On admettra le théorème de Fermat : si p est premier, pour tout a premier avec p, on a $a^{p-1} \equiv 1\ [p]$

Hypothèse :

Soit p et q deux nombres premiers distincts et tous deux différents de 2.

On pose $n = p\,q$ et e est un entier tel que $1 < e < (p-1)(q-1)$ et e est premier avec le nombre $(p-1)(q-1)$

Résultat 1 : Alors il existe un unique réel d tel que $1 \leq d < (p-1)(q-1)$ et $e\,d \equiv 1\ [(p-1)(q-1)]$

Résultat 2 : pour tout entier m, $m^{e\,d} \equiv m\ [n]$

On va démontrer ces deux résultats :

1. *a.* Justifier que l'équation E: $e\,x + (p-1)(q-1)\,y = 1$ admet des solutions.

b. Expliquer par quelle méthode on peut trouver une solution particulière $(x_0\,;\,y_0)$

c. Exprimer la forme des solutions de E en fonction de $(x_0\,;\,y_0)$

d. En déduire le résultat 1.

2 *a.* Si p divise m, montrer que $m^{e\,d} \equiv m\ [p]$

b. Si p ne divise pas m, justifier que $m^{p-1} \equiv m\ [p]$

c. En écrivant $e\,d$ sous une autre forme montrer que $m^{e\,d} \equiv m\ [p]$

3. En s'inspirant des questions 2 montrer que $m^{e\,d} \equiv m\ [q]$

4. En déduire que $m^{e\,d} - m$ est divisible par n ce qui prouve le résultat 2.

CORRECTION

1. *a.* e est premier avec le nombre $(p-1)(q-1)$ donc d'après le théorème de Bézout, il existe deux entiers relatifs x et y tels que $e\,x + (p-1)(q-1)\,y = 1$

b. e est premier avec le nombre $(p-1)(q-1)$ donc dans l'algorithme d'Euclide, le dernier reste non nul obtenu est 1
en remontant, on peut trouver une solution particulière $(x_0\,;\,y_0)$ de l'équation E: $e\,x + (p-1)(q-1)\,y = 1$.

c. $\begin{cases} e\,x + (p-1)(q-1)\,y = 1 \\ e\,x_0 + (p-1)(q-1)\,y_0 = 1 \end{cases}$ donc par différence terme à terme $e\,(x - x_0) + (p-1)(q-1)(y - y_0) = 0$
soit $e\,(x - x_0) = -(p-1)(q-1)(y - y_0)$
donc $(p-1)(q-1)$ divise $e\,(x - x_0)$
or e est premier avec le nombre $(p-1)(q-1)$ donc d'après le théorème de Gauss, $(p-1)(q-1)$ divise $x - x_0$
Il existe un entier relatif k tel que $x - x_0 = (p-1)(q-1)\,k$ soit $x = k\,(p-1)(q-1) + x_0$
en remplaçant dans $e\,(x - x_0) = -(p-1)(q-1)(y - y_0)$ alors $y - y_0 = -e\,k$ soit $y = -e\,k + y_0$

Vérification : si $x = k\,(p-1)(q-1) + x_0$ et $y = -e\,k + y_0$ dans $e\,x + (p-1)(q-1)\,y$
$e\,x + (p-1)(q-1)\,y$
$= e\,(k\,(p-1)(q-1) + x_0) + (p-1)(q-1)(-e\,k + y_0)$
$= e\,x_0 + (p-1)(q-1)\,y_0 = 1$
Les solutions de E: $e\,x + (p-1)(q-1)\,y = 1$ sont les couples $(k\,(p-1)(q-1) + x_0\,;\,-e\,k + y_0)$ avec k entier relatif.

d. si $e\,d \equiv 1\ [(p-1)(q-1)]$ alors il existe un entier relatif y tel que $e\,d = 1 + (p-1)(q-1)\,y$
soit $e\,d - (p-1)(q-1)\,y = 1$
soit $e\,d + (p-1)(q-1)(-y) = 1$
d'après le résultat précédent, il existe un entier relatif k tel que : $d = k\,(p-1)(q-1) + x_0$ et $-y = -e\,k + y_0$
On cherche d tel que $1 \leq d < (p-1)(q-1)$ soit on cherche k tel que $1 \leq k\,(p-1)(q-1) + x_0 < (p-1)(q-1)$
$1 - x_0 \leq k\,(p-1)(q-1) < (p-1)(q-1) - x_0$

$$\Leftrightarrow \frac{1-x_0}{(p-1)(q-1)} \leq k < 1 - \frac{x_0}{(p-1)(q-1)}$$

$$1 - \frac{x_0}{(p-1)(q-1)} - \frac{1-x_0}{(p-1)(q-1)} = 1 - \frac{1}{(p-1)(q-1)}$$

$$\text{donc } 0 \leq 1 - \frac{x_0}{(p-1)(q-1)} - \frac{1-x_0}{(p-1)(q-1)} < 1$$

donc il existe un seul entier k compris entre $\dfrac{1-x_0}{(p-1)(q-1)}$ et $1 - \dfrac{x_0}{(p-1)(q-1)}$
il existe un seul entier d tel que $1 \leq d < (p-1)(q-1)$ et $e\,d \equiv 1\ [(p-1)(q-1)]$ d'où le résultat 1.

2 *a.* Si p divise m alors $m \equiv 0\ [p]$ donc $m^{e\,d} \equiv 0\ [p]$ soit $m^{e\,d} \equiv m\ [p]$

b. Si p ne divise pas m, p étant un nombre premier, p est premier avec m donc, d'après le petit théorème de Fermat, on a : $m^{p-1} \equiv 1\ [p]$ soit $m^{p} \equiv m\ [p]$

c. e est premier avec le nombre $(p-1)(q-1)$ donc il existe un unique réel d tel que $\begin{cases} 1 \leq d < (p-1)(q-1) \\ e\,d \equiv 1\ [(p-1)\ (q-1)] \end{cases}$
soit il existe un entier relatif y tel que :

$$e\,d = 1 + (p-1)(q-1)\,y$$

donc $m^{e\,d} = m^{1+(p-1)(q-1)y} = m \times m^{(p-1)(q-1)y}$
$m^{e\,d} = m \times [m^{(p-1)}]^{(q-1)y}$ donc $m^{e\,d} \equiv m \times [m^{(p-1)}]^{(q-1)y}\ [p]$
or $m^{p-1} \equiv 1\ [p]$ donc $[m^{(p-1)}]^{(q-1)y} \equiv 1\ [p]$ donc $m^{e\,d} \equiv m\ [p]$

3. e est premier avec le nombre $(p-1)(q-1)$ donc il existe un unique réel d tel que $\begin{cases} 1 \leq d < (p-1)(q-1) \\ e\,d \equiv 1\ [(p-1)\ (q-1)] \end{cases}$
de plus pour tout entier m, $m^{q-1} \equiv 1\ [q]$ donc en procédant comme ci-dessus, $m^{e\,d} \equiv m\ [q]$

4. p et q divisent $m^{e\,d} - m$ et p et q deux nombres premiers distincts et tous deux différents de 2 donc sont premiers entre eux donc d'après un corollaire du théorème de Gauss, $p\,q$ divise $m^{e\,d} - m$
or $n = p\,q$ donc n divise $m^{e\,d} - m$.