Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Departamento de Matemática
Mestrado Profissional em Matemática

O Teorema Chinês dos Restos

Antonio Luís de Souto Filho

2015
São Luís - MA

Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Departamento de Matemática
Mestrado Profissional em Matemática

O Teorema Chinês dos Restos

por

Antonio Luís de Souto Filho

sob orientação do

Prof. Dr. Felix Silva Costa

2015

São Luís - MA

Souto Filho, Antonio Luís de.

O teorema chinês dos restos / Antonio Luís de Souto Filho. – São Luis, 2015.

37 f.

Orientador: Prof. Dr. Felix Silva Costa.

Dissertação (Mestrado) – Universidade Federal do Maranhão, Curso de Matemática, 2015.

1. Teoria da informação-aspectos matemáticos. 2.Teorema . 3. Sistemas de congruências. I. Título.

CDU 519.72

Universidade Federal do Maranhão
Centro de Ciências Exatas e Tecnologia
Departamento de Matemática
Mestrado Profissional em Matemática

O Teorema Chinês dos Restos

por

Antonio Luís de Souto Filho

Dissertação apresentada ao Departamento de Matemática da Universidade Federal do Maranhão para a obtenção do Título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Felix Silva Costa - UEMA (Orientador)

Prof. Dr. João Coelho Silva Filho - UEMA

Prof. Dr. Roberto Batista dos Santos - UEMA

Agradecimentos

A Deus, pela minha vida e inspirações;

A Jesus Cristo, Senhor e Salvador de minha vida;

Ao Espírito Santo, que nos conduz, guia e direciona segundo os olhos de Deus.

À minha esposa e aos meus filhos, que sempre me incentivaram e me deram forças em todos os momentos desta longa jornada sempre me apoiando e acima de tudo tendo paciência nos momentos mais difíceis.

A todos os colegas do PROFMAT 2013, pela amizade e companheirismo.

Ao professor Dr. Felix Silva Costa, pela dedicação ao Profmat, pela paciência e orientação segura na realização deste trabalho.

Aos professores do PROFMAT, Felix Silva Costa, José Cloves Verde Saraiva, Josenildo, João Coelho e José Antônio Pires Ferreira Marão.

Ao Coordenador do PROFMAT, João de Deus Mendes Filho, pelas orientações e condução do programa no Polo em São Luís – MA.

À Sociedade Brasileira de Matemática-SBM e ao IMPA pela criação, desenvolvimento e condução do PROFMAT.

À CAPES, pelo auxílio financeiro das bolsas.

À Universidade Federal do Maranhão - UFMA, por aderir ao programa nacional.

Resumo

Neste trabalho, apresentamos o Teorema Chinês dos Restos, com início nos pré-requisitos: congruências, sistemas de congruências, pequeno Teorema de Fermat e finalizamos com o Teorema Chinês dos Restos, apresentando sua parte histórica, importância e aplicabilidade, em especial, sua utilidade na Teoria dos Números. A principal aplicação do Teorema Chinês dos Restos mostrada é a possibilidade de trabalhar com números de alta cardinalidade.

Palavras-chave: Congruências, Sistema de Congruências, Teorema Chinês dos Restos.

Abstract

In this work, we present the Chinese Remainder Theorem, beginning in the requisites: congruence, congruence systems, small Theorem of Fermat ending up with Chinese Remainder Theorem, with its historical part, importance and applicability, especially, its usefulness in number theory. The main application of Chinese Remainder Theorem shown is the possibility of working with high cardinality numbers.

Keywords: Congruence, Congruence Systems, Chinese Remainder Theorem.

Sumário

Introdução

Dentre as várias motivações que podemos citar para desenvolvimento deste trabalho, apresentamos o fato de uma teoria tão abstrata, como é a teoria dos números, ter uma infinidade de aplicações, envolvendo o nosso dia a dia. Elas surgem desde o cálculo da hora em um relógio de ponteiros, como a bela teoria da informação, por exemplo.

Importante observarmos que o conceito de congruência, em que pese não integrar a matriz curricular do ensino fundamental e médio, desperta o interesse e a curiosidade acadêmica, com intuito de desenvolvimento de trabalhos e estudos, abordada em sala de aula no próprio Profmat e sendo, inclusive, de frequência incidente nas provas de olimpíadas (OBM, OBMEP, etc.), exsurgindo, portanto, a importância do estudo do aludido conteúdo, eis que as aplicações do Teorema Chinês dos Restos (TCR) ocorrem em quase todas as áreas da matemática. Como citado por [3], a aritmética modular já era estudada desde a antiguidade, e que o algoritmo chinês foi usado na solução prática de problemas relativos à construção de paredes, na base dos edifícios, comércio de alimentos, entrega de informação, e o cálculo de calendários na antiguidade.

A sua aplicabilidade está também presente em diversas áreas da computação, onde damos enfoque na teoria da informação e codificação, em relação a vários aspectos de algoritmos e cálculos modulares. Acrescentamos ainda, que tanto a teoria de códigos, quanto a criptografia são dois campos motivadores para o processo de ensino aprendizagem em sala de aula.

Desenvolvemos este trabalho em 3 partes. No capítulo 1 tratamos da visão histórica e a parte teórica de congruências e sistemas de congruências, finalizando com o pequeno teorema de Fermat. No capítulo 2, apresentamos o teorema chinês dos restos, em particular, sua demonstração, exemplos, e sua aplicabilidade. Finalizamos com as considerações finais.

Capítulo 1

Preliminares

1.1 Uma Visão Histórica

O TCR apareceu no livro de Sun Zi, um matemático na China antiga. O livro é conhecido pelo nome, "Manual de aritmética do Sol", de Sun Zi Suanjing. A data exata é desconhecida, mas é razoável para levá-lo para ser durante o primeiro século d.C. A cada exposição de cultura havia uma manifestação de matemática, pelo menos em algumas formas primitivas. A Matemática "ocidental", como uma sistemática, teve origem no Egito e Mesopotâmia, alcançou um ponto culminante na Grécia e se espalhou para o mundo greco-romano. A Tabela 1.1 mostra um quadro resumo de desenvolvimento da matemática no oriente e no ocidente:

Tabela 1.1: Desenvolvimento da Matemática a.C.

EGITO	3000 a.C.	1500 a.C.
BABILÔNIA	1700 a.C.	300 a.C.
GRÉCIA	600 a.C.	200 a.C.

Tabela 1.2: Desenvolvimento da matemática d.C.

GRECO-ROMANO	100 d.C.	1450 d.C.
PERÍODO MEDIEVAL-RENASCIMENTO	1100 d.C.	1600 d.C.
PERÍODO MODERNO	1600 d.C.	-

A Matemática no Oriente e no Ocidente foi desenvolvida de forma isolada. Detalhes de

possíveis interações não são claras e ainda é um assunto de diversas investigações. Atualmente, as interações entre elas tem sido cada vez mais forte, o que muito se deve, a facilidade no acesso às informações, o que é possível devido à internet e a enorme quantidade de trabalhos em rede.

Vamos agora olhar brevemente para a história do início da matemática na China. De acordo com [6], antes e durante o tempo de Sun Zi Suanjing, para obter uma comparação do calendário citado anteriormente. O mais antigo clássico matemático chinês é Chou Pei Suanjing, cuja tradução literal do título é "O clássico de Aritmética do Gnômom e das trajetórias Circulares do Céu" que continha registro de matemática para cálculos astronômicos a partir de cerca de 1000 a.C. O mais influente dos livros de matemáticos chineses foi de Jiuzhang Suanshu, Nove Capítulos da Arte Matemática, foi composta sobre 50-100 d.C , um pouco mais cedo do que Sun Zi Suanjing. Inclui 246 problemas e soluções provenientes do cotidiano. Nesse livro encontramos o cálculo dos quadrados e raízes cúbicas em algumas das soluções e um método sistemático para a resolução de alguns sistemas de equações lineares, envolvendo também os números negativos. O último capítulo inclui os resultados sobre triângulos retângulos, alguns dos quais foram redescoberto mais tarde na Índia e na Europa.

1.2 Congruências

Teorema 1.1 *Sejam a e b inteiros quaisquer e seja $m > 1$ um inteiro positivo fixo. Diz-se que: a é congruente a b módulo m se, e somente se, m divide a diferença $a - b$. Em outros termos a é congruente a b módulo m se, e somente se, existe um inteiro k tal que $a - b = km$. Ou seja,*

$$a \equiv b \pmod{m} \Longrightarrow m|(a-b) \Longleftrightarrow a - b = km \Longleftrightarrow a = km + b. \tag{1.1}$$

Exemplo 1.2.1

$$\begin{aligned} &3 \equiv 24 \pmod 7 \Longleftrightarrow 7|(3-24) \Longleftrightarrow 3 - 24 = k7 \Longleftrightarrow 3 = k7 + 24 \\ &-31 \equiv 11 \pmod 6 \Longleftrightarrow 6|(-31-11) \Longleftrightarrow -31 - 11 = k6 \Longleftrightarrow -31 = k6 + 11 \\ &-15 - 63 \pmod 8 \Longleftrightarrow 8|(-15+63) \Longleftrightarrow -15 + 63 = k8 \Longleftrightarrow -15 = k8 + (-63) \end{aligned} \tag{1.2}$$

Definição 1.1 *Se m não divide a diferença $a - b$, então diz-se que a é incongruente a b módulo*

m . A notação

$$a \not\equiv b \pmod{m} \tag{1.3}$$

1.2.1 Caracterização de Inteiros Congruentes

Definição 1.2 *Dois inteiros a e b são congruentes módulo m se, e somente se, a e b deixam o mesmo resto quando divididos por m.*

Demonstração:

($\Rightarrow$) Suponhamos que $a \equiv b \pmod{m}$. Então, pela definição: $a - b = km, k \in \mathbb{Z}$. Seja r o resto da divisão de b por m; então pelo algoritmo da divisão: $b = mq + r, 0 < r < m$.
Portanto, $a = km + b = km + mq + r = (k + q)m + r$ e isto significa que r também é o resto da divisão de a por m, isto é, os inteiros a e b divididos por m deixam o mesmo resto r.
($\Leftarrow$) Reciprocamente, suponhamos que a e b divididos por m deixam o mesmo resto r. Então, podemos escrever: $a = mq_1 + r$ e $b = mq_2 + r, 0 < r < m$ e, portanto: $a - b = (q_1 - q_2)m$ $\Rightarrow m/(a - b) \Rightarrow a \equiv b \pmod{m}$.

