DM 4

Partie A. Quelques exemples

1. $4 \equiv 1 \mod 3$, donc $4^n \equiv 1^n \mod 3$ et finalement $4^n \equiv 1 \mod 3$.

2. 4 est premier avec 29 (29 est premier). Donc d'après le petit théorème de Fermat $4^{29-1} - 1 \equiv 0 \mod 29$ ou encore $4^{28} - 1$ est divisible par 29.

3. $4 = 0 \times 17 + 4$;

   $4^2 = 0 \times 17 + 16$;

   $4^3 = 3 \times 17 + 13$;

   $4^4 = 15 \times 17 + 1$.

   La dernière égalité montre que $4^4 \equiv 1 \mod 17$, d'où $(4^4)^k \equiv 1^k \mod 17$ soit $4^{4k} \equiv 1 \mod 17$ ou encore $4^{4k} - 1 \equiv 0 \mod 17$.

   Conclusion : $4^{4k} - 1$ est divisible par 17.

4. On a $4^2 = 16 = 3 \times 5 + 1$ ou $4^2 \equiv 1 \mod 5$ d'où il résulte que $4^{2k} \equiv 1 \mod 5$ ou encore $4^{2k} - 1 \equiv 0 \mod 5$.

   Conclusion : $4^n - 1$ est divisible par 5 si n est pair.

   Par contre : de $4 \equiv 4 \mod 5$ et $4^{2k} \equiv 1 \mod 5$ il résulte par produit que

   $4^{2k+1} \equiv 4 \mod 5$.

   Conclusion : $4^n - 1$ est divisible par 5 si et seulement si n est pair.

5. Diviseurs premiers de $4^{28} - 1$: la question 2 a déjà donné le nombre 29 ; la question 3 a donné le diviseur premier 17 ; la question 4 a donné le diviseur 5.

   D'autre part, $4 \equiv 1 \mod 3$ entraîne $4^n \equiv 1 \mod 3$ ou encore $4^n - 1$ est divisible par 3 qui est premier. Il y a également 5, 43 ...

Partie B. Divisibilité par un nombre premier

1. $4 = 2^2$; si p est premier différent de 2, il est premier avec 4, donc d'après le petit théorème de Fermat $4^{p-1} - 1 \equiv 0 \mod p$ ou $4^{p-1} \equiv 1 \mod p$. Le premier premier différent de 2 est 3, donc $n = p - 1 \geqslant 1$.

2. (a) On a donc : $4^n \equiv 1 \mod p$, $4^b \equiv 1 \mod p$ et il existe un unique couple de naturels $(q\ ;\ r)$ tel que $n = bq + r$ avec $r < b$. On a donc $4^n = 4^{bq+r} = 4^{bq} \times 4^r = \left(4^b\right)^q \times 4^r$.

   On déduit de la seconde congruence que $\left(4^b\right)^q \equiv 1^q \mod p \equiv 1 \mod p$.

   Donc $\left(4^b\right)^q \times 4^r \equiv 4^r \mod p$ et donc que $4^n \equiv 4^r \mod p$.

   Finalement comme $4^n \equiv 1 \mod p$, $4^r \equiv 1 \mod p$.

   (b) On vient de démontrer dans la question précédente que si $4^n \equiv 1 \mod p$, alors n est multiple de b, b étant le plus naturel positif tel que $4^b \equiv 1 \mod p$.

   Inversement si $n = kb$, de $4^b \equiv 1 \mod p$, on déduit que $\left(4^b\right)^k \equiv 1^k \mod p$ soit $4^n \equiv 1 \mod p$. L'équivalence est donc démontrée.

(c) D'après la question B. 1 $4^{p-1} \equiv 1 \mod p$ et soit b le plus petit entier tel que $4^b \equiv 1 \mod p$. D'après la question 2. b. il en résulte que $p-1$ est multiple de b ou encore b (non nul) divise $p-1$.