ISSN: 2358-8829

CONGRUÊNCIAS E CRIPTOGRAFIA: UMA VISITA DA TEORIA DOS NÚMEROS À ESCOLA BÁSICA

Dorival Lobato Junior [1]

RESUMO

A presente comunicação científica se refere à uma apresentação que se enquadra na área da Matemática Pura e tem o objetivo de apresentar em nível elementar noções de congruência. um tópico da teoria dos números, citada em algumas publicações como a rainha da matemática, para os que atuam na escola básica. Mostramos que mesmo a nível elementar é possível fazer uma conexão entre os assuntos de congruência e criptografia. Através desses tópicos procuramos destacar o poder e a elegância dos argumentos baseados na teoria dos números. Além disso, com a criptografia é possível descrever a utilidade da teoria elementar dos números em fornecer exposição a ideias matemáticas e apresentar aos que atuam na escola básica a essência da atividade matemática. Assuntos como Congruências e criptografia são como uma janela para as questões abertas e a natureza evolutiva da matemática e, em particular, a teoria dos números, muitas vezes considerada um *playground* divertido para matemáticos com pouca relevância para o mundo real.

Palavras-chave: Teoria dos números; congruências; criptografia; escola básica.

INTRODUÇÃO

É final de mais um dia de trabalho e você dirige para sua casa. Você pressiona um controle remoto em seu carro que abre o portão da garagem e você entra. Você pressiona o controle remoto novamente e o portão da garagem se fecha.

Sem que você saiba, alguém mal-intencionado está à espreita na sua rua com um *scanner* de rádio que capta o sinal do seu controle remoto. Da próxima vez que você não estiver em casa, esse mal-intencionado planeja usar o sinal salvo para abrir o portão da garagem para praticar furtos. No entanto, no dia em que faz isso e envia o sinal, o portão não abre. Agora suponha que você quer fazer uma compra na internet usando um cartão de crédito.

Você deve ter notado que o http:// típico que precede um endereço da web é substituído por https://. O “s” no final indica um site seguro. Isto significa que alguém, que pode estar tentando roubar informações de cartão de crédito, não pode interceptar as informações que você envia. Embora um controle remoto para abrir portão de garagem e um site seguro podem parecer bastantes diferentes, a matemática por trás de cada um deles é semelhante. Ambos são baseados em aritmética modular ou congruências, um importante assunto em Teoria dos Números.

[1] Professor da Escola Técnica Magalhães Barata- BELÉM/PA, dorival.junior@escola.seduc.pa.gov.br;

ISSN: 2358-8829

Está comunicação tem por objetivo geral favorecer a precisão, clareza e relevância da proposta apresentada, oportunizando mostrar tópicos da teoria dos números na Escola Básica. Acreditamos que sob esta perspectiva podemos oferecer uma grande oportunidade para apresentar aos professores da Educação Básica aplicações da matemática que são empolgantes e desempenham um papel importante, embora às vezes oculto, em nossas atividades diárias, servindo dessa maneira como uma forma de criar interesse pela participação na disciplina nessas novas formas metodológicas que o momento atual nos exige.

A teoria das congruências e sua aplicação na criptografia das informações são usadas não apenas pelas pessoas no seu dia a dia e governos para manter as comunicações em segredo, mas também por bancos e outras empresas para proteger informações confidenciais. Com o número crescente de transações que ocorrem na Internet, a criptografia é de importância cada vez maior.

Muitas pessoas têm a impressão equivocada de que a Aritmética (e a Matemática de forma geral) é um assunto estático, no qual tudo já se sabe há centenas de anos. Nossa intenção é com nossos futuros professores cooperar para que essa visão seja revertida.

METODOLOGIA

A metodologia de pesquisa adotada neste artigo foi do tipo exploratória, com enfoque bibliográfico, pois será necessária uma revisão de estudos em relação ao contexto do conteúdo e aplicações de congruências na criptografia. Com isso serão utilizadas pesquisas exploratórias sobre o tema com de forma que possa dialogar com conteúdo da escola básica.

