UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Claudenildo Castro Batista Júnior

O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA

RECIFE
2020

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Claudenildo Castro Batista Júnior

O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Thiago Dias

RECIFE
2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal Rural de Pernambuco
Sistema Integrado de Bibliotecas
Gerada automaticamente, mediante os dados fornecidos pelo(a) autor(a)

615t Júnior, Claudenildo Castro Batista
O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA / Claudenildo Castro Batista Júnior. - 2020.
81 f.

Orientador: Thiago Dias.
Inclui referências.

Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, 2020.

1. Teorema Chinês dos Restos. 2. Criptografia RSA. 3. Congruência. I. Dias, Thiago, orient. II. Título

CDD 510

CLAUDENILDO CASTRO BATISTA JÚNIOR

O teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de matemática com aplicações em Criptografifia RSA

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática – PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 08 / 09 / 2020

BANCA EXAMINADORA

_____

Prof. Dr. Thiago Dias Oliveira Silva (Orientador)– UFRPE

_____

Prof. Dr. Eudes Naziazeno Galvão – **DMat/UFPE**

_____

Profª. Drª. Bárbara Costa da Silva– PROFMAT/UFRPE

À minha família

Agradecimentos

Primeiramente, agradeço por ter nascido e ter tido saúde para chegar até aqui nesta fase tão importante da minha vida, por isso, meus agradecimentos especiais vão para meus pais, Maria da Penha Dias Batista e Claudenildo de Castro Batista, que também os merecem pelo incentivo aos estudos e pelo apoio incondicional.

Agradeço à minha companheira de sempre, Fabiana Paula Soares dos Santos, por estar ao meu lado em todos os momentos e me ajudar a melhorar todas as minhas estratégias.

Sou grato pela confiança depositada pelo meu orientador, Professor Doutor Thiago Dias, cuja dedicação e atenção foram essenciais para que este trabalho fosse concluído satisfatoriamente.

Por fim, agradeço à Universidade Federal Rural de Pernambuco e aos seus docentes que nos incentivaram a percorrer o caminho da pesquisa científica.

Cada dia, a natureza produz o suficiente para nossas carências. Se cada um tomasse o que lhe fosse direito, não haveria pobreza no mundo e ninguém morreria de inanição.
Mahatma Gandhi.

DECLARAÇÃO

Eu, Claudenildo Castro Batista Júnior declaro, para devidos fins e efeitos, que a dissertação sob título O Teorema Chinês dos Restos: uma abordagem voltada para olimpíadas de Matemática com aplicações em Criptografia RSA, entregue como Trabalho de Conclusão de curso para obtenção do título de mestre, com exceção das citações diretas e indiretas claramente indicadas e referenciadas, é um trabalho original. Eu estou consciente que a utilização de material de terceiros incluindo uso de paráfrase sem a devida indicação das fontes será considerado plágio, e estará sujeito à processos administrativos da Universidade Federal Rural de Pernambuco e sanções legais. Declaro ainda que respeitei todos os requisitos dos direitos de autor e isento a Pós-graduação PROFMAT/UFRPE, bem como o professor orientador Thiago Dias, de qualquer ônus ou responsabilidade sobre a sua autoria.

Recife, 08 de outubro de 2020.

Assinatura: _____

Resumo

Este trabalho é uma amostra de algumas aplicações do Teorema Chinês dos Restos - problema numérico descoberto no livro *Sunzi Suanjing*, do matemático Sunzi, no Século lll. Esse teorema que foi utilizado como uma simples ferramenta para resolver problemas básicos sobre calendários e contagem de soldados, transformou-se num dispositivo atualmente aplicado à encriptação de mensagens. Neste trabalho, inicialmente desenvolveremos o conceito de Congruências, exporemos a teoria de resolução das equações modulares e, em seguida, demonstraremos os Teoremas de Fermat, Euler e Wilson. No texto apresentamos um conjunto de problemas resolvidos que poderão servir de material suplementar para a preparação de estudantes para as Olimpíadas de Matemática. Por fim, demonstraremos o Teorema Chinês dos Restos e o aplicaremos em cálculos de codificação RSA. Embora o nome atribuído a este teorema se refira a pesquisadores chineses, ele foi amplamente difundido pelo mundo devido à sua capacidade de resolver problemas aritméticos. Com o presente estudo, desejamos que tais conceitos ingressem no ensino básico e, que, essa difusão se dê também a nível pedagógico. Por fim, esperamos que este trabalho contribua de forma significativa como referência para pesquisas nesta área, bem como para professores de Matemática e estudantes interessados em competições olímpicas de Matemática.

Palavras-chave: Teorema Chinês dos Restos, Criptografia RSA, Congruência.

Abstract

This work is a sample of some applications of the Chinese Remainder Theorem - a numerical problem discovered in the book *Sunzi Suanjing*, by the mathematician Sunzi, in the lll Century. This theorem, which was used as a simple tool to solve basic problems about calendars and soldier counting, has become a device currently applied to message encryption. In this work, we will initially develop the concept of Congruences, expose the theory of solving modular equations and then demonstrate the theorems of Fermat, Euler and Wilson. In the text we will present a set of solved problems that may serve as supplementary material for the preparation of students for the Mathematics Olympics. Finally, we will demonstrate the Chinese Remainder Theorem and apply it to RSA coding calculations. Although the name assigned for this theorem reffers to chinese researchers, it was vastely spreaded around the world due to it is capability on solving arithmetic problems. With the present study, we hope that such concepts will enter basic education and that this diffusion will also take place at the pedagogical level. Finally, we hope that this work will contribute significantly as a reference for research in this area, as well as for mathematics teachers and students interested in Olympic Mathematics competitions.

Keywords: Chinese Remainder Theorem, Cryptography RSA, Congruence.

Sumário

1 Introdução

A afirmação mais antiga conhecida do Teorema Chinês dos Restos apresentada como um problema numérico, aparece no livro do século III, *Sunzi Suanjing*, escrito pelo matemático chinês Sunzi.

"Há certas coisas cujo número é desconhecido. Se contá-los por três, restamos dois; aos cinco, temos três sobrando, e aos setes, sobram dois. Quantas coisas existem?"

Modernamente para responder a essa pergunta, deve-se resolver o seguinte sistema de congruências:

$$\begin{aligned} x &\equiv 2 \ (mod\ 3), \\ x &\equiv 3 \ (mod\ 5), \\ x &\equiv 2 \ (mod\ 7). \end{aligned}$$

O trabalho de Sunzi não contém prova nem algoritmo completo para resolver este tipo de problema. O que equivale a um algoritmo para solucioná-lo foi descrito por Aryabhata (século VI). Casos especiais do Teorema Chinês dos Restos também eram conhecidos por Brahmagupta (século VII), e aparecem no livro *Liber Abaci* de Fibonacci (1202). Mais tarde, o resultado foi generalizado com uma solução completa chamada Dayanshu no Tratado de Matemática de 1247 de Qin Jiushao em nove seções, que foi traduzido para o inglês no início do século XIX pelos missionários britânicos.

O Teorema Chinês dos Restos e a noção de congruências aparecem no livro de Gauss em 1801, *Disquisitiones Arithmeticae*. Gauss ilustra o Teorema Chinês dos Restos sobre um problema que envolve calendários, a saber, "encontrar os anos que têm um certo número de período em relação ao ciclo solar e lunar e a indicação romana". Gauss introduz um procedimento para resolver o problema, isso já havia sido usado por Euler, mas era de fato um método antigo que havia aparecido várias vezes.

O objetivo principal deste trabalho é a aplicabilidade do Teorema Chinês dos Restos em diversas situações do cotidiano. No capítulo 2, abordamos alguns assuntos dentre os quais podemos destacar: Equações Diofantinas Lineares, Divisão nos Inteiros, Sistemas de Congruências, Inverso Módulo n, Potências e, no capítulo 4, Noções de Criptografia.

Além do mais, esses conteúdos foram tratados de uma maneira mais densa do que habitualmente é feita no ensino básico, pois embora tenham um papel importante na resolução de muitos problemas envolvendo os números inteiros, estão de certa forma subutilizados no ensino básico, em especial, quando se trata de fundamentações para olimpíadas e graduações em Matemática.

No capítulo 3, apresentamos a demonstração do Teorema Chinês dos Restos e alguns exemplos de suas aplicações. Acreditamos que tais assuntos da forma em que foram tratados neste trabalho de conclusão de curso, possam servir de apoio para professores e alunos que buscam material suplementares para resolução de problemas.

Os nossos objetivos específicos são: analisar a ocorrência do Teorema Chinês dos Restos em problemas de Olimpíadas, aprofundar a aplicação do teorema Chinês dos Restos na resolução de equações, e por fim verificar o uso do Teorema Chinês dos Restos na Criptografia RSA.

2 Congruências

Para embasarmos o Teorema Chinês dos Restos e por conseguinte a Criptografia, apresentaremos um capítulo sobre congruências. Aqui, trabalharemos sempre com os números naturais $\mathbb{N} = \{1, 2, 3, \ldots\}$ e os números inteiros $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. Durante essas notas iremos assumir, como axiomas, algumas propriedades desses conjuntos. Não faremos a construção dos inteiros a partir dos naturais, nem iremos definir e demonstrar as Proposições, Lemas e Teoremas referente a Aritmética de Números Inteiros, como por exemplo: Divisibilidade, Algoritmo da divisão, Algoritmo de Euclides, o Máximo Divisor Comum e o Mínimo Múltiplo Comum. Para o estudo de tais conceitos, indicamos ao leitor o Trabalho de Conclusão de curso do Mestre Sidmar Bezerra dos Prazeres (4), denominado, *Teorema Chinês dos Restos e a Partilha de Senhas.*

2.1 Equações Diofantinas Lineares

O nome equação diofantina é um tributo a Diofanto de Alexandria, matemático grego do século III a.C.. Durante toda sua vida, Diofanto escreveu alguns livros, sendo o mais importante *Aritmética.* Há neste livro uma pequena introdução sobre equações cujas soluções são números inteiros ou racionais que são chamadas de Equações Diofantinas.

Consideraremos ao longo de todo o trabalho a notação para o Máximo Divisor Comum de a e b, $mdc(a, b)$, como sendo (a, b) e, não raramente, quando o $(a, b) = 1$, a e b serão chamados primos entre si ou coprimos.

Definição 2.1. Uma equação diofantina é uma equação linear com coeficientes inteiros com uma ou mais incógnitas. Uma equação da forma $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ chama-se equação diofantina linear, em que $a_1, \ldots, a_n$ são inteiros dados, chamados coeficientes, c que também é um número inteiro, é chamado de constante e $x_1, \ldots, x_n$ são as incógnitas.

Teorema 2.2. *A equação diofantina de duas variáveis da forma $ax + by = c$, onde, a, b e $c \in \mathbb{Z}$, admite solução inteira se, e somente se, (a, b) divide c.*

Demonstração. Suponha que existam x_0, y_0 inteiros que satisfaçam a equação acima. Então vale a igualdade $ax_0 + by_0 = c$. Como (a, b) divide a e divide b, então divide $ax_0 + by_0$, logo divide c. Reciprocamente, suponha que (a, b) divida c, ou seja, $c = (a, b) \cdot d$, para algum inteiro d. Por outro lado, sabemos que existem inteiros r e s tais que $(a, b) = a \cdot r + b \cdot s$. Multiplicando ambos os lados da igualdade acima por d, obtemos $c = (a, b) \cdot d = a \cdot (r \cdot d) + b \cdot (s \cdot d)$. Logo, a equação diofantina $ax + by = c$ admite pelo menos a solução $x = r \cdot d$ e $y = s \cdot d$.

□

Se a equação $ax + by = c$ admite uma solução, então o número $d = (a, b)$ divide c e, portanto, temos que $a = k_1 \cdot d$, $b = k_2 \cdot d$ e $c = k_3 \cdot d$, onde $(k_1, k_2) = 1$.

Assim, é imediato verificar que x_0, y_0 é uma solução da equação $ax + by = c$ se, e somente se, é solução da equação $k_1x + k_2y = k_3$, onde agora $(k_1, k_2) = 1$. Portanto, toda equação diofantina linear que possui solução é equivalente a uma equação reduzida, ou seja, uma equação da forma $ax + by = c$, com $(a, b) = 1$:

O próximo resultado nos dá uma fórmula para resolver a equação diofantinas linear $ax + by = c$, onde $(a, b) = 1$, conhecida uma solução particular (x_0, y_0) da equação.

Teorema 2.3. *Seja x_0, y_0 uma solução inteira particular da equação $ax + by = c$, onde $(a, b) = 1$. Então, as infinitas soluções x e y em Z da equação são $x = x_0 + tb$; $y = y_0 - ta$; $t \in \mathbb{Z}$.*

Demonstração. Se x, y é uma solução qualquer da equação, então $ax + by = ax_0 + by_0 = c$; donde $a(x - x_0) = b(y_0 - y)$.

Daí segue que $a \mid b(y_0 - y)$ e $b \mid a(x - x_0)$. Como $(a, b) = 1$, $a \mid (y_0 - y)$ e $b \mid (x - x_0)$. Assim, $y_0 - y = ta$ e $x - x_0 = sb$; para alguns inteiros t e s. Substituindo esses valores em $a(x - x_0) = b(y_0 - y)$, obtemos $asb = bta$; o que implica que $s = t$. Logo, da lei do cancelamento, Proposição 2.43, a solução é dada por $x = x_0 + tb$; $y = y_0 - ta$; $t \in \mathbb{Z}$. Reciprocamente, se $x = x_0 + tb$ e $y = y_0 - ta$, substituindo esses valores na equação $ax + by = c$, obtemos $a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 + abt - bat = ax_0 + by_0 = c$. □

Segue-se do teorema acima que a equação diofantina $ax + by = c$, com $(a, b) = 1$, admite infinitas soluções em $\mathbb{Z}$. Note também que as soluções da equação diofantina $ax + by = c$, podem ser escritas na forma $x = x_0 - tb, y = y_0 + ta; t \in \mathbb{Z}$, bastando para isso trocar t por $-t$.

Exemplo 2.4. Determinar todas as soluções inteiras da seguinte equação diofantina linear

- $56x + 72y = 40$

  Solução: Calculando o $(72, 56)$, utilizando o algoritmo de Euclides, temos:

  $72 = 56 \cdot 1 + 16$
  $56 = 16 \cdot 3 + 8$
  $16 = 8 \cdot 2 + 0$

$8 = 56 - 16 \cdot 3 = 56 - (72 - 56 \cdot 1) \cdot 3 = 56 \cdot 4 - 72 \cdot 3 = 56 \cdot (4) + 72(-3)$

Temos: $40 = 8 \cdot 5 = 56 \cdot (4 \cdot 5) + 72 \cdot (-3 \cdot 5) = 56 \cdot 20 + 72(-15)$.

Solução particular: $x_0 = 20$ e $y_0 = -15$.

Todas as soluções: $x = 20 + (72/8)t = 20 + 9t$ e $y = -15 - (56/8)t = -15 - 7t$.

Resposta: $x = 20 + 9t$ e $y = -15 - 7t$

Observação: O Teorema 2.2. pode ser ampliado a equações com mais variáveis e sua demonstração se faz por indução.

Teorema 2.5. *A equação diofantina linear $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ possui solução se e, somente se $(a_1, \ldots, a_n)$ divide c.*

Exemplo 2.6. Verifique se a equação $120x + 180y + 84z = 72$ tem solução e caso exista encontre sua solução geral.

Solução: Como $(120, 180, 84) = 12$, a equação acima possui solução, uma vez que $12 \mid 72$. Podemos reescrevê-la da seguinte forma $10x + 15y + 7z = 6$. Considere $p = 10x + 15y$. Logo, $p + 7z = 6$.

Essa última equação admite solução pois $(1, 7) = 1$, sendo uma solução particular o par 20 e -2. Logo, as soluções inteiras p, z são da forma

$p = 20 + 7t$

$z = -2 - t$,

com $t \in \mathbb{Z}$

Por outro lado, $10x + 15y = p = 20 + 7t$.

Diante disso, devemos encontrar as soluções inteiras da equação $10x + 15y = 20 + 7t$.

Para esta admitir soluções inteiras, $(10, 15) = 5$ deve dividir $20 + 7t$. Repare que t não pode assumir qualquer valor inteiro uma vez que $5 \mid 20 + 7t$, que acontece somente se t é um múltiplo de 5.

Logo, t é da forma $5k$, sendo k um número inteiro arbitrário.

Dessa forma, a equação $10x + 15y = 20 + 7t$ pode ser expressa por $2x + 3y = 4 + 7k$ a qual possui solução devido 2 e 3 serem primos entre si. Com isso pelo algoritmo de Euclides, decorre que $1 = 2(-1) + 3$.

Multiplicando a equação por $4 + 7k$, obtemos uma solução particular que é expressa por $(-4 - 7k, 4 + 7k)$.

Nesse sentido, as soluções x, y da equação $10x + 15y = 20 + 7t$ são da forma

$x = -4 - 7k + 3t_1$

$y = 4 + 7k - 2t_1$, $t_1 \in Z$

Levando em consideração que $z = -2 - t = -2 - 5k$, segue, portanto, que o conjunto solução da equação diofantina $120x + 180y + 84z = 72$ é

$S = \{(-4 - 7k + 3t_1, 4 + 7k - 2t_1, -2 - 5k)$ tal que $k, t_1 \in \mathbb{Z}\}$.

Observação: O método acima pode ser aplicado a uma equação diofantina com um número qualquer de variável.

Exemplo 2.7. (Proposto por Euler - adaptado) Uma pessoa comprou estojos e cadernos. Foram pagos 31 reais por estojo e 20 reais por caderno e sabe-se que todos os estojos custaram 7 reais a menos do que todos os cadernos. Quantos estojos e quantos cadernos foram comprados? Encontre a solução minimal.

Solução: Seja E o número de estojos, C o número de cadernos e P o preço pago pela pessoa.

Sabemos que a diferença entre preços de cadernos e estojos é 7 reais. Assim,

$$20C - 31E = 7$$

Observemos que $(20, -31) = (20, 31) = 1$, logo a equação acima tem solução. Vamos determinar uma solução particular. Pelo algoritmo de Euclides, temos que

$$31 = 20 + 11$$
$$20 = 11 + 9$$
$$11 = 9 + 2$$
$$9 = 2 \cdot 4 + 1$$

Isolando os restos do algoritmo e fazendo as substituições convenientes, obtemos

$$1 = 9 - 2 \cdot 4 = 9 - 4(11 - 9) = 5 \cdot 9 - 4 \cdot 11$$
$$= 5\ (20 - 11) - 4 \cdot 11 = 5 \cdot 20 - 9 \cdot 11$$
$$= 5 \cdot 20 - 9(31 - 20) = 14 \cdot 20 - 9 \cdot 31$$

Multiplicando a última expressão por 7, tem-se $98 \cdot 20 - 63 \cdot 31 = 7$. Como $63 = 3 \cdot 20 + 3$, podemos reescrever a igualdade como $5 \cdot 20 - 3 \cdot 31 = 7$.

Portanto, $C_0 = 5$ e $E_0 = 3$ é uma solução particular da equação diofantina que representa a diferença entre os preços dos itens. Assim, pela teoria desenvolvida até aqui, a solução geral pode ser expressa pelo conjunto

$S = \{(5 + 31t, 3 + 20t) | t \in \mathbb{Z}\}$

2.2 Congruência Modular

Definição 2.8. Se a, b e m são inteiros ($m > 0$), dizemos que a é congruente a b módulo m se $m \mid (a - b)$. Denotaremos essa situação por $a \equiv b$ (mod m).

Proposição 2.9. *Dizer que a é congruente a b módulo m significa que a e b deixam o mesmo resto quando divididos por m.*

Exemplo 2.10.