1.2.2 Propriedades das Congruências

Teorema 1.2 *Seja m um inteiro positivo fixo* ($m > 1$) *e sejam a, b e c inteiros quaisquer. Valem as propriedades:*

Propriedade 1: $a \equiv a \pmod{m}$ (Reflexiva)
Propriedade 2: Se $a \equiv b \pmod{m}$, então $b \equiv a \pmod{m}$ (Simétrica)
Propriedade 3: Se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, então $a \equiv c \pmod{m}$ (Transitiva)
Demonstração:

- **Propriedade 1**: Se $m|0$, ou seja, $m|(a - a)$, então: $a \equiv a \pmod{m}$.
- **Propriedade 2**: Se $a \equiv b \pmod{m}$, então $a - b = km$ com $k \in \mathbb{Z}$.

  Então: $b - a = -(km) = (-k)m \Rightarrow b \equiv a \pmod{m}$
- **Propriedade 3**: Se $a \equiv b \pmod{m}$ e se $b \equiv c \pmod{m}$, existem inteiros h e k tais que $a - b = hm$ e $b - c = km$. Assim, $a - c = (a - b) + (b - c) = hm + km = (h + k)m$ e que implica $a \equiv c \pmod{m}$.

Concluímos que a relação binária R no conjunto $\mathbb{Z}$ dos inteiros definidas por $aRb \Leftrightarrow a \equiv b \pmod{m}$ é reflexiva, simétrica e transitiva, ou seja, R é uma relação de equivalência em $\mathbb{Z}$. Esta relação de equivalência R em $\mathbb{Z}$ é denominada congruência módulo m.

Teorema 1.3 *Seja m um inteiro positivo fixo ($m > 1$) e sejam a, b dois inteiros quaisquer. Valem as seguintes propriedades:*

Propriedade 1*: Se $a \equiv b \pmod{m}$ e $n|m$, com $n > 0$, então $a \equiv b \pmod{n}$*

Demonstração:

Então $a \equiv b \pmod{m} \Rightarrow a - b = km$ e $n|m \Rightarrow m = nq$ onde k, q são inteiros positivos.

Então: $a - b = (kq)n \Rightarrow a \equiv b \pmod{n}$.

Propriedade 2: Se $a \equiv b \pmod{m}$ e se $c > 0$, então $ac \equiv bc \pmod{mc}$

Demonstração:

Com efeito, se $a \equiv b \pmod{m}$, então:

$a - b = km \Rightarrow ac - bc = k(mc) \Rightarrow ac \equiv bc \pmod{mc}$.

Propriedade 3: Se $a \equiv b \pmod{m}$ e se a, b, m são todos divisíveis pelo inteiro $d > 1$, então $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Demonstração:

Com efeito, se $a \equiv b \pmod{m}$, então: $a - b = km \Rightarrow \frac{a}{d} - \frac{b}{d} = \frac{km}{d} \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Teorema 1.4 *Seja m um inteiro positivo fixo ($m > 1$) e sejam a, b, c, d inteiros quaisquer.*

Propriedade 1: Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

Demonstração: Se $a \equiv b \pmod{m}$ e se $c \equiv d \pmod{m}$, então existem inteiros h e k tais que $a - b = hm$ e $c - d = km$. Portanto: $(a + c) - (b + d) = (a - b) + (c - d) = (h + k)m$ e $ac - bd = (b + hm)(d + km) - bd = (bk + dh + hkm)m$ o que implica: $a + c \equiv b + d \pmod{m}$ e $ac \equiv bd \pmod{m}$.

Propriedade 2: Se $a \equiv b \pmod{m}$ e c um inteiro qualquer, então $a + c \equiv b + c \pmod{m}$ e $ac \equiv bc \pmod{m}$.

Demonstração:

Temos: $a \equiv b \pmod{m}$ e $c \equiv c \pmod{m}$ Logo, pela **Propriedade 1** deste teorema:

$$a + c \equiv b + c \pmod{m} \text{ e } ac \equiv bc \pmod{m} \tag{1.4}$$

Em particular, se $c = -1$, então $a(-1) \equiv b(-1) \pmod{m}$ ou $-a \equiv -b \pmod{m}$.

Propriedade 3: Se $a \equiv b \pmod{m}$, então $a^n \equiv b^n \pmod{m}$ para todo inteiro positivo n.

Demonstração:

Usando indução finita, a proposição é verdadeira para $n = 1$, e supondo verdadeira para o inteiro positivo k, vamos mostrar que também é válida para $k + 1$:

Usando a **Propriedade 1** deste teorema $a^k a \equiv b^k b \pmod{m}$ ou $a^{k+1} \equiv b^{k+1} \pmod{m}$. isto é, a proposição é verdadeira para o inteiro positivo $k + 1$. Logo, a preposição é verdadeira para todo inteiro positivo n.

Teorema 1.5 *Se* $ac \equiv bc \pmod{m}$ *e se o* $mdc(c, m) = d$, *então* $a \equiv b \pmod{\frac{m}{d}}$

Demonstração:

Com efeito, se $ac \equiv bc \pmod{m}$, então: $ac - bc = (a - b)c = km$, com $k \epsilon Z$. Como o $mdc(c, m) = d$, existem inteiro r e s tais que $c = dr$ e $m = ds$, onde r e s são primos entre si. Portanto: $(a - b)dr = kds$ ou $(a - b)r = ks$ o que implica que $s|(a - b)r$, com o $mdc(r, s) = 1$. Logo, pelo Teorema de Euclides: $s|(a - b)$ e $a \equiv b \pmod{s}$ ou, por ser $s = \frac{m}{d}$ e $a \equiv b \pmod{\frac{m}{d}}$.

Apesar da congruência $a \equiv b \pmod{m}$ satisfazer várias regras da álgebra elementar. Uma regra que não é válida para a congruência módulo m é o cancelamento, pois $ac \equiv bc \pmod{m}$ e $c \neq 0$ não é necessariamente verdade que $a \equiv b \pmod{m}$, por exemplo, $4.3 \equiv 8.3 \pmod{12}$ mas $4 \not\equiv 8 \pmod{12}$.

Corolário 1 *Se* $ac \equiv bc \pmod{m}$ *e o* $mdc(c, m) = 1$, *então* $a \equiv b \pmod{m}$.

Esta propriedade mostra que é permitido cancelar fatores de ambos os membros de uma congruência que são primos com o módulo m.

Corolário 2 *Se* $ac \equiv bc \pmod{p}$, *com p primo, e se p não divide c, então* $a \equiv b \pmod{p}$

Demonstração:

As condições: p não divide c e p é primo implicam que o $mdc(c, p) = 1$.

Exemplo 1.2.2 *Mostre que* $31 \mid 20^{15} - 1$.

Este problema pode ser reescrito da forma: mostrar que $20^{15} \equiv 1 \pmod{31}$.

Inicialmente, observamos que $20 \equiv -11 \pmod{31}$ e assim $20^2 \equiv (-11)^2 \pmod{31} \Leftrightarrow 20^2 \equiv 121 \pmod{31}$. Como $121 \equiv -3 \pmod{31}$, temos que $20^2 \equiv -3 \pmod{31}$. Multiplicando estes resultados, membro a membro, obtemos $20^3 \equiv 33 \pmod{31}$ e, como $33 \equiv 2 \pmod{31}$, temos que $20^3 \equiv 2 \pmod{31}$.
Elevando a 5, temos que $20^{15} \equiv 32 \pmod{31}$ e como $32 \equiv 1 \pmod{31}$, temos $20^{15} \equiv 1 \pmod{31}$.

Exemplo 1.2.3 *Encontre os restos das divisões de:*

a) 3^{1000} por 101

b) 5^3 por 13

a) Solução: Como $3^4 \equiv 20 \pmod{101}$, elevando ao quadrado obtemos:
$3^8 \equiv 400 \pmod{101} \Leftrightarrow 3^8 \equiv -4 \pmod{101}$. Multiplicando por 3^2 , obtemos
$3^{10} \equiv -36 \pmod{101}$. Portanto
$3^{20} \equiv 1296 \pmod{101} \Leftrightarrow 3^{20} \equiv -17 \pmod{101}$
$3^{40} \equiv 289 \pmod{101} \Leftrightarrow 3^{40} \equiv -14 \pmod{101}$
$3^{80} \equiv 196 \pmod{101} \Leftrightarrow 3^{80} \equiv -6 \pmod{101}$
$3^{80}3^{20} \equiv (-6)(-17) \pmod{101} \Leftrightarrow 3^{100} \equiv 1 \pmod{101}$.
Assim, elevando a última congruência a 10, obtemos $3^{1000} \equiv 1 \pmod{101}$, ou seja, deixa resto 1 na divisão por 101.
b) Solução: Para encontrar o resto da divisão de $5^{3^{20}}$ por 13, note que como $5^4 \equiv 1 \pmod{13}$, os restos de 5^n por 13 se repetem com período 4:

$$5^0 \equiv 1 \pmod{13} \qquad 5^4 \equiv 1 \pmod{13}$$
$$5^1 \equiv 5 \pmod{13} \qquad 5^5 \equiv 5 \pmod{13}$$
$$5^2 \equiv -1 \pmod{13} \qquad 5^6 \equiv -1 \pmod{13}$$
$$5^3 \equiv -5 \pmod{13} \qquad 5^7 \equiv -5 \pmod{13}$$

Por outro lado, temos $3 \equiv 1 \pmod{4}$, isto é, deixa resto 1 na divisão por 4. Assim, encontramos $5^{3^{20}} \equiv 51 \pmod{13}$, ou seja, deixa resto 5 na divisão por 13.

