UNIVERSIDADE FEDERAL DO PIAUÍ - UFPI
CENTRO DE CIÊNCIAS DA NATUREZA - CCN
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

SAMUEL CARDOSO OLIVEIRA SILVA

ARITMÉTICA MODULAR E APLICAÇÕES

Teresina - PI
2016

SAMUEL CARDOSO OLIVEIRA SILVA

ARITMÉTICA MODULAR E APLICAÇÕES

Dissertação apresentada como requisito para obtenção do Diploma de Mestre em Matemática pela Univerisdade Federal do Piauí.

Orientador: Prof. Dr. Paulo Alexandre Araújo Sousa.

Teresina - PI
2016

FICHA CATALOGRÁFICA
Serviço de Processamento Técnico da Universidade Federal do Piauí
Biblioteca Setorial do CCN

S586a Silva, Samuel Cardoso Oliveira.
Aritmética modular e aplicações / Samuel Cardoso Oliveira Silva. – Teresina, 2016.
40f. il.: color

Dissertação (Mestrado Profissional) – Universidade Federal do Piauí, Centro de Ciências da Natureza, Pós-Graduação em Matemática, 2016.
Orientador: Prof. Dr. Paulo Alexandre Araújo Sousa.

1. Teoria dos Números – Aritmética Modular. 2.Congruência. I. Título

CDD 513.6

PROFMAT

UNIVERSIDADE FEDERAL DO PIAUÍ
CENTRO DE CIÊNCIAS DA NATUREZA
CENTRO DE EDUCAÇÃO ABERTA E À DISTÂNCIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

SBM

Dissertação de Mestrado submetida à coordenação Acadêmica Institucional, na Universidade Federal do Piauí, do Programa de Mestrado Profissional em Matemática em Rede Nacional para obtenção do grau de **mestre em matemática** intitulada: Aritmética Modular a Aplicações, defendida por Samuel Cardoso Oliveira Silva em 29/03/2016 e aprovada pela banca constituída pelos professores:

Paulo Alexandre Araújo Sousa

Presidente da Banca Examinadora

Examinador

José Arimatéa Rodrigues Melo Júnior

Examinador Externo

A minha família pelo apoio e confiança, aos meus professores que estavam sempre disponíveis a ensinar, ao meu orientador pelo empenho demonstrado na produção do trabalho, enfim a todos que de alguma forma tornaram este desafio mais fácil de vencer.

Agradecimentos

A Deus, por essa oportunidade e por me dar saúde e muita força para superar os momentos difíceis.

A Universidade Federal do Piauí – UFPI, pela oportunidade de fazer o curso.

Ao professor e orientador, Paulo Alexandre, por todo empenho e paciência nos momentos de resolver os problemas. Profissional que tem uma preocupação em garantir um curso de boa qualidade.

Aos meus pais, que estavam sempre me apoiando e que por tantas vezes nas dificuldades era meu alicerce.

A minha namorada Mayara Gomes, por me incentivar desde a graduação e estando sempre ao meu lado.

A todos os colegas da turma, em especial Bruno, Delano, Gideone, Gilson, Huérllen, Jerson, Leonardo, Pedro, Perivaldo, Queiroz, Raimundo, Renee, Rubens e Valderino pelo aprendizado e troca de conhecimentos.

Aos meus colegas de trabalho, em especial Jesus Cunha e Luzia Campos pela compreensão e apoio nos momentos em que precisei.

A todos que fizeram parte da minha formação, o meu muito obrigado.

"Deus faz aritmética"

Carl Friedrich Gauss.

Resumo

O seguinte trabalho refere-se a uma ferramenta da Teoria dos Números, denominado aritmética modular. Inicialmente foi feito um estudo da origem da Teoria dos Números mostrando os principais matemáticos que desenvolveram resultados importantes para a sua evolução, e logo após foram apresentados alguns conceitos de congruência. Em seguida mostramos como parte dos erros existentes no uso de tecnologias, principalmente relacionados a dispositivos ópticos e a digitações cadastrais, vem diminuindo com o uso da aritmética modular que dá embasamento teórico aos dígitos de verificação, a problemas que envolvem periodicidade e aos estudos dos critérios de divisibilidade.

Palavras-chave: Teoria dos Números, congruência e aritmética modular.

Abstract

The present study refers to a tool of Number Theory, called modular arithmetic. Initially was made a study about the origin of Number Theory, Showing the main mathematicians who have developed great outcomes; then was presented some concepts of congruence. Then show as part of the existing errors in the use of technologies, mainly related to optical devices and registration fingerings, has decreased with the use of modular arithmetic that gives theoretical basis to check digits, the problems involving frequency and the criteria studies divisibility.

Keywords: Number Theory, congruence, modular arithmetic.

Sumário

Lista de Figuras

1 Introdução

A aritmética é o termo que deriva do grego *arithmos*, que significa número, sendo considerada a ciência dos números. É denominado o mais simples e mais antigo ramo da matemática, supõe-se que seu surgimento foi da necessidade do homem de contar.

O termo aritmética é usado para se referir à Teoria dos Números, ramo da matemática que estuda mais profundamente as propriedades dos números em geral, chamada também de aritmética superior.

Para chegar à Teoria dos Números, a humanidade percorreu longos caminhos. A técnica da contagem e as regras de calcular foram fatos estabelecidos no final do período renascentista, em meados do século XVII. Nesse período, muitas batalhas aconteceram: lutas por territórios ou por religião em que os povos traziam sua cultura e tomavam conhecimento de outras. Com isto práticas de quantificar, contar, medir ou de representar essas ações foram se mesclando no decorrer da história, e algumas acabaram se impondo, de maneira que, hoje se tem quase uma universalidade dessas práticas.

A aritmética é mais acessível devido à generalidade e simplicidade de suas regras, enquanto que a Teoria dos Números é de difícil compreensão, devido seus métodos individuais de abordagem dos problemas.

A aritmética modular é uma das ferramentas da Teoria dos Números, cujas bases teóricas foram iniciadas pelo matemático suíço Euler, por volta de 1750. Na qual tornou-se mais compreensível através das ideias do matemático alemão Carl Friedrich Gauss publicado no livro *Disquisitiones Arithmeticae* no ano de 1801, as simbologias e definições inseridas no livro são utilizadas até hoje.

A motivação da escolha do tema aritmética modular para essa dissertação, foi os diversos problemas vinculados ao crescente uso das tecnologias de comunicação, relacionados aos erros de digitações cadastrais. E com o uso da aritmética modular grande parte de erros realizados vem sendo amenizados.

O presente trabalho apresenta um breve histórico da Teoria dos Números e algumas aplicações da aritmética modular, referente aos códigos de verificação do sistema ISBN (International Standard Book Number), CPF (Cadastro de Pessoas Físicas) e RG (Registro Geral) que foram criados para registrar, referenciar e organizar documentos. Dentre outras aplicações, alguns critérios de divisibilidade e problemas envolvendo periodicidade.

2 Fundamentação Teórica

Neste capítulo, a referência da numeração **2.1** à **2.1.3** são encontradas em [9] e a subseção **2.1.4** é encontrado na referência [8].

2.1 A origem da Teoria dos Números

Apesar de ficarem cada vez mais fascinados pela geometria, os matemáticos não perderam seu interesse pelos números. Mas começaram a fazer perguntas mais profundas, e responderam a muitas delas. Algumas tiveram de esperar por técnicas mais poderosas. Algumas permanecem sem resposta até hoje.(STEWART, 2007)

2.1.1 Teoria dos Números

Existe algo mágico nos números. Os números naturais 1, 2, 3, 4, 5,... são claros, e simples, mas na simplicidade esconde grandes segredos, e muitas das mais desconcertantes questões em matemática abordam as propriedades dos números inteiros. Essa área é conhecida como Teoria dos Números, apesar de seus elementos serem básicos acaba se mostrando uma área difícil.

