UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

CENTRO DE EDUCAÇÃO E SAÚDE

UNIDADE ACADÊMICA DE FÍSICA E MATEMÁTICA

TRABALHO DE CONCLUSÃO DE CURSO

IRANIR PONTES SILVA

CONGRUÊNCIA MODULAR: CRITÉRIOS DE DIVISIBILIDADE E CONTRIBUIÇÕES NO RAMO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Cuité-PB

2017

IRANIR PONTES SILVA

CONGRUÊNCIA MODULAR: CRITÉRIOS DE DIVISIBILIDADE E CONTRIBUIÇÕES NO RAMO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso Graduação em Licenciatura em Matemática do Centro de Educação e Saúde da Universidade Federal de Campina Grande em cumprimento às exigências do Componente Curricular Trabalho Acadêmico Orientado, para obtenção do grau de Graduada em Licenciatura em Matemática.

Orientadora: Maria de Jesus Rodrigues da Silva
Coorientadora: Jaqueline Aparecida F. Lixandrão Santos

Cuité-PB
2017

FICHA CATALOGRÁFICA ELABORADA NA FONTE
Responsabilidade Jesiel Ferreira Gomes ¯ CRB 15 ¯ 256

S586c Silva, Iranir Pontes.

Congruência modular: critérios de divisibilidade e contribuições no ramo da segurança da informação e comunicação. / Iranir Pontes Silva. ¯ Cuité: CES, 2017.

74 fl.

Monografia (Curso de Licenciatura em Matemática) ¯ Centro de Educação e Saúde / UFCG, 2017.

Orientadora: Maria de Jesus Rodrigues da Silva.
Coorientadora: Jaqueline Aparecida Foratto Lixandrão Santos.

1. Congruência. 2. Critérios de divisibilidade. 3. Criptografia. I. Título.

Biblioteca do CES - UFCG CDU 514

IRANIR PONTES SILVA

CONGRUÊNCIA MODULAR: Critérios de divisibilidade e contribuições no ramo da segurança da informação e comunicação

Trabalho de Conclusão de Curso submetido a banca examinadora como parte dos requisitos necessários à obtenção do grau de Graduação em Licenciatura em Matemática.

Aprovada em: 14 de março de 2017.

BANCA EXAMINADORA

Profª. Ms. Maria de Jesus Rodrigues da Silva

(Orientadora)

Profª. Dra. Jaqueline Aparecida F. Lixandrão Santos

(Coorientadora)

Profº. Ms. Renato Oliveira Silva

(Examinador)

Aos meus pais,

Ildebrando Dutra Silva e

Marinêz Clelia de P. Silva e ao meu esposo,

Carlos Silva Alves.

Agradecimentos

Agradeço primeiramente a Deus, por ter me dado forças, para que diante de cada obstáculo me tornasse ainda mais persistente na realização de meus objetivos.

Aos meus pais, Ildebrando Dutra e Marinêz Clelia pela educação que me deram, por todo esforço prestado para que nada me faltasse e por serem minha inspiração, pois foi pensando no melhor para eles que nunca pensei em desistir.

Ao meu esposo Carlos, pelo carinho, atenção e por toda ajuda que me deu durante todo o decorrer do curso, não permitindo que me abalasse com as diculdades enfrentadas.

As minhas irmãs Iraneide e Iramara, que sempre me apoiaram, incentivaram, e elogiaram pela força de vontade e determinação.

A todos os meus amigos e, em particular, a Ioneris Oliveira e Renato Oliveira pela orientação de uso do LATEX, à Dayane Ribeiro, Jayane Nunes, Marinalva Oliveira e Jucimere Lima pelas contribuições prestadas durante o curso.

A minha orientadora Prof[a]. Maria de Jesus pela ótima orientação, paciência, amizade e principalmente pela confiança. Tê-la como orientadora foi um privilégio.

A Prof[a]. Jaqueline Lixandrão, pela qual tenho enorme admiração, por ter aceito o convite para ser minha coorientadora e por toda atenção prestada.

Ao professor Renato Oliveira, pelas sugestões e por ter aceito o convite de participar da banca examinadora deste trabalho.

Ao professor supervisor dos Estágios Supervisionados I, II, e III Fernando Múcio, pelas oportunidades oferecidas, sugestões e por toda confiança em minha pessoa.

A todos os professores que contribuiram para minha formação e, em especial, aos professores, Luciano Barros, Célia Maria, Aluísio Freire, Jadilson Almeida, Aluska Dias, Maria Ioneris, Nayara Costa, Kiara Tatiane, Izayana Feitosa, Vladimir Catão, Marciel Medeiros, Clebson Huan, Glageane Souza, Edna Cordeiro e Jussiê Ubaldo.

Enfim, a todos aqueles que sempre me apoiaram ao longo de todo percurso e contribuiram para minha formação.

”Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas Graças a Deus, não sou o que era antes.”

Marthin Luther King

RESUMO

O presente trabalho se caracteriza como uma pesquisa bibliográfica de caráter exploratório sobre a Teoria dos Números, especialmente no que tange a congruência modular e suas aplicações. Dentre elas, abordaremos alguns critérios de divisibilidade, conteúdo visto com alunos do 6^{o} ano do Ensino Fundamental II; a criptografia baseada na Cifra de César e a criptografia RSA que é um dos sistemas criptográficos atualmente utilizados em transações comerciais por ser um método considerado seguro; como aplicar a congruência na geração dos dígitos de verificação de CPF, cartão de crédito e em cálculo envolvendo calendários para obtenção do dia da semana de qualquer data a partir de 1600. O texto, no qual apresentamos nossa pesquisa, se inicia com alguns conceitos básicos indispensáveis ao desenvolvimento do trabalho e em seguida, são apresentadas as aplicações supracitadas, acompanhadas de um breve contexto histórico e sua relação com congruências. A presente pesquisa nos possibilitou observar que há diversos estudos voltados para Teoria dos Números, com foco especial em congruência modular. Contudo, não é muito comum estudos sobre suas aplicações, que são inúmeras.

Palavras-chave: Congruência. Critérios de Divisibilidade. Criptografia. Dígito de Verificação. Calendário.

ABSTRACT

The present work is characterized as an exploratory bibliographical research on the Theory of Numbers, especially with regard to modular congruence and its applications. Among them, we will approach some criteria of divisibility, content seen with students of the 6th grade of Elementary School II; encryption based on the Cipher of Caesar and the RSA encryption which is one of the cryptographic systems currently used in business transactions as a method considered secure; how to apply congruence in the generation of the CPF verification digits, credit card and in calculations involving calendars for obtaining the day of the week of any date from 1600. The text in which we present our research begins with some basic concepts indispensable to the development of the work and then the above mentioned applications are presented, accompanied by a brief historical context and its relation with congruences. The present research allowed us to observe that there are several studies focused on Number Theory, with special focus on modular congruence. However, it is not very common to study its applications, which are numerous.

Keywords: Congruence. Divisibility Criteria. Encryption. Verification Digit. Calendar.

SUMÁRIO

INTRODUÇÃO

De acordo com Vieira (2015), a Teoria dos Números é o ramo da Matemática que estuda os números inteiros e suas particularidades. Esta abrange vários ramos, sendo que três deles têm destaque especial: a Teoria Algébrica voltada ao estudo dos números complexos e no uso da álgebra abstrata na resolução de problemas específicos; a Teoria Analítica dedicada ao estudo mais profundo dos números primos com o emprego de resultados da Análise Real e complexa, e a Teoria Elementar que consiste em técnicas relevantes da Aritmética para a validação e comprovação das propriedades fundamentais dos números inteiros.

Neste trabalho daremos ênfase a Teoria Elementar, em especial ao que compete à congruência modular com o objetivo de apresentar alguns pontos essenciais e trazer noções de sua aplicabilidade em situações cotidianas. Existem inúmeros estudos a respeito desse tema, sobretudo nos livros de Teoria dos Números. Porém, na maioria das literaturas não é frequente a abordagem de muitas de suas aplicações, como por exemplo, nas demonstrações de alguns dos critérios de divisibilidade, na geração dos dígitos de verificação de CPF e cartão de crédito, em cálculos com calendários, bem como em aplicações envolvendo criptografia. Tais aplicações serão apresentadas em nossa pesquisa que está organizada em três capítulos os quais descrevemos na sequência.

O primeiro capítulo é destinado a alguns conceitos e resultados referentes aos números inteiros, mais especificamente ao estudo de divisibilidade, algoritmo da divisão, representação decimal dos números inteiros, máximo divisor comum, números primos e equações diofantinas lineares, sendo estes indispensáveis à compreensão dos próximos capítulos.

No segundo, abordaremos alguns conceitos, teoremas, proposições, demonstrações e exemplos de congruências, conceito base para a construção e exposição das aplicações apresentadas no capítulo seguinte.

Por último, no terceiro capítulo, focamos nosso estudo em quatro aplicações de congruência modular. A primeira dessas aplicações trata dos critérios de divisibilidade mais co-

muns ensinados no 6^{o} ano do Ensino Fundamental II. Na segunda aplicação apresentamos o uso de congruências na criptografia baseada na Cifra de César, método constituído pelo imperador Júlio César com o objetivo de manter secretas correspondências militares e na criptografia RSA, método criptográfico de chave pública frequentemente usado em transações comerciais. Na terceira, mostramos como se dá a geração dos números de verificação do CPF e de cartão de crédito, especificamente da bandeira VISA e MASTERCARD. E por fim, enfatizamos cálculos com calendários para obtenção do dia da semana de qualquer data após o ano 1600, fazendo um breve histórico sobre a evolução de calendários, particularmente o gregoriano que é o mais utilizado no mundo inteiro.

Ao concluir este trabalho, pudemos perceber que há diversos estudos voltados para Teoria dos Números, com foco especial em congruência modular. Contudo, não é muito comum estudos sobre suas aplicações, que são inúmeras.

Capítulo 1

CONCEITOS FUNDAMENTAIS

Apresentamos neste capítulo noções básicas de Teoria dos Números que serão necessárias para o desenvolvimento e compreensão deste trabalho. Denotaremos por $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ o conjunto dos números naturais e por $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ o conjunto dos números inteiros.

1.1 Indução

O Princípio de Indução Matemática é uma ferramenta bastante útil em demonstrações de diversos teoremas. Enunciaremos a seguir as duas formas desse princípio.

1.1.1 Primeira Forma do Princípio de Indução Matemática

Seja $a \in \mathbb{N}$ e $p(n)$ uma sentença aberta em n. Suponha que
(i) $p(a)$ é verdade, e que
(ii) $\forall n \geq a,\ p(n) \Longrightarrow p(n+1)$ é verdade,
então, $p(n)$ é verdade para todo $n \geq a$.

1.1.2 Segunda Forma do Princípio de Indução Matemática

Seja $p(n)$ uma sentença aberta tal que
(i) $p(a)$ é verdade, e que
(ii) $\forall n,\ p(a)$ e $p(a+1)$ e $\ldots$ e $p(n) \Longrightarrow p(n+1)$ é verdade,
então, $p(n)$ é verdade para todo $n \geq a$.

A demonstração de ambos os princípios de indução encontra-se na referência [13].

1.2 Divisibilidade

Definição 1.1. *Sejam a, $b \in \mathbb{Z}$, com $a \neq 0$. Dizemos que a divide b, e denotamos por $a|b$, quando existir $c \in \mathbb{Z}$, tal que $b = ac$. O elemento c, tal que $b = ac$ é chamado o quociente de b por a, também denotado por $\frac{b}{a}$.*

Observação 1.1. *Como a divide b, podemos dizer que a é um divisor de b, ou ainda que b é um múltiplo de a. Se a não divide b, denotamos por $a \nmid b$.*

Exemplo 1.1. *Para ilustrar o conceito de divisibilidade seguem os exemplos:* $2|216$*, pois* $216 = 2 \cdot 108$ *;* $5|525$*, pois* $525 = 5 \cdot 105$ *e* $-6|846$*, pois* $846 = -6 \cdot (-141)$.

Teorema 1.1. *A divisão em $\mathbb{Z}$ satisfaz as seguintes propriedades:*

(i) *$a|a$;*

(ii) *Sejam $a, b \in \mathbb{Z}$. Se $a|b$ e $b|a$, então $b = \pm a$;*

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

(iv) *Se $a|b$ e $a|c$, então $a|(bx+cy)$ com $x, y \in \mathbb{Z}$;*

(v) *Se $a|b$ e $c|d$, então $ac|bd$;*

(vi) *Se $a = b + c$ e $d|c$, então $d|a \Leftrightarrow d|b$;*

(vii) *Se $a|b$, então $ac|bc$.*

Demonstração: (i) De fato, podemos escrever $a = a \cdot 1$. Logo, $a|a$.

(ii) Por hipótese, $a|b$ e $b|a$, assim existem $w, k \in \mathbb{Z}$, tais que

$$b = aw. \tag{1.1}$$

$$a = bk. \tag{1.2}$$

Substituindo (1.2) em (1.1), temos que $b = (bk)w \Rightarrow b = b(kw) \Rightarrow b = b(wk)$. Logo, $wk = 1$, pois, caso contrário, se fosse $wk \neq 1$ teríamos $b(wk) \neq b \cdot 1 = b$, já que $b \neq 0$, o que seria uma contradição. Portanto, $w = k = 1$ ou $w = k = -1$ e daí, $b = \pm a$.

(iii) Vamos supor que $a|b$ e $b|c$, assim existem $w, k \in \mathbb{Z}$, tais que

$$b = aw. \tag{1.3}$$

$$c = bk. \tag{1.4}$$

Substituindo (1.3) em (1.4), obtemos $c = (aw)k \Rightarrow c = a(wk)$. Como $w,k \in \mathbb{Z}$ segue que $wk \in \mathbb{Z}$. Logo, $a|c$.

(iv) Suponhamos que $a|b$ e $a|c$, assim existem $w,k \in \mathbb{Z}$, tais que

$$b = aw. \tag{1.5}$$
$$c = ak. \tag{1.6}$$

Multiplicando as equações (1.5) por x e (1.6) por y, obtemos $bx = (aw)x \quad e \quad cy = (ak)y$. Somando as duas igualdades anteriores, temos

$$bx + cy = (aw)x + (ak)y = a(wx + ky).$$

Como w,k,x e $y \in \mathbb{Z}$ segue que $wx + ky \in \mathbb{Z}$. Logo, $a|(bx + cy)$.

(v) Como $a|b$ e $c|d$, temos que existem $w,k \in \mathbb{Z}$, tais que

$$b = aw. \tag{1.7}$$
$$d = ck. \tag{1.8}$$

Multiplicando (1.7) por (1.8), obtemos

$$bd = (aw)(ck) \Longrightarrow bd = a(wc)k \Longrightarrow bd = a(cw)k \Longrightarrow bd = (ac)(wk).$$

Como $w,k \in \mathbb{Z}$ segue que $wk \in \mathbb{Z}$ e portanto, $ac|bd$.

(vi) $(\Longrightarrow)$ Por hipótese $a = b + c$, $d|c$ e $d|a$. Mostraremos que $d|b$. Como $d|c$ e $d|a$, então existem $w,k \in \mathbb{Z}$, tais que

$$c = dw. \tag{1.9}$$
$$a = dk. \tag{1.10}$$

Substituindo (1.9) e (1.10) em $a = b + c$, temos $dk = b + (dw) \Rightarrow b = d(k - w)$, com $(k - w) \in \mathbb{Z}$. Logo, $d|b$.

$(\Longleftarrow)$ Consideremos agora que $a = b + c$, $d|c$ e $d|b$. Mostraremos que $d|a$. Como $d|c$ e $d|b$, existem $w,k \in \mathbb{Z}$, tais que $c = dw$ e $b = dk$. Mas, $a = b + c$ e daí,

$$a = (dk) + (dw) \Longrightarrow a = d(k + w),$$

com $k + w \in \mathbb{Z}$. Portanto, $d|a$.

(vii) Vamos supor que $a|b$, assim existe $w \in \mathbb{Z}$ tal que $b = aw$. Multiplicando essa equação por $c \in \mathbb{Z}$, segue que

$$bc = (aw)c \Longrightarrow bc = a(wc) \Longrightarrow bc = a(cw) \Longrightarrow bc = (ac)w.$$

Logo, $ac|bc$. □

1.3 Algoritmo da divisão

Vamos agora introduzir um resultado que nos permite efetuar a divisão entre dois números inteiros a e b ($b > 0$) obtendo-se um resto.

Teorema 1.2. ***(Algoritmo da Divisão)*** *Sejam a e b inteiros, com $b > 0$. Então existem e são únicos os inteiros q e r que satisfazem a condição:*

$$a = bq + r, \quad com \quad 0 \leq r < b.$$

Demonstração (Existência): Seja $b > 0$. Para o inteiro a existem duas possibilidades:
(i) a é um múltiplo de b e nesse caso, $a = bq + 0$ $(r = 0)$ para algum inteiro q.
(ii) a está entre dois múltiplos consecutivos de b, isto é,

$$qb < a < (q+1)b.$$

Adicionando $(-qb)$ aos membros da desigualdade anterior, temos:

$$qb + (-qb) < a + (-qb) < qb + b + (-qb) \Longrightarrow 0 \leq a - qb < b.$$

Fazendo $r = a - qb$ temos $a = bq + r$, com $0 \leq r < b$. Agora, se $r = 0$ então $a = bq$. Logo,

$$a = bq + r, \quad com \quad 0 \leq r < b.$$

(Unicidade): Por outro lado, suponhamos que existam r, r_1, q, q_1 tais que

$$a = bq + r \quad e \quad a = bq_1 + r_1, \quad com \quad 0 \leq r, r_1 < b.$$

Assim,

$$a = bq + r = bq_1 + r_1 \Longrightarrow r - r_1 = bq_1 - bq \Longrightarrow r - r_1 = b(q_1 - q). \tag{1.11}$$

Se $r \neq r_1$, digamos $r > r_1$, então $r - r_1 > 0$. Como por hipótese $b > 0$, segue da última equação obtida em (1.11) que $q_1 - q > 0$ o que implica em $q_1 - q \geq 1$. Daí,

$$r = b(q_1 - q) + r_1 \geq b,$$

o que é um absurdo. Portanto, $r = r_1$, e de (1.11) segue que $q = q_1$, o que mostra a unicidade de q e r. □

Exemplo 1.2. *Seja m um inteiro cujo resto da divisão por 6 é 5. Mostre que o resto da divisão de m por 3 é 2.*

Temos $m = 6q+5$ e $m = 3q+r$, com $0 \leq r < 3$, isto é, $r = 0, 1$, ou 2. Mostraremos que $r = 2$. Se $r = 0$, então $6q+5 = 3q+0$ o que nos dá $3(q-2q) = 5$, ou seja, $3 \mid 5$ o que é um absurdo, assim $r \neq 0$. Se $r = 1$, então $6q+5 = 3q+1$ o que implica que $3(q-2q) = 4$, isto é, $3 \mid 4$, o que também é um absurdo. Logo, $r \neq 1$, e consequentemente $r = 2$.

