Une application des congruences : l'exponentiation modulaire

Plantons le décor

On se place dans l'ensemble **Z** des entiers relatifs. Soit n un entier naturel strictement positif.

Définition de la congruence modulo n :
Deux entiers a et b ont même reste dans la division euclidienne par n si et seulement si $a-b$ est un multiple de n. Dans ce cas, on dit que a est congru à b modulo n et on écrit : $a \equiv b \ (n)$.

Une caractérisation de la congruence modulo n :
Soit a et b deux entiers relatifs ; a est congru à b modulo n si et seulement il existe un entier relatif k tel que : $b = a + k\,n$.

Ensemble des entiers congrus à un entier a donné :
Le nombre entier a étant fixé et r étant le reste de la division euclidienne de a par n, l'ensemble des nombres entiers x qui sont congrus à a modulo n est l'ensemble des entiers relatifs x de la forme : $x = r + k\,n$ où k est un entier relatif. En particulier, r est l'unique nombre entier vérifiant à la fois : $\begin{cases} r \equiv a \ (n) \\ 0 \le r \le n-1 \end{cases}$.

La congruence est une relation d'équivalence compatible avec l'addition et la multiplication des entiers relatifs ainsi qu'avec l'élévation à une puissance strictement positive (c'est-à-dire que $a \equiv b \ (n)$ implique que $a^p \equiv b^p \ (n)$ pour tout entier p strictement positif).

Traduction à l'aide d'une congruence du théorème de Bézout
Soit n un entier naturel strictement positif et a un entier relatif. Les entiers a et n sont premiers entre eux si et seulement si il existe un entier relatif u tel que : $a\,u \equiv 1 \ (n)$

1. Le sujet

Soit a et n deux entiers strictement supérieurs à 1.

On considère la suite $(r_p)_{p\in N}$ telle que, pour tout entier positif p, r_p est le reste de la division euclidienne de a^p par n.

C'est-à-dire que r_p est défini de la manière suivante : $\begin{cases} a^p \equiv r_p \ (n) \\ 0 \le r_p \le n-1 \end{cases}$

Les deux premiers termes de cette suite sont $r_0 = 1$; $r_1 = r$.

Les termes de cette suite satisfont la relation de récurrence : $\begin{cases} r_{p+1} \equiv a \times r_p \ (n) \\ 0 \le r_{p+1} \le n-1 \end{cases}$.

1. Justifier que, parmi les termes de l'ensemble $\{r_0, r_1, ..., r_n\}$, deux au moins sont égaux.

2. On note respectivement u et $u+q$ les indices des deux premiers termes égaux : r_u et r_{u+q}. Montrer que , à partir du rang u, la suite $(r_p)_{p\in N}$ est une suite périodique de période q.

Déterminer, à titre d'exemple, les entiers u et q lorsque $a = 2$; $n = 24$.

3. Un théorème d'Euler et ce qu'il s'ensuit.

Soit n un entier strictement positif. On désigne par $\phi(n)$ (fonction indicatrice d'Euler) le nombre d'entiers u vérifiant $1 \le u \le n$ et qui sont premiers avec n.

On désigne par $U_n = \{u_1, u_2, ..., u_{\phi(n)}\}$ l'ensemble de ces entiers.

(Par exemple : $U_{10} = \{1, 3, 7, 9\}$ et $\phi(10) = 4$)

3.1. Soit a un entier premier avec n. Pour tout entier k tel que $1 \le k \le \phi(n)$, on désigne par v_k l'unique entier défini par : $\begin{cases} v_k \equiv a \times u_k \ (n) \\ 0 \le v_k \le n-1 \end{cases}$ et on désigne par V_n l'ensemble : $V_n = \{v_1, v_2, ..., v_{\phi(n)}\}$.

Montrer que $V_n = U_n$

Dans cette question, on se propose de montrer que, si a est premier avec n, alors il existe un entier $q > 0$ tel que $r_q = 1$ et que la suite $(r_p)_{p\in N}$ est périodique dès son rang zéro.

3. Un théorème d'Euler et ce qu'il s'ensuit.

Soit n un entier strictement positif. On désigne par $\phi(n)$ (fonction indicatrice d'Euler) le nombre d'entiers u vérifiant $1 \le u \le n$ et qui sont premiers avec n.

