1. Soit p un nombre premier et a un nombre entier, supérieur à 2, non divisible par p.
Considérons la suite (S) des multiples de a : a, 2 a, 3 a, ... $(p-1)\,a$.

a. Montrez que les nombres 1, 2, ... $p-1$ sont premiers avec p.

b. Soit k un entier tel que $1 \leq k \leq p-1$. Montrez par l'absurde, que le reste r_k de la division de $k\,a$ par p est non nul.
En utilisant les congruences, on peut alors écrire $k\,a \equiv r_k\ [p]$

c. Montrez que les restes obtenus sont deux à deux distincts.
Déduisez-en que l'ensemble R des restes possibles est {1 ; 2 ; 3 ; ... ; $p-1$ }; quel est leur produit ?

d. En choisissant $a = 8$ et $p = 5$, vérifiez les résultats ci-dessus.

2. *a.* En utilisant la compatibilité de la multiplication avec les congruences modulo p, montrez que: $(p-1)!\,a^{p-1} - (p-1)! \equiv 0\ [p]$

b. Déduisez-en que: $(p-1)!\,(a^{p-1}-1)$ est divisible par p.

c. Montrez que p et $(p-1)!$ sont premiers entre eux. Déduisez-en que p divise $a^{p-1}-1$.

Vous venez de démontrer le résultat suivant ou petit théorème de Fermat :
Si p est un nombre premier et a un entier non divisible par p alors $a^{p-1} - 1$ est divisible par p, soit encore $a^{p-1} - 1 \equiv 0\ [p]$.

d. Appliquez ce résultat lorsque : $p = 7$ et $a = 10$, $p = 11$ et $a = 6$

e. En prenant $p = 14$ et $a=4$ prouvez que la réciproque de petit théorème de Fermat est fausse.

3. p est toujours un nombre premier.

a. Montrez que si a n'est pas divisible par p le produit $a\,(a^{p-1}-1)$ est divisible par p.

b. Montrez que si a est divisible par p le produit $a\,(a^{p-1}-1)$ est encore divisible par p.

c. Concluez que : Si p est nombre premier et a un entier quelconque alors $a^p - a$ est divisible par p.

d. Appliquez ce résultat lorsque $p = 7$ et $a = 10$; $p = 5$ et $a = 15$.

4. Application: Les nombres p et q sont deux nombres premiers, a est un nombre entier naturel qui n'est divisible ni par p, ni par q.
On désigne par n le produit $p\,q$.

a. Démontrez que $a^{q-1} \equiv 1\ [p]$

b. Démontrez que $(a^{p-1})^{q-1} \equiv 1\ [q]$
Déduisez en que $a^{(p-1)(q-1)} \equiv 1[n]$

CORRECTION

1. *a.* p est un nombre premier donc il n'est divisible dans $\mathbb{N}$ que par 1 et lui-même donc il est premier avec tous les nombres qui lui sont inférieurs. Les nombres 1, 2, ... $p-1$ sont premiers avec p.

b. Supposons que le reste de la division de $k\,a$ par p est nul alors p divise $k\,a$ or a n'est pas divisible par p donc est premier avec p donc d'après le théorème de Gauss, p divise k. D'après la question précédente, les nombres 1, 2, ... $p-1$ sont premiers avec p donc p est premier avec k. L'hypothèse est donc fausse, le reste r_k de la division de $k\,a$ par p est non nul.

c. Supposons qu'il existe deux entiers k et k' tels que $1 \leq k' \leq k \leq p-1$ et $k\,a \equiv r\ [p]$ et $k'\,a \equiv r\ [p]$.
$(k-k')\,a \equiv 0\ [p]$ donc p étant premier avec a, p divise $k-k'$
$0 \leq k-k' \leq p-1$ or les nombres 1, 2, ... $p-1$ sont premiers avec p donc $k-k' = 0$. Les restes obtenus sont deux à deux distincts.
La suite (S) des multiples de a : a, 2 a, 3 a, ... $(p-1)\,a$ comporte $p-1$ termes dont les restes dans la division par p sont distincts et non nuls, donc il existe $p-1$ restes compris entre 1 et $p-1$.
Leur produit est $1 \times 2 \times 3 \times \ldots \times (p-1) = (p-1)!$