1.4 Máximo divisor comum

Sejam a e b inteiros, não simultaneamente nulos, dizemos que $d \in \mathbb{Z}$ é um divisor comum de a e b se $d|a$ e $d|b$.

Definição 1.2. *Sejam a, b e $d \in \mathbb{Z}$, dizemos que d é o máximo divisor comum (mdc) de a e b se, as seguintes condições forem satisfeitas:*
(i) $d \geq 0$;
(ii) $d|a$ *e* $d|b$;
(iii) *Se existe* $d' \in \mathbb{Z}$, *com* $d'|a$ *e* $d'|b$, *então* $d'|d$, *isto é, todo divisor comum de a e b é divisor de d.*

Exemplo 1.3. *Podemos comprovar que, no caso em que* $a = 16$ *e* $b = 24$, *o número* 8 *é o máximo divisor comum entre eles.*
De fato,
(i) $8 > 0$;
(ii) $8|16$ *e* $8|24$;
(iii) *Se* $d'|16$ *e* $d'|24$, *então* $d' = 1, 2, 4$ *ou* 8 *e portanto* $d'|8$.
Logo, o $mdc(16, 24) = 8$.

Veremos a seguir algumas proposições que decorrem da definição de máximo divisor comum.

Proposição 1.1. *O máximo divisor comum de a e b é único.*

Demonstração: Sejam d e d_1 de modo que $d = mdc(a,b)$ e $d_1 = mdc(a,b)$. Pelo item (iii) da Definição 1.2 segue que $d|d_1$ e $d_1|d$, com $d \geq 0$ e $d_1 \geq 0$. Logo $d = d_1$. □

Proposição 1.2. *Se* $a = bq + r$, *então* $d = mdc(a,b)$ *se, e somente se,* $d = mdc(b,r)$.

Demonstração: $(\Longrightarrow)$ Seja $d = mdc(a,b)$ com $a = bq + r$, mostraremos que $d = mdc(b,r)$. Segue da definição de MDC que:

(i) $d \geq 0$, pois $d = mdc(a,b)$;

(ii) Como $d|a$ e $d|b$, então $d|(a-bq)$, isto é, $d|r$. Daí, $d|b$ e $d|r$;

(iii) Se $d^{'}|b$ e $d^{'}|r$, então $d^{'}|(bq+r)$, isto é, $d^{'}|a$. Assim, $d^{'}|a$ e $d^{'}|b$, mas como $d = mdc(a,b)$ segue que $d^{'}|d$. Logo, $d = mdc(b,r)$.

$(\Longleftarrow)$ Suponhamos que $d = mdc(b,r)$ com $a = bq+r$. Mostraremos que $d = mdc(a,b)$.

(i) $d \geq 0$, pois $d = mdc(b,r)$;

(ii) Como $d|b$ e $d|r$, então $d|(bq+r)$, isto é, $d|a$. Daí, $d|a$ e $d|b$;

(iii) Se $d^{'}|a$ e $d^{'}|b$, então $d^{'}|(a-bq)$, isto é, $d^{'}|r$. Assim $d^{'}|b$ e $d^{'}|r$, mas como $d = mdc(b,r)$ vem que $d^{'}|d$. Portanto, $d = mdc(a,b)$. □

Proposição 1.3. *Se $a|b$, então $mdc(a,b) = |a|$.*

Demonstração: Por definição, temos:

(i) $|a| \geq 0$;

(ii) $(|a|)|a$, pois $a = |a| \cdot (\pm 1)$. Como $(|a|)|a$ e $a|b$, por transitividade $(|a|)|b$.

(iii) Se $d^{'}|a$ e $d^{'}|b$, então $a = d^{'} \cdot x$, $x \in \mathbb{Z}$.

Daí,

$$a = d^{'} \cdot x \Longrightarrow (\pm 1)a = (\pm 1)(d^{'} \cdot x) \Longrightarrow \pm a = d^{'}(\pm x) \Longrightarrow |a| = d^{'}(\pm x).$$

Logo, $d^{'}|(|a|)$. □

Proposição 1.4. *Se $d = mdc(a,b)$, então existem inteiros x_0 e y_0 tais que $d = ax_0 + by_0$.*

Demonstração: Se $a = b = 0$, então $d = 0$ e qualquer par (x_0, y_0) satisfaz $0 = 0x_0 + 0y_0$. Seja $a \neq 0$ ou $b \neq 0$ (ou ambos) e consideremos o conjunto $S = \{ax + by; x, y \in \mathbb{Z}\}$. Como $a \cdot a + b \cdot b = a^2 + b^2 \in S$ e $a^2 + b^2 > 0$, então em S há elementos estritamente positivos. Se d é o menor desses inteiros, mostraremos que $d = mdc(a,b)$. De fato:

(i) $d \geq 0$;

(ii) Como $d \in S$, então existem $x_0, y_0 \in \mathbb{Z}$, tais que $d = ax_0 + by_0$. Aplicando o Algoritmo da Divisão aos elementos a e d, temos

$$a = dq + r, \tag{1.12}$$

com $0 \leq r < d$. Substituindo $d = ax_0 + by_0$ em (1.12), obtemos:

$$\begin{aligned} a = (ax_0 + by_0)q + r &\Longrightarrow r = a - ax_0q - by_0q \\ &\Longrightarrow r = a(1 - qx_0) + b(-qy_0) \\ &\Longrightarrow r = a(1 - qx_0) + b[q(-y_0)], \end{aligned}$$

o que mostra que r é um elemento de S. Mas, como r não pode ser estritamente positivo, pois é menor que d (igual o mínimo de S), então $r = 0$ e, portanto $a = dq$, isto é, $d|a$. Analogamente, aplicando o Algoritmo da Divisão aos elementos b e d teremos:

$$b = dq_1 + r_1, \tag{1.13}$$

com $0 \leq r_1 < d$. Substituindo $d = ax_0 + by_0$ em (1.13), obtemos

$$\begin{aligned} b = (ax_0 + by_0)q_1 + r_1 &\implies r_1 = b - ax_0q_1 - by_0q_1 \\ &\implies r_1 = b(1 - q_1y_0) + a(-q_1x_0) \\ &\implies r_1 = b(1 - q_1y_0) + a[q_1(-x_0)], \end{aligned}$$

o que mostra que r_1 é também um elemento de S. E consequentemente, $r_1 = 0$, o que implica em $b = dq_1$, ou seja, $d|b$.

(iii) Se existe $d|a$ e $d|b$, então $d^{'}|ax_0 + by_0$, ou seja, $d^{'}|d$.

Portanto, mostramos que $d = mdc(a,b) = ax + by$, $x, y \in \mathbb{Z}$. Essa identidade que acabamos de mostrar recebe o nome de *Identidade de Bezout*. □

Teorema 1.3. ***(Algoritmo de Euclides)*** *Sejam $r_0 = a$ e $r_1 = b$ inteiros positivos. Se o algoritmo da divisão for aplicado sucessivas vezes para se obter*

$$r_j = q_j r_{j+1} + r_{j+2},$$

com $0 \leq r_{j+2} < r_{j+1}$, $j = 0, 1, 2, \ldots, n-1$ e $r_{n+1} = 0$ então $mdc(a,b) = r_n$, sendo r_n o último resto não-nulo.

Demonstração: Inicialmente devemos aplicar o Teorema 1.2 para dividir $r_0 = a$ por $r_1 = b$ obtendo $r_0 = q_1r_1 + r_2$; em seguida dividimos r_1 por r_2, obtendo $r_1 = q_2r_2 + r_3$ e assim por diante, até obtermos o resto $r_{n+1} = 0$. Assim, a cada passo obtemos um resto sempre menor do que o anterior, e como estamos lidando apenas com números inteiros positivos, é óbvio que após uma quantidade finita de aplicações do Teorema 1.2, obteremos resto nulo. Temos assim, a seguinte sequência de equações:

$$\begin{aligned} r_0 &= q_1r_1 + r_2, \quad 0 < r_2 < r_1 \\ r_1 &= q_2r_2 + r_3, \quad 0 < r_3 < r_2 \\ r_2 &= q_3r_3 + r_4, \quad 0 < r_4 < r_3 \\ &\vdots \end{aligned}$$

$$\begin{aligned} r_{n-2} &= q_{n-1}r_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= q_n r_n + 0. \end{aligned}$$

A última equação nos diz que $r_n | r_{n-1}$ e pela Proposição 1.2, $mdc(r_n, r_{n-1}) = r_n$. Já a penúltima, ainda com auxílio da Proposição 1.2 diz que $r_n = mdc(r_{n-1}, r_{n-2})$, prosseguindo deste modo teremos por aplicações repetidas da Proposição 1.2 a sequência:

$$r_n = mdc(r_{n-1}, r_n) = mdc(r_{n-2}, r_{n-1}) = \ldots = mdc(r_1, r2) = mdc(r_0, r_1) = mdc(a, b).$$

Logo, o máximo divisor comum de a e b é o último resto não-nulo da sequência de divisões descritas anteriormente. □

1.5 Representação decimal dos números inteiros

Podemos representar os números inteiros pelo sistema decimal posicional, no qual todo numero inteiro é representado por uma sequência constituída pelos respectivos algarismos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9. Como são dez algarismos, tal sistema é denominado decimal. Ele também é chamado posicional pelo fato de cada algarismo possuir além do seu valor, um peso que lhe é dado em função da posição que o mesmo ocupa no número, tal peso é geralmente uma potência de dez.

Exemplo 1.4. *O número* 20819*, na base* 10*, é representado por:*

$$2 \cdot 10^4 + 0 \cdot 10^3 + 8 \cdot 10^2 + 1 \cdot 10 + 9$$

no qual temos, 9 unidades, 1 dezena, 8 centenas e 2 dezenas de milhar.

Neste sentido, o sistema decimal posicional é baseado em um resultado decorrente da divisão euclidiana que será demonstrado a seguir, já que será bastante útil no desenvolvimento dos critérios de divisibilidade.

Teorema 1.4. *Seja b um inteiro positivo maior do que* 1*. Então todo inteiro positivo n pode ser representado de forma única como:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0 \tag{1.14}$$

onde $k \geq 0$*, com* $0 \leq a_i < b, i = 0, 1, 2, \ldots, k$ *e* $a_k \neq 0$*.*

Demonstração: Inicialmente, aplicaremos o algoritmo da divisão aos inteiros n e b. Assim,

$$n = bq_0 + a_0, \quad 0 \leq a_0 < b.$$

Aplicando novamente o algoritmo da divisão, agora para os inteiros q_0 e b, temos:

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b.$$

Procedendo desta forma, obtemos a seguinte sequência:

$$\begin{aligned}
n &= bq_0 + a_0 \\
q_0 &= bq_1 + a_1 \\
q_1 &= bq_2 + a_2 \\
q_2 &= bq_3 + a_3 \\
&\vdots \\
q_{k-2} &= bq_{k-1} + a_{k-1} \\
q_{k-1} &= b \cdot 0 + a_k
\end{aligned}$$

com $0 \leq a_j < b, j = 0, 1, 2, ..., k$. Vamos agora substituir o valor de q_0 na primeira destas equações e, em seguida o valor de q_1 dado na terceira expressão, e assim por diante, obtendo:

$$\begin{aligned}
n &= bq_0 + a_0 \\
&= b(bq_1 + a_1) + a_0 \\
&= b^2 q_1 + ba_1 + a_0 \\
&= b^2(bq_2 + a_2) + ba_1 + a_0 \\
&= b^3 q_2 + a_2 b^2 + a_1 b + a_0 \\
&= b^3(bq_3 + a_3) + a_2 b^2 + a_1 b + a_0 \\
&= b^4 q_3 + a_3 b^3 + a_2 b^2 + a_1 b + a_0 \\
&\vdots \\
&= b^k q_{k-1} + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0 \\
&= a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0.
\end{aligned}$$

(Unicidade): Denotaremos por $d_b(n)$ o número de representações de n na base b e mostraremos que $d_b(n)$ é sempre igual a 1. Como alguns dos coeficientes a_j podem ser nulos vamos supor, excluindo tais termos, que n pode ser representado da seguinte forma

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_s b^s,$$

sendo a_k e a_s não nulos. Logo

$$\begin{aligned} n-1 &= a_k b^k + a_{k-1} b^{k-1} + \ldots + a_s b^s - 1 \\ n-1 &= a_k b^k + a_{k-1} b^{k-1} + \ldots + (a_s - 1) b^s + b^s - 1 \\ n-1 &= a_k b^k + a_{k-1} b^{k-1} + \ldots + (a_s - 1) b^s + (b-1) \sum_{j=0}^{s-1} b^j, \end{aligned}$$

uma vez que $b^s - 1 = (b-1) \sum_{j=0}^{s-1} b^j$. Isto significa que para cada representação de n na base b é possível encontrarmos uma representação, na mesma base, para $n-1$. Logo $d_b(n) \leq d_b(n-1)$. Esta desigualdade nos diz que para $m \geq n$, temos

$$d_b(m) \leq d_b(m-1) \leq d_b(m-2) \leq \ldots \leq d_b(n+1) \leq d_b(n).$$

Assim, como $n \geq 1$ e $d_b(n) \geq 1$, obtemos $1 \leq d_b(n) \leq d_b(1) = 1$. O que nos garante que $d_b(n) = 1$. □

1.6 Números primos

Dizemos que um inteiro $n \neq 0, \pm 1$ é primo quando possui pelo menos quatro divisores:± 1 e $\pm n$, que são chamados de divisores triviais. Por exemplo, o número 7 é primo, pois seus únicos divisores são ± 1 e ± 7.

Definição 1.3. *Seja $p \in \mathbb{Z}$. Dizemos que p é um inteiro primo, se obedece as seguintes condições:*
(i) $p \neq 0$;
(ii) $p \neq \pm 1$;
(iii) *os únicos divisores de p são ± 1 e $\pm p$ (divisores triviais).*

Observação 1.2. *Se um número inteiro a ($a \neq 0$ e $a \neq \pm 1$) possui outros divisores além dos triviais ele é chamado composto.*

Exemplo 1.5. *O número inteiro 3 é primo.*

De fato, pois $3 \neq 0$ e $3 \neq \pm 1$. E os únicos divisores de 3 são ± 1 e ± 3, isto é, $-1|3$, $1|3$, $-3|3$ e $3|3$.

Exemplo 1.6. *O número 6 é composto.*

De fato, $6 \neq 0$ e $6 \neq \pm 1$ e, além dos divisores ± 1 e ± 6 possui os divisores ± 2 e ± 3.

Definição 1.4. *Dizemos que a e b são primos entre si, se* $mdc(a,b) = 1$, *com* $a,b \in \mathbb{Z}$, *não simultaneamente nulos.*

Exemplo 1.7. *Os números* 41 *e* 12 *são primos entre si, pois* $mdc(41,12) = 1$.

Exemplo 1.8. *Mostre que dois números inteiros consecutivos são primos entre si.*

De fato, sejam r_1 e r_0 dois inteiros consecutivos. Pelo algoritmo de Euclides, temos:

$$\begin{aligned} r_0 &= r_1 \cdot 1 + r_2 \\ r_1 &= r_2 \cdot n + r_3. \end{aligned}$$

Logo, $mdc(r_1, r_0) = 1$. Portanto, r_1 e r_0 são primos entre si.

Teorema 1.5. *Sejam* $a,b \in \mathbb{Z}$, *não nulos. Dizemos que a e b são primos entre si se, e somente se, existem* $x,y \in \mathbb{Z}$ *tais que,* $ax + by = 1$.

Demostração: ($\Longrightarrow$) Suponhamos que a e b são primos entre si, assim $mdc(a,b) = 1$, ou seja, existem $x,y \in \mathbb{Z}$ tais que $ax + by = 1$.
($\Longleftarrow$) Vamos supor agora que existem $x,y \in \mathbb{Z}$ tais que, $ax + by = 1$. Assim, qualquer divisor de a e b é também divisor de 1, pois se $d|a$ e $d|b$, então pelo Teorema 1.1 item (*iv*) segue que $d|ax + by$ isto é, $d|1$.
Logo, os únicos divisores comuns à a e b são ± 1 e, portanto $mdc(a,b) = 1$. □

Corolário 1.1. *Se a e b são inteiros não simultaneamente nulos e* $d = mdc(a,b)$, *então*

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

Demostração: Como $d = mdc(a,b)$, pela Proposição 1.4 existem $x,y \in \mathbb{Z}$ tais que $d = ax + by$. Dividindo ambos os membros da igualdade anterior por $d > 0$, temos:

$$1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y.$$

Logo, pelo Teorema 1.5, $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, e portanto $mdc\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. □

Corolário 1.2. *Se* $a|bc$ *e* $mdc(a,b) = 1$, *então* $a|c$.

