CONGRUÊNCIAS MODULARES NA EDUCAÇÃO BÁSICA: DISCUSSÕES POR MEIO DE UM CLUBE DE MATEMÁTICA

Anderson Rodrigo Oliveira da Silva[1]
EREMNSF
Evellyn Vitória Leite Costa[2]
EREMNSF
Emanuel Lisboa de Lima[3]
EREMNSF
Harry Henderson Lima Oliveira[4]
EREMNSF
Mayara Cordeiro Nascimento[5]
EREMNSF

Resumo

Este resumo apresenta um estudo desenvolvido em um Clube de Matemática de uma escola estadual de Pernambuco, sobre a aritmética modular na educação básica a partir da resolução de alguns problemas. A aritmética modular é um ramo da matemática que lida com operações aritméticas em conjuntos específicos de números inteiros. Este conceito é fundamental para diferentes aplicações. Neste trabalho, com o objetivo discutir a respeito de algumas aplicações das congruências modulares, apresentamos as aplicações voltadas à geração de números de CPF, ao nosso calendário semanal e um problema olímpico. Ao longo do nosso estudo, percebe-se que a compreensão dos princípios fundamentais da aritmética modular é valiosa e abre portas para inúmeras aplicações práticas.

Palavras-chave: clube de matemática, educação básica, congruência modular, aritmética.

INTRODUÇÃO

Sabemos que um dos instrumentos mais relevantes na teoria dos números é a aritmética modular, a qual envolve o conceito de congruência. Uma congruência basicamente é a relação

1 ander.rodrigoscl@gmail.com
2 evellyn.click@gmail.com
3 emanuellisboa641@gmail.com
4 harryhenderson28007@gmail.com
5 mayaracordeiro540@gmail.com

entre dois números que divididos por um terceiro – chamado módulo de congruência – deixam o mesmo resto, que por sua vez é um conceito-chave na aritmética modular. Dois números inteiros, a e b são considerados congruentes módulo n se a diferença entre eles for um múltiplo de n. Isso é denotado como $a \equiv b\ (mod\ n)$.

A aritmética modular é uma área fundamental da matemática que desempenha um papel vital em diversas áreas da ciência, tecnologia e criptografia. Ela se concentra em operações aritméticas realizadas em um conjunto específico de números inteiros, conhecidos como anel modular ou anel de congruência. Por fim, discutiremos a importância da mesma em diversas áreas da matemática, mostrando como ela desempenha um papel central na resolução de problemas complexos e na criação de sistemas seguros.

E em suma, este trabalho tem como objetivo discutir a respeito de algumas aplicações das congruências modulares, demonstrando seu papel essencial em nosso mundo interconectado e destacando como ela capacita uma ampla gama de aplicações em ciência e tecnologia. Com isso, a pesquisa presente neste resumo se deu no âmbito do Clube de Matemática Gamma, sediado na EREM Nossa Senhora de Fátima, no município de Sanharó-PE, formado por estudantes do Ensino Médio e sob supervisão do professor orientador.

A CONGRUÊNCIA MODULAR

A congruência é um dos temas centrais da aritmética modular, sendo um conceito fundamental na teoria dos números. Ela é usada para estudar propriedades de números inteiros, divisibilidade e congruências de resíduos. Carl Friedrich Gauss foi um pioneiro na aplicação da congruência modular à teoria dos números em sua obra "Disquisitiones Arithmeticae", onde o mesmo investigou propriedades de números primos e desenvolveu teorias relacionadas aos resíduos.

A mesma se configura como um conceito matemático que descreve a relação entre dois números quando eles têm a mesma propriedade de divisibilidade em relação a um terceiro número, chamado módulo. A congruência é frequentemente representada na forma $a \equiv b\ (mod\ n)$, onde se lê *"a é côngruo a b no módulo n"*.

Abaixo, no quadro 1, apresentamos sua definição e propriedades básicas, que de acordo com Domingues e Iezzi (2018, p.50) "O conceito de congruência, bem como a notação através da qual essa noção se tornou um dos instrumentos mais poderosos da teoria dos números, foi

introduzido por Karl Friedrich Gauss (1777-1855), em sua obra Disquisitiones arithmeticae (1801)".

