Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Congruência e Aplicações. [†]

por

José Marcondes Gomes de Medeiros

sob orientação do

Prof. Dr. Carlos Bocker Neto

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - PROFMAT - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Fevereiro/2015

João Pessoa - PB

[†] Este trabalho contou com apoio financeiro do CNPq.

Congruência e Aplicações.

por

José Marcondes Gomes de Medeiros

Trabalho de Conclusão de Curso apresentado ao Corpo Docente do Programa de Pós-Graduação em Matemática - PROFMAT - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

área de Concentração: Aritmética.

Aprovada por:

Carlos Bocker Neto

Prof. Dr. Carlos Bocker Neto - UFPB(Orientador)

Gilmar Otávio Correia

Prof. Me. Gilmar Otávio Correia - UFPB(Coorientador)

Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dr. José Vicente Moreira - UNIPÊ

Fevereiro/2015

Agradecimentos

Agradeço em primeiro lugar a meu bom DEUS que me deu força e ânimo nos momentos de maiores dificuldades encontradas no curso em minha vida.

Aos meus pais, Antônio Gomes de Medeiros e Maria Idalina Gomes de Medeiros por terem me educado e me dado tanto carinho e amor, até o último dia de suas vidas aqui entre nós.

A minha esposa Rosicleide Bezerra das Neves Medeiros por tanta paciência, companheirismo e compreensão em todas as horas.

A todos os meus irmãos e familiares que direta ou indiretamente contribuíram para que esse sonho fosse realizado.

A todos os meus colegas de turma que durante todo o tempo de curso estiveram juntos comigo nessa caminhada e, em especial, os participantes de meu grupo de estudos, Antonio, Demilson, Edjane, Eli Paulo, João Paulo, Josildo e Renato Beserra.

Um agradecimento especial em dobro ao meu grande colega de turma e amigo Antonio Costa que nunca mediu esforços ao me socorrer nas horas em que encontrei dificuldades na confecção desse trabalho.

Ao meu orientador Prof. Dr. Carlos Bocker pelo auxílio e paciência nesses últimos meses.

A todos os Professores do Curso PROFMAT da Universidade Federal da Paraíba em João Pessoa pela contribuição para meu crescimento profissional e pessoal.

Ao meu mais lindo e perfeito presente que Deus me deu, meu filho Antônio Gomes de Medeiros Neto, por trazer ainda mais alegria para minha vida.

À CAPES, Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, pelo incentivo financeiro dado através da concessão da bolsa de estudos.

Dedicatória

Aos meus pais Antônio Gomes de Medeiros e Maria Idalina Gomes de Medeiros (in memorian)

Resumo

Neste trabalho faremos um breve estudo a respeito de teoria aritmética dos números, em particular, congruências modulares e testes de primalidade de inteiros. Descreveremos cuidadosamente o método de cifragem e decifragem da criptografia RSA e discutiremos algumas nuances da RSA. Para isso, apresentamos alguns resultados devido a Gauss, o príncipe dos matemáticos, no qual várias de suas ideias são de grande importância e serviram de base para o desenvolvimento da teoria dos números, até os dias atuais.

Palavras-chave: Teoria dos números, Gauss, Congruência modular, Criptografia.

Abstract

In this paper we make a brief study about arithmetic number theory, in particular, modular congruence and whole primality tests. O describe carefully the ciphering and deciphering method of RSA encryption and discuss some nuances of RSA. Therefore, this study a little about Gauss, the prince of mathematicians, in which many of his ideas are very important and the basis for the development of number theory, to the present day.

Keywords: Number theory, Gauss, Modular congruence, Encryption.

Sumário

Introdução

Em matemática, aritmética modular (chamada também de aritmética do relógio) é um sistema de aritmética para inteiros, onde os números "voltam pra trás"quando atingem um certo valor, o módulo.

O matemático suiço *Euler* foi o pioneiro na abordagem de congruência por volta de 1750, quando ele explicitamente introduziu a ideia de congruência módulo um número natural $\mathbb{N}$.

A aritmética modular foi desenvolvida posteriormente por Carl Friedrich Gauss em seu livro “Disquisitiones Arithmeticae”, publicado em 1801.

Neste trabalho realizamos uma análise aprofundada sobre teoria aritmética dos números, em especial as congruências modulares e testes de primalidade de inteiros. Durante o desenvolvimento estudamos o método de cifragem e decifragem da criptografia RSA, analisamos problemas que envolvam congruência tais como as Equações Diofantinas Lineares, o Teorema Chinês dos Restos, entre outros tópicos. Demonstramos e discutimos alguns importantes teoremas como o Pequeno Teorema de Fermat, de Euler e o de Wilson e analisamos algumas especificidades da RSA. Para isso, estudaremos um pouco sobre Gauss, o príncipe dos matemáticos, no qual várias de suas ideias são de grande importância e servem de base para o desenvolvimento da teoria dos números.

Capítulo 1

Congruência

1.1 Aspectos Históricos

Grande parte dos resultados deste capítulo foi introduzida por Gauss (1777 – 1855) em um trabalho publicado em 1801 "*Disquisitiones Arithimeticae*" quando tinha apenas 24 anos. Várias ideias de grande importância, que serviram de base para o desenvolvimento da teoria de números, aparecem neste trabalho. Até mesmo a notação, lá introduzida, é a que utilizamos hoje.

1.1.1 Gauss - O príncipe dos matemáticos

Johann Friedrich carl Benz Gauss (1777 – 1855), nasceu a: 30 de Abril de 1777, em Brunswich, na Alemanha Morreu a: 23 de Fevereiro de 1855, em Göttingen, na Alemanha. Cientista, Gauss nasceu em Brunswich e morreu em Göttingen, na Alemanha. Estudou na Universidade de Göttingen de 1795 à 1798, onde passou a ensinar Matemática a partir de 1807, sendo ao mesmo tempo diretor do Observatório Astronômico pertencente àquela Instituição. Manteve ambos os cargos até à sua morte. Gauss dedicou-se à: matemática, astronomia, geodesia, física-matemática e geometria. O seu nome consta de numerosos resultados obtidos nos domínios da astronomia, da física e da matemática. Nestas áreas, Gauss demonstrou a denominada lei fundamental da álgebra, segundo a qual uma equação do segundo grau tem duas soluções, uma do terceiro tem três e assim sucessivamente. Para tratar medidas astronômicas desenvolveu o método dos mínimos quadrados. Com este sistema conseguiu calcular em pouco tempo, e com grande exatidão, as órbitas dos corpos

celestes, a partir de poucas observações. Obteve ainda as chamadas coordenadas de Gauss - utilizam-se especialmente para a determinação de um ponto sobre a superfície da Terra (latitude e longitude); a curva de Gauss - curva da distribuição normal mediante a qual é possível representar-se medidas prováveis da Estatística; o método de eliminação de Gauss - utiliza-se na análise numérica para resolver sistemas de equações lineares; e o plano de Gauss - plano para representação dos números complexos.

Vida

Filho de um trabalhador do campo, foi criado no seio de uma família pobre, austera e sem educação científica. Dadas as precárias condições econômicas da sua família, recebeu o precioso apoio do Duque de Brunswich que reconheceu nele uma criança-prodígio. Este apoio começou quando Gauss tinha 14 anos e permitiu-lhe dedicar-se exclusivamente aos estudos, durante 16 anos.

Ainda antes do seu vigésimo quinto aniversário, já Gauss era famoso pelo seu trabalho em Matemática e Astronomia. Aos 30 anos foi nomeado Diretor do Observatório de Göttingen, cidade da qual raramente saiu, exceto por questões científicas. Aí, trabalhou durante 48 anos (de 1807 a 1855) até à sua morte, com quase 78 anos.

A vida pessoal de Gauss foi trágica e complicada. Um pai insensível, a morte prematura da sua primeira mulher, a pouca saúde da sua segunda mulher e uma terrível relação com os seus filhos negou-lhe, até tarde, a possibilidade de vida estável no seio de uma famíla equilibrada.

Mesmo com todos estes problemas, Gauss manteve uma rica e espantosa atividade científica. A sua precoce paixão pelos números e cálculos estendeu-se à Teoria dos Números, à Álgebra, à Análise, à Geometria, à Teoria das Probabilidades e à Teoria dos Erros. Ao mesmo tempo, levou em frente uma intensiva pesquisa empírica e teórica em muitos outros ramos, incluindo Astronomia Observacional, Mecânica Celeste, levantamento topográfico, Geodesia, Geomagnetismo, Eletromagnetismo e Mecanismos Ópticos.

Gauss não encontrou nenhum colaborador entre os seus colegas matemáticos tendo trabalhado sempre sozinho. Mas, se é verdade que o seu isolamento relativo, a sua compreensão das matemáticas puras e aplicadas, a sua preocupação com a

astronomia e o uso frequente que faz do latim têm a marca do século XVIII, é inegável que, nos seus trabalhos, se reflete o espírito de um novo período. Se, tal como os seus contemporâneos Kant, Goethe, Beethoven e Hegel, se manteve à margem das grandes lutas políticas da sua época, a verdade é que, no seu próprio campo, Gauss expressou as novas ideias da sua época de uma forma poderosíssima.

As suas publicações, a sua abundante correspondência, as suas notas, e os seus manuscritos mostram que ele possuía uma das maiores virtuosidades científicas de todos os tempos.

A infância

Começaram cedo os indícios que faziam adivinhar o talento incrível que Gauss demonstraria ao longo de sua vida. Isso é patente em alguns dos excertos que relatam a sua infância. É o caso do seguinte episódio: durante os verões, Gebhard Gauss, que era contramestre numa firma de alvenaria, pagava o salário semanal aos seus trabalhadores. Uma vez, quando Gebhard estava prestes a pagar o salário a um dos trabalhadores, Carl Friedrich, na altura com apenas três anos, levantou-se e disse: "Papa, cometeste um erro!", indicando em seguida a quantia certa. Gauss tinha seguido os cálculos sem sequer poder ver os registros escritos (dado que a sua altura ainda não era suficiente para alcançar a mesa), e para surpresa dos presentes, uma confirmação provou que Carl Friedrich estava certo.

É portanto natural que Gauss tivesse o costume de dizer que tinha aprendido a contar e a calcular antes de ter aprendido a falar.

Outra das suas proezas foi aprender a ler sozinho. Como o conseguiu? Segundo reza a história apenas perguntando aos adultos como se pronunciavam as letras do alfabeto. E isto foi só o início do que viria a ser a sua obra.

A educação

Carl Friedrich tinha sete anos quando entrou para a Escola Primária St. Catherine, sendo inicialmente apenas mais um no meio de tantos alunos. O seu professor era J.G. Büttner, um professor tradicional que, em geral, considerava os seus alunos como incapazes e pouco dotados. No entanto, cedo descobriu que Gauss era diferente. Como o descobriu? Quando o seguinte episódio aconteceu:

Gauss tinha cerca de dez anos e frequentava a classe de aritmética quando Büttner propôs o seguinte difícil problema:

"Escrevam todos os números de 1 à 100 e depois vejam quanto dá a sua soma."

Era hábito, quando a classe tinha uma tarefa deste tipo, que se fizesse o seguinte: o primeiro aluno a acabar iria até à secretária do professor com a sua ardósia e colocá-la-ia em cima da mesa. O seguinte a acabar colocaria a sua ardósia em cima da do colega e assim sucessivamente, até a pilha de ardósias estar completa. O problema em questão não era difícil para alguém que tivesse alguma familiaridade com as progressões aritméticas. Como os rapazes ainda eram principiantes, Büttner certamente pensou que lhe seria possível fazer um intervalo por um bom bocado. Mas estava enganado... Em alguns segundos, Gauss colocou a sua ardósia na mesa, e ao mesmo tempo disse no seu dialecto Braunschweig: "Ligget se"(Aqui jaz). Enquanto os outros alunos continuavam a somar, Gauss sentou-se calmo e sereno, impassível aos olhares desdenhosos e suspeitos de Büttner.

No final da aula os resultados foram examinados. A grande maioria dos alunos tinha apresentado resultados errados pelo que foram severamente corrigidos com uma cana-da-índia. Na ardósia de Gauss, que se encontrava no fim, estava apenas um número: 5050 (É desnecessário dizer que o resultado está correto). Como seria de esperar, Gauss teve que explicar ao espantado professor Büttner como é que tinha obtido aquele resultado:

"Então, $1 + 100 = 101, 2 + 99 = 101, 3 + 98 = 101$, e por ai em diante, até finalmente $49 + 52 = 101$ e $50 + 51 = 101$. Isto dá um total de 50 pares de números cuja soma dá 101. Portanto, a soma total é $50 \cdot 101 = 5050$."

Desta maneira aparentemente simples, Gauss tinha encontrado a propriedade da simetria das progressões aritméticas, derivando a fórmula da soma para uma progressão aritmética arbitrária - fórmula que, provavelmente, Gauss descobriu por si próprio.

Este acontecimento marcou o ponto de viragem na sua vida. Büttner imediatamente percebeu que pouco mais tinha para ensinar a Gauss e deu-lhe o melhor livro escolar de aritmética, especialmente encomendado de Hamburg. Por essa altura, Gauss teve um estreito contato com Martin Bartels, na altura com 18 anos, assistente de Büttner nas aulas o que constituiu um golpe de sorte, não tanto para

Gauss que pouco tinha a aprender com ele mas para Bartels que, mais tarde, se tornou professor de Matemática.

Perante este gênio, tanto Büttner como Bartels visitaram o pai de Gauss para lhe falarem da educação do seu filho. Gebhard estava habituado a que a sua vontade fosse lei na família e havia idealizado que os seus dois filhos seguissem os seus passos (o que, de facto, aconteceu com o meio irmão de Carl Friedrich, George, fruto do primeiro casamento de seu pai). Inicialmente Gebhard mostrou-se relutante e perguntou-lhes (com razão) como é que iria arranjar dinheiro suficiente para subsidiar a educação superior do seu filho. A isto Bartels e Büttner responderam com o único argumento que era habitual e, frequentemente, o único possível, nesses dias: "Não temos dúvida que arranjaremos qualquer pessoa distinta que queira servir de patrono a um tal gênio."

