DOMAINE : Arithmétique
NIVEAU : Débutants
CONTENU : Cours et exercices

AUTEUR : Nicolas SÉGARRA
STAGE : Montpellier 2014

Congruences

Commençons par trois exercices permettant de rappeler ce qui a été vu lors de la séance précédente.

Exercice 1. Soit p un entier naturel. Montrer que si p est pair alors p^2 est pair. La réciproque est-elle vraie ?

Solution de l'exercice 1. On suppose que p est pair donc il existe un entier k tel que : $p = 2k$. On a alors : $p^2 = 4k^2 = 2 \times 2k^2$ et $2k^2$ est entier, donc p^2 est pair.
La réciproque est vraie, on peut la démontrer par contraposée : supposons que p est impair alors il existe un entier k tel que : $p = 2k + 1$. On a donc : $p^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$ et $2k^2 + 2k$ est un entier. Ainsi, p^2 est impair. Par conséquent, par contraposée, si p^2 est pair alors p est pair.

Exercice 2. Pour quelles valeurs de l'entier naturel n, $n + 2$ divise-t-il $n^3 - 2n^2 - 5n + 7$?

Solution de l'exercice 2. On écrit : $\forall\, n \in \mathbb{N}$, $n^3 - 2n^2 - 5n + 7 = n^3 - 2n^2 - 5n + 6 + 1 = (n-1)(n+2)(n-3) + 1$. Donc si d est un diviseur commun à $n+2$ et à $n^3 - 2n^2 - 5n + 7$, d divise 1 donc le $PGCD$ de $n^3 - 2n^2 - 5n + 7$ et de $n+2$ est 1. Par conséquent, $n^3 - 2n^2 - 5n + 7$ et $n + 2$ sont premiers entre eux pour tout entier naturel n. Ainsi, pour tout entier naturel n, $n + 2$ ne divise pas $n^3 - 2n^2 - 5n + 7$.

Exercice 3. Soit n un entier naturel non nul. Déterminer le reste dans la division euclidienne par n, de la somme des n premiers entiers naturels non nuls.

Solution de l'exercice 3. La somme des n premiers entiers naturels non nuls est : $S_n = 1 + 2 + \ldots + n = \dfrac{n(n+1)}{2}$. Distinguons deux cas.
Supposons que n est impair, alors $n + 1$ est pair donc 2 divise $n + 1$ ainsi $\dfrac{n+1}{2}$ est un entier et n divise S_n. Par conséquent, le reste dans la division euclidienne par n, de la somme des n premiers entiers naturels non nuls est 0 si n est impair.
Supposons maintenant que n est pair. On écrit : $S_n = \dfrac{n^2 + n}{2} = \dfrac{n^2}{2} + \dfrac{n}{2} = n \times \dfrac{n}{2} + \dfrac{n}{2}$. Comme n est pair, $\dfrac{n}{2}$ est entier et on a : $0 \leq \dfrac{n}{2} < n$ (car $n \geq 1$). Ainsi, le reste dans la division

euclidienne par n, de la somme des n premiers entiers naturels non nuls est $\frac{n}{2}$ si n est pair.

Définition. Soient a, b et n trois entiers, $n \geq 2$. On dit que a est congru à b modulo n si n divise $a - b$.

Remarque. On peut écrire que : $a \equiv b \pmod{n} \Leftrightarrow n|a-b \Leftrightarrow \exists k \in \mathbb{Z}, a-b = kn$. De plus, $a \equiv 0 \pmod{n} \Leftrightarrow n|a \Leftrightarrow \exists k \in \mathbb{Z}, a = kn$.

Quelques propriétés résultent de la définition :

Propriétés. Soient a, b, c, a', b' et n des entiers, $n \geq 2$.
1. (Réflexivité) $a \equiv a \pmod{n}$.
2. (Symétrie) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$.
3. (Transitivité) $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$.
4. $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n} \Rightarrow a + b \equiv a' + b' \pmod{n}$.
5. $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n}$.
6. Si $a \equiv b \pmod{n}$ alors pour tout entier naturel $q \geq 1$, $a^q \equiv b^q \pmod{n}$.

