Universidade Federal de Juiz de Fora

Instituto de Ciências Exatas

PROFMAT - Mestrado Profissional em Matemática em Rede Nacional

Renato da Cruz Avelar

Uma Abordagem da Aritmética Modular na Primeira Série do Ensino Médio

Juiz de Fora

2015

Renato da Cruz Avelar

Uma Abordagem da Aritmética Modular na Primeira Série do Ensino Médio

Dissertação apresentada ao PROFMAT - Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática , como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Professor Dr. Sandro Rodrigues Mazorche

Juiz de Fora

2015

Ficha catalográfica elaborada através do Modelo Latex do CDC da UFJF
com os dados fornecidos pelo(a) autor(a)

Avelar, Renato da Cruz.
Uma Abordagem da Aritmética Modular na Primeira Série do Ensino Médio / Renato da Cruz Avelar. – 2015.
52 f. : il.

Orientador: Professor Dr. Sandro Rodrigues Mazorche
Dissertação (Mestrado Profissional) – Universidade Federal de Juiz de Fora, Instituto de Ciências Exatas. PROFMAT - Mestrado Profissional em Matemática em Rede Nacional, 2015.

1. Aritmética Modular. I. Mazorche, Sandro. Título.

Renato da Cruz Avelar

Uma Abordagem da Aritmética Modular na Primeira Série do Ensino Médio

Dissertação apresentada ao PROFMAT - Mestrado Profissional em Matemática em Rede Nacional da Universidade Federal de Juiz de Fora, na área de concentração em Ensino de Matemática , como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em: 11/04/2015

BANCA EXAMINADORA

Professor Dr. Sandro Rodrigues Mazorche - Orientador
Universidade Federal de Juiz de Fora

Professor Dr. Francinildo Nobre Ferreira
Universidade Federal de São João del-Rei

Professor Dr. Luiz Fernando de Oliveira Faria
Universidade Federal de Juiz de Fora

AGRADECIMENTOS

Gostaria de agradecer a todos que de alguma maneira contribuíram ao longo dessa caminhada, em especial

- a meus pais, Jaira (in memorian) e Iracides, que não mediram esforços para que eu pudesse estudar;
- à minha irmã Janaína;
- à minha esposa Tatiana pela compreensão e dedicação, sempre me apoiando nos momentos mais difíceis;
- aos meus colegas de curso, com quem tive o prazer de conviver ao longo desses dois anos, em especial a Ariosvaldo e Ricardo Almeida, com quem a troca de experiência foi maior durante esse trabalho e ainda ao colega Carlos Henrique, que me passou muita força em diversos momentos;
- ao meu orientador, Prof. Sandro, por toda atenção, dedicação e paciência, além das dicas valiosas que ajudaram muito na conclusão desse trabalho;
- aos professores que ministraram aulas aos sábados na UFJF;
- à CAPES pelo apoio financeiro.

Enfim, agradeço a DEUS pelas oportunidades que tive e por me permitir ter convivido e ainda conviver com pessoas que sempre me desejaram o bem.

A Matemática é a rainha das ciências e a teoria dos números é a rainha das Matemáticas."
(Gauss)

RESUMO

Este trabalho tem como principal objetivo apresentar um abordagem da aritmética modular direcionada para o aluno do 1º ano do ensino médio regular, baseado na experiência do autor nessa modalidade de ensino, fazendo uma breve revisão de alguns requisitos básicos para compreensão do conteúdo. A teoria é apresentada utilizando uma linguagem simples, sempre seguida de exemplos, sendo alguns deles retirados de provas de nível nacional, além de propor atividades para fixação, seguidas das respectivas soluções e atividades de aplicação, que permitem a verificação e percepção da importância do conteúdo.

Palavras-chave: Aritmética Modular.

ABSTRACT

This work aims to present a modular arithmetic approach directed to the student on his first year of regular high school, based on the experience of author in this type of education, making a brief review of some basic requirements to understand the content. The theory is presented using simple language, always followed by examples, some of which are drawn from national tests, and to propose activities for fixation, followed by their solutions and activities application that allow the verification and perceived importance of the content.

Key-words: Modular Arithmetic

SUMÁRIO

1 INTRODUÇÃO

A palavra aritmética vem do grego arithmetiké, o que significa ciência dos números. De acordo com [1]:

> Ao longo do ensino fundamental o conhecimento sobre os números é construído e assimilado pelo aluno num processo em que tais números aparecem como instrumento eficaz para resolver determinados problemas, e também como objeto de estudo em si mesmos, considerando-se, nesta dimensão, suas propriedades, suas inter-relações e o modo como historicamente foram constituídos.

Cada vez mais em provas como OBMEP, ENEM e também em alguns concursos, é percebido um aumento de questões que poderiam ser desenvolvidas utilizando-se a Aritmética Modular. Tal conceito fundamental no desenvolvimento e aprofundamento das operações usuais com números inteiros, foi introduzido primeiramente por Euler, por volta de 1750 e desenvolvida posteriormente por Carl Friedrich Gauss em seu livro Disquisitiones Arithmeticae, publicado em 1801.

Apesar desse conteúdo ser desenvolvido com alunos do ensino fundamental através do Programa de Iniciação Científica-jr. (PIC-Jr) da OBMEP, propomos que esse trabalho seja feito com alunos do primeiro ano do ensino médio, por possuírem mais maturidade nesse momento, pois a maioria destes não tiveram a oportunidade, muitas vezes até por falta de incentivo, de participar de um programa de excelência como o PIC-Jr. Esperamos que isso possa ser feito no inicio do anos letivo, em no máximo duas semanas e meia de aula, com uma carga horária de 14 horas/aula, que serão melhor detalhadas ao longo do trabalho.

Na seção denominada Conceitos Fundamentais, apresentaremos um desenvolvimento voltado para o aluno, enunciando alguns teoremas sem nos preocuparmos com as demonstrações, que podem ser encontradas em [4], utilizado na disciplina de Aritmética no PROFMAT, que serviu de inspiração para a construção desse trabalho, além de [2], [3] e [6] que contribuíram para o desenvolvimento do texto. Começamos com o conceito de divisibilidade, descrito por Euclides, para representar uma divisão com restos, será de fundamental importância no desenvolvimento de problemas e exemplos que exploram os restos das divisões, que também serão objeto de estudo mais a frente. Em seguida exploramos os números primos, mostrando que todos os números podem ser escritos de forma única através de um produto de fatores primos (Teorema Fundamental da Aritmética). Desenvolveremos também um teste de primalidade e utilizaremos o Crivo de Eratóstenes na resolução de um exemplo, por acreditarmos que nenhum desses métodos são apresentados hoje no ensino regular, o que dificulta muitas vezes a determinação de um número primo por parte dos alunos. Faremos uma breve abordagem do máximo divisor comum e do mínimo múltiplo comum, mostrando o cálculo de cada um deles

através de alguns exemplos. Para o cálculo do máximo divisor comum, apresentamos ainda o algoritmo de Euclides, mostrando em cada exemplo, todas as divisões na ordem em que foram realizadas. Isso é muito importante para a continuidade do conteúdo, pois visa que o aluno consiga escrever o máximo divisor comum entre dois números de acordo com o teorema de Bézout. Escrever o máximo divisor comum dessa forma, fornecerá uma ferramenta para resolver equações diofantinas lineares em duas variáveis, que será apresentada em sequência. Apresentando ainda as equações diofantinas lineares através de um exemplo prático levaremos os alunos a determinarem soluções imediatas, percebendo aí que estas não são únicas. Espera-se nesse momento que venha com naturalidade o questionamento sobre todas as soluções possíveis. Faremos uso desse mesmo problema para mostrar como determinar essas soluções, verificando a validade de cada uma delas de acordo com o problema. Esse tópico será um pouco mais explorado que os anteriores através de exemplos e atividades, por se tratar de algo nunca visto anteriormente pelos alunos do ensino médio. Espera-se com essa seção, resgatar alguns conceitos vistos pelos alunos no ensino fundamenta, mas que com o passar do tempo passaram a ser aplicados de forma mecânica, muitas vezes não percebendo o significado e até mesmo o motivo da aplicação de tais conceitos em determinadas situações.

Em seguida, na seção denominada Aritmética Modular, abordaremos os principais tópicos da aritmética modular, apresentando suas principais propriedades seguidas de exemplos. Apresentamos o Pequeno Teorema de Fermat, mostrando como este pode ser escrito através da notação de congruências. Apresentamos ainda nessa seção, exemplos de questões da OBMEP, ENEM e outras que podem ser resolvidas aplicando conceitos de congruência modular. Finalizando a seção, propomos uma pequena lista de atividades, retiradas de [5], que servirão como referência, não impedindo que se busque novas atividades para serem apresentadas aos alunos.

Finalmente, na última seção apresentaremos algumas atividades contextualizadas retiradas de [8], como cálculo de dígitos verificadores de alguns sistemas de identificações, atividades envolvendo calendários que permitem determinar o dia da semana em que ocorreu uma determinada data e finalizamos com um breve estudo sobre criptografia. De acordo com [7]:

> O currículo do Ensino Médio deve garantir também espaço para que os alunos possam estender e aprofundar seus conhecimentos sobre números e álgebra, mas não isoladamente de outros conceitos, nem em separado dos problemas e da perspectiva sócio-histórica que está na origem desses temas. Estes conteúdos estão diretamente relacionados ao desenvolvimento de habilidades que dizem respeito à resolução de problemas, à apropriação da linguagem simbólica, à validação de argumentos, à descrição de modelos e à capacidade de utilizar a Matemática na interpretação e intervenção no real.

Contudo, espera-se que os alunos submetidos ao trabalho absorvam o conteúdo, reconheçam sua importância e sejam capazes de aplicá-lo nas situações em que seja viável, trazendo uma nova visão de diversas situações, baseada nessa teoria.

2 CONCEITOS FUNDAMENTAIS

Nesta seção, revisaremos conceitos básicos de divisibilidade vistos pelos alunos no ensino fundamental, que devem estar bem claros, uma vez que serão fundamentais para a teoria que pretendemos desenvolver. O objetivo desta seção é que o aluno reveja como escrever uma divisão envolvendo resto descrita por Euclides.

2.1 DIVISÃO EUCLIDIANA

Muitas vezes ao efetuarmos uma divisão, esperamos que o resultado encontrado seja um número inteiro, ou seja, uma divisão sem resto, como por exemplo $16 \div 2 = 8$.

Porém, na maioria das vezes isso não acontece. Euclides, matemático conhecido como pai da geometria, nasceu na Síria aproximadamente 330 A.C., definiu em sua obra intitulada "Elementos"uma forma de representar esse tipo de divisão.

Antes da definição formal, vejamos alguns exemplos:

I) Ao dividir 20 por 3, obtemos quociente 6 e resto 2. Desta forma, podemos escrever $20 = 3 \times 6 + 2$.

II) Dividindo 31 por 4, obtemos quociente 7 e resto 3. Desta forma podemos escrever $31 = 4 \times 7 + 3$.

Observando os exemplos acima, podemos perceber que o número a ser dividido, ou seja, o dividendo pode ser escrito como o produto do divisor pelo quociente, adicionado do resto.

Não faremos a demonstração do teorema a seguir, mas se o professor julgar conveniente fazer a demonstração para seus alunos, poderá encontrá-la em [4].

Teorema 2.1.1. *Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros q e r tais que $b = a \times q + r$, com $0 \leq r < |a|$, onde $|a|$ denota o módulo de a.*

Observação: Utilizamos $|a|$ no teorema para o caso em que a é um numero inteiro negativo. Nesse caso, como $r \geq 0$, devemos ter $r < |a|$.