Segundo Gil (2008) a pesquisa bibliográfica é desenvolvida a partir de material já elaborado, constituído principalmente de livros e artigos científicos. Embora em quase todos os estudos seja exigido algum tipo de trabalho desta natureza, há pesquisas desenvolvidas exclusivamente a partir de fontes bibliográficas. Parte dos estudos exploratórios podem ser definidos como pesquisas bibliográficas, assim como certo número de pesquisas desenvolvidas a partir da técnica de análise de conteúdo, nesse caso, a congruência e criptografia.

REFERENCIAL TEÓRICO

Noções de Aritmética Modular

Uma vez que o tema da divisibilidade e restos (resíduos) é relativamente pesado com provas algébricas, estaremos aqui nos aproximando desse assunto de forma gradual

ISSN: 2358-8829

tendo em vista uma aproximação do assunto na educação básica. Começaremos com um caso em particular: vamos explorar a divisibilidade por 3.

Resíduos quando dividimos por 3

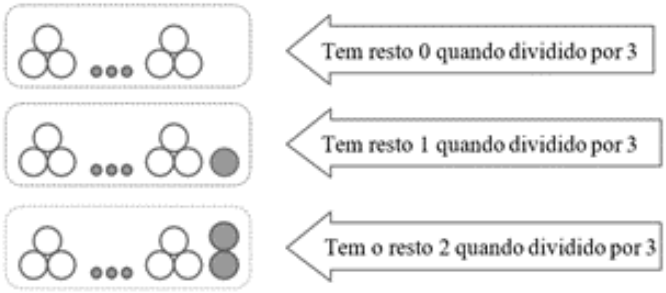
Vamos começar a discussão principal com um lembrete sobre *paritismo ou paridade* nos inteiros: uma técnica simples, mas poderosa na resolução de questões aritméticas, que é muito útil para uma variedade muito grande de questões. (O paritismo é definido por um resíduo: um número é *par* quando, ao ser dividido por 2, deixa resíduo 0; é *ímpar* quando o resíduo é 1.).

Se os resíduos após uma divisão por 2 podem ser tão úteis na resolução de desafios aritméticos, os resíduos de divisões por outros números poderiam também ser tão úteis? A resposta é com toda certeza afirmativa. E foi uma resposta definitiva, dada a esta pergunta pelo matemático alemão Johann Carl Friedrich Gauss (1777-1855) que deu origem ao nascimento da Teoria das Congruências, e colocou a Aritmética na posição de destaque que hoje ela desfruta na Matemática.

Vamos começar explorando a divisibilidade por 3 e aprenderemos a usá-la na resolução de alguns desafios aritméticos. Começamos definindo todos os termos relacionados com a divisão de números inteiros não negativos {0, 1, 2, 3,...}, por 3. Assim: O número X tem resíduo 0 quando dividido por 3, se $X = 3K$. O número X tem o resíduo 1 quando dividido por 3, se $X = 3K + 1$. O número X tem o resíduo 2 quando dividido por 3, se $X = 3K + 2$.

Essa definição formal torna muito mais fácil provar questões sobre divisibilidade e restos. Para quem está iniciando, também é útil ter em mente um modelo visual da divisibilidade por 3 (Figura 1).

Figura 1 – Modelo visual da divisibilidade por 3



Fonte: Elaborado pelo autor (2022)

Também podemos considerar uma definição “informal” de um resíduo: “o menor

ISSN: 2358-8829

número inteiro não negativo que, se subtraído, nos leva a um múltiplo de 3". Vamos ilustrar essas definições:

1. O número 36 tem resíduo 0 quando dividido por 3. De fato, 36 pode ser dividido em 12 grupos de 3 e pode ser escrito como $36 = 3 \times 12$.
2. O número 19 tem resíduo 1 quando dividido por 3. De fato, 19 pode ser dividido em 6 grupos de 3 e deixar um resíduo igual 1 e pode ser escrito como $19 = 3 \times 6 + 1$. Assim, o menor número inteiro não negativo subtraído de 19 de modo a termos um múltiplo de 3 seria o 1.
3. O número 26 tem resíduo 2 quando dividido por 3. De fato, 26 pode ser dividido em 8 grupos de 3 e deixar um resíduo igual 2 e pode ser escrito como $26 = 3 \times 8 + 2$. Assim, o menor número inteiro não negativo subtraído de 26 de modo a termos um múltiplo de 3 seria o 2.

