

ARITMÉTICA MODULAR E ALGUMAS DE SUAS APLICAÇÕES

Ilydio Pereira de Sá¹

Introdução:

Uma das ferramentas mais importantes na teoria dos números é a aritmética modular, que envolve o conceito de congruência. Uma congruência é a relação entre dois números que, divididos por um terceiro - chamado módulo de congruência - deixam o mesmo resto. Por exemplo, o número 9 é congruente ao número 2, módulo 7, pois ambos deixam resto 2, ao serem divididos por 7. Representamos essa congruência do exemplo por $9 \equiv 2, \text{ mod. } 7$. Foi o brilhante Gauss que observou que usávamos com muita frequência frases do tipo “*a dá o mesmo resto que b quando divididos por m*” e que essa relação tinha um comportamento semelhante à igualdade. Foi Gauss então que introduziu uma notação específica para este fato e que denominou de “**congruência**”.

Muito se tem escrito sobre esse tema, principalmente nos livros sobre teoria dos números. É um conceito muito importante e que está relacionado com divisibilidade e os restos de uma divisão de números inteiros.

O que não é muito comum é o estudo das muitas aplicações que o tema possui no cotidiano de todas as pessoas. Diferentes códigos numéricos de identificação, como códigos de barras, números dos documentos de identidade, CPF, CNPJ, ISBN, ISSN, criptografia, calendários e diversos fenômenos periódicos estão diretamente ligados ao tema, conforme mostraremos em nosso estudo.

É um tema bastante atual e que pode ser trabalhado já nas classes do Ensino Fundamental e gerador de excelentes oportunidades de contextualização no processo de ensino / aprendizagem de matemática.

Inicialmente vamos mostrar alguns elementos teóricos sobre a aritmética modular e, na segunda parte do trabalho teremos a apresentação de alguns exemplos de aplicação desse importante e interessante tema da área de teoria dos números.

1) Noções básicas da aritmética modular

1.1) Exemplos iniciais:

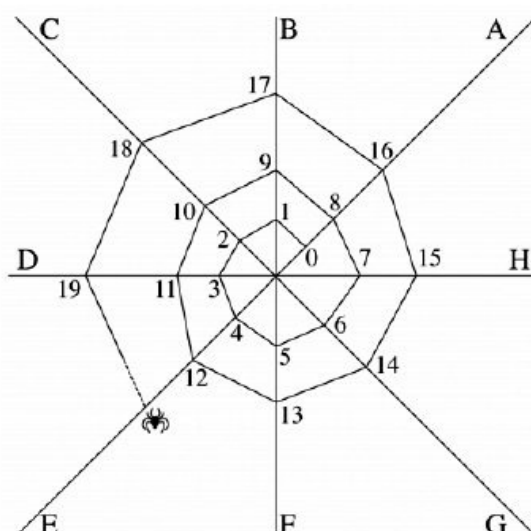
Antes de apresentarmos as definições e propriedades relacionadas à congruência, vamos desenvolver três exemplos que poderiam ser colocados a alunos da Educação Básica, ainda não familiarizados com o tema, como introdução ao assunto.

Exemplo 1:

Vamos apresentar uma questão retirada do banco de questões do site da OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas). Lá sempre temos encontrado questões interessantes e provocativas para o preparo de nossos alunos da Educação Básica.

A, B, C, D, E, F, G e H são 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?

¹ Ilydio Pereira de Sá – Mestre em Educação Matemática, professor da UERJ, da Universidade Severino Sombra e do Colégio Pedro I, Rio de Janeiro.



SOLUÇÃO:

Vejamos o que está acontecendo?

FIOS	A	B	C	D	E	F	G	H
	0	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

É claro que alguma pessoa bem paciente poderia continuar construindo a tabela até que aparecesse o número 118. Assim ela saberia em qual fio a aranha iria estar. Convenhamos que não seria uma solução muito prática e nem rápida. Imagine se a questão perguntasse o fio correspondente ao número 890?

Podemos observar que os fios se repetem a cada oito números e essa periodicidade faz com que os números de cada fio formem uma progressão aritmética de razão igual a 8, ou seja, aumentem de oito em oito. Observamos também que cada fio pode ser representado a partir dos múltiplos de 8. O fio A corresponde aos números que são múltiplos de 8, ou seja, números que divididos por 8 deixam resto zero ($8 \cdot n$, com $n \in \mathbb{N}$). O fio B corresponde aos números que são múltiplos de 8, mais 1, ou seja, números que divididos por 8 deixam resto 1 ($8 \cdot n + 1$, com $n \in \mathbb{N}$). O fio C corresponde aos números que são múltiplos de 8, mais 2, ou seja, números que divididos por 8 deixam resto 2 ($8 \cdot n + 2$, com $n \in \mathbb{N}$) e essa lógica se mantém até o fio H, definido pelos números que divididos por oito deixam resto 7. É claro que para saber sobre qual fio estará o número 118, basta verificarmos a qual dessas famílias tal número pertence e isso pode ser facilmente obtido ao dividirmos 118 por 8. Vejamos:

$$\begin{array}{r} 118 \\ 8 \overline{) 118} \\ \underline{64} \\ 54 \\ \underline{40} \\ 14 \end{array}$$

Verificamos que o número 118 é igual a $8 \cdot 14 + 6$, ou seja, pertence à família dos números que estão no fio G.

Todos os números de nosso exemplo, que estão no mesmo fio, tem uma particularidade em comum, deixam o mesmo resto ao serem divididos por 8 e, como já comentamos na introdução, são congruentes entre si, no módulo 8.