Nos trabalhos de Euclides foram encontradas as primeiras contribuições para a Teoria dos Números, com afirmações seguidas de provas. A Teoria dos Números teve um grande avanço no ano de 1600, dado por Fermat, e desenvolvida por Leonhard Euler, Joseph-Louis, Lagrange e Carl Friedrich Gauss. No fim do século XX a famosa conjectura feita por Fermat conhecida como seu último Teorema, foi demonstrada.

A Teoria dos Números na maior parte da história foi voltada para mecanismos internos da matemática, com poucas ligações na vida cotidiana. O surgimento do computador digital mudou isso, através das representações eletrônicas dos números inteiros que os computadores funcionam. Após 2500 anos, a Teoria dos Números causou impacto na vida cotidiana.

Diofanto de Alexandria teve grande influência na Teoria dos Números. Ele estudou questões gerais, por exemplo: “Ache três números tais que sua soma, e a soma de dois quaisquer entre eles, seja um quadrado perfeito”. “Sua resposta foi 41, 80 e 320”.

Uma das mais conhecidas equações resolvidas por Diofanto é uma consequência cola-

teral do Teorema de Pitágoras, o teorema diz que o triângulo retângulo com medidas dos lados a, b e c sendo c o lado maior, então $a^2 + b^2 = c^2$, concluído que existem infinitas trincas pitagóricas.

A Teoria dos Números não teve importantes avanços por mais de 1000 anos, depois de Diofanto, até que apareceu Fermat com muitas descobertas importantes. Um de seus teoremas mais refinado nos diz que um determinado inteiro X é a soma de dois quadrados perfeitos: $X = a^2 + b^2$, a solução fica mais simples quando é primo. Observando os números primos, Fermat verificou que existem três tipos básicos de primos:

I) O número 2, o único primo par;
II) Primos que têm uma unidade a mais que um múltiplo de 4, tais como 5, 13, 17 e assim por diante esses primos são todos ímpares;
III) Primos que tem uma unidade a menos que um múltiplo de 4, tais como 3, 7, 11 e assim por diante, esses primos também são ímpares.

Fermat provou que um primo é a soma de dois quadrados se pertence aos (item I) ou (item II), e não é a soma de dois quadrados se pertence ao (item III). Por exemplo, 37 está no (item II), sendo $4\times9 + 1$, e $37 = 36 + 1$ uma soma de dois quadrados. Por outro lado, $31 = 4\times8 - 1$ está no (item III), pode-se tentar de todas as maneiras possíveis escrever 31 como soma de dois quadrados, e não vai ser encontrado números que dê certo. (Por exemplo, $31 = 25 + 6$, onde 25 é quadrado, mas 6 não é).

A conclusão é que um número é a soma de dois quadrados se, e somente se, todo divisor primo da forma $(4k - 1)$, com $k \in \mathbb{Z}$, ocorre para uma potência par. Fermat apresentou o seguinte resultado, todo número inteiro positivo é a soma de quatro quadrados, mas foi Joseph-Louis Lagrange que provou esse resultado em 1770. O resultado conhecido como Pequeno Teorema de Fermat, afirma que: "se p é um primo qualquer e $a \in \mathbb{Z}$, então $(a^p - a)$ é um múltiplo de p", foi uma das descobertas mais influentes e simples de Fermat.

Com as ideias do exemplar da aritmética de Diofanto, Fermat apresentou por volta de 1640 o resultado mais comemorado por ele, que levou 350 anos para ser provado. O resultado nos diz que a equação $x^n + y^n = z^n$ não tem soluções com números inteiros quando n é maior do que 2, a prova foi desenvolvida por Andrew Wiles em 1994.

Vários matemáticos importantes produziram resultados em Teoria dos Números depois de Fermat. Com destaque para Euler e Lagrange, os resultados que Fermat formulou, mas não provou, foram polidos e refinados durante esse período.

O enorme avanço seguinte na Teoria dos Números foi feito por Gauss, em sua obra-prima *Disquisitiones Arithmeticae* (investigações em aritmética), publicada em 1801. Esse trabalho colocou a Teoria dos Números para o centro do palco matemático. Nesse livro Gauss inseriu novidades na Teoria dos Números, junto a isso sistematizou as ideias de seus predecessores.

Gauss teve uma ideia muito simples, mas poderosa, a aritmética modular um novo tipo de sistema numérico. Essa ideia curiosa foi de fundamental importância para a compreensão das propriedades de divisibilidade dos inteiros comuns.

O resultado de Gauss foi: "dado um inteiro $\mathfrak{m} > 1$, dizemos que $\mathfrak{a}$ e $\mathfrak{b}$ são congruentes módulo $\mathfrak{m}$, representado por:

$$\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$$

se a diferença $(\mathfrak{a} - \mathfrak{b})$ for exatamente divisível por $\mathfrak{m}$."

A expressão "aritmética do relógio" representa o espírito da ideia de Gauss. Portanto, a aritmética modular é como um relógio que leva $\mathfrak{m}$ horas para dar uma volta inteira. Os fatos que mudam em ciclos repetitivos estão ligados à aritmética modular.

Com os estudos de Fermat a Teoria dos Números começou a ficar matematicamente fascinante, identificando padrões ocultos no enigmático e intrigante comportamento dos números inteiros. Fermat desenvolvia resultados, mas não fornecia as provas, isso foi corrigido por Euler e Lagrange, a Teoria dos Números consistia em teoremas isolados, na maioria das vezes complicada, sem ter uma relação entre si. Quando Gauss inseriu os fundamentos conceituais gerais para a Teoria dos Números, tais como a aritmética modular, isso tudo mudou. A partir desse momento, a Teoria dos Números tornou-se importante na matemática.

Os estudos de Gauss levaram ao desenvolvimento de um novo tipo de estrutura em matemática, novos sistemas numéricos, tais como os inteiros módulo $\mathfrak{m}$. A moderna abordagem da matemática, começou a ser desenvolvida no livro *Disquisitiones Arithmeticae*, marco significante para o tal começo e um dos motivos de Gauss ser muito respeitado entre os matemáticos.

2.1.2 A importância dos números primos na Teoria dos Números

Tem números que podem ser decompostos em peças menores, sendo que esses números surgem da multiplicação dessas peças menores. Por exemplo, 6 é 2×3 e 9 é 3×3, tem-se

também números que não se decompõem dessa maneira, não há como expressar 17 como produto de dois números inteiros menores, seguindo o mesmo raciocínio para $2, 3, 5, 7, 11$ e muitos outros números primos.

Os números expressos na multiplicação de dois números menores são ditos compostos, os que não podem ser assim expressos são primos. Seguindo essa definição, o número 1 deveria ser considerado primo, mas ele está numa classe própria especial chamado de unidade. Observe os primeiros números primos:

$$2 \quad 3 \quad 5 \quad 7 \quad 11 \quad 13 \quad 17 \quad 19 \quad 23 \quad 29 \quad 31 \quad 37 \quad 41$$

Observando a lista, nota-se que não existe um padrão para os números primos. Mas, não há dúvidas que podemos determinar o próximo número primo da lista.

Apesar de não seguir um padrão os primos são de importância vital em matemática. Eles formam os blocos construtivos básicos para todos os números, no sentido em que números maiores são criados realizando o produto de números menores. Na química a molécula é composta por átomos, partículas indivisíveis. De forma análoga, na matemática qualquer número é composto de primos, números indivisíveis. Segue que os primos são os átomos da Teoria dos Números.

Nos livros de Euclides, ele introduziu os números primos e deu provas de três propriedades básicas, apresentadas a seguir.