Vejamos um exemplo para esse caso:

O quociente e o resto da divisão de 19 por -5 são respectivamente $q = -4$ e $r = 1$. Logo, podemos escrever $19 = (-5).4 + 1$, onde $0 \leq r = 1 < |-5| = 5$.

Vejamos um outro exemplo para o caso em que b é um inteiro negativo e q é um inteiro positivo:

Para dividir -11 por 2, devemos verificar que $2.(-6) = -12$ é o múltiplo de 2 imediatamente menor que -11. Assim, $q = -6$. Já o resto é dado por $|-12-(-11)| = 1$.

Logo, podemos escrever $-11 = (-6).2 + 1$, onde onde $0 \leq r = 1 < |-6| = 6$.

De modo geral, temos que em divisões desse tipo, o quociente será o número que devemos multiplicar o divisor para obtermos seu múltiplo imediatamente que o dividendo. O resto será dado pelo módulo da diferença entre esse múltiplo e o dividendo.

Apresentaremos alguns exemplos com as respectivas soluções contendo orientações para o professor, servindo apenas como referência, não impedindo que o mesmo busque outras atividades a serem desenvolvidas com seus alunos. No primeiro exemplo, exploramos diretamente o teorema 2.1.1, fazendo com que seja necessário o conhecimento de como escrever uma divisão com resto e ainda que o resto dessa divisão não pode ser maior que o divisor. Já no segundo exemplo, apresentamos uma questão do nível 1 da OBMEP. Cabe observarmos que a questão poderia ser solucionada mais facilmente se o aluno conhecesse a teoria das congruências. Nesse caso, ele poderia verificar que a soma das potencias tomadas de 4 em 4 são congruentes a 0 módulo 4. Como essa questão foi proposta para alunos do ensino fundamental (6^o e 7^o anos), seria um bom momento para que o professor comece a tocar em pontos como esse.

Exemplo 1. *Um fazendeiro deixou como herança para seus 7 filhos uma grande quantidade de gados de corte. Em seu testamento ele pediu que seu melhor funcionário fizesse a contagem dos gados e dividisse de modo que cada filho recebesse a mesma quantidade. Como agradecimento aos serviços prestados por tantos anos, o fazendeiro pediu ainda que os gados que sobrassem após a divisão, ficassem para seu empregado. Analisando essa situação, responda:*

(a) Qual a maior quantidade de cabeças de gado que o funcionário poderá receber?

(b) Seria melhor para o funcionário se o patrão tivesse deixado 343 ou 157 cabeças de gado?

(c) Após fazer e refazer a contagem a divisão foi a seguinte:

- *Cada filho recebeu 51 cabeças de gado;*
- *O funcionário responsável pela contagem recebeu 5 cabeças de gado.*

Baseado nessas informações, quantas cabeças de gado o patrão possuía?

Solução:*Essa atividade visa a fixação do conceito de que o resto deve ser menor que o quociente da divisão e ainda reforça o algoritmo da divisão de Euclides.*

(a) *Como a divisão será realizada entre 7 filhos, de acordo com o teorema 3.1, temos que* $a = 7$ *e como* $0 \leq r < 7$, *com* r *inteiro, podemos ter no máximo* $r = 6$.

(b) *Escrevendo os dois resultados de acordo com o algoritmo de Euclides, temos:*

- $343 = 7 \times 49 + 0$
- $157 = 7 \times 22 + 3$

Como o resto da primeira divisão é 0 e o da segunda divisão é 3, temos que é mais vantajoso para o empregado que o fazendeiro tenha 157 cabeças de gado. Pode-se notar aqui que quanto maior for o número de cabeças de gado, melhor para os filhos, mas não necessariamente para o empregado, já que o mais importante para ele é o resto da divisão.

(c) *De acordo com o problema, temos que* $q = 51$ *e* $r = 5$, *além de sabermos que* $a = 7$, *pois a divisão foi realizada entre 7 filhos. Chamando o total de gados de* D, *temos:* $D = a.q + r$, *ou seja,*

$D = 7.51 + 5$

$D = 362$

Logo, na fazenda haviam 362 cabeças de gado.

Exemplo 2. *(OBMEP 2013) Qual o algarismo das unidades do número* $3^1 + 3^2 + 3^3 + 3^4 + \ldots + 3^{2013}$*?*

Solução:*Seria muito trabalhoso calcularmos todas as potências para depois efetuarmos as somas.*

Vamos então observar o que acontece, calculando algumas potências:

- $3^1 = 3$
- $3^2 = 9$
- $3^3 = 27$
- $3^4 = 81$
- $3^5 = 343$
- $3^6 = 1029$
- $3^7 = 2187$
- $3^8 = 6561$

Se observarmos os algarismos das unidades de cada grupo de quatro potências, começando da primeira, temos sempre 3,9,7 e 1, onde $3 + 9 + 7 + 1 = 20$, *ou seja, a soma das potências tomadas de 4 em 4 e em ordem terminam em 0.*

Como são 2013 potências e $2013 = 4.503 + 1$, *teremos 503 grupos de 4 potências, mais a potência* 3^{2013}.

Assim, a soma $3^1 + 3^2 + 3^3 + 3^4 + \ldots + 3^{2012}$ *possui algarismo da unidade igual a 0 e como* 3^{2013} *inicia uma nova sequência, só poderá terminar em 3.*

Logo, o algarismo das unidades de $3^1 + 3^2 + 3^3 + 3^4 + \ldots + 3^{2013}$ *é 3.*

2.2 NÚMEROS PRIMOS

Nessa seção apresentaremos os números primos. Isso ocorre na maioria das vezes de forma muito direta, sendo apresentado ao aluno apenas a definição de um número primo, o que faz com que ele tenha dificuldade de determinar se alguns números, relativamente pequenos são primos. Para que ele não decore a sequência dos primeiros números primos apenas, apresentamos um teste de primalidade seguido do Crivo de Eratóstenes apresentado através de um exemplo.

Definição Um número natural maior do que 1 que só possui como divisores 1 e ele próprio é chamado primo.

Euclides em seu livro IX dos Elementos afirma que esses números são infinitos. Um número que não é primo é denominado composto. Por exemplo, 2, 3, 5, 7, 11, 13 e 17 são números primos, enquanto os números 4, 6, 8, 9, 10, 12 e 14 são compostos.

Os números primos desempenham papel fundamenta na matemática, como veremos no teorema a seguir, que nos diz que todos os números naturais podem ser escritos de forma única como um produto de números primos.

Esse teorema já é conhecido pelos alunos do ensino fundamental, porém não é enunciado desta forma. O termo usado é fatoração. Fatorar um número significa escrevê-lo através de fatores primos. Não apresentaremos a demonstração do teorema, mas a mesma pode ser encontrada em [4].

Teorema 2.2.1 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como um produto de primos.*

Exemplo 3. *O número 60 não é primo, pois sua forma fatorada é o produto* $2^2.3.5$.

Exemplo 4. *O número 29 é primo, pois ele não pode ser escrito como produto de outros primos.*

Até agora, para determinarmos se um número N é primo, devemos dividir esse número por todos os primos p, tais que $p < N$. Se em nenhum dos casos a divisão for exata, significa que N é primo.

Não há nada de errado no raciocínio acima, mas isso pode se tornar muito trabalhoso para números maiores.

Vamos agora, apresentar um método que permitirá determinar com mais facilidade se um número é primo ou não.

2.2.1 Teste de Primalidade

Para determinar se um número N é primo, devemos primeiramente extrair a raiz quadrada de N. Neste momento então, tomamos todos os primos p, tais que $p < \sqrt{N}$.

Se N não for divisível por nenhum desses primos, podemos afirmar que N é primo, caso contrário, N é composto.

Vejamos alguns exemplos:

Exemplo 5. *Tomando $N = 223$, temos que $\sqrt{N} \cong 14,9$, ou seja, $14 < \sqrt{N} < 15$.*

Logo, os primos menores que $\sqrt{N}$ são 2,3,5,7,11 e 13.

Como $\sqrt{N}$ não é divisível por nenhum deles, temos que 223 é primo;

Exemplo 6. *Tomando $N = 391$, temos que $\sqrt{N} \cong 19,8$, ou seja, $19 < \sqrt{N} < 20$.*

Logo, os primos menores que $\sqrt{N}$ são 2,3,5,7,11,13,17 e 19, sendo que o único que divide 391 é o 17. Logo, 391 não é primo.

Crivo de Eratóstenes

O Crivo de Eratóstenes baseia-se no teste de primalidade acima e serve para determinar todos os primos menores que um número qualquer.

Vejamos como aplicá-lo, para determinarmos todos os primos menores que número N inteiro positivo.

1º) Construímos uma tabela com todos os números inteiros ordenadamente, começando pelo número 2 e terminando em N.

2º) Calculamos o valor de $\sqrt{N}$.

3º) Riscamos todos os primos menores que $\sqrt{N}$.

4º) Riscamos os múltiplos dos primos descritos no item anterior.

5º) Os números restantes na tabela são primos.

Exemplo 7. *(OBMEP 2010) Quais são os números cujos triplos somados com 1 dão um numero primo entre 70 e 110?*

Solução: *Para resolver essa questão vamos utilizar o Crivo de Eratóstenes.*

Nesse caso, vamos determinar os primos menores que 110 e tomarmos então os compreendidos entre 70 e 110.

De acordo com o Crivo de Eratóstenes calculamos $\sqrt{110} \cong 10,49$.

Riscamos então os primos 2,3,5 e 7 da tabela abaixo e todos os seus múltiplos. Os números restantes são primos.

	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	32	33
34	35	36	37	38	39	40	41	42	43	44
45	46	47	48	49	50	51	52	53	54	55
56	57	58	59	60	61	62	63	64	65	66
67	68	69	70	71	72	73	74	75	76	77
78	79	80	81	82	83	84	85	86	87	88
89	90	91	92	93	94	95	96	97	98	99
100	101	102	103	104	105	106	107	108	109	110

Logo, podemos observar que os únicos primos compreendidos entre 70 e 110 são:

71 ; 73 ; 79 ; 83 ; 89 ; 97 ; 101 ; 103 ; 107 ; 109.

Subtraindo 1, em cada um deles, temos: 70 ; 72 ; 78 ; 82 ; 88 ; 96 ; 100 ; 102 ; 106 ; 108.

Desses, os únicos que são múltiplos de 3 são:

72 ; 78 ; 96 ; 102 ; 108.

Dividindo cada um deles por 3, obtemos respectivamente: 24 ; 26 ; 32 ; 34 ; 36, que são os números procurados.

2.3 MÁXIMO DIVISOR COMUM (M.D.C) e MÍNIMO MÚLTIPLO COMUM (M.M.C.)

Vamos nessa seção tratar de dois conceitos bastante importantes estudados no ensino fundamental. Esperamos além de revisar os assuntos, resgatar também os seus significados, pois é comum nos depararmos com alunos do ensino médio que calculam perfeitamente o M.D.C. e o M.M.C., porém não são capazes de compreenderem os seus significados. Segue então abaixo uma breve explicação do que é o M.D.C. e o M.M.C. entre dois números. Logo depois, apresentaremos um método para o cálculo de cada um deles, seguido de exemplo.

Se tomarmos dois números inteiros positivos a e b, temos que o M.D.C. entre a e b será um número inteiro d, se d for o maior número que divide a e b.

Considerando ainda esses inteiros positivos a e b, temos que o M.M.C. entre a e b será um número inteiro m, se m for o menor número que é múltiplo de a e b.

Vamos utilizar a fatoração para determinarmos o M.D.C e o M.M.C. entre dois ou mais números.

