Sur le théorème de Fermat

1. (a) Pour k compris entre 1 et $p-1$, le théorème de division euclidienne nous dit qu'il existe un unique couple d'entiers (q_k, r_k) tel que :

$$\begin{cases} ka = q_k p + r_k \\ 0 \leq r_k \leq p-1 \end{cases}$$

Le reste r_k est nul si, et seulement si, le nombre premier p divise ka, ce qui implique qu'il divise k ou a, ce qui est impossible pour $1 \leq k \leq p-1$ et a premier avec p.
On a donc $1 \leq r_k \leq p-1$.
Si $1 \leq j < k \leq p-1$ sont tels que $r_k = r_j$, on a alors $(k-j)\,a = (q_k - q_j)\,p$ et p divise $(k-j)\,a$ en étant premier avec $k-j$ et a, ce qui est impossible.
On a donc $r_k \neq r_j$ pour $1 \leq j \neq k \leq p-1$.

(b) Pour k compris entre 1 et $p-1$, on a $ka \equiv r_k \ (p)$, donc :

$$(p-1)!a^{p-1} = (a)\,(2a)\cdots((p-1)\,a) \equiv r_1, r_2, \cdots, r_{p-1} \ (p)$$

(c) Comme les r_k sont deux à deux distincts dans $\{1, 2, \cdots, p-1\}$, on a $r_1 r_2 \cdots r_{p-1} = (p-1)!$ et l'identité précédente s'écrit $(p-1)!a^{p-1} \equiv (p-1)! \ (p)$, ce qui revient à dire que p divise $(p-1)!\,(a^{p-1}-1)$.
Le nombre premier p étant premier avec $(p-1)!$ (dans le cas contraire p divise le produit $(p-1)!$ donc l'un des termes du produit, ce qui n'est pas possible), le théorème de Gauss nous dit qu'il divise $a^{p-1}-1$, ce qui revient à dire que $a^{p-1} \equiv 1 \ (p)$.

2. Multipliant par a, on a aussi $a^n \equiv a \ (n)$, identité qui est aussi valable pour a multiple de n. Réciproque par Gauss.

3. (a) $3\,045 \equiv 3 \pmod{13} \Rightarrow 3\,045^{2\,018} \equiv 3^{2\,018} \pmod{13}$
3 est premier avec 13, d'après le théorème de Fermat $3^{12} \equiv 1 \pmod{13}$.
On a alors $3^{12\times 168+2} \equiv 3^3 \pmod{13} \Rightarrow 3^{2\,018} \equiv 1 \pmod{13}$ et finalement $3\,045^{2\,018} \equiv 1 \pmod{13}$.

(b) En utilisant le même raisonnement, on montre que $3\,044^{2\,018} \equiv 4 \pmod{13}$.

4. Si p divise a, il divise aussi a^b et le reste cherché est nul.
On suppose donc que p ne divise pas a.
En vue de diminuer a, on effectue la division euclidienne de a par p, soit $a = q'p + s$ avec $1 \leq s \leq p-1$ et on a $a^b \equiv s^b \ (p)$.
Ensuite, en vue de diminuer b, on effectue la division euclidienne de b par $p-1$, soit $b = q\,(p-1) + r$ avec $0 \leq r \leq p-2$ et on a $a^b = (a^{p-1})^q\,a^r$ avec $a^{p-1} \equiv 1 \ (p)$ puisque p ne divise pas a, ce qui donne :

$$\begin{aligned} a^b &\equiv a^r \ (p) \\ &\equiv s^r \ (p) \end{aligned}$$

Le reste cherché est donc celui de la division de s^r par p avec $1 \leq s \leq p-1$ et $0 \leq r \leq p-2$. Voir les exemples précédents.

5. En calculant 2^{n-1} modulo n, si on trouve un reste différent de 1, l'entier n n'est pas premier. Si on trouve 1, on recommence avec 3 et ainsi de suite.

6. Pour $2 \leq a \leq n-1$, il existe un entier q tel que $a^{n-1} - qn = 1$, ce qui signifie que a est premier avec n (Bézout) et en conséquence, n est premier.

7. Soit n un nombre de Carmichaël.
Si n est pair, alors $n-1$ est impair et $(-1)^{n-1} = -1$ n'est pas congru à 1 modulo n (on a $n \geq 3$), donc n n'est pas un nombre de Carmichaël.

8. (a) On a la décomposition en facteurs premiers $561 = 3 \cdot 11 \cdot 17 = \prod_{k=1}^{3} p_k$ (critères de divisibilité par 3 et par 11).

   (b) $560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$.
   Soit $a \in \mathbb{Z}$ premier avec 561.

