Exercice E6

Première Partie

1. On a :
   $4^2-1=15=3\times 5$; $3^6-1=728=7\times 104$; $6^4-1=1295=5\times 259$; $2^{10}-1=1023=11\times 93$
   Donc : $\boxed{3 \text{ divise } 4^2-1 \quad ; \quad 7 \text{ divise } 3^6-1 \quad ; \quad 5 \text{ divise } 6^4-1 \quad ; \quad 11 \text{ divise } 2^{10}-1}$.

2. On a :
   $2^5-1=31$; $9^2-1=80$; $2^9-1=511$
   6 ne divise pas 31 ; 3 ne divise pas 80 ; 10 ne divise pas 511
   donc : $\boxed{6 \text{ ne divise pas } 2^5-1 \quad ; \quad 3 \text{ ne divise pas } 9^2-1 \quad ; \quad 10 \text{ ne divise pas } 2^9-1}$.
   - On ne peut pas appliquer le petit théorème de Fermat avec $p=6$ puisque p doit être un nombre premier, on ne peut donc pas en déduire que 6 divise 2^5-1 .
   - On ne peut pas appliquer le petit théorème de Fermat avec $p=3$ et $a=9$ puisque a ne doit pas être un multiple de p, on ne peut donc pas en déduire que 3 divise 9^2-1 .
   - On ne peut pas appliquer le petit théorème de Fermat avec $p=10$ puisque p doit être un nombre premier, on ne peut donc pas en déduire que 10 divise 2^9-1 .

3. Le petit théorème de Fermat ne peut pas s'appliquer avec $p=4$ et $a=5$ puisque p doit être un nombre premier.
   Dans ce cas particulier on a : $a^{p-1}-1=5^3-1=124$ donc 4 divise 5^3-1.
   On peut en déduire que :
   $\boxed{\text{« } p \text{ premier » est une condition suffisante mais non nécessaire pour que } a^{p-1}-1 \text{ soit divisible par } p}$.

Deuxième Partie

1. r_1 est le reste de la division euclidienne de 8 par 5, donc $r_1=3$.
   r_2 est le reste de la division euclidienne de 16 par 5, donc $r_2=1$.
   r_3 est le reste de la division euclidienne de 24 par 5, donc $r_3=4$.
   r_4 est le reste de la division euclidienne de 32 par 5, donc $r_4=2$.
   On a donc $\{r_1;r_2;r_3;r_4\}=\{3;1;4;2\}$, donc $\boxed{\{r_1;r_2;r_3;r_4\}=E}$.

2. On a : $8\equiv 3$; $16\equiv 1$; $24\equiv 4$; $32\equiv 2$ modulo (5).
   Donc : $8\times 16\times 24\times 32\equiv 3\times 1\times 4\times 2 \quad (5)$.
   c'est-à-dire : $\boxed{8\times 16\times 24\times 32\equiv 1\times 2\times 3\times 4 \quad (5)}$.
   On en déduit que : $8\times 1\times 8\times 2\times 8\times 3\times 8\times 4\equiv 1\times 2\times 3\times 4 \quad (5)$.
   c'est-à-dire : $8^4(1\times 2\times 3\times 4)\equiv(1\times 2\times 3\times 4) \quad (5)$
   donc : $8^4(1\times 2\times 3\times 4)-(1\times 2\times 3\times 4)\equiv 0 \quad (5)$
   c'est-à-dire : $\boxed{\left(8^4-1\right)(1\times 2\times 3\times 4)\equiv 0 \quad (5)}$.

3. D'après la question précédente 5 divise $\left(8^4-1\right)(1\times 2\times 3\times 4)$.
   5 étant un nombre premier, il est premier avec 1, 2, 3 et 4.
   Le théorème de Gauss permet d'en déduire que : $\boxed{5 \text{ divise } 8^4-1}$.

Troisième Partie

p est un nombre premier et a un entier naturel non multiple de p.
$E = \{1; 2; ....; p-1\}$.

1. Soit k un élément de E, et r_k le reste de la division euclidienne de ka par p.
   On a : $0 < k < p$, donc p ne divise pas k.
   D'autre part on sait que a n'est pas un multiple de p, donc p ne divise a.
   Sachant que p est un nombre premier, on en déduit que p ne divise pas ka.
   On a donc : $\boxed{r_k \neq 0 \text{ pour tout } k \text{ élément de } E}$.