1. $22 \equiv 16$ (mod 6), pois $6 \mid (22 - 16)$. Observe que o resto da divisão dos dois números por 6 é igual a 4;
2. $5 \equiv 16$ (mod 11), pois $11 \mid (5 - 16)$;
3. $36 \equiv 0$ (mod 4), pois $4 \mid (36 - 0)$.

Exemplo 2.11. Consideremos o mês de outubro do ano de 2017, cujos dias estão descritos na tabela abaixo. Suponha que não dispomos de um calendário em si, mas apenas do primeiro número de cada coluna e seu respectivo dia,

Tabela 1 – Os sete primeiros dias do mês de Outubro

Domingo	Segunda	Terça	Quarta	Quinta	Sexta	Sábado
1	2	3	4	5	6	7

Qual o dia da semana que corresponde o dia 26 de outubro de 2017?

Solução:

Consideremos o mês de outubro do ano de 2017, cujos dias estão descritos na tabela abaixo:

Tabela 2 – Outubro

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

Em cada uma das colunas referentes aos dias da semana, encontram-se números naturais que são congruentes entre si módulo 7. No domingo, os inteiros congruentes a 1 módulo 7, na segunda os inteiros congruentes a 2 módulo 7, e assim por diante. Para isto,

basta determinarmos o inteiro r, com $0 \leq r \leq 6$, congruente a 26 módulo 7. Ora, como $26 = 7 \cdot 3 + 5$, ou seja, $26 \equiv 5 \equiv r \ (mod\ 7)$, e 5 corresponde a quinta-feira, concluímos que o dia 26 de outubro de 2017 também refere-se a uma quinta-feira.

Proposição 2.12. *Se a e b são inteiros, temos que $a \equiv b \ (mod\ m)$ se, e somente se, existe um inteiro k tal que $a = b + km$.*

Demonstração. Se $a \equiv b \ (mod$ m), então $m \mid (b - a)$ o que implica na existência de um inteiro km, isto é, $a = b + km$.

Reciprocamente, suponha a existência de um inteiro k satisfazendo a igualdade $a = b + km$, ou seja, $km = a - b$, o que implica que $m \mid (b - a)$, isto é, $a \equiv b \ (mod$ m). □

2.2.1 Relações de Equivalência

Definição 2.13. Uma relação R em um conjunto A é uma relação de equivalência se e somente se R for

- reflexiva, xRx.
- simétrica, xRy ⇒ yRx e
- transitiva, xRy ∧ yRz ⇒ xRz.

Em geral, uma relação de equivalência ocorre quando desejamos "identificar" dois elementos de um conjunto que compartilham um atributo comum. A definição é motivada pela observação de que qualquer processo de "Identificação" deve se comportar de alguma forma como a relação de igualdade e a relação de igualdade satisfaz o reflexivo ($x = x$ para todo x), simétrico ($x = y$ implica $y = x$) e propriedades transitivas ($x = y$ e $y = z$ implica $x = z$).

Exemplo 2.14. Seja R a relação no conjunto de números reais $\mathbb{R}$ definidos por xRy se $x - y$ é um número inteiro. Prove que R é uma relação de equivalência em $\mathbb{R}$.

Solução:

1. Reflexiva: Suponha $x \in \mathbb{R}$. Então $x - x = 0$, que é um número inteiro. Assim, xRx.

2. Simétrica: suponha x, $y \in \mathbb{R}$ e xRy. Então $x - y$ é um número inteiro. Desde a $y - x = -(x - y), y - x$ também é um número inteiro. Assim, yRx.

3. Suponha x, y, $z \in \mathbb{R}$, xRy e yRz. Então $x - y$ e $y - z$ são números inteiros. Portanto, a soma $(x - y) + (y - z) = x - z$ também é um número inteiro e, portanto, xRz.

Proposição 2.15. *A relação de congruência, definida no conjunto dos inteiros é uma relação de equivalência, pois, é Reflexiva, Simétrica e Transitiva. Se a, b, m e d são inteiros, $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a \ (mod \ m)$.
2. *Se* $a \equiv b \ (mod \ m)$, *então* $b \equiv a \ (mod \ m)$.
3. *Se* $a \equiv b \ (mod \ m)$ *e* $b \equiv d \ (mod \ m)$, *então* $a \equiv d \ (mod \ m)$.

Demonstração.

1. Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \ (mod$ m), assim a relação de congruência é Reflexiva.
2. Se $a \equiv b \ (mod$ m), então $a - b = mk$. com $k \in \mathbb{Z}$. Logo, $b - a = m(-k)$ $e - k \in \mathbb{Z}$, isto é, $b \equiv a \ (mod$ m), assim a relação de congruência é Simétrica.
3. Assumindo que $a \equiv b \ (mod$ m) e $b \equiv d \ (mod$ m), existem k_1; $k_2 \in \mathbb{Z}$ tais que $a - b = mk_1$ e $b - d = mk_2$. Somando membro a membro estas duas igualdades, obtemos $a - d = mk_3$, com $k_3 = k_1 + k_2 \in \mathbb{Z}$, ou seja, $a \equiv d \ (mod$ m), assim a relação de congruência é Transitiva.

□

Teorema 2.16. *Se a, b, c e m são inteiros tais que* $a \equiv b \ (mod \ m)$, *então*

1. $a + c \equiv b + c \ (mod \ m)$.
2. $a - c \equiv b - c \ (mod \ m)$.
3. $ac \equiv bc \ (mod \ m)$.

Demonstração.

1. Como $a \equiv b \ (mod$ m), então existe $k \in \mathbb{Z}$ tal que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \ (mod$ m).
2. Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$, $k \in \mathbb{Z}$, temos que $a - c \equiv b - c \ (mod$ m).
3. Como $a - b = km$, $k \in \mathbb{Z}$ então $ac - bc = ckm$ o que implica $m \mid (ac - bc)$ e, portanto, $ac \equiv bc \ (mod$ m).

□

Teorema 2.17. *Se a, b, c, d e m são inteiros tais que* $a \equiv b \ (mod\ m)$, *e* $c \equiv d \ (mod\ m)$, *então*

1. $a + c \equiv b + d \ (mod\ m)$.
2. $a - c \equiv b - d \ (mod\ m)$.
3. $ac \equiv bd \ (mod\ m)$

Demonstração.

1. De $a \equiv b \ (mod$ m) e $c \equiv d \ (mod$ m) temos $a - b = km$ e $c - d = k_1 m$, $k, k_1 \in \mathbb{Z}$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d \ (mod$ m).
2. Basta subtrair membro a membro $a-b = km$ e $c-d = k_1 m$ obtendo $(a-b)-(c-d) = (a - c) - (b - d) = (k - k_1)m$, $k, k_1 \in \mathbb{Z}$, o que implica $a - c \equiv b - d \ (mod$ m).
3. Multiplicando ambos os lados de $a - b = km$ por c e ambos os lados de $c - d = k_1 m$ por b, com $k, k_1 \in \mathbb{Z}$, obtemos $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$ o que implica $ac \equiv bd \ (mod$ m).

   Em particular, $a \equiv b \ (mod\ m) \Rightarrow a^n \equiv b^n \ (mod\ m), \forall n \leq 0$ □

Exemplo 2.18. $58 \equiv 43 \ (mod\ 5)$, pois $58 - 43 = 15$, que é divisível por 5.

Exemplo 2.19. $58 \equiv 43 \ (mod\ 5)$ e $43 \equiv 18 \ (mod\ 5)$, Logo $58 \equiv 18 \ (mod\ 5)$

Exemplo 2.20. Calcule o resto de 4^{100} por 3.

Solução: Como $4 \equiv 1 \ (mod\ 3)$, temos $4^{100} \equiv 1^{100} \equiv 1 \ (mod\ 3)$.

Exemplo 2.21. Calcule o resto de 4^{100} por 5.

Solução: Como $4 \equiv -1 \ (mod\ 5)$, temos $4^{100} \equiv (-1)^{100} \equiv 1 \ (mod\ 5)$.

Exemplo 2.22. Calcule o resto de 4^{100} por 7.

Solução: Você deve ter percebido que encontrar relações do tipo $a \equiv \pm 1 \ (mod\ m)$ podem simplificar bastante o cálculo de $a^k \ (mod\ m)$. Procuremos alguma relação como essa para 4 e 7. Veja que: $4^0 \equiv 1 \ (mod\ 7)$, $4^1 \equiv 4 \ (mod\ 7)$, $4^2 \equiv 2 \ (mod\ 7)$, $4^3 \equiv 1 \ (mod\ 7)$. Assim, $4^{99} \equiv (4^3)^{33} \equiv 1^{33} \equiv 1 \ (mod\ 7)$, assim $4^{99} \cdot 4 \equiv 4^{100} \equiv 1 \cdot 4 \ (mod\ 7)$. Como $4^3 \equiv 1 \ (mod\ 7)$, os restos das potências de 4 na divisão por 7 se repetem periodicamente de 3 em 3 pois $4^{3k+r} \equiv 4^{3k} \cdot 4^r \equiv 4^r \ (mod\ 7)$.

Exemplo 2.23. Qual o resto de $36^{36} + 41^{41}$ na divisão por 77?

Solução: Inicialmente devemos perceber que existe uma relação entre os números do problema: $36 + 41 = 77$. Assim:

$-36 \equiv 41 \ (mod\ 77)$,

$(-36)^{41} \equiv 41^{41} \ (mod\ 77)$,

$36^{36}(1 - 36^5) \equiv 36^{36} + 41^{41} \ (mod\ 77)$.

Nosso próximo passo é encontrar o resto de 36^5 na divisão por 77. Como $36 \equiv 1 \ (mod\ 7)$, $36^5 \equiv 1 \ (mod\ 7)$. Além disso, $36 \equiv 3 \ (mod\ 11)$ produzindo $36^5 \equiv 3^5 \equiv 1 (mod 11)$.

Como $(7, 11) = 1$ e ambos dividem $36^5 - 1$, podemos concluir que $77 \mid 36^5 - 1$. Logo, $36^{36} + 41^{41}$ deixa resto 0 na divisão por 77.

Definição 2.24. Um conjunto de inteiros $\{a_1, \ldots, a_r\}$ é um sistema completo de resíduos módulo m quando:

1. $a_i \not\equiv a_j \ (mod\ \mathrm{m})$ para $i \neq j$;
2. Para todo inteiro b, existe a_i tal que $b \equiv a_i \ (mod\ \mathrm{m})$.

Note que, todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números $\{0, 1, \ldots, m-1\}$. Além disso, qualquer par de números distintos deste conjunto são incongruentes módulo m. Assim, afirmamos que $\{0, 1, \ldots, m-1\}$ é um sistema completo de resíduos e possui m elementos. De fato, que se $a_1, \ldots, a_m$ são m números inteiros, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. Além disso, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que esses restos são os números $0, 1, \ldots, m-1$ em alguma ordem. Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m.

Exemplo 2.25. Seja m um inteiro positivo par. Suponha que

$$\{a_1, a_2, \cdots, a_m\} \text{ e } \{b_1, b_2, \cdots, b_m\}$$

são dois sistemas completos de resíduos módulo m. Prove que

$$S = \{a_1 + b_1, a_2 + b_2, \cdots, a_m + b_m\}$$

não é um sistema completo de resíduos módulo m.

Solução: Suponha que S seja um sistema completo de resíduos, então:
$1+2+\cdots+m \equiv (a_1+b_1)+(a_2+b_2)+\cdots+(a_n+b_n)(mod\ m)$
$\equiv (a_1+a_2+\cdots+a_n)+(b_1+b_2+\cdots+b_n) \equiv 2(1+2+\cdots+n)$
$\equiv 2(1+2+\cdots+m)$
Isso implica que $m \mid \frac{m(m+1)}{2}$, ou seja, $\frac{m+1}{2}$ é inteiro. Um absurdo pois m é par.

Proposição 2.26. *Seja R um sistema completo de resíduos módulo m. Então, a divisão euclidiana por m pode ser generalizada como segue:*

Para todo $a \in \mathbb{Z}$ existem inteiros q e r univocamente determinados tais que $a = mq + r$, com $r \in R$.

Nessa divisão dizemos tratar-se da divisão com resto em $R = \{0, 1, \ldots, m-1\}$.

Proposição 2.27. *Para todo $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$, se $a \equiv b\ (mod\ m)$, então tem-se que $a^n \equiv b^n\ (mod\ m)$.*

Demonstração. A demonstração faz-se por indução sobre n. Para $n = 1$, a sentença é verdadeira, pois $a^1 \equiv b^1\ (mod\ \mathrm{m}) \Rightarrow a \equiv b\ (mod\ \mathrm{m})$. Suponha a sentença verdadeira para algum $n \in \mathbb{N}$ e mostremos que ele vale para $n+1$. Logo, $a \equiv b\ (mod\ \mathrm{m}) \Rightarrow a^n \cdot a \equiv b^n \cdot b\ (mod\ \mathrm{m}) \Rightarrow a^{(\mathrm{n}+1)} \equiv b^{(\mathrm{n}+1)} (mod\ \mathrm{m})$.

Logo, a sentença vale para $n+1$. Portanto, $a^n \equiv b^n\ (mod\ \mathrm{m})$ para todo $n \in \mathbb{N}$. □

Exemplo 2.28. Mostrar que $10^k \equiv 1\ (mod\ 11)$ ou $10^k \equiv -1\ (mod\ 11)$, conforme $k \in N$ é par ou ímpar, respectivamente.

Solução: Como $10 \equiv -1\ (mod\ 11)$, então $10^k \equiv (-1)^k\ (mod\ 11)$ para todo $k \in N$. Por outro lado, visto que

$$(-1)^k = \begin{cases} 1;\ k \text{ é } par \\ -1;\ k \text{ é } impar \end{cases}$$

temos o resultado.

2.2.2 Base de numeração

Seja $\beta \geq 2$ um número natural, considere o número natural x. Dada a sequência $c_N, \cdots, c_0$ e os dígitos c_j forem de $\{0, 1, \cdots, \beta-1\}$, tal que

$$\mathrm{x}=\sum_{k=0}^{N} c_k \beta^k,$$

então dizemos que $(c_N, \cdots, c_0)_\beta$ é a representação de x na base β.

As bases mais utilizadas são $\beta = 2$, 8, 10 e 16. Consideramos o exemplo:

Exemplo 2.29. Reescreva na base 10 o número $x = (1001)_2$.

Solução: Nós temos $x = 1 \cdot 2^4 + 0 \cdot 2^3 + 0 \cdot 2^1 + 1 \cdot 2^0 = (17)_{10}$.

Vamos agora converter um número na base 10 para uma base β, faremos a conversão decimal para a base 2 que servirá como exemplo para outras bases.

Se avaliarmos a expressão,

$$\mathrm{x} = \sum_{k=0}^{N} c_k \beta^k,$$

usando a aritmética da base 10, podemos converter a base da forma decimal para a base β.

Se temos um número inteiro x, mostraremos como escrever a expansão binária de x, $(c_N, \cdots, c_0)_\beta$.

Começamos dividindo por 2, ou seja, $x = 2 \cdot q + r$ onde o resto r é 0 ou 1. O resto r é o dígito das unidades, c_0 é o quociente q possui expansão binária $(c_N \cdots c_1)_2$.

Continuando dessa maneira, podemos encontrar dígitos adicionais por divisão repetida.

Um exemplo simples ilustra esse procedimento.

Exemplo 2.30. Converta (61) para base 2 por divisão repetida.

Solução: Escrevemos $61 = 2 \cdot 30 + 1$, depois $30 = 2 \cdot 15 + 0$ e continuamos dando

$61 = 2 \cdot 30 + 1$

$30 = 2 \cdot 15 + 0$

$15 = 2 \cdot 7 + 1$

$7 = 2 \cdot 3 + 1$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$

podemos ler o lado direito e obter a expansão binária é $(111101)_2$.

Outra maneira de analisar isso é que podemos inserir cada expressão em seu antecessor para obter:

$61 = 2 \cdot 30 + 1$

$61 = 2 \cdot (2 \cdot 15 + 0) + 1$

$61 = 2 \cdot (2 \cdot 15 + 0) + 1$

$61 = 2 \cdot (2 \cdot (2 \cdot 7 + 1) + 0) + 1$

$$61 = 2 \cdot (2 \cdot (2 \cdot (2 \cdot 3 + 1) + 1) + 0) + 1$$

$$61 = 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot 1 + 1) + 1) + 1) + 0) + 0) + 1$$

$$61 = 2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot (2 \cdot 0 + 1) + 1) + 1) + 1) + 1) + 0) + 1$$

$$61 = 2^5 + 2^4 + 2^3 + 2^2 + 0 \cdot 2^1 + 1$$

Podemos ler a expansão binária da próxima para a última expressão e depois a última expressão é obtida multiplicando os dígitos.

Exemplo 2.31. Determinar o dígito das unidades de 2^{70} escrito na base 15.

Observação: Utiliza-se a partir da base 10 símbolos nos dígitos, por exemplo, na base hexadecimal são utilizados os dígitos 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F.

Solução: O problema é equivalente a determinar um inteiro r tal que $2^{70} \equiv r \ (mod\ 15)$, com $0 \leq r \leq 14$. É claro que não é conveniente desenvolver a potência 2^{70} e, após isso, dividir o resultado por 15. Este de fato não é o melhor caminho. Ao contrário disso, é apropriado encontrar uma congruência base ou inicial de modo que, a partir dela, possamos usar as propriedades da congruência, afim de chegar ao resultado desejado. Um bom ponto de partida é a congruência $2^4 \equiv 1 \ (mod\ 15)$. Elevando ambos os membros desta congruência a 17 (o quociente da divisão de 70 por 4), assim. $(2^4)^{17} \equiv 1^{17} \ (mod\ 15)$ $\Rightarrow 2^{68} \equiv 1 \ (mod\ 15)$. Agora, multiplicando os membros da última congruência por 2^2, obtemos que $2^{70} \equiv 4 \ (mod\ 15)$. Assim, o dígito das unidades é $r = 4$.

As congruências iniciais ideais para resolver um problema análogo ao anterior são congruências da forma $a^k \equiv 1 \ (mod\ m)$ ou $a^k \equiv -1 \ (mod\ m)$, em que k é um inteiro positivo, pois $1^n = 1$ e $(-1)^n = \pm 1$ para $n \in \mathbb{N}$. Ocorre que essas congruências não são fáceis de se obter sem o uso de resultados especiais tais como o Pequeno Teorema de Fermat e o Teorema de Euler, que serão considerados mais adiante.

Exemplo 2.32. Determine o resto de $2^{20} - 1$ na divisão por 41.

Exemplo 2.33. Qual o resto na divisão de $2^{70} + 3^{70}$ por 13?

Exemplo 2.34. Qual o resto de 3^{200} por 100?

Exemplo 2.35. Prove que $2222^{5555} + 5555^{2222}$ é divisível por 7.

Exemplo 2.36. Calcular o dígito das unidades do número 9^{9^9} escrito na base 11.

Solução: O dígito das unidades de 9^{9^9} é o resto r da divisão de 9^{9^9} por 11. Sob a congruência módulo 11, temos

$9 \equiv -2$, $9^2 \equiv 4$, $9^3 \equiv 3$, $9^4 \equiv 5$, $9^5 \equiv 1 \ (mod\ 11)$ e, a partir desta última congruência, os resultados se repetem ciclicamente módulo 5. Este fato nos permite

calcular com facilidades o resto r. Senão vejamos. Considerando agora a congruência módulo 5, temos $9^2 \equiv 1\ (mod\ 5)$ e, por isso, $9^9 \equiv 4\ (mod\ 5)$. Assim, $9^9 = 4 + 5k$ para algum $k \in \mathbb{N}$. Logo, $9^{9^9} = 9^{4+5k}$, e como $9^5 \equiv 1\ (mod\ 11)$, segue sob a congruência módulo 11 que $9^{9^9} = 9^{4+5k} = 9^4 \cdot 9^{5k} \equiv 9^4 \equiv 5\ (mod\ 11)$. Portanto, o resto r é igual a 5.