- Todo número pode ser expresso como produto de primos;
- Essa expressão é única exceto pela ordem em que os primos ocorrem;
- Há infinitos números primos.

2.1.3 O que a Teoria dos Números fez por eles

O uso de engrenagens foi uma das primeiras aplicações práticas da Teoria dos Números. Se duas rodas dentadas são unidas de modo que seus dentes se encaixem, tendo uma roda com $\mathfrak{m}$ dentes e a outra com $\mathfrak{n}$ dentes, então os movimentos das rodas está relacionado com esses números.

Um dispositivo impressionante projetado com engrenagens, chamado de Antiquitera, foi descoberto nos destroços de um naufrágio de 65 a.C., em 1900 pelo mergulhador Elias Stadiatis, próximo a ilha de Anticítera, ao sul da Grécia.

Figura 1: Antiquitera
Fonte:http://astronautasantigos.com.br/arqueologia-proibida/o-mecanismo-de-antikythera/

Com os estudos de raios-X e fotografias avançadas descobriram os mistérios dos mecanismos de Antiquitera, que podia ser utilizado para prever o mês, dia e hora de um eclipse, representar os anos bissextos, indicava as posições do sol e da lua em relação ao zodíaco, mostrava as fases da lua numa determinada data, as posições astronômicas dos planetas Mercúrio, Vênus, Marte, Júpiter e Saturno, calculava a data das competições (como as olimpíadas).

Ainda hoje permanece o mistério de quem construiu o mecanismo de Antiquitera, segundo pesquisadores o mecanismo é baseado num projeto de Arquimedes, mesmo não sabendo a certeza da autoria desse mecanismo temos a plena convicção que os antigos humanos eram capazes de façanhas intelectuais e de engenharia que surpreende as nossas mentes modernas.

A Teoria dos Números permaneceu um ramo da matemática pura, até a última parte do século XX, com aplicações dentro da própria matemática e sendo pouco importante no mundo externo. Isso mudou com o desenvolvimento da comunicação digital no fim do século XX, pois o mundo digital passou a depender de números e a Teoria dos Números passou a ser o centro nessas áreas de aplicação.

Às vezes leva tempo para uma boa ideia matemática adquirir importância prática, às vezes centenas de anos, mas em algum momento a maior parte dos temas que os

matemáticos consideram significativos em si mesmos acabam se revelando valiosos também no mundo real.

2.1.4 Gauss e a congruência módulo n

Johann Friedrich Karl Benz Gauss nasceu em 30 de abril de 1777, em Brunswich, na Alemanha. Foi matemático, astrônomo e físico. Gauss era uma criança-prodígio, tinha uma precoce paixão pelos números, desde cedo demonstrava o seu talento. Com três anos corrigiu seu pai de um erro aritmético em um cálculo complicado, apresentando a resposta correta. Outra de suas façanhas foi aprender a ler sozinho.

Em 1784 Gauss entrou para a escola primaria St. Catherine, durante as aulas de aritmética o professor J.G. Buttner descobriu que Gauss era um garoto diferenciado, ele propôs o seguinte problema "escrevam todos os números de 1 a 100 e depois vejam quanto dá a sua soma". Em alguns segundos, Gauss apresentou o resultado 5050. Como seria de esperar, Gauss teve que explicar ao espantado professor Buttner como é que tinha obtido aquele resultado: "então, $1 + 100 = 101$, $2 + 99 = 101$, prosseguindo o raciocínio, $49 + 52 = 101$ e $50 + 51 = 101$, isto da um total de 50 pares de números em que a soma é 101. Portanto, a soma total é $50 \times 101 = 5050$".

Johann Martin Bartels, assistente de Buttner, passou a ensinar o garoto Gauss, os dois costumavam discutir problemas de matemática até longas horas. Em pouco tempo Bartels compreendeu que nada tinha para ensinar a Gauss.

Figura 2: Johann Friedrich Karl Benz Gauss, pintado por Christian Albrecht Jense. Fonte:http:carlgaussmatematico.blogspot.com.br

A família de Gauss não tinha condições de manter seus estudos, e foi através de Bartels que Gauss foi apresentado ao Duque Ferdinand, que começou a fornecer os meios necessários de apoio a seus estudos, com isso Gauss frequentou o colégio Carolinum durante os anos $1792 - 1795$.

As investigações de Gauss sobre a distribuição de números primos marcaram os seus quinze ou dezesseis anos de transições do que ele próprio mais tarde chamou "a pesquisa mais sutil na aritmética superior" (o que é denominado hoje por Teoria dos Números).

No dia 15 de outubro de 1795, Gauss foi admitido na universidade de Gottingen como um estudante de matemática, foi onde descobriu como construir um polígono de dezessete lados com régua e compasso e desenvolveu até hoje a obra mais importante da Teoria dos Números *Disquisitiones Arithmeticae* (investigações em aritmética), onde foi inserida a noção de congruência.

O livro *Disquisitiones Arithmeticae* constitui um dos grandes clássicos da literatura matemática e estão divididas em sete partes: congruência em geral, congruência de primeiro grau, resto de potências, congruências de segundo grau, formas quadráticas, aplicações e divisões do circulo. Vamos enfatizar apenas na congruência geral e congruência de primeiro grau. Apresentaremos apenas um esboço do conteúdo do livro *Disquisitiones Arithmeticae*.

▪ Congruências em geral e congruências de primeiro grau

Na primeira página Gauss introduziu um novo símbolo matemático e diz que: Se um número $\mathfrak{m}$ divide a diferença $(\mathfrak{a} - \mathfrak{b})$ ou $(\mathfrak{b} - \mathfrak{a})$ de dois números $\mathfrak{a}$ e $\mathfrak{b}$ sem resto, então $\mathfrak{a}$ e $\mathfrak{b}$ dizem-se congruentes módulo $\mathfrak{m}$, Gauss escreveu

$$\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}.$$

Esta expressão lê-se: $\mathfrak{a}$ é congruente com $\mathfrak{b}$ módulo $\mathfrak{m}$. A relação é chamada congruência, e $\mathfrak{m}$ é chamado de módulo da congruência. O número $\mathfrak{b}$ é chamado o resto de $\mathfrak{a}$ módulo $\mathfrak{m}$, analogamente $\mathfrak{a}$ é chamado o resto de $\mathfrak{b}$ módulo $\mathfrak{m}$. Se a diferença $(\mathfrak{a} - \mathfrak{b})$ não for divisível por $\mathfrak{m}$, então $\mathfrak{a}$ e $\mathfrak{b}$ dizem-se incongruentes módulo $\mathfrak{m}$, e $\mathfrak{a}$ e $\mathfrak{b}$ não são restos um do outro, módulo $\mathfrak{m}$.

De acordo com a definição, $\mathrm{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ é o mesmo que $(\mathfrak{a} - \mathfrak{b}) = \mathfrak{m}\mathfrak{y}$, onde $\mathfrak{y}$ é um número inteiro qualquer.

2.2 Principais conceitos de congruência

Parte substancial dos resultados apresentados nesta seção podem ser encontrados na referência [3].

Vamos apresentar uma das noções mais fecundas da aritmética, introduzida por Gauss no seu livro Disquisitiones Arithmeticae, de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

2.2.1 Aritmética dos Restos

Seja $\mathfrak{m}$ um número natural. Diremos que dois números inteiros $\mathfrak{a}$ e $\mathfrak{b}$ são congruentes módulo $\mathfrak{m}$ se os restos de sua divisão euclidiana por $\mathfrak{m}$ são iguais. Quando os inteiros $\mathfrak{a}$ e $\mathfrak{b}$ são congruente módulo $\mathfrak{m}$, escreve-se:

$$\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}.$$

Por exemplo, $21 \equiv 13 \bmod 2$ já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Quando a relação $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ for falsa, diremos que $\mathfrak{a}$ e $\mathfrak{b}$ não são congruentes, ou que são incongruentes, módulo $\mathfrak{m}$. Escreveremos, nesse caso, $\mathfrak{a} \not\equiv \mathfrak{b} \bmod \mathfrak{m}$.

