Congruences et théorème chinois des restes

Michel Van Caneghem

Février 2003

Les congruences

Développé au début du 19ème siècle par Carl Friedrich Gauss. On dit que $a \equiv b \pmod{n}$ si $a - b$ est divisible par n. Si r est le reste de la division de a par n, r s'appelle le résidu de a modulo n.

- **$a \equiv b \pmod{n}$ si et seulement si leurs résidus sont égaux.**
- **La relation $a \equiv b \pmod{n}$ est une relation d'équivalence sur $\mathbb{Z}$**
- **On notera $\overline{a}$ le représentant de a.**

L'ensemble de ces classes d'équivalence est noté $\mathbb{Z}/n\mathbb{Z}$, et s'appelle l'ensemble des entiers modulo n.

Les opérations modulo n

On définit l'addition et la multiplication modulo n de la manière suivante :

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \overline{a} \times \overline{b} = \overline{a \times b}$$

modulo 7

x	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

modulo 6

x	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Les propriétés de ces opérations

L'addition modulo n est (groupe abélien) :

- ✗ **commutative**
- ✗ **associative**
- ✗ **il y a un élément neutre**
- ✗ **tout élément à un inverse**

La multiplication modulo n (anneau commutatif)

- ✘ **commutative**
- ✘ **associative**
- ✘ **il y a un élément neutre**
- ✘ **La multiplication est distributive par rapport à l'addition**

Si p est un nombre premier, alors $\mathbb{Z}/p\mathbb{Z}$ est un corps fini commutatif (Corps de Galois)

Les diviseurs de zéro

- **Pour que x possède une classe inverse, il faut et il suffit que $x \wedge n = 1$. Cet inverse est unique et on le note x^{-1}.**
- **Si $x \wedge n \neq 1$ alors il existe y tel que $x \times y = 0$. On dit que x est un diviseur de zéro.**
- **Si n est premier alors tout élément sauf 0 possède un inverse.**

Ex : $\mathbb{Z}/15\mathbb{Z}$:

- **0,3,5,6,9,10,12 sont des diviseurs de zéro**
- **1(1), 2(8), 4(4), 7(13), 8(2), 11(11), 13(7), 14(14) ont un inverse**

Les éléments inversibles

L'ensemble des éléments inversibles :

$$\mathbb{Z}_p^* = \{x \mid 1 \leq x < p, \quad x \wedge p = 1\}$$

forment un sous-groupe multiplicatif du groupe multiplicatif $\mathbb{Z}/p\mathbb{Z}$. En effet si :

- ✮ $x \in \mathbb{Z}_p^*$ **alors** $x \wedge p = 1$
- ✮ $y \in \mathbb{Z}_p^*$ **alors** $y \wedge p = 1$
- ✮ **donc** $xy \wedge p = 1$
- ✮ **et par conséquent** $xy \in \mathbb{Z}_p^*$.

l'élément neutre est bien sûr 1.

Résolution des équations sur les congruences

Supposons que l'on cherche à résoudre :

$$3x \equiv 5 \pmod 7$$

Cela est facile car le modulo est premier : On sait que $3^{-1} \equiv 5 \pmod 7$, on a donc $x \equiv 5 \times 5 \equiv 4 \pmod 7$.

Quand le modulo n'est pas premier nous avons le théorème suivant : Si a, b et m sont des entiers, et si $a \wedge m = d$ alors :

- ✓ **Si d ne divise pas b, alors $\boxed{ax \equiv b \pmod m}$ n'a pas de solution**
- ✓ **Sinon l'équation précédente a exactement d solutions.**

équations sur les congruences (2)

Cherchons à résoudre par exemple :

$$6x \equiv 9 \pmod{15} \Longrightarrow 3(2x-3) \equiv 0 \pmod{15}$$

On sait que 3 est un diviseur de zéro, donc :

$$3{\times}0 \equiv 0 \pmod{15} \quad 3{\times}5 \equiv 0 \pmod{15} \quad 3{\times}10 \equiv 0 \pmod{15}$$

Donc les solutions sont :

- ✔ $2x - 3 \equiv 0 \pmod{15}$ **d'ou** $x \equiv 9 \pmod{15}$**,**
- ✔ $2x - 3 \equiv 5 \pmod{15}$ **d'ou** $x \equiv 4 \pmod{15}$**,**
- ✔ $2x - 3 \equiv 10 \pmod{15}$ **d'ou** $x \equiv 14 \pmod{15}$**.**

Recherche de l'inverse

On veut chercher l'inverse de a modulo m : $a^{-1} \equiv ? \pmod{m}$. On sait que cet inverse existe si : $a \wedge m = 1$. On sait alors qu'il existe deux nombres x et y tels que :

$$ax + my = 1$$

Ce qui entraine que $ax \equiv 1 \pmod{m}$ et x est l'inverse cherché.

