2, 1) \equiv 0 \bmod 11$

$\Rightarrow 10a_1 + 9a_2 + ... + b_i(11-i) + ... + 2a_9 + a_{10} \equiv 0 \bmod 11$

$\Rightarrow 10a_1 + 9a_2 + ... + (a_i + c)(11-i) + ... + 2a_9 + a_{10} \equiv 0 \bmod 11$

$\Rightarrow 10a_1 + 9a_2 + ... + a_i(11-i) + ... + 2a_9 + a_{10} + c(11-i) \equiv 0 \bmod 11$

$\Rightarrow c(11-i) \equiv 0 \bmod 11$

$\Rightarrow 11 \mid c$ ou $11 \mid (11-i)$. Absurdo, já que $mdc(11, c) = 1$ e $mdc(11, (11-i)) = 1$.

Portanto o erro será detectado.

■

Teorema 2.3.2 Se na leitura do sistema ISBN-10 acontece um erro de transposição, então esse erro será detectado.

Demonstração: Seja $\alpha = (a_1, a_2, ..., a_i, ..., a_j, ..., a_9, a_{10})$ o código certo do produto no ISBN-10, e $\alpha' = (a_1, a_2, ..., a_j, ..., a_i, ..., a_9, a_{10})$ o código após o erro de transposição. Considere $1 \le i < j \le 10$, sabemos que $(a_1, a_2, ..., a_i, ..., a_j, ..., a_9, a_{10}).(10, 9, ..., 2, 1) \equiv 0 \bmod 11$.

$\Rightarrow 10a_1 + 9a_2 + ... + (11-i)a_i + ... + (11-j)a_j + ... + 2a_9 + a_{10} \equiv 0 \bmod 11$

Usando a contra positiva, suponha que $(a_1, a_2, ..., a_j, ..., a_i, ..., a_9, a_{10}).(10, 9, ..., 2, 1) \equiv 0 \bmod 11$

$\Rightarrow 10a_1 + 9a_2 + ... + (11-i)a_j + ... + (11-j)a_i + ... + 2a_9 + a_{10} \equiv 0 \bmod 11$

$\Rightarrow 10a_1 + 9a_2 + ... + (11-j+j-i)a_j + ... + (11-i+i-j)a_i + ... + 2a_9 + a_{10} \equiv 0 \bmod 11$

$$\Rightarrow 10a_1 + 9a_2 + ... + (11-j)a_j + ... + (11-i)a_i + ... + 2a_9 + a_{10} + a_j(j-i) - a_i(j-i) \equiv 0 \bmod 11$$

$$\Rightarrow 10a_1 + 9a_2 + ... + (11-j)a_j + ... + (11-i)a_i + ... + 2a_9 + a_{10} + (a_j - a_i)(j-i) \equiv 0 \bmod 11$$

$$\Rightarrow (a_j - a_i)(j-i) \equiv 0 \bmod 11$$

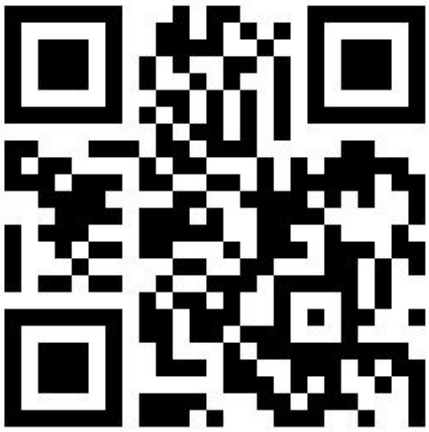
$\Rightarrow 11 \mid (a_j - a_i)$ ou $11 \mid (j-i)$. Absurdo, já que $mdc(11,(a_j - a_i)) = 1$ e $mdc(11,(j-i)) = 1$.

Portanto o erro será detectado.

■

2.4 QR Code

Figura 2.5 – QR Code.



O termo QR deriva de *Quick Response*, que na língua portuguesa significa resposta rápida. Do mesmo modo, *Code* traduzindo para o Português significa código. O QR Code foi desenvolvido no Japão em 1994 pela Denso Wave, uma empresa do grupo Toyota, com a finalidade de identificar peças de carros, assim como, agilizar o processo de logística. Contudo, somente a pouco tempo o QR Code se popularizou e hoje em dia também é usado para transmitir informações rápidas e precisas a dispositivos móveis. Com essa outra finalidade anteriormente citada o QR Code passou a figurar nas embalagens de produtos em supermercados, em placas de carros e principalmente em ações de *marketing*, em particular são encontrados nos *outdoors* e anúncios.

O QR Code é um código de barras bidimensional que contém informações pré-estabelecidas. Essas informações podem ser um texto, imagem, página da internet, vídeo ou número de telefone. Usando a câmera do celular para capturar a imagem através de um aplicativo e ao mesmo tempo um programa específico utiliza o processador para decodificar o conteúdo presente no código.

Se o QR Code está codificando uma mensagem, esta pode ser codificada ou escrita em diferentes unidades de valores. Se a mensagem contiver somente dados numéricos, isto é, somente os dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 este QR Code tem a capacidade de armazenar uma mensagem de 7089 caracteres. Se a mensagem tiver dados alfanuméricos combinados com esses noves caracteres: $ % * + – / : . e o espaço, este QR Code tem a capacidade de armazenar uma mensagem de 4296 caracteres.

OS QUADRADOS

Os quadrados maiores e que estão presentes em três dos quatro cantos servem para facilitar a localização de sua posição, tamanho e inclinação.

O quadrado encontrado próximo ao quarto canto, e um pouco menor que os quadrados dos cantos e maior que os demais quadrados faz o papel de guia de alinhamento para que o código possa ser lido e em seguida processado.

Os quadrados menores são chamados de módulos e representam as informações contidas presentes no código. Os módulos trabalham em conjunto, a cada oito módulos é formado um grupo que é parecido em sua maioria com uma pecinha do jogo Tetris. Cada grupo desses pode ser chamado de *bytes* que pode ser lido ou não pelo sistema que processará o código. Em caso negativo, podemos trocar esses *bytes* por imagens que não altera o funcionamento do código, inclusive muitos usuários usam esses *bytes* para personalizar os seus QR Codes.

