Proposition 1. (Le théorème chinois des restes.)

. $m_1, m_2, m_3, ..., m_n$ sont n entiers supérieurs ou égaux à 2, premiers entre eux deux à deux.

. $a_1, a_2, a_3, ..., a_n$ sont n entiers relatifs quelconques.

. Le système de congruences : $\begin{cases} x \equiv a_1 \,[m_1] \\ x \equiv a_2 \,[m_2] \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \,[m_n] \end{cases}$ admet une unique solution modulo $m_1 m_2 m_3 .... m_n$.

Remarque. "*admet une unique solution modulo* $m_1 m_2 m_3 .... m_n$" signifie que si x_0 est une solution du système, alors toutes les autres solutions lui sont congrues modulo $m_1 m_2 m_3 ... m_n$, i.e. sont de la forme $x_0 + k m_1 m_2 m_3 ... m_n$, où k décrit $\mathbb{Z}$.

Note historique.

1. La première formulation connue de ce théorème apparaît dans le *Jiuzhang suanshu* [l'Art du calcul en neuf chapitres], ouvrage anonyme de l'époque des Han (206 avant notre ère à 220 après). Ce texte est le grand classique des mathématiques chinoises. Il fut commenté et complété par les mathématiciens Liu Hui (fin du III^e siècle de notre ère), Zu Chongzhi (V^e siècle) et Li Chunfeng (VII^e siècle) : plus précisément, ceux-ci fournirent les démonstrations prouvant les procédés présentés sans justification dans l'ouvrage original. Il sera utilisé jusqu'au XVII^e siècle comme manuel d'enseignement en Chine. Voici comment ce traité présente notre théorème : "*Nous avons des choses dont nous ne connaissons pas le nombre, mais :*

- *si nous les comptons par paquets de trois, il en reste deux ;*
- *si nous les comptons par paquets de cinq, il en reste trois ;*
- *si nous les comptons par paquets de sept, il en reste deux.*

Combien y a-t-il de choses ? Réponse : 23."

Suit une méthode de résolution en deux parties dont la formulation est algorithmique et la portée limitée au cas où l'on compte par paquets de trois, cinq et sept.

Dans le langage des congruences ce problème s'énonce : quel est l'entier naturel *n* vérifiant : $n \equiv 2\,[3]$, $n \equiv 3\,[5]$ et $n \equiv 2\,[7]$?

Nous verrons que la solution donnée ci-dessus est la plus petite, mais non la seule.

2. On trouve dans l'*Introduction à l'Arithmétique* de Nicomaque de Gérase, vers l'an 100 de notre ère, un problème numérique du même genre, accompagné d'une solution comme on en rencontre dans les manuscrits chinois de l'époque : il semble que Nicomaque a repris des connaissances qui avaient diffusé en Occident depuis la Chine.

3. À l'époque de la dynastie des Song du Sud, le problème des restes réapparut. Qin Jiushao publia en 1247 le *Shushu jiuzhang*

[Écrits mathématiques en neuf chapitres], présenté par d'aucuns comme le sommet des mathématiques chinoises classiques. Ce livre contient un algorithme général de résolution de congruences simultanées ayant des modules quelconques, non nécessairement premiers entre eux (le "*théorème chinois des restes*" généralisé).

4. À peu près à la même époque, Léonard de Pise, alias Leonardo Fibonacci, traitait de ce problème dans son *Liber abaci* avec une formulation très proche de celle des origines (*cf.* **1.** ci-dessus), mais sur un mode ludique qui a persisté pendant des années dans la littérature mathématique (*cf.* le fameux *Récréations mathématiques et problèmes des temps anciens et modernes* de W.W. Rouse Ball, page 65 de la deuxième édition française, traduite par J. Fitz-Patrick.).

5. Toujours la même chose, mais cinq siècles plus tard, sous la plume du grand Leonhard Euler (*Commentarii Academiae Scientarum Petropolitanae*, 7 (1734-1735)) :

"On doit trouver un nombre qui, lorsqu'il est divisé par a, b, c, d, e, nombres que je suppose relativement premiers, conduit respectivement aux restes p, q, r, s, t. Pour ce problème les nombres suivants satisfont à :

$Ap + Bq + Cr + Ds + Et = m \times abcde$ où A est un nombre qui divisé par $bcde$ n'a pas de reste, toutefois, divisé par a, a le reste 1 ; B est un nombre qui divisé par $acde$ n'a pas de reste, toutefois, divisé par b, a le reste 1… lesquels nombres peuvent par conséquent être trouvés par la règle donnée pour deux diviseurs."

