UNIVERSIDADE FEDERAL DE ALAGOAS

Mestrado Profissional em Matemática em Rede Nacional

PROFMAT

DISSERTAÇÃO DE MESTRADO

O USO DE ALGORITMOS PARA A SOLUÇÃO DE SISTEMAS DE CONGRUÊNCIAS LINEARES

José Roberto de Almeida Lima

Maceió, agosto de 2016

Instituto de Matemática

PROFMAT

Universidade Federal de Alagoas
Instituto de Matemática
Programa de Mestrado Profissional em Matemática
em Rede Nacional-PROFMAT

O Uso de Algoritmos para a Solução de Sistemas de Congruências Lineares

José Roberto de Almeida Lima

Maceió, Brasil
2016

José Roberto de Almeida Lima

O Uso de Algoritmos para a Solução de Sistemas de Congruências Lineares

Dissertação de Mestrado Profissional, submetida em 06 de agosto de 2016 à banca examinadora, designada pelo Colegiado do Programa de Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Alagoas em associação com a Sociedade Brasileira de Matemática, como parte dos requisitos necessários a obtenção do grau de mestre em Matemática.

Orientador: Prof. Dr. André Luiz Flores.

Maceió
2016

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Bibliotecário Responsável: Marcelino de Carvalho

L732u Lima, José Roberto de Almeida.
O uso de algoritmos para solução de sistemas de congruência lineares / José Roberto de Almeida Lima. – 2016.
59 f. : il.

Orientador: André Luiz Flores.
Dissertação (Mestrado Profissional em Matemática) – Universidade Federal de Alagoas. Instituto de Matemática. Programa de Pós Graduação em Matemática em Rede Nacional. Maceió, 2016.

Bibliografia: f. 59.

1. Algoritmos. 2. Sistemas lineares. 3. Congruências e restos. 4. Teorema chinês do resto. I. Título.

CDU: 510.51

Folha de Aprovação

JOSÉ ROBERTO DE ALMEIDA LIMA

O USO DE ALGORITMOS PARA A SOLUÇÃO DE SISTEMAS DE CONGRUÊNCIAS LINEARES

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) do Instituto de Matemática da Universidade Federal de Alagoas e aprovada em 18 de agosto de 2016.

Banca Examinadora:

Prof. Dr André Luiz Flores - UFAL (Presidente)

Prof. Dr. Vânio Fragoso de Melo - UFAL

Prof. Dr Júlio César de Souza Almeida - UFES

Dedicatória

Dedico este trabalho aos esforços dos amigos José Wilson Almeida de Araújo e Givaneide Oliveira Farias.

Agradecimentos

Primeiramente, a Deus todo poderoso que me concede vida, saúde e saber para as lutas do dia-a-dia.

Em seguida meus agradecimentos vão para minha mãe Rosana Januário dos Santos que, em toda minha vida, investiu nos meus estudos de forma financeira, quando pôde, e, principalmente, dando incentivo nos momentos em que pensei que não pudesse conseguir, pois seu apoio sempre foi fundamental para minhas realizações.

A todos os professores que colaboraram com o meu currículo escolar e acadêmico, pela paciência que tiveram comigo e pelo conhecimento transferido, em especial cito os seguintes nomes:

- Professor e orientador Dr. André Luiz Flores que acompanhou meu desenvolvimento em toda graduação, dando orientações que se tornavam, em muitas vezes, conselhos de como seguir em minha carreira acadêmica e, em suma, fez com que eu "aprendesse a aprender".

- Professor Rory Nicholas, por colaborar na minha decisão em seguir na docência matemática.

- Professores Vânio Fragoso, José carlos Almeida, Ediel Guerra, Viviane Oliveira, Márcio Batista, Hilário Alencar, Gregório Silva e Isnaldo Isaac, pelos esforços em garantir boas aulas a turma Profmat-2014.

Aos amigos José Wilson Almeida e Givaneide Oliveira pelo companheirismo e força.

Ao amigo Max pelo companheirismo e orientação na digitação deste trabalho de conclusão.

Ao amigo Juvino por trazer alegria a nossa turma até nos dias mais difíceis.

Aos colegas e amigos de turma, especialmente ao grupo "unidos para sempre": Peixoto, Anne, Josivaldo, Leandro, Erlando, Henrique e Fabiano, que me acompanharam de perto nesse curso. Bem como Camila, Luana, Eduarda, Newton, Humberto, Fernando e Cristiano.

Ao professor Diogo Meurer e Heitor Barros pela orientação gráfica e digital.

Aos companheiros de trabalho do IFAL, Campus Penedo, pelo incentivo em realizar este curso.

Aos companheiros da área técnica do IFAL, Campus Arapiraca, pela colaboração e sugestões.

Lista de Figuras

Lista de Tabelas

Sumário

"Quem me dera, ao menos uma vez,
provar que quem tem mais do que precisa ter
quase sempre se convence que não tem o bastante,
fala demais por não ter nada a dizer."
Renato Russo

Resumo

Neste trabalho tratamos do estudo de congruências como ferramenta de apoio na resolução de problemas que venham a figurar em diversas provas de concursos e olimpíadas. No decorrer do trabalho faremos a exposição de questões de olimpíadas, a fim de justificar a necessidade da abordagem do tema no ensino básico. Apresentaremos o Teorema Chinês dos Restos e alguns algoritmos a fim de simplificar a resolução de sistemas de congruências.

Palavras-chave: Aritmética; Congruências lineares; Teorema Chinês dos Restos ; Algoritmo.

Abstract

In this paper we treat the congruence of study as a support tool in solving problems that may appear in several competitions contests and Olympiads . During the work we will display upcoming issues in order to justify the need for the approach to the subject in primary education . We present the Chinese Remainder Theorem and an algorithm based on some algorithms in order to simplify the resolution of congruences systems.

Palavras-chave: Arithmetic; linear congruences ; Chinese Remainder Theorem ;algorithm.

Introdução

O estudo da Teoria dos Números baseia-se nas propriedades dos números inteiros, bem como a grande classe de problemas que surge no decorrer de seu estudo. Em particular, ressaltamos a importância das congruências dentro deste grande ramo da matemática, pois a mesma vem obtendo cada vez mais destaque no cenário de provas de olimpíadas de matemáticas e concursos públicos na área. Isso se deve ao fato de que a Teoria dos Números exige estratégias do estudante para resolução de seus problemas mais rebuscados.

De forma geral, o estudo das congruências, em especial, os sistemas de congruências lineares, possui características específicas e para resolução das mesmas precisamos compreender a teoria e métodos práticos de como chegar ao resultado desejado.

Diante das exigências diretas ou indiretas ocorridas em sala de aula e/ou nas disputas em olimpíadas escolares, um fator que permanece em evidência é a importância de se obter meios eficientes de chegar aos resultados de problemas, minimizando o tempo gasto nas resoluções. Portanto, para solucionar tais situações é que se resolve fazer uso de algoritmos na intenção de resolver sistemas de congruências lineares. Tais algoritmos são de notável relevância, em especial quando o número de equações e/ou a cardinalidade dos números envolvidos é grande.

Objetivamos com este trabalho criar algoritmos que auxilie a resolução dos sistemas de congruências lineares, bem como mostrar através de exemplos como aplicar tais algoritmos fazendo uso de tabelas, pois temos como finalidade facilitar a resolução de problemas voltados para este conteúdo tanto no ensino básico quanto no ensino superior.

A escolha deste trabalho provém da intenção de mostrar para o público discente do ensino básico a utilidade de algoritmos baseados no estudo da divisibilidade e congruências, os quais auxiliarão muitos alunos que participam de olimpíadas regionais, nacionais ou internacionais, além de reforçar o conhecimento daqueles que buscam apenas conhecer estratégias eficientes de como resolver problemas que envolvam congruências lineares. Nota-se, claramente, que se não houver uma preparação diferenciada, os estudantes geralmente não tem um desempenho adequado em olimpíadas matemáticas. A maioria das questões olímpicas envolvem um raciocínio mais apurado e que exige um treinamento prévio.

Este trabalho de conclusão de curso estrutura-se em três capítulos, apresentando-se no primeiro uma introdução ao estudo da divisibilidade e MDC a fim de expor as primeiras definições e resultados que embasam o conteúdo principal do trabalho. Segue no capítulo 2 que exibimos o conteúdo das congruências e congruências lineares de forma bastante teórica, todavia com a resolução de diversas

situações problemas para maior entendimento. No capítulo 3 deixamos toda sua estrutura baseada na construção de algoritmos, em total de seis, embasados em resultados dos capítulos anteriores com o objetivo final de resolver sistemas de congruências lineares.

Capítulo 1

Divisibilidade e MDC

Este capítulo fica destinado ao estabelecimento de definições e propriedades de cunho elementares a respeito de divisibilidade e congruências no conjunto dos números inteiros, a fim de dar um maior apoio na resolução de problemas e/ou demonstrações posteriores. Nas secções a seguir encontraremos problemas e resultados interessantes, dentre estes últimos destacamos o Teorema de Bézout.

Os resultados apresentados neste capítulo são clássicos e podem ser encontrados nas referências [2], [3], [6], [9].

Definição 1.1. *Considere dois inteiros a e b, distintos ou não, com $b \neq 0$. Dizemos que b divide a, e escrevemos $b|a$, se existir $c \in \mathbb{Z}$ tal que $a = b.c$.*

Mesmo quando um número inteiro $b \neq 0$ não divide o inteiro a, o matemático Euclides utiliza em sua obra, Os Elementos, sem enunciá-los explicitamente, o fato de que é sempre possível efetuar a divisão de a por b, com resto. Observe a seguir importantes resultados, quais sejam, a Propriedade Arquimediana e em seguida o Teorema da Divisão Euclidiana.

Proposição 1.1. *(Propriedade Arquimediana) [6] Considere $a, b \in \mathbb{Z}$, com $b \neq 0$. Desse modo existe $n \in \mathbb{Z}$ tal que $nb > a$.*

Demonstração 1.0.1. *Considerando que temos os seguintes dados $|b| \neq 0$ e $b \in \mathbb{Z}$, então podemos afirmar que $|b| \geqslant 1$, logo escrevemos*

$$(|a| + 1) \cdot |b| \geqslant |a| + 1, \tag{1}$$

pois por hipótese $|b| \geqslant 1$. Segue que:

$$(|a| + 1) \cdot |b| \geqslant |a| + 1 > |a| \geqslant a. \tag{2}$$

Assim, tomando na desigualdade

i) $n = |a| + 1$ *se* $b > 0$; *ou*

ii) $n = -(|a| + 1)$ *se* $b < 0$.

Daí chegamos ao resultado desejado.

Teorema 1.1. *(Divisão Euclidiana) [6] Considere* $a, b \in \mathbb{Z}$, *com* $b \neq 0$. *Assim, existem dois inteiros* q *e* r, *unicamente determinados, de tal modo que* $a = b.q + r$, *com* $0 \leqslant r < |b|$.

Demonstração 1.0.2. *Dividiremos nossa demonstração em duas partes, as quais se seguem:*

i) Unicidade:

Suponha que $a = bq + r = bq' + r'$, *onde* $q, q', r, r' \in \mathbb{Z}, 0 \leqslant r < |b|$ *e* $0 \leqslant r' < |b|$. *Desse modo, temos que* $-|b| < -r \leqslant r' - r \leqslant r' < |b|$. *Portanto,* $|r' - r| < |b|$. *Por outro lado, notamos que* $b(q - q') = r' - r$, *e isto implica em*

$$|b||q - q'| = |r' - r| < |b|,$$

fato que só é possível se $q = q'$. *Segue daí que*

$$|r' - r| = |b|.0 = 0 \Rightarrow r = r'.$$

ii) Existência:

Consideremos inicialmente o conjunto $T = \{x = a - by; y \in \mathbb{Z}\} \bigcap (\mathbb{N} \cup \{0\})$.

Pela Propriedade Arquimediana enunciada anteriormente, existe $n \in \mathbb{Z}$ *tal que* $n(-b) > -a$, *segue então que* $a - nb > 0$, *mostrando que o conjunto* T *é não vazio. Agora note que o conjunto* T *é limitado inferiormente por* 0, *fato observado na intersecção se* T *com* $(\mathbb{N} \cup \{0\})$, *assim, pelo Princípio da Boa Ordenação, temos que* T *possui um menor elemento, o qual denominaremos* r. *Suponha que* $r = a - bq$. *Sabemos que* $r \geqslant 0$, *pois* T *não possui elementos negativos. Vamos mostrar que* $r < |b|$. *Suponhamos por absurdo que* $r \geqslant |b|$. *Desse modo, existe* $s \in \mathbb{N} \cup \{0\}$ *tal que* $r = |b| + s$, *logo* $0 \leqslant s < r$. *Contudo, isso contradiz o fato de* r *ser o menor elemento de* T, *pois* $s = a - (q \pm 1)\, b \in T$, *com* $s < r$.

Concluindo nossa demonstração a respeito da unicidade de q *e* r.

Nas condições do teorema acima, os números inteiros q e r, são chamados, respectivamente, de *quociente* e *resto* da divisão de a por b.

Exemplo 1.1. *O quociente e o resto da divisão de* 23 *por* 6 *são* $q = 3$ *e* $r = 5$, *pois*

$$23 = 6.3 + 5.$$

Faremos a definição de divisor comum a seguir a fim de introduzir logo em seguida a ideia de máximo divisor comum entre dois ou mais números.

Definição 1.2. *Considere dois inteiros* a *e* b, *distintos ou não. Um número inteiro* d *será considerado divisor comum de* a *e* b *caso tenhamos* $d|a$ *e* $d|b$.

Desse modo, é fácil ver que os números $\pm 1, \pm 3, \pm 5$ e ± 15 são divisores comuns de 30 e 45.

Definição 1.3. *Qualificamos um inteiro $d \geqslant 0$ como um máximo divisor comum (mdc) dos inteiros a e b, se d é um divisor comum de a e b e, simultaneamente, é divisível por todo divisor comum que houver de a e b.*

O mdc de a e b será denotado por (a, b).

