K A F E M A T H - 10-11-2022

Les AVENTURES du THÉORÈME CHINOIS

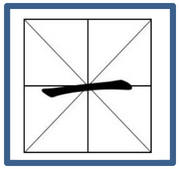
«Même en maths, les choses vieillissent !»

(Denis Guedj)

« Mais en Chine, elles vieillissent plus longtemps ! »

(Anonyme)

SOMMAIRE



Le THÉORÈME CHINOIS, de l'ORIGINE à nos JOURS

Carte des provinces à l'époque des Printemps et Automnes (Vè siècle av. JC) [Wikipedia]

La Chine … au temps où elle n'était pas encore la Chine … pays d'Origine du Théorème Chinois

Les **mathématiques chinoises**, à cette époque, n'existaient pas encore ...

► Le **théorème chinois** a connu jusqu'à nos jours de nombreuses aventures … à travers l'histoire des mathématiques …

► Il apparaît dans un livre d'arithmétique sous le pinceau du mathématicien et astronome **Sun Zi**, (ou **Sun Tzu**), né en Chine entre le IIIème et le Vème siècle.

► Il sera généralisé en *1247* par le mathématicien chinois **Qin Jiushao** dans le «Livre Mathématique en 9 Chapitres» ...

► Parti de Chine, où il s'appliquait notamment aux calculs astronomiques (almanachs), ce théorème se retrouve dans des textes indiens à partir du Vème siècle ...

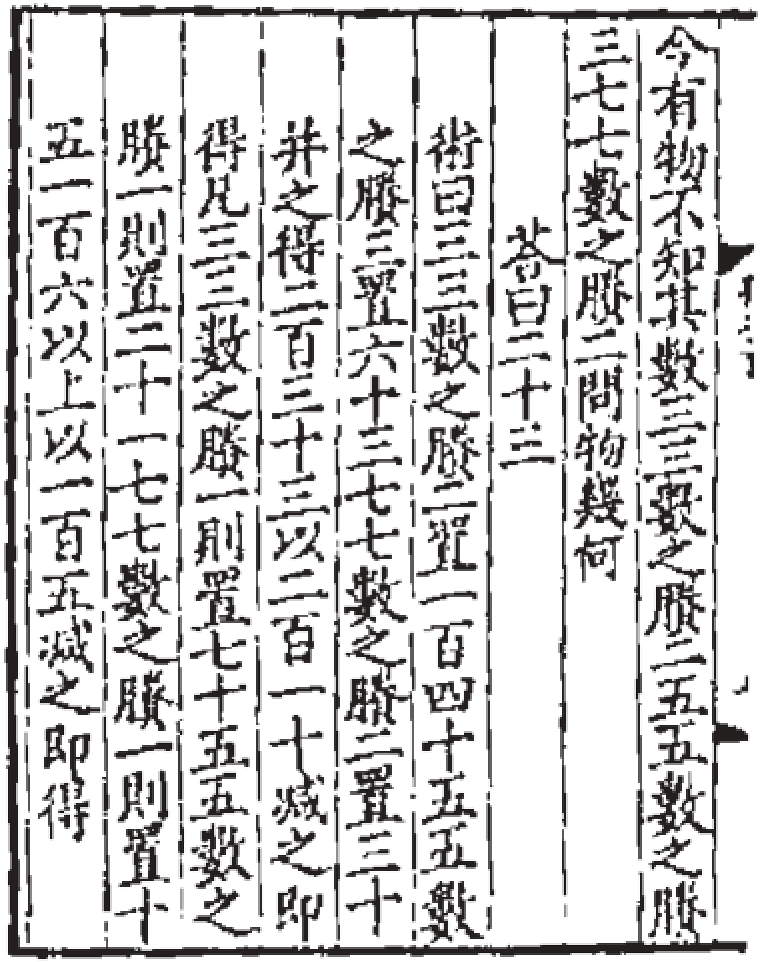
► En Europe, au Moyen-Age, il fait plutôt figure de curiosité mathématique et ne connaîtra pas de développement notable ...

► De nos jours, le théorème chinois a retrouvé sa place dans la recherche, surtout grâce aux applications ...

1-1 La formulation du théorème chinois d'après Sun Zi et autres auteurs

► La Formulation Ancienne du Théorème Chinois

Les mathématiciens chinois formulaient les problèmes, non pas de façon abstraite, mais en s'appuyant sur des exemples numériques … et ne donnaient pas de démonstration à proprement parler ...



今有物不知其數三三數之賸二五五數之賸
三七七數之賸二問物幾何
荅曰二十三
術曰三三數之賸二置一百四十五五數
之賸三置六十三七七數之賸二置三十
并之得二百三十三以二百一十減之即
得凡三三數之賸一則置七十五五數之
賸一則置二十一七七數之賸一則置十
五一百六以上以一百五減之即得

Problème de Sun Zi, reproduit dans la Collection Tianlu linlang (1932)

Le problème de **Sun Zi** se pose typiquement de la manière suivante :

Nous avons un certain nombre de choses à ranger ; ce nombre est inconnu, mais nous savons que :

- Si nous rangeons les choses **3** par 3, à la fin, il en restera **2** qui ne seront pas rangées ;
- Si nous les rangeons **5** par 5, il en restera **3** à ranger ;
- Si nous les rangeons **7** par 7, il en restera **2** à ranger.

Question :

Quel est *le nombre* total de choses à ranger ?

Autre formulation :

“Quel nombre donne pour reste 2, 3, ou 2 quand on le divise par 3, 5 ou 7 respectivement ?”

► <u>Les Mathématiciens Indiens reprennent le Problème</u> :

Le savant indien **Brahmagupta** (né au VIème siècle) propose le problème similaire suivant :

Au marché du village, une vieille femme voit son panier d'œufs renversé par le cheval d'un cavalier. Celui-ci, pour la dédommager, lui demande combien elle avait d'œufs. La femme ne s'en rappelle pas le nombre exact, mais elle déclare :

- quand j'eus fini de les ranger **2** par 2, il m'en restait **1** en main ;
- chaque fois que je vidais le panier en retirant les œufs par **3**, par **4**, par **5** ou par **6** à la fois, il en restait aussi **1** ;
- mais quand je les retirais **7** par 7, le panier contenait à la fin **0** œuf.