A primeira versão do QR Code tem formatação de 21×21 módulos. Contudo, hoje são conhecidas um pouco mais de 40 versões diferentes, sendo que a última tem formatação de 177×177 módulos.

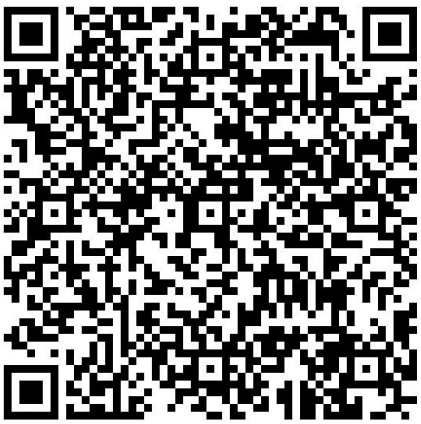
Os QR Codes também são conhecidos pela sua precisão, pois há exatamente 4 níveis de correção de erros que permitem a recuperação de dados. O sistema funciona, dando uma ideia intuitiva de grandezas inversamente proporcionais, da seguinte maneira: quanto menor for o número de caracteres presentes no código melhor será o sistema de detecção de erros. Os níveis são:

- L: com 7% de poder de correção;
- M: com 15% de poder de correção;
- Q: com 25% de poder de correção;
- H: com 30% de poder de correção.

Com essa correção de erro, o QR Code pode ser lido corretamente mesmo estando borrado, sujo ou danificado até o nível de correção de erros, aumentando assim a vida útil código.

Com essas inúmeras vantagens o QR Code vem sendo muito utilizado no mercado publicitário. Além disso, seu uso é livre, logo, qualquer usuário pode gerar seu próprio QR Code e ainda podem ocupar pouquíssimo espaço nos produtos, ficando fácil introduzi-los nos produtos, nas propagandas e onde desejar.

Figura 2.6 – QR Code.



3 CRIPTOGRAFIA

Criptografia é a arte dos códigos secretos. Em grego, *cryptos* significa secreto, oculto. A criptografia estuda as maneiras de codificar uma mensagem de modo que somente o seu destinatário legítimo consiga interpretá-la.

3.1 Outros códigos

3.1.1 *O código de César*

Começaremos com uma pequena ilustração:

Sherlock Holmes recebeu um bilhete de um malfeitor e o estudou por um momento antes de passá-lo para seu amigo Watson.

A mensagem era:
"FV WPV TFRVFUSBS B SBJOIB EB JOHMBUFSSB IPKF B OPJUF. NPSJBSUZ".

- É algum tipo de código! – exclamou Watson – O que significa e de quem é?
Holmes apanhou seu chapéu e seu casaco.
- É de Moriarty, Watson. Rápido, precisamos detê-lo!
- Mas como você descobriu o conteúdo da mensagem?
- Elementar, meu caro Watson. Moriarty utilizou, para cada letra do nosso alfabeto, a função definida por $f(n) = n + 1$ para gerar o código a partir da mensagem original.
- Como assim? O que significa esse n ? Perguntou Watson.
- Ora Watson, n representa a posição de uma letra no nosso alfabeto e $f(n)$ é a letra que a substitui, gerando a mensagem codificada.
Após decifrar o código, Watson percebeu que o terrível crime era uma ameaça de sequestro.

De fato, a mensagem dizia: "EU VOU SEQUESTRAR A RAINHA DA INGLATERRA HOJE A NOITE. MORIARTY".

Uma das primeiras pessoas a criptografar mensagens foi o ditador romano Júlio César (100-44 a.C.). Ele usava esse modelo de criptografia para comunicar-se com suas legiões em combate pelo continente europeu.

A tabela 6 indica a frequência com que as letras do nosso alfabeto aparecem em textos.

Tabela 6 – Frequência das letras no português.

Letra	%	Letra	%	Letra	%	Letra	%
A	14,64	G	1,30	N	5,05	T	4,34
B	1,04	H	1,28	O	10,73	U	4,64
C	3,88	I	6,18	P	2,52	V	1,70
D	4,10	J	0,40	Q	1,20	X	0,21
E	12,57	L	2,78	R	6,53	Z	0,47
F	1,02	M	4,75	S	7,81		

Uma mensagem não curta codificada, de tal maneira em que as letras são substituídas sistematicamente por outras letras (ou símbolos), é muito fácil de ser lida, isto é, o código é fácil de quebrar, visto que a frequência média com que as letras aparecem em determinada língua é mais ou menos constante.

3.1.2 *Código de bloco*

Outra maneira de criptografar uma mensagem é usar o *código de bloco*, que consiste na seguinte receita:

1º passo: verifica-se a paridade de letras da mensagem, e caso a mensagem tenha uma quantidade ímpar de letras então é acrescentado à letra A no final da mensagem. Se a mensagem tiver uma quantidade par de letras, então se inicia a partir do 2º passo;

2º passo: eliminam-se os espaços da mensagem;

3º passo: subdividimos a mensagem em blocos de duas letras;

4º passo: refletimos cada bloco;

5º passo: permutam-se os blocos da seguinte maneira: o primeiro com o último, o terceiro com o antepenúltimo, e assim por diante, mas deixando os outros blocos como estão.

Para exemplificar o que foi dito, codificaremos a seguinte mensagem:

NÚMEROS INTEIROS E CRIPTOGRAFIA RSA.

Inicialmente devemos acrescentar no final mensagem a letra A, já que a ela têm 31 letras. Fazendo também o segundo passo teremos

NUMEROSINTEIROSECRIPTOGRAFIARSAA,

em seguida faz-se o terceiro passo, e obtêm

NU-ME-RO-SI-NT-EI-RO-SE-CR-IP-TO-GR-AF-IA-RS-AA,

fazendo o quarto passo encontraremos

UN-EM-OR-IS-TN-IE-OR-ES-RC-PI-OT-RG-FA-AI-SR-AA,

finalmente aplicaremos o quinto passo para encerrar a codificação

AA-EM-AI-IS-RG-IE-PI-ES-RC-OR-OT-TN-FA-OR-SR-UM,

assim a mensagem codificada será

AAEMAIISRGIEPIESRCOROTTNFAORSRUN.