O lema a seguir é bastante eficaz no cálculo do mdc de dois números naturais.

Lema 1.1. *(Lema de Euclides) [6] Considere os inteiros a, b e n. Sempre que existir $(a, b - na)$, então existe (a, b) e*

$$(a, b) = (a, b - na).$$

Demonstração 1.0.3. *Com efeito, escrevendo $d = (a, b - na)$, desse modo é fácil ver que $d|a$ e $d|b - na$, bem como $b|na$. Segue dessa forma que*

$$d|\,[na + (b - na)] \Rightarrow d|b.$$

Observamos então que d é divisor comum de a e b. Para mostrar que d é o maior dos divisores comuns de a e b vamos considerar um $c \in \mathbb{Z}$ qualquer também divisor comum de a e b. Note que $c|a$ e $c|b \Rightarrow c|b - na$.

Como $c|a$ e $c|b - na$, então c é divisor comum de a e $b - na$. Sendo d o máximo divisor comum de a e $b - na$, então chegamos a conclusão de que $c|d$ e, consequentemente, $d = (a, b)$.

Exemplo 1.2. *Seja $n \in \mathbb{N}$. Mostre que*

$$(n! + 1, (n + 1)! + 1) = 1.$$

Solução.

Fazendo uso do Lema acima algumas vezes conseguimos provar tal resultado. Veja:

$$\begin{aligned}
(n! + 1, (n + 1)! + 1) &= (n! + 1, (n + 1)! + 1 - (n + 1) \cdot (n! + 1)) \\
&= (n! + 1, (n + 1)! + 1 - (n + 1)! - n - 1)) \\
&= (n! + 1, -n) \\
&= (n! + 1 - [-(n - 1)! \cdot (-n)], -n) \\
&= (n! + 1 - n!, -n) \\
&= (1, -n) \\
&= 1.
\end{aligned}$$

Definição 1.4. *[9] Qualificamos um número inteiro positivo maior do que 1 que só possui como divisores positivos 1 e ele mesmo como número primo.*

São exemplos de primos os números $2, 3, 5, 7$ e 11, pois seus únicos divisores positivos são 1 e ele próprio.

Definição 1.5. *Dois números inteiros a e b serão denominados primos entre si (coprimos) se $(a, b) = 1$, isto é, se o único divisor comum positivo de ambos for 1.*

Observe que os números 12 e 35 são primos entre si, pois $(12, 35) = 1$, mesmo que eles não sejam necessariamente primos.

Definição 1.6. *Sejam $a, b \in \mathbb{Z}$. Definimos o conjunto*

$$d\mathbb{Z} = I(a,b) = \{xa + yb; x, y \in \mathbb{Z}\},$$

onde $d = (a,b)$.

Proposição 1.2. *Para que dois números inteiros a e b sejam primos entre si é necessário e suficiente que existam números inteiros m e n inteiros de tal forma que $ma + nb = 1$.*

Demonstração 1.0.4. *Ver [6].*

O teorema a seguir é bastante utilizado na resolução de problemas de teoria dos números, muito conhecido por "Lema de Gauss".

Teorema 1.2. *[9] Considere $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $(a,b) = 1$, então, consequentemente, $a|c$.*

Demonstração 1.0.5. *Note a princípio que $a|bc$ implica na existência de $f \in \mathbb{Z}$ de tal modo que $bc = af$. Considerando o fato de que $(a,b) = 1$, então pela proposição anterior, notamos que existem $k, l \in \mathbb{Z}$ tais que*

$$ka + lb = 1.$$

Fazendo a multiplicação por c em ambos os membros da igualdade acima, temos

$$c = kac + lbc.$$

Segue que podemos substituir bc por af nesta última igualdade e, consequentemente, teremos

$$c = kac + laf = a(kc + lf)$$

e, portanto, $a|c$.

Definição 1.7. *O menor múltiplo comum de dois ou mais números, diferente de zero, é chamado de mínimo múltiplo comum (MMC) desses números. Usamos a abreviação a notação $[a,b]$ para indicar o MMC entre os números a e b.*

Étienne Bézout (1730 - 1783) foi um matemático francês da escola de Mézières nascido em Nemours, Seine-et-Marne, consagrado pela publicação da coleção Cours de mathématique, em seis volumes, cobrindo toda a matemática elementar até a de alto nível conhecida até então, com ênfase para a mecânica e a navegação (1764-1769), que teve várias reedições e versões em outras línguas, inclusive adotada em West Point.

Filho de um magistrado da cidade de Nemours, Pierre Bézout, e de Hélène-Jeanne Filz, por tradição familiar deveria seguir a carreira do pai e do avô. Porém ao tomar contato com os trabalhos de Leonard Euler, ele resolveu se dedicar a matemática. Em seguida enunciamos um de seus trabalhos que muito contribui para o estudo da aritmética.

Teorema 1.3. *(Bézout) Considere $a, b \in \mathbb{Z}$, ambos não nulos, e $d = (a,b)$. Então existem inteiros x e y tais que $d = a.x + b.y$.*

Figura 1.1: Étiènne Bézout.

Demonstração 1.0.6. *Considere inicialmente* $S = \{ax + by; ax + by > 0, x, y \in \mathbb{Z}\}$. *Note que o conjunto S é não vazio, pois tomando* $x = a$ *e* $y = b$, *temos*

$$a^2 + b^2 > 0.$$

Considerando f *o menor elemento do conjunto S. Assim,* $d = (a, b)|f$, *pois* $d|a$ *e* $d|b$, *consequentemente* $d|ax + by$, $\forall x, y \in \mathbb{Z}$. *Como* $f, d > 0$, *para mostrarmos que* $d = f$, *nos resta provar que* $f|d$. *Note que, pelo Teorema da Divisão Euclidiana* $a = q.f + r$, *com* $q, r \in \mathbb{Z}$ *e* $0 \leqslant r < f$. *Assim, como* $a = q.f + r = q.(ax + by) + r$, *então* $a - qax - qby = r \Longrightarrow a(1 - qx) + b.(-qy) = r \geqslant 0$, *então* $r \in \mathbb{Z}$ *e sendo* $r < f$, *segue que* $r = 0$. *Daí* $f|a$ *e, de modo semelhante, mostramos que* $f|b$. *Portanto* $f|(a, b) = d$, *concluindo nossa demonstração.*

Capítulo 2

Congruências e Sistemas de Congruências Lineares

Neste capítulo estudaremos o conceito de congruência, que revolucionou o estudo da Aritmética, permitindo tratar as questões de divisibilidade com um enfoque mais fácil e mais eficiente. Foi Carl Friederich Gauss (1777- 1855) quem introduziu este conceito, em 1801, no seu livro Disquisitiones aritmeticae (Investigações na Aritmética). Gauss escreveu este livro quando ele tinha apenas 24 anos.

Figura 2.1: Johann Carl Friedrich Gauss.

Observe que ao ter que escolher entre um laço de fita azul ou vermelha para colocar no cabelo, a menina começa a recitar em voz alta: Ma-mãe man-dou eu es-co-lher es-ta da-qui, mas co-mo sou tei-mo-sa vou es-co-lher es-ta da-qui! Apontando com o dedo alternadamente para o laço azul e para o vermelho ao ritmo cadenciado das sílabas. O laço escolhido é aquele apontado por último. Certamente, conhecemos esse procedimento ou outro semelhante com cantigas diferentes. Mas o que tem isso a ver com o estudo das congruências?

Quando dois inteiros deixam o mesmo resto ao serem divididos por m, dizemos que eles são congruentes (ou côngruos) módulo m. Por exemplo, 13 e 9 são côngruos módulo 4, porque ambos deixam resto 1 quando divididos por 4.

Ao recitar a cantiga, a menina aponta alternadamente para as duas fitas. Como a quantidade de sílabas da cantiga é 27, então a menina escolhe a primeira fita, pois 27 é ímpar, isto é, deixa resto 1,

quando dividido por 2. De um modo geral, a fita escolhida será sempre a primeira, caso o número de sílabas da cantiga seja ímpar, e será sempre a segunda, caso o número de sílabas da cantiga seja par.

Antes de dar início as próximas seções, queremos salientar que os resultados apresentados neste capítulo são clássicos e podem ser encontrados nas referências [2], [6], [9].

2.1 Introdução às Congruências

Definição 2.1. *Considere o inteiro positivo m. Dizemos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Desse modo, quando os inteiros a e b são congruentes módulo m, escreve-se*

$$a \equiv b \ (mod m).$$

Da definição acima podemos observar que $35 \equiv 23 \ (\text{mod}12)$, pois os restos da divisão de 35 e 23 por 12 são iguais a 11.

O problema a seguir foi retirado da primeira fase da prova de nível 1 da OBMEP 2012. Observe, para este caso, o quanto o resto da divisão se torna importante quando trabalhamos com situações cíclicas.

Exemplo 2.1. *Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda, a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?*

Figura 2.2: OBMEP 2012, nível 1, 2ª fase.

Solução.

A princípio vamos listar as posições das cartas e fazer os embaralhamentos sucessivos de acordo com a regra dada no enunciado da questão. Desse modo, observe a construção da tabela a seguir:

Situação	A
Inicial	$A2345$
Após 1º embaralhamento	$3A524$
Após 2º embaralhamento	$534A2$
Após 3º embaralhamento	$4523A$
Após 4º embaralhamento	$24A53$
Após 5º embaralhamento	$A2345$

Tabela 2.1: Embaralhamentos sucessivos.

Observamos que a cada cinco embaralhamentos sucessivos retornamos à primeira posição, então para determinar a posição após o 2012^o *embaralhamento basta efetuar a divisão euclidiana de 2012 por 5, isto é,*

$$2012 = 5.402 + 2.$$

Assim posição das cartas depois do 2012^o *embaralhamento é a mesma que a posição depois do* 2^o *embaralhamento. Concluímos, dessa forma, que a primeira carta é a de número 5.*

Devemos observar que se dois números são congruentes módulo m, podemos simplificar nossos esforços aplicando o resultado que segue:

Proposição 2.1. *[6] Considere os inteiros* a, b, m, *com* $m > 1$. *Assim, para termos* $a \equiv b \bmod m$ *é necessário e suficiente que* $m \mid b - a$.

Demonstração 2.1.1. *De acordo com a divisão euclidiana de* a *e* b *por* m *podemos escrever respectivamente* $a = mq + r$, *com* $0 \leqslant r < m$ *e* $b = ms + t$, *com* $0 \leqslant s < t$. *Dessa forma,*

$$b - a = (ms + t) - (mq + r) = m(s - q) + (t - r).$$

Como, por definição, $a \equiv b \bmod m$ *indica que* a *e* b *deixam o mesmo resto na divisão por* m. *Assim,*

$$b - a = m(s - q),$$

isto é, $m|b - a$. *Concluindo nossa primeira parte da demonstração.*

Por outro lado, se $m|b - a$, *então podemos escrever* $m|t - r$. *Como* $|t - r| < m$, *temos em consequência que* $t = s$. *Concluindo nossa demonstração.*

Definição 2.2. *Chamaremos de sistema completo de resíduos módulo* m (m *inteiro positivo) a todo conjunto de números inteiros cujos restos pela divisão por* m *são os números* $0, 1, 2, 3, ..., m - 1$, *sem repetições e não necessariamente na mesma ordem.*

Exemplo 2.2. *Verifique que o conjunto* $\{3, 16, 38\}$ *é um sistema completo de restos módulo 3.*

Solução. Com efeito, basta observamos as congruências:

$$3 \equiv 0(mod3)$$

$$16 \equiv 1(mod3)$$

$$38 \equiv 2(mod 3).$$

Como na divisão por 3 *os únicos restos possíveis são 0, 1 e 2, concluímos que o conjunto* $\{3, 16, 38\}$ *é um sistema completo de resíduos módulo 3.*

De acordo com a definição, nota-se que para acharmos o resto da divisão de um número a por m basta encontrar o número natural r dentre os números $0, 1, 2, 3, ..., m-1$ que seja congruente a a módulo m.

Em seguida faremos exposição de alguns exemplos contextualizados, os quais figuram no dia a dia do aluno, isto é, casos que podem ser aplicados em sala de aula a fim de haver uma melhor compreensão por parte do discente quanto ao conteúdo de congruências.

Exemplo 2.3. *A distribuição dos dias do mês num calendário é um exemplo do uso do conceito de congruência. Vejamos o calendário do mês de abril do ano de 2016:*

DOM	SEG	TER	QUA	QUI	SEX	SÁB
					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

Tabela 2.2: Calendário Abril de 2016.

Observe a última coluna, a das sextas-feiras, que começa com o 1 e todos os outros números dessa coluna deixam resto 1 quando divididos por 7. A coluna do sábado, começa com 2 e todos os outros números deixam resto 2 quando divididos por 7. Ou seja, em todas as colunas os números são côngruos entre si módulo 7.

Vamos apresentar a seguir uma questão retirada do banco de questões do site da OBMEP, local onde encontramos inúmeras questões interessantes e provocativas para o preparo de nossos alunos da Educação Básica.

Exemplo 2.4. *A, B, C, D, E, F, G e H são os fios de apoio que uma aranha usa para construir sua teia, conforme mostra a figura. A aranha continua seu trabalho. Sobre qual fio de apoio estará o número 118?*

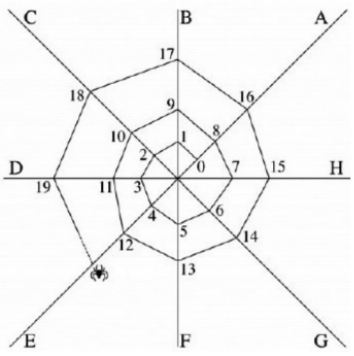

Figura 2.3: Exemplo do Banco de Questões OBMEP.

Solução.