2. Soient k et k' deux éléments de E tels que $r_k = r_{k'}$.
   Par définition de r_k et de $r_{k'}$, on a : $ka \equiv r_k \quad (p)$ et $k'a \equiv r_{k'} \quad (p)$
   donc : $ka - k'a \equiv r_k - r_{k'} \quad (p)$ donc $(k-k')a \equiv 0 \quad (p)$.
   On en déduit que : $\boxed{(k-k')a \text{ est divisible par } p}$.
   p est un nombre premier qui ne divise pas a, donc p est premier avec a.
   Sachant que p divise $(k-k')a$, le théorème de Gauss permet de conclure que p divise $k-k'$.
   Or on sait que : $0 < k < p$ et $0 < k' < p$, donc $-p < -k' < 0$, donc $-p < k - k' < p$.
   Le seul multiple de p strictement compris entre $-p$ et p est 0.
   Donc $k - k' = 0$, c'est-à-dire $\boxed{k = k'}$.

3. E est un ensemble ayant $(p-1)$ éléments et F est l'ensemble des restes r_k lorsque k décrit E.
   D'après la question précédente, à deux éléments distincts k et k' de E correspondent des restes r_k et $r_{k'}$ distincts.
   On en déduit qu'il y a autant de reste r_k que d'éléments dans E.
   Donc : $\boxed{F \text{ est un ensemble ayant } (p-1) \text{ éléments}}$.

   r_k étant le reste de la division euclidienne de ka par p, on sait que : $0 \leqslant r_k < p$.
   On a vu que $r_k \neq 0$ pour tout k élément de E, donc $1 \leqslant r_k \leqslant p-1$ pour tout k élément de E.
   Donc $r_k \in E$ pour tout k élément de E.
   On en déduit que F est une partie de E, et comme E et F ont le même nombre d'éléments $(p-1)$, on a : $\boxed{F = E}$.

4. On sait que pour tout k élément de E, on a : $ka \equiv r_k \quad (p)$.
   Donc : $a \times 2a \times ... \times (p-1)a \equiv r_1 \times r_2 \times ... \times r_{p-1} \quad (p)$.
   Comme l'ensemble F est égal à l'ensemble E, on a $r_1 \times r_2 \times ... \times r_{p-1} = 1 \times 2 \times ... \times (p-1)$.
   Donc : $a \times 2a \times ... \times (p-1)a \equiv 1 \times 2 \times ... \times (p-1) \quad (p)$,
   c'est-à-dire $(1 \times a) \times (2 \times a) \times (3 \times a) ... \times ((p-1) \times a) \equiv 1 \times 2 \times ... \times (p-1) \quad (p)$
   Soit : $a^{p-1} \times 1 \times 2 \times 3 ... \times (p-1) \equiv 1 \times 2 \times 3 ... \times (p-1) \quad (p)$
   donc : $a^{p-1} \times 1 \times 2 \times 3 ... \times (p-1) - 1 \times 2 \times 3 ... \times (p-1) \equiv 0 \quad (p)$
   donc : $\boxed{\left(a^{p-1} - 1\right) \times 1 \times 2 \times 3 ... \times (p-1) \equiv 0 \quad (p)}$.

5. On déduit de la question précédente que p divise $\left(a^{p-1} - 1\right) \times 1 \times 2 \times 3 ... \times (p-1)$.
   p étant un nombre premier, il est premier avec tous les nombres qui ne sont pas ses multiples, donc p est premier avec $1\,;\, 2\,;\, 3\,;\, ...\,;\, (p-1)$.
   Le théorème de Gauss permet alors d'en déduire que : $\boxed{p \text{ divise } a^{p-1} - 1}$.

Quatrième Partie

Soit a un entier naturel et p un nombre premier.
On peut écrire : $a^p - a = a\left(a^{p-1} - 1\right)$

- Si p ne divise pas a, on sait d'après le petit théorème de Fermat démontré précédemment que p divise $a^{p-1} - 1$, donc p divise $a\left(a^{p-1} - 1\right)$, donc p divise $a^p - a$.
- Si p divise a, alors p divise $a\left(a^{p-1} - 1\right)$, donc p divise $a^p - a$.

On en déduit que : $\boxed{\text{pour tout entier naturel } a \text{ et pour tout nombre premier } p, \text{ le nombre } a^p - a \text{ est divisible par } p}$.