<u>Question</u> :

Quel est *le plus petit nombre* d'œufs que contenait le panier ?

1-2 Les Ingrédients de la formulation moderne du théorème chinois

► <u>Théorème Chinois, Division Euclidienne, PGCD et Congruence</u>

En langage moderne, le type de problème formulé par **Sun Zi** ou par **Brahmagupta** s'exprime à l'aide des notions d'arithmétique :

- de **division euclidienne**,
- de **Plus Grand Commun Diviseur** (PGCD) de **n** entiers,
- de relation de **congruence**,
- d'**équation diophantienne** linéaire.

1-2-1 La DIVISION EUCLIDIENNE

La **division euclidienne**, opération fondamentale

de l’arithmétique dans l’ensemble des entiers,

associe à deux entiers,

- le *dividende* **a** et le *diviseur* **b<a**,

deux autres entiers,

- le *quotient* **q** et le *reste* **r**,

tels que :

$$\boxed{a = bq + r, \quad \text{avec } r<b}$$

L’Empereur Qin

1-2-2 PGCD : PLUS GRAND COMMUN DIVISEUR

Soient **a**,**b**$\in$Z des entiers. L'entier **d**$\in$Z, noté PGCD**(a,b)**, ou simplement **(a,b)**, est appelé

PLUS GRAND COMMUN DIVISEUR (**PGCD**)

de **a** et de **b** si, et seulement si,

(1) **d**|**a** et **d**|**b**
(**d** divise **a** et **b**)

(2) si **c**|**a** et **c**|**b**, alors **c** $\leq$ **d**
(si **c** divise aussi **a** et **b**, alors **c** est inférieur ou égal à **d**)

1-2-3 La RELATION de CONGRUENCE

La relation de **congruence** entre nombres entiers se définit à partir de la **division euclidienne**.

► Une définition *simple* de la Relation de Congruence

Deux entiers **x** et **y** sont **congrus modulo n** s'ils vérifient la condition suivante :

x et y ont le même RESTE dans la division euclidienne par n

L'entier **n** est appelé le **module**.

► Savoir si un entier n est **DIVISIBLE** par un entier ***d***

En utilisant la notion de congruence, on a la condition :

Un entier n est DIVISIBLE par un entier d, si, et seulement si,

$$\boxed{n \equiv 0 \pmod{d}}$$

► La Fonction **MOD** DES TABLEURS

mod(n;d)

La règle est alors :

si **r** = **0**,

d est un **diviseur** (exact) de **n**

n est un **multiple** de **d**

si **r** ≠ **0**,

d n'est pas un diviseur de **n**

(**n** n'est pas un multiple de **d**)

♣ <u>Exemple</u> : On peut illustrer la relation de congruence en déterminant, avec un *tableur*, les <u>entiers pairs</u> **n** = 0 (mod **2**) :

`=if(mod(A2;2)=0;"OUI";"-")`

A	B	C	D	E	F	G	H	I	J
n	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
2	OUI	-	-	-	-	-	-	-	-
3	-	OUI	-	-	-	-	-	-	-
4	OUI	-	OUI	-	-	-	-	-	-
50	OUI	-	-	OUI	-	-	-	-	OUI
71	-	-	-	-	-	-	-	-	-
157	-	-	-	-	-	-	-	-	-
359	-	-	-	-	-	-	-	-	-
360	OUI	OUI	OUI	OUI	OUI	-	OUI	OUI	OUI
361	-	-	-	-	-	-	-	-	-
1062	OUI	OUI	-	-	OUI	-	-	OUI	-
9275	-	-	-	OUI	-	OUI	-	-	-
13794	OUI	OUI	-	-	OUI	-	-	-	-
102784	OUI	-	OUI	-	-	-	OUI	-	-
3254781	-	OUI	-	-	-	-	-	-	-

mod(n;2)

Mais **d** = **2** *ne divise pas* les entiers n = 3, 5, 71, 157, etc

(à chaque fois, le reste est **r** ≠ **0**).

♣ Exemple : Avec le module **n** = **5**, le nombre de « valeurs » possibles du reste **r**, dans la division euclidienne d'un entier **x** par **n** = **5**, est un ensemble de **n** = **5** éléments, appelés **classes résiduelles** (mod **5**) :

5 classes résiduelles modulo **5**

Chaque classe résiduelle a pour éléments les entiers qui ont même reste **r** dans la division euclidienne par **n** = **5**.

0	$E_0 = \bar{0}$	...	-15	-10	-5	**0**	5	10	15	...
1	$E_1 = \bar{1}$	...	-14	-9	-4	**1**	6	11	16	...
2	$E_2 = \bar{2}$	...	-13	-8	-3	**2**	7	12	17	...
3	$E_3 = \bar{3}$	...	-12	-7	-2	**3**	8	13	18	...
4	$E_4 = \bar{4}$	...	-11	-6	-1	**4**	9	14	19	...

Suite arithmétique de raison **n** = **5**

L'ensemble des **n** classes résiduelles pour un module **n** est une partie *stricte* infinie de l'ensemble $\mathbb{Z}$ des entiers relatifs.

On le note : $\mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ ou simplement : $\mathbb{Z}_5$.