Aritmética dos resíduos: Adição e resíduos após a divisão por 3

É muito importante entender como as operações aritméticas nos números inteiros afetam os restos.

Podemos verificar que se dois números são divisíveis por 3, então sua soma é divisível por 3 também.

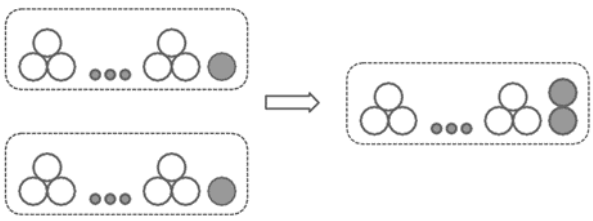
De fato, se $X = 3K$ e $Y = 3M$, então $X + Y = 3K + 3M = 3(K + M)$.

Agora, suponha que tanto X quanto Y tenham restos 1 quando divididos por 3. O que acontece com a soma $X + Y$?

Antes de passar para a prova algébrica, vamos explicar a resposta usando um modelo visual.

Se um número inteiro não negativo tem resíduo 1, então é composto por vários grupos de 3 e um acréscimo de 1. Assim, quando dois desses números forem adicionados, a soma será composta por vários grupos de 3 e dos acréscimos, ou seja, 2. Então, a soma tem resto 2 (Figura 2).

Figura 2 – Soma composta por grupos de 3 e resto 2



Fonte: Elaborado pelo autor (2022)

Agora, é hora de uma prova algébrica.

ISSN: 2358-8829

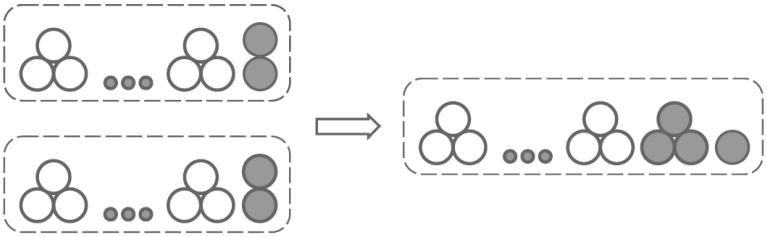
$$X = KG + 1 \text{ e } Y = 3M + 1.$$

Portanto, $X + Y = 3K + 3M + 1 = 3(K + M) + 1 + 1 = 3(K + M) + 2$. Assim, $X + Y$ tem resto 2. Em seguida, suponha que tanto X quanto Y tenham restos 2. Qual seria o resto de $X + Y$? Vai ser 4 ou 1? Vamos provar:

$$\begin{aligned} X + Y &= 3K + 2 + 3M + 2 \\ &= 3K + 3M + 2 + 2 \\ &= 3K + 3M + 3 + 1 \\ &= 3(K + M + 1) + 1. \end{aligned}$$

Então, o resto é 1. Podemos ilustrar isso visualmente também (Figura 3):

Figura 3 – Somas com resto 1



Fonte: Elaborado pelo autor (2022)

Vamos continuar analisando: temos várias outras combinações de restos para explorar. Para manter nossos resultados organizados, vamos criar uma tabela para esses resíduos. Com o que já foi visto acima, temos condições de preencher uma tabela para a adição de resíduos. A tabela 1 completa está abaixo:

Tabela 1 – Tabela completa de resíduos

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Fonte: Elaborado pelo autor (2022)

Agora, é hora de formular a regra geral de como os resíduos na divisão por 3 se comportam sob a adição.

Seria tentador dizer que os restos da soma de dois números é ***igual*** à soma de seus restos. Infelizmente, esta afirmação não é bem assim: dê uma olhada na tabela no par de restos (2, 2). Enquanto sua soma é 4, o resto de sua soma é 1.

Assim, a regra correta é: *a soma de dois números tem o mesmo resto que a soma de seus restos.*

Aplicando o mesmo raciocínio, podemos chegar a uma regra semelhante para vários números: *a soma de vários números* tem *o mesmo restante* que a soma *de seus restos.*

ISSN: 2358-8829

Exemplificando: Suponha que gostaríamos de encontrar o resto da soma 1+2 + + 99 + 100 quando dividida por 3.