Preuves.
1. Pour tout entier $n \geq 2$, n divise 0 donc n divise $a - a$ ainsi, $a \equiv a \pmod{n}$.
2. On suppose que $a \equiv b \pmod{n}$. Alors n divise $a - b$ donc il existe un entier k tel que : $a - b = kn$. En écrivant : $b - a = -kn$, on en déduit que n divise $b - a$ donc $b \equiv a \pmod{n}$.
3. On a : $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n}$ donc n divise $a - b$ et $b - c$. Alors, il existe des entiers k et k' tels que : $a - b = kn$ et $b - c = k'n$ donc : $a - c = n(k + k')$ et alors n divise $a - c$.
4. Comme $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, on a : n divise $a - a'$ et $b - b'$ donc il existe des entiers k et k' tels que : $a - a' = nk$ et $b - b' = nk'$. On obtient alors : $a + b - (a' + b') = n(k + k')$ donc n divise $a + b - (a' + b')$ ainsi, $a + b \equiv a' + b' \pmod{n}$.
5. Comme précédemment, on écrit : $a - a' = kn$ et $b - b' = k'n$ avec k, $k' \in \mathbb{Z}$, ainsi, on a : $a = a' + kn$ et $b = b' + k'n$ donc $ab - a'b' = (a' + kn)(b' + k'n) - a'b' = a'k'n + knb' + kk'n^2 = n(a'k' + kb' + kk'n)$ et $a'k' + kb' + kk'n$ est un entier, donc n divise $ab - a'b'$ ainsi, $ab \equiv a'b' \pmod{n}$.
6. Raisonnons par récurrence sur $q \in \mathbb{N}^*$.
Pour $q = 1$, on a bien : $a \equiv b \pmod{n}$ par hypothèse.
Supposons que $a^q \equiv b^q \pmod{n}$ pour $q \geq 1$. Comme on a aussi : $a \equiv b \pmod{n}$, on obtient : $a^q \times a \equiv b^q \times b \pmod{n}$ en utilisant la propriété 5. Ainsi, $a^{q+1} \equiv b^{q+1} \pmod{n}$. Ce qui achève la récurrence.

Théorème. Soient n et a des entiers avec $n \geq 2$. Alors a est congru modulo n à exactement un des entiers $0, 1, 2, ..., n - 1$.

Démonstration. Par division euclidienne de a par n, on peut écrire qu'il existe des entiers q et r tels que : $a = nq + r$ avec $0 \leq r \leq n - 1$. Comme $a - r = nq$, on en déduit que : n divise $a - r$ donc $a \equiv r \pmod{n}$ donc a est congru à un des nombres $0, 1, ..., n - 1$.
Supposons maintenant que a est congru à deux nombres s et t parmi $0, 1, ..., n-1$. Par symétrie

et par transitivité, on peut en déduire que $s \equiv t \pmod{n}$ donc il existe $k \in \mathbb{Z}$ tel que : $s = nk + t \Rightarrow s - t = nk$. Or, on a : $0 \leq s < n$ et $-n < -t \leq 0$ donc $-n < s - t < n$ et en divisant par $n \geq 2$ (donc non nul), on obtient : $-1 < k < 1$ (car $s - t = nk$). Comme k est un entier, on a : $k = 0$ et ainsi, $s = t$.

Exercice 4. Montrer que le carré d'un entier est congru à 0 ou 1 modulo 4.

Solution de l'exercice 4. Soit n un entier. L'entier n est congru à 0 ou 1 ou 2 ou 3 modulo 4 (par le théorème précédent) donc n^2 est congru à 0 ou 1 modulo 4.