O número 14, por exemplo, é congruente ao número 22, no módulo 8, e isso significa que esses dois números deixam o mesmo resto quando divididos por 8 (verifique que ambos estão sobre o fio G). Verificando:

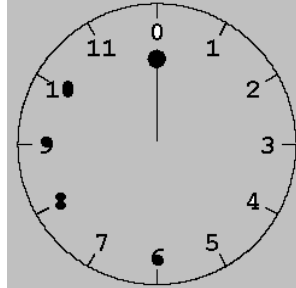
$$\begin{array}{r|l} 14 & 8 \\ \hline 6 & 1 \end{array}$$

$$\begin{array}{r|l} 22 & 8 \\ \hline 6 & 2 \end{array}$$

Simbolicamente, poderemos escrever: $14 \equiv 22, \text{ mod. } 6$

Exemplo 2:

Aritmética do relógio



Trata-se de um caso de congruência, módulo 12 (nos relógios analógicos, é claro). Note que 13 horas é congruente a 1 hora, no módulo 12. Ambos divididos por 12, deixam resto 1. 17 horas é congruente a 5 horas, módulo 12. Tanto 17, como 5, divididos por 12, deixam resto 5... e assim, sucessivamente.

$$1 \equiv 13 \equiv 25 \equiv \dots, \text{ mod } 12$$

$$5 \equiv 17 \equiv 29 \equiv \dots, \text{ mod } 12$$

Assim as horas marcadas num relógio analógico constituem também um caso clássico de congruência, nesse caso com módulo 12.

Exemplo 3:

Vejamos uma aplicação interessante sobre o tema, relacionada aos calendários:

Vamos supor que você saiba em qual dia da semana caiu o dia 1º de janeiro de um determinado ano. Em 2006, por exemplo, foi um domingo. Imaginemos que você deseja saber quando cairá um outro dia qualquer (vale para qualquer ano). É só montar uma tabela para essa primeira semana, que no caso será:

Domingo → 1 Segunda → 2 Terça → 3 Quarta → 4 Quinta → 5 Sexta → 6 Sábado → 7

Verificamos aqui que estamos novamente diante de um caso de congruência, módulo 7 nesse caso. Digamos que estivéssemos interessados em descobrir em que dia da semana caiu o dia 5 de julho (e não temos um calendário em mãos, é claro). Primeiro precisamos ver quantos dias existem de 1 de janeiro até 5 de julho. Vejamos:

Janeiro = 31 dias
 Fevereiro = 28 dias (2006 não é bissexto)
 Março = 31 dias
 Abril = 30 dias
 Maio = 31 dias
 Junho = 30 dias
 Julho = 5 dias
Total = 186 dias.

Agora, é como se tivéssemos uma fila de 186 dias e estamos desejando saber, na congruência de módulo 7 (7 dias da semana) qual o correspondente ao 186. Acho que você concorda que estamos

diante de uma situação bem semelhante à que vimos no problema da aranha e também no problema dos relógios analógicos.

Se dividirmos 186 por 7, teremos:

$$\begin{array}{r} 186 \quad | \quad 7 \\ \underline{4 \quad 26} \end{array}$$

Logo, o 186 é congruente ao 4, no módulo 7. Como o dia 4 de janeiro de 2006 foi uma quarta-feira, o 186º desse mesmo ano também o será e, é claro, que todas as demais quarta-feiras deste ano serão ocupados por números congruentes ao 4, módulo 7.

Assim, com os três exemplos que mostramos, podemos observar que em nosso cotidiano existem inúmeras situações onde se faz presente a noção de congruência, módulo k . Calendários, relógios analógicos e problemas em geral envolvendo repetições periódicas. Mostraremos em nosso estudo que na criptografia e em diversos números de documentos de identificação (como no CPF, por exemplo), também está presente a Aritmética Modular e a noção de congruência.

1.2) Conceitos Básicos da Congruência módulo k

- Se os inteiros a e b dão o mesmo resto quando divididos pelo inteiro k ($k > 0$) então podemos dizer que a e b são côngruos, módulo k e podemos representar:

$$a \equiv b \pmod{k}$$

- Uma maneira equivalente de dizer isso é afirmar que a diferença $(a - b)$ ou $(b - a)$ é divisível por k , ou que k é divisor dessa diferença. Veja um exemplo:
 $47 \equiv 43 \pmod{4}$, logo $(47 - 43)$ é divisível por 4.
- A congruência define uma equivalência, pois atende às propriedades reflexiva, simétrica e transitiva, ou seja:
 $a \equiv a, \pmod{k}$ (reflexiva)
 $a \equiv b, \pmod{k}$, então $b \equiv a, \pmod{k}$ (simétrica)
 $a \equiv b, \pmod{k}$ e $b \equiv c, \pmod{k}$, então $a \equiv c, \pmod{k}$ (transitiva)
- Algumas propriedades da congruência**
- Se $a \equiv b, \pmod{k}$ e $c \equiv d, \pmod{k}$, então:**
 $a + c \equiv b + d, \pmod{k}$; $a - c \equiv b - d, \pmod{k}$; $a \cdot c \equiv b \cdot d, \pmod{k}$

É claro que todas essas propriedades precisam ser demonstradas. Vejamos a demonstração da primeira.

Se $a \equiv b, \pmod{k}$, então $a - b$ é divisível por k , analogamente, se $c \equiv d, \pmod{k}$, então $c - d$ também é divisível por k , para provarmos que $a + c \equiv b + d$, teremos que mostrar que $(a + c) - (b + d)$ é divisível por k . Vamos colocar essa diferença na forma $(a - b) + (c - d)$ e verificar se é divisível por k . Como, pela hipótese, $(a - b)$ e $(c - d)$ eram divisíveis por k , é claro que a soma $(a - b) + (c - d)$ é também divisível por k , o que demonstra a primeira propriedade. Tente fazer as demais demonstrações, de modo análogo.

2) Algumas aplicações da congruência

2.1) Sistemas de identificação

Em qualquer texto, um erro de ortografia numa palavra pode ser facilmente percebido, pois ou a palavra não faz parte do idioma ou não faz sentido com o contexto. Por exemplo, se digitamos **engeneior**, logo percebemos que fizemos uma inversão das duas últimas letras. Mas, quando isso ocorre com os algarismos de um número, de um código de identificação qualquer, não teríamos como perceber a troca num simples olhar. Para isso e também para minimizar fraudes, foram criados os chamados dígitos de controle ou verificação. Tais dígitos são normalmente baseados na noção de **congruência** que mostramos anteriormente.