Exemplo 2.37. Determinar a maior potência de 2 que divide $3^{50} - 1$.

Solução: Temos que 2 divide $3^{50} - 1$, pois 3 é ímpar e, assim, $3^{50} - 1$ é par. Para cada inteiro positivo r, obtemos $2^r \mid 3^{50} - 1 \Rightarrow 3^{50} \equiv 1\ (mod\ 2^r)$.

Já sabemos que esta congruência é válida para $r = 1$. Analisemos, a congruência acima para outros valores de r. Para $r = 2$, temos $3^2 \equiv 1\ (mod\ 4)$, de modo que $(3^2)^{25} \equiv 1\ (mod\ 4)$, ou seja, $3^{50} \equiv 1\ (mod\ 4)$.

Temos também:

$3^2 \equiv 1\ (mod\ 8) \Rightarrow 3^{50} \equiv 1\ (mod\ 8)$, $3^4 \equiv 1\ (mod\ 16) \Rightarrow 3^{50} \equiv 9\ (mod\ 16)$.

Logo, 2^4 não divide $3^{50} - 1$. Portanto, a maior potência de 2 que divide $3^{50} - 1$ é 2^3.

Exemplo 2.38. Prove que $p^2 - 1$ é divisível por 24 se p é um primo maior que 3.

Solução: Se p é um primo maior que 3, $p \equiv \pm 1\ (mod\ 3)$ e $p \equiv 1\ (mod\ 2)$. Daí, $p^2 \equiv 1\ (mod\ 3)$. Além disso, se $p = 2k + 1$, segue que $p^2 = 4k(k + 1) + 1 \equiv 1\ (mod\ 8)$ pois $k(k + 1)$ é par. Como $(8, 3) = 1$ e ambos dividem $p^2 - 1$, segue que $24 \mid p^2 - 1$.

Exemplo 2.39. *(OCM-2001)* Achar o menor natural n tal que 2001 é a soma dos quadrados de n inteiros impares.

Solução: Podemos concluir da solução do problema anterior que todo todo inteiro ímpar ao quadrado deixa resto 1 por 8. Usemos isso para estimar o valor de n. Sejam $x_1, x_2, \ldots, x_n$ inteiros ímpares tais que: $x_1^2 + x_2^2 + \ldots x_n^2 = 2001$.

Analisando a congruência módulo 8, obtemos:

$x_1^2 + x_2^2 + \ldots x_n^2 \equiv 2001\ (mod\ 8)$

$1 + 1 + ... + 1 \equiv 1\ (mod\ 8)$

$n \equiv 1\ (mod\ 8)$

Como 2001 não é quadrado perfeito, não podemos ter $n = 1$. O próximo candidato para n seria $1 + 8 = 9$. Se exibirmos um exemplo para $n = 9$, teremos achado o valor mínimo. Veja que: $2001 = 43^2 + 11^2 + 5^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2 + 1^2$

Proposição 2.40. *Sejam $a, b, c, m \in \mathbb{Z}$, com $m > 1$. Tem-se que $a + c \equiv b + c\ (mod\ m) \Leftrightarrow a \equiv b\ (mod\ m)$.*

Demonstração. Se $a \equiv b \ (mod \ \text{m})$, segue imediatamente do Teorema 2.16. que $a + c \equiv b + c \ (mod \ \text{m})$, pois $c \equiv c \ (mod \ \text{m})$. Reciprocamente, se $a + c \equiv b + c \ (mod \ \text{m})$, então $m \mid b + c - (a + c)$, o que implica que $m \mid b - a$ e consequentemente, $a \equiv b \ (mod \ \text{m})$. □

A proposição acima nos diz que, para as congruências, vale o cancelamento com relação à adição. Quando é multiplicação isto em geral nem sempre é verificado.

Exemplo 2.41. $15 \equiv 3 \ (mod \ 6)$, mas, $5 \not\equiv 1 \ (mod \ 6)$.

Teorema 2.42. *Sejam a, b, c, $m \in \mathbb{Z}$, com $m > 1$. Temos que $ac \equiv bc \ (mod \ m) \Leftrightarrow a \equiv b \ (mod \ \frac{m}{d})$, onde $d = (c, m)$.*

Demonstração. Se $ac \equiv bc \ (mod \ \text{m})$, então $ac - bc = c(a - b) = km$, com $k \in \mathbb{Z}$. Sendo $d = (c, m)$, então $m = dr$ e $c = ds$, em que r e s são primos entre si, pois $(r, s) = (\frac{m}{d}, \frac{c}{d}) = 1$. Substituindo os valores de m e c em $ac - bc = c(a - b) = km$, obtemos $ds(a - b) = kdr \Rightarrow s(a - b) = kr \Rightarrow r \mid s(a - b)$, de modo que $r \mid (a - b)$, pois $(r, s) = 1$. Logo, $a \equiv b \ (mod \ \text{r})$, ou melhor, $a \equiv b \ (mod \ \frac{m}{d})$. Reciprocamente, sejam, $c = d\lambda_1$ e $m = d\lambda_2$. Como $a \equiv b \ (mod \ \frac{m}{d})$, isto é, $a \equiv b \ (mod \lambda_2)$, então $a - b = k\lambda_2$, com $k \in \mathbb{Z}$. Portanto, $c(a - b) = (d\lambda_1) \cdot (k\lambda_2) = mk\lambda_1$, ou seja, $ac \equiv bc \ (mod \ \text{m})$. □

Como consequência do teorema anterior, temos a lei do cancelamento, Proposição 2.43, para congruências, a qual no será bastante útil.

Proposição 2.43. *(Lei do Cancelamento) Suponhamos $ac \equiv bc \ (mod \ m)$, com $(c, m) = 1$. Então, $a \equiv b \ (mod \ m)$.*

Demonstração. Se $ac \equiv bc \ (mod \ m)$, com $d = (c, m) = 1$, então pelo teorema anterior, $a \equiv b \ (mod \ \frac{m}{d})$, isto é, $a \equiv b \ (mod \ \text{m})$. □

Proposição 2.44. *Sejam $a, k, m \in Z$, com $m > 1$ e $(k, m) = 1$. Se $a_1, \ldots, a_m$ é um sistema completo de resíduos módulo m, então $a + ka_1, \ldots, a + ka_m$ também é um sistema completo de resíduos módulo m.*

Demonstração. Como, da proposição acima, para $i, j = 0, 1, \ldots, m-1$, temos que $a+ka_i \equiv a + ka_j \ (mod \ \text{m}) \Leftrightarrow ka_i \equiv ka_j \ (mod \ \text{m}) \Leftrightarrow a_i \equiv a_j \ (mod \ \text{m}) \Leftrightarrow i = j$. Isso mostra que $a + ka_1, \ldots, a + ka_m$ são, dois a dois, incongruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m. □

2.3 Congruências Lineares

Definição 2.45. Dados a e b inteiros, com $a \neq 0$, uma congruência da forma $ax \equiv b (mod \ \text{m})$ é chamada congruência linear, em que x é uma incógnita.

Nosso objetivo é determinar todas as soluções inteiras de $ax \equiv b\ (mod\ \mathrm{m})$, isto é, todos os inteiros x_0 para os quais $ax_0 \equiv b\ (mod\ \mathrm{m})$. Por exemplo, 3 é uma solução de $4x \equiv 7\ (mod\ 5)$, pois $4 \cdot 3 = 12 \equiv 7\ (mod\ 5)$. Por outro lado, a congruência linear $4x \equiv 3\ (mod\ 2)$ não tem solução inteira, pois se $x_0 \in \mathbb{Z}$ e $4x_0 \equiv 3\ (mod\ 2)$, então $4x_0 - 3 = 2k$, com $k \in \mathbb{Z}$, de maneira que 2 divide 3, o que não é possível.

Inicialmente, vamos dar um critério para determinar se tais congruências, da forma como definidas acima, admitem solução.

Teorema 2.46. *Dados a, b, e $m \in \mathbb{Z}$, com $m > 1$, a congruência linear $ax \equiv b\ (mod\ m)$ admite solução inteira se, e somente se, $d \mid b$, em que $d = (a, m)$.*

Demonstração. Suponhamos que x_0 seja solução de $ax \equiv b\ (mod\ \mathrm{m})$ e tomemos $d = (a, m)$. Assim, $ax_0 - b = km$, isto é $b = ax_0 - km$. Como, $d \mid a$ e $d \mid m$, então $d \mid b$.

Reciprocamente, suponha que $d \mid b$. Pela identidade de Bachet-Bézout, existem inteiros r e s tais que $d = a \cdot r + s \cdot m$. Como $b = dt$, com $t \in \mathbb{Z}$, $d \mid b$, então $b = (ar + sm)t = art + smt$, ou seja, $a(rt) \equiv b\ (mod\ \mathrm{m})$. Logo, $x_0 = rt$ é solução de $ax \equiv b\ (mod\ \mathrm{m})$. □

Proposição 2.47. *A congruência $ax \equiv 1\ (mod\ m)$ tem solução se, e somente se, $(a, m) = 1$.*

A seguir vamos caracterizar as soluções de $ax \equiv b\ (mod\ m)$.

Teorema 2.48. *Se x_0 é uma solução da congruência linear $ax \equiv b\ (mod\ m)$, então todas as soluções desta congruência são da forma $x = x_0 + \frac{m}{d}k$, com $k \in \mathbb{Z}$ em que $d = (a, m)$.*

Demonstração. Inicialmente, vamos provar que $x = x_0 + (\frac{m}{d})k$, com $d = (a, m)$, é uma solução de $ax \equiv b\ (mod\ \mathrm{m})$ para cada inteiro k. Desde que $ax_0 \equiv b\ (mod\ \mathrm{m})$, ou seja, $ax_0 = b + \lambda m$, com $\lambda \in \mathbb{Z}$, temos $ax = a[x_0 + (\frac{m}{d})k] = (ax_0) + a(\frac{m}{d})k$. Substituindo $ax_0 = b + \lambda m$, temos, $(b + \lambda m) + a(\frac{m}{d})k$, e evidenciando m, $b + m(\lambda + \frac{ak}{d})$. Portanto, $ax \equiv b\ (mod\ \mathrm{m})$, pois $\frac{ak}{d} \in \mathbb{Z}$.

Agora, seja $x_1 \in \mathbb{Z}$ tal que $ax_1 \equiv b\ (mod\ \mathrm{m})$. Como $ax_0 \equiv b\ (mod\ \mathrm{m})$, então, por transitividade, $ax_0 \equiv ax_1\ (mod\ \mathrm{m})$. Assim, pela Proposição 2.43., $x_0 \equiv x_1\ (mod\ \frac{m}{d})$, ou seja, $x_1 = x_0 + \frac{m}{d}k$, com $k \in \mathbb{Z}$. □

Como um caso particular do teorema anterior, temos:

No teorema anterior vimos que uma congruência do tipo $ax \equiv b\ (mod\ m)$ possui infinitas soluções inteiras. O próximo resultado mostra que o número de soluções é (a, m).

Teorema 2.49. *Consideremos a congruência $ax \equiv b\ (mod\ m)$. Se $d \mid b$, com $d = (a, m)$, então esta congruência possui exatamente d soluções, duas a duas incongruentes módulo m, dadas por x_0, $x_0 + \frac{m}{d}$, $x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$, em que x_0 é uma solução particular qualquer de $ax \equiv b\ (mod\ m)$.*

Demonstração. Pelo Teorema 2.48., para cada inteiro k, $x = x_0 + \frac{m}{d}k$ é uma solução de $ax \equiv b\ (mod\ \text{m})$. O que devemos mostrar é que $(x_0 + \frac{m}{d}k_1) \not\equiv (x_0 + \frac{m}{d}k_2)\ (mod\ m)$; com $0 \leq k_1 < k_2 \leq d-1$. De fato, nestas condições, se $(x_0 + \frac{m}{d}k_1) \equiv (x_0 + \frac{m}{d}k_2)\ (mod\ m)$; então $\frac{m}{d}k_1 \equiv \frac{m}{d}k_2\ (mod\ \text{m})$; e pela Proposição 2.43., $k_1 \equiv k_2\ (mod\ \frac{m}{d_1})$; sendo $d_1 = (\frac{m}{d}, m)$. Como $m = (\frac{m}{d})d$, então $d_1 = \frac{m}{d}$, de modo que $\frac{m}{d_1} = \frac{m}{\frac{m}{d}} = d$. Portanto, $k_1 \equiv k_2\ (mod\ \text{d})$, ou seja, $d \mid k_2 - k_1$, o que é uma contradição, já que $0 < k_2 - k_1 < d-1$. Por conseguinte, as soluções são duas a duas incongruentes módulo m. Resta-nos mostrar que qualquer solução $x = x_0 + (\frac{m}{d})k$ de $ax \equiv b\ (mod\ m)$ é congruente módulo m a uma das d soluções dadas em x_0, $x_0 + \frac{m}{d}$, $x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$. Pelo Algoritmo da Divisão, temos $k = dq + r$, com $0 \leq r \leq d-1$. Assim, $x = x_0 + \frac{m}{d}k = x_0 + \frac{m}{d}(dq + r) = x_0 + mq + r\frac{m}{d} \equiv x_0 + r\frac{m}{d}\ (mod\ m)$; em que $x_0 + r(\frac{m}{d})$ é uma das soluções em x_0, $x_0 + \frac{m}{d}$, $x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}$. □

O resultado é uma consequência dos dois teoremas anteriores.

Proposição 2.50. *A solução geral da congruência linear $ax \equiv 1\ (mod\ m)$ com, $(a, m) = 1$, é dada por $x = x_0 + km$, com $k \in \mathbb{Z}$, em que x_0 é uma solução inicial. Existem soluções de $ax \equiv b\ (mod\ m)$ que são incongruentes duas a duas módulo m. Essas ocorrem em um número finito e são obtidas da expressão $x = x_0 + \frac{m}{d}k$; para $k = 0, 1, \ldots, d-1$, se $d \mid b$, sendo $d = (a, m)$.*

Resumindo os resultados anteriores, podemos resolver uma congruência linear $ax \equiv b\ (mod\ \text{m})$, com $d = (a, m)$ e $d \mid b$, seguindo os seguintes passos:

1. Através do Algoritmo de Euclides, obtemos inteiros r e s tais que $d = a \cdot r + m \cdot s$.

2. Se $b = dt$, então $x_0 = rt$ é uma solução de $ax \equiv b\ (mod\ m)$, de modo que sua solução geral é dada por $x = x_0 + \frac{m}{d}k$, com $k \in \mathbb{Z}$.

Exemplo 2.51. $3x \equiv 6\ (mod\ 15)$ é satisfeita por todo inteiro x da forma $2 + 5t$, $t \in \mathbb{Z}$ e $\{2, 7, 12\}$ são três soluções incongruentes módulo 15.

2.3.1 Sistemas de Congruências Lineares

Um sistema de congruências lineares é uma coleção de congruências lineares, da forma:

$$\begin{cases} a_1 x \equiv b_1\ (mod\ m_1) \\ a_2 x \equiv b_2\ (mod\ m_2) \\ \vdots \\ a_k x \equiv b_k\ (mod\ m_k) \end{cases} \tag{2.1}$$

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

Para que este sistema tenha solução, é necessário que cada uma das k congruências tenha solução, ou seja, que $d_i \mid b_i$, em que $d_i = (a_i, m_i)$ para cada $i = 1, \ldots, k$. Entretanto, esta condição não é suficiente. Por exemplo, não existe um inteiro x_0 que verifique simultaneamente as congruências lineares

$$\begin{cases} x \equiv 1 \ (mod\ 2) \\ x \equiv 0 \ (mod\ 4) \end{cases}$$

O sistema não possui solução, embora cada uma das congruências tenha solução. A proposição a seguir nos mostrará como obter um sistema equivalente ao dado em 2.1, mas com os coeficientes iguais a 1.

Proposição 2.52. *A congruência linear $ax \equiv b \ (mod\ m)$, em que $d = (a, m)$, com $d \mid b$, é equivalente a $x \equiv rb_1 \ (mod\ n)$, sendo $b = b_1 d$ e $m = nd$.*

Dois sistemas de congruências lineares são equivalentes quando possuem as mesmas soluções. O mesmo ocorre com duas congruências lineares.

Demonstração. Considerando $a = a_1 d$, $b = b_1 d$ e $m = nd$, $ax \equiv b \ (mod\ m) \Leftrightarrow a_1 dx \equiv b_1 d \ (mod\ nd)$: Pela Proposição 2.43., temos $a_1 x \equiv b_1 \ (mod\ n)$. Sendo $d = a \cdot r + s \cdot m$, então $d = a_1 d \cdot r + s \cdot nd$, ou seja, $1 = a_1 \cdot r + s \cdot n$, isto é, $ra_1 \equiv 1 \ (mod\ n)$. Multiplicando a congruência em $a_1 x \equiv b_1 \ (mod\ n)$ por r, temos $ra_1 x \equiv rb_1 \ (mod\ n)$, e como $a_1 r \equiv 1 \ (mod\ n)$, então $x \equiv a_1 rx \ (mod\ n)$, isto é, $x \equiv b_1 r \ (mod\ n)$, o que prova a primeira parte. Reciprocamente, se $x \equiv b_1 r \ (mod\ n)$, então como $ra_1 \equiv 1 \ (mod\ n)$, segue $xra_1 \equiv b_1 r \ (mod\ n)$. Por outro lado, visto que $1 = a_1 \cdot r + s \cdot n$, temos $(r, n) = 1$. Portanto, podemos cancelar o fator r da última congruência de modo a obter $xa_1 \equiv b_1 \ (mod\ n)$, ou seja, $x(\frac{a}{d}) \equiv \frac{b}{d} \ (mod\ \frac{m}{d})$; donde $ax \equiv b \ (mod\ m)$. A vantagem de se considerar uma congruência da forma $x \equiv b \ (mod\ m)$ é que sua solução geral é obtida de forma direta, $x = b + km$, com $k \in \mathbb{Z}$. □

De acordo como o lema anterior, o sistema dado em (2.1) é equivalente ao sistema

$$\begin{cases} x \equiv c_1 \ (mod\ n_1) \\ x \equiv c_2 \ (mod\ n_2) \\ \vdots \\ x \equiv c_k \ (mod\ n_k) \end{cases} \tag{2.2}$$

Este último será resolvido através do teorema a seguir com uma hipótese adicional, cujo título faz lembrar a origem desse problema.

2.4 O Teorema de Wilson, O Pequeno Teorema de Fermat e O Teorema de Euler

Vamos demonstrar duas proposições que nos auxiliarão nas demonstrações a seguir.

Proposição 2.53. *Seja p um número primo. Os únicos elementos do conjunto C=$\{1, 2, \ldots, (p-1)\}$ que satisfaz a equação $a^2 \equiv 1 \ (mod\ p)$ são 1 e -1.*

Demonstração. Tomemos $a \in C$, se x_0 é uma solução da congruência $a^2 \equiv 1 \ (mod\ p)$, então $x_0^2 \equiv 1 \ (mod\ p)$, ou seja, $p \mid x^2 - 1 = (x_0 + 1)(x_0 - 1)$.

Como p é primo, segue que $p \mid (x_0 + 1)$ ou $p \mid (x_0 - 1)$. Por conseguinte, $x_0 \equiv -1 \equiv (p-1) \ (mod\ p)$ ou $x_0 \equiv 1 \ (mod\ p)$. □

Proposição 2.54. *Sejam p um número primo e $A = \{1, 2, \ldots, p-1\}$. Então, para cada $a \in A$, existe único $b \in A$ tal que $ab \equiv 1 \ (mod\ p)$.*

Demonstração. **(Existência)** Dado $a \in A$, $(a, p) = 1$, de modo que, pela identidade de Bachet-Bézout, existem inteiros r e s tais que $1 = ar + ps$, isto é, $ar \equiv 1 \ (mod\ p)$. Como $r \not\equiv 0 \ (mod\ p)$, pois $p \nmid 1$, temos $r \equiv b \ (mod\ p)$ para algum $b \in A$. Assim, $ar \equiv ab \ (mod\ p)$ e, por transitividade, $ab \equiv 1 \ (mod\ p)$, provando a existência de $b \in A$.

