Plan

Partie I : Resolution Mathématique

Partie II : Resolution Informatique

AVANT PROPOS

Les problèmes de congruences simultanées sont connus dans l'histoire des mathématiques comme « problèmes des restes » ou « des restes chinois ». C'est un sujet qui a donné lieu, depuis des siècles, à de riches développements mathématiques et dont l'origine reste hypothétique puisqu'il est très difficile de démêler les motivations premières qui en ont suscité l'intérêt.

L'objet de ce projet n'est pas de faire une histoire exhaustive ou quasi exhaustive de ces problèmes. Notre perspective d'étude est avant tout d'étudie un théorème (reste chinois)

Dans un premier temps, nous présenterons la résolution mathématique du problème des congruences simultanées avec des outils connus, d'abord dans la situation la plus simple où les modules sont premiers entre eux deux à deux, puis dans un cadre général.

Dans un seconde temps, nous établirons une résolution informatique du problème des congruences simultanées dans des différents langages (C++, JAVA, JAVA SCRIPT).

En tant que les théorèmes des mathématiques se réfèrent à la réalité ils ne sont pas exacts.
En tant qu'ils sont exacts, ils ne se réfèrent pas à la réalité.

Albert Einstein
<< La géométrie et l'expérience >>

PARTIE I: Resolution Mathématique

I. Introduction

Par son histoire et sa religion, la chine a toujours mis l'accent sur l'astronomie. Ainsi, dans le but de prévoir des dates ou événements astronomiques, les astronomes chinois ont découverts le théorème des restes chinois. D'après certains textes, on peut évaluer l'apparition du théorème au 3ème siècle.

Le théorème a évolué au cours du temps sous diverses formes et avec l'apparition de nouveaux, dérivés du théorème initial.

Ce théorème, permettant de calculer des systèmes de congruences, peut servir à la résolution de petits problèmes courant mais est également appliqué à des projets de plus grande envergure

Aujourd'hui, le théorème des restes chinois a pris beaucoup d'importance dans la cryptographie. En effet, sans le savoir, ce sont des millions de personnes qui l'utilise chaque jour. Certains modes de paiement sécurisé, par exemple, font appel au système de cryptage RSA qui utilise le théorème des restes chinois (voir complémentaire).

II. DISPOSITION MATHEMATIQUE DU THEOREME

1) Le Théorème des restes chinois ou << comment résoudre des systèmes de congruences >>

Avant de vouloir résoudre un système de congruences peut-être faut il rappeler ce qu'est une congruence :

On dit que a et b sont congru modulo n (n > 1) si n divise a - b. On écrit a ≡b (mod n), notation introduite par Gauss.
C'est donc une autre façon de parler de divisibilité. Ainsi a ≡ 0 (mod n) signifie que n divise a (ou que le reste de la division de a par n est nul).
On a alors les propriétés suivantes (d'après les propriétés de la division) :

- **Si a ≡b (mod n) et c ≡ d (mod n) alors a + c ≡ b + d (mod n)**
- **Si a ≡b (mod n) et c ≡ d (mod n) alors ac ≡ bd (mod n)**
- **Si ac ≡ bc (mod n) et pgcd(c,n) = 1 alors a ≡b (mod n) (théorème de Gauss) (voir complémentaire le Theoreme et la démonstration de GAUSS)**

- **l'identité de Bezout : < *Si a et b sont premiers entre eux, alors il existe u et v entiers tels que au +bv = 1.* >**

Venons-en à notre problème :
comment résoudre le système de congruences suivant :

$$\begin{cases} X_1 \equiv a_1 \bmod m_1 \\ \vdots \\ \vdots \\ X_n \equiv a_n \bmod m_n \end{cases}$$

C'est le théorème des restes chinois qui nous fournit la réponse :

2. Théorème et Démonstration

A) Théorème des restes chinois

Théorème :

Prenons m_1, ..., m_n des entiers supérieurs à 2 deux à deux premiers entre eux, et a_1,...,a_n des entiers. Le système d'équations :

$$\begin{cases} X_1 \equiv a_1 \bmod m_1 \\ \vdots \\ \vdots \\ X_n \equiv a_n \bmod m_n \end{cases}$$

admet une unique solution modulo $M=m_1 \times ... \times m_n$ donnée par la formule :

$$x=a_1M_1y_1+...+a_nM_ny_n \bmod M$$

où $M_i=M/m_i$, et $y_i=M_i^{-1} \bmod m_i$ pour i compris entre 1 et n.

