Universidade Federal do ABC
Centro de Matemática, Computação e Cognição

Aritmética Modular e Criptografia

Jeovah Pereira de Alencar
Orientador: Prof. Dr. Antonio Cândido Faleiros

Dissertação apresentada junto ao Programa de Mestrado Profissionalizante em Matemática da Universidade Federal do ABC, para obtenção do Título de Mestre em Matemática.

Santo André - SP
Agosto de 2013.

Aritmética Modular e Criptografia

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Jeovah Pereira de Alencar e aprovada pela comissão julgadora.

Santo André, 22 de agosto de 2013.

Prof. Dr. Antonio Cândido Faleiros
Orientador

Banca examinadora:

1. Prof. Dr. Antonio Cândido Faleiros - UFABC (Presidente)

2. Prof. Dr. Adail de Castro Cavalheiro - UnB (Membro Titular)

3. Prof. Dr. Daniel Miranda Machado - UFABC (Membro Titular)

Dissertação apresentada junto ao Programa de Mestrado Profissional em Matemática da UFABC, como requisito parcial para obtenção do Título de Mestre em Matemática.

Universidade Federal do ABC

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato **Jeovah Pereira de Alencar**, realizada em 22 de agosto de 2013.

Prof. Dr. Antonio Cândido Faleiros (UFABC) – Presidente

Prof. Dr. Adail de Castro Cavalheiro (UnB) – Membro Titular

Prof. Dr. Daniel Miranda Machado (UFABC) – Membro Titular

Prof. Dr. Jerônimo Cordoni Pellegrini (UFABC) – Membro Suplente

Prof. Dr. Geraldo Pompeu Junior (UFSCAR) – Membro Suplente

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 27 de agosto de 2013.

Assinatura do autor: _____

Assinatura do orientador: _____

Dedico este trabalho à minha mãe, que está sempre no meu coração e no meu pensamento, e à minha família, em especial ao meu filho Pedro.

Agradecimentos

Agradeço primeiramente a Deus por me conduzir até aqui, ao Programa de Mestrado Profissional em Matemática (PROFMAT), à CAPES pelo auxílio concedido, à UFABC e seus professores, ao meu orientador Prof. Dr. Antonio Cândido Faleiros e aos colegas de turma do mestrado. A todos minha sincera gratidão.

Resumo

Acreditando que a aritmética modular possa ser introduzida no ensino médio e usando como centro de interesse a criptografia, discorremos sobre as cifras de César, Vigenère e de Hill, mostrando a aritmética modular por detrás de cada uma delas, até chegarmos à moderna criptografia de chave pública RSA utilizada na Internet. O texto é uma introdução à aritmética modular, mostrando algumas de suas aplicações, como por exemplo, criptografia, cálculo de dígitos de verificação e regras de divisibilidade.

Palavras-Chave

Aritmética Modular, Criptografia, Criptografia RSA

Abstract

We believe modular arithmetic can be introduced to high school students and cryptography plays an important motivational role. We discourse about the ciphers of Caesar, Vigenere and Hill, and the modular arithmetic behind each one, until we reach the modern RSA public key encryption used on the Internet. The text is an introduction to modular arithmetic, with some of its applications, for example, cryptography, calculation of check digits and divisibility rules.

Keywords

Modular Arithmetic, Cryptography, RSA public key encryption

Sumário

Capítulo 1

Aritmética Modular para o Ensino Médio

1.1 Introdução

O matemático suíço Leonhard Euler (1707-1783) foi quem introduziu, por volta de 1750, a aritmética modular (também chamada aritmética do relógio). Em 1801, Carl Friedrich Gauss, matemático alemão, utilizou e desenvolveu a aritmética modular em seu livro *"Disquisitiones Arithmeticae"*. Durante muito tempo não houve aplicações importantes da aritmética modular até que na segunda metade do século XX uma aplicação surpreendente dessa idéia veio resolver um problema que desafiava matemáticos e criptógrafos, o problema da troca de chaves criptográficas.

Vamos utilizar uma ideia simples para ilustrar o conceito básico da aritmética modular. Imagine um relógio comum de ponteiros registrando 3 horas. Se quisermos saber que hora ele estará marcando após se passarem 38 horas, verificamos que o resultado é 5 horas e não 41. A cada 12 horas o ponteiro volta ao ponto de partida, portanto após 36 horas (3 voltas completas) o ponteiro estará novamente sobre as 3 horas, adicionando mais 2 horas chegamos ao resultado. A ideia permanece válida para um relógio com um número qualquer de subdivisões. Um relógio com 7 subdivisões apenas, numeradas sequencialmente no sentido horário, por exemplo. Se o ponteiro está sobre o número 5 e o fazemos saltar 43 subdivisões, a adição comum resultaria 48, mas não temos esse resultado no mostrador do relógio. Agora, o ponteiro volta ao 5 a cada 7 saltos, ou seja, após 42 voltas completas, que é o múltiplo de 7 mais próximo de 43, o ponteiro estará novamente sobre o 5, adicionando 1 chegamos ao resultado: 6.

A aritmética modular normalmente é tratada no ensino superior. Entretanto, devido à facilidade de compreensão do conceito, suas bases podem ser introduzidas já no ensino médio. Evidentemente, com uma linguagem matemática apropriada para esta etapa do ensino e sem que sejam feitas todas as demonstrações dos teoremas e proposições. Aqueles cujas demonstrações não sejam essenciais à compreensão do conteúdo seriam apenas enunciados e utilizados quando necessário. A aritmética modular está presente em métodos criptográficos como a cifra de César, a cifra de Vigenère e mais recentemente na criptografia de chave pública RSA, da qual é a base. O assunto está relacionado à segurança digital e ao cotidiano de quem utiliza a internet, em especial os jovens, para se comunicar, se relacionar nas redes sociais, fazer compras e transações bancárias. Isto apenas já constitui uma excelente motivação para o seu estudo.

As transações comercias pela internet bem como a correspondência dos usuários da rede são protegidas por criptografia baseada na aritmética modular. Além desta importante aplicação há outras, como veremos mais adiante. A ideia básica da aritmética modular é bem simples. Fixado um inteiro m, todos os demais números inteiros a são substituídos pelo resto de sua divisão euclidiana por m e representados por $a \bmod m = b$, $b \in \{0, 1, \ldots, m-1\}$. Desse modo, o conjunto $\mathbb{Z}$ dos números inteiros se transforma no conjunto $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$, denominado conjunto dos inteiros módulo m (cujos elementos são os restos possíveis da divisão de um inteiro a qualquer por m).

Assim como no conjunto dos números racionais temos as frações equivalentes, dizemos que dois inteiros que dão o mesmo resto quando divididos por m são congruentes (equivalentes) módulo m. Por exemplo,

$$11 \bmod 7 = 4, \text{ assim como } 25 \bmod 7 = 4$$

Portanto, 11 e 25 são congruentes módulo 7 e representamos $11 \equiv 25 \bmod 7$. A congruência módulo m também pode ser verificada se fizermos a diferença entre os dois inteiros e o resultado for um múltiplo de m. No caso do exemplo, $25 - 11 = 14 = 2 \cdot 7$, o que também mostra que 11 e 25 são congruentes módulo 7. A congruência módulo m é uma relação de equivalência que subdivide o conjunto $\mathbb{Z}$ em m classes de equivalência, cada uma correspondendo a um resto da divisão euclidiana por m.

Proposição 1. *Dois inteiros p e q são congruentes módulo m, $m \in \mathbb{Z}$, $m > 1$ se, e somente se, $p - q$ for divisível por m e representamos*

$$p \equiv q \bmod m.$$

Demonstração. Sejam $p = k_1m + r_1$ *e* $q = k_2m + r_2$, então $r_1 = p \bmod m$ e $r_2 = q \bmod m$.

($\Longrightarrow$) Se p e q são congruentes módulo m, então

$p \equiv q \bmod m \Longrightarrow p \bmod m = q \bmod m \Longrightarrow r_1 = r_2 \Longrightarrow$

$p-q = k_1m+r_1-k_2m-r_2 = (k_1-k_2)m+(r_1-r_2) \Longrightarrow p-q = (k_1-k_2)m \Longrightarrow$

$m|p-q$.

($\Longleftarrow$) Se $p-q$ é múltiplo de m, então

$p - q = km \Longrightarrow p = km + q \Longrightarrow p \bmod m = (km + q) \bmod m \Longrightarrow$

$p \bmod m = km \bmod m + q \bmod m \Longrightarrow p \bmod m = q \bmod m \Longrightarrow$

$p \equiv q \bmod m$. □

Exemplo 1. Determinar o valor de $x = 139 \bmod 11$.

Solução Basta efetuar a divisão euclidiana de 139 por 11, cujo resultado é quociente 12 e resto 7. Portanto, $x = 7$.

Exemplo 2. Dentre os inteiros 111, 370, 341, 80 e 203 qual(is) é(são) congruente(s) a 139 módulo 11?

Solução Procuramos $x \equiv 139 \bmod 11$, $x \in \{111, 370, 341, 80, 203\}$. Pela proposição 1 acima, x é tal que $11|(x - 139)$. Verificamos que somente $x = 370$ é solução.

$$370 - 139 = 231 = 21 \cdot 11$$

Exemplo 3. Hoje é quarta- feira, 27 de fevereiro. Pedro tem 9 anos e fará aniversário no dia 21 de junho. Em que dia da semana Pedro completará 10 anos?

Solução Se não temos um calendário à mão, mesmo assim podemos determinar o dia da semana em que Pedro fará aniversário. Primeiro contamos os dias até 21 de junho: $1 + 31 + 30 + 31 + 21 = 114$ dias. Como iniciamos a contagem a partir de uma quarta-feira, associamos 0 mod 7 a esse dia da semana. Veja abaixo como fica:

$$\begin{array}{ll} \text{quarta-feira} & \longrightarrow \quad 0 \bmod 7 = 0 \\ \text{quinta-feira} & \longrightarrow \quad 1 \bmod 7 = 1 \\ \text{sexta-feira} & \longrightarrow \quad 2 \bmod 7 = 2 \\ \text{sábado} & \longrightarrow \quad 3 \bmod 7 = 3 \\ \text{domingo} & \longrightarrow \quad 4 \bmod 7 = 4 \\ \text{segunda-feira} & \longrightarrow \quad 5 \bmod 7 = 5 \\ \text{terça-feira} & \longrightarrow \quad 6 \bmod 7 = 6 \end{array}$$

Agora adicionamos 114 mod 7 ao dia de hoje (0 mod 7),

$$0 \bmod 7 + 114 \bmod 7 = 0 + 2 = 2 = 2 \bmod 7$$

Isto significa que o 114º dia a partir de hoje, dia do aniversário do Pedro, cairá numa sexta-feira (2 mod 7 na tabela).

Exemplo 4. Determine o primeiro termo (a_1) de uma P.A. de razão 7, sabendo que $0 < a_1 < r$ e um dos termos dessa P.A. é 21888. Qual a ordem do termo dado?

Solução O termo geral de uma P.A. é $a_n = a_1 + (n-1)r$, onde a_1 é o primeiro termo e r é a razão.

Observe que

$a_n \bmod r = [a_1 + (n-1)r] \bmod r = a_1 \bmod r + [(n-1)r] \bmod r =$

$a_1 \bmod r \Longrightarrow$

$a_n \bmod r = a_1 \bmod r \Longrightarrow a_n \equiv a_1 \bmod r \ \ (\forall n, n \in \mathbb{N}^*)$

Como $a_1 < r \Longrightarrow a_1 \bmod r = a_1 \Longrightarrow a_n \bmod r = a_1 \ \ (\forall n, n \in \mathbb{N}^*)$

Logo,

$a_1 = a_n \bmod r \Longrightarrow a_1 = 21888 \bmod 7 \Longrightarrow a_1 = 6.$

Usando agora a fórmula do termo geral da P.A. temos,

$a_n = a_1 + (n-1)r \Longrightarrow 6 + (n-1) \cdot 7 = 21888 \Longrightarrow$

$n = \frac{21888-6}{7} + 1 \Longrightarrow n = 3127 \Longrightarrow 21888 = a_{3127}.$

Exemplo 5. Determine o 2954º algarismo da dízima períodica gerada pela fração $\frac{11}{7}$.

Solução Efetuando a divisão do numerador 11 pelo denominador 7, obtemos a dízima $1,\overline{571428}$ cujo período possui 6 algarismos. O primeiro algarismo da dízima é 1 (unidades). Portanto, o que queremos é o 2953º algarismo da parte decimal. Calculando 2953 mod 6 obtemos quociente 492 e resto 1, o que significa 492 períodos e um algarismo, que no caso é o 5. Logo, o 2954º algarismo desta dízima periódica é 5.

Exemplo 6. Qual é o 1234º termo da sequência periódica abaixo?

$\cup, \subset, \cap, \supset, \vee, <, \wedge, >, \cup, \subset, \cap, \supset, \vee, <, \ldots$

Solução A sequência possui oito termos distintos repetindo-se na mesma ordem, portanto basta calcularmos 1234 mod 8 = 2. Conforme a tabela abaixo, o resultado corresponde ao segundo termo, ou seja, $\subset$.

$$\begin{array}{lcl}
1º \text{ termo: } \cup & \longrightarrow & 1 \bmod 8 = 1 \\
2º \text{ termo: } \subset & \longrightarrow & 2 \bmod 8 = 2 \\
3º \text{ termo: } \cap & \longrightarrow & 3 \bmod 8 = 3 \\
4º \text{ termo: } \supset & \longrightarrow & 4 \bmod 8 = 4 \\
5º \text{ termo: } \vee & \longrightarrow & 5 \bmod 8 = 5 \\
6º \text{ termo: } < & \longrightarrow & 6 \bmod 8 = 6 \\
7º \text{ termo: } \wedge & \longrightarrow & 7 \bmod 8 = 7 \\
8º \text{ termo: } > & \longrightarrow & 8 \bmod 8 = 0
\end{array}$$

Exemplo 7. Determine o algarismo das unidades de 273^{100}.

Solução O algarismo das unidades de qualquer número é o resto da divisão desse número por 10. Sendo assim, devemos resolver $273^{100} \bmod 10$.

$273 \equiv 3 \bmod 10 \Longrightarrow 273^{100} \equiv 3^{100} \bmod 10 = (3^2)^{50} \bmod 10 =$

$9^{50} \bmod 10$.

Como $9 \equiv -1 \bmod 10$, temos

$9^{50} \bmod 10 = (-1)^{50} \bmod 10 = 1$.

Portanto o algarismo das unidades de 273^{100} é 1.

Exemplo 8. Calcule o $mdc(858, 546)$.

Solução O método mais eficiente para calcular o máximo divisor comum de dois inteiros é o algoritmo de Euclides, que consiste primeiramente em dividir o maior pelo menor. Em seguida divide-se o divisor pelo resto e assim sucessivamente até obter resto zero. O *mdc* será o último resto diferente de zero obtido. Vejamos o processo do ponto de vista da aritmética modular.

$858 \bmod 546 = 312$
$546 \bmod 312 = 234$
$312 \bmod 234 = 78$
$234 \bmod 78 = 0$

Logo, o $mdc(858, 546) = 78$.

Observação: Como desafio, encontre o $mdc(12119247318071, 673624408921)$ usando o método descrito acima e a função MOD da planilha Excel. (solução: 151609)

1.2 Propriedades e Operações

1.2.1 Propriedades da Congruência Módulo m

O conjunto $\mathbb{Z}_m = \{1, 2, \ldots, m-1\}$ dos inteiros módulo m, é fechado para as operações de soma e multiplicação módulo m e valem as seguintes propriedades.