On désigne par $U_n = \{u_1, u_2, ..., u_{\phi(n)}\}$ l'ensemble de ces entiers compris entre 1 et n et qui sont premiers avec n. Cet ensemble est non vide car il contient au moins l'entier 1 et, si $n > 1$, il contient aussi l'entier $n-1$.

3.1. Soit a un entier premier avec n. Pour tout entier k tel que $1 \le k \le \phi(n)$, on désigne par v_k l'unique entier défini par : $\begin{cases} v_k \equiv a \times u_k \ (n) \\ 0 \le v_k \le n-1 \end{cases}$ et on désigne par V_n l'ensemble : $V_n = \{v_1, v_2, ..., v_{\phi(n)}\}$.

Montrer que $V_n \subset U_n$

3.2. Supposons qu'il existe deux entiers k et k' tous deux compris entre 1 et $\phi(n)$ et tels que $v_k = v_{k'}$. Montrer qu'alors : $k = k'$. En déduire que : $V_n = U_n$.

3.3. En comparant modulo n les deux produit d'entiers $\prod_{k=1}^{k=\phi(n)} a \times u_k$ et $\prod_{k=1}^{k=\phi(n)} u_k$, montrer que $a^{\phi(n)} \equiv 1 \ (n)$

Ce qui constitue le théorème d'Euler.

En déduire que, si a est premier avec n, la suite $(r_p)_{p \in N}$ est périodique dès son terme de rang zéro.

4. Application :

On élève le nombre 2021 aux puissances 1515, 1789, 2021 ou 4444. On obtient ainsi quatre nombres entiers. Quel est le reste de la division par 17 de chacun de ces quatre nombres ?

NB. Une application « classique » de l'exponentiation modulaire est la justification de critères de divisibilité (par 3, 9, ou 11 en numération décimale notamment).

2. Eléments de correction

1. Par construction de la suite en question, pour tout entier naturel p : $0 \le r_p \le n-1$ c'est-à-dire que l'application $p \in \mathbf{N} \mapsto f(p) = r_p$ a pour ensemble-image un ensemble inclus dans l'ensemble $\{0, 1, ..., n-1\}$ qui a pour cardinal *n*.

L'ensemble $\{0, 1, ..., n\}$ a pour cardinal $n+1$ donc un cardinal strictement supérieur à celui de ensemble-image. La restriction de *f* à cet ensemble ne peut pas être injective : au moins deux entiers parmi $\{0, 1, ..., n\}$ ont la même image par *f*.

Parmi les termes de l'ensemble $\{r_0, r_1, ..., r_n\}$, deux au moins sont égaux.

On note *u* et $u+q$ les deux premiers indices pour lesquels une telle égalité se produit.

2. Montrons par récurrence que, pour tout entier *p* supérieur ou égal à *u* : $r_{p+q} = r_p$.

- Par définition des deux indices *u* et $u+q$, l'égalité est vérifiée lorsque $p = u$.
- Supposons que $r_{p+q} = r_p$ soit vérifiée pour un certain entier *p*.

Alors : $\begin{cases} r_{p+q+1} \equiv a \times r_{p+q} \equiv a \times r_p \equiv r_{p+1} \ (n) \\ 0 \le r_{p+q+1} \le n-1 \end{cases}$ (*abus assumé de congruences en chapelet …*)

Ainsi : $\begin{cases} r_{p+q+1} \equiv r_{p+1} \ (n) \\ 0 \le r_{p+q+1} \le n-1 \\ 0 \le r_{p+1} \le n-1 \end{cases}$. Par unicité dans un intervalle de longueur *n* d'un nombre entier congru à un nombre donné modulo *n* : $r_{p+q+1} = r_q$, l'égalité est héréditaire.

On peut conclure que tout entier *p* supérieur ou égal à *u* : $r_{p+q} = r_p$; à partir du rang *u*, la suite $(r_p)_{p \in N}$ est une suite périodique de période *q*.

Par exemple, pour $a = 2$; $n = 24$, on vérifie que $u = 3$; $q = 2$ car $r_5 = r_3 = 8$

3. Un théorème d'Euler et ce qu'il s'ensuit.

Soit *n* un entier strictement positif. On désigne par $\phi(n)$ (fonction indicatrice d'Euler) le nombre d'entiers *u* vérifiant $1 \le u \le n$ et qui sont premiers avec *n*.