(Unicidade) Se b_1 e b_2 são elementos de A, com $ab_1 \equiv 1 \ (mod\ p)$ e $ab_2 \equiv 1 \ (mod\ p)$, então $ab_2 \equiv ab_1 \ (mod\ p)$. Como $(a, p) = 1$, temos $b_2 \equiv b_1 \ (mod\ p)$. Isso mostra a unicidade do elemento b módulo p. □

2.4.1 O Teorema de Wilson

Teorema 2.55. *Se p é primo, então $(p-1)! \equiv -1 \ (mod\ p)$.*

Demonstração. O caso $p = 2$ é de imediata verificação. Entre os números 1, 2, $\cdots$, $p-1$, apenas 1 e $p-1$ são seus próprios inversos módulo p. Os demais, 2, $\cdots$, $p-2$, podem ser agrupados em pares cujo produto é congruente a 1 módulo p. Isso se deve ao fato de que eles possuem inverso módulo p, diferente de si mesmo e pertencente ao conjunto, ou seja, se $a \in \{2, \cdots, p-2\}$, existe $b \in \{2, \cdots, p-2\}$, com $b \neq a$, tal que $ab \equiv 1 \ (mod\ p)$. Se multiplicarmos todas essas congruências sem repetir os números, obteremos $2 \cdot 3 \cdots (p-2) \equiv 1 \ (mod\ p)$. Se multiplicarmos esta última congruência pela

imediata $p-1 \equiv -1 \ (mod\ p)$, obteremos $2 \cdot 3 \cdots (p-2)(p-1) \equiv -1 \ (mod\ p)$, isto é, $(p-1)! \equiv 1 \ (mod\ p)$. Por outro lado, vamos supor que $(n-1)! \equiv -1 \ (mod\ n)$. Se $a < n$, aparece a no cálculo de $(n-1)!$, de onde concluímos que $(n-1)! \equiv 0 \ (mod\ a)$. Se tivermos $a \mid n$, da hipótese $n \mid n(n-1)! + 1$ e da transitividade da divisibilidade, $a \mid (n-1)! + 1$, ou seja, $(n-1)! + 1 \equiv 0 \ (mod\ a)$. Subtraindo $(n-1)! + 1 \equiv 0 \ (mod\ a)$ e $(n-1)! \equiv 0 \ (mod\ a)$, obtemos $1 \equiv 0 \ (mod\ a)$, mas isso somente é possível se $a = 1$. Assim, 1 é o único inteiro positivo menor que n que é divisor de n, de onde concluímos que n é primo, assim $(n-1)! \equiv -1 \ (mod\ n)$, então n é primo. □

Exemplo 2.56. Mostrar que a divisão de 15! por 17 deixa resto 1.

Demonstração. Pelo Teorema de Wilson sabemos que, $16! \equiv -1 \ (mod\ 17) \Rightarrow 16 \cdot 15! \equiv -1 \ (mod\ 17)$, por outro lado, $-1 \equiv 16 \ (mod\ 17)$, por transitividade $16 \cdot 15! \equiv 16 \ (mod\ 17)$, como $(16, 17) = 1$, temos $15! \equiv 1 \ (mod\ 17)$. Logo, o resto da divisão de 15! por 17 é igual a 1.

□

Exemplo 2.57. Determinar o resto da divisão de 2(26)! por 29.

Solução: Como $p = 29$ é primo, então pelo Teorema de Wilson, temos que $28! \equiv -1 \ (mod\ 29)$, ou melhor, $28 \cdot 27 \cdot 26! \equiv -1 \ (mod\ 29)$. Por outro lado, sendo $28 \equiv -1 \ (mod\ 29)$ e $27 \equiv -2 \ (mod\ 29)$, $28 \cdot 27 \equiv 2 \ (mod\ 29)$ e, por conseguinte, $28 \cdot 27 \cdot 26! \equiv 2 \cdot 26! \ (mod\ 29)$. Desse modo, por transitividade, $2 \cdot 26! \equiv -1 \equiv 28 \ (mod\ 29)$. Portanto, o resto é $r = 28$.

Exemplo 2.58. *(Estônia 2000)* Prove que não é possível dividir qualquer conjunto de 18 inteiros consecutivos em dois conjuntos disjuntos A e B tais que o produtos dos elementos de A seja igual ao produto dos elementos de B.

Solução: Suponha, por absurdo, que existam tais conjuntos. Considere o primo $p = 19$. Como o produto dos elementos de A é igual ao produto dos elementos de B, se um dos conjuntos contém um múltiplo de 19, o outro necessariamente também conterá. Como entre 18 inteiros consecutivos não existem dois múltiplos de 19, nenhum dos conjuntos do problema contém tais números.

Seja x o resto na divisão por 19 do produto dos elementos de A.

Calculemos então o resto na divisão por 19 do produto de todos os 18 inteiros consecutivos:

$$x \cdot x \equiv n(n+1)(n+2)(n+3) \cdots (n+17) \equiv 1 \cdot 2 \cdot 3 \cdot \cdots \cdot 18 \equiv -1 \ (mod\ 19).$$

(Pelo teorema de Wilson). Como $x^2 \equiv -1 \ (mod\ 19)$, $x^{18} \equiv (-1)^9 \equiv -1 \ (mod\ 19)$. Isso contraria o teorema de Fermat e obtemos um absurdo, pois $x^{18} \equiv 1 \ (mod\ 19)$.

2.4.2 O Pequeno Teorema de Fermat

Teorema 2.59. *(Pequeno Teorema de Fermat) Sejam p um primo e a um inteiro tal que $p \nmid a$. Então, $a^{p-1} \equiv 1 \ (mod\ p)$.*

Demonstração. Consideremos os primeiros $p-1$ múltiplos de a, ou seja, $a, 2a, 3a, \ldots, (p-1)a$. Observemos primeiramente que estes números são dois a dois incongruentes módulo p. De fato, se $ak_1 \equiv ak_2 \ (mod\ p)$, com $1 \leq k_1 < k_2 \leq p-1$, então como $(a,p) = 1$, segue da *Lei do cancelamento* que $k_1 \equiv k_2 \ (mod\ p)$, isto é, $p \mid k_2 - k_1$, o que é impossível. Além disso, se $1 \leq r \leq p-1$ e $p \mid ra$, então $p \mid a$ ou $p \mid r$, o que também não é possível. Portanto, $ra \not\equiv 0 \ (mod\ p)$ para todo $r = 1, \ldots, p-1$. De acordo com o Algoritmo da Divisão, cada inteiro é congruente módulo p a um, e somente um, número da sequência $1, 2, 3, \ldots, p-1$. Portanto, cada inteiro de $a, 2a, 3a, \ldots, (p-1)a$ é congruente a um número de $1, 2, 3, \ldots, p-1$ numa determinada ordem, digamos $a \equiv b_1 \ (mod\ p)$, $2a \equiv b_2 \ (mod\ p), \ldots (p-1)a \equiv b(p-1) \ (mod\ p)$, em que $b_i \in \{1, 2, \ldots, p-1\}$ para $i = 1, 2, \ldots, p-1$. Multiplicando membro a membro estas congruências, temos que $a \cdot 2a \ldots (p-1)a \equiv 1 \cdot 2 \ldots (p-1) \ (mod\ p)$, isto é, $a^{p-1}(p-1)! \equiv (p-1)! \ (mod\ p)$. Como $((p-1)!, p) = 1$, podemos cancelar $(p-1)!$ desta última congruência, de modo $a^{p-1} \equiv 1 \ (mod\ p)$.

O resultado anterior implica que para um inteiro a qualquer, divisível por p ou não, $a^p \equiv a \ (mod\ p)$. □

Proposição 2.60 (O pequeno Teorema de Fermat)**.** *Se p é primo, então $a^p \equiv a \ (mod\ p)$ para qualquer inteiro a.*

Demonstração. Se $p \nmid a$, então pelo teorema anterior, $a^{p-1} \equiv 1 \ (mod\ p)$. Assim, multiplicando esta congruência por a, segue que $a^p \equiv a \ (mod\ p)$. Se $p \mid a$, então $p \mid a^p$ e, por isso, $p \mid a^p - a$, ou seja, $a^p \equiv a \ (mod\ p)$. □

Note que *o Pequeno Teorema de Fermat* fornece-nos um teste de não Primalidade. De fato, dado $m \in \mathbb{N}$, com $m > 1$, se existir algum $a \in \mathbb{N}$, com $(a, m) = 1$, tal que $m \nmid a^{(m-1)} - 1$, então m não é primo.

Exemplo 2.61. Mostrar que $2^{70} + 3^{70}$ é divisível por 13.

Solução: Do Pequeno Teorema de Fermat com $p = 13$ e $a = 2$, temos que $2^{12} \equiv 1 \ (mod\ 13)$. Por isso, $(2^{12})^5 \equiv 1^5 \ (mod\ 13)$, isto é, $2^{60} \equiv 1 \ (mod\ 13)$.

Agora, $2^5 \equiv 6 \ (mod\ 13) \Rightarrow 2^{10} \equiv 36 \ (mod\ 13)$. Assim, $2^{60} \cdot 2^{10} \equiv 1 \cdot 36 \ (mod\ 13)$, de modo que $2^{70} \equiv 36 \ (mod\ 13)$.

Da mesma forma, com $a = 3$ temos $3^{12} \equiv 1 \ (mod\ 13)$, de onde obtemos $(3^{12})^5 \equiv 1^5 \ (mod\ 13) \Rightarrow 3^{60} \equiv 1 \ (mod\ 13)$.

Além disso, $3^3 \equiv 1 \ (mod\ 13) \Rightarrow 3^9 \equiv 1 \ (mod\ 13) \Rightarrow 3^{10} \equiv 3 \ (mod\ 13)$.

Logo, $3^{10} \cdot 3^{60} \equiv 3 \cdot 1 \ (mod\ 13)$, isto é,

$\Rightarrow 3^{70} \equiv 3 \ (mod\ 13)$.

Somando membro a membro as congruências,

$2^{70} + 3^{70} \equiv 36 + 3 \ (mod\ 13) \Rightarrow 2^{70} + 3^{70} \equiv 39 \ (mod\ 13)$. Como $39 \equiv 0 \ (mod\ 13)$, então por transitividade, $2^{70} + 3^{70} \equiv 0 \ (mod\ 13)$.

Exemplo 2.62. Determinar o resto da divisão de 2^{2017} por 7.

Solução: Considerando $p = 7$ e $a = 2$, temos que $p \nmid a$. Assim, pelo Pequeno Teorema de Fermat, $2^6 \equiv 1 \ (mod\ 7)$. Elevando ambos os membros desta congruência por 336, pois $(2016 = 6 \cdot 336)$, obtemos $2^{2016} \equiv 1 \ (mod\ 7)$, Multiplicando esta congruência por 2, $2^{2017} \equiv 2 \ (mod\ 7)$. Logo, o resto da divisão é $r = 2$.

Exemplo 2.63. Prove que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ é um inteiro para todo inteiro n.

Solução: Primeiramente note que $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15} = \frac{3n^5+5n^3+7n}{15}$. Como $(3, 5) = 1$, basta mostrarmos que o numerador é múltiplo de 3 e 5. Pelo pequeno teorema de Fermat:

$3n^5 + 5n^3 + 7n \equiv 5n^3 + 7n \equiv 5n + 7n = 12n \equiv 0 \ (mod\ 3)$,

$3n^5 + 5n^3 + 7n \equiv 3n^5 + 7n \equiv 3n + 7n = 10n \equiv 0 \ (mod\ 5)$.

Exemplo 2.64. Mostre que $n^7 \equiv n \ (mod\ 42)$, $\forall n \in N$.

Solução: Pelo pequeno teorema de Fermat, $n^7 \equiv n \ (mod\ 7)$

$n^7 \equiv (n^3)^2 \cdot n \equiv n^2 \cdot n = n^3 \equiv n \ (mod\ 3)$

$n^7 \equiv (n^2)^3 \cdot n \equiv n^3 \cdot n = (n^2)^2 \equiv n^2 \equiv n \ (mod\ 2)$

Como 2, 3 e 7 são primos entre si, $n^7 \equiv n \ (mod\ 2 \cdot 3 \cdot 7 = 42)$.

Exemplo 2.65. *(Bulgária 95)* Encontre o número de inteiros $n > 1$ para os quais o número $a^{25} - a$ é divisível por n para cada inteiro a.

Solução: Se n satisfaz o enunciado, p^2 (p primo) não pode dividí-lo, pois $p^{25} - p$ não é divisível por p^2. Assim, n é múltiplo de primos diferentes. Os fatores primos de n são fatores de $2^{25} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$. Entretanto, n não é divisível por 17 e 241 pois $3^{25} \equiv -3 \ (mod\ 17)$ e $3^{25} \equiv 32 \ (mod\ 241)$. Seguindo o exemplo anterior, podemos usar o teorema de Fermat para mostrar que $a^{25} \equiv a \ (mod\ p)$ para $p \in \{2, 3, 5, 7, 13\}$. Portanto, n deve ser igual a um dos divisores de $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ diferente de 1. A quantidade de tais divisores é $2^5 - 1 = 31$.

Exemplo 2.66. Prove que para cada primo p, a diferença

$111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99 - 123456789$ (onde cada digito está escrito exatamente p vezes) é múltiplo de p.

Solução: Uma boa maneira de associar os números do problema com o teorema de Fermat é perceber que: $111\ldots11(p\ dígitos) = \frac{10^p-1}{9}$.

Assim, podemos escrever o número $S = 111\ldots11222\ldots22333\ldots33\ldots888\ldots88999\ldots99$ como:

$S = \frac{10^p-1}{9} \cdot 10^{8\mathrm{p}} + 2 \cdot \frac{10^p-1}{9} \cdot 10^{7\mathrm{p}} + \ldots 9 \cdot \frac{10^p-1}{9}$

$9S = (10^p - 1) \cdot 10^{8\mathrm{p}} + 2 \cdot (10^p - 1) \cdot 10^{7\mathrm{p}} + \ldots 9 \cdot (10^p - 1)$

Para $p = 2$ ou $p = 3$, o resultado do enunciado segue dos critérios de divisibilidade por 2 e 3. Podemos então nos concentrar no caso $p > 3$. Nesse caso, é suficiente mostrarmos que $9(S - 123456789)$ é divisível por p pois $(p, 9) = 1$. Pelo teorema de Fermat:

$9S = (10^p - 1) \cdot 10^{8\mathrm{p}} + 2 \cdot (10^p - 1) \cdot 10^{7\mathrm{p}} + \ldots 9 \cdot (10^p - 1) \equiv (10 - 1) \cdot 10^8 + 2 \cdot (10 - 1) \cdot 10^7 + \ldots + 9 \cdot (10 - 1)\ (mod\ p) \equiv 9 \cdot 123456789\ (mod\ p)$.

Exemplo 2.67. Dado um primo p, prove que existem infinitos naturais n tais que p divide $2^n - n$.

Solução: Se $p = 2$, n pode ser qualquer número par. Suponha que $p > 2$. Considere $(p - 1)^{2\mathrm{k}}$, pelo teorema de Fermat temos:

$2^{(p-1)^{2k}} \equiv (2^{(p-1)})^{(p-1)^{2k-1}}$

$\equiv 1^{(p-1)^{2k-1}} = 1 \equiv (p - 1)^{2\mathrm{k}}\ (mod\ p)$.

Assim, para qualquer k, $n = (p - 1)^{2\mathrm{k}}$ satisfaz o problema.

Exemplo 2.68. Dado um número qualquer $n \in \mathbb{N}$, tem-se que n^9 e n, quando escritos na base 10, têm o mesmo algarismo da unidade.

Solução: A afirmação acima é equivalente a $10 \mid n^9 - n$. Como n^9 e n têm a mesma paridade, segue-se que $n^9 - n$ é par; i.e., $2 \mid n^9 - n$.

Por outro lado, $n^9 - n = n(n^4 - 1)(n^4 + 1) = (n^5 - n)(n^4 + 1)$.

Logo, pelo Pequeno Teorema de Fermat, temos que $5 \mid n^5 - n$ e, portanto, $5 \mid n^9 - n$. Tem-se, então, que $10 \mid n^9 - n$.

2.4.3 O Teorema de Euler

Dedicaremos esta secção ao Teorema de Euler. Antes mostraremos alguns resultados necessários a sua demonstração.

Definição 2.69. Chama-se função φ *(leia-se fi) de Euler* ou função totiente, a função $\varphi : \mathbb{N} \to \mathbb{N}$, tal que $\varphi(1) = 1$ e para cada $m > 1$ temos que $\varphi(m)$ é a quantidade de inteiros positivos menores que m que são coprimos com m. Para cada $m > 1$, seja $\varphi(m) = s$, em que s é o número de inteiros positivos b, $1 \leq b < m$, tais que $(m, b) = 1$.

Por definição, temos que $\varphi(m) \leq m - 1$, para todo $m \geq 2$. Além do mais, se $m \geq 2$, então $\varphi(m) = m - 1$, se e somente se, p é primo. Os resultados a seguir serão relevantes para determinarmos uma expressão para $\varphi(m)$.

Exemplo 2.70. Temos que $\varphi(8) = 4$, pois 1, 3, 5 e 7 são menores do que 8 e coprimos com ele.

Exemplo 2.71. Temos que $\varphi(11) = 10$, pois 1, 2, 3, ..., 10 são menores do que 11 e coprimos com ele.

Teorema 2.72. *Se p é primo e $k \geq 1$, então $\varphi(p^k) = p^k - p^{k\text{ - }1} = p^k(1 - \frac{1}{p})$.*

Demonstração. Inicialmente, note que $(m, p^k) = 1$ se, e somente se, $p \not| m$. Agora, entre 1 e p^k existem $p^{\text{k-1}}$ números que são divisíveis por p, a saber $p, 2p, 3p, \ldots, (p^{\text{k - 1}})p$, pois $p\lambda \leq p^k$ se, e somente se, $\lambda = 1, 2, \ldots, p^{\text{k-1}}$. Desse modo, o conjunto $\left\{1, 2, \ldots, p^k\right\}$ contém exatamente $p^k - p^{\text{k - 1}}$ números que são relativamente primos com p^k. Daí, por definição, $\varphi(p^k) = p^k - p^{\text{k-1}} = p^k(1 - \frac{1}{p})$. □

Definição 2.73. Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $r_1, \ldots, r_s$ tais que

1. $(r_i, m) = 1$, para todo $i = 1, \ldots, s$,
2. $r_i \not\equiv r_j \ (mod\ m)$, se $i \neq j$,
3. Para cada $n \in \mathbb{Z}$ tal que $(n, m) = 1$, existe i tal que $n \equiv r_i \ (mod\ m)$.

Pode-se obter um sistema reduzido de resíduos módulo m a partir de um sistema completo qualquer de resíduos $a_1, \ldots, a_m$ módulo m, bastando para isso eliminar do sistema completo de resíduos todos os elementos que não são primos com m. De fato, as propriedades 1 e 2 da definição são claramente verificadas para $r_i, \ldots, r_s$. Por outro lado, dado um número inteiro n, existe j que $n \equiv a_j \ (mod\ m)$. Se $(n, m) = 1$, então, $(a_j, m) = 1$, e portanto, para algum j, temos que $a_j = r_i$ e, consequentemente, $n \equiv r_i \ (mod\ m)$.

Vamos designar por $\varphi(m)$ o número de elementos de um sistema reduzido de resíduos módulo $m > 1$, que corresponde à quantidade de números naturais entre 0 e $m - 1$ que são primos com m. Note ainda que dois sistemas reduzidos de resíduos módulo m têm o mesmo número de elementos.