6. Puis vint Carl Friedrich Gauss avec la terminologie et la notation des congruences… avant d'attaquer le système de congruences de la proposition 1, nous allons étudier <u>en détail</u> les équations de la forme $ax \equiv b\,[m]$: autrement dit, *a*, *b* et *m* étant des entiers relatifs donnés, avec $m \geq 2$, nous allons nous demander :

i) À quelle(s) condition(s), portant évidemment sur *a*, *b* et *m*, existe-t-il des entiers *x* tels que $ax \equiv b\,[m]$?

ii) Et, quand il en existe, quelle est leur forme ? Combien y en a-t-il ?

Les deux exemples qui suivent contiennent des indications à ce sujet.

Exemple 1 : $2x \equiv 3[6]$.

Chercher toutes les solutions de cette équation revient à chercher tous les couples (x,k) tels que $2x-6k=3$. Il n'y en a aucun car $PGCD(2,6)=2$ ne divise pas 3. Ainsi apparaît une condition nécessaire pour que l'équation $ax \equiv b[m]$ ait des solutions : $PGCD(a,m)$ divise b. Nous verrons dans la proposition 2 qu'elle est aussi suffisante.

Exemple 2 : (e) : $3x \equiv 6[15]$.

On a : $3x \equiv 6[15] \Leftrightarrow \exists k \in \mathbb{Z}; 3x = 6+15k \Leftrightarrow \exists k \in \mathbb{Z}; x = 2+5k$.

Les solutions de (e) sont donc les entiers de la forme $2+5k$, où k décrit $\mathbb{Z}$. Remarquons que pour connaître toutes les solutions, il nous suffit de connaître celles de l'intervalle $[\![0,14]\!]$, à savoir : 2, 7 et 12 ; toutes les autres étant congrues à celles-là modulo 15, i.e. étant de la forme $2+15K$, $7+15K$ et $12+15K$, K décrivant $\mathbb{Z}$.

Cela explique pourquoi, pour les équations du type $ax \equiv b[m]$, on entend souvent par solutions celles de l'intervalle $[\![0,m-1]\!]$.

Ainsi, on dira que (e) admet trois solutions, en précisant éventuellement : définies à une congruence modulo 15 près.

Notons enfin que le nombre de solutions de (e) est le *PGCD* de a et de m. Précisons tout cela :

Proposition 2 : Soit *a* et *b* deux entiers quelconques et *m* un entier supérieur ou égal à 2.

On note (E) l'*équation* d'inconnue x $(x \in \mathbb{Z})$: $ax \equiv b[m]$, et *d* le *PGCD* de *a* et de *m*.

Alors : **1)** (E) admet au moins une solution $\Leftrightarrow$ d/b.

2) Si (E) admet au moins une solution, alors elle en admet une infinité et toutes les solutions sont de la forme $\alpha + k\frac{m}{d}$, où α est une solution particulière et *k* un entier quelconque.

3) Si (*E*) admet au moins une solution, alors elle en admet exactement d dans l'intervalle $[\![0,m-1]\!]$; et si on les note x_1, x_2, x_3, … , x_d, toutes les autres sont de la forme x_1+km, x_2+km, x_3+km, … , x_d+km, où *k* est un entier quelconque. On dit alors que (*E*) possède *d* solutions définies à une congruence modulo *m* près.

4) En particulier, si *a* et *m* sont premiers entre eux, (*E*) a une solution unique modulo *m*.

Preuve. $PGCD(a,m)=d$. Il existe donc des entiers *a'* et *m'* tels que : $a=da'$, $m=dm'$ et $PGCD(a',m')=1$.

1) $\Rightarrow$: Supposons que (*E*) admette au moins une solution : notons-la α.

Il existe donc $k \in \mathbb{Z}$ tel que : $a\alpha - b = km$,

$da'\alpha - kdm' = b$,

$d(a'\alpha - km') = b$.

$a'\alpha - km'$ étant un entier, il est clair que d divise b.

$\Leftarrow$: Réciproquement, supposons que *d* divise *b* : il existe un entier *b'* tel que $b=db'$.

On a : $ax \equiv b[m] \Leftrightarrow \exists k \in \mathbb{Z}; ax - b = km$.

$da'x - kdm' = db'$.

$a'x - km' = b'$ (*E'*).

Ainsi : (*E*) admet au moins une solution si, et seulement si, l'équation (*E'*) d'inconnues $(x,k) \in \mathbb{Z}^2$ en admet au moins une. Or, le *PGCD* de *a'* et *m'* étant 1, d'après l'identité de Bézout, il existe des entiers *u* et *v* tels que : $a'u+m'v=1$, $a'(b'u)-m'(-b'v)=b'$. (E') admet au moins une solution : $(b'u,-b'v)$.