Dados a, b e c inteiros, então:

1) $a \equiv a \bmod m$; (reflexiva)

2) $a \equiv b \bmod m \implies b \equiv a \bmod m$; (simétrica)

3) $a \equiv b \bmod m$ e $b \equiv c \bmod m \implies a \equiv c \bmod m$; (transitiva)

4) Se $a \equiv b \bmod m$ então

$a \pm c \equiv b \pm c \bmod m$;

$a \times c \equiv b \times c \bmod m$;

$a \equiv b + cm \bmod m$;

5) $a + c \equiv b \bmod m \implies c \equiv b - a \bmod m$;

Observação: As três primeiras propriedades fazem da congruência módulo m uma relação de equivalência. Cada número inteiro corresponde a um dos restos da divisão euclidiana por m. Isto reduz o conjunto infinito $\mathbb{Z}$ ao conjunto finito $\mathbb{Z}_m = \{1, 2, \ldots, m-1\}$ onde cada elemento representa uma classe de equivalência.

Além disso, quando a e m forem co-primos ($mdc(a, m) = 1$),

6) $ac \equiv b \bmod m \implies c \equiv ba^{-1} \bmod m$;

7) $ac \equiv ab \bmod m \implies c \equiv b \bmod m$. (lei do cancelamento).

O conjunto $\mathbb{Z}_p$, p primo, munido das operações de adição e multiplicação módulo p com as propriedades a seguir constitui uma estrutura algébrica denominada *corpo*. Dados a, b, c e k inteiros, temos:

A1) adição associativa: $a + (b + c) \bmod p = (a + b) + c \bmod p$;

A2) adição comutativa: $a + b \bmod p = b + a \bmod p$;

A3) neutro aditivo: $a + kp \bmod p = kp + a \bmod p = a \bmod p$;

A4) inversos aditivos: $a+(kp-a) \bmod p = (kp-a)+a \bmod p = 0 \bmod p$;

M1) multiplicação associativa: $a(bc) \bmod p = (ab)c \bmod p$;

M2) multiplicação comutativa: $ab \bmod p = ba \bmod p$;

M3) neutro multiplicativo: $a1 \bmod p = 1a \bmod p = a \bmod p$;

M4) inversos multiplicativos: $aa^{-1} \bmod p = a^{-1}a \bmod p = 1 \bmod p$, quando $p \nmid a$;

D) distributiva: $a(b + c) \bmod p = ab \bmod p + ac \bmod p$.

1.2.2 Adição e Multiplicação Modular

Efetuar adições e multiplicações módulo m consiste basicamente em tomar os operandos módulo m, fazer as operações indicadas e reduzir o resultado módulo m.

Proposição 2. *Para todo a, b e m inteiros, $m > 1$, valem:*

1) $a \pm b \ mod\ m = [(a \ mod\ m) \pm (b \ mod\ m)] \ mod\ m$;

2) $ab \ mod\ m = [(a \ mod\ m)(b \ mod\ m)] \ mod\ m$;

Demonstração. 1. Sejam a, b, e m inteiros, $m > 1$. Então,

$$a = mq + r \Longrightarrow r = a \bmod m,\ 0 \leq r < m$$

e $\quad b = mq' + r' \Longrightarrow r' = b \bmod m,\ 0 \leq r' < m$

e segue que

$$a \pm b = m(q \pm q') \pm (r \pm r') \Longrightarrow$$

$$(a \pm b) \bmod m = (r \pm r') \bmod m \Longrightarrow$$

$$(a \pm b) \bmod m = [(a \bmod m) \pm (b \bmod m)] \bmod m.$$

2. Agora,

$$ab = [(mq + r)(mq' + r')] = [m(mqq' + qr' + q'r) + rr'] \Longrightarrow$$

$$ab \bmod m = rr' \bmod m \Longrightarrow$$

$$ab \bmod m = [(a \bmod m)(b \bmod m)] \bmod m.$$

□

Por indução, pode-se provar que valem as igualdades:

$$(a_1 + a_2 + \ldots + a_n) \bmod m = (a_1 \bmod m + a_2 \bmod m + \ldots + a_n \bmod m) \bmod m$$

$$(a_1 a_2 \cdots a_n) \bmod m = [(a_1 \bmod m)(a_2 \bmod m) \cdots (a_n \bmod m)] \bmod m.$$

Exemplo 9. Calcule:

a) $(202 + 813 + 4455 + 2390) \bmod 2$

b) $(43 \cdot 365 \cdot 1007) \bmod 3$

Solução

a) $(202 + 813 + 4455 + 2390) \bmod 2 =$

$(202 \bmod 2 + 813 \bmod 2 + 4455 \bmod 2 + 2390 \bmod 2) \bmod 2 =$

$(0 + 1 + 1 + 0) \bmod 2 = 2 \bmod 2 = 0$

b) $(43 \cdot 365 \cdot 1007) \bmod 3 =$

$[(43 \bmod 3) \cdot (365 \bmod 3) \cdot (1007 \bmod 3)] \bmod 3 =$

$(1 \cdot 2 \cdot 2) \bmod 3 = 4 \bmod 3 = 1$

Exemplo 10. Resolva a expressão $(23 \cdot 8 + 13 \cdot 6 - 25) \bmod 7$.

Solução

$[(23 \bmod 7) \cdot (8 \bmod 7) + (13 \bmod 7) \cdot (6 \bmod 7) - (25 \bmod 7)] \bmod 7 =$

$(2 \cdot 1 + 6 \cdot 6 - 4) \bmod 7 = (2 + 36 - 4) \bmod 7 = 34 \bmod 7 = 6$

1.2.3 Inversos Módulo m

Dizemos que um inteiro a é o inverso módulo m de outro inteiro b e vice-versa quando

$$ab \equiv 1 \bmod m.$$

O teorema seguinte estabelece a condição para que um inteiro qualquer k possua inverso módulo m.

Teorema 1. *Dados k e m inteiros, $m > 1$. O inteiro k possui inverso módulo m, se e somente se, k e m forem co-primos, ou seja, $mdc(k, m) = 1$.*

Demonstração. ($\Longrightarrow$) Se k e m forem co-primos o $mdc(k, m) = 1$ e, como consequência do algoritmo estendido de Euclides, existem inteiros a e b, tais que

$$ak + bm = 1 \Longrightarrow ak \bmod m + bm \bmod m = 1 \Longrightarrow$$

$ak \bmod m = 1$ (pois $bm \bmod m = 0$) $\Longrightarrow ak \equiv 1 \bmod m \Longrightarrow$

a é o inverso de k módulo m e escrevemos $a = k^{-1} \bmod m$.

($\Longleftarrow$) Se a for o inverso de k módulo m, ou seja, $ak \equiv 1 \bmod m$, então existe $-b$ inteiro, tal que

$$ak = -bm + 1 \Longrightarrow ak + bm = 1 \Longrightarrow mdc(k, m) = 1$$

□

Exemplo 11. Determine, se houver, o inverso de 7 módulo 12.

Solução

Como $mdc(7, 12) = 1$, isto significa que 7 tem inverso módulo 12. Então existem inteiros a e b, tais que $7a + 12b = 1$. Usando o algoritmo estendido de Euclides, temos:

(1) $12 = 7 \times 1 + 5$
(2) $7 = 5 \times 1 + 2$
(3) $5 = 2 \times 2 + 1$
(4) $2 = 2 \times 1 + 0$

De (3): $5 - 2 \times 2 = 1$ (5)

De (2): $2 = 7 - 5$, substituindo em (5): $5 - 2 \times (7 - 5) = 1 \Longrightarrow$

$3 \times 5 - 2 \times 7 = 1$ (6)

De (1): $5 = 12 - 7$, substituindo em (6): $3 \times (12 - 7) - 2 \times 7 = 1 \Longrightarrow$

$3 \times 12 - 5 \times 7 = 1$

Aplicando módulo, temos

$(3 \times 12) \bmod 12 + [(-5) \times 7] \bmod 12 = 1 \Longrightarrow$

$[(-5) \times 7] \bmod 12 = 1 \Longrightarrow 7^{-1} \bmod 12 = -5 \equiv 7 \bmod 12$

Portanto 7 é o seu próprio inverso módulo 12.

1.2.4 Equações Módulo m

É possível resolver equações do tipo $aX + b \equiv c \bmod m$ quando o $mdc(a, m) = 1$, ou seja, quando a tem inverso módulo m.

$aX + b \equiv c \bmod m \Longrightarrow aX \equiv c - b \bmod m \Longrightarrow$

$X \equiv (c - b)a^{-1} \bmod m$, fazendo $(c - b)a^{-1} = d$, temos $X = d + km, k \in \mathbb{Z}$.

Exemplo 12. Resolva a equação modular $3X - 13 \equiv 4 \bmod 5$.

Solução

Como $mdc(3, 5) = 1$, temos:

$3X - 13 \equiv 4 \bmod 5 \Longrightarrow 3X \equiv 17 \bmod 5 \Longrightarrow 3X \equiv 2 \bmod 5 \Longrightarrow$

$X \equiv (2 \cdot 3^{-1}) \bmod 5 \Longrightarrow X \equiv 4 \bmod 5$, já que $3^{-1} \bmod 5 = 2$

Portanto, $X = 4 + 5k$, $k \in \mathbb{Z}$.

Se $mdc(a, m) = d > 1$, a equação $aX \equiv b \bmod m$ terá solução apenas se d dividir b, ou seja, se toda a equação puder ser dividida por d, de modo que $a'X \equiv b' \bmod m'$, onde $a' = a/d$, $b' = b/d$, $m' = m/d$ e $mdc(a', m') = 1$.

Exemplo 13. Resolva a equação $9X \equiv 6 \bmod 15$.

Solução

Como o $mdc(9, 15) = 3$, que divide 6, simplificamos a equação e obtemos

$9X \equiv 6 \bmod 15 \Longrightarrow 3X \equiv 2 \bmod 5$,

cujas soluções, conforme o exemplo anterior, são da forma $X = 4 + 5k$, $k \in \mathbb{Z}$.

1.2.5 Potenciação

A maneira mais eficiente para calcular potências módulo m consiste em usar o expoente na base 2. Observe também que

$$a^b \bmod m = (a \bmod m)^b \bmod m.$$

Exemplo 14. Calcule $43^{11} \bmod 5$.

Solução

$43^{11} \bmod 5 = (43 \bmod 5)^{11} \bmod 5 = 3^{11} \bmod 5$

$11 = 1011_2 = 8 + 2 + 1 \Longrightarrow 3^{11} \bmod 5 = 3^{8+2+1} \bmod 5 =$

$(3^8 \times 3^2 \times 3^1) \bmod 5 = (3^8 \bmod 5 \times 3^2 \bmod 5 \times 3^1 \bmod 5) \bmod 5$

$3^1 \bmod 5 = 3 \bmod 5 = 3$

$3^2 \bmod 5 = 9 \bmod 5 = 4$

$3^4 \bmod 5 = (3^2)^2 \bmod 5 = (3^2 \bmod 5)^2 \bmod 5 = 4^2 \bmod 5 =$

$16 \bmod 5 = 1$

$3^8 \bmod 5 = (3^4)^2 \bmod 5 = (3^4 \bmod 5)^2 \bmod 5 = 1^2 \bmod 5 = 1$

$43^{11} \bmod 5 = (1 \times 4 \times 3) \bmod 5 = 12 \bmod 5 = 2.$

Portanto, $43^{11} \bmod 5 = 2$.

1.3 Cálculo de potências x^y mod m com auxílio da base 2

Para calcular potências módulo m de expoentes elevados existe um método simples e eficiente utilizando a base 2. Vamos exemplificar calculando 117^{327} mod 143. Primeiro escreve-se o expoente 327 na base 2, dividindo-o sucessivamente por 2 e tomando os restos.

$$327 = 163 \times 2 + 1$$

$$327 = (81 \times 2 + 1) \times 2 + 1$$

$$327 = 81 \times 2^2 + 1 \times 2 + 1$$

$$327 = (40 \times 2 + 1) \times 2^2 + 1 \times 2 + 1$$

$$327 = 40 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = (20 \times 2 + 0) \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = 20 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = (10 \times 2 + 0) \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = 10 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = (5 \times 2 + 0) \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = 5 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = (2 \times 2 + 1) \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = 2 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = (1 \times 2 + 0) \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$327 = 1 \times 2^8 + 0 \times 2^7 + 1 \times 2^6 + 0 \times 2^5 + 0 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1$$

$$\Longrightarrow 327_{10} = 101000111_2$$

Então,

$117^{327_{10}} \bmod 143 = 117^{101000111_2} \bmod 143 =$

$117^{2^8+0+2^6+0+0+0+2^2+2+1} \bmod 143 =$

$(117^{256} \cdot 117^{64} \cdot 117^4 \cdot 117^2 \cdot 117^1) \bmod 143 =$

$[(117^{256} \bmod 143) \cdot (117^{64} \bmod 143) \cdot (117^4 \bmod 143) \cdot (117^2 \bmod 143) \cdot (117^1 \bmod 143)] \bmod 143 \Longrightarrow$ *(continua mais abaixo)*

Algumas potências modulares $117^x \bmod 143$, sendo x uma potência de 2, foram calculadas a seguir (somente aquelas correspondentes ao algarismo 1 no expoente $101000111_2 = 327_{10}$ serão usadas no cálculo de $117^{327} \bmod 143$).

$117^1 \bmod 143 = 117$

$117^2 \bmod 143 = 13689 \bmod 143 = 104$

$117^4 \bmod 143 = (117^2)^2 \bmod 143 = (117^2 \bmod 143)^2 \bmod 143 = 104^2 \bmod 143 = 10816 \bmod 143 = 91$

$117^8 \bmod 143 = (117^4)^2 \bmod 143 = (117^4 \bmod 143)^2 \bmod 143 = 91^2 \bmod 143 = 8281 \bmod 143 = 130$

$117^{16} \bmod 143 = (117^8)^2 \bmod 143 = (117^8 \bmod 143)^2 \bmod 143 = 130^2 \bmod 143 = 16900 \bmod 143 = 26$

$117^{32} \bmod 143 = (117^{16})^2 \bmod 143 = (117^{16} \bmod 143)^2 \bmod 143 = 26^2 \bmod 143 = 676 \bmod 143 = 104$

$117^{64} \bmod 143 = (117^{32})^2 \bmod 143 = (117^{32} \bmod 143)^2 \bmod 143 = 104^2 \bmod 143 = 10816 \bmod 143 = 91$

$117^{128} \bmod 143 = (117^{64})^2 \bmod 143 = (117^{64} \bmod 143)^2 \bmod 143 = 91^2 \bmod 143 = 8281 \bmod 143 = 130$

$117^{256} \bmod 143 = (117^{128})^2 \bmod 143 = (117^{128} \bmod 143)^2 \bmod 143 = 130^2 \bmod 143 = 16900 \bmod 143 = 26$

Finalizando o cálculo de $117^{327} \bmod 143$, temos:

$117^{327_{10}} \bmod 143 = 117^{101000111_2} \bmod 143 =$

$(117^{256} \cdot 117^{64} \cdot 117^4 \cdot 117^2 \cdot 117^1) \bmod 143 =$

$[(117^{256} \bmod 143) \cdot (117^{64} \bmod 143) \cdot (117^4 \bmod 143) \cdot (117^2 \bmod 143) \cdot (117^1 \bmod 143)] \bmod 143 =$

$(26 \cdot 91 \cdot 91 \cdot 104 \cdot 117) \bmod 143$, que calculamos em etapas como segue:

$(26 \cdot 91) \bmod 143 = 2366 \bmod 143 = 78 \bmod 143$

$(78 \cdot 91) \bmod 143 = 7098 \bmod 143 = 91 \bmod 143$

$(91 \cdot 104) \bmod 143 = 9464 \bmod 143 = 26 \bmod 143$

$(26 \cdot 117) \bmod 143 = 3042 \bmod 143 = 39 \bmod 143$

Concluimos que $117^{327} \bmod 143 = 39$. As contas podem ser feitas numa calculadora comum, entretanto, calcular diretamente 117^{327} na calculadora não é possível porque o número é muito grande chegando a "estourar"a capacidade de armazenamento de um computador pessoal.