► OPÉRATIONS dans un Ensemble Z_n d'Entiers modulo *n*

Les opérations (modulo n) *usuelles* dans un ensemble $\mathbf{Z_n}$ sont l'addition, la multiplication et l'exponentiation. Par exemple, on a les propriétés :

Si : $\begin{cases} \mathbf{a} \equiv \mathbf{c} \pmod{\mathbf{n}} \\ \mathbf{b} \equiv \mathbf{d} \pmod{\mathbf{n}} \end{cases}$, alors :

$\mathbf{a} + \mathbf{b} \equiv \mathbf{c} + \mathbf{d} \pmod{\mathbf{n}}$ (addition)

$\mathbf{a} \times \mathbf{b} \equiv \mathbf{c} \times \mathbf{d} \pmod{\mathbf{n}}$ (multiplication)

Dans la suite, nous nous intéresserons essentiellement à la **multiplication** modulo **n**

二

THÉORÈME CHINOIS et ÉQUATIONS DIOPHANTIENNES

► Système de 2 ou plusieurs équations modulaires

Résoudre le problème de **Sun Zi** ou de **Brahmagupta** consiste à résoudre un **système d'équations diophantiennes** (équations à solutions dans **Z**), c'est-à-dire à :

Sun Zi ⟶

Trouver un entier x tel que :

$x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$ et $x \equiv 2 \pmod{7}$.

Brahmagupta ⟶

Trouver un entier x tel que :

$x \equiv 1 \pmod{2}$,

$x \equiv 1 \pmod{3}$,

$x \equiv 1 \pmod{4}$,

$x \equiv 1 \pmod{5}$,

et

$x \equiv 0 \pmod{7}$.

2-1 La Solution de Sun Zi

► Imaginons qu'une certaine quantité **x**>0 s'exprime de deux façons en langage des congruences, par les deux équations modulaires :

Le tableur de Sun Zi

$\mathbf{E_1}$: $\mathbf{x} \equiv 2 \pmod{3}$ et $\mathbf{E_2}$: $\mathbf{x} \equiv 3 \pmod{5}$

<u>Question</u> : quelle est la valeur de **x** ?

$\mathbf{E_1}$: $\mathbf{x} \equiv 2 \pmod{3}$, $\mathbf{E_2}$: $\mathbf{x} \equiv 3 \pmod{5}$																
x	0	1	2	3	4	5	6	7	**8**	9	10	11	12	13	14	**15**
x (mod **3**)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
x (mod **5**)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0

Sun Zi résout le système d'équations S = {$\mathbf{E_1}$,$\mathbf{E_2}$}, *à la main*, à partir d'un *tableau* des valeurs possibles de **x** (mod 3) ...

x = 8 est la solution du système

… et de **x** (mod 5). Il lit alors la solution sur ce tableau.

Sun Zi fait la même chose
pour les deux équations :

$\mathbf{E_1} : \mathbf{x} \equiv 2 \pmod{3}$ et $\mathbf{E_3} : \mathbf{x} \equiv 2 \pmod{7}$

Il résout le système d'équations S = {$\mathbf{E_1}$,$\mathbf{E_3}$} à partir du tableau des valeurs possibles de **x** (mod **3**) et **x** (mod **7**) :

$\mathbf{E_1} : \mathbf{x} \equiv 2 \pmod{3}$, $\mathbf{E_3} : \mathbf{x} \equiv 2 \pmod{7}$																						
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	**21**
x (mod 3)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0
x (mod 7)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

x = 2 est la solution du système

Remarques :

a) les modules **3** et **7** sont des entiers **premiers entre eux** :

PGCD(**3**,**7**) = 1 ;

b) le nombre de colonnes du tableau est égal à :

21 = **3** x **7** = produit des modules = **PPCM**(**3**,**7**)

Enfin, Sun Zi dresse le même type de tableau pour résoudre les deux équations :

$$\mathbf{E_2} : \mathbf{x} \equiv 3 \pmod{5} \text{ et } \mathbf{E_3} : \mathbf{x} \equiv 2 \pmod{7}$$

$\mathbf{E_2} : \mathbf{x} \equiv 3 \pmod{5}$, $\mathbf{E_3} : \mathbf{x} \equiv 2 \pmod{7}$																																				
x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	**23**	24	25	26	27	28	29	30	31	32	33	34	35
x (mod 5)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0
x (mod 7)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0

x = **23** est la solution du système

Remarques :

a) les modules **5** et **7** sont des entiers **premiers entre eux** : **PGCD**(**5**,**7**) = 1 ;

b) le nombre de colonnes du tableau est égal à :

35 = **5** x **7** = produit des modules = **PPCM**(**5**,**7**)

Y-a-t-il une <u>solution *commune* aux trois équations</u> ?

Sun Zi prolonge les tableaux des résidus des équations **E_1**, **E_2** et **E_3**, et voit que **23** est la *plus petite solution commune* des trois équations **E_1**, **E_2** et **E_3**.

23

E_1 : $x \equiv 2 \pmod{3}$, E_2 : $x \equiv 3 \pmod{5}$

x	0	1	2	3	4	5	6	7	**8**	9	10	11	12	13	14	15	16	17	18	19	20	21	22	**23**	24	25	26	27	28	29	30	31	32	33	34	**35**
x (mod **3**)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	**2**	0	1	2	0	1	2	0	1	2	0	1	2
x (mod **5**)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	**3**	4	0	1	2	3	4	0	1	2	3	4	0

E_1 : $x \equiv 2 \pmod{3}$, E_3 : $x \equiv 2 \pmod{7}$

x	0	1	**2**	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	**23**	24	25	26	27	28	29	30	31	32	33	34	**35**
x (mod **3**)	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	2	0	1	**2**	0	1	2	0	1	2	0	1	2	0	1	2
x (mod **7**)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	**2**	3	4	5	6	0	1	2	3	4	5	6	0

E_2 : $x \equiv 3 \pmod{5}$, E_3 : $x \equiv 2 \pmod{7}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	**23**	24	25	26	27	28	29	30	31	32	33	34	**35**
x (mod **5**)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	**3**	4	0	1	2	3	4	0	1	2	3	4	0
x (mod **7**)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	**2**	3	4	5	6	0	1	2	3	4	5	6	0

L'entier **23** est donc *une* solution du système **S** = {$\mathbf{E_1}$,$\mathbf{E_2}$,$\mathbf{E_3}$} :

$$\mathbf{S} = \begin{cases} \mathbf{E_1} : \mathbf{x} \equiv 2 \pmod{3} \\ \mathbf{E_2} : \mathbf{x} \equiv 3 \pmod{5} \\ \mathbf{E_3} : \mathbf{x} \equiv 2 \pmod{7} \end{cases}$$

Il reste une question à laquelle Sun Zi n'a pas répondu :

Pour quel *module commun* aux trois équations,
l'entier **23** est-il la solution du système S ?