2.3.1 Cálculo do M.D.C.

Para determinarmos o M.D.C. entre dois ou mais números, devemos escrevê-los em sua forma fatorada e tomarmos todos os fatores comuns e que possuem o menor expoente. A partir desse momento, quando nos referirmos ao M.D.C. entre dois números a e $b \in Z$, escreveremos simplesmente (a, b).

Exemplo 8. *Vamos determinar* $(700, 784)$.

Primeiramente devemos escrever os números em sua forma fatorada:

- $700 = 2^2.5^2.7$
- $784 = 2^4.7^2$

Nesse caso, os fatores primos que aparecem em ambas as fatorações são 2 e 7 e seus menores expoentes correspondentes a eles são respectivamente 2 e 1. Assim, temos que $(700, 784) = 2^2.7 = 28$.

Exemplo 9. *(PUC) "A Dengue é uma doença causada por um vírus, transmitida de uma pessoa doente para uma pessoa sadia por meio de um mosquito: o Aedes aegypti. Ela se manifesta de maneira súbita – com febre alta, dor atrás dos olhos e dores nas costas – e, como não existem vacinas específicas para o seu tratamento, a forma de prevenção é a única arma para combater a doença."*

Fonte (adaptado): prdu.unicamp.br/dengue/dengue.html

Assim sendo, suponha que 450 mulheres e 575 homens inscreveram-se como voluntários para percorrer alguns bairros do ABC paulista, a fim de orientar a população sobre os procedimentos a serem usados no combate à Dengue. Para tal, todas as 1.025 pessoas inscritas serão divididas em grupos, segundo o seguinte critério: todos os grupos deverão ter a mesma quantidade de pessoas e em cada grupo só haverá pessoas de um mesmo sexo. Nessas condições, se grupos distintos deverão visitar bairros distintos, o menor número de bairros a serem visitados é:

(A) 25

(B) 29

(C) 37

(D) 41

(E) 45

Solução: Quanto maior for o número de pessoas em cada grupo, menor será a quantidade de grupos formados. Assim, vamos determinar o maior número de pessoas que poderemos ter em cada grupo, considerando grupos de homens e mulheres separados. Esse número será o M.D.C.(450,575)=25 pessoas em cada grupo. Como o número de bairros visitados é igual ao número de grupos, teremos $450 \div 25 = 18$ grupos de mulheres e $575 \div 25 = 23$ grupos de homens. Logo o total de grupos, assim como o total de bairros a serem visitados será $18 + 23 = 41$.

Logo a resposta correta será a letra D.

2.3.2 Cálculo do M.M.C.

Para determinarmos o M.M.C. entre dois ou mais números, devemos escrevê-los em sua forma fatorada e tomarmos todos os fatores de maior expoente que aparecem na fatoração de pelo menos um deles. A partir desse momento, quando nos referirmos ao M.M.C entre dois números a e $b \in Z$, escreveremos simplesmente $[a, b]$.

Exemplo 10. *Vamos determinar [36,48].*

Primeiramente devemos escrever os números em sua forma fatorada:

- $36 = 2^2.3^2$
- $48 = 2^4.3$

Nesse caso, os únicos fatores primos que aparecem nas fatorações são 2 e 3, onde o maior expoente do fator 2 é 4 e o maior expoente do fator 3 é 2. Assim, temos que $[36, 48] = 2^4.3^2 = 144$.

Exemplo 11. *(UEL PR/2010) Três ciclistas percorrem um circuito saindo todos ao mesmo tempo, do mesmo ponto, e com o mesmo sentido. O primeiro faz o percurso em 40 s, o segundo em 36 s e o terceiro em 30 s. Com base nessas informações, depois de quanto tempo os três ciclistas se reencontrarão novamente no ponto de partida, pela primeira vez, e quantas voltas terá dado o primeiro, o segundo e o terceiro ciclistas, respectivamente?*

(A) 5 minutos, 10 voltas, 11 voltas e 13 voltas.

(B) 6 minutos, 9 voltas, 10 voltas e 12 voltas.

(C) 7 minutos, 10 voltas, 11 voltas e 12 voltas.

(D) 8 minutos, 8 voltas, 9 voltas e 10 voltas.

(E) 9 minutos, 9 voltas, 11 voltas e 12 voltas.

Solução: A primeira vez que eles se encontrarão no ponto de partida será quando ocorrer o primeiro múltiplo comum entre os tempos de volta de cada ciclista. Assim M.M.C.(40,36,30)= 360 segundos, ou seja, 6 minutos. Por eliminação, sabemos que a resposta é a letra B, porém vamos agora determinar quantas voltas terá dado cada um deles no momento do encontro. Para isso, vamos dividir o período que eles levam para se encontrar pelo tempo de volta de cada um deles.

O primeiro terá dado $360 \div 40 = 9$ voltas.

O segundo terá dado $360 \div 36 = 11$ voltas.

O terceiro terá dado $360 \div 30 = 12$ voltas.

Logo a resposta correta é a letra D.

2.3.3 Algoritmo de Euclides para o Cálculo do M.D.C.

Vamos dar uma breve explicação sobre o algoritmo de Euclides, omitindo sua demonstração. A mesma poderá ser encontrada em [4]. O motivo principal da apresentação desse algoritmos é fornecer uma maneira para o aluno escrever o M.D.C. entre dois números como soma de um múltiplo de um dos números com um múltiplo do outro, de acordo com o teorema de Bézout. Saber apresentar o M.D.C. desta forma nos auxiliará na resolução de equações diofantinas, que serão objetos de estudo na próxima seção.

Supondo $a > b > 1$, para calcularmos (a, b) utilizando o algoritmo de Euclides, efetuamos a divisão de a por b e obtemos quociente q_1 e resto r_1, ou seja, $a = b.q_1 + r_1$ e colocamos os números envolvidos no diagrama a seguir:

	q_1	
a	b	
r_1		

Novamente, fazemos a divisão de b por r_1, obtendo como quociente q_2 e resto r_2, ou seja, $b = r_1.q_2 + r_2$ e colocamos os números envolvidos no diagrama:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

O próximo passo seria a divisão de r_1, obtendo quociente q_3 e resto r_3, ou seja, $r_1 = r_2.q_3 + r_3$ e colocamos os números envolvidos no diagrama:

	q_1	q_2	q_3	
a	b	r_1	r_2	
r_1	r_2	r_3		

O procedimento não pode continuar indefinidamente, pois temos uma sequência $b > r_1 > r_2 > ...$ e termina quando encontramos uma divisão com resto 0. Nesse caso, temos então que (a, b) é o resto obtido na divisão anterior. Por exemplo, suponhamos que no esquema acima tivéssemos encontrado $r_3 = 0$, então, teríamos encontrado $(a, b) = r_2$.

Apresentaremos um exemplo prático para fixar o conceito, escrevendo posteriormente todas as divisões na ordem em que foram realizadas. Essas divisões serão utilizadas após apresentarmos o teorema de Bézout, onde escreveremos $(236, 100) = 4$ como um múltiplo de 236 mais um múltiplo de 100.

Exemplo 12. *Vamos determinar* $(236, 100)$ *utilizando o algoritmo de Euclides: Montando o diagrama e efetuando os cálculos, temos:*

	2	*2*	*1*	*3*	*2*
236	*100*	*36*	*28*	*8*	*4*
36	*28*	*8*	*4*	*0*	

As divisões realizadas nesse exemplo foram as seguintes:

$236 = 2.100 + 36$

$100 = 2.36 + 28$

$36 = 1.28 + 8$

$28 = 3.8 + 4$

$8 = 2.4 + 0$

Observe que na última divisão obtemos resto 0 e como sabemos, $(236, 100)$ *será o resto da divisão anterior, ou seja,* $(236, 100) = 6$.

Teorema 2.3.1 (Teorema de Bézout)**.** *Sejam* a, b *inteiros e* $d = (a, b)$*. Então, existem inteiros* r *e* s *tais que* $d = r.a + s.b$.

Vejamos como escrever (a, b) como um múltiplo de a somado a um múltiplo de b, utilizando o algoritmo de Euclides de trás pra frente. De acordo com o teorema de Bézout, sabemos que isso será sempre possível.

De acordo com o **exemplo 12**, temos o seguinte esquema:

	2	2	1	3	2
236	100	36	28	8	4
36	28	8	4	0	

Vamos escrever as divisões que foram realizadas , isolando os restos e depois substituindo os valores nas outras equações:

(i) $4 = 28 - 3.8$

(ii) $8 = 36 - 1.28$

(iii) $28 = 100 - 2.36$

(iv) $36 = 236 - 2.100$

Substituindo (ii) em (i), temos:

$$\begin{aligned} 4 &= 28 - 3.(36 - 1.28) \\ 4 &= 1.28 - 3.36 + 3.28 \\ 4 &= 4.28 - 3.36 \end{aligned} \tag{2.1}$$

Substituindo (iii) na equação (2.1), temos:

$$\begin{aligned} 4 &= 4.(100 - 2.36) - 3.36 \\ 4 &= 4.100 - 8.36 - 3.36 \\ 4 &= 4.100 + (-11).36 \end{aligned} \tag{2.2}$$

Finalmente, substituímos (iv) na equação (2.2):

$$\begin{aligned} 4 &= 4.100 + (-11).(236 - 2.100) \\ 4 &= 4.100 + (-11).236 + 22.100 \\ 4 &= 26.100 + (-11).236 \end{aligned} \tag{2.3}$$

Acabamos de escrever na equação (2.3), o $(236, 100) = 4$ como um múltiplo de 100 somado a um múltiplo de 236. Neste caso dizemos que 4 é combinação linear de 100 e 236.

Escrever o M.D.C. dessa forma será muito importante para os próximos resultados.

2.4 EQUAÇÕES DIOFANTINAS LINEARES

Vamos imaginar a seguinte situação: Possuímos apenas notas de 20 e 50 reais e precisamos pagar uma compra no valor de 330 reais. Seria possível agrupar essa quantia com os tipos de notas que possuímos?

Sabemos que sim, é possível, com por exemplo 5 notas de 50 e 4 notas de 20, ou ainda 1 nota de 50 e 14 notas de 20. Mas essas não são as únicas possibilidades. Vamos descrever matematicamente essa situação, chamando de x a quantidade de notas de 20 e y a quantidade de notas de 50. Logo, o número $20.x$ será o valor total em notas de 20 reais e $50.y$ será o valor total em notas de 50 reais. Somando esses dois valores, o resultado

deve ser sempre igual a 330 reais, o que pode ser escrito através da seguinte equação: $20.x + 30.y = 330$.

Essa equação é denominada "equação diofantina linear"em homenagem a Diophanto de Alexandria (em torno de 250 d.C.) que foi o primeiro a considerar problemas desse tipo.

Como já vimos, a equação possui mais de uma solução e vamos nos basear nela para aprendermos como se resolve esse tipo de equação.

Teorema 2.4.1. *Sejam a, b inteiros não ambos nulos, $c \in Z$ e $d = (a, b)$. A equação $a.x + b.y = c$ tem solução se e somente se d divide c.*

Além disso, se x_0, y_0 são tais que $a.x_0 + b.y_0 = c$ então a solução geral da equação $a.x + b.y = c$ é

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t, \end{cases}$$

com $t \in Z$.

Vamos verificar isso com a equação inicial. Nela, temos que $a = 20, b = 50$ e $c = 330$. Pelo Teorema 2.4.1, a equação só possui soluções inteiras se $(20, 50)$ divide 330. Temos que $(20, 50) = 10$ e como 10 divide 330, a equação $20.x + 50.y = 330$ possui soluções inteiras, como já sabíamos.

Vamos então dar sequência a resolução da equação, dividindo ambos os membros por $(20, 50) = 10$. Isso será sempre possível se a equação possuir solução.