Pode-se implementar o algoritmo a seguir em linguagem de programação para efetuar o cálculo da potência $y = x^k \bmod m$, onde k está escrito na base 2.

$y := 1; A := x \bmod m$; // atribuição dos valores iniciais de y e A

$y := (y * A) \bmod m$; // y recebe o valor de $(1 \cdot x) \bmod m$

$A := (A * A) \bmod m$; // A recebe o valor de $(x \cdot x = x^2) \bmod m$

$y := (y * A) \bmod m$; // y recebe o valor de $(1 \cdot x \cdot x^2) \bmod m$

$A := (A * A) \bmod m$; // A recebe o valor de $(x^2 \cdot x^2 = x^4) \bmod m$

$y := (y * A) \bmod m$; // y recebe o valor de $(1 \cdot x \cdot x^2 \cdot x^4) \bmod m$

...

Os valores da variável A são calculados sempre, mas os valores de y são calculados apenas quando o algarismo do número binário k for 1. Começamos pelo primeiro algarismo à direita de k. Se for 1, calculamos y, calculamos A, eliminamos este algarismo e passamos ao seguinte. Caso contrário, se o primeiro dígito à direita de k for zero, calculamos A e eliminamos o zero, passando ao próximo algarismo. Repetimos isso até eliminarmos todos os dígitos de k. Ao final do processo temos $y = x^k \bmod m$. Num programa, como o do exemplo abaixo, usamos um comando 'if' para testar os dígitos e um 'loop while' para reduzir a quantidade de linhas de programa, permitindo rodá-lo para qualquer tamanho do número binário k.

```
y = 1; A = x % m;
while (x  != 0)
{
    if (k & 1) // verifica se o bit menos significativo é 1
    {
        y = y * A % m;
    }
    A = A * A % m;
    k = k >> 1; // elimina o bit menos significativo de k
}
```

Exemplo em linguagem C.

Como atividade em sala de aula, podemos propor aos alunos implementar o algoritmo numa planilha do Excel e calcular uma potência modular de expoente grande como $117^{327} \bmod 143$ usando essa planilha.

Abaixo a descrição da planilha:

$B1 : x$	$B2 : 117$
$C1 : k$	$C2 : 327$
$D1 : m$	$D2 : 143$
$B4 : A$	$C4 : y$
$A5$: vazia	$A10 : 5$
$A6 : 1$	$A11 : 6$
$A7 : 2$	$A12 : 7$
$A8 : 3$	$A13 : 8$
$A9 : 4$	$A14 : 9$
$B5 : 0$	$C5 : 1$
$B6 :=\text{MOD}(B2; D2)$	$C6 :=\text{MOD}(B6 * C5; D2)$
$B7 :=\text{MOD}(B6 * B6; D2)$	$C7 :=\text{MOD}(B7 * C6; D2)$
$B8 :=\text{MOD}(B7 * B7; D2)$	$C8 :=\text{MOD}(B8 * C7; D2)$
$B9 :=\text{MOD}(B8 * B8; D2)$	$C9 :$ vazia
$B10 :=\text{MOD}(B9 * B9; D2)$	$C10$: vazia
$B11 :=\text{MOD}(B10 * B10; D2)$	$C11$: vazia
$B12 :=\text{MOD}(B11 * B11; D2)$	$C12 :=\text{MOD}(B12 * C8; D2)$
$B13 :=\text{MOD}(B12 * B12; D2)$	$C13$: vazia
$B14 :=\text{MOD}(B13 * B13; D2)$	$C14 :=\text{MOD}(B14 * C12; D2)$

Planilha excel para cálculo de 117^{327} mod 143.

Capítulo 2

Criptografia e Aritmética Modular

2.1 Criptografia

A necessidade de sigilo nas comunicações militares, diplomáticas e comerciais levou à criação de códigos para mascarar mensagens de modo que somente os legítimos destinatários pudessem decifrá-las. Assim surgiu a criptografia (do grego *kryptos* = secreto), a arte de codificar uma mensagem segundo uma convenção pré-estabelecida entre o emissor e o receptor, impedindo que qualquer outra pessoa que a intercepte consiga ler o seu conteúdo. As técnicas criptográficas consistem na transposição e na substituição. A transposição é o rearranjo das letras da mensagem original gerando um anagrama. O número de anagramas cresce rapidamente quanto maior o texto a ser cifrado. Matematicamente, uma transposição nada mais é do que uma das possíveis permutações com repetição do conjunto das letras da mensagem original. Para que seja eficiente, a transposição deve ser feita segundo um sistema objetivo conhecido pelo receptor da mensagem, ou seja, o anagrama não pode ser gerado de forma aleatória, caso contrário o alto número de anagramas possíveis torna inviável a decifração. Um exemplo de cifra por transposição consiste em escrever a mensagem original em blocos de n letras e a seguir copiar as n colunas resultantes de cima para baixo, da esquerda para a direita. Preliminarmente, excluímos os espaços entre as palavras e excluímos também os sinais gráficos (cedilha, til, pontuação, etc.), se houver. Além disso, os dígrafos (*rr*, *ss*, *oo*, etc.) na mensagem são substituídos por uma só letra. Tais medidas visam dificultar a quebra do código. Vamos cifrar a frase *"O matemático é um cego numa sala escura, procurando um gato que não está lá"*, atribuída a Charles Darwin (1809-1882), naturalista inglês (na

verdade, fazendo um elogio aos matemáticos), com o método acima e usando n=7.

o	*m*	*a*	*t*	*e*	*m*	*a*
t	*i*	*c*	*o*	*e*	*u*	*m*
c	*e*	*g*	*o*	*n*	*u*	*m*
a	*s*	*a*	*l*	*a*	*e*	*s*
c	*u*	*r*	*a*	*p*	*r*	*o*
c	*u*	*r*	*a*	*n*	*d*	*o*
u	*m*	*g*	*a*	*t*	*o*	*q*
u	*e*	*n*	*a*	*o*	*e*	*s*
t	*a*	*l*	*a*	*a*	*m*	*a*

A mensagem cifrada fica assim:

“ o t c a c c u u t m i e s u u m e a a c g a r r g n l t o o l a a a a a e e n a p n t o a m u u e r d o e m a m m s o o q s a”,

que é um anagrama do texto original, obtido segundo a regra descrita anteriormente. Observe que completamos a última linha a ser cifrada com caracteres nulos (*a m a*).

O destinatário, conhecendo a chave n= 7, divide o número de caracteres da mensagem cifrada por 7 (no caso, $63 \div 7 = 9$) para obter o número de caracteres que colocará em cada coluna para decifrar a mensagem. O ponto fraco neste caso é que um espião pode obter a chave fatorando o número de caracteres da mensagem.

A substituição, como o nome sugere, consiste em substituir cada letra da mensagem original por outra segundo um sistema previamente acertado, de modo que a substituição inversa forneça o texto original.

2.1.1 A Cifra de César

No cifrário de César, uma das cifras de substituição mais antigas, cada letra da mensagem original é substituída pela terceira letra após ela na ordem alfabética. Ou seja, trata-se de corresponder o alfabeto original com uma translação do mesmo de três letras adiante.

alfabeto original: a b c d e f g h i j ... x y z

substituição ... : d e f g h i j k l m ... a b c

A frase de Darwin codificada usando a cifra de César ficaria assim: *"r p d w h p d w l f r h x p f h j r q x p d v d o d h v f x u d s u r f x u d q g r x p j d w r t x h q d r h v w d o d"*.

2.1.2 A Matemática da Cifra de César

Associamos a cada letra do alfabeto um número inteiro não negativo da seguinte maneira: $a = 0, b = 1, c = 2, d = 3$ e assim por diante até $z = 25$. Desse modo nos referimos a uma letra pelo seu número correspondente e vice-versa. Pensando na cifra de César como uma função c que a cada letra λ da mensagem original associa uma única letra $c(\lambda) = \lambda + 3$, surge um problema quando desejamos cifrar as letras *x, y* ou *z*. Com essa função obtemos $c(x) = c(23) = 23 + 3 = 26$, $c(y) = c(24) = 24 + 3 = 27$ e $c(z) = c(25) = 25 + 3 = 28$ que não correspondem a nenhuma letra do alfabeto original (que vai até z=25). Como sabemos, x corresponde à letra a, y à letra b e z à letra c. A solução é tomar o resto da divisão euclidiana de $c(\lambda)$ por 26. No caso da letra x, $c(x) = 26$ e o resto da divisão por 26 é 0, portanto $c(x) = 0 = a$. Analogamente, $c(y) = 1 = b$ e $c(z) = 2 = c$. Para decodificar a cifra de César usamos a função inversa $d[c(\lambda)] = c(\lambda) - 3$ e novamente temos problemas para decodifcar $c(\lambda) = 0, c(\lambda) = 1$ e $c(\lambda) = 2$ cujas decodificações seriam inteiros negativos. Como vemos, as funções adequadas para cifrar e decifrar usando a cifra de César são as funções modulares correspondentes $c(\lambda) = (\lambda + 3) \bmod 26$ e $d[c(\lambda)] = [c(\lambda) - 3] \bmod 26$.

Podemos generalizar o procedimento utilizado na cifra de César. Fixado um número natural k (denominado chave), $0 < k < 26$, a cifragem é feita substituindo cada letra por aquela k posições adiante no alfabeto. Em termos de aritmética modular isto significa adicionar, módulo 26, k ao número λ correspondente a letra a ser cifrada, ou seja

$$c(\lambda) = (\lambda + k) \bmod 26$$

A decifragem consiste em substitiuir cada letra do texto cifrado por aquela obtida retrocedendo k posições no alfabeto. Em termos de aritmética modular significa subtrair, módulo 26, k de $c(\lambda)$, ou seja

$$d[c(\lambda)] = [c(\lambda) - k] \bmod 26 = (\lambda + k) - k \bmod 26 = \lambda$$

O ponto fraco da cifra de César está no pequeno número de chaves possíveis (25 apenas), o que permite a quebra do código por tentativas.

Vamos exemplificar cifrando *"legiões romanas"* com a chave $k = 11$. Após a supressão de espaços e acentos temos *"legioesromanas"*. Substituindo as letras por números temos 11-04-06-08-14-04-18-17-14-12-00-13-00-18.

$$c(11) = (11 + 11) \bmod 26 \Longrightarrow c(11) = 22 \bmod 26 = 22$$

$$c(04) = (04 + 11) \bmod 26 \Longrightarrow c(04) = 15 \bmod 26 = 15$$

$$c(06) = (06 + 11) \bmod 26 \Longrightarrow c(06) = 17 \bmod 26 = 17$$

$$c(08) = (08 + 11) \bmod 26 \Longrightarrow c(08) = 19 \bmod 26 = 19$$

$$c(14) = (14 + 11) \bmod 26 \Longrightarrow c(14) = 25 \bmod 26 = 25$$

$$c(04) = (04 + 11) \bmod 26 \Longrightarrow c(04) = 15 \bmod 26 = 15$$

$$c(18) = (18 + 11) \bmod 26 \Longrightarrow c(18) = 29 \equiv 03 \bmod 26 = 03$$

$$c(17) = (17 + 11) \bmod 26 \Longrightarrow c(17) = 28 \equiv 02 \bmod 26 = 02$$

$$c(14) = (14 + 11) \bmod 26 \Longrightarrow c(14) = 25 \bmod 26 = 25$$

$$c(12) = (12 + 11) \bmod 26 \Longrightarrow c(12) = 23 \bmod 26 = 23$$

$$c(00) = (00 + 11) \bmod 26 \Longrightarrow c(00) = 11 \bmod 26 = 11$$

$$c(13) = (13 + 11) \bmod 26 \Longrightarrow c(13) = 24 \bmod 26 = 24$$

$$c(00) = (00 + 11) \bmod 26 \Longrightarrow c(00) = 11 \bmod 26 = 11$$

$$c(18) = (18 + 11) \bmod 26 \Longrightarrow c(18) = 29 \equiv 03 \bmod 26 = 03$$

Obtemos assim 22-15-17-19-25-15-03-02-25-23-11-24-11-03 e a mensagem cifrada é *"w p r t z p d c z x l y l d"*. Agora vamos decifrar a mensagem.

$$d(22) = (22 - 11) \bmod 26 \Longrightarrow d(22) = 11 \bmod 26 = 11$$

$$d(15) = (15 - 11) \bmod 26 \Longrightarrow d(15) = 04 \bmod 26 = 04$$

$d(17) = (17 - 11) \bmod 26 \Longrightarrow d(17) = 06 \bmod 26 = 06$

$d(19) = (19 - 11) \bmod 26 \Longrightarrow d(19) = 08 \bmod 26 = 08$

$d(25) = (25 - 11) \bmod 26 \Longrightarrow d(25) = 14 \bmod 26 = 14$

$d(15) = (15 - 11) \bmod 26 \Longrightarrow d(15) = 04 \bmod 26 = 04$

$d(03) = (03 - 11) \bmod 26 \Longrightarrow d(03) = -8 \equiv 18 \bmod 26 = 18$

$d(02) = (02 - 11) \bmod 26 \Longrightarrow d(02) = -9 \equiv 17 \bmod 26 = 17$

$d(25) = (25 - 11) \bmod 26 \Longrightarrow d(25) = 14 \bmod 26 = 14$

$d(23) = (23 - 11) \bmod 26 \Longrightarrow d(23) = 12 \bmod 26 = 12$

$d(11) = (11 - 11) \bmod 26 \Longrightarrow d(11) = 00 \bmod 26 = 00$

$d(24) = (24 - 11) \bmod 26 \Longrightarrow d(24) = 13 \bmod 26 = 13$

$d(11) = (11 - 11) \bmod 26 \Longrightarrow d(11) = 00 \bmod 26 = 00$

$d(03) = (03 - 11) \bmod 26 \Longrightarrow d(03) = -8 \equiv 18 \bmod 26 = 18$

Como esperado obtemos 11-04-06-08-14-04-18-17-14-12-00-13-00-18, que corresponde à mensagem original *"legiões romanas"*.

2.1.3 A Cifra de Vigenère

A cifra de César e suas variações são denominadas cifras de substituição monoalfabética, ou seja, cada letra é substituída sempre por um mesmo símbolo em toda a mensagem. Existe uma correspondência biunívoca entre o alfabeto original e o alfabeto de substituição. Para decifrar a mensagem, basta substituir cada símbolo pela letra correspondente do alfabeto original. Este tipo de cifra foi eficaz por muito tempo, mas com o surgimento da técnica de análise de frequência, descoberta pelos árabes, tornou-se insegura. A análise de frequência baseia-se no fato de que cada letra aparece com uma determinada frequência em textos de um certo idioma. Assim, contando-se os símbolos na mensagem cifrada e sabendo-se o idioma do texto original, basta comparar a frequência dos símbolos com uma tabela de frequência previamente elaborada (a partir de um livro, por exemplo). A técnica é muito

eficaz quando se tem um texto relativamente longo ou muitos textos curtos, mas pode não ser possível aplicá-la a um único texto muito pequeno. Abaixo mostramos a tabela de frequência do idioma português.

