

Chapitre 2 – Exercice guidé page 57

1. a. On peut faire quelques essais :

$$A(2) = 17, A(3) = 82, A(4) = 257, A(5) = 626.$$

Il semble que $A(n)$ soit pair quand n est impair et qu'il soit impair quand n est pair.

Démontrons-le (en admettant connaître la parité de n^2 selon la parité de n):

1^{er} cas : si n est pair, n^2 est pair donc $(n^2)^2 = n^4$ est pair et par suite, $A(n)$ est impair

2^e cas : si n est impair, n^2 est impair donc $(n^2)^2 = n^4$ est impair d'où $A(n)$ est pair.

Remarque

On peut le justifier rigoureusement à l'aide des congruences.

1^{er} cas : si n est pair, $n \equiv 0 \pmod{2}$ donc $n^4 \equiv 0 \pmod{2}$ et $A(n) \equiv 1 \pmod{2}$, donc $A(n)$ est impair.

2^e cas : si n est impair, $n \equiv 1 \pmod{2}$ donc $n^4 \equiv 1 \pmod{2}$ et $A(n) \equiv 2 \pmod{2} \equiv 0 \pmod{2}$, donc $A(n)$ est pair.

b. Dire que d divise $A(n)$, c'est dire que $A(n) \equiv 0 \pmod{d}$ c'est-à-dire $n^4 + 1 \equiv 0 \pmod{d}$.

On en déduit que $n^4 \equiv -1 \pmod{d}$ donc $(n^4)^2 \equiv (-1)^2 \pmod{d}$ ce qui s'écrit $n^8 \equiv 1 \pmod{d}$.

2. a. •Effectuons comme suggéré par l'énoncé la division euclidienne de k par s . Comme $s \neq 0$, on peut diviser k par s :

$k = sq + r$ avec $0 \leq r < s$, avec q et r entiers naturels.

Remarque

On nous demande de démontrer que s divise k , ceci revient donc à démontrer que $r = 0$.

- Examinons les renseignements que l'on peut en déduire sur les puissances de n :

On a donc $n^k = n^{qs+r} = n^{qs} \times n^r = (n^s)^q \times n^r$.

Or par définition de s , $n^s \equiv 1 \pmod{d}$, donc $(n^s)^q \equiv 1^q \pmod{d} \equiv 1 \pmod{d}$.

Par conséquent n^k congru à $n^r \pmod{d}$.

Or par hypothèse sur k , $n^k \equiv 1 \pmod{d}$.

On en déduit donc que $n^r \equiv 1 \pmod{d}$.

- Montrons que $r = 0$

Supposons que $r \neq 0$.

On a montré que $n^r \equiv 1 \pmod{d}$ donc r est l'un des exposants h entiers naturels non nuls tels que $n^h \equiv 1 \pmod{d}$.

Alors de la définition de s , qui est le plus petit de ces exposants h non nuls, on déduit que $s \leq r$.

Mais r étant le reste dans une division euclidienne par s , on a $r < s$.

On arrive donc à une contradiction.

On en déduit que $r = 0$, c'est dire que $k = qs + 0 = qs$ avec q entier naturel.

Autrement dit, s divise k .

b. Par la question 1.b., on sait que $n^8 \equiv 1 \pmod{d}$. Donc 8 est l'un des entiers naturels k non nuls tels que $n^k \equiv 1 \pmod{d}$.

De la question 2.a., on déduit donc que s divise 8.

c. Raisonnement analogue à celui de la question précédente avec $d-1$ à la place de 8.

3. Soit p un diviseur premier de $A(n)$.

Par la question 1.b., $n^8 \equiv 1 \pmod{p}$ et par la question 2, s est un diviseur positif de 8 donc s est égal à 1, 2, 4 ou 8.

- Examinons les cas $s = 1, s = 2, s = 4$

De $n^s \equiv 1 \pmod{p}$ on déduit que si $s = 1, n \equiv 1 \pmod{p}$; si $s = 2, n^2 \equiv 1 \pmod{p}$;

si $s = 4, n^4 \equiv 1 \pmod{p}$.

Dans ces quatre cas, on a $n^4 \equiv 1 \pmod{p}$ donc $A(n) \equiv 2 \pmod{p}$.

Or p est un diviseur premier de $A(n)$ donc $A(n) \equiv 0 \pmod{p}$.

On en déduit que $2 \equiv 0 \pmod{p}$ donc que $p = 2$.

Dans ce cas, $A(n)$ étant divisible par $p = 2$, est pair.

Or par hypothèse n est pair, donc par la question 1.a., $A(n)$ est impair.

On arrive à une contradiction.

On en déduit donc que s n'est égal ni à 1, ni à 2, ni à 4.

Par conséquent $s = 8$.

- Montrons que $p \equiv 1 \pmod{8}$.

Par la question 2.c., on sait que s divise $p-1$. Donc 8 divise $p-1$.

Par conséquent $p - 1 \equiv 0 \pmod{8}$ ou encore $p \equiv 1 \pmod{8}$.

4. On est dans le cadre d'application de la question 2 puisque $n = 12$ est pair et on cherche les diviseurs premiers de $A(12)$.

On sait donc qu'un diviseur premier de $A(12)$ est congru à 1 modulo 8.

On teste donc les nombres premiers congrus à 1 modulo 8 proposés, à la calculatrice :

$A(12)$ n'est divisible ni par 17, ni par 41, ni par 7, mais est divisible par 89 :

$A(12) = 20\,737 = 89 \times 233$.

Montrons que 233 est premier : on vérifie que 233 n'est divisible par aucun des entiers premiers inférieurs ou égaux à $\sqrt{233} \approx 15,2$ car il n'est divisible ni par 2, par 3, par 5, par 7, par 11, par 13.

On peut donc en conclure que les diviseurs premiers de $A(12)$ sont 89 et 233.