Para uma questão como essa não há necessidade de se obter primeiro o resultado dessa adição. Tudo o que temos que fazer é adicionar os restos dos números 1, 2,..., 100. Para enfatizar o padrão dos restos, vamos agrupar os números por 3:

(1 + 2 + 3) + (4 + 5 + 6) + ... + (97 + 98 + 99) + 100.

Em seguida, vamos substituir estas adições pelas adições de seus restos:

(1 + 2 + 0) + (1+2+ 0) + + (1+2+ 0) + 1.

Não há necessidade de obter essa nova soma também, porque nosso objetivo é encontrar o *resto* desta soma quando dividido por 3. Não é difícil notar que cada soma entre parênteses tem resto 0. Portanto, o resultado tem resto 1. Assim 1 + 2 + ..+ 99 + 100 quando dividido por 3 deixa resto 1.

Subtração e resíduos após a divisão por 3

Quando subtraímos, os restos se comportam da mesma forma. Podemos ilustrar a ideia geral usando dois exemplos.

1. *Suponha que X tem resto 2 e Y tem o resto 1 quando dividido por 3.* Qual é o resto de *X - Y* ?

Pode-se provar que o resto é 2 – 1 = 1.

2. *Suponha que X tenha resto 1 e Y tenha o resto 2 quando divididos por 3.* Qual é o resto de $X - Y$?

Seria tentador dizer que o resto é $1 - 2 = -1$. No entanto, na divisão euclidiana por 3, um resto não pode ser negativo: ele tem que ser 0 ou 1 ou 2. Então, o que devemos fazer?

Façamos uma prova mais formal. Se subtrairmos um número com resto 2 de um número com resto 1, então obtemos um resultado que é expresso como 3*K* - 1. Esta expressão pode ser reescrita como 3(*K* -1) + 2. Logo, o resto é 2.

Segue-se, a partir dessa discussão, que, por exemplo, o resto -1 numa divisão por 3 corresponde a 2, e o resto -4 também corresponde a 2. O que se pode dizer do resto -2 ? E do resto -3?

Multiplicação e restos após a divisão por 3

Vamos agora investigar o que acontece com os restos quando os números são multiplicados.

ISSN: 2358-8829

O objetivo é provar que o resto de um produto é definido pelos restos dos fatores. Vamos provar caso a caso.

Podemos observar que quando pelo menos **um dos dois termos é divisível por 3**, todo o produto é divisível por 3 também. De fato, suponha que $X = 3M$. Neste caso, $XY = (3M)\ Y = 3\ (MY)$. Esse número é claramente divisível por 3. Assim, essa observação nos permite preencher algumas entradas na tabela de multiplicação de restos (veja a tabela 2 abaixo):

Tabela 2 – Tabela de multiplicação de restos

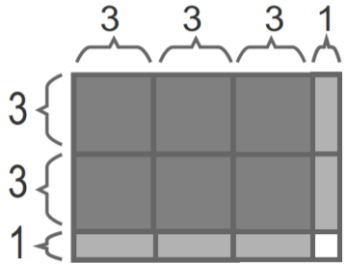
x	0	1	2
0	0	0	0
1	0		
2	0		

Fonte: Elaborado pelo autor (2022)

Em seguida, vamos *multiplicar dois números, cada um* tendo o resto 1. O resto do produto será 1, e vamos provar esse fato de 2 maneiras: visualmente e algebricamente.

Prova Visual: Vamos utilizar o fato de que o produto de dois números pode ser visualizado como uma área de um retângulo com lados iguais a estes números. A figura abaixo ilustra a multiplicação de dois números que tem resto 1. Cada desses números contém vários grupos de 3 e um acréscimo de 1. Assim, o produto dos números é composto por vários quadrados 3×3 (cinza escuro), vários retângulos 1×3 (cinza claro), e um único quadrado 1×1 (branco). Todos quadrados 3×3 e todos os retângulos 1×3 são múltiplos de 3. Portanto, o resto do produto é o quadrado branco 1×1, que tem uma área 1.