► Comment **Sun Zi** va-t-il procéder pour trouver une solution *commune* aux trois équations ?

Multiples communs de 3, 5 et 7																
3	6	9	12	15	18	21	24	27	30	33	36	39	42	45	48	51
5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85
7	14	21	28	35	42	49	56	63	70	77	84	91	98	**105**	112	119

3	54	57	60	63	66	69	72	75	78	81	84	87	90	93	96	99	102	**105**
5	90	95	100	**105**	110	115	120	125	130	135	140	145	150	155	160	165	170	175
7	126	133	140	147	154	161	168	175	182	189	196	203	210	217	224	231	238	245

► En comparant avec son tableur, les *multiples* de **3**, **5** et **7**, Sun Zi remarque que **105** est le plus petit entier commun à **3**, **5** et **7**.

► Et aussi que **3**, **5** et **7** sont *premiers entre eux*, donc que leur **PPCM** est égal à leur produit : PPCM(**3**,**5**,**7**) = **3** x **5** x **7** = **105**.

Sun Zi constate aussi que

- **35** est le PPCM de **5** et **7**,
- **21** est le PPCM de **3** et **7**,
- **15** est le PPCM de **3** et **5**

et se demande comment *concilier* tout ça !

Sun Zi recherche donc un entier **N** qui vérifie les trois équations E_1, E_2 et E_3, modulo un entier **M** à trouver ...

Il se dit :

- que, si **l'entier N** vérifie deux des trois équations, alors il doit aussi vérifier la troisième ;

- que, de plus, **N** ne peut être inférieur au plus grand des PPCM, **35**.

1) <u>En partant des deux équations **E2** et **E3**</u>, **Sun Zi** recherche les multiples s1 de **35** = **5*7** qui sont solution de la <u>3ème équation **E1**</u> ...

$E_1 : x \equiv 2 \pmod{3}$
$E_2 : x \equiv 3 \pmod{5}$
$E_3 : x \equiv 2 \pmod{7}$

Son tableur lui répond :

	Mod	s1	35	70	105	140	175	210
E1 : x=2 mod 3	3		2	1	0	2	1	0

Les valeurs possibles de l'entier **N** sont donc **35** et **140** ...

2) Ensuite **Sun Zi**, à partir des deux équations **E_1** et **E_3**, recherche les multiples s2 du produit des modules **21** = **3*7** qui vérifient l'équation **E_2** ; le tableur répond à nouveau :

E_1 : **x** ≡ **2** (mod **3**)
E_2 : **x** ≡ **3** (mod **5**)
E_3 : **x** ≡ **2** (mod **7**)

	Mod									
E2 : x=**3** mod 5	5	s2		21	42	63	84	105	126	147
				1	2	3	4	0	1	2

Une autre valeur possible de l'entier **N** est donc **63** ...

3) Enfin, **Sun Zi** considère les deux équations **E_1** et **E_2** et recherche les multiples s3 du produit des modules **15** = **3*5** qui vérifient l'équation **E_3** :

E_1 : $x \equiv 2 \pmod{3}$
E_2 : $x \equiv 3 \pmod{5}$
E_3 : $x \equiv 2 \pmod{7}$

Le tableur encore une fois donne la réponse :

Mod

E_3 : x=**2** mod 7

7	s3	15	30	45	60	75	90	105	120	135	150
		1	2	3	4	5	6	0	1	2	3

Une autre valeur possible de l'entier **N** est donc **30**.

	Mod															
		s1	**35**	70	105	**140**	175	210					**245**	280	315	**350**
E_1 : x=**2** mod 3	**3**		**2**	1	0	**2**	1	0					**2**	1	0	**2**
		s2		21	42	**63**	84	105	126	147			**168**	189	210	
E_2 : x=**3** mod 5	**5**			1	2	**3**	4	0	1	2			**3**	4	0	
		s3			15	**30**	45	60	75	90	105	120	**135**	150		
E_3 : x=**2** mod 7	**7**				1	**2**	3	4	5	6	0	1	**2**	3		
		s1+s2+s3 =				**233**							**548**			
		(s1+s2+s3)-**23** =				**210**							**525**			

… En rassemblant les éléments des trois tableaux précédents, **Sun Zi** voit que : **N** = 140+63+30 = **233** = **210**+**23** = (2***105**)+**23**

Autrement dit : **N** = **233** ≡ **23** (mod **105**)

<u>Le module **M** cherché est donc le produit des modules</u> des équations du système : **M** = **105** = (3*5*7)

Produit des modules

Le résultat obtenu par **Sun Zi** correspond à l'énoncé moderne du Théorème (des restes) Chinois, dans le cas d'un système de 3 équations modulaires :

Soient m_1, m_2, m_3 trois entiers *premiers entre eux*. Alors le système de 3 congruences

$$S = \begin{cases} x = a \pmod{m_1} \\ x = b \pmod{m_2} \\ x = c \pmod{m_3} \end{cases}$$

admet *au moins une* solution modulo le produit des modules $\prod m_i$.
De plus, deux quelconques des solutions <u>diffèrent d'un multiple de</u> $\prod m_i$.

2-2

Problème de Sun Zi et Équations Diophantiennes

Si le produit des modules est grand, la solution d'un système de deux équations modulaires par lecture d'un tableau n'est guère praticable ...

► Résolution d'un Système de 2 équations modulaires à partir d'une équation diophantienne

♣ 1ER Exemple : Soient les deux équations modulaires :

$$\mathbf{E_4} : \mathbf{x} \equiv \mathbf{13} \pmod{\mathbf{104}},\ \mathbf{E_5} : \mathbf{x} \equiv \mathbf{49} \pmod{\mathbf{60}}$$

Le tableau correspondant au système S = {$\mathbf{E_4}$,$\mathbf{E_5}$} aurait un nombre de colonnes important, égal à :

$$\mathbf{1560} = \mathbf{PPCM}(\mathbf{104},\mathbf{60})$$

Une première méthode consiste à

<u>transformer un système S à *deux* équations modulaires</u> :

$$S = \begin{cases} E_4 : \mathbf{s} \equiv 13 \pmod{104} \\ E_5 : \mathbf{s} \equiv 49 \pmod{60} \end{cases}$$

<u>en *une seule* « équation diophantienne linéaire »</u>, d'inconnue **s**,

qu'on cherche à résoudre ...