Proposição 2.74. *Seja $r_1, \ldots, r_\varphi(m)$ um sistema reduzido de resíduos módulo m e seja $a \in \mathbb{Z}$ tal que $(a, m) = 1$. Então, $ar_1, \ldots, a_r\varphi(m)$ é um sistema reduzido de resíduos módulo m.*

Demonstração. Seja $a_1, \ldots, a_m$ um sistema completo de resíduos módulo m do qual foi retirado o sistema reduzido de resíduos $r_1, \ldots, r_{\varphi}(m)$. Do fato de que $(a, m) = 1$, tem-se que $(a_i, m) = 1$ se, e somente se, $(aa_i, m) = 1$, o resultado segue. □

Teorema 2.75. *A função φ de Euler é multiplicativa, isto é, se m e n são números naturais tais $(m, n) = 1$, então $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demonstração. O resultado é imediato se $m = 1$ ou $n = 1$. Portanto, vamos supor que $m > 1$ e $n > 1$. Vamos considerar a tabela formada pelos inteiros de 1 a mn, dada como segue:

$$\begin{bmatrix} 1 & 2 & \ldots r & \cdots & m \\ m+1 & m+2 & \ldots m+r & \cdots & 2m \\ 2m+1 & 2m+2 & \ldots 2m+r & \cdots & 3m \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (n-1)m+1 & (n-1)m+2 & \ldots (n-1)m+r & \cdots & nm \end{bmatrix}$$

Como se tem que $(t, mn) = 1$ se, e somente se, $(t, n) = (t, m) = 1$, para calcular $\varphi(mn)$, devemos determinar os inteiros na tabela acima que são simultaneamente primos com m e n. Se o primeiro elemento de uma coluna não for primo com n, então todos os elementos da coluna não são primos com n. Portanto, os elementos primos com n estão necessariamente nas colunas restantes que são em número $\varphi(n)$, cujos elementos são primos com n. Vejamos agora quais são os elementos primos com m em cada uma dessas colunas. Como $(m, n) = 1$, a sequência

$k, n + k, \ldots, (m-1)n + k$ forma um sistema completo de resíduos módulo m e, portanto, $\varphi(m)$ desses elementos são primos com m. logo, o número de elementos simultaneamente primos com n e m é $\varphi(m)\varphi(n)$. □

O próximo exemplo nos mostra como calcular $\varphi(n)$.

Exemplo 2.76. Calcular $\varphi(1008)$.

Solução: Como $1008 = 2^4 \cdot 3^2 \cdot 7$, $\varphi(1008) = \varphi(2^4 \cdot 3^2 \cdot 7) = \varphi(2^4)\varphi(3^2)\varphi(7) = (2^4 - 2^3)(3^2 - 3)(7 - 1) = 8 \cdot 6 \cdot 6 = 288$.

Usando o Teorema 2.72., com $m = 1008$, $p_1 = 2, p_2 = 3$ e $p_3 = 7$, segue que $\varphi(1008) = (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 1008(\frac{1}{2})(\frac{1}{3})(\frac{1}{7}) = 288$

Teorema 2.77. *Se $m = p_1^{r_1} \ldots p_k^{r_k}$ é uma decomposição de m em fatores primos, então, $\varphi(m) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k})$.*

Demonstração. Temos $\varphi(p_i^{r_i}) - p_i^{r_i} - 1 = p_i^{r_i}(1 - \frac{1}{p_i})$.

Portanto, $\varphi(p_1^{r_1} \ldots p_k^{r_k}) = p_1^{r_1}(1 - \frac{1}{p_1})p_2^{r_2}(1 - \frac{1}{p_2}) \ldots p_k^{r_k}(1 - \frac{1}{p_k}) = p_1^{r_1}p_2^{r_2} \ldots p_k^{r_k}(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \ldots (1 - \frac{1}{p_k}) = m(1 - \frac{1}{p_1})(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$. □

Teorema 2.78 (Teorema de Euler)**.** *Sejam m, $a \in \mathbb{Z}$ com $m > 1$ e $(a, m) = 1$. Então, $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.*

Solução:

Seja $r_1, \ldots, r_{\varphi(m)}$ um sistema reduzido de resíduos módulo m. Logo, pela Proposição 2.74., $ar_1, \ldots, ar_{\varphi(m)}$ formam um sistema reduzido de resíduos módulo m e, portanto, $ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\varphi}(m) \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\varphi(m)} \ (mod\ m)$.

Consequentemente, $a^{\varphi(m)} r_1 \cdot r_2 \ldots r_{\varphi(m)} = ar_1 \cdot ar_2 \ldots ar_{\varphi(m)} \equiv r_1 \cdot r_2 \ldots r_{\varphi(m)} \ (mod\, m)$. Como $(r_1 \cdot r_2 \ldots r_{\varphi(m)}, m) = 1$, é válida a lei do cancelamento e, então, $a^{\varphi(m)} \equiv 1 \ (mod\ m)$.

Observação: O Teorema de Euler é a forma generalizada do Pequeno Teorema de Fermat, que considera congruências módulo m, em que m pode ser primo ou não.

Exemplo 2.79.

Determinar o resto da divisão de 3^{2017} por 8.

Solução: Como $(3, 8) = 1$, podemos aplicar o Teorema de Euler considerando $a = 3$ e $m = 8$. Fazendo isso, como $\varphi(8) = \varphi(2^3) = 2^3 - 2^2 = 4$, $3^4 \equiv 1 \ (mod\ 8)$.

Elevando ambos os membros desta congruência a $504 (2017 = 4 \cdot 504 + 1)$, obtemos que $3^{2016} \equiv 1 \ (mod\ 8)$. Logo, $3^{2017} \equiv 3 \ (mod\ 8)$ e, portanto, o resto procurado é $r = 3$.

Exemplo 2.80. *(IMO)* Seja $s(n)$ a soma dos dígitos de n. Se $N = 4444^{4444}$, $A = s(N)$ e $B = s(A)$. Quanto vale $s(B)$?

Solução:

Observação: Solução dada pela professora Ana Paula Chaves.

Pelo critério de divisibilidade por 9, $N \equiv A \equiv B \ (mod\ 9)$. Inicialmente calculemos o resto de N por 9. Como $4444 \equiv 16 \equiv 7 \ (mod\ 9)$, precisamos encontrar $7^{4444} \ (mod\ 9)$. Seguindo os métodos dos primeiros exemplos, seria interessante encontrarmos um inteiro r tal que $7^r \equiv \pm 1 \ (mod\ 9)$. O menor inteiro positivo com essa propriedade é $r = 3$. Como $4444 = 1481 \cdot 3 + 1$, temos: $7^{4444} \equiv 7^{1481\ \cdot\ 3+1} \equiv (7^3)^{1481} \cdot 7 \equiv 7 \ (mod\ 9)$. Nosso próximo passo é estimar o valor de $s(B)$. Como $N = 4444^{4444} < 10^{5\ \cdot\ 4444}$, $A = s(N) \leq 5 \cdot 4444 \cdot 9 = 199980$. Além disso, $B = s(A) \leq 1 + 9 \cdot 5 = 46$ e $s(B) \leq 12$. O único inteiro menor ou igual a 12 com resto 7 por 9 é o próprio 7, daí $s(B) = 7$.

Exemplo 2.81. Prove que $11^{n+2} + 12^{2n+1}$ é divisível por 133 para qualquer natural n.

Solução: Duas relações que podemos extrair dos números envolvidos são: $144 - 11 = 133$ e $133 - 12 = 121$. Assim:

$144 \equiv 11 \ (mod\ 133)$,

$12^2 \equiv 11 \ (mod\ 133)$,

$12^{2n} \equiv 11^n \ (mod\ 133)$,

$12^{2n+1} \equiv 11^n \cdot 12 \ (mod\ 133)$,

$12^{2n+1} \equiv 11^n \cdot (-121) + 133 \cdot 11^n \ (mod\ 133)$,

$12^{2n+1} \equiv -11^{n+2} \ (mod\ 133)$.

Exemplo 2.82. Prove que $n^5 + 4n$ é divisíivel por 5 para todo inteiro n.

Solução: Inicialmente note que $n^5 + 4n = n(n^4 + 4)$. Se $n \equiv 0 \ (mod\ 5)$, não há o que fazer. Se $n \equiv \pm 1 \ (mod\ 5)$, $n^4 + 4 \equiv 1 + 4 = 0 \ (mod\ 5)$. Finalmente, se $n \equiv \pm 2 \ (mod\ 5)$, $n^2 \equiv 4 \equiv -1 \ (mod\ 5)$ e consequentemente $n^4 + 4 \equiv 1 + 4 = 0 \ (mod\ 5)$.

Exemplo 2.83. Seja $n > 6$ um inteiro positivo tal que $n - 1$ e $n + 1$ são primos. Mostre que $n^2(n^2 + 16)$ é divisível por 720. A recíproca é verdadeira?

Solução: Veja que n é da forma $6k$, pois $n - 1$ e $n + 1$ são primos maiores que 3, portanto da forma $6k - 1$ e $6k + 1$, respectivamente. Logo, $n^2(n^2 + 16) = 144(9k^4 + 4k^2)$. Resta provar que $9k^4 + 4k^2$ é um múltiplo de 5. Vamos analisar a igualdade acima módulo 5.

i) Se $k \equiv 0$, 2 ou 3 $(mod\ 5)$, temos $9k^4 + 4k^2 \equiv 0 \ (mod\ 5)$;

ii) Se $k \equiv 1 \ (mod\ 5) \Rightarrow n \equiv 1 \ (mod\ 5)$, temos $n - 1 \equiv 0 \ (mod\ 5)$, um absurdo;

iii) Se $k \equiv 4 \ (mod\ 5) \Rightarrow n \equiv 4 \ (mod\ 5)$, temos $n + 1 \equiv 0 \ (mod\ 5)$, novamente um absurdo.

Isso conclui a demonstração. A recíproca não é verdadeira. Considere, por exemplo, $n = 90$.

Exemplo 2.84. Se $(a, m) = 1$ então existe um inteiro x tal que $ax \equiv 1 \ (mod\ m)$. Tal x é único módulo m. Se $(a, m) > 1$ então não existe tal x.

Solução: Pelo teorema de Bachet-Bézout, existem inteiros x e y tais que $ax + my = 1$. Analisando essa congruência módulo m, obtemos $ax \equiv 1 \ (mod\ m)$. Se y é outro inteiro que satisfaz a congruência, temos $ax \equiv ay \ (mod\ m)$. Pelo primeiro lema, $x \equiv y (mod\ m)$. Se $d = (a, m) > 1$, não podemos ter $d \mid m$ e $m \mid ax - 1$ pois $d \nmid ax - 1$.

3 Teorema Chinês dos restos

3.1 Uma primeira abordagem para o Teorema Chinês dos Restos

Historicamente narra-se que alguns generais chineses, na antiguidade, contavam suas tropas, para saber o efetivo perdido em batalha, ordenando-as em diversas linhas e colunas com um determinado tamanho e, depois, contava as tropas que sobravam, desta forma sabendo o total das perdas. Suponha que um general chinês possuísse 3000 soldados para uma batalha. Terminado o confronto, o general precisava verificar essas perdas. Então, mandou que os soldados se pusessem em formação, alinhados de 3 em 3 tropas, e sobraram 2 tropas. Em seguida, ordenou que se colocassem em formação alinhados de 5 em 5 e verificou que sobraram 3. Por fim, fez com que os soldados formassem alinhados de 7 em 7 e sobrou apenas uma tropa. Diante disso, a questão era a seguinte:

Quantos soldados morreram na batalha?

Modernamente resolvemos a sistema de congruência abaixo:

Para resolver o sistema de congruências:

$$\begin{aligned} x &\equiv 2 \ (mod\ 3), \\ x &\equiv 3 \ (mod\ 5), \\ x &\equiv 2 \ (mod\ 7). \end{aligned}$$

Nota-se que os números 3, 5 e 7 são coprimos em pares. Vamos agora encontrar um x que é solução do sistema. Para isto vamos pensar em x como a soma de três parcelas que serão representadas na seguinte equação: $x = \underline{1^{a}parcela} + \underline{2^{a}parcela} + \underline{3^{a}parcela}$.

O intuito desta representação é tornar visível a construção da solução do sistema de congruências. Como desejamos que este número satisfaça o sistema, vamos fazer com que a primeira parcela seja relativa à primeira equação, a segunda referente a segunda equação e a terceira relativa a terceira equação. Assim, ao aplicarmos $(mod\ 3)$ na equação das parcelas de x devemos apenas ficar com a primeira parcela. Para isto ocorrer, podemos colocar na segunda e na terceira parcela o valor 3, já que $3 \equiv 0\ (mod\ 3)$. Então temos: $x = \underline{1^{a}parcela} + 3 + 3$.

Pelo mesmo pensamento anterior, queremos que a primeira e a terceira parcela sejam insignificantes quando aplicarmos $(mod\ 5)$. Então as transformaremos em múltiplos de cinco. Sendo assim, temos: $x = 5 + 3 + 5 \times 3$.

Analogamente, como queremos que a terceira parcela seja referente à terceira equação, vamos multiplicar as duas primeiras por 7, obtendo: $x = 7 \times 5 + 7 \times 3 + 5 \times 3$, $x = 35 + 21 + 15$.

Agora vamos nos lembrar do que queríamos originalmente. Aplicando $(mod\ 3)$ na equação parcelada de x, obtemos: $x \equiv 35\ (mod\ 3) + 21\ (mod\ 3) + 15\ (mod\ 3)$, $x \equiv 2\ (mod\ 3) + 0\ (mod\ 3) + 0\ (mod\ 3)$, $x \equiv 2\ (mod\ 3)$, como queríamos. Fazendo o mesmo processo desta vez com $(mod\ 5)$, obteremos a seguinte equivalência: $x \equiv 1\ (mod\ 5)$, porém, pela segunda equação queremos $x \equiv 3\ (mod\ 5)$, então precisamos encontrar um número tal que, ao multiplicar a terceira parcela por ele, obteremos a equivalência desejada. Por tentativa, vemos facilmente que $3 \times 21 = 63 \equiv 3\ (mod\ 5)$. Então devemos multiplicar 21, que é a segunda parcela, por 3; obtendo $63 \equiv 3\ (mod\ 5)$. Analogamente, aplicando $(mod\ 7)$ obteremos a seguinte equivalência: $x \equiv 1\ (mod\ 7)$. Utilizando o algoritmo da divisão de Euclides concluímos facilmente que será necessário multiplicar a terceira parcela por 2, obtendo $30 \equiv 2\ (mod\ 7)$. Então, somando as três parcelas obtemos: $x = 35 + 63 + 30 = 128$. Pela própria construção do número x verificamos que ele satisfaz o sistema. Porém, esta não é a única solução. Ao somar ou subtrair o $(3, 5, 7) = 105$, vamos obter uma nova solução para este sistema, então, podemos escrever as soluções como sendo $x \equiv 128\ (mod\ 105) \equiv 23\ (mod\ 105)$.

3.1.1 Uma abordagem Técnica do Teorema Chinês dos Restos

Teorema 3.1. *(Teorema Chinês dos Restos) Sejam $n_1, n_2, \ldots, n_k$ números naturais tais que $(n_i, n_j) = 1$ para $i \neq j$. Então, o sistema de congruências lineares dado em 2.2 possui uma solução, que é única módulo $n = n_1 \cdot n_2 \ldots n_k$.*

Demonstração. Sendo $n = n_1 \cdot n_2 \ldots n_k$, então $N_i = \frac{n}{n_i} = n_1 \cdot n_2 \ldots (n_i - 1)(n_i + 1) \ldots n_k$, ou seja, N_i é o produto de todos os inteiros $n_1 n_2 \ldots n_k$ excluindo n_i. Como $(n_i, n_j) = 1$ para $i \neq j$, então $(N_i, n_i) = 1$. Assim, pela identidade de Bachet-Bézout, existem inteiros r_i e s_i tais que $r_i N_i + s_i n_i = 1$, para cada $i = 1, \ldots, k$. Vamos provar que o inteiro $x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \ldots + c_k r_k N_k$ é uma solução do sistema dado. Inicialmente, se $i \neq j$, então $N_j \equiv 0\ (mod\ n_i)$, já que $n_i \mid N_i$.
Logo, $c_j r_j N_j \equiv 0\ (mod\ n_i)$, de modo que $x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + \ldots + c_k r_k N_k \equiv c_i r_i N_i\ (mod\ n_i)$.

Por outro lado, de $r_i N_i + s_i n_i = 1$, $r_i N_i \equiv 1\ (mod\ n_i)$ para cada $i = 1, \ldots, k$. Daí, $c_i r_i N_i \equiv c_i\ (mod\ n_i)$ e, por transitividade, $x_0 \equiv c_i\ (mod\ n_i)$ para todo i. Isso mostra que x_0 é uma solução do sistema. Por fim, se y_0 é outra solução do sistema, então $y_0 \equiv c_i\ (mod\ n_i)$ para cada $i = 1, \ldots, k$. Desse modo, $x_0 \equiv y_0\ (mod\ n_i)$, isto é, $n_i \mid x_0 - y_0$. Como $(n_i, n_j) = 1$, com $i \neq j$, segue do Lema de Euclides que, $n = n_1 n_2 \ldots n_k$ divide

$x_0 - y_0$, ou seja, $x_0 \equiv y_0 \ (mod\ n)$, o que prova a unicidade de solução módulo n. Por isso, a solução geral do sistema é $x = x_0 + kn, k \in \mathbb{Z}$. □

Exemplo 3.2. Determine a solução do sistema

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

usando o Teorema Chinês dos Restos.

Solução: Desde que $(3,5) = (3,7) = (5,7) = 1$, então podemos aplicar o Teorema Chinês dos Restos. Note que $n_1 = 3$, $n_2 = 5$, $n_3 = 7$ e $n = n_1 \cdot n_2 \cdot n_3 = 3 \cdot 5 \cdot 7 = 105$, por outro lado, $N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$, $N_2 = \frac{n}{n_2} = \frac{105}{5} = 21$ e $N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$:

Agora, vamos determinar os inteiros r_i, s_i com $i = 1, 2, 3$ tais que, $r_i N_i + s_i n_i = 1$.

$r_1 N_1 + s_1 n_1 = 1 \Rightarrow r_1 \cdot 35 + s_1 \cdot 3 = 1 \Rightarrow r_1 = -1$ e $s_1 = 12$
$r_2 N_2 + s_2 n_2 = 1 \Rightarrow r_2 \cdot 21 + s_2 \cdot 5 = 1 \Rightarrow r_2 = 1$ e $s_2 = -4$
$r_3 N_3 + s_3 n_3 = 1 \Rightarrow r_3 \cdot 15 + s_3 \cdot 7 = 1 \Rightarrow r_3 = 1$ e $s_3 = -2$:

Como $c_1 = 2$, $c_2 = 3$ e $c_3 = 2$, então uma solução para o sistema pode ser dada por: $x_0 = c_1 r_1 N_1 + c_2 r_2 N_2 + c_3 r_3 N_3 = 2 \cdot (-1) \cdot 35 + 3 \cdot 1 \cdot 21 + 2 \cdot 1 \cdot 15 = 23$.

Logo, a solução geral do sistema pode ser expressa da seguinte forma $x = 23 + 105t$, $t \in \mathbb{Z}$

Exemplo 3.3. 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 diferia 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 total?

Solução: Após a colheita, o montante produzido de arroz é distribuídos de forma igualitária entre os trés fazendeiros. Então, seja x a quantidade de arroz de cada um dos fazendeiros.

Equacionando o problema, teremos que:

Primeiro Fazendeiro: $x \equiv 18\ (mod\ 87)$;

Segundo Fazendeiro: $x \equiv 58\ (mod\ 170)$;

Terceiro Fazendeiro: $x \equiv 40\ (mod\ 143)$.

