

ARITMÉTICA MODULAR E SISTEMAS DE IDENTIFICAÇÃO

José Luiz Pastore Mello
São Paulo, SP

Introdução

Recentemente fui obrigado a solicitar uma segunda via do meu registro geral (RG) e para minha surpresa acrescentaram um dígito ao final do meu antigo número de RG. Na ocasião fiquei curioso em saber as razões desse dígito adicional, fato que só esclareci recentemente e que compartilho com o leitor neste artigo devido ao grande interesse matemático da questão.

A abordagem aqui proposta procura despertar a curiosidade do professor e sugerir material para aulas de aritmética do ensino fundamental e álgebra do ensino médio.

Sistemas de informação e a segurança na transmissão de dados

Aqueles que por ofício são obrigados a digitar enormes quantidades de números, como, por exemplo, o caixa de um banco ou o caixa de um supermercado, sabem muito bem que frequentemente acabam cometendo erros de digitação. Um erro de digitação pode ter sérias implicações, dependendo da natureza do que está sendo registrado. Imagine, por exemplo, que em diversos institutos de investigação médica, os dados de cada paciente em estudo são mantidos em sigilo, o que faz com que cada um seja apenas identificado por um código numérico. Um erro de digitação de um código nessa circunstância pode implicar sérios riscos ao paciente.

Pesquisas recentes ([2]) sobre a natureza dos erros de digitação cometidos revelam um fato curioso. Cerca de 79% dos erros ocorrem com a digitação equivocada de um único dígito (ou algarismo), como, por exemplo, digitar 1 573, quando o correto seria 1 673.

Esse tipo de erro recebe o nome de erro singular.

Outros 11% dos erros, chamados de erros de transposição, referem-se à troca de dois dígitos (ou algarismos), como, por exemplo, escrever MTAEMÁTICA, quando o correto seria MATEMÁTICA. Os demais 10% dos erros estão distribuídos em diversas categorias, nenhuma delas representando mais de 1% do total.

É bom que fique claro que existem particularidades em cada sistema de códigos, ou até mesmo em cada idioma, que podem mudar significativamente essa distribuição de probabilidades. Apenas para citar um exemplo, na Suécia os números de identificação de cada cidadão são constituídos por 6 algarismos para a data de nascimento (ano/mês/dia), seguidos de 3 algarismos para evitar duplicações de datas. Muitas pessoas, no entanto, ao digitar, permutam os algarismos do ano com os do dia, criando um erro muito frequente, que não é singular nem de transposição (trata-se aqui de um erro de trocas duplas).

Sabendo-se que nos dias de hoje cada vez mais usamos os computadores para armazenar e processar as informações digitadas, não seria possível criar um sistema que pudesse identificar com 100% de segurança um erro de digitação do tipo singular ou de transposição? Se isso fosse possível, nosso sistema daria conta de evitar cerca de 90% dos erros mais frequentes de digitação.

A aritmética modular e a solução do problema

O sistema ISBN (*International Standard Book Number*), criado em 1969 para a identificação numérica de livros, CD-Roms e publicações em *braille*, talvez seja um dos pioneiros na utilização de um dígito de verificação ao final de cada código capaz de resolver o problema dos erros singulares e de transposição. Por exemplo, o código ISBN 85-00-00669-2 refere-se ao livro *Os números governam o mundo*, de Malba Tahan. Com exceção do último dígito da direita, que é o dígito de controle, os demais 9 dígitos são responsáveis por identificar o país de origem da obra, a editora e o livro propriamente dito.

Os equipamentos que recebem a digitação de um código ISBN $x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9$ e seu dígito de verificação x_{10} estão programados para verificar se o resultado, S , da conta

$$10 \times x_1 + 9 \times x_2 + 8 \times x_3 + \dots + 2 \times x_9 + 1 \times x_{10}$$

é divisível por 11 ou não: o algoritmo de verificação é escolhido de tal forma que o resultado dessa conta tenha sempre resto zero na divisão por 11, ou com a notação de congruência, $S \equiv 0 \pmod{11}$. Veja, no exemplo do livro de Malba Tahan, que

$10 \times 8 + 9 \times 5 + 8 \times 0 + 7 \times 0 + 6 \times 0 + 5 \times 0 + 4 \times 6 + 3 \times 6 + 2 \times 9 + 1 \times 2 = 187$,
que é divisível por 11.

Podemos demonstrar um importante resultado com relação a esse sistema de aritmética módulo 11:

Proposição

Se ocorrer na leitura de um código ISBN um, e apenas um, dos dois erros (singular ou de transposição), então a soma S não será um múltiplo de 11.

Demonstração

Caso 1: ocorre um erro singular.