On désigne par $U_n = \{u_1, u_2, ..., u_{\phi(n)}\}$ l'ensemble de ces entiers compris entre 1 et *n* et qui sont premiers avec *n*. Cet ensemble est non vide car il contient au moins l'entier 1 et, si $n > 1$, il contient aussi l'entier $n-1$.

3.1. Soit *a* un entier premier avec *n*. Pour tout entier *k* tel que $1 \le k \le \phi(n)$, on désigne par v_k l'unique entier défini par : $\begin{cases} v_k \equiv a \times u_k \ (n) \\ 0 \le v_k \le n-1 \end{cases}$ et on désigne par V_n l'ensemble : $V_n = \{v_1, v_2, ..., v_{\phi(n)}\}$.

Montrer que $V_n = U_n$

On sait que le produit de deux entiers premiers avec un entier donné *n* est lui-même un entier premier avec *n*.

Pour tout entier *k* tel que $1 \le k \le \phi(n)$, l'entier $a \times u_k$ est un entier premier avec *n* .

On sait que, si l'on ajoute ou si l'on retranche un multiple de *n* à un nombre premier avec *n*, le nombre obtenu est lui aussi premier avec *n*. L'entier v_k est congru à $a \times u_k$ modulo *n* donc il diffère de $a \times u_k$ d'un multiple de *n* : il est premier avec *n*. De plus, il est compris entre 1 et *n* : v_k appartient à U_n.

En conclusion : $V_n \subset U_n$.

3.2. Supposons qu'il existe deux entiers k et k' tous deux compris entre 1 et $\phi(n)$ et tels que $v_k = v_{k'}$. Alors, d'après la définition de ces entiers : $a \times u_k \equiv a \times u_{k'} \ (n)$. Mais les entiers a et n étant premiers entre eux, il existe un entier relatif u tel que $u\,a \equiv 1 \ (n)$. Alors la congruence $a \times u_k \equiv a \times u_{k'} \ (n)$ implique que : $u\,a \times u_k \equiv u\,a \times u_{k'} \ (n)$ c'est-à-dire : $u_k \equiv u_{k'} \ (n)$.

Or, u_k et $u_{k'}$ étant tous deux compris entre 1 et n, ils ne peuvent être congrus modulo n que s'ils sont égaux. Nécessairement $u_k = u_{k'}$ et en conséquence, $k = k'$.

Ainsi : $v_k = v_{k'} \Rightarrow k = k'$. Les éléments de V_n sont tous distincts. L'ensemble V_n a $\phi(n)$ éléments, le même nombre d'éléments que U_n.
En conclusion : $V_n = U_n$.

3.3. D'une part : $\prod_{k=1}^{k=\phi(n)} a \times u_k = a^{\phi(n)} \prod_{k=1}^{k=\phi(n)} u_k$

D'autre part : $\prod_{k=1}^{k=\phi(n)} a \times u_k \equiv \prod_{k=1}^{k=\phi(n)} v_k \ \ (n)$. Mais puisque $V_n = U_n$, $\prod_{k=1}^{k=\phi(n)} u_k \equiv \prod_{k=1}^{k=\phi(n)} v_k$, car il s'agit du produit des mêmes entiers. Donc $\prod_{k=1}^{k=\phi(n)} u_k \equiv a^{\phi(n)} \times \prod_{k=1}^{k=\phi(n)} u_k \ \ (n)$.

Mais $\prod_{k=1}^{k=\phi(n)} u_k$ est un nombre entier premier avec n, car produit d'entiers premiers avec n. Il existe un entier relatif x tel que : $x \times \prod_{k=1}^{k=\phi(n)} u_k \equiv 1 \ (n)$

En multipliant par x la congruence précédente : $a^{\phi(n)} \equiv 1 \ \ (n)$

Il en résulte que $r_{\phi(n)} = 1$

Ce qui constitue le théorème d'Euler.

On en déduit que, si a est premier avec n, il existe au moins un entier q plus petit que n tel que $r_q = 1 = r_0$.