O problema a seguir tem uma história interessante. Em um artigo publicado em 1969, D. J. Lewis afirmava que a equação $x^3 - 117y^3 = 5$ tem no máximo 18 soluções inteiras. Na

verdade, ela não possui nenhuma, como foi provado dois anos mais tarde por R. Finkelstein e H. London, utilizando métodos de Teoria Algébrica dos Números. Em 1973, F. Halter-Koch e V. St. Udresco observaram, independentemente, que existe uma prova muito mais simples deste fato, como mostra o exemplo a seguir [18].

Exemplo 1.2.4 *Mostre que a equação* $x^3 - 117y^3 = 5$ *não possui soluções inteiras.*

Solução: Como 117 é múltiplo de 9, qualquer solução inteira deve satisfazer $x^3 - 117y^3 \equiv 5(\text{mod } 9) \Leftrightarrow x^3 \equiv 5 \text{ (mod 9)}$.

Porém, x só pode deixar resto $0, 1, \ldots, 8$ na divisão por 9. Analisando estes 9 casos, temos:

x (mod 9)	0	1	2	3	4	5	6	7	8
x^3 (mod 9)	0	1	8	0	1	8	0	1	8

Ou seja, x^3 só pode deixar resto 0, 1 ou 8 na divisão por 9. Logo, $x^3 \equiv 5 \text{ (mod 9)}$ é impossível e a equação não possui soluções inteiras.

Exemplo 1.2.5 *Determine o resto da divisão por 7 do número* $2222^{5555} + 5555^{2222}$.

Solução: Sabemos que $2222 \equiv 3 \text{ (mod 7)} \Rightarrow 2222^3 \equiv 3^3 \text{ (mod 7)}$ assim $2222^3 \equiv -1 \text{ (mod 7)} \Rightarrow (2222^3)^{1851} \equiv -1 \text{ (mod 7)}$ logo,$2222^{5553} \equiv -1 \text{ (mod 7)}$ como $2222^2 \equiv 3^2 \text{ (mod 7)}$ segue que $2222^{5553} \times 2222^2 \equiv (-1) \times 9 \text{ (mod 7)} \Rightarrow 2222^{55555} \equiv 5 \text{ (mod 7)}$.
Por outro lado, sabemos que $5555 \equiv 4 \text{ (mod 7)} \Rightarrow 5555^3 \equiv 1 \text{ (mod 7)}$ assim $5555^3 \equiv 1 \text{ (mod 7)} \Rightarrow (5555^3)^{740} \equiv 1 \text{ (mod 7)}$ logo, $5555^{2220} \equiv 1 \text{ (mod 7)}$ como $5555^2 \equiv 4^2 \text{ (mod 7)}$ segue $5555^{2220} \times 5555^2 \equiv (1) \times 4^2 \text{ (mod 7)} \Rightarrow 5555^{2222} \equiv 2 \text{ (mod 7)}$.
Com os resultados acima, temos: $2222^{5555} + 5555^{2222} \equiv (5 + 2) \text{ (mod 7)}$ logo, $2222^{5555} + 5555^{2222} \equiv 0 \text{ (mod 7)}$.

Exemplo 1.2.6 *Determine o algarismo das unidades do número* 9^{9^9}

Solução: Sabemos que $9 + 1 \equiv 0 \text{ (mod 10)}$, como $9 = 2(4) + 1$ é ímpar, então $9^{9^k} + 1^{9^k} \equiv 0 \text{ (mod 10)}$ então $10/9^{9^k} + 1 + 9 - 9$, logo $10/9^{9^k} - 9 + 10$, isto é,$9^{9^k} \equiv 9 \text{ mod } 10$.
Portanto, o algarismo das unidades é 9.

Exemplo 1.2.7 *Ache os algarismos das centenas e das unidades do número* 7^{999999}

Sugestão: Observe que $7^4 = 2401 \cong 1 \bmod 100$.

Solução: Observe que $7^{999996} = (7^4)^{249999} \equiv 1^{249999} \pmod{100}$. Logo, $7^{999996} \equiv 1 \bmod 100$. Por outro lado, $7^3 = 343 \equiv 43 \pmod{100}$, assim pela Propriedade segue que $7^{999996} \cdot 7^3 \equiv 1 \cdot 343 \pmod{100}$, de onde $7^{999999} \equiv 343 \pmod{100} \Rightarrow 7^{999999} = m(100) + 343 = ...00343$
Os algarismos das centenas e unidade é 3.

Exemplo 1.2.8 *Determine o resto da divisão por 4 dos números:*

a) $1 + 2 + 2^2 + ... + 2^{19}$ $\qquad$ $b) 1^5 + 2^5 + ... + 100^5$

Solução: a) Seja $N = 1+2+2^2+...+2^{19}$ então $N = 3+2^2(1+2+...+2^{17})$, logo $N \equiv 3 \pmod 4$. Portanto, o resto da divisão de N por 4 é 3.
b) Seja $M = 1^5 + 2^5 + ... + 100^5$ fazendo $M = (1^5 + 3^5 + ... + 99^5) + (2^5 + 4^5 + ... + 100^5)$, logo, como $2^5 + 4^5 + ... + 100^5 \equiv 0 \pmod 4$, o resto se obtém de $1^5 + 3^5 + ... + 99^5$. Como $(2k+1)^5 = \Sigma_{i=0}^{3} C_5^i \cdot (2k)^{5-i} + 2k + 1$, então $(2k+1)^5 \equiv 2k+1 \pmod 4$, assim, temos $1^5+3^5+...+99^5 \equiv (1+3+...+99) \pmod 4$ a soma dos 50 primeiros números ímpares $1+3+...+99 = 50^2 = 4k, k \epsilon N$, assim temos $1^5 + 2^5 + ... + 100^5 \equiv (0 + 0) \pmod 4$. Portanto o resto da divisão de M por 4 é 0.

1.3 Sistemas de congruências lineares

Definição 1.3 *Um sistema de congruências lineares é uma coleção de congruências lineares. Por exemplo,*

$$\begin{cases} x & \equiv 1 \ (mod\ 3) \\ x & \equiv 2 \ (mod\ 4) \\ x & \equiv 3 \ (mod\ 5) \end{cases} \tag{1.5}$$

É um sistema de congruências lineares.

Uma solução do sistema de congruências lineares é um x_0 inteiro que satisfaz a cada uma das congruências lineares do sistema.

Sistemas de congruências lineares não necessariamente possuem solução, mesmo que cada equação do sistema de congruência possua solução. Por exemplo, não existe inteiro x_0 que verifique simultaneamente as congruências lineares $x \equiv 1 \pmod 2$ e $x \equiv 0 \pmod 4$, embora

cada uma delas, isoladamente, tenha solução.

Se tivermos alguma equação do sistema de congruência, que não tenha solução, então o sistema também não tem solução.

Exemplo 1.3.1 *Resolva o sistema de congruências lineares*

$$\begin{cases} x & \equiv 1 \ (mod\ 3) \\ x & \equiv 2 \ (mod\ 4) \\ x & \equiv 3 \ (mod\ 5) \end{cases} \tag{1.6}$$

A primeira congruência nos dá $x = 3y + 1$, onde $y \in \mathbb{Z}$. Substituindo este valor de x na segunda congruência, obtemos:

$3y + 1 \equiv 2 \pmod 4 \Leftrightarrow 3y \equiv 1 \pmod 4 \Leftrightarrow y \equiv 3 \pmod 4$

Logo, $y = 4z + 3$ com $z \in \mathbb{Z}$ e $x = 3 \cdot (4z + 3) + 1 \Leftrightarrow x = 12z + 10$.

Observamos que qualquer inteiro da forma $12z + 10$ satisfaz as duas primeiras congruências do sistema, substituindo este valor de x na terceira congruência obtemos:

$12z + 10 \equiv 3 \pmod 5 \Leftrightarrow 2z \equiv 3 \pmod 5 \Leftrightarrow z \equiv 4 \pmod 5$ onde $z = 5w + 4$ com $w \in \mathbb{Z}$.

Portanto, $x = 12 \cdot (5w + 4) + 10 \Leftrightarrow x = 60w + 58$, ou seja, $x = 60w + 58$ com $w \in \mathbb{Z}$ é solução.

Neste exemplo, resolvemos o sistema de congruências, calculando cada uma das congruências e substituindo o resultado na equação seguinte. Além disso, os módulos 3, 4 e 5 são dois a dois primos entre si e o $mmc(3, 4, 5) = 60$.

Teorema 1.6 *(Bézout) Sejam a e b inteiros não nulos e d seu mdc. Então existem inteiros x e y tais que d = ax + by. Se a e b são positivos podemos escolher x >0 e y <0, ou vice-versa.*

Demonstração: Seja $P = \{ax + by | ax + by > 0 \text{ e } x, y \in Z\}$. O conjunto P é não vazio pois $0 < a^2 + b^2 = a \times a + b \times b \in P$. Seja f o menor elemento de P. Claramente $d = mdc(a, b) | f$. Como $f, d > 0$, para mostrarmos que $d = f$ basta que $f | d$. Seja $a = qf + r$, com $q \in Z$ e $0 \leq r < f$. Assim $0 \leq r = a(1 - qx) + b(-qy) \in Z$. Como $r < f \Rightarrow r = 0$. Analogamente $f | b$. Então $f | mdc(a, b) = d$.