B)Démonstration du Théorème

- ***x* est solution**

Quel que soit i, $a_i\, y_i\, M_i = a_i\, M_i^{-1}\, M_i$ modulo m_i = a_i modulo m_i.

Si $i \neq j$, $a_j\, y_j\, M_j = a_j\, y_j\, M/m_j = 0$ modulo m_i
[M est un multiple de m_i et $D(m_i,m_j) = 1$]

Ainsi, $X = \left(\sum_{i=1}^{n} a_i M_i Y_i \right) \mathrm{modulo} M$ **= a_i modulo m_i .**

- **La solution *x* est unique modulo M**

Supposons l'existence de deux solutions *x* et *x'*.
Quel que soit i, *x* = *x'* modulo m_i,
Ainsi, *x* - *x'* est divisible par chacun des coefficients m_i.
Comme ceux-ci sont deux à deux premiers entre eux, x - x' est divisible par leur produit M et *x* = *x'* modulo M.

3. Exemples d'Application

A) Exemples simples

$$\begin{cases} X \equiv 3 \bmod 17 \\ X \equiv 4 \bmod 11 \\ X \equiv 5 \bmod 6 \end{cases}$$

Critère du théorème

Premièrement

il faut que les m_i soit premiers entre eux deux a deux

-17 et 11 sont premiers entre eux
-17 et 6 sont premiers entre eux
-11 et 6 sont premiers entre eux

Deuxièmement

On a $M=m_1 \times \ldots \times m_n$ D'ou M=17*11*6=1122 $M_i = M/m_i$

M_1=1122/17 = 66
M_2= 1122/11 = 102
M_3 =1122/6=187

Troisièmement

On a $Y_i M_i \equiv 1 \bmod m_i$ ou $Y_i \equiv M_i^{-1} \bmod m_i$

Pour calculer les Y_i utilisons l'Algorithme d'Euclide étendue

Par Définition :
L'algorithme d'Euclide étendu est une variante de l'algorithme d'Euclide qui permet, à partir de deux entiers *a* et *b*, de calculer non seulement leur plus grand commun diviseur (PGCD), mais aussi un de leurs couples de coefficients de Bézout (deux entiers *u* et *v* tels que *au* + *bv* = PGCD(*a*, *b*)). Quand *a* et *b* sont premiers entre eux, *u* est alors l'inverse pour la multiplication de *a* modulo *b*, ce qui est un cas particulièrement utile.

r													=	u	×	a	+	v	×	b
66													=	1	×	66	+	0	×	17
17													=	0	×	66	+	1	×	17
15	=	66	-	3	×	17							=	1	×	66	+	-3	×	17
2	=	17	-	1	×	15	=	1×17	-	1	×	(1×66 - 3×17)	=	-1	×	66	+	4	×	17
1	=	15	-	7	×	2	=	(1×66 - 3×17)	-	7	×	(-1×66 + 4×17)	=	8	×	66	+	-31	×	17

Remarquons que la dernière ligne donne 1= 8*66+ -31*17 , nous fournit exactement ce que nous voulons : $U_1 = 8$ et $V_1 = -31$

Ceci signifie que 8 est l'inverse pour la multiplication 66 modulo 17

D'où $Y_1=U_1=8$

ET de même on obtient : $Y_2=U_2=4$, $Y_3=U_3=1$

Finalement on obtient donc :

