UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL
(PROFMAT)

Congruência e Aplicações

por Guilherme Liegel Leopold

Orientador: Prof. Dr. Laerte Bemm

Maringá - PR
2015

GUILHERME LIEGEL LEOPOLD

Congruência e Aplicações

Dissertação de mestrado apresentada ao Programa de Mestrado Profissional em Matemática em Rede Nacional do Departamento de Matemática, Centro de Ciências Exatas da Universidade Estadual de Maringá, como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Laerte Bemm

Maringá - PR

2015

Dedico este trabalho a Deus

Agradecimentos

Quero manifestar aqui minha sincera gratidão a todas as pessoas que de alguma forma me ajudaram a conquistar mais essa vitória. Agradeço em especial:

- Meus pais Frederico e Viviane, pelo amor, inspiração, ensinamentos e por não medirem esforços para que eu pudesse ter condições de realizar os meus sonhos. Muito obrigado pelo incentivo e apoio incondicional.
- Meus amados avós maternos Ferdinando Ernesto Guilherme Liegel "in memorian"e Noemia Cordeiro Liegel, pelo carinho, pela forte presença em minha vida e por sempre acreditarem em mim.
- Meus amados avós paternos "in memorian" Hans Leopold e Norma de Oliveira Leopold pelos ensinamentos de vida.
- Minha irmã Margareth, pela cumplicidade e companheirismo de uma vida toda.
- Minha namorada Andrea, pela paciência, por compreender meus momentos de ausência e por me apoiar nas horas mais difíceis.
- Meus amigos e colegas de mestrado Sonivaldo e Wagner, pelas horas de estudo, companheirismo e ajuda na conclusão desta dissertação.
- A todos os meus demais amigos, muito obrigado. Em particular, meus amigos Marcus e Jota por compartilharmos tantas coisas boas durante todos esses anos.
- Meu cunhado Daniel, pelas parcerias, momentos em família e por me ajudar neste trabalho.

- Meu orientador Laerte Bemm, pela paciência, pelos conselhos, por compreender minhas dificuldades de deslocamento e trabalho, por acreditar em mim e pelas ótimas idéias.
- Aos demais professores do Programa de Mestrado, meu muito obrigado pelos ensinamentos.
- Ao IFPR - Câmpus Umuarama pelo incentivo à minha capacitação.
- Ao IMPA pela valiosa oportunidade de ingressar no Programa de Mestrado Profissional em Matemática.

Finalmente, quero agradecer ao departamento de Matemática da UEM por acreditar no Programa, proporcionando condições para o meu aprimoramento profissional.

Resumo

O presente estudo configura-se como uma oportunidade de aprofundamento acerca de alguns conceitos de Congruência, mais especificamente no que tange às suas aplicações em alguns critérios de divisibilidade, no cálculo envolvendo calendários, dígitos verificadores e criptografia. Sua concepção se inicia pela relevância do tema, com consequente consulta bibliográfica, o que levou a uma investigação matemática que permite elevar este ao status de material de apoio teórico ao professor de matemática.

Palavras chaves: Congruência, Aritmética Modular, CPF, Cartão de Crédito, Calendário, Critérios de Divisibilidade, Criptografia.

Abstract

The following study presents itself as an opportunity to deepen understanding over congruence concepts, more specifically to its applications on divisibility tests, calculations involving calendars, verifying digits and encryption. This theme was selected due to its relevance to the mathematic research field, and its main aspiration is to serve as a consistent theoretical support material to math teachers.

Key Words: Congruences, Modular Arthimetic, CPF, Credit Card, Calendar, Divisibility Tests, Cryptography.

Sumário

Introdução

Compreender os conceitos matemáticos é de extrema relevância para o sucesso do processo de ensino e aprendizagem em matemática. Tal compreensão auxilia na estruturação do raciocínio e contribui para o desenvolvimento de processos que transcendem o âmbito da própria Matemática. Assimilar esses conceitos é fator preponderante para conferir à Matemática, o status de ciência que possibilita interpretar situações do cotidiano, servindo como ferramenta de suporte ao pensamento humano. Nesse sentido, o grande desafio deste trabalho se constitui em abordar alguns conceitos de Congruência, os quais nos permitem classificar números com características semelhantes e aplicar critérios de divisibilidade de forma atrativa, sem se afastar do rigor e da essência dos conceitos matemáticos clássicos historicamente construídos pois, estes são, segundo os PCN's (1997), veículos para o desenvolvimento de ideias fundamentais para a instrumentalização e o desenvolvimento do raciocínio lógico matemático.

A noção de aritmética modular está diretamente associada com o cálculo do resto da divisão de números inteiros. A operação de determinar o resto, e suas aplicações, vão desde a simples abordagem de conceitos de divisibilidade a aplicações mais elaboradas, empregadas em programas computacionais avançados. A aritmética modular possibilita contextualizações desafiadoras e também a realização de operações aritméticas que permitem conjecturar, argumentar e demonstrar, ações que legitimam a Matemática como ciência.

Neste trabalho, os estudos se voltam mais especificamente para as demonstrações e aplicações de alguns dos critérios de divisibilidade, aplicações envolvendo a geração do número de CPF (Cadastro de Pessoas Físicas), criptografia e cálculo com calendários.

Mais explicitamente, este estudo é dividido em três capítulos os quais, resumiremos nos próximos parágrafos.

O primeiro capítulo é dedicado aos conceitos e resultados da aritmética dos números inteiros, tais como divisibilidade, a representação dos inteiros, máximo divisor comum e números primos, conceitos necessários para o desenvolvimento dos capítulos subsequentes.

No segundo capítulo é realizada a abordagem de conceitos de congruência, com a apresentação de definições, teoremas, propriedades, exemplificações e demonstrações que servirão de base para fundamentar as aplicações, abordadas no capítulo seguinte.

Finalmente, no Capítulo 3, faremos uma abordagem de algumas aplicações de congruência. A primeira seção é dedicada à apresentação, demonstração e exemplificação dos critérios de divisibilidade mais usuais que, a priori, são ensinados no 6º ano do Ensino Fundamental. A segunda seção é destinada a aplicação de congruência na criptografia, baseada nos conceitos primitivos da "Cifra de César", técnica criada pelo imperador Júlio César para enviar mensagens secretas aos seus soldados e aliados. Na Seção 3 abordamos a aplicação de congruência na geração do número do CPF. A curiosidade apresentada nesta seção é que a soma dos algarismos dos números do CPF é, invariavelmente, um valor múltiplo de 11, fato que a maioria da população desconhece. Por último e não menos importante, apresentamos a aplicação de congruência envolvendo o cálculo com calendários, onde é possível determinar o dia da semana de qualquer data a partir de 1600. Nesta seção, fazemos uma viagem histórica para compreender não apenas as mudanças de calendários, mas também e, essencialmente, o nosso calendário atual mundialmente utilizado, o calendário gregoriano, desde sua concepção, até os conceitos matemáticos utilizados para determinação dos anos bissextos. Ressalta-se aqui a construção de uma "fórmula matemática" que possibilita fazer estes cálculos de maneira simples e eficiente.

Capítulo 1

Resultados Preliminares

Neste primeiro capítulo vamos estabelecer alguns conceitos e resultados da Teoria de Divisibilidade de números inteiros que nos serão úteis para o desenvolvimento do trabalho. Em geral não apresentamos as demonstrações destes resultados, mas tomamos o cuidado de sempre indicar uma bibliografia na qual o leitor interessado poderá obtê-las. Esperamos que o leitor domine tópicos básicos da aritmética de números inteiros. Observamos que as notações aqui usadas são as clássicas e encontradas na maioria dos livros relacionados ao tema.

Vamos denotar por $\mathbb{Z}$ o conjunto dos números inteiros e $\mathbb{Z}_+$ o conjuntos dos números inteiros não negativos.

1.1 Divisibilidade

Observemos que uma equação do tipo $a \cdot x = b$, com $a, b \in \mathbb{Z}$, pode ou não ter solução inteira, dependendo dos valores de a e b. Quando tal equação tem solução dizemos que a é divisível por b. Mais precisamente:

Definição 1.1 *Sejam $a, b \in \mathbb{Z}$. Dizemos que a divide b se existir $k \in \mathbb{Z}$ tal que $b = a \cdot k$. Se a divide b, diremos também que a é um divisor ou um fator de b ou, ainda que b é um múltiplo de a.*

Quando a divide b escrevemos $a \mid b$, enquanto a negação desta sentença é representada por $a \nmid b$. Desta forma $a \nmid b$ se e somente se $b \neq a \cdot k$, para todo $k \in \mathbb{Z}$.

Exemplo 1.2 *A seguir apresentamos alguns exemplos que ilustram o conceito de divibilidade:* $2 \mid 24$, *pois* $24 = 2 \cdot 12$; $3 \mid 243$, *pois* $243 = 3 \cdot 81$; $-42 \mid 9996$, *pois* $9996 = -42 \cdot (-238)$.

Exemplo 1.3 *Os dividores de* 8 *são* ± 1, ± 2, ± 4 *e* ± 8 *e os divisores de* 19 *são* ± 1 *e* ± 19.

Exemplo 1.4 *Sabemos que* $2 \nmid 7$, *pois* $7 \neq 2 \cdot c$, *para todo* $c \in \mathbb{Z}$.

Vamos supor que $a \mid b$ com $a \neq 0$ e seja $k \in \mathbb{Z}$ tal que $b = a \cdot k$. O número inteiro k é único e chamado de *quociente* de b por a e usaremos a notação $k = \dfrac{b}{a}$ para indicar tal inteiro. Em contrapartida, $0 \mid b$ se, e somente se, $b = 0$. Nesse caso, o quociente não é único, pois $0 = 0 \cdot k$, para todo $k \in \mathbb{Z}$. Desta forma, o quociente $\dfrac{0}{0}$ é indeterminado. Por isso, vamos excluir o caso com divisor nulo e adotar esta convenção daqui em diante.

Exemplo 1.5 *É fácil ver que* $\dfrac{0}{1} = 0$, $\dfrac{8}{2} = 4$, $\dfrac{10}{5} = 2$, $\dfrac{7}{7} = 1$, $\dfrac{12}{3} = 4$, $\dfrac{15}{5} = 3$, $\dfrac{24}{12} = 2$.

Ressaltamos que $\dfrac{b}{a}$ é apenas uma notação e não uma fração. Agora estabeleceremos, sem demonstração, algumas propriedades da divisibilidade.

Proposição 1.6 *([7], Proposição 2.1.4) Sejam* $a, b, c, d \in \mathbb{Z}$ *(lembrando que assumimos os dividores não nulos). As seguintes propriedades são verdadeiras:*

(*i*) $a \mid a$;

(*ii*) *Para quaisquer* $a, b \in \mathbb{Z}_+$, *se* $a \mid b$ *e* $b \mid a$, *então* $a = b$;

(*iii*) *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$;

(*iv*) *Se* $a \mid b$ *e* $c \mid d$, *então* $a \cdot c \mid b \cdot d$;

(*v*) *Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid (b + c)$;

(*vi*) *Se* $a \mid b$, *então para todo* $m \in \mathbb{Z}$ *temos que* $a \mid mb$;

(*vii*) *Se* $a \mid b$ *e* $a \mid c$*, então, para quaisquer* $m, n \in \mathbb{Z}$*, temos que* $a \mid (mb + nc)$.

Exemplo 1.7 *Temos os seguintes exemplos:*

(*a*) *Pela Proposição 1.6* (*i*)*, temos* $3 \mid 3$*,* $10 \mid 10$*,* $15 \mid 15$*,* $17 \mid 17$.

(*b*) *Observe que* $3 \mid 6$*,* $6 \mid 720$ *e* $2 \mid 10$*,* $10 \mid 50$*. Assim, pela Proposição 1.6* (*iii*)*, temos* $3 \mid 720$ *e* $2 \mid 50$.

(*c*) $2 \mid 6$ *e* $5 \mid 15$ *e assim, pela Proposição 1.6* (*iv*)*,* $10 \mid 90$.

(*d*) *Como* $3 \mid 9$ *e* $3 \mid 27$*, segue da Proposição 1.6* (*v*) *que* $3 \mid (9 + 27) = 36$.

(*e*) *Uma vez que* $2 \mid 4$*, da Proposição 1.6* (*vi*)*, vem que* $2 \mid 4 \cdot 2 = 8$*,* $2 \mid 4 \cdot 3 = 12$*,* $2 \mid 4 \cdot 4 = 16$*, ...*

(*f*) *Observe que* $3 \mid 21$ *e* $3 \mid 33$*. Consequentemente, pela Proposição 1.6* (*vii*)*,* $3 \mid (5 \cdot 21 - 3 \cdot 33) = 6$.

Se a e b são inteiros e b não divide a, é possível empregarmos um método que possibilite executar a "divisão"de a por b, obtendo-se um resto. Sendo assim, dados a e b inteiros, com $b \neq 0$, existem q e r inteiros tais que $a = b \cdot q + r$ e $0 \leq r < |b|$, onde $|b|$ denota o módulo de b.

Observemos que $b \cdot q$ é múltiplo de b e $r = a - b \cdot q$. A condição $0 \leq r < |b|$ pode ser entendida da seguinte forma: estamos procurando um múltiplo de b, menor ou igual a a pois, $a - b \cdot q \geq 0$, de tal forma que este múltiplo seja "o mais próximo possível de a".

Teorema 1.8 *([7], Teorema 2.1.6)* ***(Algoritmo da Divisão).*** *Se* $a, b \in \mathbb{Z}$*, com* $b \neq 0$*, então existem dois únicos* $q, r \in \mathbb{Z}$ *tais que*

$$a = b \cdot q + r,$$

com $0 \leq r < |b|$.

Os números q e r são chamados, respectivamente, de *quociente* e *resto* da divisão de a por b. Observemos que o resto da divisão de a por b é zero se, e somente se, $b \mid a$.

Exemplo 1.9 *Se* $a = 32$ *e* $b = 5$*, então* $q = 6$ *e* $r = 2$*, pois* $32 = 5 \cdot 6 + 2$ *e* $0 \leq 2 < 5$*.*

Exemplo 1.10 *Considere* $a = -27$ *e* $b = 4$*. Claramente,* $27 = 4 \cdot 6 + 3$*. Desta forma,* $-27 = 4 \cdot (-6) - 3$ *(*). Note que o quociente e o resto da divisão de* -27 *por* 4 *não são* -6 *e* -3*, respectivamente, pois não vale* $0 \leqslant -3 < 4$*. Porém, somando e subtraindo 4 no lado direito de (*) temos* $-27 = 4 \cdot (-6) - 3 + 4 - 4 = 4 \cdot (-6 - 1) + 1$*, ou seja,* $-27 = 4 \cdot (-7) + 1$*. Logo, o quociente procurado é* -7 *e o resto é* 1*. Veja Teorema 1.8.*

Definição 1.11 *Seja* $x \in \mathbb{R}$*. O maior inteiro em* x*, denotado por* $[x]$*, é o maior número inteiro menor ou igual a* x*.*

Exemplo 1.12 *Vamos determinar o maior inteiro em* x*, para certos valores de* $x \in \mathbb{R}$*. Assim,* $[2,8] = 2$*,* $[5] = 5$*,* $[-3,4] = -4$ *e* $[\sqrt{2}] = 1$*.*

A proposição a seguir decorre diretamente da Definição 1.11.

Proposição 1.13 *([9], Proposição 1.5) Se* $x \in \mathbb{R}$*, então* $x - 1 < [x] \leq x$*.*

É fácil observar que na divisão de a por b, obtemos o quociente q tal que $q = \left[\frac{a}{b}\right]$ e o resto $r = a - b\left[\frac{a}{b}\right]$.