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $\mathfrak{a} \equiv \mathfrak{b} \bmod 1$, quaisquer que sejam $\mathfrak{a}, \mathfrak{b} \in \mathbb{Z}$. Isso torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, consideraremos sempre $\mathfrak{m} > 1$.

Decorre, imediatamente, da definição que a congruência, módulo um inteiro fixado $\mathfrak{m}$, é uma relação de equivalência. Vamos enunciar isso explicitamente abaixo.

Proposição 2.1. *Seja* $\mathfrak{m} \in \mathbb{N}$. *Para todos* $\mathfrak{a}, \mathfrak{b}, \mathfrak{c} \in \mathbb{Z}$, *tem-se que:*

(i) $\mathfrak{a} \equiv \mathfrak{a} \bmod \mathfrak{m}$,
(ii) se $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$, então $\mathfrak{b} \equiv \mathfrak{a} \bmod \mathfrak{m}$,
(iii) se $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ e $\mathfrak{b} \equiv \mathfrak{c} \bmod \mathfrak{m}$, então $\mathfrak{a} \equiv \mathfrak{c} \bmod \mathfrak{m}$.

Para verificar se dois números são congruente módulo $\mathfrak{m}$, não é necessário efetuar a divisão euclidiana de ambos por $\mathfrak{m}$ para depois comparar os seus restos. É suficiente aplicar o seguinte resultado:

Proposição 2.2. *Suponha que* $\mathfrak{a}, \mathfrak{b}, \mathfrak{m} \in \mathbb{Z}$, *com* $\mathfrak{m} > 1$. *Tem-se que* $\mathfrak{a} \equiv \mathfrak{b} \bmod \mathfrak{m}$ *se, e somente se,* $\mathfrak{m}$ *divide* $(\mathfrak{b} - \mathfrak{a})$.

Demonstração. Sejam $a = mq + r$, com $0 \leqslant r < m$ e $b = mq' + r'$, com $0 \leqslant r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo,

$$b - a = m(q' - q) + (r' - r).$$

Portanto, $a \equiv b \bmod m$ se, e somente se, $r = r'$, o que, em vista da igualdade acima, é equivalente a dizer que m divide $(b - a)$, já que |r -r' |< m. $\square$

Note que todo número inteiro é congruente módulo m ao seu resto pela divisão euclidiana por m e, portanto, é congruente módulo m a um dos números 0,1, ... , $m - 1$. Além disso, dois desses números distintos não são congruente módulo m.

Portanto, para achar o resto da divisão de um número a por m, basta achar o número natural r dentre os números 0, ..., $m - 1$ que seja congruente a a módulo m.

Chamaremos de sistema completo de resíduos módulo m a todo conjunto de números inteiros cujos restos pela divisão por m são os números 0, 1,..., $m - 1$, sem repetições e numa ordem qualquer.

Portanto, um sistema completo de resíduos módulo m possui m elementos. É claro que, se $a_1, ..., a_m$ são m números inteiros, dois a dois não congruentes módulo m, então eles formam um sistema completo de resíduos módulo m. De fato, os restos da divisão dos a_i por m são dois a dois distintos, o que implica que são os números 0, 1, ..., $m - 1$ em alguma ordem.

Em particular, um conjunto formado por m inteiros consecutivos é um sistema completo de resíduos módulo m.

Seja R um sistema completo de resíduos módulo m, então a divisão euclidiana por m pode ser generalizada como segue:

Para todo $a \in \mathbb{Z}$ existem inteiros q e r univocamente determinados tais que

$$a = mq + r, \text{ com } r \in R.$$

Nessa situação dizemos tratar-se da divisão com resto em R. A divisão euclidiana corresponde ao caso em que $R = \{0,1,2,...,m\text{-}1\}$.

Se tomarmos

$$R = \{r \in \mathbb{Z};\ \tfrac{-m}{2} \leqslant r < \tfrac{m}{2}\ \},$$

que é um conjunto de m inteiros consecutivos, a correspondente divisão será chamada de *divisão com menor resto.*

O que torna útil e poderosa a noção de congruência é o fato de ser uma relação de equivalência compatível com as operações de adição e multiplicação nos inteiros, conforme veremos na proposição a seguir.

Proposição 2.3. *Sejam* a, b, c, d, $m \in \mathbb{Z}$, *com* $m > 1$.

i)Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $a + c \equiv b + d \bmod m$;
ii)Se $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $ac \equiv bd \bmod m$.

Demonstração. Suponhamos que $a \equiv b \bmod m$ e $c \equiv d \bmod m$. Logo, temos que m divide $(b - a)$ e m divide $(d - c)$.

(i)Basta observa que m divide $[(b - a) + (d - c)]$ e, portanto, m divide
$[(b + d) - (a + c)]$, o que prova essa parte do resultado.
(ii)Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que m divide
$(bd - ac)$. □

Corolário 2.1. *Para todo* $n \in \mathbb{N}$, a,$b \in \mathbb{Z}$, *se* $a \equiv b \bmod m$, *então tem-se que*

$a^n \equiv b^n \bmod m$.

A demonstração faz-se por indução sobre n.

Com a notação de congruências, o Pequeno Teorema de Fermat enuncia-se como se segue:

Se p é número primo e $a \in \mathbb{Z}$, então

$$a^p \equiv a \bmod p.$$

Além disso, se $p \nmid a$, então

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

Proposição 2.4. *Sejam* a,b,c,$m \in \mathbb{Z}$, *com* $m > 1$. *Tem-se que* $a + c \equiv b + c \bmod m$ $\iff a \equiv b \bmod m$.

Demonstração. Se $a \equiv b \bmod m$, segue que $a + c \equiv b + c \bmod m$, pois $c \equiv c \bmod m$.

Reciprocamente, se $a + c \equiv b + c \bmod m$, então m divide $[(b + c) - (a + c)]$, o que implica que m divide $(b - a)$ e, consequentemente, $a \equiv b \bmod m$. □

A proposição acima nos diz que, para as congruências, vale o cancelamento com relação à adição. Entretanto, não vale, em geral, o cancelamento para a multiplicação, como se pode verificar no exemplo a seguir.

Exemplo 2.1. *Como* $6 \times 9 - 6 \times 5 = 24$ *e* 8 *divide* 24*, temos que* $6 \times 9 \equiv 6 \times 5 \bmod 8$*, e,no entanto,* $9 \not\equiv 5 \bmod 8$*.*

Temos a seguir um resultado relacionado com o cancelamento multiplicativo.

Proposição 2.5. *Sejam* a*,* b*,* c*,* $m \in \mathbb{Z}$*, com* $m > 1$*. Temos que*

$ac \equiv bc \bmod m \iff a \equiv b \bmod \frac{m}{(c,m)}$.

Demonstração. Como $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são coprimos, temos que

$ac \equiv bc \bmod m \iff m$ divide $(b-a)c \iff \frac{m}{(c,m)}$ divide $(b-a)\frac{c}{(c,m)} \iff \frac{m}{(c,m)}$ divide $(b-a) \iff a \equiv b \bmod \frac{m}{(c,m)}$ $\square$.

Corolário 2.2. *Sejam* a*,* b*,* c*,* $m \in \mathbb{Z}$*, com* $m > 1$ *e* $(c, m) = 1$*. Temos que*

$ac \equiv bc \bmod m \iff a \equiv b \bmod m$.