A equação $20.x + 50.y = 330$ é equivalente a $\frac{20.x}{10} + \frac{50.x}{10} = \frac{330}{10}$ ou seja,

$$2.x + 5.y \quad = \quad 33. \tag{2.4}$$

Essa última equação é equivalente a primeira e como sabemos possui solução. Vamos então utilizar o algoritmo de Euclides para escrever de acordo com o teorema de Bézout o $(2, 5) = 1$ como um produto envolvendo o fator 2 somado a um produto envolvendo o fator 5. Vejamos:

	2	2
5	2	1
1	0	

Reescrevendo as divisões:

- $5 = 2.2 + 1 \Rightarrow 1 = 5 - 2.2$
- $2 = 1.2 + 0$

Substituindo a segunda equação na primeira, temos:

$$\begin{aligned} 1 &= 5 - 2.(1.2 + 0) \\ 1 &= 1.5 - 2.2 \\ 1 &= 2.(-2) + 5.1 \end{aligned} \tag{2.5}$$

Vamos fazer uma comparação entre (2.4) e (2.5), ou seja,

- $2.x + 5.y = 33$
- $2.(-2) + 5.1 = 1$

Podemos observar que as equações possuem os mesmos valores para a e b. Vamos então igualar c, multiplicando (2.5) por 33, obtendo

- $2.(-66) + 5.33 = 33$

Encontramos assim uma solução para a equação (2.4).

Logo, temos que uma das soluções inteiras é $x_0 = -66$ e $y_0 = 33$. Essa é uma solução particular, mas não pode ser uma solução do problema, uma vez que x e y são quantidades de notas e $x_0 = -66$ não é possível. Vejamos então como obter as outras soluções.

De acordo com o teorema 2.4.1, temos que a solução geral é da forma

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t, \end{cases}$$

com $t \in Z$. Como $a = 20$, $b = 50$, $d = 10$ e determinamos $x_0 = -66$ e $y_0 = 33$, a solução geral será

$$\begin{cases} x = -66 + 5.t \\ y = 33 - 2.t, \end{cases}$$

com $t \in Z$.

A equação em si possui infinitas soluções, mas no contexto do problema devemos ter $x \geq 0$ e $y \geq 0$, com x e $y \in Z$, pois x e y são números de notas de 20 e 50 reais respectivamente. Então,

$$\begin{aligned} -66 + 5.t &\geq 0 \\ t &\geq 13,2 \end{aligned} \quad \text{e} \quad \begin{aligned} 33 - 2.t &\geq 0 \\ t &\leq 16,5 \end{aligned}$$

Como $t \in Z$, devemos ter $14 \leq t \leq 16$. Vamos organizar esses valores em uma tabela.

t	x	y
14	$-66 + 5.14 = 4$	$33 - 2.14 = 5$
15	$-66 + 5.15 = 9$	$33 - 2.15 = 3$
16	$-66 + 5.16 = 14$	$33 - 2.16 = 1$

Podemos notar que temos mais uma solução, além das duas soluções que indicamos no início do problema, totalizando assim três soluções.

Exemplo 13. *Se um macaco sobe uma escada de dois em dois degraus, sobra um degrau; se ele sobe de três em três degraus, sobram dois degraus. Quantos degraus a escada possui, sabendo que o número de degraus é múltiplo de sete e está compreendido entre 40 e 100.*

Solução: *Seja D o número de degraus.*

Se o macaco sobe a escada de 2 em 2 degraus e sobra 1, temos que $D = 2.x + 1$.

Se o macaco sobe a escada de 3 em 3 degraus e sobra 2, temos que $D = 3.y + 2$.

Igualando as duas equações, temos:

$$2.x - 3.y = 1$$

Observando a equação, percebemos que uma equação particular será dada por $x_0 = 2$ e $y_0 = 1$ e sendo assim, a solução geral será dada por $x = 2 + 3.t$ e $y = 1 + 2.t$, pois $(2, 3) = 1$.

Por outro lado, como $40 \leq D \leq 100$ e é múltiplo de 7 Isto implica que $6 \leq t \leq 15$, e para que D seja múltiplo de 7, devemos ter $t = 12$, ou seja, $D = 77$.

3 ARITMÉTICA MODULAR

Neste capítulo estudaremos a aritmética modular, também conhecida como aritmética dos restos, uma das ferramentas mais importantes da teoria dos números. Essa teoria foi desenvolvida por Carl Friedrich Gauss ao observar a frequência em que a frase do tipo "a dá o mesmo resto que b quando divididos por m", introduzindo uma nova notação que denominou "congruência". A simbologia encontrada por Gauss para descrever a frase acima foi $a \equiv b \mod m$ (lê-se a é congruente a b módulo m). Vamos então introduzir essa noção, com suas principais propriedades utilizando exemplos e propondo atividades práticas que contam com o auxílio da aritmética modular, esperando assim um maior interesse por parte dos alunos.

Vamos então introduzir essa noção com suas principais propriedades, utilizando exemplos atuais de algumas questões retiradas de provas como ENEM, OBMEP e alguns vestibulares, resolvidas utilizando a aritmética modular. Gostaria de observar que no momento de uma prova, talvez o aluno não resolva uma questão com todo o formalismo aplicado aqui, porém conhecer essa teoria facilitará muito o seu raciocínio, além de ser uma ferramenta a mais que poderá ser utilizada a seu favor.

3.1 CONGRUÊNCIA

Definição 1. *Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais e escrevemos:*

$$a \equiv b \ mod \ m$$

Exemplo 14. *Temos que $14 \equiv 8 \mod 6$, pois tanto 14 quanto 8 deixam resto 2 ao serem divididos por 6.*

Exemplo 15. *Temos que $9 \equiv 1 \mod 4$, pois tanto 9 quanto 1 deixam resto 1 ao serem divididos por 4.*

Decorre da definição que a congruência módulo um natural m é uma relação de equivalência, como enunciaremos abaixo.

Proposição 3.1.1. *Seja $m \in N$. Para todos a, b, $c \in Z$, tem-se que:*

(i) $a \equiv a \ mod \ m$.

(ii) *se* $a \equiv b \ mod \ m$, *então* $b \equiv a \ mod \ m$.

(iii) *se* $a \equiv b \ mod \ m$ *e* $b \equiv c \ mod \ m$, *então* $a \equiv c \ mod \ m$.

Para verificar se dois números são congruentes módulo m, não precisamos fazer a divisão de cada um deles por m, basta apenas verificar se m divide a diferença entre eles, como descreve a proposição as seguir. Vamos apresentar a demonstração dessa proposição por usar o conceito de divisão euclidiana, um assunto que os alunos estão bem familiarizados.

Proposição 3.1.2. *Suponha que a, b, m ∈ Z, com m > 1. Tem-se que a ≡ b mod m se, e somente se, m |(b - a).*

Demonstração. Seja $a = m.q + r$, com $0 \leq r < m$ e $b = m.q' + r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Logo

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

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

Vamos agora apresentar uma série de propriedades das congruências, onde faremos as demonstrações de (i) e (ii) utilizando o resultado da Proposição 3.1.2. As demonstrações dos outros resultados podem ser encontrados em [4] que nos serviu de referência para a escrita desse trabalho.

Sejam a, b, c, d e $m \in Z$, com $m > 1$.

(i) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então $a + c \equiv b + d$ mod m.

(ii) Se $a \equiv b$ mod m e $c \equiv d$ mod m, então $a.c \equiv b.d$ mod m.

Demonstração. Suponhamos que $a \equiv b$ mod m e $c \equiv d$ mod m. Logo, temos que $m \mid b - a$ e $m \mid d - c$.

(i) Basta observar que $m \mid (b - a) + (d - c)$ e portanto, $m \mid (b + d) - (a + c)$, o que prova o primeiro item.

(ii) Basta notar que $bd - ac = d(b - a) + a(d - c)$ e concluir que $m \mid bd - ac$. □

(iii) Para todo $n \in N$, se $a \equiv b$ mod m, então $a^n \equiv b^n$ mod m

(iv) Tem-se que $a + c \equiv b + c$ mod m se, e somente se, $a \equiv b$ mod m.

(v) Temos que $a.c \equiv b.c$ mod m se, e somente se, $a \equiv b$ mod $\frac{m}{(c,m)}$, para $c \neq 0$.

Vamos resolver um exemplo numérico de cada uma das propriedades para melhor fixá-las.

(i) Temos que $7 \equiv 3 \bmod 4$ e $21 \equiv 1 \bmod 4$, então $7 + 21 \equiv 3 + 1 \bmod 4$, ou seja $28 \equiv 4 \bmod 4$.

(ii) Temos que $14 \equiv 4 \bmod 5$ e $3 \equiv 8 \bmod 5$, então $14.3 \equiv 4.8 \bmod 5$, ou seja, $42 \equiv 32 \bmod 5$.

(iii) Temos que $3 \equiv 1 \bmod 2$, então $3^4 \equiv 1^4 \bmod 2$.

(iv) Temos que $5 + 7 \equiv 25 + 7 \bmod 10$ se e somente se $5 \equiv 25 \bmod 10$.

(v) Temos que $7.5 \equiv 15.5 \bmod 10$ se e somente se $7 \equiv 15 \bmod \frac{10}{(5,10)}$, ou seja, $7 \equiv 15 \bmod 2$.

3.2 PEQUENO TEOREMA DE FERMAT

Vamos enunciar o pequeno teorema de Fermat, sem fazer a demonstração, lembrando que a mesma poderá ser encontrada em [4]. Apresentaremos o teorema usando a notação de congruências.

Teorema 3.2.1. *Dado um número primo p, tem-se que p divide o número $a^p - a$ para todo $a \in N$.*

Se $p \mid a^p - a$, podemos escrever o pequeno teorema de Fermat utilizando a notação de congruências da seguinte forma:

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

Colocando a em evidência, temos $p \mid a(a^{p-1} - 1)$. Nesse caso, se p não divide a, então $p \mid a^{p-1} - 1$, o que na linguagem de congruências, temos:

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

Exemplo 16. *Temos que $7^5 \equiv 7$ mod 5 e podemos escrever ainda $7^4 \equiv 1$ mod 5.*

Exemplo 17. *Temos que $2^{53} \equiv 2$ mod 53 e podemos escrever ainda que $2^{52} \equiv 1$ mod 53.*

Perceber quando usar o pequeno teorema de Fermat, será uma alternativa para resolver muitos problemas.

Vamos agora apresentar uma série de exemplos de algumas provas, como OBMEP, ENEM, vestibulares, entre outras que serão resolvidos com o auxílio da congruência modular.

Exemplo 18. *(OBMEP 2010 - Nível 1) O dobro de um número dividido por 5 deixa resto 1. Qual é o resto da divisão desse número por 5?*

Solução: *Seja x o número em questão. O problema nos diz que $5 \mid 2x - 1$. Podemos escrever esse problema utilizando congruências da seguinte forma:*

$$2x \equiv 1 \ mod\ 5.$$

Isso significa que $2x - 1$ é um múltiplo de 5, ou seja, existe um $y \in Z$ tal que $2x - 1 = 5y$, o que nos leva a seguinte equação diofantina

$$2x + 5y = 1$$

que sabemos que possui solução, pois (2,5)=1.