$X=(a_1M_1Y_1 + a_2M_2Y_2 + a_3M_3Y_3)$ modulo 1122

X=(3*66*8+ 4*102*4 + 5*187*1) modulo 1122

X= 4151 modulo 1122

X= 785 mod 1122

4. Problèmes

A) Problème du phare

Problème :

Un phare émet un signal jaune toutes les 15 minutes et un signal rouge toutes les 28 minutes. On aperçoit le signal jaune a 0h02 mn et le rouge a 0h08 mn. A quelle heure verra–t–on pour la première fois les deux signaux émis en même temps

AUTRE ASTUCE DE RESOLUTION

Pour résoudre ce problème utilisons une ou deux propositions qui découle du théorème des restes chinois

Proposition :

Soient $(n1,n2) \in (\mathbb{N} \setminus \{0,1\})^2$, $d=PGCD(n1,n2)$

$$\begin{cases} x \equiv a1 \ [n1] \\ x \equiv a2 \ [n2] \end{cases} \quad \text{avec } (a1,a2) \in N^2$$

admet des solutions si et seulement si $d \mid a1-a2$

Proposition :

$$x \text{ solution} \iff \begin{cases} x-x0 \equiv 0 \ [n1] \\ x-x0 \equiv 0 \ [n2] \end{cases} \iff x-x0 \in PPCM(n1,n2)N$$

Résolution :

$$\begin{cases} X \equiv 2 \ [15] \\ X \equiv 8 \ [28] \end{cases}$$

$15=3.5$ et $28=2^2.7$ $\Rightarrow$ PGCD (15,28)=1
1 divise a1-a2=-6

Donc admet des solutions.

L'algorithme d'Euclide appliqué à 28 et 15 donne :

$28 = 15*1 + 13$

$15 = 13*1 + 2$

$13 = 2*6 + 1$

On en déduit que $1 = 13 - 2*6 = 13 - 6*(15 - 13)$

Soit $1 = 7*13 - 6*15 = 7*(28 - 15) - 6*15$

Soit $7*28 - 13*15 = 1$

$1 = 7*28 + (-13)*15 \Rightarrow \begin{cases} 7*28 \equiv 1 \ [15] \\ (-13)*15 \equiv 1 \ [28] \end{cases}$

$\Rightarrow \begin{cases} 2*7*28 \equiv 2 \ [15] \\ 8*(-13)*15 \equiv 8 \ [28] \end{cases}$

Soit $x0 = 2*7*28 + 8*(-13)*15 = -1168$

$\begin{cases} x0 \equiv 2 \ [15] \\ x0 \equiv 8 \ [28] \end{cases}$ $PPCM(15,28) = 15*28 = 420$

x solution de (S2) $\Leftrightarrow$ $x \equiv -1168 \ [420]$

$\Leftrightarrow x \equiv -328 \ [420]$

$\Leftrightarrow x \equiv 92 \ [420]$

L'ensemble des solutions de (S2) est $\{92 + 420.k \ ; \ k \in N\}$

On a ainsi : x0 = 1h32mn

Les deux signaux sont émis en même temps, pour la première fois, au temps x0

La résolution étant la même que le exemple cite dans le 3eme sous parties du théorème de restes chinois (Exemple d'application)

SOIT :

$$\begin{cases} X \equiv 2 \ [15] \\ X \equiv 8 \ [28] \end{cases}$$

On a $M=m_1 \times \ldots \times m_n$ D'ou $M=15*28= 420$

$M_i = M/m_i$ d'ou $M_1=420/15 =28$ $M_2= 420/28 =15$

On a $Y_i M_i \equiv 1 \mod m_i$ ou $Y_i \equiv M_i^{-1} \mod m_i$

Pour calculer les Y_i utilisons l'Algorithme d'Euclide étendue

On a : D'où $Y_1=U_1=7$ ET $Y_2=U_2=-13$

Finalement on obtient donc :

$X=(a_1M_1Y_1 + a_2M_2Y_2)$ modulo 420

X=(2*28*7+8*15*-13) modulo 420

X = -1168 modulo 420

FINALEMENT

X = 92 modulo 420

B) Problème des soldats

Problème :

Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés par 3 colonnes, il reste deux soldats, rangés par 5 colonnes, il reste trois soldats et, rangés par 7 colonnes, il reste deux soldats ?