Proposição 2.6. *Sejam* a*,* k*,* $m \in \mathbb{Z}$*, com* $m > 1$ *e* $(k, m) = 1$*. Se* $a_1, ..., a_m$ *é um sistema completo de resíduos módulo* m*, então*

$$a + ka_1, ..., a + ka_m$$

também é um sistema completo de resíduos módulo m*.*

Demonstração. Como, da proposição acima, para $i, j = 0, ...m–1$, temos que

$$a + ka_i \equiv a + ka_j \bmod m \iff ka_i \equiv ka_j \bmod m \iff a_i \equiv a_j \bmod m \; i = j.$$

$\square$

Isso mostra que $a + ka_i, ..., a + ka_m$ são, dois a dois, não congruentes módulo m e, portanto, formam um sistema completo de resíduos módulo m.

Daremos, a seguir, algumas propriedades adicionais das congruências relacionadas com a multiplicação.

Proposição 2.7. *Sejam* a*,* $b \in \mathbb{Z}$ *e* $m, n, m_1, ..., m_r$ *inteiros maiores do que 1. Temos que*

i)Se $a \equiv b \bmod m$ e n divide m, então $a \equiv b \bmod n$;

ii)$a \equiv b \bmod m_i$, $\forall i = 1,...,\ r \iff a \equiv b \bmod [m_1, ..., m_r]$;

iii)Se $a \equiv b \bmod m$, então $(a, m) = (b, m)$.

Demonstração. (i)Se $a \equiv b \bmod m$, então m divide $(b - a)$. Como n divide m, segue-se que n divide $(b - a)$. Logo $a \equiv b \bmod n$.

(ii)Se $a \equiv b \bmod m_i$, $i = 1, ..., r$, então m_i divide $(b - a)$, para todo i. Sendo $(b - a)$ um múltiplo de cada m_i, segue-se que $[m_1, ..., m_r]$ divide $(b - a)$, o que prova que $a \equiv b \bmod [m_1, ..., m_r]$.

A reciproca decorre do item (i).

(iii)Se $a \equiv b \bmod m$, então m divide $(b - a)$ e, portanto, $b = a + tm$, com $t \in \mathbb{Z}$.

Logo, pelo seguinte resultado sejam a, b, $n \in \mathbb{Z}$, se existe $(a, b - na)$, então, (a, b) existe e $(a, b) = (a, b - na)$, temos que

$$(a, m) = (a + tm, m) = (b, m). \quad \square$$

3 Aplicações

Neste capítulo, apresentaremos algumas aplicações do cotidiano relacionadas a aritmética modular. Para tanto nos baseamos nas referências [1], [2], [4], [6] e [7].

3.1 Aritmética modular e sistemas de identificação

Na Teoria dos Números a aritmética modular é uma das ferramentas mais importantes envolvendo o conceito de congruência. Já vimos que congruência é a relação entre dois números que, divididos por um terceiro, chamado módulo de congruência, deixam o mesmo resto. Foi o brilhante Gauss que observou que usávamos com muita frequência frases do tipo "$\mathfrak{a}$ dá o mesmo resto que $\mathfrak{b}$ quando divididos por $\mathfrak{m}$", denominando este fato de congruência.

Esse tema é encontrado principalmente nos livros de Teoria dos Números, é uma definição muito importante que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O estudo das aplicações que o tema possui não é habitual relacionar com a rotina das pessoas, por exemplo, diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF(Cadastro de Pessoas Físicas), CNPJ(Cadastro Nacional da Pessoa Jurídica), ISBN(International Standard Book Number), ISSN(International Standard Serial Number), criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos em nossos estudos.

Figura 3: R.G.

Fonte: www.noticiasaominuto.com.br/brasil

Figura 4: Código de barra

Fonte:revistapegn.globo.com/Revista

Figura 5: Número ISBN
Fonte:itaca.com.br/noticias/post/1297

Figura 6: CNPJ
Fonte:www.uolhost.uol.com.br/academia

3.1.1 Sistemas de informação e a segurança na transmissão de dados

Os profissionais que exercem a função de operador de caixa sabem muito bem que frequentemente acabam cometendo erros de digitação, pois digitam enormes quantidades de números. Um erro de digitação pode ter sérias consequências, dependendo da natureza do que está sendo registrado. Um fato ocorreu em Uberaba, município de Minas Gerais. O homem teve seu número de telefone residencial publicado equivocadamente como sendo de um plantão de vendas de um plano de saúde, devido à troca de um número no catálogo telefônico. Esse erro gerou incômodo, pois o homem recebia diariamente inúmeras ligações. Esse caso foi resolvido judicialmente, a justiça entendeu que o erro ocasionou inegáveis incômodos, violando sua privacidade, intimidade e perturbando o sossego de sua casa, pois recebia ligações com frequência, isso gerou uma indenização de R$5.450.

Pesquisas revelam um fato curioso, sobre a natureza dos erros de digitação. Cerca de 79% dos erros ocorrem com a digitação equivocada de um único dígito (ou algarismo), como por exemplo: digitar 1573 quando o correto seria 1673, esse tipo de erro é denominado de erro singular.

Outros 11% dos erros, chamados de erros de transposição, referem-se à troca de dois dígitos (ou algarismo), como por exemplo: escrever MTAEMÁTICA, quando o correto seria MATEMÁTICA. Os demais 10% dos erros estão distribuídos em diversas categorias, nenhuma delas representando mais de 1% do total.

Nos dias de hoje usamos os computadores para armazenar e processar as informações digitadas, não seria possível criar um sistema que pudesse identificar com 100% de segu-

rança um erro de digitação do tipo singular ou de transposição? Se isso fosse possível, nosso sistema daria conta de evitar cerca de 90% dos erros mais frequentes de digitação.

3.1.2 Aritmética modular e a solução do problema

O sistema ISBN (International Standard Book Number) desenvolvido em 1967, com a função de identificação numérica de livros, CD-Roms e publicações em Braille, possivelmente seja um dos primeiros na utilização de um dígito de verificação ao final de cada código, com condições de resolver o problema dos erros singulares e de transposição.

Por exemplo, o código ISBN $85-0000669-2$ refere-se ao livro *Os números governam o mundo*, de Malba Tahan. Com exceção do último dígito da direita, que é o dígito de controle, os demais nove dígitos são responsáveis por identificar o país de origem da obra, a editora e o livro propriamente dito.

Os dígitos do código ISBN-10 $x_1x_2x_3x_4x_5x_6x_7x_8x_9$ e seu dígito de verificação x_{10} estão programados para verificar se o resultado S da conta

$$S = 10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + 1x_{10}$$

é divisível por 11 ou não: o algarismo de verificação é escolhido de tal forma que o resultado dessa conta tenha sempre resto zero na divisão por 11, ou com a notação de congruência $S \equiv 0 \mod 11$. Observe, no exemplo do livro de Malba Tahan, que

$$10 \times 8 + 9 \times 5 + 8 \times 0 + 7 \times 0 + 6 \times 0 + 5 \times 0 + 4 \times 6 + 3 \times 6 + 2 \times 9 + 1 \times 2 = 187$$

que é divisível por 11.

Apresentaremos um importante resultado com relação a esse sistema de aritmética módulo 11.

Proposição 3.1. *Se ocorrer na leitura de um código ISBN um, e apenas um, dos dois erros (singular ou de transposição), então a soma S não será um múltiplo de* 11.

Demonstração. Caso 1. Ocorrer um erro singular

Seja $x_1...x_i...x_{10}$ um código ISBN com dígito de verificação x_{10} e $x_1...x_i^*...x_{10}$ o resultado da ocorrência de um erro singular na i-ésima posição. Chamemos de S e S^* as somas correta e errada respectivamente. Temos evidentemente que

$$S \equiv 0 \mod 11 \text{ e } S^* - S = (11 - i)(x_i^* - x_i).$$

Se admitirmos por hipótese que S^* é múltiplo de 11 então, como 11 é primo, concluímos que 11 divide $(11 - i)$ ou divide $(x_i^* - x_i)$, o que é um absurdo, pois $(11 - i)$ e $(x_i^* - x_i)$ são números inteiros não nulos entre -10 e 10. Logo, S^* não é múltiplo de 11.