O resultado foi um compromisso... Gebhard permitiu que o rapaz abandonasse o seu trabalho de rotina fiando linho. A roca de fiar desapareceu (Gebhard disse que havia feito dela lenha para a lareira) e, no seu lugar, apareceram livros. Gauss e Bartels passaram então a trabalhar juntos. Costumavam sentar-se e discutir problemas de Matemática até longas horas da noite. Mas cedo Bartels compreendeu que nada tinha para ensinar a Gauss. O aluno tinha superado o mestre.

Em 1788, Gauss matriculou-se (quase contra a vontade do pai) no Liceu Catharineum em Braunschweig. O Professor Hellwing devolveu o primeiro trabalho escrito de Gauss com o comentário de que "não era necessário, para um estudante tão dotado, continuar a ter aulas naquela classe".

Com a ajuda de Bartels e do filólogo Meyerhoff, Gauss depressa ultrapassou os seus colegas, não só em Matemática como também nas línguas clássicas. No entanto, para que fosse possível continuar a sua educação, e terminado o período de frequência neste colégio, era necessário dinheiro, coisa que Gauss não tinha.

Disputationes arithmeticae

As ideias que fluíram de Gauss durante os anos frutuosos de $1795-1801$ foram, na sua maioria, reunidas num trabalho que publicou em Leipzig em 1801, *Disputationes arithmeticae*.

A impressão foi paga pelo Duque Ferdinand razão pela qual o trabalho começa

com uma dedicatória a "Sua Graciosa Alteza, Príncipe e Lorde Carl Wilhelm Ferdinand, Duque de Braunschweig e Lüneburg". Entre outras coisas, Gauss declara que, sem a bondade do Duque, "nunca teria conseguido dedicar-se à Matemática, na qual tenho estado sempre mergulhado com apaixonado amor". Esta dedicatória é fortalecida pelo estilo rococó que era usado na altura mas, neste caso, não estamos perante uma bajulação vazia de sentimento. Estas palavras refletiam aquilo que Gauss sentia.

As Disquisitiones arithmeticae estão divididas em sete partes:

1. Congruências em geral
2. Congruências de primeiro grau
3. Resto de potências
4. Congruências de segundo grau
5. Formas quadráticas
6. Aplicações
7. Divisões do círculo

Apresentamos em seguida apenas um esboço do conteúdo das Disquisitiones arithmeticae que, com propriedade, podem ser consideradas como uma sinfonia clássica em sete momentos, onde os diferentes temas são combinados num final que é levado a cabo com grande força e magnífica clareza.

Congruências em Geral e Congruências de Primeiro Grau

Na primeira página Gauss introduz um novo símbolo matemático e diz que:

Se um número m divide a diferença $a - b$ (ou $b - a$) de dois números a e b sem deixar resto, então a e b dizem-se congruentes módulo m, e Gauss escreveu

$$a \equiv b \bmod m$$

Esta expressão lê-se: a é congruente com b módulo m. A relação é chamada congruência; e m é chamado de módulo da congruência. O número b é chamado

o resto de a módulo m, e inversamente a é chamado o resto de b módulo m. Se a diferença $a - b$ não for divisível por m, então a e b dizem-se incongruentes módulo m, e a e b não são restos um do outro, módulo m.

De acordo com a definição, $a \equiv b \bmod m$ é o mesmo que $a - b = my$, onde y é um número inteiro qualquer.

Gauss escolheu o símbolo com grande previdência, dada a analogia entre congruências e igualdades. A noção de congruência é mais inclusiva, dado que podemos considerar a igualdade uma congruência de módulo 0.

Na segunda seção do seu Disquisitiones arithmeticae Gauss primeiro provou alguns teoremas donde saiu aquele que usualmente é chamado o Teorema Fundamental da Aritmética:

Todo o número natural maior que 1 pode, exceto pela ordem dos fatores, ser escrito de uma e uma só maneira como produto de números primos.

Usando o teorema fundamental da álgebra Gauss depois determinou o máximo divisor comum (a, b) e o mínimo múltiplo comum $[a, b]$, de dois números a e b.

O resultado de Gauss para a solubilidade das congruências lineares é:

Se $(a, m) = d$, então é condição necessária e suficiente para que a congruência $a \equiv b \bmod m$ seja solúvel que d seja um divisor de b. Então logo existem d diferentes sequências de soluções, ou seja, d soluções.

1.2 Congruência

Definição 1.1 *Se a e b são inteiros, dizemos que a é congruente a b módulo m se $m \mid (a - b)$. Denotamos isto por $a \equiv b \bmod m$. Se $m \nmid (a - b)$ dizemos que a é incongruente a b módulo m e denotamos $a \not\equiv b \bmod m$.*

Exemplo 1.1 $11 \equiv 3 \bmod 2$ *pois* $2 \mid (11 - 3)$. *Como* $5 \nmid 6$ *e* $6 = 17 - 11$ *temos que* $17 \not\equiv 11 \bmod 5$.

Proposição 1.1 *Se a e b são inteiros, temos que $a \equiv b \bmod m$ se, e somente se, existir um inteiro k tal que $a = b + km$.*

Demonstração: Se $a \equiv b \bmod m$, então $m \mid (a - b)$ o que implica na existência de um inteiro k tal que $a - b = km$, isto é, $a = b + km$. A recíproca é trivial pois

da existência de um k satisfazendo $a = b + km$, temos $km = a - b$, ou seja, que $m \mid (a - b)$ isto é, $a \equiv b \bmod m$.

■

Proposição 1.2 *Se a, b, m e d são inteiro, $m > 0$, as seguintes sentenças são verdadeiras:*

1. $a \equiv a \bmod m$
2. Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$
3. Se $a \equiv b \bmod m$ e $b \equiv d \bmod m$, então $a \equiv d \bmod m$.

Demonstração:

1. Como $m \mid 0$, então $m \mid (a - a)$, o que implica $a \equiv a \bmod m$.
2. Se $a \equiv b \bmod m$, então $a = b + k_1 m$ para algum inteiro k_1. Logo, $b = a - k_1 m$, o que implica, pela Proposição 1.1, $b \equiv a \bmod m$.
3. Se $a \equiv b \bmod m$ e $b \equiv a \bmod m$, então existem inteiros k_1 e k_2 tais que $a - b = k_1 m$ e $b - d = k_2 m$. Somando-se, membro a membro, estas últimas equações, obtemos $a - d = (k_1 + k_2)m$, o que implica $a \equiv d \bmod m$.

■

Esta proposição nos diz que a relação de congruência, no conjunto dos inteiros, é uma relação de equivalência, pois acabamos de provar que ela, é reflexiva, simétrica e transitiva.

Teorema 1.1 *Se a, b, c e m são inteiros tais que $a \equiv b \bmod m$, então*

(1) $a + c \equiv b + c \bmod m$

(2) $a - c \equiv b - c \bmod m$

(3) $ac \equiv bc \bmod m$

Demonstração:

(1) Como $a \equiv b \bmod m$, temos que $a - b = km$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c \bmod m$.

(2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = km$ temos que $a - c \equiv b - c \bmod m$.

(3) Como $a - b = km$ então $ac - bc = ckm$ o que implica $m \mid (ac - bc)$ e, portanto, $ac \equiv bc \bmod m$.

■

Teorema 1.2 *Se a, b, c, d e m são inteiros tais que $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então*

(1) $a + c \equiv b + d \bmod m$

(2) $a - c \equiv b - d \bmod m$

(3) $ac \equiv bd \bmod m$

Demonstração:

(1) De $a \equiv b \bmod m$ e $c \equiv d \bmod m$ temos $a - b = km$ e $c - d = k_1 m$. Somando-se ambos os lados da igualdade, obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d \bmod m$.

(2) Basta subtrair ambos os lados da igualdade $a - b = km$ e $c - d = k_1 m$ obtendo $(a - b) - (c - d) = (k - k_1)m$ o que implica $a - c \equiv b - d \bmod m$.

(3) Multiplicamos ambos os lados de $a - b = km$ por c e ambos os de $c - d = k_1 m$ por b, obtendo $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta, agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = (ck + bk_1)m$ o que implica $ac \equiv bd \bmod m$

■

Teorema 1.3 *Se a, b, c e m são inteiros e $ac \equiv bc \bmod m$, então $a \equiv b \bmod \frac{m}{d}$ onde $d = (c, m)$.*

Demonstração: De $ac \equiv bc \bmod m$ temos $ac - bc = km$. Se dividirmos os dois membros por d, teremos $(c/d)(a-b) = k(m/d)$. Logo $\left(\frac{m}{d}\right) \mid \left(\frac{c}{d}\right)(a-b)$ e como $(m/d, c/d) = 1$, temos que, $(m/d) \mid (a-b)$ o implica $a \equiv b \bmod \frac{m}{d}$.

■

Definição 1.2 *Se h e k são dois inteiros, com $h \equiv k \bmod m$, dizemos que k é um resíduo de h módulo m.*

Definição 1.3 *o conjunto dos inteiros $\{r_1, r_2, \ldots, r_s\}$ é um sistema completo de resíduos módulo m se (1) $r_i \not\equiv r_j \bmod m$ para $i \neq j$ (2) para todo inteiro n existe um r_i tal que $n \equiv r_i \bmod m$.*

Exemplo 1.2 *$\{0, 1, 2, \ldots, m-1\}$ é um sistema completo de resíduos módulo m.*

Exemplo 1.3 *Para m ímpar o conjunto seguinte é um sistema completo de resíduos módulo m.* $\left\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\right\}$.

Teorema 1.4 *Se k inteiros $r_1, r_2, \ldots, r_k$ formam um sistema completo de resíduos módulo m então $k = m$.*

Demonstração: Primeiramente demonstramos que os inteiros $t_0, t_1, \ldots, t_{m-1}$, com $t_i = i$ formam, de fato, um sistema completo de resíduos módulo m. Sabemos que , para cada n, existe um único par de inteiros q e s, tais que $n = mq + s, 0 \leq s < m$. Logo, $n \equiv s \bmod m$, sendo s um dos t_i. Como $|t_i - t_j| \leq m-1$, temos $t_i \not\equiv t_j \bmod m$ para $i \neq j$. Portanto, o conjunto $\{t_0, t_1, \ldots, t_{n-1}\}$, é um conjunto de resíduos módulo m. Disto concluímos que cada r_i é congruente a exatamente a um dos t_i, o que nos garante $k \leq m$. Como o conjunto $\{r_1, r_2, \ldots, r_k\}$ forma, por hipótese, um sistema completo de resíduos módulo m, cada t_i é congruente a exatamente um dos r_i e, portanto, $m \leq k$. Desta forma $k = m$.

■

Teorema 1.5 *Se $r_1, r_2, \ldots, r_m$ é um sistema completo de resíduos módulo m e a e b são inteiros com $(a, m) = 1$, então*

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

também é um sistema completo de resíduos módulo m.

Demonstração: Considerando-se o resultado do teorema anterior, será suficiente mostrar que quaisquer dois inteiros do conjunto $ar_1 + b, ar_2 + b, \ldots, ar_m + b$, são incongruentes módulo m. Para isto vamos supor que $ar_i + b \equiv ar_j + b \bmod m$. Logo, pelo Teorema 1.1, temos $ar_i \equiv ar_j \bmod m$. Mas, como $(a, m) = 1$, pelo Teorema 1.1 nos diz que $r_i \equiv r_j \bmod m$. O fato de $r_i \equiv r_j \bmod m$ implica $i = j$, uma vez que, $r_1, r_2, \ldots, r_m$ formam um sistema completo de resíduos módulo m, o que completa a demonstração.

■

Proposição 1.3 *Se a, b, k e m são inteiros com $k > 0$ e $a \equiv b \bmod m$, então $a^k \equiv b^k \bmod m$.*

Demonstração: Isto segue, imediatamente, da identidade:

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1})$$

■

Teorema 1.6 *Se $a \equiv b \bmod m_1, a \equiv b \bmod m_2, \ldots, a \equiv b \bmod m_k$*
onde $a, b, m_1, m_2, \ldots, m_k$ são inteiros com m_i positivos, $i = 1, 2, \ldots, k$, então

$$a \equiv b \bmod [m_1, m_2, \ldots, m_k]$$

Onde $[m_1, m_2, \ldots, m_k]$ é o mínimo múltiplo comum de $m_1, m_2, \ldots, m_k$.

Demonstração: Seja p_n o maior primo que aparece nas fatorações de $m_1, m_2, \ldots, m_k$. Cada m_i, $i = 1, 2, \ldots, k$ pode, então, ser expresso como

$$m_i = p_1^{\alpha_{1i}} \cdot p_2^{\alpha_{2i}} \ldots p_n^{\alpha_{ni}},$$

(alguns α_{ji} podem ser nulos).

Como $m_i \mid (a-b), i = 1, 2, \ldots, k$, temos que $p_j^{\alpha_{ji}} \mid (a-b), i = 1, 2, \ldots, k$, $j = 1, 2, \ldots, n$. Logo, se tomarmos $\alpha_j = \max_{1 \leq i \leq k}\{\alpha_{ji}\}$ teremos que

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} \mid (a-b)$$

Mas,

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = [m_1, m_2, \ldots, m_k]$$

O que implica $a \equiv b \bmod [m_1, m_2, \ldots, m_k]$

■

1.3 Congruência Linear

Chamamos de congruência linear de uma variável a uma congruência da forma $ax \equiv b \bmod m$ onde x é uma incógnita. É fácil de se verificar que se x_0 é uma solução, i.e., $ax_0 \equiv b \bmod m$ e $x_1 \equiv x_0 \bmod m$, então x_1 também é solução. Isto é obvio, pois se $x_1 \equiv x_0 \bmod m$, então $ax_1 \equiv ax_0 \equiv b \bmod m$. O que acabamos de verificar é que se um membro de uma classe de equivalência é solução, então todo membro desta classe é solução. Destas observações surge uma questão natural: No caso de existir alguma solução, quantas soluções incongruentes existem? Antes de respondermos a esta importante questão, necessitamos provar um teorema que nos dá informações sobre a existência de soluções para uma equação diofantina linear. Uma equação da forma $ax + by = c$, onde a, b e c são inteiros é chamada equação diofantina linear (o nome vem do matemático grego Diofanto).

