Centres étrangers juin 2006

Le but de l'exercice est d'étudier certaines propriétés de divisibilité de l'entier $4^n - 1$, lorsque n est un entier naturel.
On rappelle la propriété connue sous le nom de petit théorème de Fermat : « si p est un nombre entier et a un entier naturel premier avec p, alors $a^{p-1} - 1 \equiv 0 \bmod p$ ».

Partie A. Quelques exemples.

1. Démontrer que, pour tout entier naturel n, 4^n est congru à 1 modulo 3.

2. Prouver à l'aide du petit théorème de Fermat, que $4^{28} - 1$ est divisible par 29.

3. Pour $1 \leq n \leq 4$, déterminer le reste de la division de 4^n par 17. En déduire que, pour tout entier k, le nombre $4^{4k} - 1$ est divisible par 17.

4. Pour quels entiers naturels n le nombre $4^n - 1$ est-il divisible par 5 ?

5. À l'aide des questions précédentes, déterminer quatre diviseurs premiers de $4^{28} - 1$.

Partie B. Divisibilité par un nombre premier

Soit p un nombre premier différent de 2.

1. Démontrer qu'il existe un entier $n > 1$ tel que $4^n \equiv 1$ [p].

2. Soit $n > 1$ un entier naturel tel que $4^n \equiv 1$ [p]. On note b le plus petit entier strictement positif tel que $4^b \equiv 1$ [p] et r le reste de la division euclidienne de n par b.

a. Démontrer que $4^r \equiv 1$ [p]. En déduire que $r = 0$.

b. Prouver L'équivalence : $4^n - 1$ est divisible par p si et seulement si n est multiple de b.

c. En déduire que b divise $p - 1$.

CORRECTION

Partie A.

1. $4 \equiv 1 \bmod 3$, donc $4^n \equiv 1^n \bmod 3$ donc $4^n \equiv 1 \bmod 3$.

2. 29 est un nombre premier donc 4 est premier avec 29 Donc d'après le petit théorème de Fermat $4^{29-1} - 1 \equiv 0 \bmod 29$
soit $4^{28} - 1$ est divisible par 28.

3. $4 = 0 \times 17 + 4$; $4^2 = 16 = 17 - 1$ donc $4^2 \equiv -1$ (17)
donc $(4^2)^2 \equiv (-1)^2 \bmod 17$ soit $4^4 \equiv 1 \bmod 17$ donc $4^{4k} \equiv 1 \bmod 17$ ou encore $4^{4k} - 1 \equiv 0 \bmod 17$.
$4^{4k} - 1$ est divisible par 17.

4. $4^2 = 16 = 3 \times 5 + 1$ donc $4^2 \equiv 1 \bmod 5$ donc $4^{2k} \equiv 1 \bmod 5$ soit $4^{2k} - 1 \equiv 0 \bmod 5$.
$4^n - 1$ est divisible par 5 si n est pair.
Si n est impair, il existe un entier relatif k tel que $n = 2k + 1$
$4^{2k} \equiv 1 \bmod 5$ donc $4^{2k} \times 4 \equiv 4 \bmod 5$ soit $4^{2k+1} \equiv 4 \bmod 5$
$4^n - 1$ est divisible par 5 si et seulement si n est pair.

5. D'après la question 2. 29 divise $4^{28} - 1$
D'après la question 3, 17 divise $4^{4k} - 1$ donc pour $k = 7$, 17 divise $4^{28} - 1$;
D'après la question 4, 5 divise $4^{2n} - 1$ donc pour $k = 14$, 5 divise $4^{28} - 1$;
D'autre part, $4 \equiv 1 \bmod 3$ donc $4^n \equiv 1 \bmod 3$ en particulier, $4^{28} - 1$ est divisible par 3 qui est premier.

Partie B.

1. si p est un nombre premier différent de 2, il est premier avec 4, donc d'après le petit théorème de Fermat $4^{p-1} - 1 \equiv 0 \bmod p$
ou $4^{p-1} \equiv 1 \bmod p$.
p est un nombre premier différent de 2, donc $p \geq 3$ donc $p - 1 > 1$.

2. *a.* Il existe deux entiers r et q tels que : $n = bq + r$ avec $0 \leq r < b$.
$4^b \equiv 1 \bmod p$ et $4^n \equiv 1 \bmod p$, donc $4^{bq+r} \equiv 1 \bmod p$ soit $(a^b)^q \times a^r \equiv 1 \bmod p$ donc $a^r \equiv 1 \bmod p$.
b est le plus petit naturel vérifiant $4^b \equiv 1 \bmod p$, donc $r = 0$.

b. D'après la question précédente que si $4^n \equiv 1 \bmod p$, alors n est multiple de b, b étant le plus naturel positif tel que $4^b \equiv 1 \bmod p$.
Réciproquement si $n = kb$, puisque $4^b \equiv 1 \bmod p$, alors $(a^b)^q \equiv 1 \bmod p$ soit $4^n \equiv 1 \bmod p$.

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