Teorema 1.7 *Se mdc(a,m) = 1, então existe um inteiro x tal que* $ax \equiv 1 (\text{mod } m)$. *Quaisquer dois tais x são congruentes (mod m) e se mdc(a, m) >1 não existe solução.*

Demonstração: Pelo teorema de Bézout, se $mdc(a, m) = 1$ existem x e y tais que $ax + my = 1$. mas isto significa que $ax \equiv 1 \pmod{m}$. Reciprocamente, se $ax \equiv 1 \pmod{m}$ existe um y tal que $ax + my = 1 \Rightarrow mdc(a, m) = 1$. Se $ax_1 \equiv 1 \equiv ax_2 \pmod{m} \Rightarrow a(x_1 - x_2) \equiv 0 \pmod{m}$, mas $mdc(a, m) = 1 \Rightarrow m|(x_1 - x_2) \Rightarrow x_1 \equiv x_2 \pmod{m}$.
Tal inteiro x é chamado de inverso de a módulo m. Acabamos de mostrar que se $mdc(a, m) = 1$, o inverso de a existe e é único módulo m. Dizemos que dois inteiros a_i e a_j, com $i \neq j$, são primos entre si, se $mdc(a_i, a_j) = 1$.

Exemplo 1.3.2 *Encontre x inteiro tal que:*

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{7} \end{cases} \tag{1.7}$$

Solução:

A primeira congruência nos diz que $x = 11k + 1$ para algum $k \in Z$. Sejam q e r o quociente e o resto da divisão de k por 7, respectivamente. Assim, $k = 7q + r$ e $x = 77q + 11r + 1$. Para x satisfazer a segunda congruência, devemos encontrar $r \in \{0, 1, 2, 3, 4, 5, 6\}$ tal que $11r + 1 \equiv 2 \pmod{7}$, ou seja, $4r \equiv 1 \pmod{7}$. Como o inverso de 4 (mod 7) é 2, obtemos $r = 2$ e $x = 77q + 23$. Veja que para qualquer q inteiro, tal x é solução do sistema de congruências.

Exemplo 1.3.3 *Encontre x inteiro tal que*

$$\begin{cases} x \equiv 1 \ (mod\ 11) \\ x \equiv 2 \ (mod\ 7) \\ x \equiv 4 \ (mod\ 5) \end{cases} \tag{1.8}$$

Solução:

Pelo exemplo anterior, para x satisfazer as duas primeiras equações, devemos ter $x = 77q + 23$. Dividindo q por 5, obtemos $q = 5l + s$ com $0 \leq s < 5$. Daí, $x = 385l + 77s + 23$. Para satisfazer a última congruência, devemos ter $77s + 23 \equiv 4 \pmod{5}$, ou seja, $2s \equiv 1 \pmod{5}$. Como 3 é o inverso de 2 (mod 5), $s = 3$ e consequentemente $x = 385l + 254$.
Observamos que nos dois exemplos anteriores, o problema foi reduzido a encontrarmos o inverso de um inteiro. No último exemplo, a solução geral possui a forma: $x = 11 \cdot 7 \cdot 5l + 231 +$

22 + 1. Essencialmente, o trabalho de encontrar esses inversos foi possível poís os inteiros 5, 7 e 11 são primos entre si dois a dois.

Teorema 1.8 ("Pequeno Teorema de Fermat"- PTF)*: Se p é primo e se o mdc(p, a) = 1, então:*

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

Demonstração: consideremos os $(p-1)$ primeiros positivos de a, isto é,

$$a, 2a, 3a, ..., (p-1)a$$

Os inteiros $(p-1)$ são divisíveis por p e, além disso, dois quaisquer deles são incongruentes módulo p, pois, se fosse: $r.a \equiv s.a \pmod{p}, 1r < sp - 1$, então, o fator comum a poderia ser cancelado, visto que o $mdc(a, p) = 1$, e teríamos: $r \equiv s \pmod{p}$, isto é, $p|(a - x)$ o que é impossível, porque $0 < s - r < p$.
Assim sendo, dois quaisquer dos $(p-1)$ inteiros $a, 2a, 3a, ..., (p-1)a$ divididos por p deixam restos distintos, e por conseguinte cada um desses $p-1$ inteiros é congruente módulo p a um único dos inteiros $1, 2, 3, ..., p-1$, naturalmente numa certa ordem, multiplicando ordenadamente essas $p-1$ congruências, temos:
$a.2a.3a.....(p-1)a \equiv 1.2.3.....(p-1) \pmod{p}$, ou seja,

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

Como o $mdc(p, (p-1)!) = 1$, porque p é primo e p não divide $(p-1)!$, podemos cancelar o fator $(p-1)!$, o que dá a congruência de Fermat: $a^{p-1} \equiv 1 \pmod{p}$.

Exemplo 1.3.4 *Seja o primo $p = 7$ e o inteiro $a = 3$ tais que 7 não divide 3, temos os $p - 1 = 6$ primeiros múltiplos positivos de 3: 3, 6, 9, 12, 15, 18. Nenhum desses 6 inteiros é divisível por 7, todos são incongruentes módulo 7, e cada um deles é congruente módulo 7 a um único dos inteiros 1, 2, 3, 4, 5, 6:* $3 \equiv 3 \pmod{7}$, $6 \equiv 6 \pmod{7}$, $9 \equiv 2 \pmod{7}$, $12 \equiv 5 \pmod{7}$, $15 \equiv 1 \pmod{7}$, $18 \equiv 4 \pmod{7}$. *Multiplicando ordenadamente essas 6 congruências, temos:* $3 \cdot 6 \cdot 9 \cdot 12 \cdot 15 \cdot 18 \equiv 3 \cdot 6 \cdot 2 \cdot 5 \cdot 14 \pmod{p}$, *ou seja,* $36 \,.\, 6! \equiv 6! \pmod{7}$ *Como o mdc(7, 6!) = 1, podemos cancelar o fator comum 6!, que resulta em:*

$$3^6 \equiv 1 \pmod 7.$$

Corolário 3 *Se p é um primo, então $a^p \equiv a \pmod p$, qualquer que seja o inteiro a.*

Demonstração: Se p divide a, então $a \equiv 0 \pmod p$ e $a^p \equiv 0 \pmod p$, que implica em: $a^p \equiv a \pmod p$. Se, ao invés disto, p não dividisse a, então pelo PTF: $a^{p-1} \equiv 1 \pmod p$, e $a^p \equiv a \pmod p$.

Capítulo 2

TEOREMA CHINÊS DOS RESTOS

2.1 Introdução

Conforme [6], o livro "Manual Aritmético do Mestre Sol" foi escrito por Sun Zi Suanjing (ou Sun Tsu Suan Ching), provavelmente entre 280 d.C. a 483 d.C. O livro está dividido em 3 capítulos. O capítulo 1 contém apenas dois problemas que dizem respeito sobretudo a métodos para fazer multiplicações e divisões, utilizando "palitinhos chineses". O capítulo 2 contém 28 problemas, apresenta métodos para o cálculo com frações, extração da raiz quadrada, determinação de áreas e volumes, proporções e regra de três simples. O capítulo 3 contém 36 problemas aritméticos.

No problema 26 (também conhecido como "problema do Mestre Sun") do capítulo 3, Sun Tsu utiliza pela primeira vez o TCR. A data exata deste livro é incerto, no entanto, de acordo com o Livro de história de Dickson [5]. é por volta do primeiro século d.C.. O Problema original sobre restos chinês, proposto pelo Sun Zi em Sun Zi Suanjing (Problema 26, Volume 3), que consiste em três volumes, é como se segue:

Exemplo 2.1.1 *(*Problema proposto por Sun Zi*) Temos coisas, mas não sabemos quantas; se as contarmos de três em três, o resto é 2; se as contarmos de cinco em cinco, o resto é 3; se as contarmos de sete em sete, o resto é 2. Quantas coisas temos?*

Este problema pode ser escrito da forma:

$$\begin{cases} x & \equiv 2\ (mod\ 3) \\ x & \equiv 3\ (mod\ 5) \\ x & \equiv 2\ (mod\ 7) \end{cases}, \tag{2.1}$$

onde sua solução é dada na próxima seção.

2.2 Teorema Chinês dos Restos

Teorema 2.1 *(TCR): Sejam $m_1,\ m_2, ...,\ m_k$ inteiros positivos primos entre si dois a dois, isto é, tais que o $mdc(m_i, m_j) = 1$ se $i \neq j$. Nestas condições, o sistema de congruências lineares:*

$$\begin{cases} x & \equiv a_1\ (mod\ m_1) \\ x & \equiv a_2\ (mod\ m_2) \\ & \quad ... \\ x & \equiv a_k\ (mod\ m_k) \end{cases} \tag{2.2}$$

tem única solução módulo $m = m_1 \times\ m_2 \times\ ... \times\ m_k$ dada por:
$x \equiv a_1M_1x_1 + a_2M_2x_2 + ... + a_kM_kx_k\ (\text{mod}\ m)$

Demonstração: Para cada $k = 1, 2, 3, ..., r$, seja, $M_k = \frac{m}{m_k} = \frac{m_1 \times m_2 \times ... \times m_r}{m_k}$ Como os inteiros m_i são todos primos entre si dois a dois, o $mdc(M_r, m_r) = 1$, de modo que a congruência linear $M_r \cdot x \equiv 1\ (\text{mod}M_r)$ tem única solução $x \equiv x_r\ (\text{mod}\ m_r)$.
Posto isto, vamos mostrar que o inteiro $x \equiv a_1M_1x_1 + a_2M_2x_2 + ... + a_kM_kx_k\ (\text{mod}\ m)$ é uma solução do sistema considerado.
Com efeito se $i \neq r$, então $m_r|M_i$ e $M_i \equiv 0\ (\text{mod}\ m_r)$, que implica em:
$x \cong a_1M_1x_1 + a_2M_2x_2 + ... + a_kM_kx_k\ (\text{mod}\ m)$.
Para demonstrar a unicidade desta solução, suponhamos que x_1 é uma outra solução qualquer do sistema considerado. Então:

$$x \equiv a_r\ (\text{mod}\ m_r) \equiv x_1\ (\text{mod}\ m_r), r = 1, 2, ..., k$$

e, portanto, $m_r|(x - x_1), r = 1, 2, ..., k$.

