Devoir maison n° 8

À rendre le vendredi 28 novembre 2025

Rédigez sur une copie double lisiblement et proprement. Laissez une marge à gauche, écrivez à l'encre bleue ou noire et encadrez ou soulignez les résultats principaux.

Veuillez apporter un soin particulier à la rédaction, à la rigueur et aux raisonnements. Tout résultat doit être justifié. N'oubliez pas d'introduire toutes les variables que vous utilisez.

Ordre d'un entier modulo un autre

Dans tout cet exercice, on se donne $n \in \mathbb{N}\backslash\{0;1\}$, $a \in \mathbb{N}\backslash\{0;1\}$ et $b \in \mathbb{N}\backslash\{0;1\}$.

Partie A : Préliminaires

1) On suppose qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\,[n]$. Justifier que $a \wedge n = 1$.

2) Supposons que a est premier avec n.
   a) Justifier qu'il existe k_1 et k_2 des entiers naturels distincts tels que $a^{k_2} \equiv a^{k_1}\,[n]$.
   b) Quitte à échanger leurs noms, supposons que $k_2 > k_1$. En déduire qu'il existe $k \in \mathbb{N}^*$ tel que $a^k \equiv 1\,[n]$.

3) a) En utilisant le petit théorème de Fermat, montrer que $4^{12} \equiv 1\,[195]$.
   b) Vérifier (à la main) que $4^6 \equiv 1\,[195]$ et que, pour tout $k \in [\![1\,;5]\!]$, $4^k \not\equiv 1\,[195]$.

   Ainsi 6 est la plus petite puissance (sans compter 4^0) de 4 qui est congrue à 1 modulo 195.

L'exemple précédent illustre le fait que le petit théorème de Fermat est très utile pour trouver une puissance d'un entier congrue à 1 modulo n (du moins lorsque n n'admet pas de facteur premier carré) mais qu'il ne donne pas a priori la plus petite puissance congrue à 1.

Partie B : Notion d'ordre d'un entier modulo n

1) a) On suppose que $a \wedge n = 1$. Justifier que $\{k \in \mathbb{N}^* \,|a^k \equiv 1\,[n]\}$ admet un plus petit élément. On le note $\omega_n(a)$ et on l'appelle l'ordre de a modulo n. Autrement dit $a^{\omega_n(a)}$ est la plus petite puissance de a (sans compte a^0) qui est congrue à 1 modulo n.
   b) Est-ce que $\omega_n(a)$ a un sens lorsque $a \wedge n \neq 1$.

Dans la suite, supposons que $a \wedge n = 1$

2) Soit $k \in \mathbb{N}^*$. Montrer que $a^k \equiv 1\,[n]$ si et seulement si $\omega_n(a)|k$.
   Pour le sens direct, on pourra commencer par écrire la division euclidienne de k par $\omega_n(a)$.

3) Justifier que, lorsque n est premier, $\omega_n(a)|n-1$.

Partie C : Quelques propriétés de l'ordre

On suppose dans toute cette partie que $a \wedge n = 1$ et $b \wedge n = 1$. On pensera à bien à utiliser le critère de la question B2.

1) Montrer que $\omega_n(ab)|\omega_n(a) \vee \omega_n(b)$.

2) Soit $d \in \mathbb{N}^*$.
   a) Justifier que $\omega_n(a^d) \,\Big|\, \dfrac{\omega_n(a)}{d \wedge \omega_n(a)}$.
   b) Justifier que $d \vee \omega_n(a) \,\big|\, d\,\omega_n(a^d)$.
   c) En déduire que $\omega_n(a^d) = \dfrac{\omega_n(a)}{d \wedge \omega_n(a)}$.

3) Supposons que b est un inverse de a modulo n (c'est-à-dire $ab \equiv 1\,[n]$). Montrer que $\omega_n(a) = \omega_n(b)$.

4) On suppose que $\omega_n(a) \wedge \omega_n(b) = 1$.

   a) Notons $m = \omega_n(ab)$. Déduire des questions précédentes que

$$\frac{\omega_n(a)}{m \wedge \omega_n(a)} = \frac{\omega_n(b)}{m \wedge \omega_n(b)}.$$

   b) Conclure que $\omega_n(a) \vee \omega_n(b) | m$ puis que $\omega_n(ab) = \omega_n(a) \vee \omega_n(b)$.

Partie D : Application : résolution d'une équation diophantienne

On considère l'équation $(E) : 3^m - 2^n = 1$ d'inconnue $(m, n) \in \mathbb{N}^2$.

1) Déterminer toutes les solutions de l'équation pour lesquelles $n \leqslant 3$.

2) Donnons-nous un couple (m, n) solution de (E) avec $n \geqslant 4$.

   a) Calculer $\omega_{16}(3)$. Qu'en déduit-on sur m ?

   b) Conclure en raisonnant modulo 5.

Partie E : Application : infinité des nombres premiers congrus à 1 modulo p^n

On se donne un nombre premier p. Pour tout $n \in \mathbb{N}$, posons $x_n = 2^{p^n} - 1$.

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

2) Soit $n \in \mathbb{N}$.

   a) Montrer que $x_n | x_{n+1}$ et donner une expression de $y_n = \dfrac{x_{n+1}}{x_n}$ sous la forme d'une somme.

   b) Vérifier que $y_n \neq 1$ et que $y_n \equiv p\,[x_n]$.

3) En déduire que, pour tout $(i, j) \in \mathbb{N}^2$ tel que $i \leqslant j$, $x_i \wedge y_j = 1$.

4) Soit $n \in \mathbb{N}$. On se donne alors q un diviseur premier de y_n.

   a) En utilisant la question précédente, montrer que $\omega_q(2) = p^{n+1}$.

   b) En déduire que $q \equiv 1\left[p^{n+1}\right]$.

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