Figura 8 – Multiplicação de dois números com resto 1



Fonte: Elaborado pelo autor (2022)

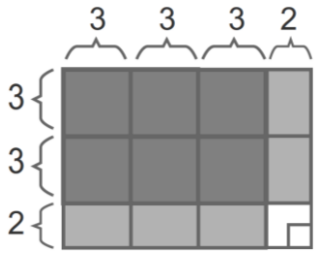
A prova algébrica demonstra a mesma ideia, expressa de forma mais compacta e formal:

$$(3M + 1)\ .\ (3N + 1) = 3M\ .\ 3N + 3M + 3N + 1$$
$$= 3\ (3M\ .\ N + M + N)\ +\ 1.$$

ISSN: 2358-8829

Agora suponha que *cada um dos dois números tenha resto 2*. Qual seria o resto do produto? Mais uma vez, vamos começar com uma prova visual. A figura abaixo ilustra a multiplicação de dois números que tem restos 2. Da mesma forma que a prova anterior, cada quadrado cinza 3×3 é um múltiplo de 3, e cada retângulo cinza claro 2×3 é um múltiplo de 3 também. Portanto, o resto é definido pelo quadrado branco 2×2. Três quadrados brancos 1×1 formam um múltiplo de 3 (em forma de L na figura 4). Assim, o resto é o quadrado branco 1×1, que tem uma área 1.

Figura 4 – Multiplicação de dois números que tem resto 2



Fonte: Elaborado pelo autor (2022)

Podemos seguir com uma prova algébrica:

$$(3M + 2) \,.\, (3N + 2) = 3M \,.\, 3N + 6M + 6N + 4$$

$$= 3(3M \,.\, N + M + N + 1) + 1.$$

Da mesma forma, o produto dos dois números com os restos 1 e 2 terá resto 2. Finalmente, podemos preencher toda a tabela 3 de multiplicação.

Tabela 3 – Tabela completa da multiplicação

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Fonte: Elaborado pelo autor (2022)

Olhando para esta tabela, estamos prontos para formular a regra da multiplicação. Tal como no caso da adição, a alegação de que "o resto de um produto é igual ao produto dos restos" não é inteiramente verdadeira.

> A regra correta é: *o produto de dois números tem o mesmo restante que o produto de seus restos.* O mesmo vale para o produto de vários números.

Exemplificando. Calcule o resíduo de 8^{200} quando dividido por 3.

Discussão. Podemos simplificar o problema substituindo todos os 200 fatores "8" pelos seus resíduos. O novo problema simplificado seria calcular o resíduo de $8^{200} = (2^3)^{200} =$

ISSN: 2358-8829

2^{600}. Vamos abordar este novo problema gradualmente, a partir das menores potências de 2.

$2^1 = 2$. Tem resíduo 2.

$2^2 = 4$. Tem o resíduo 1.8

$2^3 = 2^2.2$. Assim, o resíduo de 2^3 é determinado pelo produto dos resíduos de 2^2 e 2. É igual a 1.2 = 2.

$2^4 = 2^3.2$. Assim, o resíduo de 2^4 é determinado pelo produto dos resíduos de 2^3 e 2. É igual ao resíduo de 2.2, que é 1.

Assim, vemos um padrão – os resíduos das potências de 2 vão se alternando, com todos os expoentes pares tendo resíduos 1, e todos os expoentes ímpares tendo resíduos 2. Portanto, 8^{200} tem resíduo 1 quando dividido por 3.

Linguagem e notação em módulo

A frase *"resíduo (resto) quando dividido por..."* é um pouco longa. Matemáticos são um grupo que odeiam a fadiga, por isso eles sempre criam maneiras de encurtar as coisas - a notação "***modulo***", significa "o resto quando dividido". Por exemplo, a frase "o resto de 10, quando dividido por 3" pode ser substituída por "10 módulo 3", e a frase "5 tem resto 2 quando dividido por 3" pode ser substituída por "5 é igual a 2 modulo 3". Vamos praticar:

1. "19 modulo 3" significa "resto 19 quando dividido por 3".
2. "19 é igual a 1 modulo 3" significa "19 dividido por 3 tem o resto 1".
3. "20 é igual a 0 modulo 2" significa "20 dividido por 2 tem resto 0".
4. "17 é igual a 2 modulo 5" significa "17 dividido por 5 tem o resto 2".

