

# Pagamentos de serviços e transferências: o papel da Matemática no reforço da segurança



**Ricardo Cunha Teixeira**  
Professor do Departamento de Matemática e Estatística da Faculdade de Ciências e Tecnologia da Universidade dos Açores  
ricardo.ec.teixeira@uac.pt

Os meses que antecedem o Natal constituem um período do ano propício ao consumismo. Por entre prendas, convívios, viagens e iguarias, muitas são as oportunidades para “abrir os cordões à bolsa”. Na verdade, esta expressão colocada entre aspas já não corresponde à realidade do dia a dia dos pagamentos e transações comerciais que, muitas vezes, se efetuam através dos serviços de Multibanco e de homebanking.

Diversas são as operações bancárias que podemos efetuar recorrendo ao Multibanco ou ao homebanking. Neste artigo, destacamos duas operações (os pagamentos de serviços e as transferências com recurso ao NIB ou ao IBAN) em que a Matemática desempenha um papel importante no reforço da segurança.

Começamos pelas transferências bancárias e por analisar o NIB (Número de Identificação Bancária). O NIB é composto por 21 algarismos, da esquerda para a direita: os 4 primeiros identificam o banco a que pertence a conta (por exemplo, 0007 para o Novo Banco, 0018 para o Santander, 0033 para o Millennium BCP e 0035 para a Caixa Geral de Depósitos); os 4 seguintes, o balcão ou agência; os 11 que se seguem, o número de conta propriamente dito; e os 2 últimos são algarismos de controlo.

Qual é o papel desempenhado pelos algarismos de controlo? Ora, quando lidamos com números de identificação arriscamos a que possam ser cometidos erros de escrita, nomeadamente nos casos em que o seu registo é feito por meios eletrónicos (por exemplo, podemos cometer um erro na escrita de um determinado algarismo, quando premimos uma tecla errada, ou podemos trocar dois algarismos consecutivos, quando as teclas correspondentes são carregadas pela ordem errada). Para evitar este tipo de situações, é habitual acrescentar-se no final da sequência de algarismos de um número de identificação um ou mais algarismos suplementares ou de controlo, que não têm informação específica, apenas se destinam a garantir que sejam detetados os erros que venham a ser cometidos.

Para cada tipo de número de identificação, é estabelecido o algoritmo que permite gerar os algarismos de controlo na criação de novos números. Quando os números já estão em circulação, esse algoritmo permite detetar erros que possam ocorrer na escrita, transmissão ou leitura da informação.

No caso do NIB, o algoritmo que permite verificar a sua validade designa-se por MOD 97-10 e é regulamentado pela norma ISO/IEC 7064. Este sistema é bastante eficaz. Deteta 100% dos erros singulares (quando escrevemos o algarismo

A	
←	$  \begin{array}{cccccccccccccccccccc}  0 & 0 & 3 & 5 & 0 & 0 & 2 & 1 & 0 & 3 & 7 & 8 & 2 & 9 & 6 & 0 & 5 & 4 & 6 & 2 & 7 \\  \times & \times \\  73 & 17 & 89 & 38 & 62 & 45 & 53 & 15 & 50 & 5 & 49 & 34 & 81 & 76 & 27 & 90 & 9 & 30 & 3 & 10 & 1  \end{array}  $
$S = 7 \times 1 + 2 \times 10 + 6 \times 3 + 4 \times 30 + \dots + 3 \times 89 + 0 \times 17 + 0 \times 73 = 2426 = 25 \times 97 + 1$	
potências de base 10	resto da divisão por 97
$10^0 = 1 \rightarrow 1$	$10^1 = 10 \rightarrow 10$
$10^2 = 100 \rightarrow 3$	$10^3 = 1000 \rightarrow 30$
$10^4 = 10\,000 \rightarrow 9$	$10^5 = 100\,000 \rightarrow 90$
...	...
B	
<b>IBAN → PT50 NIB</b> Verificação: <b>NIB PT50 → NIB 25 29 50</b> $\text{NIB} \times 1\,000\,000 = p \times 97 + 27$ $25\,2900 = 2607 \times 97 + 21$	
C	
ENTIDADE: 10155	→ 10155
REFERÊNCIA: 633 434 038	→ 6334340 38
VALOR: 109,33 €	→ 00010933
10155	6334340
00010933	38

“b” em vez do algarismo “a”), 100% das transposições de algarismos adjacentes (quando escrevemos “ba” em vez de “ab”) e, ainda, 100% das transposições intercaladas (quando escrevemos “bca” em vez de “acb”).

