Congruências, Matrizes e Cifras

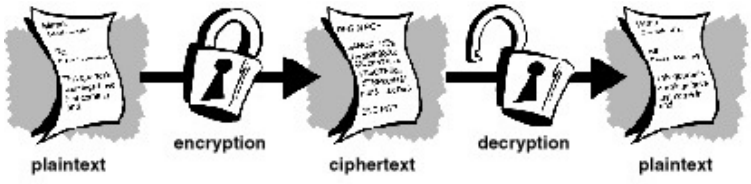
por José Veiga de Faria

Nota Inicial

Este pequeno artigo já foi aqui publicado há mais de dois anos. Como entretanto a audiência cresceu muito decidimos voltar a editá-lo. Publicamos este mês a primeira parte introduzindo algumas noções e resultados simples; no próximo artigo vamos usá-los para cifrar e decifrar mensagens.
Entretanto desafiamos os nossos leitores a provarem o resultado do ponto 5; se quiserem podem deixar um esboço da vossa prova na página do Clube no Facebook de forma a tornar esta rubrica mais rica e participada.

Introdução

Para transmitir uma mensagem com segurança é necessário cifrá-la.
Uma forma de o fazer é atribuir a cada letra do alfabeto um número de 0 a 25 e reeordenar os números de forma a obter uma nova chave; depois substituir cada letra da mensagem pelo número que lhe corresponde na nova chave e finalmente substitur cada um desses números pela letra correspondente na correspondência inicial.
Depois transmitimos a mensagem assim obtida que pode ser decifrada pelo receptor desde que este conheça a chave da reordenação.
A mensagem torna-se ainda mais difícil de decifrar se em vez de simples letras usarmos sequências de N letras.
O objectivo dos artigos deste e do próximo mês é mostrar como recorrendo a matrizes e congruências podemos cifrar e decifrar mensagens trabalhando com pares de letras.
A generalização para qualquer número de letras é simples de fazer para quem conhecer um pouco de Álgebra Linear.



Cifrando, decifrando

NOTA: Neste artigo usaremos propriedades das congruências estabelecidas em Critérios de Divisibilidade

1. A noção de matriz e vector de inteiros

Chamamos matriz a um quadro de inteiros com N linhas e M colunas. Se N = M a matriz diz-se quadrada.

NOTA: trabalharemos sempre só com inteiros.

Exemplo:

$$\begin{pmatrix} 2 & 3 \\ 7 & -1 \end{pmatrix}$$

Se a matriz só tem uma coluna chama-se um vector.

Exemplo:

$$\begin{pmatrix} 21 \\ 7 \end{pmatrix}$$

2. Produto de um inteiro por uma matriz e soma de vectores

Sendo n um inteiro é:

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

e dados dois vectores de inteiros é:

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

3. Produto de uma matriz por um vector

Dadas uma matriz quadrada e um vector com duas entradas é:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} u \\ v \end{pmatrix} = u \times \begin{pmatrix} a \\ c \end{pmatrix} + v \times \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} u \times a + v \times b \\ u \times c + v \times d \end{pmatrix}$$

A definição do produto de uma matriz com N linhas e colunas por um vector com N entradas é dada de igual modo.

4. Vectores congruentes

Se m é um inteiro positivo:

$$\begin{pmatrix} a \\ b \end{pmatrix} \equiv \begin{pmatrix} c \\ d \end{pmatrix} (mod\, m) \Leftrightarrow a \equiv c\, (mod\, m) \wedge b \equiv d\, (mod\, m)$$

Definimos resíduo positivo mínimo, para um módulo m, de um vector por:

$$rpm\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} rpm(a) \\ rpm(b) \end{pmatrix}$$

5. Um resultado importante

Agora deixamos o resultado fulcral cuja prova apresentamos no fim deste artigo.
Se a matriz M igual a

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

satisfaz a condição de ad - bc $\neq 1$ então a transformação

$$\begin{pmatrix} u \\ v \end{pmatrix} = T\begin{pmatrix} x \\ y \end{pmatrix} = rpm(M \times \begin{pmatrix} x \\ y \end{pmatrix})$$

define uma bijeção do conjunto de pares ordenados de elementos do conjunto

$$\{0, 1, ..., m-1\}$$

em si mesmo.
Além disso a matriz

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

faz o trabalho inverso:

$$\begin{pmatrix} x \\ y \end{pmatrix} = rpm(M^{-1}\begin{pmatrix} u \\ v \end{pmatrix})$$