O símbolo especial de congruência "≡ " pode ser usado para encurtar ainda mais as coisas e nos ajudar a não fazer mais uso da palavra "igual" que já está bem enraizada na teoria das equações. Por exemplo: "5 é igual a 2 modulo 3" pode ser reescrito como "5 é congruente a 2 módulo 3" e simbolizado por "$5 \equiv 2(mod3)$". Vamos praticar novamente:

1. "19 é igual a 1 modulo 3" ou "19 é congruente a 1 modulo 3" e "$19 \equiv 1(mod3)$".
2. "20 é igual a 0 modulo 2" ou "20 é congruente 0 módulo 2" e "$20 \equiv 0(mod2)$".
3. "17 é igual a 2 modulo 5" ou "17 é congruente a 2 módulo 5" e "$17 \equiv 2(mod3)$".

ISSN: 2358-8829

RESULTADOS E DISCUSSÃO

Atividades de aplicações na Criptografia

Na década de 1970, foi descoberto um novo tipo de código que mudou a maneira como as pessoas podiam enviar mensagens secretas. Isso significava que eles não precisavam concordar com antecedência sobre os detalhes do código que usariam. Isso veio em um bom momento porque um pouco mais de duas décadas depois, em 1994, as pessoas começaram a usar a Internet nos moldes atuais de navegador web e serviços, e aquele novo tipo de código, chamado de cifra de chave pública, tornou prático para empresas e para pessoas comuns se comunicarem com segurança.

Há um tipo muito utilizado mundialmente de cifra de chave pública usa números primos e a segurança da chave repousa sobre esses números. É muito empolgante pensar que pessoas muito jovens podem entender alguns dos tópicos envolvidos na criptografia de chave pública. Os alunos da escola básica aprendem sobre números primos e fatoração, então por que não apresentar em cursos como o de licenciatura em matemática, como esses tópicos são usados hoje?

Quanto mais pensamos sobre isso, mais percebemos que há muitas cifras interessantes que envolvem conteúdos de matemática da escola básica. Uma dessas cifras, que era usada em batalhas nos tempos do império Romano, envolve nada mais do que adição e subtração. Outra, a Cifra de Vigenère, que foi usada durante a Guerra Civil nos Estados Unidos e até mesmo no século XX e que já foi considerada inquebrável, pode na verdade ser quebrada por alunos do ensino médio de hoje (desde que a chave não seja muito longa) por encontrar fatores comuns de certos números.

A Criptografia apela à curiosidade natural que pessoas de todas as idades têm por mistérios e segredos, e pode ser contextualizada com relatos de como foi usado e mal utilizada ao longo da história. Assim, junto com o conteúdo matemático a ser ensinado ao fazermos essas conexões interdisciplinares procuramos de certa forma responder a questões como: que conhecimento matemático sobre aritmética modular e a criptografia deve ser ensinado? Por que isso é importante? Por que isso é útil? Questões muito importantes para refletir sobre nossa prática.

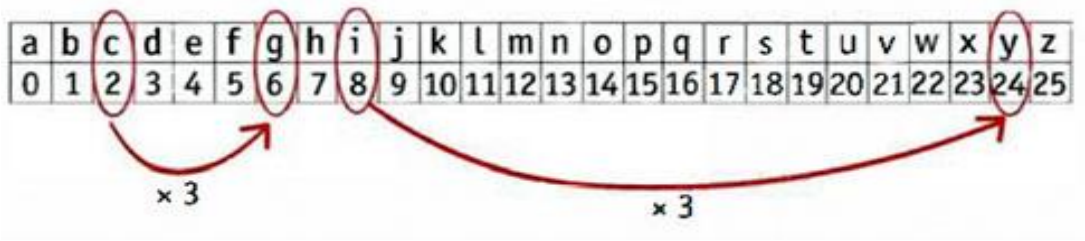
A seguir, apresentamos um resumo de algumas atividades que os professores da escola básica poderiam apresentar aos seus alunos.

Cifras multiplicativas

ISSN: 2358-8829

Vamos construir um método de criptografar chamado de *cifra 3-vezes* onde se multiplica os números correspondentes às letras por 3 (Tabela 4). Como exemplo, vamos encriptar a letra c. O número para c na tira é 2, multiplicando 2 por 3 e obtemos 6. Como 6 é o número para a letra g, encriptamos c como g. Encriptamos a letra i como y porque o número para i é 8 e 3 . 8 = 24, e 24 corresponde à letra y.