Quadro 1 – Definição de congruência (mod m)

Sejam a e b inteiros quaisquer, e m um número inteiro estritamente positivo, diz-se que a é côngruo a b, no módulo m se $m\|(a-b)$. A qual também possui algumas das propriedades a seguir: (i) $a \equiv a(mod\ m)$ (ii) $Se\ a \equiv b(mod\ m)$ e $b \equiv c\ (mod\ m)$, então $a \equiv c(mod\ m)$.

Fonte: Domingues e Iezzi (2018)

APLICAÇÕES DA CONGRUÊNCIA

Abaixo, apresentaremos algumas das interessantes aplicações da aritmética modular e as congruências em diferentes situações. A primeira delas, versará sobre nosso calendário e base de contagem dos nossos dias da semana (módulo 7); em seguida apresentaremos a sua aplicação na elaboração dos dígitos verificadores do documento do Cadastro de Pessoas Físicas (CPF), e por fim, um interessante problema aritmético olímpico, mostrando assim diferentes situações passíveis de aplicação da aritmética modular.

Aplicação 1: Suponhamos que o dia de hoje é uma terça-feira, e queremos imaginar que dia da semana será daqui a exatamente 300 dias. Para determina-lo, usando aritmética modular, podemos observar que há 7 dias em uma semana, então a cada 7 dias, a sequência de dias da semana se repete. Logo, vamos calcular a congruência $300 \equiv x\ (mod\ 7)$ para encontrar o "resto" (x) dos 300 dias quando divididos por 7, o que nos dirá quantos dias depois de terça-feira estaremos. Utilizamos a tabela a seguir como referência.

Tabela 1 – Dias da semana e restos da divisão por 7

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

Fonte: os autores

Sabendo que $300 = 42 \cdot 7 + 6$, utilizamos o algoritmo de Euclides para determinar resto 6 nesta divisão, o que nos leva a afirmar que daqui a 300 dias estaremos em uma segunda-feira.

Aplicação 2: Na segunda aplicação, versaremos sobre a construção do dígito verificador do Cadastro de Pessoas Físicas (CPF), que de acordo com Brasil (2023), "O Cadastro de Pessoas Físicas (CPF) é um banco de dados gerenciado pela Receita Federal, que armazena informações cadastrais de contribuintes obrigados à inscrição no CPF, ou de cidadãos que se

inscreveram voluntariamente.” Assim, o CPF se configura como um documento essencial para a realidade dos brasileiros.

De acordo com DDDDDD (2016), o CPF é composto por 11 dígitos, no formato $aaa.aaa.aaa - xx$, onde os dois últimos são os dígitos verificadores, cujo primeiro é o verificador do CPF, e o último se refere à identificação do estado onde foi emitido. O algoritmo para obtenção dos dados se segue abaixo:

1) Passo 1: organizar os nove primeiros dígitos (A, B, C, D, E, F, G, H, I)
2) Passo 2: multiplicar os números pela sequência confirmadora: (1, 2, 3, 4, 5, 6, 7, 8, 9)
3) Passo 3: determinar o valor da soma (S) de todas as multiplicações anteriores e determinar sua congruência no módulo 11, obtendo assim o primeiro dígito verificador.
4) Passo 4: em seguida, proceder os passos 1 e 2, incluindo o primeiro dígito de verificação, e iniciando o passo 3 pela multiplicação de (0, 1, 2, 3, 4, 5, 6, 7, 8, 9).
5) Passo 5: Assim que obtido o 11º dígito, verificar o resultado e o estado ao qual está vinculado.

Utilizaremos a seguir o algoritmo para obtenção dos dados. Tomemos um CPF fictício cujo os primeiros 9 dígitos são $234.167.398 - AB$. Para determinar o primeiro dígito (A), faremos a multiplicação dos dígitos pela sequência apresentada no algoritmo: $S = 2 \cdot 1 + 3 \cdot 2 + 4 \cdot 3 + 1 \cdot 4 + 6 \cdot 5 + 7 \cdot 6 + 3 \cdot 7 + 9 \cdot 8 + 8 \cdot 9 = 261$. Tomando $261 \equiv x(mod\ 11) \rightarrow 261 = 11 \cdot 23 + \mathbf{8}$. Assim, o primeiro dígito verificador (A) deste CPF é 8.