Veja que tanto o código de César como o código de bloco são fáceis de serem decodificados. Uma vez que se sabe como foi codificado, basta desfazê-la e encontra-se a mensagem original, isto é, decodifica-se a mensagem. Portanto, se um destinatário não legítimo interceptasse a mensagem codificada, ele então, com a posse da receita de codificação, poderia decodificá-la sem muito trabalho, visto que os métodos de criptografia apresentados até aqui são fáceis de fazer e fáceis de desfazer.

3.2 Criptografia RSA

Este código foi inventado em 1977 no *Massachussets Institute of Techology* (M.I.T) por R. L. Rivest, A. Shamir e L. Adleman. Daí letras RSA, que correspondem as iniciais dos inventores do código.

A criptografia RSA é um método de codificação que é fácil de fazer e muito difícil de desfazer caso a pessoa não seja o destinatário legítimo, podendo levar muito tempo para decodificar uma mensagem no sistema RSA. Tanto tempo que uma vida só seria insuficiente para quebrar o RSA.

A receita do RSA

- Escolhemos dois primos p e q, em seguida calculamos o produto $n = p.q$;
- Usaremos n para codificar a mensagem;

- Usaremos p e q para decodificar a mensagem;
- n pode ser tornado público;
- p e q precisam ser mantidos em segredos;
- Quebrar o RSA consiste em fatorar n, que leva muito tempo se n for grande.

3.2.1 *Pré-codificação*

Inicialmente devemos supor que a mensagem original é formada por apenas letras e espaços entre as palavras, isto é, não há nenhum número e nenhum símbolo na mensagem. Em seguida deve-se converter a mensagem numa sequência numérica.

A conversão de letras para números é de acordo com a tabela 7

Tabela 7 – Correspondência das letras com os números.

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Quando estiver ocorrendo à conversão das letras para os números, devemos também converter os espaços entre as palavras, que será representado por 99.

Exemplo 3.2.1.1 Converta a frase *NÚMEROS INTEIROS E CRIPTOGRAFIA RSA* na sequência numérica.
Solução: Usando a tabela 3.2 encontraremos a seguinte sequência numérica
233022142724289918232914182724289914991227182529241627101518109927281O.

Vale lembrar ainda que as letras acentuadas ou não será transformada em um único número. Por exemplo, as letras A, Á, À, Ã, Â serão convertidas no número 10. Note que, se fizéssemos A corresponder ao número 1, B ao 2, C ao 3, D ao 4, e assim por diante, quando aparecesse por exemplo o número 14 teríamos, desta forma, duas escolhas possíveis: AD ou N que é a décima quarta letra do alfabeto. Porém, ao fazer cada letra corresponder a um número com dois dígitos evitará ambiguidades.

Para continuar o processo de pré-codificação é preciso escolher dois números primos distintos p e q, esses primos serão chamados de parâmetros do sistema RSA. Entretanto, precisa-se ainda do produto desses primos escolhidos, o qual denota-se por $n = p.q$. Dando continuidade à pré-codificação, deve-se quebrar em blocos o número encontrado após a conversão de tal maneira que cada bloco seja um número menor que n. A maneira para a escolha dos blocos não é única, mas é importante evitar que os blocos comecem por 0, porque isto traria problemas na decodificação, já que, por exemplo, não temos como diferenciar o bloco 014 do bloco 14.

Exemplo 3.2.1.2 Pré-codifique a frase *Paraty é linda.*

Solução: Inicialmente devemos converter a frase para a sequência numérica, deste modo, tem-se: 25102710293499149921182313 10.

Escolhendo os primos $p = 11$ e $q = 13$, teremos $n = 11 \times 13 = 143$.

Devemos agora quebrar o número em blocos. Assim podemos ter os seguintes blocos

25 – 102 – 7 – 102 – 93 – 49 – 91 – 49 – 92 – 118 – 23 – 13 – 10.

Observe que poderíamos ter escolhidos os blocos assim:

2 – 5 – 10 – 27 – 102 – 93 – 49 – 91 – 49 – 92 – 118 – 23 – 13 – 10,

ou ainda, 25 – 10 – 27 – 10 – 29 – 34 – 99 – 14 – 99 – 21 – 18 – 23 – 13 – 10.

De fato, a maneira para escolher os blocos não é única.

3.2.2 *Codificação*

Para codificar a mensagem precisamos do produto dos números primos que foi chamado de n e de um número inteiro positivo e tal que $mdc(e, \varphi(\mathrm{n})) = 1$, onde $\varphi(n) = (p-1)(q-1)$. O par (n, e) será a *chave de codificação* do sistema RSA. Além disso, esse par é acessível a qualquer usuário. Pegaremos os blocos da mensagem pré-codificada e o codificaremos, um a um, separadamente. A mensagem codificada será a sequência dos blocos codificados. Depois da codificação os blocos não podem ser reunidos formando um novo número. Caso isso aconteça será impossível decodificar a mensagem.

Chamaremos de $C(b)$ a codificação do bloco b, onde $C(b)$ é o resto da divisão de b^e por n, isto é, $b^e \equiv C(b) \bmod n$. Deste modo, a mensagem formada pelos blocos $b_1 - b_2 - b_3 - \cdots - b_n$ terá a seguinte codificação $C(b_1) - C(b_2) - C(b_3) - \cdots - C(b_n)$.

Exemplo 3.2.2.1 Codifique a frase *AMO A OBMEP*.

