Sur le théorème de Fermat

Pour tout entier naturel n, la factorielle de n est l'entier $n!$ défini par $0! = 1$ et $n! = n\cdot(n-1)\cdot\cdots\cdot 1$ pour $n > 1$.

Soient n un entier naturel et a, b deux entiers relatifs.

On dit que a est congru à b modulo n si, et seulement si, n divise $b - a$, ce qui se note :

$$a \equiv b \ \ (n)$$

On rappelle le théorème de division euclidienne.

Soit $(a, b) \in \mathbb{Z} \times \mathbb{N}^*$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que :

$$\begin{cases} a = bq + r \\ 0 \leq r < b \end{cases}$$

On dit qu'un entier naturel p est premier s'il est supérieur ou égal à 2 et si les seuls diviseurs positifs de p sont 1 et p.

On rappelle le théorème de Gauss.

Soient a, b, c des entiers relatifs non nuls. Si a divise bc et a est premier avec b alors a divise c.

On rappelle le lemme d'Euclide.

Soit p un nombre premier et r un entier naturel supérieur ou égal à 2. Si p divise le produit $n_1 n_2 \cdots n_r$ de r entiers naturels non nuls, alors p divise l'un des n_k.

1. **Une démonstration du théorème de Fermat.**
   Soit $p \geq 2$ un nombre premier.
   (a) Soit a un entier relatif premier avec p.
   Pour tout entier k compris entre 1 et $p - 1$, on note r_k le reste dans la division euclidienne de ka par p.
   Montrer que les r_k sont deux à deux distincts et compris entre 1 et $p - 1$.
   (b) En utilisant les notations de la question précédente, montrer que pour tout entier relatif a premier avec p, on a :
   $$(p-1)!\ a^{p-1} \equiv r_1 r_2 \cdots r_{p-1} \ \ (p)$$
   (c) En déduire que, pour tout entier relatif a premier avec p, on a :
   $$a^{p-1} \equiv 1 \ \ (p)$$
   (théorème de Fermat).

2. Soit $n \geq 2$ un entier. Montrer que les assertions suivantes sont équivalentes :
   (i) pour tout entier relatif a premier avec n, on a : $a^{n-1} \equiv 1 \ \ (n)$
   (ii) pour tout entier relatif a, on a : $a^n \equiv a \ \ (n)$

3.
   (a) Calculer le reste dans la division euclidienne de 3045^{2018} par 13.
   (b) Calculer le reste dans la division euclidienne de 3044^{2018} par 13.

4. De manière plus générale, comment simplifier le calcul du reste dans la division euclidienne par un nombre premier p d'un entier de la forme a^b, où a, b sont des entiers naturels plus grands que p.

5. **Un test de non primalité.**
   Comment utiliser le théorème de Fermat comme test de non primalité d'un entier $n \geq 3$?

6. Soit $n \geq 2$ un entier tel que $a^{n-1} \equiv 1 \ (n)$ pour tout entier a compris entre 2 et $n-1$.
   En utilisant le théorème de Bézout, montrer que n est premier.

   Définition : On appelle nombre de Carmichaël tout entier $n \geq 3$ non premier tel que pour tout entier relatif a premier avec n, on a $a^{n-1} \equiv 1 \ (n)$ (propriété de Fermat).

7. Montrer qu'un nombre de Carmichaël est impair.
8. 561 **est un nombre de Carmichaël.**
   (a) Donner la décomposition en facteurs premiers de l'entier $n = 561$ (sans utiliser de calculatrice, bien sûr).
   (b) Vérifier que 560 est divisible par 2, par 10 et par 16.

   Soit $a \in \mathbb{Z}$ premier avec 561.

   (c) Montrer que a est premier avec chaque entier $p_1 = 3$, $p_2 = 11$ et $p_3 = 17$.
   (d) Montrer que, pour $k = 1, 2, 3$, p_k divise $a^{p_k - 1} - 1$.
   (e) Montrer que, pour $k = 1, 2, 3$, p_k divise $a^{560} - 1$.
   (f) En déduire que 561 divise $a^{560} - 1$ et conclure.
9. Soit $n \geq 3$ un entier pour lequel, il existe un entier $r \geq 2$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$.
   (a) Dans cette question nous allons démontrer que nécessairement $r \geq 3$.
       On suppose que $r = 2$, c'est-à-dire que $n = p_1 p_2$ avec $p_1 < p_2$ premiers tels que $p_1 - 1$ et $p_2 - 1$ divisent $n - 1$.
       En effectuant la division euclidienne de $n-1$ par p_2-1 de deux manière différentes, montrer que l'on aboutit à une contradiction et conclure.
   (b) Montrer que n un nombre de Carmichaël.
   (c) Vérifier que 1105 et 41041 sont des nombres de Carmichaël.
10. Soit $a \in \mathbb{N}^*$ tel que les entiers $p_1 = 6a + 1$, $p_2 = 12a + 1$ et $p_3 = 18a + 1$ soient premiers.
    Montrer que $n = p_1 p_2 p_3 = p_1 (2p_1 - 1)(3p_1 - 2)$ est un nombre de Carmichaël.
    Donner des exemples.
    On peut montrer le résultat suivant, ce qui est plus difficile.

Théorème 1 (Korselt) *Soit $n \geq 3$ un entier. Les propriétés suivantes sont équivalentes :*

1. *il existe un entier $r \geq 3$ et des nombres premiers $3 \leq p_1 < \cdots < p_r$ tels que $n = \prod_{j=1}^{r} p_j$ et, pour tout indice j compris entre 1 et r, $p_j - 1$ divise $n - 1$;*
2. *n est non premier et :*
$$\forall a \in \mathbb{Z},\ a^n \equiv a \ (n)$$
3. *n est un nombre de Carmichaël.*