Português												
A	14,63	E	12,57	I	6,18	M	4,74	Q	1,20	U	4,63	Y	0,01
B	1,04	F	1,02	J	0,40	N	5,05	R	6,53	V	1,67	Z	0,47
C	3,88	G	1,30	K	0,02	O	10,73	S	7,81	W	0,01	-	-,-
D	4,99	H	1,28	L	2,78	P	2,52	T	4,74	X	0,21	-	-,-

Tabela de frequência de letras do idioma português (em porcentagem).

Para escapar à análise de frequência, Blaise de Vigenère (1523-1596), diplomata e criptógrafo francês, utilizou uma cifra polialfabética que leva o seu nome. A cifra de Vigenère consiste numa tabela com 26 alfabetos dispostos horizontalmente e, a partir do segundo, deslocados uma letra para a direita em relação ao anterior. Ou seja, cada alfabeto começa por uma letra diferente. O primeiro começa pela letra A, o segundo pela letra B, e assim por diante.

	A	*B*	*C*	*D*	*E*	*F*	*G*	*H*	*I*	*J*	*K*	*L*	*M*	*N*	*O*	*P*	*Q*	*R*	*S*	*T*	*U*	*V*	*W*	*X*	*Y*	*Z*
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
P	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t
V	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u
W	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
X	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w
Y	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x
Z	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y

Alfabetos da cifra de Vigenère.

O método consiste em usar uma palavra ou frase como chave. Cada letra da chave indica um alfabeto horizontal a ser usado na substituição de uma letra do texto original. Vejamos um exemplo. Se queremos cifrar a palavra *"tempestade"* usando como chave a palavra *RAIO* procedemos assim:

buscamos a letra no cruzamento da coluna do T com a linha do R e achamos que é k;
buscamos a letra no cruzamento da coluna do E com a linha do A e achamos que é e;
buscamos a letra no cruzamento da coluna do M com a linha do I e achamos que é u;
buscamos a letra no cruzamento da coluna do P com a linha do O e achamos que é d;
buscamos a letra no cruzamento da coluna do E com a linha do R e achamos que é v;

buscamos a letra no cruzamento da coluna do S com a linha do A e achamos que é s;
buscamos a letra no cruzamento da coluna do T com a linha do I e achamos que é b;
buscamos a letra no cruzamento da coluna do A com a linha do O e achamos que é o;
buscamos a letra no cruzamento da coluna do D com a linha do R e achamos que é u;
buscamos a letra no cruzamento da coluna do E com a linha do A e achamos que é e.

A mensagem cifrada é então *"k e u d v s b o u e"*. A mensagem agora não é vulnerável à análise de frequência já que uma mesma letra do texto original é substituída por mais de uma no texto cifrado (t, por exemplo, é cifrado como k e b e a letra e é cifrada como e e v).

Para decifrar *"k e u d v s b o u e"*, procuramos a letra k na linha R e substituímos pela letra no topo da coluna, ou seja T; localizamos a letra e na linha A e substituímos pela letra no topo da coluna, E; procuramos a letra u na linha I e substituímos pela letra no topo da coluna, M; buscamos a letra d na linha O e substituímos pela primeira letra da coluna, ou seja P.

Repetindo o procedimento até a última letra do texto cifrado, obtemos o texto original *"tempestade"*.

2.1.4 A Matemática da Cifra de Vigenère

Em termos de aritmética modular a cifra de Vigenère é semelhante à cifra de César. Só que agora a chave é constituída de um conjunto de naturais $k = \{k_1, k_2, \ldots, k_m\}$, $0 \leq k_i < 26$, $i = 1, 2, 3, \ldots, m$. Uma mensagem $n_1 n_2 \ldots n_p$ é criptografada segundo o procedimento:

$C(n_1) = (n_1 + k_1) \bmod 26$;

$C(n_2) = (n_2 + k_2) \bmod 26$;

...

$C(n_{i-1}) = (n_{i-1} + k_m) \bmod 26$;

$C(n_i) = (n_i + k_1) \bmod 26$;

$C(n_{i+1}) = (n_{i+1} + k_2) \bmod 26$;

...

$C(n_p) = (n_p + k_j) \bmod 26$, para $1 \leq j \leq m$;

Vamos exemplificar cifrando e decifrando a frase 'Os números governam o mundo.' atribuída ao geômetra grego Pitágoras. Inicialmente fazemos uma pré-codificação (para dificultar a quebra do código) onde os dígrafos, se existirem, são substituídos por uma letra apenas ("ss"por "s", por exemplo) e também os acentos e os espaços entre as palavras são suprimidos. Como resultado obtemos o bloco único: *'osnumerosgovernamomundo'*. A cada letra do alfabeto fazemos corresponder um número do seguinte modo: $a = 0$, $b = 1$, $c = 2$, e assim por diante. Temos agora o bloco numérico (separamos com hífen para facilitar o entendimento do exemplo),

14-18-13-20-12-04-17-14-18-06-14-21-04-17-13-00-12-14-12-20-13-03-14

Usaremos como chave para cifragem a palavra **cateto**, que convertida em números é $k = \{02, 00, 19, 04, 19, 14\}$. Agora fazemos a codificação:

$$c(14) = (14 + 02) \bmod 26 = 16 \bmod 26 = 16$$
$$c(18) = (18 + 00) \bmod 26 = 18 \bmod 26 = 18$$
$$c(13) = (13 + 19) \bmod 26 = 32 \bmod 26 = 06$$
$$c(20) = (20 + 04) \bmod 26 = 24 \bmod 26 = 24$$
$$c(12) = (12 + 19) \bmod 26 = 31 \bmod 26 = 05$$
$$c(04) = (04 + 14) \bmod 26 = 18 \bmod 26 = 18$$

$$c(17) = (17 + 02) \bmod 26 = 19 \bmod 26 = 19$$
$$c(14) = (14 + 00) \bmod 26 = 14 \bmod 26 = 14$$
$$c(18) = (18 + 19) \bmod 26 = 37 \bmod 26 = 11$$
$$c(06) = (06 + 04) \bmod 26 = 10 \bmod 26 = 10$$
$$c(14) = (14 + 19) \bmod 26 = 33 \bmod 26 = 07$$
$$c(21) = (21 + 14) \bmod 26 = 35 \bmod 26 = 09$$
$$c(04) = (04 + 02) \bmod 26 = 06 \bmod 26 = 06$$
$$c(17) = (17 + 00) \bmod 26 = 17 \bmod 26 = 17$$
$$c(13) = (13 + 19) \bmod 26 = 32 \bmod 26 = 06$$
$$c(00) = (00 + 04) \bmod 26 = 04 \bmod 26 = 04$$
$$c(12) = (12 + 19) \bmod 26 = 31 \bmod 26 = 05$$
$$c(14) = (14 + 14) \bmod 26 = 28 \bmod 26 = 02$$
$$c(12) = (12 + 02) \bmod 26 = 14 \bmod 26 = 14$$
$$c(20) = (20 + 00) \bmod 26 = 20 \bmod 26 = 20$$
$$c(13) = (13 + 19) \bmod 26 = 32 \bmod 26 = 06$$
$$c(03) = (03 + 04) \bmod 26 = 07 \bmod 26 = 07$$
$$c(14) = (14 + 19) \bmod 26 = 33 \bmod 26 = 07$$

A sequência obtida,

16-18-06-24-05-18-19-14-11-10-07-09-06-17-06-04-05-02-14-20-06-07-07,

corresponde à mensagem encriptada *"q s g y f s t o l k h j g r g e f c o u g h h"*.

Deciframos com a mesma chave $k = \{02, 00, 19, 04, 19, 14\}$, observando que, se $a = c(\lambda) - k_i < 0$, então $d[c(\lambda)] = a \bmod 26 = (a + 26) \bmod 26$.

$$d(16) = (16 - 02) \bmod 26 = 14 \bmod 26 \Longrightarrow d(16) = 14$$
$$d(18) = (18 - 00) \bmod 26 = 18 \bmod 26 \Longrightarrow d(18) = 18$$
$$d(06) = (06 - 19) \bmod 26 = -13 \bmod 26 \equiv (-13 + 26) \bmod 26 \Longrightarrow d(06) = 13$$

$d(24) = (24 - 04) \bmod 26 = 20 \bmod 26 \Longrightarrow d(24) = 20$

$d(05) = (05-19) \bmod 26 = -14 \bmod 26 \equiv (-14+26) \bmod 26 \Longrightarrow d(05) = 12$

$d(18) = (18 - 14) \bmod 26 = 04 \bmod 26 \Longrightarrow d(18) = 04$

$d(19) = (19 - 02) \bmod 26 = 17 \bmod 26 \Longrightarrow d(19) = 17$

$d(14) = (14 - 00) \bmod 26 = 14 \bmod 26 \Longrightarrow d(14) = 14$

$d(11) = (11-19) \bmod 26 = -08 \bmod 26 \equiv (-8+26) \bmod 26 \Longrightarrow d(11) = 18$

$d(10) = (10 - 04) \bmod 26 = 06 \bmod 26 \Longrightarrow d(10) = 06$

$d(07) = (07-19) \bmod 26 = -12 \bmod 26 \equiv (-12+26) \bmod 26 \Longrightarrow d(07) = 14$

$d(09) = (09-14) \bmod 26 = -05 \bmod 26 \equiv (-5+26) \bmod 26 \Longrightarrow d(09) = 21$

$d(06) = (06 - 02) \bmod 26 = 04 \bmod 26 \Longrightarrow d(06) = 04$

$d(17) = (17 - 00) \bmod 26 = 17 \bmod 26 \Longrightarrow d(17) = 17$

$d(06) = (06-19) \bmod 26 = -13 \bmod 26 \equiv (-13+26) \bmod 26 \Longrightarrow d(06) = 13$

$d(04) = (04 - 04) \bmod 26 = 00 \bmod 26 \Longrightarrow d(04) = 00$

$d(05) = (05-19) \bmod 26 = -14 \bmod 26 \equiv (-14+26) \bmod 26 \Longrightarrow d(05) = 12$

$d(02) = (02-14) \bmod 26 = -12 \bmod 26 \equiv (-12+26) \bmod 26 \Longrightarrow d(02) = 14$

$d(14) = (14 - 02) \bmod 26 = 12 \bmod 26 \Longrightarrow d(14) = 12$

$d(20) = (20 - 00) \bmod 26 = 20 \bmod 26 \Longrightarrow d(20) = 20$

$d(06) = (06-19) \bmod 26 = -13 \bmod 26 \equiv (-13+26) \bmod 26 \Longrightarrow d(06) = 13$

$d(07) = (07 - 04) \bmod 26 = 03 \bmod 26 \Longrightarrow d(07) = 03$

$d(07) = (07-19) \bmod 26 = -12 \bmod 26 \equiv (-12+26) \bmod 26 \Longrightarrow d(07) = 14$

O resultado é o bloco original

14-18-13-20-12-04-17-14-18-06-14-21-04-17-13-00-12-14-12-20-13-03-14

cuja mensagem é a frase de Pitágoras *"Os números governam o mundo"*.

2.1.5 Cifrário de Hill

Essa cifra foi proposta em 1920 pelo americano Lester S. Hill (1891-1961) e utiliza o produto de matrizes. Vejamos como funciona. Primeiramente escolhe-se uma matriz quadrada K de ordem n com entradas k_{ij} tais que, $0 \leq k_{ij} < 26$,

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix}$$

Para cifrar um texto original X, primeiro quebramos o texto em blocos de n letras $(x_1x_2x_3 \dots x_n)$. Em seguida, obtemos o bloco cifrado $(y_1y_2y_3 \dots y_n)$ efetuando o produto matricial abaixo, módulo 26.

$$\begin{bmatrix} y_1 \\ y_2 \\ y_3 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1n} \\ k_{21} & k_{22} & \dots & k_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ k_{n1} & k_{n2} & \dots & k_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{bmatrix}$$

Caso o número de caracteres de X não seja múltiplo de n, completamos o último bloco com letras ao acaso. Também costuma-se acrescentar de 1 a $n-1$ letras aleatoriamente no final da mensagem cifrada para dificultar que se descubra o valor de n (se isso não fosse feito toda mensagem cifrada teria um número de caracteres múltiplo de n, o que facilitaria a vida do criptoanalista de plantão).

A mensagem original X é resgatada fazendo o produto da matriz K^{-1}, inversa de K mod 26, por cada bloco cifrado $(y_1y_2y_3 \dots y_n)$, operando módulo 26. Obviamente, a matriz K deve ser invertível em $\mathbb{Z}_{26}$, o que é verdadeiro se o determinante de K possuir inverso em $\mathbb{Z}_{26}$. Por exemplo, a matriz

$$A = \begin{bmatrix} 8 & 12 \\ 3 & 9 \end{bmatrix}$$

cujo determinante é $(\det A) \bmod 26 = 36 \bmod 26 = 10$ não é invertível em $\mathbb{Z}_{26}$, pois 10 e 26 não são co-primos e, portanto, 10 não tem inverso módulo 26. Já a matriz

$$B = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix}$$

cujo determinante (det B) mod 26 = 41 mod 26 = 15 é co-primo de 26, possui inversa

$$B^{-1} = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix}$$

A frase "A terra é azul"dita pelo cosmonauta soviético Iuri A. Gagarin (1934-1968), quando avistou nosso planeta pela janela de sua cápsula espacial, será usada como exemplo da cifra de Hill. Utilizaremos $n = 2$ e a matriz

$$K = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix}$$

como chave.

Na pré-codificação temos *'ateraeazul'* que corresponde a 00-19-04-17-00-04-00-25-20-11 utilizando a convenção estabelecida anteriormente para representação do alfabeto numericamente. Formamos então os blocos:

$$X_1 = \begin{bmatrix} 00 \\ 19 \end{bmatrix} X_2 = \begin{bmatrix} 04 \\ 17 \end{bmatrix} X_3 = \begin{bmatrix} 00 \\ 04 \end{bmatrix} X_4 = \begin{bmatrix} 00 \\ 25 \end{bmatrix} X_5 = \begin{bmatrix} 20 \\ 11 \end{bmatrix}$$

O próximo passo é a cifragem. Primeiro fazemos $Y_i' = KX_i$, $i \in \{1, 2, 3, 4, 5\}$. Depois calculamos $Y_i = Y_i'$ mod 26.

$$Y_1' = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 00 \\ 19 \end{bmatrix} = \begin{bmatrix} 95 \\ 152 \end{bmatrix}$$

$$Y_2' = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 04 \\ 17 \end{bmatrix} = \begin{bmatrix} 113 \\ 148 \end{bmatrix}$$

$$Y_3' = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 00 \\ 04 \end{bmatrix} = \begin{bmatrix} 20 \\ 32 \end{bmatrix}$$

$$Y_4' = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 00 \\ 25 \end{bmatrix} = \begin{bmatrix} 125 \\ 200 \end{bmatrix}$$

$$Y_5' = \begin{bmatrix} 7 & 5 \\ 3 & 8 \end{bmatrix} \begin{bmatrix} 20 \\ 11 \end{bmatrix} = \begin{bmatrix} 195 \\ 148 \end{bmatrix}$$

$Y_1 = Y_1' \bmod 26$

$$Y_1 = \begin{bmatrix} 17 \\ 22 \end{bmatrix}$$

$Y_2 = Y_2' \bmod 26$

$$Y_2 = \begin{bmatrix} 09 \\ 18 \end{bmatrix}$$

$Y_3 = Y_3' \bmod 26$

$$Y_3 = \begin{bmatrix} 20 \\ 06 \end{bmatrix}$$

$Y_4 = Y_4' \bmod 26$

$$Y_4 = \begin{bmatrix} 21 \\ 18 \end{bmatrix}$$

$Y_5 = Y_5' \bmod 26$

$$Y_5 = \begin{bmatrix} 13 \\ 18 \end{bmatrix}$$

Então a mensagem cifrada é 17-22-09-18-20-06-21-12-13-18. Em letras: *'r w j s u g v m n s'*.