Si q est le plus petit de ces entiers, il ne peut pas y avoir de période plus courte car s'il existait deux restes de rangs strictement intermédiaires u et $u+q$ donnant un même reste, la périodicité à partir du rang u interdirait que l'on retrouve 1 comme reste.

La suite $(r_p)_{p \in N}$ est périodique dès son terme de rang zéro et non plus « à partir d'un certain rang ».

Résolution de l'exemple proposé

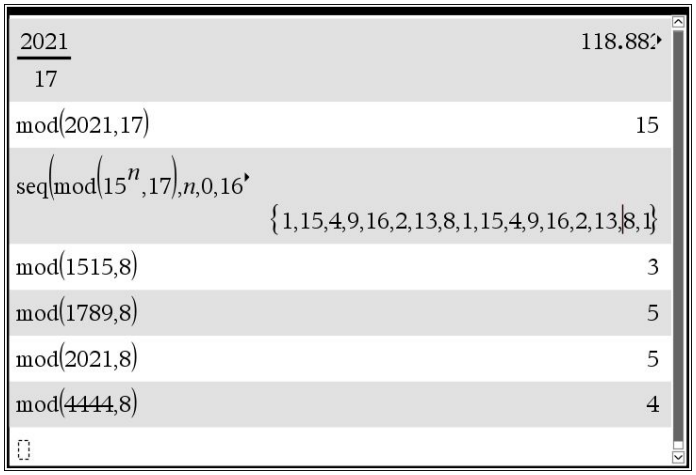
Recherche des restes des la divisions euclidiennes de 2021^{1515}, 2021^{1789}, 2021^{2021}, 2021^{4444} par 17

La division euclidienne de 2021 par 17 s'écrit : $2021 = 118 \times 17 + 15$.
Ainsi : $2021 \equiv 15 \ (17)$ et pour tout entier n : $2021^n \equiv 15^n \ (17)$.

Il y a 16 diviseurs entre 1 et 17 qui sont premiers avec 17.

L'entier 15 étant premier avec 17, d'après le théorème d'Euler, il y a au moins un entier n entre 1 et 16 tel que $15^n \equiv 1 \ (17)$.

L'examen des premières puissances de 15 modulo 17 montre que 8 est le plus petit entier ayant cette propriété.



Dès lors que $2021^8 \equiv 15^8 \equiv 1 \ (17)$, pour tout entier naturel k : $2021^{8k} \equiv 15^{8k} \equiv 1 \ (17)$
La suite des restes des divisions par 17 des puissances de 15 est donc une suite périodique de période 8.
Suivant qu'un entier n est congru modulo 8 à 0, 1, 2, 3, 4, 5, 6 ou 7, le reste de la division euclidienne de 15^n par 17 est 1, 15, 4, 9, 16, 2, 13 ou 8 (dans l'ordre respectif).

Or, modulo 8, les entiers 1515, 1789, 2021 et 4444 sont congrus respectivement à 3, 5, 5 et 4.
Le reste des divisions euclidiennes de 2021^{1515}, 2021^{1789}, 2021^{2021}, 2021^{4444} par 17 sont, respectivement, 9, 2, 2 et 16.

Une autre application des congruences : Le théorème des restes chinois

Quasiment le même décor

On se place dans l'ensemble **Z** des entiers relatifs.

« Théorème des restes chinois », version congruences.

Théorème
Soit m et n deux entiers strictement positifs et premiers entre eux.
Soit a et b deux entiers relatifs quelconques.

- Alors le système (S) des deux congruences $\begin{cases} x \equiv a \ \ (m) \\ x \equiv b \ \ (n) \end{cases}$ d'inconnue entière relative admet toujours au moins une solution.
- Le système (S) admet un entier relatif solution et un seul x_0 tel que : $0 \leq x_0 < m \times n$
- L'ensemble des entiers relatifs solutions de (S) est l'ensemble : $\{x_0 + k \times m \times n \quad k \in \mathbf{Z}\}$

Ce théorème est susceptible de généralisation à plusieurs entiers premiers entre eux deux à deux.

Nous allons voir ce théorème à l'œuvre dans un sujet de baccalauréat : sujet national, 2006.

Ce sujet propose une « démonstration » sur un exemple du théorème, mais on remarquera que cette « démonstration » est téléguidée par l'auteur du sujet.