Mas, o $mdc(m_i, m_j) = 1$ implica em $(m_1 \cdot m_2 \cdot ... \cdot m_k)|(x - x_1)$, isto é, $m|(x - x_1) ex \equiv x_1 \pmod{m}$, com o que termina a demonstração do teorema chinês do resto.

Teorema 2.2 *Sejam $m_1, m_2, ..., m_k$ inteiros positivos primos entre si dois a dois, e sejam $a_1, a_2, ..., a_k$ inteiros tais que $mdc(a_r, m_r) = 1$ para $r = 1, 2, ..., k$. Nestas condições, o sistema de congruências lineares:*

$$\begin{cases} a_1 \cdot x \equiv b_1 \ (mod\ m_1) \\ a_2 \cdot x \equiv b_2 \ (mod\ m_2) \\ \cdots\cdots\cdots\cdots\cdots \\ a_3 \cdot x \equiv b_k \ (mod\ m_k) \end{cases} \tag{2.3}$$

tem única solução módulo $m = m_1 \cdot m_2 \cdot ... \cdot m_k$

Demonstração: Como o mdc$(a_r, m_r) = 1$, a congruência linear $a_1 \cdot x \equiv 1 \pmod{m_r}$ tem única solução $x \equiv a_r \pmod{m_r}$, de modo que: $a_r \cdot a_r \equiv 1 \pmod{m_r}$ e $a_r \cdot a_r \cdot x \equiv x \pmod{m_r}$ e, portanto, é equivalente a congruência $x \equiv a_r \cdot b_r \pmod{m_r}$. Assim sendo, o sistema considerado é equivalente ao seguinte sistema de congruências lineares:

$$\begin{cases} x \equiv a_1 \cdot b_1 \ (mod\ m_1) \\ x \equiv a_2 \cdot b_2 \ (mod\ m_2) \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv a_k \cdot b_k \ (mod\ m_k) \end{cases} \tag{2.4}$$

o qual tem, pelo TCR, uma única solução módulo $m = m_1 \cdot m_2 \cdot ... \cdot m_k$, $x_k \cdot M_k \equiv 1 \pmod{m_k} \Leftrightarrow x_k \equiv M_k^{\phi(m)-1} \pmod{m_k}$ onde:

(i) $M_k = \frac{m}{m_k}, k = 1, 2, 3, ...$

(ii) $x_k \cdot M_k \equiv 1 \pmod{m_k} \Leftrightarrow x_k \equiv M_k^{\phi(m)-1} \pmod{m_k}$, ou seja, x_k é o inverso de M_k módulo m_k.

Podemos enunciar o TCR da seguinte forma:

Teorema 2.3 *Se* $mdc(m,n) = 1$ *então* $f : \mathbb{Z}/\mathbb{Z}_{mn} \longrightarrow \mathbb{Z}/\mathbb{Z}_m \times \mathbb{Z}/\mathbb{Z}_n$*, definida por* $f\ (\bar{a} \pmod n) = (\bar{a} \pmod m,\ \bar{a} \pmod n)$ *é uma bijeção.*

Demonstração: f está bem definida, pois se $a \equiv b \pmod{mn}$ então $a \equiv b \pmod m$ e $a \equiv b \pmod n$. Como $\mathbb{Z}/\mathbb{Z}_{mn}$ e $\mathbb{Z}/\mathbb{Z}_m \times \mathbb{Z}/\mathbb{Z}_n$ têm $m \cdot n$ elementos cada, é suficiente verificar que f é injetiva. E, de fato, se $a \equiv b \pmod m$ e $a \equiv b \pmod n$ então $m/(b-a)$ e $n/(b-a) \Rightarrow b - a = mk, n/mk \Rightarrow n/k$, pois $mdc(m,n) = 1 \Rightarrow mn/(b-a) \Rightarrow a \equiv b \pmod{mn}$.

Exemplo 2.2.1 *Utilizando o TCR, resolver o sistema de congruências lineares:*

$$\begin{cases} x \equiv 8\ (mod\ 5) \\ x \equiv 5\ (mod\ 3) \\ x \equiv 11\ (mod\ 7) \\ x \equiv 2\ (mod\ 4) \end{cases} \tag{2.5}$$

Resolução: os módulos 5, 3, 7 e 4 das congruências lineares que formam o sistema são primos entre si dois a dois, de modo que pelo TCR este sistema tem uma única solução módulo $m = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 5 \cdot 3 \cdot 7 \cdot 4 = 420$, temos:

$M_1 = \frac{m}{m_1} = \frac{420}{5} = 84, \qquad M_2 = \frac{m}{m_2} = \frac{420}{3} = 140, \qquad M_3 = \frac{m}{m_3} = \frac{420}{7} = 60 \qquad$ e

$M_4 = \frac{m}{m_4} = \frac{420}{4} = 105$

Os inversos x_k dos M_k são dados por:

$$\begin{cases} 84 \cdot x_1 \equiv 1\ (mod\ 5) \\ 140 \cdot x_2 \equiv 1\ (mod\ 3) \\ 60 \cdot x_3 \equiv 1\ (mod\ 7) \\ 105 \cdot x_4 \equiv 1\ (mod\ 4) \end{cases} \Rightarrow \begin{cases} 4 \cdot x_1 \equiv 1\ (mod\ 5) \\ 2 \cdot x_2 \equiv 1\ (mod\ 3) \\ 4 \cdot x_3 \equiv 1\ (mod\ 7) \\ 5 \cdot x_4 \equiv 1\ (mod\ 4) \end{cases} \Rightarrow \begin{cases} x_1 = 4 \\ x_2 = 2 \\ x_3 = 2 \\ x_4 = 1 \end{cases} \tag{2.6}$$

Portanto, temos:

$x \equiv a_1 \cdot M_1 \cdot x_1 + a_2 \cdot M_2 \cdot x_2 + \cdots + a_k \cdot M_k \cdot x_k \pmod m$

$x \equiv 8 \cdot 84 \cdot 4 + 5 \cdot 140 \cdot 2 + 11 \cdot 60 \cdot 2 + 2 \cdot 105 \cdot 1 \pmod{m}$

$x \equiv 5618 \pmod{420} \Rightarrow x \equiv 158 \pmod{420}$, segue-se que $x = 158$ é a menor solução positiva módulo 420, do sistema de congruências lineares dado. Qualquer outra solução é da forma: $x \equiv 158 \pmod{420} \Leftrightarrow x = 158 + 420 \cdot k$, com $k \in Z$.

Exemplo 2.2.2 *(Um antigo problema Chinês) 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.

Solução: Seja x a quantidade de ovos que estavam inicialmente no cesto. Podemos escrever:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases} \tag{2.7}$$

Não podemos aplicar diretamente o Teorema Chinês dos Restos, pois, como $mdc(2,3) = mdc(2,5) = mdc(3,5) = 1$ e $mdc(2,4) = 2 \neq 1$, escreveremos o sistema assim:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{4} \end{cases} \tag{2.8}$$

Para resolvermos o problema, inicialmente, trabalhamos somente com o sistema de congruências lineares:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 4 \pmod{5} \end{cases} \tag{2.9}$$

Portanto, $M = 2 \cdot 3 \cdot 5 = 30, M_1 = 3 \cdot 5 = 15, M_2 = 2 \cdot 5 = 10$ e $M_3 = 2 \cdot 3 = 6$.

Os inversos y_k dos M_k são dados por:

$$\begin{cases} 15 \cdot y_1 \equiv 1 \pmod 2 \\ 10 \cdot y_2 \equiv 2 \pmod 3 \\ 6 \cdot y_3 \equiv 4 \pmod 5 \end{cases} \Rightarrow \begin{cases} y_1 \equiv 1 \pmod 2 \\ y_2 \equiv 1 \pmod 3 \\ y_3 \equiv 1 \pmod 5 \end{cases} \Rightarrow \begin{cases} y_1 = 1 \\ y_2 = 1 \\ y_3 = 1 \end{cases} \tag{2.10}$$

$x \equiv r_1M_1y_1 + r_2M_2y_2 + r_3M_3y_3 \pmod M x \equiv 1 \cdot 15 \cdot 1 + 1 \cdot 10 \cdot 1 + 1 \cdot 6 \cdot 1 \pmod{30} \Rightarrow x \equiv 59 \pmod{30} \Rightarrow x \equiv 29 \pmod{30}$.

Portanto a solução do sistema é dada por $x \equiv 29 \pmod{30}$, ou seja, $x = 29 + 30k$, com k inteiro.

Agora, temos o sistema

$$\begin{cases} x \equiv 29 \pmod{30} \\ x \equiv 3 \pmod 4 \end{cases} \tag{2.11}$$

substituímos $x = 29 + 30k$ na congruência $x \equiv 3 \pmod 4$.