Vamos agora decifrar com a matriz inversa $K^{-1} = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix}$. Primeiramente, calculamos $X_i' = K^{-1}Y_i$. Depois $X_i = X_i' \bmod 26$, com $00 \leq X_i \leq 25$. Vejamos,

$$Y_1 = \begin{bmatrix} 17 \\ 22 \end{bmatrix} Y_2 = \begin{bmatrix} 09 \\ 18 \end{bmatrix} Y_3 = \begin{bmatrix} 20 \\ 06 \end{bmatrix} Y_4 = \begin{bmatrix} 21 \\ 18 \end{bmatrix} Y_5 = \begin{bmatrix} 13 \\ 18 \end{bmatrix}$$

$$X_1' = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix} \begin{bmatrix} 17 \\ 22 \end{bmatrix} = \begin{bmatrix} 442 \\ 591 \end{bmatrix}$$

$$X_2' = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix} \begin{bmatrix} 09 \\ 18 \end{bmatrix} = \begin{bmatrix} 342 \\ 459 \end{bmatrix}$$

$$X_3' = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix} \begin{bmatrix} 20 \\ 06 \end{bmatrix} = \begin{bmatrix} 182 \\ 238 \end{bmatrix}$$

$$X_4' = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix} \begin{bmatrix} 21 \\ 18 \end{bmatrix} = \begin{bmatrix} 390 \\ 519 \end{bmatrix}$$

$$X_5' = \begin{bmatrix} 4 & 17 \\ 5 & 23 \end{bmatrix} \begin{bmatrix} 13 \\ 18 \end{bmatrix} = \begin{bmatrix} 358 \\ 479 \end{bmatrix}$$

$X_1 = X_1' \bmod 26$

$$X_1 = \begin{bmatrix} 00 \\ 19 \end{bmatrix}$$

$$X_2 = X_2' \bmod 26$$
$$X_2 = \begin{bmatrix} 04 \\ 17 \end{bmatrix}$$

$$X_3 = X_3' \bmod 26$$
$$X_3 = \begin{bmatrix} 00 \\ 04 \end{bmatrix}$$

$$X_4 = X_4' \bmod 26$$
$$X_4 = \begin{bmatrix} 00 \\ 25 \end{bmatrix}$$

$$X_5 = X_5' \bmod 26$$
$$X_5 = \begin{bmatrix} 20 \\ 11 \end{bmatrix}$$

O resultado 00-19-04-17-00-04-00-25-20-11, em letras *'ateraeazul'* é a mensagem original "A terra é azul".

2.2 Criptografia de Chave Pública

2.2.1 Introdução

Ao final da segunda guerra mundial e durante o período da chamada guerra fria, a criptografia consistia em métodos sofisticados de substituição utilizando uma chave previamente acertada entre o emissor e o receptor, que a utilizava para inverter o processo e decodificar a mensagem. Para que fosse eficiente, era necessário que o número de chaves disponíveis fosse muito grande, de modo que mesmo conhecendo o processo de substituição não fosse viável para um espião descobrir a chave por tentativas, mantendo seguro o conteúdo do texto cifrado. O problema com esse procedimento é que emissor e receptor precisavam combinar de antemão qual a chave a ser utilizada. Além disso, para que houvesse máxima segurança, essa chave deveria ser alterada com muita frequência, sendo ideal que fosse trocada a cada mensagem. Com isso chegou-se a um beco sem saída, pois o problema da troca de chaves de maneira segura parecia não ter solução. A frequência das trocas, a quantidade de chaves a ser distribuída e as distâncias entre os destinatários eram os obstáculos, além da insegurança causada pelo manuseio dessas chaves por terceiros. Durante a segunda guerra mundial os alemães usaram a máquina Enigma nos campos de batalha para codificar suas comunicações, transmitindo via rádio a chave juntamente com a mensagem cifrada. Foi isso que permitiu que os criptoanalistas poloneses, liderados por Marian Rejewski (1905-1980) iniciassem a quebra do código da Enigma. A partir da análise de muitas mensagens interceptadas e da comparação entre elas foi possível descobrir em que parte do texto cifrado se encontrava a chave o que deu início à quebra do código. Quando a Polônia foi invadida pelas tropas alemãs, os poloneses já haviam comunicado seus avanços em relação à Enigma aos franceses e ingleses, que dessa forma não tiveram de começar do zero. Em 1939, os criptoanalistas ingleses instalaram em Bletchley Park, Buckinghamshire, a Escola de Cifras e Códigos do Governo, onde trabalharam intensamente na quebra do código da Enigma. Foi lá que o brilhante Alan Turing (1912-1954), matemático e criptoanalista inglês, teve a idéia do que chamou *"máquina universal de Turing"* precursora do conceito do computador moderno.

Na segunda metade do século XX, o desenvolvimento tecnológico, com o advento do computador e das telecomunicações, acarretou um aumento no fluxo de informações sigilosas entre governos, empresas e pessoas o que pressionou ainda mais a logística da distribuição das chaves. A troca de chaves por meios convencionais, assim como as mensagens, estava sujeita a interceptação. Nessa época, as chaves eram entregues diretamente por bancos, governos e militares aos destinatários, utilizando mensageiros de

confiança. Era uma falha de segurança, pois as chaves podiam cair em mãos indevidas e além disso, esse expediente consumia cada vez mais recursos. O grande problema dos criptógrafos nessa época era a logística da distribuição de chaves, que infelizmente parecia ser insolucionável.

A crença geral era de que o problema da troca de chaves de maneira segura não tivesse solução. Foi então que, em 1976, os pesquisadores Whitfield Diffie e Martin Hellman publicaram um artigo onde descreveram um método pelo qual emissor e receptor podem combinar uma chave utilizando um canal inseguro, que mesmo sujeito a interceptação não permite a dedução da chave por um espião. O método de Diffie-Hellman mostrou que o problema da distribuição de chaves podia ser superado e lançou as bases da criptografia de chave pública, amplamente utilizada nas transações pela internet.

Diffie e Hellman encontraram na aritmética modular a solução que buscavam. Quando calculamos valores de uma função $f(x)$ usando a aritmética normal, esta função pode apresentar um comportamento previsível (crescente, decrescente, periódica, etc.). Agora, se calculamos os mesmos valores para a função modular correspondente a $f(x)$, ou seja, calculamos $f(x)$ mod m, $m \in \mathbb{N}$, $m > 1$, observamos que, em geral, a função modular não apresenta regularidade. Isto significa que com a aritmética normal, conhecendo $f(x)$ podemos inferir x por tentativas ou usando métodos computacionais, se necessário, baseados no comportamento da função. O mesmo não ocorre com a maioria das chamadas funções modulares, onde o conhecimento de $f(x)$ não ajuda em nada na dedução de x. Um exemplo disso é a função exponencial $y = a^x$. Na tabela 1 a seguir calculamos alguns valores da função exponencial de base $a = 3$ e na tabela 2 fazemos o mesmo para esta função módulo 7.

Aritmética Normal						
x	1	2	3	4	5	6
$f(x) = 3^x$	3	9	27	81	243	729

Tabela 1

Aritmética Modular						
x	1	2	3	4	5	6
$f(x) = 3^x \bmod 7$	3	2	6	4	5	1

Tabela 2

Podemos observar na tabela 1 que a função é crescente, ou seja, os valores de $f(x)$ aumentam à medida que x aumenta. Não ocorre nada semelhante no caso da função modular (tabela 2). Os valores de $f(x)$ neste caso variam aleatoriamente.

2.2.2 O Método de Diffie-Hellman

Considere o conjunto $\mathbb{Z}_p \backslash \{0\}$ dos inteiros módulo p menos o zero, sendo p um número primo, que representaremos por $\mathbb{Z}_p^*$:

$$\mathbb{Z}_p^* = \{1, \ldots, p-1\}.$$

Este conjunto, com a operação de multiplicação usual constitui uma estrutura algébrica denominada grupo, no caso o grupo multiplicativo dos inteiros módulo p. Existem elementos g em $\mathbb{Z}_p^*$ para os quais $\{g^i \bmod p : i = 1, \ldots, p-1\} = \mathbb{Z}_p^*$, ou seja, elementos que geram o conjunto. Tais elementos g são chamados geradores de $\mathbb{Z}_p^*$. Por exemplo, $3 \in \mathbb{Z}_7^*$ é um gerador, pois $\{3^i \bmod 7 : i = 1, \ldots, 6\} = \mathbb{Z}_7^*$, como podemos ver abaixo:

$3^6 = 729 \equiv 1 \bmod 7$;

$3^2 = 9 \equiv 2 \bmod 7$;

$3^1 = 3 \bmod 7$;

$3^4 = 81 \equiv 4 \bmod 7$;

$3^5 = 243 \equiv 5 \bmod 7$;

$3^3 = 27 \equiv 6 \bmod 7$.

Pois bem, suponha que Alice e Bob queiram combinar uma chave por telefone. Primeiro um liga para o outro e eles escolhem um número primo p e um gerador g do grupo multiplicativo $\mathbb{Z}_p^*$. Depois cada um faz o seguinte:

1) Alice escolhe um número x_A, $1 < x_A < p-1$, e calcula $y_A = g^{x_A} \bmod p$. Depois ela informa o resultado y_A para Bob, mantendo em segredo o valor de x_A.

2) Bob, por sua vez, faz o mesmo escolhendo um número x_B, $1 < x_B < p-1$, e calculando $y_B = g^{x_B} \bmod p$. Ele informa apenas o resultado y_B para Alice mantendo secreto o valor de x_B.

3) Agora ambos calculam a chave:

Alice toma o valor de y_B informado por Bob e faz

$$(y_B)^{x_A} \bmod p = (g^{x_B})^{x_A} \bmod p = g^{x_B x_A} \bmod p = K$$

Bob por sua vez calcula

$$(y_A)^{x_B} \bmod p = (g^{x_A})^{x_B} \bmod p = g^{x_A x_B} \bmod p = K$$

obtendo a mesma chave K.

Por exemplo, Bob liga para Alice e eles combinam usar o primo $p = 7$ e o gerador $g = 3$. Então Alice pode escolher, por exemplo, $x_A = 2$ e Bob, $x_B = 3$. Vejamos:

1) Alice calcula $y_A = 3^2 \bmod 7 = 2 \Longrightarrow y_A = 2$.

2) Bob calcula $y_B = 3^3 \bmod 7 = 6 \Longrightarrow y_B = 6$.

Eles voltam a se falar por telefone e trocam os valores de $y_A = 2$ e $y_B = 6$.

3) Agora Alice faz $(y_B)^{x_A} = 6^2 = 36 \bmod 7 = 1$ e obtém a chave $K = 1$.

4) Bob por sua vez calcula $(y_A)^{x_B} = 2^3 = 8 \bmod 7 = 1$, obtendo a mesma chave $K = 1$.

Evidentemente, escolhemos o primo p muito grande, de modo que o grupo $\mathbb{Z}_p^*$ possua muitos elementos x, tais que $1 < x < p-1$.

Vamos analisar agora o problema da escuta. Caso alguém intercepte a ligação de Alice e Bob vai ter acesso ao primo p, ao gerador g, a y_A e a y_B. Escolhendo p suficientemente grande, o número de possibilidades para $1 < x < p - 1$ é também muito elevado. Além disso, é muito difícil calcular a inversa da função exponencial módulo p ($x = \log_g y \bmod p$), pois como sabemos a função exponencial módulo p não tem comportamento previsível. Desse modo, não é possível para um espião determinar x_A nem x_B e, mesmo utilizando um canal inseguro, o método permite a Alice e Bob acertar uma chave criptográfica com segurança.

Capítulo 3

Criptografia RSA

3.1 Introdução

Em 1977 Ronald Rivest, Adi Shamir e Leonard Adleman apresentaram à comunidade científica o método que ficaria conhecido como criptografia RSA. A criptografia de chave pública RSA tornou-se a mais utilizada na internet em transações comerciais e na codificação de mensagens que circulam pela rede. O método se baseia em uma função exponencial modular $C(X) = X^e \bmod n$. Nesta função, X é o bloco a ser codificado (um número inteiro, obtido após um processo de pré-codificação que consiste na substituição das letras da mensagem original por números, encadeados em um único grande número que depois é quebrado em blocos cujo valor é menor do que n). O par de números (n, e) é a chave pública do destinatário da mensagem, n consiste no produto de dois números primos p e q muito grandes, da ordem de 100 dígitos cada enquanto e é um expoente escolhido de maneira que exista o seu inverso $d \bmod (p-1) \cdot (q-1)$. Obviamente, os números primos p e q são de conhecimento exclusivo do usuário do RSA, que os utiliza para obter o expoente d com o qual decodifica as mensagens que recebe segundo a fórmula $D(C) = C^d \bmod n$. Uma vez obtido o expoente d, os primos p e q não são mais necessários, podendo ser descartados. A segurança do método consiste na dificuldade de fatorar o produto de números primos muito grandes (da ordem de 100 dígitos decimais), mesmo tendo à disposição recursos computacionais. Para se ter uma idéia, o tempo estimado para a fatoração do produto de dois primos dessa magnitude supera, em muito, a idade do universo e só poderia ser realizada num tempo aceitável por um computador quântico, uma tecnologia que ainda está mais no plano teórico do que no operacional.

Uma ressalva deve ser feita, com relação à segurança, no que diz respeito a mensagens falsas que podem ser enviadas para o usuário do RSA. Como a chave pública (n, e) é acessível a qualquer pessoa, as mensagens recebidas devem ser verificadas quanto à origem. Isto é feito utilizando-se uma *assinatura digital*. O remetente também deve possuir uma chave pública (n', e') e uma chave privada d', com a qual assina digitalmente a mensagem, ou seja, o remetente cifra a *assinatura digital* com sua chave privada d', à qual somente ele tem acesso, e o destinatário decifra a *assinatura digital* com a chave pública (n', e') do remetente. Procedendo assim, fica garantida a procedência da mensagem.

3.2 A matemática do RSA

O primeiro passo para implementar o método criptográfico RSA é a escolha dos primos p e q. Por questões de segurança, é preciso que esses primos sejam grandes, da ordem de 100 dígitos decimais. Isto é feito gerando-se aleatoriamente números inteiros ímpares de 100 dígitos e testando sua primalidade por meios computacionais. Felizmente, a densidade de números primos entre os inteiros de 100 dígitos é bastante grande e os algoritmos para teste de primalidade oferecem uma margem de erro muito pequena. Podemos demonstrar a alta densidade de primos de 100 dígitos decimais a partir do "Teorema dos Números Primos"que diz que, sendo $\pi(n)$ o número de inteiros menores do que n e primos relativos de n (dois inteiros são primos relativos quando o máximo divisor comum entre eles é 1), então

$$\pi(n) \sim \frac{n}{\ln n} \quad , quando\, n \longrightarrow \infty$$

Se n é um inteiro com 100 dígitos então $10^{99} \leq n < 10^{100}$, o que significa que o número de primos no intervalo acima é aproximadamente,

$$\pi(10^{100}) - \pi(10^{99}) = \frac{10^{100}}{\ln 10^{100}} - \frac{10^{99}}{\ln 10^{99}} \approx 4 \times 10^{97}$$

Para se ter uma idéia da magnitude desse número vamos fazer cálculos. A densidade do universo é equivalente a aproximadamente 5,9 prótons por metro cúbico [1] enquanto o raio do universo conhecido é atualmente estimado

[1] http://map.gsfc.nasa.gov/universe/uni_matter.html 02/03/2013 23H29min.

em aproximadamente 14 bilhões de anos-luz [2]. A luz percorre 3×10^8 metros a cada segundo, o que significa que o raio do universo, em metros, é

$$(14 \times 10^9) \times (60 \times 60 \times 24 \times 365) \times (3 \times 10^8) \approx 1,3 \times 10^{26}$$

Considerando um universo esférico, o seu volume seria

$$\frac{4}{3}\pi r^3 = \frac{4}{3}\pi(1,3 \times 10^{26})^3 \approx 10^{79}\ m^3$$

Pois bem, sendo a densidade do universo aproximadamente 6 prótons por m^3 teríamos $6 \times 10^{79} \approx 10^{80}$ prótons no universo.