On utilise alors une variante de la définition de la congruence :

$$\boxed{x \equiv y \pmod{n} \text{ si, et seulement si, il existe un } k \in \mathbb{N} \text{ tel que } x = y + kn}$$

Autrement dit, **x** et **y** diffèrent d'un *multiple* de **n**.

On peut récrire le système **S** :

$$S' = \begin{cases} E_1 : \mathbf{s} \equiv 13 \pmod{104} \Leftrightarrow \text{Il existe un } \mathbf{X} \text{ tel que } \mathbf{s} \equiv 13 + 104\mathbf{X} & E_6 \\ E_2 : \mathbf{s} \equiv 49 \pmod{60} \Leftrightarrow \text{Il existe un } \mathbf{Y} \text{ tel que } \mathbf{s} \equiv 49 + 60\mathbf{Y} & E_7 \end{cases}$$

A partir des deux équations E_6 et E_7 de S', on obtient l'égalité :

$$13 + 104\mathbf{X} = 49 + 60\mathbf{Y}$$

qui se simplifie en :

$$104\mathbf{X} - 60\mathbf{Y} = 36 \quad \text{puis en} \quad \boxed{26\mathbf{X} - 15\mathbf{Y} = 9} \qquad E_8$$

$$a\mathbf{X} + b\mathbf{Y} = c$$

<u>Conclusion</u> :

Traiter le type de problème formulé par **Sun Zi**, revient à **résoudre une équation diophantienne**.

Sur un *tableur*, on peut vérifier (laborieusement) que, parmi les couples
(X,Y) = (36,63), (-36,63), (36,-63) et (-36,-63),
la solution de $\mathbf{E_8}$ s'écrit : -936-(-945) = **-936 + 945** = **9** ; donc :
(X,Y) = (-36,-63)

M12 | =SI(ABS(B12-M2)=9;"OUI";"non")

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1			**Y**	1	2	3	4	---	---	60	61	62	**63**	64	65
2			**15Y**	15	30	45	60	---	---	900	915	930	**945**	960	975
3	**X**	**26X**	**26X-9**												
4	1	26	17	0	0	0	0	---	---	0	0	0	0	0	0
5	2	52	43	0	0	0	0	---	---	0	0	0	0	0	0
6	3	78	69	0	0	0	0	---	---	0	0	0	0	0	0
7	4	104	95	0	0	0	0	---	---	0	0	0	0	0	0
8	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
9	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---
10	34	884	875	0	0	0	0	---	---	0	0	0	0	0	0
11	35	910	901	0	0	0	0	---	---	0	0	0	0	0	0
12	**36**	**936**	927	0	0	0	0	---	---	0	0	0	**OUI**	0	0
13	37	962	953	0	0	0	0	---	---	0	0	0	0	0	0
14	38	988	979	0	0	0	0	---	---	0	0	0	0	non	0

► Résolution d’un Système d’Equations modulaires à partir des Classes Résiduelles

Une autre méthode de résolution d’un système

d’équations modulaires consiste à

exploiter le fait que les éléments d’une classe

résiduelle forment une *suite arithmétique* ...

♣ 2EME Exemple :

Soit le système de deux équations modulaires :

$$\mathbf{S} = \begin{cases} \mathbf{E_1} : \mathbf{s} \equiv \mathbf{8} \pmod{\mathbf{11}} \\ \mathbf{E_2} : \mathbf{s} \equiv \mathbf{3} \pmod{\mathbf{19}} \end{cases}$$

... / ...

$$\begin{cases} E_1 : s \equiv 8 \pmod{11} \\ E_2 : s \equiv 3 \pmod{19} \end{cases}$$

• On part de l'équation E_1, qui s'écrit : [1] $s = 11y + 8$

• On remplace ensuite **s** par $11y + 8$ dans l'équation E_2 :

[2] $11y + 8 \equiv 3 \pmod{19}$, qui devient :

[3] $11y \equiv -5 \pmod{19}$.

Pour obtenir **y**, il faut simplifier [3] $11y \equiv -5 \pmod{19}$

en divisant par **11** …

<u>On cherche alors un élément de la *classe résiduelle* modulo **19**</u>

<u>qui soit un multiple de **11**</u> :

-19 … **-5** … **0** … **14** … **19** … **33** … **38** … ← suite arithmétique de *raison* **19**

$-5 + 19 = 14$ $14 + 19 = 33$

… / …

-19 … **-5** … **0** … **14** … **19** … **33** … **38** … ← suite arithmétique de *raison* **19**

-5 + **19** = **14** **14** + **19** = **33**

- On voit que **33** est un multiple de **11,** donc l'équation [3] devient :

[4] $11y \equiv 33 \pmod{19}$, d'où en divisant par **11** :

[5] $y = 3$

- On remplace **y** par **3** dans [1] $s = 11y + 8$, d'où la solution

$$s = (11 \times 3) + 8 = 41$$

- On vérifie que c'est la solution du système **S** : $\begin{cases} E_1 : s \equiv 8 \pmod{11} \\ E_2 : s \equiv 3 \pmod{19} \end{cases}$

$41 \equiv 8 \pmod{11}$ et $41 \equiv 3 \pmod{19}$

► **Résolution d'un Système d'Équations modulaires à l'aide de la notion d'inverse pour la multiplication**

Un exemple de **table de multiplication** modulo **n** ≥ 2, établie à l'aide d'un *tableur*, nous montre comment ça fonctionne ...