   (c) Si l'un des p_k divise a, il divise aussi $\operatorname{pgcd}(a, n)$ et a n'est pas premier avec n.

   (d) Dire que $a \in \mathbb{Z}$ est premier avec 561 équivaut à dire qu'il est premier avec chaque p_k et le théorème de Fermat nous dit que $a^{p_k - 1} \equiv 1 \bmod (p_k)$.

   (e) En remarquant que 560 est divisible par chaque $p_k - 1$ ($560 = 2 \cdot 280 = 10 \cdot 56 = 16 \cdot 35$), on en déduit que $a^{560} \equiv 1 \bmod (p_k)$ pour $k = 1, 2, 3$, ce qui équivaut à dire que $a^{560} - 1$ est multiple de chaque p_k.

   (f) En conséquence $a^{560} - 1$ est multiple du produit $n = \prod_{k=1}^{3} p_k$ puisque les p_k sont premiers deux à deux distincts, ce qui équivaut à $a^{560} \equiv 1 \ (561)$.
   Conclusion, 561 est de Carmichaël.

9. (a) En écrivant que $n - 1 = (p_1 - 1) + p_1 (p_2 - 1)$, on déduit que $n - 1$ ne peut être divisible par $p_2 - 1$, en effet si $p_2 - 1$ divise $n - 1$ il divise $p_1 - 1$ avec $p_1 < p_2$, ce qui est impossible.
   On peut aussi dire qu'on a une autre division euclidienne $n - 1 = q (p_2 - 1)$ qui donne $p_1 - 1 = 0$.
   En conséquence un nombre de Carmichaël a au moins trois facteurs premiers.

   (b) Même démonstration que pour 561.
   Soit $n = \prod_{j=1}^{r} p_j$, où $r \geq 3$, $3 \leq p_1 < \cdots < p_r$ sont premiers tels que chaque $p_j - 1$, pour j compris entre 1 et r, divise $n - 1$.
   Un tel entier, produit d'au moins trois nombres premiers est non premier.
   Dire que $a \in \mathbb{Z}$ est premier avec n équivaut à dire qu'il est premier avec chaque p_k, pour k compris entre 1 et r, et le théorème de Fermat nous dit que $a^{p_k - 1} \equiv 1 \bmod (p_k)$.
   Comme $n - 1$ est divisible par chaque $p_k - 1$, on a aussi $a^{n-1} = a^{q_k (p_k - 1)} = (a^{p_k - 1})^{q_k} \equiv 1 \bmod (p_k)$ pour k compris entre 1 et r, ce qui signifie que $a^{n-1} - 1$ est multiple de tous les p_k, donc de $n = \prod_{j=1}^{r} p_j$ puisque les p_k sont premiers deux à deux distincts, ce qui signifie que $a^{n-1} \equiv 1 \ (n)$. [1]

   (c) $n = 1105 = 5 \cdot 13 \cdot 17$ [2] ; $n = 41041 = 7 \cdot 11 \cdot 13 \cdot 41$. [3]

10. L'entier n est non premier et on a $n \equiv 1 \pmod{6a}$, $n \equiv (6a+1)^2 \equiv 1 \pmod{12a}$, $n \equiv (6a+1)(12a+1) \equiv 1 \pmod{18a}$, ce qui signifie que $p_k - 1$ divise $n - 1$ pour $k = 1, 2, 3$. Donc n est de Carmichaël.
    Pour $a = 1$, on obtient $n = 7 \cdot 13 \cdot 19 = 1729$.
    Pour $a = 6$, on obtient $n = 37 \cdot 73 \cdot 109 = 294\,409$.
    Pour $a = 35$, on obtient $n = 211 \cdot 421 \cdot 631 = 56\,052\,361$. [4]
    On admet le résultat suivant. [5]

---

1. Cela se déduit aussi immédiatement du théorème chinois qui dit que $\mathbb{Z}_n^{\times} \xrightarrow{\sim} \prod_{j=1}^{r} (\mathbb{Z}_{p_j})^{\times}$ et du théorème de Fermat
2. Il est somme de deux carrés puisque chaque facteur premier est somme de deux carrés.
3. En 1994, Alford, Granville et Pomerance ont montré qu'il existe une infinité de nombres de Carmichaël.
4. On ne sait s'il existe une infinité de triplets de nombres premiers de la forme $(p_1, 2p_1 - 1, 3p_1 - 2)$
5. On utilise le fait que $\mathbb{F}_p^*$ est cyclique.

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 :*
$$\forall x \in \mathbb{Z}_n,\ x^n = x$$
3. *n est un nombre de Carmichaël.*