2) Conservons les notations de la proposition et indiquons la propriété suivante, que nous allons utiliser ici (et que nous démontrerons plus bas) : $\forall (x,y)\in\mathbb{Z}^2,\ ax\equiv ay[m] \Leftrightarrow x\equiv y\left[\frac{m}{d}\right]$.

Supposons que (E) admette au moins une solution ; notons-la α. On a : x est une solution de $(E) \Leftrightarrow ax\equiv b[m] \Leftrightarrow$ $ax\equiv a\alpha[m]$ (car $a\alpha\equiv b[m]$) $\Leftrightarrow x\equiv\alpha\left[\frac{m}{d}\right]$ (d'après la propriété ci-dessus) $\Leftrightarrow \exists k\in\mathbb{Z}; x=\alpha+k\frac{m}{d}$.

3) (E) admet au moins une solution, notée α.

$\alpha,\ \alpha+\frac{m}{d},\ \alpha+2\frac{m}{d},\ \alpha+3\frac{m}{d},\ \dots,\ \alpha+(d-1)\frac{m}{d}$ sont, d'après **2)**, d solutions distinctes de (E).

Il est clair que : **.** ces d entiers sont, deux à deux, non congrus modulo m ;

. toutes les autres solutions de (E) sont congrues, modulo m, à l'une de ces d solutions-là. Or, tout entier est congru modulo m à un et un seul élément de $[\![0,m-1]\!]$: $\forall x\in\mathbb{Z},\ \exists!(q,r)\in\mathbb{Z}^2; x=mq+r$, avec $0\le r\le m-1$ (c'est le reste de la division euclidienne de cet entier par m). Si l'on note $x_1, x_2, x_3, \dots, x_d$ les d entiers de $[\![0,m-1]\!]$ congrus aux d solutions citées plus haut, on obtient le résultat recherché.

Exemples : Résoudre dans $\mathbb{Z}$ les équations suivantes : 1) $3x\equiv 1[12]$; 2) $9x\equiv 3[15]$.

Réponse. 1) $PGCD(3,12)=3$, qui ne divise pas 1 : il n'y a pas de solution.

2) $PGCD(9,15)=3$: il y a trois solutions modulo 15.

2 est une solution évidente ; les deux autres sont $2+\frac{15}{3}=7$ et $2+2\times\frac{15}{3}=12$. Nous avons obtenu directement les trois solutions de $[\![0,14]\!]$. Les solutions sont donc les entiers de la forme $2+15k$, $7+15k$ et $12+15k$ $(k\in\mathbb{Z})$.

Démontrons maintenant la propriété utilisée au cours de la démonstration du **2)** de la proposition 2 ; ajoutons-y un résultat de même ordre, c'est-à-dire intéressant pour le maniement des congruences.

Proposition 3. a est un entier relatif, m et n sont deux entiers supérieurs ou égaux à 2.

On a : **1)** $\forall (x,y)\in\mathbb{Z}^2,\ ax\equiv ay[m] \Leftrightarrow x\equiv y\left[\frac{m}{pgcd(a,m)}\right]$.

2) $\forall (x,y)\in\mathbb{Z}^2, \begin{cases} x\equiv y[m] \\ x\equiv y[n] \end{cases} \Leftrightarrow x\equiv y[ppcm(m,n)]$.

Preuve.

1) Posons $PGCD(a,m)=d$. Il existe alors des entiers a' et m' tels que : $a=da'$, $m=dm'$ et $PGCD(a',m')=1$.

$\Rightarrow$: $ax\equiv ay[m] \Leftrightarrow \exists k\in\mathbb{Z}; ax-ay=km$.

$a(x-y)=km$.

$da'(x-y)=kdm'$.

$a'(x-y)=km'$.

$\begin{cases} pgcd(a',m')=1 \\ m'/a'(x-y) \end{cases} \Rightarrow m'/x-y$ (théorème de Gauss) $\Rightarrow x\equiv y[m']$. Rappelons que $m=dm'$; on a donc $x\equiv y\left[\frac{m}{d}\right]$.

$\Leftarrow$: $x\equiv y\left[\frac{m}{d}\right] \Leftrightarrow \exists k\in\mathbb{Z}; x-y=k\frac{m}{d}$.

$ax-ay=ka\frac{m}{d}=kda'\frac{m}{d}=ka'm \quad (ka'\in\mathbb{Z})$.

$ax\equiv ay[m]$.

Exemples.

1) Résoudre dans $\mathbb{Z}$ le système (d'inconnue x) : (S) $\begin{cases} x \equiv 3[17] \\ x \equiv 4[11] \\ x \equiv 5[6] \end{cases}$.