Assim, temos: $29 + 30k \equiv 3 \pmod 4$, que é o mesmo que $1 + 2k \equiv 3 \pmod 4$. Ou ainda:

$3 + 1 + 2k \equiv 3 + 3 \pmod 4$, que nos leva para $2k \equiv 2 \pmod 4$, que é equivalente a dizer $2k - 2 = 4t$, onde t é um inteiro. Ou seja, $2(k - 1) = 4t$.

Portanto, k tem de ser um número ímpar, $k = 2s + 1$, onde s é um número inteiro. Logo,

$$\bar{x} = 29 + 30(2s + 1) = 59 + 60s.$$

Deste modo, o número mínimo de ovos que a cesta inicialmente poderia conter é 59.

Exemplo 2.2.3 [16] *Vamos resolver o sistema, a seguir, que corresponde ao problema de Sun-Tsu, que apresentamos no início deste capítulo:*

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \tag{2.12}$$

Neste caso, temos que: $M = 3 \times 5 \times 7 = 105$, $M_1 = 35$, $M_2 = 21$ e $M_3 = 15$.

Por outro lado, as congruências

$35y_1 \equiv 1 \pmod 3$, $21y_2 \equiv 1 \pmod 5$ e $15y_3 \equiv 1 \pmod 7$

tem como soluções, respectivamente, $y_1 = 2$, $y_2 = 1$ e $y_3 = 1$.

Portanto, as soluções módulo $M = 105$ é dada por $x \equiv c_1M_1y_1 + c_2M_2y_2 + c_3M_3y_3 \pmod{105}$, ou seja, $x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105} \Rightarrow x \equiv 233 \pmod{105} \Rightarrow x \equiv 23 \pmod{105}$, segue-se que 23 é uma solução, única módulo 105, do Problema de Sun-Tsu e qualquer outra solução é da forma $23 + 105t$, com $t \in Z$.

Exemplo 2.2.4 [16] *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 arroz. Cada um destes mercados só comprava arroz em múltiplos de um peso padrão, que deferia em cada um dos mercados. O primeiro fazendeiro vendeu seu arroz em um mercado onde o peso padrão era de 87 kg. ele vendeu tudo que podia e voltou para casa com 18 kg de arroz. O segundo fazendeiro vendeu todo o arroz que podia em um mercado cujo o peso padrão era de 170 kg e voltou para casa com 58 kg de arroz. O terceiro fazendeiro vendeu todo o arroz que podia em um mercado cujo peso padrão era de 143 kg e voltou (ao mesmo tempo que os outros dois) com 40 kg. Qual a quantidade mínima de arroz que eles podiam ter cultivado, no tocal?*

Solução: Após a colheita, o montante produzido de arroz é distribuido de forma igualitária entre os três fazendeiros. Então, seja x a quantidade de arroz de cada um dos fazendeiros. Equacionando o problema, teremos que:
Primeiro Fazendeiro: $x \equiv 18 \pmod{87}$;
Segundo Fazendeiro: $x \equiv 58 \pmod{170}$;
Terceiro Fazendeiro: $x \equiv 40 \pmod{143}$.
De acordo com estas equações e como $87 = 3 \cdot 29$, $170 = 2 \cdot 5 \cdot 17$ e $143 = 11 \cdot 13$, teremos o seguinte sistema de congruências:

$$\begin{cases} x \equiv 18 \pmod 3 \Rightarrow x \equiv 0 \pmod 3 \\ x \equiv 18 \pmod{29} \Rightarrow x \equiv 18 \pmod{29} \\ x \equiv 58 \pmod 2 \Rightarrow x \equiv 0 \pmod 2 \\ x \equiv 58 \pmod 5 \Rightarrow x \equiv 3 \pmod 5 \\ x \equiv 58 \pmod{17} \Rightarrow x \equiv 7 \pmod{17} \\ x \equiv 40 \pmod{11} \Rightarrow x \equiv 7 \pmod{11} \\ x \equiv 40 \pmod{13} \Rightarrow x \equiv 1 \pmod{13} \end{cases} \Rightarrow \begin{cases} x \equiv 0 \pmod 6 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod{13} \\ x \equiv 7 \pmod{11} \\ x \equiv 7 \pmod{17} \\ x \equiv 18 \pmod{29} \end{cases} \tag{2.13}$$

Utilizando o TCR:

$M = 6 \cdot 5 \cdot 13 \cdot 11 \cdot 17 \cdot 29 = 2114970$, $M_1 = 5 \cdot 13 \cdot 11 \cdot 17 \cdot 29 = 352495$, $M_2 = 6 \cdot 13 \cdot 11 \cdot 17 \cdot 29 = 422994$, $M_3 = 6 \cdot 5 \cdot 11 \cdot 17 \cdot 29 = 162690$, $M_4 = 6 \cdot 5 \cdot 13 \cdot 17 \cdot 29 = 192270$, $M_5 = 6 \cdot 5 \cdot 13 \cdot 11 \cdot 26 = 124410$ e $M_6 = 6 \cdot 5 \cdot 13 \cdot 11 \cdot 17 = 72930$

Aqui, temos que: $r_1 = 0,\ r_2 = 3,\ r_3 = 1,\ r_4 = 7,\ r_5 = 7,\ r_6 = 18$

Basta agora, encontrar os inversos de $M_1,\ M_2,\ M_3, M_4,\ M_5,\ M_6$ que são dados por:

$y_1 M_1 \equiv 1 \pmod 6 \Rightarrow y_1 \cdot 352495 \equiv 1 \pmod 6 \Rightarrow y_1 \equiv 1 \pmod 6$;

$y_2 M_2 \equiv 1 \pmod 5 \Rightarrow y_2 \cdot 422994 \equiv 1 \pmod 5 \Rightarrow y_2 \equiv 4 \pmod 5$;

$y_3 M_3 \equiv 1 \pmod{13} \Rightarrow y_3 \cdot 162690 \equiv 1 \pmod{13} \Rightarrow y_3 \equiv 5 \pmod{13}$;

$y_4 M_4 \equiv 1 \pmod{11} \Rightarrow y_4 \cdot 192270 \equiv 1 \pmod{11} \Rightarrow y_4 \equiv 1 \pmod{11}$;

$y_5 M_5 \equiv 1 \pmod{17} \Rightarrow y_5 \cdot 124410 \equiv 1 \pmod{17} \Rightarrow y_5 \equiv 13 \pmod{17}$;

$y_6 M_6 \equiv 1 \pmod{29} \Rightarrow y_6 \cdot 72930 \equiv 1 \pmod{29} \Rightarrow y_6 \equiv 23 \pmod{29}$.

Assim, a solução será dada por:

$x \equiv r_1 M_1 y_1 + r_2 M_2 y_2 + r_3 M_3 y_3 + r_4 M_4 y_4 + r_5 M_5 y_5 + r_6 M_6 y_6 \pmod M$

$x \equiv 0 \cdot 352495 \cdot 1 + 3 \cdot 422994 \cdot 4 + 1 \cdot 162690 \cdot 5 + 7 \cdot 192270 \cdot 1 + 7 \cdot 124410 \cdot 13 + 18 \cdot 72930 \cdot 23 \pmod{2114970}$

$x \equiv 0 + 5075928 + 813450 + 1345890 + 11321310 + 30193020$

$x \equiv 48749598 \pmod{2114970} \Rightarrow x \equiv 105288 \pmod{2114970}$

Logo, a solução geral do sistema é $x = 105288 + 2114970 \cdot k$, com $k \in \mathbb{Z}$, e a quantidade mínima de arroz é 105288 kg.

Exemplo 2.2.5 [18] *Um inteiro é livre de quadrados se ele não é divisível pelo quadrado de nenhum número inteiro maior do que 1. Demonstrar que existem intervalos arbitrariamente*

grandes de inteiros consecutivos, nenhum dos quais é livre de quadrados.

Solução: Seja n um número natural qualquer. Sejam $p_1,\ p_2,\ ..., p_n$ primos distintos. O teorema chinês dos restos nos garante que o sistema

$$\begin{cases} x \equiv -1\ (mod\ p_1^2) \\ x \equiv -2\ (mod\ p_2^2) \\ \cdots\cdots\ \cdots\cdots \\ x \equiv -n\ (mod\ p_n^2) \end{cases} \tag{2.14}$$

tem solução. Se x_0 é uma solução positiva do sistema, então cada um dos números $x_0 + 1,\ x_0 + 2,\ \cdots,\ x_0 + n$ é divisível pelo quadrado de um inteiro maior do que 1, logo nenhum deles é livre de quadrados.

Exemplo 2.2.6 [18] *Para cada número natural n, existe uma sequência arbitrariamente longa de números naturais consecutivos, cada um deles sendo divisível por uma s-ésima potência de um número natural maior que* 1.

Solução: Sejam $p_1,\ p_2,\ \cdots,\ p_n$ primos distintos, pelo teorema chinês dos restos, existem infinitos inteiros positivos x que satisfazem as congruências:

$$\begin{cases} x \equiv -1\ (mod\ p_1^s) \Rightarrow p_1^s/x+1 \\ x \equiv -2\ (mod\ p_2^s) \Rightarrow p_2^s/x+2 \\ x \equiv -3\ (mod\ p_3^s) \Rightarrow p_3^s/x+3 \\ \qquad\qquad \cdots \\ x \equiv -n\ (mod\ p_n^s) \Rightarrow p_n^s/x+n \end{cases} \tag{2.15}$$

Logo, $x+1, x+2, x+3, \cdots, x+n$ satisfazem as condições do enunciado.