Solução: Convertendo a frase para a sequência numérica teremos,

$$10222499109924112221425.$$

Escolhendo os parâmetros $p = 17$ e $q = 23$, teremos $n = 17 \times 23 = 391$. Assim podemos quebrar a sequência numérica, que representa a mensagem, nos seguintes blocos:

$$102 - 224 - 99 - 109 - 92 - 41 - 122 - 142 - 5.$$

Veja que $\varphi(391) = (17-1)(23-1) = 16 \times 22 = 352$, podemos escolher $e = 3$, já que $mdc(3, 352) = 1$. De fato, aplicando o algoritmo de Euclides tem-se que,

$352 = 3 \times 117 + 1$

$117 = 1 \times 117$.

Deste modo, têm-se que:

$$b_1 = 102,\ b_2 = 224,\ b_3 = 99,\ b_4 = 109,\ b_5 = 92,\ b_6 = 41,\ b_7 = 122,\ b_8 = 142 \text{ e } b_9 = 5.$$

Codificando a mensagem bloco por bloco, têm-se que:

$102^3 \equiv 102^2 \times 102 \equiv 238 \times 102 \equiv 24276 \equiv 34 \bmod 391 \Rightarrow C(b_1) = 34$;

$224^3 \equiv 224^2 \times 224 \equiv 128 \times 224 \equiv 28672 \equiv 129 \bmod 391 \Rightarrow C(b_2) = 129$;

$99^3 \equiv 99^2 \times 99 \equiv 26 \times 99 \equiv 2574 \equiv 228 \bmod 391 \Rightarrow C(b_3) = 228$;

$109^3 \equiv 109^2 \times 109 \equiv 151 \times 109 \equiv 16459 \equiv 37 \bmod 391 \Rightarrow C(b_4) = 37$;

$92^3 \equiv 92^2 \times 92 \equiv 253 \times 92 \equiv 23276 \equiv 202 \bmod 391 \Rightarrow C(b_5) = 202$;

$41^3 \equiv 41^2 \times 41 \equiv 117 \times 41 \equiv 4797 \equiv 105 \bmod 391 \Rightarrow C(b_6) = 105$;

$122^3 \equiv 122^2 \times 122 \equiv 26 \times 122 \equiv 3172 \equiv 44 \bmod 391 \Rightarrow C(b_7) = 44$;

$142^3 \equiv 142^2 \times 142 \equiv 223 \times 142 \equiv 31666 \equiv 386 \bmod 391 \Rightarrow C(b_8) = 386$;

$5^3 \equiv 125 \bmod 391 \Rightarrow C(b_9) = 125$.

Portanto a mensagem codificada será:

$$34 - 129 - 228 - 37 - 207 - 105 - 44 - 386 - 125.$$

3.2.3 *Decodificação*

Aprenderemos agora a decodificar os blocos, isto é, reconstruir o bloco original a partir dos blocos codificados. Para conseguir tal feito precisa-se dos números n e d para o processo de decodificação, onde n é o produto dos primos escolhidos e d é o inverso de e em $\varphi(\mathrm{n})$, ou seja, $ed \equiv 1 \bmod \varphi(n)$. O par (n,d) é chamado de *chave de decodificação.*

Seja a um bloco da mensagem codificada, chamaremos por $\mathrm{D}(a)$ a decodificação do bloco a, onde $\mathrm{D}(a)$ é o resto da divisão de a^d por n, isto é, $a^d \equiv \mathrm{D}(a) \bmod n$. Deste modo, a mensagem codificada formada pelos blocos $C(b_1) - C(b_2) - C(b_3) - \cdots - C(b_n)$ terá a seguinte decodificação $D(C(b_1)) - D(C(b_2)) - D(C(b_3)) - \cdots - D(C(b_n))$. Note que se b é um bloco da mensagem original então é de se esperar que $\mathrm{D}(\mathrm{C}(b)) = b$. Assim, ao decodificar os blocos $D(C(b_1)) - D(C(b_2)) - D(C(b_3)) - \cdots - D(C(b_n))$ esperamos encontrar os respectivos blocos $b_1 - b_2 - b_3 - \cdots - b_n$ que correspondem à mensagem original. Caso isso não aconteça, então não faz sentido esse tipo de criptografia.

Exemplo 3.2.3.1 Decodificar os blocos do Exemplo 3.2.2.1.

Solução: De posse da receita de decodificação, aplicaremos nos blocos codificados:

$$34 - 129 - 228 - 37 - 207 - 105 - 44 - 386 - 125.$$

Inicialmente devemos encontrar o valor de d sabendo que $ed \equiv 1 \bmod \varphi(n)$. Nesse caso, temos $e = 3$ e $\varphi(391) = 352$. Aplicando o algoritmo de Euclides, teremos:

$352 = 3 \times 117 + 1$

$1 = 352 + 3 \times (-117)$

$1 = 352 + 3 \times (-117) + 3 \times 352 - 3 \times 352$

Deste modo, $1 = 3 \times 235 - 352 \times 2$, logo $d = 235$.

O primeiro bloco a ser decodificado será 34.

Veja inicialmente que,

$34 \equiv 0 \bmod 17$ e $34 \equiv 11 \bmod 23$.

Logo,

$34^{235} \equiv 0 \bmod 17$

$34^{235} \equiv 11^{235} \equiv (11^{22})^{10}.11^{15} \equiv 11^{15} \equiv 20^5 \equiv 9^2.20 \equiv 10 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 0 \bmod 17 \\ x \equiv 10 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 0 \\ c_2 = 10 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 0 + 17 \times 19 \times 10$

$x = 3230$, mas $3230 \equiv 102 \bmod 391$

Portanto $34^{235} \equiv 102 \bmod 391$.

O próximo bloco a ser decodificado será 129.

Veja que, $129 \equiv 10 \bmod 17$ e $129 \equiv 14 \bmod 23$.