Teorema 1.7 *Sejam a e b inteiros positivos e $d = (a, b)$. Se $d \nmid c$, então a equação $ax + by = c$ não possui nenhuma solução inteira. Se $d|c$ ela possui infinitas soluções e se $x = x_0$ e $y = y_0$ é uma solução particular, então todas as soluções são dadas por*

$$x = x_0 + (b/d)k$$

$$y = y_0 - (a/d)k,$$

onde k é um inteiro

Demonstração: Se $d \nmid c$, então a equação $ax + by = c$ não possuí solução pois, como $d|a$ e $d|b$, d deveria dividir c, o qual é uma combinação linear de a e b. Suponhamos, pois, que $d|c$. Pelo Teorema 1.3, existem inteiros n_0 e m_0, tais que

$$an_0 + bm_0 = d \tag{1.1}$$

Como $d|c$, existe um inteiro k tal que $c = kd$. Se multiplicarmos, ambos os membros de (1.1) por k, teremos $a(n_0k) + b(m_0k) = kd = c$. Isto nos diz que o par (x_0, y_0) com $x_0 = n_0k$ e $y_0 = m_0k$ é uma solução de $ax + by = c$. É fácil a verificação de que os pares da forma

$$x = x_0 + (b/d)k$$

$$y = y_0 - (a/d)k$$

são soluções, uma vez que

$$ax + by = a(x_0 + (b/d)k) + b(y_0 - (a/d)k) = ax_0 + \frac{ab}{d}k + by_0 - \frac{ab}{d}k = ax_0 + by_0 = c$$

O que acabamos de mostrar é que, conhecida uma solução particular (x_0, y_0) podemos, a partir dela, gerar infinitas soluções. Precisamos, agora, mostrar que toda solução da equação $ax + by = c$ é da forma $x = x_0 + (b/d)k, y = y_0 - (a/d)k$. Vamos supor que (x, y) seja uma solução, i.e., $ax + by = c$. Mas, como $ax_0 + by_0 = c$, obtemos, subtraindo membro a membro, que

$$ax + by - ax_0 - by_0 = a(x - x_0) + b(y - y_0) = 0,$$

o que implica $a(x - x_0) = b(y_0 - y)$. Como $d = (a, b)$ temos, pelo Corolário da Proposição 1.4, que

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

Portanto, dividindo-se os dois membros da última igualdade por d, teremos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \tag{1.2}$$

Logo, pelo Teorema 1.6, $(b/d)|(x - x_0)$ e portanto existe um inteiro k satisfazendo $x - x_0 = k(b/d)$, ou seja $x = x_0 + (b/d)k$. Substituindo-se este valor de x na equação (1.2) temos $y = y_0 - (a/d)k$, o que conclui a demonstração.

■

Com este teorema à mão podemos, agora, dizer quantas são as soluções incongruentes (caso exista alguma) que a congruência linear $ax \equiv b \bmod m$ possui.

Teorema 1.8 *Sejam a, b e m inteiros tais que $m > 0$ e $(a, m) = d$. No caso em que $d \nmid b$ a congruência $ax \equiv b \bmod m$ não possui nenhuma solução e quando $d \mid b$, possui exatamente d soluções incongruentes módulo m.*

Demonstração: Pela Proposição 1.1, sabemos que o inteiro x é solução de $ax \equiv b \bmod m$ se, e somente se, existe um inteiro y tal que $ax = b + my$, ou, o que é equivalente, $ax - my = b$. Do teorema anterior sabemos que esta equação não possui nenhuma solução caso $d \nmid b$, e que se $d|b$ ela possui infinitas soluções dadas por $x = x_0 - (m/d)k$ e $y = y_0 - (a/d)k$, onde (x_0, y_0) é uma solução particular de $ax - my = b$. Logo, a congruência $ax \equiv b \bmod m$ possui infinitas soluções dadas por $x = x_0 - (m/d)k$. Como estamos interessados em saber o número de soluções incongruentes, vamos tentar descobrir sobre que condições $x_1 = x_0 - (m/d)k_1$ e $x_2 = x_0 - (a/d)k_2$ são congruentes módulo m. Se x_1 e x_2 são congruentes, então $x_0 - (m/d)k_1 \equiv x_0 - (m/d)k_2 \bmod m$. Isto implica $(m/d)k_1 \equiv (m/d)k_2 \bmod m$, e como $(m/d)m$ temos $(m/d, m) = m/d$, o que nos permite o cancelamento de m/d resultando, pelo Teorema 1.3, $k_1 \equiv k_2 \bmod d$. Observe que m foi substituído por $d = m/(m/d)$. Isto nos mostra que soluções incongruentes serão obtidas ao tomarmos $x = x_0 - (m/d)k$, onde k percorre um sistema completo de resíduos módulo d, o que conclui a demonstração.

■

Definição 1.4 *Dizemos que uma solução x_0 de $ax \equiv b \bmod m$ é única módulo m quando qualquer outra solução x_1 for congruente a x_0 módulo m.*

Definição 1.5 *Uma solução $\bar{a}$ de $ax \equiv 1 \bmod m$ é chamada de um inverso de a módulo m. Segue, agora, do Teorema 1.8, que se $(a, m) = 1$, então a possui um único inverso módulo m. A proposição seguinte nos diz quando um inteiro a e o seu próprio inverso módulo p, onde p é um número primo.*

Proposição 1.4 *Seja p um número primo. O inteiro positivo a é o seu próprio inverso módulo p se, e somente se, $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$.*

Demonstração: Se a é o seu próprio inverso, então $a^2 \equiv 1 \bmod p$, o que significa que $p \mid (a^2-1)$. Mas se $p \mid (a-1)(a+1)$, sendo p primo, $p|(a-1)$ ou $p|(a+1)$, o que implica $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$. A recíproca é imediata pois, se $a \equiv 1 \bmod p$ ou $a \equiv -1 \bmod p$, então $p|(a-1)$ ou $p|(a+1)$. Portanto, $p|(a-1)(a+1)$ o que significa $a^2 \equiv 1 \bmod p$, o que conclui a demonstração.

■

1.4 Os Teoremas de Euler, Fermat e Wilson

Antes de demonstrarmos o Teorema de Wilson, que diz que para p primo $(p-1)! \equiv -1 \bmod p$, fornecemos um exemplo, tomando $p = 13$, com a finalidade de apresentarmos a ideia utilizada na demonstração. Dentre os números $1, 2, 3, \ldots, 12$ somente os números 1 e 12 são os seus próprios inversos módulo 13. Isto segue da Proposição 1.4, pois $1 \equiv 1 \bmod 13$ e $12 \equiv -1 \bmod 13$ e nenhum dos números $2, 3, \ldots, 11$ é congruente a 1 ou -1 módulo 13. Mas, como os números $2, 3, 4, \ldots, 11$ são todos relativamente primos com 13, cada um deles possui, pelo Teorema 1.8, um único inverso módulo 13. Eles podem, portanto, ser agrupados em 5 pares $(5 = (13-3)/2)$ que são os seguintes:

$$2 \times 7 \equiv 1 \bmod 13$$

$$3 \times 9 \equiv 1 \bmod 13$$

$$4 \times 10 \equiv 1 \bmod 13$$

$$5 \times 8 \equiv 1 \bmod 13$$

$$6 \times 11 \equiv 1 \bmod 13$$

Pelo Teorema 1.2 (3) podemos multiplicar estas congruências, membro a membro, obtendo

$$2 \times 3 \times 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \equiv 1 \bmod 13$$

Se multiplicarmos os dois lados por 12 teremos

$$2 \times 3 \times 4 \times \cdots \times 11 \times 12 \equiv 12 \bmod 13$$

e, portanto, como $12 \equiv -1 \bmod 13$ temos, finalmente, $(13-1)! \equiv -1 \bmod 13$.

Teorema 1.9 (Teorema de Wilson) *Se p é primo, então* $(p-1)! \equiv -1 \bmod p$.

Demonstração: Como $(2-1)! \equiv -1 \bmod 2$ o resultado é válido para $p = 2$. Pelo Teorema 1.8, a congruência $ax \equiv 1 \bmod p$ tem uma única solução para todo a no conjunto $1, 2, 3, .., p-1$ e como, destes elementos, somente 1 e $p-1$ são seus próprios inversos módulo p, podemos agrupar os números $2, 3, 4, \ldots, p-2$ em $(p-3)/2$ pares cujo produto seja congruente a 1 módulo 13. Se multiplicarmos estas congruências, membro a membro, teremos, pelo Teorema 1.2 (3) $2 \times 3 \times 4 \times \cdots \times (p-2) \equiv 1 \bmod p$. multiplicando-se ambos os lados desta congruência por $p-1$ teremos

$$2 \times 3 \times 4 \times \cdots \times (p-2) \times (p-1) \equiv (p-1) \bmod p,$$

isto é, $(p-1)! \equiv -1 \bmod p$ uma vez que $p - 1 \equiv -1 \bmod p$.

■

O teorema seguinte nos diz que se um número satisfaz a relação do teorema de Wilson, ele deve ser primo.

Teorema 1.10 *Se n é um inteiro tal que* $(n-1)! \equiv -1 \bmod n$, *então n é primo.*

Demonstração: A prova é por contradição. Vamos supor que $(n-1)! \equiv -1 \bmod n$, isto é, $n \mid ((n-1)! + 1)$ e que n não seja primo, ou seja, $n = rs$, $1 < r < n$ e $1 < s < n$. Nestas condições $r \mid (n-1)!$ e, sendo r um divisor de n, $r \mid ((n-1)!+1)$ e, portanto, r deve dividir a diferença $(n-1)! + 1 - (n-1)! = 1$, o que é absurdo, uma vez que $r > 1$. Logo, um tal n satisfazendo $(n-1)! \equiv -1 \bmod n$ deve ser primo.

■

O próximo teorema nos diz que se p é primo e $p \nmid a$, então $p|(a^{p-1} - 1)$. Vamos primeiramente provar isto num caso particular com a finalidade de ilustrar a ideia usada na demonstração. Sejam $p = 11$ e $a = 5$. Logo temos:

$$1 \times 5 \equiv 5 \bmod 11$$

$$2 \times 5 \equiv 10 \bmod 11$$

$$3 \times 5 \equiv 4 \bmod 11$$

$$4 \times 5 \equiv 9 \bmod 11$$

$$5 \times 5 \equiv 3 \bmod 11$$

$$6 \times 5 \equiv 8 \bmod 11$$

$$7 \times 5 \equiv 2 \bmod 11$$

$$8 \times 5 \equiv 7 \bmod 11$$

$$9 \times 5 \equiv 1 \bmod 11$$

$$10 \times 5 \equiv 6 \bmod 11$$

Observe que 11 não divide nenhum dos produtos $j \times 5$, $1 \leq j \leq 10$ que estão na coluna da esquerda nas congruências acima. Observe, também, que todos eles são incongruentes módulo 11, pois se $5j \equiv 5k \bmod 11$, devemos ter $j \equiv k \bmod 11$ com $1 \leq j \leq 10$ e $1 \leq k \leq 10$, e, portanto, $j = k$. Logo, como nenhum é congruente a zero módulo 11 e todos são incongruentes módulo 11, eles devem ser congruentes a diferentes números dentre $1, 2, 3, \ldots, 10$. Observe que todos estes números aparecem, sem repetições, na coluna. da direita nas congruências acima. Agora podemos multiplicar, membro a membro, estas congruências para obter

$$(1 \times 5)(2 \times 5)(3 \times 5) \cdots (10 \times 5) \equiv 5 \times 10 \times 4 \times 9 \times 3 \times 8 \times 2 \times 7 \times 1 \times 6 \bmod 11$$

e, portanto, $5^{10}10! \equiv 10! \bmod 11$. Mas, como $(10!, 11) = 1$ temos, pelo Teorema 1.3, que

$$5^{10} \equiv 1 \bmod 11,$$

o que mostra a validade do teorema neste caso particular em que $a = 5$ e $p = 11$. Com este exemplo cm mente será fácil provar o teorema.

Teorema 1.11 *[Pequeno Teorema de Fermat] Seja p primo. Se $p \nmid a$ então $a^{p-1} \equiv 1 \bmod p$.*

Demonstração: Sabemos que o conjunto formado pelos p números $\{0, 1, 2, \ldots, p-1\}$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado correspondência biunívoca com um subconjunto de $\{0, 1, 2, \ldots, p-1\}$. Vamos, agora, considerar os números $a, 2a, 3a, \ldots, (p-1)a$. Como $(a, p) = 1$, nenhum destes

números ia,$1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak \bmod p$ implica $j \equiv k \bmod p$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto do $p-1$ elementos incongruentes módulo p e não-divisíveis por p. Logo, cada um deles é congruente a exatamente um dentre os elementos $\{1, 2, 3, \ldots, p-1\}$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)(4a)\cdots(p-1)a \equiv 1 \times 2 \times 3 \times \cdots \times (p-1) \bmod p,$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Mas, como$((p-1)!, p) = 1$, podemos cancelar o fator $(p-1)!$ em ambos os lados, obtendo

$$a^{p-1} \equiv 1 \bmod p$$

o que conclui a demonstração.

■

Corolário 1.11.1 *Se p é um primo e a é um inteiro positivo, então $a^p \equiv a \bmod p$.*

Demonstração: Temos que analisar dois casos, se $p \mid a$ e se $p \nmid a$. Se $p \mid a$, então $p \mid (a(a^{p-1} - 1))$ e, portanto $a^p \equiv a \bmod p$. Se $p \nmid a$, $p \mid a^{p-1} - 1$ e, portanto, $p \mid (a^p - a)$. Logo, em ambos os casos, $a^p \equiv a \bmod p$.

