# APLICAÇÕES DE CONGRUÊNCIA MODÚLO M

Larisse Araújo Bitencourt [1]
Mayra Caroline Silva Santos [2]
Stheffany Gabrielle da Silva [3]
Victor Brito Villar [4]
Cassius Gomes de Oliveira [5]

Ciências da Computação

cadernos de graduação
ciências exatas e tecnológicas

ISSN IMPRESSO 1980-1777
ISSN ELETRÔNICO 2316-3135

## RESUMO

A congruência modular é uma função muito importante na aritmética e também na teoria dos números. Uma congruência pode ser definida como uma analogia entre dois números inteiros que divididos por outro número (chamado módulo de congruência) deixam o mesmo resto. Por meio das propriedades das congruências módulo "m", podemos encontrar o resto das divisões sem muitos esforços e de forma breve. Este método tende a facilitar o desenvolvimento das questões propostas em sala de aula como, por exemplo, encontrar algum dia da semana que caiu em uma data de alguns anos atrás, ou em empresas que precisam gerar códigos ou números distintos para a criação de códigos de barras, CPF, RG, placa de veículos, entre outras situações. Podemos afirmar que seria possível a realização desses problemas por meio de outros métodos, mas entendemos que gastaria mais tempo parar ser concluído, pois este é indicado por ser um procedimento fácil e rápido de se utilizar.

## PALAVRAS-CHAVE

Códigos. Números. Problemas. Congruências.

## ABSTRACT

The modular congruence is a very important function in arithmetic and also in number theory. A matching can be defined as an analogy between two integers divided by another number (called matching module) make it rest. Through the properties of congruence module "m", we can find the rest of the divisions without much effort and briefly. This method tends to facilitate the development of the questions proposed in the classroom, for example, find any day of the week it fell on a date a few years ago, or in companies that need to generate codes or different numbers for creating code bars, ID number, vehicle plate, among other situations. We can say that it would be possible to perform these problems through other methods, but we believe that more time spend stop complete, as this is indicated to be a quick and easy procedure to use.



## KEYWORDS:

Codes. Numbers. Problems. Congruences.


## 1 INTRODUÇÃO

Este artigo se propõe a demonstrar como funcionam as aplicações no dia a dia, utilizando a congruência de modulo "m". Acreditamos que nem todas as pessoas sabem como são gerados, por exemplo, os números de Cadastro de Pessoa Física (CPF), Registro Geral (RG), Códigos de Barras, entre outros tópicos e, com isso surgem às dúvidas/perguntas de como são determinados estes dados. É com este objetivo que iremos mostrar como se chega a esta conclusão, pois são gerados vários números diferentes sem que um fique igual ao outro.

Segundo um dos estudiosos da Teoria dos Números, que por sinal era físico, matemático e astrônomo, o alemão Karl Friedrick Gauss, disse que esta Teoria estuda as propriedades dos números inteiros, usando métodos avançados.

A congruência modulo "m" é uma forma de facilitar a vida das pessoas que desejam fazer divisões de números amplos ou gerar diversos códigos distintos. Dizemos que dois números inteiros, a e b, são congruentes de módulo m quando deixam o mesmo resto na divisão, ou seja, descrever que "a é congruente a b módulo m" quando "a e b" deixam o mesmo resto na divisão por "m", por exemplo, se "b" for menor ou igual à zero e "b" menor que "m", então neste caso, b é o resto da divisão de "a" por "m".

Para que as resoluções das congruências sejam mais explicitas, sendo m um número inteiro positivo. As congruências modulo "m" satisfazem as seguintes propriedades:

Reflexiva – Se "a" é um inteiro positivo, então "a congruente a" (mod m), pois m | (a – a) = 0.

Simétrica – Se "a e b" são inteiros positivos tais que "a congruente b" (mod m), então "b congruente a" (mod m).

Transitiva – Se "a, b e c" são inteiros positivos tais que "a congruente b" (mod m) e "b congruente c" (mod m), então "a congruente c" (mod m).

Como se verifica facilmente, a congruência é uma relação de equivalência em Z, para qualquer escolha do módulo m.

