Um sistema de identificação módulo k, com pesos $p_1, p_2, \ldots, p_n$, detecta todos os erros singulares na posição i se e só se $\text{mdc}(p_i, k) = 1$.

PROVA: Consideremos um número $a_1 a_2 \ldots a_n$ de um sistema de identificação módulo k. Um erro $a_i \to a_i'$ na i-ésima posição é detectável se e só se $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$. De facto, como a soma de teste $S' = p_1 a_1 + \cdots + p_i a_i' + \cdots + p_n a_n$ do número incorrecto e a soma de teste $S = p_1 a_1 + \cdots + p_i a_i + \cdots + p_n a_n$ do número correcto diferem $p_i(a_i' - a_i)$ unidades, então o erro será detectável se e só se $p_i(a_i' - a_i) \not\equiv 0 (\text{mod } k)$.

Assim, o sistema detecta todos os erros na posição i se e só se para quaisquer $a_i, a_i' \in \{0, 1, \ldots, k-1\}$ com $a_i \neq a_i'$, $p_i(a_i' - a_i) \not\equiv 0 \pmod{k}$. Esta condição é claramente equivalente a $\text{mdc}(p_i, k) = 1$. Com efeito, sob aquela condição, se $\text{mdc}(p_i, k)$ fosse igual a $d > 1$ teríamos $p_i = dd_1$ e $k = dd_2$ com $d_2 \in \{1, 2, \ldots, k-1\}$. Fazendo $a_i' = d_2$ e $a_i = 0$ obteríamos a condição absurda $p_i(a_i' - a_i) \equiv 0 \pmod{k}$. Reciprocamente, sendo $\text{mdc}(p_i, k) = 1$, se existissem diferentes a_i e a_i' em $\{0, 1, \ldots, k-1\}$ tais que $p_i(a_i' - a_i)$ é múltiplo de k, teríamos $(a_i' - a_i)$ múltiplo de k, o que é também absurdo pois $a_i' - a_i \in \{1, 2, \ldots, k-1\}$.

■

Um sistema de identificação módulo k, com pesos $p_1, p_2, \ldots, p_n$, detecta todas as transposições de algarismos nas posições i e j se e só se $\text{mdc}(p_i - p_j, k) = 1$.

PROVA: Consideremos um número $a_1 a_2 \ldots a_n$ de um sistema de identificação módulo k. Uma transposição dos algarismos a_i e a_j nas posições i e j é detectável se e só se $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$. Neste caso a diferença entre a soma de teste $S' = p_1 a_1 + \cdots + p_i a_j + \cdots + p_j a_i + \cdots + p_n a_n$ do número errado e a soma de teste $S = p_1 a_1 + \cdots + p_i a_i + \cdots + p_j a_j + \cdots + p_n a_n$ do número correcto é igual a $(p_i a_j + p_j a_i) - (p_i a_i + p_j a_j) = (p_i - p_j)(a_j - a_i)$. Portanto, o erro é detectável se e só se $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$.

Assim, o sistema detecta todas as transposições de algarismos nas posições i e j se e só se para quaisquer $a_i, a_j \in \{0, 1, \ldots, k-1\}$ com $a_i \neq a_j$, se tem $(p_i - p_j)(a_j - a_i) \not\equiv 0 \pmod{k}$. A prova do caso anterior diz-nos que esta condição é equivalente a $\text{mdc}(p_i - p_j, k) = 1$. ■

De modo análogo, podemos fazer o mesmo relativamente aos outros tipos de erros, obtendo a seguinte tabela com as condições de detecção dos tipos de erros mais comuns:

Tipo de erro	**Condições de detecção**
Erro singular: $a_i \to a_i'$	$\text{mdc}(p_i, k) = 1$
Transposição: $\ldots a_i \ldots a_j \ldots \to \ldots a_j \ldots a_i \ldots$	$\text{mdc}(p_i - p_j, k) = 1$
Erro gémeo: $aa \to bb$ (posições $i, i+1$)	$\text{mdc}(p_i + p_{i+1}, k) = 1$
Erro fonético: $a0 \to 1a$ (posições $i, i+1$), $a \in \{2, \ldots, k-1\}$	$ap_{i+1} \not\equiv (a-1)p_i (\text{mod } k)$
Erro gémeo intercalado: $aca \to bcb$ (posições $i, i+2$)	$\text{mdc}(p_i + p_{i+2}, k) = 1$
Erro gémeo generalizado: $a \ldots a \to b \ldots b$ (posições i, j)	$\text{mdc}(p_i + p_j, k) = 1$

Com esta tabela é agora muito fácil a qualquer pessoa desenhar sistemas de identificação modulares que detectem estes tipos de erros.

Observações: (1) É evidente porque é que os sistemas módulo 11 são muito comuns.

(2) A tabela revela ainda porque é que os sistemas que usem $k < 10$ são pouco utilizados: é impossível que todos os erros singulares e todas as transposições sejam detectados se não tivermos o cuidado de usar somente os algarismos entre 0 e $k-1$ (o que pode reduzir consideravelmente o tamanho do sistema). Por exemplo, não houve esse cuidado no sistema módulo 7 usado nos bilhetes de avião: como utiliza todos os algarismos entre 0 e 9, não distingue entre a_i e a_i' quando $|a_i - a_i'| = 7$. Por sua vez, o sistema módulo 9 utilizado nas notas de euros usa o algarismo 9 pelo que não detecta os erros $0 \to 9$ e $9 \to 0$.

(3) No caso $k = 10$ as condições da Tabela são incompatíveis: é impossível satisfazer a segunda se quisermos satisfazer a primeira pois, nesse caso, p_{i+1} e p_i são ímpares. É por isso que o sistema do código de barras, detectando todos os erros singulares, só tem 88.9% de eficiência na detecção das transposições de algarismos adjacentes.

Melhor eficácia num sistema destes é impossível. De facto, sendo p_{i+1} e p_i necessariamente ímpares, a diferença $p_{i+1} - p_i$ é um número par, digamos $2t$ ($t \in \mathbb{Z}$). Então, como $S' - S = (p_{i+1} - p_i)(a_i - a_{i+1})$, o sistema não detectará a transposição dos algarismos a_i e a_{i+1} se e só se $2t(a_i - a_{i+1})$ é múltiplo de 10, ou seja, não detectará nenhuma caso t seja múltiplo de 5 e, caso t não seja múltiplo de 5, não detectará aquelas em que $|a_i - a_{i+1}| = 5$. Portanto, qualquer sistema deste tipo que tenha 100% de eficiência na detecção dos erros singulares, detectará somente 88.9% das transposições adjacentes no caso em que a diferença entre os pesos p_{i+1} e p_i não seja múltipla de 10 ou, caso contrário, não detectará nenhuma.