Exemplo 1.14 *Dividindo* $a = 2053$ *por* $b = 26$*, obtemos quociente* $q = \left[\frac{2053}{26}\right] = 78$ *e resto* $r = 2053 - 26 \cdot \left[\frac{2053}{26}\right] = 2053 - 78 \cdot 26 = 25$*.*

1.2 Representação dos Inteiros

A maneira convencional de representar os números inteiros é o sistema decimal posicional. Neste sistema, todo número inteiro é representado por uma sequência formada por dez algarismos 1, 2, 3, 4, 5, 6, 7, 8, 9, além do símbolo 0 (zero), que representa a ausência de algarismo. Por serem dez algarismos o sistema é chamado decimal e também é chamado posicional, pois cada algarismo, além do seu valor, possui um peso que lhe é atribuído em função da posição que ele ocupa no número. Esse peso, é sempre uma potência de dez. O sistema decimal posicional baseia-se no seguinte resultado.

Teorema 1.15 *([9], Teorema 1.3) Todo número inteiro positivo n pode ser escrito de forma única da seguinte maneira:*

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10^1 + a_0,$$

onde $a_j \in \mathbb{Z}$, com $0 \leq a_j \leq 9$ para todo $j = 0, 1, 2, \ldots, k$ e $a_k \neq 0$.

Exemplo 1.16 *Seja $n = 24581$. Pelo Teorema 1.15, o número n é escrito da seguinte maneira:*

$$n = 2 \cdot 10^4 + 4 \cdot 10^3 + 5 \cdot 10^2 + 8 \cdot 10^1 + 1.$$

Exemplo 1.17 *Considere $n = 703609$. Pelo Teorema 1.15, o número n é escrito da seguinte maneira:*

$$n = 7 \cdot 10^5 + 0 \cdot 10^4 + 3 \cdot 10^3 + 6 \cdot 10^2 + 0 \cdot 10^1 + 9.$$

A representação decimal posicional representa uma grande economia de notação, pois usando apenas os algarismos $0, 1, 2, \ldots, 9$, podemos escrever qualquer número inteiro positivo. Porém a vantagem mais importante é que tal representação permite dar regras simples de cálculos aritméticos.

Exemplo 1.18 *Vamos determinar o quociente e o resto da divisão de* 683 *por* 22. *Note que* 683 *e* 22 *são números "distantes", e por isso fica mais difícil encontrar o quociente e o resto da divisão. Porém,* 68 *e* 22 *são "próximos"e vemos facilmente que* $68 = 22 \cdot 3 + 2$. *Afim de obtermos* 683, *multiplicamos ambos os lados por* 10 *e obtemos* $680 = 22 \cdot 30 + 20$. *Somando* 3 *de ambos os lados temos* $683 = 22 \cdot 30 + 23$. *Como* $23 > 22$, *segue que* 23 *não é o resto da divisão de* 683 *por* 22. *Mas* $23 = 1 \cdot 22 + 1$. *Assim,* $683 = 22 \cdot 30 + 22 \cdot 1 + 1$, *ou seja,* $683 = 22 \cdot 31 + 1$. *Logo, o quociente procurado é* 31 *e o resto é* 1.

1.3 Máximo Divisor Comum

Vamos denotar por $\mathbb{N}^*$ o conjunto dos números naturais não negativos (ou chamamos de $\mathbb{N}^*$ o conjunto dos números naturais formado por $1, 2, 3, \ldots$).

Definição 1.19 *Sejam* $a, b \in \mathbb{Z}$, *não simultaneamente nulos. Diremos que o número* $d \in \mathbb{N}^*$ *é um divisor comum de* a *e* b *se* $d \mid a$ *e* $d \mid b$.

Exemplo 1.20 *Os números* ± 1, ± 2, ± 5 *e* ± 10 *são os divisores comuns de* 10 *e* 20.

Definição 1.21 *Sejam* $a, b \in \mathbb{Z}$, *não simultaneamente nulos, e* $d \in \mathbb{N}^*$. *Diremos que* d *é o máximo divisor comum e denotado abreviadamente por mdc de* a *e* b *se:*

(i) $d \mid a$ *e* $d \mid b$;

(ii) *Se* $c \in \mathbb{N}^*$, $c \mid a$ *e* $c \mid b$, *então* $c \mid d$.

Sejam d, d' máximos divisores comuns de a e b. Então $d \mid a$ e $d \mid b$. Mas d' é um *mdc* entre a e b. Assim $d' \mid d$ por definição. Analogamente, $d \mid d'$. Como $d, d' \in \mathbb{N}^*$, segue da Proposição 1.6 (ii) que $d = d'$. Logo, o *mdc* entre a e b quando existe é único. Além disso, o *mdc* entre a e b sempre existe. (Veja Lema 5.1.1 de [5]).

O *mdc* de a e b será denotado por $mdc(a, b)$. Como o máximo divisor comum de a e b não depende da ordem dos termos, temos $mdc(a, b) = mdc(b, a)$.

Se $d = mdc(a, b)$ e c é um divisor comum desses números, então $c \leq d$. Assim, o máximo divisor comum é o maior divisor comum de a e b.

Exemplo 1.22 *Os números* ± 1, ± 2, ± 5 *e* ± 10 *são os divisores comuns de* 10 *e* 20. *Logo,* $mdc(10, 20) = 10$.

Proposição 1.23 *[6] Sejam* $a, b \in \mathbb{Z}$, *não simultaneamente nulos, então:*

(*i*) $mdc(a, 0) = |a|$, *desde que* $a \neq 0$;

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

(*iii*) $mdc(a, a) = |a|$;

(*iv*) *Se* $a \mid b$, *então* $mdc(a, b) = |a|$.

Exemplo 1.24 *Como* $5 \mid 125$, *então* $mdc(5, 125) = 5$.

Proposição 1.25 *([7], Proposição 2.3.6) Dados* $a, b \in \mathbb{Z}$, *não simultaneamente nulos, tem-se*

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

Teorema 1.26 *([7], Teorema 2.3.7)* ***(Teorema de Euclides).*** *Sejam* $a, b, c \in \mathbb{Z}$ *não nulos. Se* $mdc(a, b) = 1$ *e* $a \mid (b \cdot c)$, *então* $a \mid c$.

1.4 Números Primos

Esta seção é dedicada a um breve estudo dos números primos. Os gregos foram os primeiros a perceber estes números. A primeira pessoa, até onde se sabe, que produziu uma tabela de números primos foi *Eratóstenes*, no terceiro século antes de cristo. Os números primos desempenham papel fudamental na matemática e a eles estão associados muitos problemas famosos cujas soluções intrigam matemáticos até hoje. Como veremos adiante, todo número inteiro pode ser expresso como produto de números primos de forma única, a menos da ordem dos fatores. Desta forma, os números primos desempenham na Teoria dos Números um papel análogo aos átomos na estrutura da matéria.

Definição 1.27 *Dizemos que um número inteiro p é primo, se p tem exatamente dois divisores:* 1 *e* $|p|$.

Note que -1, 0 e 1 não são primos por definição.

Exemplo 1.28 *Existem* 168 *números primos positivos menores do que* 1000. *São eles:* 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293, 307, 311, 313, 317, 331, 337, 347, 349, 353, 359, 367, 373, 379, 383, 389, 397, 401, 409, 419, 421, 431, 433, 439, 443, 449, 457, 461, 463, 467, 479, 487, 491, 499, 503, 509, 521, 523, 541, 547, 557, 563, 569, 571, 577, 587, 593, 599, 601, 607, 613, 617, 619, 631, 641, 643, 647, 653, 659, 661, 673, 677, 683, 691, 701, 709, 719, 727, 733, 739, 743, 751, 757, 761, 769, 773, 787, 797, 809, 811, 821, 823, 827, 829, 839, 853, 857, 859, 863, 877, 881, 883, 887, 907, 911, 919, 929, 937, 941, 947, 953, 967, 971, 977, 983, 991 *e* 997.

Definição 1.29 *Um número inteiro, diferente de* -1, 0 *e* 1, *que não é primo, é chamado número composto. Desta forma, um inteiro a é composto, se a admite um divisor b tal que* $1 < |b| < |a|$.

Exemplo 1.30 *Os inteiros* $6 = 2 \cdot 3$, $10 = 2 \cdot 5$, $22 = 2 \cdot 11$ $-8 = 2 \cdot (-4)$, $-12 = 2 \cdot (-6)$, $-20 = 5 \cdot (-4)$, *são números compostos.*

Teorema 1.31 *([7], Teorema 2.6.6) Seja $a \in \mathbb{Z}$ e $a > 1$. Então existem únicos números primos $p_1 \leqslant p_2 \leqslant p_3 \leqslant \ldots \leqslant p_m$ tais que*

$$a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m.$$

Exemplo 1.32 *Note que* $240 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5$, $6468 = 2 \cdot 2 \cdot 3 \cdot 7 \cdot 7 \cdot 11$ *e* $114075 = 3 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 13 \cdot 13$.

Este teorema afirma que todos os números inteiros maiores que 1 podem ser escrito como produtos de números primos, sendo esta decomposição única a menos de permutações dos fatores.

Reunindo no Teorema 1.31 os fatores primos repetidos, se preciso, e ordenando os primos em ordem crescente, temos o seguinte enunciado:

Teorema 1.33 *([7], Teorema 2.6.8)* ***(Teorema Fundamental da Aritmética)*** *Dado $a \in \mathbb{Z}$ com $a \neq -1, 0$ e 1, existem números primos positivos $p_1 < p_2 < p_3 < \ldots < p_m$ e $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_m \in \mathbb{N}^*$, unicamente determinados, tais que*

$$a = E \cdot p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot \ldots \cdot p_m^{\alpha_m},$$

onde $E = 1$ ($E = -1$) se a é positivo (a é negativo).

A escrita de um número inteiro a diferente de $-1, 0$ e 1 na forma do teorema anterior é chamada de decomposição (fatoração) de a em fatores primos.

Exemplo 1.34 *Observemos que* $240 = 2^4 \cdot 3^1 \cdot 5^1$, $6468 = 2^2 \cdot 3^1 \cdot 7^2 \cdot 11^1$ *e* $114075 = 3^3 \cdot 5^2 \cdot 13^2$.

Capítulo 2

Congruência

2.1 Introdução

Neste capítulo apresentamos uma grande ferramenta no estudo de dividibilidade que é a congruência. Tal noção foi introduzida por Gauss em seu livro *Disquisitiones Arithmeticae*. A seguir, apresentamos a noção de congruência. Inicialmente, consideremos os restos fornecidos pelas sucessivas divisões de números inteiros não negativos por 7.

$0 = 0 \cdot 7 + 0$	$7 = 1 \cdot 7 + 0$	$14 = 2 \cdot 7 + 0$	$21 = 3 \cdot 7 + 0$
$1 = 0 \cdot 7 + 1$	$8 = 1 \cdot 7 + 1$	$15 = 2 \cdot 7 + 1$	$22 = 3 \cdot 7 + 1$
$2 = 0 \cdot 7 + 2$	$9 = 1 \cdot 7 + 2$	$16 = 2 \cdot 7 + 2$	$23 = 3 \cdot 7 + 2$
$3 = 0 \cdot 7 + 3$	$10 = 1 \cdot 7 + 3$	$17 = 2 \cdot 7 + 3$	$24 = 3 \cdot 7 + 3$
$4 = 0 \cdot 7 + 4$	$11 = 1 \cdot 7 + 4$	$18 = 2 \cdot 7 + 4$	$25 = 3 \cdot 7 + 4$
$5 = 0 \cdot 7 + 5$	$12 = 1 \cdot 7 + 5$	$19 = 2 \cdot 7 + 5$	$26 = 3 \cdot 7 + 5$
$6 = 0 \cdot 7 + 6$	$13 = 1 \cdot 7 + 6$	$20 = 2 \cdot 7 + 6$	...

Observamos, primeiramente, que os restos variam de 0 a 6 conforme Teorema 1.8. Se fixarmos nossa atenção, veremos que no quadro acima encontramos números que fornecem

o mesmo resto quando divididos por 7. Assim, encontramos os seguintes conjuntos: $\{0,\ 7,\ 14,\ 21,\ \ldots\}$ cujos elementos são divisíveis por 7; $\{1,\ 8,\ 15,\ 22,\ \ldots\}$ cujos elementos deixam resto 1 quando divididos por 7; $\{2,\ 9,\ 16,\ 23,\ \ldots\}$ cujos elementos deixam resto 2 quando divididos por 7; $\{3,\ 10,\ 17,\ 24,\ \ldots\}$ cujos elementos deixam resto 3 quando divididos por 7; $\{4,\ 11,\ 18,\ 25,\ \ldots\}$ cujos elementos deixam resto 4 quando divididos por 7; $\{5,\ 12,\ 19,\ 26,\ \ldots\}$ cujos elementos deixam resto 5 quando divididos por 7 e $\{6,\ 13,\ 20,\ \ldots\}$ cujos elementos deixam resto 6 quando divididos por 7.

Os números que pertencem a cada um destes conjuntos são ditos congruentes módulo 7. Assim, os elementos do conjunto $\{1,\ 8,\ 15,\ \ldots\}$, são congruentes módulo 7, pois ao serem divididos por 7 deixam resto igual a 1.

2.2 Definições e Exemplos

Definição 2.1 *Sejam a, b e $m \in \mathbb{Z}$, tal que $m \neq 0$. Dizemos que a é congruente a b módulo m, se a e b tem o mesmo resto quando divididos por m.*

Se a é congruente a b módulo m, escrevemos $a \equiv b\,(mod\, m)$. Se a e b não são congruentes módulo m, diremos que a e b são *incongruentes* módulo m e escrevemos $a \not\equiv b\,(mod\, m)$.

Exemplo 2.2 $31 \equiv 6\,(mod\, 5)$*, pois* 31 *e* 6 *tem mesmo resto quando divididos por* 5*. Em contrapartida,* $31 \not\equiv 6\,(mod\, 3)$*, pois* 31 *e* 6 *não deixam mesmo resto quando divididos por* 3.

Proposição 2.3 *Sejam $a, b \in \mathbb{Z}$, então $a \equiv b\,(mod\, m)$ se, e somente se, $m|(a-b)$, ou seja, existe $k \in \mathbb{Z}$ tal que $a = b + k \cdot m$.*

Demonstração: Sejam $a, b \in \mathbb{Z}$. Se $a \equiv b\,(mod\, m)$, então a e b tem mesmo resto quando divididos por m. Assim, existem $q_1, q_2, r \in \mathbb{Z}$ tais que $a = m \cdot q_1 + r$ e $b = m \cdot q_2 + r$, com $0 \leq r < |m|$. Logo, $a - b = m \cdot (q_1 - q_2)$, e portanto, $m \mid (a - b)$.

Reciprocamente, suponhamos que $m \mid (a-b)$. Pelo Teorema 1.8, existem únicos $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ tais que $a = m \cdot q_1 + r_1$ e $b = m \cdot q_2 + r_2$, com $0 \leq r_1, r_2 < |m|$. Assim, $a - b = m \cdot (q_1 - q_2) + (r_1 - r_2)$. Queremos provar que $r_1 - r_2 = 0$, ou seja, $r_1 = r_2$.

Visto que $m \mid (a-b)$ e $m \mid m \cdot (q_1 - q_2)$, segue da Proposição 1.6 (vii) que $m \mid [(a-b) - m \cdot (q_1 - q_2)]$, ou seja, $m \mid (r_1 - r_2)$.