Mostraremos a seguir alguns desses casos de dígitos de controle usados como identificadores.

2.1.1) ISBN

Um dos exemplos mais antigos é o sistema International Standard Book Number (ISBN) de catalogação de livros, CD-Roms e publicações em braile, que foi criado em 1969. A necessidade que as editoras têm de catalogar os seus livros e informatizar o sistema de encomendas serviu de motivação na geração desse código.

A vantagem é que, por ser um código numérico, ultrapassa as dificuldades geradas pelos diversos idiomas do mundo, bem como a grande diversidade de alfabetos existentes. Dessa forma, poderíamos, por exemplo, identificar através do ISBN um livro japonês.

Em tal sistema, as publicações são identificadas através de 10 algarismos, sendo que o último (dígito de controle) é calculado através da aritmética modular envolvendo operações matemáticas com os outros nove dígitos. Esses nove primeiros dígitos são sempre subdivididos em 3 partes, de tamanho variável, separadas por hífen, que transmitem informações sobre o país, editora e sobre o livro em questão.

Por exemplo, a língua inglesa é identificada somente pelo algarismo 0 e a editora McGraw-Hill tem um código de 2 algarismos que a identifica, dessa forma, restam ainda 6 algarismos para a identificação de suas publicações, havendo pois a possibilidade de $10^6 = 1\ 000\ 000$ de títulos.

Vejamos como se processa o cálculo do dígito final do ISBN (controle).

Representando por $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9$ a seqüência formada pelos 9 primeiros dígitos, devemos multiplica-los, nessa ordem, pela base $\{10, 9, 8, 7, 6, 5, 4, 3, 2\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser o menor valor possível, tal que ao ser acrescentado à soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é **S**, o número **S + a₁₀** deve ser múltiplo de 11, ou seja, **S + a₁₀ ≡ 0 mod 11**.

Vejamos um exemplo:

Na contracapa do livro Temas e Problemas Elementares, da Coleção Professor de Matemática, da SBM, temos o seguinte código do ISBN: 85-85818-29-8. Vejamos o cálculo do dígito de controle que, como estamos observando, é igual a 8.

8	5	8	5	8	1	8	2	9
10	9	8	7	6	5	4	3	2

Efetando as multiplicações correspondentes e somando os produtos obtidos, teremos:

$$8 \cdot 10 + 5 \cdot 9 + 8 \cdot 8 + 5 \cdot 7 + 8 \cdot 6 + 1 \cdot 5 + 8 \cdot 4 + 2 \cdot 3 + 9 \cdot 2 =$$

$$= 80 + 45 + 64 + 35 + 48 + 5 + 32 + 6 + 18 = 333$$

$$\begin{array}{r} 333 \quad | \quad 11 \\ \underline{ } \\ 3 \quad 30 \end{array}$$

Para obtermos um múltiplo de 11, ao acrescentarmos o décimo algarismo, o menor valor que atende a tal condição será o número 8, pois $11 - 3 = 8$. O que confere o valor apresentado no código dado. Isso significa dizer que $333 + 8 = 341$ é um múltiplo de 11, ou ainda, que $341 \equiv 0 \pmod{11}$.

Um outro exemplo:

O livro Matemática Aplicada à Administração, Economia e Contabilidade, da Editora Thompson, tem o seguinte código ISBN 85-221-0399-?

Qual o seu dígito de controle?

Solução:

$$\begin{array}{r} 8 \ 5 \ 2 \ 2 \ 1 \ 0 \ 3 \ 9 \ 9 \\ 10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \end{array}$$

Efetuando a soma dos produtos correspondentes, teremos:

$$80 + 45 + 16 + 14 + 6 + 0 + 12 + 27 + 18 = 218$$

$$\begin{array}{r} 218 \quad | \quad 11 \\ \underline{ } \\ 9 \quad 19 \end{array}$$

Dessa forma, o dígito de controle será igual a 2 ($11 - 9 = 2$).

Podemos observar que os dois livros que usamos como exemplo tem o prefixo 85, que identifica livros publicados no Brasil.

Vejam os um exemplo de outro país:

O livro “Hilbert”, de Constance Reid, publicado em alemão (Berlim), tem o seguinte código ISBN: 3-540-04999-1. Façamos a verificação do cálculo do dígito de controle (1).

$$\begin{array}{r} 3 \ 5 \ 4 \ 0 \ 0 \ 4 \ 9 \ 9 \ 9 \\ 10 \ 9 \ 8 \ 7 \ 6 \ 5 \ 4 \ 3 \ 2 \end{array}$$

$$30 + 45 + 32 + 0 + 0 + 20 + 36 + 27 + 18 = 208$$

$$\begin{array}{r} 208 \quad | \quad 11 \\ \underline{ } \\ 10 \quad 18 \end{array}$$

Logo, o dígito é igual a 1 ($11 - 10$).

OBSERVAÇÕES:

- No ISBN, se o dígito for igual a 10 (no caso do resto da divisão por 11 ser igual a 1), é usada a representação do 10 em algarismos romanos, ou seja usa-se um X.

- Em todos os casos que iremos mostrar, que usam aritmética modular, são usadas bases de multiplicação que operadas com os dígitos do número geram um determinado valor S . A esse valor obtido deve ser somado ou subtraído um valor x , de modo a que exista uma congruência ao zero, num módulo que normalmente é 11 ou 10, conforme o caso.
- A partir de janeiro de 2007 os códigos do ISBN estão sendo representados com 13 dígitos. No caso dos livros editados no Brasil há um acréscimo dos dígitos 978 antes do 85.

2.1.2) CÓDIGO DE BARRAS EAN-13

Um dos códigos de barras mais usados no mundo todo é o EAN-13, constituído de 13 algarismos, sendo que o último é o dígito de controle. Nesse caso é usada a congruência módulo 10 e os fatores que compõem a base de multiplicação são os dígitos 1 e 3, que vão se repetindo da esquerda para a direita.