Uma observação importante é que a aritmética modular é compatível com as operações de uma estrutura algébrica dos números inteiros que são as adições, subtrações e multiplicações. Como é comum considerar várias relações de congruência com diferentes módulos ao mesmo tempo, o módulo é incorporado na notação.

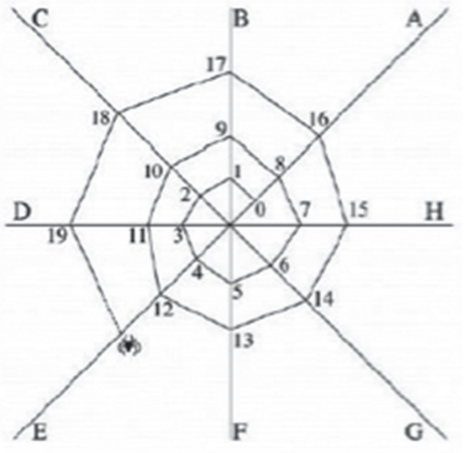
Ao longo do artigo será demonstrado como são feitos os cálculos/problemas para determinar os algarismos dos temas que serão tratados no trabalho, entre eles estão, a criação dos dados do ISBN, criação de códigos de barras, ou seja, como encontrar valores em determinados pontos. Visando essas ocasiões pretendemos atender as circunstâncias dos problemas, buscando soluções das aplicações por meio da congruência módulo "m".

Este método ajuda bastante na hora que precisamos fazer uma divisibilidade de números extensos, pois além de facilitar o processo do cálculo é uma maneira rápida para obter a conclusão.

Como já foi visto, uma das aplicações principais do conceito de congruência consiste precisamente em, dado um problema definido no conjunto dos inteiros, passar a um problema no conjunto das classes de congruência módulo "m", e deduzir da solução deste problema informações sobre o problema original.

## 2 CASO DA TEIA DE ARANHA

A congruência módulo "m" pode ser aplicada em questões de sequência. Como pode ser notada na questão da teia de aranha.




A sequência de A, B, C, D, E, F, G e H se repetem a cada volta que a aranha faz em sua teia. Assim, as oito linhas são usadas em uma volta completa da teia e notemos ainda que a cada linha um número é acrescido de um em um e na mesma sequência, o próximo número será acrescido de oito. Esse fato está explicado nas exatas oito linhas necessárias para dar uma volta na teia. Agora, segundo esta sequência, podemos dizer em qual linha o número 118 estará?

Percebemos que a teia segue as regras de uma progressão aritmética de razão oito. E que, a linha A, possui todos os números que divididos por 8 tem resto 0, a linha B, todos os número que divididos por 8 tem resto 1, e assim segue até a linha H.

Sabendo disso, agora é fácil dizer em qual linha se encontrará o número 118. Se dividirmos 118 por 8, teremos um resultado 14 com resto 6. Logo o número 118 se encontra na linha G.

## 3 CASO DO CALENDÁRIO

Ainda sobre sequências, podemos usar a congruência módulo "m" para calcular em que dia da semana caiu uma data específica. Percebamos que o método é o mesmo usado no caso da teia de aranha. É dada uma sequência que se repete a cada número X e um número Y que queremos encontrar em uma posição da sequência.

Dados os sete dias da semana domingo, segunda-feira, terça-feira, quarta-feira, quinta-feira, sexta-feira e sábado. E dado uma data específica conhecida, exemplo 1º de janeiro de 2006. Podemos calcular – sem uso de calendário, em que dia da semana caiu 5 de julho de 2006.

Contando quantos dias houve entre 1º de janeiro de 2006 e 5 de julho de 2006, temos 186 dias. O que queremos calcular é qual número na congruência módulo 7

corresponde a 186. Pela definição, 186 é um número inteiro multiplicado por 7 com resto X.

Fazendo a divisão de 186 por 7, temos 26 como resultado e resto 4. O que nos diz que 5 de julho de 2006 caiu numa quarta-feira, o número 4 na sequência de domingo à sábado.