Então, claramente, $|m| \mid (r_1 - r_2)$. Disso e do fato de que $0 \leq |r_1 - r_2| < |m|$, temos $|r_1 - r_2| = 0$, ou seja, $r_1 = r_2$, como queríamos demonstrar. □

Exemplo 2.4 *Temos que* $73 \equiv 13 \,(mod\, 5)$ *e, pela Proposição 2.3,* $5|(73-13)$*, ou seja,* $73 = 13 + 12 \cdot 5$.

Observação 2.5 *Pela proposição anterior e pelo fato de que* $m \mid (a-b)$ *se e somente se* $|m| \mid (a-b)$*, podemos nos restringir ao estudo de congruências módulo* $m > 0$.

As proposições seguintes decorrem imediatamente da definição de congruência.

Proposição 2.6 *Sejam* $a, b, c, m \in \mathbb{Z}$ *tal que* $m > 0$*. Então as seguintes propriedades são satisfeitas:*

(i) *Reflexiva:* $a \equiv a \,(mod\, m)$*;*

(ii) *Simétrica: se* $a \equiv b \,(mod\, m)$*, então* $b \equiv a \,(mod\, m)$*;*

(iii) *Transitiva: se* $a \equiv b \,(mod\, m)$ *e* $b \equiv c \,(mod\, m)$*, então* $a \equiv c \,(mod\, m)$.

Demonstração:

(i) É óbvio, pois $m|(a-a) = 0$.

(ii) Se $a \equiv b \,(mod\, m)$, então $m \mid (a-b)$. Pela Proposição 1.6 (vi), $m|-(a-b)$, ou seja, $m|(b-a)$. Portanto, $b \equiv a \,(mod\, m)$.

(iii) Se $a \equiv b \,(mod\, m)$ e $b \equiv c \,(mod\, m)$, então $m \mid (a-b)$ e $m \mid (b-c)$. Pela Proposição 1.6 (v), temos que $m \mid (a-c)$, ou seja, $a \equiv c \,(mod\, m)$.

□

Sejam $a \in \mathbb{Z}$ e $m \neq 0$. Dividindo a por m, obtemos os seguintes restos possíveis: $0, 1, 2, \ldots, m-1$. Desta forma, existe $r \in \{0, 1, 2, \ldots, m-1\}$ tal que

$$a \equiv r \,(mod\, m).$$

Agora, para todo $i \in \{0, 1, 2, \ldots, m-1\}$ definimos $Cl(i)$ como sendo o subconjunto de $\mathbb{Z}$ formado por todos os inteiros que são congruentes a i módulo m. Simbolicamente,

$$Cl(i) = \{x \in \mathbb{Z} \,/\, x \equiv i \,(mod\, m)\}.$$

Tais subconjuntos são chamados *classes de congruência módulo* m.

Disso e do que vimos acima, para todo $a \in \mathbb{Z}$, existe $i \in \{0, 1, 2, \ldots, m-1\}$ tal que $a \in Cl(i)$. Portanto, $\mathbb{Z} \subseteq \bigcup_{i=0}^{m-1} Cl(i)$. Como a inclusão contrária é óbvia, temos que

$$\mathbb{Z} = \bigcup_{i=0}^{m-1} Cl(i).$$

Mais ainda, como $i \equiv i \,(mod\, m)$, $Cl(i) \neq \emptyset$. Finalmente, se $i \neq j$, então $Cl(i) \cap Cl(j) = \emptyset$, pois se $x \in Cl(i) \cap Cl(j)$ então $x \equiv i \,(mod\, m)$ e $x \equiv j \,(mod\, m)$. Então, pela Proposição 2.6 (ii), $i \equiv x \,(mod\, m)$ e pela Proposição 2.6 (iii), $i \equiv j \,(mod\, m)$, o que é uma contradição, pois i e j são elementos distintos de $\{0, 1, 2, \ldots, m-1\}$, e consequentemente, eles não tem o mesmo resto quando divididos por m.

Desta forma, podemos "partir" o conjunto dos números inteiros $\mathbb{Z}$ em m subconjuntos, em que cada subconjunto é formado por inteiros mutuamente congruentes módulo m.

Exemplo 2.7 *As três classes de congruência módulo 3 são os conjuntos:* $\{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$, $\{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}$ *e* $\{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}$. *De fato,*

$$\cdots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv \cdots \,(mod\, 3)$$
$$\cdots \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots \,(mod\, 3)$$
$$\cdots \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots \,(mod\, 3)$$

Exemplo 2.8 *Consideremos o mês de Outubro de 2014:*

Domingo	*Segunda*	*Terça*	*Quarta*	*Quinta*	*Sexta*	*Sábado*
			1	*2*	*3*	*4*
5	*6*	*7*	*8*	*9*	*10*	*11*
12	*13*	*14*	*15*	*16*	*17*	*18*
19	*20*	*21*	*22*	*23*	*24*	*25*
26	*27*	*28*	*29*	*30*	*31*	

Como podemos notar, em cada coluna (dia da semana) encontramos os números congruentes entre si módulo 7*. Na coluna do domingo encontramos os números congruentes a* 5*; na segunda, os congruentes a* 6*; na terça, a* 7*; na quarta, a* 1*; na quinta, a* 2*; na sexta, a* 3 *e no sábado, a* 4 *módulo* 7*.*

Agora, como 31 de outubro de 2014 é sexta-feira, 1º de novembro de 2014 é sábado, dia 2 é domingo, dia 3 é segunda-feira, dia 4 é terça-feira, dia 5 é quinta-feira, dia 6 é sexta-feira e dia 7 é um sábado. Como saber o dia da semana correspondente a 24 de novembro de 2014?

Basta procurarmos um número entre 1 *e* 7 *que seja congruente a* 24 *módulo* 7*. Para isto dividimos* 24 *por* 7 *e obtemos* $24 = 7 \cdot 3 + 3$*. Achamos resto igual a* 3*, isto é,* $24 \equiv 3\,(mod\,7)$*. Como 3 de novembro de 2014 corresponde a segunda-feira, pois dia 1º foi sábado, concluímos que o dia 24 de novembro de 2014 foi uma segunda-feira.*

Definição 2.9 *Um sistema completo de resíduos módulo* m *é todo conjunto de números inteiros cujos restos da divisão por* m *são exatamente os números* $0, 1, \ldots, m-1$*, em qualquer ordem e sem repetições.*

Um sistema completo de resíduos módulo m possui m elementos. O Teorema 1.8 mostra que o conjunto $\{0, 1, \ldots, m-1\}$ é um sistema completo de resíduos módulo m. Este conjunto recebe o nome de *conjunto de resíduos não negativos módulo* m*.*

Exemplo 2.10 *É óbvio que, se* $a_1, \ldots, a_m$ *são* m *números inteiros, dois a dois não congruentes módulo* m*, então eles formam um sistema completo de resíduos módulo* m*.*

De fato, tais restos da divisão dos a_i por m são, dois a dois distintos, e assim podemos concluir que são exatamente os números do conjunto $\{0, 1, \ldots, m-1\}$.

A noção de congruência e suas propriedades são muito semelhantes as estruturas de equações algébricas. Primeiramente, iremos mostrar que se adicionarmos, ou subtrairmos, ou multiplicarmos um número nos dois membros de uma congruência, ela será preservada.

Proposição 2.11 *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 0$. Se $a \equiv b \,(mod\, m)$, então*

(*i*) $a + c \equiv b + c \,(mod\, m)$;

(*ii*) $a - c \equiv b - c \,(mod\, m)$;

(*iii*) $a \cdot c \equiv b \cdot c \,(mod\, m)$.

Demonstração:

(*i*) Se $a \equiv b \,(mod\, m)$, então $m \mid (a-b)$. Da identidade $(a+c)-(b+c) = a-b$, temos que $m \mid [(a+c)-(b+c)]$. Portanto, $a + c \equiv b + c \,(mod\, m)$.

(*ii*) Usa a mesma idéia da prova do item (*i*) e utilizando a identidade $(a-c)-(b-c) = a-b$, temos que $m \mid [(a-c)-(b-c)]$. Portanto, $a-c \equiv b-c \,(mod\, m)$.

(*iii*) Se $a \equiv b \,(mod\, m)$, então $m \mid (a-b)$. Da Proposição 1.6 (*vi*), segue que $m \mid c \cdot (a-b)$, ou seja, $m \mid (a \cdot c - b \cdot c)$. Portanto, $a \cdot c \equiv b \cdot c \,(mod\, m)$.

□

Exemplo 2.12 *Como $32 \equiv 7 \,(mod\, 5)$, segue da Proposição 2.11 (i) que*

$$37 = 32 + 5 \equiv 7 + 5 = 12 \,(mod\, 5).$$

Exemplo 2.13 *Visto que $44 \equiv 5 \,(mod\, 13)$, segue da Proposição 2.11 (ii) que*

$$40 = 44 - 4 \equiv 5 - 4 = 1 \,(mod\, 13).$$

Exemplo 2.14 *Como* $10 \equiv 3\,(mod\,7)$*, segue da Proposição 2.11 (iii) que*

$$200 = 10 \cdot 20 \equiv 3 \cdot 20 = 60\,(mod\,7).$$

O que será que acontece se "dividirmos" por um número inteiro os dois membros da congruência? Consideremos o seguinte exemplo.

Exemplo 2.15 *Temos que* $20 \equiv 8\,(mod\,4)$*, porém* $\frac{20}{2} \not\equiv \frac{8}{2}\,(mod\,4)$.

Este exemplo nos diz que, para as congruências, não vale, em geral, a simplificação (Lei do Corte) com relação à multiplicação. O próximo resultado, mostra quando é possível efetuar a simplificação com relação à multiplicação.

Proposição 2.16 *Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 0$*,* $d = mdc(c, m)$ *e* $a \cdot c \equiv b \cdot c\,(mod\,m)$*. Então*

$$a \equiv b\left(mod\,\frac{m}{d}\right).$$

Demonstração: Primeiramente, notemos que como $d \neq 0$, podemos escrever $c = \frac{c}{d} \cdot d$ e $m = \frac{m}{d} \cdot d$. Uma vez que $a \cdot c \equiv b \cdot c\,(mod\,m)$, segue, da Proposição 2.3, que existe $k \in \mathbb{Z}$, tal que $c \cdot (a - b) = k \cdot m$. Assim, $\left(\frac{c}{d} \cdot d\right) \cdot (a - b) = k \cdot \left(\frac{m}{d} \cdot d\right)$. Como $d \neq 0$, segue da Lei do Corte que $\left(\frac{c}{d}\right) \cdot (a - b) = k \cdot \left(\frac{m}{d}\right)$. Portanto, $\frac{m}{d} \Big| \left(\frac{c}{d}\right) \cdot (a - b)$.

Da Proposição 1.25, temos que $mdc\left(\frac{m}{d}, \frac{c}{d}\right) = 1$. Logo, pelo Teorema 1.26, $\frac{m}{d} \Big| (a-b)$, ou seja, $a \equiv b\left(mod\,\frac{m}{d}\right)$. □

Exemplo 2.17 *Note que* $180 \equiv 36\,(mod\,12)$ *e* $mdc(9, 12) = 3$*. Pela Proposição 2.16*

$$\frac{180}{9} \equiv \frac{36}{9}\left(mod\,\frac{12}{3}\right),$$

ou seja, $20 \equiv 4\,(mod\,4)$.

Como consequência imediata das Proposições 2.11 e 2.16 temos:

Corolário 2.18 *Sejam* $a, b, c, m \in \mathbb{Z}$*, com* $m > 0$*,* $mdc(c, m) = 1$*. Então* $a \cdot c \equiv b \cdot c\,(mod\,m)$ *se, e somente se,* $a \equiv b\,(mod\,m)$.

Exemplo 2.19 *Sendo* $52 \equiv 2\,(mod\,5)$ *e* $mdc(2,5) = 1$*, segue do Corolário 2.18 que* $\frac{52}{2} \equiv \frac{2}{2}\,(mod\,5)$*, ou seja,* $26 \equiv 1\,(mod\,5)$*.*

A proposição apresentada a seguir, generaliza a Proposição 2.11.

Proposição 2.20 *Sejam* $a, b, c, d, m \in \mathbb{Z}$*, com* $m > 0$*. Se* $a \equiv b\,(mod\,m)$ *e* $c \equiv d\,(mod\,m)$*, então:*

(i) $a + c \equiv b + d\,(mod\,m)$*;*

(ii) $a - c \equiv b - d\,(mod\,m)$*;*

(iii) $a \cdot c \equiv b \cdot d\,(mod\,m)$*.*

Demonstração: Se $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, então, pela Proposição 2.3, existem $k, l \in \mathbb{Z}$ tais que $k \cdot m = a - b$ e $l \cdot m = c - d$.

(i) Como $(a+c)-(b+d) = (a-b)+(c-d)$, temos que $(a+c)-(b+d) = k \cdot m + l \cdot m = (k+l) \cdot m$. Portanto, $m \mid [(a+c)-(b+d)]$, ou seja, $a + c \equiv b + d\,(mod\,m)$.

(ii) Com efeito na prova do item (i), utilizando a identidade $(a-c)-(b-d) = (a-b)-(c-d)$, temos que $(a-c)-(b-d) = k \cdot m - l \cdot m = (k-l) \cdot m$. Portanto, $m \mid [(a-c)-(b-d)]$, ou seja, $a - c \equiv b - d\,(mod\,m)$.

(iii) Agora, utilizando a identidade $a \cdot c - b \cdot d = a \cdot c - b \cdot c + b \cdot c - b \cdot d = c \cdot (a-b) + b \cdot (c-d)$, temos que $a \cdot c - b \cdot d = c \cdot (k \cdot m) + b \cdot (l \cdot m) = m \cdot (c \cdot k + b \cdot l)$. Portanto, $m \mid (a \cdot c - b \cdot d)$, ou seja, $a \cdot c \equiv b \cdot d\,(mod\,m)$.

□

Exemplo 2.21 *Visto que* $18 \equiv 3\,(mod\,5)$ *e* $12 \equiv 2\,(mod\,5)$*, segue, da Proposição 2.20 (i), que* $(18 + 12) \equiv (3 + 2)\,(mod\,5)$*, ou seja,* $30 \equiv 5\,(mod\,5)$*.*

Exemplo 2.22 *Como* $17 \equiv 3\,(mod\,7)$ *e* $8 \equiv 1\,(mod\,7)$*, temos da Proposição 2.20 (ii), que* $(17 - 8) \equiv (3 - 1)\,(mod\,7)$*, ou seja,* $9 \equiv 2\,(mod\,7)$*.*

Exemplo 2.23 *Note que* $13 \equiv 4\,(mod\,3)$ *e* $7 \equiv 1\,(mod\,3)$. *Portanto, pela Proposição 2.20 (iii),* $13 \cdot 7 \equiv 4 \cdot 1\,(mod\,3)$, *ou seja,* $91 \equiv 4\,(mod\,3)$.

O próximo resultado, nos mostra que a congruência é preservada, quando elevamos a uma mesma potência positiva os seus membros. Mais precisamente, enunciamos o resultado a seguir.

Teorema 2.24 *Sejam* $a, b, k, m \in \mathbb{Z}$, $k > 0$ *e* $m > 0$. *Se* $a \equiv b\,(mod\,m)$, *então*

$$a^k \equiv b^k\,(mod\,m).$$

Demonstração: Sejam $a, b, m \in \mathbb{Z}$ e $m > 0$, tais que $a \equiv b\,(mod\,m)$. Logo, $m \mid (a-b)$. Agora, seja $k \in \mathbb{Z}$ e $k > 0$. Note que

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

Desta identidade é fácil observar que $(a-b) \mid (a^k - b^k)$. Como $m \mid (a-b)$ e $(a-b) \mid (a^k - b^k)$, pela Proposição 1.6 *(iii)*, segue que $m \mid (a^k - b^k)$, isto é, $a^k \equiv b^k\,(mod\,m)$.