Logo,

$129^{235} \equiv (10^{16})^{14}.10^{11} \equiv 10^{11} \equiv 14^3.10^2 \equiv 7.10^2 \equiv 700 \equiv 3 \bmod 17$,

$129^{235} \equiv 14^{235} \equiv (14^{22})^{10}.14^{15} \equiv 14^{15} \equiv -9^{15} \equiv -16^5 \equiv -1024^2 \equiv -12^2 \equiv -144 \equiv -6 \equiv 17 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 3 \bmod 17 \\ x \equiv 17 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 3 \\ c_2 = 17 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 3 + 17 \times 19 \times 17$

$x = 5698$, mas $5698 \equiv 224 \bmod 391$

Portanto $129^{235} \equiv 224 \bmod 391$.

Em seguida decodificaremos o bloco 228.

Note que, $228 \equiv 7 \bmod 17$ e $228 \equiv 21 \bmod 23$.

Logo,

$228^{235} \equiv 7^{235} \equiv (7^{16})^{14}.7^{11} \equiv 7^{11} \equiv 49^5.7 \equiv -2^5.7 \equiv -224 \equiv 14 \bmod 17$,

$228^{235} \equiv 21^{235} \equiv (21^{22})^{10}.21^{15} \equiv 21^{15} \equiv -2^{15} \equiv -16 \equiv 7 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{cases} x \equiv 14 \bmod 17 \\ x \equiv 7 \bmod 23 \end{cases}$ deste modo, $\begin{cases} c_1 = 14 \\ c_2 = 7 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 14 + 17 \times 19 \times 7$

$x = 3227$, mas $3227 \equiv 99 \bmod 391$

Portanto $228^{235} \equiv 99 \bmod 391$.

Agora decodificaremos o bloco 37.

Perceba que, $37 \equiv 3 \bmod 17$ e $37 \equiv 14 \bmod 23$.

Logo,

$37^{235} \equiv 3^{235} \equiv (3^{16})^{14}.3^{11} \equiv 3^{11} \equiv 5^2.3 \equiv 75 \equiv 7 \bmod 17$,

$37^{235} \equiv 14^{235} \equiv (14^{22})^{10}.14^{15} \equiv 14^{15} \equiv 7^5 \equiv 3^2.7 \equiv 63 \equiv 17 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{cases} x \equiv 7 \bmod 17 \\ x \equiv 17 \bmod 23 \end{cases}$ deste modo, $\begin{cases} c_1 = 7 \\ c_2 = 17 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 7 + 17 \times 19 \times 17$

$x = 5974$, mas $5974 \equiv 109 \bmod 391$

Portanto $37^{235} \equiv 109 \bmod 391$.

O próximo bloco a ser decodificado será 207.

Veja que, $207 \equiv 3 \bmod 17$ e $207 \equiv 0 \bmod 23$.

Logo,

$207^{235} \equiv 3^{235} \equiv (3^{16})^{14}.3^{11} \equiv 3^{11} \equiv 5^2.3 \equiv 75 \equiv 7 \bmod 17$,

$207^{235} \equiv 0 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{cases} x \equiv 7 \bmod 17 \\ x \equiv 0 \bmod 23 \end{cases}$ deste modo, $\begin{cases} c_1 = 7 \\ c_2 = 0 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 7 + 17 \times 19 \times 0$

$x = 483$, mas $483 \equiv 92 \bmod 391$

Portanto $207^{235} \equiv 92 \bmod 391$.

Agora decodificaremos o bloco 105.

Perceba que, $105 \equiv 3 \bmod 17$ e $105 \equiv 13 \bmod 23$.

Logo,

$105^{235} \equiv 3^{235} \equiv (3^{16})^{14}.3^{11} \equiv 3^{11} \equiv 5^2.3 \equiv 75 \equiv 7 \bmod 17$,

$105^{235} \equiv 13^{235} \equiv (13^{22})^{10}.13^{15} \equiv 13^{15} \equiv 12^5 \equiv 3^5.2^{10} \equiv 13.12 \equiv 156 \equiv 18 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 7 \bmod 17 \\ x \equiv 18 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 7 \\ c_2 = 18 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 7 + 17 \times 19 \times 18$

$x = 6297$, mas $6297 \equiv 41 \bmod 391$

Portanto $105^{235} \equiv 41 \bmod 391$.

O próximo bloco a ser decodificado será 44.

Note que, $44 \equiv 10 \bmod 17$ e $44 \equiv 21 \bmod 23$.

Logo,

$44^{235} \equiv 10^{235} \equiv (10^{16})^{14}.10^{11} \equiv 10^{11} \equiv 14^3.10^2 \equiv 7.10^2 \equiv 700 \equiv 3 \bmod 17$,

$44^{235} \equiv 21^{235} \equiv (21^{22})^{10}.21^{15} \equiv 21^{15} \equiv -2^{15} \equiv -16 \equiv 7 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 3 \bmod 17 \\ x \equiv 7 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 3 \\ c_2 = 7 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 3 + 17 \times 19 \times 7$

$x = 2468$, mas $2468 \equiv 122 \bmod 391$

Portanto $44^{235} \equiv 122 \bmod 391$.

O penúltimo bloco a ser decodificado será 386.

Note que, $386 \equiv 12 \bmod 17$ e $386 \equiv 18 \bmod 23$.

Logo,

$386^{235} \equiv 12^{235} \equiv (12^{16})^{14}.12^{11} \equiv 12^{11} \equiv 12.8^5 \equiv 6.2^{16} \equiv 6 \bmod 17$,

$368^{235} \equiv 18^{235} \equiv (18^{22})^{10}.18^{15} \equiv 18^{15} \equiv 13^5 \equiv 8^2.13 \equiv 832 \equiv 4 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 6 \bmod 17 \\ x \equiv 4 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 6 \\ c_2 = 4 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 6 + 17 \times 19 \times 4$

$x = 1706$, mas $1706 \equiv 142 \bmod 391$

Portanto $368^{235} \equiv 142 \bmod 391$.

O último bloco a ser decodificado será 125.

Note que, $125 \equiv 6 \bmod 17$ e $125 \equiv 10 \bmod 23$.