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:

$$\begin{cases} \text{x} \equiv 18 \equiv 0\ (mod\ 3) \\ \text{x} \equiv 18\ (mod\ 29) \\ \text{x} \equiv 58 \equiv 0\ (mod\ 2) \\ \text{x} \equiv 58 \equiv 3\ (mod\ 5) \\ \text{x} \equiv 58 \equiv 7\ (mod\ 17) \\ \text{x} \equiv 40 \equiv 7\ (mod\ 11) \\ \text{x} \equiv 40 \equiv 1\ (mod\ 13) \end{cases}$$

Utilizando o Teorema Chinês dos Restos:

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

$y_1 M_1 \equiv 1\ (mod\ 6) \Rightarrow y_1 \cdot 352495 \equiv 1\ (mod\ 6) \Rightarrow y_1 \equiv 1\ (mod\ 6)$;

$y_2 M_2 \equiv 1\ (mod\ 5) \Rightarrow y_2 \cdot 422994 \equiv 1\ (mod\ 5) \Rightarrow y_2 \equiv 4\ (mod\ 5)$;

$y_3 M_3 \equiv 1\ (mod\ 13) \Rightarrow y_3 \cdot 162690 \equiv 1\ (mod\ 13) \Rightarrow y_3 \equiv 5\ (mod\ 13)$;

$y_4 M_4 \equiv 1\ (mod\ 11) \Rightarrow y_4 \cdot 192270 \equiv 1\ (mod\ 11) \Rightarrow y_4 \equiv 1\ (mod\ 11)$;

$y_5 M_5 \equiv 1\ (mod\ 17) \Rightarrow y_5 \cdot 124410 \equiv 1\ (mod\ 17) \Rightarrow y_5 \equiv 13\ (mod\ 17)$;

$y_6 M_6 \equiv 1\ (mod\ 29) \Rightarrow y_6 \cdot 72930 \equiv 1\ (mod\ 29) \Rightarrow y_6 \equiv 23\ (mod\ 29)$.

Assim, a solução será dada por: $x \equiv r_1 M_1 y_1 + r_2 M_2 y_2 + r_3 M_3 y_3 + r_4 M_4 y_4 + r_5 M_5 y_5 + r_6 M_6 y_6\ (mod\ M)$

$x \equiv 0 \cdot 352495 \cdot 1 + 3 \cdot 422994 \cdot 4 + 1 \cdot 162690 \cdot 5 + 7 \cdot 192270 \cdot 1 + 7 \cdot 124410 \cdot 13 + 18 \cdot 72930 \cdot 23\ (mod\ 2114970)$

$x \equiv 0 + 5075928 + 813450 + 1345890 + 11321310 + 30193020\ (mod\ 2114970)$

$x \equiv 48749598\ (mod\ 2114970) \Rightarrow x \equiv 105288\ (mod\ 2114970)$

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 3.4. Para cada número natural, 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: Dado $m \in \mathbb{N}$ considere o conjunto $\{p_1, p_2, \cdots, p_m\}$ de primos distintos. Como $(p_i^s, p_j^s) = 1$, então, existe x tal que $x \equiv -i \ (mod\ p_i^s)$ para $i = 1, 2, \cdots m$. Cada um dos números do conjunto $\{x+1, x+2, \cdots, x+m\}$ é divisível por um número da forma p_i^s.

Exemplo 3.5. (USAMO 1986)

(a) Existem 14 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 11$?

(b) Existem 21 inteiros positivos consecutivos tais que, cada um é divisível por um ou mais primos p do intervalo $2 \leq p \leq 13$?

Solução:

(a) Não. Suponha que existam tais inteiros. Da nossa lista de 14 inteiros consecutivos, 7 são números pares. Vamos observar os ímpares: a, $a+2$, $a+4$, $a+6$, $a+8$, $a+10$ e $a+12$. Podemos ter no máximo três deles divisíveis por 3, dois por 5, um por 7 e um por 11. Veja que $3 + 2 + 1 + 1 = 7$. Pelo Princípio da Casa dos Pombos, cada um desses ímpares é divisível por exatamente um primo do conjunto $\{3, 5, 7, 11\}$. veja que os múltiplos de 3 só podem ser $\{a, a+6, a+12\}$. Dois dos números restantes $a+2, a+4, a+8$, e $a+10$ são divisíveis por 5. Mas isto é impossível.

(b) Sim. Como os números

$$\{210, 11, 13\}$$

são primos entre si, dois a dois, existe um inteiro positivo $n > 10$ tal que:

$n \equiv 0 \ (mod\ 210)$ e $210 = 2 \cdot 3 \cdot 5 \cdot 7$

$n \equiv 1 \ (mod\ 11)$

$n \equiv -1 \ (mod\ 13)$

Veja que o conjunto $\{n-10, n-9, \cdots, n+9, n+10\}$ satisfaz as condições do item (b).

Exemplo 3.6. *(Estônia 2000)* Determine todos os restos possíveis da divisão do quadrado de um número primo com 120 por 120.

Solução: Seja n tal que $(n, 120) = 1$. Como $120 = 3 \cdot 5 \cdot 8$, temos que $n \not\equiv 0 \ (mod\ 3)$, $(mod\ 5), (mod\ 2)$. Daí, $n^2 \equiv 1 \ (mod\ 8)$ e $n^2 \equiv 1$ ou $4 \ (mod\ 5)$. Sendo assim, n^2 satisfaz o sistema:

$$x \equiv 1 \ (mod\ 3)$$
$$x \equiv 1 \ (mod\ 8)$$
$$x \equiv \pm 1 \ (mod\ 5)$$

cujas soluções são $x \equiv 1 \ (mod\ 120)$ e $x \equiv 49 \ (mod\ 120)$.

Aconselhamos ao leitor a resolução de alguns exemplos numéricos até adquirir prática com o algoritmo usado para encontrar x_0.

Exemplo 3.7. Existem n inteiros consecutivos tal que cada um contém um fator primo repetido k vezes?

Exemplo 3.8. *(OBM 2005)* Dados os inteiros positivos a, c e o inteiro b, prove que existe um inteiro positivo x tal que $a^x + x \equiv b \ (mod\ c)$.

Exemplo 3.9. Sejam a e b inteiros positivos tais que, para qualquer n natural, $a^n + n \mid b^n + n$.

Prove que $a = b$.

Solução: Seja p um primo maior que a e b. Então $(p, a) = (p, b) = 1$. Como $(p, p-1) = 1$, existe um inteiro positivo n tal que $n \equiv 1 \ (mod\ p-1)$ e $n \equiv -a \ (mod\ p)$. Pelo teorema de Fermat, $a^n + n \equiv 0 \ (mod\ p)$ e $b^n + n \equiv b - a \ (mod\ p)$. Assim, $p \mid |b - a|$. Como $|b - a| < p$, segue que $|b - a| = 0$ e $a = b$.

Exemplo 3.10. (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:

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

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

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

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

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

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:

$$\begin{cases} 15 \cdot y_1 \equiv 1 \ (mod\ 2) \\ 10 \cdot y_2 \equiv 2 \ (mod\ 3) \\ 6 \cdot y_3 \equiv 4 \ (mod\ 5) \end{cases}$$

$$\begin{cases} y_1 \equiv 1 \ (mod\ 2) \\ y_2 \equiv 1 \ (mod\ 3) \\ y_3 \equiv 1 \ (mod\ 5) \end{cases}$$

$$\begin{cases} y_1 = 1 \\ y_2 = 1 \\ y_3 = 1 \end{cases}$$

$x \equiv r_1 \cdot M_1 \cdot y_1 + r_2 \cdot M_2 \cdot y_2 + r_3 \cdot M_3 \cdot y_3 \ (mod\ M)$

$\mathrm{x} \equiv 1 \cdot 15 \cdot 1 + 1 \cdot 10 \cdot 1 + 1 \cdot 6 \cdot 1 \ (mod\ 30) \Rightarrow$

$\mathrm{x} \equiv 59 \ (mod\ 30) \Rightarrow x \equiv 29 \ (mod\ 30)$.

Portanto a solução do sistema é dada por $x \equiv 29 \ (mod\ 30)$, ou seja, $x = 29 + 30k$, com k inteiro. Agora, temos o sistema :

$$\begin{cases} x \equiv 29 \ (mod\ 30) \\ x \equiv 3 \ (mod\ 4) \end{cases}$$

substituímos $x = 29 + 30k$ na congruência $x \equiv 3 \ (mod\ 4)$.

Assim, temos: $29 + 30k \equiv 3 \ (mod\ 4)$, que é o mesmo que $1 + 2k \equiv 3 \ (mod\ 4)$. Ou ainda: $3 + 1 + 2k \equiv 3 + 3 \ (mod\ 4)$, que nos leva para $2k \equiv 2 \ (mod\ 4)$, 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.

Finalizamos este capítulo deixando para o leitor os seguintes problemas:

Problema Proposto 3.11. Use o Teorema Chinês de Restos para resolver o seguinte sistema de congruências lineares:

$$\begin{cases} \text{x} \equiv 2 \ (mod\ 3) \\ \text{x} \equiv 3 \ (mod\ 5) \\ \text{x} \equiv 2 \ (mod\ 7) \end{cases}$$

Problema Proposto 3.12. Utilizando O Teorema Chinês dos Restos, resolver o sistema de congruências lineares:

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

Problema Proposto 3.13. 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

Problema Proposto 3.14. Dispomos de uma quantia x reais menor do que 3000. Se distribuirmos essa quantia entre 11 pessoas, sobra RS1,00; se a distribuirmos entre 12 pessoas, sobram RS2,00 e se a distribuirmos entre 13 pessoas, sobram RS3,00. De quantos reais dispomos?

Problema Proposto 3.15. Um macaco, ao subir uma escada de dois em dois degraus, deixa de sobra um degrau, ao subir de três em três degraus, sobram dois degraus; e ao subir de cinco em cinco degraus, sobram três degraus. Quantos degraus possui a escada, sabendo que o número de degraus está entre 150 e 200?

Observação: Existe uma forma mais geral do Teorema Chinês dos Restos. O sistema de congruências $X \equiv c_i \ (mod\ m_i)$, $i = 1, \cdots r$, admite solução se, e somente se, $c_i \equiv c_j \ (mod(m_i, m_j))$, $\forall i,\ j = 1, \cdots, r$. Nesse caso, a solução é única módulo $[m_1, \cdots, m_r]$. Não demonstraremos esse resultado, pois, foge do escopo do trabalho. Indicamos o Módulo 2, Volume 2 do livro Introdução a Criptografia, cujo autor, Luiz Manoel Figueiredo da

Fundação CECIERJ, aprofunda o conceito do Teorema Chinês dos Restos até a sua generalização.

4 Noções de Criptografia

4.1 Introdução

Criptografia é um processo de conversão de mensagens, informações ou dados em um formato ilegível para qualquer pessoa, exceto pelo destinatário pretendido. Os dados criptografados devem ser decifrados ou descriptografados, antes que possam ser lidos pelo destinatário. A raiz da palavra criptografia vem da língua grega, da palavra kryptos, que significa oculto ou secreto. Na sua forma mais antiga, as pessoas tentavam ocultar certas informações que eles queriam manter sua autoria substituindo partes da informação por símbolos, números ou fotos. Este capítulo destaca em cronologia a história da criptografia ao longo dos séculos. Por motivos diferentes os seres humanos têm se interessado em proteger suas mensagens. Os assírios estavam interessados em proteger seu comércio e os segredos da fabricação da cerâmica. Os chineses eram interessados em proteger seu segredo comercial de fabricação da seda. Os alemães estavam interessados em proteger seus segredos militares usando sua famosa máquina Enigma. Com o avanço dos computadores e da interconectividade, instituições e indústrias governamentais estão sujeitos a ataques cibernéticos, intrusão e espionagem.

Neste capítulo iniciaremos uma discussão sobre criptografia, isto é, a técnica de ocultar de terceiros uma informação compartilhada. Por exemplo, deseja-se encaminhar uma mensagem pelo aplicativo de relacionamentos *WhatsApp*, que apenas o destinatário do número consiga ter acesso a este dado. Neste caso, quem envia os seus dados pessoais transforma-os de forma que apenas a companhia envolvida na transação pode recuperá-los através de um procedimento que é de seu conhecimento apenas. Neste caso a comunicação que seja interceptada por alguém não autorizado, se transforma em um conteúdo não legível, pois, a informação é acessível apenas para aqueles que possuem o algoritmo para decifrá-la, no caso, a firma. Discutiremos procedimentos para ocultar a informação contida em uma mensagem e como recuperá-la. A seguir, é apresentada a história cronológica da criptografia.

Por volta de 1900 a.C. um escriba egípcio usou uns hieróglifos, não comuns, em uma inscrição. O historiador David Kahn lista como o primeiro exemplo documentado de criptografia escrita. Aproximadamente 1500 a.C. antigos comerciantes assírios usavam o intaglio, um pedaço de pedra lisa esculpida em uma colagem de imagens, e utilizavam para se identificar nas transações comerciais. Usando esse mecanismo, eles estavam produzindo um produto muito semelhante ao que hoje conhecemos como assinatura digital. O público sabia que uma determinada assinatura pertencia a esse profissional, mas somente ele tinha o intaglio para produzir essa assinatura.

Por volta de 500-600 a.C. os escribas hebreus escreveram o livro de Jeremias usando uma substituição simples de alfabeto reverso, que era conhecida como ATBASH, algumas cifras hebraicas da época. (Jeremias começou a ditar para Baruch em 605 a.C., mas os capítulos que contêm esses pedaços de cifra são atribuídos a uma fonte rotulada como C. Baruch, que poderia ser um editor escrevendo após o Exílio babilônico em 587 a.C., alguém contemporâneo a Baruch ou até o próprio Jeremias).

Júlio César (100-44 a.C.) usou uma simples substituição por o alfabeto normal apenas mudando as letras para um número fixo nas comunicações do governo. Essa cifra era menos forte que ATBASH. Ele também usou a transliteração do latim para o grego e várias outras cifras simples. Quando Julius César enviava mensagens para seus conhecidos de confiança, ele não confiava nos mensageiros. Então ele substituiu todo A por um D, todo B por um E, e assim por diante através do alfabeto. Só alguém que soubesse a regra poderia decifrar suas mensagens.

Em 1917 William Frederick Friedman, mais tarde reconhecido como o pai da criptoanálise dos EUA, foi empregado como cripto analista civil (junto com com sua esposa Elisabeth) nos Laboratórios Riverbank e realizou criptoanálise para o governo dos EUA, que não possuia nenhuma experiência cripto analítica própria. O governo norte americano criou uma escola para cripto analistas militares em Riverbank, mais tarde levando esse trabalho para Washington e deixando Riverbank.

Em 1933-1945 a máquina Enigma foi melhorada para se tornar o cavalo de batalha criptográfico da Alemanha nazista. Foi quebrada pelo matemático polonês, Marian Rejewski, baseado apenas no texto cifrado capturado e em uma lista de três meses de chaves diárias obtidas através de um espião. Como também, Alan Mathison Turing que planejou uma série de técnicas para quebrar os códigos alemães, incluindo o método da bomba eletromecânica, uma máquina eletromecânica que poderia encontrar definições para a máquina Enigma.

Em 1976 um projeto da IBM, o algoritmo de criptografia DES foi desenvolvido pelo National Bureau of Standarts com ajuda da National Security Agency. O propósito era criar um método padrão para proteção de dados. A IBM criou o primeiro rascunho do algoritmo, chamando-o de LUCIFER. O DES tornou-se oficialmente a norma de proteção de dados federal americana em novembro de 1976, baseado na cifra do algoritmo LUCIFER criado por Horst Feistel com algumas alterações (incluindo melhorias na caixa S e redução do tamanho da chave) pela NSA dos EUA. Desde então, esse algoritmo encontrou aceitação mundial, em grande parte porque se mostrou forte contra 20 anos de ataques. Ainda em 1976 Whitfield Diffie e Martin Hellman publicaram Novas direções em criptografia, introduzindo a ideia de criptografia de chave pública.

Foram três americanos que deram um grande passo para o nascimento de um sistema revolucionário chamado Sistema RSA, são eles: Whitfield Diffie, Martín Hellman e Ralph Merkle. Quebraram um paradigma, que era resolver de modo mais racional o

problema da troca de chaves entre correspondentes sem a intermediação de um portador. É aí que começa a entrar no campo da criptografia, timidamente, mas de modo irreversível, a Teoria dos Números através da noção de congruência, descrita como segue.

Bruno e Alice querem trocar entre si uma chave secreta por meio de comunicação insegura, com por exemplo, por telefone. Eles escolhem em comum acordo um par de números naturais a e m e os torna públicos. Bruno escolhe um outro número natural α_J e o mantém secreto. Com ele, calcula o único número $0 \leq \beta_J < m$ tal que $a^{\alpha_J} \equiv \beta_J \ (mod\ m)$, e o envia para Alice. Por sua vez, Alice escolhe um número natural α_M, mantendo-o secreto, e com ele calcula o único número $0 \leq \beta_M < m$ tal que $a^{\alpha_M} \equiv \beta_M \ (mod\ m)$, e o envia para Bruno.

Em seguida, Bruno calcula $\beta_M^{\alpha_J}$, obtendo

$\beta_M^{\alpha_J} \equiv (a^{\alpha_M})^{\alpha_J} \equiv a^{\alpha_M \alpha_J} \equiv \alpha \ (mod\ m)$, com $\alpha < m$.

Por sua vez, Alice calcula $\beta_J^{\alpha_M}$, obtendo

$\beta_J^{\alpha_M} \equiv (a^{\alpha_J})^{\alpha_M} \equiv a^{\alpha_J \alpha_M} \equiv \alpha \ (mod\ m)$, com $\alpha < m$. Assim, está trocada a chave secreta α entre Bruno e Alice.

Exemplo 4.1. Suponha que Bruno e Alice tenham escolhido de comum acordo $a = 52$ e $m = 271$. Por outro lado, Bruno escolhe sua chave secreta $\alpha_J = 7$, enquanto Alice escolhe $\alpha_M = 5$. Vejamos qual é a chave secreta α que ambos compartilharão.

Bruno faz o seguinte cálculo para determinar β_J e enviá-lo a Alice:

$52^2 \equiv 2704 \equiv 265 \ (mod\ 271)$,

$52^4 \equiv 265^2 \equiv 36 \ (mod\ 271)$,

$52^7 = 52^4 \cdot 52^2 \cdot 52 \equiv 36 \cdot 265 \cdot 52 \equiv 150 \ (mod\ 271)$.

Agora vamos calcular β_M

$52^2 \equiv 2704 \equiv 265 \ (mod\ 271)$,

$52^4 \equiv 265^2 \equiv 36 \ (mod\ 271)$,

$52^5 \equiv 52^4 \cdot 52 \equiv 3653 \equiv 246 \ (mod\ 271)$,

Logo, $\beta_M = 246$.

Para determinar a chave α, Bruno tem que reduzir $\beta_M^{\alpha_j} = 246^7 \ (mod\ 271)$. Logo,

$246^2 = 60516 \equiv 83 \ (mod\ 271)$,

$246^4 = 246^2 \cdot 246^2 \equiv 83 \cdot 83 \equiv 114 \ (mod\ 271)$,

$246^7 = 246^4 \cdot 246^2 \cdot 246 \equiv 114 \cdot 83 \cdot 246 \equiv 33 \ (mod\ 271)$.

Bruno encontra então $\alpha = 33$.

Agora é a vez de Alice calcular o resíduo de $\beta_J^{\alpha_M} = 150^5 \ (mod\ 271)$. Mas,

$150^2 = 22500 \equiv 7 \ (mod\ 271)$,

$150^5 = 150^2 \cdot 150^2 \cdot 150 = 7 \cdot 7 \cdot 150 \equiv 33 \ (mod\ 271)$, encontrando também, como era de se esperar, $\alpha = 33$.

