Pendant les vacances.

1) SE REPOSER !
   Quelques suggestions pour organiser votre travail.
2) **Un calcul par jour !**
3) Revoir le cours. Refaire les petits contrôles du lundi peut être un bon moyen de revoir le cours.
4) **Eventuellement**, refaire des exercices qui ont posé problème sur les chapitres traités, en particulier refaire des calculs (limites, primitives, résolution équa diff, équivalents).
   Faire des exercices déjà vus, papier crayon en main sans lire le corrigé est un travail. Lire des corrigés d'exercices qu'on n'a pas cherchés n'est pas un travail.
5) Passer du temps sur ce DM10, en plusieurs fois s'il le faut.
6) BONNES VACANCES !

Problème 1. Autour du théorème de Fermat

La partie I plus proche du cours est obligatoire.
La partie II demande plus de réflexion, mais est accessible. La question 6) est obligatoire.
La partie III est facultative, faite pour ceux qui veulent aller plus loin.

Partie I - Inverse modulo n

L'objectif de cette partie est d'introduire la notion d'inverse modulo n et d'apprendre à résoudre l'équation :

$$ax \equiv b\,[n]$$

Soit $n \in \mathbb{Z}$. On dit qu'un entier $a \in \mathbb{Z}$ admet un inverse modulo n s'il existe $a' \in \mathbb{Z}$ tel $aa' \equiv 1\,[n]$. On dit que a' est UN inverse modulo n.

1) Déterminer les couples $(u, v) \in \mathbb{Z}^2$ vérifiant $3u + 7v = 1$.
   En déduire que 3 admet un inverse modulo 7 et donner les inverses de 3 modulo 7.
2) Montrer que 4 n'admet pas d'inverse modulo 6.
3) Soit $a \in \mathbb{Z}$. Montrer que a admet un inverse modulo n si et seulement si $a \wedge n = 1$.
4) Soit $a \in \mathbb{Z}$ et on suppose $a \wedge n = 1$. On pose a' un inverse de a modulo n.
   Déterminer en fonction de a' les solutions $x \in \mathbb{Z}$ de l'équation $ax \equiv b\,[n]$.
5) **Application**. Résoudre les deux équations : (E_1) $3x \equiv 4\,[20]$ (E_2) $12x \equiv 8\,[34]$.

Partie II - Une autre démonstration du petit théorème de Fermat

Dans cette partie p est un entier premier et $a \in \mathbb{Z}$.
Dans les questions II) 1),2),3),4), on suppose que p ne divise pas a.

1) Pour $k \in [\![1, p-1]\!]$, on note r_k le reste de la division euclidienne de ka par p. Montrer que $r_k \in [\![1, p-1]\!]$.
2) On a donc défini une application $\begin{array}{rccc} f : & [\![1,p-1]\!] & \to & [\![1,p-1]\!] \\ & k & \mapsto & r_k \end{array}$.
   A l'aide de I-4) montrer que l'application f est bijective.
3) En déduire que $\displaystyle\prod_{k=1}^{p-1} r_k = (p-1)!$.

4) En calculant $\prod_{k=1}^{p-1} r_k$ d'une autre manière, montrer que l'on obtient le petit théorème de Fermat :

$$a^{p-1} \equiv 1\ [p].$$

5) En déduire que pour tout $a \in \mathbb{Z}$, $a^p \equiv a\ [p]$.

6) **Applications du petit théorème de Fermat**

-a- Montrer que $13|2^{70} + 3^{70}$.

-b- -i- Soit $\forall (m,n) \in \mathbb{Z}^2$. Montrer que : $3|mn(m^4 - n^4)$; puis $5|mn(m^4 - n^4)$.

-ii- En déduire que $15|mn(m^4 - n^4)$.

Partie III - Indicatrice d'Euler - **Facultative**

On définit l'application φ, appelée indicatrice d'Euler, par :

$$\forall n \in \mathbb{N}^*, \quad \varphi(n) = \text{Card}\left\{k \in [\![1, n-1]\!] \,/\, k \wedge n = 1\right\}.$$

$\varphi(n)$ est donc le nombre d'entiers de $[\![1, n-1]\!]$ premiers avec n.

1) Calculer $\varphi(7)$, $\varphi(15)$.

2) Soit p un entier premier et $\alpha \in \mathbb{N}^*$. Calculer $\varphi(p)$ puis $\varphi(p^\alpha)$.

3) Soient m et n deux entiers premiers distincts. Montrer que $\varphi(mn) = \varphi(m)\varphi(n)$.
On admet que ce résultat reste vrai si m et n sont deux entiers premiers entre eux.

4) Soit $n \in \mathbb{N}$, on pose sa décomposition en facteurs premiers $n = \prod_{i=1}^{N} p_i^{\alpha_i}$ où les p_i sont des entiers premiers deux à deux distincts et les α_i sont des entiers naturels non nuls. Montrer que :

$$\varphi(n) = n \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

5) Soit $n \in \mathbb{N}^*$. On pose $A_n = \{k_1, \ldots, k_{\varphi(n)}\}$ l'ensemble des entiers de $[\![1, n-1]\!]$ premiers avec n.
Soit $a \in [\![1, n-1]\!]$ tel que $a \wedge n = 1$. On définit l'application $k_i \in A_n \mapsto r_{k_i}$ où r_{k_i} est le reste de la division euclidienne de ak_i par n.

-a- Montrer que pour tout $k_i \in A_n$, $r_{k_i} \in A_n$.

On montre comme dans II)2) que l'application $\begin{array}{ccc} A_n & \to & A_n \\ k_i & \mapsto & r_{k_i} \end{array}$ est bijective.

-b- En calculant $\prod_{i=1}^{\varphi(n)} r_{k_i}$ de deux façons montrer alors que

$$a^{\varphi(n)} \equiv 1\ [n]$$

On a ainsi démontré le petit théorème de Fermat étendu.