Exercice 5. Soit n un entier.
1) Montrer que si n est pair, $n^2 \equiv 0 \pmod{8}$ ou $n^2 \equiv 4 \pmod{8}$ et que si n est impair, $n^2 \equiv 1 \pmod{8}$.
2) Montrer que si n est impair, $n^4 \equiv 1 \pmod{8}$.

Solution de l'exercice 5.
1) Si n est pair alors il existe un entier k tel que $n = 2k$. Donc $n^2 = 4k^2$. Si k est pair, alors il existe un entier p tel que $k = 2p$. Ainsi, on a : $n^2 = 16p^2 = 8 \times 2p^2$ et $2p^2$ est un entier donc 8 divise n^2 ainsi, $n^2 \equiv 0 \pmod{8}$, si k est pair.
Si k est impair, alors il existe un entier m tel que $k = 2m + 1$ et alors : $n^2 = 4(2m + 1)^2 = 4(4m^2 + 4m + 1) = 16m^2 + 16m + 4 = 8(2m^2 + 2m) + 4$ donc $n^2 \equiv 4 \pmod{8}$ si k est impair.
Si n est impair alors il existe un entier k tel que $n = 2k + 1$. Donc $n^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Le produit $k(k + 1)$ est le produit de deux entiers consécutifs donc il est pair. Ainsi, 2 divise $k(k + 1)$ donc 8 divise $4k(k + 1)$. D'où, $n^2 \equiv 1 \pmod{8}$.
2) D'après la question précédente, si n est impair, alors $n^2 \equiv 1 \pmod{8}$. Ainsi, $n^4 \equiv 1 \pmod{8}$.

Exercice 6. Déterminer le chiffre des unités de 1789^{1789}.

Solution de l'exercice 6. On a : $1789 \equiv 9 \pmod{10} \Rightarrow 1789^{1789} \equiv 9^{1789} \pmod{10}$.
Regardons les puissances de 9 modulo 10. On a : $9^0 \equiv 1 \pmod{10}$, $9^1 \equiv 9 \pmod{10}$, $9^2 \equiv 1 \pmod{10}$, $9^3 \equiv 9 \pmod{10}$ etc. On a alors pour tout entier naturel k, $9^{2k} \equiv 1 \pmod{10}$ (en effet, $9^{2k} = 81^k$ et $81 \equiv 1 \pmod{10}$) et $9^{2k+1} \equiv 9 \pmod{10}$ (en effet, $9^{2k+1} = 9^{2k} \times 9$ et $9^{2k} \equiv 1 \pmod{10}$). Comme 1789 est impair, on en déduit que : $9^{1789} \equiv 9 \pmod{10}$. Ainsi, le chiffre des unités de 1789^{1789} est 9.

Exercice 7. Déterminer le chiffre des unités de 2^{49}.

Solution de l'exercice 7. On a : $2^1 \equiv 2 \pmod{10}$, $2^2 \equiv 4 \pmod{10}$, $2^3 \equiv 8 \pmod{10}$, $2^4 \equiv 6 \pmod{10}$ et $2^5 \equiv 2 \pmod{10}$.
On peut alors démontrer que $\forall\, k \in \mathbb{N}^*$, $2^{4k} \equiv 6 \pmod{10}$. Raisonnons par récurrence sur $k \in \mathbb{N}^*$. Pour $k = 1$, on a : $2^{4k} = 2^4 \equiv 6 \pmod{10}$. Supposons que : $2^{4k} \equiv 6 \pmod{10}$ pour $k \in \mathbb{N}^*$, $2^{4(k+1)} = 2^{4k} \times 2^4 \equiv 6 \pmod{10}$, ce qui achève la récurrence. Il en résulte que $\forall\, k \in \mathbb{N}$, $2^{4k+1} \equiv 2 \pmod{10}$ (en effet, pour $k = 0$, $2^1 \equiv 2 \pmod{10}$ et pour $k \in \mathbb{N}^*$,