C'est ce qu'on peut appeler un « sujet IKEA ». Il y a une notice de montage, et cela est assez fréquent dans les sujets de baccalauréat.

Travailler sur de tels sujets, c'est très intéressant pour les candidats au CAPES car il leur appartient de remettre en place la logique d'une démonstration (distinguer le pourquoi alors qu'on dispose du comment).

Je reproduis tout le sujet, y compris la question de cours que je ne corrige pas.

Partie A : Question de cours
1. Énoncer le théorème de Bézout et le théorème de Gauss.

2. Démontrer le théorème de Gauss en utilisant le théorème de Bézout.

Partie B
Il s'agit de résoudre dans **Z** le système (S) : $\begin{cases} n \equiv 13 \ \ (19) \\ n \equiv 6 \ \ \ (12) \end{cases}$

1. Démontrer qu'il existe un couple (u, v) d'entiers relatifs tel que: $19u + 12v = 1$.
(On ne demande pas dans cette question de donner un exemple d'un tel couple).
Vérifier que, pour un tel couple, le nombre $N = 13\times12v + 6\times19u$ est une solution de (S).

2. Soit n_0 une solution de (S).
2.1. Vérifier que le système (S) équivaut à : $\begin{cases} n \equiv n_0 \ \ (19) \\ n \equiv n_0 \ \ \ (12) \end{cases}$
2.2. Démontrer que le système : $\begin{cases} n \equiv n_0 \ \ (19) \\ n \equiv n_0 \ \ \ (12) \end{cases}$ équivaut à : $n \equiv n_0 \ \ (12\times19)$

3.1. Trouver un couple (u, v) solution de l'équation $19u + 12v = 1$ et calculer la valeur de N correspondante.
3.2. Déterminer l'ensemble des solutions de (S).

4. Un entier naturel n est tel que lorsqu'on le divise par 12 le reste est 6 et lorsqu'on le divise par 19 le reste est 13.
On divise n par $228 = 12\times19$. Quel est le reste r de cette division ?

Eléments de correction

Correction de la partie B
Il s'agit de résoudre dans **Z** le système (S) : $\begin{cases} n \equiv 13 \ \ (19) \\ n \equiv 6 \ \ \ (12) \end{cases}$

1. Les entiers 19 et 12 sont des entiers premiers entre eux. D'après le théorème de Bézout, il existe un couple (u, v) d'entiers relatifs tel que: $19u + 12v = 1$

Si $N = 13\times12v + 6\times19u$
- D'une part $N = 13\times(1-19u) + 6\times19u = 13 - 7\times19u$ donc $N \equiv 13 \ \ (19)$ car la différence $N - 13$ est un multiple de 19.
- D'autre part $N = 13\times12v + 6\times(1-12v) = 6 + 7\times12v$ donc $N \equiv 6 \ \ (12)$ car la différence $N - 6$ est un multiple de 12.

N est une solution de (S).

2. Soit n_0 une solution de (S).

2.1. Le système (S) équivaut à : $\begin{cases} n \equiv n_0 \quad (19) \\ n \equiv n_0 \quad (12) \end{cases}$ en raison de la transitivité de la relation de congruence.

En effet, les trois congruences même modulo $a \equiv b\ (m)$; $b \equiv c\ (m)$; $c \equiv a\ (m)$ sont toutes vérifiées si et seulement si deux quelconques d'entre elles le sont. On applique cette transitivité pour *n,* n_0 et 13 modulo 19 puis *n,* n_0 et 6 modulo 12.

2.2. D'une part, $n \equiv n_0 \ (19)$ si et seulement si $n - n_0$ est un multiple de 19.

D'autre part, $n \equiv n_0 \ (12)$ si et seulement si $n - n_0$ est un multiple de 12.

Les deux congruences : $\begin{cases} n \equiv n_0 \quad (19) \\ n \equiv n_0 \quad (12) \end{cases}$ sont simultanément vérifiées si et seulement si $n - n_0$ est un multiple à la fois de 12 et de 19, c'est-à-dire est un multiple de leur PPCM. Or, les entiers 12 et 19 sont premiers entre eux : leur PPCM est égal à leur produit.