Em 1977 Inspirado pelo artigo Diffie-Hellman e atuando como novatos completos em criptografia, Ronald L. Rivest, Adi Shamir e Leonard M. Adleman estavam discutindo como criar um sistema prático de chave pública. Uma noite em abril, Ron Rivest ficou com uma enorme dor de cabeça e o algoritmo RSA veio a ele. Ele escreveu para Shamir e Adleman e enviou a eles na manhã seguinte. Foi um cifra prática de chave pública para confidencialidade e assinaturas digitais, com base na dificuldade de fatorar grandes números. Eles o enviaram a Martin Gardner em 4 de abril para publicação na Scientific American. Apareceu na Edição de setembro de 1977. O artigo da Scientific American incluiu uma oferta para enviar o relatório técnico completo a qualquer pessoa enviando um envelope selado e endereçado. Havia milhares de pedidos, de todo o mundo.

Em 1990 Xuejia Lai e James Massey na Suíça publicaram uma proposta para uma nova criptografia de bloco Standard, uma proposta de criptografia internacional de dados Algoritmo chamado de IDEA, para substituir o DES. O IDEA usa uma placa de 128 bits chaves e emprega operações convenientes para computadores de uso geral.

Em 1991 Phil Zimmermann lançou sua primeira versão do PGP (Pretty Good Privacy) em resposta à ameaça do FBI exigir acesso ao texto claro das comunicações dos cidadãos. O PGP ofereceu alta segurança ao cidadão em geral e, como tal, poderia ter sido visto como um concorrente para produtos comerciais como o Mailsafe da RSADSI.

No entanto, o PGP é especialmente notável porque foi lançado como freeware e tornou-se um padrão mundial enquanto seus concorrentes permanecem efetivamente desconhecido.

Em 1994 Professor Ron Rivest, autor do RC2 anterior ao Algoritmos RC4 incluídos no BSAFE da RSADSI biblioteca criptográfica, publicou um algoritmo proposto, RC5, na Internet. Esse algoritmo usa dados dependentes de rotação como sua operação não linear e é parametrizado de modo que o usuário pode variar o tamanho do bloco, o número de rodadas e comprimento da chave. Ainda é novo demais para ter sido analisado o suficiente para permitir que se saiba quais parâmetros usar para um resultado desejado, embora uma análise do RSA Labs, sugere que esse fornece força superior ao DES. Deve-se lembrar, no entanto, que esta é apenas uma primeira análise.

4.1.1 O Problema da troca de chaves entre correspondentes sem a intermediação de um portador

Existem quatro procedimentos específicos e essenciais para um sistema de criptografia de chave pública:

1. A decifração de uma mensagem criptografada fornece a mensagem original, especificamente

   $D(E(M)) = M$.

2. A reversão dos procedimentos ainda retorna M:

   $E(D(M)) = M$.

3. E e D são fáceis de calcular.

4. A publicidade de E não compromete o sigilo de D, o que significa que você não pode descobrir facilmente D de E.

Com um dado E, ainda não temos uma maneira eficiente de calcular D. Se $C = E(M)$ é o texto cifrado, então tentar descobrir D tentando satisfazer um M em $E(M) = C$ é irracionalmente difícil, o número de mensagens para testar seria impraticavelmente grande.

Um E que satisfaz (1), (3) e (4) é chamado de função unidirecional trap-door e também é uma trap-door permutação unidirecional. É uma armadilha (trap) porque, como o D é inverso, é fácil calcular se informações da porta (door) estão disponíveis, caso contrário, são difíceis. É unidirecional porque é fácil calcular em uma direção, mas difícil na outra. É uma permutação porque satisfaz (2), significando que todo texto cifrado é uma mensagem em potencial e toda mensagem é um texto cifrado de outra mensagem.

Agora, passamos a chaves específicas e imaginamos os usuários A e B (Alice e Bruno) em uma chave pública de dois usuários de sistema de criptografia, com suas chaves: EA, EB, DA, DB.

Suponha que Bruno quer enviar uma mensagem privada para Alice. Ele recuperará o EA do arquivo público, codificará M, obtendo $C = EA(M)$, após o que Alice o decodifica com seu próprio DA, o que somente ela pode fazer, devido à propriedade (4). Ela também poderia responder a Bruno, usando EB. Então, tudo o que é necessário é o consentimento do usuário para fazer parte do sistema de criptografia, colocando seus dados de criptografia em um arquivo público. Nenhuma comunicação prévia é necessário, privado ou não. Além disso, devido à propriedade (4), nenhum bisbilhoteiro pode deduzir D da escuta em E.

Para total garantia de que a mensagem se originou de um remetente e foi enviada apenas por ele e não por terceiros que possam ter usado a mesma chave de criptografia (a

do receptor), precisamos de um assinatura para vir com a mensagem. Isso tem implicações óbvias de importância nas aplicações da vida real. Bruno quer enviar uma mensagem privada para Alice. Para assinar o documento, criamos um pequeno truque inteligente, tudo assumindo que o algoritmo RSA seja rápido e confiável, principalmente devido à propriedade (3). Descriptografamos uma mensagem com a chave de Bruno, permitida pelas propriedades (1) e (2), que afirmam que toda mensagem é o texto cifrado de outra mensagem e que todo texto cifrado possa ser interpretado como uma mensagem. Formalmente, $DB(M) = S$. Em seguida, criptografamos S com a chave de criptografia de Alice.

$$EA(S) = EA(DB(M))$$

Dessa forma, podemos garantir apenas que ela possa descriptografar o documento. Quando ela faz, ela recebe a assinatura por $DA(EA(DB(M)) = S$. Ela agora sabe que a mensagem veio de Bruno, já que apenas sua chave de descriptografia poderia calcular a assinatura. A mensagem não precisa ser enviada separadamente, pois Alice pode deduzi-la da própria assinatura, usando a chave de criptografia disponível publicamente de Bruno, formalmente $EB(S) = EB(DB(M)) = M$.

Como S depende de M, e a transmissão criptografada que Bruno enviou depende de S, temos uma transmissão que depende da mensagem e da assinatura, para que ambos possam ser deduzidos dos documentos transmitidos. Isso garante brilhantemente que a mensagem não pode ser modificada (se for necessário ser apresentada a, digamos, uma autoridade), já que um M modificado na forma de $M0$ também teria que gerar uma assinatura $S0 = DB(M0)$, que é impossível, pois ela não conhece DB por propriedade (4). Portanto, Alice não apenas possui prova de que Bruno assinou a mensagem e realmente a enviou, mas também não pode modificar M nem forjar uma assinatura para nenhuma outra mensagem. Agora, digamos que um intruso tentou mentir e dizer que ele era do arquivo público? Isso não é um problema no RSA, uma vez que as assinaturas são usadas. Uma assinatura só precisa garantir que veio do arquivo público (PF) em si. Sempre que um usuário entra em uma rede, todos recebem uma cópia enviada com segurança das atualizações atualizadas mais recentemente (PF), que é armazenado em seu sistema, e eles nunca precisam procurar. Alguém tentando enviar uma mensagem e fingir estar em público não teria a assinatura apropriada e seria destacado como um intruso . Ele também nunca receberia o (PF), pois nunca se juntou a ele.

4.1.2 A Matemática do método da Criptografia RSA

Até o momento, esperamos facilitar a computação de E e D por meio de aritmética simples. Agora devemos representar a mensagem numericamente, para que possamos executar esses algoritmos aritméticos nela. Agora vamos representar M por um número inteiro entre 0 e $n-1$. Se a mensagem for muito longa, poupe-a e criptografe separadamente.

Sejam e, d e n sejam inteiros positivos, com (e, n) como a chave de criptografia, (d, n) a chave de descriptografia, $n = pq$. Agora, criptografamos a mensagem elevando-a a potência e ao módulo n para obter C, o texto cifrado. Nós então decodifiquemos C elevando-o a potência d ao módulo n para obter M novamente. Formalmente, obtemos esses algoritmos de criptografia e descriptografia para E e D:

$$C \equiv E(M) \equiv M^e \ (mod\ n)$$

$$M \equiv D(C) \equiv C^d \ (mod\ n) :$$

Agora queremos obter os e e d apropriados. Escolhemos d como um número inteiro grande e aleatório, que deve ser coprimo com $(p-1)(q-1)$, o que significa que a seguinte equação deve ser satisfeita:

$$(d, (p-1)(q-1)) = 1$$

A razão pela qual queremos d coprimo com $\phi(n)$ é peculiar e ficará claro no final desta seção.

Queremos calcular e para d, p e q, onde e é o inverso multiplicativo de d módulo $\phi(n)$. Que significa satisfazer $e \cdot d \equiv 1 \ (mod\ \phi(n))$. Para n, obtemos, pelas propriedades elementares que provamos no Teorema 2.75, referente a função totiente, que $\phi(n) = \phi(pq) = \phi(p) \cdot \phi(q) = (p-1)(q-1) = n - (p+q) + 1$. A partir desta equação, podemos substituir $\phi(n)$ na equação $e \cdot d \equiv 1 \ (mod\ (n))$ e obter $e \cdot d \equiv 1 \ (mod\ \phi(n))$, que é equivalente a $e \cdot d = k\phi(n) + 1$, para algum número inteiro k. Na aritmética modular, o inverso multiplicativo do número a módulo m existe se, e somente se, a e m são coprimos. De fato, como d e $\phi(n)$ são coprimos, d tem um inverso multiplicativo no anel de módulo inteiro $\phi(n)$.

Até agora, podemos garantir com segurança o seguinte:

$$D(E(M)) \equiv (E(M))^d \equiv (M^e)^d \ (mod\ n) = M^{e \cdot d} \ (mod\ n)$$

$$E(D(M)) \equiv (D(M))^e \equiv (M^d)^e \ (mod\ n) = M^{e \cdot d} \ (mod\ n)$$

Além disso, como $e \cdot d = k\phi(n) + 1$, podemos substituir as equações acima e obter $M^{ed} \equiv M^{k\phi(n)+1} \ (mod\ n)$.

Claramente, queremos mostrar que $M^{k\phi(n)+1} \equiv M \ (mod\ n)$.

Temos três casos a considerar:

Caso 1: M é coprimo com $n = pq$.
Nesse caso necessariamente temos $M \neq p$, $M \neq q$ e, consequentemente, $(M, n) = 1$.

Aqui, será necessário a identidade devida a Euler e Fermat que provamos no Teorema 2.78 (Teorema de Euler). Para qualquer par de números inteiros se são coprimos M e n, temos $M^{\phi(n)} \equiv 1 \ (mod\ n)$.

Como $0 \leq M < n$, assim segue, $M^{e \cdot d} = M^{k\phi(n)+1} \equiv (M^{\phi(n)})^k M \equiv 1^k M \ (mod\ n) = M$.

Acontece que isso funciona para todos os M e, de fato, vemos que $D(E(M)) = M$ e $E(D(M)) = M$ valem para todos os M, $0 \leq M < n$. Portanto, E e D são permutações inversas.

Caso 2: M múltiplo de p.

Nesse caso o Teorema de Euler não funciona. Vamos usar o Teorema Chinês dos restos. Chamemos $D(C(M)) = x$, queremos encontrar x tal que

$$\begin{cases} \mathrm{x} \equiv p^{k\phi(n)+1} \ (mod\ p) \\ \mathrm{x} \equiv p^{k\phi(n)+1} \ (mod\ q) \end{cases}$$

A primeira equação do sistema nos dá $p^{k\phi(n)+1} \equiv 0^{k\phi(n)+1} \equiv 0 \ (mod\ p)$.

Usando o Teorema de Euler obtemos:

$p^{k(p-1)(q-1)+1} \equiv (p^{p-1})^{k(q-1)} \cdot p \equiv 1^{k(q-1)} \cdot p \equiv 1 \cdot p \equiv p \ (mod\ q)$.

Assim,

$x \equiv 0 \ (mod\ p), \Rightarrow x = kp$.

Como, $x \equiv p \ (mod\ q)$, temos:

$kp \equiv p \ (mod\ q) \Rightarrow (k-1)p \equiv 0 \ (mod\ q)$.

Desse modo, $(p, q) = 1$ e $q \mid (k-1)p \Rightarrow \mathrm{q} \mid (k-1)$

Assim, $k - 1 = \alpha q \Rightarrow k = 1 + \alpha q$. Logo, $x = (1 + \alpha q)p = p + \alpha pq \Rightarrow x \equiv p \ (mod\ pq)$

Caso 3: M múltiplo de q.

Nesse caso procedemos de modo análogo ao item 2, e fica como exercício para o leitor.

4.1.3 Pré-codificação

A primeira coisa a fazer para utilizar o método RSA é converter a mensagem em uma sequência de números relacionados em uma tabela de letras com seus respectivos números.

Por exemplo, A=10, B=11, C=12, ..., Z=35

Então, por exemplo a palavra RSA pela tabela. Com a conversão da mensagem letra a letra, ficaria assim, 27.28.10

4.1.4 Codificação

Exemplo 4.2. Iremos utilizar números primos pequenos $p = 5$ e $q = 7$, assim, $n = p \cdot q = 5 \cdot 7 = 35$ e $\phi(n) = (p-1)(q-1)$, logo $\phi(n) = 24$. Para iniciar o processo vamos quebrar o código 272810 em blocos menores que 35, $B_1 = 27$, $B_2 = 28$ e $B_3 = 10$. Cada um dos blocos será codificado por $B_i \equiv A_i \ mod \ n$, em que o $(\lambda, 24) = 1$, escolhendo assim $\lambda = 7$. Codificaremos da seguinte maneira:

$B_i \equiv A_i \ (mod \ n)$

$27^7 \equiv A_1 \ (mod \ 35)$

$27^7 \equiv (-8)^7 \equiv [(-8)^2]^3 \cdot (-8) \equiv (-6)^3 \cdot (-8) \equiv 48 \equiv 13 \ (mod \ 35)$

$28^7 \equiv A_2 \ (mod \ 35)$

$28^7 \equiv (-7)^7 \equiv [(-7)^2]^3 \cdot (-7) \equiv (-49)^3 \cdot (-7) \equiv 21 \cdot (-3) \equiv 7 \ (mod \ 35)$

$10^7 \equiv A_3 \ (mod \ 35)$

$10^7 \equiv [(10)^2]^3 \cdot (10) \equiv (-5)^3 \cdot (10) \equiv (-125) \cdot 10 \equiv 15 \cdot (10) \equiv 10 \ (mod \ 35)$.

Desse modo os valores encriptados são: $A_1 = 13$, $A_2 = 7$ e $A_3 = 10$, logo a mensagem codificada é 13.7.10. A informação necessária para a decodificação consiste no par (n, d), lembrando que $\phi(n) = (p-1)(q-1)$ e o valor d é o valor inverso de n em $\phi(n)$, ou seja,

$\lambda d \equiv 1 \ (mod \ \phi(n))$. Neste caso, $\lambda = 7$, $\phi(n) = 24$, de onde $7d \equiv 1 \ (mod \ 24)$, logo $d = 7$. Assim, decodifica-se 13.7.10, da seguinte maneira:

$A_i^d \equiv B_i \ (\ mod \ n)$

$13^7 \equiv B_1 \ (\ mod \ 35)$

$13^7 \equiv [(13)^2]^3 \cdot 13 \equiv (-6)^2 \cdot (-6) \cdot 13 \equiv (-6) \cdot 13 \equiv -78 \equiv 27 \ (mod \ 35)$

$7^7 \equiv B_2 \ (\ mod \ 35)$

$7^7 \equiv [(7)^2]^3 \cdot 7 \equiv (14)^3 \cdot (7) \equiv 196 \cdot 14 \cdot 7 \equiv -147 \equiv 28 \ (mod \ 35)$

$10^7 \equiv B_3 \ (mod \ 35)$

$10^7 \equiv [(10)^2]^3 \cdot 10 \equiv (-5)^3 \cdot (10) \equiv (-125) \cdot 10 \equiv 15 \cdot 10 \equiv 10 \ (mod \ 35)$

Os valores são, $B_1 = 27$, $B_2 = 28$ e $B_3 = 10$.

4.1.5 Decodificação

A segurança utilizando-se o sistema RSA para decodificar mensagens, na prática, depende de uma chave com muitos dígitos, como também, se aumentarmos o número de caracteres da mensagem, o tempo gasto pelo sistema aumenta, se aumentarmos muito tais números o sistema torna-se totalmente inviável de implementação. Por isso, urge a

necessidade de se usar o Teorema Chinês dos Restos como algoritmo para executar essa tarefa.

A mensagem de texto pode ser recuperada quando a chave de decodificação d, um inverso de λ módulo $(p-1)(q-1)$, é conhecida. O inverso existe, quando o $(\lambda,(p-1)(q-1))=1$, note que, se $d\lambda \equiv 1\ (mod\ (p-1)(q-1))$, há um número inteiro k tal que $d\lambda = 1+k(p-1)(q-1)$. Portanto, $c^d=(M^\lambda)^d=M^{d\lambda}=M^{1+k(p-1)(q-1)}(mod\ n)$, pelo Pequeno Teorema de Fermat supondo $(M,p)=(M,q)=1$ temos, $M^{p-1}\equiv 1\ (mod\ p)$ e $M^{q-1}\equiv 1\ (mod\ q)$.

Consequentemente $c^d \equiv M\cdot(M^{p-1})^{k(q-1)} \equiv M\cdot 1 \equiv M\ (mod\, p)$ e $c^d \equiv M(M^{q-1})^{k(p-1)} \equiv M\cdot 1 \equiv M\ (mod\ q)$, como o $(p,q)=1$, temos que pelo Teorema Chinês dos Restos $c^d \equiv M\ (mod\ pq)$

4.1.6 Criptografando com o Teorema Chinês dos Restos

Os Teoremas, Chinês dos Restos, de Wilson, O Pequeno Teorema de Fermat e O Teorema de Euler, nos permitirá criptografar com números maiores.

Exemplo 4.3. Neste problema vamos codificar e decodificar uma mensagem com e sem o uso do Teorema Chinês dos Restos, para que o leitor possa observar a eficiência do teorema.

Dados os primos p e q, sendo $p=11$ e $q=17$, pode-se obter $n=pq=11\cdot 17=187$ e $\phi(n)=(p-1)(q-1)=(11-1)(17-1)=160$. Dada uma tabela, de tal maneira que, $A=21$, $B=22$, $C=23$, ..., $Z=48$, vamos criptografar a mensagem "CHAVE". Primeiro é preciso transformar as letras em números de acordo com a tabela, assim tem-se, $C=23$, $H=28$, $A=21$, $V=44$ e $E=25$. A mensagem deve ser separada em blocos b de modo que cada bloco tenha números menores que 187. Como os primos escolhidos são pequenos, os blocos também devem ser, assim a sequência 2328214425 será separada em seis blocos, 2.32.82.14.42.5

O valor de e deve ser escolhido de modo que $(e,\phi(n))=1$, deste modo será escolhido o número 3 e d deverá seguir a congruência $ed\equiv 1\ (mod\ \phi(n))$, assim:

$3d\equiv 1\ (mod\ 160)$.

Deste modo, $160k=3d-1 \Leftrightarrow 1=3d-160k$, resolvendo pelo método do algoritmo de euclides:

$160=3\cdot 53+1 \Leftrightarrow 1=160-3\cdot 53$.

Como o valor de d não pode ser negativo e as soluções desta equação são: $d=-53+160t$ e $k=-1-3t$:

$-53+160t>0 \Leftrightarrow t>\frac{53}{160}$.

Substituindo $t = 1$ tem-se o menor valor possível para d que é 107. Deste modo já tem-se a chave para Criptografar $\langle e, n\rangle = \langle 3, 187\rangle$ e para descriptografar $\langle d, n\rangle = \langle 107, 187\rangle$.