■

Definição 1.6 *Se n é um inteiro positivo, a função ϕ de Euler, denotada por $\phi(n)$, é definida como sendo o número de inteiros positivos menores do que ou iguais a n que são relativamente primos com n.*

Definição 1.7 *Um sistema reduzido de resíduos módulo m é um conjunto de $\phi(n)$ inteiros $r_1, r_2, \ldots, r_{\phi(m)}$, tais que cada elemento do conjunto é relativamente primo com m, e se $i \neq j$, então $r_i \not\equiv r_j \bmod m$.*

Exemplo 1.4 *O conjunto $\{0, 1, 2, 3, 4, 5, 6, 7\}$ é um sistema completo de resíduos módulo 8, portanto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8. A fim de se obter um sistema reduzido de resíduos de um sistema completo módulo m, basta retirar os elementos do sistema completo que não são relativamente primos com m.*

Teorema 1.12 *Seja a um inteiro positivo tal que $(a, m) = 1$. Se $r_1, r_2, \ldots, r_{\phi(m)}$ é um sistema reduzido de resíduos módulo m, então $ar_1, ar_2, \ldots, ar_{\phi(m)}$ é, também, um sistema reduzido de resíduos módulo m.*

Demonstração: Como na sequência $ar_1, ar_2, \ldots, ar_{\phi(m)}$ temos $\phi(m)$ elementos, devemos mostrar que todos eles são relativamente primos com m e, dois a dois, incongruentes módulo m. Como $(a, m) = 1$ e $(r_i, m) = 1$, temos $(ar_i, m) = 1$. Logo, nos resta mostrar que $ar_i \not\equiv ar_j \bmod m$ se $i \neq j$. Mas, como $(a, m) = 1$ de $ar_i \equiv ar_j \bmod m$ temos $r_i \equiv r_j \bmod m$, o que implica $i = j$, uma vez que $ar_1, ar_2, \ldots, ar_{\phi(m)}$, é um sistema reduzido de resíduos módulo m, o que conclui a demonstração.

■

Vamos, agora, mostrar a validade do Teorema de Euler num caso especial para ilustrar a ideia que usaremos na demonstração. Sejam $m = 8$ e $a = 5$. Sabemos que o conjunto $\{1, 3, 5, 7\}$ é um sistema reduzido de resíduos módulo 8.

Consideremos o conjunto formado por $5 \times 1, 5 \times 3, 5 \times 5$ e 5×7. Pelo Teorema 1.12 este conjunto também constitui um sistema reduzido de resíduos módulo 8. Isto significa que cada um dos elementos $5 \times 1, 5 \times 3, 5 \times 5, 5 \times 7$ é congruente módulo 8 a exatamente um dos elementos $1, 3, 5, 7$. Temos, na realidade que

$$5 \times 1 \equiv 5 \bmod 8$$

$$5 \times 3 \equiv 7 \bmod 8$$

$$5 \times 5 \equiv 1 \bmod 8$$

Multiplicando-se membro a membro, estas congruências obtemos

$$5^4(1 \times 3 \times 5 \times 7) \equiv (1 \times 3 \times 5 \times 7) \bmod 8$$

Como $(1 \times 3 \times 5 \times 7, 8) = 1$ podemos cancelar o fator $(1 \times 3 \times 5 \times 7)$ obtendo

$$5^4 \equiv 1 \bmod 8.$$

Observe que $4 = \phi(8)$, ou seja, provamos que $5^{\phi(8)} \equiv 1 \bmod 8$.

Teorema 1.13 *(Euler) Se m é um inteiro positivo e a um inteiro com $(a, m) = 1$, então*

$$a^{\phi(m)} \equiv 1 \bmod m.$$

Demonstração: No Teorema 1.12 mostramos que os elementos $ar_1, ar_2, \ldots, ar_{\phi(m)}$ constituem um sistema reduzido de resíduos módulo m se $(a, m) = 1$ e $r_1, r_2, \ldots, r_{\phi(m)}$ for um sistema reduzido de resíduos módulo m, Isto significa que ar_i é congruente a exatamente um dos $r_j, 1 \leq j \leq \phi(m)$, e portanto o produto dos ar_i, deve ser congruente ao produto dos r_j módulo m, isto é,

$$ar_1 \cdot ar_2 \cdot \ldots \cdot ar_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \bmod m$$

ou seja,

$$a^{\phi(m)} \cdot r_1 \cdot r_2 \cdot \ldots r_{\phi(m)} \equiv r_1 \cdot r_2 \cdot \ldots \cdot r_{\phi(m)} \bmod m.$$

Como

$$\left(\prod_{i=1}^{\phi(m)} r_i, m \right) = 1$$

podemos cancelar

$$\prod_{i=1}^{\phi(m)} r_i$$

em ambos os lados para obter $a^{\phi(m)} \equiv 1 \bmod m$. Como para p primo, $\phi(p) = p - 1$, o teorema acima é uma generalização do Teorema 1.11.

■

1.5 O Teorema Chinês dos Restos

O nome dado ao teorema seguinte se deve ao fato de que este resultado já era conhecido, na antiguidade, pelos matemáticos chineses.

Teorema 1.14 (O Teorema Chinês dos Restos) *Se $(m_i, m_j) = 1$ para $i \neq j$ e c_i são inteiros, então o sistema*

$$\begin{cases} x \equiv c_1 \bmod m_1 \\ x \equiv c_2 \bmod m_2 \\ x \equiv c_3 \bmod m_3 \\ \vdots \\ x \equiv c_r \bmod m_r \end{cases} \tag{1.3}$$

possui solução e a solução é única módulo m, onde $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Demonstração: Se definirmos $y_i = m/m_i$, onde $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$, teremos $(y_i, m_i) = 1$, pois $(m_i, m_j) = 1$ para $i \neq j$. Dessa forma, pelo Teorema 1.8, cada uma das congruências $y_i x \equiv 1 \bmod m_i$ possui uma única solução que denotamos por $\overline{y_i}$. Logo, $y_i\overline{y_i} \equiv 1 \bmod m_i, i = 1, 2, \cdots, r$. Afirmamos que o número x dado por

$$x = c_1 y_1 \overline{y_1} + c_2 y_2 \overline{y_2} + \cdots + c_r y_r \overline{y_r}$$

é uma solução simultânea para o nosso sistema de congruências.

De fato, pela definição dos y_j, temos que $m_i \mid y_j$ para $i \neq j$. Assim, $c_j y_j \equiv 0 \bmod m_i$ e, consequentemente,

$$x = c_1 y_1 \overline{y_1} + c_2 y_2 \overline{y_2} + \cdots + c_i y_i \overline{y_i} + \ldots + c_r y_r \overline{y_r} \equiv c_i y_i \overline{y_i} \bmod m_i \equiv c_i \bmod m_i.$$

Provamos, a seguir, que esta solução é única módulo m. Se $\bar{x}$ é uma outra solução para o nosso sistema, então $\bar{x} \equiv c_i \equiv x \bmod m_i$ e, portanto, $\bar{x} \equiv x \bmod m_i$. Logo, $m_i \mid (\overline{x} - x), i = 1, 2, \ldots, r$.

Por outro lado, como $(m_i, m_j) = 1$ para $i \neq j$ temos que

$$[m_1, m_2, \ldots, m_r] = m_1 \cdot m_2 \cdot \ldots \cdot m_r.$$

Portanto, pelo Teorema 1.6, $mm_1 \cdot m_2 \cdot \ldots \cdot m_r \mid (\bar{x} - x)$, ou seja, $\bar{x} \equiv x \bmod m$, o que conclui a demonstração.

■

O corolário seguinte é uma versão mais completa do Teorema 1.14. Sua prova segue imediatamente dos teoremas 1.8 e 1.14.

Corolário 1.14.1 (O Teorema Chinês dos Restos - versão 2) *Se $(a_i, m_i) = 1$, $(m_i, m_j) = 1$ para $i \neq j$ e c_i inteiro, então o sistema*

$$\begin{cases} a_1x \equiv c_1 \bmod m_1 \\ a_2x \equiv c_2 \bmod m_2 \\ a_3x \equiv c_3 \bmod m_3 \\ \vdots \\ a_rx \equiv c_r \bmod m_r \end{cases} \tag{1.4}$$

possui solução e a solução é única módulo m, onde $m = m_1 \cdot m_2 \cdot \cdots \cdot m_r$.

Demonstração: Pelo Teorema 1.8, para cada $i = 1, \ldots, r$, existe $\overline{a_i}$ tal que $a_i\overline{a_i} \equiv 1 \bmod m_i$ e, portanto, o sistema de congruências (1.4) é equivalente a

$$\begin{cases} x \equiv \overline{a_1}c_1 \bmod m_1 \\ x \equiv \overline{a_2}c_2 \bmod m_2 \\ x \equiv \overline{a_3}c_3 \bmod m_3 \\ \vdots \\ x \equiv \overline{a_r}c_r \bmod m_r \end{cases} \tag{1.5}$$

Como o sistema (1.5) é idêntico ao do Teorema 1.14, o resultado segue.

■

Capítulo 2

Aplicações

2.1 Aritmética modular e alguma de suas aplicações

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Foi o brilhante Gauss que observou que usávamos com muita frequência frases do tipo: a dá o mesmo resto que b quando divididos por m; e que essa relação tinha um comportamento semelhante à igualdade. Foi Gauss então que introduziu uma notação específica para este fato e que denominou de *congruência*. Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O que não é muito comum é o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos em nosso estudo.

Este tema é bastante atual e pode ser trabalhado já nas classes do Ensino Fundamental e gerador de excelentes oportunidades de contextualização no processo de ensino/aprendizagem de matemática.

Inicialmente vamos mostrar alguns elementos teóricos sobre a aritmética modular e, na segunda parte do trabalho teremos a apresentação de alguns exemplos de aplicação desse importante e interessante tema da área de teoria dos números.

2.1.1 Noções básicas de aritmética modular

Antes de apresentarmos as definições e propriedades relacionadas à congruência, vamos desenvolver três exemplos que poderiam ser colocados a alunos da Educação Básica, ainda não familiarizados com o tema, como introdução ao assunto.

Exemplo 2.1 *Vamos apresentar uma questão retirada do banco de questões do site da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas).*

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

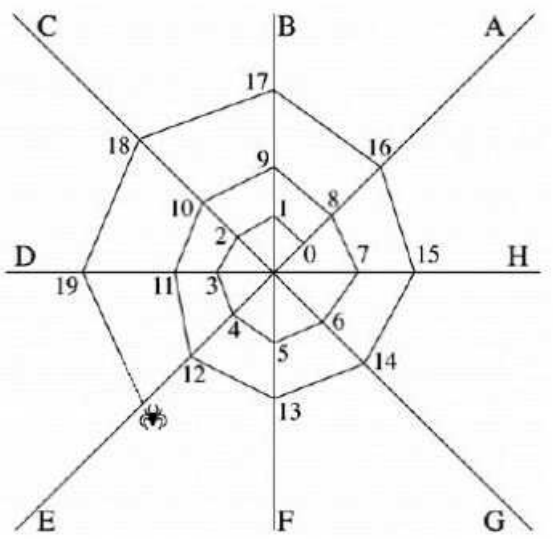

Figura 2.1: Teia da Aranha

Vejamos o que está acontecendo?

	0	1	2	3	4	5	6	7
	8	9	10	11	12	13	14	15
	16	17	18	19	20	21	22	23
	24	25	26	27	28	29	30	31
	...	...	...	...	...	...	...	...

É claro que alguma pessoa bem paciente poderia continuar construindo a tabela até que aparecesse o número 118. Assim ela saberia em qual fio a aranha iria estar. Convenhamos que não seria uma solução muito prática e nem rápida. Imagine se a questão perguntasse o fio correspondente ao número 890?

Podemos observar que os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentem de oito em oito. Observamos também que cada fio pode ser representado a partir dos múltiplos de 8. O fio A corresponde aos números que são múltiplos de 8, ou seja, números que divididos por 8 deixam resto zero ($8.n$, com $n \in \mathbb{N}$). O fio B corresponde aos números que são múltiplos de 8, mais 1, ou seja, números que divididos por 8 deixam resto 1 ($8.n + 1$, com $n \in \mathbb{N}$). O fio C corresponde aos números que são múltiplos de 8, mais 2, ou seja, números que divididos por 8 deixam resto 2 ($8.n + 2$, com $n \in \mathbb{N}$) e essa lógica se mantém até o fio H, definido pelos números que divididos por oito deixam resto 7. É claro que para saber sobre qual fio estará o número 118, basta verificarmos a qual dessas famílias tal número pertence e isso pode ser facilmente obtido ao dividirmos 118 por 8. Vejamos:

$$\begin{array}{r|l} 118 & 8 \\ \hline (6) & 14 \end{array}$$

Verificamos que o número 118 é igual a $8.14 + 6$, ou seja, pertence à família dos números que estão no fio G.

Todos os números de nosso exemplo, que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8 e, como já comentamos na introdução, são congruentes entre si, no módulo 8. O número 14, por exemplo, é congruente ao número 22, no módulo 8, e isso significa que esses dois números deixam o mesmo resto quando divididos por 8 (verifique que ambos estão sobre o fio G). Verificando:

$$\begin{array}{r|l} 14 & 8 \\ \hline (6) & 1 \end{array} \qquad \begin{array}{r|l} 22 & 8 \\ \hline (6) & 2 \end{array}$$

Simbolicamente, podemos escrever: $14 \equiv 22 \bmod 6$

Exemplo 2.2 ***Aritmética do relógio***

Trata-se de um caso de congruência, módulo 12 *(nos relógios analógicos, é claro). Note que* 13 *horas é congruente a* 1 *hora, no módulo* 12. *Ambos divididos por* 12,

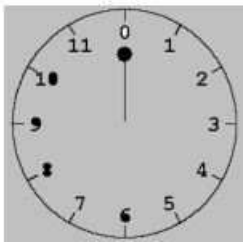

Figura 2.2: Relógio analógico

deixam resto 1. 17 *horas é congruente a* 5 *horas, módulo* 12. *Tanto* 17, *como* 5, *divididos por* 12, *deixam resto* 5 ... *e assim, sucessivamente.*

$$1 \equiv 13 \equiv 25 \equiv \ldots, \mathrm{mod}12$$

$$5 \equiv 17 \equiv 29 \equiv \ldots, \mathrm{mod}12$$

Assim as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12.