Tabela 4 – Ecriptação das letras c, g, i, y [1]



Fonte: Elaborado pelo autor (2022)

[1] Cifra 3-vezes

Chaves de codificação

Nas atividades que forem distribuídas, os participantes irão perceber que quando multiplicamos os números por 3, cada produto é diferente. Mas, quando multiplicarem por 2, algumas letras têm a mesma codificação. Portanto, multiplicar por 2 não é uma boa forma de cifragem.

Numa cifra multiplicativa, o número pelo qual se multiplica determina a cifra. Portanto, esta é a chave de codificação. Chamamos um número de uma boa chave se codifica cada letra de forma diferente. O número 3 é uma boa chave, mas o 2 não é. Uma questão a ser discutida é o que faz alguns números serem boas chaves e alguns números chaves ruins.

A regra geral é: Um número é uma boa chave para uma cifra multiplicativa se for relativamente primo com o tamanho do alfabeto.

Decodificação e Inversos

Na aritmética regular, a maneira de desfazer a multiplicação por 3 é dividir por 3. Podemos mostrar isso com setas, $5 \rightarrow \times 3 \rightarrow 15 \rightarrow \div 3 \rightarrow 5$. ou como uma equação.,$(5 \times 3) \div 3 = 5$.

CONSIDERAÇÕES FINAIS

As ideias aqui propostas, são uma oportunidade de aplicar conceitos matemáticos, que são geralmente encontrados durante a escolaridade formal. Contextualizando esses conceitos com a criptografia, espera-se que os professores e alunos aprofundem sua compreensão,

ISSN: 2358-8829

reforcem suas habilidades e aumentem sua apreciação da matemática. Explorar padrões matemáticos é uma experiência fundamental para quem estuda matemática. Apresentamos matemática básica para criptografar algumas das cifras clássicas.

A criptografia requer matemática como multiplicação, divisão com resto, fatores comuns e números primos. Também requer codificadores e decodificadores para criar e encontrar padrões, o que exige um nível mais profundo de pensamento.

Muitas pessoas têm a impressão errada de que a matemática é um assunto estático, um no qual tudo é conhecido há centenas de anos. Assuntos como Congruências e criptografia são como uma janela para as questões abertas e a natureza evolutiva da matemática e, em particular, a teoria dos números, muitas vezes considerada um *playground* divertido para matemáticos com pouca relevância para o mundo real. Neste artigo, quisemos mostrar que essas duas visões nunca foram um problema dentro da Matemática: diversão e aplicação.

REFERÊNCIAS

BRASIL. Secretaria de Educação Fundamental. **Parâmetros Curriculares Nacionais**: Matemática. Brasília: MEC, 1998.

BRASIL. Ministério da Educação. Secretária de Educação Básica. **Orientações Curriculares para o Ensino Médio**. Ciências da Natureza e suas Tecnologias, Brasília, 2006. 2. v.

BRASIL. Ministério da Educação. Secretaria de Educação Básica. **BNCC**. 2015. Disponível em: http://basenacionalcomum.mec.gov.br. Acesso em: 9 jul. 2015.

CADAR, Luciana; DUTENHEFNER, Francisco. Encontros de aritmética. Apostila do PICOBMEP, 2015.

DANTE, L. R. **Didática da resolução de problemas**. 12. ed. São Paulo: Ática, 2002.

GIL, Antônio Carlos**. Métodos e técnicas de pesquisa social.** 6.ed. – São Paulo: Atlas, 2008**.**

MENDONÇA, Maria do Carmo D. **Problematização**: um caminho a ser percorrido em educação matemática. 1993. 306 p. Tese (Doutorado em Educação) – Universidade Estadual de Campinas, Faculdade de Educação, Campinas, São Paulo, 1993.

POLYA, G. **How to Solve It**. New Jersey: Princeton University Press, 1985.

SCHROEDER, T. L.; LESTER JR, F. K. Developing understanding in mathematics via problem solving. *In*: TRAFTON, P. R. (ed.). **New directions for elementary school mathematics**. Reston, VA: NCTM, 1989. p. 31-42.

VAN DE WALLE, J. A. **Elementary and Middle School Mathematics**. New York: Longman, 2001.