Se $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 a_{10} a_{11} a_{12}$ a seqüência formada pelos 12 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 3, 1, 3, 1, 3, 1, 3, 1, 3, 1, 3\}$ e somar os produtos obtidos. Vamos representar por S a soma obtida. O dígito que está faltando, que vamos representar por a_{13} deve ser tal que ao ser somado com S , deve gerar um múltiplo de 10, isto é, o número $S + a_{13}$ deve ser múltiplo de 10, ou seja, $S + a_{13} \equiv 0 \pmod{10}$.

Vejamos um exemplo:

Numa embalagem de uma garrafa para bebidas, de Portugal, temos o seguinte código de barras:



Vamos efetuar os cálculos para a determinação do dígito de controle (que estamos vendo ser o dígito 7).

8 4 2 4 9 0 6 2 0 1 7 6
1 3 1 3 1 3 1 3 1 3 1 3 (esta é a base de multiplicação, nesse caso)

Efetuando os produtos, teremos:

$$8 + 12 + 2 + 12 + 9 + 0 + 6 + 6 + 0 + 3 + 7 + 18 = 83$$

$$\begin{array}{r} 83 \quad | \quad 10 \\ \underline{\quad} \\ 3 \quad 8 \end{array}$$

Logo, o dígito de controle será igual a 7 ($10 - 3$). Note que $83 + 7 = 90$ (múltiplo de 10)

Sabemos também que, no código de barras com 13 algarismos, os **três primeiros** dígitos do código representam o país de registro do produto (verifique que para produtos filiados no Brasil teremos sempre os dígitos 7, 8 e 9); os **quatro dígitos seguintes** identificam o fabricante; os

próximos cinco dígitos identificam o produto e o último, como já sabemos, é o dígito verificador ou de controle, que se pode calcular através da congruência, módulo 10.

2.1.3) Cadastro das pessoas físicas na Receita Federal – CPF

Outro exemplo importante, do nosso cotidiano: Verificação dos dois dígitos de controle do CPF de uma pessoa:

O número de CPF de uma pessoa, no Brasil, é constituído de 11 dígitos, sendo um primeiro bloco com 9 algarismos e um segundo, com mais dois algarismos, que são, como no ISBN e nos códigos de barra, dígitos de controle ou de verificação . A determinação desses dois dígitos de controle é mais um caso de aplicação da noção de congruência.

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

Se $a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9$ é a seqüência formada pelos 9 primeiros dígitos, devemos multiplicá-los, nessa ordem, pela base $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ e somar os produtos obtidos. O dígito que está faltando, que vamos representar por a_{10} deve ser tal que ao ser subtraído da soma obtida, deve gerar um múltiplo de 11, isto é, se a soma obtida é S , o número $S - a_{10}$ deve ser múltiplo de 11, ou seja, $S - a_{10} \equiv 0 \pmod{11}$. Note que tal número será o próprio resto da divisão por 11 da soma obtida.

Por exemplo, se o CPF de uma pessoa tem os seguintes 9 primeiros dígitos: 235 343 104, o primeiro dígito de controle será obtido da seguinte maneira:

Escrevemos os nove primeiros e, abaixo deles, a base de multiplicação com os dígitos de 1 a 9.

$$\begin{array}{cccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 & \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \end{array}$$

Efetuando as multiplicações correspondentes, teremos:

$$2 \times 1 + 3 \times 2 + 5 \times 3 + 3 \times 4 + 4 \times 5 + 3 \times 6 + 1 \times 7 + 0 \times 8 + 4 \times 9 = 116.$$

Dividindo o número 116 por 11, teremos:

$$\begin{array}{r} 11 \\ 116 \\ \underline{110} \\ 6 \end{array}$$

Dessa forma, o primeiro dígito de controle será o algarismo **6**.

A determinação do segundo dígito de controle é feita de modo similar, sendo que agora acrescentamos o décimo dígito (que é o que acabamos de calcular) e usamos uma base de multiplicação de 0 a 9.

Vejamos:

$$\begin{array}{cccccccccc} 2 & 3 & 5 & 3 & 4 & 3 & 1 & 0 & 4 & 6 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array}$$

Efetuando as multiplicações, teremos:

$$2 \times 0 + 3 \times 1 + 5 \times 2 + 3 \times 3 + 4 \times 4 + 3 \times 5 + 1 \times 6 + 0 \times 7 + 4 \times 8 + 6 \times 9 = 145$$

Dividindo o número 145 por 11, teremos:

$$\begin{array}{r} 11 \\ 145 \\ \underline{132} \\ 2 \end{array}$$

Logo, o segundo dígito de controle é o **2**.

Concluimos então que, no nosso exemplo, o CPF completo seria: 235 343 104 **62**

Se o resto da divisão fosse 10, ou seja, se o número obtido fosse congruente ao 10, módulo 11, usaríamos, nesse caso, o dígito **zero**.

2.2) Congruência e Criptografia

Gpukpq Hwpcfogpvcn

Com certeza a frase acima nada significa para você. Parece algum idioma desconhecido ou de outro planeta. Experimente agora substituir cada letra pela segunda letra que vem antes dela, na seqüência do alfabeto completo (26 letras, incluindo k, w e y). Sem grande dificuldade você terá escrito "**Ensino Fundamental**".

De uma forma simplificada é o que ocorre na criptografia, quando alguém deseja transmitir alguma informação que não deseja partilhar com os outros, a não ser o destinatário final e combina uma chave qualquer para transmissão e recepção da informação. O receptor, de posse da chave, decodifica a mensagem, transformando-a novamente para que possa entender e ler o que lhe foi enviado. No exemplo que demos, que é bastante simples, o emissor substituiu cada letra do alfabeto por uma outra que ficava duas posições depois dela, no alfabeto. O receptor, sabendo da chave dessa "criptografia", aplicava a operação inversa na frase recebida, ou seja, substituía cada letra recebida pela que ficava duas posições antes dela, no alfabeto.