O leitor pode verificar a validade do seu NIB. A regra é a seguinte: os dois algarismos de controlo são escolhidos de forma que a divisão do NIB por 97 dê resto 1 (por outras palavras, um NIB é sempre composto por várias cópias do “97” mais uma unidade). Contudo, não é muito prático verificar que um número de 21 algarismos dá resto 1 ao dividir por 97, se recorrermos às calculadoras menos sofisticadas que são disponibilizadas nos telemóveis ou computadores. Em alternativa, a regra pode ser aplicada recorrendo a potências de base 10. Da direita para a esquerda, multiplica-se cada algarismo do NIB por uma potência de base 10. Quanto ao expoente, começa-se com 0 e, de um algarismo para o seguinte, aumenta-se uma unidade. Ao adicionarmos todos esses produtos, obtemos a soma de teste que coincide com o próprio número devido à natureza decimal do nosso sistema de numeração e que, por isso, deve dar resto 1 quando dividida por 97, para que o NIB seja válido. Como o sistema é validado mediante o cálculo do resto da divisão da soma de teste por 97, de modo a facilitar as contas, os valores das potências de base 10 podem ser substituídos pelos seus restos da divisão por 97. Em termos práticos, isto significa que podemos multiplicar os algarismos do NIB, da direita para a esquerda, pelos valores apresentados a cinza na Figura A. De notar que a forma mais simples de calcular o resto da divisão de um número por 97 consiste em retirar todos os “97” e verificar o que sobra. Por exemplo, o resto da divisão de 100 por 97 é 3, porque podemos retirar ao 100 um “97” (100-97=3). Já o resto da divisão de 1000 por 97 é 30, pois podemos retirar ao 1000 dez “97” (1000-10x97=1000-970=30). E assim sucessivamente.

Na Figura A, apresentam-se os cálculos de validação de um exemplo de um NIB, sendo que a soma de teste é igual a 2426, que dá resto 1 ao dividir por 97.

Da próxima vez que o leitor fizer uma transferência bancária, não fique preocupado em confirmar repetidas vezes que não se enganou na escrita do NIB, pois se cometer um erro a probabilidade de ele ser detetado é bastante elevada.

Passamos, agora, à análise do IBAN (International Bank Account Number). O IBAN identifica o número de conta de um cliente num contexto internacional, validando o país, o banco e a conta do beneficiário. Este sistema permite melhorar a eficácia do serviço prestado pelos bancos em transferências internacionais na Área Única de Pagamentos em Euros (SEPA). Não está ainda generalizado a todo o planeta, mas alguns países fora desta área já o adotaram também. Para contas portuguesas, o IBAN resulta de acrescentar PT50 à esquerda da sequência de algarismos do NIB. As letras PT identificam o país (neste caso, Portugal) e 50 corresponde aos dois algarismos de controlo do IBAN. Para verificar a validade de um IBAN, procede-se como ilustrado na Figura B: troca-se PT50 com o NIB e as letras são convertidas em valores numéricos: A = 10; B = 11; ...; Z = 35. Obtém-se uma sequência com 21+6=27 algarismos. O número formado por estes 27 algarismos deve dar resto 1 quando dividido por 97. Portanto, o IBAN também obedece ao algoritmo MOD 97-10.

Como os 21 algarismos que compõem o NIB já formam um número que dividido por 97 dá resto 1, ao multiplicar o NIB por um milhão de modo a acomodar os 6 algarismos correspondentes a PT50, obtém-se um número que dá resto 27 ao dividir por 97 (porque um milhão dá resto 27 ao dividir por 97). Por sua vez, ao substituir as letras pelos seus valores numéricos, PT00 representa o número 252900 (pois P=25 e T=29), que dá resto 21 quando dividido por 97. Como 21+27=48, preciso de 50 para obter 98, retirar 97 e, assim, o número composto pela totalidade dos 27 algarismos dar resto 1 quando dividido por 97. Por este motivo, todos os IBAN de contas portuguesas têm sempre 5 e 0 como algarismos de controlo.

Por fim, passamos aos pagamentos de serviços via Multibanco ou homebanking. Normalmente,

as plataformas que geram a informação (como a If Then Pay) recorrem também ao algoritmo MOD 97-10. Na Figura C apresenta-se um exemplo. Há a considerar a Entidade, a Referência e o Valor, que correspondem a números com, respetivamente, 5, 9 e 8 algarismos. O Valor deve ser sempre convertido numa sequência de 8 algarismos (6 algarismos para a parte inteira e 2 algarismos para a parte decimal relativa aos cêntimos), usando os zeros que forem necessários (por exemplo, 25 euros devem ser representados pela sequência 00002500). Em relação à Referência, da esquerda para a direita, os três primeiros algarismos identificam a subentidade (o vendedor), os quatro seguintes a encomenda ou o cliente e os últimos dois são os algarismos de controlo.

Os 22 algarismos são rearranjados como se ilustra na Figura C. O número obtido deve dar resto 1 quando dividido por 97. Os dois algarismos de controlo são calculados de modo que esta propriedade se verifique. O leitor poderá comprovar que o número obtido na Figura C dá, de facto, resto 1 quando dividido por 97. Para tal, basta recorrer à estratégia exemplificada na Figura A. Como este número tem mais um algarismo que um NIB, o primeiro algarismo (da esquerda para a direita) é multiplicado por 51, que corresponde ao resto da potência de base 10 e expoente 21, quando dividida por 97. Fazendo as contas, obtém-se  $S=1844=19 \times 97 + 1$ .

Para os leitores curiosos, na segunda parte do livro “Das calçadas aos ananases: investigar o mundo com um olhar matemático”, da editora Letras Lavadas, disponível para venda em letras-lavadas.pt, explicam-se os algoritmos que estão na base da criação de muitos números de identificação, como os códigos de barras, os números de identificação do Cartão de Cidadão e os números dos cartões VISA e MasterCard.

Sempre que lidamos com números de identificação, é possível que ocorram erros na leitura, na transmissão ou na escrita desses números. Contudo, podemos ficar descansados pois, na maioria das vezes, esses erros são detetados. E tudo isso graças à Matemática!