Exemplo 2.3 *Vejamos uma aplicação interessante sobre o tema, relacionada aos calendários:*

Vamos supor que você saiba em qual dia da semana caiu o dia 1^o *de janeiro de um determinado ano. Em* 2006, *por exemplo, foi um domingo. Imaginemos que você deseja saber quando cairá um outro dia qualquer (vale para qualquer ano). É só montar uma tabela para essa primeira semana, que no caso será:*

$$Domingo \rightarrow (1)$$
$$Segunda \rightarrow (2)$$
$$Terça \rightarrow (3)$$
$$Quarta \rightarrow (4)$$
$$Quinta \rightarrow (5)$$
$$Sexta \rightarrow (6)$$
$$Sábado \rightarrow (7)$$

Verificamos aqui que estamos novamente diante de um caso de congruência, módulo 7 *nesse caso. Digamos que estivéssemos interessados em descobrir em que dia*

da semana caiu o dia 5 *de julho (e não temos um calendário em mãos, é claro). Primeiro precisamos ver quantos dias existem de* 1 *de janeiro até* 5 *de julho. Vejamos:*

$$\begin{aligned} Janeiro &= 31 \text{ dias} \\ Fevereiro &= 28 \text{ dias (2006 não é bissexto)} \\ Março &= 31 \text{ dias} \\ Abril &= 30 \text{ dias} \\ Maio &= 31 \text{ dias} \\ Junho &= 30 \text{ dias} \\ Julho &= 5 \text{ dias} \\ Total &= 186 \text{ dias.} \end{aligned} \tag{2.1}$$

Agora, é como se tivéssemos uma fila de 186 *dias e estamos desejando saber, na congruência de módulo* 7 *(*7 *dias da semana) qual o correspondente ao* 186*. Estamos diante de uma situação bem semelhante à que vimos no problema da aranha e também no problema dos relógios analógicos. Se dividirmos* 186 *por* 7*, teremos:*

$$\begin{array}{r|l} 186 & 7 \\ \hline (4) & 26 \end{array}$$

Logo, o 186 *é congruente ao* 4*, no módulo* 7*. Como o dia* 4 *de janeiro de* 2006 *foi uma quarta-feira, o* 186^o *desse mesmo ano também o será e, é claro, que todas as demais quarta-feiras deste ano serão ocupados por números congruentes ao* 4*, módulo* 7*.*

Assim, com os três exemplos que mostramos, podemos observar que em nosso cotidiano existem inúmeras situações onde se faz presente a noção de congruência, módulo k*. Calendários, relógios analógicos e problemas em geral envolvendo repetições periódicas. Mostraremos em nosso estudo que na criptografia e em diversos números de documentos de identificação (como no CPF, por exemplo), também está presente a Aritmética Modular e a noção de congruência.*

2.1.2 Sistemas de identificação

Em qualquer texto, um erro de ortografia numa palavra pode ser facilmente percebido, pois ou a palavra não faz parte do idioma ou não faz sentido com o contexto. Por exemplo, se digitamos engenheiro, logo percebemos que fizemos uma inversão das duas últimas letras. Mas, quando isso ocorre com os algarismos de um número, de um código de identificação qualquer, não teríamos como perceber a troca num simples olhar. Para isso e também para minimizar fraudes, foram criados os chamados dígitos de controle ou verificação. Tais dígitos são normalmente baseados na noção de congruência que mostramos anteriormente.

Mostraremos a seguir alguns desses casos de dígitos de controle usados como identificadores.

ISBN

Um dos exemplos mais antigos é o sistema International Standard Book Number (ISBN) de catalogação de livros, CD-Roms e publicações em braile, que foi criado em 1969. A necessidade que as editoras têm de catalogar os seus livros e informatizar o sistema de encomendas serviu de motivação na geração desse código.

A vantagem é que, por ser um código numérico, ultrapassa as dificuldades geradas pelos diversos idiomas do mundo, bem como a grande diversidade de alfabetos existentes. Dessa forma, poderíamos, por exemplo, identificar através do ISBN um livro japonês.

Em tal sistema, as publicações são identificadas através de 10 algarismos, sendo que o último (dígito de controle) é calculado através da aritmética modular envolvendo operações matemáticas com os outros nove dígitos. Esses nove primeiros dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

Por exemplo, a língua inglesa é identificada somente pelo algarismo 0 e a editora McGraw-Hill tem um código de 2 algarismos que a identifica, dessa forma, restam ainda 6 algarismos para a identificação de suas publicações, havendo pois a possibilidade de $10^6 = 1000000$ de títulos.

Vejamos como se processa o cálculo do dígito final do ISBN (controle).

Representando por $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ a sequência formada pelos 9 pri-

meiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser o menor valor possível, tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S + a_{10}$ deve ser múltiplo de 11, ou seja, $S + a_{10} \equiv 0 \bmod 11$.

Vejamos um exemplo:

Na contracapa do livro Temas e Problemas Elementares, da Coleção Professor de Matemática, da SBM, temos o seguinte código do ISBN: $85 - 85818 - 29 - 8$. Vejamos o cálculo do dígito de controle que, como estamos observando, é igual a 8.

$$\begin{array}{cccccccccc} 8 & 5 & 8 & 5 & 8 & 1 & 8 & 2 & 9 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \end{array}$$

Efetuando as multiplicações correspondentes e somando os produtos obtidos, teremos:

$$8.10 + 5.9 + 8.8 + 5.7 + 8.6 + 1.5 + 8.4 + 2.3 + 9.2 =$$

$$= 80 + 45 + 64 + 35 + 48 + 5 + 32 + 6 + 18 = 333$$

$$\begin{array}{r|l} 333 & 11 \\ \cline{2-2} (3) & 30 \end{array}$$

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, o menor valor que atende a tal condição será o número 8, pois $11 - 3 = 8$. O que confere o valor apresentado no código dado. Isso significa dizer que $333 + 8 = 341$ é um múltiplo de 11, ou ainda, que $341 \equiv 0 \bmod 11$.

Código de barras EAN-13

Um dos códigos de barras mais usados no mundo todo é o EAN-13, constituído de 13 algarismos, sendo que o último é o dígito de controle. Nesse caso é usada a congruência módulo 10 e os fatores que compõem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita. Se $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9, a_{10}, a_{11}, a_{12}$ a sequência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. Vamos representar por S a soma obtida. O dígito que está faltando, que vamos representar por a 13 deve ser tal que ao ser somado

com S, deve gerar um múltiplo de 10, isto é, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \bmod 10$.

Vejamos um exemplo:

Numa embalagem de uma garrafa para bebidas, de Portugal, temos o seguinte código de barras:

Figura 2.3: Código de barras

Vamos efetuar os cálculos para a determinação do dígito de controle (que estamos vendo ser o dígito 7).

8	4	2	4	9	0	6	2	0	1	7	6
1	3	1	3	1	3	1	3	1	3	1	3 esta é a base de multiplicação nesse caso.

Efetuando os produtos, teremos: $8+12+2+12+9+0+6+6+0+3+7+18 = 83$

$$\begin{array}{r|l} 83 & 10 \\ \hline (3) & 8 \end{array}$$

Logo, o dígito de controle será igual a $7(10-3)$. Note que $83+7 = 90$ (múltiplo de 10)

Sabemos também que, no código de barras com 13 algarismos, os três primeiros dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos $7, 8$ e 9); os quatro dígitos seguintes identificam o fabricante; os próximos cinco dígitos identificam o produto e o último, como já sabemos, é o dígito verificador ou de controle, que se pode calcular através da congruência, módulo 10.

Cadastro das Pessoas Físicas na Receita Federal/CPF

Outro exemplo importante, do nosso cotidiano: Verificação dos dois dígitos de controle do CPF de uma pessoa:

O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como no ISBN e nos códigos de barra, dígitos de controle ou de verificação . A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência.

No caso do CPF, o décimo dígito (que é o primeiro dígito verificador) é o resultado de uma congruência, módulo 11 de um número obtido por uma operação dos primeiros nove algarismos.

Se $a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8, a_9$ é a sequência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base 1, 2, 3, 4, 5, 6, 7, 8, 9 e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a 10 deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S, o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \bmod 11$. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Por exemplo, se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira: Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

$$\begin{array}{ccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

Efetuando as multiplicações correspondentes, teremos: $2 \times 1 + 3 \times 2 + 5 \times 3 + 3 \times 4 + 4 \times 5 + 3 \times 6 + 1 \times 7 + 0 \times 8 + 4 \times 9 = 116$. Dividindo o número 116 por 11, teremos:

$$\begin{array}{r|l} 116 & 11 \\ \cline{2-2} (10) & 6 \end{array}$$

Dessa forma, o primeiro dígito de controle será o algarismo 6.

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

Vejamos:

$$\begin{array}{cccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

Efetuando as multiplicações, teremos: $2 \times 0 + 3 \times 1 + 5 \times 2 + 3 \times 3 + 4 \times 4 + 3 \times 5 + 1 \times 6 + 0 \times 7 + 4 \times 8 + 6 \times 9 = 145$

Dividindo o número 145 por 11, teremos:

$$\begin{array}{r|l} 145 & 11 \\ \hline (2) & 13 \end{array}$$

Logo, o segundo dígito de controle é o 2.

Concluímos então que, no nosso exemplo, o CPF completo seria: 23534310462

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

2.2 Congruência e Criptografia

A **Criptografia** (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é a ciência que oculta o significado de uma mensagem e tem como ferramenta os recursos matemáticos para cifrar e decifrar mensagens. O ato de cifrar consiste em transformar um texto normal em texto secreto,e o ato de decodificar é a operação inversa, consiste em transformar um texto cifrado em texto normal. Veremos conceitos históricos da criptografia, suas definições e aplicações matemáticas.

Uma informação não-cifrada que é enviada de uma pessoa (ou organização) para outra é chamada de texto claro (plaintext). Cifragem é o processo de conversão de um texto claro para um código cifrado e decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado. De fato, o estudo da criptografia cobre bem mais do que apenas cifragem e decifragem. É um ramo especializado da teoria da informação com muitas contribuições de outros campos da matemática e do conhecimento. A criptografia moderna é basicamente formada pelo estudo dos algoritmos criptográficos que podem ser implementados em computadores.

Sabe-se que a primeira aplicação de criptografia foi inventada pelo imperador romano Júlio César, que enviava mensagens aos seus generais trocando letras do alfabeto a partir de uma simples regra, similar à que exemplificamos acima, que

seria "pule três"(chave 3). Através deste esquema, as letras eram trocadas pela terceira letra anterior no alfabeto. Desta forma, somente quem soubesse da regra conseguia desfazer o algoritmo e ler a mensagem original. Veja como funcionava essa chave 3, de Júlio César:

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

Ou seja, uma palavra simples como ***atacar*** seria codificada como "xqxzxo". Este sistema e outros similares, obtidos através de permutações, em que as letras são "embaralhadas", são muito simples e, não difíceis de serem "decifrados", mas por muito tempo serviram para esconder mensagens. Vejamos um exemplo mais completo e a relação que tem com a aritmética modular:

Exemplo 2.4

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
n	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
14	*15*	*16*	*17*	*18*	*19*	*20*	*21*	*22*	*23*	*24*	*25*	*26*

Chave: somar 4

Cada letra fica representada por um número que representa a sua posição no alfabeto. Com essa chave, ela fica substituída pela letra cujo número corresponde ao número original, aumentado de 4*. Quando acontecer do resultado ser superior ao* 26*, voltamos ao início do alfabeto. Por exemplo, o número* 28 *corresponderá à letra b, pois* $28 = 26 + 2$ *e, como já sabemos* $28 \equiv 2 \bmod 26$*.*

Atividades como essa, aplicadas nas classes do Ensino Fundamental, levarão os alunos a perceber que, na tradução da mensagem enviada eles terão, que aplicar a operação inversa da que foi usada pelo emissor da mensagem, na criação da mensagem criptografada.

No Ensino Médio poderia representar cada chave por uma função bijetora (para que tivesse inversa) e o receptor da mensagem criptografada teria que obter a função inversa, para traduzir a mensagem recebida.

Ainda no Ensino Médio a chave poderia ser representada por matrizes inversíveis e a decodificação pelo receptor seria através da matriz inversa.

Exemplo 2.5 *Através da chave dada como exemplo (somar* 4 *ou* $y = x + 4$*), se a mensagem a ser enviada fosse* $CIDADE\ MARAVILHOSA$*, o grupo emissor teria que criptografá-la como:* $GMHEHI\ QEVEZMPLSWE$.

O grupo receptor da mensagem, sabendo que a chave foi somar 4*, teria agora que subtrair* 4 *unidades dos números que representam cada letra da mensagem criptografada, para obter a mensagem original, decifrando o código. Vejamos:*

G	$7\text{-}4=3=\boldsymbol{C}$	Q	$17\text{-}4=13=\boldsymbol{M}$
M	$13\text{-}4=9=\boldsymbol{I}$	E	$5\text{-}4=1=\boldsymbol{A}$
H	$8\text{-}4=4=\boldsymbol{D}$	V	$22\text{-}4=18=\boldsymbol{R}$
E	$5\text{-}4=1=\boldsymbol{A}$	E	$=\boldsymbol{A}$
H	$=\boldsymbol{D}$	Z	$26\text{-}4=22=\boldsymbol{V}$
I	$9\text{-}4=5=\boldsymbol{E}$	M	$13\text{-}4=9=\boldsymbol{I}$
		P	$16\text{-}4=12=\boldsymbol{L}$
		L	$12\text{-}4=8=\boldsymbol{H}$
		S	$19\text{-}4=15=\boldsymbol{O}$
		W	$23\text{-}4=19=\boldsymbol{S}$
		E	$=\boldsymbol{A}$

Durante a segunda guerra mundial sistemas eletromecânicos na codificação e decodificação das mensagens foram muito usados. Nestes dispositivos, rotores incorporavam internamente uma permutação e sua instalação em mecanismos parecidos com "counters"(ou contadores) permitiam transformações polialfabéticas produzindo uma quantidade impressionante de combinações.