Se designarmos por x a letra original e por y a letra que a substituirá no código, é como se tivéssemos uma função, definida por $y = x + 2$.

Sabe-se que a primeira aplicação de criptografia foi inventada pelo imperador romano Julio César, que enviava mensagens aos seus generais trocando letras do alfabeto a partir de uma simples regra, similar à que exemplificamos acima, que seria "pule três" (chave 3). Através deste esquema, as letras eram trocadas pela terceira letra anterior no alfabeto. Desta forma, somente quem soubesse da regra conseguia desfazer o algoritmo e ler a mensagem original.

Veja como funcionava essa chave 3, de Julio César:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W

Ou seja, uma palavra simples como "**atacar**" seria codificada como "**xqxzxo**". Este sistema e outros similares, obtidos através de permutações, em que as letras são "embaralhadas", são muito simples e, não difíceis de serem "decifrados", mas por muito tempo serviram para "esconder" mensagens.

Vejamos um exemplo mais completo e a relação que tem com a aritmética modular:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
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

Chave: Somar 4

Cada letra fica representada por um número que representa a sua posição no alfabeto. Com essa chave, ela fica substituída pela letra cujo número corresponde ao número original, aumentado de 4. Quando acontecer do resultado ser superior ao 26, voltamos ao início do alfabeto. Por exemplo, o número 28 corresponderá à letra b, pois $28 = 26 + 2$ e, como já sabemos $28 \equiv 2 \pmod{26}$.

Atividades como essa, aplicadas nas classes do Ensino Fundamental, levarão os alunos a perceber que, na tradução da mensagem enviada eles terão, que aplicar a operação inversa da que foi usada pelo emissor da mensagem, na criação da mensagem criptografada.

Em classes do Ensino Médio o professor poderia representar cada chave por uma função bijetora (para que tivesse inversa) e o receptor da mensagem criptografada teria que obter a função inversa, para traduzir a mensagem recebida.

Ainda no Ensino Médio a chave poderia ser representada por matrizes inversíveis e a decodificação pelo receptor seria através da matriz inversa

Através da chave dada como exemplo (somar 4 ou $y = x + 4$), se a mensagem a ser enviada fosse **CIDADE MARAVILHOSA**, o grupo emissor teria que criptografá-la como: **GMHEHI QVEZMPLSWE**.

O grupo receptor da mensagem, sabendo que a chave foi “somar 4”, teria agora que subtrair 4 unidades dos números que representam cada letra da mensagem criptografada, para obter a mensagem original, decifrando o código. Vejamos:

G $7 - 4 = 3 = \mathbf{C}$	Q $17 - 4 = 13 = \mathbf{M}$
M $13 - 4 = 9 = \mathbf{I}$	E $5 - 4 = 1 = \mathbf{A}$
H $8 - 4 = 4 = \mathbf{D}$	V $22 - 4 = 18 = \mathbf{R}$
E $5 - 4 = 1 = \mathbf{A}$	E $\quad = \mathbf{A}$
H $\quad = \mathbf{D}$	Z $26 - 4 = 22 = \mathbf{V}$
I $9 - 4 = 5 = \mathbf{E}$	M $13 - 4 = 9 = \mathbf{I}$
	P $16 - 4 = 12 = \mathbf{L}$
	L $12 - 4 = 8 = \mathbf{H}$
	S $19 - 4 = 15 = \mathbf{O}$
	W $23 - 4 = 19 = \mathbf{S}$
	E $\quad = \mathbf{A}$

Durante a segunda guerra mundial sistemas eletromecânicos na codificação e decodificação das mensagens foram muito usados. Nestes dispositivos, rotores incorporavam internamente uma permutação e sua instalação em mecanismos parecidos com "counters" (ou contadores) permitiam transformações polialfabéticas produzindo uma quantidade impressionante de combinações.

Graças aos mais de sete mil ingleses que trabalharam no famoso Quartel General das Comunicações Governamentais ("Government Communications Headquarters") em "Bletchey Park", os códigos alemães foram quebrados. Eles tratavam em torno de quatro mil sinais alemães *por dia* e, secretamente, mantinham os comandos britânico e americano muito bem informados. Ainda durante a guerra computadores (como o "Colossus") foram usados na "quebra" de códigos alemães, italianos e japoneses e, desde então, a Criptografia passou a ser estudada de forma mais científica.

Depois da Segunda Guerra Mundial, com o desenvolvimento dos computadores, a área realmente floresceu incorporando complexos algoritmos matemáticos. Na verdade, esse trabalho criptográfico formou a base para a ciência da computação moderna.

Diversos filmes e livros têm explorado de forma inteligente esse tema, como "Uma Mente Brilhante" um filme estrelado por Russel Crowe e que contava a história do brilhante matemático

John Nash. Os livros “Fortaleza Digital” e “Código Da Vinci”, de Don Brown também tratam desse tema.

Mas como funciona a aritmética modular na Criptografia?

Imaginemos um casal, Alice e Bob, que vivem isolados e apenas podem comunicar através do correio. Eles sabem que o carteiro é um tremendo “fofoqueiro” e que lê todas as suas cartas. Alice tem uma mensagem para Bob e não quer que ela seja lida. Que é que pode fazer? Ela pensou em lhe enviar um cofre com a mensagem, fechado a cadeado. Mas como lhe fará chegar a chave? Não pode enviar dentro do cofre, pois assim Bob não o poderá abrir. Se enviar a chave em separado, o carteiro pode fazer uma cópia.

Depois de muito pensar, ela tem uma idéia. Envia-lhe o cofre fechado com um cadeado. Sabe que Bob é esperto e acabará por perceber a sua idéia. Com mais uma ida e uma volta do correio, e sem nunca terem trocado chaves, a mensagem chega até Bob, que abre o cofre e a lê. Como é que você acha que resolveram o problema? Pense bem no assunto, tente responder a questão. É simples... depois que você descobrir, é claro.