Comparando este resultado com o obtido para o número de primos com 100 dígitos decimais, observamos que o número de primos é 10^{17} vezes maior. Portanto existe uma quantidade enorme de primos de 100 dígitos decimais disponíveis. A densidade de primos no intervalo de 10^{99} a 10^{100} é

$$4 \times 10^{97} \div (10^{100} - 10^{99}) \approx \frac{4}{1000} = \frac{1}{250}$$

Para obter primos dessa ordem gera-se aleatoriamente um inteiro ímpar com 100 dígitos e testa-se a sua primalidade utilizando recursos computacionais. O algoritmo mais utilizado para testar a primalidade é o Miller-Rabin que retorna se o inteiro é ou não primo com probabilidade de erro de 1/4 se o resultado for positivo para número primo. O que se faz é testar várias vezes o número e a cada vez que o algoritmo retorna que ele é primo a probabilidade de erro diminui. Para n rodadas, a probabilidade de erro é $(1/4)^n$.

De posse dos primos p e q, calculamos $n = pq$ e o valor da função ϕ de Euler para n, que no caso é $\phi(n) = (p-1)(q-1)$. Testamos até obter um valor e, tal que o mdc [e, $\phi(n)$] = 1. O par de números (n, e) constituirá a chave pública necessária para encriptar as mensagens endereçadas ao usuário do RSA. Em seguida, calculamos $d = e^{-1} \bmod \phi(n)$ que é a chave privada necessária para decriptar as mensagens recebidas e que deve ser mantida em sigilo, assim como os primos p e q. Quem quiser mandar uma mensagem usará a chave pública (n, e) da seguinte maneira. Após uma pré-codificação a mensagem é convertida em um único bloco numérico $N = N_1N_2N_3 \ldots N_k$, com $N_i < n$, para $i = 1, 2, 3, \ldots k$ (N_i deve ser menor do que n para que o resultado da decodificação seja exatamente a mensagem original) ao qual aplicamos

$$C(N_i) = N_i^e \bmod n$$

[2] http://map.gsfc.nasa.gov/universe/uni_expansion.html 03/03/2013 00H09min.

A mensagem recebida $C(N)$ é então decodificada fazendo

$$D[C(N_i)] = C(N_i)^d \bmod n = (N_i^e)^d \bmod n = N_i \bmod n = N_i$$

Observação: A pré-codificação de N é feita utilizando-se a tabela ASCII (*American Standard Code for Information Interchange*). Esta tabela é composta por 256 números binários de 8 dígitos cada e contém as letras maiúsculas e minúsculas (na base 10, respectivamente de 65 até 90 e de 97 a 122), além dos caracteres alfabéticos acentuados, sinais de pontuação, etc.

decimal	binário	hexadecimal	símbolo
56	00111000	38	8
57	00111001	39	9
58	00111010	3A	:
59	00111011	3B	;
60	00111100	3C	<
61	00111101	3D	=
62	00111110	3E	>
63	00111111	3F	?
64	01000000	40	@
65	01000001	41	A
66	01000010	42	B

Uma parte da tabela ASCII.

3.3 Uma Função e dois Teoremas Importantes

A quantidade de números inteiros menores e relativamente primos de um inteiro a, $a > 1$, é dada por uma função chamada função *fi* de Euler, $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}$, onde $\mathbb{N}^*$ denota o conjunto dos naturais menos o zero ($\mathbb{N}^* = \mathbb{N} \setminus \{0\}$). Para $a, b \in \mathbb{N}^*$ e $mdc(a, b) = 1$, a função ϕ é multiplicativa, ou seja, $\phi(ab) = \phi(a) \cdot \phi(b)$. Sendo p primo, $\phi(p) = p - 1$. Assim, o número de inteiros menores e relativamente primos de $n = pq$, p e q primos, é $\phi(n) = (p - 1) \cdot (q - 1)$.

Teorema 2. *Sejam $a, b \in \mathbb{N}^*$ e $mdc(a, b) = 1$. Então $\phi(ab) = \phi(a) \cdot \phi(b)$.*

Demonstração. Observe que $mdc(c, ab) = 1$, se, e somente se, $mdc(c, a) = 1$ e $mdc(c, b) = 1$. Portanto, dispondo os números de 1 a ab na tabela abaixo com b linhas e a colunas devemos verificar quais são co-primos de a e de b.

$$\begin{array}{ccccccc} 1 & 2 & 3 & \dots & a-1 & a \\ a+1 & a+2 & a+3 & \dots & a+(a-1) & 2a \\ 2a+1 & 2a+2 & 2a+3 & \dots & 2a+(a-1) & 3a \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \dots & (b-1)a+(a-1) & ba \end{array}$$

O elementos das colunas são da forma $ka + j$ com $0 \leq k \leq b-1$ e $1 \leq j \leq a$. Se j não for co-primo de a então todos os elementos da coluna j também não são co-primos de a. Portanto os elementos co-primos de a estão nas $\phi(a)$ colunas restantes.

Como $mdc(a, b) = 1$, os elementos das colunas j formam um sistema completo de resíduos módulo b,

$$ka + j \equiv k'a + j \bmod b \iff ka \equiv k'a \bmod b \iff k \equiv k' \bmod b$$

e portanto, $\phi(b)$ deles são co-primos de b. Logo, o número de elementos co-primos de a e co-primos de b na tabela é $\phi(a) \cdot \phi(b)$.

□

Teorema 3 (Fermat)**.** *Sejam p um número primo, r e s côngruos módulo $(p-1)$.*

1. Se um número inteiro a não for divisível por p, então

$$a^{p-1} \equiv 1 \bmod p$$

$$a^r \equiv a^s \bmod p$$

2. Se $r > 0$ e $s > 0$ então, para todo $a \in \mathbb{Z}$

$$a^r \equiv a^s \bmod p.$$

Demonstração. 1. Considere o conjunto $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ dos números $x \in \mathbb{Z}_p$ que são primos com p. Como p não divide a, se $x \in \mathbb{Z}_p^*$, então $ax \bmod p \in \mathbb{Z}_p^*$. Isto significa que a função $f\colon \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$, tal que $f(x) = ax \bmod p$ é injetora e o conjunto imagem é um rearranjo de $\mathbb{Z}_p^*$. Portanto, são iguais os produtos

$$f(1) \times f(2) \times \ldots \times f(p-1) = 1 \times 2 \times \ldots \times (p-1),$$

ou seja,

$$1a \times 2a \times \ldots \times (p-1)a \bmod p = 1 \times 2 \times \ldots \times (p-1) \bmod p$$

Multiplicando ambos os lados pelos inversos módulo p de 2 a $p-1$, obtemos

$$a^{p-1} \bmod p = 1 \quad \Longrightarrow \quad a^{p-1} \equiv 1 \bmod p.$$

Agora

$$r \equiv s \bmod (p-1) \quad \Longrightarrow \quad r = k(p-1) + s$$

e

$$a^r \equiv a^{k(p-1)+s} \equiv (a^{p-1})^k \cdot a^s \equiv 1^k \cdot a^s \equiv a^s \bmod p \quad \Longrightarrow \quad a^r \equiv a^s \bmod p.$$

2. Se p não divide a, já mostramos que $a^r \equiv a^s \bmod p$. Se p divide a, as potências de a módulo p de expoente negativo não existem (pois $a \equiv 0 \bmod p$) e as potências de a módulo p de expoente positivo são congruentes a zero módulo p, ou seja, são iguais. Isso prova que $a^r \equiv a^s \bmod p$ para qualquer a inteiro.

□

Teorema 4 (Euler)**.** *Sejam $n \geq 2$, $n \in \mathbb{Z}$, r e s côngruos módulo $\phi(n)$.*

1. Se a e n forem primos entre si,

$$a^{\phi(n)} \equiv 1 \bmod n$$

$$a^r \equiv a^s \bmod n$$

2. Se n for produto de primos distintos, $r > 0$ e $s > 0$, então

$$a^r \equiv a^s \bmod n, \forall a \in \mathbb{Z}.$$

Demonstração. 1. A demonstração é análoga à do Teorema de Fermat. Sendo $\mathbb{Z}_n^*$ o conjunto dos elementos inversíveis de $\mathbb{Z}_n$, a função f: $\mathbb{Z}_n^* \longrightarrow \mathbb{Z}_n^*$, tal que $f(x) = ax \bmod n$ é injetora e o conjunto $\{ax \bmod n : x \in \mathbb{Z}_n^*\}$ é igual a $\mathbb{Z}_n^*$. Desse modo, são iguais os produtos

$$\left(\prod_{x \in \mathbb{Z}_n^*} ax\right) \bmod n = \left(\prod_{x \in \mathbb{Z}_n^*} x\right) \bmod n$$

ou seja,

$$a^{\phi(n)} \left(\prod_{x \in \mathbb{Z}_n^*} x\right) \bmod n = \left(\prod_{x \in \mathbb{Z}_n^*} x\right) \bmod n$$

Multiplicando ambos os lados da igualdade acima pelos inversos $x^{-1} \bmod n$ de cada $x \in \mathbb{Z}_n^*$, obtemos

$$a^{\phi(n)} \bmod n = 1 \quad \Longrightarrow \quad a^{\phi(n)} \equiv 1 \bmod n$$

2. Se $n = p_1 p_2 \dots p_k$, onde $p_i \neq p_j$, $\forall\, i, j$ com $1 \leq i, j \leq k$

$$\phi(n) = \phi(p_1)\phi(p_2)\dots\phi(p_k) = (p_1 - 1)(p_2 - 1)\dots(p_k - 1)$$

Como $r \equiv s \bmod \phi(n)$, então $r \equiv s \bmod (p_i - 1)$, $i = 1, 2, ..., k$. Pelo teorema de Fermat, $r \equiv s \bmod (p_i - 1)$ implica $a^r \equiv a^s \bmod p_i$, ou seja, p_i divide $a^r - a^s$, para $i = 1, 2, ..., k$ o que significa que n divide $a^r - a^s$ e consequentemente $a^r \equiv a^s \bmod n$. □

A função de Euler, bem como o teorema de Fermat e o teorema de Euler são muito importantes. O teorema de Fermat facilita o cálculo de potências módulo n, n inteiro positivo, e o teorema de Euler (generalização do teorema de Fermat) está no centro do método criptográfico RSA.

3.4 Como Funciona a Criptografia RSA

Neste ponto, podemos entender como tudo funciona:

1) Primeiro escolhemos dois primos p e q suficientemente grandes.

2) Depois fazemos $n = pq$ e calculamos $k = \phi(n) = (p-1)(q-1)$.

3) Escolhemos ao acaso um inteiro e, $1 < e < k$ e verificamos se $mdc(e, k) = 1$, o que significa que e tem inverso módulo k. Caso contrário, escolhemos outro e até encontrar um que seja invertível módulo k.

4) Calculamos $d = e^{-1} mod\ k$. A chave secreta utilizada pelo usuário do RSA para decifrar as mensagens que recebe é um inteiro positivo d, tal que $ed \equiv 1 \bmod k$, onde $k = \phi(n)$. Ou seja, d é o inverso de e módulo k. Tomando e, tal que $mdc(e, k) = 1$, existem d e b inteiros, tais que

$$de + bk = 1 \Longrightarrow de \bmod k + bk \bmod k = 1 \Longrightarrow$$

$$de \bmod k = 1 \Longrightarrow d = e^{-1} \bmod k.$$

Observação: Os inteiros d e b acima são determinados aplicando o algoritmo estendido de Euclides a e e k e fazendo substituições sucessivas nas igualdades até obter a equação $de + bk = 1$. Para valores elevados de e e k, como ocorre na criptografia RSA, usamos um programa para realizar o algoritmo estendido de Euclides. Devido à velocidade de processamento e do algoritmo, o resultado é obtido em segundos.

5) Divulgamos a chave pública (n, e) na internet e mantemos em sigilo a chave privada d e também os primos p e q, que podem até ser esquecidos.

Vejamos como utilizamos o RSA para cifrar e decifrar:

Para cifrar:

1) Transformamos a mensagem em blocos numéricos (menores do que n, para que a decifragem retorne o bloco cifrado e não

outro congruente a ele módulo n).

2) Ciframos um bloco M calculando $c(M) = M^e \bmod n$.

Para decifrar:

1) O destinatário, de posse da chave privada d, calcula para cada bloco $c(M)$, $d[c(M)] = [c(M)]^d \bmod n$ e fazendo isso obtém a mensagem original.

$$d[c(M)] = [c(M)]^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n \equiv$$

$$M^{s\cdot\phi(n)+1} \bmod n = [(M^{\phi(n)})^s \cdot M^1] \bmod n \equiv$$

$$(1^s \cdot M) \bmod n = M \bmod n = M.$$

3.4.1 Algoritmo Estendido de Euclides

Lema 1 (Euclides)**.** Sejam $a, b, n \in \mathbb{N}$ tais que $a < na < b$. Então $mdc(a, b) = mdc(a, b - na)$.

Demonstração. Seja $d = mdc(a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que $d|b = b - na + na$. Portanto d é divisor comum de a e b. Seja c um divisor comum de a e b, então c é divisor comum de a e $b - na$, logo, $c|d$ o que prova que $d = mdc(a, b)$. □

Algoritmo Estendido de Euclides

Dados $a, b \in \mathbb{N}$, podemos supor $a \leq b$. Então, se $a = 1$, ou $a = b$, ou $a|b$, o $mdc(a, b) = a$. Supondo que $1 < a < b$ e $a \nmid b$, podemos escrever

$$b = aq_1 + r_1, \quad \text{com } r_1 < a.$$

Se $r_1|a$, pelo lema de Euclides $r_1 = mdc(a, r_1) = mdc(a, b - aq_1) = mdc(a, b)$. Caso contrário, fazemos a divisão de a por r_1, obtendo

$$a = r_1q_2 + r_2, \quad \text{com } r_2 < r_1.$$

Novamente, se $r_2|r_1$, então

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

$mdc(a, b - aq_1) = mdc(a, b)$.

Caso contrário, fazemos a divisão de r_1 por r_2, obtendo

$r_1 = q_3 r_2 + r_3, \quad \text{com } r_3 < r_2.$

Repetimos o processo até obter o $mdc(a, b)$. Pela Propriedade da Boa Ordem, a sequência dos naturais $a > r_1 > r_2 > r_3 > \ldots$ possui mínimo, ou seja, para algum n, temos que $r_n | r_{n-1}$ e o $mdc(a, b) = r_n$. A partir das equações obtidas no algoritmo estendido de Euclides pode-se obter inteiros x e y, tais que

$$ax + by = mdc(a, b)$$

A existência de x e y que satisfazem a equação é garantida pelo Teorema de Bézout, cuja demonstração pode ser encontrada na referência bibliográfica [4].