Réponse. La démonstration de la proposition 1 nous fournit un moyen effectif de résoudre ce système. Si l'on conserve les notations utilisées pour cette démonstration, on a :

$a_1 = 3$, $a_2 = 4$, $a_3 = 5$, $m_1 = 17$, $m_2 = 11$, $m_3 = 6$, $M_1 = m_2 m_3 = 66$, $M_2 = m_1 m_3 = 102$, $M_3 = m_1 m_2 = 187$.

Cherchons d'abord les entiers b_1, b_2 et b_3 tels que : $66b_1 \equiv 1[17]$, $102b_2 \equiv 1[11]$ et $187b_3 \equiv 1[6]$.

Utilisons pour cela l'algorithme d'Euclide :

$$\left.\begin{array}{l} 66 = 3\times 17 + 15 \\ 17 = 1\times 15 + 2 \\ 15 = 7\times 2 + 1 \end{array}\right| \begin{array}{l} \times 8 \\ \times(-7) \\ \\ \end{array}$$

$66\times 8 + 17\times(-7) = 17\times 24 + 1$. On obtient : $66\times 8 - 1 = 17\times 31$; autrement dit, $b_1 = 8$.

Des calculs analogues nous donnent : $b_2 = 4$ et $b_3 = 1$.

$a_1 b_1 M_1 + a_2 b_2 M_2 + a_3 b_3 M_3 = (3\times 8\times 66) + (4\times 4\times 102) + (5\times 1\times 187) = 4151$

est l'unique solution de (*S*) modulo 1122 $(= m_1 m_2 m_3)$.

Ainsi : x est une solution de (*S*) $\Leftrightarrow$ $x \equiv 4151[1122]$ $\Leftrightarrow$ $x \equiv 785[1122]$ $(785 = 4151 - 3\times 1122)$.

Les solutions de (*S*) sont les entiers de la forme $785 + 1122k$, où k décrit $\mathbb{Z}$.

2) Le problème du cuisinier chinois :

Une bande de dix-sept pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager équitablement et de donner le reste au cuisinier chinois : celui-ci recevrait alors trois pièces. Mais les pirates se querellent et six d'entre eux sont tués : le cuisinier recevrait alors quatre pièces. Dans un naufrage ultérieur, seuls six pirates et le cuisinier sont sauvés (avec le butin !), et le partage laisserait cinq pièces d'or à ce dernier. Quelle est alors la fortune minimale que peut espérer le cuisinier quand il décide d'empoisonner le reste des pirates ?

Réponse : Notons x le nombre de pièces d'or du butin. La deuxième phrase du texte indique que la division de x par 17 donne 3 comme reste, soit $x \equiv 3[17]$.

Les deux phrases suivantes conduisent aux deux autres équations : $x \equiv 4[11]$ et $x \equiv 5[6]$.

On reconnaît le système de l'exemple **1)**. La fortune minimale à laquelle peut prétendre le cuisinier est donc de 785 pièces d'or.

3) Le problème du phare :

Un phare émet un signal jaune toutes les quinze minutes et un signal rouge toutes les vingt-huit minutes. On aperçoit le signal jaune à 0 h 02 min et le rouge à 0 h 08 min. À quelle heure verra-t-on pour la première fois les deux signaux émis en même temps ?

Réponse : Notons x le temps, exprimé en minutes, qui s'est écoulé depuis 0 h 00 min et au bout duquel les deux signaux sont émis simultanément pour la première fois.

On a : $\begin{cases} x \equiv 2[15] \\ x \equiv 8[28] \end{cases}$.

Procédons de la même manière que dans l'exemple **1)** [ici : $a_1 = 2$, $a_2 = 8$, $m_1 = M_2 = 15$, $m_2 = M_1 = 28$].

Cherchons des entiers b_1 et b_2 tels que : $28b_1 \equiv 1[15]$ et $15b_2 \equiv 1[28]$.

$$\left.\begin{array}{l} 28 = 1\times 15 + 13 \\ 15 = 1\times 13 + 2 \\ 13 = 6\times 2 + 1 \end{array}\right| \begin{array}{l} \times 7 \\ \times(-6) \\ \\ \end{array}$$

$28\times 7 + (-6)\times 15 = 7\times 15 + 1$.

On obtient : $7\times 28 - 1 = 13\times 15$ et $(-13)\times 15 - 1 = (-7)\times 28$; autrement dit, $b_1 = 7$ et $b_2 = -13$.

$a_1 b_1 M_1 + a_2 b_2 M_2 = (2\times 7\times 28) + (8\times(-13)\times 15) = -1168$ est l'unique solution du système modulo 420 $(= 15\times 28)$.