Caso 2. Ocorre um erro de transposição

Seja $x_1...x_i...x_j...x_{10}$ um código ISBN, x_{10} o dígito de verificação e $x_1...x_j...x_i...x_{10}$ o resultado da ocorrência de uma transposição dos algarismos x_i e x_j nas posições i e j. Nesse caso, a diferença $(S^* - S)$ é igual a

$$(11\text{-}i)x_j + (11\text{–}j)x_i\text{–}(11\text{–}i)x_i\text{–}(11\text{–}j)x_j = (j\text{–}i)(x_j\text{–}x_i).$$

A hipótese de S^* ser múltiplo de 11 mais uma vez é absurda porque nos conduziria à conclusão de que um dos números $(j - i)$ ou $(a_j - a_i)$, que são números inteiros não nulos entre -10 e 10, é múltiplo de 11. Segue que S^* não pode ser múltiplo de 11. □

Quando é digitado um código ISBN cometendo um erro singular ou de transposição, o equipamento que recebe os dados será capaz apenas de acusar a existência de um erro devido ao fato de S não ser divisível por 11, mas não será capaz de encontrá-lo; o que implica dizer que o digitador tem ainda como tarefa procurar o erro cometido.

3.1.3 Um pouco mais do sistema ISBN (International Standard Book Number)

É um sistema internacional padronizado que identifica numericamente os livros segundo o título, o autor, o país, a editora, individualizando-os inclusive por edição. Utilizado também para identificar software, seu sistema numérico é convertido em código de barras, o que elimina barreiras linguísticas e facilita a circulação e comercialização das obras.

Criado em 1967 por editores ingleses, o sistema passou a ser amplamente empregado, tanto pelos comerciantes de livros quanto pelas bibliotecas, até ser oficializado, em 1972, como norma internacional pela International Organization For Standartization – ISO 2108 – 1972.

O sistema ISBN é controlado pela agência Internacional do ISBN, que orienta, coordena e delega poderes às agências nacionais designadas em cada país. Desde 1978, a Fundação Biblioteca Nacional representa a agência brasileira, com a função de atribuir o número de identificação aos livros editados no país.

Uma vez fixada a identificação, ela só se aplica àquela obra e edição, não se repetindo jamais em outra. A versatilidade deste sistema de registro facilita a interconexão de arquivos e a recuperação e transmissão de dados em sistemas automatizados, razão pela qual é adotado internacionalmente.

3.1.4 ISBN – 13

O ISBN passou a ter 13 dígitos a partir de 1 de janeiro de 2007, para aumentar a capacidade do sistema devido ao crescente número de publicações, sendo composto pelos seguintes elementos:

√ O prefixo
√ O identificador do grupo de registro
√ O identificador do registrante (o editor)
√ O elemento de edição
√ O dígito de controle

O ISBN deve ser escrito ou impresso, precedido pela sigla ISBN, a cada segmento separado por hífen.

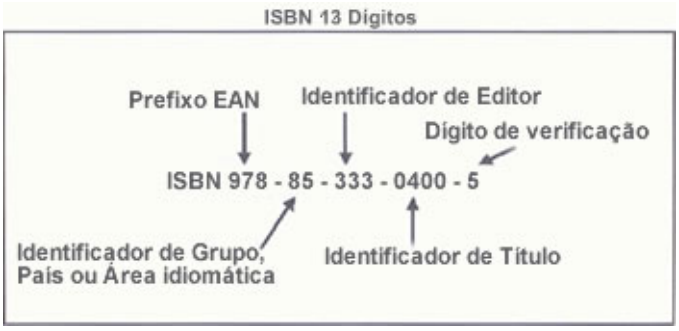


Figura 7: ISBN-13Fonte: http:www.isbn.bn.br/website/como-e-onde-utilizar-o-isbn

Quando impresso, o ISBN é sempre precedido das letras “ISBN”, os elementos tem que estar separados por hífen ou espaços, e apresentados de forma legível:

ISBN 978 – 571 – 08989 – 5
Ou
ISBN 978 571 08686 5

O uso de hifens ou espaços não tem significado lexical, é apenas para facilitar a legibilidade.

Já vimos anteriormente o cálculo para encontrar o dígito de controle do ISBN-10, agora vamos determinar o cálculo do dígito de controle do ISBN-13.

Por exemplo, ISBN $978 - 0 - 11 - 000222 - ?$

Para determinar o dígito de controle, seguiremos três passos:

1º passo: determine a soma dos produtos ponderados pelos doze dígitos do ISBN (veja a tabela):

Tabela referente à soma dos produtos ponderados

	Prefixo			Ident. do grupo de registro	Ident. do registrante		Elem. edição						Dígito de controle	Soma
ISBN	9	7	8	0	1	1	0	0	0	2	2	2	?	_
Pesos	1	3	1	3	1	3	1	3	1	3	1	3	_	_
Produto	9	21	8	0	1	3	0	0	0	6	2	6	_	56

2º passo: dividir a soma dos produtos ponderados dos primeiros doze dígitos do ISBN, calculada no primeiro passo, por 10, determinado o resto:

56 dividido por 10, tem-se quociente 5 e resto igual a 6.

3º passo: subtrair 10 pelo resto encontrado no segundo passo. A diferença resultante é o valor do dígito de controle, com uma exceção: se o resto for 10, o dígito de controle é 0(zero). Note que

$10 - 6 = 4$, logo

o dígito de controle é 4. Daí,

ISBN $978 - 0 - 11 - 000222 - 4$.

3.2 O dígito de verificação do R.G.(Registro Geral)

Para o estado de São Paulo e muitos outros estados brasileiros, o dígito de verificação do R.G.

Figura 8: R.G. Fonte: http:acev.com.br/adm/servicos/alertas-de-fraude

é calculado da seguinte maneira.

Seja $x_1x_2x_3x_4x_5x_6x_7x_8x_9$ o R.G de um individuo e x_{10} o dígito de verificação, para $i = 1, ..., 10$ e $x_{0 \leqslant i \leqslant 9}$ algarismos de 0 a 9. Temos que a soma

$$100x_{10} + 9x_9 + 8x_8 + 7x_7 + 6x_6 + 5x_5 + 4x_4 + 3x_3 + 2x_2 + 1x_1$$

deverá ser divisível por 11 para que não tenha ocorrido um erro singular ou um erro de transposição. Caso o dígito de verificação seja 10 usa-se a letra X para representá-lo. Por exemplo, o R.G $251.356.22 - X$ note que;

$$100 \times 10 + 9 \times 2 + 8 \times 2 + 7 \times 6 + 6 \times 5 + 5 \times 3 + 4 \times 1 + 3 \times 5 + 2 \times 2 + 1 \times 0$$

é divisível por 11.

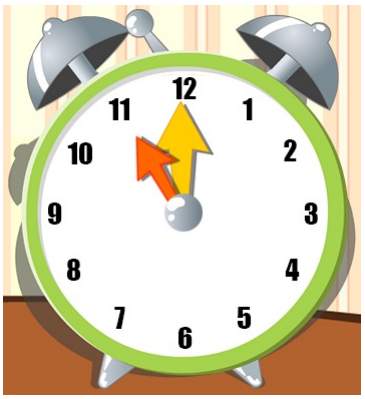
Esse modo de calcular o dígito verificador não é uniforme no sistema brasileiro, tem cidades que não segue o mesmo algoritmo. Na tabela a seguir apresentamos como é composto o R.G. nos estados brasileiros.