Escrevendo o m.d.c. como um múltiplo de 2 mais um múltiplo de 5, temos:

$$\begin{aligned} 5 &= 2.2 + 1, \\ 1 &= 2.(-2) + 5.1. \end{aligned}$$

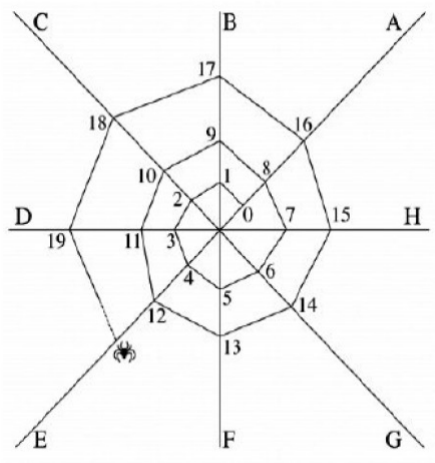
Logo, uma solução particular será $x_0 = -2$ e $y_0 = 1$. Como estamos apenas interessados em x e sabemos que a solução geral é da forma $x = x_0 + \frac{b}{d}t$, com $t \in Z$, temos:

$x = -2 + 5t$, que deixa sempre resto 3 ao ser dividido por 5.

Organizando alguns valores numa tabela, para melhor visualização, temos:

t	x
1	*3*
2	*8*
3	*13*
4	*18*

Exemplo 19. *(OBMEP-Nível 2) Sejam A, B, C, D, E, F, G e H 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?*



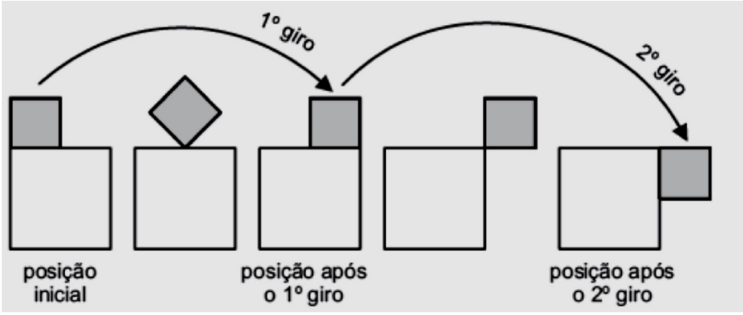
Solução: *Como são 8 pontos de apoio, teremos uma congruência módulo 8.*

Observando o esquema, temos:

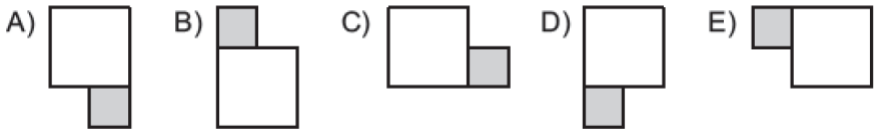
- *Sobre o fio A estão os números congruentes a 0 módulo 8, pois deixam resto 0 quando divididos por 8.*
- *Sobre o fio B estão os números congruentes a 1 módulo 8, pois deixam resto 1 quando divididos por 8.*
- *Sobre o fio C estão os números congruentes a 2 módulo 8, pois deixam resto 2 quando divididos por 8.*
- *Sobre o fio D estão os números congruentes a 3 módulo 8, pois deixam resto 3 quando divididos por 8.*
- *Sobre o fio E estão os números congruentes a 4 módulo 8, pois deixam resto 4 quando divididos por 8.*
- *Sobre o fio F estão os números congruentes a 5 módulo 8, pois deixam resto 5 quando divididos por 8.*
- *Sobre o fio G estão os números congruentes a 6 módulo 8, pois deixam resto 6 quando divididos por 8.*
- *Sobre o fio H estão os números congruentes a 7 módulo 8, pois deixam resto 7 quando divididos por 8.*

Como $118 \equiv 6 \mod 8$ *temos que o número 118 estará sobre o fio G.*

Exemplo 20. *(OBMEP - 2012 - Nível 3) Um quadrado de lado 1 cm roda em torno de um quadrado de lado 2 cm, como na figura, partindo da posição inicial e completando um giro cada vez que um de seus lados fica apoiado em um lado do quadrado maior.*



Qual das figuras a seguir representa a posição dos dois quadrados após o 2012º giro?



Solução: *O quadrado em cinza faz exatamente 8 movimentos para retornar a posição inicial e por isso teremos uma congruência módulo 8. Como* $2012 \equiv 4$ *mod 8, temos que o dado irá parar quatro posições após a posição inicial. Logo a resposta correta é a letra A.*

Exemplo 21. *(OBMEP - 2012 - Nível 3) Cinco cartas, inicialmente dispostas como na figura, serão embaralhadas. Em cada embaralhamento, a primeira carta passa a ser a segunda,a segunda passa a ser a quarta, a terceira passa a ser a primeira, a quarta passa a ser a quinta e a quinta passa a ser a terceira. Qual será a primeira carta após 2012 embaralhamentos?*

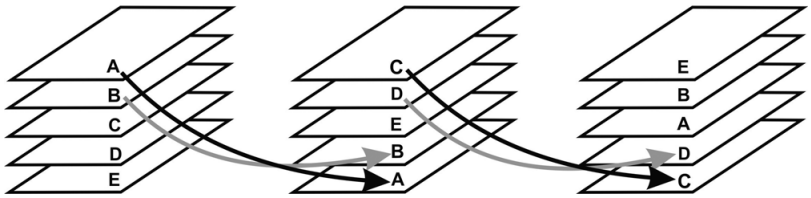
Solução: *Primeiramente vamos organizar esses dados em uma tabela de acordo com os embaralhamentos.*

	1^a *Carta*	2^a *Carta*	3^a *Carta*	4^a *Carta*	5^a *Carta*
Posição Inicial	*A*	*2*	*3*	*4*	*5*
Embaralhamento I	*3*	*A*	*5*	*2*	*4*
Embaralhamento II	*5*	*3*	*4*	*A*	*2*
Embaralhamento III	*4*	*5*	*2*	*3*	*A*
Embaralhamento IV	*2*	*4*	*A*	*5*	*3*
Embaralhamento V	*A*	*2*	*3*	*4*	*5*

De acordo com os dados que organizamos na tabela, podemos perceber que após 5 embaralhamentos, as cartas voltam a posição inicial. Logo, temos uma congruência módulo 5.

Como estamos interessados em saber a posição da primeira carta após o embaralhamento 2012 e $2012 \equiv 2 \mod 5$*, temos que as posições das cartas estarão de acordo com o embaralhamento II, onde a primeira carta é a de número 5.*

Exemplo 22. *(OBMEP – Banco de Questões 2012)Estefânia tem cinco cartas marcadas com as letras A, B, C, D e E, empilhadas nessa ordem de cima para baixo. Ela embaralha as cartas pegando as duas de cima e colocando-as, com a ordem trocada, embaixo da pilha. A figura mostra o que acontece nas duas primeiras vezes em que ela embaralha as cartas.*



Se Estefânia embaralhar as cartas 74 vezes, qual carta estará no topo da pilha?

(a) A

(b) B

(c) C

(d) D

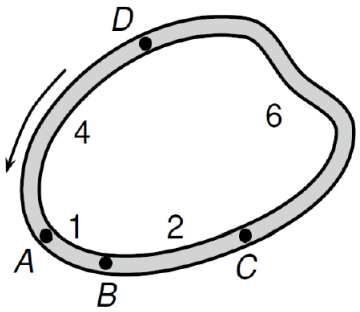
(e) E

Solução: *Vamos novamente montar uma tabela que nos ajude a obtermos algum padrão na posição das cartas.*

Pilha Inicial	*Pilha I*	*Pilha II*	*Pilha III*	*Pilha IV*	*Pilha V*	*Pilha VI*
A	*C*	*E*	*A*	*C*	*E*	*A*
B	*D*	*B*	*D*	*B*	*D*	*B*
C	*E*	*A*	*C*	*E*	*A*	*C*
D	*B*	*D*	*B*	*D*	*B*	*D*
E	*A*	*C*	*E*	*A*	*C*	*E*

De acordo com a tabela podemos perceber que as cartas voltam a posição inicial a cada 6 movimentos. Logo, temos uma congruência módulo 6. Como queremos saber qual a carta estará no topo após Estefânia ter embaralhado 74 vezes, devemos notar que $74 \equiv 2 \mod 6$ *e por isso as cartas estarão dispostas de acordo com a pilha II, onde a carta E aparece no topo.*

Exemplo 23. *(Banco de Questões 2012 - Nível 3)A figura abaixo representa o traçado de uma pista de corrida.*



Os postos A, B, C e D são usados para partidas e chegadas de todas as corridas. As distâncias entre postos vizinhos, em quilômetros, estão indicadas na figura e as corridas são realizadas no sentido indicado pela flecha. Por exemplo, uma corrida de 17 quilômetros pode ser realizada com partida em D e chegada em A.

(a) Quais são os postos de partida e chegada de uma corrida de 14 quilômetros?

(b) E para uma corrida de 100 quilômetros, quais são esses postos?

(c) Mostre que é possível realizar corridas com extensão igual a qualquer número inteiro de quilômetros.

Solução:

(a) Temos uma congruência módulo 13, pois a pista tem 13 quilômetros e como $14 \equiv 1 \mod 13$*, devemos ter uma volta completa mais 1 quilômetro. Logo, podemos partir de A dar uma volta completa e chegar em B.*

(b) Temos que $100 \equiv 9$ *mod 13, ou seja, devemos dar 7 voltas completas, pois o quociente da divisão de 100 por 13 é 7, mais 9 quilômetros. O único trecho com 9 quilômetros na pista é de A até D, teremos 7 voltas completas a partir de A e na oitava volta iremos até D.*

(c) Como o resto da divisão podem ser apenas os números 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11 e 12, vamos construir uma tabela mostrando que para um $K \in Z$ *e* $0 \leq r < 13$ *sempre poderemos teremos um ponto de partida e chegada.*

$13.K \equiv r$ *mod 13*	*Ponto de Partida*	*Ponto de Chegada*
$13.K \equiv 0$ *mod 13*	*Qualquer Ponto*	*Mesmo Ponto da Partida*
$13.K \equiv -1 \equiv 12$ *mod 13*	A	B
$13.K \equiv -2 \equiv 11$ *mod 13*	B	C
$13.K \equiv -3 \equiv 10$ *mod 13*	A	C
$13.K \equiv -4 \equiv 9$ *mod 13*	D	A
$13.K \equiv -5 \equiv 8$ *mod 13*	D	B
$13.K \equiv -6 \equiv 7$ *mod 13*	C	D
$13.K \equiv -7 \equiv 6$ *mod 13*	D	C
$13.K \equiv -8 \equiv 5$ *mod 13*	B	D
$13.K \equiv -9 \equiv 4$ *mod 13*	A	D
$13.K \equiv -10 \equiv 3$ *mod 13*	C	A
$13.K \equiv -11 \equiv 2$ *mod 13*	C	B
$13.K \equiv -12 \equiv 1$ *mod 13*	B	A

Por exemplo, se quisermos um percurso de 153 quilômetros, basta tomarmos a congruência $13.K \equiv 3$ *mod 13, onde* $K = 12$*. Nesse caso daremos 11 voltas partindo e voltando a C e na 13º iremos apenas até A.*

Exemplo 24. *(ENEM 2013 - Adaptada) O ciclo de atividade magnética do Sol tem um período de 11 anos. O início do primeiro ciclo registrado se deu no começo de 1755 e se estendeu até o final de 1765. Desde então, todos os ciclos de atividade magnética do Sol têm sido registrados.*

Disponível em: http://g1.globo.com. Acesso em: 27 fev. 2013

De acordo com os dados acima, é correto afirmar que um determinado ciclo de atividade magnética do Sol teve início no ano de:

(a) 1842

(b) 1854

(c) 1906

(d) 1958

(e) 2013

Solução: *Como o ciclo de atividade magnética do sol tem um período de 11 anos, teremos uma congruência módulo 11.*

Como queremos saber dentre as respostas qual o ano em que se inicia um novo ciclo, podemos testar cada uma delas, buscando a única que será congruente a 1755 módulo 11, que é o início do primeiro ciclo registrado.