Exemplo

Obter o inverso de 18, módulo 1247.

Solução

$1247 = 69 \times 18 + 5 \quad (1)$
$18 = 3 \times 5 + 3 \quad (2)$
$5 = 1 \times 3 + 2 \quad (3)$
$3 = 1 \times 2 + 1 \quad (4)$
$2 = 2 \times 1 + 0 \Longrightarrow mdc(1247, 18) = 1$

De (4): $3 - 2 = 1 \quad (5)$

De (3): $2 = 5 - 3$, substituindo em (5): $3 - (5 - 3) = 1 \Longrightarrow$
$2 \times 3 - 5 = 1 \quad (6)$

De (2): $3 = 18 - 3 \times 5$, substituindo em (6): $2 \times (18 - 3 \times 5) - 5 = 1 \Longrightarrow$
$2 \times 18 - 7 \times 5 = 1 \quad (7)$

De (1): $5 = 1247 - 69 \times 18$, substituindo em (7): $2 \times 18 - 7 \times (1247 - 69 \times 18) = 1$

$\Longrightarrow (2 + 7 \times 69) \times 18 - 7 \times 1247 = 485 \times 18 - 7 \times 1247 = 1$

Aplicando módulo, temos

$(485 \times 18) \bmod 1247 - (7 \times 1247) \bmod 1247 = 1 \Longrightarrow (485 \times 18) \bmod 1247 = 1$

$\Longrightarrow 18^{-1} \bmod 1247 = 485$

Exemplo

Calcular d, tal que $19d = 1 \bmod 120$ (observe que $mdc(19, 120) = 1$).

Solução

Aplicando o algoritmo estendido de Euclides obtemos as igualdades:

$120 = 19 \times 6 + 6 \Longrightarrow 6 = 120 - 19 \times 6$ (1)

$19 = 6 \times 3 + 1 \Longrightarrow 19 - 6 \times 3 = 1$ (2)

Substituindo (1) em (2),

$19 - (120 - 19 \times 6) \times 3 = 1 \Longrightarrow 19 \times 19 - 120 \times 3 = 1$ (3)

Agora aplicamos módulo em (3) para achar o inverso de 19 mod 120.

$(19 \times 19) \bmod 120 - (120 \times 3) \bmod 120 = 1 \Longrightarrow$

$(19 \times 19) \bmod 120 = 1 \Longrightarrow 19^{-1} \bmod 120 = 19.$

Ou seja, 19 é seu próprio inverso módulo 120.

3.5 Exemplificando o uso da RSA

Como exemplo do uso da criptografia RSA, vamos codificar e decodificar a palavra *"enigma"*. Para fins didáticos e para facilitar as contas utilizaremos números primos bem pequenos. Tomando $p = 11$ e $q = 13$, o valor de n será $n = 11 \cdot 13 = 143$. Associamos a cada letra do alfabeto

um número inteiro a partir de 10 ($a = 10$, $b = 11$, $c = 12$ e assim por diante). Neste caso, ficamos com *"enigma"*= 142318162210, que dividiremos em blocos. O tamanho de cada bloco a ser cifrado, assim como o tamanho de cada bloco a ser decifrado é estabelecido previamente. Para garantir que cada bloco a ser cifrado seja menor do que n, tomamos os blocos com um algarismo decimal a menos do que n. No caso do exemplo, como $n = 143$ tem três algarismos decimais, dividimos a mensagem em blocos com dois dígitos apenas. Ficamos então com os blocos 14-23-18-16-22-10. Estes blocos depois de cifrados podem ter de um a três algarismos, então convencionamos que os blocos cifrados terão todos o tamanho de n, no caso, três algarismos. Aqueles com dois ou um algarismo apenas serão completados com zeros à esquerda, que serão desprezados quando for feita a decifração.

Para cifrar cada bloco X usamos a fórmula $C(X) = X^e \bmod 143$. Para isso, escolhemos o expoente $e = 7$ (co-primo de $\phi(n) = 10 \cdot 12 = 120$, logo possui inverso módulo $\phi(n)$). A chave pública é então $(n, e) = (143, 7)$.

Primeiro, escrevemos o expoente $e = 7$ na base 2:

$$7 = 111_2 = 2^2 + 2^1 + 2^0 = 4 + 2 + 1$$

Ciframos os dois primeiros blocos, os demais são cifrados de modo análogo:

$C(14) = 14^7 \bmod 143 = (14^{4+2+1}) \bmod 143 =$

$(14^4 \times 14^2 \times 14) \bmod 143 =$

$(14^4 \bmod 143 \times 14^2 \bmod 143 \times 14 \bmod 143) \bmod 143$

Mas,

$14^2 \bmod 143 = 196 \bmod 143 = 53$

$14^4 \bmod 143 = (14^2)^2 \bmod 143 = (14^2 \bmod 143)^2 \bmod 143 =$

$53^2 \bmod 143 = 2809 \bmod 143 = 92$

Então,

$C(14) = (92 \times 53 \times 14) \bmod 143 =$

$[(92 \times 53) \bmod 143 \times 14] \bmod 143 =$

$[(4876 \bmod 143) \times 14] \bmod 143 =$

$(14 \times 14) \bmod 143 = 196 \bmod 143 = 53$

$C(14) = 53;$

$C(23) = 23^7 \bmod 143 = (23^{4+2+1}) \bmod 143 =$

$(23^4 \times 23^2 \times 23) \bmod 143 =$

$(23^4 \bmod 143 \times 23^2 \bmod 143 \times 23 \bmod 143) \bmod 143$

Mas,

$23^2 \bmod 143 = 529 \bmod 143 = 100$

$23^4 \bmod 143 = (23^2)^2 \bmod 143 = (23^2 \bmod 143)^2 \bmod 143 =$

$100^2 \bmod 143 = 10000 \bmod 143 = 133$

Então,

$C(23) = (133 \times 100 \times 23) \bmod 143 =$

$[(133 \times 100) \bmod 143 \times 23] \bmod 143 =$

$[(13300 \bmod 143) \times 23] \bmod 143 =$

$(1 \times 23) \bmod 143 = 23 \bmod 143 = 23$

$C(23) = 23.$

O resultado, cifrando-se todos os blocos, é 53-23-138-3-22-10.

De acordo com a convenção estabelecida para o tamanho dos blocos, acrescentamos zeros à esquerda aos blocos com menos de três algarismos decimais e a mensagem transmitida é 053-023-138-003-022-010.

Vejamos agora como decifrar a mensagem. Primeiramente, calculamos d, tal que $7d = 1 \bmod k$, $k = \phi(143)$, usando o algoritmo estendido de Euclides.

$e = 7 \qquad k = \phi(143) = 120$

$120 = 17 \times 7 + 1 \Longrightarrow -17 \times 7 + 1 \times 120 = 1 \Longrightarrow$

$(-17 \times 7) \bmod 120 + (1 \times 120) \bmod 120 = 1 \Longrightarrow$

$(-17 \times 7) \bmod 120 = 1 \Longrightarrow 7^{-1} \bmod 120 = -17 \equiv 103 \Longrightarrow$

$d = 103$

A função modular que decodifica é, então, $D(C) = C^{103} \bmod 143$. Para decifrar, primeiro escrevemos o expoente $d = 103$ na base 2:

$$103 = 1100111_2 = 2^6 + 2^5 + 2^2 + 2^1 + 2^0 = 64 + 32 + 4 + 2 + 1$$

A mensagem recebida é quebrada em blocos com a mesma quantidade de dígitos de n (três, no exemplo) e os zeros à esquerda nestes blocos são desprezados. A seguir, decifamos os dois primeiros blocos de 053-023-138-003-022-010, os demais são decifrados de maneira análoga:

$D(53) = 53^{103} \bmod 143 = (53^{64+32+4+2+1}) \bmod 143 =$

$(53^{64} \times 53^{32} \times 53^4 \times 53^2 \times 53) \bmod 143 =$

$[(53^{64} \bmod 143) \times (53^{32} \bmod 143) \times (53^4 \bmod 143) \times (53^2 \bmod 143) \times$

$(53 \bmod 143)] \bmod 143$

$53^2 \bmod 143 = 2809 \bmod 143 = 92$

$53^4 \bmod 143 = (53^2)^2 \bmod 143 = (53^2 \bmod 143)^2 \bmod 143 =$

$92^2 \bmod 143 = 8464 \bmod 143 = 27$

$53^8 \bmod 143 = (53^4)^2 \bmod 143 = (53^4 \bmod 143)^2 \bmod 143 =$

$27^2 \bmod 143 = 729 \bmod 143 = 14$

$53^{16} \bmod 143 = (53^8)^2 \bmod 143 = (53^8 \bmod 143)^2 \bmod 143 =$

$14^2 \bmod 143 = 196 \bmod 143 = 53$

$53^{32} \bmod 143 = (53^{16})^2 \bmod 143 = (53^{16} \bmod 143)^2 \bmod 143 =$

$53^2 \bmod 143 = 2809 \bmod 143 = 92$

$53^{64} \bmod 143 = (53^{32})^2 \bmod 143 = (53^{32} \bmod 143)^2 \bmod 143 =$

$92^2 \bmod 143 = 8464 \bmod 143 = 27$

$D(53) = (27 \times 92 \times 27 \times 92 \times 53) \bmod 143 \Longrightarrow$

$D(53) = [(27 \times 92) \bmod 143 \times (27 \times 92) \bmod 143 \times 53] \bmod 143 \Longrightarrow$

$D(53) = [(2484 \bmod 143) \times (2484 \bmod 143) \times 53] \bmod 143 \Longrightarrow$

$D(53) = (53 \times 53 \times 53) \bmod 143 =$

$D(53) = [(53 \times 53) \bmod 143 \times 53] \bmod 143 \Longrightarrow$

$D(53) = [(2809 \bmod 143) \times 53] \bmod 143 \Longrightarrow$

$D(53) = (92 \times 53) \bmod 143 \Longrightarrow$

$D(53) = 4876 \bmod 143 = 14$

$D(53) = 14;$

$D(23) = 23^{103} \bmod 143 = (23^{64+32+4+2+1}) \bmod 143 =$

$(23^{64} \times 23^{32} \times 23^4 \times 23^2 \times 23) \bmod 143 =$

$[(23^{64} \bmod 143) \times (23^{32} \bmod 143) \times (23^4 \bmod 143) \times (23^2 \bmod 143) \times$

$(23 \bmod 143)] \bmod 143$

$23^2 \bmod 143 = 529 \bmod 143 = 100$

$23^4 \bmod 143 = (23^2)^2 \bmod 143 = (23^2 \bmod 143)^2 \bmod 143 =$

$100^2 \bmod 143 = 10000 \bmod 143 = 133$

$23^8 \bmod 143 = (23^4)^2 \bmod 143 = (23^4 \bmod 143)^2 \bmod 143 =$

$133^2 \bmod 143 = 17689 \bmod 143 = 100$

$23^{16} \bmod 143 = (23^8)^2 \bmod 143 = (23^8 \bmod 143)^2 \bmod 143 =$

$100^2 \bmod 143 = 10000 \bmod 143 = 133$

$23^{32} \bmod 143 = (23^{16})^2 \bmod 143 = (23^{16} \bmod 143)^2 \bmod 143 =$

$133^2 \bmod 143 = 17689 \bmod 143 = 100$

$23^{64} \bmod 143 = (23^{32})^2 \bmod 143 = (23^{32} \bmod 143)^2 \bmod 143 =$

$100^2 \bmod 143 = 10000 \bmod 143 = 133$

$D(23) = (133 \times 100 \times 133 \times 100 \times 23) \bmod 143 \Longrightarrow$

$D(23) = [(133 \times 100) \bmod 143 \times (133 \times 100) \bmod 143 \times 23] \bmod 143 \Longrightarrow$

$D(23) = [(13300 \bmod 143) \times (13300 \bmod 143) \times 23] \bmod 143 \Longrightarrow$

$D(23) = (1 \times 1 \times 23) \bmod 143 = 23 \bmod 143 = 23$

$D(23) = 23.$

Com a decifração dos blocos 053-023-138-003-022-010 obtemos 14-23-18-16-22-10, que agora podemos converter novamente para texto desfazendo o que foi feito na etapa de pré-codificação, ou seja, juntamos tudo (142318162210), e substituimos cada dois algarismos a partir da esquerda pela letra correspondente na seguinte convenção: a=10, b=11, c=12, ... , z=35. O resultado final, como esperávamos, é a palavra *"enigma"*.

Capítulo 4

Aplicações da Aritmética Modular

Vamos supor que você deseja fazer um depósito em dinheiro no caixa eletrônico do seu banco. Para isso é necessário que você informe os dados da conta-corrente, isto é, o número da agência com dígito e o número da conta-corrente com o dígito verificador. Pois bem, a função do dígito de verificação é evitar erros. Se você trocar um número na conta-corrente ou na agência o dígito respectivo não vai conferir e o caixa eletrônico não aceitará o depósito. Isto fará com que você verifique novamente os dados e evitará que o depósito entre na conta de outra pessoa causando transtornos para você e para o banco.

Em muitos documentos (RG, CPF, CNPJ, Título de Eleitor, etc.) os dígitos de verificação estão presentes e quando preenchemos um formulário eletrônico (um cadastro on-line por exemplo), esses dígitos são checados para evitar possíveis erros de digitação. O cálculo do dígito nestes casos é feito utilizando a aritmética modular.

4.1 Cálculo do dígito do CPF e do CNPJ

Vamos calcular os dígitos verificadores de um CPF (*Cadastro de Pessoas Físicas*) hipotético 234.400.562−??.

Devemos, primeiramente, multiplicar cada algarismo da direita para a esquerda respectivamente por 9, 8, 7, 6, 5, 4, 3, 2, 1 e 0.

2	3	4	4	0	0	5	6	2
×	×	×	×	×	×	×	×	×
1	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓
2	6	12	16	0	0	35	48	18

Depois somamos os resultados e calculamos o total módulo 11 (se o resultado for 10 consideramos 0 como dígito).

$$2 + 6 + 12 + 16 + 0 + 0 + 35 + 48 + 18 = 137 \longrightarrow 137 \bmod 11 = 5$$

O primeiro dígito é, portanto, igual a 5.

Para calcular o segundo dígito, incluímos o primeiro dígito junto com os demais algarimos do CPF e repetimos o procedimento acima.

2	3	4	4	0	0	5	6	2	5
×	×	×	×	×	×	×	×	×	×
0	1	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	3	8	12	0	0	30	42	16	45

Depois somamos os resultados e calculamos o total módulo 11.

$$0 + 3 + 8 + 12 + 0 + 0 + 30 + 42 + 16 + 45 = 156 \longrightarrow 156 \bmod 11 = 2$$

O segundo dígito é 2 e o CPF completo com os dois dígitos verificadores é $234.400.562-52$. Os dígitos de verificação calculados tomando-se o resto da divisão por 11 são conhecidos como DV módulo 11.

Os dígitos do CNPJ (*Cadastro Nacional de Pessoas Jurídicas*) também são calculados módulo 11. Vamos calcular os dígitos do CNPJ hipotético $22.345.293/0001-??$.

Multiplicamos da direita para a esquerda cada algarismo respectivamente por 9, 8, 7, 6, 5, 4, 3, 2, 9, 8, 7, 6 e 5. E procedemos de maneira análoga ao que foi feito para o CPF.