Vamos observar o que está acontecendo na tabela seguinte que descreve a construção da teia pela aranha deste exemplo.

A	B	C	D	E	F	G	H
0	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
...	...	...	...	...	...	...	...

Tabela 2.3: Correspondência entre o Número e o Fio de Apoio.

É claro que podemos, pacientemente, continuar construindo a tabela até que aparecesse o número 118. Assim saberíamos em qual fio a aranha iria estar. Entretanto, convenhamos que não seria uma solução muito prática e nem rápida. Imagine se a questão perguntasse o fio correspondente ao número 331?

É fácil perceber que os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8*, isto é, há um aumento de oito em oito. Notamos também que cada fio pode ser representado a partir dos múltiplos de* 8*. O fio A corresponde aos números que são múltiplos de* 8*, ou seja, números que divididos por* 8 *deixam resto zero (*$8.n$*, com* $n \in \mathbb{N}$*). O fio B corresponde aos números que são múltiplos de* 8 *acrescidos de* 1*, ou seja, números que divididos por 8 deixam resto 1 (*$8.n + 1$*, com* $n \in \mathbb{N}$*). O fio C corresponde aos números que são múltiplos de 8, mais 2, ou seja, números que divididos por 8 deixam resto 2 (*$8.n + 2$*, com* $n \in \mathbb{N}$*) e essa lógica se mantém até o fio H, definido pelos números que divididos por oito deixam resto 7. É claro que para saber sobre qual fio estará o número 331, basta verificarmos a qual dessas famílias tal número pertence e isso pode ser facilmente obtido ao dividirmos 331 por 8, pois o resto da divisão indicará a qual das famílias o 331 pertence, em outras palavras, procuramos a congruência de 331 módulo 8. Desta forma, verificamos que o número 331 é igual a* $8.41 + 3$*, ou seja, pertence à família dos números que estão no fio D.Todos os números de nosso exemplo, que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8, isto é, são congruentes entre si, no módulo 8.*

Outro exemplo importante, do nosso cotidiano é a verificação dos dois dígitos de controle do CPF (Cadastro das pessoas físicas na Receita Federal) de uma pessoa.

Figura 2.4: Modelo de CPF.

Observe que o número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como no ISBN e

nos códigos de barra, dígitos de controle ou de verificação . A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência. No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Se $n_1n_2n_3n_4n_5n_6n_7n_8n_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1,2,3,4,5,6,7,8,9\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por n_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, então $S - n_{10} \equiv 0(mod 11)$. Observe que tal número será o próprio resto da divisão da soma obtida por 11 .

A determinação do segundo dígito de controle, representado por n_{11}, é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9.

Exemplo 2.5. *Suponha que o CPF de uma pessoa tem os seguintes 9 primeiros dígitos:* 092.152.785. *Vamos determinar os dois dígitos verificadores de tal CPF.*

Seguindo os passos indicados anteriormente e efetuando as multiplicações correspondentes, obtemos o dígito n_{10} da seguinte forma:

$$0.1 + 9.2 + 2.3 + 1.4 + 5.5 + 2.6 + 7.7 + 8.8 + 5.9 = 223.$$

Dividindo o número 223 por 11, obtemos $223 = 20.11 + 3$ ou, equivalentemente, $223 \equiv 3(mod 11)$. Dessa forma, o primeiro dígito de controle será o algarismo $n_{10} = 3$.

Para o segundo dígito, denominado n_{11}, é obtido através das multiplicações:

$$0.0 + 9.1 + 2.2 + 1.3 + 5.4 + 2.5 + 7.6 + 8.7 + 5.8 + 3.9 = 211$$

Efetuando a divisão de 211 por 11, obtemos $211 = 19.11 + 2$, isto é, $211 \equiv 2(mod 11)$. Logo, o segundo dígito de controle é o $n_{11} = 2$.

Concluímos então que, no nosso exemplo, o CPF completo é 092.152.785 − 32.

Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito zero.

Abaixo enumeramos algumas propriedades das congruências no intuito de auxiliar na resolução de exemplos e demonstrações de resultados que prosseguem neste trabalho.

i) (Reflexividade) $a \equiv a(mod m)$;

Demonstração 2.1.2. *De fato, note que $m|0 \Leftrightarrow m|a - a \Leftrightarrow a \equiv a(mod m)$.*

ii) (Simetria) Se $a \equiv b$ (mod m), então $b \equiv a$ (mod m);

Demonstração 2.1.3. *Observe que se $a \equiv b\ (mod\ m)$, então existe $k \in \mathbb{Z}$ tal que $a - b = k.m$. Segue que podemos escrever $b - a = -(k.m) = (-k).m$, implicando em $b \equiv a\ (mod\ m)$.*

iii) (Transitividade) Se $a \equiv b$ (mod m) e $b \equiv c$ (mod m), então $a \equiv c$ (mod m);

Demonstração 2.1.4. *Dados $a \equiv b\ (mod\ m)$ e $b \equiv c\ (mod\ m)$, então existem $k, l \in \mathbb{Z}$ tais que $a - b = k.m$ e $b - c = l.m$. Segue que podemos escrever $a - c = (a - b) + (b - c) = km + lm = (k + l)m$, implicando em $a \equiv c\ (mod\ m)$.*

iv) (Soma) Se $a \equiv b($ (mod m) e $c \equiv d$ (mod m), então $a + c \equiv b + d$ (mod m);

Demonstração 2.1.5. *Dadas as congruências $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, então existem $k, l \in \mathbb{Z}$ tais que $a-b = k.m$ e $c-d = l.m$. Desse modo podemos escrever $(a+c)-(b+d) = (a-b)+(c-d) = km+lm = (k+l)m$, implicando em $a + c \equiv b + d\ (mod\ m)$.*

v) (Diferença) Se $a \equiv b$ (mod m) e $c \equiv d$ (mod m)$(modm)$, então $a - c \equiv b - d$ (mod m);

Demonstração 2.1.6. *Considere as congruências $a \equiv b\ (mod\ m)$ e $c \equiv d\ (mod\ m)$, as quais podemos reescrever da forma $a - b = mk$ e $d - c = ml$, para algum $k, l \in \mathbb{Z}$. Somando membro a membro as igualdades, temos*

$$(a - b) + (d - c) = mk + ml \Rightarrow (a - c) - (b - d) = m.(k + l) \Rightarrow a - c \equiv b - d\ (mod\ m).$$

vi) Se $a \equiv b$ (mod m) e c é um inteiro não negativo, então $a.c \equiv b.c$ (mod m);

Demonstração 2.1.7. *De fato, considere $a \equiv b\ (mod\ m)$, então podemos escrever $a - b = km$, com $k \in \mathbb{Z}$. Multiplicando ambos os lados por $c \in \mathbb{Z}$, temos*

$$ac - bc = kmc,$$

mas isso implica em $ac \equiv bc\ (mod\ m)$.

vii) (Produto) Se $a \equiv b$ (mod m) e $c \equiv d$ (mod m), então $a.c \equiv b.d$ (mod m);

Demonstração 2.1.8. *Vamos escrever as congruências $a \equiv b\ (mod\ m)$ e $c \equiv d($ $(mod\ m)$ da seguinte forma: $a - b = mk$ e $c - d = ml$, para algum $k, l \in \mathbb{Z}$. Daí temos $a = b + mk$ e $c = d + ml$. Segue que*

$$ac - bd = (b + mk)(d + ml) - bd = (bd + bml + mkd + m^2kl) - bd = (bl + kd + mkl)m$$

e, portanto, podemos concluir que $a.c \equiv b.d\ (mod\ m)$.

viii) (Potência) Se $a \equiv b$ (mod m) e k é um inteiro positivo, então $a^k \equiv b^k$ (mod m);

Demonstração 2.1.9. *Usando o Princípio da Indução Finita para esta demonstração, observamos que o fato é verdadeiro para k=1. Suponhamos verdadeiro para o inteiro n positivo, vamos mostrar que também é válido para n+1.*

Como $a \equiv b\ (mod\ m)$ e $a^n \equiv b^n\ (mod\ m)$, então pela propriedade anterior, temos

$$a^n a \equiv b^n b \ (mod\ m) \Rightarrow a^{n+1} \equiv b^{n+1} \ (mod\ m).$$

Desse modo mostramos a validade para o inteiro $n+1$. Concluímos, portanto, que a propriedade é válida para todo k inteiro positivo.

ix) (Cancelamento para a soma) Se $a + c \equiv b + c$ (mod m), então $a \equiv b$ (mod m).

Demonstração 2.1.10. *Se $a + c \equiv b + c\ (mod\ m)$, então podemos afirmar que $m|b + c - (a + c)$, implicando em $m|b - a$ e, em consequência disso, obtemos $a \equiv b\ (mod\ m)$.*

Ressaltando novamente a importância do tema de nosso trabalho, exporemos a seguir uma questão contida na prova de admissão ao Colégio Militar de Fortaleza no ano de 2011.

Exemplo 2.6. *Dois números inteiros positivos são tais que a divisão do primeiro deles por 7 deixa resto 6, enquanto a divisão do segundo, também por 7, deixa resto 5. Somando os dois números e dividindo o resultado por 7, o resto será:*

a) 1 b) 2 c) 3 d) 4 e) 5

Solução.

Sejam a e b os dois números inteiros positivos citados. Além disso, as seguintes congruências são enunciadas no problema:

$a \equiv 6\ (mod7)$

$b \equiv 5\ (mod7)$.

Como ambas as congruências têm o mesmo módulo, então podemos utilizar a propriedade da "Soma de Congruências"vista anteriormente. Assim, podemos escrever:

$$a + b \equiv 6 + 5 = 11 \equiv 4\ (mod7).$$

Logo, o resto desejado é 4.

Exemplo 2.7. *Dados os números a, b, c inteiros positivos cujos restos na divisão por 7 são, respectivamente,2,4 e 6. Determine o resto da divisão de a+b+c por 7.*

Solução. De acordo com o enunciado da questão, temos as seguintes congruências:

$$a \equiv 2\ (mod7)$$

$$b \equiv 4\ (mod7)$$

$$c \equiv 6\ (mod7).$$

Assim, somando membro a membro as três congruências, obtemos:

$$a + b + c \equiv 2 + 4 + 6 = 12 \equiv 5\ (mod7).$$

Portanto, o resto da divisão de $a + b + c$ por 7 é 5.

São exemplos como este que demonstram para o aluno a importância em se trabalhar com o resto da divisão euclidiana e não com o quociente, como se é esperado. Fato semelhante observamos no exemplo a seguir.

Exemplo 2.8. *Determinar o resto da divisão de* 3^{100} *por 4.*

Solução. Observe inicialmente que $3-(-1)=4\equiv 0$ *(mod4), somando* (-1) *a ambos os lados, temos*

$$3\equiv -1(mod4).$$

Daí, elevando ambos os lados a 100*, podemos escrever*

$$3^{100}\equiv (-1)^{100}=1(mod4).$$

Assim, o resto da divisão de 3^{100} *por 4 é 1.*

Uma observação que deve ser feita refere-se ao cancelamento multiplicativo na congruência. Veja o exemplo dado a seguir.

Exemplo 2.9. *Sendo* $12.5-12.3=24$ *e* $8|24$*, segue que* $12.5\equiv 12.3$ *mod* 8*. Entretanto não se verifica o fato* $5\equiv 3$ *mod* 8*, isto é, nem sempre podemos realizar o cancelamento multiplicativo numa congruência.*

O resultado a seguir trata a respeito da possibilidade deste cancelamento multiplicativo.

Proposição 2.2. *[6] Considere os inteiros* a,b,m*, com* $m>1$*. Assim, para termos* $ac\equiv bc(modm)$ *é necessário e suficiente que* $a\equiv b(\ mod\dfrac{m}{(c,m)})$*.*

Demonstração 2.1.11. *Tomando* $d=(c,m)$*, temos as equivalências*

$$ac\equiv bc(modm)\Leftrightarrow m|bc-ac\Leftrightarrow m|(b-a)c.$$

Segue que podemos tornar esta situação equivalente a

$$\frac{m}{d}|(b-a)\frac{c}{d}.$$

Como $\dfrac{m}{d}$ *e* $\dfrac{c}{d}$ *são primos entre si, então ainda é equivalente a situação acima a expressão*

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

concluindo nossa demonstração.

Observamos, dessa forma, no exemplo anterior o seguinte fato: $12.5\equiv 12.3 \bmod 8$ se, e somente se, $5\equiv 3 \bmod \dfrac{8}{(12,8)}$.

Há cerca de 2500 anos, os chineses já sabiam que se p é um número primo, então $p|2^p-2$. Entretanto, foi Pierre de Fermat (1601-1665), matemático francês, que generalizou esse resultado, enunciando um pequeno, todavia notável teorema o qual enunciaremos mais adiante. Historicamente, percebe-se que o campo predileto de estudos de Fermat foi o da teoria dos números, na qual se consagrou. Fermat deu considerável impulso à aritmética superior moderna exercendo, assim, grande influência sobre o desenvolvimento da álgebra.

Figura 2.5: Pierre de Fermat.

Teorema 2.1. *(Pequeno Teorema de Fermat) Se p é um número primo e se a é um número natural não divisível por p, então p divide* $a^{p-1} - 1$.

Demonstração 2.1.12. *Seja p primo e* $a \in \mathbb{Z}$ *de tal modo que* $p \nmid a$. *Considere os conjuntos* $\{1, 2, 3, 5, ..., p-1\}$ *e* $\{a, 2a, 3a, 5a, ..., (p-1)\,a\}$.