## 4 CÓDIGO DE BARRA

O código de barra nada mais é do que a representação gráfica da sequência de números apresentadas abaixo dele. O código funciona como um identificador do produto, cada número pertencente à sequência tem uma função de localização especifica. Seja ela identificando o país, a empresa detentora do produto, a identificação do produto na empresa ou apenas o dígito de controle.

O código de barras mais usados do Brasil é o EAN13. Ele é composto de 13 dígitos. O exemplo abaixo mostra qual a funcionalidade de cada algarismo.

As três primeiras barras mais compridas servem como uma sinalização, e indica que a seguir vem o código do produto. As barras e a sequência não ficam alinhadas, por isso o número 7 vem antes das barras de sinalização.

Figura 2: Código de barras


**7897833700053**
**789:** Identifica o país. Neste caso, o Brasil.
**783370**: Identifica a empresa detentora do código de barras.
**005**: Identifica o produto da empresa.
**3**: Dígito de Controle.

O código de barras é um tipo de aplicação de congruência modulo "m", não existem códigos de barras iguais, pois cada número é selecionado criteriosamente. Como exemplificado, os 3 primeiros identificam o pais de origem, os 6 primeiros (podendo variar de 4 até 7 números) é fornecido por uma organização internacional, a EAN, que faz o controle para que não sejam distribuídos números iguais, os 3 números seguintes representam o produto (a numeração varia a depender do tipo, tamanho, quantidade, peso e embalagem do produto), e o último é um digito de controle, o código de barras estará correto se a partir de um cálculo complexo com os outros números da sequência se obter como resultado o digito de controle.

## 5 NÚMERO PADRÃO INTERNACIONAL DE LIVRO (ISBN)

É um número padrão internacional de 13 caracteres para identificação de um livro ou software. Criado em 1967 por editores ingleses, e foi oficializado com norma internacional em 1972. Antecedendo 2007 o mesmo possuía 10 dígitos e após o dia primeiro de janeiro passou a ter 13 dígitos. Este pode ser visto na parte inferior da contracapa com o código de barras. Para diferenciá-los, escreve-se ISBN-10 e ISBN-13.

Um ISBN divide-se em cinco grupos separados por meio de espaços ou hifens:

1. ISBN de 13 dígitos, um *prefixo GS1*: 978 ou 979 (indica a indústria, neste caso, 978 significa publicação de livros);
2. Identificador de grupo;
3. Código do editor;
4. Número do item (título do livro);
5. Dígito de verificação.

Tabela 1 – Contém alguns exemplos de variações de comprimento no bloco de códigos ISBN-10

| ISBN | Pais ou Língua | Editor |
|---|---|---|
| 99921-58-10-7 | Qatar | NCCAH, Doha |
| 9971-5-0210-0 | Singapore | World Scientific |
| 972-662-905-4 | Portugal | Gradiva |
| 85-359-0277-5 | Brasil | Companhia das Letras |
| 0-684-84328-5 | English-speaking area | Scribner |
| 0-8044-2957-X | English-speaking area | Frederick Ungar |
| 0-85131-041-9 | English-speaking area | J. A. Allen & Co. |
| 0-943396-04-2 | English-speaking area | Willmann–Bell |
| 0-9752298-0-X | English-speaking area | KT Publishing |

Fonte: Sítio da International ISBN Agency.

### 4.1 ISBN-10

Nos primeiros 9 dígitos, multiplica-se pela base {10, 9, 8, 7, 6, 5, 4, 3, 2} e

$$(0\times 1)+(3\times 2)+(0\times 3)+(6\times 4)+(4\times 5)+(0\times 6)+(6\times 7)+(1\times 8)+(5\times 9)$$
$$=0+6+0+24+20+0+42+8+45$$
$$=145=13\times 11+2$$

somar os produtos obtidos. Por exemplo, o dígito de verificação para o ISBN 0-306-40615 é calculado da seguinte forma:

O dígito de validação é 2, com a sequência completa 0-306-40615-2.