AUTRE ASTUCE DE RESOLUTION

Règle : « En comptant par trois, il en reste deux » : poser 140. « En comptant par cinq, il en reste trois » : poser 63. « En comptant par sept, il en reste deux » : poser 30.
Faire la somme de ces trois nombres, obtenir 233. Soustraire 210 de ce total, d'où la réponse.
Reponse : 23

En général, pour chaque unité restante d'un décompte par trois, poser 70 ; pour chaque unité restante d'un décompte par 5, poser 21 ; pour chaque unité restante d'un décompte par 7, poser 15. Si [la somme ainsi obtenue] vaut 106 ou plus, ôter 105 pour trouver la réponse

Utilisons maintenant le théorème :

Le problème des soldats se réduit donc a :

$$\begin{cases} X \equiv 2 \bmod 3 \\ X \equiv 3 \bmod 5 \\ X \equiv 2 \bmod 7 \end{cases}$$

On a donc $M=m_1 \times \ldots \times m_n$ **D'ou** $M=3*5*7=105$ $M_i = M/m_i$

$M_1=105/3=35$
$M_2=105/5=21$
$M_3=105/7=15$

On sait que $Y_i M_i \equiv 1 \bmod m_i$ **ou** $Y_i \equiv M_i^{-1} \bmod m_i$ **on a donc d'après Euclide étendue :** $Y_1=U_1=2$, $Y_2=U_2=1$, $Y_3=U_3=1$

Finalement on obtient donc :

$X=(a_1M_1Y_1 + a_2M_2Y_2 + a_3M_3Y_3)$ modulo 105

$X=(2*35*2+ 3*21*1+ 2*15*1)$ modulo 105

X= 233 modulo 105

X = 23 mod 105

III. CAS PARTICULIER

1. Première Méthode

On commence par résoudre, pour i fixe, le système

$$\begin{aligned}
x_i &\equiv 0 \pmod{m_1} \\
x_i &\equiv 0 \pmod{m_2} \\
&\vdots \\
x_i &\equiv 0 \pmod{m_{i-1}} \\
x_i &\equiv 1 \pmod{m_i} \\
x_i &\equiv 0 \pmod{m_{i+1}} \\
&\vdots \\
x_i &\equiv 0 \pmod{m_r}
\end{aligned}$$

Pour ce faire, on pose $k_i = m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_r$. Par hypothèse, k_i et m_i sont premiers entre eux et l'identité de Bezout nous donne une égalité

$$1 = rk_i + sm_i.$$

On pose $x_i = rk_i$. On a alors que x_i satisfait le système ci-dessus. Pour chaque $i = 1, 2, \ldots, n$, on trouve un tel x_i tel que $x_i \equiv 1 \pmod{m_i}$ et tel que x_i soit un multiple des autres m_j. Une solution

est alors

$$x = a_1 x_1 + a_2 x_2 + \cdots + a_r x_r.$$

Résolvons le système

$$\begin{aligned} x &\equiv 3 \pmod{11} \\ x &\equiv 6 \pmod{8} \\ x &\equiv -1 \pmod{15} \end{aligned}$$

par la méthode décrite ci-dessus. Premièrement, nous résolvons le système

$$\begin{aligned} x &\equiv 1 \pmod{11} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 0 \pmod{15} \end{aligned}$$

en cherchant une identité de Bezout pour 11 et $120 = 8 \cdot 15$. De

$$\begin{aligned} 120 &= 11 \cdot 10 + 10 \\ 11 &= 10 + 1 \end{aligned}$$

on tire que $1 = 11 - 10 = 11 - (120 - 11 \cdot 10) = 11 \cdot 11 - 120$. On obtient donc $x_1 = -120$ qui est bien un multiple de 8 et de 15 et qui est congru à 1 modulo 11.
Nous résolvons ensuite le système