Demonstração: Supondo que $mdc(a,b) = 1$, existem $x,y \in \mathbb{Z}$ tais que:

$$ax + by = 1. \tag{1.15}$$

Multiplicando (1.15) por c, obtemos:

$$acx + bcy = c. \tag{1.16}$$

Mas $a|bc$, isto implica que $bc = ak$, com $k \in \mathbb{Z}$. Substituindo bc em (1.16), temos:

$$acx + aky = c \Longrightarrow a(cx + ky) = c.$$

Logo, $a|c$. □

Corolário 1.3. *Se a e b são inteiros primos entre si, então $a|c$ e $b|c$ com $c \neq 0$, se, e somente se, $ab|c$.*

Demonstração: ($\Longrightarrow$) Como a e b são primos entre si, existem $x, y \in \mathbb{Z}$ tais que:

$$ax + by = 1.$$

Multiplicando a igualdade anterior por c, obtemos:

$$acx + bcy = c. \tag{1.17}$$

Por hipótese $a|c$ e $b|c$, assim existem $k_1, k_2 \in \mathbb{Z}$ de forma que

$$c = ak_1 \quad e \quad c = bk_2.$$

Substituindo ambos os valores de c em (1.17), temos:

$$a(bk_2)x + b(ak_1)y = c \Rightarrow ab(k_2x + k_1y) = c.$$

Portanto, $ab|c$.

($\Longleftarrow$) Suponhamos agora que $ab|c$, assim existe $k \in \mathbb{Z}$ tal que $c = abk$. Como por hipótese, a e b são primos entre si, segue que $mdc(a,b) = 1$. Desta forma, existem $x_1, y_1 \in \mathbb{Z}$ de modo que

$$ax_1 + by_1 = 1. \tag{1.18}$$

Multiplicando (1.18) por c, obtemos:

$$acx_1 + bcy_1 = c. \tag{1.19}$$

Substituindo $c = abk$ na primeira parcela da equação (1.19), temos:

$$a(abk)x_1 + bcy_1 = c \Longrightarrow b(a^2kx_1 + cy_1) = c.$$

o que implica que $b|c$. Agora, substituindo $c = abk$ na segunda parcela de (1.19), vem

$$acx_1 + b(abk)y_1 = c \Longrightarrow a(cx_1 + b^2ky_1) = c.$$

o que nos diz que $a|c$. Portanto, $a|c$ e $b|c$. □

Proposição 1.5. *Sejam $a,b,p \in \mathbb{Z}$. Se p é primo e $p|ab$, então $p|a$ ou $p|b$.*

Demonstração: Consideremos p primo, com $p|ab$ e mostraremos que se $p \nmid a$, então $p|b$. Se $p \nmid a$, então $-p \nmid a$. Como p é primo, os únicos divisores de p são ± 1 e $\pm p$, daí os divisores comuns à a e p são ± 1. Logo $mdc(a,p) = 1$, assim existem $x,y \in \mathbb{Z}$ tais que $ax + py = 1$. Multiplicando toda a igualdade anterior por b, temos:

$$abx + pby = b. \tag{1.20}$$

Mas por hipótese $p|ab$, ou seja, $ab = pk$, com $k \in \mathbb{Z}$. Substituindo ab em (1.20), temos:

$$pkx + pby = b \Longrightarrow p(kx + by) = b,$$

com $kx + by \in \mathbb{Z}$. Logo, $p|b$.

Analogamente, mostra-se que se $p \nmid b$, então $p|a$. Se $p \nmid b$, então $-p \nmid b$. Como p é primo, seus únicos divisores são ± 1 e $\pm p$, daí os divisores comuns à b e p são ± 1. Logo $mdc(p,b) = 1$, assim existem $x,y \in \mathbb{Z}$ tais que $px + by = 1$. Vamos multiplicar a igualdade anterior por a, para obter:

$$pax + bay = a. \tag{1.21}$$

Mas por hipótese $p|ab$, ou seja, $ab = pk$, com $k \in \mathbb{Z}$. Substituindo ab em (1.21), temos:

$$pax + pky = a \Longrightarrow p(ax + ky) = a,$$

com $ax + ky \in \mathbb{Z}$. Logo, $p|a$. □

1.7 Equações diofantinas lineares

Dedicaremos esta seção ao estudo das equações diofantinas lineares, que são equações do tipo

$$ax + by = c. \tag{1.22}$$

sendo $a,b,c \in \mathbb{Z}, a \neq 0$ e $b \neq 0$. Uma solução da equação (1.22) é um par $(x_0,y_0) \in \mathbb{Z} \times \mathbb{Z}$, tal que a sentença $ax_0 + by_0 = c$ seja verdadeira. Vale ressaltar que nem sempre essas equações possuem soluções inteiras. Por exemplo, a equação $4x + 4y = 3$ não possue nenhuma solução, visto que não existem inteiros x e y que a satisfaça, pois temos $4x + 4y$ par e, portanto, nunca igual a 3. Desta forma, precisamos de condições para garantir que equações do tipo (1.22) admitam soluções.

Proposição 1.6. *Uma equação diofantina $ax+by=c$, em que $a,b,c\in\mathbb{Z}$, admite solução se, e somente se, $d|c$, sendo $d=mdc(a,b)$.*

Demonstração: ($\Longrightarrow$) Suponhamos que o par (x_0,y_0) seja uma solução de $ax+by=c$. Assim, a igualdade $ax_0+by_0=c$ é verdadeira e como $d=mdc(a,b)$, segue que $d|a$ e $d|b$, daí $d|ax_0+by_0$, isto é, $d|c$.
($\Longleftarrow$) Como $d=mdc(a,b)$, existe um par de números inteiros (x_1,y_1) tais que $ax_1+by_1=d$. Mas por hipótese $d|c$, assim existe $k\in\mathbb{Z}$ tal que $c=dk$. Daí obtemos

$$c=(ax_1+by_1)k=ax_1k+by_1k=a(x_1k)+b(y_1k).$$

Logo, a equação $ax+by=c$ admite solução e tem o par (x_1k,y_1k) como uma solução. □

Teorema 1.6. *Sejam a e b inteiros e $d=mdc(a,b)$. Se $d|c$, então a equação $ax+by=c$ possui infinitas soluções. Se (x_0,y_0) é uma solução particular, então o conjunto de todas as soluções é dado por*

$$S=\left\{\ \left(x_0+\frac{b}{d}k,y_0-\frac{a}{d}k\right);k\in\mathbb{Z}.\ \right\}.$$

Demonstração: Como $d=mdc(a,b)$, existe o par (x_1,y_1) tal que

$$ax_1+by_1=c=ax_0+by_0\Longrightarrow a(x_1-x_0)=b(y_0-y_1).$$

Como $d|a$ e $d|b$, existem $k_1,k_2\in\mathbb{Z}$ tais que, $a=dk_1$ e $b=dk_2$. Logo,

$$dk_1(x_1-x_0)=dk_2(y_0-y_1)\Longrightarrow k_1(x_1-x_0)=k_2(y_0-y_1), \tag{1.23}$$

onde $mdc(k_1,k_2)=mdc\left(\frac{a}{d},\frac{b}{d}\right)=1$. Como pela igualdade (1.23), $k_1\mid k_2(y_0-y_1)$, segue do Corolário 1.2 que $k_1\mid(y_0-y_1)$. Portanto, $y_0-y_1=k_1k$, com $k\in\mathbb{Z}$. Daí,

$$y_0-y_1=k_1k=\frac{a}{d}k\Longrightarrow y_1=y_0-\frac{a}{d}k.$$

Ainda da igualdade (1.23), obtemos

$$k_1(x_1-x_0)=k_2k_1k\Longrightarrow x_1-x_0=k_2k,$$

isto é,

$$x_1=x_0+\left(\frac{b}{d}\right)k.$$

Portanto para todo $k\in\mathbb{Z}$, o conjunto de todas as soluções da equação $ax+by=c$ é dado por

$$S=\left\{\ \left(x_0+\frac{b}{d}k,\ y_0-\frac{a}{d}k\right)\ \right\}.$$

□

Capítulo 2

CONGRUÊNCIAS

Neste capítulo apresentaremos o conceito de congruência, bem como resultados imprescindíveis ao desenvolvimento de algumas de suas aplicações que serão abordadas no capítulo seguinte.

Segundo Hygino e Iezzi (1972) a noção e notação de congruência foi introduzida por Karl Friedrich Gauss (1777-1855), em sua obra *Disquisitiones arithmeticae*. Esta ferramenta é considerada uma das mais relevantes da Teoria dos Números e está presente em nosso dia a dia mesmo não percebendo. Um exemplo de sua aplicação é o relógio de ponteiros. Observemos a figura de um relógio, cujo ponteiro das horas está sobre o número 12.

Figura 2.1: Relógio

Fonte: FURLÃO (2015).

Como sabemos, o dia divide-se em dois períodos, sendo que cada um é composto por 12 horas. Neste sentido, em que posição o ponteiro das horas se encontrará após 5 horas? Para responder a essa questão, iremos apenas somar $12+5=17$, só que não existe "17 horas" no relógio de ponteiros, uma vez que as horas se repetem a cada 12 horas. No sentido que discutiremos no decorrer deste capítulo, isto significa que a congruência módulo 12 está presente no relógio de ponteiro. Assim, o número 5 no relógio equivale ao número 17, em termos de congruência isto

implica que: $17 \equiv 5\ (mod\ 12)$. A seguir formalizaremos o conceito de congruência modular.

Definição 2.1. *Sejam a, b e $m \in \mathbb{Z}$, com $m > 0$. Dizemos que a é* ***côngruo*** *a b módulo m, se $m|(a-b)$, ou seja, $a-b=mq$, para algum q inteiro. Para indicar que a é côngruo a b, módulo m, usamos a notação $a \equiv b\ (mod\ m)$.*

Por esta definição, temos que $8 \equiv 4\ (mod\ 2)$, pois $2|(8-4)$. Se $m \nmid (a-b)$, então dizemos que a é incôngruo a b módulo m, e denotamos por $a \not\equiv b\ (mod\ m)$. A Definição 2.1 estabelece uma relação sobre $\mathbb{Z}$, chamada congruência módulo m.

Definição 2.2. *Consideremos os conjuntos A e B. Uma relação de A em B é um subconjunto $\mathcal{R}$ do produto cartesiano $A \times B$. Uma relação de A em A, isto é, um subconjunto de A^2, é chamado uma relação sobre A. Para indicar que o par $(x,\ y)$ pertence à relação $\mathcal{R}$, escrevemos $x\mathcal{R}y$, que significa dizer que x está relacionado com y segundo $\mathcal{R}$. Portanto*

$$(x,\ y) \in \mathcal{R} \Longleftrightarrow x\mathcal{R}y.$$

Definição 2.3. *Uma relação $\mathcal{R}$ em um conjunto A é chamada* ***relação de equivalência*** *quando as seguintes condições forem satisfeitas:*
(i) $x\mathcal{R}x$, para todo $x \in A$. ($\mathcal{R}$ é reflexiva)
(ii) Se $x\mathcal{R}y$, então $y\mathcal{R}x$, para todo $x, y \in A$. ($\mathcal{R}$ é simétrica)
(iii) Se $x\mathcal{R}y$ e $y\mathcal{R}z$, então $x\mathcal{R}z$, para todo $x, y, z \in A$. ($\mathcal{R}$ é transitiva)

Proposição 2.1. *A relação congruência módulo m denotada por " $\equiv$ " é uma relação de equivalência.*

Demonstração: Devemos verificar que a relação " $\equiv$ " satisfaz para quaisquer $a, b, c, m \in \mathbb{Z}$, com $m > 0$, as seguintes condições:
(i) $a \equiv a\ (mod\ m)$.
(ii) $a \equiv b\ (mod\ m) \Rightarrow b \equiv a\ (mod\ m)$.
(iii) $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m) \Rightarrow a \equiv c\ (mod\ m)$.
De fato: (i) $a \equiv a\ (mod\ m)$, pois $m|(a-a)$.
(ii) Se $a \equiv b\ (mod\ m)$, então por definição $m|(a-b)$ e daí $a-b=mq$, para algum $q \in \mathbb{Z}$. Assim $(-1)(a-b)=m(-q)$, ou seja,$m|b-a$.
(iii) Por hipótese $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$. Assim existem inteiros k_1 e k_2 tais que $a-b=mk_1$ e $b-c=mk_2$. Somando membro a membro as equações obtemos $a-c=mk_1+k_2)$, e isto implica que $a \equiv c\ (mod\ m)$. □

Proposição 2.2. *Para $a,b \in \mathbb{Z}$, temos que $a \equiv b \ (mod\ m)$ se, e somente se, a e b fornecem mesmo resto na divisão euclidiana por m.*

Demonstração: ($\Longrightarrow$) Por hipótese $a-b=mq,\ q \in \mathbb{Z}$. Daí,

$$a = b + mq. \tag{2.1}$$

Sejam q_1 e r o quociente e o resto na divisão euclidiana de a por m, assim

$$a = mq_1 + r, \tag{2.2}$$

com $0 \leq r < m$. De (2.1) e (2.2) temos que $b+mq = mq_1 + r \Rightarrow b = m(q_1 - q) + r$, sendo $0 \leq r < m$. Logo r é o resto da divisão euclidiana de b por m.
($\Longleftarrow$) Supondo que a e b fornecem mesmo resto na divisão euclidiana por m, temos $a = mq_1 + r$ e $b = mq_2 + r$ com $0 \leq r < m$. Subtraindo-se membro a membro as duas igualdades anteriores, obtemos $a - b = m(q_1 - q_2)$ o que implica em $a \equiv b \ (mod\ m)$. □

Proposição 2.3. *Se $a \equiv b \ (mod\ m)$, então $(a \pm c) \equiv (b \pm c) \ (mod\ m)$ e para todo $c \in \mathbb{Z}$, $ac \equiv bc \ (mod\ m)$.*

Demonstração: Mostraremos inicialmente que se $a \equiv b \ (mod\ m)$, então $(a \pm c) \equiv (b \pm c) (mod\ m)$. Como $a \equiv b \ (mod\ m)$, segue que $m|(a-b)$, ou seja,

$$a - b = mq, \tag{2.3}$$

para algum q inteiro. Somando e subtraindo c em (2.3), temos

$$a + c - c - b = mq \Rightarrow m|[(a+c) - (b+c)],$$

ou seja, $(a+c) \equiv (b+c) \ (mod\ m)$. Agora, somando e subtraindo $(-c)$ em (2.3), obtemos $a - c + c - b = mq \Rightarrow m|[(a-c) - (b-c)]$, isto é, $(a-c) \equiv (b-c) \ (mod\ m)$. Mostraremos agora que se, $a \equiv b \ (mod\ m)$, então $ac \equiv bc \ (mod\ m), \forall\ c \in \mathbb{Z}$. Por hipótese $a - b = mq, q \in \mathbb{Z}$. Multiplicando a igualdade anterior por c, obtemos $(a-b)c = mqc \Rightarrow ac - bc = m(qc)$. Daí, podemos notar que $m|(ac - bc)$ e consequentemente $ac \equiv bc \ (mod\ m)$. □

Proposição 2.4. *Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $(a \pm c) \equiv (b \pm d) \ (mod\ m)$ e $ac \equiv bd \ (mod\ m)$.*

Demonstração: De início, mostraremos que se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $(a \pm c) \equiv (b \pm d) \ (mod\ m)$. Por hipótese, $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$. Assim, existem $k, k_1 \in \mathbb{Z}$, tais que

$$a - b = mk \tag{2.4}$$

$$c - d = mk_1. \tag{2.5}$$

Somando-se (2.4) e (2.5) obtemos $(a-b)+(c-d) = mk + mk_1$, ou ainda,

$$(a+c)-(b+d) = m(k+k_1) \Longrightarrow (a+c) \equiv (b+d) \ (mod\ m).$$

Agora, subtraindo-se membro a membro (2.4) e (2.5) obtemos

$$(a-b)-(c-d) = mk - mk_1 = m(k-k_1) \Rightarrow (a-c) \equiv (b-d) \ (mod\ m).$$

Vamos agora mostrar que se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$. Multiplicando (2.4) por c e (2.5) por b, obtemos $ac - bc = mkc$ e $bc - bd = mk_1 b$. Somando membro a membro ambas as igualdades, teremos $ac - bc + bc - bd = ac - bd = m(ck + bk_1)$, o que implica que $ac \equiv bd \ (mod\ m)$. □

Proposição 2.5. *Se $a \equiv b \ (mod\ m)$, então $ra \equiv rb \ (mod\ m)$, para todo inteiro $r \geq 1$ e $a^r \equiv b^r \ (mod\ m)$.*

1ª Afirmação- Se $a \equiv b \ (mod\ m)$, então $ra \equiv rb \ (mod\ m)$. Usaremos indução sobre r em $p(r)$: $ra \equiv rb \ (mod\ m)$, $\forall\ r \geq 1$.

(i) $p(1)$ é verdade, pois $1a \equiv 1b \ (mod\ m)$, isto é, $a \equiv b \ (mod\ m)$.

(ii) Suponhamos que $p(k)$ é verdade para todo $k \geq 1$, e mostraremos que $p(k+1)$ também é verdade. Por hipótese de indução temos $ka \equiv kb \ (mod\ m)$ e como $a \equiv b \ (mod\ m)$, podemos usar a Proposição 2.4 para obter

$$a + ka \equiv b + kb \ (mod\ m) \Longrightarrow a(k+1) \equiv b(k+1) \ (mod\ m).$$

Assim, $p(k+1)$ é verdade e, portanto, pelo *Primeiro Princípio de Indução Matemática* $ra \equiv rb \ (mod\ m)$.

2ª Afirmação - Se $a \equiv b \ (mod\ m)$, então $a^r \equiv b^r \ (mod\ m)$ para todo inteiro $r \geq 1$. Usando indução sobre r, em $p(r) : a^r \equiv b^r \ (mod\ m)$, temos que

(i) $p(1)$ é verdade, pois $a^1 \equiv b^1 \ (mod\ m)$.