Ainsi : $\begin{cases} x \equiv 2[15] \\ x \equiv 8[28] \end{cases}$ $\Leftrightarrow$ $x \equiv -1168[420]$ $\Leftrightarrow$ $x \equiv 92[420]$ $(92 = -1168 + 3\times 420)$.

92 est le plus petit entier positif solution du système. 92 min = 1 h 32 min.

C'est donc à 1h 32 min que l'on verra pour la première fois simultanément les deux signaux.

On trouve de nombreuses applications du théorème des restes en astronomie et en cryptographie.

Le théorème chinois des restes sert en particulier (principalement ?) dans les deux situations suivantes.

. Situation 1 : on cherche un entier vérifiant un certain nombre de conditions arithmétiques. Il s'agit d'abord de traduire ces conditions en termes de congruences, ce qui en général n'est pas si aisé. Donnons un exemple :

Démontrer que pour chaque entier strictement positif *n*, il existe *n* entiers strictement positifs consécutifs tels qu'aucun d'entre eux ne soit une puissance entière d'un nombre premier (Olympiades Internationales de Mathématiques, Brunswick, 1989, exercice n° 5.).

Réponse : *n* est un entier ≥ 1. Il s'agit de montrer qu'il existe *n* entiers strictement positifs consécutifs tels qu'aucun d'entre eux ne s'écrivent sous la forme p^m, où *p* est un nombre premier et *m* un entier ≥ 2.

Choisissons $2n$ nombres premiers, deux à deux distincts : $p_1, p_2, p_3, \cdots, p_{2n-1}, p_{2n}$.

Considérons les *n* entiers suivants : $c_1 = p_1p_2,\ c_2 = p_3p_4,\ c_3 = p_5p_6, \cdots, c_n = p_{2n-1}p_{2n}$.

Puisque deux nombres premiers distincts sont premiers entre eux et qu'un nombre premier avec d'autres est premier avec leur produit, il est clair que les c_i sont premiers entre eux deux à deux; et il existe donc, d'après le théorème des restes, un entier *a* tel que :

$$(\Sigma)\quad \begin{cases} x \equiv 0\ [c_1] \\ x \equiv -1[c_2] \\ x \equiv -2[c_3] \\ \cdots\cdots\cdots\cdots \\ x \equiv -(n-1)[c_n] \end{cases} \Leftrightarrow\ x \equiv a[c_1c_2c_3...c_n].$$

Ainsi on peut trouver (au moins) un entier naturel solution du système (Σ). Notons *k* l'un d'eux.

Alors : $k \equiv 0[c_1],\ k+1 \equiv 0[c_2],\ k+2 \equiv 0[c_3], \ldots\ldots, k+(n-1) \equiv 0[c_n]$.

Autrement dit : $\forall i \in [\![0, n-1]\!],\ c_{i+1}/k+i$.

Aucun des *n* entiers $k+i$ $(i \in [\![0, n-1]\!])$ ne peut être une puissance entière d'un nombre premier puisque dans la décomposition en facteurs premiers de chacun de ces *n* entiers intervient au moins deux nombres premiers distincts $(c_{i+1} = p_{2i+1}p_{2i+2})$.

On peut donner à ce problème une solution constructive en exhibant $n-1$ entiers consécutifs qui ne sont pas des puissances entières d'un nombre premier : $(n!)^2+2,\ (n!)^2+3,\ (n!)^2+4, \ldots., (n!)^2+n$.

Raisonnons par l'absurde et supposons qu'il existe $k \in [\![2, n]\!]$, *p* premier et $m \in [\![2, +\infty[\![$, tels que : $(n!)^2 + k = p^m$.

$k \in [\![2, n]\!]$, donc *k* est l'un des facteurs de $n!$, d'où : $k/(n!)^2$,

$k/(n!)^2 + k$,

k/p^m,

$\exists s \in [\![1, m]\!];\ k = p^s$ (puisque *p* est premier et $k > 1$).

$n! \geq 1 \Rightarrow\ k = p^m - (n!)^2 < p^m \Rightarrow\ s < m$.

$\dfrac{(n!)^2}{k} + 1 = \dfrac{(n!)^2 + k}{k} = \dfrac{p^m}{p^s} = p^{m-s}$, avec $1 \leq m-s \leq m-1$.

p divise donc $\dfrac{(n!)^2}{k} + 1$ (*).

p/k $(k = p^s$ et $s \geq 1)$ et $k \Big/ \dfrac{(n!)^2}{k}$ (*k* est l'un des facteurs de $n!$), d'où $p \Big/ \dfrac{(n!)^2}{k}$ (**).

De (*) et (**), on tire $p/1$ … et *p* est premier !