$2^{4k+1} = 2^{4k} \times 2$ et pour $k \in \mathbb{N}^*$, $2^{4k} \equiv 6 \pmod{10}$), $2^{4k+2} \equiv 4 \pmod{10}$ et $2^{4k+3} \equiv 8 \pmod{10}$. Effectuons la division euclidienne de 49 par 4. On a : $49 = 4 \times 12 + 1 = 4k + 1$ avec $k = 12$. Ainsi, $2^{49} \equiv 2 \pmod{10}$. Donc, le chiffre des unités de 2^{49} est 2.
On aurait pu raisonner plus simplement en écrivant que $2^{49} = 2^{10} \times 2^{10} \times 2^{10} \times 2^{10} \times 2^9$. Comme $2^{10} = (2^5)^2$ et $2^5 \equiv 2 \pmod{10}$, on a : $2^{10} \equiv 4 \pmod{10}$. De plus, $2^4 \equiv 6 \pmod{10}$, donc $2^9 \equiv 2 \pmod{10}$ (en écrivant que $2^9 = (2^4)^2 \times 2$). Ainsi, $2^{10} \times 2^{10} \equiv 6 \pmod{10}$ et $2^{10} \times 2^{10} \times 2^{10} \times 2^{10} \times 2^9 \equiv 2 \pmod{10}$.

Exercice 8. Démontrer que la somme des cubes de trois entiers consécutifs est divisible par 9.

Solution de l'exercice 8. Soit n un entier. Calculons : $n^3 + (n+1)^3 + (n+2)^3$.
On a : $n^3+(n+1)^3+(n+2)^3 = n^3+n^3+3n^2+3n+1+n^3+6n^2+12n+8 = 3n^3+9n^2+15n+9 = 3n(n^2+5)+9(n^2+1)$. Ainsi, pour montrer que 9 divise $n^3 + (n+1)^3 + (n+2)^3$, il suffit de démontrer que 9 divise $3n(n^2+5)$ i.e : que 3 divise $n(n^2+5)$. Si $n \equiv 0 \pmod{3}$, c'est bien sûr vrai. Si $n \equiv 1 \pmod{3}$, alors $n^2 \equiv 1 \pmod{3}$ et $5 \equiv 2 \pmod{3}$ donc 3 divise $n(n^2+5)$. Enfin, si $n \equiv 2 \pmod{3}$ alors $n^2 \equiv 1 \pmod{3}$ et $5 \equiv 2 \pmod{3}$ donc 3 divise $n(n^2+5)$. Donc dans tous les cas, 9 divise $3n(n^2+5)$.

Théorème. Soient $n > 1$ un entier et c un entier. Alors, il existe un entier c' tel que $cc' \equiv 1 \pmod{n}$ si et seulement si c est premier avec n. L'entier c' est appelé : inverse de c modulo n.

Démonstration. Sens direct : supposons qu'il existe un entier c' tel que $cc' \equiv 1 \pmod{n}$. Alors $n | cc' - 1$ donc il existe $k \in \mathbb{Z}$ tel que : $cc' - 1 = kn \Rightarrow cc' - kn = 1$ et par le théorème de Bézout, on en déduit que c et n sont premiers entre eux.
Réciproquement, supposons que c et n sont premiers entre eux. Alors, d'après le théorème de Bézout, il existe deux entiers u et v tels que $cu+nv = 1 \Rightarrow cu-1 = nv \Rightarrow n | cu-1 \Rightarrow cu \equiv 1 \pmod{n}$ donc on a prouvé qu'il existe $c' = u \in \mathbb{Z}$ tel que $cc' \equiv 1 \pmod{n}$.

Remarque. Un nombre entier naturel n s'écrit en base 10 de la manière suivante : $n = a_k a_{k-1} ... a_0$ où les a_i, $\forall\ 0 \leq i \leq k$ sont des chiffres donc des entiers compris entre 0 et 9 inclus. On peut aussi écrire : $n = a_k \times 10^k + a_{k-1} \times 10^{k-1} + ... + a_1 \times 10 + a_0$.