Exemplo 2.2.7 *Sejam a e b inteiros positivos tais que, para qualquer n natural, $a^n + n/b^n + n$. Prove que $a = b$.*

Prova: Seja p primo maior que a e b, ou seja, $p > a + b$. Escolhendo n natural tal que

$$\begin{cases} n \equiv 1\ (mod\ p-1) \\ n \equiv -a\ (mod\ p) \end{cases} \tag{2.16}$$

como p e $p-1$ são primos consecutivos, então $mdc(p, p-1) = 1$ pelo teorema chinês dos restos há inteiros positivos que satisfazem o sistema. Temos $a^{p-1} \equiv 1 \pmod{p}$ pelo pequeno teorema de Fermat $\Rightarrow a^n \equiv a \pmod{p}$ de fato, $n = (p-1)\cdot r + 1 \Rightarrow a^n = a^{(p-1)\cdot r+1} = (a^{p-1})^r \cdot a \equiv 1^r \cdot a \equiv a \pmod{p} \Rightarrow n \equiv -a \pmod{p} \Rightarrow a^n + n \equiv a - a \equiv 0 \pmod{p}$, portanto, $p|a^n + n$.
Se $a^n + n|b^n + n$ então, $p|b^n + n$, portanto, $b^n = b^{(p-1)\cdot r+1} = (b^{p-1})^r \cdot b \equiv 1^r \cdot b \equiv b \pmod{p} \Rightarrow n \equiv -a \pmod{p} \Rightarrow b^n + b \equiv b - a \pmod{p}$, assim, $p|b-a$, mas $p > a + b$ e como $|b-a| < a + b$, logo, $b - a = 0$ e $a = b$

A generalização deste teorema foi obtido por Yih - Hing, no século VII, para o caso em que os módulos não são primos entre si [10].

Teorema 2.4 Teorema Chinês dos Restos Generalizado

Consideramos os inteiros positivos $m_1, m_2, \cdots, m_k$ e também $a_1, a_2, \cdots, a_k$ inteiros quaisquer. O sistema de congruências

$$\begin{cases} x \equiv a_1 \ (mod\ m_1) \\ x \equiv a_2 \ (mod\ m_2) \\ \qquad \cdots \\ x \equiv a_k \ (mod\ m_k) \end{cases} \tag{2.17}$$

Admite solução se, e só se, $mdc(m_i, m_j)$ divide $a_i - a_j$ para qualquer $i \neq j$. Quando verificamos esta condição, a solução geral constitui uma única classe de congruência módulo m, onde m é o mínimo comum múltiplo de $m_1, m_2, \cdots, m_k$.

Demostração:

• Se existe solução

$x_0 \equiv a_i \pmod{m_i} \Rightarrow m_i|(x_0 - a_i) \ \ \forall i = 1, 2, \cdots, k$

Para cada par $i \neq j$ temos $m_{ij} = mdc(m_i, m_j)$

Como $m_{ij}|m_i \Rightarrow m_{ij}|(x_0 - a_i)$ e $m_{ij}|m_j \Rightarrow m_{ij}|(x_0 - a_j) \Rightarrow m_{ij}|[(x_0 - a_i) - (x_0 - a_j)] = a_i - a_j$

Se x é uma solução qualquer que se verifica para cada $i = 1, 2, ..., k$, temos:

$$\begin{cases} x \equiv a_i \ (mod\ m_i) \\ x_0 \equiv a_i \ (mod\ m_i) \end{cases} \Rightarrow x \equiv x_0 \pmod{m_i} \ \ \Rightarrow m_i|(x - x_0) \ \ \forall i = 1, 2, \cdots, k \Rightarrow \tag{2.18}$$

$x - x_0 = m_i$ com $1 \leq i \leq k \Rightarrow x - x_0 = m$ com $m = mmc(m_1, m_2, \cdots, m_k) \Rightarrow x \equiv x_0 \pmod{m}$.

- Se $m_{ij}|(a_i - a_j) \ \ \forall i \neq j$

Sabemos que $x \equiv a_i \pmod{m}$ com $m = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_s^{a_s}$, ou seja,

$$\begin{cases} x \equiv a_1 \ (mod \ p_1^{\alpha_1}) \\ x \equiv a_2 \ (mod \ p_2^{\alpha_2}) \\ \qquad \vdots \\ x \equiv a_s \ (mod \ p_s^{\alpha_s}) \end{cases} \tag{2.19}$$

Assim, podemos substituir cada equação por um sistema equivalente de equações em que os módulos não são necessariamente potências de primos diferentes.
Além disso, se nós obtivemos duas equações da forma

$$\begin{cases} x \equiv a_i \pmod{p^e} \ \text{ obtida a parti de } \ x \equiv a_i \pmod{m_i} \\ x \equiv a_j \pmod{p^f}, f \leq i \ \text{ obtida a parti de } \ x \equiv a_j \pmod{m_j} \end{cases} \Rightarrow \begin{cases} p^f | n_j \\ p^f | p^e | m_i \end{cases} \tag{2.20}$$

$\Rightarrow p^f | m_{ij} | (a_i - a_j) \Rightarrow a_j \equiv a_j \pmod{p^f}$, como $x \equiv a_i \pmod{p^e}$, então, $x \equiv a_i \pmod{p^f} \Rightarrow x \equiv a_j \pmod{p^f}$

Isto significa que nós podemos eliminar todas as congruências para este primo, com exceção da única congruência $x \equiv a_i \pmod{p^e}$ não envolvendo a mais alta potencia de p, uma vez que esta última congruência implica nas demais.

Se fizermos isso com cada primo p, ficamos com um sistema de congruências da forma $x \equiv a_i \pmod{p^e}$ envolvendo diferentes primos p e dado que os módulos p^e são mutuamente primos entre si, pelo Teorema chinês dos restos implica que as congruências tem solução comum, que é automaticamente, a solução do sistema original.

Exemplo 2.2.8 [10] *Resolver o sistema de congruências:*

$$\begin{cases} x \equiv 11 \pmod{36} \\ x \equiv 7 \pmod{40} \\ x \equiv 32 \pmod{75} \end{cases} \tag{2.21}$$

Solução: Como

$$\begin{cases} mdc\ (36,40) = 4 | (a_1 - a_2) = 11 - 7 = 4 \\ mdc\ (36,75) = 3 | (a_1 - a_3) = 11 - 32 = -21 \\ mdc\ (40,75) = 5 | (a_2 - a_3) = 7 - 32 = -25 \end{cases} \Rightarrow \text{ o sistema tem solução.} \qquad (2.22)$$

Cujos módulos são mutuamente primos entre si, e assim, podemos aplicar os métodos anteriores, basados no TCR para encontrarmos a solução geral $x \equiv 407 \pmod{1800}$. Como $mdc(9,8) = mdc(9,25) = mdc(8,25) = 1$:

$$M = 9 \cdot 8 \cdot 25 = 1800 \qquad M_1 = 8 \cdot 25 = 200$$

$$M_2 = 9 \cdot 25 = 225 \qquad M_3 = 9 \cdot 8 = 72$$

Calculo dos inversos de M_i, temos:

$M_1 \cdot y_1 \equiv 1 \pmod 9 \Leftrightarrow 200 \cdot Y_1 \equiv 1 \pmod 9 \Leftrightarrow 2 \cdot y_1 \equiv 1 \pmod 9 \Leftrightarrow y_1 = 5$

$M_2 \cdot y_2 \equiv 1 \pmod 8 \Leftrightarrow 200 \cdot Y_2 \equiv 1 \pmod 8 \Leftrightarrow 2 \cdot y_2 \equiv 1 \pmod 8 \Leftrightarrow y_2 = 9$

$M_3 \cdot y_3 \equiv 1 \pmod{25} \Leftrightarrow 200 \cdot Y_3 \equiv 1 \pmod{25} \Leftrightarrow 2 \cdot y_3 \equiv 1 \pmod{25} \Leftrightarrow y_3 = 8$

Portanto;

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M$

$x \equiv 2 \cdot 200 \cdot 5 + 7 \cdot 225 \cdot 9 + 7 \cdot 72 \cdot 8 \pmod{1800}$

$x \equiv 2000 + 14175 + 4032 \pmod{1800} \Leftrightarrow x \equiv 20207 \pmod{1800} \Leftrightarrow x \equiv 407 \pmod{1800}$, ou seja, a solução geral do sistema é $x = 407 + 1800t, \ \forall\ t \in \mathbb{Z}$.