Logo,

$125^{235} \equiv 6^{235} \equiv (6^{16})^{14}.6^{11} \equiv 6^{11} \equiv (6^2)^5.6 \equiv 2^5.6 \equiv 192 \equiv 5 \bmod 17$,

$125^{235} \equiv 10^{235} \equiv (10^{22})^{10}.10^{15} \equiv 10^{15} \equiv (10^2)^7.10 \equiv 8^7.10 \equiv 2^{22}.5 \equiv 5 \bmod 23$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 5 \bmod 17 \\ x \equiv 5 \bmod 23 \end{matrix}$ deste modo, $\begin{cases} c_1 = 5 \\ c_2 = 5 \end{cases}$, $\begin{cases} N_1 = 23 \\ N_2 = 17 \end{cases}$ e $\begin{cases} 23y_1 \equiv 1 \bmod 17 \Rightarrow y_1 = 3 \\ 17y_2 \equiv 1 \bmod 23 \Rightarrow y_2 = 19 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 23 \times 3 \times 5 + 17 \times 19 \times 5$

$x = 1960$, mas $1960 \equiv 5 \bmod 391$

Portanto $125^{235} \equiv 5 \bmod 391$.

Portanto, os blocos codificados

34 – 129 – 228 – 37 – 207 – 105 – 44 – 386 – 125

correspondem ao seguintes blocos, após a decodificação,

102 – 224 – 99 – 109 – 92 – 41 – 122 – 142 – 5.

Teorema 3.2.3.1 Se b é um bloco da mensagem original, com $1 \le b < n$, e $C(b)$ é um bloco codificado, então $DC(b) = b$.

Demonstração: Sabemos que $C(b)$ é o resto da divisão de b^e por n e D(a) é o resto da divisão de a^d por n, e que $n = pq$. Além disso, temos que $ed \equiv 1 \bmod n$, daí existe $k \in \mathbb{N}$ tal que $ed = 1 + k\varphi(n)$, pois e, d e $\varphi(n)$ são todos naturais maiores que 2, com $\varphi(n) = (\mathrm{p}-1)(\mathrm{q}-1)$.

Pela definição,

$DC(b) \equiv D(C(\mathrm{b})) \equiv [C(b)]^d \equiv (b^e)^d \equiv \mathrm{b}^{ed} \equiv b^{1+k\varphi(n)} \equiv b.b^{k(p-1)(q-1)} \bmod n$.

Se $p \nmid b$ então, pelo pequeno teorema de Fermat,

$DC(b) \equiv b.b^{k(p-1)(q-1)} \equiv b.(b^{p-1})^{k(q-1)} \equiv b \bmod p$.

Se $p \mid b$ então, $b \equiv 0 \bmod p$, daí $DC(b) \equiv b^{ed} \equiv b \bmod p$.

Do mesmo modo, podemos provar que $DC(b) \equiv b^{ed} \equiv b \bmod q$.

Isso nos diz que, $p \mid b^{ed} - b$ e $q \mid b^{ed} - b$. Como p e q são primos entre si, então $n = pq \mid b^{ed} - b$, isto é, $DC(b) \equiv b^{ed} \equiv b \bmod n$.

Portanto $DC(b) = b$, já que, tanto $DC(b)$ quanto b pertencem ao intervalo $1 \le b < n$, logo só podem ser congruentes módulo n se são iguais.

■

Era de se esperar que ao decodificar os blocos codificados tenhamos de volta os blocos que correspondem à mensagem original, isto é, os blocos pré-codificados. De fato, isso sempre acontece. Além disso, é muito difícil quebrar um código do RSA visto que para conseguir tal feito precisaríamos encontrar os valores de p e q. Em seguida, com posse p e q acharíamos $\varphi(n)$. Depois com posse de $\varphi(n)$ descobriríamos o valor de d que juntamente com n formam a chave de decodificação. A dificuldade de fatorar n é que hoje, nas aplicações comerciais do RSA, n possui no mínimo 200 algarismos, e podem chegar a ter 2467 algarismos. Além disso, hoje não são conhecidos algoritmos rápidos de fatoração para números desse porte. Na verdade, nem sabemos se existem tais algoritmos.

Entretanto, se n e $\varphi(n)$ são conhecidos de qualquer pessoa então será fácil encontrar p e q. De fato, sabemos que $n = pq$ e $\varphi(n) = (p-1)(q-1)$. Desenvolvendo

$\varphi(n)=(p-1)(q-1)=pq-(p+q)+1$ encontraremos a seguinte relação $p+q=n-\varphi(n)+1$. Ou seja, encontraremos o valor numérico de $p+q$.

Além disso $(p+q)^2=p^2+2pq+q^2=p^2-2pq+q^2+4n=(p-q)^2+4n$. Assim, temos outra relação, dada por $p-q=\sqrt{(p+q)^2-4n}$. Isto é, encontraremos o valor numérico de $p-q$.

De posse dos valores numéricos de $p+q$ e $p-q$, basta resolver um simples sistema linear para encontrar os valores de p e q.

Exemplo 3.2.3.2 Sabendo-se que $n=3552377$ é igual ao produto de dois números primos e que $\varphi(n)=3548580$. Determine os parâmetros do RSA.

Solução: Basta achar os valores dos primos p e q. Sabe-se que, $p+q=n-\varphi(n)+1$ e $p-q=\sqrt{(p+q)^2-4n}$.

Substituindo os valores encontraremos o seguinte sistema:

$\begin{cases} p+q=3798 \\ p-q=464 \end{cases}$ Daí, conclui-se que $p=2131$ e $q=1667$.

Exemplo 3.2.3.3 A chave pública utilizada pelo Banco de Toulouse para codificar suas mensagens é a seguinte: $n=10403$ e $e=8743$. Recentemente os computadores do banco receberam, de local indeterminado, a seguinte mensagem:

$$4746-8214-9372-9009-4453-8198.$$

O que diz a mensagem mandada ao Banco de Toulouse?

Solução: É claro que o banco conhece os primos escolhidos, ou seja, $p=101$ e $q=103$. De fato, $101\times103=10403$, assim $\varphi(10403)=100\times102=10200$. Encontraremos o valor de d, já que devemos encontrar o resto da divisão de a^d por n, onde a é o bloco codificado.