Institutos de Identificação			
UF	Instituto de Identificação	Perfuração mecânica sigla do órgão	Composição RG
SP	Inst. Indent. Ricardo G. Daunt	I.I.R.G.D.	8 díg. + 1 dígito verificador
RJ	Inst. Ident. Félix Pacheco Detran (Agosto 1999)	I.F.P.D.I.C.	8 díg. + 1 dígito verificador
BA	Inst. Identificação Pedro Mello	I.I.P.M.	8 díg. + 2 dígito verificador
PE	Inst. Identificação Tavares Buril	I.I.T.B. / I.TB	8 díg. sem dígito verificador
PI	Inst. Identificação João Deus Martins (1999)	I.J.D.M.	7 díg. sem dígito verificador
AC	Inst. Ident. Raimundo H. de Melo	I.I.R.H.M.	6 díg. sem dígito verificador
AM	Inst. Ident. Anderson C. de Melo	I.I.A.C.M.	7 díg. + 1 dígito verificador
MT	Inst. Ident. Aroldo M. Paiva	I.I.A.M.P.	7 díg. + 1 dígito verificador
MS	Inst. Ident. Gonçalo Pereira	I.I.G.P.	7 díg. sem dígito verificador
SE	Inst. Ident. Carlos Meneses	I.I.C.M.	7 díg. sem dígito verificador
PR	Inst. de Identificação	S.E.S.P.	7 díg. + dígito verificador
SC	Inst. Identificação	S..S.P.S.C./I.I.S.C.	7 díg. + 1 dígito verificador
DF	Inst. Identificação	I..I.S.E.P.	7 dígitos
ES	Inst. Identificação	D.E.I.D.	7 díg. sem dígito verificador
GO	Divisão identificação	S..S.P.G.O.	7 díg. sem digito verificador
MG	Inst. Identificação	I.I.M.G.	8 díg. (alfanumérico) sem díg. verificador
AL	Inst. Identificação	I.A.L	7 díg. sem dígito verificador
AM	Dep. De Ident. Civil e Criminal	I.I.A.P	6 díg. sem dígito verificador
MA	Inst. Identificação	I.I.M.A.	8 díg. + 1 dígito verificador
PA	Inst. Identificação	I.I.P.A.	7 díg. + 2 dígito verificador
PB	Departamento Identificador	I.I.P.B.	7 díg. sem dígito verificador
RO	Inst. Ident. Engracia da C. Fco	I.I.C.C.R.O.	6 díg. sem dígito verificador
RR	Inst. Identificação		6 díg. sem dígito verificador
RN	Inst. Identificação	I.T.E.P.	7 díg. sem dígito verificador
TO	Inst. Ident. Judicial e Civil	I.I.J.C.	6 díg. sem dígito verificador
CE	Inst. Ident. Milton B. de Souza	I.I.C.E.	2 díg. referente ano RG + 9 dígito seq.(parte Inform.) 7 díg. seq. + 2 díg. ref. ano RG após 1980
RS	Depto Identificação	I.I.R.S.	2 díg. verific. + 7 díg. seq. + 1 díg. verific.

3.3 Problemas envolvendo periodicidade

Na matemática, a aritmética modular também é conhecida como aritmética do relógio ou calculadora – relógio, sendo um sistema de aritmética para inteiros, onde os números voltam para trás quando atingem certo valor, o módulo.

Uma maneira de assimilar esse sistema é considerar as horas. Se agora são 11h00min a.m.,



que horas serão daqui a seis horas? Serão cinco horas da tarde, trata-se de um caso de congruência, módulo 12 (considerando o relógio analógico). Note que $11 + 6 = 17$ e 17 é congruente a 5, módulo 12. Depois que passa das 12 horas, volta à zero hora, reiniciando a contagem das horas. Se são 11h00min a.m., daqui a seis horas serão cinco horas da tarde:

$$11 + 6 = 17 \text{ e } 17 - 12 = 5.$$

Isso se chama “aritmética do relógio” e acontece com qualquer fenômeno periódico, ou seja, fatos que se repete da mesma forma, em um mesmo intervalo de tempo. Por exemplo, analisando os movimentos que a Terra realiza, o seu período de rotação para

dar uma volta completa em torno de si mesma é de 24 horas, e a lua tem período de rotação e translação em torno da Terra ambos com periodicidade de 27 dias.

Vivenciamos isso no nosso dia a dia, por exemplo, nos horários das aulas da turma do Profmat, programa de mestrado executado pela UFPI, as aulas são realizadas às sexta-feira, note que os encontros vão se repetir a cada sete dias, ou seja, a periodicidade de uma semana.

No sábado, 01 de agosto de 2015, alguém faz um questionamento se terá aula em 30 de agosto de 2015.

Agosto 2015

Segunda-Feira	Terça-Feira	Quarta-Feira	Quinta-Feira	Sexta-Feira	Sábado	Domingo
					1	

Como é, 01 de agosto, e sabendo que $30 - 1 = 29$, o dia 30 está a 29 dias desse sábado. Temos que

$$29 = 7 + 7 + 7 + 7 + 1,$$

note que passou 4 semanas e um dia para chegar em 30 de agosto. Passados as quatro semanas novamente estarão no sábado, somando mais um dia será domingo, segue que 30 de agosto é um domingo, como as aulas só serão as sextas-feiras, não haverá aula na turma do Profmat nesse dia, pois dia 30 de agosto é domingo.

Agora vamos detalhar o processo utilizado no exemplo mencionado anteriormente. Primeiramente, é necessário conhecer a periodicidade do horário da disciplina, que é de sete dias, e o intervalo de tempo entre hoje e o dia no qual queremos saber se haverá ou não aula. Se $\mathtt{n}$ dias vão se passar, dividimos $\mathtt{n}$ por 7 e tomamos nota do quociente $\mathtt{q}$ e do resto $\mathtt{r}$ dessa divisão. Observe que, a cada 7 dias caímos no mesmo dia da semana. Logo,

$n - r = 7q$ representa que terão passado exatamente q semanas. Assim, será possível determinar o dia da semana daqui a n dias a partir do resto r.

Veja a tabela

Tabela dos restos							
Resto r	0	1	2	3	4	5	6
Dia	Sábado	Domingo	Segunda feira	Terça feira	Quarta feira	Quinta feira	Sexta feira

Nesse exemplo, apresentou-se um caso de congruência modulo 7.

3.4 Cadastro das Pessoas Físicas na Receita Federal – CPF

A constatação dos dois dígitos de controle do CPF de uma pessoa é mais um caso importante, do nosso dia-a-dia usando a noção de congruência.

Figura 9: CPF

Fonte: http:jornaldosmunicipiosrj.com.br/receita-federal-atualiza-normas-sobre-cpf/

No Brasil, o número do CPF de uma pessoa é formado por 11 dígitos, mas nem todos são aleatórios ou seguem uma ordem necessariamente crescente. Os dois últimos dígitos do CPF servem para verificar se os nove dígitos anteriores foram escritos corretamente. Esses dois últimos dígitos são, portanto, dígitos de verificação.

O dígito que antecede aos dígitos de verificação representa um conjunto de estados específicos onde a pessoa realizou o seu cadastro. Por exemplo, um CPF com o número XXX. XXX. XX8 − XX, dígito anterior aos dígitos de verificação é o 8, significa que o registro ocorreu em São Paulo. Conforme pode ser observado na tabela abaixo, do código do estado onde é emitido o CPF.