Observe que $a, 2a, 3a, 5a, ..., (p-1)\,a$ *são incongruentes a* 0 *módulo p. Assim, se* $i, j \in \{1, 2, 3, 5, ..., p-1\}$ *e* $ia \equiv ja(modp)$, *então* $i \equiv j(modp)$, *pois* $(a, p) = 1$. *Como* $0 \leqslant |i - j| < p$, *segue que* $i = j$. *Daí notamos que os números* $a, 2a, 3a, 5a, ..., (p-1)\,a$ *são incongruentes entre si módulo p. Desse modo,* $a, 2a, 3a, 5a, ..., (p-1)\,a$ *são congruentes a* $1, 2, 3, 5, ..., p-1$ *em alguma ordem. Assim, podemos escrever a seguinte congruência*

$$(p-1)! = 1.2.3...(p-1) \equiv a.2a.3a...(p-1)a \ (mod\ p),$$

isto é,

$$(p-1)! \equiv a^{p-1}(p-1)! \ (mod\ p).$$

Como os números p e $(p-1)!$ *são primos entre si, ou seja,* $(p, (p-1)!) = 1$, *então podemos realizar o cancelamento de* $(p-1)!$ *de ambos os lados da congruência, obtendo*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

Portanto, concluímos nossa demonstração.

Observe que este Teorema oferece um teste de não primalidade, pois se tomarmos $m \in \mathbb{N}$, com $m > 1$, e existe algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que m não divide $a^{m-1} - 1$, então m é primo.

Exemplo 2.10. *Vamos usar o Pequeno Teorema de Fermat para mostrar que* $2^{50} + 3^{50}$ *é divisível por* 13.

Solução.

Note que 50=12.4+2, então podemos escrever

$$2^{50} = 2^{12.4+2} = (2^{12})^4.2^2.$$

Como 13 *é um número primo, então pelo Teorema Pequeno Teorema de Fermat escrevemos*

$$(2^{12})^4.2^2 \equiv 1^4.2^2 = 4 \text{ (mod 13)}.$$

De maneira análoga, fazemos

$$3^{50} = 3^{12.4+2} = (3^{12})^4.3^2 \equiv 1^4.3^2 = 9 \text{ (mod 13)}.$$

Segue daí que $2^{50} + 3^{50} \equiv 4 + 9 = 13 \equiv 0$ *(mod 13). E portanto* $13|2^{50} + 3^{50}$.

2.2 Congruências Lineares

Trataremos nesta secção a respeito da resolução de congruências da forma: $ax \equiv b \bmod m$, em que $a, b, m \in \mathbb{Z}$, $m > 1$.

Em outras palavras, vamos determinar, caso existam, os números inteiros x de modo que $ax \equiv b \bmod m$.

Proposição 2.3. *[6] Considere os inteiros* a, b, m, *com* $m > 1$. *Desse modo, para que a congruência* $ax \equiv b \bmod m$ *possua solução é necessário e suficiente que* $(a, m)|b$.

Demonstração 2.2.1.

($\Rightarrow$) *Suponha, a princípio, que a congruência* $ax \equiv b \text{ (mod } m)$ *possua uma solução* x_0. *Desse modo temos que* $ax_0 \equiv b \text{ (mod } m)$ *e, consequentemente,* $m|ax_0 - b$. *Assim, existe* $y_0 \in \mathbb{Z}$ *de tal forma que* $ax_0 - b = my_0$. *Segue que a equação* $ax - my = b$ *admite solução. Logo, podemos concluir* $(a, m)|b$.

($\Leftarrow$) *De maneira recíproca, considere* $(a, m)|b$. *Daí, podemos afirmar, claramente, que a equação* $ax - my = b$ *admite solução. Segue que* $ax = b + my$ *e, em consequência disso,* x *é solução da congruência* $ax \equiv b(modm)$, *pois* $ax - b = my$.

Note que toda solução particular x_0 da congruência $ax \equiv b \bmod m$ determina uma quantidade infinita de soluções, pois todo $x \equiv x_0 \bmod m$ é também solução da congruência, como pode ser visto abaixo:

$$ax \equiv ax_0 \equiv b \text{ (modm)}.$$

Na prática, tratamos como iguais duas soluções quaisquer da congruência $ax \equiv b$ (mod m) que são côngruas módulo m, mesmo que elas não sejam iguais no sentido tradicional. Por exemplo, $x = 2$ e $x = 7$ satisfazem a congruência linear $4x \equiv 3 \text{ (mod } 5)$. Como $2 \equiv 7 \text{ (mod } 5)$, tratamos 2 e 7 como a mesma solução da congruência linear $4x \equiv 3 \text{ (mod } 5)$. Por outro lado, $x = 3$ e $x = 5$ são soluções incongruentes (não congruentes) da equação $2x \equiv 6 \text{ (mod } 4)$, pois $4 \nmid 5 - 3$. Ou seja, quando falamos do número de soluções da congruência linear $ax \equiv b$ (mod m), estaremos contando somente aquelas que são incongruentes módulo m.

Desse modo, almejando encontrar a coleção completa de soluções duas a duas incongruentes módulo m, as quais serão chamadas de sistema completo de soluções não congruentes é que enunciamos o teorema a seguir.

Teorema 2.2. *[6] Considere os inteiros a, b, m, com $m > 1$ e $d = (a, m)|b$. Se x_0 é uma solução da congruência $ax \equiv b \ mod \ m$, então temos em consequência que*

$$x_0, x_0 + \frac{m}{d}, x_0 + 2.\frac{m}{d}, ..., x_0 + (d-1).\frac{m}{d},$$

formam um sistema completo de soluções da congruência, duas a duas não congruentes módulo m.

Demonstração 2.2.2. *Afirmamos inicialmente que toda solução $\tilde{x}$ da congruência $ax \equiv b \ (mod \ m)$ é congruente a $x_0 + k\frac{m}{d}$ módulo m, para algum $0 \leqslant k < d$.*

Para demonstrar este fato, observe que se $\tilde{x}$ é uma solução da congruência, então,

$$a\tilde{x} \equiv ax_0 \ (mod \ m),$$

consequentemente, obtemos

$$\tilde{x} \equiv x_0 \ (mod \ \frac{m}{d}).$$

Portanto, temos $\tilde{x} - x_0 = \frac{km}{d}$. Segue pela Divisão Euclidiana que existe $0 \leqslant k < d$ de tal modo que $k = qd + k$ e, consequentemente,

$$\tilde{x} = x_0 + qm + k\frac{m}{d} \equiv x_0 + k\frac{m}{d} \ (mod \ m).$$

Finalmente, note que estes números são dois a dois incongruentes módulo m, pois quando $0 \leqslant k, l < d$, temos

$$x_0 + k\frac{m}{d} \equiv x_0 + l\frac{m}{d} \ (mod \ m),$$

daí

$$k\frac{m}{d} \equiv l\frac{m}{d} \ (mod \ m).$$

Como $0 \leqslant k, l < d$, então $0 \leqslant k\frac{m}{d}, l\frac{m}{d} < m$, e como m divide $|k\frac{m}{d} - l\frac{m}{d}|$, segue-se que $k\frac{m}{d} = l\frac{m}{d}$ e, portanto, $k = l$.

Exemplo 2.11. *Vamos resolver a seguinte congruência $6x \equiv 4 \ mod \ 10$.*

Como o mdc $d = (6, 10) = 2$ divide 4, então, de acordo com o teorema anterior, esta congruência tem $d = 2$ soluções módulo 10.

Fazendo os cálculos por tentativa e erro, obtemos a solução $x_0 = 4$. Daí, as soluções módulo 10 são 4 e $4 + \frac{10}{2}$, isto é, 4 e 9.

Uma observação a respeito do teorema enunciado mais acima aparece quando tomamos $(a, m) = 1$, pois daí a congruência $ax \equiv b$ (mod m) passa a possuir uma única solução módulo m.

Definição 2.3. *Dizemos que a é invertível, módulo m, com $(m > 1)$, se existir x tal que a congruência linear $ax \equiv 1 \ (mod \ m)$ tem solução.*

Proposição 2.4. *[6] Para que um inteiro a seja invertível módulo m* $(m > 1)$ *é necessário e suficiente que* $(a, m) = 1$. *Neste caso, quaisquer dois inversos de a módulo m são congruentes, módulo m.*

Demonstração 2.2.3.

$(\Rightarrow)$ *Note que se a for invertível módulo m, então existe* $x \in \mathbb{Z}$ *tal que* $ax \equiv 1$ *(mod m). Segue que existe* $y \in \mathbb{Z}$ *para o qual* $ax = my + 1$ *ou podemos escrever ainda* $ax - ym = 1$. *Portanto, obtemos* $(a, m) = 1$.

$(\Leftarrow)$ *De maneira recíproca, note que pelo teorema de Bézout obtemos a garantia de que o mdc de dois inteiros sempre pode ser escritos como combinação linear dos mesmos. Segue daí que se* $(a, m) = 1$, *então existem* $x, y \in \mathbb{Z}$ *tais que* $ax + my = 1$ *e, consequentemente,* $ax \equiv 1$ *(mod m).*

Por fim, vamos mostrar que a possui um único inverso módulo m. Considere x e y inversos de a, módulo m. Segue que:

$$ax \equiv 1 \equiv ay \text{ (mod } m),$$

o que implica $ax \equiv ay$ *(mod m). Entretanto, como* $(a, m) = 1$, *então podemos realizar o cancelamento em ambos os lados da congruência, ou seja, obtemos* $x \equiv y$ *(mod m). Desse modo, a possui um único inverso módulo m.*

Exemplo 2.12. *Observe que as congruências a seguir não tem solução:*

a) $4x \equiv 1$ *(mod 6)*

Observe que o mdc $(4, 6) = 2 \neq 1$, *segue que não existe x que satisfaça tal congruência.*

b) $15x \equiv 1$ *(mod 10)*

De modo semelhante ao item anterior desta questão, a congruência linear acima não possui solução, pois 15 *não possui inverso módulo* 10.

A seguir vamos resolver o problema 3 do nível 3 da 2ª fase da 37ª Olimpíada Brasileira de Matemática, a fim de justificar, mesmo que parcialmente, a necessidade da abordagem de conteúdos da teoria dos números no ensino básico.

Exemplo 2.13. *Qual é o menor inteiro* $a > 1$ *para o qual existe n inteiro positivo tal que* $a^{2^n} - 1$ *é múltiplo de* 2015*?*

Solução. Antes de darmos início a resolução deste problema vamos enunciar e demonstrar um Lema que servirá como uma forte ferramenta para nossa solução.

Lema 2.1. *[9] Considere* $a > 1$ *inteiro e* $k, l \in \mathbb{N}$. *Desse modo temos* $(a^k - 1, a^l - 1) = a^{(k,l)} - 1$. *Em particular,* $a^k \equiv 1$ *(mod m) e* $a^l \equiv 1$ *(mod m)* $\Rightarrow a^{(k,l)} \equiv 1$ *(mod m).*

Demonstração 2.2.4. *Considere a princípio* $d = mdc(a^k - 1, a^l - 1)$. *Então podemos escrever* $a^k \equiv 1$ *(mod d) e* $a^l \equiv 1$ *(mod d) e, portanto,* $a^{kx+ly} \equiv 1$ *(mod d),* $\forall x, y \in \mathbb{Z}$. *Pelo Teorema de Bezóut, o menor valor inteiro de* $kx + ly$, *com* $x, y \in \mathbb{Z}$ *é* $mdc(k, l)$, *logo* $a^{(k,l)} \equiv 1$ *(mod d), isto é,*

$$d | a^{(k,l)} - 1 \Rightarrow d \leqslant a^{(k,l)} - 1.$$

Por outro lado, como

i) $mdc(k,l)|k$;

ii) $mdc(k,l)|l$;

iii) $a^k \equiv 1(moda^{(k,l)} - 1)$

iv) $a^l \equiv 1(moda^{(k,l)} - 1)$

então podemos escrever $a^{(k,l)} - 1|a^k - 1$ *e* $a^{(k,l)} - 1|a^l - 1$, *consequentemente, obtemos*

$$d \geqslant a^{(k,l)} - 1.$$

Concluímos então que $d = a^{k,l)} - 1$. *E está provado este Lema.*

Voltando a resolução do exemplo, veja que $2015 = 5.13.31$. *Então basta que* $a^{2^n} - 1$ *seja múltiplo de* $5, 13$ *e* 31 *para algum* $n \in \mathbb{N}$. *O número a não pode ser múltiplo de nenhum desses primos.*

Pelo Pequeno Teorema de Fermat $a^4 = a^{5-1} \equiv 1$ *(mod 5), assim a pode ser qualquer inteiro positivo não múltiplo de* 5.

Além disso $a^{12} = a^{13-1} \equiv 1$ *(mod 13), como* $(2^n, 12) \leqslant 4$, *devemos ter:*

$$a^{(2^n,12)} \equiv 1 \text{ (mod 13)} \Rightarrow a^4 \equiv 1 \text{ (mod 13)} \Leftrightarrow a \equiv \pm 1, \pm 5 \text{ (mod 13)}.$$

Finalmente, $a^{30} = a^{31-1} \equiv 1$ *(mod 31). Daí,*

$$a^{(2^n,30)} \equiv 1 \text{ (mod 31)} \Rightarrow a^2 \equiv 1 \text{ (mod 31)} \Leftrightarrow a \equiv \pm 1 \text{ (mod 31)}.$$

Com isso podemos formar a seguinte tabela com os menores valores de $a > 1$, *não múltiplos de* 5, *que satisfazem cada uma das congruências. Veja:*

Equações	$a \equiv 1$ mod 13	$a \equiv 5$ mod 13	$a \equiv 8$ mod 13	$a \equiv 12$ mod 13
$a \equiv 1$ mod 31	$a = 404$	$a = 187$	$a = 528$	$a = 311$
$a \equiv 30$ mod 31	$a = 92$	$a = 278$	$a = 216$	$a = 402$

Tabela 2.4: Possíveis Valores de a.

Dessa forma, notamos que o valor mínimo de a é 92. *Nesse caso, podemos escolher* $n = 2$ *e* $92^4 - 1$ *é múltiplo de 2015.*

2.3 Teorema Chinês dos Restos

Neste capítulo estudaremos a solução de sistemas de congruências lineares, baseado no que ficou conhecido como Teorema Chinês de Restos.