O “truque” usado foi o seguinte: Bob colocou um outro cadeado no cofre e ele tinha a chave desse segundo cadeado. Devolve o cofre a Alice por correio, desta vez fechado com os dois cadeados. Alice remove o seu cadeado, com a chave que possui e reenvia o cofre pelo correio só com o cadeado colocado por Bob. É claro que Bob tem apenas que abrir o cofre, com a sua própria chave e ler a mensagem enviada pela sua amada. O carteiro não tem como saber o conteúdo do cofre.

CRATO, N., Alice e Bob. *Expresso / Revista*, 22 de Setembro, pp. 118-120. (2001)

Na criptografia usam-se chaves que, de certa forma, são análogas à estratégia usada pelos namorados de nossa história.

Esta história relata a velha charada do sigilo nas comunicações e uma de suas brilhantes soluções. Talvez tenha servido de inspiração para os três jovens norte-americanos, Whitefield Diffie, Martin Hellman e Ralph Merkle, ao construírem em 1976 um sistema de **criptografia** em que o segredo da comunicação é assegurado por duas chaves, que os comunicantes não precisam trocar entre si, como aconteceu na historinha do Bob e da Alice. Foi esta invenção que inspirou o sistema de criptografia RSA.

Alice e Bob são personagens fictícios, mas são nomes sistematicamente utilizados pelos especialistas de criptografia. É mais interessante do que falar apenas no emissor e receptor, ou apenas em A e B. Costuma se acrescentar a eles uma terceira personagem, representada na nossa história pelo carteiro, que costuma receber o nome de Eva - «Eve», em inglês - e que representa aquela que se põe à escuta - ou seja, aquela que “eavesdrop”.

Até à descoberta de Diffie, Hellman e Merkle, a comunicação de mensagens cifradas exigia uma troca da chave da cifra, como fizemos nas atividades anteriores e como era feito nas chaves de Júlio César. Era preciso que Alice e Bob se encontrassem previamente e combinassem uma chave que apenas eles dois conhecessem. Só isso lhes permitiria, posteriormente, trocar mensagens à distância sem que Eva, sempre à escuta, conseguisse percebê-las. Assim funcionaram as mensagens secretas desde os tempos de César até aos tempos modernos, assim funcionaram espiões, conspiradores e simples amantes. A chave poderia ser simples, mas era sempre necessário que Alice e Bob combinassem tudo antes, e nem sempre isso era possível.

A idéia de Diffie, Hellman e Merkle é pois revolucionária. Segundo o esquema que propuseram, Alice e Bob começam por acordar em dois números. E estes podem ser públicos, pois mesmo que Eva os consiga descobrir não terá como descobrir a chave do processo. Cada um deles escolhe um outro número, que mantém secreto. Feitas algumas contas, baseadas em aritmética modular,

ambos chegam a um mesmo resultado: um número que mais ninguém conhece e que será a chave de codificação das suas mensagens. O processo que inventaram é relativamente simples, embora muito engenhoso, e será mostrado no quadro abaixo. Tudo se passa de forma parecida com a da história dos dois cadeados. As chaves não são trocadas, mas cada um acaba por poder abrir o cofre, sem que o carteiro, o consiga.

O processo inventado por Diffie, Hellman e Merkle marca o nascimento da criptografia com chaves públicas, que funcionam em conjunto com chaves secretas que não precisam ser “trocadas”. Baseia-se na aritmética modular, que consiste, essencialmente, em trabalhar com os restos da divisão inteira por um número determinado, chamado módulo. Esse processo foi denominado de congruência, módulo k , pelo famoso gênio da Matemática Gauss, conforme já observamos introdução desse artigo.

Simon Singh, no seu “Livro dos Códigos”, dá um exemplo que retrata bem o processo matemático da aritmética modular, envolvido nessas chaves públicas.

Os comunicantes, como Alice e Bob combinam nos números que servem: o primeiro de base para uma potenciação e o segundo para o módulo da congruência. Digamos que tenham optado pelos números **5** e **11**. Estariam então se referindo ao cálculo de 5^x e da congruência no módulo 11.

(O expoente x seria secreto, à escolha de cada um deles).

Alice escolhe **3** para seu número secreto (expoente da potência)

Alice calcula $5^3 = 125$ e, através de congruência módulo 11, gera o número 4, pois 125 dividido por 11 deixa resto 4.

Alice envia o resultado, 4, para Bob.

Bob escolhe **6** para seu número secreto (novamente o expoente da potência)

Bob calcula $5^6 = 15\ 625$ e, através de congruência módulo 11, gera o número 5, pois 15 625 dividido por 11 deixa resto 5.

Bob envia o resultado, 5, para Alice

Note que, mesmo que esses dois números que eles enviaram um ao outro, fossem interceptados, as pessoas não teriam como saber a chave final do processo.

Alice pega o resultado de Bob, **5**, e o seu número secreto, **3**, e calcula $5^3 = 125 = 4 \pmod{11}$. 125 dividido por 11 deixa resto 4.

Bob pega o resultado de Alice, **4**, e o seu número secreto, **6**, e calcula $4^6 = 4096 = 4 \pmod{11}$. 4096 dividido por 11 também deixa resto 4.

Veja que Alice e Bob encontraram o mesmo número, **4**, sem que tivessem informado um ao outro os seus números secretos pessoais. Esse número seria agora usado como chave para a composição das mensagens criptográficas. A congruência, como foi aplicada aqui, funcionou exatamente como a história dos cadeados e do correio, contada por Crato.

Tente fazer com outros números secretos, verifique que você sempre irá obter resultados iguais.

É através da criptografia que, diariamente, através da internet, uma luta sempre se processa: a de enviar dados e a de tentar captar esses dados (são os famigerados hackers).