□

Exemplo 2.25 *Se* $9 \equiv 2\,(mod\,7)$, *segue, do Teorema 2.24, que* $9^4 \equiv 2^4\,(mod\,7)$, *ou seja,* $6561 \equiv 16\,(mod\,7)$.

Observemos que, por definição, todo número inteiro a é congruente módulo m. Portanto, uma maneira de encontrar o resto da divisão de a por m, consiste em encontrar o número $r \in \{0, \ldots, m-1\}$ que seja congruente a a módulo m.

Exemplo 2.26 *Vamos determinar o resto da divisão de* $\left(116 + 17^{17}\right)^{21}$ *por* 8.

Certamente calcular $\left(116 + 17^{17}\right)^{21}$, para depois dividir o resultado por 8, não é o melhor caminho. Faremos isto de modo mais eficiente.

Primeiramente, note que $116 \equiv 4\,(mod\,8)$ e $17 \equiv 1\,(mod\,8)$, pois $8|(116-4) = 112$ e $8|(17-1) = 16$. Pelo Teorema 2.24, temos que $17^{17} \equiv 1^{17} \equiv 1\,(mod\,8)$. Pela Proposição 2.20 (i), obtemos $\left(116 + 17^{17}\right) \equiv 5\,(mod\,8)$.

Utilizando, novamente, o Teorema 2.24, temos que $\left(116 + 17^{17}\right)^2 \equiv 25\,(mod\,8)$ e sabemos que $25 \equiv 1\,(mod\,8)$. Então, pela Proposição 2.6 (iii), $\left(116+17^{17}\right)^2 \equiv 1\,(mod\,8)$. Mais uma vez, utilizando o Teorema 2.24, obtemos $\left(116 + 17^{17}\right)^{20} \equiv 1^{20} \equiv 1\,(mod\,8)$.

Como $\left(116+17^{17}\right) \equiv 5\,(mod\,8)$ e $\left(116+17^{17}\right)^{20} \equiv 1\,(mod\,8)$, então, pela Proposição 2.20 (iii), $\left(116 + 17^{17}\right)^{21} \equiv 5\,(mod\,8)$.

Como $5 \in \{0, 1, \ldots, 7\}$, temos que o resto da divisão de $\left(116 + 17^{17}\right)^{21}$ por 8 é 5.

Observação 2.27 *Seja $a \in \mathbb{Z}$, $a > 0$. Pelo que vimos na seção 1.2,*

$$a = a_k \cdot 10^k + \cdots + a_1 \cdot 10 + a_0,$$

onde $0 \leqslant a_i \leqslant 9$, para todo $i = 0, 1, \ldots, k$ e $a_k \neq 0$. Então,

$$a - a_0 = 10 \cdot (a_k \cdot 10^{k-1} + \cdots + a_1),$$

ou seja, $10|(a - a_0)$.

Logo, $a \equiv a_0\,(mod\,10)$. Isto significa que todo inteiro positivo é congruente módulo 10 ao seu algarismo das unidades.

Exemplo 2.28 *Vamos determinar o algarismo das unidades de 101^{101} e 99^{101}.*

Como $101 \equiv 1\,(mod\,10)$, então, pelo Teorema 2.24, $101^{101} \equiv 1^{101} \equiv 1\,(mod\,10)$. Então, o último algarismo de 101^{101} é 1.

Da mesma forma, $99 \equiv -1\,(mod\,10)$. Assim, $99^{101} \equiv (-1)^{101} \equiv -1 \equiv 9\,(mod\,10)$. Portanto, o último algarismo de 99^{101} é 9.

Capítulo 3

Aplicações

3.1 Critérios de Divisilibilidade

Os critérios de divisibilidade, são, em geral, regras práticas que permitem verificar se um dado número inteiro a é múltiplo de outro número inteiro b, tomando como base sua representação decimal (base 10). A seguir são apresentados critérios de divisibilidade para os números inteiros 2, 3, 4, 5, 6, 7, 8, 9, 10 e 11. Outros números inteiros também possuem regras de divisibilidade, no entanto pouco práticas.

3.1.1 Critério de Divisibilidade por 2

Teorema 3.1 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 2 *se, e somente se,* $2 \mid a_0$*, ou seja, se, e somente se,* $a_0 = 0, 2, 4, 6$ *ou* 8*.*

Demonstração: Como $10 \equiv 0\,(mod\,2)$, segue, do Teorema 2.24, que $10^k \equiv 0\,(mod\,2)$, para todo $k \in \mathbb{Z}$ e $k > 0$. Logo, $10^n \equiv 0\,(mod\,2)$, $10^{n-1} \equiv 0\,(mod\,2)$, $\cdots$, $10^1 \equiv 0\,(mod\,2)$.

Pela Proposição 2.11 (iii), temos que $(a_n \cdot 10^n) \equiv 0\,(mod\,2)$, $(a_{n-1} \cdot 10^{n-1}) \equiv 0\,(mod\,2)$, $\cdots$, $(a_1 \cdot 10) \equiv 0\,(mod\,2)$. Logo, pela Proposição 2.20 (i), $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10) \equiv 0\,(mod\,2)$. Suponha $2 \mid a$. Então $a \equiv 0\,(mod\,2)$, ou seja, $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2)$. Disso, do parágrafo anterior e da Proposição 2.20 (ii), podemos concluir que $a_0 \equiv 0\,(mod\,2)$. Portanto, $2 \mid a_0$. Como $0 \leq a_0 \leq 9$, segue que $a_0 = 0, 2, 4, 6\,ou\,8$.

Reciprocamente, suponha que $2|a_0$, ou seja, $a_0 \equiv 0\,(mod\,2)$. Como $a_n \cdot 10^n \equiv 0\,(mod\,2)$, $a_{n-1} \cdot 10^{n-1} \equiv 0\,(mod\,2)$, $\cdots$, $a_1 \cdot 10 \equiv 0\,(mod\,2)$ segue da Proposição 2.20 (i) que $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2)$. Portanto, $2|a$. □

Exemplo 3.2 *Seja* $a = 53716$. *Como* $2 \mid 6$, *pelo Teorema 3.1, temos que* $2 \mid 53716$. *Observemos que* $53716 = 2 \cdot 26858$.

3.1.2 Critério de Divisibilidade por 3

Teorema 3.3 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a, *onde* $a_k \in \mathbb{N}$, $0 \leqslant a_k < 10$, $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$. *Então,* a *é divisível por* 3 *se, e somente se,* $3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$.

Demonstração: Como $10 \equiv 1\,(mod\,3)$, segue, do Teorema 2.24, que $10^k \equiv 1\,(mod\,3)$, para todo $k \in \mathbb{Z}$ e $k > 0$. Logo, $10^n \equiv 1\,(mod\,3)$, $10^{n-1} \equiv 1\,(mod\,3)$, $\cdots$, $10 \equiv 1\,(mod\,3)$. Assim, pela Proposição 2.11 (iii), temos que $(a_n \cdot 10^n) \equiv a_n\,(mod\,3)$, $(a_{n-1} \cdot 10^{n-1}) \equiv a_{n-1}\,(mod\,3)$, $\cdots$, $(a_1 \cdot 10) \equiv a_1\,(mod\,3)$. Além disso, $a_0 \equiv a_0\,(mod\,3)$. Logo, pela Proposição 2.20 (i) temos que

$$(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0) \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0)\,(mod\,3).$$

Portanto, $3 \mid a$ implica que $a \equiv 0\,(mod\,3)$, ou seja,

$$(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,3).$$

Logo $(a_n + a_{n-1} + \cdots + a_1 + a_0) \equiv 0\,(mod\,3)$, ou seja, $3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$. □

Exemplo 3.4 *Seja* $a = 111111$. *Como* $3 \mid (1+1+1+1+1+1) = 6$, *pelo Teorema 3.3 temos que* $3 \mid 111111$. *Observemos que* $111111 = 3 \cdot 37037$.

3.1.3 Critério de Divisibilidade por 4

Teorema 3.5 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 4 *se, e somente se,* $4 \mid (a_1 \cdot 10 + a_0)$*.*

Demonstração: Como $10 = 2 \cdot 5$, temos que $10^k = 2^k \cdot 5^k$, para todo $k \in \mathbb{Z}$ e $k > 0$. Assim, para todo $k \in \mathbb{Z}$, $k \geq 2$, $2^2 \mid 2^k \cdot 5^k$, isto é, $10^k \equiv 0\,(mod\,2^2)$. Disso e da Proposição 2.11 (iii), segue que $(a_n \cdot 10^n) \equiv 0\,(mod\,2^2)$, $(a_{n-1} \cdot 10^{n-1}) \equiv 0\,(mod\,2^2)$, $\cdots$, $(a_2 \cdot 10^2) \equiv 0\,(mod\,2^2)$. Então, pela Proposição 2.20 (i) concluímos que

$$(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2) \equiv 0\,(mod\,2^2). \tag{3.1}$$

Agora, se $4 \mid a$, então, $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2^2)$. Logo, por 3.1 e pela Proposição 2.20 (ii), segue que $(a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2^2)$, ou seja, $4 \mid (a_1 \cdot 10 + a_0)$.

Reciprocamente, se $4 \mid (a_1 \cdot 10 + a_0)$, então $(a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2^2)$. Por 3.1 e pela Proposição 2.20 (i), segue que $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,2^2)$. Portanto, $4 \mid a$. □

Exemplo 3.6 *Seja* $a = 1250612$*. Como* $4 \mid 12$*, então, pelo Teorema 3.5, temos que* $4 \mid 1250612$*. Observemos que* $1250612 = 4 \cdot 312653$*.*

3.1.4 Critério de Divisibilidade por 5

Teorema 3.7 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 5 *se, e somente se,* $5 \mid a_0$*, ou seja, se, e somente se,* $a_0 = 0$ *ou* $a_0 = 5$*.*

Demonstração: Basta observar que $10 \equiv 0\,(mod\,5)$ e proceder como na prova do Critério de Divisibilidade por 2. Veja Teorema 3.1. □

Exemplo 3.8 *Seja* $a = 732180$*. Como* $a_0 = 0$*, pelo Teorema 3.7, temos que* $5 \mid 732180$*. Observemos que* $732180 = 5 \cdot 146436$*.*

3.1.5 Critério de Divisibilidade por 6

Teorema 3.9 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 6 *se, e somente se,* $2 \mid a$ *e* $3 \mid a$*.*

Demonstração: Note que $2 \mid 6$ e $3 \mid 6$. Assim, se $6 \mid a$, então, pela Proposição 1.6 (iii), $2 \mid a$ e $3 \mid a$. Pelos Critérios de Divisibilidade por 2 e 3, segue que a é par e $3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$.

Reciprocamente, se a é par e $3 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$, então $a = 2 \cdot b$, para algum $b \in \mathbb{Z}$ e $3 \mid a$. Portanto, $3 \mid (2 \cdot b)$ e $mdc(2, 3) = 1$, implicam que $3 \mid b$, ou seja, $b = 3 \cdot c$. Logo, $a = 2 \cdot b = 2 \cdot 3 \cdot c = 6 \cdot c$, e consequentemente $6 \mid a$. □

Exemplo 3.10 *Seja* $a = 5826$*. Como* $2 \mid 5826$ *e* $3 \mid 5826$*, pois* $3 \mid (5 + 8 + 2 + 6) = 21$ *, pelo Teorema 3.9, temos que* $6 \mid 5826$*.*

3.1.6 Critério de Divisibilidade por 7

Teorema 3.11 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 7 *se, e somente se,* $7 \mid [(a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1) - 2 \cdot a_0]$.

Demonstração: Se a é divisível por 7, então existe $k \in \mathbb{Z}$ tal que $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 = 7 \cdot k$, isto é,

$$\begin{aligned} a_0 &= 7 \cdot k - (a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10) \\ &= 7 \cdot k - 10 \cdot (a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1). \end{aligned}$$

Agora,

$$\begin{aligned} a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1 - 2 \cdot a_0 &= a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1 - \\ &\quad - 2 \cdot [7 \cdot k - 10 \cdot (a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1)] \\ &= a_n \cdot 10^{n-1} + + \cdots + a_2 \cdot 10 + a_1 - \\ &\quad - 14 \cdot k + 20 \cdot (a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) \\ &= 21 \cdot (a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 14 \cdot k \\ &= 7 \cdot [3 \cdot (a_n \cdot 10^{n-1} + \cdots + a_2 \cdot 10 + a_1) - 2 \cdot k]. \end{aligned}$$

Portanto, $7 \mid [(a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1) - 2 \cdot a_0]$.

Reciprocamente, suponhamos que $7 \mid [(a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1) - 2 \cdot a_0]$. Então existe $l \in \mathbb{Z}$ tal que $a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \cdots + a_2 \cdot 10 + a_1 - 2 \cdot a_0 = 7 \cdot l$.

Mas,

$$\begin{aligned} a_n \cdot 10^n + \cdots + a_1 \cdot 10 + a_0 &= 10 \cdot (a_n \cdot 10^{n-1} + \cdots + a_1) + a_0 \\ &= 10 \cdot (7 \cdot l + 2 \cdot a_0) + a_0 \\ &= 70 \cdot l + 21 \cdot a_0 = 7 \cdot (10 \cdot l + 3 \cdot a_0). \end{aligned}$$

Portanto, $7 \mid a$. □

Exemplo 3.12 *Seja* $a = 371$*. Como* $7 \mid (37 - 2 \cdot 1) = 35$*, pelo Teorema 3.11, temos que* $7 \mid 371$*. Observemos que* $371 = 7 \cdot 53$.

3.1.7 Critério de Divisibilidade por 8

Teorema 3.13 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 8 *se, e somente se,* $8 \mid (a_2 \cdot 10^2 + a_1 \cdot 10 + a_0)$*.*

Demonstração: Note que para todo $k \in \mathbb{Z}$, $k \geq 3$, temos que $2^3 \mid 2^k \cdot 5^k = 10^k$, ou seja, $10^k \equiv 0\,(mod\,2^3)$. Disso e da Proposição 2.11 (iii), vem que $(a_n \cdot 10^n) \equiv 0\,(mod\,2^3)$, $(a_{n-1} \cdot 10^{n-1}) \equiv 0\,(mod\,2^3)$, $\ldots$, $(a_3 \cdot 10^3) \equiv 0\,(mod\,2^3)$. Então, pela Proposição 2.20 (i) temos que $(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_3 \cdot 10^3) \equiv 0\,(mod\,2^3)$. O restante da prova segue a idéia da prova do Critério de Divisibilidade por 4, Teorema 3.5. □

Exemplo 3.14 *Seja* $a = 735424$*. Como* $8 \mid 424$*, então, pelo Teorema 3.13,* $8 \mid 735424$*. Observemos que* $735424 = 8 \cdot 91928$*.*

3.1.8 Critério de Divisibilidade por 9

Teorema 3.15 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 9 *se, e somente se,* $9 \mid (a_n + a_{n-1} + \cdots + a_1 + a_0)$*.*

Demonstração: Como $10 \equiv 1\,(mod\,9)$, segue, do Teorema 2.24, que $10^k \equiv 1\,(mod\,9)$, para todo $k \in \mathbb{Z}$ e $k > 0$. O final da prova segue a idéia da demonstração do Teorema 3.3 (Critério de Divisibilidade por 3). □

Exemplo 3.16 *Seja* $a = 1000800$*. Como* $9 \mid (1 + 0 + 0 + 0 + 8 + 0 + 0) = 9$*, então, pelo Teorema 3.15, vale que* $9 \mid 1000800$*. Observemos que* $1000800 = 9 \cdot 111200$*.*

3.1.9 Critério de Divisibilidade por 10

Teorema 3.17 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 10 *se, e somente se,* $a_0 = 0$*.*

Demonstração: Basta observar que $10 \equiv 0\,(mod\,10)$ e proceder como na prova do Teorema 3.1 (Critério de Divisibilidade por 2). □

Exemplo 3.18 *Seja* $a = 97260$*. Como* $a_0 = 0$*, então, pelo Teorema 3.17, temos que* 97260 *é divisível por* 10*.*

3.1.10 Critério de Divisibilidade por 11

Teorema 3.19 *Seja* $a = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0$ *a representação decimal do inteiro* a*, onde* $a_k \in \mathbb{N}$*,* $0 \leqslant a_k < 10$*,* $1 \leqslant k \leqslant n$ *e* $a_n \neq 0$*. Então,* a *é divisível por* 11 *se, e somente se,* $11 \mid \Big[(a_0 - a_1 + a_2 + \ldots + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n\Big]$.