(ii) Vamos supor que $p(k)$ é verdade, isto é, $a^k \equiv b^k \ (mod\ m)$, para algum $k \geq 1$ e mostraremos que $p(k+1)$ também o é. Como $a \equiv b \ (mod\ m)$ e $a^k \equiv b^k \ (mod\ m)$, temos pela Proposição 2.4 que:

$$aa^k \equiv bb^k \ (mod\ m) \Longrightarrow a^{k+1} \equiv b^{k+1} \ (mod\ m).$$

□

Proposição 2.6. *Se $ca \equiv cb \ (mod\ m)$, e $mdc\ (c,m) = d > 0$, então $a \equiv b \left(mod\ \frac{m}{d}\right)$.*

Demonstração: Temos por hipótese que

$$ca \equiv cb \ (mod\ m) \Longrightarrow ca - cb = c(a-b) = mq, q \in \mathbb{Z}.$$

Dividindo-se os dois membros da igualdade anterior por d, o que é possível em $\mathbb{Z}$, pois d é divisor de c e m, temos

$$\frac{c}{d}(a-b) = \frac{m}{d}q,$$

o que mostra que $\frac{m}{d}$ é divisor de $\frac{c}{d}(a-b)$, ou seja, $\frac{m}{d}\Big|\frac{c}{d}(a-b)$. Como $mdc\ (c,m) = d$, segue do Corolário 1.1 que $mdc\left(\frac{c}{d}, \frac{m}{d}\right) = 1$. Logo $\frac{c}{d}$ e $\frac{m}{d}$ são primos entre si e pelo Corolário 1.2 $\frac{m}{d}\Big|(a-b)$ e, portanto $a \equiv b \left(mod\ \frac{m}{d}\right)$. □

Proposição 2.7. *Se $a \equiv b \ (mod\ m)$, e $0 \leq b < m$, então b é o resto da divisão euclidiana de a por m. Reciprocamente, se r é o resto da divisão de a por m, então $a \equiv r \ (mod\ m)$.*

Demonstração: Se $a \equiv b \ (mod\ m)$ e $0 \leq b < m$, então $m|(a-b)$ o que garante a existência de $q \in \mathbb{Z}$, tal que $a - b = mq$. Daí, $a = mq + b$ com $0 \leq b < m$. Usando a unicidade do resto e do quociente no *Algoritmo da Divisão*, temos que b é o resto da divisão de a por m. Reciprocamente, se r é o resto da divisão de a por m, então existe $q \in \mathbb{Z}$ tal que $a = mq + r$, com $0 \leq r < m$. Assim $a - r = mq$, isto é, $m|(a-r)$ e, portanto $a \equiv r \ (mod\ m)$. □

2.1 Sistemas completos de resto

Definiremos a seguir a classe de equivalência de um número inteiro.

Definição 2.4. *Seja a um número inteiro. A classe de restos módulo m ou classe de equivalência de a, denotada por $\overline{a}$, é o conjunto dos inteiros que são côngruos à a módulo m, ou seja*

$$\overline{a} = \{x \in \mathbb{Z};\ x \equiv a \ (mod\ m)\}.$$

Exemplo 2.1. *Para $m = 3$, determinar as classes de equivalência de* 0, 1 *e* 2.

Temos,

$$\begin{aligned}
\overline{0} &= \{x \in \mathbb{Z};\ x \equiv 0\ (mod\ 3)\} \\
&= \{x \in \mathbb{Z};\ 3|(x-0)\} \\
&= \{x \in \mathbb{Z};\ 3|x\} \\
&= \{x \in \mathbb{Z};\ x = 3k \quad k \in \mathbb{Z}\} \\
&= \{\ldots, -6, -3, 0, 3, 6, \ldots\}
\end{aligned}$$

Daí, $\overline{0}$ é o conjunto dos inteiros, cuja divisão por 3 deixa resto 0.

$$\begin{aligned}
\overline{1} &= \{x \in \mathbb{Z};\ x \equiv 1\ (mod\ 3)\} \\
&= \{x \in \mathbb{Z};\ 3|(x-1)\} \\
&= \{x \in \mathbb{Z};\ x-1 = 3k \quad k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z};\ x = 3k+1 \quad k \in \mathbb{Z}\} \\
&= \{\ldots, -5, -2, 1, 4, 7, \ldots\}
\end{aligned}$$

Assim, $\overline{1}$ representa o conjunto dos inteiros, cuja divisão por 3 deixa resto 1. E, por último,

$$\begin{aligned}
\overline{2} &= \{x \in \mathbb{Z};\ x \equiv 2\ (mod\ 3)\} \\
&= \{x \in \mathbb{Z};\ 3|(x-2)\} \\
&= \{x \in \mathbb{Z};\ x-2 = 3k \quad k \in \mathbb{Z}\} \\
&= \{x \in \mathbb{Z};\ x = 3k+2 \quad k \in \mathbb{Z}\} \\
&= \{\ldots, -4, -1, 0, 5, 8, \ldots\}
\end{aligned}$$

Essa classe de equivalência $(\overline{2})$ representa o conjunto dos inteiros que deixam resto 2 ao serem divididos por 3.

Definição 2.5. *Um conjunto de m inteiros, $m > 0$ forma um sistema completo de restos módulo m se, dois quaisquer desses números, diferentes entre si, são incôngruos módulo m.*

Exemplo 2.2. *O conjunto* $\{0,\ 1,\ 2\}$ *é um sistema completo de restos módulo* 3.

De fato, dois quaisquer desses números, diferentes entre si, são incôngruos módulo 3. Ou seja, $0 \not\equiv 1\ (mod\ 3)$; $0 \not\equiv 2\ (mod\ 3)$ e $1 \not\equiv 2\ (mod\ 3)$, pois a diferença entre dois quaisquer desses números não é múltiplo de 3.

Exemplo 2.3. *O conjunto* $\{0,1,2,3,\ldots,m-1\}$ *é um sistema completo de restos módulo m.*

De fato, se i e j são inteiros tais que $0 \leq i < j < m$, então i, j pertencem ao conjunto dado e são distintos entre si. Assim, $0 < j - i < m$ e portanto $j \not\equiv i \ (mod\ m)$, pois como $j - i < m$ segue que $m \nmid j - i$.

Observação 2.1. *O conjunto* $\{0,1,2,3,\ldots,m-1\}$ *é chamado sistema completo de restos mínimos positivos.*

Proposição 2.8. *Se o conjunto* $\{r_1,\ r_2,\ldots,r_m\}$ *é um sistema completo de restos módulo m, então todo inteiro a é côngruo a um, e somente um dos* r_i.

Demonstração: Vamos aplicar inicialmente o *Algoritmo da divisão* aos elementos a e m. Assim, $a = mq + r$, com $0 \leq r < m$. Daí, temos que $a \equiv r \ (mod\ m)$, com $r \in \{0,1,2,\ldots,m-1\}$. Por outro lado, se aplicarmos o *Algoritmo da divisão* para os elementos $r_1, r_2, \ldots, r_m$ e m, obtemos:

$$\begin{aligned} r_1 &= mq_1 + r_1^{'} \\ r_2 &= mq_2 + r_2^{'} \\ r_3 &= mq_3 + r_3^{'} \\ &\vdots \\ r_m &= mq_m + r_m^{'} \end{aligned}$$

sendo $r_1^{'}, r_2^{'}, r_3^{'}, \ldots, r_m^{'} \in \{0,1,2,\ldots,m-1\}$. Para um certo r_j, teremos

$$r_j = mq_j + r.$$

Como $a = mq + r$, segue que a e r_j deixam mesmo resto na divisão euclidiana por m. Portanto, eles são côngruos, isto é, $a \equiv r_j \ (mod\ m) \Rightarrow r_j \equiv a \ (mod\ m)$. Se $a \equiv r_k \ (mod\ m)$, então $r_j \equiv r_k \ (mod\ m)$. Como por hipótese, $\{r_1, r_2, \ldots, r_m\}$ é um sistema completo de restos, segue que $r_j = r_k$. □

Exemplo 2.4. *Se m é ímpar, então o conjunto* $\left\{0, \pm 1, \pm 2, \ldots, \pm\left(\frac{m-1}{2}\right)\right\}$ *é um sistema completo de restos módulo m.*

De fato, sejam i e j dois elementos desse conjunto, com $i \neq j$. Assim,

$$|\, i \,| \leq \frac{m-1}{2} \quad e \quad |\, j \,| \leq \frac{m-1}{2}.$$

Daí,

$$\begin{aligned} 0 < |\, i-j\,| &\leq |\, i\,| + |\, j\,| \\ &\leq \frac{m-1}{2} + \frac{m-1}{2} = 2\left(\frac{m-1}{2}\right) = m-1, \end{aligned}$$

ou seja, $0 < |\, i-j\,| \leq m-1 < m \Longrightarrow i-j < m$ e portanto $i \not\equiv j \ (mod\ m)$.

Exemplo 2.5. *Se m é par, então o conjunto* $\left\{0, \pm 1, \pm 2, \ldots, \pm\frac{m-2}{2}, \frac{m}{2}\right\}$ *é um sistema completo de restos módulo m.*

De fato, sejam i e j dois elementos desse conjunto, com $i \neq j$. Assim,

$$0 \leq i < j \leq \frac{m}{2} \Longrightarrow 0 \leq |\, j-i\,| \leq \frac{m}{2} < m.$$

Daí,

$$0 < |\, j-i\,| < m \implies j-i < m,$$

e portanto $j \not\equiv i \ (mod\ m)$.

2.2 Congruência linear

Definição 2.6. *Denominamos congruência linear em uma variável, toda congruência da forma* $ax \equiv b \ (mod\ m)$*, sendo x uma incógnita em* $\mathbb{Z}$ *e* $a, b, m \in \mathbb{Z}$ *com* $a \neq 0$ *e* $m > 0$*.*

Todo inteiro x_0, tal que $ax_0 \equiv b \ (mod\ m)$ é uma solução da congruência $ax \equiv b \ (mod\ m)$. Por exemplo, o número 4 é solução de $2x \equiv 3 \ (mod\ 5)$, pois $2 \cdot 4 \equiv 3 \ (mod\ 5)$. Mas vale ressaltar que nem sempre uma congruência linear possui solução inteira. É o caso da congruência $2x \equiv 1 \ (mod\ 4)$, pois qualquer que seja $x \in \mathbb{Z}$, $4 \nmid (2x-1)$.

Teorema 2.1. *Uma congruência linear* $ax \equiv b \ (mod\ m)$*, com* $a \neq 0$*, admite solução em* $\mathbb{Z}$ *se, e somente se,* $d|b$*, sendo* $d = mdc(a, m)$*.*

Demonstração: $(\Longrightarrow)$ Suponhamos que a congruência $ax \equiv b \ (mod\ m)$ admite solução. Assim existe $x_0 \in \mathbb{Z}$ tal que $ax_0 \equiv b \ (mod\ m)$ e por definição de congruência existe $y_0 \in \mathbb{Z}$ tal que, $ax_0 - b = my_0$. Como $d = mdc(a, m)$, segue que $d|a$ e $d|m$, e com isto $d|ax_0 - my_0$, ou seja, $d|b$.
$(\Longleftarrow)$ Suponhamos agora que $d|b$ sendo $d = mdc(a, m)$. Usando a Proposição 1.6 segue que a equação diofantina $ax - my = b$ admite solução. Daí, existem $x_0, y_0 \in \mathbb{Z}$ tais que $ax_0 - my_0 = b$, ou seja, $ax_0 - b = my_0$. Logo $ax_0 \equiv b \ (mod\ m)$ e, portanto x_0 é uma solução da congruência $ax \equiv b \ (mod\ m)$. □

Exemplo 2.6. *Vamos verificar se a congruência* $3x \equiv 21 \ (mod\ 42)$ *possui solução e, em caso afirmativo, encontrá-la.*

Note que $d = mdc(a,m) = mdc(3,42) = 3$ e $3|21$. Assim, a congruência admite solução. Daí, $3x \equiv 21 \ (mod\ 42) \Longleftrightarrow 42|(3x-21)$, ou seja, $3x-21 = 42y_0 \Rightarrow 3x-42y_0 = 21$ com $y_0 \in \mathbb{Z}$. Logo, resolver a congruência $3x \equiv 21 \ (mod\ 42)$ é o mesmo que resolver a equação diofantina $3x-42y_0 = 21$. Para isso, basta-nos resolver a Identidade de Bezout $3x-42y_0 = 3$. Mas, notemos que $x = 15$ e $y_0 = 1$ satisfaz essa identidade. Desse modo, a equação diofantina $3x-42y_0 = 21$ tem solução $(7 \cdot 15, 7 \cdot 1) = (105, 7)$. E portanto, uma solução para a congruência é $x = 105$.

Capítulo 3

APLICAÇÕES

Dedicaremos este capítulo ao estudo de algumas aplicações de congruência modular, tais como; critérios de divisibilidade, criptografia, cartão de crédito, CPF e calendário.

3.1 Critérios de divisibilidade

Dentre as mais diversas aplicações, podemos utilizar a congruência modular para determinar critérios de divisibilidade, que consistem em regras práticas que permitem determinar se um número inteiro a é divisor de um número inteiro b em sua representação decimal, ou seja, na base 10. A seguir, serão abordados os critérios de divisibilidade para os respectivos inteiros $2, 3, 4, 5, 6, 8, 9, 10$ e 11 por meio de congruência modular.

Os critérios de divisibilidade aqui abordados são definidos por Iezzi, Dolce e Machado (2009) como:

- "Um número é divisível por 2 quando ele é par" (p.113).
- "Um número é divisível por 3 quando a soma de seus algarismos é divisível por 3" (p.114).
- "Um número é divisível por 4 quando seus dois últimos algarismos formam um número divisível por 4" (p.116).
- "Um número é divisível por 5 quando termina em 0 ou 5" (p.115).
- "Um número é divisível por 6 quando é divisível por 2 e por 3" (p.114).

- “Um número é divisível por 8 quando os três últimos algarismos formam um número divisível por 8” (p.117).

- “Um número é divisível por 9 quando a soma de seus algarismos é divisível por 9” (p.118).

- “Um número é divisível por 10 quando termina em 0” (p.116).

O critério de divisibilidade por 11, dado a seguir, é definido por Vieira (2015) como:

- “Um inteiro a é divisível por 11 se, e somente se, $\mathcal{S}_P - \mathcal{S}_I$ é divisível por 11, com $\mathcal{S}_P = a_0 + a_2 + a_4 + ...$ (a soma dos dígitos de índice par) e $\mathcal{S}_I = a_1 + a_3 + a_5 + ...$ (a soma dos dígitos de índice ímpar)” (p.94).

Para todos os critérios de divisibilidade que serão abordados adiante, iremos considerar $N = a_k a_{k-1} \cdots a_1 a_0$, um número natural, cuja representação decimal é dada por:

$$N = a_k 10^k + a_{k-1} 10^{k-1} + a_{k-2} 10^{k-2} + \ldots + a_1 10 + a_0; \;\; k \in \mathbb{Z}.$$

3.1.1 Critério de Divisibilidade por 2

Observemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv 0 \,(mod\ 2) \\ 10^2 &\equiv 0 \,(mod\ 2) \\ 10^3 &\equiv 0 \,(mod\ 2) \\ &\vdots \\ 10^k &\equiv 0 \,(mod\ 2). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 0 \,(mod\ 2)$ por a_i, com $i = 1, 2, 3, \ldots, k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv 0 \,(mod\ 2) \\ a_2 10^2 &\equiv 0 \,(mod\ 2) \\ a_3 10^3 &\equiv 0 \,(mod\ 2) \\ &\vdots \\ a_k 10^k &\equiv 0 \,(mod\ 2). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv 0 \ (mod\ 2).$$

Da Proposição 2.3 de congruências, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_0 \ (mod\ 2).$$

Logo, pela Proposição 2.2 N e a_0 possuem o mesmo resto na divisão por 2 e, consequentemente, N é divisível por 2 se, e somente se, a_0 o é, ou seja, $2|a_0 \Rightarrow a_0 = 2t$, $t \in \mathbb{Z}$, implicando que a_0 é par. □

Exemplo 3.1. *O número* 5834 *é divisível por* 2*, pois* $a_0 = 4$ *e* $2|4$.

3.1.2 Critério de Divisibilidade por 3

Notemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv 1 \ (mod\ 3) \\ 10^2 &\equiv 1 \ (mod\ 3) \\ 10^3 &\equiv 1 \ (mod\ 3) \\ &\vdots \\ 10^k &\equiv 1 \ (mod\ 3). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 1 \ (mod\ 3)$ por a_i, com $i = 1, 2, 3, \ldots, k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv a_1 \ (mod\ 3) \\ a_2 10^2 &\equiv a_2 \ (mod\ 3) \\ a_3 10^3 &\equiv a_3 \ (mod\ 3) \\ &\vdots \\ a_k 10^k &\equiv a_k \ (mod\ 3). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv a_k + \ldots + a_3 + a_2 + a_1 \ (mod\ 3).$$

Da Proposição 2.3 de congruências, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_k + \ldots + a_3 + a_2 + a_1 + a_0 \ (mod\ 3).$$

Logo, pela Proposição 2.2 N e $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ possuem o mesmo resto na divisão por 3, e consequentemente, N é divisível por 3 se, e somente se, $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ é divisível por 3. □

Exemplo 3.2. *O número* 576 *é divisível por* 3*, pois* $3|(5+7+6)$*, ou seja,* $3|18$.