Les deux congruences : $\begin{cases} n \equiv n_0 \quad (19) \\ n \equiv n_0 \quad (12) \end{cases}$ sont simultanément vérifiées si et seulement si $n - n_0$ est un multiple de 12×19, ce qui équivaut à : $n \equiv n_0 \quad (12 \times 19)$

3.1. En considérant l'algorithme d'Euclide : $\begin{cases} 19 = 12 + 7 \\ 12 = 7 + 5 \\ 7 = 5 + 2 \\ 5 = 2 \times 2 + 1 \end{cases}$ on obtient :

$$\begin{cases} 7 = 19 - 12 \\ 5 = 12 - (19 - 12) = 2 \times 12 - 19 \\ 2 = 7 - 5 = (19 - 12) - (2 \times 12 - 19) = 2 \times 19 - 3 \times 12 \\ 1 = 5 - 2 \times 2 = (2 \times 12 - 19) - 2 \times (2 \times 19 - 3 \times 12) = 8 \times 12 - 5 \times 19 \end{cases}.$$

On en déduit que le couple $(-5,\ 8)$ est une solution particulière de l'équation $19u + 12v = 1$ et la valeur de N correspondante est : $N = 13 \times 12 \times 8 + 6 \times 19 \times (-5) = 678$

3.2. En vertu de la question **2.2**, l'ensemble des solutions de (S) est l'ensemble des entiers relatifs de la forme $n = 678 + 12 \times 19\,k = 678 + 228\,k$ où k est un entier relatif.

4. Si un entier naturel *n* est tel que lorsqu'on le divise par 12 le reste est 6 et lorsqu'on le divise par 19 le reste est 13, il s'agit d'une solution du système précédent. Il est de la forme $n = 678 + 12 \times 19\,k = 678 + 228\,k$ où k est un entier relatif. Il est congru à 678 modulo 228.

Le reste de sa division euclidienne par 228 est le même que le reste de la division euclidienne de 678 par 228. Or : $678 = 2 \times 228 + 222$.

Le reste *r* de cette division est l'entier 222.

Démonstration du théorème dans le cas général

D'une part : $x \equiv a \ (m) \Leftrightarrow (\exists\, u \in \mathbf{Z}) : x = a + u \times m$

D'autre part : $x \equiv b \ (n) \Leftrightarrow (\exists\, v \in \mathbf{Z}) : x = b + v \times n$

Un entier x conforme aux exigences existe si on peut trouver deux entiers relatifs u et v tels que : $a + u \times m = b + v \times n$, c'est-à-dire tels que : $u \times m - v \times n = b - a$.

Nous sommes amenés à la résolution de l'équation diophantienne d'inconnues entières relatives u et v : $u \times m - v \times n = b - a$

Les entiers m et n étant supposés premiers entre eux, ils vérifient la relation de Bézout, relation qui garantit l'existence de deux entiers relatifs p et q vérifiant : $p \times m - q \times n = 1$.

Les entiers $u = p(b-a)$ et $v = q(b-a)$ vérifient les conditions requises et le nombre entier $x_0 = a + p(b-a) \times m$ vérifie bien le système de deux congruences

(On note que $x_0 = a + p(b-a)m = a + (1 - q\,n)(b-a) = -q(b-a)n + b$).

Dés lors : $\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$ équivaut à $\begin{cases} x - x_0 \equiv 0 \ (m) \\ x - x_0 \equiv 0 \ (n) \end{cases}$, ce qui équivaut au fait que $(x - x_0)$ est un multiple commun de m et de n (donc de leur PPCM).

Les deux entiers m et n étant supposés premiers entre eux, leur PPCMN est égal à leur produit

$\begin{cases} x \equiv a \ (m) \\ x \equiv b \ (n) \end{cases}$ équivaut au fait qu'il existe un entier relatif k : $x = x_0 + k\,m\,n$.