Demonstração: Uma vez que $10 \equiv -1\,(mod\,11)$, segue, do Teorema 2.24, que $10^k \equiv (-1)^k\,(mod\,11)$, para todo $k \in \mathbb{Z}$ e $k > 0$, ou seja, $10^k \equiv 1\,(mod\,11)$, se k é par e $10^k \equiv -1\,(mod\,11)$, se k é ímpar. Assim, pela Proposição 2.11 (iii), temos $(a_1 \cdot 10) \equiv -a_1\,(mod\,11)$, $(a_2 \cdot 10^2) \equiv a_2\,(mod\,11)$, ..., $(a_{n-1} \cdot 10^{n-1}) \equiv (-1)^{n-1}\,(mod\,11)$, $(a_n \cdot 10^n) \equiv (-1)^n\,(mod\,11)$. Além disso, $a_0 \equiv a_0\,(mod\,11)$. Logo, pela Proposição 2.20 (i), temos que

$$(a_n \cdot 10^n + \cdots + a_0) \equiv (a_0 - a_1 + a_2 + \cdots + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n)\,(mod\,11).$$

Logo, $11 \mid a$, se e somente se $a \equiv 0\,(mod\,11)$, ou seja,

$$(a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \cdots + a_1 \cdot 10 + a_0) \equiv 0\,(mod\,11).$$

Daí $(a_0 - a_1 + a_2 + \cdots + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n) \equiv 0\,(mod\,11)$, isto é,

$$11 \mid \Big[a_0 - a_1 + a_2 + \cdots + a_{n-1} \cdot (-1)^{n-1} + a_n \cdot (-1)^n\Big].$$

□

Exemplo 3.20 *Seja* $a = 2450459$. *Como* $11 \mid (9-5+4-0+5-4+2) = 11$, *pelo Teorema 3.19 vemos que* $11 \mid 2450459$. *Observemos que* $2450459 = 11 \cdot 222769$.

Exemplo 3.21 *Seja* $a = 65044980$. *Como* $11 \mid (0-8+9-4+4-0+5-6) = 0$, *pelo Teorema 3.19,* $11 \mid 65044980$. *Notemos que* $65044980 = 11 \cdot 5913180$.

Inspirados na demonstração do Critério de Divisibilidade por 6, Teorema 3.9, temos o seguinte resultado:

Teorema 3.22 *Sejam* $m, n \in \mathbb{Z}$, $m, n > 1$ *tais que* $mdc(m, n) = 1$. *Então,* $a \in \mathbb{Z}$ *é divisível por* $m \cdot n$ *se, e somente se,* $m \mid a$ *e* $n \mid a$.

Demonstração: Note que $m \mid m \cdot n$ e $n \mid m \cdot n$. Assim, se $(m \cdot n) \mid a$ então, pela Proposição 1.6 (iii), $m \mid a$ e $n \mid a$.

Reciprocamente, se $m \mid a$ e $n \mid a$, então $a = m \cdot l$, para algum $l \in \mathbb{Z}$ e $n \mid a$. Assim, $n \mid (m \cdot l)$ e como $mdc(m, n) = 1$, temos que $n \mid l$. Logo, $l = n \cdot k$ para algum $k \in \mathbb{Z}$ e portanto $a = m \cdot n \cdot k$, ou seja, $(m \cdot n) \mid a$. □

Exemplo 3.23 *O número inteiro* $a = 476328$ *é divisível por* 12. *De fato,* $12 = 3 \cdot 4$ *e* $mdc(3, 4) = 1$. *Pelos Critérios de Divisibilidade por* 3 *e* 4, *concluímos que* $3 \mid 476328$ *e* $4 \mid 476328$. *Logo,* $12 \mid 476328$.

3.2 Dígito Verificador

Dígito verificador é um método de autenticação empregado para verificar a validade e a autenticidade de um valor numérico, evitando possíveis fraudes ou erros de digitação. Tal recurso é muito difundido em números de documentos de identificação, cartões de crédito e quaisquer outros códigos numéricos que demandam maior segurança.

O dígito verificador é composto de um ou mais algarismos incorporado ao valor original e calculado a partir deste, através de um determinado algoritmo.

Em seguida, mostraremos alguns casos de dígitos verificadores utilizados como identificadores.

3.2.1 Cartão de Crédito

Os principais Cartões de Crédito do mundo possuem de 14 a 19 dígitos, que não são aleatórios. Os primeiros dígitos definem a bandeira emissora. Por exemplo, os cartões de crédito *VISA* começam por 4, os cartões de crédito *MASTERCARD* começam por um número entre 51 e 55, *AMERICAN EXPRESS* começam por 34 ou 37. Os demais dígitos, exceto o último, definem o cliente do cartão. O último número representa o dígito verificador que é obtido dos anteriores cuja finalidade é garantir a correspondência entre o cartão de crédito e o cliente e evitar falsificações.

Este último dígito é gerado por um algoritmo matemático criado em 1954 por Hans Peter Luhn, engenheiro da IBM . Por conveniência, vamos considerar cartões de crédito com 16 dígitos, os mais comuns no Brasil. Assim, o número de um cartão de crédito constitui uma sequência de números da seguinte forma:

$$a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}a_{13}a_{14}a_{15}a_{16},$$

onde $a_i \in \mathbb{Z}$, $0 \leq a_i \leq 9$ para todo $i \in \{1, 2, \ldots, 16\}$ e a_{16} é o dígito verificador.

Para determinarmos o dígito verificador, precisamos de algumas condições.

Seja $b_i \in \mathbb{Z}$, onde i é ímpar entre 0 e 16, de tal forma que $b_i = 2 \cdot a_i$, se $2 \cdot a_i \leqslant 9$ e $b_i = 2 \cdot a_i - 9$, se $2 \cdot a_i > 9$. Desta forma, seja $S \in \mathbb{Z}$, tal que

$$S = \sum_{i=1}^{8} b_{(2i-1)} + \sum_{i=1}^{8} a_{2i}. \tag{3.2}$$

O dígito verificador, é determinado pela seguinte fórmula:

$$(S + a_{16}) \equiv 0 \,(mod\, 10), ou\, equivalente, a_{16} \equiv -S \,(mod\, 10). \tag{3.3}$$

Exemplo 3.24 *Vamos determinar o dígito verificador, de um cartão de crédito hipotético da* VISA*, iniciando por* 479358103469814*.*

Seja a_{16} o dígito verificador deste cartão de crédito. Primeiramente, vamos calcular os b_i.

$2 \cdot a_1 = 2 \cdot 4 = 8 < 9 \Rightarrow b_1 = 2 \cdot 4 = 8.$

$2 \cdot a_3 = 2 \cdot 9 = 18 > 9 \Rightarrow b_3 = 2 \cdot 9 - 9 = 9.$

$2 \cdot a_5 = 2 \cdot 5 = 10 > 9 \Rightarrow b_5 = 2 \cdot 5 - 9 = 1.$

$2 \cdot a_7 = 2 \cdot 1 = 2 < 9 \Rightarrow b_7 = 2 \cdot 1 = 2.$

$2 \cdot a_9 = 2 \cdot 3 = 6 < 9 \Rightarrow b_9 = 2 \cdot 3 = 6.$

$2 \cdot a_{11} = 2 \cdot 6 = 12 > 9 \Rightarrow b_{11} = 2 \cdot 6 - 9 = 3.$

$2 \cdot a_{13} = 2 \cdot 8 = 16 > 9 \Rightarrow b_{13} = 2 \cdot 8 - 9 = 7.$

$2 \cdot a_{15} = 2 \cdot 4 = 8 < 9 \Rightarrow b_{15} = 2 \cdot 4 = 8.$

Assim, de (3.2), temos que

$$S = (8 + 9 + 1 + 2 + 6 + 3 + 7 + 8) + (7 + 3 + 8 + 0 + 4 + 9 + 1) = 76.$$

Logo, de (3.3)

$$(76 + a_{16}) \equiv 0 \, (mod \, 10)$$

ou

$$a_{16} \equiv -76 \, (mod \, 10).$$

Como $-76 = (-7) \cdot 10 - 6 = (-7) \cdot 10 - 10 + 10 - 6 = (-8) \cdot 10 + 4$, temos que

$$a_{16} \equiv 4 \, (mod \, 10).$$

Como devemos ter $0 \leq a_{16} \leq 9$, segue que $a_{16} = 4$.

Exemplo 3.25 *Vamos verificar se o seguinte número corresponde a um cartão de crédito da bandeira MASTERCARD:*

$$5207159834271246$$

Como $a_1 a_2 = 52$, este cartão pode ser da bandeira *MASTERCARD*. Basta, agora, verificarmos se o dígito verificador, $a_{16} = 6$, está correto.

Primeiramente, vamos calcular os b_i.

$2 \cdot a_1 = 2 \cdot 5 = 10 > 9 \Rightarrow b_1 = 2 \cdot 5 - 9 = 1.$

$2 \cdot a_3 = 2 \cdot 0 = 0 < 9 \Rightarrow b_3 = 2 \cdot 0 = 0.$

$2 \cdot a_5 = 2 \cdot 1 = 2 < 9 \Rightarrow b_5 = 2 \cdot 1 = 2.$

$2 \cdot a_7 = 2 \cdot 9 = 18 > 9 \Rightarrow b_7 = 2 \cdot 9 - 9 = 9.$

$2 \cdot a_9 = 2 \cdot 3 = 6 < 9 \Rightarrow b_9 = 2 \cdot 3 = 6.$

$2 \cdot a_{11} = 2 \cdot 2 = 4 < 9 \Rightarrow b_{11} = 2 \cdot 2 = 4.$

$2 \cdot a_{13} = 2 \cdot 1 = 2 < 9 \Rightarrow b_{13} = 2 \cdot 1 = 2.$

$2 \cdot a_{15} = 2 \cdot 4 = 8 < 9 \Rightarrow b_{15} = 2 \cdot 4 = 8.$

Assim, de (3.2), temos que

$$S = (1 + 0 + 2 + 9 + 6 + 4 + 2 + 8) + (2 + 7 + 5 + 8 + 4 + 7 + 2) = 67.$$

Logo,

$$(S + a_{16}) = (67 + 6) = 73 \not\equiv 0 \, (mod \, 10).$$

Portanto, o número do cartão 5207159834271246 não é válido.

3.2.2 CPF - Cadastro de Pessoas Físicas

O Cadastro de Pessoas Físicas (CPF) é o registro de um cidadão na Receita Federal brasileira. O CPF guarda informações fornecidas pelo próprio contribuinte e por outros sistemas da Receita Federal.

O número de cada CPF é composto por 9 dígitos, mais 2 dígitos verificadores, totalizando 11 casas decimais. Assim, o número de CPF, é uma sequência de dígitos da seguinte forma:

$$a_1a_2a_3.a_4a_5a_6.a_7a_8a_9 - a_{10}a_{11},$$

onde $a_i \in \mathbb{Z}$ tal que $0 \leq a_i \leq 9$ para todo $i \in \{1, 2, \ldots, 11\}$.

O número composto pelos oito primeiros dígitos é chamado de número-base, o nono dígito define a Região Fiscal conforme quadro abaixo, o décimo e o décimo primeiro são os dígitos verificadores.

Dígito	Região Fiscal
0	RS
1	DF, GO, MS, MT, TO
2	AC, AM, AP, PA, RO, RR
3	CE, MA, PI
4	AL, PB, PE, RN
5	BA, SE
6	MG
7	ES, RJ
8	SP
9	PR, SC

Os dígitos verificadores são definidos aplicando Congruência módulo 11, da seguinte maneira:

Primeiramente, vamos apresentar a maneira de determinarmos o décimo dígito (a_{10}), que corresponde ao primeiro dígito verificador do CPF. Seja $S \in \mathbb{Z}$ dado por

$$S = \sum_{i=1}^{9} i \cdot a_i. \tag{3.4}$$

O número $S - a_{10}$ deve ser divisível por 11, ou seja, $11 \mid (S - a_{10})$. Portanto,

$$a_{10} \equiv S \,(mod\, 11). \tag{3.5}$$

Exemplo 3.26 *Vamos determinar o décimo dígito, de um CPF hipotético gerado no estado do Paraná, iniciando por* 112.358.139.

Seja a_{10} o décimo dígito deste CPF. Temos que

$$S = \sum_{i=1}^{9} i \cdot a_i = 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 5 \cdot 5 + 6 \cdot 8 + 7 \cdot 1 + 8 \cdot 3 + 9 \cdot 9 = 206.$$

Logo, de (3.5), devemos ter que

$$a_{10} \equiv 206 \,(mod\, 11).$$

Como $206 = 18 \cdot 11 + 8$, temos que $206 \equiv 8\,(mod\,11)$. Por transitividade, devemos ter $a_{10} \equiv 8\,(mod\,11)$ visto que $0 \leq a_{10} \leq 9$, segue que $a_{10} = 8$.

Agora, vamos descrever o método para determinarmos o décimo primeiro dígito (a_{11}) do CPF, que corresponde ao segundo dígito verificador do CPF.

Seja $S' \in \mathbb{Z}$ dado por

$$S' = \sum_{i=1}^{10} (i-1) \cdot a_i. \tag{3.6}$$

O número $S' - a_{11}$ deve ser divisível por 11, ou seja, $11 \mid (S' - a_{11})$. Portanto,

$$a_{11} \equiv S'\,(mod\,11). \tag{3.7}$$

Exemplo 3.27 *A partir do exemplo anterior, vamos determinar o décimo primeiro dígito, do CPF dada pela sequência* $112.358.139 - 8a_{11}$.

Primeiramente, temos

$$S' = \sum_{i=1}^{10} (i-1) \cdot a_i = 0 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 + 3 \cdot 3 + 4 \cdot 5 + 5 \cdot 8 + 6 \cdot 1 + 7 \cdot 3 + 8 \cdot 9 + 9 \cdot 8 = 245.$$

De (3.7), devemos ter

$$a_{11} \equiv 245\,(mod\,11).$$

Como $245 = 23 \cdot 11 + 3$, temos que $245 \equiv 3\,(mod\,11)$. Logo, $a_{11} \equiv 3\,(mod\,11)$ e como $0 \leq a_{11} \leq 9$, segue que $a_{11} = 3$.

Concluímos que no nosso exemplo, o número completo do CPF seria $112.358.139 - 83$.

Observação 3.28 *Se o resto da divisão de* S *ou* S' *por* 11 *for* 10*, ou seja,* $S \equiv 10\,(mod\,11)$ *ou* $S' \equiv 10\,(mod\,11)$*, o dígito* a_{10} *ou* a_{11} *será* 0.