3.1.3 Critério de Divisibilidade por 4

Observemos que pela Proposição 2.5

$$\begin{aligned} 10^2 &\equiv 0\ (mod\ 4) \\ 10^3 &\equiv 0\ (mod\ 4) \\ 10^4 &\equiv 0\ (mod\ 4) \\ &\vdots \\ 10^k &\equiv 0\ (mod\ 4). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 0\ (mod\ 4)$ por a_i, com $i = 2,3,4,\ldots,k$, obtemos:

$$\begin{aligned} a_2 10^2 &\equiv 0\ (mod\ 4) \\ a_3 10^3 &\equiv 0\ (mod\ 4) \\ a_4 10^4 &\equiv 0\ (mod\ 4) \\ &\vdots \\ a_k 10^k &\equiv 0\ (mod\ 4). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_4 10^4 + a_3 10^3 + a_2 10^2 \equiv 0\ (mod\ 4).$$

Segue da Proposição 2.3 de congruências, que

$$a_k 10^k + \ldots + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_1 10 + a_0\ (mod\ 4).$$

Logo, pela Proposição 2.2 N e $a_1 10 + a_0$ possuem o mesmo resto na divisão por 4, e consequentemente, N é divisível por 4 se, e somente se, $a_1 10 + a_0 = a_1 a_0$ é divisível por 4. □

Exemplo 3.3. *O número* 3524 *é divisível por* 4*, pois* $4|(24)$*, que é o número formado pelos dois últimos algarismos.*

3.1.4 Critério de Divisibilidade por 5

Notemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv 0\ (mod\ 5) \\ 10^2 &\equiv 0\ (mod\ 5) \\ 10^3 &\equiv 0\ (mod\ 5) \\ &\vdots \\ 10^k &\equiv 0\ (mod\ 5). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 0\ (mod\ 5)$ por a_i, com $i = 1,2,3,\ldots,k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv 0\ (mod\ 5) \\ a_2 10^2 &\equiv 0\ (mod\ 5) \\ a_3 10^3 &\equiv 0\ (mod\ 5) \\ &\vdots \\ a_k 10^k &\equiv 0\ (mod\ 5). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv 0\ (mod\ 5).$$

Da Proposição 2.3 de congruências, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_0\ (mod\ 5).$$

Logo, pela Proposição 2.2 N e a_0 possuem o mesmo resto na divisão por 5, e consequentemente, N é divisível por 5 se, e somente se, a_0 o é, ou seja, $a_0 = 0$ ou $a_0 = 5$. □

Exemplo 3.4. *O número* 2765 *é divisível por* 5*, pois* $a_0 = 5$*.*

3.1.5 Critério de Divisibilidade por 6

Observemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv (-2)\ (mod\ 6) \\ 10^2 &\equiv (-2)\ (mod\ 6) \\ 10^3 &\equiv (-2)\ (mod\ 6) \\ &\vdots \\ 10^k &\equiv (-2)\ (mod\ 6). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv (-2)\ (mod\ 6)$ por a_i, com $i = 1,2,3,\ldots,k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv a_1(-2)\ (mod\ 6) \\ a_2 10^2 &\equiv a_2(-2)\ (mod\ 6) \\ a_3 10^3 &\equiv a_3(-2)\ (mod\ 6) \\ &\vdots \\ a_k 10^k &\equiv a_k(-2)\ (mod\ 6). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv a_k(-2) + \ldots + a_3(-2) + a_2(-2) + a_1(-2)\ (mod\ 6).$$

Da Proposição 2.3 de congruências, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv (-2)(a_k + \ldots + a_3 + a_2 + a_1 + a_0) + 3a_0\ (mod\ 6).$$

Logo, pela Proposição 2.2 N e $(-2)(a_k + \ldots + a_3 + a_2 + a_1 + a_0) + 3a_0$ possuem o mesmo resto na divisão por 6 e, consequentemente, N é divisível por 6 se, e somente se, $(-2)(a_k + \ldots + a_3 + a_2 + a_1 + a_0) + 3a_0$ o é, ou seja, $6|(-2)(a_k + \ldots + a_3 + a_2 + a_1 + a_0) + 3a_0$, e para que isto aconteça, devemos ter $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ divisível por 3 e a_0 par. Portanto, N é divisível por 6 se, e somente se, é divisível por 2 e por 3. □

Exemplo 3.5. *O número* 1734 *é divisível por* 6*, pois* $1+7+3+4$ *é divisível por* 3 *e* $a_0 = 4$ *é par.*

3.1.6 Critério de Divisibilidade por 8

Notemos que pela Proposição 2.5

$$\begin{aligned} 10^3 &\equiv 0\ (mod\ 8) \\ 10^4 &\equiv 0\ (mod\ 8) \\ 10^5 &\equiv 0\ (mod\ 8) \\ &\vdots \\ 10^k &\equiv 0\ (mod\ 8). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 0\ (mod\ 8)$ por a_i, com $i = 3,4,5,\ldots,k$, obtemos:

$$\begin{aligned} a_3 10^3 &\equiv 0\ (mod\ 8) \\ a_4 10^4 &\equiv 0\ (mod\ 8) \\ a_5 10^5 &\equiv 0\ (mod\ 8) \\ &\vdots \\ a_k 10^k &\equiv 0\ (mod\ 8). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_5 10^5 + a_4 10^4 + a_3 10^3 \equiv 0\ (mod\ 8).$$

Da Proposição 2.3 de congruências, segue que

$$a_k 10^k + \ldots + a_5 10^5 + a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_2 10^2 + a_1 10 + a_0\ (mod\ 8).$$

Logo, pela Proposição 2.2 N e $a_2 10^2 + a_1 10 + a_0$ possuem o mesmo resto na divisão por 8 e, consequentemente, N é divisível por 8 se, e somente se, $a_2 10^2 + a_1 10 + a_0 = a_2 a_1 a_0$ é divisível por 8. □

Exemplo 3.6. *O número* 6104 *é divisível por* 8. *De fato;* $8|(104)$, *que é o número formado pelos três últimos algarismos.*

3.1.7 Critério de Divisibilidade por 9

Observemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv 1 \ (mod\ 9) \\ 10^2 &\equiv 1 \ (mod\ 9) \\ 10^3 &\equiv 1 \ (mod\ 9) \\ &\vdots \\ 10^k &\equiv 1 \ (mod\ 9). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 1 \ (mod\ 9)$ por a_i, com $i = 1, 2, 3, \ldots, k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv a_1 \ (mod\ 9) \\ a_2 10^2 &\equiv a_2 \ (mod\ 9) \\ a_3 10^3 &\equiv a_3 \ (mod\ 9) \\ &\vdots \\ a_k 10^k &\equiv a_k \ (mod\ 9). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv a_k + \ldots + a_3 + a_2 + a_1 \ (mod\ 9).$$

Da Proposição 2.3, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_k + \ldots + a_3 + a_2 + a_1 + a_0 \ (mod\ 9).$$

Logo, pela Proposição 2.2 N e $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ possuem o mesmo resto na divisão por 9, e consequentemente, N é divisível por 9 se, e somente se, $a_k + \ldots + a_3 + a_2 + a_1 + a_0$ é divisível por 9. □

Exemplo 3.7. *O número* 1935 *é divisível por* 9. *De fato;* $9|(1+9+3+5)$, *ou seja,* $9|18$.

3.1.8 Critério de Divisibilidade por 10

Notemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv 0\ (mod\ 10) \\ 10^2 &\equiv 0\ (mod\ 10) \\ 10^3 &\equiv 0\ (mod\ 10) \\ &\vdots \\ 10^k &\equiv 0\ (mod\ 10). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv 0\ (mod\ 10)$ por a_i, com $i = 1,2,3,\ldots,k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv 0\ (mod\ 10) \\ a_2 10^2 &\equiv 0\ (mod\ 10) \\ a_3 10^3 &\equiv 0\ (mod\ 10) \\ &\vdots \\ a_k 10^k &\equiv 0\ (mod\ 10). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv 0\ (mod\ 10).$$

Da Proposição 2.3, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_0\ (mod\ 10).$$

Logo, pela proposição (2.2) N e a_0 possuem o mesmo resto na divisão por 10 e, consequentemente, N é divisível por 10 se, e somente se, a_0 o é, ou seja, $a_0 = 0$. □

Exemplo 3.8. *O número* 3470 *é divisível por* 10*, pois* $a_0 = 0$*.*

3.1.9 Critério de Divisibilidade por 11

Observemos que pela Proposição 2.5

$$\begin{aligned} 10 &\equiv -1 \ (mod\ 11) \\ 10^2 &\equiv 1 \ (mod\ 11) \\ 10^3 &\equiv -1 \ (mod\ 11) \\ &\vdots \\ 10^k &\equiv (-1)^k \ (mod\ 11). \end{aligned}$$

Ao multiplicarmos as congruências $10^i \equiv (-1)^i \ (mod\ 11)$ por a_i, com $i = 1,2,3,\ldots,k$, obtemos:

$$\begin{aligned} a_1 10 &\equiv -1a_1 \ (mod\ 11) \\ a_2 10^2 &\equiv 1a_2 \ (mod\ 11) \\ a_3 10^3 &\equiv -1a_3 \ (mod\ 11) \\ &\vdots \\ a_k 10^k &\equiv (-1)^k a_k \ (mod\ 11). \end{aligned}$$

Com o auxílio da Proposição 2.4, temos

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 \equiv a_k(-1)^k + \ldots - a_3 + a_2 - a_1 \ (mod\ 11).$$

Da Proposição 2.3, segue que

$$a_k 10^k + \ldots + a_3 10^3 + a_2 10^2 + a_1 10 + a_0 \equiv a_k(-1)^k + \ldots - a_3 + a_2 - a_1 + a_0 \ (mod\ 11).$$

Logo, pela Proposição 2.2 N e $a_k(-1)^k + \ldots - a_3 + a_2 - a_1 + a_0$ possuem o mesmo resto na divisão por 11 e, consequentemente, N é divisível por 11 se, e somente se, a soma de seus algarismos de ordem par subtraída da soma de seus algarismos de ordem ímpar resultar em um número divisível por 11. □

Exemplo 3.9. *O número* 1353 *é divisível por* 11*, pois temos* $a_0 = 3, a_1 = 5, a_2 = 3, a_3 = 1$ *e* $a_0 + a_2 - (a_1 + a_3) = 3 + 3 - (5 + 1) = 6 - 6 = 0$*, que é divisível por* 11*.*

3.2 Criptografia

De acordo com Singh (2007), a palavra "criptografia" deriva da palavra grega kriptos (oculto) e graphen (grafia) e pode ser entendida como "escrita oculta". A criptografia tem como

objetivo esconder o significado de uma mensagem, cujo processo é denominado encriptação. Seu uso consiste em enviar mensagens, independentemente do conteúdo e interesse, de forma segura, sem que ninguém além do emissor e receptor possa ter acesso as informações contidas nas mesmas. Isso acontece pelo fato de que, tanto o emissor quanto o receptor possuem um protocolo específico, geralmente chamado de chave, o que dificulta a compreensão e nitidez da mensagem caso seja interceptada por terceiros.

Essa técnica de escrita vem desde os tempos antigos e, até os dias atuais mensagens secretas são enviadas de diferentes formas. Antigas civilizações como as gregas, romanas e egípcias fizeram uso da criptografia em suas trocas de mensagens. Durante a Segunda Guerra Mundial grupos de americanos dedicavam-se a interceptar e decodificar mensagens secretas de espiões alemães, isso fez com que técnicas criptográficas fossem evoluindo cada vez mais. Segundo Singh (2007), a criptografia é um dos ramos mais poderosos da comunicação secreta graças a sua capacidade de impedir que informações sejam violadas.

Existem dois tipos de criptografias: a simétrica e a assimétrica, as quais passaremos a descrever.

3.2.1 Criptografia Simétrica

Essa criptografia limita-se a transformar uma simples mensagem numa outra, cifrada e de difícil entendimento, por meio de uma chave secreta definida, usada tanto para cifrar [1] como para decifrar a mensagem, sendo a mesma conhecida pelo emissor e receptor. Nesse sistema criptográfico é usado dois tipos de cifras[2], a transposição e a substituição.

Cifra de transposição

Na transposição, as letras das mensagens são rearranjadas gerando um anagrama. Para mensagens curtas este método não é muito seguro, visto que existe um número limitado de maneiras para as letras serem rearranjadas. Porém, à medida que a mensagem vai se estendendo, a segurança aumenta, pois cresce o número de letras e consequentemente o número de rearranjos, o que torna mais difícil a decifragem da mensagem.

Conforme Singh (2007), o primeiro aparelho criptográfico militar que usou o método da transposição surgiu no século V a.C, denominado Citale. O mesmo consiste em um bastão

[1] Cifrar significa misturar uma mensagem por meio de uma cifra.

[2] Cifras são geralmente definidas como substituições de letras.

de madeira, envolto por uma tira de couro, no qual o emissor escreve a mensagem conforme seu comprimento, em seguida desenrola a tira contendo uma porção de letras sem sentido, verificando assim, a mistura da mensagem. Para que o receptor possa decodificar, basta enrolar a tira de couro recebida em um citale com mesmo diâmetro do usado pelo emissor.

Figura 3.1: Citale

Fonte: WIKIPEDIA.

Cifra de substituição

Na substituição, troca-se cada letra da mensagem por outra, obedecendo algum critério determinado. Singh (2007) destaca que o primeiro documento que utilizou uma cifra de substituição, para objetivos militares, surgiu nas Guerras da Gália elaborado pelo imperador Júlio César, sendo essa vista como monoalfabética, ou seja, o texto cifrado pode consistir de letras ou de símbolos.

3.2.2 Criptografia Assimétrica

De acordo com Cavalcante [2014?], a criptografia de chave pública, conhecida também como criptografia assimétrica, possui duas chaves diferentes: uma pública (todos tem acesso), a qual serve para codificar uma mensagem, e outra privada (apenas o emissor conhece), sendo esta utilizada para decodificar a mensagem.

Segundo Coutinho (2015), o mais conhecido dos métodos de criptografia de chave pública é o RSA. Essa sigla refere-se as iniciais dos nomes de seus criadores; R. L. Rivest, A. Shamir e L. Adleman criada em 1977. Existem vários tipos de métodos criptográficos assimétricos, porém o sistema RSA é atualmente o mais usado em aplicações comerciais.

A seguir, apresentaremos mais detalhadamente dois tipos de criptografia, a Cifra de César que usa um método criptográfico simétrico e a RSA que consiste em um método criptográfico assimétrico.

3.2.3 Cifra de César

A Cifra de César foi criada pelo imperador Júlio César com a finalidade de manter secretas correspondências militares, a mesma restringia-se a uma regra na qual, cada letra original do alfabeto era trocada pela que se encontrava três posições a sua frente. Assim, para que o receptor pudesse ler a mensagem ele precisava saber a chave da criptografia utilizada (neste caso, 3) para decifrá-la. Desta forma, bastava substituir cada letra da mensagem pela equivalente a três posições anteriores a ela no alfabeto.

Consideremos a seguinte representação

Tabela 3.1: Representação da Cifra de César

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

Fonte: Autoria própria

Vejamos por exemplo, como a palavra “ARITMÉTICA” seria cifrada:

“DULWPHWLFD”

Vamos agora abordar a Cifra de César com base em congruência modular. Inicialmente devemos estabelecer uma correspondência entre as letras do alfabeto e os números de 0 a 25. A este processo daremos o nome de pré-codificação, ou seja, devemos associar o texto original a um equivalente numérico. Vejamos a tabela abaixo

Tabela 3.2: Pré-Codificação

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

Fonte: Autoria própria

Desta forma, para codificar[3] uma mensagem através da Cifra de César, usaremos a seguinte expressão:

$$C(N) \equiv N + 3 \ (mod\ 26), \ \ 0 \leq C \leq 25. \tag{3.1}$$

onde N é o número pré-codificado, $C(N)$ o número codificado e 3 a chave da codificação.

No caso da decodificação, as letras da mensagem deverão de início serem transformadas em números para que posteriormente possamos aplicar a seguinte expressão:

$$N \equiv C(N) - 3 \ (mod\ 26), \ \ 0 \leq C \leq 25.$$

Exemplo 3.10. *Codifique a mensagem abaixo usando a Cifra de César:*

"CONGRUÊNCIA".

De acordo com a Tabela 3.2, podemos pré-codificar a mensagem dada da seguinte forma

$$2 - 14 - 13 - 6 - 17 - 20 - 4 - 13 - 2 - 8 - 0.$$

Usando a equação (3.1), obtemos:

$$5 - 17 - 16 - 9 - 20 - 23 - 7 - 16 - 5 - 11 - 3.$$

Utilizando novamente a correspondência da Tabela 3.2, teremos:

"FRQJUXHQFLD"

que é a mensagem codificada.

Para a decodificação da mensagem "FRQJUXHQFLD" aplicaremos o processo inverso. Inicialmente substituímos cada letra pelo número que a corresponde, obtendo:

$$5 - 17 - 16 - 9 - 20 - 23 - 7 - 16 - 5 - 11 - 3.$$

Feito isso, aplicaremos a expressão $N \equiv C(N) - 3 \ (mod\ 26)$ que nos dará o número correspondente ao texto simples. Ou seja,

$$2 - 14 - 13 - 6 - 17 - 20 - 4 - 13 - 2 - 8 - 0.$$

Agora basta usarmos a correspondência da Tabela 3.2 e teremos a mensagem decodificada: "CONGRUÊNCIA".

[3]Codificar: processo no qual se oculta uma mensagem usando um código.

Vale ressaltar que a Cifra de César é um caso particular de cifras, definidas da seguinte maneira:

$$C(N) \equiv N + K \ (mod\ 26),\ \ 0 \leq C \leq 25, \tag{3.2}$$

sendo K a chave que corresponde ao tamanho do deslocamento de cada letra do alfabeto no processo de codificação. Para a decodificação, iremos aplicar a expressão:

$$D(Z) \equiv Z - K \ (mod\ 26),\ \ 0 \leq C \leq 25,$$

sendo $Z = C(N)$. Daí,

$$D(C(N)) \equiv C(N) - K \ (mod\ 26). \tag{3.3}$$

Ao substituirmos a expressão (3.2) em (3.3) obtemos:

$$D(C(N)) \equiv N + K - K \ (mod\ 26).$$

Portanto, $D(C(N)) \equiv N \ (mod\ 26)$, isto significa que ao decodificarmos um número codificado obteremos exatamente o número original da mensagem e assim, basta substituí-lo pela letra do alfabeto que o corresponde e teremos a mensagem decifrada.