Graças aos mais de sete mil ingleses que trabalharam no famoso Quartel General das Comunicações Governamentais ("Government Communications Headquarters") em "Bletchey Park", os códigos alemães foram quebrados. Eles tratavam em torno de quatro mil sinais alemães por dia e, secretamente, mantinham os comandos britânico e americano muito bem informados.

Ainda durante a guerra computadores (como o "Colossus") foram usados na "quebra"de códigos alemães, italianos e japoneses e, desde então, a Criptografia passou a ser estudada de forma mais científica. Depois da Segunda Guerra Mundial, com o desenvolvimento dos computadores, a área realmente floresceu incorporando complexos algoritmos matemáticos. Na verdade, esse trabalho criptográfico formou

a base para a ciência da computação moderna.

2.2.1 Aritmética modular na criptografia

Na criptografia usam-se chaves que, de certa forma, são análogas à estratégia usada pelos namorados de nossa história.

Esta história relata a velha charada do sigilo nas comunicações e uma de suas brilhantes soluções. Talvez tenha servido de inspiração para os três jovens norte-americanos, Whitefield Diffie, Martin Hellman e Ralph Merkle, ao construirem em 1976 um sistema de criptografia em que o segredo da comunicação é assegurado por duas chaves, que os comunicantes não precisam trocar entre si, como aconteceu na historinha do Bob e da Alice. Foi esta invenção que inspirou o sistema de criptografia RSA.

Chamaremos por João e Maria os personagens fictícios, mas são nomes sistematicamente utilizados pelos especialistas de criptografia. É mais interessante do que falar apenas no emissor e receptor, ou apenas em A e B. Costuma-se acrescentar a eles uma terceira personagem, que costuma receber o nome de Eva - Eve, em inglês e que representa aquela que se põe à escuta, ou seja, aquela que "eavesdrop".

Até à descoberta de Diffie, Hellman e Merkle, a comunicação de mensagens cifradas exigia uma troca da chave da cifra, como fizemos nas atividades anteriores e como era feito nas chaves de Júlio César. Era preciso que João e Maria se encontrassem previamente e combinassem uma chave que apenas eles dois conhecessem. Só isso lhes permitiria, posteriormente, trocar mensagens à distância sem que Eva, sempre à escuta, conseguisse percebê-las. Assim funcionaram as mensagens secretas desde os tempos de César até aos tempos modernos, assim funcionaram espiões, conspiradores e simples amantes. A chave poderia ser simples, mas era sempre necessário que João e Maria combinassem tudo antes, e nem sempre isso era possível.

A ideia de Diffie, Hellman e Merkle é pois revolucionária. Segundo o esquema que propuseram, João e Maria começam por acordar em dois números. E estes podem ser públicos, pois mesmo que Eva os consiga descobrir não terá como descobrir a chave do processo. Cada um deles escolhe um outro número, que mantém secreto. Feitas algumas contas, baseadas em aritmética modular,ambos chegam a um mesmo resultado: um número que mais ninguém conhece e que será a chave de codificação

das suas mensagens. O processo que inventaram é relativamente simples, embora muito engenhoso, e será mostrado no quadro abaixo. Tudo se passa de forma parecida com a da história dos dois cadeados. As chaves não são trocadas, mas cada um acaba por poder abrir o cofre, sem que o carteiro, o consiga.

O processo inventado por Diffie, Hellman e Merkle marca o nascimento da criptografia com chaves públicas, que funcionam em conjunto com chaves secretas que não precisam ser "trocadas". Baseia-se na aritmética modular, que consiste, essencialmente, em trabalhar com os restos da divisão inteira por um número determinado, chamado módulo. Esse processo foi denominado de congruência, módulo k, pelo famoso gênio da Matemática Gauss.

Simon Singh , no seu "Livro dos Códigos", dá um exemplo que retrata bem o processo matemático da aritmética modular, envolvido nessas chaves públicas. Os comunicantes, como João e Maria combinam nos números que servem: o primeiro de base para uma potenciação e o segundo para o módulo da congruência. Digamos que tenham optado pelos números 5 e 11. Estariam então se referindo ao cálculo de 5^x e da congruência no módulo 11.

(O expoente x seria secreto, à escolha de cada um deles).

Maria escolhe 3 para seu número secreto (expoente da potência) Maria calcula $5^3 = 125$ e, através de congruência módulo 11, gera o número 4, pois 125 dividido por 11 deixa resto 4.

Maria envia o resultado, 4, para João. João escolhe 6 para seu número secreto (novamente o expoente da potência) João calcula $5^6 = 15625$ e, através de congruência módulo 11, gera o número 5, pois 15625 dividido por 11 deixa resto 5.
João envia o resultado, 5, para Maria

Note que, mesmo que esses dois números que eles enviaram um ao outro, fossem interceptados, as pessoas não teriam como saber a chave final do processo. Maria pega o resultado de João, 5, e o seu número secreto, 3, e calcula $5^3 = 125 \equiv 4 \bmod 11$. 125 dividido por 11 deixa resto 4.

João pega o resultado de Maria, 4, e o seu número secreto, 6, e calcula $4^6 = 4096 \equiv 4 \bmod 11$. 4096 dividido por 11 também deixa resto 4.

Veja que João e Maria encontraram o mesmo número, 4, sem que tivessem informado um ao outro os seus números secretos pessoais. Esse número seria agora

usado como chave para a composição das mensagens criptográficas.

É através da criptografia que, diariamente, através da internet, uma luta sempre se processa: a de enviar dados e a de tentar captar esses dados (são os famigerados hackers). É claro que o tema criptografia é muito mais complexo do que mostramos aqui. O que exemplificamos, através de chaves criptográficas simples, foi para mostrar a relação que existe entre esse tema e a aritmética modular. É um assunto bastante atual, interessante, e que pode ser usado em classes da Educação Básica, relacionado a conceitos importantes da Matemática, como Operações Inversas, divisibilidade e Funções.

2.2.2 Criptografia e calendários

Nosso calendário, o calendário Gregoriano, vem desde a segunda metade do século XVI. O calendário anterior, introduzido por Júlio César, foi baseado em um ano de $365\frac{1}{4}$ de dias, com um ano bissexto de 4 em 4 anos. Esta não foi uma medida precisa porque o ano solar é de aproximadamente $365,2422$ dias. Este pequeno erro fazia com que o calendário de César pulasse um dia a cada 128 anos.

Por volta do século XVI, o erro acumulado fez com que o 1º dia da primavera caísse dia 11 de março em vez do dia correto, 21 de março. O papa Gregório XIII corrigiu essa discrepância em um novo calendário, imposto nos principais países católicos da Europa. Foi decretado que 10 dias seriam omitidos no ano de 1582, fazendo com que 15 de outubro viesse logo depois de 4 de outubro daquele ano. Os anos bissextos seriam os anos divisíveis por 4, exceto aqueles que fosse anos centenários. Anos centenários só seriam bissextos se fossem divisíveis por 400.

Apresentaremos aqui uma das maneiras, acompanhada de sua justificativa matemática, envolvendo a aritmética modular (congruência módulo 7), aplicada aos calendários.

Vejamos a regra prática, alguns exemplos e, finalmente, a explicação. O procedimento que escolhemos funciona para datas entre 1900 e 2399 (devido a uma particularidade dos anos bissextos terminados em "00"). Com algumas modificações, contudo, pode ser adaptado para atender quaisquer datas.

1. Calcule quantos anos se passaram desde 1900 até o ano em que você nasceu. Por exemplo, se você nasceu em 1980, irá anotar 80. Vamos chamar essa

quantidade de A.

2. Calcule quantos 29 de fevereiro existiram depois de 1900. Para isso, basta dividir por 4 o valor A, sem considerar o resto da divisão. Vamos chamar essa nova quantidade de B.

3. Considerando o mês do nascimento, obtenha o número associado a ele, que está na tabela logo abaixo. Procure o mês e anote o número que está ao lado dele. Vamos chamar esse número de C.

Tabela dos meses			
Janeiro	0	Julho	6
Fevereiro	3	Agosto	2
Março	3	Setembro	5
Abril	6	Outubro	0
Maio	1	Novembro	3
Junho	4	Dezembro	5

4. Considere o dia do nascimento (x). Calcule $x - 1$, que vamos chamar de D.

5. Some agora os quatro números que você obteve nas etapas anteriores ($A+B+C+D$). Divida essa soma obtida por sete (7) e verifique o valor do resto dessa divisão.

6. Finalmente, procure esse resto na tabela a seguir. Você terá o dia da semana do seu nascimento ou de qualquer outra pessoa que queira descobrir.

Exemplo 2.6 *Vamos imaginar uma pessoa que tenha nascido em* 16 *de fevereiro de* 1918. *Qual foi o dia da semana que essa pessoa nasceu?*

1. $(1918 - 1900) = 18$, logo, $A = 18$

2. $18 \div 4 = 4$ (desconsidere o resto), logo, $B = 4$

3. O mês é Fevereiro, então $C = 3$ (ver na tabela)

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

4. $x = 16$ (dia do nascimento), logo, $D = (x - 1) = 16 - 1 = 15$

5. Somando os quatro números, teremos $18 + 4 + 3 + 15 = 40$

6. $40 \div 7 = 5$ e resto 5. Como o resto da divisão foi 5, na tabela o 5 é um SÁBADO.

Justificativa Matemática

Fato 1 O algoritmo que foi montado partiu do fato de que o dia 1º de janeiro de 1900 foi uma segunda-feira (0, na tabela). Todos os passos que foram colocados na regra prática visam determinar o "deslocamento", na sequência de dias da semana, que a data procurada tem em relação àquela segunda-feira, 01/01/1900, que é nosso "ponto de partida".

Fato 2 Cada ano de 365 dias vê seu primeiro de janeiro "afastado" de uma posição para a direita no ciclo dos dias da semana (segunda, terça, quarta, quinta, sexta, sábado, domingo, segunda, etc.) em relação ao dia-da-semana em que caiu o primeiro de janeiro do ano anterior. Isto porque 365 dividido por 7 deixa resto 1. Quando a pessoa faz a diferença entre o ano de seu nascimento e o ano 1900, está descobrindo quantos "afastamentos", ou deslocamentos, essa data primeira sofreu em relação àquele 01/01/1900. Quando descobrimos, na fase seguinte, a quantidade de anos bissextos (ao dividir o resultado anterior por 4), estamos acrescentando o deslocamento adicional de mais uma "casa", no ciclo de dias da semana, para cada ano bissexto considerado. Isto porque os anos bissextos afastam o primeiro de janeiro do ano seguinte não em 1 "casa", mas em 2, já que 366 deixa resto 2 quando dividido por 7.

Os dois primeiros passos do processo serviram apenas para localizar o dia 1º de janeiro do ano considerado, ou seja, até aqui apenas o ANO da data desejada foi considerado. Agora é a vez de acrescentarmos os deslocamentos gerados pelo mês e pelo dia da data procurada.

Fato 3 Se todos os meses do ano tivessem 28 dias (que gera resto zero ao ser dividido por 7), todos os meses teriam o seu dia primeiro exatamente no mesmo dia da semana que o primeiro de janeiro do ano considerado. Mas como temos meses com mais de 28 dias, todos esses meses (transcorridos de janeiro até o mês considerado) "empurram" o seu dia primeiro um certo número de "casas" adiante no ciclo dos dias da semana. A tabela criada para o nosso algoritmo está relacionada à aritmética modular, ou seja, à congruência módulo 7. Vejamos como surgiram os números da tabela.

Janeiro é a nossa referência, logo não há qualquer afastamento em relação a ele próprio (não há qualquer mês antes dele, empurrando seu dia primeiro para a direita, no ciclo, em relação ao próprio 1º de janeiro do ano em questão). Por isso, na tabela dada, ao lado do mês de janeiro, temos o número zero.

Como o mês de **janeiro** tem 31 dias e 31 dividido por 7 deixa resto 3, esse mês vai "empurrar" o primeiro dia do mês seguinte 3 "casas" para a direita em relação ao primeiro de janeiro daquele ano. Por isso, o mês de **fevereiro** recebe o número 3 na tabela.

Como fevereiro tem 28 dias e 28 dividido por 7 deixa resto 0, esse mês não irá acrescentar qualquer "deslocamento" adicional ao mês seguinte. Logo, o primeiro dia do mês de março cairá no mesmo dia da semana que o primeiro de fevereiro daquele ano, ou seja, será deslocado apenas das mesmas 3 "casas" para a direita, em relação ao primeiro de janeiro daquele ano. Por isso, na tabela dada, o mês de **março** também tem o número 3.

Como **março** tem 31 dias e 31 dividido por 7 deixa resto 3, esse mês vai "empurrar" os dias do mês seguinte um total de $(3 + 0 + 3)$ "casas" para a direita, já que como num dominó em cascata, esses deslocamentos são cumulativos. Por isso na tabela, o mês de **abril** tem o número 6.

Como **abril** tem 30 dias e 30 dividido por 7 deixa resto 2, esse mês vai "empurrar" os dias do mês seguinte um total de $(3 + 0 + 3 + 2)$ "casas", mas como a semana só

tem 7 dias, na congruência módulo 7 o número 8 corresponde ao 1 ($8 \div 7 = 1$ e resto 1). Isto é, avançar oito "casas" no ciclo de dias da semana é o mesmo que avançar uma "casa" apenas. Por isso o mês de **maio** na tabela tem o número 1.

Assim por diante, justificam-se facilmente os números que estão ao lado dos outros meses.