Objetivamos que ao final deste capítulo possamos compreender o algoritmo baseado no Teorema Chinês dos Restos.

2.3.1 Um Pouco da História

Na antiguidade, os generais chineses costumavam contar suas tropas perdidas após a guerra da seguinte forma: ordenavam que as tropas formassem várias colunas com um determinado tamanho e depois contavam quantas sobravam, e faziam isto para vários tamanhos diferentes.

Por exemplo, um general chinês possuia 1200 tropas antes da guerra. Após a guerra, ele alinhou as tropas de 5 em 5 de forma que sobraram 3 tropas. Quando alinhou de 6 em 6, também sobraram 3 tropas. Quando alinhou de 7 em 7, sobrou 1 tropa. E quando alinhou de 11 em 11, não sobrou nenhuma tropa. Quantas tropas o general tinha?

Para resolver este problema, é necessário saber lidar com congruências. Além disso, vamos utilizar uma poderosa arma em Teoria dos Números, chamada de Teorema Chinês dos Restos. De fato, o problema apresentado acima é uma aplicação direta deste teorema.

Basta então um pequeno esforço para interpretar o problema. Quando o general alinha suas tropas, formando colunas de tamanho n, ele está realizando uma divisão do número de tropas por n, e depois verificando seu resto.

Observe que, na prática, contar o resto é muito mais fácil que contar o número total, ou o quociente. Na verdade, quem conhece um pouco de Teoria dos Números, sabe que raramente estamos interessados no quociente, o resto da divisão é o que importa.

2.3.2 O Teorema Chinês dos Restos

É importante o estudo do Teorema Chinês dos Restos devido a sua facilidade em resolver sistemas de congruências. Através do mesmo podemos solucionar problemas advindos da criptografia, simplificar o cálculo de potências módulo m em algumas situações, realizar cálculos com números de alta cardinalidade através de cálculos com números de cardinalidade menores, dentre outras aplicações.

Começaremos resolvendo um problema de sistema de congruências utilizando apenas os métodos que conhecemos até o momento. Queremos mostrar através deste exemplo que as ferramentas que dispomos até o instante, mesmo que suficientes para resolver problemas como este, as mesmas não se mostram eficientes para resolver casos em que a quantidade de equações seja maior, digamos cinco, seis ou sete equações num sistema de congruências.

Exemplo 2.14. *Um bando de 19 piratas, ao tentar dividir igualmente entre si as moedas de uma arca, verificou que haveria um sobra de 3 moedas. Seguiu-se uma discussão, na qual um pirata foi morto. Na nova tentativa de divisão, já com um pirata a menos, verificou-se que haveria a sobra de uma moeda. Nova confusão, e mais um pirata foi morto. Então, por fim, eles conseguiram dividir sobrando desta vez 11 moedas. Qual o menor número de moedas que a arca poderia conter?*

Resolver tal problema implica solucionar o seguinte sistema de congruências lineares

$N \equiv 3 \bmod 19$

$N \equiv 1 \bmod 18$

$N \equiv 11 \bmod 17$.

Da congruência $N \equiv 3 \bmod 19$, podemos escrever $N = 19a + 3$, com $a \in \mathbb{Z}$, o qual substituímos tal valor de N em $N \equiv 1 \bmod 18$, obtendo

$$19a + 3 \equiv 1 \pmod{18}.$$

Segue que somando -3 a ambos os lados da congruência acima, obtemos:

$$19a \equiv -2 \pmod{18}.$$

Agora multiplicando ambos os lados pelo inverso multiplicativo de 19 módulo 18, o qual é o próprio 19, pois $361 \equiv 1 \bmod 18$.

Assim,

$$19a.1 \equiv (-2).(19.19) \pmod{18}.$$

Como $(18, 19) = 1$, então podemos cancelar e concluir que: temos:

$$a \equiv (-2).19 \equiv -2 \equiv 16 \pmod{18}.$$

Daí, podemos escrever $a = 18b + 16$, com $b \in \mathbb{Z}$.

Como temos $N = 19a + 3$, então reescrevemos

$$N = 19.(18b + 16) + 3 = 342b + 307.$$

Desse modo substituímos $N = 342b + 307$ em $N \equiv 11 \bmod 17$, resultando em

$$342b + 307 \equiv 11 \pmod{17}. \qquad (*)$$

Note que $342 \equiv 2 \bmod 17$, pois $17|342 - 2$, bem como $307 \equiv 1 \bmod 17$. Desse modo, através de $(*)$, escrevemos

$$2b + 1 \equiv 11 \pmod{17}.$$

Ao efetuarmos a soma de -1 a ambos os lados da congruência, temos

$$2b \equiv 10 \pmod{17}.$$

Como o inverso multiplicativo de 2 módulo 17 é o 9, pois $2 \cdot 9 = 1 \cdot 17 + 1$, fazemos a multiplicação do mesmo a ambos os lados da congruência e obtemos

$$9 \cdot 2b \equiv 9 \cdot 10 \pmod{17}.$$

Sendo $90 = 5 \cdot 17 + 5$, escrevemos

$$b \equiv 90 \equiv 5 \pmod{17}.$$

Escrevemos então $b = 17c + 5$, com $c \in \mathbb{Z}$.

Voltando a $N = 342b + 307$, realizamos a substituição

$$N = 342.(17c + 5) + 307 = 5814c + 2017.$$

Assim, a equação acima equivale à congruência $N \equiv 2017 \bmod 5814$, isto é, temos como solução para este problema 2017 moedas, no mínimo, existentes na arca.

Entretanto, a solução pode se dar de diversas formas, pois

$$2017, 2017 + 5814, 2017 + 2.5814, 2017 + 3.5814, ...$$

são soluções deste problema.

Observe que na resolução deste problema utilizamos apenas os conhecimentos que obtivemos até este momento a respeito de congruências lineares. A solução ficou extensa e, seria bem mais trabalhosa caso tivéssemos um sistema formado por mais congruências que este, pois as substituições devem ocorrer em todas as congruências dadas de maneira semelhante ao que fizemos anteriormente na solução deste exemplo.

Enunciamos a seguir um resultado bastante significativo para resolução de sistemas de congruências. Denominado Teorema Chinês dos Restos, este traz uma forma alternativa de resolução de sistemas de congruências lineares.

Teorema 2.3. *Sejam $m_1, m_2, ..., m_k$ inteiros positivos, primos dois a dois. Então o sistema*

$x \equiv A_1 \ mod \ m_1$

$x \equiv A_2 \ mod \ m_2$

$...$

$x \equiv A_k \ mod \ m_k$

tem solução única mod $L = m_1.m_2...m_k$ e esta solução é dada por

$$x = A_1.M_1.\tilde{M_1}^{-1} + A_2.M_2.\tilde{M_2}^{-1} + ... + A_k.M_k.\tilde{M_k}^{-1},$$

onde $M_i = \dfrac{L}{m_i}$, $\tilde{M_i} \equiv M_i (mod m_i)$ e $\tilde{M_i}^{-1}\tilde{M_i} \equiv 1 (mod m_i)$.

Demonstração 2.3.1. *Observe que os M_i, com $i = 1, 2, ..., k$ são os produtos a seguir:*

$$M_1 = m_2.m_3...m_k$$

$$M_2 = m_1.m_3...m_k$$

$$...$$

$$M_k = m_1.m_2...m_{k-1}$$

Queremos mostrar, inicialmente, que a solução de fato existe e que a mesma tem a forma

$$x = A_1.M_1.\tilde{M_1^{-1}} + A_2.M_2.\tilde{M_2}^{-1} + ... + A_k.M_k.\tilde{M_k}^{-1}.$$

Note que $x \equiv A_1.M_1.\tilde{M_1}^{-1} (modm_1)$, *pois* $M_2 \equiv 0 (modm_1)$, $M_3 \equiv 0 (mod\ m_1)$, ..., $M_k \equiv 0 (mod\ m_1)$. *Como* $M_i \equiv \tilde{M_i} (mod\ m_i)$, *segue que* $x \equiv A_1.M_1.\tilde{M_1}^{-1} \equiv A_1.\tilde{M_1}.\tilde{M_1}^{-1} \equiv A_1 (mod\ m_1)$.

Dessa mesma forma, obtemos também $x \equiv A_2.M_2.\tilde{M_2}^{-1} \equiv A_2.\tilde{M_2}.\tilde{M_2}^{-1} \equiv A_2 (mod\ m_2)$, ..., $x \equiv A_k.M_k.\tilde{M_k}^{-1} \equiv A_k.\tilde{M_k}.\tilde{M_k}^{-1} \equiv A_k (mod\ m_k)$.

Concluímos, desse modo, que a solução do sistema de congruência realmente é dado por

$$x = A_1.M_1.\tilde{M_1}^{-1} + A_2.M_2.\tilde{M_2}^{-1} + ... + A_k.M_k.\tilde{M_k}^{-1}.$$

Agora nos resta provar que esta solução que encontramos é única módulo $m_1.m_2...m_k$.

Para isso, consideremos x solução do sistema e suponhamos a existência de outra solução y para o mesmo sistema dado de tal modo que não seja congruente a x módulo $m_1.m_2...m_k$. *Assim, escrevemos*

$$y \equiv A_1 (mod\ m_1)$$

$$x \equiv A_1 (mod\ m_1).$$

Então,

$$y - x \equiv 0 (mod\ m_1),$$

Daí,

$$m_1 | y - x.$$

De forma análoga observamos

$$m_2 | y - x$$

$$m_3 | y - x$$

$$...$$

$$m_k | y - x.$$

Assim, o fato seguinte se verifica

$$m_1.m_2...m_k | y - x,$$

portanto $y - x \equiv 0 (mod\ m_1.m_2...m_k)$, *isto é,* $y \equiv x (mod\ m_1.m_2...m_k)$.

Chegamos então a uma conclusão absurda, pois contraria nossa hipótese inicial. Assim, observamos que a solução para o sistema é única módulo $m_1.m_2...m_k$.

Proposição 2.5. *[6] O sistema de congruências a seguir*

$$X \equiv A_1 (mod\ m_1), X \equiv A_2 (mod\ m_2)$$

admite solução se, e somente se, $A_2 \equiv A_1 (\ mod\ (m_1, m_2))$. *Além disso, dada uma solução a do sistema, um número* a' *é também uma solução se, e somente se,* $a' \equiv a (\ mod\ [m_1, m_2])$.

Demonstração 2.3.2. *Observe inicialmente que o sistema do enunciado da proposição admite uma solução se, e somente se, existem* $a, y, z \in \mathbb{Z}$ *tais que* $a - A_1 = ym_1$ *e* $a - A_2 = zm_2$. *Desse modo, a existência de soluções do sistema é equivalente à existência de soluções da equação diofantina*

$$ym_1 - zm_2 = A_2 - A_1.$$

Observamos que essa equação diofantina possui solução se, e somente se, (m_1, m_2) *divide* $A_2 - A_1$*, o que equivale a seguinte congruência*

$$A_2 \equiv A_1 (mod (m_1, m_2)).$$

Agora suponhamos que a seja uma solução do sistema do enunciado. Se tivermos a' *como outra solução do sistema, então* $a' \equiv A_1 \equiv a \ (mod\ m_1)$ *e* $a' \equiv A_2 \equiv a \ (mod\ m_2)$*, o que implica que*

$$a' \equiv a \ (mod\ [m_1, m_2]).$$

Por outro lado, se um número a' *é tal que* $a' \equiv a \ (mod\ [m_1, m_2])$*, então* $a' \equiv a \equiv A_1 \ (mod\ m_1)$ *e* $a' \equiv a \equiv A_2 \ (mod\ m_2)$*. Portanto, chegamos a conclusão de que* a' *é solução do sistema dado.*

A seguir vamos enunciar e provar o Teorema Chinês dos Restos em sua forma generalizada, isto é, quando os $m_i's$ não forem primos entre si.

Teorema 2.4. *[6] O sistema de congruências a seguir*

$$X \equiv A_i \ (mod\ m_i), i = 1, ..., s$$

admite solução se, e somente se,

$$A_i \equiv A_j \ mod\ (m_i, m_j), \forall i, j = 1, ..., s.$$

Desse modo, a solução é única módulo $[m_1, ..., m_s]$*.*

Demonstração 2.3.3. *Faremos esta demonstração pelo método da indução sobre s. O caso* $s = 2$ *é dado pela proposição* 3.5*.*

Vamos supor então que a propriedade seja válida para $s - 1$*. Desse modo,pela hipótese de indução, temos que o sistema a seguir*

$$X \equiv A_i \ (mod\ m_i), i = 1, ..., s - 1,$$

admite uma única solução A módulo $[m_1, ..., m_{s-1}]$*. Todavia, temos ainda que mostrar que o sistema a seguir*

$$X \equiv A \ (mod\ [m_1, ..., m_{s-1}])$$

$$X \equiv A_r \ (mod\ m_s)$$

possui uma única solução módulo $[m_1, ..., m_{s-1}]$*. Para realizar tal demonstração, observando o caso para* $s = 2$ *e percebemos que nos resta entao mostrar que*

$$A_s \equiv A \ (mod\ (m_s, [m_1, ..., m_{s-1}])).$$

Considerando que temos $A \equiv A_i \ (mod\ m_i)$ *para* $i = 1, ..., s - 1,$*, podemos escrever deste modo que* $A \equiv A_i \ (mod\ (m_s, m_i))$*, para todo i, e, portanto* $A_s \equiv A \ (mod\ (m_s, m_i))$*, para todo* $i = 1, ..., s - 1$*, o que acarreta que*

$$A_s \equiv A \ (mod\ [(m_s, m_1), (m_s, m_2), ..., (m_s, m_{s-1})]).$$

Consequentemente, obtemos

$$A_s \equiv A \ (mod \ (m_s, [m_1, m_2, ..., m_{s-1}]).$$

Chegamos então a conclusão de que a solução é única módulo o MMC a seguir

$$[m_s, [m_1, m_2, ..., m_{s-1}]] = [m_1, m_2, ..., m_{s-1}, m_s].$$

Vamos generalizar o algoritmo para determinar as soluções do sistema exposto no Teorema anterior.