Para codificar a mensagem usaremos a chave $\langle 3, 187\rangle$ e a congruência $b^e \equiv C(b)\ (mod\ n)$, assim teremos:

$2^3 \equiv C(b_1)\ (mod\ 187) \Leftrightarrow C(b_1) = 8$

$32^3 \equiv C(b_2)\ (mod\ 187) \Leftrightarrow C(b_2) = 43$

$82^3 \equiv C(b_3)\ (mod\ 187) \Leftrightarrow C(b_3) = 92$

$14^3 \equiv C(b_4)\ (mod\ 187) \Leftrightarrow C(b_4) = 126$

$42^3 \equiv C(b_5)\ (mod\ 187) \Leftrightarrow C(b_5) = 36$

$5^3 \equiv C(b_6)\ (mod\ 187) \Leftrightarrow C(b_6) = 125$

O bloco codificado será: 8.43.92.126.36.125.

Para decodificar é preciso da chave $\langle 107, 187\rangle$ e da congruência $C(b)^d \equiv D(C(b))\ (mod\, n)$. Como 107 é um número primo e usá-lo como expoente faz com que não seja possível usar uma calculadora comum serão usadas algumas propriedades de congruências citadas ao longo do trabalho.

Para decodificar o primeiro bloco, 8 deve-se usar:

$8^{107} \equiv D(C(b))\ (mod\ 187)$

Assim como $107 = 3 \cdot 7 \cdot 5 + 2$ temos:

$8^3 \equiv 512 \equiv 138\ (mod\ 187)$.

$(8^3)^5 \equiv 138^5\ (mod\ 187)$ e $138^5 = 138^2 \cdot 138^2 \cdot 138$

então: $8^{15} \equiv 138^2 \cdot 138^2 \cdot 138\ (mod\ 187) \Leftrightarrow$

$8^{15} \equiv 19044 \cdot 19044 \cdot 138\ (mod\ 187) \Leftrightarrow 8^{15} \equiv 157 \cdot 157 \cdot 138\ (mod\ 187)$ pois $19044 \equiv 157\ (mod\ 187)$.

Portanto $3401562 \equiv 32\ (mod\ 187) \Leftrightarrow$

$8^{15} \equiv 32\ (mod\ 187)$.

Ainda, $(8^{15})^7 \equiv 32^7 \equiv 32^3 \cdot 32^3 \cdot 32\ (mod\ 187) \Leftrightarrow$

$8^{105} \equiv 32768 \cdot 32768 \cdot 32 \equiv 43 \cdot 43 \cdot 32\ (mod\ 187) \Leftrightarrow$

$8^{105} \equiv 59168 \equiv 75\ (mod\ 187). \Leftrightarrow$

$8^{105} \cdot 8^2 \equiv 76 \cdot 8^2 \equiv 4864 \equiv 2\ (mod\ 187)$.

$\Leftrightarrow 8^{107} \equiv 2\ (mod\ 187)$.

Contudo gasta-se muito tempo nesse método, e deve-se fazer muitos cálculos, um

método mais eficiente é utilizar o Teorema Chinês dos Restos.

Assim como sabe-se que $n = 187 = 11 \cdot 17$ tem-se que, pelo Pequeno Teorema de Fermat, $p \mid a^{p-1} - 1$. Desta forma

$8^{10} \equiv 1(mod\ 11)$ e $8^{16} \equiv 1\ (mod\ 17)$.

Assim,

$(8^{10})^{10} \equiv 1^{10}\ (mod\ 11)$

$8^{100} \cdot 8^7 \equiv 1 \cdot 8^7\ (mod\ 11) \equiv 2\ (mod\ 11)$

$8^{107} \equiv 2\ (mod\ 11)$

$(8^{16})^6 \equiv 1^6\ (mod\ 17)$

$8^{96} \cdot 8^5 \equiv 1 \cdot 8^5\ (mod\ 17)$

$8^{101} \equiv 9\ (mod\ 17)$

$8^{101} \cdot 8^5 \equiv 9 \cdot 8^5 \equiv 9 \cdot 9 \equiv 13\ (mod\ 17)$

$8^{106} \cdot 8 \equiv 13 \cdot 8 \equiv 2\ (mod\ 17)$

$8^{107} \equiv 13 \cdot 8 \equiv 2\ (mod\ 17)$

Substituindo 8^{107} por x tem-se um sistema de congruências

$x \equiv 2\ (mod\ 11)$

$x \equiv 2\ (mod\ 17)$.

Pelo Teorema Chinês dos Restos:

$M = 11 \cdot 17 = 187$

$M_1 = \frac{187}{11} = 17$

$M_2 = \frac{187}{17} = 11$

Assim,

$17y_1 \equiv 1\ (mod\ 11)$

$\Leftrightarrow \mathrm{y}_1 = 2$

e

$11y_2 \equiv 1\ (mod\ 17)$

$\Leftrightarrow \mathrm{y}_2 = 14$

$X = 17 \cdot 2 \cdot 2 + 11 \cdot 14 \cdot 2 + 187t$

$X = 376 + 187t$

O menor valor de X no conjunto dos naturais para a equação é com $t = 2$, desta

forma $X = 2$.

Obtém-se o primeiro bloco decodificado. Para obter os próximos blocos decodificados o processo é o mesmo. Assim, deixamos como exercício para o leitor.

5 Proposta pedagógica

5.0.1 Conteúdo

Desenvolvimento de Congruências, Equações Diofantinas Lineares, Congruências Lineares, Sistemas de Congruências, O Teorema de Wilson, O Pequeno Teorema de Fermat e a sua generalização, O Teorema de Euler, para embasar o desdobramento do Teorema Chinês dos Restos para aplicações, principalmente, em alguns casos da Criptografia RSA.

5.0.2 Objetivos

1. Fornecer uma linha estratégica ao professor, afim de que ele possa aplicar alguns conceitos da Aritmética Modular nas demonstrações e resoluções de questões olímpicas e desse modo plantar esse conteúdo no ensino médio;

2. Assistir o professor a traçar uma sequência dos tópicos e problemas, onde ele possa avançar gradualmente no ensino de Congruências, para dar suporte a aplicações do Teorema Chinês dos Restos.

3. Alcançar um maior desenvolvimento no processo de raciocínio, a partir de uma ou mais afirmações, para chegar a uma certa conclusão lógica do raciocínio lógico-dedutivo do estudante.

5.0.3 Duração e Público Alvo

As atividades propostas nesse trabalho terão uma duração total de 15 (quinze) horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma, que devem, se possível, ser ministradas em semanas diferentes e têm como público alvo todos os estudantes que se pretende envolver em futuras Olimpíadas e professores de Matemática.

5.0.4 Metodologia

Recomendamos como metodologia de ensino, a metodologia de resolução de problemas, pois, reconhecemos que essa é uma das formas mais eficazes e acessíveis de proporcionar aos estudantes que aprendam a aprender, sendo esse desenvolvimento um dos principais pormenores que governam as transições educacionais. Em diferentes etapas da educação ver-se a necessidade de que os alunos obtenham habilidades e competências que provenham a apreensão de novos conhecimentos por si mesmos e não prontos e acabados. É necessário estimular os estudantes a tornarem-se pessoas capazes de enfrentar diversas situações, envolvidos em contextos diversificados, fazendo com que busquem aprender

novos conceitos, pois, assim estarão preparados para adaptar-se às diversas mudanças. A resolução de problemas baseia-se na apresentação de situações abertas e atraentes que exijam dos discentes postura ativa ou um esforço para buscar suas próprias respostas, pressupondo, promover nestes o domínio de procedimentos, assim como a utilização dos conhecimentos disponíveis, para dar resposta a situações variáveis e diferentes.

5.0.5 Recursos Metodológicos

Para a aplicação e desenvolvimento da sequência didática o professor vai utilizar: o quadro branco; marcador para quadro branco e um aplicativo para apresentação do conteúdo, por exemplo, Prezi ou PowerPoint.

5.0.6 A sequência didática

Com o intuito de generalizar e aprofundar os resultados obtidos para os estudantes do ensino médio e, principalmente, aqueles que farão olimpíadas de Matemática, neste capítulo sugerimos uma forma de como lecionar conteúdos da Aritmética Modular, na intenção particular de facilitar seu entendimento, tendo ciência de que o mais importante é a de disseminar esses conteúdos ora esquecidos nessa modalidade de ensino. Utilizaremos uma abordagem pedagógica baseada na resolução de problemas motivadores, por isso, é necessária a exposição clara do problema, o assentamento das metas esperadas para a solução, a condução do tempo esperado para a resolução, detecção e a importância do trabalho em relação aos objetivos. Para isso, seguiremos algumas etapas.

5.0.7 Congruências

Primeira parte

Etapa 1 - Investigação

Para iniciar esta seção sugerimos que seja proposto, aos estudantes, o problema do Exemplo 2.7., criado por Euler e adaptado para este trabalho. Trata-se de uma transação comercial que recai em uma Equação Diofantina Linear, mas, que os discentes devem tentar resolvê-lo, apenas, usando seus conhecimentos prévios.

Etapa 2 - Apresentação da teoria

Na sequência, deve-se mencionar como aconteceu o desenvolvimento das equações Diofantinas, para em seguida definir formalmente o que é uma Equação Diofantina Linear, quando admite solução e em seguida executar algumas demonstrações. É importante deixar claro desde o início aonde se quer chegar, pois, essa abordagem servirá como base para entender o Teorema Chinês dos Restos e suas aplicações, como por exemplo na Criptografia.

Etapa 3 - Resolução de problemas

Agora faz-se necessário resolver alguns problemas, primeiro deve-se resolver os problemas dos Exemplos 2.4. e 2.6. e na sequência o problema do Exemplo 2.7., com os conceitos apreendidos na Etapa 2.

Etapa 4 - Avaliação

Nessa etapa, elabore um exercício avaliativo composto com três problemas, semelhantes aos que você resolveu nas etapas anteriores. Essa avaliação deverá ser aplicada individualmente, sem que haja qualquer tipo de consulta.

Exercício avaliativo: A função do exercício avaliativo é mostrar ao professor aquilo que de fato o estudante conseguiu assimilar dentro do que se esperava. É nele que o professor visualizará o modo como os estudantes estão utilizando os métodos aplicados nas demonstrações dos resultados anteriores.

Para o assunto Equações Diofantinas Lineares, deverão ser dedicadas duas horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

Segunda parte

Na segunda parte, Congruências devem ser mostradas como uma das noções que trouxe mais frutos da aritmética, como uma realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

Etapa 1 - Investigação

Para iniciar esta secção sugerimos que seja proposto, aos estudantes, a resolução do problema do Exemplo 2.11.. Trata-se de um problema de calendários que é interpretado como aplicação da noção de congruência, que os discentes devem tentar resolvê-lo, apenas, usando seus conhecimentos prévios.

Etapa 2 - Apresentação da teoria

Deve-se estabelecer na resolução do problema do Exemplo 2.11. uma fórmula para descobrir qual é o dia da semana correspondente a uma data passada ou futura. Em seguida é primordial atenção e demonstrações das definições e propriedades básicas, que aqui englobam também: Relações de Equivalência e Base de numeração, que serão essenciais para resolução de problemas olímpicos.

Etapa 3 - Resolução de problemas

Ao longo do capítulo 2 existe uma miscelânea de problemas que podem ser resolvidos em ordem crescente de dificuldades a serem escolhidos e propostos pelo professor.

Etapa 4 - Avaliação

Nessa etapa, elabore um exercício avaliativo composto com três problemas, se-

melhantes aos que você resolveu na etapa anterior. Essa avaliação deverá ser aplicada individualmente, sem que haja qualquer tipo de consulta.

Para o assunto Congruências, deverão ser dedicadas três horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

Terceira parte

Etapa 1 - Apresentação da teoria

Na terceira parte é inserida a definição das Congruências Lineares. Dados a e b inteiros, com $a \neq 0$, uma congruência da forma $ax \equiv b \ (mod \ \text{m})$ é chamada congruência linear, em que x é uma incógnita.

O objetivo é determinar todas as soluções inteiras de $ax \equiv b \ (mod \ \text{m})$, isto é, todos os inteiros x_0 para os quais $ax_0 \equiv b \ (mod \ \text{m})$. Por exemplo, 3 é uma solução de $4x \equiv 7 \ (mod \ 5)$, pois $4 \cdot 3 = 12 \equiv 7 \ (mod \ 5)$. Por outro lado, a congruência linear $4x \equiv 3 \ (mod \ 2)$ não tem solução inteira, pois se $x_0 \in \mathbb{Z}$ e $4x_0 \equiv 3 \ (mod \ 2)$, então $4x_0 - 3 = 2k$, com $k \in \mathbb{Z}$, de maneira que 2 divide 3, o que não é possível.

Inicialmente, deve-se dar um critério para determinar se tais congruências, da forma como definidas acima, admitem solução.

Etapa 2 - Resolução de problemas

Nessa etapa deve-se dar enfase a demonstrações dos Teoremas e Proposições, culminando com a resolução do Exemplo 2.51., preparando a inserção nos Sistemas de Congruências Lineares, que em seguida são definidos.

Etapa 3 - Avaliação

Nessa etapa, elabore um exercício avaliativo composto com três problemas, semelhantes aos que você resolveu na etapa anterior.

Essa avaliação deverá ser aplicada em duplas.

Para o assunto Congruências Lineares, deverão ser dedicadas duas horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

5.0.8 O Teorema de Wilson, O Pequeno Teorema de Fermat e O Teorema de Euler

Quarta parte

Etapa 1 - Apresentação da teoria

Na quarta parte, deve-se mostrar esses três Teoremas: O Teorema de Wilson, O Pequeno Teorema de Fermat e sua generalização, O Teorema de Euler, como ferramentas poderosas na resolução de problemas olímpicos, como também será de suma importância

nessa etapa frisar suas utilidades na resolução de Problemas que utilizam o Teorema Chinês dos Restos e na Criptografia.

Etapa 2 - Resolução de problemas

Devem ser resolvidos os Exemplos 2.56, 2.57, 2.61, 2.62, 2.70, 2.71 e a escolha do professor vários problema sugeridos nas subseções 2.4.1, 2.4.2, e 2.4.3.

Etapa 3 - Avaliação

Nessa etapa, elabore um exercício avaliativo composto com três problemas, semelhantes aos que você resolveu na etapa anterior.

Essa avaliação deverá ser aplicada em duplas.

Para os assuntos O Teorema de Wilson, O Pequeno Teorema de Fermat e O Teorema de Euler, deverão ser dedicadas duas horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

5.0.9 O Teorema Chinês dos Restos

Quinta parte

Etapa 1 - Investigação

O Teorema Chinês dos Restos deverá, inicialmente, ser apresentado para resolver problemas do tipo:

Qual é o número que deixa restos 2, 3 e 2 quando dividido, respectivamente, por 3, 5 e 7? Contextualizado no início do terceiro capítulo, que os discentes devem tentar resolvê-lo, apenas, usando seus conhecimentos prévios.

Etapa 2 - Apresentação da teoria

Traduzindo em linguagem matemática, o problema contextualizado e sugerido na introdução deverá ser mostrado como uma equivalência a procurar as soluções do seguinte sistema de congruências:

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

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

$X \equiv 2 \ (mod \ 7)$

De modo geral, estudaremos sistemas de congruências da forma:

$a_i X \equiv b_i \ mod \ n_i, \ i = 1, \cdots, r.$

Aqui faz-se necessário a demonstração do Teorema Chinês dos Restos, que deve ser construída a partir de uma primeira abordagem, menos formal, para daí, ser executada tecnicamente a demonstração formal, como sugerida na seção 3.1.

Etapa 3 - Resolução de problemas

Existem, ao longo do capítulo 3, uma miscelânia de problemas a serem resolvidos para estruturar a construção desse conhecimento que será utilizado na resolução de questões olímpicas, como também, servirá como ferramenta no capítulo 4, para decodificação de alguns tipos de mensagens.

Etapa 4 - Avaliação

Nessa etapa, elabore um exercício avaliativo composto com três problemas, semelhantes aos que você resolveu na etapa anterior. Essa avaliação deverá ser aplicada individualmente, sem que haja qualquer tipo de consulta.

Para o assunto Teorema Chinês dos Restos, deverão ser dedicadas três horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

5.0.10 Noções de Criptografia

Sexta parte

Etapa 1 - Investigação

Para introduzir uma noção do problema da troca de chaves, deverá ser proposto aos estudantes o problema do Exemplo 4.1., em que duas pessoas, Bruno e Alice, desejam trocar uma informação secreta, sem a intermediação de um portador, em um ambiente inseguro.

Etapa 2 - Apresentação da teoria

Deve-se abordar nessa secção, como o desenvolvimento da Teoria da Informação mudou a perspectiva da Teoria dos Números, considerada a área mais pura e abstrata da Matemática e como esse panorama muda radicalmente a partir do desenvolvimento da Criptografia, motivada pela evolução e popularização dos computadores e a facilidade de conexão entre as pessoas.

Na sequência deve-se discutir o problema da troca de chaves entre correspondentes sem a intermediação de um portador, demonstrando a Matemática do método mencionado no Exemplo 4.1.. Em seguida demonstra-se a matemática do método da Criptografia RSA, a pré-codificação, codificação e a decodificação. Sugerimos a resolução do Exemplo 4.2. e o problema sugerido na subseção 4.1.6.

Para essa sexta parte deverão ser dedicadas três horas aulas de aproximadamente 50 (Cinquenta) minutos cada uma.

6 Considerações Finais

Neste trabalho, apresentamos um método para determinar soluções de uma Equação Diofantina, demonstramos, o Teorema de Wilson, o Pequeno Teorema de Fermat e sua generalização; o Teorema de Euler, como também, alguns teoremas e proposições importantes sobre Congruências e Sistemas de Congruências. Nossa principal intenção é embasar o Teorema Chinês dos Restos para aplicarmos em Criptografia RSA, e com a teoria desenvolvida solucionar diversos problemas retirados das Olimpíadas de Matemática.

Dessa forma, a partir das análises realizadas podemos perceber que a Aritmética envolve um raciocínio muito sofisticado sendo este usado a muito tempo pelos chineses e empregado como apoio teórico em conteúdos avançados da Matemática, e ainda assim, pode ser trabalhado facilmente, com alunos do ensino básico, como foi abordado ao logo do texto.

Dissertar sobre a Aritmética Modular, justifica-se por se tratar de uma aplicação de conteúdos matemáticos para a sociedade, que atrai a atenção especial para as utilizações no dia a dia, um exemplo disso encontramos na Criptografia RSA, que é responsável em promover maior segurança na troca de informações bancárias. Diante disso, o desenvolvimento de estudos neste trabalho serve como subsídio para fomentar o conhecimento e a investigação científica, além de abrir caminhos para incursões mais detalhadas sobre Aritmética no futuro.

Sendo assim, aplicamos o Teorema Chinês dos Restos em diversas situações do cotidiano, verificamos a análise da ocorrência deste teorema em problemas de Olimpíadas de Matemática, aprofundamos sua aplicação na resolução de equações, sistemas e na Criptografia RSA.

Enfim, salientamos que os resultados esperados a partir do desenvolvimento deste trabalho irão possibilitar aos estudantes e professores a imersão nos estudos da Aritmética, incentivar o interesse por Olimpíadas de Matemática, bem como de fornecer uma discussão lúcida sobre a aplicação matemática no cotidiano das pessoas, tendo como base, ou ponto de partida, suas aplicações.

Referências

1 COUTINHO, Severino Collier *Números Inteiros e Criptografia RSA*. Rio de Janeiro; Série Computação e matemática, IMPA, 2003.

2 DING, C., Pei, D., Salomaa, A: *Chinese Remainder Theorem*. Application in computing, Coding, Cryptography. Word Scientific, Singapore (1996).

3 LEMOS, MANOEL *Criptografia, Números Primos e Algoritmos*. IMPA, 2001.

4 PRAZERES, SIDMAR BEZERRA DOS *O teorema Chinês dos Restos e a partilha de senhas*. T.C.C., Profmat, 2014.

5 FEITOSA, SAMUEL *Polo Olímpico de treinamento, teoria dos números* , aula 1, 2019.