Exercice 9 : critères de divisibilité. Enoncer et démontrer les critères de divisibilité par 2, 3, 5, 9 et 10.

Solution de l'exercice 9. Soit n un entier naturel. On écrit n en base 10 : $n = a_k a_{k-1} ... a_0 = a_k \times 10^k + a_{k-1} \times 10^{k-1} + ... + a_1 \times 10 + a_0$ (où les a_i, $\forall\ 0 \leq i \leq k$ sont des chiffres). Montrons que n est divisible par 2 si et seulement si son chiffre des unités est pair, i.e : congru à 0 modulo 2.
On a : $10 \equiv 0 \pmod{2} \Rightarrow 10^i \equiv 0 \pmod{2}, \forall\ i \in \mathbb{N}^*$. Ainsi, $n \equiv a_0 \pmod{2}$. Donc 2 divise n si et seulement si 2 divise a_0.
Montrons que n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3. On a : $10 \equiv 1 \pmod{3} \Rightarrow 10^i \equiv 1 \pmod{3}, \forall\ i \in \mathbb{N}^*$. Ainsi, $n \equiv a_k + a_{k-1} + ... + a_0 \pmod{3}$. D'où 3 divise n si et seulement si 3 divise $(a_0 + ... + a_k)$.
On montre que n est divisible par 5 si et seulement si son chiffre des unités est divisible par 5

(i.e : se termine par 0 ou 5) de la même façon que le critère de divisibilité par 2. Enfin, 9 divise n si et seulement si 9 divise la somme de ses chiffres et 10 divise n si et seulement si 10 divise a_0 (i.e : $a_0 = 0$). Les preuves de ces deux derniers critères de divisibilité sont très proches des autres preuves.

Etudions maintenant des équations linéaires à une inconnue modulo un entier.
Considérons les deux équations $7x \equiv 21 \pmod{17}$ et $6x \equiv 18 \pmod{36}$. Nous avons deux équations comportant chacune une inconnue entière : x.
Dans les deux équations, on est tenté de diviser par 7 pour la première et par 6 pour la deuxième...

Intéressons-nous à la première : si x est solution de $7x \equiv 21 \pmod{17}$ alors il existe $k \in \mathbb{Z}$ tel que : $7x = 17k + 21$. 7 divise $7x$ donc 7 divise $17k + 21$ donc 7 doit diviser $17k$ mais comme 7 et 17 sont premiers entre eux, on en déduit, en utilisant le lemme de Gauss, que 7 divise k donc il existe $k' \in \mathbb{Z}$ tel que : $k = 7k'$ et on obtient : $7x = 17 \times 7k' + 21$ donc $x = 17k' + 3$, $k' \in \mathbb{Z}$. Réciproquement, on vérifie que les entiers de la forme $7(17k' + 3)$ sont congrus à 21 modulo 17. Si on avait divisé par 7 à gauche et à droite, on aurait obtenu le bon résultat : $x \equiv 3 \pmod{17}$. Ici, cette méthode fonctionne car diviser par 7 revient en fait à multiplier par un inverse de 7 modulo 17 (qui existe bien car 7 et 17 sont premiers entre eux) et un inverse de 7 modulo 17 est 5 et si l'on multiplie les deux membres par 5, on obtient bien : $x \equiv 3 \pmod{17}$.