	A	B	C	D	E	F
1						
2	MULTIPLICATION Modulo 6					
3	**6**	1	2	3	4	5
4	**1**	1	2	3	4	5
5	**2**	2	4	0	2	4
6	**3**	3	0	3	0	3
7	**4**	4	2	0	4	2
8	**5**	5	4	3	2	1

Table de multiplication dans $\mathbf{Z}_6$

Certains produits de cette table de multiplication sont égaux à **0** (modulo 6), alors qu'aucun des facteurs du produit n'est nul :

2x3 , 3x2 , 3x4 , 4x3 .

Les entiers

2, **3** et **4**

sont des **diviseurs de 0**.

On remarque que seuls **1** et **5** ont un **inverse** pour la multiplication modulo 6 : **1** x **1** = **1** et **5** x **5** = **1** .

La multiplication modulaire a une propriété importante :

Si le module **p** est un entier **premier**, alors tout élément de $\mathbf{Z}_p$ est **inversible**.

H	I	J	K	L	M	N
MULTIPLICATION Modulo 7						
7	**1**	**2**	**3**	**4**	**5**	**6**
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	**6**	**5**	**4**	**3**	**2**	**1**

Aucun produit de la table n'est égal à **0** modulo 7 :
dans l'ensemble $\mathbf{Z}_7$,
il n'existe pas de **diviseurs de 0** !

Tous les éléments de l'ensemble $\mathbf{Z}_7$,
ont un **inverse** !

Table de multiplication dans $\mathbf{Z}_7$

♣ 3EME Exemple :

Sun Zi aurait pu trouver la valeur de **x** dans ses équations en faisant une recherche d'inverse dans une table $\mathbf{Z_p}$

$$\mathbf{S} = \begin{cases} \mathbf{E_1} : \mathbf{x} \equiv \mathbf{2} \pmod{\mathbf{3}} \\ \mathbf{E_2} : \mathbf{x} \equiv \mathbf{3} \pmod{\mathbf{5}} \\ \mathbf{E_3} : \mathbf{x} \equiv \mathbf{2} \pmod{\mathbf{7}} \end{cases}$$

1) ● On part de l'équation $\mathbf{E_3} : \mathbf{x} \equiv \mathbf{2} \pmod{\mathbf{7}}$, qui s'écrit :

[1] $\mathbf{x} = \mathbf{7y} + \mathbf{2}$

● On remplace **x** par **7y** + **2** dans l'équation

$\mathbf{E_2}$: $\mathbf{x} \equiv \mathbf{3} \pmod{\mathbf{5}}$, qui s'écrit : $\mathbf{x} = \mathbf{5y} + \mathbf{3}$;

Donc :

[2] $\mathbf{7y} + \mathbf{2} = \mathbf{5y} + \mathbf{3} \pmod{\mathbf{5}}$, qui devient :

[3] $\mathbf{2y} = \mathbf{1}$, donc : $\mathbf{y} = \mathbf{1}/\mathbf{2}$,

autrement dit : **y** est l'**inverse** de **2** modulo **5**

● On cherche alors dans la table de multiplication de $\mathbf{Z_5}$ quel est l'inverse de **2** modulo **5** :

... / ...

- On lit dans la table de $\mathbf{Z}_5$ que :

$$y = 1/2 = \boxed{3}$$

- D'où :

$\mathbf{E}_3 : \mathbf{x} = 7y+2 = 7\,.\,\boxed{3} + 2 = 23$, ce qui correspond à la solution trouvée dans le tableur de **Sun Zi** pour les équations

$$\mathbf{E}_2 : \mathbf{x} \equiv 3 \pmod{5}$$

$$\mathbf{E}_3 : \mathbf{x} \equiv 2 \pmod{7}$$

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table de multiplication dans $\mathbf{Z}_5$

$\mathbf{E}_2 : \mathbf{x} \equiv 3 \pmod{5}$, $\mathbf{E}_3 : \mathbf{x} \equiv 2 \pmod{7}$

x	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
x (mod 5)	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3	4	0	1	2	3
x (mod 7)	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2

2) • On part de l'équation $\mathbf{E_1}$: $\mathbf{x} \equiv 2 \pmod 3$ qui s'écrit :

[1] $\mathbf{x} = 3y + 2$

$\mathbf{E_1}$: $\mathbf{x} \equiv 2 \pmod 3$

$\mathbf{E_2}$: $\mathbf{x} \equiv 3 \pmod 5$

$\mathbf{E_3}$: $\mathbf{x} \equiv 2 \pmod 7$

• On remplace ensuite **x** par $3y + 2$ dans l'équation $\mathbf{E_2}$:

[2] $3y + 2 \equiv 3 \pmod 5$, qui devient :

[3] $3y \equiv 1 \pmod 5$.

Donc : $y = 1/3$,

autrement dit :

... / ...

y est l'**inverse** de **3** modulo **5**

• On cherche alors dans la table de multiplication de $\mathbb{Z}_5$ quel est l'inverse de **3** modulo **5** :

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table de multiplication dans $\mathbf{Z}_5$

- On lit dans la table de $\mathbf{Z}_5$ que :

$$y = 1/3 = \boxed{2}$$

- D'où :

E₁ : $\mathbf{x} = 3\mathbf{y} + 2$ s'écrit

$$\mathbf{x} = 3 \cdot \boxed{2} + 2 = 8,$$

ce qui correspond à la solution trouvée dans le tableur de **Sun Zi** pour les équations

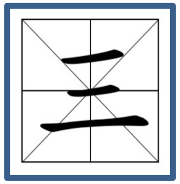
$$\mathbf{E_1} : \mathbf{x} \equiv 2 \pmod{3}$$

$$\mathbf{E_2} : \mathbf{x} \equiv 3 \pmod{5}$$

x	0	1	2	3	4	5	6	7	8
x (mod 3)	0	1	2	0	1	2	0	1	2
x (mod 5)	0	1	2	3	4	0	1	2	3

x = 8 est la solution du système

… **etc.**



EXEMPLES SIMPLES d'APPLICATION du THÉORÈME CHINOIS ...