Exemplo 3.11. *Codifique a mensagem: "Os números governam o mundo". Use a expressão* $C(N) \equiv N + K \ (mod\ 26)$, $0 \leq C \leq 25$ *e* $K = 5$.

Observação 3.1. *Utilizaremos o símbolo "//" para representar o espaço entre as palavras.*

Faremos inicialmente uma pré-codificação da frase dada, melhor dizendo, substituiremos cada letra por seu equivalente numérico de acordo com a Tabela 3.2, obtendo:

$$14-18\ //\ 13-20-12-4-17-14-18\ //\ 6-14-21-4-17-13-0-12\ //$$
$$14\ //\ 12-20-13-3-14.$$

Usaremos agora a expressão $C(N) \equiv N + 5 \ (mod\ 26)$ para codificar cada número.

$$C(14) \equiv 14 + 5 \equiv 19 \ (mod\ 26)$$
$$C(18) \equiv 18 + 5 \equiv 23 \ (mod\ 26)$$
$$C(13) \equiv 13 + 5 \equiv 18 \ (mod\ 26)$$
$$C(20) \equiv 20 + 5 \equiv 25 \ (mod\ 26)$$

$$C(12) \equiv 12+5 \equiv 17 \ (mod\ 26)$$

$$C(4) \equiv 4+5 \equiv 9 \ (mod\ 26)$$

$$C(17) \equiv 17+5 \equiv 22 \ (mod\ 26)$$

$$C(14) \equiv 14+5 \equiv 19 \ (mod\ 26)$$

$$C(18) \equiv 18+5 \equiv 23 \ (mod\ 26)$$

$$C(6) \equiv 6+5 \equiv 11 \ (mod\ 26)$$

$$C(14) \equiv 14+5 \equiv 19 \ (mod\ 26)$$

$$C(21) \equiv 21+5 \equiv 26 \ (mod\ 26)$$

$$C(4) \equiv 4+5 \equiv 9 \ (mod\ 26)$$

$$C(17) \equiv 17+5 \equiv 22 \ (mod\ 26)$$

$$C(13) \equiv 13+5 \equiv 18 \ (mod\ 26)$$

$$C(0) \equiv 0+5 \equiv 5 \ (mod\ 26)$$

$$C(12) \equiv 12+5 \equiv 17 \ (mod\ 26)$$

$$C(14) \equiv 14+5 \equiv 19 \ (mod\ 26)$$

$$C(12) \equiv 12+5 \equiv 17 \ (mod\ 26)$$

$$C(20) \equiv 20+5 \equiv 25 \ (mod\ 26)$$

$$C(13) \equiv 13+5 \equiv 18 \ (mod\ 26)$$

$$C(3) \equiv 3+5 \equiv 8 \ (mod\ 26)$$

$$C(14) \equiv 14+5 \equiv 19 \ (mod\ 26).$$

Notemos que, $C(21) \equiv 21+5 \equiv 26 \ (mod\ 26)$, mas $0 \leq C \leq 25$ e como $26 \equiv 0 \ (mod\ 26)$, segue que $C(21) \equiv 0 \ (mod\ 26)$.

Daí obtemos,

$$19-23\ //\ 18-25-17-9-22-19-23\ //\ 11-19-0-9-22-18-5-17\ //$$
$$19\ //\ 17-25-18-8-19.$$

Aplicando a correspondência outra vez encontraremos a mensagem codificada:

"TX SZRJWTX LTAJWSFR T RZSIT".

Para decodificar esta mensagem, seguiremos o processo inverso da codificação, de maneira que cada letra será convertida no seu número equivalente, isto é,

$$19-23\ //\ 18-25-17-9-22-19-23\ //\ 11-19-0-9-22-18-5-17\ //$$
$$19\ //\ 17-25-18-8-19.$$

Utilizando agora a expressão $D(Z) \equiv Z-5\ (mod\ 26)$, sendo Z os números codificados da mensagem, temos:

$$C(19) \equiv 19-5 \equiv 14\ (mod\ 26)$$
$$C(23) \equiv 23-5 \equiv 18\ (mod\ 26)$$
$$C(18) \equiv 18-5 \equiv 13\ (mod\ 26)$$
$$C(25) \equiv 25-5 \equiv 20\ (mod\ 26)$$
$$C(17) \equiv 17-5 \equiv 12\ (mod\ 26)$$
$$C(9) \equiv 9-5 \equiv 4\ (mod\ 26)$$
$$C(22) \equiv 22-5 \equiv 17\ (mod\ 26)$$
$$C(19) \equiv 19-5 \equiv 14\ (mod\ 26)$$
$$C(23) \equiv 23-5 \equiv 18\ (mod\ 26)$$
$$C(11) \equiv 11-5 \equiv 6\ (mod\ 26)$$
$$C(19) \equiv 19-5 \equiv 14\ (mod\ 26)$$
$$C(0) \equiv 0-5 \equiv -5\ (mod\ 26)$$
$$C(9) \equiv 9-5 \equiv 4\ (mod\ 26)$$
$$C(22) \equiv 22-5 \equiv 17\ (mod\ 26)$$
$$C(18) \equiv 18-5 \equiv 13\ (mod\ 26)$$
$$C(5) \equiv 5-5 \equiv 0\ (mod\ 26)$$
$$C(17) \equiv 17-5 \equiv 12\ (mod\ 26)$$
$$C(19) \equiv 19-5 \equiv 14\ (mod\ 26)$$
$$C(17) \equiv 17-5 \equiv 12\ (mod\ 26)$$
$$C(25) \equiv 25-5 \equiv 20\ (mod\ 26)$$
$$C(18) \equiv 18-5 \equiv 13\ (mod\ 26)$$
$$C(8) \equiv 8-5 \equiv 3\ (mod\ 26)$$
$$C(19) \equiv 19-5 \equiv 14\ (mod\ 26)$$

Notemos que $-5 \equiv 21\ (mod\ 26)$, consequentemente $C(0) \equiv 21\ (mod\ 26)$ por transitividade.

Assim, temos

$$14-18\,//\,13-20-12-4-17-14-18\,//\,6-14-21-4-17-13-0-12\,//$$
$$14\,//\,12-20-13-3-14.$$

E com o uso da Tabela 3.2 temos a mensagem decodificada:

"Os números governam o mundo".

3.2.4 Criptografia RSA

Esta seção será dedicada a um breve estudo sobre a criptografia RSA.

Pré-codificação

Ao utilizarmos o método RSA para codificar uma mensagem, devemos a princípio converter a mensagem dada em uma sequência de números, processo já conhecido por pré-codificação. Para facilitar o entendimento deste método, vamos considerar a mensagem original como um texto contendo apenas palavras. Sendo assim, a mensagem será formada apenas pelas letras que compõem as palavras e os espaços entre as mesmas.

Consideremos a seguinte tabela.

Tabela 3.3: Pré-codificação para o método RSA

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

Fonte: Autoria própria.

Ao fazer a conversão, tomaremos o número 66 para representar o espaço entre as palavras.

Exemplo 3.12. *A frase "AMIZADE SECRETA" será convertida no seguinte número*

$$10221835101314662814122714 2910$$

Observemos que, na Tabela 3.3 a pré-codificação tem início com o número 10, cujo intuito é de evitar ambiguidades, ou seja, caso utilizássemos uma tabela de pré-codificação

onde a letra C correspondesse ao número 2, e a letra D ao número 3, não saberíamos ao certo se o número 23 por exemplo, representaria CD ou somente a letra X.

Antes de darmos continuidade ao método RSA, devemos definir os parâmetros desse sistema. Tais parâmetros denominaremos por p e q, sendo ambos dois números primos distintos e tomemos $n = pq$. Além disso, para finalizarmos o processo de pré-codificação devemos dividir o grande número formado no procedimento da conversão em blocos, sendo que cada bloco deverá ser menor do que n.

Exemplo 3.13. *Consideremos a mensagem*

$$10221835101314662814122714 2910.$$

do Exemplo 3.12. Vamos supor que $p = 11$ *e* $q = 17$. *Daí,* $n = 11 \cdot 17 = 187$. *Logo, a mensagem pode ser quebrada nos blocos:*

$$10 - 22 - 18 - 35 - 101 - 31 - 46 - 62 - 81 - 41 - 22 - 71 - 42 - 91 - 0.$$

Vale ressaltar que a forma de quebrar uma mensagem não é única. Por isso, deve-se evitar que o bloco inicie com o número 0 para evitar problemas no processo de decodificação.

Codificação

Após o processo de pré-codificação, inicia-se o de codificação e para isto, precisamos do par (n, e) denominado de chave pública de codificação do sistema RSA. Consideraremos $n = pq$, $m = (p-1)(q-1)$ e e um inteiro positivo que seja inversível módulo m, isto é, $mdc(e, m) = 1$.

Do processo de pré-codificação, obtemos uma sequência de números em blocos. Cada bloco será codificado separadamente e assim permanecerão para que seja possível a decodificação dos mesmos.Vejamos agora como ocorre a codificação de cada bloco. Denominaremos determinado bloco por b. E como já vimos, b deve ser um inteiro positivo menor do que n. Assim, codificaremos cada bloco b pela seguinte expressão:

$$C(b) \equiv b^e \ (mod\ n), \tag{3.4}$$

onde $C(b) =$ resto da divisão de b^e por n, corresponde a codificação do bloco b.

Retomemos agora ao Exemplo 3.13, onde $p = 11$, $q = 17$ e $n = 187$. Além disso, $m = (11-1)(17-1) = 10 \cdot 16 = 160$. Devemos ainda encontrar o valor do inteiro e. Notemos que, o menor valor possível para e é 3, já que este é o menor inteiro primo que não divide m. Deste

modo, temos que $mdc(3,160) = 1$. Logo, a chave pública que deverá ser utilizada é $(3,160)$. Do Exemplo 3.13, temos a seguinte mensagem pré-codificada e separada em blocos

$$10 - 22 - 18 - 35 - 101 - 31 - 46 - 62 - 81 - 41 - 22 - 71 - 42 - 91 - 0.$$

Codificaremos agora, cada um desses blocos utilizando a expressão (3.4). Temos:

$C(10) = 65$, pois $10^3 \equiv 65\ (mod\ 187)$;
$C(22) = 176$, pois $22^3 \equiv 176\ (mod\ 187)$;
$C(18) = 35$, pois $18^3 \equiv 35\ (mod\ 187)$;
$C(35) = 52$, pois $35^3 \equiv 52\ (mod\ 187)$;
$C(101) = 118$, pois $101^3 \equiv 118\ (mod\ 187)$;
$C(31) = 58$, pois $31^3 \equiv 58\ (mod\ 187)$;
$C(46) = 96$, pois $46^3 \equiv 96\ (mod\ 187)$;
$C(62) = 90$, pois $62^3 \equiv 90\ (mod\ 187)$;
$C(81) = 174$, pois $81^3 \equiv 174\ (mod\ 187)$;
$C(41) = 105$, pois $41^3 \equiv 105\ (mod\ 187)$;
$C(22) = 176$, pois $22^3 \equiv 176\ (mod\ 187)$;
$C(71) = 180$, pois $71^3 \equiv 180\ (mod\ 187)$;
$C(42) = 36$, pois $42^3 \equiv 36\ (mod\ 187)$;
$C(91) = 148$, pois $91^3 \equiv 148\ (mod\ 187)$;
$C(0) = 0$, pois $0^3 \equiv 0\ (mod\ 187)$.

Portanto, a mensagem codificada obtida é:

$$65 - 176 - 35 - 52 - 118 - 58 - 96 - 90 - 174 - 105 - 176 - 180 - 36 - 148 - 0.$$

Decodificação

Conhecendo o processo de codificação de uma mensagem por meio do sistema RSA, podemos prosseguir nossos estudos, agora com o desenvolvimento do processo de decodificação.

Para decodificarmos uma mensagem precisamos de dois números: n e d, em que d é o inverso de e módulo m, isto é, $ed \equiv 1\ (mod\ m)$, com $m = (p-1)(q-1)$. Assim, o par (n,d) será a chave de decodificação do sistema RSA. Desta forma, a decodificação de cada bloco b da mensagem codificada, denotada por $D(b)$ será feita por meio da seguinte expressão:

$$D(b) \equiv b^d\ (mod\ n) \tag{3.5}$$

onde $D(b)$ é o resto da divisão de b^d por n. Voltaremos ao Exemplo 3.13 para explanar o processo de decodificação.

Exemplo 3.14. *No Exemplo 3.13 temos $n = 187$, $e = 3$ e $m = 160$. Usaremos tais informações para decodificar cada bloco da mensagem codificada neste mesmo exemplo.*

Inicialmente, devemos determinar d por meio da congruência

$$ed \equiv 1 \ (mod\ m) \Longrightarrow 3d \equiv 1 \ (mod\ 160).$$

Daí, obtemos $3d - 1 = 160k \Rightarrow 3d - 160k = 1$, $k \in \mathbb{Z}$. Nos cabe agora encontrar uma solução particular da equação diofantina:

$$3d - 160k = 1, \tag{3.6}$$

com $k \in \mathbb{Z}$. Observemos que $mdc(3, 160) = 1$ e que $1|1$, isto implica que a equação (3.6) possui solução. Aplicando o Algoritmo de Euclides, temos

$$\begin{aligned} 160 &= 3 \cdot 53 + 1 \\ 3 &= 1 \cdot 2 + 1 \\ 1 &= 1 \cdot 1 + 0. \end{aligned}$$

Pela Identidade de Bezout iremos obter

$$\begin{aligned} 1 &= 3 - 1 \cdot 2 \\ &= 3 - (160 - 3 \cdot 53) \cdot 2 \\ &= 3 - 160(2) + 3(106) \\ &= 3(107) - 160(2). \end{aligned}$$

Logo, $d = 107$ e $k = 2$ é uma solução particular da equação (3.6) e sendo $d = 107$, podemos iniciar o processo de decodificaçao de cada bloco b usando a expressão

$$D(b) \equiv b^{107} \ (mod\ 160).$$

Assim,

$D(65) = 10$, pois $65^{107} \equiv 10 \ (mod\ 187)$;
$D(176) = 22$, pois $176^{107} \equiv 22 \ (mod\ 187)$;

$D(35) = 18$, pois $35^{107} \equiv 18\ (mod\ 187)$;

$D(52) = 35$, pois $52^{107} \equiv 35\ (mod\ 187)$;

$D(118) = 101$, pois $118^{107} \equiv 101\ (mod\ 187)$;

$D(58) = 31$, pois $58^{107} \equiv 31\ (mod\ 187)$;

$D(96) = 46$, pois $96^{107} \equiv 46\ (mod\ 187)$;

$D(90) = 62$, pois $90^{107} \equiv 62\ (mod\ 187)$;

$D(174) = 81$, pois $174^{107} \equiv 81\ (mod\ 187)$;

$D(105) = 41$, pois $105^{107} \equiv 41\ (mod\ 187)$;

$D(176) = 22$, pois $176^{107} \equiv 22\ (mod\ 187)$;

$D(180) = 71$, pois $180^{107} \equiv 71\ (mod\ 187)$;

$D(36) = 42$, pois $36^{107} \equiv 42\ (mod\ 187)$;

$D(148) = 91$, pois $148^{107} \equiv 91\ (mod\ 187)$;

$D(0) = 0$, pois $0^{107} \equiv 0\ (mod\ 187)$.

Portanto, a mensagem decodificada obtida é

$$10221835101314662814122714291 0.$$

que representa a frase “AMIZADE SECRETA.”

Observação 3.2. *Os cálculos realizados anteriormente tanto no processo de codificação como no de decodificação, respectivamente, foram realizados com o auxílio da calculadora científica.*

Segurança do sistema RSA

Como já foi dito, a RSA é um sistema de chave pública que consiste nos parâmetros p e q aqui utilizados e $n = pq$, além do par (n, e) que corresponde a chave pública de codificação do sistema, sendo esta acessível a qualquer pessoa. Neste sentido, para que se possa decodificar uma mensagem conhecendo apenas n e e, basta fatorar n para encontrar os valores de p e q que serão utilizados para calcular d. Isto parece muito fácil, porém não o é, pois para encontrarmos o valor de d precisamos aplicar o Algoritmo de Euclides aos elementos m e e. Mas, só será possível calcular m se n for fatorado para obtermos p e q, o que é um problema se n for um número grande (acima de 200 algarismos), já que “não existe nenhum algoritmo conhecido capaz de fatorar inteiros grandes de modo realmente eficiente.”(COUTINHO, 2015, p.157).

Portanto, quebrar o código RSA é tão difícil quanto fatorar n, o que faz com que esse método criptográfico seja considerado seguro.

3.3 Dígitos de verificação

Dígitos de verificação (DV) consistem em números que são geralmente o(s) último(s) algarismo(s) de uma sequência numérica de identificação de CPF, RG, código de barras, entre outros códigos que requerem maior segurança.

Os dígitos de verificação são utilizados para certificar a validade e autenticidade de um código, evitando desta forma possíveis fraudes. Os DV são determinados por meio de congruência modular, mais precisamente pelo uso do módulo 10 ou 11.

Apresentaremos a seguir, dois casos de dígitos de verificação empregados como identificadores.

3.3.1 Cartão de Crédito

Os cartões de crédito predominantes no mundo são constiuídos por números de 14 a 19 dígitos. Os primeiros 4 dígitos definem o banco emissor, sendo que o primeiro desses define a rede emissora. Os cartões de crédito VISA e MASTERCARD por exemplo, começam por 4 e 5, respectivamente. O último dígito do número de identificação do cartão constitui o DV, este por sua vez, é obtido dos anteriores por meio de congruência módulo 10.

Em outras palavras, o dígito de verificação de qualquer cartão de crédito equivale ao número que faltar para completar um múltiplo de 10 com relação ao somatório do produto de cada número pela sequência $\{2,1,2,1,2,1,2,1,2,1,\ldots\}$.