Assim, temos:

(a) $1842 \not\equiv 1755 \ mod\ 11$, *pois* $11 \nmid (1842\text{-}1755)$.

(b) $1854 \equiv 1755 \ mod\ 11$, *pois* $11 \mid (1854\text{-}1755)$.

(c) $1906 \not\equiv 1755 \ mod\ 11$, *pois* $11 \nmid (1906\text{-}1755)$.

(d) $1958 \not\equiv 1755 \ mod\ 11$, *pois* $11 \nmid (1958\text{-}1755)$.

(e) $2013 \not\equiv 1755 \ mod\ 11$, *pois* $11 \nmid (2013\text{-}1755)$.

Temos que a único ano congruente a 1755 módulo 11 é 1854, letra b. Poderíamos ter parado aí, pois temos apenas uma resposta correta, mas analisamos as outras respostas para ilustração.

Exemplo 25. *(Unesp 98) Imagine os números inteiros não negativos formando a seguinte tabela:*

0	3	6	9	12	...
1	4	7	10	13	...
2	5	8	11	14	...

(a) Em que linha da tabela se encontra o número 319? Por quê?

(b) Em que coluna se encontra esse número? Por quê?

Solução:

(a) Observando a tabela, temos que na primeira linha estão os números que deixam resto 0 ao serem divididos por 3. Logo os números são congruentes a 0 módulo 3.

Na segunda linha, os números deixam resto 1 ao serem divididos por 3, ou seja, são congruentes a 1 módulo 3.

Já na terceira linha, temos os números que deixam resto 2 na divisão por 3, ou seja, são congruentes a 2 módulo 3.

Como $319 \equiv 1$ *mod 3, temos que o resto da sua divisão por 3 é 1 e com isso, pertencerá a segunda linha.*

(b) Contando os números em colunas iniciando do 0, temos que o número 319 ocupa a posição 320. Cada coluna é composta por 3 números, vamos então verificar a congruência de 320 módulo 3.

Como $320 \equiv 2$ *mod 3, temos que a coluna ocupada pelo número 319 será o quociente da divisão de 320 por 3, mais 1.*

Mas $320 = 106 \times 3 + 2$ *e com isso a coluna ocupada pelo número 310 será a 107.*

3.3 ARITMÉTICA MODULAR

Introduzida por Gauss em seu livro Disquisitiones Aritmeticae publicado em 1801, a aritmética modular também é conhecida como aritmética dos fenômenos cíclicos.

Tomando sempre m como um inteiro maior que 1, associaremos a um número inteiro a qualquer o símbolo $\bar{a}$ representado o resto de sua divisão por m.

Definição 2. *Seja a um inteiro. Chama-se classe de congruência de a módulo m o conjunto formado por todos os inteiros que são congruentes ao número a módulo m. Denotaremos esse conjunto por* $\bar{a}$*. Temos então:*

$$\bar{a}=\{x \in Z / x \equiv a \ mod \ m\}.$$

Em outras palavras que número pertence a uma classe de congruência $\bar{a}$, se deixa o mesmo resto que a na divisão por m.

Proposição 3.3.1. *Sejam a e b inteiros. Então* $a \equiv b$ *mod m se, e somente se,* $\bar{a} = \bar{b}$*.*

Demonstração. Suponhamos que $a \equiv b \bmod m$; queremos provar que $\bar{a} = \bar{b}$, isto é, uma igualdade entre conjuntos.

Dado $x \in \bar{a}$, temos por definição, que $x \equiv a \bmod m$. Da propriedade transitiva da congruência (proposição 3.1.1 parte (iii)) e da hipótese, segue imediatamente que $x \in \bar{b}$. Logo, $\bar{a} \subset \bar{b}$. Para provar que $\bar{b} \subset \bar{a}$, procedemos de forma análoga.

Reciprocamente, se $\bar{a} = \bar{b}$, como $a \in \bar{a}$, temos também que $a \in \bar{b}$, logo, $a \equiv b \bmod m$. □

Vejamos, como exemplo, todas as classes possíveis para $m = 6$:

- $\bar{0} = \{0, 6, -6, 12, -12, \cdots\}$
- $\bar{1} = \{1, 7, -5, 13, -11, \cdots\}$
- $\bar{2} = \{2, 8, -4, 14, -10, \cdots\}$
- $\bar{3} = \{3, 9, -3, 15, -9, \cdots\}$
- $\bar{4} = \{4, 10, -2, 16, -8, \cdots\}$
- $\bar{5} = \{5, 11, -1, 17, -7, \cdots\}$

Não escrevemos por exemplo as classes $\bar{6}$, $\bar{7}$, $\bar{8}$ e outras, pois $\bar{6} = \bar{0}$, $\bar{7} = \bar{1}$, $\bar{8} = \bar{2}$ e assim sucessivamente.

Cada um dos inteiros pertencentes a uma dada classe diz-se representante dessa classe. Por exemplo, 10 é um representante da classe $\bar{4}$ módulo 6, assim como 13 é um representante da classe $\bar{1}$ módulo 6.

Podemos denotar por Z_m o conjunto de congruências módulo m. Chamamos esse conjunto de inteiros módulo m.

Tomando o sistema de restos (resíduos) mais simples, podemos escrever $Z_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$.

Vale observar que esse conjunto possui exatamente m elementos.

Assim: $Z_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$.

3.3.1 **Operações**

As operações decorrem diretamente das propriedades e são definidas da seguinte forma:

Sejam a, a', b e b' inteiros em que $\bar{a} = \bar{a'}$ e $\bar{b} = \bar{b'}$. Então:

- $\overline{a+b} = \overline{a'+b'}$
- $\overline{a.b} = \overline{a'.b'}$

Vamos apresentar alguns exemplos através da construção de algumas tabelas de soma e produto:

Exemplo 26. *Tabelas de soma e produto em Z_4:*

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	0	1	0
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Exemplo 27. *Tabelas de soma e produto em Z_5:*

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Atividades

Apresentaremos algumas atividades retiradas de [5], que está disponível no site da OBMEP. Nosso objetivo é aplicar alguns resultados de aritmética modular.

1) Verifique se são verdadeiras ou falsas as seguintes afirmações:

   (a) $35 \equiv 27 \bmod 4$

   (b) $72 \equiv 32 \bmod 5$

   (c) $83 \equiv 72 \bmod 5$

   (d) $78 \equiv 33 \bmod 9$

2) Se $a \equiv b \bmod 4$, mostre que $a \equiv b \bmod 2$.

3) Mostre que $10^n \equiv 1 \bmod 9$, para todo número natural n.

4) Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine os restos da divisão de $a + b$, $a - b$ e de $b - a$ por 7.

   Sugestão: Para o último resto, observe que $-4 \equiv 3 \bmod 7$.

5) Sejam a e b dois números inteiros cujos restos da divisão por 7 são respectivamente 6 e 2. Determine o resto da divisão de $a \times b$ por 7.

6) Sabendo que $2^4 = 16 \equiv -1 \bmod 17$, ache o resto da divisão de 2^{30} por 17.

7) Determine o resto da divisão de 2^{325} por 17.

8) Diga se é Verdadeiro ou Falso:

   (a) $19 \equiv 7 \bmod 2$

   (b) $1213 \equiv 212 \bmod 13$

9) Se $1066 \equiv 2090 \bmod m$, quais são os possíveis valores de m?

10) Ache todos os inteiros x, tais que $0 < x < 15$ e $3.x \equiv 6 \bmod 15$.

11) Dê todos os inteiros positivos x menores que 100, tais que $x \equiv 8 \bmod 13$.

12) Determine as tabelas da adição e da multiplicação para Z_6.

Solução das Atividades

1) (a) Como $4 \mid (35 - 27) = 8$, temos que a congruência é verdadeira, ou seja, 35 e 27 deixam o mesmo resto quando divididos por 4.

   (b) Como $5 \mid (72 - 32) = 40$, temos que a congruência é verdadeira, ou seja, 72 e 32 deixam o mesmo resto quando divididos por 5.

   (c) Como $5 \nmid (83 - 72) = 11$, temos que a congruência é falsa, ou seja, 83 e 72 deixam restos diferentes quando divididos por 5.

   (d) Como $9 \mid (78 - 33) = 45$, temos que a congruência é verdadeira, ou seja, 78 e 33 deixam o mesmo resto quando divididos por 9.

2) Se $a \equiv b \bmod 4$, temos de acordo com a proposição 3.1.2 que $4 \mid (a - b)$, mas como $4 = 2.2$, temos que $2 \mid (a - b)$, ou seja, $a \equiv b \bmod 2$.

3) Antes de mostrarmos o resultado, vamos verificar alguns casos particulares:

   - $10^1 - 1 = 10 - 1 = 9$
   - $10^2 - 1 = 100 - 1 = 99$
   - $10^3 - 1 = 1000 - 1 = 999$
   - $10^4 - 1 = 10000 - 1 = 9999$

   Podemos observar que quando temos um potencia de 10 menos 1, o resultado é um número composto apenas de algarismos noves, cuja quantidade é igual ao expoente da potência de 10.

   Assim, se $10^n \equiv 1 \bmod 9$, então $9 \mid (10^n - 1) = \underbrace{999...9}_{n}$, o que prova a congruência é válida, pois $\underbrace{999...9}_{n} \equiv 0 \bmod 9$ para qualquer n.

4) Se a e b deixam restos 6 e 2 respectivamente na divisão por 7, podemos escrever:

   $a \equiv 6 \bmod 7$ e $b \equiv 7 \bmod 7$.

   De acordo com as propriedades, temos:

   - $a + b \equiv 6 + 2 \equiv 1 \bmod 7$, ou seja, $a + b$ deixa resto 1 na divisão por 7.
   - $a - b \equiv 6 - 2 \equiv 4 \bmod 7$, ou seja, $a - b$ deixa resto 4 na divisão por 7.
   - $b - a \equiv 2 - 6 \equiv -4 \equiv 3 \bmod 7$, ou seja, $b - a$ deixa resto 3 na divisão por 7.

5) De acordo com as propriedades, temos $a.b \equiv 6.2 \equiv 12 \equiv 5 \bmod 7$.

6) Como $2^4 \equiv 16 \equiv -1 \bmod 17$ e sabemos que $30 = 4.7 + 2$, vamos aplicar as propriedades de congruências:

   $(2^4)^7 \equiv (-1)^7 \bmod 17$, ou seja, $2^{28} \equiv -1 \bmod 17$.

   Precisamos ainda adicionar duas unidades ao expoente para obtermos 2^{30}. Isso pode ser feito multiplicando a congruência acima por 2^2 em ambos os membros.

   Assim, $2^{28}.2^2 \equiv (-1).2_2 \bmod 17$, ou seja, $2^{30} \equiv -4 \equiv 13 \bmod 17$.

   Logo o resto da divisão é 13.

7) Sabemos que $2^4 \equiv 16 \equiv -1 \bmod 17$. Como $325 = 4.80 + 5$, temos:

   $(2^4)^{80} \equiv (-1)^{80} \bmod 11$, ou seja, $2^{230}.2^5 \bmod 17$, ou seja, $2^{325} \equiv 32 \equiv 15 \bmod 17$.

   Logo, o resto da divisão de 2^{325} por 7 é 15.

8) (a) Como $2 \mid (19 - 7)$, temos que a congruência é verdadeira.

   (b) Como $13 \mid (1213 - 212)$, temos que a congruência é verdadeira.

9) Devemos verificar os valores de m tais que $m \mid (2090 - 1066) = 1024$.

   Logo, temos que $m \in \{2, 4, 8, 16, 32, 64, 128, 256, 512, 1024\}$.