On peut aussi donner à cet énoncé des Olympiades une forme plus générale :

Démontrer que pour chaque entier strictement positif *n*, il existe *n* entiers strictement positifs consécutifs tels qu'aucun d'entre eux n'est une puissance entière d'un entier naturel (*i.e.* de la forme a^k, avec $(a,k) \in \mathbb{N}^2$ et $k \geq 2$).

Ici aussi, on peut faire intervenir le théorème des restes.

Lemme : Soit x un entier naturel.

S'il existe un nombre premier p tel que $x \equiv p\left[p^2\right]$, alors x ne peut être une puissance entière d'un entier.

(Preuve du lemme : $x \equiv p\left[p^2\right] \Rightarrow \exists q \in \mathbb{Z} ; x = p + q.p^2 = p(1+q.p) \Rightarrow p/x$.

Le nombre premier p intervient donc dans la décomposition en facteurs premiers de x, et intervient avec l'exposant 1; en effet, si le facteur p^k $(k \geq 2)$ apparaissait dans la décomposition de x, on aurait $x \equiv 0\left[p^2\right]$. Or, si x est la puissance entière d'un entier, les nombres premiers apparaissant dans sa décomposition ont un exposant supérieur ou égal à 2.)

Considérons p_1, p_2, p_3, … et p_n, n nombres premiers deux à deux distincts, et (Σ') le système (d'inconnue x) suivant :

$$\begin{cases} x \equiv p_1 - 1\left[p_1^2\right] \\ x \equiv p_2 - 2\left[p_2^2\right] \\ \ldots\ldots\ldots\ldots \\ x \equiv p_n - n\left[p_n^2\right] \end{cases}.$$

$\forall (i,j) \in [\![1,n]\!]^2$, $i \neq j$, $\operatorname{pgcd}\left(p_i^2, p_j^2\right) = 1$ [rappel : $\operatorname{pgcd}(a,b) = 1 \Rightarrow \forall (k,l) \in \mathbb{N}^2$, $\operatorname{pgcd}\left(a^k, b^l\right) = 1$], d'où, d'après le théorème des restes, (Σ') admet une infinité de solutions : notons x_0 l'une d'elles. On a : $\forall i \in [\![1,n]\!]$, $x_0 + i \equiv p_i\left[p_i^2\right]$; d'après le lemme, les n entiers consécutifs x_0+1, x_0+2, x_0+3, … , x_0+n ne peuvent être la puissance entière d'un entier.

Venons-en à l'autre cas (principal) d'utilisation du théorème chinois :

. Situation 2 : pour trouver un entier x tel que $x \equiv a[n]$ $\left[(a,n) \in \mathbb{Z}^2 ; n \geq 2\right]$, il peut être commode de décomposer n en un produit de facteurs premiers : $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots\ldots p_r^{\alpha_r}$. Puisque deux nombres premiers distincts sont premiers entre eux, le théorème des restes nous permet alors d'écrire :

$$x \equiv a[n] \Leftrightarrow \begin{cases} x \equiv a\left[p_1^{\alpha_1}\right] \\ x \equiv a\left[p_2^{\alpha_2}\right] \\ \ldots\ldots\ldots\ldots \\ x \equiv a\left[p_r^{\alpha_r}\right] \end{cases},$$

et il est plus simple d'étudier une congruence modulo un nombre premier ou une puissance d'un nombre premier, compte tenu des nombreux résultats, concernant la divisibilité par un nombre premier, à notre disposition.

Nous avons écrit plus haut que l'astronomie et la cryptographie recèlent de nombreuses applications du théorème des restes.

Il est un autre domaine, grand consommateur d'arithmétique lui aussi, dans lequel ce théorème fait de fréquentes apparitions : l'horlogerie ancienne, avec ses engrenages. Ainsi, le problème suivant :

Une roue dentée (R_1) comportant cinq dents s'engrène dans une roue dentée (R_2) comportant huit dents. Combien de dents doivent passer pour que la troisième dent de (R_1) rencontre la deuxième de (R_2) ?

peut être modélisé par le système $\begin{cases} x \equiv 3[5] \\ x \equiv 2[8] \end{cases}$.

On trouvera en annexe une interprétation du théorème des restes en termes d'engrenages, proposée par Jean-Paul Delahaye (*cf.* la bibliographie). Dans le problème ci-dessus, les nombres de dents des deux roues sont premiers entre eux; ce qui assure (vérifiez-le) que chaque dent de l'une des roues rencontre chaque dent de l'autre. Mais que se passe-t-il si ces deux nombres ne sont pas premiers entre eux ? Une généralisation du théorème des restes permet de s'affranchir de cette condition.

Proposition 4. (Le "théorème chinois des restes" généralisé.)

. $m_1, m_2, m_3, \dots, m_n$ sont n entiers supérieurs ou égaux à 2.