d. Si $a = 8$ et $p = 5$, k prend les valeurs : 1 ; 2 ; 3 ; 4

k	1	2	3	4
$k\,a$	8	16	24	32
r_k	3	1	4	2

2. *a.* En utilisant la compatibilité de la multiplication avec les congruences modulo p, montrez que: $(p-1)!\,a^{p-1} - (p-1)! \equiv 0\ [p]$

$$\begin{aligned} a &\equiv r_1 \quad [p] \\ 2\,a &\equiv r_2 \quad [p] \\ \ldots &\equiv \ldots \\ (p-1)\,a &\equiv r_{p-1} \quad [p] \end{aligned}$$

donc en multipliant terme à terme les congruences :
$1 \times 2 \times \ldots \times (p-1)\,a^{p-1} \equiv r_1 \times r_2 \times \ldots r_{p-1}\ [p]$
Le produit des restes est $1 \times 2 \times 3 \times \ldots \times (p-1) = (p-1)!$ donc $(p-1)!\,a^{p-1} - (p-1)! \equiv 0\ [p]$

b. $(p-1)!\,a^{p-1} - (p-1)! \equiv 0\ [p]$ donc en factorisant : $(p-1)!\,(a^{p-1}-1) \equiv 0\ [p]$ donc $(p-1)!\,(a^{p-1}-1)$ est divisible par p.

c. p est premier avec les nombres entiers compris entre 1 et $p-1$ donc avec leur produit donc p et $(p-1)!$ sont premiers entre eux.
p et $(p-1)!$ sont premiers entre eux et $(p-1)!\,(a^{p-1}-1)$ est divisible par p donc d'après le théorème de Gauss, p divise $a^{p-1}-1$.

d. **$p = 7$ et $a = 10$,**

k	1	2	3	4	5	6
a^k est congru modulo 7 à	3	2	6	4	5	1

$p = 11$ et $a = 6$

k	1	2	3	4	5	6	7	8	9	10
a^k est congru modulo 11 à	6	3	7	9	10	5	8	4	2	1

e. **$p = 14$ et $a = 4$**

k	1	2	3	4	5	6	7	8	9	10	11	12	13
a^k est congru modulo 14 à	4	2	8	4	2	8	4	2	8	4	2	8	4

$a^{p-1} \equiv 4$ [p] mais a et p ne sont pas premiers entre eux donc la réciproque de petit théorème de Fermat est fausse.

3. *a.* Si a n'est pas divisible par p, d'après les questions précédentes, p divise $a^{p-1} - 1$ donc le produit $a\,(a^{p-1} - 1)$ est divisible par p.

b. si a est divisible par p, p divise l'un des termes du produit $a\,(a^{p-1} - 1)$ donc p divise le produit $a\,(a^{p-1} - 1)$.

c. Dans tous les cas (a divisible par p ou a non divisible par p), si p est nombre premier et a un entier quelconque alors $a\,(a^{p-1} - 1)$ est divisible par p donc en développant ; $a^p - a$ est divisible par p.

d. **$p = 7$ et $a = 10$;**

k	1	2	3	4	5	6	7
a^k est congru modulo 7 à	3	2	6	4	5	1	3
$a^k - a$	2	0	0	0	0	0	0

$p = 5$ et $a = 15$,
5 divise 15 donc 5 divise 15^5 donc 5 divise $15^5 - 15$

4. Application :
a. p est un nombre premier et a un entier non divisible par p alors $a^{p-1} - 1$ est divisible par p, soit encore $a^{p-1} - 1 \equiv 0$ [p].
(petit théorème de Fermat appliqué à p et a)

b. q est un nombre premier et a un entier non divisible par q alors a^{p-1} n'est pas divisible par q, donc $(a^{p-1})^{q-1} \equiv 1$ [q]
(petit théorème de Fermat appliqué à q et a^{p-1})

$a^{p-1} - 1 \equiv 0$ [p] donc $a^{(p-1)(q-1)} \equiv 1$ [p]
p et q sont deux nombres premiers distincts qui divisent tous deux $a^{(p-1)(q-1)} - 1$ donc leur produit divise $a^{(p-1)(q-1)} - 1$ donc $a^{(p-1)(q-1)} \equiv 1$ [n].