3-1 FACILITER les CALCULS avec le THÉORÈME CHINOIS

► Une conséquence du théorème chinois est que :

Étant donnés k≥2 entiers $\mathbf{m_1}$, $\mathbf{m_2}$, premiers entre eux, alors des entiers **x** et **y** sont congrus modulo $\prod \mathbf{m_k} = (\mathbf{m_1} \times \mathbf{m_2})$, si, et seulement si, on a :

$\mathbf{x} \equiv \mathbf{y}$ modulo $\mathbf{m_1}$

et

$\mathbf{x} \equiv \mathbf{y}$ modulo $\mathbf{m_2}$

Autrement dit, en général :

Des entiers congrus modulo un produit $\mathbf{m_1.m_2. \ldots .m_k}$, sont congrus modulo *chacun* des entiers du produit.

On tire de ce résultat une procédure de <u>simplification de certains calculs</u> ...

<u>Exemple</u> : Soit l'équation $\mathbf{E_1}$: $\mathbf{x^3} \equiv \mathbf{2} \pmod{\mathbf{55}}$

Comme **55** = **5** x **11** (produit d'entiers *premiers*), un entier **x** qui vérifie l'équation $\mathbf{E_1}$ est aussi solution du système :

$$\mathbf{S} = \begin{cases} \mathbf{E_2} : \mathbf{x^3} \equiv \mathbf{2} \pmod{\mathbf{5}} \\ \mathbf{E_3} : \mathbf{x^3} \equiv \mathbf{2} \pmod{\mathbf{11}} \end{cases}$$

A l'aide de notre fidèle tableur, nous éliminons le terme $\mathbf{x^3}$ de **S**.

On voit alors que les congruences $\mathbf{E_2}$ et $\mathbf{E_3}$ sont équivalentes aux congruences :

$$\mathbf{S'} = \begin{cases} \mathbf{E_4} : \mathbf{x} \equiv \pmod{\mathbf{5}} \\ \mathbf{E_5} : \mathbf{x} \equiv \mathbf{7} \pmod{\mathbf{11}} \end{cases}$$

$$S' = \begin{cases} E_4 : x \equiv 3 \pmod{5} \\ \\ E_5 : x \equiv 7 \pmod{11} \end{cases}$$

R5 | f_x Σ = | =MOD(R2;5)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
1																			
2	**x**	2	**3**	4	5	6	**7**	**8**	9	10	11	12	**13**	14	15	16	17	**18**	19
3	**x^3**	8	**27**	64	125	216	**343**	**512**	729	1000	1331	1728	**2197**	2744	3375	4096	4913	5832	6859
4	**x^3 mod 5**	3	**2**	4	0	1	3	**2**	4	0	1	3	**2**	4	0	1	3	2	4
5	**x mod 5**	2	3	4	0	1	2	**3**	4	0	1	2	3	4	0	1	2	3	4
6																			
7	**x^3 mod 11**	8	5	9	4	7	**2**	6	3	10	0	1	8	5	9	4	7	2	6
8	**x mod 11**	2	3	4	5	6	**7**	8	9	10	0	1	**2**	3	4	5	6	**7**	8
9																			
10	**x mod 55**	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

Le tableur, toujours lui, nous donne la solution du système :

$$x = \boxed{18}$$

qui convient pour les trois modules, **5**, **11** et **55**.

3-2

THÉORÈME CHINOIS et COMPTAGE des CARRÉS MODULO m

Un problème d'arithmétique modulaire *classique* est de <u>compter tous les carrés modulo un certain module</u> ...

Le Théorème Chinois permet de mettre en pratique le résultat suivant :

> Étant donnée la décomposition en facteurs premiers d'un entier :
>
> $$\mathbf{n} = \mathbf{p}^{\mathbf{e1}} \times \mathbf{p}^{\mathbf{e2}} \times \ldots \times \mathbf{p}^{\mathbf{ek}}$$
>
> L'équation
>
> $$\mathbf{n}^2 \equiv \mathbf{a} \pmod{\mathbf{m}}$$
>
> a *une* solution si, et seulement si, *toutes les congruences*
>
> $$\mathbf{n}^2 \equiv \mathbf{a} \pmod{\mathbf{p}^{\mathbf{ei}}}$$
>
> ont une solution.

On dira que :

n est un **carré modulo m** s'il existe **y** tel que **n** $\equiv$ **y**^{2} (mod **m**)

<u>Exemple</u> :

On se demande si **n** = **61** est un **carré** modulo **m** = **75** …

La décomposition en facteurs premiers de **m** = **75** est :

$$m = 75 = 3^1 \times 5^2 = 3 \times 25$$

On se demande donc si **n** = **61** est un **carré** modulo p_1 = **3** *et* modulo p_2 = **25** …

La table des multiples de **3** nous montre que :

x	1	2	3	4	5	6	7	8	9
x mod 3	1	2	0	1	2	0	1	2	0

x $\equiv$ **1** (mod **3**)

2	**x**	**1**	2	3	**4**	5	6	**7**	8	9	**10**
3											
4	**x mod 3**	**1**	2	0	**1**	2	0	**1**	2	0	**1**
5											
6	**x mod 25**	1	2	3	4	5	**6**	7	8	9	10

Il nous faut trouver une équation modulaire pour p_2 = **25** …

La table des multiples de **25** nous montre que :

x ≡ **6** (mod **25**)

Nous obtenons donc le système d'équations modulaires :

$$\mathbf{S} = \begin{cases} \mathbf{E_1} : \mathbf{x} \equiv \mathbf{1} \pmod{\mathbf{3}} \\ \mathbf{E_2} : \mathbf{x} \equiv \mathbf{6} \pmod{\mathbf{25}} \end{cases}$$

Le **Théorème Chinois** s'applique et nous demandons à notre tableur favori de nous donner *une* solution ...