$$\begin{aligned} x &\equiv 0 \pmod{11} \\ x &\equiv 1 \pmod{8} \\ x &\equiv 0 \pmod{15} \end{aligned}$$

de la même manière. On a

$$\begin{aligned} 165 &= 8 \cdot 20 + 5 \\ 8 &= 5 + 3 \\ 5 &= 3 + 2 \\ 3 &= 2 + 1 \end{aligned}$$

d'où l'on tire l'identité de Bezout

$$1 = 3 - 2 = 3 - (5 - 3) = 2 \cdot (8 - 5) - 5 = 2 \cdot 8 - 3 \cdot (165 - 8 \cdot 20) = 62 \cdot 8 - 3 \cdot 165.$$

On a alors $x_2 = -3 \cdot 165 = -495$.
Troisièmement, on résout le système

$$\begin{aligned} x &\equiv 0 \pmod{11} \\ x &\equiv 0 \pmod{8} \\ x &\equiv 1 \pmod{15} \end{aligned}$$

L'identité de Bezout $1 = 7 \cdot 88 - 41 \cdot 15$ donne $x_3 = 7 \cdot 88 = 616$.
Finalement, on obtient

$$x = 3x_1 + 6x_2 - x_3 = -3946$$

qui est une solution du système proposé. Si l'on veut la solution dont la valeur absolue est la plus petite, on rajoute à -3946 des multiples de $M = 8 \cdot 11 \cdot 15 = 1320$ pour obtenir

$$x' = -3946 + 3 \cdot 1320 = 14.$$

2. Seconde Méthode

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

par une unique équation

$$x \equiv b \pmod{m_1 m_2}.$$

(On suppose toujours que les m_i sont premiers deux à deux.)
Pour ce faire, on écrit

$$\begin{aligned} x &= a_1 + m_1 u \\ x &= a_2 + m_2 t \end{aligned}$$

On peut maintenant remplacer les deux premières équations par l'unique équation

$$x \equiv b \pmod{m_1 m_2}$$

et continuer de manière récursive jusqu'à ce qu'il ne reste qu'une seule équation.

Résolvons le système

$$x \equiv 3 \pmod{11}$$
$$x \equiv 6 \pmod{8}$$
$$x \equiv -1 \pmod{15}$$

par cette seconde méthode. On commence par résoudre

$$x \equiv 3 \pmod{11}$$
$$x \equiv 6 \pmod{8}$$

en cherchant t et u tels que

$$3 + 11t = 6 + 8u$$

ou

$$11t - 8u = 3.$$

On peut résoudre ceci par l'algorithme d'Euclide et par Bezout mais ici, on constate que $t = u = 1$ est une solution. Donc $x \equiv 14 \pmod{88}$ est une solution des deux premières équations. On remplace ces deux équations par cette dernière et le système devient

$$x \equiv 14 \pmod{88}$$
$$x \equiv -1 \pmod{15}.$$

On résout ce dernier système de la même manière en cherchant t et u tels que

$$14 + 88t = -1 + 15u.$$

On peut prendre $t = 0$ et $u = 1$ ce qui nous donne la solution finale

$$x \equiv 14 \pmod{1320}.$$

I. Cas Particulier

1) Si le nombre ne sont pas premier entre eux

Quelquefois, les systèmes de congruences peuvent être résolus même si les m_i ne sont pas premiers entre eux deux à deux. Le critère précis est le suivant : une solution *x* existe si et seulement si $a_i \equiv a_j \pmod{Pgcd(n_i, n_j)}$ pour tous *i* et *j*. Toutes les solutions *x* sont congrues modulo le PPCM des m_i .

Exemple : résoudre le système

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 5 \pmod 6 \end{aligned}$$

équivaut à résoudre le système

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

équivaut au système

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

PARTIE II: Resolution Informatique