É claro que o tema criptografia é muito mais complexo do que mostramos aqui. O que exemplificamos, através de chaves criptográficas simples, foi para mostrar a relação que existe entre esse tema e a aritmética modular. É um assunto bastante atual, interessante, e que pode ser usado em classes da Educação Básica, relacionado a conceitos importantes da Matemática, como Operações Inversas, divisibilidade e Funções.

2.3) Criptografia e calendários: Em que dia da semana você nasceu?

No sábado, dia 22 de julho de 2006, eu assistia ao programa Caldeirão do Huck, da Rede Globo de televisão quando, numa certa parte do programa, apareceu um rapaz de São Paulo que foi apresentado como o brasileiro possuidor da melhor memória. Ele representaria o Brasil num campeonato mundial de memorização. Esse rapaz, além da proeza de uma memória bem treinada, mostrou um truque que surpreendeu a todos: ele era capaz de descobrir o dia da semana correspondente a uma data qualquer que as pessoas escolhessem. O programa, muito bem produzido, colocou no telão um software que, após a pessoa ter escolhido uma data qualquer, mostrava o calendário do mês e do ano escolhidos, destacando o dia mencionado pela pessoa. O rapaz, com uma venda colocada nos olhos, acertou todos.

Na entrevista que deu ao apresentador do programa, o rapaz comentou que essa atividade não se tratava tanto de memória, mas sim de um cálculo que ele efetuava e que envolvia o número 7.

Lembrei que já tinha visto vários truques similares e que na Internet existem diversos sites com softwares onde você digita uma data qualquer e imediatamente aparece o dia da semana correspondente. Algumas calculadoras financeiras também têm programas prontos (função “calendário”) que fazem o mesmo. O que me ocorreu na hora é que, normalmente, a justificativa do método usado não é dada. As pessoas seguem certas “regrinhas” decoradas e conseguem descobrir os dias da semana desejados, que são normalmente datas de nascimento, casamento etc.

Após alguma pesquisa e com a fundamental ajuda do meu filho Vinícius, apresento aqui uma dessas “regrinhas”, acompanhada de sua justificativa matemática. Aos professores informo que é mais uma excelente atividade para sala de aula, envolvendo novamente a aritmética modular (congruência módulo 7).

Vejamos a regra prática, alguns exemplos e, finalmente, a explicação. O procedimento que escolhemos funciona para datas entre 1900 e 2399 (devido a uma particularidade dos anos bissextos terminados em “00”). Com algumas modificações, contudo, pode ser adaptado para atender quaisquer datas.

- 1) Calcule quantos anos se passaram desde 1900 até o ano em que você nasceu. Por exemplo, se você nasceu em 1980, irá anotar **80**. Vamos chamar essa quantidade de **A**.
- 2) Calcule quantos 29 de fevereiro existiram depois de 1900. Para isso, basta dividir por 4 o valor **A**, sem considerar o resto da divisão. Vamos chamar essa nova quantidade de **B**.
- 3) Considerando o mês do nascimento, obtenha o número associado a ele, que está na tabela logo abaixo. Procure o mês e anote o número que está ao lado dele. Vamos chamar esse número de **C**.

Tabela dos meses			
Janeiro	0	Julho	6
Fevereiro	3	Agosto	2
Março	3	Setembro	5
Abril	6	Outubro	0
Mai	1	Novembro	3
Junho	4	Dezembro	5

- 4) Considere o dia do nascimento (x). Calcule $x - 1$, que vamos chamar de D .
- 5) **Some** agora os quatro números que você obteve nas etapas anteriores ($A + B + C + D$). Divida essa soma obtida por sete (7) e verifique o valor do **resto** dessa divisão.
- 6) Finalmente, procure esse resto na tabela a seguir. Você terá o dia da semana do seu nascimento ou de qualquer outra pessoa que queira descobrir.

SEGUNDA-FEIRA	0	SEXTA-FEIRA	4
TERÇA-FEIRA	1	SÁBADO	5
QUARTA-FEIRA	2	DOMINGO	6
QUINTA-FEIRA	3		

Vejamos um exemplo. Vamos imaginar uma pessoa que tenha nascido em 16 de fevereiro de 1918. Qual foi o dia da semana?

- 1) **18** (1918 – 1900), logo, **A = 18**
- 2) $18:4 = 4$ (desconsidere o resto), logo, **B = 4**
- 3) O mês é Fevereiro, então **C = 3** (ver na tabela)
- 4) **$x = 16$** (dia do nascimento), logo, **D = 15** ($x - 1$)
- 5) Somando os quatro números, teremos $18 + 4 + 3 + 15 = 40$

$40 : 7 = 5$ e resto **5**. Na tabela o **5** é um **SÁBADO**.

Só para conferir, fomos procurar um calendário de 1918, destacando o mês de fevereiro. Veja que o dia 16 foi realmente um **SÁBADO**.

Fevereiro - 1918						
D	S	T	Q	Q	S	S
					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		

Interessante, não?

Justificativa matemática:

Fato número 1. O algoritmo (regrinha) que foi montado partiu do fato de que o dia 1º de janeiro de 1900 foi uma segunda-feira (0, na tabela). Todos os passos que foram colocados na regra prática visam determinar o “deslocamento”, na seqüência de dias da semana, que a data procurada tem em relação àquela segunda-feira, 01/01/1900, que é nosso “ponto de partida”.

Fato número 2. Cada ano de 365 dias vê seu primeiro de janeiro “afastado” de uma posição para a direita no ciclo dos dias da semana (segunda, terça, quarta, quinta, sexta, sábado, domingo, segunda, etc.) em relação ao dia-da-semana em que caiu o primeiro de janeiro do ano anterior. Isto porque 365 dividido por 7 deixa resto 1. Quando a pessoa faz a diferença entre o ano de seu nascimento e o ano 1900, está descobrindo quantos “afastamentos”, ou deslocamentos, essa data primeira sofreu em relação ao àquele 01/01/1900. Quando descobrimos, na fase seguinte, a quantidade de anos bissextos (ao dividir o resultado anterior por 4), estamos acrescentando o deslocamento adicional de mais uma “casa”, no ciclo de dias da semana, para cada ano bissexto

considerado. Isto porque os anos bissextos afastam o primeiro de janeiro do ano seguinte não em 1 “casa”, mas em 2, já que 366 deixa resto 2 quando dividido por 7.