Consideraremos os cartões VISA e MASTERCARD que possuem uma sequência numérica de 16 dígitos e que podemos expressar matematicamente por:

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

sendo $a_i \in \mathbb{Z}, \quad 0 \leq a_i \leq 9$ e $i \in \{1,2,3,\ldots,16\}$. Logo, o dígito de verificação é definido pela congruência:

$$(S + a_{16}) \equiv 0 \ (mod\ 10) \ \ ou \ \ a_{16} \equiv -S \ (mod\ 10), \tag{3.7}$$

com

$$S = \sum_{i=1}^{8} (x_{(2i-1)} + a_{2i})$$

de modo que

$$x_j = \begin{cases} 2a_j, \ se\ 2a_j \leq 9; \\ 2a_j - 9, \ se\ 2a_j > 9. \end{cases}$$

sendo j ímpar, $0 \leq j \leq 16$.

Exemplo 3.15. *Suponhamos que o número* 468352179045726 *seja de um cartão de crédito VISA. Vamos determinar o dígito de verificação que o corresponde.*

Inicialmente iremos determinar S, ou seja,

$$S = \sum_{i=1}^{8} [x_{(2i-i)} + a_{2i}] = (x_1 + a_2) + (x_3 + a_4) + \cdots + (x_{15} + a_{16}).$$

Mas, antes disso determinaremos os x_j.

$$\begin{aligned}
x_1 &= 2 \cdot a_1 = 2 \cdot 4 = 8 < 9 \Longrightarrow x_1 = 8 \\
x_3 &= 2 \cdot a_3 = 2 \cdot 8 = 16 > 9 \Longrightarrow x_3 = 16 - 9 = 7 \\
x_5 &= 2 \cdot a_5 = 2 \cdot 5 = 10 > 9 \Longrightarrow x_5 = 10 - 9 = 1 \\
x_7 &= 2 \cdot a_7 = 2 \cdot 1 = 2 < 9 \Longrightarrow x_7 = 2 \\
x_9 &= 2 \cdot a_9 = 2 \cdot 9 = 18 > 9 \Longrightarrow x_9 = 18 - 9 = 9 \\
x_{11} &= 2 \cdot a_{11} = 2 \cdot 4 = 8 < 9 \Longrightarrow x_{11} = 8 \\
x_{13} &= 2 \cdot a_{13} = 2 \cdot 7 = 14 > 9 \Longrightarrow x_{13} = 14 - 9 = 5 \\
x_{15} &= 2 \cdot a_{15} = 2 \cdot 6 = 12 > 9 \Longrightarrow x_{15} = 12 - 9 = 3.
\end{aligned}$$

Assim, temos que

$$S = 8 + 6 + 7 + 3 + 1 + 2 + 2 + 7 + 9 + 0 + 8 + 5 + 5 + 2 + 3 + a_{16},$$

isto é, $S = 68 + a_{16}$. Logo, por (3.7), $68 + a_{16} \equiv 0 \ (mod\ 10)$ ou ainda, $a_{16} \equiv -68 \ (mod\ 10)$. Como $-68 \equiv 2 \ (mod\ 10)$, temos que $a_{16} \equiv 2 \ (mod\ 10)$ por transitividade. Portanto, $a_{16} = 2$.

Exemplo 3.16. *Vamos averiguar se o número* 5108260945382357 *equivale a um cartão de crédito da MASTERCARD.*

Notemos que $a_1 = 5$, isto significa que este cartão pode ser da MASTERCARD. Nos resta agora, verificar se o dígito de verificação está correto, ou seja, se $a_{16} = 7$. Determinaremos de início, os valores de cada x_j. Vejamos:

$$\begin{aligned}
x_1 &= 2 \cdot a_1 = 2 \cdot 5 = 10 > 9 \Longrightarrow x_1 = 10 - 9 = 1 \\
x_3 &= 2 \cdot a_3 = 2 \cdot 0 = 0 < 9 \Longrightarrow x_3 = 0 \\
x_5 &= 2 \cdot a_5 = 2 \cdot 2 = 4 < 9 \Longrightarrow x_5 = 4
\end{aligned}$$

$$x_7 = 2 \cdot a_7 = 2 \cdot 0 = 0 < 9 \Longrightarrow x_7 = 0$$

$$x_9 = 2 \cdot a_9 = 2 \cdot 4 = 8 < 9 \Longrightarrow x_9 = 8$$

$$x_{11} = 2 \cdot a_{11} = 2 \cdot 3 = 6 < 9 \Longrightarrow x_{11} = 6$$

$$x_{13} = 2 \cdot a_{13} = 2 \cdot 2 = 4 < 9 \Longrightarrow x_{13} = 4$$

$$x_{15} = 2 \cdot a_{15} = 2 \cdot 5 = 10 > 9 \Longrightarrow x_{15} = 10 - 9 = 1.$$

Encontrados os valores de cada x_j, calcularemos o valor de S, a seguir

$$S = \sum_{i=1}^{8} [x_{(2i-i)} + a_{2i}] = (x_1 + a_2) + (x_3 + a_4) + \cdots + (x_{15} + a_{16}).$$

Assim,

$$S = 1 + 1 + 0 + 8 + 4 + 6 + 0 + 9 + 8 + 5 + 6 + 8 + 4 + 3 + 1 + 7 = 71.$$

Logo, por (3.7) $S + a_{16} = 71 + 7 = 78 \not\equiv 0 \ (mod\ 10)$ e portanto, o número 5108260945382357 não é autêntico.

3.3.2 Cadastro de Pessoas Físicas

O Cadastro de Pessoas Físicas (CPF) é o registro de qualquer pessoa na Receita Federal do Brasil, o mesmo contém diversas informações, muitas vezes fornecidas por nós e outras pelo próprio sistema da Receita Federal. O número de todo CPF é constituído por uma sequência de 11 digítos, que podem ser expressos por

$$a_1 a_2 a_3 . a_4 a_5 a_6 . a_7 a_8 a_9 - a_{10} a_{11},$$

sendo $a_i \in \mathbb{Z}$, de tal modo que $0 \leq a_i \leq 9$ e $i \in \{1, 2, 3, \ldots, 11\}$.

Os oito primeiros digítos são denominados de números base, o nono denota a região fiscal e os dois últimos são os dígitos de verificação do CPF. Ambos os dígitos de verificação são determinados por meio de congruência módulo 11. Neste caso, o primeiro DV equivale ao resto da divisão por 11 do somatório do produto de cada algarismo respectivamente por $1, 2, 3, 4, 5, 6, 7, 8, 9$.

Em notação de congruência, isto significa que

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

com $S \in \mathbb{Z}$, determinado por $\sum_{i=1}^{9} (i \cdot a_i)$.

Observação 3.3. *Quando o resto da divisão de S ou $\bar{S}$ por 11 for 10, considera-se sempre zero (0).*

O segundo DV é obtido por meio de outra congruência modular de forma análoga ao primeiro, mas considerando agora o primeiro DV encontrado e, estendendo a base de multiplicação para $0,1,2,3,4,5,6,7,8,9$.

Teremos a seguinte notação

$$a_{11} \equiv \bar{S} \ (mod\ 11),$$

com $\bar{S} \in \mathbb{Z}$ definido por $\sum_{i=1}^{10}(i-1)\cdot a_i$.

Exemplo 3.17. *Vamos determinar os dígitos de verificação de um CPF que tem como número* $094.994.864 - a_{10}a_{11}$.

Para determinar o primeiro DV, devemos ter

$$S = \sum_{i=1}^{9}(i\cdot a_i) = 1a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6 + 7a_7 + 8a_8 + 9a_9,$$

ou seja,

$$S = \sum_{i=1}^{9}(i\cdot a_i) = 1\cdot 0 + 2\cdot 9 + 3\cdot 4 + 4\cdot 9 + 5\cdot 9 + 6\cdot 4 + 7\cdot 8 + 8\cdot 6 + 9\cdot 4 = 275.$$

Como $a_{10} \equiv S \ (mod\ 11)$, temos que $a_{10} \equiv 275 \ (mod\ 11)$. Mas, $275 \equiv 0 \ (mod\ 11)$. Por transitividade, $a_{10} \equiv 0 \ (mod\ 11)$. Portanto, $a_{10} = 0$.

Vamos agora determinar o a_{11} que é o segundo dígito de verificação. Procederemos de forma análoga a determinação do primeiro dígito, que será agora acrescentado ao número base. Temos que

$$\bar{S} = \sum_{i=1}^{10}(i-1)\cdot a_i = 0a_1 + 1a_2 + 2a_3 + 3a_4 + 4a_5 + 5a_6 + 6a_7 + 7a_8 + 8a_9 + 9a_{10}.$$

Daí,

$$\bar{S} = \sum_{i=1}^{10}(i-1)\cdot a_i = 0\cdot 0 + 1\cdot 9 + 2\cdot 4 + 3\cdot 9 + 4\cdot 9 + 5\cdot 4 + 6\cdot 8 + 7\cdot 6 + 8\cdot 4 + 9\cdot 0 = 222.$$

Logo, $a_{11} \equiv 222 \ (mod\ 11)$. E portanto, $a_{11} \equiv 2 \ (mod\ 11)$. Concluímos então que, o número completo do CPF é $094.994.864 - 02$.

Exemplo 3.18. *Vamos verificar se o número* $080.990.754 - 21$ *corresponde ao número de um CPF.*

Iremos inicialmente verificar se o primeiro dígito de verificação (a_{10}), está correto. Temos,

$$S = \sum_{i=1}^{9} (i \cdot a_i) = 1 \cdot 0 + 2 \cdot 8 + 3 \cdot 0 + 4 \cdot 9 + 5 \cdot 9 + 6 \cdot 0 + 7 \cdot 7 + 8 \cdot 5 + 9 \cdot 4 = 222.$$

Devemos ter,

$$a_{10} \equiv S \ (mod\ 11) \Longrightarrow a_{10} \equiv 222 \ (mod\ 11).$$

Mas, $222 \equiv 2 \ (mod\ 11)$, por transitividade segue que $a_{10} \equiv 2 \ (mod\ 11)$. Isto confirma a validade do primeiro DV.

Vamos verificar agora a validade do segundo DV (a_{11}). Temos,

$$\bar{S} = \sum_{i=1}^{10} (i-1) \cdot a_i = 0 \cdot 0 + 1 \cdot 8 + 2 \cdot 0 + 3 \cdot 9 + 4 \cdot 9 + 5 \cdot 0 + 6 \cdot 7 + 7 \cdot 5 + 8 \cdot 4 + 9 \cdot 2 = 198.$$

Devemos ter,

$$a_{11} \equiv \bar{S} \ (mod\ 11) \Longrightarrow a_{11} \equiv 198 \ (mod\ 11).$$

Como $198 \equiv 0 \ (mod\ 11)$ segue que, $a_{11} \equiv 0 \ (mod\ 11)$. Portanto, o número dado não corresponde a um número de CPF.

3.4 Calendário

Desde a pré-história, o homem empenhou-se em registrar a passagem do tempo de diferentes formas, as quais foram evoluindo até a invenção do calendário, que constitui um sistema de contagem que representa o passar dos dias, sendo estes agrupados em semanas, meses, anos entre outros, de acordo com a cultura de cada civilização. Atualmente existem diferentes calendários utilizados no mundo inteiro, e que são classificados como solares, lunares e lunisolares. Daremos ênfase aos calendários solares, em especial, ao calendário Gregoriano, que é o mais usado e que utilizam o dia como unidade de contagem do tempo.

De acordo com Koshy (2007) o calendário Gregoriano foi estabelecido pelos astrônomos Fr.Cristopher Clavius e Aloysius Giglio em 1582 a pedido do Papa Gregório XIII, sendo o mesmo uma forma do calendário Juliano. No calendário Gregoriano, tem-se um agrupamento de dias em 12 meses, estes constituídos por 30 ou 31 dias, com exceção do mês de Fevereiro que possui 28 ou 29 dias quando o ano é bissexto. Esse tipo de calendário deriva do calendário solar que tem duração de 365,2425 dias por ano, que correspondem a 365 dias, 5 horas, 48 min e 47 segundos.

Por praticidade, o calendário Gregoriano considera exatamente 365 dias para o período de um ano, o que causa uma diferença do ano solar equivalente a 0,2425 dia, que somados a cada 4 anos resultam em 0,97 dia. Por consequência, tem-se a cada 4 anos um acréscimo de 1 dia no mês de Fevereiro que representa o chamado ano bissexto, composto por 366 dias. Este acréscimo provoca um erro de 3 dias a cada 10.000 anos e para corrigí-lo foram estabelecidas as seguintes regras (KOSHY, 2007):

- Qualquer ano divisível por 4 é bissexto;
- Qualquer ano divisível por 100 e não divisível por 400, não é bissexto;
- Qualquer ano divisível por 400 é bissexto.

Neste sentido, o primeiro ano bissexto após a inclusão do calendário Gregoriano ocorreu em 1600. Por isso, iremos considerar anos a partir de 1600.

Vamos a seguir, desenvolver uma fórmula que nos permite determinar o dia da semana para qualquer data independente do ano. Como os dias da semana se repetem a cada sete dias, devemos utilizar congruência módulo 7. Antes disso, façamos cada um dos dias da semana denominados por Domingo, Segunda-feira, Terça-feira, Quarta-feira, Quinta-feira, Sexta-feira e Sábado, corresponder a um número entre 0 e 6 de acordo com a tabela abaixo:

Tabela 3.4: Dias da semana

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

Fonte: Autoria Própria.

Além disso, faremos alguns ajustes nos meses, já que Fevereiro possui 28 ou 29 dias. Assim, consideraremos Março como o primeiro mês do ano, Abril o segundo e daí por diante, sendo que os meses de Janeiro e Fevereiro serão considerados como $11^{\underline{o}}$ e $12^{\underline{o}}$ meses do ano que se passou. A partir desses ajustes, podemos determinar qualquer dia da semana para datas posteriores a $1^{\underline{o}}$ de Março de 1600, que é nossa data base.

Seja $D_N \in \{0,1,2,3,4,5,6\}$ o número que denota o dia da semana correspondente a 1^{o} de Março do ano N, sendo $N \geq 1600$. Como $365 \equiv 1 \ (mod\ 7)$, para N não bissexto, tem-se um deslocamento de 1 dia em relação aos dias da semana. E para N bissexto, o deslocamento será de 2 dias, já que todo ano bissexto contém 366 dias, assim $366 \equiv 2 \ (mod\ 7)$. Em termos matemáticos isto significa que:

- $D_N \equiv D_N + 1 \ (mod\ 7)$, se N não for bissexto.
- $D_N \equiv D_N + 2 \ (mod\ 7)$, se N for bissexto.

Com isso, podemos determinar que dia da semana será 1^{o} de Março de qualquer ano $N \geq 1600$. Mas antes, precisamos determinar quantos foram os anos bissextos e quantos anos se passaram no período de 1600 a N.

Vamos supor que $Z = N - 1600$, sendo Z o total de anos passados entre 1600 e N. Logo, podemos calcular a quantidade de anos bissextos entre 1600 e o ano desejado pela seguinte expressão:

$$W = \frac{Z}{4} - \frac{Z}{100} + \frac{Z}{400},$$

em que $\frac{Z}{n}$ representa o número de múltiplos de n entre 1600 e N, para $n = 4, 100$ e 400.

Desta forma, podemos concluir que

$$D_N \equiv (D_{1600} + Z + W) \ (mod\ 7). \tag{3.8}$$

Exemplo 3.19. *Determinar que dia da semana foi 1^{o} de Março de 1600.*

Consideremos o calendário de Março de 2017 (abaixo). Observemos que 1^{o} de Março é uma quarta-feira.

Figura 3.2: Calendário: Março de 2017

Março 2017

Segunda	Terça	Quarta	Quinta	Sexta	Sábado	Domingo
		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		

Fonte: ABC - Calendário

Deste modo, $D_{2017} = 3$ de acordo coma a Tabela 3.4. Temos ainda que,

$$\begin{aligned} Z &= 2017 - 1600 = 417; \\ W &= \frac{417}{4} - \frac{417}{100} + \frac{417}{400} = 104 - 4 + 1 = 101. \end{aligned}$$

Assim,

$$\begin{aligned} D_{2017} &\equiv (D_{1600} + Z + W)(mod\ 7); \\ 3 &\equiv (D_{1600} + 417 + 101)(mod\ 7). \end{aligned}$$

Pela Proposição 2.3, temos que

$$-515 \equiv D_{1600}\ (mod\ 7).$$

Como $-515 \equiv 3\ (mod\ 7)$, temos por transitividade que $D_{1600} \equiv 3\ (mod\ 7)$. Logo $D_{1600} = 3$, ou seja, $1^{\underline{o}}$ de Março foi uma quarta-feira.

Observação 3.4. *Como $D_{1600} = 3$, temos que*

$$D_N \equiv (3 + Z + W)(mod\ 7).$$

Vimos até agora como determinar o dia da semana de $1^{\underline{o}}$ de Março de qualquer ano. Determinaremos a seguir, que dia da semana será um dia qualquer de Março de um certo ano $N \geq 1600$.

Seja y o dia que será escolhido para determinarmos o dia da semana equivalente ao mesmo. Para tal, devemos verificar a quantidade de deslocamentos sofridos por este dia em relação ao dia $1^{\underline{o}}$ de Março do ano em questão. Como $1^{\underline{o}}$ de Março de 1600 foi uma quarta-feira, consequentemente dia 2 foi uma quinta-feira, ou seja, houve um deslocamento de apenas um dia na semana.

Assim, podemos dizer que para qualquer dia do mês de Março que for escolhido, o deslocamento dos dias da semana relacionados a $1^{\underline{o}}$ de Março do ano N será de $y - 1$ dias e seja $X = y - 1$, a expressão que representa o número deste deslocamento.

