Congruências, Matrizes e Cifras

por José Veiga de Faria

1. Introdução

Esta é a parte final do artigo que começámos no mês anterior e que pode ver carregando no link:

Cifras, congruências e matrizes

2. Cifrar e decifrar uma mensagem

Suponha que queremos cifrar a mensagem: $*A Matematica e fixe*$ (tirámos os acentos...) usando a matriz de cifra

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

Começamos por numerar as letras do alfabeto (se quisermos usar sinais e acentos temos de numerar os sinais e as letras acentuadas). Então: a=0, b=1, ... , w=25 e vamos usar o módulo 26 para que o conjunto dos resíduos positivos mínimos seja {0,...,25}. Agora emparelhamos as letras da mensagem a transmitir: am, at, em, at, ic, ae, fi, xe. A cada par corresponde um vector que transformamos usando a matriz escolhida. Assim, por exemplo, a xe corresponde o vector

$$\begin{pmatrix} 22 \\ 4 \end{pmatrix}$$

que se transforma no resíduo positivo mínimo de:

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \times \begin{pmatrix} 22 \\ 4 \end{pmatrix} = \begin{pmatrix} 70 \\ 48 \end{pmatrix}$$

ou seja em:

$$\begin{pmatrix} 18 \\ 22 \end{pmatrix}$$

que corresponde ao par: sx.
Se fizermos o mesmo para cada par (experimente) obtemos a sequência: $mmttzuttaseeyssx$ que é a sequência que transmitimos.
O receptor decifra a mensagem usando a matriz

$$\begin{pmatrix} 1 & -1 \\ -2 & 3 \end{pmatrix}$$

e procedendo de forma análoga. Testemos com o par inicial: mm. Corresponde-lhe o vector:

$$\begin{pmatrix} 12 \\ 12 \end{pmatrix}$$

que se transforma pela matriz indicada no vector:

$$\begin{pmatrix} 0 \\ 12 \end{pmatrix}$$

cujo resíduo positivo mínimo é ele próprio e a que correspondem as letras am as primeiras da mensagem transmitida. Convidamos o leitor a decifrar o resto da mensagem.

Nota final: Podíamos ter juntado as letras N a N. Nesse caso a matriz de cifra teria N linhas e N colunas e deveria ter determinante (aqui supomos que o leitor conhece Álgebra Linear) diferente de zero. Para decifrar usaríamos a inversa dessa matriz. Se escolher uma matriz com determinante igual a 1 obterá uma matriz de inteiros.

Observação: Claro que este código de cifra seria desastroso se fosse usado na Net: é muito fácil de quebrar. Na Net usa-se um sistema de Chave Pública e Chave Privada cuja eficácia assenta na impossibilidade prática de decompor em factores primos o produto de dois primos com elevado número de digitos.

Sugestão para os tempos livres: Desafiamos o leitor que goste de programar a fazer um pequeno programa, por exemplo em JustBasic (pode fazer o **download** grátis da net), para cifrar e decifrar mensagens.

Saudação final: OjetjLttll ; *matriz usada para cifrar*

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

Apêndice

Deixamos agora uma prova muito simples do tal resultado fulcral: se a matriz

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

é uma matriz de inteiros onde ad-bc=1 e C é o conjunto dos vectores com entradas em {0,...,m-1} então a transformação T definida por T(u)=rpm(Mxu) é uma bijeção de C em C.

Lema 1: Se M é uma matriz nas condições indicadas então

$$M^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

também está nessas condições e se u e v são vectores de inteiros

$$v = M \times u \Leftrightarrow u = M^{-1}v$$

Repare que disto resulta que a aplicação $v = M\ u$ é uma bijeção dos conjunto dos vectores com entradas inteiras nele próprio.

Prova: verifique directamente.

Lema 2: Se u e v pertencem a C e M é uma matriz nas condição indicadas então:

$$u \equiv\ v\,(mod\,m) \Rightarrow M \times u \equiv\ M \times v\,(mod\,m)$$

Prova: Provamos que as primeiras entradas dos transformados de u e v são congruentes para o módulo m. Ponhamos:

$$u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix} v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix}$$

Usando os resultados estabelecidos em Critérios de Divisibilidade temos, tomando congruências de módulo m:

$(u_1 \equiv v_1 \wedge u_2 \equiv v_2\,) \Rightarrow (a \times u_1 \equiv a \times v_1\ \wedge b \times u_2 \equiv b \times v_2\,) \Rightarrow a \times u_1 + b \times u_2 \equiv a \times v_1 + b \times v_2$

Agora é muito simples provar que:

Teorema: T(u)=rpm(Mxu) é uma bijeção de C em C:

Injectividade Se u e v são vectores de C, e tomando congruências dde módulo m, então:

$T(u) = T(v) \Leftrightarrow rpm(M{\times}u) = rpm(M{\times}v) \Rightarrow M{\times}u \equiv\ M{\times}v \Rightarrow M^{-1}(M{\times}u) \equiv\ M^{-1}(M{\times}v) \Leftrightarrow u \equiv\ v \Rightarrow u = v$

resultando a útima implicação de u e v serem resíduos positivos mínimos.

Sobrejectividade Resulta da injectividade e de C ser um conjunto finito.