Aplicando o algoritmo de Euclides para achar o valor de d.

$10200=8743+1457$

$8743=6\times1457+1$

Deste modo, $1=7\times8743-6\times10200$, logo $d=7$.

Decodificaremos os blocos de duas maneiras

O primeiro bloco a ser decodificado será 4746.

Veja que, $4746\equiv100\bmod101$ e $4746\equiv8\bmod103$.

Logo,

$4746^7 \equiv 100^7 \equiv (100^2)^3.100 \equiv 100 \bmod 101$,

$4746^7 \equiv 8^7 \equiv 2^{21} \equiv 25^3 \equiv 15625 \equiv 72 \bmod 103$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 100 \bmod 101 \\ x \equiv 72 \bmod 103 \end{matrix}$ deste modo, $\begin{cases} c_1 = 100 \\ c_2 = 72 \end{cases}$, $\begin{cases} N_1 = 103 \\ N_2 = 101 \end{cases}$ e $\begin{cases} 103y_1 \equiv 1 \bmod 101 \Rightarrow y_1 = 51 \\ 101y_2 \equiv 1 \bmod 103 \Rightarrow y_2 = 51 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 103 \times 51 \times 100 + 101 \times 51 \times 72$

$x = 896172$, mas $896172 \equiv 1514 \bmod 10403$.

Portanto $4746^7 \equiv 1514 \bmod 10403$.

O segundo bloco a ser decodificado será 8214.

Veja que, $8214 \equiv 33 \bmod 101$ e $8214 \equiv 77 \bmod 103$.

Logo,

$8214^7 \equiv 33^7 \equiv 79^2.79.33 \equiv 80.82 \equiv 6560 \equiv 96 \bmod 101$,

$8214^7 \equiv 77^7 \equiv 58^2.58.77 \equiv 68.37 \equiv 2516 \equiv 44 \bmod 103$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 96 \bmod 101 \\ x \equiv 44 \bmod 103 \end{matrix}$ deste modo, $\begin{cases} c_1 = 96 \\ c_2 = 44 \end{cases}$, $\begin{cases} N_1 = 103 \\ N_2 = 101 \end{cases}$ e $\begin{cases} 103y_1 \equiv 1 \bmod 101 \Rightarrow y_1 = 51 \\ 101y_2 \equiv 1 \bmod 103 \Rightarrow y_2 = 51 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 103 \times 51 \times 96 + 101 \times 51 \times 44$

$x = 730932$, mas $730932 \equiv 2722 \bmod 10403$.

Portanto $8214^7 \equiv 2722 \bmod 10403$.

O terceiro bloco a ser decodificado será 9372.

$9372^7 \equiv -1031^7 \equiv -1855^3.1031 \equiv -8035.8756 \equiv -9374 \equiv 1029 \bmod 10403$.

Portanto $9372^7 \equiv 1029 \bmod 10403$.

O quarto bloco a ser decodificado será 9009.

$9009^7 \equiv -1394^7 \equiv -8278^3.1394 \equiv -723.2605 \equiv -472 \equiv 9931 \bmod 10403$.

Portanto $9009^7 \equiv 9931 \bmod 10403$.

O quinto bloco a ser decodificado será 4453.

$4453^7 \equiv 1091^3.4453 \equiv 4339.22 \equiv 1831 \bmod 10403$.

Portanto $4453^7 \equiv 1831 \bmod 10403$.

O sexto bloco a ser decodificado será 8198.

Veja que, $8198 \equiv 17 \bmod 101$ e $8198 \equiv 61 \bmod 103$.

Logo,

$8198^7 \equiv 17^7 \equiv 87^2.87.17 \equiv 95.65 \equiv 6175 \equiv 14 \bmod 101$,

$8198^7 \equiv 61^7 \equiv 13^2.13.61 \equiv 66.72 \equiv 4752 \equiv 14 \bmod 103$.

Usando o algoritmo chinês do resto, teremos que achar a menor solução positiva do sistema:

$\begin{matrix} x \equiv 14 \bmod 101 \\ x \equiv 14 \bmod 103 \end{matrix}$ deste modo, $\begin{cases} c_1 = 14 \\ c_2 = 14 \end{cases}$, $\begin{cases} N_1 = 103 \\ N_2 = 101 \end{cases}$ e $\begin{cases} 103y_1 \equiv 1 \bmod 101 \Rightarrow y_1 = 51 \\ 101y_2 \equiv 1 \bmod 103 \Rightarrow y_2 = 51 \end{cases}$

Assim, $x = N_1 y_1 c_1 + N_2 y_2 c_2$

$x = 103 \times 51 \times 14 + 101 \times 51 \times 14$

$x = 145656$, mas $145656 \equiv 14 \bmod 10403$.

Portanto $8198^7 \equiv 14 \bmod 10403$.

Assim,

mensagem codificada:	4746 – 8214 – 9372 – 9009 – 4453 – 8198,
mensagem decodificada:	1514 – 2722 – 1029 – 9931 – 1831 – 14,
sequência numérica:	1514272210299931183114
mensagem original:	FERMAT VIVE .

Portanto, a mensagem enviada ao banco foi FERMAT VIVE.

Exemplo 3.2.3.4 A mensagem 6355 – 5075 foi codificada pelo método RSA usando a senha $n = 7597$ e $e = 4947$. Além disso, sabe-se que $\varphi(n) = 7420$. Decodifique a mensagem.

Solução: Inicialmente, devemos encontrar o valor de d, onde $ed \equiv 1 \bmod 7420$. Aplicando o algoritmo de Euclides,

$7420 = 4947 + 2473$

$4947 = 2 \times 2473 + 1$,

deste modo, $1 = 3 \times 4947 - 2 \times 7420$, logo $d = 3$.

Decodificando,

$6355^3 \equiv 373.6355 \equiv 2370415 \equiv 151 \bmod 7595$,

$5075^3 \equiv 1795.5075 \equiv 9109625 \equiv 822 \bmod 7595$

Assim,

mensagem codificada: 6355 – 5075,

mensagem decodificada: 151 – 288,

sequência numérica: 151288,

mensagem original: FIM .