Os passos que demos até aqui determinaram a quantidade de "casas" em que o primeiro dia do mês da data considerada está adiante, no ciclo dos dias da semana, do dia primeiro de janeiro de 1900. Precisamos agora, para finalizar, determinar a quantidade de deslocamentos necessários para atingirmos o exato dia procurado. Ora, se localizamos o dia 1 e queremos localizar o dia x de um determinado mês, precisamos ainda de um deslocamento correspondente a $(x - 1)$ "passos".
Veja, por exemplo, se a data procurada fosse o dia 4 de um determinado mês, teríamos ainda mais $3 = 4 - 1$ deslocamentos à direita no ciclo de dias da semana. Se o dia primeiro daquele mês caiu numa terça-feira, por exemplo, o dia 4 cairá numa sexta-feira (que está, evidentemente, 3 "casas" adiante de terça-feira, no ciclo).

É claro que a soma dos quatro números obtidos nas etapas do processo terá sempre de ser dividida por 7, pois são sete os dias da semana e o ciclo se repete sempre. Essa atividade, ou brincadeira, ou truque é um outro exemplo interessante da nossa congruência módulo k, que nesse caso é igual a 7.

2.2.3 O algoritmo RSA

RSA é um algoritmo de criptografia de dados, que deve o seu nome a três professores do Instituto de Tecnologia de Massachusetts (MIT), Ronald Rivest, Adi Shamir e Leonard Adleman, fundadores da actual empresa RSA Data Security, Inc., que inventaram este algoritmo - até a data (2008) a mais bem sucedida implementação de sistemas de chaves assimétricas, e fundamenta-se em teorias clássicas dos números. É considerado dos mais seguros, já que mandou por terra todas as tentativas de quebrá-lo. Foi também o primeiro algoritmo a possibilitar criptografia e assinatura digital, e uma das grandes inovações em criptografia de chave pública

O RSA envolve um par de chaves, uma chave pública que pode ser conhecida por todos e uma chave privada que deve ser mantida em sigilo. Toda mensagem cifrada usando uma chave pública só pode ser decifrada usando a respectiva chave

privada. A criptografia RSA atua diretamente na internet, por exemplo, em mensagens de emails, em compras on-line e o que você imaginar; tudo isso é codificado e recodificado pela criptografia RSA.

Os impactos da RSA são fortes na matemática, e, em contrapartida, o desenvolvimento da cifra só foi permitido por conta de grandes avanços na teoria aritmética dos números. Pesquisas na área de codificação devem envolver a garantia da aleatoriedade dos blocos e dos números primos na implementação do sistema de cifragem. Já no ramo de decodificação, o melhor rumo a se tomar é tentar fatorar o número n de maneira eficiente. Entretanto, repetimos que este problema já foi exaustivamente atacado por matemáticos de todo o mundo, desde muito tempo, e até hoje não aparenta ter alguma solução.

O primeiro passo para se começar a cifrar uma mensagem pelo sistema RSA é transformar a mensagem em um número, e isso é feito através do padrão ASCII [tabela disponível em http://www.asciitable.com]. Por exemplo, a mensagem *teorema de fermat*, convertida em código ASCII, sem os espaços, ficaria:

$$116101111114101109971001011021011141099711 6$$

Em segundo lugar, deve-se quebrar a mensagem em blocos relativamente pequenos. O tamanho máximo dos blocos será esclarecido na subseção seguinte, em que determinaremos os parâmetros de cifragem da RSA. Os blocos devem ser escolhidos aleatoriamente, tomando-se alguns cuidados, para que não seja permitida a técnica de análise de frequência na tentativa de quebra do código.

Codificação e decodificação

Os parâmetros de entrada para a cifragem pelo método RSA são dois primos p e q suficientemente grandes, sobre os quais se calculará um número $n = pq$ e $\phi(n) = (p-1)(q-1)$. Além disso, é necessário gerar aleatoriamente um número e tal que $(e, (p-1)(q-1)) = 1$, ou seja, e e $\phi(n)$ são primos entre si. Definamos $C(b)$ como o bloco b codificado e $D(a)$ como o bloco a decodificado (utilizaremos esta notação sempre, daqui para frente). Vejamos quais propriedades devemos esperar de um bom algoritmo de cifragem.

Em primeiro lugar, é claro que queremos que $D(C(b)) = b$ sempre, ou seja, que a decifragem de um bloco pelo algoritmo sempre produza o mesmo bloco cifrado.

Utilizando jargão matemático, queremos a unicidade de decifragem. Em segundo, é importante que seja difícil obter a função $D(a)$ a partir de $C(b)$, o que quer dizer que um interceptador terá dificuldades em decifrar a mensagem. O conceito de difícil é, de fato, muito abstrato, mas do ponto de vista da RSA, ele está intimamente relacionado com os esforços computacionais para quebrar a cifra, considerando as condições necessárias e suficientes para a decifragem.

No sentido da RSA, as fórmulas de codificação e decodificação são:

$$C(b) \equiv b^e \bmod n, 0 < C(b) < n$$
$$D(a) \equiv a^d \bmod n, 0 < D(a) < n$$

sendo a um bloco codificado e b um bloco da mensagem original e d é o inverso de e módulo $\phi(n)$.
Devemos, portanto, demonstrar o seguinte:

Teorema 2.1 $D(C(b)) = b$.

Demonstração: $D(C(b)) \equiv C(b)^d \equiv b^{ed} \bmod n$. Mas, como d é inverso de e módulo $\phi(n)$, $ed = 1 + k\phi(n)$. Daí, segue que $D(C(b)) \equiv b^{1+k\phi(n)} \equiv (b^{\phi(n)})^k b \bmod n$. Como $n = pq$, temos que $\phi(n) = (p-1)(q-1)$ o que implica que $D(C(b)) \equiv (b^{p-1})^{(q-1)k} b \bmod p$. Se p não divide b, então

$$D(C(b)) \equiv b \bmod p$$

pelo Pequeno Teorema de Fermat. Se p divide b, então $b \equiv 0 \bmod n$, ou seja, $D(C(b)) = (b^{p-1})^{(q-1)k} b \equiv 0 \bmod p$. Analogamente, é possível mostrar que $D(C(b)) \equiv b \bmod q$ e como p e q são primos,

$$D(C(b)) \equiv b \bmod n$$

e o teorema está quase demonstrado, a menos da igualdade. O fato de que $D(a)$ é sempre menor que n nos diz que a congruência implica na igualdade a menos que $b = n$. Entretanto, podemos escolher b de qualquer maneira conveniente (e aqui estabelecemos o tamanho de cada bloco!). A demonstração está completa.

■

Com este teorema, temos a segurança de que o método RSA é um bom método de cifragem e decifragem, do ponto de vista da primeira propriedade listada acima. Mas por que ele é tão seguro?

Sistema de chave pública

Antes de responder a essa pergunta, entretanto, vamos discutir um pouco mais sobre o sistema de codificação da RSA. Como entrada, ele exige dois números primos e um terceiro número, e. Os parâmetros para codificar uma mensagem são os números n e e e por isso chamamos o par (n, e) de chave de codificação. Para decifrar, necessitamos apenas de (n, d) (é importante notar que d depende intimamente dos fatores, em separado, p e q).

Por razões que citaremos a seguir, é difícil obter o par de decodificação a partir apenas do par de codificação e, portanto, poderemos considerar (n, e) como parâmetros públicos (que podem ser divulgados em qualquer lugar, indiscriminadamente) e d como um parâmetro privado, assim como p e q.

Desta análise, segue que a RSA é um sistema de cifragem de chave pública, pois qualquer um pode ter acesso aos parâmetros de codificação sem comprometer o processo.

2.2.4 Segurança e aplicações

Primeiramente, vamos considerar que todos os blocos da mensagem original foram separados de maneira aleatória, ou seja, a análise de frequência é impossível, já que os blocos não possuem um padrão entre si (por exemplo, se cada bloco representasse exatamente duas letras da mensagem seria possível considerar uma técnica de análise de frequência baseada no aparecimento de dígrafos em diversas línguas).

Fatoração de inteiros

Levando em consideração o que foi dito acima, a segurança da RSA se baseia, basicamente, no seguinte:

Teorema 2.2 *Uma condição necessária e suficiente para se decodificar uma mensagem conhecendo-se apenas $\underline{e}$ e $\underline{n}$, no sentido visto anteriormente, é fatorar o número n.*

Este teorema significa, grosso modo, que, se é possível quebrar a RSA, então há um jeito eficiente de se fatorar um número em primos (ou, no mínimo, um número que é composto por dois primos), já que os números p e q podem ser arbitrariamente

grandes, e, em contrapartida, se há um bom algoritmo para fatoração, então a RSA pode ser quebrada. Entretanto, até hoje não há um algoritmo de fatoração tão eficiente de modo que a RSA possa ser quebrada em tempo razoável. Mais que isso: é possível que não exista tal algoritmo! Portanto, de acordo com o teorema acima, a segurança do sistema de cifragem RSA está garantida!.

Demonstração: A condição suficiente é facilmente demonstrada já que, se fatoramos n, então podemos encontrar $\phi(n)$ e utilizar as operações vistas anteriormente para decifrar a mensagem. A condição necessária não é trivial, mas podemos esboçar alguns casos, como por exemplo, se for inventado um algoritmo eficiente para se calcular $\phi(n)$ a partir de d e e, então:

$$\phi(n) = (p-1)(q-1) = pq - p - q + 1 = n - (p+q) + 1,$$

portanto,

$$p + q = n + 1 - \phi(n)$$

Em contrapartida, temos que

$$(p+q)^2 - 4n = p^2 + 2pq + q^2 - 4n = p^2 + q^2 - 2pq = (p-q)^2$$

logo

$$p - q = \sqrt{(n+1-\phi(n))^2 - 4n}$$

e destas duas equações segue que

$$p = \frac{\sqrt{(n+1-\phi(n))^2 - 4n} + n + 1 - \phi(n)}{2}$$

e

$$q = \frac{-\sqrt{(n+1-\phi(n))^2 - 4n} + n + 1 - \phi(n)}{2}$$

Em resumo o número n foi fatorado

■

Assinaturas digitais

Um dos impactos da criação da RSA acaba de ser enunciado acima e diz respeito ao antigo problema da fatoração de números primos. Citaremos aqui uma importante aplicação prática, que segue como um resultado imediato da RSA: a assinatura digital.

O problema da assinatura digital consiste em ter certeza de quem é o destinatário de uma mensagem, e é bastante relevante principalmente nas relações entre bancos e empresas, pois tanto o banco deve ter confiabilidade de que é o seu cliente que está enviando uma ordem, quanto a empresa deve ter certeza que ninguém está tentando se passar por ela.

Suponhamos, para resolver o problema, que Maria queira manda uma mensagem para João. Sejam C_a, D_a, C_b e D_b as funções de codificação e decodificação para Maria e João, respectivamente e seja m a mensagem original. A sequência de operações que Maria deve fazer é: aplicar $D_a(m)$ (função que só é conhecida por ela, pois se trata dos parâmetros privados da cifra) e, em seguida, aplicar $C_b(D_a(m))$. Ao receber a mensagem, João deve decifrar, fazendo $D_b(C_b(D_a(m)))$ e conseguindo $D_a(m)$. Logo depois, ele deve utilizar a cifra pública de Maria para recuperar a mensagem original, pois $C_a(D_a(m)) = m$. Se a mensagem obtida fizer sentido, então a probabilidade de ela ter sido enviada por Maria é quase 1, pois ela é a única que conhece a função D_a. Assim, temos um sistema de assinaturas seguro!

2.3 Lista de problemas motivadores e soluções

2.3.1 Problema 1

Uma tripla pitagórica (x, y, z) é um triplo de naturais tais que $x^2 + y^2 = z^2$. Uma tripla pitagórica diz-se primitiva se $mdc(x, y, z) = 1$.

a) Mostrar que se $n > m > 0$ são naturais primos entre si, em que um é par e o outro é ímpar, então $(n^2-m^2, 2nm, n^2+m^2)$ é uma tripla pitagórica. primitiva

b) Mostrar que se (x, y, z) é uma tripla pitagórica primitiva, então um entre x e y é par e o outro, bem como z, é ímpar.

c) Suponhamos que $y = 2k$ é o termo par; deduzir que

$$k^2 = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right)$$

e que os fatores do lado direito são inteiros primos entre si.

d) Deduzir que cada um daqueles dois fatores é um quadrado perfeito e concluir que todas as triplas pitagóricas primitivas (a menos de uma troca entre x e y) são da forma dada na ítem a).

Resolução:

a) Que aqueles três inteiros positivos são uma tripla pitagórica decorre de um cálculo simples:

$$(n^2 - m^2)^2 + (2nm)^2 = n^4 - 2n^2m^2 + m^4 + 4n^2m^2 = (n^2 + m^2)^2$$

Um primo p que seja fator comum dos três elementos da tripla $(n^2-m^2, 2nm, n^2+m^2)$ tem que ser ímpar, porque divide os ímpares $n^2 - m^2$ e $n^2 + m^2$; e terá também que dividir a sua soma $2n^2$ e diferença $2m^2$; mas então tem que dividir n e m, contradizendo a hipótese de estes serem primos entre si.

b) Se x e y fossem ambos pares, também z seria par e a tripla não seria primitiva; suponhamos que $x = 2t + 1$ e $y = 2s + 1$ são ímpares (e portanto $z = 2u$ é par); então por um lado

$$z^2 = (2u)^2 = 4u^2 \equiv 0 \bmod 4$$

e por outro

$$z^2 = x^2 + y^2 = (2t + 1)^2 + (2s + 1)^2 = 4t^2 + 4t + 1 + 4s^2 + 4s + 1 \equiv 2 \bmod 4$$

conduzindo a uma contradição.

c) Se $y = 2k$,

$$4k^2 = y^2 = z^2 - x^2 = (z - x)(z + x)$$

e, portanto,

$$k^2 = \frac{z - x}{2}\frac{z + x}{2}$$

Como x e z são ímpares, $z - x$ e $z + x$ são pares e, portanto, os dois fatores do lado direito da última igualdade são inteiros; se eles tivesse um fator primo comum p, ele dividiria também a soma z e a diferença x; além disso teríamos que $p^2|k^2$ e, portanto, $p|k$ e $p|y$, contradizendo o fato de (x, y, z) ser uma tripla pitagórica

d) Sejam

$$\frac{z-x}{2} = \prod_i p_i^{l_i}, \qquad \frac{z+x}{2} = \prod_i p_i^{j_i}, \qquad k = \prod_i p_i^{h_i}$$

as fatorações em fatores primos com expoentes $l_i, j_i, h_i \geq 0$ para todo o i; como os dois primeiros inteiros são primos entre si, sabemos que $j_i > 0 \Leftrightarrow l_i = 0$; se p_i divide, por exemplo, $\frac{z-x}{2}$ temos que l_i é o expoente de p_i em k^2 que é igual a $2h_i$ e portanto par; o mesmo se passa para os expoentes não nulos na fatoração de $\frac{z+x}{2}$. Concluímos que todos os expoentes na fatoração em fatores primos de $\frac{z-x}{2}$ e de $\frac{z+x}{2}$ são pares e portanto estes inteiros são quadrados perfeitos

$$\frac{z-x}{2} = m^2, \qquad \frac{z+x}{2} = n^2$$

Temos então $k = mn$ e

$$x = n^2 - m^2, \qquad y = 2mn, \qquad z = n^2 + m^2.$$

Além disso, m e n têm que ter paridade diferente, porque x e z são ímpares, e são primos entre si porque, caso contrário, x, y e z teriam um fator comum.