Regardons maintenant la deuxième équation : $6x \equiv 18 \pmod{36}$. Si x est solution de cette équation alors il existe un entier k tel que : $6x = 36k + 18$ et en divisant par 6, on obtient : $x = 6k + 3$, $k \in \mathbb{Z}$. Réciproquement, les entiers de la forme : $6k + 3$, $k \in \mathbb{Z}$ sont solutions de l'équation : $6x \equiv 18 \pmod{36}$.
Si on avait divisé par 6 ici, on aurait obtenu : $x \equiv 3 \pmod{36}$, ce qui n'est pas le bon résultat...
En fait, ici, 6 et 36 ne sont pas premiers entre eux, donc le théorème précédent garantit qu'il n'existe pas d'entier a tel que : $6a \equiv 1 \pmod{36}$ donc nous n'avons pas le droit de diviser par 6.

Finalement, la "morale" à retenir à travers ces deux exemples est que le fait de vouloir simplifier des congruences en divisant est très dangereux et peut donner lieu à des raisonnements totalement faux ! C'est pourquoi, il ne faut jamais le faire ! Par contre, on peut multiplier à gauche et à droite par un inverse d'un entier modulo un autre entier en justifiant bien pourquoi cet inverse existe avant de faire la multiplication !

Intéressons-nous maintenant aux systèmes de congruences, par exemple, au système suivant :
$$(S) \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}.$$
Résolvons ce système : la première équation nous donne l'existence d'un entier k tel que : $x = 5k + 3$ et avec la seconde équation, on doit avoir : $5k \equiv 2 \pmod{7}$.
Comme 5 et 7 sont premiers entre eux, 5 admet un inverse modulo 7 et un inverse de 5 modulo 7 est 3 donc en multipliant par 3, on obtient : $k \equiv 6 \pmod{7}$ donc il existe un entier k' tel que : $k = 7k' + 6$ et on a alors : $x = 5(7k' + 6) + 3 = 35k' + 33$. On vérifie, réciproquement

que les entiers de la forme : $35k' + 33$, avec $k' \in \mathbb{Z}$ sont bien solutions du système (S).

En réalité, derrière cet exemple se cache un théorème qui donne une méthode générale pour trouver les solutions d'un tel système. Ce théorème est le théorème des restes chinois.

Théorème des restes chinois. Soient $m_1, m_2, ..., m_k$ des entiers strictement positifs deux à deux premiers entre eux et $a_1, a_2, ..., a_k$ des entiers quelconques. Alors, il existe un entier a tel que le système de congruences : $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$ soit équivalent à la simple congruence : $x \equiv a \pmod{m_1...m_k}$. En particulier, le système précédent possède au moins une solution.

Démonstration dans le cas : $k = 2$. Démontrons le théorème dans le cas $k = 2$. (Une récurrence permet de le démontrer dans le cas général).
On veut résoudre le système suivant : $(S) \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$. Supposons que x soit solution du système (S) alors la première équation nous donne l'existence d'un entier k tel que $x = km_1 + a_1$ et la seconde congruence s'écrit alors : $a_1 + km_1 \equiv a_2 \pmod{m_2}$ i.e : $k \equiv (a_2 - a_1)m_1' \pmod{m_2}$ où m_1' désigne un inverse de m_1 modulo m_2 et m_1' existe car m_1 et m_2 sont premiers entre eux. Ainsi, si l'on pose : $a = (a_2 - a_1)m_1m_1' + a_1$, on a bien : $x \equiv a \pmod{m_1m_2}$.
Réciproquement, si $x \equiv a \pmod{m_1m_2}$ avec $a = (a_2 - a_1)m_1m_1' + a_1$, on a bien : $x \equiv a_1 \pmod{m_1}$ et $x \equiv a_2 \pmod{m_2}$.

Remarque. La preuve fournit un moyen de trouver a. On peut remarquer qu'en fait, pour avoir a, il suffit de trouver une relation de Bézout entre les entiers m_1 et m_2 qui sont premiers entre eux. En effet, on peut écrire qu'il existe deux entiers u et v tels que : $m_1u + m_2v = 1$ donc u est un inverse de m_1 modulo m_2. On peut alors poser : $a = (a_2 - a_1)m_1u + a_1 = a_2m_1u + a_1(1 - m_1u) = a_2m_1u + a_1m_2v$. Il suffit alors de trouver u et v pour trouver a (les u et v proviennent de notre relation de Bézout) et pour trouver une relation de Bézout entre m_1 et m_2, on peut appliquer l'algorithme d'Euclide (ou la "voir" directement) !