Código dos Estados	
NÚMERO	ESTADOS
0	Rio Grande do Sul.
1	Distrito Federal, Goiás, Mato Grosso, Mato Grosso do Sul, e Tocantins.
2	Amazonas, Pará, Roraima, Amapá, Acre e Rondônia.
3	Ceará, Maranhão e Piauí.
4	Paraíba, Pernambuco, Alagoas e Rio Grande do Norte.
5	Bahia e Sergipe.
6	Minas Gerais.
7	Rio de Janeiro e Espírito Santo.
8	São Paulo.
9	Paraná e Santa Catarina.

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

Seja $a_1\ a_2\ a_3\ a_4\ a_5\ a_6\ a_7\ a_8\ a_9$ 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} deverá ser subtraído da soma obtida, gerando um múltiplo de 11, ou seja, se a soma obtida é S, o número $(S - a_{10})$ deve ser múltiplo de 11, podendo ser escrita da seguinte maneira $(S - a_{10}) \equiv 0 \mod 11$. Note que o a_{10} é o resto da divisão de S por 11. Se o resto da divisão for 10, usamos nesse caso o dígito 0(zero), para representar o dígito de controle.

Caso o CPF de uma pessoa tenha os seguintes 9 primeiros dígitos 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira, observe a tabela.

Tabela referente à soma dos produtos ponderados											
										Dígito de Controle	Soma
CPF	2	3	5	3	4	3	1	0	4	a_{10}	-
Pesos	1	2	3	4	5	6	7	8	9	-	-
Produto	2	6	15	12	20	18	7	0	36	-	116

Dividindo o número 116 por 11, obtemos:

$$\text{quociente 10 e resto 6 ou } 116 \equiv 6 \mod 11$$

Dessa forma, o primeiro dígito de controle será o algarismo 6. Para determinar o segundo dígito de controle, deve-se acrescentar o décimo dígito, encontrado anteriormente, e usar a seguinte base $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, as operações utilizadas para encontrar o a_{10}, de forma análoga determina o a_{11}.

Tabela referente à soma dos produtos ponderados												
										Dígitos de Controle		Soma
CPF	2	3	5	3	4	3	1	0	4	a_{10}= 6	a_{11}	-
Pesos	0	1	2	3	4	5	6	7	8	9	-	-
Produto	0	3	10	9	16	15	6	0	32	54	-	145

Dividindo o número 145 por 11, obtemos:

$$\text{quociente 13 e resto 2 ou } 145 \equiv 2 \mod 11.$$

Dessa forma o segundo dígito de controle é o 2. Portanto, o CPF completo seria: 235 343 104 − 62.

3.5 Alguns critérios de divisibilidade

Agora apresentaremos algumas consequências matemáticas do conceito de congruência.

3.5.1 Critérios de divisibilidade por dois, cinco e dez

Usando a noção de congruência, tem-se que:

$$10 \equiv 0 \mod 2,\ 10 \equiv 0 \mod 5 \text{ e } 10 \equiv 0 \mod 10, \text{ daí}$$

$$n_i 10^i \equiv 0 \mod 2,\ n_i 10^i \equiv 0 \mod 5,\ n_i 10^i \equiv 0 \mod 10;\ i \geqslant 1 \text{ e } 0 \leqslant n_i \leqslant 9$$

Portanto, dado um número $n = n_r n_{r-1} ... n_0$ na base 10 com $n \in \mathbb{N}$, temos que

$$n \equiv n_0 \mod 2,\ n \equiv n_0 \mod 5,\ n \equiv n_0 \mod 10,$$

o que nos diz que n é divisível por 2, 5 ou 10 se, e somente se, n_0 é divisível por 2, 5 ou 10.

3.5.2 Critérios de divisibilidade por três e nove

Como $10 \equiv 1 \mod 3$ e $10 \equiv 1 \mod 9$, segue-se que $n_i 10^i \equiv n_i \mod 3$ e $n_i 10^i \equiv n_i \mod 9$. Isso mostra que, se n é representado na base 10 como $n_r n_{r-1} ... n_0$, então

$$n \equiv n_r + n_{r-1} + ... + n_0 \mod 3$$

e

$$n \equiv n_r + n_{r-1} + ... + n_0 \mod 9,$$

o que prova que n é divisível por 3 ou 9 se, e somente se, $n_r + n_{r-1} + ... + n_0$ é divisível, respectivamente, por 3 ou por 9.

Para verificar se um dado número é divisível por 3 ou por 9, somam-se os seus algarismos, desprezando-se, ao efetuar a soma, cada parcela igual a nove. Se o resultado final for 0, então o número é divisível por 9. Se o resultado for um dos algarismos 0, 3 ou 6, então o número é divisível por 3.

3.5.3 Critério de divisibilidade por onze

Como $10 \equiv -1 \mod 11$, pelo **Corolário 3.1** $an \equiv bn \mod m$, temos que

$$10^{2i} \equiv 1 \mod 11 \text{ e } 10^{2i+1} \equiv -1 \mod 11.$$

Seja $n = n_r...n_5n_4n_3n_2n_1n_0$ um número escrito na base 10. Temos, então, que

$$\begin{aligned} n_0 10^0 &\equiv n_0 \mod 11 \\ n_1 10^1 &\equiv -n_1 \mod 11 \\ n_2 10^2 &\equiv n_2 \mod 11 \\ n_3 10^3 &\equiv -n_3 \mod 11 \end{aligned}$$

...

Somando, membro a membro, as congruências acima, temos que

$$n \equiv n_0 - n_1 + n_2 - n_3 + ... \mod 11$$

Portanto, n é divisível por 11 se, e somente se, é divisível por 11 o número

$$(n_0 + n_2 + n_4 + ...) - (n_1 + n_3 + n_5 + ...).$$

4 Considerações Finais

As proposições e os corolários básicos da aritmética modular apresentadas neste trabalho pode-se considerar de fácil assimilação. Com a compreensão desses resultados o cálculo do dígito verificador passa a ser mais acessível.

Aplicações relacionadas aos problemas envolvendo periodicidade, por exemplo, descobrir o dia da semana de uma determinada data. Esses problemas matemáticos são resolvidos de forma rápida e eficaz, por meio da aritmética modular.

Com a utilização de congruências, podemos estabelecer os critérios de divisibilidade, assim não se tem a necessidade de memorizar regras.

As aplicações relacionadas ao cotidiano sendo os sistemas de identificação e os problemas envolvendo periodicidade, mostra a contextualização da aritmética modular, que podem ser utilizadas pelos professores como elementos motivadores ao ministrar o tema em sala de aula.

Referências

[1] Agência Brasileira do ISBN. Disponível em:<**www.isbn.bn.br/website/tudo-sobre-o-isbn**>

[2] DUARTE, Julio C.Blogspot. Mina Gerais, 8 de marco de 2012. Disponível em:<**http:juliocesarduarte.blogspot.com.br/2012/03/04 archive.html**>. Acesso em: 27 de dezembro de 2015.

[3] HEFEZ, Abramo. **Aritmética**. – Rio de Janeiro: SBM, 2013.

[4] ISBN-International Standard Book Number. **Manual do Utilizador do ISBN**. Londres: sexta edição, 2011, 29 p. disponível em:<**http:www.isbn-international.org**>

[5] KLUSENER, Renita. **Aritmética nas séries iniciais. O que é? Para que estudar? Como ensinar?** Porto Alegre. Junho de 2002.

[6] LLYDIO. P. de Sá. **Aritmética modular e algumas de suas aplicações**.

[7] MELLO, José Luiz Pastore, RPM 48 São Paulo, SP. Baseado no artigo **Aritmética modular e sistemas de identificação**.

[8] Miniweb, cursos. Disponível em:
<**www.miniweb.com.br/ciencias/artigos/gauss1.html**>Acesso em dezembro de 2015.

[9] STEWART, Ian. **Em busca do infinito: uma história da matemática dos primeiros números a teoria do caos**. Editora: Zahar, 2007.