Exemplo 3.29 *Vamos determinar o décimo e o décimo primeiro dígitos, de um CPF hipotético, iniciando por* $098.302.491 - a_{10}a_{11}$.

Note que

$$S = \sum_{i=1}^{9} i \cdot a_i = 1 \cdot 0 + 2 \cdot 9 + 3 \cdot 8 + 4 \cdot 3 + 5 \cdot 0 + 6 \cdot 2 + 7 \cdot 4 + 8 \cdot 9 + 9 \cdot 1 = 175.$$

De (3.5), devemos ter

$$a_{10} \equiv 175 \,(mod\, 11).$$

Como $175 = 15 \cdot 11 + 10$, temos que $175 \equiv 10 \,(mod\, 11)$. Por transitividade, devemos ter $a_{10} \equiv 10 \,(mod\, 11)$. Visto que se o resto da divisão de S por 11 é 10, segue que $a_{10} = 0$.

Temos também

$$S' = \sum_{i=1}^{10} (i-1) \cdot a_i = 0 \cdot 0 + 1 \cdot 9 + 2 \cdot 8 + 3 \cdot 3 + 4 \cdot 0 + 5 \cdot 2 + 6 \cdot 4 + 7 \cdot 9 + 8 \cdot 1 + 9 \cdot 0 = 139.$$

Logo, de (3.7),

$$a_{11} \equiv 139 \,(mod\, 11).$$

Como $139 = 12 \cdot 11 + 7$, segue que $139 \equiv 7 \,(mod\, 11)$. Logo, $a_{11} \equiv 7 \,(mod\, 11)$, e portanto, $a_{11} = 7$.

Concluímos, então, que o número completo do CPF completo seria $098.302.491 - 07$.

Exemplo 3.30 *Vamos verificar se o número* $001.492.910 - 43$ *pode ser o número de um CPF.*

Primeiramente, vamos verificar se o primeiro dígito verificador está correto. Seja a_{10} o primeiro dígito verificador deste CPF. Temos que

$$S = \sum_{i=1}^{9} i \cdot a_i = 1 \cdot 0 + 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 4 + 5 \cdot 9 + 6 \cdot 2 + 7 \cdot 9 + 8 \cdot 1 + 9 \cdot 0 = 147.$$

De (3.5), devemos ter que

$$a_{10} \equiv 147 \,(mod\, 11).$$

Como $147 = 13 \cdot 11 + 4$, temos que $147 \equiv 4\,(mod\,11)$. Por transitividade, devemos ter $a_{10} \equiv 4\,(mod\,11)$ visto que $0 \leq a_{10} \leq 9$, segue que $a_{10} = 4$.

O primeiro dígito verificador está correto. Agora, vamos verificar se o segundo dígito verificador também está correto. Temos que

$$S' = \sum_{i=1}^{10}(i-1) \cdot a_i = 0 \cdot 0 + 1 \cdot 0 + 2 \cdot 1 + 3 \cdot 4 + 4 \cdot 9 + 5 \cdot 2 + 6 \cdot 9 + 7 \cdot 1 + 8 \cdot 0 + 9 \cdot 4 = 157.$$

Logo, de (3.7), devemos ter

$$a_{11} \equiv 157\,(mod\,11).$$

Como $157 = 14 \cdot 11 + 3$, temos que $157 \equiv 3\,(mod\,11)$. Logo, $a_{11} \equiv 3\,(mod\,11)$ e como $0 \leq a_{11} \leq 9$, segue que $a_{11} = 3$.

Portanto, o número do CPF dado neste exemplo está correto.

3.3 Criptografia

Desde os tempos antigos até o presente, mensagens secretas são enviadas. A palavra "criptografia" é de origem grega e pode ser traduzida como "escrita escondida". A necessidade de comunicar de forma secreta ocorreu, a princípio, na diplomacia e em assuntos militares. A criptografia é uma técnica de escrita tão antiga quanto a própria escrita convencional. Os egípcios, os gregos e, especialmente os romanos, faziam uso da criptografia para evitar que suas mensagens fossem lidas por quem não deveria, caso interceptadas. Seu uso na Segunda Guerra mundial foi de tamanha grandeza. Nesta época os britânicos criaram um grupo de trabalho especialmente dedicado a interceptar e decodificar as mensagens trocadas entre os alemães, italianos e japoneses e, desde então, as técnicas criptográficas tornaram-se cada vez mais evoluídas.

Atualmente, temos a mesma necessidade de criptografar, ou seja, "tornar secretas", diversas informações, especialmente através de meios eletrônicos, onde a segurança da informação tornou-se de extrema importância para garantir o sigilo no envio e recebimento de documentos, operações financeiras e trocas de mensagens diversas. Nesse sentido,

a codificação de mensagens se tornou essencial para garantir que apenas o destinatário tenha acesso às informações nelas contidas. A criptografia pode se considerada como base para a evolução da computação moderna, e suas técnicas são aprimoradas constantemente, o que leva ao uso de algoritmos matemáticos cada vez mais complexos na busca de garantir a inviolabilidade da informação.

Neste capítulo, apresentamos um sistema simples de sigilo com base na aritmética modular. Esta tem origem com o imperador romano Júlio César, que enviava mensagens sigilosas aos seus exércitos. O princípio que Júlio César aplicava, chamado de "Cifra de César", consistia numa regra simples, a qual o emissor substituía cada letra do alfabeto pela letra correspondente a três posições (chave 3) depois dela, no alfabeto. O receptor, sabendo da chave dessa "criptografia", aplicava a operação inversa, ou seja, substituía cada letra recebida pela correspondente a três posições antes dela no alfabeto e, assim, poderia ler a mensagem de forma correta.

Vejamos como funcionava essa "Cifra de César". Primeiramente "deslocamos"as letras três casas e com as últimas três letras deslocadas para as três primeiras letras do alfabeto.

Texto Simples	A	B	C	D	E	F	G	H	I	J	K	L	M
Encriptado	X	Y	Z	A	B	C	D	E	F	G	H	I	J
Texto Simples	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Encriptado	K	L	M	N	O	P	Q	R	S	T	U	V	W

Assim, uma palavra simples como "MATEMATICA" seria codificada como "JXQBJXQFZX".

É claro, que se estivéssemos enviando mensagens em russo, grego, hebraico ou qualquer outra linguagem usaríamos o alfabeto adequada a cada idioma. Além disso, podemos querer incluir sinais de pontuação, um símbolo para indicar espaços em branco, e talvez os dígitos para representar números como parte da mensagem. No entanto, por uma questão de simplicidade, vamos nos restringir às letras do alfabeto Português.

3.3.1 Criptografia e Congruência

Um código, como na "Cifra de César", baseia-se em aritmética modular. Vamos definir, inicialmente, os números correspondentes a cada letra do alfabeto, variando de 0 a 25, de acordo com o quadro que segue.

Letra	A	B	C	D	E	F	G	H	I	J	K	L	M
Número Equivalente	0	1	2	3	4	5	6	7	8	9	10	11	12
Letra	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número Equivalente	13	14	15	16	17	18	19	20	21	22	23	24	25

Assim, seja P o equivalente numérico de uma letra do texto e C o equivalente numérico do texto cifrado correspondente. Logo,

$$C \equiv P + 3 \,(mod\, 26), \text{ onde } 0 \leqslant C \leqslant 25.$$

De acordo com a "Cifra de César", a correspondência entre as letras do "texto simples"e as letras do texto encriptado é dada de acordo com o quadro abaixo:

Simples	A	B	C	D	E	F	G	H	I	J	K	L	M
Número Equivalente	0	1	2	3	4	5	6	7	8	9	10	11	12
Encripatado	D	E	F	G	H	I	J	K	L	M	N	O	P
Número Equivalente	3	4	5	6	7	8	9	10	11	12	13	14	15
Simples	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número Equivalente	13	14	15	16	17	18	19	20	21	22	23	24	25
Encriptado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
Número Equivalente	16	17	18	19	20	21	22	23	24	25	0	1	2

Para cifrar uma mensagem usando essa transformação, primeiro agrupamos as letras em blocos de cinco letras e, em seguida, convertemos as letras para o seu equivalente numérico. O agrupamento de letras em blocos dificulta a descodificação baseado no reconhecimento de palavras específicas.

Agora, vamos mostrar como esse procedimento de cifragem de mensagem acontece. Primeiro fixamos uma frase. Por exemplo:

ESTA MENSAGEM E SECRETA

Agrupando em blocos de cincos letras, a mensagem fica:

ESTAM ENSAG EMESE CRETA

Agora, convertendo as letras em números equivalentes de acordo com o quadro acima, obtemos:

$$4\ \ 18\ 19\ 0\ 12 \qquad 4\ \ 13\ \ 18\ 0\ 6 \qquad 4\ 12\ 4\ 18\ 4 \qquad 2\ 17\ 4\ 19\ 0$$

Usando a Cifra de César ($C \equiv P + 3\,(mod\,26)$, com $0 \leq C \leq 25$), obtemos

$$7\ \ 21\ 22\ 3\ 15 \qquad 7\ \ 16\ 21\ 3\ 9 \qquad 7\ 15\ 7\ 21\ 7 \qquad 5\ \ 20\ 7\ 22\ 3$$

Aplicando a equivalência numérica correspondente a cada letra, temos:

HVWDP HQVAG HPHVH FUHWD

Esta é, portanto, a mensagem codificada.

O receptor irá decifrá-la da seguinte maneira: primeiramente, as letras são convertidas em números e, em seguida, aplica-se a relação $P \equiv C - 3\,(mod\,26)$, com $0 \leq C \leq 25$, para transformar o texto cifrado na versão numérica do texto simples e, finalmente, a mensagem é convertida em letras.

Vamos ilustrar este procedimento de decifração com a mensagem que codificamos anteriormente. A mensagem codificada era:

HVWDP HQVAG HPHVH FUHWD

Primeiro, trocamos as letras pelos seus números correspondentes. Assim, temos:

$$7\ \ 21\ 22\ 3\ 15 \qquad 7\ \ 16\ 21\ 3\ 9 \qquad 7\ 15\ 7\ 21\ 7 \qquad 5\ \ 20\ 7\ 22\ 3$$

Em seguida, utilizamos a relação $P \equiv C - 3\,(mod\,26)$ para alterar o código recebido para o "texto simples", obtendo:

$$4\ \ 18\ 19\ 0\ 12 \qquad 4\ \ 13\ \ 18\ 0\ 6 \qquad 4\ 12\ 4\ 18\ 4 \qquad 2\ 17\ 4\ 19\ 0$$

Aplicando a equivalência numérica correspondente a cada letra, temos:

ESTAM ENSAG EMESE CRETA

Combinando as letras de forma apropriada em palavras, encontramos a mensagem original:

ESTA MENSAGEM E SECRETA

A "Cifra de César"é uma das famílias de cifras, determinadas da seguinte forma:

$$C \equiv P + k\,(mod\,26),\ \text{onde}\ 0 \leqslant C \leqslant 25,$$

onde k é a chave que representa o tamanho do deslocamento de letras do alfabeto. Existem 26 diferentes transformações desse tipo, incluindo o caso de $k \equiv 0\,(mod\,26)$, em que as letras não são alteradas, neste caso, $C \equiv P\,(mod\,26)$.

Exemplo 3.31 *Vamos cifrar a frase "A matemática é um instrumento poderoso". Adotando chave* 17*, ou seja,* $C \equiv P + 17\,(mod\,26)$*, onde* $0 \leqslant C \leqslant 25$*.*

Como adotamos a chave 17, vejamos como fica a correspondência entre as letras.

A letra "A"corresponde a 0; logo $P = 0$. Assim, $C \equiv 0 + 17\,(mod\,26)$, ou seja,

$$C \equiv 17\,(mod\,26).$$

Desta forma 17 é o número equivalente a letra "A".

A letra "B"corresponde a 1; logo $P = 1$. Assim, $C \equiv 1 + 17\,(mod\,26)$, isto é,

$$C \equiv 18\,(mod\,26).$$

Isto significa que o número equivalente a letra "B"é 18.

A letra "C"corresponde a 2; logo $P = 2$. Assim, $C \equiv 2 + 17\,(mod\,26)$, ou seja,

$$C \equiv 19\,(mod\,26).$$

Desta forma 19 é o número equivalente a letra "C".

E assim, montamos o quadro abaixo:

Simples	A	B	C	D	E	F	G	H	I	J	K	L	M
Número Equivalente	0	1	2	3	4	5	6	7	8	9	10	11	12
Encripatado	R	S	T	U	V	W	X	Y	Z	A	B	C	D
Número Equivalente	17	18	19	20	21	22	23	24	25	0	1	2	3
Simples	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número Equivalente	13	14	15	16	17	18	19	20	21	22	23	24	25
Encriptado	E	F	G	H	I	J	K	L	M	N	O	P	Q
Número Equivalente	4	5	6	7	8	9	10	11	12	13	14	15	16

Agrupando em blocos de cincos letras, a mensagem fica:

AMATE MATIC AEUMI NSTRU MENTO PODER OSO

Agora, convertendo as letras em números equivalentes de acordo com o quadro acima, obtemos:

$$0\ 12\ 0\ 19\ 4 \quad 12\ 0\ 19\ 8\ 2 \quad 0\ 4\ 20\ 12 \quad 8$$
$$13\,18\,19\,17\,20 \quad 12\ 4\ 13\ 19\ 14 \quad 15\ 14\ 3\ 4\ 17 \quad 14\ 18\ 14$$

Usando a Cifra de César ($C \equiv P + 17\,(mod\,26)$, com $0 \leq C \leq 25$), obtemos

$$17\ 3\ 17\ 10\ 21 \quad 3\ 17\ 10\ 25\ 19 \quad 17\ 21\ 11\ 3 \quad 25$$
$$4\,9\,10\,8\,11 \quad 3\ 21\ 4\ 10\ 5 \quad 6\ 5\ 20\ 21\ 8 \quad 5\ 9\ 5$$

Aplicando a equivalência numérica correspondente a cada letra, temos:

RDRKV DRKZT RVLDZ EJKIL DVEKF GFUVI FJF

Esta é, portanto, a mensagem cifrada.

Exemplo 3.32 *Vamos decifrar a mensagem cifrada*

RDRKV DRKZT RVLDZ EJKIL DVEKF GFUVI FJF.

Primeiro, trocamos as letras pelos seus números correspondentes. Assim, temos:

$$17\ 3\ 17\ 10\ 21 \quad 3\ 17\ 10\ 25\ 19 \quad 17\ 21\ 11\ 3 \quad 25$$
$$4\,9\,10\,8\,11 \quad 3\ 21\ 4\ 10\ 5 \quad 6\ 5\ 20\ 21\ 8 \quad 5\ 9\ 5$$

Em seguida, utilizamos a relação $P \equiv C - 17\,(mod\,26)$ para alterar o código recebido para o "texto simples", obtendo:

$$0\ 12\ 0\ 19\ 4 \quad 12\ 0\ 19\ 8\ 2 \quad 0\ 4\ 20\ 12 \quad 8$$
$$13\,18\,19\,17\,20 \quad 12\ 4\ 13\ 19\ 14 \quad 15\ 14\ 3\ 4\ 17 \quad 14\ 18\ 14$$

Aplicando a equivalência numérica correspondente a cada letra, temos:

AMATE MATIC AEUMI NSTRU MENTO PODER OSO

Combinando as letras de forma apropriada em palavras, encontramos a mensagem original:

A MATEMÁTICA É UM INSTRUMENTO PODEROSO

Observação 3.33 *Notamos que a medida que aumentarmos o alfabeto acrescentando símbolos como @, +, * ou letras acentuadas, tais como, á, é, ô, etc, aumentamos automaticamente as possibilidades da chave k, e portanto, fica mais difícil para um interceptador decodificar.*

3.4 Calendário

Há indícios de que o homem pré-histórico usou de diversas técnicas para contar o tempo, como pinturas ou ranhuras em cavernas, evoluindo-as até a criação do calendário, que nada mais é do que um sistema para contagem e agrupamento de dias, visando atender as necessidades civis e religiosas de uma cultura.