2	2	3	4	5	2	9	3	0	0	0	1
×	×	×	×	×	×	×	×	×	×	×	×
6	7	8	9	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
12	14	24	36	10	6	36	15	0	0	0	9

$12+14+24+36+10+6+36+15+0+0+0+9 = 162 \longrightarrow 162 \bmod 11 = 8$

Agora incluímos o primeiro dígito calculado com os demais e repetimos o procedimento para encontrar o segundo dígito

2	2	3	4	5	2	9	3	0	0	0	1	8
×	×	×	×	×	×	×	×	×	×	×	×	×
5	6	7	8	9	2	3	4	5	6	7	8	9
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
10	12	21	32	45	4	27	12	0	0	0	8	72

$10 + 12 + 21 + 32 + 45 + 4 + 27 + 12 + 0 + 0 + 0 + 8 + 72 = 243 \longrightarrow$

$243 \bmod 11 = 1$

O CNPJ com DV é 22.345.293/0001−81.

4.2 Cálculo do dígito do RG

As carteiras de identidade emitidas no estado de São Paulo possuem dígito verificador também módulo 11. Como exemplo, vamos calcular o DV do RG 11.966.756−?.

Multiplicamos da direita para a esquerda cada algarismo respectivamente por 2, 3, 4, 5, 6, 7, 8 e 9. A seguir, somamos os resultados e calculamos o total módulo 11.

1	1	9	6	6	7	5	6
×	×	×	×	×	×	×	×
9	8	7	6	5	4	3	2
↓	↓	↓	↓	↓	↓	↓	↓
9	8	63	36	30	28	15	12

$9 + 8 + 63 + 36 + 30 + 28 + 15 + 12 = 201 \longrightarrow 201 \bmod 11 = 3$

O RG com dígito é 11.966.756−3.

No caso das contas-correntes e boletos de cobrança, os bancos utilizam o módulo 11 ou o módulo 10 (com variações, como por exemplo começar da esquerda para a direita ou utilizar X no lugar do dígito 0). Não há um padrão e o algoritmo varia de banco para banco.

Exercício 1. Calcule os dígitos verificadores do seu CPF utilizando os procedimentos descritos acima.

4.3 Cálculo do dígito ISBN-13

Outro importante dígito de verificação é o do ISBN-13 (*International Standard Book Number*), número padrão internacional de livros. Vejamos como o dígito ISBN-13 é calculado tomando como exemplo o livro *"The Code Book"* do renomado autor Simon Singh. O código sem o dígito de verificação é ISBN 978-85-01-05598-?(onde colocamos o símbolo de interrogação no lugar do dígito verificador).

9	7	8	8	5	0	1	0	5	5	9	8
×	×	×	×	×	×	×	×	×	×	×	×
1	3	1	3	1	3	1	3	1	3	1	3
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
9	21	8	24	5	0	1	0	5	15	9	24

$$9 + 21 + 8 + 24 + 5 + 0 + 1 + 0 + 5 + 15 + 9 + 24 = 121$$

Agora calculamos $121 \bmod 10 = 1$. Por fim, o dígito verificador do ISBN-13 é obtido subtraindo o resultado de 10. No caso, $10 - 1 = 9$ é o dígito. Portanto o ISBN-13 do livro de Singh é ISBN 978-85-01-05598-9, o que é possível confirmar olhando em um exemplar.

4.4 Critérios de Divisibilidade

Usando artimética modular podemos deduzir os critérios de divisibilidade. Vejamos como isto é feito.

4.4.1 Divisibilidade por 3

Sabemos que um número inteiro α é divisível por 3 quando a soma de seus algarimos for divisível por 3. Por exemplo, 915 é divisível por 3 porque a soma $9+1+5$ de seus algarismos é 15, que é divisível por 3. Vejamos como chegar a essa conclusão usando a aritmética modular.

Seja $\alpha = a_n a_{n-1} \ldots a_1 a_0$ (onde os a_i são os algarimos do sistema decimal de numeração), um número inteiro qualquer. Se α for divisível por 3, então α satisfaz a equação $\alpha \bmod 3 = 0$. Usando a expansão decimal de α, temos

$$\alpha \bmod 3 = 0 \iff (a_n a_{n-1} \ldots a_1 a_0) \bmod 3 = 0 \iff$$

$$(a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0) \bmod 3 = 0 \iff$$

$$[a_n(999\ldots9+1) + a_{n-1}(99\ldots9+1) + \ldots + a_1(9+1) + a_0] \bmod 3 = 0 \iff$$

$$[(999\ldots9a_n + 99\ldots9a_{n-1} + \ldots + 9a_1) + (a_n + a_{n-1} + \ldots + a_1 + a_0)] \bmod 3 = 0 \iff$$

$$[(999\ldots9a_n + 99\ldots9a_{n-1} + \ldots + 9a_1) \bmod 3 + (a_n + a_{n-1} + \ldots + a_1 + a_0) \bmod 3] \bmod 3 = 0 \iff$$

$$(0 + 0 + \ldots + 0) + (a_n + a_{n-1} + \ldots + a_1 + a_0) \bmod 3 = 0 \iff$$

$$(a_n + a_{n-1} + \ldots + a_1 + a_0) \bmod 3 = 0$$

Portanto, $\alpha \bmod 3 = 0 \iff (a_n + a_{n-1} + \ldots + a_1 + a_0) \bmod 3 = 0$.

4.4.2 Divisibilidade por 4

A divisibilidade de um número por 4 se verifica quando os dois últimos algarimos desse número à direita (algarismo das dezenas e algarismo das unidades) formam um número divisível por 4. Por exemplo, 12928 é divisível por 4 porque 28 é divisível por 4 ($28 = 4 \cdot 7$). Assim como 1700 também o é, pois 00 é divisível por 4.

Novamente, seja $\alpha = a_n a_{n-1} \ldots a_1 a_0$ um número inteiro qualquer. Vamos resolver $\alpha \bmod 4 = 0$, usando a expansão decimal de α,

$$\alpha \bmod 4 = 0 \iff (a_n a_{n-1} \ldots a_1 a_0) \bmod 4 = 0 \iff$$

$$(a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0) \bmod 4 = 0 \iff$$

$$[(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \ldots + a_2) \times 100 + a_1 10 + a_0] \bmod 4 = 0 \iff$$

$$[(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \ldots + a_2) \times 100] \bmod 4 +$$
$$(a_1 10 + a_0) \bmod 4 = 0 \iff$$

$$(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \ldots + a_2) \bmod 4 \times 100 \bmod 4 +$$
$$(a_1 10 + a_0) \bmod 4 = 0 \iff$$

Como $100 \bmod 4 = 0$,

$$[(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \ldots + a_2) \bmod 4] \times 0 +$$
$$(a_1 10 + a_0) \bmod 4 = 0 \iff$$

$$(a_1 10 + a_0) \bmod 4 = 0$$

Portanto

$$\alpha \bmod 4 = 0 \iff (a_1 10 + a_0) \bmod 4 = 0 \iff$$

$$(a_1 a_0) \bmod 4 = 0$$

Desse modo, justificamos o critério de divisibilidade por 4.

4.4.3 Divisibilidade por 5

Procedemos de maneira semelhante aos casos anteriores para justificar o critério de divisibilidade por 5. Seja $\alpha = a_n a_{n-1} \ldots a_1 a_0$,

$$\alpha \bmod 5 = 0 \iff (a_n a_{n-1} \ldots a_1 a_0) \bmod 5 = 0 \iff$$

$$(a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0) \bmod 5 = 0 \iff$$

$$[(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1) \times 10 + a_0] \bmod 5 = 0 \iff$$

$$[(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1) \times 10] \bmod 5 +$$
$$a_0 \bmod 5 = 0 \iff$$

$$(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1) \bmod 5 \times 10 \bmod 5 +$$
$$a_0 \bmod 5 = 0 \iff$$

Como $10 \bmod 5 = 0$,

$$(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \ldots + a_2 10 + a_1) \bmod 5 \times 0 +$$
$$a_0 \bmod 5 = 0 \iff$$

$$a_0 \bmod 5 = 0$$

Portanto,

$$\alpha \bmod 5 = 0 \iff a_0 \bmod 5 = 0$$

Desse modo, temos

$$\alpha \bmod 5 = 0 \iff a_0 \bmod 5 = 0 \iff a_0 = 5 \text{ ou } a_0 = 0$$

Justifica-se assim o critério de divisibilidade por 5.

4.4.4 Divisibilidade por 6

Sabemos que um número é divisível por 6 quando é par e divisível por 3. Esse é o critério de divisibilidade por 6. Mas podemos verificar a divisibilidade por 6 de outra forma. Observe que

$10 \bmod 6 = 4;$

$10^2 \bmod 6 = 100 \bmod 6 = 4;$

$10^3 \bmod 6 = (10^2 \cdot 10) \bmod 6 = (100 \bmod 6) \cdot (10 \bmod 6) =$

$4 \cdot 4 \bmod 6 = 16 \bmod 6 = 4$

Observamos que $10^i \equiv 4 \bmod 6$, para $i \in \mathbb{N}$. Então

$\alpha = (a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0) \bmod 6 = 0 \iff$

$(4a_n + 4a_{n-1} + \ldots + 4a_1 + a_0) \bmod 6 = 0$

Logo, α é divisível por 6 se $4 \cdot (a_n + a_{n-1} + \ldots + a_1) + a_0$ também for divisível por 6.

4.4.5 Divisibilidade por 11

Novamente, seja $\alpha = a_n a_{n-1} \ldots a_1 a_0$, então

$\alpha = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0$

Como $10 \equiv -1 \bmod 11 \Longrightarrow 10^k \equiv (-1)^k \bmod 11$, então

$\alpha = a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_1 10 + a_0 \equiv$

$[a_n(-1)^n + a_{n-1}(-1)^{n-1} + \ldots + a_1(-1) + a_0] \bmod 11$, ou seja,

$\alpha \equiv 0 \bmod 11 \iff$

$a_n(-1)^n + a_{n-1}(-1)^{n-1} + \ldots + a_1(-1) + a_0 \equiv 0 \bmod 11$

Sendo assim, se n for de ordem par, por exemplo, α será divisível por onze se a soma a seguir for divisível por 11

$$a_n - a_{n-1} + a_{n-2} + \ldots + a_2 - a_1 + a_0$$

Justificando a regra que diz que um número é divisível por 11 se a soma dos algarismos de ordem ímpar subtraída da soma dos algarismos de ordem par for divisível por 11.

4.4.6 Divisibilidade por 7, 11 e 13

Fatorando 1001, obtemos $1001 = 7 \cdot 11 \cdot 13$. Isto significa que

$$1001 \equiv 0 \bmod [7, 11, 13] \Longrightarrow 1000 \equiv -1 \bmod [7, 11, 13] \Longrightarrow$$

$$10^3 \equiv -1 \bmod [7, 11, 13];$$

$$10^6 = (10^3)^2 \equiv (-1)^2 \equiv 1 \bmod [7, 11, 13];$$

$$10^9 = (10^3)^3 \equiv (-1)^3 \equiv -1 \bmod [7, 11, 13];$$

$$\vdots$$

Agora,

$$\alpha = a_n a_{n-1} \ldots a_2 a_1 a_0 =$$

$$a_n 10^n + a_{n-1} 10^{n-1} + \ldots + a_2 10^2 + a_1 10 + a_0 =$$

$$a_2 a_1 a_0 + a_5 a_4 a_3 \times 10^3 + a_8 a_7 a_6 \times 10^6 + \ldots \equiv$$

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 + \ldots$$

Então o número $\alpha = a_n a_{n-1} \ldots a_2 a_1 a_0$ será divisível por 7, 11 e 13 se o resultado a seguir:

$$a_2 a_1 a_0 - a_5 a_4 a_3 + a_8 a_7 a_6 + \ldots$$

também for divisível por 7, 11 e 13.

4.4.7 Outros critérios de Divisibilidade

Para outros critérios de divisibilidade procedemos de maneira análoga, utilizando a expansão decimal de α. O critério de divisibilidade por 9 é obtido de maneira semelhante ao que foi feito para o 3, ou seja,

$$\alpha \bmod 9 = 0 \iff (a_n + a_{n-1} + \ldots + a_1 + a_0) \bmod 9 = 0.$$

O critério de divisibilidade por 8 é semelhante ao que foi feito para o 4, sendo que

$$\alpha \bmod 8 = 0 \iff (a_2 10^2 + a_1 10 + a_0) \bmod 8 = 0 \iff$$

$$(a_2 a_1 a_0) \bmod 8 = 0.$$

O critérios de divisibilidade por 2 e por 10 seguem o modelo da divisibilidade por 5, sendo que

$$\alpha \bmod 2 = 0 \iff a_0 \bmod 2 = 0 \quad \text{e}$$

$$\alpha \bmod 10 = 0 \iff a_0 \bmod 10 = 0.$$

4.5 Considerações Finais

O objetivo do presente trabalho foi apresentar a aritmética modular de uma forma que pudesse ser objeto de estudo no ensino médio da educação básica, ou seja, relacionada a aplicações que pudessem despertar o interesse dos alunos desse segmento. Para tanto nos valemos da criptografia, pela aura de mistério em que está envolvida e pela sua importância em vários momentos da história. A criptografia sempre esteve presente nas relações comercias e diplomáticas entre os países, com destaque para os grandes conflitos mundiais (as grandes guerras e a guerra fria) onde a segurança das comunicações foi de vital importância.

Ainda hoje esse ramo da matemática é largamente utilizado para garantir a privacidade das comunicações no mundo globalizado, especialmente na internet com as chamadas cifras de chave pública.

Na abordagem do assunto, utilizamos exemplos de cifras de fácil manipulação pelos alunos, como as cifras de César, de Vigenère e de Hill (que envolve matrizes) procurando mostrar a matemática por detrás de cada uma delas. Apresentamos também o método de Diffie-Hellman que revolucionou a criptografia ao permitir a troca de chaves criptográficas com segurança. A criptografia RSA, por ser de maior complexidade, pode constituir um exercício exemplar que o professor usará em sala de aula para ilustrar a atualidade do tema e despertar o interesse pela pesquisa.

Na proposta para o ensino médio, quisemos mostrar exemplos de problemas envolvendo aritmética modular e cuja resolução está ao alcance dos alunos. Não esgotamos as possibidades nos exemplos dados, havendo espaço para a criação de inúmeros outros que certamente enriquecerão o conteúdo. Exploramos também a relação da aritmética modular com as regras de divisibilidade e outras aplicações como o cálculo de dígitos de verificação de documentos.

Atividades práticas como a cifragem e a decifragem de mensagens entre grupos de alunos utilizando os métodos apresentados aqui, o cálculo do dígito de verificação das cédulas de identidade dos alunos, a implementação de algoritmo para cálculo de potências de expoente muito grande, usando os recursos da sala de informática, entre outras, contribuiriam para aumentar a participação e o interesse pelas aulas.

Referências Bibliográficas

[1] Antonio Cândido Faleiros: *Criptografia*, SBMAC, São Carlos (2011)

[2] Abramo Hefez: *Elementos de Aritmética*, SBM, Rio de Janeiro (2011)

[3] Abramo Hefez: *Iniciação à Aritmética*, OBMEP, Niterói (2009)

[4] César Polcino Milies *Números, Uma Introdução à Matemática*, Edusp, São Paulo (2000)

[5] Ilydio P. Sá: *Aritmética Modular e Algumas de suas Aplicações*, *in* http://magiadamatematica.com

[6] Simon Singh: *O Livro dos Códigos*, Record, São Paulo (2007)

[7] http://map.gsfc.nasa.gov/universe