Sejam $m_1, m_2, ..., m_s$ números inteiros, estabelecemos as seguintes notações:

$$M = [m_1, ..., m_s]$$

e

$$M_i = \frac{M}{m_i}, i = 1, 2, ..., s.$$

Lema 2.2. *[6] A partir das notações expostas anteriormente, existem inteiros $x_1, ..., x_s$ tais que*

$$x_1 M_1 + ... + x_s M_s = 1.$$

Lema 2.3. *[6] Para todos os valores de $i, j = 1, ..., s$, temos que*

$$m_j | M_i (m_i, m_j).$$

Teorema 2.5. *[6] Caso o sistema dado no teorema* 3.4 *admitir solução, as soluções são dadas do modo seguinte*

$$x = A_1 x_1 M_1 + ... + A_s x_s M_s + kM,$$

onde $k \in \mathbb{Z}$ e $x_1, x_2, ..., x_s$ são tais que

$$x_1 M_1 + ... + x_s M_s = 1.$$

Demonstração 2.3.4. *Observe que pelo teorema* 3.4 *temos o seguinte*

$$A_i \equiv A_j \ mod \ (m_i, m_j), \forall i, j = 1, ..., s.$$

Realizando a multiplicação por M_i a ambos os lados de cada uma das congruências, temos

$$M_i A_i \equiv M_i A_j \ mod \ M_i (m_i, m_j),$$

assim, pelo Lema 3.3*, podemos escrever*

$$M_i A_i \equiv M_i A_j \ mod \ m_j.$$

Agora, fazendo a multiplicação em ambos os lados das congruências por x_i, obtemos

$$x_i M_i A_i \equiv x_i M_i A_j \ mod \ m_j.$$

Escrevendo o somatório ao variar i, temos, para todo $j = 1, ..., s$,

$$x = x_1 M_1 A_1 + ... + x_s M_s A_s \equiv A_j(x_1 M_1 + ... + x_s M_s) = A_j \ mod \ m_j,$$

finalizando nossa demonstração.

Capítulo 3

Proposta de um Novo Método de Resolução de Sistema de Congruências Lineares

3.1 Algoritmos

Listamos nas subseções abaixo três algoritmos que auxiliarão na resolução se sistemas de congruências.

3.1.1 Algoritmo 1: Encontrar o MDC de dois números a e b

Este algoritmo é muito conhecido, e baseia-se no Lema 2.1 (Lema de Euclides).

Sejam a e b dois inteiros com $b > a$. Considere também q_1 e r_1 o quociente e o resto da divisão euclidiana de b por a. Então

$$b = aq_1 + r_1.$$

Pelo Lema de Euclides, temos:

$$(b, a) = (a, r_1).$$

Dividindo-se a por r_1 , obtemos

$$a = r_1q_2 + r_2.$$

Aplicando sucessivamente o processo, até obtermos $r_n = 0$, temos:

$$(b, a) = (a, r_1) = (r_1, r_2) = (r_2, r_3) = ... = (r_{(n-1)}, r_n) = (r_{(n-1)}, 0) = r_{(n-1)}.$$

O processo pode ser realizado como na tabela abaixo:

Dividendo	Divisor	Quociente	Resto
b	a	q_1	r_1
a	r_1	q_2	r_2
r_1	r_2	q_3	r_3
...	...	...	...
r_{n-3}	r_{n-2}	q_{n-1}	$r_{n-1} = d$
r_{n-2}	r_{n-1}	q_n	$r_n = 0$

Tabela 3.1: Encontrando o MDC de dois números a e b.

Na tabela acima denotamos por d o MDC entre os inteiros a e b.

É de se observar que este algoritmo é bastante simples e auxilia na busca pelo MDC de dois inteiros positivos de maneira célere. Veja o exemplo a seguir.

Exemplo 3.1. *Uma empresa de logística é composta de duas áreas: administrativa e operacional. A área administrativa é composta de* 72 *funcionários e a operacional de* 112*. Ao final do ano, a empresa realiza uma integração entre as duas áreas, de modo que todos os funcionários participem ativamente. As equipes devem conter o mesmo número de funcionários com o maior número possível. Determine quantos funcionários devem participar de cada equipe.*

Solução.

Observe que para resolução deste problema devemos determinar o MDC entre 72 *e* 112*, pois daí teremos a quantidade máxima de funcionários por equipe, como é exigida.*

Assim, seguindo o algoritmo exposto na tabela anterior, inserimos os valores dados e os obtidos a partir das operações realizadas. Veja:

Dividendo	Divisor	Quociente	Resto
112	72	1	40
72	40	1	32
40	32	1	$8 = d$
32	8	4	0

Tabela 3.2: Encontrando o MDC de dois números 72 e 112.

Concluímos, dessa forma, que a quantidade máxima exigida por equipe é de 8 *funcionários.*

3.1.2 Algoritmo 2: Encontrar inteiros m e n tais que $d = (a, b) = am + bn$

O algoritmo que trataremos nesta subseção não figura em livros de autores com trabalhos voltados para aritmética como Antonio Caminha, Abramo Hefez, Carlos Gustavo Moreira, Nicolau Saldanha, entre outros, os quais são bem conceituados no país e fora dele. Todavia, há estudos voltados a construção de algoritmos como este e derivados deles em trabalhos internacionais, como podemos observar em [11].

Considere os inteiros a e b de modo que $b > a$. Utiliza-se a Tabela 4.14 para a e b , até chegar no valor do MDC $r_{s-1} = d$, e em seguida inserimos duas colunas adicionais com os números 0 e 1 como pode ser vista abaixo:

				X_i	Y_i
					0
Dividendo	Divisor	Quociente	Resto	0	1
b	a	q_1	r_1	1	
a	r_1	q_2	r_2		
r_1	r_2	q_3	r_3		
...	...	...	...		
r_{s-3}	r_{s-2}	q_{s-1}	$r_{s-1} = d$		
r_{s-2}	r_{s-1}	q_s	$r_s = 0$		

Tabela 3.3: Encontrando inteiros m e n tais que $d = (a, b) = am + bn$

O objetivo é encontrar inteiros m e n de tal forma que o MDC d seja igual a $(a, b) = am + bn$.
Na tabela acima, completamos a primeira coluna em branco com a sequência $X_1, X_2, ..., X_s$, onde

$$\begin{aligned} X_1 &= 0 \\ X_2 &= 1 \\ X_k &= -q_{(k-1)}X_{(k-1)} + X_{(k-2)}. \end{aligned}$$

De forma análoga, completamos a segunda coluna em branco com a sequência $Y_0, Y_1, ..., Y_s$, onde

$$\begin{aligned} Y_0 &= 0 \\ Y_1 &= 1 \\ Y_k &= -q_{(k-1)}Y_{(k-1)} + Y_{(k-2)}. \end{aligned}$$

				X_i	Y_i
					$0 = Y_0$
Dividendo	Divisor	Quociente	Resto	$0 = X_1$	$1 = Y_1$
b	a	q_1	r_1	$1 = X_2$	Y_2
a	r_1	q_2	r_2	X_3	Y_3
r_1	r_2	q_3	r_3	X_4	Y_4
...	...	...	...	...	...
r_{s-3}	r_{s-2}	q_{s-1}	$r_{s-1} = d$	X_s	Y_s
r_{s-2}	r_{s-1}	q_s	$r_s = o$	X_{s+1}	Y_{s+1}

Tabela 3.4: Encontrando inteiros m e n tais que $d = (a, b) = am + bn$

Então

$$d = (a, b) = aX_s + bY_s.$$

Em seguida faremos a demonstração a respeito de

$$r_{k-1} = aX_k + bY_k.$$

Vamos mostrar por indução sobre k, para $k \geqslant 2$, que esta igualdade acima é válida.

Note que para $k = 2$, temos $r_1 = a - bq_1 = aX_2 + bY_2$,

Suponha válido para r_t, para todo $t \leqslant k - 1$. Temos

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_k \\ &= (aX_{k-1} + bY_{k-1}) - (aX_k + bY_k)q_k \\ &= a(-q_kX_k + X_{k-1}) + b(-q_kY_k + Y_{k-1}) \\ &= aX_{k+1} + bY_{k+1}. \end{aligned}$$

Assim, a prova por indução fica completa.

Exemplo 3.2. *Determine o MDC= d entre* 292 *e* 348 *e valores de m e n tais que* $d = 348m + 292n$.

Solução.

Vamos construir uma tabela como observado no conteúdo desta subseção seguindo os passos determinados por nosso algoritmo.

Dividendo	Divisor	Quociente	Resto
348	292	1	56
292	56	5	12
56	12	4	8
12	8	1	$4 = d$
8	4	2	0

Tabela 3.5: Primeira inserção de valores do exemplo.

Ao inserir as duas colunas à direita desta tabela como vemos a seguir, partiremos para os cálculos necessários ao seu devido preenchimento. Como $X_k = -q_{k-1}.X_{k-1} + X_{k-2}$ *e* $Y_k = -q_{k-1}.Y_{k-1} + Y_{k-2}$, *então após algumas operações básicas chegamos a tabela a seguir:*

				X_i	Y_i
					0
Dividendo	Divisor	Quociente	Resto	0	1
348	292	1	56	1	-1
292	56	5	12	-5	6
56	12	4	8	21	-25
12	8	1	$4 = d$	$-26 = m$	$31 = n$
8	4	2	0	73	-87

Tabela 3.6: Inserção dos valores nas duas colunas à direita da tabela inicial do exemplo.

Assim, concluímos que o MDC entre 348 *e* 292 *é* 4, *bem como* $m = -26$ *e* $n = 31$.

3.1.3 Algoritmo 3: Encontrando o inverso de a módulo n: $(a, n) = 1$

Este algoritmo é consequência do Algoritmo 2, pois aplicando este chegamos a

$$nX_k + aY_k = 1.$$

Então Y_k é o inverso de a módulo n, ou seja, satisfaz à equação:

$$aY_k \equiv 1 \pmod{n}.$$

Assim, basta acrescentar a coluna dos Y_i , como descrito logo mais.

Utiliza-se a Tabela 4.1 para n e a , até chegar em $r_{s-1} = 1$, inserindo uma coluna adicional com os números 0 e 1 como abaixo:

				Y_i
				0
Dividendo	Divisor	Quociente	Resto	1
n	a	q_1	r_1	
a	r_1	q_2	r_2	
r_1	r_2	q_3	r_3	
...	...	...	...	
r_{s-3}	r_{s-2}	q_{s-1}	1	

Tabela 3.7: Encontrando o inverso de a módulo n: $(a, n) = 1$

Completa-se a coluna em branco com a sequência $Y_0, Y_1, ..., Y_s$, onde

$$\begin{aligned} Y_0 &= 0 \\ Y_1 &= 1 \\ Y_k &= -q_{k-1}Y_{k-1} + Y_{k-2}. \end{aligned}$$

obtendo a tabela acima.

				Y_i
				$0 = Y_0$
Dividendo	Divisor	Quociente	Resto	$1 = Y_1$
n	a	q_1	r_1	Y_2
a	r_1	q_2	r_2	Y_3
r_1	r_2	q_3	r_3	Y_4
...	...	...	...	...
r_{s-3}	r_{s-2}	q_{s-1}	1	Y_s

Tabela 3.8: Encontrando o inverso de a módulo n: $(a, n) = 1$

Do que vimos, tal Y_k satisfaz $aY_k \equiv 1(modn)$.

Exemplo 3.3. *Encontrar m e n tais que* $60m + 13n = 1$.

Solução. Primeiramente encontramos o mdc:

Dividendo	Divisor	Quociente	Resto
60	13	4	8
13	8	1	5
8	5	1	3
5	3	1	2
3	2	1	1

Tabela 3.9: Primeira inserção de dados do Exemplo.

Acrescentamos as duas colunas com zero e um no início:

				X_i	Y_i
					0
Dividendo	Divisor	Quociente	Resto	0	1
60	13	4	8	1	
13	8	1	5		
8	5	1	3		
5	3	1	2		
3	2	1	1		

Tabela 3.10: Segunda inserção de dados do Exemplo.

A partir de então usamos as fórmulas utilizadas no algoritmo anterior, quais sejam $X_k = -q_{k-1}.X_{k-1} + X_{k-2}$ e $Y_k = -q_{k-1}.Y_{k-1} + Y_{k-2}$ e insere os resultados dos cálculos na tabela seguinte:

				X_i	Y_i
					0
Dividendo	Divisor	Quociente	Resto	0	1
60	13	4	8	1	-4
13	8	1	5	-1	5
8	5	1	3	2	-9
5	3	1	2	-3	14
3	2	1	1	5	-23

Tabela 3.11: Terceira inserção de dados do Exemplo..

$$60(+5) + 13(-23) = 1.$$

3.1.4 Algoritmo 4:Encontrar inteiros $x_i's$ no enunciado do Lema 3.2

O algoritmo apresentado a seguir será de muita utilidade, pois o teorema 3.5 trata a respeito da existência dos $x_i's$, e a seguir propomos este algoritmo a fim de calculá-los.

Observe que estamos relatando o uso do algoritmo 2 por recorrência, considerando que:

$$(M_1, ..., M_n) = ((M_1, ..., M_{n-1}), M_n)$$

podemos perceber, por exemplo, que dados M_1, M_2, M_3 de modo que

$$x_1M_1 + x_2M_2 + x_3M_3 = 1$$

escrevemos $(M_1, M_2) = aM_1 + bM_2$.

Segue que $1 = ((M_1, M_2), M_3) = e.(M_1, M_2) + f.M_3 = e.(aM_1 + bM_2) + f.M_3 = ea.M_1 + eb.M_2 + f.M_3$.

Desse modo obtemos os coeficientes $x_i's$ desejados.

