# Problema 2: Resolução

1. Fermat viu[1] que, pondo $m = (2k+1) \times d$, $2^{(2k+1)d} + 1$ é divisível por $2^d + 1$.
   De facto, se nestas duas expressões, substituir $2^d$ por $x$ obtém os polinómios:

   $$x^{2k+1} + 1 \quad \text{e} \quad x + 1$$

   Ora o primeiro é múltiplo do segundo, pois -1 é uma raiz comum, logo:

   $2^{(2k+1)d} + 1$ é múltiplo de $2^d + 1$.

   **NOTA** - *Se quiser obter o quociente dos dois números pode dividir o primeiro polinómio pelo segundo, recorrendo ao algoritmo habitual para a divisão de polinómios ou à Regra de Ruffini, obtendo:*

   $$x^{2k+1} + 1 = (x^{2k} - x^{2k-1} + \cdots + x^2 - x + 1)\,(x + 1)$$

   *Se substituir $x$ por $2^d$ no primeiro factor do segundo membro obtém o quociente:*

   $$2^{2kd} - 2^{(2k-1)d} + \cdots + 2^{2d} - 2^d + 1$$

2. Repare, caro leitor/a, que das igualdades:

   $$641 = 5 \times 2^7 + 1 \quad e \quad 641 = 5^4 + 2^4$$

   resulta, respetivamente:

   $$5 \times 2^7 \equiv -1 \; mod \; 641 \quad e \quad 2^4 \equiv -5^4 \; mod \; 641$$

   Euler notou que: $5 \times 2^7 \equiv -1 \; mod \; 641 \Rightarrow 5 \times 2^8 \equiv -2 \; mod \; 641$

   e ainda que, elevando ambos os membros à quarta potência[2], se obtém:

   $$5^4 \times 2^{32} \equiv 2^4 \; mod \; 641$$

   Como $2^4 \equiv -5^4 \; mod \; 641$ é $5^4 \times 2^{32} \equiv -5^4 \; mod \; 641$ pela propriedade transitiva e, dividindo ambos os membros por $5^4$ :

   $$2^{32} \equiv -1 \; mod \; 641 \quad \text{ou} \quad 2^{32} + 1 = 6\dot{4}1$$

---

[1] A verdade é que não estou certo que tenha sido este o raciocínio de Fermat…

[2] Resulta, imediatamente, da propriedade que designamos por (3) no artigo sobre **Critérios de Divisibilidade** que pode ver aqui.