DM 12 Arithmétique.

Exercice 1. Exercice n° 94 de la banque CCP. En bleu mes ajouts/commentaires/indication

1. Énoncer le théorème de Bézout dans $\mathbb{Z}$.
2. Soit a et b deux entiers naturels premiers entre eux. Soit $c \in \mathbb{N}$.

   Démontrer que : $(a \text{ divise } c \text{ et } b \text{ divise } c) \iff (ab) \text{ divise } c$.

   Ceci est un théorème du cours. Je l'ai démontré en classe. Retrouver le ! ! !
3. On considère le système (S) : $\begin{cases} x \equiv 6 & [17] \\ x \equiv 4 & [15] \end{cases}$ dans lequel l'inconnue x appartient à $\mathbb{Z}$.

   On a $\left.\begin{array}{l} x \equiv 6[17] \iff x = 6 + k.17 \\ x \equiv 4[15] \iff x = 4 + k'.15 \end{array}\right\} \iff x = 6 + k.17 = x = 4 + k'.15$ avec $k, k' \in \mathbb{Z}$

   (a) Déterminer une solution particulière x_0 de (S) dans $\mathbb{Z}$.

   Trouver x_0 revient à trouver k et k', CàD résoudre dans $\mathbb{Z}$, $6 + k.17 = x = 4 + k'.15 \iff 17.k - 15.k' = -2$
   Or on sait résoudre $17.a - 15.b = 1$

   (b) *Déduire des questions précédentes* la résolution dans $\mathbb{Z}$ du système (S).

Exercice 2.

Partie A On considère l'équation (E) : $25x - 108y = 1$ où x et y sont des entiers relatifs.

1. Déterminer une solution particulière (x_0, y_0) de l'équation (E)
2. Déterminer l'ensemble des couples d'entiers relatifs solutions de l'équation (E).

Partie B Dans cette partie, a désigne un entier naturel.
Les nombres c et g sont des entiers naturels vérifiant la relation $25g - 108c = 1$.

On admettra le théorème suivant, dit petit théorème de Fermat
Si p est un nombre premier et a un entier non divisible par p,
alors a^{p-1} est congru à 1 modulo p que l'on note $a^{p-1} \equiv 1$ $[p]$.

1. Soit x un entier naturel.

   Trouver dans le cours, le théorème qui assure que : Si $n \equiv 0$ $[7]$ et $n \equiv 0$ $[19]$ alors $n \equiv 0$ $[\underbrace{133}_{=7.19}]$

   En déduire que : si $x \equiv a$ $[7]$ et $x \equiv a$ $[19]$, alors $x \equiv a$ $[133]$.
2. Une congruence.

   (a) On suppose que a n'est pas un multiple de 7.

   Démontrer que $a^6 \equiv 1$ $[7]$ puis que $a^{108} \equiv 1$ $[7]$.
   En déduire que $\left(a^{25}\right)^g \equiv a$ $[7]$.

   (b) On suppose que a est un multiple de 7.

   Démontrer que $\left(a^{25}\right)^g \equiv a$ $[7]$.

   (c) On admet que pour tout entier naturel a, $\left(a^{25}\right)^g \equiv a$ $[19]$.

   Démontrer que $\left(a^{25}\right)^g \equiv a$ $[133]$.

Partie C On note $\mathcal{A}$ l'ensemble des entiers naturels a tels que : $1 \leqslant a \leqslant 26$.

Un message, constitué d'entiers appartenant à $\mathcal{A}$, est codé puis décodé.

$>$ La phase de codage consiste à associer, à chaque entier a de $\mathcal{A}$, l'entier r tel que $a^{25} \equiv r$ $[133]$ avec $0 \leqslant r < 133$.
$>$ La phase de décodage consiste à associer à r , l'entier r_1 tel que $r^{13} \equiv r_1$ $[133]$ avec $0 \leqslant r_1 < 133$.

1. Justifier que $r_1 \equiv a$ $[133]$.
2. Un message codé conduit à la suite des deux entiers suivants : 128 59.

   Décoder ce message et lire le message.

Bonus plus difficile : la formule de Popoviciu

L'exemple : c'est un exercice de Centrale dont l'énoncé est
Combien de couples d'entiers (x, y) avec x et y positifs, vérifie $12x + 7y = 100$.

Le théorème de Popoviciu : c'est un exercice des ENS (que j'ai détaillé)

Exercice 3. [Correction]

Un exemple

1. Calculer $pgcd(12, 17)$ puis déterminer deux entiers u et v tels que $12u + 7v = 100$.
2. Déterminer tous les couples d'entiers $(x, y) \in \mathbb{Z}^2$ tels que $12x + 7y = 100$.
3. Parmi toutes ces solutions, combien de couples d'entiers (x, y) avec x et y positifs y a-t-il ?

Le théorème de Popoviciu

Dans toute la suite, on considère deux entiers a et b premiers entre eux avec $1 \leqslant b < a$.
Soit $n \in \mathbb{N}^*$, un entier naturel non nul.
On note (E_n) l'équation diophantienne $ax + by = n$ d'inconnues x et y dans $\mathbb{Z}$.
On note s_n le nombre de couples de solutions de (E_n) dans $\mathbb{N} \times \mathbb{N}$.
On note $\{\theta\}$ la partie fractionnaire d'un réel θ définie par $\{\theta\} = \theta - \lfloor \theta \rfloor$
ainsi on a $\{\theta\} \in [0, 1[$ et $\theta = \lfloor \theta \rfloor + \{\theta\}$.
Exemple : $\lfloor \pi \rfloor = \lfloor 3,14159... \rfloor = 3$ et $\{\pi\} = \{3,14159...\} = 0,14159...$

1. les nombre a^* et b^*
   (a) En regardant la relation de Bézout modulo [b] et modulo [a],
   justifier qu'il existe un nombre $a^* \in \{1, \dots, b-1\}$ et un nombre $b^* \in \{1, \dots, a-1\}$,
   tels que : $aa^* \equiv 1[b]$ et $bb^* \equiv 1[a]$.
   (b) Montrer que : a^* est unique. (De même b^* est unique)
2. On note $b' = a - b^*$.
   (a) Montrer que $a^*a - b'b \equiv 1[ab]$.
   (b) En déduire $a^*a - b'b = 1$.
   (c) Montrer que l'ensemble des solutions de (E_n) est l'ensemble $\Big\{ \big(a^*n + kb, -b'n - ka\big), k \in \mathbb{Z} \Big\}$.
3. On suppose que $\dfrac{a^*n}{b}$ et $\dfrac{b'n}{a}$ ne sont pas entiers.
   (a) Montrer que $s_n = \left\lfloor \dfrac{a^*n}{b} \right\rfloor - \left\lfloor \dfrac{b'n}{a} \right\rfloor$ *C'est la formule de Popoviciu* On convient que si la formule renvoie à $s_n < 0$ alors $s_n = 0$

   Puis que $s_n = \left\lfloor \dfrac{n}{ab} \right\rfloor$ ou $s_n = \left\lceil \dfrac{n}{ab} \right\rceil$

   (b) Application : Dans le cas $a = 12$ et $b = 7$, déterminer la valeur de s_{100}.