Exemplo 3.4. *Determine os valores de* x_1, x_2, x_3 *de modo que*

$$50x_1 + 45x_2 + 24x_3 = 1.$$

Solução.

Comparamos a princípio $M_1 = 50, M_2 = 45$ *e* $M_3 = 24$, *a fim de nos basearmos no modelo* $x_1M_1 + x_2M_2 + x_3M_3 = 1$.

Tomando o MDC $(50, 45) = 5$ *notamos claramente que podemos escrever* $5 = 1.50 + (-1).45$, *isto é,* $a = 1$ *e* $b = -1$.

Agora observe o MDC

$$1 = ((50, 45), 24) = e.(50, 45) + f.24 = e.5 + f.24 = 5.5 + (-1).24.$$

Segue que $e = 5$ *e* $f = -1$. *Desse modo, obtemos* $x_1 = e.a = 5.1 = 5$, $x_2 = e.b = 5.(-1) = -5$ *e* $x_3 = f = -1$.

3.2 Aplicação de Algoritmo na Resolução de Sistemas de Congruências

À medida que o número de equações aumenta, as dificuldades em operar com as congruências se eleva, pois a quantidade de substituições cresce e torna exaustivo a solução da questão.

Reservamos esta secção para mostrar um algoritmo que pode tranquilamente ser ministrado no ensino básico e que muito facilitará na resolução de problemas que surgem em diversas olimpíadas matemáticas.

Algoritmo: Caso Clássico

Para resolução deste problema, utilizamos um algoritmo bastante interessante, pois o mesmo se justifica pelo Teorema Chinês do Resto. Para isso criamos uma tabela cuja quantidade de linhas depende do

número de equações do sistema de congruências do problema em questão. Cada inserção que venha a ser feita nesta tabela refere-se à equação correspondente da mesma linha.

A respeito do Exemplo 3.14 que resolvemos na Subseção 3.3.2, observe que as três equações que compõe a primeira coluna da tabela criada abaixo dão uma síntese do problema enunciado.

Dispusemos logo abaixo o passo a passo de como devemos proceder para o preenchimento da tabela. É evidente que o leitor confeccionará apenas uma tabela e fará a inserção dos valores de forma mais ágil logo após o conhecimento do algoritmo que executaremos a seguir.

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$					
$N \equiv 1 \pmod{18}$					
$N \equiv 11 \pmod{17}$					

Tabela 3.12: Primeiro Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

A primeira coluna, a qual denominamos "A" deve conter os valores das classes de congruência indicadas no sistema ao lado. Inserimos então tais valores de acordo com a congruência respectiva, como visto na tabela abaixo.

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$	3				
$N \equiv 1 \pmod{18}$	1				
$N \equiv 11 \pmod{17}$	11				

Tabela 3.13: Segundo Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

A terceira coluna que corresponde a letra "M" é onde serão colocados os produtos de todos os "m_i", exceto o correspondente da linha. Veja na tabela seguinte como proceder a tais multiplicações.

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$	3	18.17			
$N \equiv 1 \pmod{18}$	1	19.17			
$N \equiv 11 \pmod{17}$	11	19.18			

Tabela 3.14: Terceiro Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

A coluna encabeçada por "$\tilde{M}$" indica que incluiremos na mesma as classes de congruência de cada M_i módulo m_i, respectivamente.

Como $18 \equiv -1 \pmod{19}$, $17 \equiv -2 \pmod{19}$, $19 \equiv 1 \pmod{18}$, $17 \equiv -1 \pmod{18}$, $19 \equiv 2 \pmod{17}$ e $18 \equiv 1 \pmod{17}$, seque que podemos escrever:

$18.17 \equiv (-1).(-2) \equiv 2 \pmod{19}$

$19.17 \equiv 1.(-1) \equiv -1 \equiv 17 \pmod{18}$

$19.18 \equiv 2.1 \equiv 2 \pmod{17}$.

Dessa forma, basta inserir tais valores na coluna indicada por "$\tilde{M}$".

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$	3	18.17	2		
$N \equiv 1 \pmod{18}$	1	19.17	17		
$N \equiv 11 \pmod{17}$	11	19.18	2		

Tabela 3.15: Quarto Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

Os valores que compõem a coluna indicada por "$\tilde{M}^{-1}$" refere-se ao inverso multiplicativo dos valores dispostos na coluna "$\tilde{M}$" tomados módulo m_i.

Observe que fazendo uso do Algoritmo 3, encontramos os inversos dos $\tilde{M}_i's$. Veja:

$2.10 = 20 \equiv 1 \pmod{19}$

$17.17 = 289 \equiv 1 \pmod{18}$

$2.9 = 18 \equiv 1 \pmod{17}$.

Basta inseri-los em suas respectivas posições como indicado na tabela seguinte.

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$	3	18.17	2	10	
$N \equiv 1 \pmod{18}$	1	19.17	17	17	
$N \equiv 11 \pmod{17}$	11	19.18	2	9	

Tabela 3.16: Quinto Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

Esta última coluna encabeçada por "$A.M.\tilde{M}^{-1}$" é bastante clara, pois trata do produto a ser tomado por valores disponíveis nas linhas anteriores. Façamos o acompanhamento dos produtos requeridos:

(3).(18.17).(10) = 9180

(1).(19.17).(17) = 5491

(11).(19.18).9 = 33858.

Após fazermos esta nossa última inserção na tabela, partiremos para nosso último passo da resolução deste problema.

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$N \equiv 3 \pmod{19}$	3	18.17	2	10	9180
$N \equiv 1 \pmod{18}$	1	19.17	17	17	5491
$N \equiv 11 \pmod{17}$	11	19.18	2	9	33858

Tabela 3.17: Sexto Passo do Algoritmo Aplicado ao Teorema Chinês dos Restos.

Agora, apenas nos resta calcular a soma dos valores da última coluna, indicada por "$A.M.\tilde{M}^{-1}$", e tomar sua classe de congruência módulo 19.18.17 = 5814. Assim, obtemos:

9180 + 5491 + 33858 = 48529 = 8.5814 + 2017 ≡ 2017 (mod 5814).

E, portanto a quantidade mínima de moedas que pode ter na arca é 2017 unidades. Observe que as quantidades de moedas pode tomar proporções maiores, desde que obedeça à congruência acima.

Exemplo 3.5. *Determine o resto da divisão de* 2^{327} *por 1463.*

Solução.

A princípio é importante notar que 1463=7.11.19. Daí, vamos encontrar a classe de equivalência de 2^{327} *módulo 7, em seguida módulo 11 e, por fim, módulo 19. Essa é a primeira etapa da nossa solução. Observe que podemos escrever:*

$$2^{327} \equiv X \ (mod\ 7).$$

Como 7 é um número primo, então este fato nos permite usar o Pequeno Teorema de Fermat. Assim, sabendo que $2^6 \equiv 1$ *(mod* 7*), segue que:*

$$2^{327} = (2^6)^{54}.2^3 \equiv 1^{54}.8 \equiv 1 \ (mod\ 7).$$

De maneira semelhante podemos fazer:

$$2^{327} = (2^{10})^{32}.2^7 \equiv 1^{32}.128 \equiv 7 \ (mod\ 11)$$

e

$$2^{327} = (2^{18})^{18}.2^3 \equiv 1^{18}.8 \equiv 8 \ (mod\ 19).$$

A segunda etapa de nossa solução consiste em resolver o seguinte sistema de congruências: $X \equiv 1$ *(mod* 7*)* $X \equiv 7$ *(mod* 11*)* $X \equiv 8$ *(mod* 19*).*

O Teorema chinês dos Restos nos permite afirmar que o este sistema tem solução única módulo 7.11.19 = 1463*, pois* 7*,* 11 *e* 19 *são primos entre si dois a dois.*

Note que 2^{237} *é uma solução para este sistema, no entanto este número é maior que* 1463*.*

O que o Teorema Chinês dos Restos nos garante afirmar é que há um número $X \in \mathbb{Z}$ *menos que* 1463 *que também satisfaz o sistema dado acima.*

Vamos aplicar o algoritmo estudado nesta secção para solucionar este nosso sistema. Observe a tabela a seguir com os valores dispostos em seus devidos lugares:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$X \equiv 1$ mod 7	1	209	6	6	1254
$X \equiv 7$ mod 11	7	233	1	1	931
$X \equiv 8$ mod 19	8	77	1	1	616

Tabela 3.18: Algoritmo para Resolução do Exemplo.

Observando que 1254 + 931 + 616 = 2801 ≡ 1338 *(mod* 1463*), concluímos que o resto da divisão desejada é 1338.*

Mesmo que tenhamos obtido uma fórmula exata para a solução de sistemas de congruências, isto foi feito ao preço de uma hipótese bastante forte, a de que os módulos são primos entre si. Surge então o seguinte questionamento: será que a fórmula continua verdadeira mesmo se esta hipótese não se verifica?

Algoritmo: Caso Geral

Vejamos a seguir dois exemplos em que os módulos não são primos entre si. A ideia é verificar que não é possível aplicar o algorítimo do Teorema Chinês dos Restos a casos como estes, pois a hipótese de os módulos m_i serem dois a dois primos entre si não se verifica.

Exemplo 3.6. *Resolva o sistema de congruências a seguir:*

$$x \equiv 1 \ (mod\ 2)$$

$$x \equiv 1 \ (mod\ 3)$$

$$x \equiv 3 \ (mod\ 4).$$

Solução.

Aparentemente temos aqui mais um sistema de congruências simples de ser resolvido através de nosso Teorema Chinês dos Restos, a princípio, vamos construir uma tabela semelhante a que viemos utilizando no algoritmo para resolver esse tipo de sistemas. Observe:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$x \equiv 1 \bmod 2$					
$x \equiv 1 \bmod 3$					
$x \equiv 3 \bmod 4$					

Tabela 3.19: Inserção das Congruências.

Após a inserção das equações, passamos aos próximos passos de pôr os valores referentes às colunas. Veja a tabela abaixo com os valores inseridos:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$x \equiv 1 \bmod 2$	1	12	0	$\nexists$	
$x \equiv 1 \bmod 3$	1	8	2	2	
$x \equiv 3 \bmod 4$	3	6	2	$\nexists$	

Tabela 3.20: Inserção de Valores referentes às Colunas.

Note que não dá para continuar a usar o algoritmo, pois aconteceu esse entrave na coluna do $\overline{M}^{-1}$. Entretanto, o fato de o algoritmo não ter dado certo não quer dizer que o sistema não tem solução. Observe:

$$x \equiv 3 \ (\text{mod } 4) \Longrightarrow x \in \{3, 7, 11, 15, 19, 23, 27, 31, 35, ...\}$$

$$x \equiv 1 \ (\text{mod } 2) \Longrightarrow x = 2.n + 1, n \in \mathbb{N}$$

$$x \equiv 1 \pmod 3 \Longrightarrow x = 3.l + 1, l \in \mathbb{N}.$$

Fazendo alguns cálculos por tentativa e erro, temos

$$x \equiv 7 \pmod{12}.$$

Notamos que existe a solução para o sistema em questão. Daí podemos verificar o fato de que há casos em que não podemos aplicar o Teorema, pois as hipóteses não estão satisfeitas, mas isso não inibe a existência de soluções.

Exemplo 3.7. *Vamos resolver o sistema de congruências seguinte seguindo pelo algoritmo estudado.*

$$x \equiv 2 \ (mod\ 4)$$

$$x \equiv 3 \ (mod\ 6).$$

Solução. Vamos construir nossa tabela observando os passos já estudados. Veja:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$x \equiv 2 \bmod 4$	2	6	2	$\nexists$	
$x \equiv 3 \bmod 6$	3	4	4	$\nexists$	

Tabela 3.21: Inserção das Congruências.

Após este entrave encontrado ao tomar os inversos multiplicativos de 2 e 4, respectivamente nos módulos 4 e 6, partimos para resolução do sistema através dos conhecimentos obtidos a respeito de restos nas divisões. Assim, notamos que

$$x \equiv 2 \pmod 4$$

indica que x é par.

Por outro lado, observamos também que

$$x \equiv 3(mod6) \Longrightarrow x \in \{3, 9, 15, 21, 27, ...\}.$$

Dessa forma, não existe x que satisfaça ambas as congruências e, portanto, não existe solução para este sistema.

Exemplo 3.8. *Resolva o seguinte sistema de congruências:*

$$X \equiv 23 \ (mod\ 36)$$

$$X \equiv 3 \ (mod\ 40)$$

$$X \equiv 23 \ (mod\ 75).$$

Solução.

Para verificar, inicialmente, se o sistema possui solução basta notar que $(36, 40) = 4$ *divide a diferença* $23 - 3$, *assim como* $(36, 75) = 3$ *divide* $23 - 23$ *e* $(40, 75) = 5$ *divide* $23 - 3$. *Logo, este sistema possui sim solução e a mesma se dá módulo* $[36, 40, 75] = 1800$.

Sendo 1800=9.8.25 e $9|36$, $8|40$ *e* $25|75$, *escrevemos então um novo sistema de congruências equivalente ao primeiro:*

$$X \equiv 23 \equiv 5 \ (mod\ 9)$$

$$X \equiv 3 \ (mod\ 8)$$

$$X \equiv 23 \ (mod\ 25).$$

Utilizando nosso algoritmo para resolução deste sistema, obtemos a seguinte tabela:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$X \equiv 5$ (mod 9)	5	200	2	5	23000
$X \equiv 3$ (mod 8)	3	225	1	1	675
$X \equiv 23$ (mod 25)	25	72	22	8	13248

Tabela 3.22: Algoritmo para Resolução do Exemplo.

Segue que a solução para este sistema é obtida através da congruência

$$23000 + 675 + 13248 = 18923 \equiv 923 \ (mod\ 1800).$$

Desse modo, concluímos que a solução geral é dada por $X = 923 + 1800.t$, *com* $t \in \mathbb{Z}$.

