DES PUISSANCES QUI FONT PSCHITT

Pour calculer une puissance d'entier comme 3^{562} modulo 11, on commencer par chercher un entier $k \in \mathbb{N}^*$, petit si possible, pour lequel $3^k \equiv 1\ [11]$. Le petit théorème de Fermat 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 un peu le monde de ces puissances qui font pschitt et d'en donner quelques 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 $E = \left\{k \in \mathbb{N}^* \mid \quad a^k \equiv 1\ [b]\right\}$.

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 que $E = e\mathbb{N}^*$.

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

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

À présent, soit (m,n) un couple 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) Deuxième application : On souhaite montrer qu'un entier n supérieur à 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) Troisième application : Soit p un nombre premier fixé. On pose $x_n = 2^{p^n} - 1$ pour tout $n \in \mathbb{N}$.

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

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

c) Montrer que $x_i \wedge \dfrac{x_{j+1}}{x_j} = 1$ pour tous $i, j \in \mathbb{N}$ pour lesquels $i \leqslant j$.

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

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