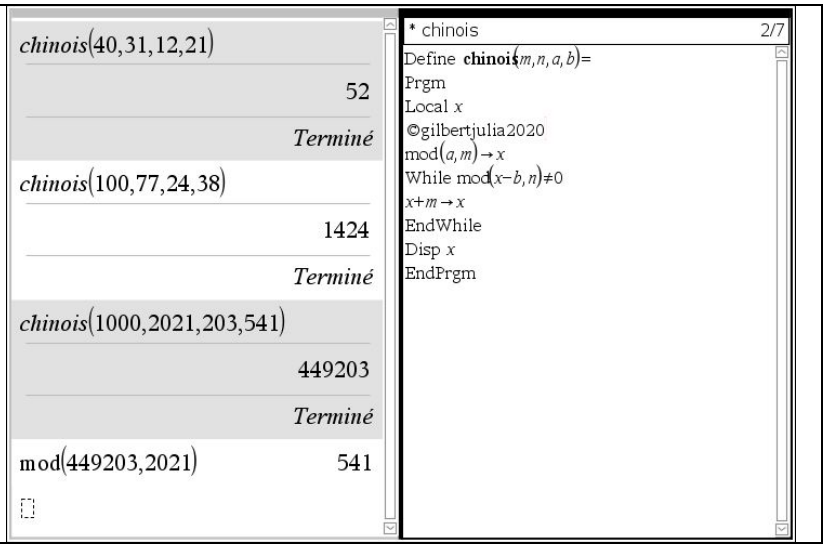
Les nombres solutions se déduisent d'une solution particulière en ajoutant ou en retranchant un multiple du nombre *m.n.* l'écart entre deux solutions consécutives est égal à $m \times n$.

Or, tout intervalle de la forme $[\alpha,\ \alpha \pm m \times n[$ contient exactement un nombre de cette forme Il y a une solution et une seule dans $[0,\ m \times n[$ (on va noter x_1 cette solution).

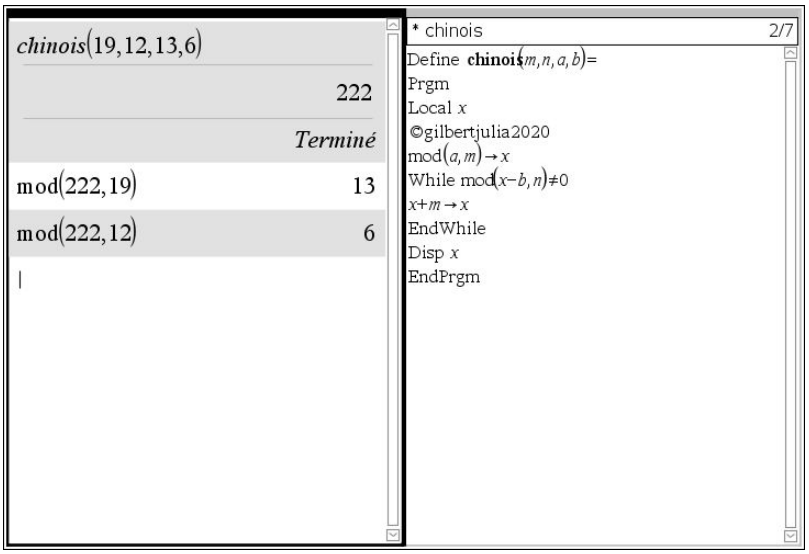
L'ensemble des solutions est l'ensemble des nombres entiers de la forme $x = x_1 + k\,m\,n$

Une programmation pour obtenir une solution particulière

Le programme **chinois** ci-contre exploite la certitude de trouver une solution entre 0 et *mn*.
Il parcourt les entiers congrus à *a* modulo *m* à partir du premier entier positif ayant cette propriété et cela jusqu'à trouver un entier qui est congru aussi à *b* modulo *n*.



Si on applique ce programme à l'exemple du bac national 2006, nous obtenons 222 comme solution particulière du système de congruences.
L'ensemble des solutions est l'ensemble des entiers de la forme $222+228k$ où k est un entier relatif.
De ce fait, $\begin{cases} n \equiv 13 \quad (19) \\ n \equiv 6 \quad (12) \end{cases}$ équivaut à $n \equiv 222 \quad (12\times 19)$. Or, 222 est l'unique entier parmi ceux de la forme $222+228k$ qui est entre 0 et 227 : parmi ces nombres, c'est le seul à être le reste d'une division euclidienne par 228.



Un entier a pour reste 6 dans la division par 12 et 13 dans sa division par 19 si et seulement le reste est 222 dans sa division par 228.