O primeiro calendário foi inventado pelos Sumérios, na Mesopotâmia, por volta de 2700 a.C. tendo sido posteriormente melhorado pelos Caldeus. Este calendário era constituído de 12 meses lunares com 29 ou 30 dias. Cada mês se iniciava na lua nova, o que totalizava 354 dias no ano, e o tornava mais curto do que o calendário solar, criado pelos egípcios por volta de 2500 a.C. Os Caldeus o corrigiam, acrescentando um mês a cada três anos.

As diversas civilizações ao redor do mundo criaram diferentes calendários, baseados em suas crenças e conhecimentos. Atualmente, o Calendário Gregoriano é utilizado no mundo todo para demarcar o ano civil. Ele foi instituído pelo Papa Gregório XIII em 1582, e sua composição é resultado de uma reformulação do Calendário Juliano, implantado pelos romanos.

O Calendário Gregoriano é solar, ou seja, baseado no movimento da Terra em torno do Sol, que tem a duração de $365 + \frac{97}{400}$ dias (365,2425 dias), que equivale a 365 dias, 5 horas, 48 minutos e 47 segundos. A contagem do tempo no Calendário Gregoriano é feita em dias, agrupados em 12 meses. Os meses são constituídos por 30 ou 31 dias, com exceção de fevereiro, que é constituído por 28 ou 29 dias.

A ocorrência de 29 dias no mês de fevereiro se dá pois, como instrumento de uso prático, o calendário adota a quantidade exata de 365 dias para o período de um ano, ou seja, período de tempo menor do que a duração de uma volta completa da Terra em torno do Sol. Temos, então, que esta diferença, equivalente a 0,2425 dia, quando multiplicada por 4 resulta em 0,97 dia. Daí, faz-se, a cada 4 anos, o acréscimo de 1 dia no mês de fevereiro, o que corresponde ao chamado ano bissexto com 366 dias. Todavia, essa alteração provoca uma nova discrepância, de +0,03 dia. Para corrigi-la, estabeleceu-se

as seguintes regras:

- ano múltiplo de 4 é bissexto;
- ano múltiplo de 100 e não múltiplo de 400, não é bissexto;
- ano múltiplo de 400, é bissexto.

Tais regras se justificam pois, $0,2425$ equivale a $\frac{1}{4} - \frac{1}{100} + \frac{1}{400}$.

Desta forma, os anos 2008, 2012, 2016, 2020, 2024 e 2028 são bissextos, pois são múltiplos de 4 e não são múltiplos de 100. Os anos 1700, 1800 e 1900 não são bissextos, pois são múltiplos de 100 e não são múltiplos de 400. Finalmente, os anos 1600, 2000, 2400 e 2800 são bissextos, pois são múltiplos de 400.

3.4.1 Calendário e Congruência

Antes de relacionarmos o Calendário com Congruência, vamos estabelecer que os dias da semana são quarta-feira, quinta-feira, sexta-feira, sábado, domingo, segunda-feira e terça-feira, sempre nesta ordem e vamos estabelecer que cada dia da semana corresponde a um determinado número entre 0 e 6 (inclusive), conforme quadro abaixo.

Quarta-feira	0
Quinta-feira	1
Sexta-feira	2
Sábado	3
Domingo	4
Segunda-feira	5
Terça-feira	6

(Quadro I)

A correspondência do quadro acima é aleatório. Algo curioso, é que é sempre possível descobrir qual é o dia da semana referente a datas passadas ou futuras aplicando conceitos de Congruência.

Precisamos, primeiramente, fazer alguns ajustes nos meses, pois em Fevereiro temos 29 dias, nos anos bissextos, e nos outros anos apenas 28 dias. Diante disso, iremos reenumerar os meses do ano da seguinte forma: Março será o 1º mês, Abril o 2º, Maio o 3º, e assim sucessivamente. Desta forma, Janeiro e Fevereiro, serão considerados o 11º e o 12º meses do ano anterior, respectivamente.

Assim, por exemplo, Fevereiro de 2015 será considerado como 12º mês de 2014, e Junho de 2015, será considerado 4º mês de 2015.

Com base nestes ajustes, vamos utilizar 1º de Março de 1600 como base, ou seja, iremos determinar o dia da semana apenas para datas após 1º de Março de 1600.

Seja $X_N \in \{0, 1, 2, 3, 4, 5, 6\}$ o número que representa o dia da semana de 1º de Março no ano N, conforme quadro I. Por exemplo, quando $N = 2015$, $X_{2015} = 4$ (Domingo).

Considerando o ano N como não bissexto, temos que 1º de Março do ano $N-1$ e 1º de Março do ano N tem um deslocamento de 1 dia, em relação aos dias da semana, pois o ano não bissexto possui 365 dias e $365 \equiv 1\,(mod\,7)$. Então, $X_N \equiv X_{N-1} + 1\,(mod\,7)$.

Agora, se N for um ano bissexto, o deslocamento, em relação aos dias da semana, será de 2 dias, pois o ano bissexto possui 366 dias e $366 \equiv 2\,(mod\,7)$. Então, $X_N \equiv X_{N-1} + 2\,(mod\,7)$, quando N for ano bissexto.

Vamos, primeiramente, determinar em qual dia da semana será 1º de Março de qualquer ano N após 1600. Para isto, precisamos determinar quantos anos se passaram e quantos anos bissextos existiram no intervalo de 1600 a N.

Seja $A = N - 1600$. Note que A é a quantidade de anos que se passaram entre 1600 e o ano desejado, e assim podemos determinar os deslocamentos nos dias da semana.

Seja $B = \left[\frac{A}{4}\right] - \left[\frac{A}{100}\right] + \left[\frac{A}{400}\right]$. Sendo $\left[\frac{A}{n}\right]$ a quantidade de múltiplos de n entre 1600 e N, para $n = 4$, 100 e 400, temos que B é a quantidade de anos bissextos entre 1600 e o ano desejado. Lembramos que cada ano bissexto desloca um dia a mais na semana, além do deslocamento de um ano para outro.

Desta forma, podemos concluir que

$$X_N \equiv (X_{1600} + A + B)\,(mod\,7).$$

Exemplo 3.34 *Vamos determinar que dia da semana foi 1º de março de 1600.*

Verificando no calendário de 2015 (abaixo), observamos que 1º de março de 2015 é um Domingo.

CALENDÁRIO (MARÇO DE 2015)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 13/01/2015 às 13:00

Desta forma, $X_{2015} = 4$ conforme o Quadro I. Além disso,
$A = 2015 - 1600 = 415$.

$$B = \left[\frac{415}{4}\right] - \left[\frac{415}{100}\right] + \left[\frac{415}{400}\right] = 103 - 4 + 1 = 100.$$

Substituindo em

$$X_{2015} \equiv (X_{1600} + A + B)\,(mod\,7),$$

temos

$$4 \equiv (X_{1600} + 415 + 100)\,(mod\,7),$$

Pela Proposição 2.11 (ii)

$$-511 \equiv X_{1600}\,(mod\,7).$$

Agora, pelo Critério de Divisibilidade por 7, $7 \mid 511$, pois $7 \mid (51-2) = 49$. Logo, $-511 \equiv 0\,(mod\,7)$ e pela Proposição 2.6 (ii) temos que $0 \equiv X_{1600}\,(mod\,7)$. Como $X_{1600} \in \{0, 1, \ldots, 6\}$ segue que $X_{1600} = 0$, ou seja, 1º de Março de 1600 foi uma quarta-feira.

Observação 3.35 *Como $X_{1600} = 0$, segue que*

$$X_N \equiv (A + B)\,(mod\,7),$$

Até este momento, conseguimos determinar o dia da semana de 1º de Março de qualquer ano. Agora, vamos determinar o dia da semana de um dia qualquer de Março de um ano $N \geq 1600$.

Seja y o dia escolhido para determinarmos o correspondente dia da semana. Precisamos determinar a quantidade de deslocamentos que este dia sofreu em relação ao dia 1º de Março daquele ano. Observemos, por exemplo, que dia 2 de Março de 1600 é uma quinta-feira. Então o deslocamento foi de 1 dia na semana, ou seja, qualquer dia de Março que escolhermos o deslocamento será sempre de $y - 1$ dias da semana em relação ao dia 1º de Março do ano N. Desta forma, seja $C = y - 1$ o cálculo deste deslocamento.

Seja $X \in \{0, 1, 2, 3, 4, 5, 6\}$ o número que representa o dia da semana, conforme quadro I, do dia y de Março no ano N. Vamos deduzir uma maneira de determiná-lo.

Afirmamos que

$$(X - X_N) \equiv C\,(mod\,7).$$

De fato, note que $C \in \{0, 1, 2, 3, \ldots, 29, 30\}$.

- Se $C = 0$, $C = 7$, $C = 14$, $C = 21$ ou $C = 28$, então y de Março do ano N e 1º de Março do ano N correspondem ao mesmo dia da semana. Daí $X = X_N$, ou seja, $X - X_N = 0$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 1$, $C = 8$, $C = 15$, $C = 22$ ou $C = 29$, então y de Março do ano N e 1º de Março do ano N diferem de 1 em relação aos dias da semana. Daí $X = X_N + 1$, ou seja, $X - X_N = 1$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 2$, $C = 9$, $C = 16$, $C = 23$ ou $C = 30$, então y de Março do ano N e 1º de Março do ano N diferem de 2 em relação aos dias da semana. Daí $X = X_N + 2$, ou seja, $X - X_N = 2$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 3$, $C = 10$, $C = 17$ ou $C = 24$, então y de Março do ano N e 1º de Março do ano N diferem de 3 em relação aos dias da semana. Daí $X = X_N + 3$, ou seja, $X - X_N = 3$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 4$, $C = 11$, $C = 18$ ou $C = 25$, então y de Março do ano N e 1º de Março do ano N diferem de 4 em relação aos dias da semana. Daí $X = X_N + 4$, ou seja, $X - X_N = 4$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 5$, $C = 12$, $C = 19$ ou $C = 26$, então y de Março do ano N e 1º de Março do ano N diferem de 5 em relação aos dias da semana. Daí $X = X_N + 5$, ou seja, $X - X_N = 5$, então $(X - X_N) \equiv C\,(mod\,7)$.

- Se $C = 6$, $C = 13$, $C = 20$ ou $C = 27$, então y de Março do ano N e 1º de Março do ano N diferem de 6 em relação aos dias da semana. Daí $X = X_N + 6$, ou seja, $X - X_N = 6$, então $(X - X_N) \equiv C\,(mod\,7)$.

Portanto, $X_N \equiv (A + B)\,(mod\,7)$ e $(X - X_N) \equiv C\,(mod\,7)$. Pela Proposição 2.20 (i), temos que $X \equiv (A + B + C)\,(mod\,7)$. Com esta fórmula, podemos determinar o dia da semana de qualquer dia de Março do ano $N \geq 1600$.

Exemplo 3.36 *Vamos determinar que dia da semana corresponde ao dia 28 de março de 2000.*

Inicialmente, temos

$A = 2000 - 1600 = 400$.

$$B = \left[\frac{400}{4}\right] - \left[\frac{400}{100}\right] + \left[\frac{400}{400}\right] = 100 - 4 + 1 = 97.$$

Como $y = 28$, *temos que* $C = 28 - 1 = 27$.

Então, $X \equiv (400 + 97 + 27)\,mod\,7$, *ou seja,* $X \equiv 524\,mod\,7$. *Logo,* $X = 6$. *Portanto, o dia 28 Março de 2000 foi terça-feira.*

Verificando no calendário de 2000 (abaixo), observamos que 28 de março de 2000 foi, realmente, terça-feira.

CALENDÁRIO (MARÇO DE 2000)

Domingo	*Segunda*	*Terça*	*Quarta*	*Quinta*	*Sexta*	*Sábado*
			1	*2*	*3*	*4*
5	*6*	*7*	*8*	*9*	*10*	*11*
12	*13*	*14*	*15*	*16*	*17*	*18*
19	*20*	*21*	*22*	*23*	*24*	*25*
26	*27*	*28*	*29*	*30*	*31*	

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 11:00

Finalmente, vamos determinar o dia da semana para qualquer data que desejarmos (a partir de 1º de Março de 1600).

Se todos os meses do ano fossem de 28 dias e, sabendo que 28 é divisível por 7, todos os meses do ano se iniciariam no mesmo dia da semana. Ocorre que nos anos não bissextos, há meses com 28, 30 ou 31 dias, o que gera um deslocamento nos dias da semana.

Como antes X, representa o dia da semana de qualquer data de março do ano N, precisamos, agora, encontrar o deslocamento que cada mês produz nos dias da semana.

Seja $W \in \{0, 1, 2, 3, 4, 5, 6\}$ o número que representa o dia da semana, conforme quadro I, de qualquer dia, mês e ano (a partir de Março de 1600).

Sabendo que março, mês anterior a abril, possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias deslocarão os dias da semana de abril em 3 unidades. Logo, para **abril**,

$$W \equiv (X + 3)\,(mod\,7).$$

Assim, já que abril (mês anterior) possui 30 dias, e $30 \equiv 2\,(mod\,7)$, segue que estes 2 dias, somados com os 3 dias acumulados no mês anterior, deslocarão os dias da semana de maio em 5 unidades. Logo, para **maio**,

$$W \equiv (X + 5)\,(mod\,7).$$

Agora maio (mês anterior) possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias, somados com os 5 dias acumulados no mês anterior, deslocarão os dias da semana de junho em 8 unidades. Logo, para **junho**, $W \equiv (X+8)\,(mod\,7)$. Como $8 \equiv 1\,(mod\,7)$, temos que

$$W \equiv (X+1)\,(mod\,7).$$

No próximo mês, sabendo que junho (mês anterior) possui 30 dias, e $30 \equiv 2\,(mod\,7)$, segue que estes 2 dias, somados com 1 dia acumulado no mês anterior, deslocarão os dias da semana de julho em 3 unidades. Logo, para **julho**,

$$W \equiv (X+3)\,(mod\,7).$$

Agora, sabendo que julho (mês anterior) possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias, somados com os 3 dias acumulados no mês anterior, deslocarão os dias da semana de agosto em 6 unidades. Logo, para **agosto**,

$$W \equiv (X+6)\,(mod\,7).$$

Sabendo que agosto (mês anterior) possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias, somados com os 6 dias acumulados no mês anterior, deslocarão os dias da semana de setembro em 9 unidades. Logo, para **setembro**, $W \equiv (X+9)\,(mod\,7)$. Como $9 \equiv 2\,(mod\,7)$, temos que

$$W \equiv (X+2)\,(mod\,7).$$

Assim, já que agosto (mês anterior) possui 30 dias, e $30 \equiv 2\,(mod\,7)$, segue que estes 2 dias, somados com os 2 dias acumulados no mês anterior, deslocarão os dias da semana de outubro em 4 unidades. Logo, para **outubro**,

$$W \equiv (X+4)\,(mod\,7).$$

Agora, sabendo que outubro (mês anterior) possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias, somados com os 4 dias acumulados no mês anterior, deslocarão os dias da semana de novembro em 7 unidades. Logo, para **novembro**, $W \equiv (X+7)\,(mod\,7)$. Como $7 \equiv 0\,(mod\,7)$, temos que

$$W \equiv (X+0)\,(mod\,7).$$

No próximo mês, sabendo que novembro (mês anterior) possui 30 dias, e $30 \equiv 2\,(mod\,7)$, como o mês anterior não produziu deslocamento, segue que estes 2 dias deslocarão os dias da semana de dezembro em 2 unidades. Logo, para **dezembro**,

$$W \equiv (X + 2)\,(mod\,7).$$

Vamos reelembrar que mudamos a ordem dos meses, portanto janeiro é considerado mês após dezembro. Desta forma, sabendo que dezembro possui 31 dias, e $31 \equiv 3\,(mod\,7)$, e que antecede janeiro, segue que estes 3 dias, somados com os 2 dias acumulados no mês "anterior"deslocarão os dias da semana de janeiro em 5 unidades. Logo, para **janeiro**,

$$W \equiv (X + 5)\,(mod\,7).$$

Agora para **fevereiro**, sabendo que janeiro (mês anterior) possui 31 dias, e $31 \equiv 3\,(mod\,7)$, segue que estes 3 dias, somados com os 5 dias acumulados no mês anterior deslocarão os dias da semana de novembro em 8 unidades. Logo, para **fevereiro**, $W \equiv (X + 8)\,(mod\,7)$. Como $8 \equiv 1\,(mod\,7)$, temos que

$$W \equiv (X + 1)\,(mod\,7).$$

E finalmente, sabendo que fevereiro possui 28 dias (anos não bissextos), e $28 \equiv 0\,(mod\,7)$, segue que o mês de março vai acumular 1 dia, entretanto este acúmulo já é calculado no valor de A.