Seja $x_1 \dots x_i \dots x_{10}$ um código ISBN com dígito de verificação x_{10} e $x_1 \dots x_i^* \dots x_{10}$ o resultado da ocorrência de um erro singular na i -ésima posição. Chamemos de S e S^* as somas correta e errada respectivamente. Temos evidentemente que $S \equiv 0 \pmod{11}$ e $S^* - S = (11 - i)(x_i^* - x_i)$.

Se admitirmos por hipótese que S^* é múltiplo de 11 então, como 11 é primo, concluímos que 11 divide $11 - i$ ou divide $x_i^* - x_i$, o que é um absurdo, pois $11 - i$ e $x_i^* - x_i$ são números inteiros não nulos entre -10 e 10 . Logo, S^* não é múltiplo de 11.

Caso 2: ocorre um erro de transposição.

Seja $x_1 \dots x_i \dots x_j \dots x_{10}$ um código ISBN, x_{10} o dígito de verificação e $x_1 \dots x_j \dots x_i \dots x_{10}$ o resultado da ocorrência de uma transposição dos algarismos x_i e x_j nas posições i e j ($i \neq j$). Nesse caso, a diferença $S^* - S$ é igual a

$$(11 - i)x_j + (11 - j)x_i - (11 - i)x_i - (11 - j)x_j = (j - i)(x_j - x_i).$$

A hipótese de S^* ser múltiplo de 11 mais uma vez é absurda porque nos conduziria à conclusão de que um dos números $j - i$ ou $a_j - a_i$, que são números inteiros não nulos entre -10 e 10 , é múltiplo de 11. Segue que S^* não pode ser múltiplo de 11.

Se agora admitirmos que na leitura de um código ISBN só ocorrem erros singulares ou de transposição, não mais do que uma vez em cada número, então não ocorrem erros na leitura de um código ISBN se e somente se a soma S for um múltiplo de 11.

É bom lembrar que, ao digitarmos um código ISBN cometendo um erro singular ou de transposição, o equipamento que recebe os dados será capaz apenas de acusar a existência de um erro devido ao fato de S não ser divisível por 11, mas não será capaz de encontrá-lo; o que implica dizer que o digitador tem ainda como tarefa procurar o erro cometido.

O dígito de verificação do RG

Para o Estado de São Paulo e muitos outros Estados brasileiros, o dígito de verificação do RG é calculado da seguinte maneira:

Seja $x_1 x_2 x_3 x_4 x_5 x_6 x_7 x_8 x_9$ o RG de um indivíduo e x_{10} o dígito de verificação. Temos que a soma

$$100 \times x_{10} + 9 \times x_9 + 8 \times x_8 + 7 \times x_7 + \dots + 2 \times x_2 + 1 \times x_1$$

deverá ser divisível por 11 para que não tenha ocorrido um erro singular ou um erro de transposição. Como normalmente se reserva apenas um algarismo para o dígito de verificação, que é um inteiro entre 0 e 10 na aritmética módulo 11, normalmente se usa a letra X para representar o dígito de verificação 10, como, por exemplo, o RG número 25135622 - X . Verifique que

$100 \times 10 + 9 \times 2 + 8 \times 2 + 7 \times 6 + 6 \times 5 + 5 \times 3 + 4 \times 1 + 3 \times 5 + 2 \times 2 + 1 \times 0$
é divisível por 11.

Em Portugal, onde o algoritmo de verificação dos documentos de identificação é igual ao nosso, com a diferença de que lá se utiliza peso 10 no dígito de verificação em vez de peso 100, os responsáveis pela concepção do sistema decidiram não utilizar a letra X para um dígito de verificação 10, optando pelo uso do zero para representá-lo. É curioso notar, no caso português, onde um dígito de verificação 0 pode significar o número zero ou o número dez, que toda a concepção do sistema de

detecção de erros singulares e de transposição está comprometida para os portadores de documentos de identificação com dígito de verificação igual a 10.

É bom notar que o sistema brasileiro também não é uniforme. Recentemente descobri que o dígito de verificação do RG de um amigo nascido no interior do Rio Grande do Sul não segue o mesmo algoritmo válido para São Paulo e muitos outros Estados.

Bibliografia

[1] BUESCU, Jorge. *O mistério do Bilhete de Identidade e outras histórias*. Lisboa: Gradiva, 2001.

[2] PICADO, Jorge. *A álgebra dos sistemas de identificação: da aritmética modular aos grupos diedrais*, Boletim da Sociedade Portuguesa de Matemática, nº 44, abril/2001.

José Luiz Pastore Mello é mestrando em Educação Matemática na FE – USP e professor de Matemática do ensino médio no Colégio Visconde de Porto Seguro.
e-mail: jlpmello@uol.com.br