2.3 Operando com números de alta cardinalidade

A maioria dos processadores não são tão diferentes de nós, quando trabalhamos com números inteiros, executam muito mais rápido com números de baixa cardinalidade. O TCR permite realizar cálculos com números de alta cardinalidade através de cálculos com números de cardinalidade mais pequenas , como apresentamos no exemplo, a seguir:

Exemplo 2.3.1 [19] *Suponhamos como exemplo de que temos de trabalhar com um hardwere que só pode executar toda aritmética inteira com até 4 bites. Teríamos uma gama de números inteiros* $\{0, 1, 2, \cdots, 15\}$. *Poderíamos não fazer operações como* 16×11 *usando aritmética inteira, pois o resultado ultrapassa nossa capacidade de cálculo e representação.*

Consideremos os seguintes números primos entre si: $m_1 = 13$, $m_2 = 14$, e $m_3 = 15$ pelo que $m = m_1 \cdot m_2 \cdot m_3 = 13 \cdot 14 \cdot 15 = 2730$, consideremos o número 16, que ultrapassa nossa capacidade de representação (em binária, 16 se representa como 10000, logo são necessários 5 bites). Podemos fazer aqui uma bijeção proporcionada como consequência do teorema chinês dos restos: Seja $f : \mathbb{Z}_{2730} \longrightarrow \mathbb{Z}_{13} \times \mathbb{Z}_{14} \times \mathbb{Z}_{15}$, para isto consideremos 16 como uma classe de congruência modúlo 2730. A imagem de $\overline{16}$ pela aplicação f é $f(\overline{16}) = (\overline{16}, \overline{16}, \overline{16}) = (\overline{3}, \overline{2}, \overline{1})$. Em seguida, buscamos uma representação adequada para as classes em $\mathbb{Z}_{mi}$, ou seja, representantes de r_i tal que $0 \leq r_i \leq m_i - 1$. Assim podemos representar o número 16 como o vetor $(\overline{3}, \overline{2}, \overline{1})$. Analogamente, o número 11 pode ser representado como o vetor (11, 11, 11). Para multiplicar 16×11 multiplicamos os vetores em paralelo componente a componente: $(\overline{3}, \overline{2}, \overline{1}) \cdot (\overline{11}, \overline{11}, \overline{11}) = (\overline{33}, \overline{22}, \overline{11}) = (\overline{7}, \overline{8}, \overline{11})$. Como consequência do teorema chinês dos restos, este vetor (7, 8, 11), mais exatamente, o elemento de $\mathbb{Z}_{13} \times \mathbb{Z}_{14} \times \mathbb{Z}_{15}$, dado por $(\overline{7}, \overline{8}, \overline{11})$ deve corresponder ao elemento de $\mathbb{Z}_{2730}$ dado pelo produto $16 \cdot 11 = 176$.

De outro modo, $f^{-1}(\overline{7}, \overline{8}, \overline{11}) = \overline{176}$ comprovemos a veracidade. Calculemos primeiro os valores M_k e y_k necessários para calcular $f^{-1}(\overline{7}, \overline{8}, \overline{11})$.

$$\begin{cases} M_1 = m_2 \cdot m_3 = 14 \cdot 15 = 210; \\ M_2 = m_1 \cdot m_3 = 13 \cdot 15 = 195. \\ M_3 = m_1 \cdot m_2 = 13 \cdot 14 = 182. \end{cases} \tag{2.23}$$

$y_1 = M_1^{-1} \pmod{13} = 210^{-1} \pmod{13} = 2^{-1} \pmod{13} = 7 \pmod{13}$
$y_2 = M_2^{-1} \pmod{14} = 195^{-1} \pmod{14} = 13^{-1} \pmod{14} = 13 \pmod{14}$
$y_3 = M_3^{-1} \pmod{15} = 182^{-1} \pmod{15} = 2^{-1} \pmod{15} = 8 \pmod{15}$.

Portanto, $f^{-1}(\overline{7}, \overline{8}, \overline{11}) = \overline{7 \cdot M_1 \cdot y_1 + 8 \cdot M_2 \cdot y_2 \cdot +11 \cdot M_3 \cdot y_3} =$
$= \overline{7 \cdot 210 \cdot 7 + 8 \cdot 195 \cdot 13 \cdot +11 \cdot 182 \cdot 8}$

$$= \overline{46586}$$
$$= \overline{176}$$

O processo descrito permite utilizar aritmética com 4 bits para realizar operações que, realizadas de forma usual necessitariam mais de 4 bits. Observe que não se poderia, com este sistema multiplicar por exemplo 60×60 já que o resultado excede a $M = 2730$.

Exemplo 2.3.2 [19] *Resolver a congruência* $91 \cdot x \equiv 419 \pmod{440}$

Solução: Como $mdc(91, 440) = 1$ portanto, o sistema tem solução única, por ser $440 = 23 \cdot 5 \cdot 11$, Então, a congruência é equivalente ao sistema de congruências dado por:

$$\begin{cases} 91x \equiv 419 (\text{mod } 8) \\ 91x \equiv 419 (\text{mod } 5) \\ 91x \equiv 419 (\text{mod } 11) \end{cases} \Leftrightarrow \begin{cases} 3x \equiv 3 (\text{mod } 8) \\ x \equiv 4 (\text{mod } 5) \\ 3x \equiv 1 (\text{mod } 11) \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 (\text{mod } 8) \\ x \equiv 4 (\text{mod } 5) \\ x \equiv 4 (\text{mod } 11) \end{cases} \tag{2.24}$$

Como (8, 5) = (8, 11) = (5, 11) = 1, pelo Teorema Chinês dos Restos o sistema tem solução única, portanto, para resolver este último sistema, temos que: $a_1 = 1$, $a_2 = 4$ e $a_3 = 4$. Sendo, $M = m_1 \cdot m_2 \cdot m_3 = 8 \cdot 5 \cdot 11 = 440$ e $M_1 = M_2 \cdot M_3 = 5 \cdot 11 = 55$, $M_2 = M_1 \cdot M_3 = 8 \cdot 11 = 88$ e $M_3 = M_1 \cdot M_2 = 8 \cdot 5 = 40$

Para os inversos temos,

$y_1 \cdot M_1 \equiv 1 \pmod{M_1} \Rightarrow 55 \cdot Y_1 \equiv 1 \pmod 8 \Rightarrow y_1 \equiv 7 \pmod 8 \Rightarrow y_1 = 7$

$y_2 \cdot M_2 \equiv 1 \pmod{M_2} \Rightarrow 88 \cdot Y_2 \equiv 1 \pmod 5 \Rightarrow y_2 \equiv 2 \pmod 5 \Rightarrow y_2 = 2$

$y_3 \cdot M_3 \equiv 1 \pmod{M_3} \Rightarrow 40 \cdot Y_3 \equiv 1 \pmod{11} \Rightarrow y_3 \equiv 8 \pmod{11} \Rightarrow y_3 = 8$

Portanto,

$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 \pmod M$

$x \equiv 1 \cdot 55 \cdot 7 + 4 \cdot 88 \cdot 2 + 4 \cdot 40 \cdot 8 \pmod{440}$

$x \equiv 385 + 704 + 1280 \pmod{440} \Rightarrow x \equiv 2369 \pmod{440} \Rightarrow x \equiv 169 \pmod{440}$

Cuja solução geral é dado por $x = 169 + 440 \cdot k$, com $k \in \mathbb{Z}$.

Considerações finais

O TCR é uma das joias da matemática. Ele é uma combinação perfeita de beleza e utilidade ou, nas palavras de Horácio, “omne tulit punctum qui miscuit utile dulci ”(é uma verdadeira mistura de unir o útil ao agradável). Sempre aparecendo de forma surpreendente na resolução de vários problemas matemáticos, como observamos nos exemplos apresentados. Isto ratifica sua importância e sua abrangência nos diversos ramos da Matemática.

Mostramos que o conteúdo sobre congruências e sistemas de congruências, e claro, o TCR têm sua grande aplicabilidade, inclusive na própria teoria dos números. Além disso, acrescentamos que essas teorias podem e devem ser levadas para sala de aula, contribuindo para o desenvolvimento e compreensão do aluno, em problemas práticos e teóricos, sendo esta, uma das nossas propostas. Finalizamos, descrevendo que dentre suas inúmeras aplicações, podemos citar a teoria de informação da codificação como umas das grandes áreas responsáveis pela difusão e crescimento da teoria dos números.

Referências Bibliográficas

[1] ANTON, H.. **Cálculo Volume II**. 8.ed. São Paulo: Bookman, 2005.

[2] BARBOSA, S.. **Teorema Chinês dos Restos. Olimpíada Brasileira de Matemática**. Disponível em http://samuelbf85.googlepages.com/chines.pdf. Acesso em 20/07/2015.

[3] BOYER, Carl Benjamin. **História da Matemática** / Carl B. Boyer, Uta C. Merzbach; tradução de Helena Castro. São Paulo: Blucher, 2012.

[4] COUTINHO, S. C.. **Números inteiros e criptografia RSA**. 2.ed.. Rio de Janeiro: IMPA/SBM, 2009.

[5] DICKSON, L. E.. **History of the theory of numbers: Divisibility and Primality**. American Mathematical Society, 1966.

[6] DING, C.. **CHINESE REMAINDER THEOREM, Applications in Computing, Coding, Cryptography**, 1996.

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

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

[9] FONSECA, R. V., **Teoria dos números**. Belém: UEPA-Centro de Ciências Sociais e Educação, 2011.

[10] GAVALA, F. J. C., **Introducción a la Matematica Discreta**.

[11] GONÇALVES, A.. **Introdução à Álgebra**. 1ed.. Rio de Janeiro: SBM, 2012.

[12] HEFEZ, A.. **Elementos de Aritmética**. SBM, Rio de Janeiro, segunda edition, 2011.

[13] HEFEZ, A.. **Curso de Álgebra, volume 1**. 5.ed.. Rio de Janeiro: IMPA, 2013.

[14] Howard, E.. **Introdução à História da Matemática**. Campínas: Editora Unicamp, 2008.

[15] NIVEN, I; ZUCKERMAN, H. S.; MONTGOMERY, H. L.. An introduction to the theory of numbers. 5.ed.. New York: John Wiley and Sons, 1991.

[16] PRAZERES, S. B..**O teorema chinês dos restos e a partilha de senhas**. Dissertação de mestrado, PROFMAT. Pernambuco: UFRPE, 2014.

[17] SANTOS, J. P. H.. **Introdução à teoria dos números**. São Paulo: Livro Técnico S.A, 1998.

[18] www.poti.impa.br/teoria dos números/Carlos Gustavo.

[19] (Aplicacion del Teorema Chino del Resto: operar con números grandes_Chino_pdf_Internet Acessado em Agosto/2015)

[20] Araújo, Maria Julieta Ventura Carvalho, Introdução à Álgebra, Notas de Aula_ pdf_Internet Acessado em Agosto/2015).