O calculo formal do dígito de validação é efetuado da seguinte forma:

$$(10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 + x_{10}) \mod 11 \equiv 0.$$
$$c = 145 \mod 11 = 2$$

Se o valor $x_{10}$necessário para satisfazer esta condição for 10, este será substituído por um X.

Um dígito errado ou a troca de dígitos adjacentes são os dois erros mais comuns. A única garantia é que esses dois erros sempre serão detectados, de acordo com o método de cálculo de verificação de dígito do ISBN. Não sendo detectado o livro será editado com ISBN inválido.

## 4.2 ISBN-13

$$\begin{aligned} &1\times 9+3\times 7+1\times 8+3\times 0+1\times 3+3\times 0+1\times 6+3\times 4+1\times 0+3\times 6+1\times 1+3\times 5\\ &=9+21+8+0+3+0+6+12+0+18+1+15\\ &=93 \end{aligned}$$

Nos primeiros 12 dígitos multiplicam-se pela base {1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3} e somar os produtos obtidos. Por exemplo, o dígito de verificação para o ISBN 978-0-306-40615 é calculado da seguinte forma:

O dígito de validação é 7, com a sequência completa 978-0-306-40615-7. O calculo formal do dígito de validação é efetuado da seguinte forma:

$$x_{13} = (10 - (x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12}) \bmod 10) \bmod 10.$$

De acordo com a verificação similar de utilização do UPC, todos os erros de transposição adjacente não serão detectados por este sistema, se a diferença entre eles for igual a 5. No exemplo acima os últimos dois dígitos são 6, seguindo por 1.

# 5 CONCLUSÃO

Diante do que foi tratado neste artigo, conclui-se que quando fazemos aplicações utilizando a congruência módulo "m", estamos visando uma facilidade durante o processo de aplicação. Este tema nos ajuda bastante, pois se não fosse com essas aplicações seria bem difícil conseguir gerar números, ou códigos distintos para pessoas diferentes.

Verificamos como são feitas algumas aplicações, utilizando a congruência módulo "m", alguns cálculos foram mostrados, e chegados à conclusão dos dígitos criados. Mas não só foi a criação de números distintos apontados neste trabalho. Visamos, também, como são calculados os problemas de longas terminações, como foi o caso da teia de aranha e do calendário, caso esses que se fosse para serem feitos de um por um, consumiria muito tempo até chegar à conclusão.

Estes métodos podem ser usados em empresas para gerar os códigos, como podem ser utilizados, também, em salas de aulas ou no próprio dia a dia das pessoas que queiram fazer esse tipo de problema a qualquer momento. Poderá economizar tempo, por consistir técnicas fáceis e rápidas de serem resolvidas.

## REFERÊNCIAS

ISBN Users' Manual International edition. PDF (685 KB), 2001.

LORIMER, Rowland. **Vancouver:** CCSP Press. 2005, 376, p.299. ISBN 9780973872705

MARQUES, Paulo. Números congruentes – apenas introduzindo o conceito. 1999. Disponível em: <http://www.paulomarques.com.br/arq1-12.htm>. Acesso em: 19 nov. 2014.

SÍTIO da International ISBN Agency.

SPLANE, Lily. The Book Book: A Complete Guide to Creating a Book on Your Computer. **Anaphase II Publishing**. 2002, p.37. ISBN 978-0945962144.

**Data do recebimento:** 8 de Janeiro de 2015
**Data da avaliação:** 9 de Janeiro de 2015
**Data de aceite:** 15 de Janeiro de 2015

1 Graduanda em Ciência da Computação – Universidade Tiradentes. E-mail: larissebitencourt1@gmail.com
2 Graduanda em Ciência da Computação – Universidade Tiradentes. E-mail: mayra.caroline10@gmil.com
3 Graduanda em Ciência da Computação – Universidade Tiradentes. E-mail: stheffany.gabtielle@gmail.com
4 Graduando em Ciência da Computação – Universidade Tiradentes. E-mail: stheffany.gabtielle@gmail.com
5 Prof. Msc. Universidade Tiradentes. E-mail: cassiusunit@yahoo.com.br