Portanto, a mensagem decodificada é FIM.

REFERÊNCIAS

[1] COUTINHO, S. C. *Criptografia*. Rio de Janeiro: Sociedade Brasileira de Matemática. (Programa de Iniciação Científica).

[2] COUTINHO, S. C. *Números inteiros e criptografia RSA*. 2.ed. Rio de Janeiro: Instituto de Matemática Pura e Aplicada. Rio de Janeiro, 2009.

[3] FEITOSA, S. B. *Teoria dos números*: nível 2.[S.1]: Polos Olímpicos de Treinamentos, 2013. Disponível em: <http://poti.impa.br/index.php/material>. Acesso em: 28/02/2014

[4] FEITOSA, S. B.; MOREIRA, C. A. *Teoria dos números*: nível 3.[S.1]: Polos Olímpicos de Treinamentos, 2013. Disponível em: <http://poti.impa.br/index.php/material>. Acesso em: 28/02/2014

[5] HEFEZ, A. *Elementos de aritmética.* 2 ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2005.

[6] MILIES, C. P. *Números*: uma introdução à matemática. 3. ed. 2. reimpr. São Paulo: Editora da Universidade de São Paulo, 2006.

[7] MUNIZ NETO, A. C. *Tópicos de matemática elementar*: teoria dos números. 1.ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

[8] POLCINO MILIES, F. P. *A matemática dos códigos de barras*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2006. (Programa de Iniciação Científica).

[9] RIBENBOIM, P. *Números primos*: mistérios e recordes. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2001.

[10] SHINE, C. Y. *21 aulas de matemática olímpica*. Rio de Janeiro: Sociedade Brasileira de Matemática, 2009.

[11] *http://www.tecmundo.com.br/qr-code/37372-o-que-significa-cada-quadrado-de-um-qr-code-.htm*. Acesso em: 20/04/2014.

[12] *http://www.tecmundo.com.br/imagem/1995-o-que-sao-os-qr-codes-.htm*. Acesso em: 20/04/2014.

[13]*http://revistatecnologiagrafica.com.br/index.php?option=com_content&view=article&id*=2690:o-que-e-e-para-que-serve-o-codigo-qr&catid=60:normalizacao&Itemid=185. Acesso em: 20/04/2014.

APÊNDICE A – CRITÉRIOS DE DIVISIBILIDADE

Apresentaremos alguns critérios de divisibilidade como aplicação das congruências. Seja a um número inteiro escrito na base decimal. Queremos verificar, a partir de seus dígitos, quais são as condições para que a seja divisível por um número inteiro b. Digamos que

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

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

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

Começaremos com o critério de divisibilidade por 2.

Inicialmente, veja que $10 \equiv 0 \bmod 2$.

$a \equiv a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 \equiv a_0 \bmod 2$. Portanto, um número é divisível por 2 se, e somente se, $2 \mid a_0$. Em outras palavras, um número divisível por 2 quando o algarismo das unidades é par.

Critério de divisibilidade por 3.

Análogo ao critério de divisibilidade por 9, trocando apenas o 9 por 3.

Critério de divisibilidade por 5.

Veja que $10 \equiv 0 \bmod 5$.

$a \equiv a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 \equiv a_0 \bmod 5$. Portanto, um número é divisível por 5 se, e somente se, $5 \mid a_0$. Em outras palavras, um número é divisível por 5 quando seu algarismo das unidades é 0 ou 5.

Critério de divisibilidade por 7.

Neste caso, usaremos o exemplo 1.1.1 para explicitar o processo. O exemplo 1.1.1 diz que, se $7 \mid 10m+n$ então $7 \mid m-2n$.

Por exemplo, vamos verificar se $7 \mid 2016$. Inicialmente, note que, $2016 = 10 \times 201 + 6$. Assim, se $7 \mid 2016$ então $7 \mid 201 - 2 \times 6 = 189$. Veja que $189 = 10 \times 18 + 9$, se $7 \mid 189$ então $7 \mid 18 - 2 \times 9 = 0$. Como $7 \mid 0$ então $7 \mid 2016$.

Critério de divisibilidade por 9.

Observe que $10 \equiv 1 \bmod 9$. Logo qualquer potência de 10 é congruente a 1 módulo 9.

Assim, $a \equiv a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 \equiv a_n + a_{n-1} + ... + a_1 + a_0 \bmod 9$. Portanto, um número é divisível por 9 se, e somente se, $9 \mid a_n + a_{n-1} + ... + a_1 + a_0$. Por exemplo, 2016 é divisível por 9, já que $2+0+1+6=9$ é divisível por 9.

Critério de divisibilidade por 10.

Observe que $10 \equiv 0 \bmod 10$. Logo qualquer potência de 10 é congruente a 0 módulo 10.

Assim, $a \equiv a_n 10^n + a_{n-1} 10^{n-1} + ... + a_1 10 + a_0 \equiv a_0 \bmod 10$. Portanto, um número é divisível por 10 se, e somente se, seu algarismo das unidades é divisível por 10. Em outras palavras, um número é divisível se, e somente se, seu algarismo das unidades é zero.

Critério de divisibilidade por 11.

Inicialmente, veja que, $10 \equiv -1 \bmod 11$, daí $10^n \equiv (-1)^n \bmod 11$. Logo, se n é par tem-se $10^n \equiv 1 \bmod 11$, se n for ímpar, então $10^n \equiv -1 \bmod 11$. Assim,

$a \equiv a_n 10^n + a_{n-1}10^{n-1} + ... + a_1 10 + a_0 \equiv a_n(-1)^n + a_{n-1}(-1)^{n-1} + ... + a_2 - a_1 + a_0 \bmod 11$. Portanto, um número é divisível por 11 se, e somente se, a soma alternada é divisível por 11. Por exemplo, 75919251 é divisível por 11, já que $7-5+9-1+9-2+5-1=22$ que é divisível por 11.