. $a_1, a_2, a_3, \dots, a_n$ sont n entiers relatifs quelconques.

. Le système de congruences : $\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \\ \dots\dots\dots\dots \\ x \equiv a_n [m_n] \end{cases}$ admet une solution si, et seulement si, $\forall (i,j) \in [\![1,n]\!]^2$, $a_i \equiv a_j \left[\text{pgcd}(m_i, m_j) \right]$.

. Dans ce cas, le système admet une unique solution modulo $\text{ppcm}(m_1, m_2, m_3, \dots, m_n)$.

Preuve.

$\Rightarrow$: Supposons que notre système admette une solution x_0.

Soient i et j deux entiers quelconques de $[\![1,n]\!]$.

On a : $x_0 \equiv a_i [m_i]$, i.e. $m_i / x_0 - a_i$.

D'où, puisque $\text{pgcd}(m_i, m_j)$ divise m_i : $x_0 \equiv a_i \left[\text{pgcd}(m_i, m_j) \right]$ (*).

De même, $x_0 \equiv a_j \left[\text{pgcd}(m_i, m_j) \right]$ (**).

De (*) et (**) on tire : $a_i \equiv a_j \left[\text{pgcd}(m_i, m_j) \right]$.

$\Leftarrow$: Supposons maintenant que : $\forall (i,j) \in [\![1,n]\!]^2$, $a_i \equiv a_j \left[\text{pgcd}(m_i, m_j) \right]$.

Pour montrer que notre système de congruences admet une solution, nous allons raisonner par récurrence sur n (le nombre de congruences du système).

. Initialisation ($n = 2$).

Le système considéré est : (S_2) $\begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \end{cases}$; où, par hypothèse, $a_1 \equiv a_2 \left[\text{pgcd}(m_1, m_2) \right]$.

Notons δ le pgcd de m_1 et de m_2.

D'après l'hypothèse rappelée ci-dessus, δ divise $a_2 - a_1$, autrement dit $\dfrac{a_2 - a_1}{\delta}$ est un entier.

Posons $y = x - a_1$. (S_2) devient alors le système d'inconnue y : (S_2') $\begin{cases} y \equiv 0 \quad [m_1] \\ y \equiv a_2 - a_1 [m_2] \end{cases}$.

Remarquons qu'une solution de (S_2') est nécessairement divisible par m_1, et donc par δ.

Effectuons donc un nouveau changement d'inconnue : $z = \dfrac{y}{\delta}$.

(S_2') devient alors le système d'inconnue z : (S_2'') $\begin{cases} \delta z \equiv 0 \quad [m_1] \\ \delta z \equiv \delta . \dfrac{a_2 - a_1}{\delta} [m_2] \end{cases}$.

D'après le 1) de la proposition 3, (S_2'') est équivalent au système : (S_2''') $\begin{cases} z \equiv 0 \quad \left[\dfrac{m_1}{\text{pgcd}(\delta, m_1)} \right] \\ z \equiv \dfrac{a_2 - a_1}{\delta} \left[\dfrac{m_2}{\text{pgcd}(\delta, m_2)} \right] \end{cases}$.

Par définition de δ, on a : $m_1 = \delta m_1'$ et $m_2 = \delta m_2'$, avec $\text{pgcd}(m_1', m_2') = 1$.

Donc : $\text{pgcd}(\delta, m_1) = \text{pgcd}(\delta, m_2) = \delta$, $\dfrac{m_1}{\text{pgcd}(\delta, m_1)} = m_1'$ et $\dfrac{m_2}{\text{pgcd}(\delta, m_2)} = m_2'$.

D'après le théorème chinois des restes (proposition 1), (S_2''') admet des solutions qui sont de la forme $x_0 + km_1'm_2'$, x_0 étant une solution de (S_2''') et k un entier relatif. Les solutions de (S_2') sont donc de la forme $\delta x_0 + k\delta m_1'm_2'$, et celles de (S_2) de la forme $\delta x_0 + a_1 + k\delta m_1'm_2'$. On vérifie aisément que $\delta x_0 + a_1$ est une solution de (S_2) ; par ailleurs,

$k\delta m_1'm_2' = k.\text{ppcm}(m_1, m_2)$ puisque $\text{ppcm}(m_1, m_2) = \dfrac{m_1 m_2}{\text{pgcd}(m_1, m_2)} = \dfrac{\delta m_1'.\delta m_2'}{\delta} = \delta m_1'm_2'$.

Ainsi (S_2) admet des solutions qui sont les entiers de la forme $\alpha + k.\text{ppcm}(m_1, m_2)$, où α est une solution de (S_2) et k un entier relatif.

. <u>Hérédité.</u> Soit n un entier ≥ 2 quelconque.