Exemplo 3.9. *Dispomos de uma quantia de X reais maior que 2000 e menor que 2500. Se distribuirmos essa quantia entre 20 pessoas, sobra* $R\$9,00$; *se a distribuímos entre 24 pessoas, sobram* $R\$5,00$ *e se a distribuirmos entre 75 pessoas, sobram* $R\$59,00$. *De quantos reais dispomos?*

Solução.

De acordo com o enunciado do problema podemos montar o seguinte sistema de congruências:

$$X \equiv 9 \ (mod\ 20)$$

$$X \equiv 5 \ (mod\ 24)$$

$$X \equiv 59 \ (mod\ 75).$$

Como os módulos $20, 24$ *e* 75 *não são primos entre si, segue que é necessário fazermos uso do Teorema Chinês dos Restos Generalizado, entretanto precisamos identificar inicialmente se tal sistema possui solução.*

Note que o mdc $(20, 24) = 3$ *divide a diferença* $5 - 9$, *bem como* $(20, 75) = 5$ *divide* $59 - 9$ *e* $(24, 75) = 3$ *divide* $59 - 5$. *Segue então que o sistema acima possui solução e a mesma é dada módulo* $[20, 24, 75] = 600$.

Sendo $600 = 3.8.25$ *e, consequentemente,* $(3, 8) = (3, 25) = (8, 25) = 1$, *isto é,* 3, 8 *e* 25 *são primos entre si, podemos organizar um novo sistema de congruências da seguinte forma:*

$$X \equiv 9 \equiv 1 \ (mod\ 8)$$

$$X \equiv 5 \equiv 2 \ (mod\ 3)$$

$$X \equiv 59 \equiv 9 \ (mod\ 25).$$

Todavia há de se perceber a respeito dos novos e antigos módulos que $3|24$ *e* $25|75$*, mas* $8 \nmid 20$*. Portanto, apesar dos novos módulos serem primos entre si, o novo sistema de congruências é incompatível com o dado inicialmente.*

Daí podemos fazer a seguinte adaptação aos módulos:

$$X \equiv 9 \equiv 1 \ (mod\ 4)$$

$$X \equiv 5 \ (mod\ 6)$$

$$X \equiv 59 \equiv 9 \ (mod\ 25),$$

donde 4*,* 6 *e* 25 *provém do mmc* $[20, 24, 75] = 600 = 4.6.25$*.*

Observe que os módulos não são dois a dois primos entre si, como o mmc $[4, 6, 25] = 300 = 4.3.25$*, então geramos aqui um outro sistema de congruências:*

$$X \equiv 1 \ (mod\ 4)$$

$$X \equiv 5 \equiv 2 \ (mod\ 3)$$

$$X \equiv 9 \ (mod\ 25).$$

A partir de então podemos aplicar nosso algoritmo. Veja:

Equações	A	M	$\tilde{M}$	$\tilde{M}^{-1}$	$A.M.\tilde{M}^{-1}$
$X \equiv 1$ (mod 4)	1	75	3	3	225
$X \equiv 2$ (mod 3)	2	100	1	1	200
$X \equiv 9$ (mod 25)	9	12	12	23	2484

Tabela 3.23: Algoritmo para Resolução do Exemplo.

Dessa forma, a solução geral é $225 + 200 + 2484 = 2909 \equiv 509 \ (mod\ 600)$*. Note que a tomamos módulo* 600*, pois é justamente o mmc dos módulos do sistema de congruências inicial.*

Concluímos que a quantia a qual dispomos, em reais, figura no conjunto $\{509, 1109, 1709, 2309, 2909, 3509, ...\}$*, que de acordo com o contexto do problema é* $R\$2.309,00$*.*

O Algoritmo: baseado no Teorema 3.5

Em seguida resolveremos os dois exemplos anteriores fazendo uso do Teorema 3.5.

Observe que para resolver o sistema:

$$X \equiv 23 \ (\text{mod } 36)$$

$$X \equiv 3 \ (\text{mod } 40)$$

$$X \equiv 23 \ (\text{mod } 75)$$

faz-se necessário completar inicialmente a tabela a seguir, onde

$$M = [36, 40, 75] = 1800$$

$$M_1 = \frac{1800}{36} = 50$$
$$M_2 = \frac{1800}{40} = 45$$
$$M_3 = \frac{1800}{75} = 24.$$

Equações	A	M_i	x_i	$A.M_i.x_i$
$X \equiv 23 \pmod{36}$	23	50		
$X \equiv 3 \pmod{40}$	3	45		
$X \equiv 23 \pmod{75}$	23	24		

Tabela 3.24: Primeira inserção de dados para Resolução do Exemplo.

O que pretendemos é encontrar os valores de x_i, com $i = 1, 2, 3$ de tal modo que

$$50x_1 + 45x_2 + 24x_3 = 1.$$

Usando o Algoritmo 4 podemos completar nossa tabela com os valores encontrados $x_1 = 5$, $x_2 = -5$ e $x_3 = -1$. Observe:

Equações	A	M_i	x_i	$A.M_i.x_i$
$X \equiv 23 \pmod{36}$	23	50	5	5750
$X \equiv 3 \pmod{40}$	3	45	-5	-675
$X \equiv 23 \pmod{75}$	23	24	-1	-552

Tabela 3.25: Segunda inserção de dados para Resolução do Exemplo.

Pelo Teorema 3.5 a solução x é dada por:

$$x = 5750 - 675 - 552 = 4523 \equiv 923 \pmod{1800}.$$

Quanto à resolução da congruência

$$X \equiv 9 \pmod{20}$$

$$X \equiv 5 \pmod{24}$$

$$X \equiv 59 \pmod{75}$$

vamos seguir de forma análoga a que fizemos anteriormente. Note que através dos valores inseridos inicialmente na tabela a seguir, notamos que, de $M = [20, 24, 75] = 600$, obtemos também:

$$M_1 = \frac{600}{20} = 30$$
$$M_2 = \frac{600}{24} = 25$$
$$M_3 = \frac{600}{75} = 8.$$

Equações	A	M_i	x_i	$A.M_i.x_i$
$X \equiv 9 \pmod{20}$	9	30		
$X \equiv 5 \pmod{24}$	5	25		
$X \equiv 59 \pmod{75}$	59	8		

Tabela 3.26: Primeira inserção de dados para Resolução do Exemplo.

O que pretendemos é encontrar os valores de x_i, com $i = 1, 2, 3$ de tal modo que

$$30x_1 + 25x_2 + 8x_3 = 1.$$

Pelo Algoritmo 4 encontramos os valores dos $x_i's$ e podemos completar nossa tabela com os valores encontrados $x_1 = -4$, $x_2 = 1$ e $x_3 = 12$. Observe:

Equações	A	M_i	x_i	$A.M_i.x_i$
$X \equiv 9 \pmod{20}$	9	30	-4	-1080
$X \equiv 5 \pmod{24}$	5	25	1	125
$X \equiv 59 \pmod{75}$	59	8	12	5664

Tabela 3.27: Segunda inserção de dados para Resolução do Exemplo.

Pelo Teorema 3.5 a solução x é dada por:

$$x = -1080 + 125 + 5664 = 4709 \equiv 509 \pmod{600}.$$

Deste modo concluímos através da aplicação do Teorema Chinês dos Restos Generalizado que as manipulações realizadas para resolver os sistemas de congruências dos exemplos anteriores através da adaptações dos módulos dados de forma quaisquer a módulos primos entre si resolvem o sistema de maneira efetiva.

O próximo exemplo foi retirado do Programa de Iniciação Científica da OBMEP com vista em aplicar os Teoremas de Fermat e Chinês dos Restos num mesmo problema.

Exercícios Propostos para este Capítulo

1) Uma senhora transportava um cesto de ovos. Assustada por um cavalo que galopava perto dela deixa cair o cesto e todos os ovos se partem. Quando lhe perguntaram quantos ovos tivera o cesto, respondeu dizendo que é muito fraca em aritmética, mas lembra-se de ter contado os ovos de dois em dois, de três em três, de quatro em quatro e de cinco em cinco, e tivera sobra de 1, 2, 3, e 4 ovos, respectivamente. Ache a menor quantidade de ovos que o cesto inicialmente poderia ter.

2) Encontre o menor inteiro positivo x tal que $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$ e $x \equiv 3 \pmod{13}$.

3) Temos uma certa quantidade de moedas cujo número desconhecemos. Esse número, quando dividido por 3, dá resto 2; quando dividido por 5,dá resto 3; e, quando dividido por 7, dá resto 2. Qual o número de moedas que temos?

4) Resolver o sistema $3x \equiv 5 \pmod 4$, $2x \equiv 3 \pmod 5$ e $4x \equiv 2 \pmod 3$.

5) Sejam m e n dois inteiros positivos primos entre si. O Teorema Chinês dos Restos afirma que, dados inteiros i e j com $0 \leqslant i < m$ e $0 \leqslant j < n$, existe exatamente um inteiro a, com $0 \leqslant a < m.n$, tal que o resto da divisão de a por m é igual a i e o resto da divisão de a por n é igual a j. Por exemplo, para $m = 3$ e $n = 7$, temos que 19 é o único número que deixa restos 1 e 5 quando dividido por 3 e 7, respectivamente.

   Assim, na tabela a seguir, cada número de 0 a 20 aparecerá exatamente uma vez.

Restos por 7 e por 3	0	1	2	3	4	5	6
0		A				B	
1				C		19	D
2		E			F		

Tabela 3.28: Problema 1, parte B, OBM 2009.

   Qual o valor da soma $A + B + C + D + E + F$?

6) O mágico senta-se numa cadeira, de costas voltadas para o auditório. Alguém pensa num número natural qualquer não superior a 105. Divide o número por 3 e diz o resto da divisão ao mágico. Em seguida, divide o número inicialmente pensado por 5 e fala o resto da divisão ao mágico. E, finalmente, divide o número pensado por 7 e diz o resto. O mágico, conhecendo apenas os três restos, advinha o número pensado. Qual é o truque?

7) Três fazendeiros cultivavam juntos todo o seu arroz e o dividiam igualmente entre si no tempo da colheita. Um certo ano cada um deles foi a um mercado diferente vender o seu arr oz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que diferia em cada um dos mercados. O primeiro fazendeiro vendeu o seu arroz em um mercado onde o peso padrão era 87 kg. Ele vendeu tudo o que podia e voltou para casa com 18 kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 170 kg e voltou para casa com 58 kg. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 143 kg e voltou (ao mesmo tem po que os outros dois) com 40 kg. Qual a quantidade mínima de arroz que eles podem ter cultivado, no total?

Considerações Finais

Através dos estudos realizados neste trabalho, podemos notar a importância de se introduzir o conteúdo de congruências no ensino básico a fim de auxiliar nossos alunos em resolução de problemas em Olimpíadas de Matemática e exames de seleção para determinadas instituições de nível superior.

No decorrer deste trabalho enunciamos e resolvemos alguns exemplos que justificam a utilidade do ensino da aritmética modular e congruências lineares como ferramentas para o Ensino Básico, seja na resolução de problemas em sala de aula, seja para o treinamento para olimpíadas de matemática, pois observamos as cobranças que vêm sendo feitas através em provas de concursos e olimpíadas. Além do fato de que sem estas estratégias que utilizamos aqui, a resolução do problema pode tomar rumos de difíceis soluções.

Não desmerecendo os capítulos iniciais que muito servem para fixação dos conceitos e definições iniciais, entretanto o capítulo destinado à Resolução de Sistema de Congruências Lineares traz 6 (seis) algoritmos que podemos utilizar para cálculo de MDC de números inteiros, determinação dos coeficientes descritos no teorema de Bezóut, cálculo do inverso de um inteiro numa dada classe de congruência e algoritmos baseados no Teorema Chinês dos Restos para resolução de sistemas de congruências lineares.

Este trabalho se torna proveitoso e de relevante aplicação no ensino básico, pois conseguimos aplicá-lo de forma bastante simples, através de tabelas que podem ser preenchidas por meio de algumas operações básicas com os números inteiros disponíveis inicialmente.

Esperamos que com estes algoritmos expostos neste trabalho possamos resolver problemas de modo mais célere, a fim de minimizar o tempo gasto e maximizar o aproveitamento na resolução de questões a respeito de sistemas de congruências lineares.

Referências Bibliográficas

[1] BURTON, David M., *Elementary Number Theory*. University of New Hampshire, 1976.

[2] DUTENHEFNER, Francisco Cadar, Luciana. *Encontros de Aritmética*. Rio de Janeiro: IMPA, 2015.

[3] FILHO, E. A. *Teoria Elementar dos Números*. São Paulo: Nobel, 1989.

[4] FOMIN, Dmitri; GENKIN, Sergey; ITENBERG, Ilia. *Círculos Matemáticos: A experiência Russa*. Rio de Janeiro: IMPA, 2012.

[5] FREIRE, Benedito Tadeu Vasconcelos. *Notas de aulas*. Natal: UFRN, 2009.

[6] HEFEZ, Abramo. *Aritmética*. Rio de Janeiro: SBM, 2014.

[7] HEFEZ, Abramo. *Iniciação à Aritmética*. Rio de Janeiro: IMPA, 2015.

[8] MAIER,Rudolf R. *Teoria dos Números*. Brasília: Unb, 2005.

[9] MUNIZ NETO, Antonio Caminha. *Tópicos de Matemática Elementar Volume 5: Teoria dos Números*. Rio de Janeiro: SBM, 2012, 2ª ed.

[10] www.somatematica.com.br/faq/r35.html. *Como é calculado o dígito verificador do CPF?*. Acesso em 29/05/2016.

[11] CORMEN, Thomas H.; LEISERSON, Charles E.; RIVEST, Ronald L.; STEIN, Clifford. *Introduction to Algorithms*. Second Edition. MIT Press and McGraw-Hill, 2001.

[12] http://rpm.org.br/cdrpm/74/8.html. *RPM 74 - "Mamãe mandou..."*. Acesso em 29/05/2016.