On peut appliquer cette méthode dans l'exemple précédent. Revenons alors au système : $(S) \begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$.
On veut trouver a tel que : $x \equiv a \pmod{5 \times 7}$. On sait que $a_1 = 3$, $a_2 = 5$, $m_1 = 5$ et $m_2 = 7$. Comme 5 et 7 sont premiers entre eux, on peut trouver une relation de Bézout (de la forme : $5u+7v = 1$) entre 5 et 7. Par exemple : $5\times3+7\times(-2) = 1$ est une relation de Bézout entre 5 et 7. On a : $a = a_2m_1u + a_1m_2v$ avec $u = 3$ et $v = -2$ donc $a = 5 \times 5 \times 3 + 3 \times 7 \times (-2) = 33$. Ainsi, on trouve : $x \equiv 33 \pmod{35}$, ce qui est cohérent avec ce que nous avions trouvé précédemment !
En fait, le théorème des restes chinois peut être énoncé de manière différente : on peut rajouter

l'unicité de la solution du système, modulo $m_1...m_k$.

Exercice 10. Un phare émet un signal jaune toutes les 15 secondes et un signal rouge toutes les 28 secondes. On aperçoit le signal jaune 2 secondes après minuit et le rouge 8 secondes après minuit. A quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

Solution de l'exercice 10. On commence par mettre en équation le problème. On note x les temps, en secondes, depuis minuit, où les deux phares sont allumés au même moment. A l'aide des données du problème, on peut dire que x est solution du système : $(S)\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 8 \pmod{28} \end{cases}$.
On cherche le plus petit entier naturel x solution de ce système. On remarque que 15 et 28 sont premiers entre eux. On peut alors appliquer la méthode donnée par la remarque précédente pour trouver les solutions de ce système. Cherchons alors une relation de Bézout entre 15 et 28.
On a : $28 = 15 \times 1 + 13 \quad ; \quad 15 = 13 \times 1 + 2 \quad ; \quad 13 = 2 \times 6 + 1.$
En remontant les calculs, on obtient :
$1 = 13 - 2 \times 6 = 13 - 6 \times (15 - 13) = -6 \times 15 + 7 \times 13 = -6 \times 15 + 7(28 - 15) = -13 \times 15 + 7 \times 28.$
Ainsi, la relation : $-13 \times 15 + 7 \times 28 = 1$ est une relation de Bézout entre 15 et 28. On pose alors (comme pour la remarque précédente) : $a_1 = 2$, $a_2 = 8$, $m_1 = 15$, $m_2 = 28$, $u = -13$ et $v = 7$. On calcule alors $a = (a_2 - a_1)m_1u + a_1 = a_2m_1u + a_1m_2v = (8-2) \times 15 \times (-13) + 2 = -1168$ et on peut déduire que $x \equiv a \pmod{m_1m_2}$ (i.e : $x \equiv -1168 \pmod{15 \times 28}$). Ainsi, $x \equiv -1168 \pmod{420}$. Les solutions de ce système sont alors les entiers congrus à -1168 modulo 420, c'est-à-dire les entiers de la forme : $420k - 1168$, $k \in \mathbb{Z}$. On cherche le plus petit entier naturel qui est solution de ce système. Pour $k = 2$, $420k - 1168 < 0$ mais pour $k = 3$, $420k - 1168 > 0$ et on a : $420 \times 3 - 1168 = 92$. Donc le plus petit entier naturel solution de ce système est 92.
Ainsi, les deux phares seront allumés au même moment, pour la première fois, 1 minute et 32 secondes après minuit.