Com base nisso, D representa o deslocamento cumulativo dos dias da semana, mês a mês, conforme quadro abaixo.

Mês	D	Mês	D
Março	0	Setembro	2
Abril	3	Outubro	4
Maio	5	Novembro	0
Junho	1	Dezembro	2
Julho	3	Janeiro	5
Agosto	6	Fevereiro	1

(Quadro II)

Desta forma, $W \equiv (X + D)\,(mod\,7)$, ou seja,

$$W \equiv (A + B + C + D)\,(mod\,7).$$

Exemplo 3.37 *Vamos determinar que dia da semana foi 30 de Abril de 1777 (Nascimento de Johann Carl Friedrich Gauss).*

Temos:

$A = 1777 - 1600 = 277.$

$$B = \left[\frac{177}{4}\right] - \left[\frac{177}{100}\right] + \left[\frac{177}{400}\right] = 44 - 1 + 0 = 43.$$

Como $y = 30$, temos que $C = 30 - 1 = 29$.

Além disso, $D = 3$, pois o mês é abril (ver Quadro II).

Então, $W \equiv (177 + 43 + 29 + 3)\,(mod\,7)$, ou seja, $W \equiv 252\,(mod\,7)$. Logo, $W = 0$. Portanto, o dia 30 de Abril de 1777 foi quarta-feira.

Verificando no calendário de 1777 (abaixo), observamos que 30 de Abril de 1777 é, realmente, quarta-feira.

CALENDÁRIO (ABRIL DE 1777)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30			

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 14:00

Exemplo 3.38 *Vamos determinar que dia da semana foi 15 de Novembro de 1889 (Proclamação da República Brasileira).*

Temos:

$A = 1889 - 1600 = 289.$

$$B = \left[\frac{289}{4}\right] - \left[\frac{289}{100}\right] + \left[\frac{289}{400}\right] = 72 - 2 + 0 = 70.$$

Como $y = 15$, temos que $C = 15 - 1 = 14$.

Também, $D = 0$, pois o mês é novembro (ver Quadro II).

Então, $W \equiv (289 + 70 + 14 + 0)\,(mod\,7)$, ou seja, $W \equiv 373\,(mod\,7)$. Logo, $W = 2$. Portanto, o dia 15 de Novembro de 1889 foi sexta-feira.

Verificando no calendário de 1889 (abaixo), observamos que 15 de Novembro de 1889 é, realmente, sexta-feira.

CALENDÁRIO (NOVEMBRO DE 1889)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 14:30

Exemplo 3.39 *Vamos determinar que dia da semana foi 28 de Julho de 1914 (Início da Primeira Guerra Mundial).*

Temos:

$A = 1914 - 1600 = 314.$

$$B = \left[\frac{314}{4}\right] - \left[\frac{314}{100}\right] + \left[\frac{314}{400}\right] = 78 - 3 + 0 = 75.$$

Como $y = 28$, temos que $C = 28 - 1 = 27$.

$D = 3$, pois o mês é julho (ver Quadro II).

Então, $W \equiv (314 + 75 + 27 + 3)\,(mod\,7)$, ou seja, $W \equiv 419\,(mod\,7)$. Logo, $W = 6$. Portanto, o dia 28 de Julho de 1914 foi terça-feira.

Verificando no calendário de 1914 (abaixo), observamos que 28 de Julho de 1914 é, realmente, terça-feira.

CALENDÁRIO (JULHO DE 1914)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 15:00

Exemplo 3.40 *Vamos determinar que dia da semana foi 8 de Janeiro de 1942 (Nascimento de Stephen William Hawking).*

Temos:

$A = 1941 - 1600 = 341$. ($N = 1941$, pois em janeiro consideramos como o 11º mês de 1941).

$$B = \left[\frac{341}{4}\right] - \left[\frac{341}{100}\right] + \left[\frac{341}{400}\right] = 85 - 3 + 0 = 82.$$

Como $y = 8$, temos que $C = 8 - 1 = 7$.

$D = 5$, pois o mês é janeiro (ver Quadro II).

Então, $W \equiv (341 + 82 + 7 + 5)\,(mod\,7)$, ou seja, $W \equiv 435\,(mod\,7)$. Logo, $W = 1$. Portanto, o dia 8 de Janeiro de 1942 foi quinta-feira.

Verificando no calendário de 1942 (abaixo), observamos que 8 de Janeiro de 1942 é, realmente, quinta-feira.

CALENDÁRIO (JANEIRO DE 1942)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 15:30

Exemplo 3.41 *Vamos determinar que dia da semana será 21 de Outubro de 2015.*

Temos:

$A = 2015 - 1600 = 415$.

$$B = \left[\frac{415}{4}\right] - \left[\frac{415}{100}\right] + \left[\frac{415}{400}\right] = 103 - 4 + 1 = 100.$$

Como $y = 21$, temos que $C = 21 - 1 = 20$.

$D = 4$, pois o mês é outubro (ver Quadro II).

Então, $W \equiv (415 + 100 + 20 + 4)\,(mod\,7)$, ou seja, $W \equiv 539\,(mod\,7)$. Logo, $W = 0$. Portanto, o dia 21 de Outubro de 2015 será quarta-feira.

Verificando no calendário de 2015 (abaixo), observamos que 21 de Outubro de 2015 será, realmente, quarta-feira.

CALENDÁRIO (OUTUBRO DE 2015)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 16:00

Exemplo 3.42 *Vamos determinar que dia da semana será 28 de Fevereiro de 2100.*

Temos:

$A = 2099 - 1600 = 499$. ($N = 2099$, pois em fevereiro consideramos como o 12º mês de 2099).

$$B = \left[\frac{499}{4}\right] - \left[\frac{499}{100}\right] + \left[\frac{499}{400}\right] = 124 - 4 + 1 = 121.$$

Como $y = 28$, temos que $C = 28 - 1 = 27$.

$D = 1$, pois o mês é fevereiro (ver Quadro II).

Então, $W \equiv (499 + 121 + 27 + 1)\,(mod\,7)$, ou seja, $W \equiv 648\,(mod\,7)$. Logo, $W = 4$. Portanto, o dia 28 de Fevereiro de 2100 será domingo.

Verificando no calendário de 2100 (abaixo), observamos que 28 de Fevereiro de 2100 é, realmente, domingo.

CALENDÁRIO (FEVEREIRO DE 2100)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 16:30

Exemplo 3.43 *Vamos determinar que dia da semana será 11 de Fevereiro de 2400.*

Temos:

$A = 2399 - 1600 = 799$. ($N = 2399$, pois em fevereiro consideramos como o 12º mês de 2399).

$$B = \left[\frac{799}{4}\right] - \left[\frac{799}{100}\right] + \left[\frac{799}{400}\right] = 199 - 7 + 1 = 193.$$

Como $y = 11$, temos que $C = 11 - 1 = 10$.

$D = 1$, pois o mês é fevereiro (ver Quadro II).

Então, $W \equiv (799 + 193 + 10 + 1)\,(mod\,7)$, ou seja, $W \equiv 1003\,(mod\,7)$. Logo, $W = 2$. Portanto, o dia 11 de Fevereiro de 2400 será sexta-feira.

Verificando no calendário de 2400 (abaixo), observamos que 11 de Fevereiro de 2400 é, realmente, sexta-feira.

CALENDÁRIO (FEVEREIRO DE 2400)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
		1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29				

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 17:00

Exemplo 3.44 *Vamos determinar que dia da semana será 13 de Setembro de 2800.*

Temos:

$A = 2800 - 1600 = 1200.$

$$B = \left[\frac{1200}{4}\right] - \left[\frac{1200}{100}\right] + \left[\frac{1200}{400}\right] = 300 - 12 + 3 = 291.$$

Como $y = 13$, temos que $C = 13 - 1 = 12$.

$D = 2$, pois o mês é setembro (ver Quadro II).

Então, $W \equiv (1200 + 291 + 12 + 2)\,(mod\,7)$, ou seja, $W \equiv 1505\,(mod\,7)$. Logo, $W = 0$. Portanto, o dia 13 de Setembro de 2800 será quarta-feira.

Verificando no calendário de 2800 (abaixo), observamos que 13 de Setembro de 2800 é, realmente, quarta-feira.

CALENDÁRIO (SETEMBRO DE 2800)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
					1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 14/01/2015 às 17:30

Exemplo 3.45 *A mensagem abaixo está criptografada com chave $k = 20$ e contém uma data. Descubra o dia da semana desta data.*

IJLIZ GUNZI CLYWI GYHXU XIJYF UWUJY

MYGIC NIXYH IPYGV LIXYX ICMGC FYXYT

Como a mensagem foi criptografada com chave 20, vejamos como fica a correspondência das letras.

A letra "A"corresponde a 0; logo $P = 0$. Assim, $C \equiv 0 + 20\,(mod\,26)$, ou seja, $C \equiv 20\,(mod\,26)$. Desta forma 20 é o número equivalente a letra "A".

A letra "B"corresponde a 1; logo $P = 1$. Assim, $C \equiv 1 + 20\,(mod\,26)$, isto é, $C \equiv 21\,(mod\,26)$. Isto significa que o número equivalente a letra "B"é 21.

E assim, montamos o quadro abaixo:

Simples	A	B	C	D	E	F	G	H	I	J	K	L	M
Número Equivalente	0	1	2	3	4	5	6	7	8	9	10	11	12
Encripatado	U	V	W	X	Y	Z	A	B	C	D	E	F	G
Número Equivalente	20	21	22	23	24	25	0	1	2	3	4	5	6
Simples	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Número Equivalente	13	14	15	16	17	18	19	20	21	22	23	24	25
Encriptado	H	I	J	K	L	M	N	O	P	Q	R	S	T
Número Equivalente	7	8	9	10	11	12	13	14	15	16	17	18	19

Agora, vamos decifrar a mensagem cifrada.

Primeiro, trocamos as letras pelos seus números correspondentes. Assim, temos:

8 9 11 8 25 6 20 13 25 8 2 11 24 22 8 6 24 7 23 20

23 8 9 24 5 20 22 20 9 24 12 24 6 8 2 13 8 23 24 7

8 15 24 6 21 11 8 23 24 23 8 2 12 6 2 5 24 23 24 19

Em seguida, utilizamos a relação $P \equiv C - 20\,(mod\,26)$ para alterar o código recebido para o "texto simples", obtendo:

14 15 17 14 5 12 0 19 5 14 8 17 4 2 14 12 4 13 3 0

3 14 15 4 11 0 2 0 15 4 18 4 12 14 8 19 14 3 4 13

14 21 4 12 1 17 14 3 4 3 14 8 18 12 8 11 4 3 4 25

Aplicando a equivalência numérica correspondente a cada letra, temos:

OPROF MATFO IRECO MENDA

DOPEL ACAPE SEMOI TODEN

OVEMB RODED OISMI LEDEZ

Combinando as letras de forma apropriada em palavras, encontramos a mensagem original:

O PROFMAT FOI RECOMENDADO PELA CAPES EM OITO DE NOVEMBRO DE DOIS MIL E DEZ

Vamos determinar que dia da semana foi 8 de Novembro de 2010.

Temos:

$A = 2010 - 1600 = 410.$

$$B = \left[\frac{410}{4}\right] - \left[\frac{410}{100}\right] + \left[\frac{410}{400}\right] = 102 - 4 + 1 = 99.$$

Como $y = 8$, temos que $C = 8 - 1 = 7$.

Além disso, $D = 0$, pois o mês é novembro (ver Quadro II).

Então, $W \equiv (410 + 99 + 7 + 0)\,(mod\,7)$, ou seja, $W \equiv 516\,(mod\,7)$. Logo, $W = 5$. Portanto, o dia 8 de Novembro de 2010 foi segunda-feira.

Verificando no calendário de 2010 (abaixo), observamos que 8 de Novembro de 2010 é, realmente, segunda-feira.

CALENDÁRIO (NOVEMBRO DE 2010)

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Disponível em: http://ghiorzi.org/caleperp.htm. Acessado em 29/01/2015 às 10:00

Bibliografia

[1] Brasil. Secretaria de Educação Fundamental. *Parâmetros curriculares nacionais: Matemática*. Brasília: MEC/SEF, 1997.

[2] CASTELLÓ, T., VAZ, V., *Assinatura Digital*. Disponível em: < http://www.gta.ufrj.br/grad/07_1/ass-dig/Introduo.html > Acesso em 19 de janeiro de 2015.

[3] GHIORZI, T., *Calendários Perpétuos*. Disponível em: < http://ghiorzi.org/caleperp.htm > Acesso em 13 de janeiro de 2015.

[4] GHIORZI, T., *Dígitos de Verificação*. Disponível em: $< http://ghiorzi.org/DVnew.htm >$ Acesso em 24 de janeiro de 2015.

[5] HEFEZ, A., *Elementos de Aritmética*. Rio de Janeiro: SBM, 2. ed., 2011.

[6] JUNQUEIRA, L.C.S. , *Critérios de Divisibilidade*. Monografia de Licenciatura em Matemática, UFSC, 2001.

[7] MILIES, F. C. P., *Números: Uma Introdução à Matemática*. São Paulo: Editora da Universidade de São Paulo, 3. ed., 2001.

[8] PDAExpert, Saber Projetar - Saber Desenvolver. Disponível em: $< http://pdaexpert.net/artigos/palm-os/handheld-basic/hb-validacao-de-numero-de-cpf/ >$ Acesso em 24 de janeiro de 2015.

[9] ROSEN, K. H., *Elementary Number Theory and Its Applications*. São Paulo: Editora da Universidade de São Paulo, 3. ed., 2001.

[10] VIZZOTTO, J. K., *Trabalho de Algoritmos com Seleção: Lógica e Algoritmo.* Disponível em: $< http://www-usr.inf.ufsm.br/juvizzotto/elc1064-2011b/trabalho1.pdf >$ Acesso em 19 de janeiro de 2015.