Consideremos $D \in \{0, 1, 2, 3, 4, 5, 6\}$ o número que corresponde ao dia da semana, agora de um dia (y) qualquer do mês de Março do ano N de acordo com a Tabela (3.4).Vamos determinar uma forma de definí-lo. Observemos que,

$$(D - D_N) \equiv X\ (mod\ 7).$$

De fato, pois $X \in \{0, 1, 2, \ldots, 28, 29, 30\}$.

- Para $X = 0, 7, 14, 21$ ou 28, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano equivalem ao mesmo dia da semana. Assim, $D = D_N$, isto implica que $D - D_N = 0$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 1, 8, 15, 22$ ou 29, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 1 dia em relação aos dias da semana. Assim, $D = D_N + 1$, isto implica que $D - D_N = 1$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 2, 9, 16, 23$ ou 30, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 2 dias em relação aos dias da semana. Assim, $D = D_N + 2$, isto implica que $D - D_N = 2$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 3, 10, 17$ ou 24, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 3 dias em relação aos dias da semana. Assim, $D = D_N + 3$, isto implica que $D - D_N = 3$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 4, 11, 18$ ou 25, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 4 dias em relação aos dias da semana. Assim, $D = D_N + 4$, isto implica que $D - D_N = 4$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 5, 12, 19$ ou 26, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 5 dias em relação aos dias da semana. Assim, $D = D_N + 5$, isto implica que $D - D_N = 5$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

- Para $X = 6, 13, 20$ ou 27, o dia y de Março do ano N qualquer e $1^{\underline{o}}$ de Março do mesmo ano se diferenciam em 6 dias em relação aos dias da semana. Assim, $D = D_N + 6$, isto implica que $D - D_N = 6$. Logo, $D - D_N \equiv X \ (mod\ 7)$.

Sabendo que $D_{1600} = 3$, pela equação (3.8), temos que $D_N \equiv (3 + Z + W)(mod\ 7)$ além disso, $D - D_N \equiv X \ (mod\ 7)$. Pela Proposição 2.4, temos que $D \equiv (3 + Z + W + X)(mod\ 7)$, que é a expressão que devemos utilizar para determinar que dia da semana corresponde a qualquer dia do mês de Março de algum ano N.

Exemplo 3.20. *Vamos determinar que dia da semana equivale ao dia 10 de Março de 2020.*

Temos que,

$$\begin{aligned} Z &= 2020 - 1600 = 420; \\ W &= \frac{420}{4} - \frac{420}{100} + \frac{420}{400} = 105 - 4 + 1 = 102. \end{aligned}$$

Sabendo que $y = 10$, temos que $X = 10 - 1 = 9$. Daí, $D \equiv (3 + 420 + 102 + 9)(mod\ 7)$, isto é, $D \equiv 534\ (mod\ 7)$. Como $534 \equiv 2\ (mod\ 7)$, temos que $D = 2$. Logo 10 de Março de 2020 será numa terça-feira. Vejamos o calendário abaixo.

Figura 3.3: Calendário: Março de 2020

Fonte: ABC - Calendário

Determinaremos agora o dia da semana para qualquer data a partir da data base (1^{o} de Março de 1600). Consideraremos antes, algumas observações importantes: os meses possuem 28, 30 ou 31 dias, com exceção dos anos bissextos nos quais o mês de fevereiro possui 29 dias. Por não possuirem a mesma quantidade de dias acabam gerando um deslocamento nos dias da semana do mês seguinte. Em outras palavras, se todos os meses do ano fossem constituídos por 28 dias e, sabendo que $28 \equiv 0\ (mod\ 7)$, teríamos que todos os meses iniciariam no mesmo dia da semana, mas como isso não ocorre, temos para os meses com 30 dias que o deslocamento será de 2 dias para o mês seguinte, pois $30 \equiv 2\ (mod\ 7)$. Já para os meses com 31 dias, o deslocamento será de exatamente 3 dias, visto que, $31 \equiv 3\ (mod\ 7)$.

Vamos encontrar o deslocamento nos dias da semana produzidos por cada mês.

Seja $T \in \{0,1,2,3,4,5,6\}$, o número que corresponde ao dia da semana de qualquer data, após Março de 1600. Como o deslocamento dos dias da semana de Março para Abril é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$, então para *Abril* temos que,

$$T \equiv (D + 3)(mod\ 7).$$

Sabendo que de Abril para Maio o deslocamento dos dias da semana é de 2 dias, uma vez que, $30 \equiv 2\ (mod\ 7)$ e que estes adicionados aos 3 dias que já foram acumulados em Abril, provocarão um deslocamento de 5 dias nos dias da semana de Maio, temos para *Maio* que,

$$T \equiv (D + 5)(mod\ 7).$$

Agora, sabendo que de Maio para Junho o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 5 dias que já foram acumulados

em Maio, provocarão um deslocamento de 8 dias nos dias da semana de Junho. Assim, $T \equiv (D+8)(mod\ 7)$, mas $8 \equiv 1\ (mod\ 7)$. Portanto, temos para *Junho* que

$$T \equiv (D+1)(mod\ 7).$$

Já que de Junho para Julho o deslocamento dos dias da semana é de 2 dias, uma vez que, $30 \equiv 2\ (mod\ 7)$ e que estes adicionados a 1 dia acumulado em junho provocarão um deslocamento de 3 dias nos dias da semana de Julho. Portanto, temos para *Julho* que

$$T \equiv (D+3)(mod\ 7).$$

Como de Julho para Agosto o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 3 dias acumulados em Julho, provocarão um deslocamento de 6 dias nos dias da semana de Agosto. Portanto, temos para *Agosto* que

$$T \equiv (D+6)(mod\ 7).$$

Sabendo ainda que de Agosto para Setembro o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 3 dias acumulados em Agosto, provocarão um deslocamento de 9 dias nos dias da semana de Setembro. Assim, $T \equiv (D+9)(mod\ 7)$, mas $9 \equiv 2\ (mod\ 7)$. Portanto, temos para *Setembro* que

$$T \equiv (D+2)(mod\ 7).$$

Como de Setembro para Outubro o deslocamento dos dias da semana é de 2 dias, uma vez que, $30 \equiv 2\ (mod\ 7)$ e que estes adicionados aos 2 dias acumulados em Setembro, provocarão um deslocamento de 4 dias nos dias da semana de Outubro. Portanto, temos para *Outubro* que

$$T \equiv (D+4)(mod\ 7).$$

Já que de Outubro para Novembro o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 4 dias acumulados em Outubro, provocarão um deslocamento de 7 dias nos dias da semana de Outubro. Assim para *Novembro* $T \equiv (D+7)(mod\ 7)$, mas $7 \equiv 0\ (mod\ 7)$. Portanto, temos que

$$T \equiv (D+0)(mod\ 7).$$

De Novembro para Dezembro o deslocamento dos dias da semana é de 2 dias, uma vez que, $30 \equiv 2\ (mod\ 7)$ e que estes provocarão um deslocamento de apenas 2 dias nos dias da semana de Dezembro, já que o mês anterior não sofreu nenhum deslocamento. Portanto, temos para *Dezembro* que

$$T \equiv (D+2)(mod\ 7).$$

Como fizemos anteriormente alguns ajustes nos meses, considerando que Março seria o primeiro mês do ano, temos que Janeiro virá depois de Dezembro. Assim, sabendo que de Dezembro para Janeiro o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 2 dias acumulados em Dezembro, provocarão um deslocamento de 5 dias nos dias da semana de Janeiro. Portanto, temos para *Janeiro* que

$$T \equiv (D+5)(mod\ 7).$$

Agora, sabendo que de Janeiro para Fevereiro o deslocamento dos dias da semana é de 3 dias, uma vez que, $31 \equiv 3\ (mod\ 7)$ e que estes adicionados aos 5 dias acumulados em Janeiro, provocarão um deslocamento de 8 dias nos dias da semana de Fevereiro. Assim para *Fevereiro*, $T \equiv (D+8)(mod\ 7)$. Mas $8 \equiv 1\ (mod\ 7)$. Portanto, temos que

$$T \equiv (D+1)(mod\ 7).$$

Para finalizarmos, sabendo que Fevereiro é composto por 28 dias nos anos não bissextos, e que $28 \equiv 0\ (mod\ 7)$, segue que o mês de Março terá um acúmulo de 1 dia. Se K corresponde ao deslocamento cumulativo dos dias da semana de mês após mês podemos concluir que $T \equiv (D+K)(mod\ 7)$, isto é,

$$T \equiv (3+Z+W+X+K)\ (mod\ 7).$$

Exemplo 3.21. *Vamos determinar que dia da semana equivale ao dia 25 de Dezembro de 2017.*

Temos que,

$$\begin{aligned} Z &= 2017-1600=417; \\ W &= \frac{417}{4}-\frac{417}{100}+\frac{417}{400}=104-4+1=101. \end{aligned}$$

Sabendo que $y=25$, temos que $X=25-1=24$. Além disso, $K=2$, já que o mês é Dezembro. Daí, $T \equiv (3+417+101+24+2)(mod\ 7)$, isto é, $T \equiv 547\ (mod\ 7)$. Como $547 \equiv 1\ (mod\ 7)$, temos que $T=1$. Logo 25 de Dezembro de 2017 será numa segunda-feira.

Vejamos o calendário de Dezembro de 2017 (abaixo) para comprovarmos tal afirmação.

Figura 3.4: Calendário: Dezembro de 2017

Fonte: ABC - Calendário

Exemplo 3.22. *Vamos determinar que dia da semana equivale ao dia 7 de Setembro (Independência do Brasil) de 2018.*

Temos que,

$$\begin{aligned} Z &= 2018 - 1600 = 418; \\ W &= \frac{418}{4} - \frac{418}{100} + \frac{418}{400} = 104 - 4 + 1 = 101. \end{aligned}$$

Sabendo que $y = 7$, temos que $X = 7 - 1 = 6$. Além disso, $K = 2$, já que o mês é Setembro. Daí, $T \equiv (3 + 418 + 101 + 6 + 2)(mod\ 7)$, isto é, $T \equiv 530\ (mod\ 7)$. Como $530 \equiv 5\ (mod\ 7)$, temos que $T = 5$. Logo 7 de Setembro de 2018 será numa sexta-feira. Observemos o calendário abaixo.

Figura 3.5: Calendário: Setembro de 2018

Fonte: ABC - Calendário

Exemplo 3.23. *Vamos determinar que dia da semana equivale ao dia 24 de Junho de 2020.*

Temos que,

$$\begin{aligned} Z &= 2020 - 1600 = 420; \\ W &= \frac{420}{4} - \frac{420}{100} + \frac{420}{400} = 105 - 4 + 1 = 102. \end{aligned}$$

Sabendo que $y = 24$, temos que $X = 24 - 1 = 23$. Além disso, $K = 1$, já que o mês é Junho. Daí, $T \equiv (3 + 420 + 102 + 23 + 1)(mod\ 7)$, isto é, $T \equiv 549\ (mod\ 7)$. Como $549 \equiv 3\ (mod\ 7)$, temos que $T = 3$. Logo 24 de Junho de 2020 será numa quarta-feira, como mostra o calendário a seguir.

Figura 3.6: Calendário: Junho de 2020

Fonte: ABC - Calendário

CONCLUSÃO

Ao término deste trabalho, pudemos perceber que há diversos estudos voltados para Teoria dos Números, com foco especial em congruência modular. Contudo, não é muito comum estudos sobre suas aplicações, que são inúmeras. Devido a essa carência, resolvemos expor por meio deste algumas de suas aplicações, nas quais a congruência atua de maneira simples e relevante, seja nos critérios de divisibilidade, cálculos envolvendo calendários, bem como na geração de dígitos de verificação de CPF e cartão de crédito e também no uso da criptografia.

Apresentados como uma aplicação de Congruência Modular, num âmbito social, os dígitos de verificação de CPF e cartão de crédito, assim como a criptografia RSA exercem grande importância na questão de segurança de informações pessoais e ao mesmo tempo no ramo da comunicação, que está presente constantemente no nosso dia a dia. O método de Criptografia RSA é atualmente o mais usado, pois garante não só a autenticação de quem a utiliza transmitindo informações pessoais de maneira segura, como também é indispensável em transações comerciais por ser um método considerado seguro.

Nesse sentido, a relevância deste trabalho se deve ao fato de mostrar o quanto a Teoria dos Números, mais especificamente a congruência modular está presente em nosso cotidiano e possibilita resolver problemas de maneira eficaz e interessante, sem precisar de cálculos complicados e repetitivos. Acreditamos assim, que este trabalho possa servir de referência para outros que pretendam desenvolver aplicações fundamentais para a Matemática.

Referências Bibliográficas

[1] ABC- CALENDARIO. Disponível em: <http://www.abc-calendario.pt/calendario-junho-2020/>. Acesso em 10 dez. 2016.

[2] BOYER, C.B. **História da Matemática**. São Paulo. Editora Edgard Blücher Ltda, 1974.

[3] CAVALCANTE, André L. B. **Teoria dos números e criptografia**.[2014?]. Disponível em: <http://www.ebah.com.br/content/ABAAAAayYAA/teoria-dos-numeros-criptografia>. Acesso em 09 dez. 2016.

[4] COUTINHO, S.C. **Criptografia.** 1ª ed. Rio de Janeiro: IMPA 2015. Disponível em: <http://www.obmep.org.br/docs/apostila7.pdf>. Acesso em 12 dez 2016.

[5] CRUZ, Edilson Fernandes da. **A criptografia e seu papel na segurança da informação e das comunicações (SIC) - retrospectiva, atualidade e perspectiva.** 2009. 84f. Monografia (Especialização em Gestão de Segurança da Informação e Comunicações) - Departamento de Ciência da Computação. Universidade de Brasília, Brasília.

[6] DOMINGUES, Hygino. e Gelson Iezzi. **Álgebra Moderna.** 2. ed. São Paulo: Atual, 1972.

[7] DOMINGUES, Hygino H. **Fundamentos de Aritmética.** São Paulo: Atual, 1991.

[8] ESQUINCA, Josiane Colombo Pedrini. **ARITMÉTICA:** CÓDIGOS DE BARRAS E OUTRAS APLICAÇÕES DE CONGRUÊNCIAS. 2013. 63f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Centro de Ciências Exatas e Tecnologias. Universidade Federal de Mato Grosso do Sul. Mato Grosso do Sul, 2013.

[9] FRANCO, Tânia Regina Rodrigues. **Divisibilidade e Congruências:** Aplicações no Ensino Fundamental II. 2016. 80f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Universidade Federal de Goiás, Goiás, 2016.

[10] FURLÃO. Disponível em: <http://www.furlao.com.br/blog/10-ideias-para-decorar-a-casa-para-o-reveillon/horario-de-verao-o-relogio-do-corpo-no/>. Acesso em 08 dez. 2016.

[11] GHIORZI, T. **Calendários Perpétuos.** Disponível em: <http://ghiorzi.org/caleperp.htm>. Acesso em 08 out. 2016.

[12] GHIORZI, T. **Dígitos de Verificação**. Disponível em: <http://ghiorzi.org/DVnew.htm>. Acesso em 08 de out. 2016.

[13] HEFEZ, Abramo. **Elementos de Aritmética**. 2. ed. Rio de Janeiro: SBM, 2005.

[14] IEZZI, Gelson; DOLCE, Osvaldo; MACHADO, Antonio. **Matemática e realidade**.6. ed. São Paulo: Atual, 2009.

[15] KOSHY, Thomas. **Elementary number theory with applications**. 2nd ed. USA. Academic Press: PA. 2007.

[16] LEOPOLD, Guilherme Liegell. **Congruência e Aplicações**. 2015. 63f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT) - Centro de Ciências Exatas. Universidade Estadual de Maringá, Paraná, 2015.

[17] MARQUES, Manuel Nunes. **Origem e evolução do nosso calendário**. Disponível em: <http://www.mat.uc.pt/ helios/Mestre/H01orige.htm>. Acesso em 26 out. 2016.

[18] OLIVEIRA, Maykon Costa de. **Aritmética:** criptografia e outras aplicações de congruências. 2013. 63f. Dissertação (Mestrado Profissional em Matemática em Rede nacional - PROFMAT) - Centro de Ciências Exatas. Universidade Federal de Mato Grosso do Sul, Mato Grosso do Sul, 2013.

[19] PEREIRA DE SÁ, I. **A aritmética modular e suas aplicações no cotidiano.** Disponível em: <http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf>. Acesso em 27 dez. 2016.

[20] PINTO, Tales. **História do Calendário**. Disponível em: <http://escolakids.uol.com.br/historia-do-calendario.htm.>. Acesso em 26 out. 2016.

[21] PÓS-GRADUANDO. **Frases célebres para monografias, dissertações e teses.** Disponível em: <http://posgraduando.com/frases-celebres-para-monografias-dissertacoes-e-teses/>. Acesso em 20 de nov. 2016.

[22] SANTOS, José Plínio de Oliveira. **Introdução à teoria dos números**. 3. ed. Rio de Janeiro: IMPA, 2007.

[23] SINGH, Simon. **O livro dos códigos**. Tradução: Jorge Calife. 6. ed. Rio de Janeiro: Record, 2007.

[24] SILVA, Maria Ioneris Oliveira. **CRIPTOGRAFIA:** Aplicações da Teoria dos Números e Álgebra. 2015. 89f. Trabalho de Conclusão de Curso (Graduação em Licenciatura em Matemática) - Centro de Educação e Saúde. Universidade Federal de Campina Grande, Paraíba, 2015.

[25] SÓ MATEMÁTICA. **Frases matemáticas.** Disponível em: <http://www.somatematica.com.br/frases3.php/>. Acesso em 17 de mar. 2017.

[26] TAVARES, Wladimir Araújo. **Marathoncode:** aritmética do relógio. 2012. Disponível em: <http://marathoncode.blogspot.com.br/2012/03/aritmetica-do-relogio.html>. Acesso em 19 out. 2016.

[27] VIEIRA, Vandeberg Lopes. **Um curso básico em teoria dos números**. Campina Grande: EDUEPB. 2015.