10) Se $3.x \equiv 6 \bmod 15$, então $15 \mid (3x - 6)$, ou seja, $3.5 \mid 3.(x - 2)$. Logo basta verificar os valores de $0 < x < 15$ tais que $5 \mid (x - 2)$.

    Logo, temos que $x \in \{2, 7, 12\}$.

11) Se $x \equiv 8 \bmod 13$, então $13 \mid (x - 8)$. Como $0 < x < 100$, temos que $x \in \{8, 21, 34, 47, 60, 73, 86, 99\}$.

12) Tabelas de soma e produto em Z_6.

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4 ATIVIDADES CONTEXTUALIZADAS - APLICAÇÕES

Neste capítulo iremos mostrar algumas atividades contextualizadas envolvendo o uso da aritmética modular. Primeiro mostraremos como determinar o dígito verificador de dois sistemas de identificação, o ISBN utilizado para identificar livros, entre outros, e o CPF utilizado como cadastro de pessoas físicas no Brasil. Vamos apresentar também uma atividade explorando calendários que nos permitirá determinar o dia da semana em que uma pessoa nasceu ou de uma outra data qualquer. Finalizando, faremos uma breve introdução a criptografia através do deslocamento de letras no alfabeto.

Em todas as atividades, daremos alguns exemplos e deixaremos alguns exercícios, que os alunos irão realizar como uma tarefa extra classe fazendo o registro das mesmas.

Esperamos que esse capítulo, evidencie ainda mais o quanto a aritmética modular está presente em várias situações práticas, dando mais sentido ao conteúdo estudado ao longo desse trabalho.

As aplicações a seguir são baseadas em [8] e parte do texto foi desenvolvido com referência em [9].

Sistemas de Identificação

Os sistemas de identificação que apresentaremos são uma sequência de números, utilizados como o próprio nome diz, para identificar algo.

Esses sistemas possuem um ou dois dígitos verificadores, que são utilizados para detectar algum erro cometido em algum dos números anteriores da sequência. Esses dígitos são muito importantes, uma vez que não é tão simples identificar um erro em uma sequência de números, como um erro em uma palavra de nosso idioma.

4.1 ISBN

A sigla ISBN é uma abreviação de International Standard Book Number que em português significa Número Padrão Internacional do Livro. Esse sistema de identificação foi criado no Reino Unido em 1967, com a finalidade de identificar numericamente um livro.

Até o fim de 2006 era utilizado o ISBN-10, um código composto por 9 dígitos mais um dígito verificador. A partir de 2007, o ISBN passou a ser constituído por 13 dígitos, sendo o último deles o dígito verificador.

Vamos agora descrever como se calcula o dígito verificador do ISBN-13. Essa atividade pode ser utilizada em sala de aula, com livros trazidos pelos alunos:

1º) Primeiramente pegamos a sequência dos 12 primeiros dígitos e os multiplicamos

alternadamente por 1 e 3 da esquerda para a direita.

2º) Em seguida, somamos todos os produtos.

3º) Dividimos o resultado encontrado por 10, determinando o resto da divisão.

4º) Subtraímos de 10 o resto encontrado na divisão anterior, determinando assim o dígito verificador.

Se analisarmos bem cada um dos passos, percebemos que o 3º passo descreve uma congruência módulo 10.

Vamos verificar isso matematicamente:

Sejam $a_1a_2a_3a_4a_5a_6a_7a_8a_9a_{10}a_{11}a_{12}$ a sequência dos 12 primeiros dígitos.

Os passos 1 e 2 acima nos descreve a seguinte soma:

$S_{12} = a_1 + 3.a_2 + a_3 + 3.a_4 + a_5 + 3.a_6 + a_7 + 3.a_8 + a_9 + 3.a_{10} + a_{11} + 3.a_{12}$

No passo 3, determinamos o resto r da seguinte forma:

$S_{12} \equiv r \mod 10$.

O passo 4 nos diz que o dígito verificador a_{13} será dado por $10 - r$.

Temos então que $S_{12} + a_{13} \equiv r + 10 - r \equiv 10 \equiv 0 \mod 10$.

Logo, $S_{12} + a_{13} \equiv 0 \mod 10$.

Exemplo 28. *Vamos determinar o dígito verificador do ISBN-13 abaixo:*

ISBN 978-85-244-0124-?

Da figura acima, temos:

$S_{12} = 1.9 + 3.7 + 1.8 + 3.8 + 1.5 + 3.2 + 1.4 + 3.4 + 1.0 + 3.1 + 1.2 + 3.4$

$S_{12} = 9 + 21 + 8 + 24 + 5 + 6 + 4 + 12 + 0 + 3 + 2 + 12$

$S_{12} = 106$

Logo, $S_{12} + a_{13} \equiv 0$ *mod* 10*, ou seja,* $106 + a_{13} \equiv 0$ *mod* 10*.*

Como $0 \leq a_{13} \leq 9$*, com* $a_{13} \in Z$*, temos que* $a_{13} = 4$*.*

Obtendo

Exemplo de Atividade: Podemos pedir que os alunos identifiquem o ISBN-13 no livro didático de matemática ou até de outras disciplinas ministradas no mesmo dia. Cada aluno deverá realizar os cálculos detalhados acima, registrando em uma folha de papel que deverá ser entregue ao professor. Em seguida, para um momento de mais descontração, podemos formar dois grupos em sala de aula, onde cada um desses grupos fornecerá ao outro os 12 primeiros números de 5 ISBNs-13. Ganhará o grupo que devolver primeiramente os ISBNs-13 completos e corretos. Isso fará com que todos do grupo trabalhem em conjunto, afim de agilizar o trabalho.

4.2 CPF

O Cadastro de Pessoa Física (CPF) é um sistema de identificação utilizado no Brasil para identificar pessoas. Esse sistema é constituído por uma sequência de 11 dígitos, sendo o primeiro bloco composto por 9 dígitos e o segundo bloco por 2 dígitos, sendo esses últimos os dígitos verificadores.

Calcular os dígitos verificadores do CPF é uma excelente atividade que pode ser utilizada em sala de aula com o intuito de estudar uma aplicação da congruência modular.

Vejamos então como obter os dígitos verificadores do CPF.

1º) Multiplicamos os 9 primeiros dígitos do CPF, da esquerda para a direita pela sequência de números 1, 2, 3, 4, 5, 6, 7, 8 e 9.

2º) Em seguida somamos os produtos obtidos, determinando S_9.

3º) O primeiro dígito verificador é o número que deve ser retirado dessa soma para obter um múltiplo de 11.

4º) Para obter o segundo dígito verificador, procedemos da mesma forma, multiplicando os 10 primeiros dígitos pela sequência 0, 1, 2, 3, 4, 5, 6, 7, 8 e 9 e em seguida somamos esses produtos obtendo S_{10}.

5º) O segundo dígito verificador é o número que deve ser retirado dessa soma para obter um múltiplo de 11.

Vejamos isso matematicamente:

Sejam $a_1a_2a_3a_4a_5a_6a_7a_8a_9$ a sequência dos 9 primeiros dígitos do CPF.

De acordo com o 1º e 2º passos, devemos obter a seguinte soma de produtos:

$S_9 = 1.a_1 + 2.a_2 + 3.a_3 + 4.a_4 + 5.a_5 + 6.a_6 + 7.a_7 + 8.a_8 + 9.a_9$

De acordo com o 3º passo, o primeiro dígito verificador a_{10} será obtido de acordo com a congruência $S_9 - a_{10} \equiv 0 \mod 11$, ou seja, $S_9 \equiv a_{10} \mod 11$

Após obter o primeiro dígito verificador, vamos de acordo com o 4º passo, obter S_{10}.

$S_{10} = 0.a_1 + 1.a_2 + 2.a_3 + 3.a_4 + 4.a_5 + 5.a_6 + 6.a_7 + 7.a_8 + 8.a_9 + 9.a_{10}$

Observando o 5º passo, o segundo dígito verificador a_{11} será obtido através da congruência $S_{10} - a_{11} \equiv 0 \mod 11$, ou seja, $S_{10} \equiv a_{11} \mod 11$.

Observação: Se em qualquer um dos casos o resto da divisão for 10, ou seja, se o número obtido for congruente a 10 módulo 11, usamos para o dígito verificador o algarismo 0.

Exemplo 29. *Vamos determinar os dígitos verificadores do CPF que possui a sequência 123456789 como os 9 primeiros dígitos. Multiplicando esses dígitos ordenadamente pelos números 1, 2, 3, 4, 5, 6, 7, 8 e 9, teremos:*

$S_9 = 1.1 + 2.2 + 3.3 + 4.4 + 5.5 + 6.6 + 7.7 + 8.8 + 9.9$

$S_9 = 1 + 4 + 9 + 16 + 25 + 36 + 49 + 64 + 81$

$S_9 = 285$

Assim, o primeiro dígito verificador a_{10} *será dado por:* $S_9 \equiv a_{10}$ *mod* 11 *então* $285 \equiv a_{10}$ *mod* 11. *Logo, deveríamos ter* $a_{10} = 10$, *mas de acordo com o definido na atividade, quando obtemos uma congruência a 10 módulo 11 usamos o dígito verificador igual a 0. Assim, temos que* $a_{10} = 0$.

Acrescentando $a_{10} = 0$ *na sequência e multiplicando ordenadamente pelos números 0, 1, 2, 3, 4, 5, 6, 7, 8, e 9, teremos:*

$S_{10} = 0.1 + 1.2 + 2.3 + 3.4 + 4.5 + 5.6 + 6.7 + 7.8 + 8.9 + 9.0$

$S_{10} = 0 + 2 + 6 + 12 + 20 + 30 + 42 + 56 + 72 + 0$

$S_{10} = 240$

Assim, o segundo dígito verificador a_{11} *será dado por:* $S_{10} \equiv a_{11}\ mod\ 11$ *então* $240 \equiv a_{11}\ mod\ 11$. *Logo, temos* $a_{11} = 9$.

Obtendo

Logo, o CPF completo será 123.456.789-09.

Exemplo de atividade: Como o número do CPF não é algo que deve ser fornecido a qualquer pessoa, iremos propor uma atividade para casa, onde cada aluno deverá fazer os cálculos conferindo o dígito verificador de 3 CPFs de pessoas conhecidas. Esses cálculos deverão ser entregues em uma folha ao professor, e poderá ser entregue como avaliação. E ao final devolvido ao aluno, uma vez que através do CPF pode-se identificar o nome da pessoa.

4.3 CALENDÁRIOS: EM QUE DIA DA SEMANA VOCÊ NASCEU?

Vamos apresentar uma atividade que tem por finalidade determinar o dia da semana que uma pessoa nasceu, ou uma outra data qualquer. Esse procedimento funcionará para datas entre 1900 e 2099, pois anos bissextos são múltiplos de 4, não múltiplos de 100(1900 não é bissexto) e múltiplos de 400 (2000 é bissexto). Porém, essa atividade pode ser adaptada para qualquer data. Um dado importante para nossa atividade é sabermos que o dia 01/01/1900 caiu em uma segunda-feira.

Descreveremos os passos para se obter o dia da semana procurado, dando uma breve explicação em cada um deles.

1º) Calcule quantos anos se passaram desde 1900 até o ano que você nasceu. Chame essa quantidade de **A**.

Explicação: O valor **A** é o número de avanços ocorridos nos dias da semana para os anos não bissextos. Por exemplo, se o primeiro de janeiro de um ano cai na segunda-feira, no ano seguinte cairá numa terça-feira, pois $365 \equiv 1$ mod 7.

