DES PUISSANCES QUI FONT PSCHITT

Comme on l'a déjà observé, le calcul d'une puissance d'entier comme 3^{562} modulo 11 nous invite à chercher un entier $k \in \mathbb{N}^*$, petit si possible, pour lequel : $3^k \equiv 1\ [11]$. Le petit théorème de Fermat nous garantit que l'entier $k = 10$ convient, mais il en existe peut-être de plus petits. En l'occurrence, ici, le plus petit entier possible est $k = 5$. À partir de là, on calcule le reste de la division euclidienne de 561 par 5 : $562 \equiv 2\ [5]$, puis on conclut ainsi : $3^{562} \equiv 3^2 \equiv 9\ [11]$.

On se propose dans ce devoir d'explorer davantage le monde de ces puissances qui font pschitt et d'en donner plusieurs applications.

1) Ordre d'un entier modulo un autre entier : Soient $b \in \mathbb{N}^*$ et $a \in \mathbb{Z}$ premiers entre eux.

On pose : $E = \left\{k \in \mathbb{N}^* \mid \ a^k \equiv 1\ [b]\right\}$.

a) Montrer que E possède un plus petit élément e appelé l'*ordre de a modulo b*. On pourra s'intéresser pour tout $k \in \mathbb{N}^*$ au reste de la division euclidienne de a^k par b.

b) Montrer l'égalité : $E = e\mathbb{N}^*$. On pourra s'intéresser pour tout $k \in E$ à la division euclidienne de k par e.

c) Montrer que si b est un nombre premier, alors e divise $b-1$.

En résumé, l'ordre de a modulo b divise tout entier $k \in \mathbb{N}$ pour lequel : $a^k \equiv 1\ [b]$.

2) Exemples : Calculer l'ordre de 2 modulo 7 et celui de 5 modulo 13.

3) Une première application : On souhaite résoudre l'équation diophantienne : $3^m - 2^n = 1$ ★ d'inconnue $(m,n) \in \mathbb{N}^2$.

a) Déterminer toutes les solutions d'★ pour lesquelles : $n \leqslant 3$.

On se donne à présent un couple (m,n) solution d'★ pour lequel : $n \geqslant 4$.

b) Calculer l'ordre de 3 modulo 16. Qu'en déduit-on sur m ?

c) Conclure en raisonnant modulo 5.

4) Une deuxième application : On souhaite à présent montrer qu'un entier $n \geqslant 2$ ne divise jamais $2^n - 1$.

Raisonnant par l'absurde, on se donne un entier $n \geqslant 2$ qui divise $2^n - 1$. On note p le plus petit diviseur premier de n et e l'ordre de 2 modulo p.

Montrer que : $e = 1$, puis conclure.

5) Une troisième application : On fixe enfin un nombre premier p et on pose pour tout $n \in \mathbb{N}$: $x_n = 2^{p^n} - 1$.

a) Exprimer x_{n+1} en fonction de x_n pour tout $n \in \mathbb{N}$, puis montrer que x_n divise x_{n+1}.

b) Montrer que pour tout $n \in \mathbb{N}$ et pour tout diviseur d de x_n : $\dfrac{x_{n+1}}{x_n} \equiv p\ [d]$.

c) Montrer que pour tout $n \in \mathbb{N}$: $x_n \equiv 1\ [p]$.

d) En déduire que x_n et $\dfrac{x_{n+1}}{x_n}$ sont premiers entre eux pour tout $n \in \mathbb{N}$.

e) Montrer que pour tout $n \in \mathbb{N}$ et pour tout diviseur $d \neq 1$ de $\dfrac{x_{n+1}}{x_n}$, l'ordre de 2 modulo d vaut p^{n+1}.

f) En déduire que pour tout $n \in \mathbb{N}^*$, il existe une infinité de nombres premiers congrus à 1 modulo p^n.