

## Códigos modulares

**Definição** Um código modular de comprimento  $n$  e módulo  $k$  é constituído por  $n$  números naturais,  $(p_1, p_2, \dots, p_n)$ , inferiores a  $k$ .

Um número  $x_1x_2x_3\dots x_{n-1}x_n$  pertence a este código se verifica a seguinte regra:

$$p_1 \times x_1 + p_2 \times x_2 + \dots + p_n \times x_n \equiv 0 \pmod{k}$$

**Nota:** Os dígitos  $x_1, \dots, x_n$  podem não ser algarismos. Apenas é necessário que identifiquem um valor numérico. No código ISBN  $X$  representa o número 10.

### Exemplos.

- ISBN:  $n = 10$  e  $k = 11$ .
- EAN  $n = 10$  e  $k = 10$ .

**Proposição.** Um código modular  $(p_1, p_2, \dots, p_n)$  de módulo  $k$  detecta:

- (a) erros singulares na posição  $i$  se e só se  $\text{mdc}(p_i, k) = 1$ ;
- (b) a troca dos dígitos nas posições  $i$  e  $j$  se e só se  $\text{mdc}(p_i - p_j, k) = 1$ .

Deste resultado, conclui-se facilmente que se  $k$  é um número primo, então um código módulo  $k$  detecta todos os erros singulares. Esse é o caso do código ISBN, uma vez que 11 é primo.