Os dois primeiros passos do processo serviram apenas para localizar o dia 1º de janeiro do ano considerado, ou seja, até aqui apenas o **ANO** da data desejada foi considerado. Agora é a vez de acrescentarmos os deslocamentos gerados pelo mês e pelo dia da data procurada.

Fato número 3 – Se todos os meses do ano tivessem 28 dias (que gera resto zero ao ser dividido por 7), todos os meses teriam o seu dia primeiro exatamente no mesmo dia da semana que o primeiro de janeiro do ano considerado. Mas como temos meses com mais de 28 dias, todos esses meses (transcorridos de janeiro até o mês considerado) “empurram” o seu dia primeiro um certo número de “casas” adiante no ciclo dos dias da semana. A tabela criada para o nosso algoritmo está relacionada à aritmética modular, ou seja, à congruência módulo 7. Vejamos como surgiram os números da tabela.

Janeiro é a nossa referência, logo não há qualquer afastamento em relação a ele próprio (não há qualquer mês antes dele, empurrando seu dia primeiro para a direita, no ciclo, em relação ao próprio 1º de janeiro do ano em questão). Por isso, na tabela dada, ao lado do mês de janeiro, temos o número zero.

Como o mês de **janeiro** tem 31 dias e 31 dividido por 7 deixa resto 3, esse mês vai “empurrar” o primeiro dia do mês seguinte 3 “casas” para a direita em relação ao primeiro de janeiro daquele ano. Por isso, o mês de **fevereiro** recebe o número 3 na tabela.

Como **fevereiro** tem 28 dias e 28 dividido por 7 deixa resto 0, esse mês não irá acrescentar qualquer “deslocamento” adicional ao mês seguinte. Logo, o primeiro dia do mês de **março** cairá no mesmo dia da semana que o primeiro de fevereiro daquele ano, ou seja, será deslocado apenas das mesmas 3 “casas” para a direita, em relação ao primeiro de janeiro daquele ano. Por isso, na tabela dada, o mês de **março** também tem o número 3.

Como **março** tem 31 dias e 31 dividido por 7 deixa resto 3, esse mês vai “empurrar” os dias do mês seguinte um total de $(3 + 0 + 3)$ “casas” para a direita, já que como num dominó em cascata, esses deslocamentos são cumulativos. Por isso na tabela, o mês de **abril** tem o número 6.

Como **abril** tem 30 dias e 30 dividido por 7 deixa resto 2, esse mês vai “empurrar” os dias do mês seguinte um total de $(3 + 0 + 3 + 2)$ “casas”, mas como a semana só tem 7 dias, na congruência módulo 7 o número 8 corresponde ao 1 ($8 : 7 = 1$ e **resto 1**). Isto é, avançar oito “casas” no ciclo de dias da semana é o mesmo que avançar uma “casa” apenas. Por isso o mês de **maio** na tabela tem o número 1.

Assim por diante, justificam-se facilmente os números que estão ao lado dos outros meses.

Os passos que demos até aqui determinaram a quantidade de “casas” em que o primeiro dia do mês da data considerada está adiante, no ciclo dos dias da semana, do dia primeiro de janeiro de 1900. Precisamos agora, para finalizar, determinar a quantidade de deslocamentos necessários para atingirmos o exato **dia** procurado. Ora, se localizamos o dia 1 e queremos localizar o dia **x** de um determinado mês, precisamos ainda de um deslocamento correspondente a $(x - 1)$ “passos”. Veja, por exemplo, se a data procurada fosse o dia 4 de um determinado 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 numa sexta-feira (que está, evidentemente, 3 “casas” adiante de terça-feira, no ciclo).

É claro que a soma dos quatro números obtidos nas etapas do processo terá sempre de ser dividida por 7, pois são sete os dias da semana e o ciclo se repete sempre.

Essa atividade, ou brincadeira, ou truque é um outro exemplo interessante da nossa **congruência módulo k** , que nesse caso é igual a 7.

Que tal mais um exemplo?

Vamos descobrir em qual dia da semana caiu o Natal do ano 2000. Abaixo todos os passos do processo.

- 1) **100** (2000 – 1900). **A = 100**
- 2) $100 : 4 = 25$ (anos bissextos). **B = 25**
- 3) Mês dezembro, na tabela = **5**. **C = 5**
- 4) Natal = dia **25**, $x = 25$, logo **D = 24** ($x - 1$)

Somando $A + B + C + D$, teremos: $100 + 25 + 5 + 24 = 154$

Calculando o resto da divisão por 7.

$154 : 7 = 22$, resto **0**. Na tabela, temos **0 = 2ª feira**.

Vejamos o calendário de dezembro de 2000

Dezembro - 2000						
D	S	T	Q	Q	S	S
					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						

O rapaz que compareceu ao programa de TV devia usar essa regra ou outra semelhante e só teve que decorar a tabela dos meses e, é claro, ter facilidade para cálculo mental.

Referências

BRASIL, RPM, *Revista do Professor de Matemática*. Volumes 12 e 45. Sociedade Brasileira de Matemática.

BUCHMANN, J. *Introdução à Criptografia*. São Paulo: Berkeley, 2002.

BURNETT, S. & PAINE, S. *Criptografia e Segurança: o Guia Oficial RSA*. São Paulo: Campus, 2002.

CRATO, N., Alice e Bob. *Expresso / Revista*, 22 de Setembro, pp. 118-120. (2001)

MARTINI, R. *Criptografia e Cidadania Digital*. Rio de Janeiro: Ciência Moderna, 2001.

SINGH, S. *O Livro dos Códigos*. São Paulo: Record, 2001.

TERADA, R. *Segurança de Dados: Criptografia em Redes de Computadores*. São Paulo: Edgard Blucher, 2000.