Agora, iremos repetir a sequência do algoritmo para determinar B, que indicará a qual estado o CPF estaria vinculado. Tomemos o número $234.167.398 - 8B$. Definamos a soma $S = 2 \cdot 0 + 3 \cdot 1 + 4 \cdot 2 + 1 \cdot 3 + 6 \cdot 4 + 7 \cdot 5 + 3 \cdot 6 + 9 \cdot 7 + 8 \cdot 8 + 8 \cdot 9 = 290$.
Buscando $290 \equiv x(mod\ 11) \rightarrow 290 = 26 \cdot 11 + \mathbf{4}$. Assim, o segundo dígito verificador é 4, e seu estado de emissão seria Paraíba, Pernambuco, Alagoas ou Rio Grande do Norte, já que seu número completo é $234.167.398 - 84$.

Aplicação 3: Uma das realidades dos estudantes da educação básica é o contato com provas de olimpíadas de matemática. A seguir, apresentamos um problema olímpico da obra de Santos e Marques (2017, p.21), constando conteúdos referentes ao Ensino Fundamental, com desenvolvimento por meio da congruência modular. O problema é o que se segue: Mostrar que o resto da divisão de $2^{23} - 1$ por 47 é zero.

Para resolvê-lo, iremos utilizar as propriedades que constam no quadro 1. Assim, seguimos com os seguintes procedimentos:

(1) Tomando uma potência de 2, cujo resultado pode ser passível de uma congruência no módulo 47. Assim, $2^6 = \mathbf{64} \equiv \mathbf{17}$ $(\boldsymbol{mod}\ \mathbf{47})$.

(2) Em seguida, encontraremos uma forma de chegar à potência pretendida no problema (expoente 23). Com isso, elevamos ambos os lados da congruência a 3, obtendo $(2^6)^3 \equiv 17^3 = 4913 \equiv 25\ (mod\ 47) \rightarrow 2^{18} \equiv 25\ mod\ (47)$.

(3) Agora, basta multiplicarmos ambos os lados da congruência por 2^5, obtendo assim: $2^{18} \cdot 2^5 \equiv 25 \cdot 2^5 (mod\ 47) \rightarrow 2^{23} \equiv 25 \cdot 32\ (mod\ 47) \rightarrow 2^{23} \equiv 800\ (mod\ 47)$. Por sua vez, $800 \equiv 1\ (mod\ 47)$. O que resulta em $2^{23} \equiv 1\ (mod\ 47)$.

(4) Por fim, subtraindo 1 em ambos os lados da congruência, obtemos: $2^{23} - \mathbf{1} \equiv 1 - \mathbf{1}\ (mod\ 47) \rightarrow 2^{23} - 1 \equiv 0\ (mod\ 47)$.

Com isso, está provado o que se pede no enunciado do problema, pois a congruência resultou em zero. Ou seja, $2^{23} - 1$ é divisível por 47. Vemos assim que este é um resultado e procedimento adequado na educação básica, tanto para explorar o conteúdo de divisibilidade, quanto para incrementar o conhecimento matemático de turmas olímpicas.

CONSIDERAÇÕES FINAIS

A aritmética modular é uma parte essencial da matemática que desempenha um papel significativo em diversas áreas da ciência, tecnologia e segurança. Neste trabalho, exploramos os conceitos fundamentais da aritmética modular, incluindo congruências.

Ao compreender a aritmética modular, somos capazes de realizar cálculos em conjuntos específicos de números inteiros e lidar com padrões cíclicos de maneira eficiente. Isso é particularmente importante na criptografia, onde a segurança da informação é fundamental, como vimos no caso do CPF.

Em resumo, a aritmética modular é uma ferramenta matemática poderosa e versátil que desempenha um papel crucial em nosso mundo interconectado. Seu domínio é essencial para compreender e aplicar eficazmente uma variedade de conceitos e solucionar problemas complexos em diversos campos. A compreensão dos princípios fundamentais da aritmética modular é valiosa e abre portas para inúmeras aplicações práticas.

REFERÊNCIAS

BRASIL. **Meu CPF**. Receita Federal – Meu CPF, 2023. Disponível em: <<https://www.gov.br/receitafederal/pt-br/assuntos/meu-cpf>>. Acesso em: out., 2023.

DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. 5ª Ed. São Paulo – SP: Saraiva, 2018.

OLIVEIRA, C. S. **Congruência Modular e Aplicações**. 2016. Monografia (Curso de Licenciatura em Matemática a distância) – Universidade Federal de São João Del-Rei, São João Del-Rei, 2016.