Nous supposons que tout système de n congruences de la forme $x \equiv a_i [m_i]$ $(1 \leq i \leq n, a_i \in \mathbb{Z}, m_i \in \mathbb{N} - \{0,1\})$ admet une solution **<u>si</u>**, $\forall (i,j) \in [\![1,n]\!]^2$, $a_i \equiv a_j \left[\text{pgcd}(m_i, m_j)\right]$.

Considérons maintenant le système : (S) $\begin{cases} x \equiv a_1 \quad [m_1] \\ \cdots\cdots\cdots\cdots \\ x \equiv a_n \quad [m_n] \\ x \equiv a_{n+1} [m_{n+1}] \end{cases}$; où, par hypothèse, $\forall (i,j) \in [\![1,n+1]\!]^2$, $a_i \equiv a_j \left[\text{pgcd}(m_i, m_j)\right]$.

Nous avons montré ci-dessus (*cf.* l'initialisation) qu'il existe $\alpha \in \mathbb{Z}$ tel que :

$$(\Sigma) \begin{cases} x \equiv a_1 [m_1] \\ x \equiv a_2 [m_2] \end{cases} \Leftrightarrow x \equiv \alpha \left[\text{ppcm}(m_1, m_2)\right].$$

Notons que l'entier α, qui est une solution du système (Σ), est congru à a_1 modulo m_1 et à a_2 modulo m_2.

(S) est donc équivalent au système : (S') $\begin{cases} x \equiv \alpha \left[\text{ppcm}(m_1, m_2)\right] \\ x \equiv a_3 \quad [m_3] \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x \equiv a_{n+1} \quad [m_{n+1}] \end{cases}$.

Soit i un entier de $[\![3,n+1]\!]$. On a : $a_i \equiv a_1 \left[\text{pgcd}(m_i, m_1)\right]$.

Puisque $\text{pgcd}(m_i, m_1)$ divise m_1, on a aussi $\alpha \equiv a_1 \left[\text{pgcd}(m_i, m_1)\right]$; d'où : $\alpha \equiv a_i \left[\text{pgcd}(m_i, m_1)\right]$.

De même $\alpha \equiv a_i \left[\text{pgcd}(m_i, m_2)\right]$.

$\alpha - a_i$, étant un multiple de $\text{pgcd}(m_i, m_1)$ et de $\text{pgcd}(m_i, m_2)$, est un multiple de $\text{ppcm}\left[\text{pgcd}(m_i, m_1), \text{pgcd}(m_i, m_2)\right]$.

Donc $\alpha \equiv a_i \left[\text{ppcm}\left(\text{pgcd}(m_i, m_1), \text{pgcd}(m_i, m_2)\right)\right]$.

Or, on a l'égalité $\text{ppcm}\left(\text{pgcd}(m_i, m_1), \text{pgcd}(m_i, m_2)\right) = \text{pgcd}\left(m_i, \text{ppcm}(m_1, m_2)\right)$ [*cf.* la première égalité du 4) de l'annexe "propriétés élémentaires du *PGCD* et du *PPCM*"]; d'où : $\alpha \equiv a_i \left[\text{pgcd}\left(m_i, \text{ppcm}(m_1, m_2)\right)\right]$.

Ainsi : $\forall i \in [\![3,n+1]\!]$, $\alpha \equiv a_i \left[\text{pgcd}\left(m_i, \text{ppcm}(m_1, m_2)\right)\right]$, et $\forall (r,s) \in [\![3,n+1]\!]^2$, $a_r \equiv a_s \left[\text{pgcd}(m_r, m_s)\right]$ (hypothèses portant sur le système (S)).

Le système (S') vérifie l'hypothèse de récurrence, et admet donc une solution.

Il en va de même pour le système (S) qui lui est équivalent.

Bibliographie :

. Hardy, Wright, *An Introduction to the Theory of Numbers*, 5e éd., Oxford University Press, 1979 : le chapitre VIII traite du sujet qui nous intéresse.

. Pierre Bornsztein, Xavier Caruso, Pierre Nolin et Mehdi Tibouchi, *Arithmétique*, tome 1, décembre 2004 : cours écrit à l'occasion d'un stage de l'O.F.M. Concernant notre sujet, la lecture du chapitre 3, paragraphe 4 (pages 40 à 43) est particulièrement intéressante; j'en ai repris les idées essentielles.

. Jean-Paul Delahaye, *Merveilleux nombres premiers (Voyage au cœur de l'arithmétique)*, Belin-Pour la Science, 2000 : le livre entier mérite d'être lu. Notre théorème est explicitement évoqué page 68 et sqq., ainsi qu'aux pages 112 et 113.