2.3.2 Problema 2

Ao tentar formar grupos de trabalho numa turma, conclui-se que se os grupos tiverem 3 elementos ficam dois alunos de fora, se tiverem quatro fica 1 de fora, mas que se consegue formar grupos de 5 elementos desde que o professor faça parte de um deles. Quantos alunos terá a turma?

Resolução O problema corresponde à resolução do sistema de congruências

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 1 \bmod 4 \\ x \equiv 4 \bmod 5 \end{cases}$$

Como os módulos das congruências são primos dois a dois, o Teorema Chinês dos Restos garante a existência de uma solução única mod 120 (e é de esperar que o número de alunos de uma turma seja inferior a 120).

A primeira equação implica $x = 2 + 3k$; substituindo na segunda ficamos com

$$3k \equiv -1 \bmod 4 \Leftrightarrow k \equiv 1 \bmod 4$$

e, portanto,

$$k = 1 + 4j, \qquad x = 2 + 3(1 + 4j) = 5 + 12j$$

Substituindo na última equação

$$12j + 5 \equiv 4 \bmod 5 \Leftrightarrow 2j \equiv 4 \bmod 5 \Leftrightarrow j \equiv 2 \bmod 5$$

ou seja $j = 2 + 5t$ e, portanto, $x = 5 + 12(2 + 5t) = 29 + 120t$.

2.3.3 Problema 3

Determinar:

a) $0 \leq a < 73$ satisfazendo $a \equiv 9^{794} \bmod 73$.

b) $0 \leq a < 83$ satisfazendo $a \equiv 7^{670} \bmod 83$.

Resolução:

a) Como 73 é primo, sabemos pelo Teorema de Euler (ou mesmo pelo Teorema de Fermat) que $9^{72} \equiv 1 \bmod 73$. Portanto

$$9^{794} = 9^{11\times 72+2} = (9^{72})^{11}9^2$$

e

$$(9^{72})^{11}9^2 \equiv 9^2 \equiv 8 \bmod 73$$

b) Pode aplicar-se o mesmo método uma vez que também 83 é primo.

Como $670 = 8 \times 82 + 14$, somos conduzidos a calcular $7^{14} \bmod 83$, pelo que é boa ideia tentar simplificar os cálculos e não calcular todas as potências $7^2, 7^3, 7^4, \ldots, 7^{14}$ (mod 83 é claro). Uma forma passa por ver que $14 = 8+4+2$ e

$$7^2 = 49 \equiv -34, \qquad 7^3 \equiv 11, \qquad 7^4 \equiv 77 = -6$$

em que todas as congruências são mod83, e portanto $7^8 \equiv 36 \bmod 83$. Logo

$$7^14 = (-34) \times (-6) \times 36 \equiv 40 \bmod 83.$$

2.3.4 Problema 4

Determinar o menor inteiro positivo congruente com $2^{12500} + 5^{32}$ módulo 10^6.

Resolução

$$x \equiv 2^{12500} + 5^{32} \bmod 10^6$$

é equivalente, pelo Teorema Chinês dos Restos, a

$$\begin{cases} x \equiv 2^{12500} + 5^{32} \bmod 2^6 \\ x \equiv 2^{12500} + 5^{32} \bmod 5^6 \end{cases} \iff \begin{cases} x \equiv 5^{32} \bmod 2^6 \\ x \equiv 2^{12500} \bmod 5^6 \end{cases}$$

Pelo teorema de Euler, como $\phi(2^6) = 2^6 - 2^5 = 2^5 = 32$, $5^{32} \equiv 1 \bmod 2^6$. Do mesmo modo, como $\phi(5^6) = 5^6 - 5^5 = 5^5 \times 4 = 12500$, temos $2^{12500} \equiv 1 \bmod 5^5$. Portanto, $x = 1$ é a menor solução positiva de

$$x \equiv 2^{12500} + 5^{32} \bmod 10^6$$

2.3.5 Problema 5

Determinar as soluções da congruência

$$501x \equiv 345 \bmod 7 \cdot 8 \cdot 9$$

Resolução:

Pelo Teorema Chinês dos Restos as soluções da equação são as soluções do sistema

$$\begin{cases} 501x \equiv 345 \bmod 7 \\ 501x \equiv 345 \bmod 8 \\ 501x \equiv 345 \bmod 9 \end{cases} \iff \begin{cases} 4x \equiv 2 \bmod 7 \\ 5x \equiv 1 \bmod 8 \\ 6x \equiv 3 \bmod 9 \end{cases}$$

A primeira e segunda equações têm solução única enquanto que a terceira tem três soluções. Resolvendo a primeira equação

$$4x \equiv 2 \bmod 7 \Leftrightarrow x \equiv 4 \bmod 7$$

e portanto $x = 4 + 7y$; substituindo na segunda equação obtemos

$$5(4 + 7y) \equiv 1 \bmod 8 \Leftrightarrow 3y \equiv -3 \bmod 8$$

e portanto $y = -1 + 8z$, donde se conclui que $x = -3 + 56z$. Finalmente na última equação ficamos com

$$6(-3 + 56z) \equiv 3 \bmod 9 \Leftrightarrow 3z \equiv 3 \bmod 9$$

que tem as soluções $z \equiv 1 \bmod 9, z \equiv 4 \bmod 9$ e $z \equiv 7 \bmod 9$, ou seja $z \equiv 1 \bmod 3$. Substituindo os valores em x concluímos que a equação tem as soluções

$$53,\ 221,\ 389 \bmod 7 \cdot 8 \cdot 9$$

2.3.6 Problema 6

Qual é o algarismo das unidades de 7^{888} ? E o das dezenas?

Resolução

Queremos saber qual o inteiro $0 \leq x < 100$ tal que $x \equiv 7^{888} \bmod 100$. Usando o Teorema Chinês dos Restos, isso é equivalente a resolver

$$\begin{cases} x \equiv 7^{888} \bmod 4 \\ x \equiv 7^{888} \bmod 25 \end{cases}$$

Como $\phi(4) = 2$ e 7 é primo com 4, o Teorema de Euler implica que $7^2 \equiv 1 \bmod 4$ e, portanto,

$$7^{888} \equiv 1 \bmod 4$$

aplicando o mesmo à segunda equação, temos que $\phi(25) = 20$ e, portanto,

$$7^{888} = 7^{44 \times 20} 7^8 \equiv 7^8 \bmod 25$$

Mas $7^2 \equiv -1 \bmod 25$ e, portanto, $7^8 = 1 \bmod 25$. Em conclusão $7^{888} = 1 \bmod 100$ e, portanto, o algarismo das unidades é 1 e o das dezenas é 0.

2.3.7 Problema 7

Determinar a única solução da equação

$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \bmod 101$$

Resolução

Em primeiro lugar, $x \equiv 0 \bmod 101$ não é solução; portanto, como 101 é primo, podemos considerar apenas x primo com 101. Mas então $x^{100} \equiv 1 \bmod 101$ e a equação simplifica-se:

$$47x^{120} + 7x^{100} + 54x^{20} + 25x + 2 \equiv 0 \bmod 101 \Leftrightarrow$$
$$\Leftrightarrow 47x^{20} + 7 + 54x^{20} + 25x + 2 \equiv 0 \bmod 101 \Leftrightarrow 25x \equiv -9 \bmod 101 \Leftrightarrow$$
$$\Leftrightarrow -x \equiv -36 \bmod 101 \Leftrightarrow x \equiv 36 \bmod 101$$

2.3.8 Problema 8

A chave pública usada pelo banco de Toulouse para codificar suas mensagens é a seguinte $n = 10403$ e $e = 8743$. Recentemente, os computadores do banco receberam, de local indeterminado, a seguinte mensagem

$$4746 - 8214 - 9009 - 4453 - 8198$$

O que diz a mensagem enviada ao banco?

Resolução

Temos $n = 10403 = 101 \times 103$, $e = 8743$ e $\phi(n) = 100 \times 102 = 10200$. Para encontrar d, fazemos o algoritmo de Euclides estendido.

	1	6	1457
10200	8743	1457	1
1457	1	0	

$$1 = 8743 - 6.1457 = 8743 - 6.(10200 - 8743) = 8743 - 6.10200 + 6.8743$$

Assim, $10200 \times (-6) + 8746 \times 7 = 1$, donde $8743 \times 7 \equiv 1 \bmod 10200$ e $d = 7$. Agora, podemos passar ao processo de decodificação.

$$\begin{aligned}
4746^2 &= 22524516 \equiv 2021 \bmod 10403 \\
(4746^2)^2 &\equiv (2021)^2 \equiv 4084441 \equiv 6465 \bmod 10403 \\
4746^6 &\equiv 13065765 \equiv 10000 \bmod 10403 \\
4746^7 &\equiv 47460000 \equiv 1514 \bmod 10403 \\
D(4746) &= 1514
\end{aligned}$$

$$
\begin{aligned}
8214 &\equiv -2189 \bmod 10403 \\
8214^2 &= 4791721 \equiv 6341 \bmod 10403 \\
(8214^2)^2 &\equiv 4791721 \equiv 6341 \bmod 10403 \\
8214^6 &\equiv 4349926 \equiv 1472 \bmod 10403 \\
8214^7 &\equiv 12091008 \equiv 2722 \bmod 10403 \\
D(8214) &= 2722
\end{aligned}
$$

$$
\begin{aligned}
9372 &\equiv -1031 \bmod 10403 \\
9372^2 &= 1062961 \equiv 1855 \bmod 10403 \\
(9372^2)^2 &\equiv 3441025 \equiv 8035 \bmod 10403 \\
9372^6 &\equiv 14904925 \equiv 7825 \bmod 10403 \\
9372^7 &\equiv 73373388 \equiv 1029 \bmod 10403 \\
D(9372) &= 1029
\end{aligned}
$$

$$
\begin{aligned}
9009 &\equiv -1394 \bmod 10403 \\
9009^2 &= 1943236 \equiv -2125 \bmod 10403 \\
(9009^2)^2 &\equiv 4515625 \equiv 723 \bmod 10403 \\
9009^6 &\equiv -1536375 \equiv 3269 \bmod 10403 \\
9009^7 &\equiv 29450421 \equiv 9931 \bmod 10403 \\
D(9009) &= 9931
\end{aligned}
$$

$$
\begin{aligned}
4453^2 &= 19829209 \equiv 1091 \bmod 10403 \\
(4453^2)^2 &\equiv 1190281 \equiv 4339 \bmod 10403 \\
4453^6 &\equiv 4733849 \equiv 484 \bmod 10403 \\
4453^7 &\equiv 2155252 \equiv 1831 \bmod 10403 \\
D(4453) &= 1831
\end{aligned}
$$

$$\begin{aligned} 8198 &\equiv -2205 \bmod 10403 \\ 8198^2 &= 4862025 \equiv 3824 \bmod 10403 \\ (8198^2)^2 &\equiv 14622976 \equiv 6761 \bmod 10403 \\ 8198^6 &\equiv 25854064 \equiv 2609 \bmod 10403 \\ 8198^7 &\equiv 21388582 \equiv 14 \bmod 10403 \\ D(8198) &= 14 \end{aligned}$$

Assim a mensagem é

15	14	27	22	10	29	99	31	18	31	14
F	E	R	M	A	T		V	I	V	E

Referências Bibliográficas

[1] Santos, J.P.O., *Introdução à Teoria dos Números*, . 1. ed. IMPA, SBM. Rio de Janeiro, 1998.

[2] Gomes, C.A., Gomes, J.M. *Tópicos de Matemática, IME-ITA-Olimpíadas*, vol.2 1. ed. VestSeller. Fortaleza, 2012.

[3] Landau, E., *Teoria Elementar dos Números*, 1. ed. Ciência Moderna. Rio de Janeiro, 2002.

[4] Rodrigues, P.M., *Elementos de Matemática Finita*, disponível em: <http://www.math.ist.utl.pt/ pmartins/EMF/passado/ModularSolv.pdf> acesso em 05/12/2014.

[5] Soares, C.A.S., *Criptografia Básica*, disponível em: <http://www.ufjf.br/carlos_soares/files/2014/08/criptografia001.pdf> acesso em 07/12/2014.

[6] Hefez, A. *Elementos de Aritmética*, 1. ed. SBM, Rio de Janeiro: 2003.

[7] Boyer, C.B. *História da Matemática*, 2. ed. São Paulo: Edgar Blücher, 1996.

[8] Eves, H. *Introdução à História da Matemática*, Tradução: Hygino H. Domingues. Editora da Unicamp. Campinas, 2004.

[9] Lima, E. L., Carvalho, P. C. P., Wagner, E., Morgado, A. C., *A Matemática do Ensino Médio - Volume 2*, Coleção do Professor de Matemática. 6. ed. SBM. Rio de Janeiro, 2006.