2º) Calcule quantos anos bissextos, ou seja, quantos 29 de fevereiro ocorreram desde 1900 até a data de seu nascimento. Como os anos bissextos nesse caso serão apenas os múltiplos de 4, basta dividir o valor **A** por 4, sem considerar o resto da divisão. Chamaremos o quociente encontrado de **B**.

Explicação: O valor **B** encontrado é exatamente o número de anos bissextos. Como os anos bissextos possuem 366 dias e $366 \equiv 2 \bmod 7$, temos que o avanço em anos bissextos serão de dois dias da semana. Como um dia do avanço já foi contado em **A**, ao somarmos **A+B**, obtemos o número total de avanços em dias da semana.

3º) Considerando o mês de nascimento, vamos relacioná-lo com o número da tabela que aparece ao lado dele. Chamaremos 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

Explicação: Esses números da tabela que aparecem na frente de cada mês são exatamente a congruência da soma dos dias dos meses anteriores módulo 7. Por exemplo, se o dia primeiro de janeiro de um certo ano caiu num domingo, o dia primeiro de abril cairá num sábado, pois janeiro tem 31 dias, fevereiro tem 28 dias e março tem 31 dias. Logo, seus respectivos restos na divisão por 7 são 3, 0 e 3, o que nos faz avançar 6 dias a partir de domingo, chegando ao sábado.

4º) Vamos diminuir um dia da data de nascimento. Chamaremos esse número de **D**.

Explicação: Isso deve ser feito para atingirmos o exato dia procurado. Por exemplo, se a data procurada fosse o dia 4 de um 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 num sexta feira, que está a três dias adiante.

5º) Some agora os quatro números que você obteve nas etapas anteriores. Chamando esse número de **N**, temos que **N=A+B+C+D**.

6º) Vamos verificar a congruência N módulo 7 e compararmos com a tabela abaixo.

Segunda-Feira	$N \equiv 0 \bmod 7$
Terça-Feira	$N \equiv 1 \bmod 7$
Quarta-Feira	$N \equiv 2 \bmod 7$
Quinta-Feira	$N \equiv 3 \bmod 7$
Sexta-Feira	$N \equiv 4 \bmod 7$
Sábado	$N \equiv 5 \bmod 7$
Domingo	$N \equiv 6 \bmod 7$

Vejamos alguns exemplos:

Exemplo 30. *Uma pessoa nasceu no dia 21 de março de 1991. Qual o dia da semana que essa pessoa nasceu?*

Solução: *Vamos aplicar cada um dos passos descritos acima:*

1º) Temos que $1991 - 1900 = 91$. *Logo,* ***A=91****.*

2º) Dividindo 91 por 4 e desconsiderando o resto, teremos 22. Logo, ***B=22****.*

3º) O mês de março na primeira tabela corresponde ao número 3. Logo, ***C=3****.*

4º) Subtraindo um do dia de nascimento da pessoa, temos $21 - 1 = 20$. *Logo,* ***D=20****.*

5º) Somando os ***A****,* ***B****,* ***C*** *e* ***D*** *obtemos* ***N****. Logo,* ***N=91+22+3+20=136****.*

6º) Como $136 \equiv 3 \ mod\ 7$*, podemos afirmar de acordo com a segunda tabela apresentada na atividade que essa pessoa nasceu numa Quinta-Feira.*

Vamos verificar o calendário do mês de março de 1991:

Março de 1991						
Se	***Te***	***Qu***	***Qu***	***Se***	***Sá***	***Do***
				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*

Exemplo 31. *A final da Copa do Mundo FIFA de 1994 foi disputada em 17 de julho no Rose Bowl, na cidade de Pasadena nos Estados Unidos. O Brasil venceu a Itália por 3X2 nos pênaltis e se tornou tetracampeão. Em que dia da semana isso ocorreu?*

Solução: *Vamos aplicar cada um dos passos descritos acima:*

1º) Temos que $1994 - 1900 = 94$. *Logo,* ***A=94****.*

2º) Dividindo 94 por 4 e desconsiderando o resto, teremos 23. Logo, ***B=23****.*

3º) O mês de julho na primeira tabela corresponde ao número 6. Logo, ***C=6****.*

4º) Subtraindo um do dia do dia em que ocorreu a final da copa, temos $17 - 1 = 16$. *Logo,* ***D=16****.*

5º) Somando os ***A****,* ***B****,* ***C*** *e* ***D*** *obtemos* ***N****. Logo,* ***N=94+23+6+16=139****.*

6º) Como $139 \equiv 6 \ mod\ 7$*, podemos afirmar de acordo com a segunda tabela apresentada na atividade que a final ocorreu num Domingo.*

Vamos verificar o calendário do mês de Julho de 1994:

Julho de 1994						
Se	***Te***	***Qu***	***Qu***	***Se***	***Sá***	***Do***
				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*

Exemplo de Atividade: *O professor poderá solicitar aos seus alunos que façam uma pesquisa, determinando o dia da semana de nascimento de seus responsáveis, por exemplo, ou ainda alguns acontecimentos históricos dentro do período proposto na atividade.*

4.4 CRIPTOGRAFIA

A criptografia é utilizada quando queremos transmitir uma mensagem, mas não queremos que pessoas não autorizadas tenham acesso ao conteúdo. Como exemplo, podemos citar transações online, como compras via internet, para impedir que pessoas maliciosas tenham acesso a informações importantes, como senhas ou número de cartões e as usem de forma indevida.

A criptografia teve sua primeira aplicação em fins militares através do Imperador Romano Júlio César, que enviava mensagens a seus generais apenas trocando letras do alfabeto, como por exemplo avançando três letras no alfabeto. Vejamos um exemplo de como ficaria uma ordem dada por Júlio César:

XQXZXO XL XKLFQBZBO

Se α for o número correspondente a letra original no código e β o número correspondente a letra que a substituirá no código, teremos a função $\beta = \alpha + 3$.

Para determinarmos a mensagem original, basta determinar $\alpha = \beta - 3$, ou seja, recuar três letras no alfabeto. Logo, a mensagem original será:

ATACAR AO ANOITECER

Vejamos como podemos relacionar esse assunto a aritmética modular:

Primeiramente, vamos relacionar as letras do alfabeto com números de 1 a 26, de acordo com a tabela abaixo:

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

Se quisermos criptografar uma mensagem, podemos por exemplo, utilizar a chave 5 (poderia ser outra chave qualquer). Com essa chave, a letra original da mensagem, fica substituída pela letra que corresponde ao número da letra original, aumentado de 5. Por exemplo, a letra R ficará substituída pela letra W.

Numa mensagem então, onde aparece a letra W, vamos relacioná-la ao número 23 e como $23 - 5 = 18$, temos que $23 - 5 \equiv 18 \bmod 26$. Desta forma, podemos definir que sendo β o número correspondente a letra na mensagem criptografada e α o número da letra na mensagem original, temos que $\beta - 5 \equiv \alpha \bmod 26$.

De modo geral, se utilizarmos uma chave K qualquer, temos que $\beta - K \equiv \alpha \bmod 26$.

Por exemplo, vamos decodificar a mensagem abaixo, sabendo que a chave utilizada foi 3.

SURWHMD D QDWXUHCD

Vamos aplicar a congruência $\beta - 3 \equiv \alpha \bmod 26$ em cada uma das letras que aparecem na mensagem criptografada. Lembrando que β é o número correspondente a letra na mensagem criptografada e α o número correspondente a letra na mensagem original:

- S$\longrightarrow$P, pois $19 - 3 \equiv 16 \bmod 26$
- U$\longrightarrow$R, pois $21 - 3 \equiv 18 \bmod 26$
- R$\longrightarrow$O, pois $18 - 3 \equiv 15 \bmod 26$
- W$\longrightarrow$T, pois $23 - 3 \equiv 20 \bmod 26$
- H$\longrightarrow$E, pois $8 - 3 \equiv 5 \bmod 26$
- M$\longrightarrow$J, pois $13 - 3 \equiv 10 \bmod 26$
- D$\longrightarrow$A, pois $4 - 3 \equiv 1 \bmod 26$
- Q$\longrightarrow$N, pois $17 - 3 \equiv 14 \bmod 26$
- X$\longrightarrow$U, pois $24 - 3 \equiv 21 \bmod 26$
- U$\longrightarrow$R, pois $21 - 3 \equiv 18 \bmod 26$
- C$\longrightarrow$Z, pois $3 - 3 \equiv 0 \equiv 16 \bmod 26$

Assim, a mensagem original é:

PROTEJA A NATUREZA

Exemplo de Atividade: Uma atividade bastante motivadora que pode ser realizada em sala de aula é a troca de pequenas mensagens criptografadas entre grupos pré definidos. Por exemplo, podem se formar três grupos, onde dois deles transferem informações e um deles tentará descobrir qual a congruência foi utilizada para criptografar a mensagem. Podemos restringir esse número de forma que não se torne um trabalho tão difícil. Esses grupos podem se revezar e ganha o que decifrar as mensagens em menos tempo.

5 CONCLUSÃO

Concluímos que a utilização da aritmética modular é de grande relevância para o ensino da matemática frente a situações enfrentadas pelos alunos durante a vida escolar, por ser um assunto de fácil assimilação e possuir aplicações presentes no cotidiano.

Para mostrar que a aritmética modular é um tema bastante atual, procuramos explorar questões de provas como o ENEM e a OBMEP, além de utilizar materiais como as apostilas do PIC-Jr.

Nosso objetivo foi introduzir o conteúdo para alunos que nunca tiveram contato com o mesmo, mas poderíamos incluir ainda nesse trabalho alguns outros assuntos como o teorema chinês dos restos, além de fazer relação com conteúdos já estudados no ensino médio, como por exemplo trigonometria na circunferência(congruência módulo 360), sequências numéricas, potências do número complexo (congruência módulo 4), além de vários outros fenômenos cíclicos que podem ser observados sob nova perspectiva.

Finalmente, gostaríamos de observar que frente às mudanças que tem ocorrido no ensino de matemática, a aritmética modular, através de situações contextualizadas, é uma excelente ferramenta que desperta o interesse e ao mesmo tempo fortalece o pensamento aritmético dos alunos.

REFERÊNCIAS

[1] BRASIL. SEF. Parâmetros Curriculares Nacionais: **Introdução aos Parâmetros Curriculares Nacionais**. Brasília: MEC/SEF, 1998.

[2] COUTINHO, Severino Collier. **Números Inteiros e Criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2009. (Coleção Matemática e Aplicações)

[3] GONÇALVES, Adilson. **Introdução à Álgebra**. 1 ed. Rio de Janeiro: Projeto Euclides, 1979.

[4] HEFEZ, Abramo. **Elementos da Aritmética**. 2 ed. Rio de Janeiro: SBM, 2013.

[5] HEFEZ, Abramo. **Iniciação à Aritmética**. Rio de Janeiro: IMPA, 2015. Disponível em http://www.obmep.org.br/docs/apostila1.pdf. Acesso em: 20 mar. 2015.

[6] MILIES, César Polcino; COELHO, Sônia Pitta. **Números**: Uma Introdução à Matemática. 3 ed. São Paulo: edusp, 2006.

[7] PARÂMETROS CURRICULARES NACIONAIS, **ENSINO MÉDIO**. Disponível em: <http://portal.mec.gov.br/index.php?Itemid=859&id=12598%3Apublicacoes&option=com_content&view=article>, Acesso em: 12 jan. 2015

[8] SÁ, Ilydio Pereira. **Aritmética Modular e algumas de suas aplicações**. Disponível em http://www.magiadamatematica.com/diversos/eventos/20-congruencia.pdf. Acesso em: 20 março de 2015.

[9] TERADA, Routo. Criptografia e a importância das suas aplicações. **Revista do Professor de Matemática**, São Paulo, n. 12, p. 1-6, 1998.