Le tableur nous donne *une* solution :

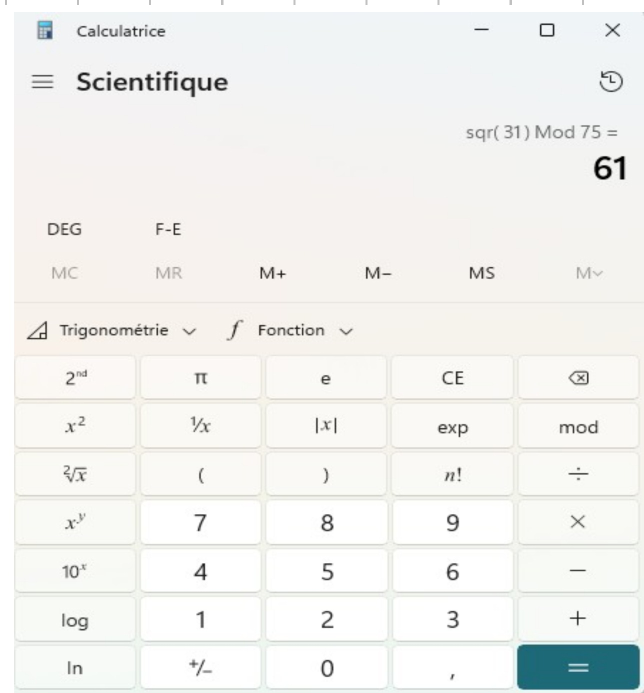
x = 31

AF6 — =MOD(AF2;25)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1																										
2	**x**	**1**	2	3	**4**	5	6	**7**	8	9	**10**	11	12	**13**	14	15	**16**	17	18	**19**	20	21	**22**	23	24	**25**
3																										
4	**x mod 3**	**1**	2	0	**1**	2	0	**1**	2	0	**1**	2	0	**1**	2	0	**1**	2	0	**1**	2	0	**1**	2	0	**1**
5																										
6	**x mod 25**	1	2	3	4	5	**6**	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	0

	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
	26	27	**28**	29	30	**31**	32	33	34	35
x mod 3	2	0	**1**	2	0	**1**	2	0	**1**	2
x mod 25	1	2	3	4	5	**6**	7	8	9	10

x = **31**



Le Théorème Chinois a donc permis de répondre que **61** est un **carré** modulo **75** :

$$61 \equiv 31^2 \pmod{75}$$

3-3

THÉORÈME CHINOIS et CRYPTOGRAPHIE : PARTAGE de CLEFS

Rappelons-nous ce que disait Benjamin Franklin :

« ***Trois individus peuvent partager un secret en toute sécurité … à condition que deux d'entre eux soient morts !*** »

A partir des années 70, l'arithmétique est devenue un outil important de la cryptographie ...

Le Théorème Chinois n'a pas manqué de s'aventurer dans ce domaine, où la <u>protection des clés d'accès aux données</u> est un problème crucial ...

Dans une banque, la porte d'accès aux coffres est verrouillée par une clef partagée entre **5** agents … Pour ouvrir la porte, au moins **2** agents doivent présenter une *partie* de la clef …

Pour constituer une clef partagée **c …**

- Les données sont :

  - un ensemble de **n** = **5** entiers premiers **P** = {11,13,17,19,23},
  - un nombre minimum de **k** = **2** agents présents,

- On calcule le produit **M** des **k-1** *plus grands* éléments de **P** :

  - ici, **k-1** = 1, donc **M** est est égal au seul plus grand élément de **P** : **M** = **23**

- On calcule le produit **N** des **k** = **2** *plus petits* éléments de **P** :

  - **N** = 11 x 13 = **143 ;**

La clef **c** sera un entier entre **M** et **N**, disons : **c** = **30**.

- On construit un ensemble **S** de **n** = **5** paires ordonnées (**p**,**r**), avec **p** dans **P** et **r** = **c** - **p** = **30** - **p** :

$$S = \{(11,19),(13,17),(17,13),(19,11),(23,7)\}$$

► Exemple : Quand deux agents porteurs des *clefs partielles* (13,17) et (23,7) se présentent, le programme d'accès traduit les données en un système d'équations modulaires :

$$\begin{cases} \mathbf{E_1} : \mathbf{x} \equiv \mathbf{13} \pmod{\mathbf{17}} \\ \mathbf{E_2} : \mathbf{x} \equiv \mathbf{7} \pmod{\mathbf{23}} \end{cases}$$

… et vérifie que la solution de ce système d'équations est bien **c** = **30**.

E_1 : $x \equiv 13 \pmod{17}$, E_2 : $x \equiv 7 \pmod{23}$																								
x	**0**	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	**17**	18	19	20	21	22	**23**
x (mod **17**)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	0	1	2	3	4	5	6
x (mod **23**)	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	0

25	26	27	28	29	**30**	31	32	33	**34**	35
8	9	10	11	12	**13**	14	15	16	0	1
2	3	4	5	6	**7**	8	9	10	11	12

c = **30** est une solution du système

$$\begin{cases} E_1 : \mathbf{x} \equiv 13 \pmod{17} \\ E_2 : \mathbf{x} \equiv 7 \pmod{23} \end{cases}$$

UN DERNIER MOT …

Le Théorème Chinois est loin d'avoir perdu en vitalité …

On le retrouve dans de nombreux domaines, entre autres :

- en **MATHÉMATIQUE** (théorie des nombres, etc),
- en **INFORMATIQUE** (utilisation de système résiduels de numération pour accélérer les calculs,

Mais aussi ...

- en **STATISTIQUE**,
- en **THÉORIE des CODES**,
- en **PHYSIQUE** (théorie du signal),

Etc.

Quelques Références sur le Théorème [des Restes] Chinois et ses Applications

► Le bouquin le plus complet (mais le plus difficile) sur le Théorème Chinois et ses Applications est :

Ding Cunsheng, **Peng Dingyi**, **Salomaa Arto**, Chinese Remainder Theorem - Applications in Computing, Coding and Cryptography

► Plus simple (niveau bac ou L1) et généraliste sur la théorie des nombres, le livre très plaisant et plein d'humour de :

Pommersheim James, **Marks Tim**, **Flapan Erica**, Number Theory--A Lively Introduction with Proofs, Applications and Stories

► Sur la question particulière des systèmes résiduels de représentation des nombres :

Omondi Amos, **Premkumar Benjamin**, Residue number systems--Theory and implementation