Si on cherche $13^{-1} \pmod{15}$, on vérifie que $13 \wedge 15 = 1$. Avec la méthode proposée dans le premier cours, on trouve que :

$$13 \times 7 + 15 \times (-6) = 1$$

donc $13^{-1} \equiv 7 \pmod{15}$.

Résolution d'un système

Dans le cas ou le modulo est premier, on a un corps et tout se passe comme dans les corps connus :

$$\begin{cases} 3x + 4y \equiv 5 \pmod{13} \\ 2x + 5y \equiv 7 \pmod{13} \end{cases}$$

$$\begin{cases} 3x + 4y \equiv 5 \pmod{13} \\ \qquad 7y \equiv 11 \pmod{13} \end{cases}$$

et on trouve :

- ✗ $y \equiv 7^{-1} \times 11 \equiv 9 \pmod{13}$
- ✗ $x \equiv 3^{-1} \times (5 - 36) \equiv 3^{-1} \times 8 \equiv 9 \times 8 \equiv 7 \pmod{13}$

Le petit théorème de Fermat

Si p est un nombre premier et si a est un entier qui n'est pas divisible par p alors :

$$a^{p-1} \equiv 1 \pmod p$$

Ce théorème est très important pour les codes secrets. La réciproque est fausse (nombres de Carmichael). [$a^{560} \equiv 1 \pmod{561}$ hors $561 = 3 \times 11 \times 17$]

Théorème de Wilson : **Si p est premier alors :**

$$(p-1)! \equiv -1 \pmod p$$

La réciproque est vraie, mais ce théorème ne sert à rien (pour l'instant !).

Le théorème d'Euler

Le nombre d'éléments ayant un inverse modulo n est noté $\Phi(n)$. Cette fonction s'appelle l'indicatrice d'Euler. C'est aussi le nombre d'entier x tels que $n \wedge x = 1$. Par exemple : $\Phi(15) = 8$

Remarque : Si p est premier alors $\Phi(p) = p - 1$.

Théorème d'Euler : Si a est un entier premier avec n alors :

$$a^{\Phi(n)} \equiv 1 \pmod{n}$$

Remarque : le théorème de Fermat est une conséquence de ce théorème.

Le théorème de Lagrange

Pour tout groupe fini $(G, \times)$ et tout sous-groupe $(H, \times)$ tel que $H \subseteq G$ alors $|H|$ divise $|G|$. On appelle ordre d'un groupe G le nombre d'éléments de ce groupe : $|G|$

Pour tout $a \in G$, considérons le sous-groupe

$$H_a = \{x \in G \mid x = y \times a \quad y \in H\}$$

H_a n'est pas vide car il contient a. C'est un sous-groupe car :

- $x1 \in H_a$ **entraine** $x1 = y1 \times a \quad y1 \in G$
- $x2 \in H_a$ **entraine** $x2 = y2 \times a \quad y2 \in G$
- **et donc** $x1 \times x2 = y1 \times a \times y2 \times a = (y1 \times a \times y2) \times a$

Le théorème de Lagrange (2)

1. **$|H|=|H_a|$ car on peut construire une bijection entre H et H_a, *car les groupes sont finis*.**
2. **ou bien $H_a = H_b$, ou bien $H_a \cap H_b = \emptyset$.**

Si il y a un élément c commun alors $c = x1 \times a = x2 \times b$. Alors $x \times a = (x \times x1^{-1} \times x1) \times a = (x \times x1^{-1} \times x2) \times b$ donc :

- **Les H_a forment une partition de G.**
- **Tous les ensembles ont la même taille**
- **donc l'ordre de H divise l'ordre de G**

Le théorème d'Euler (bis)

On définit l'ordre d'un élément $x \in G$ par :

$$ord(x) = min\{k > 0 \mid x^k = 1\}$$

On en déduit immédiatement que :

- **pour tout $x \in G$ alors $ord(x)$ divise $|G|$. Il suffit de considérer les éléments : $1, x^1, x^2, \ldots, x^{k-1}$, ils forment un sous groupe de G ;**
- **pour tout $x \in G$ alors $x^{|G|} = 1$.**

En considérant $\mathbb{Z}_p^*$ qui contient $\Phi(p)$ éléments, on en déduit immédiatement que pour tout $x \in \mathbb{Z}_p^*$ on a $x^{\Phi(p)} = 1$ dans $\mathbb{Z}_p^*$.

L'indicatrice d'Euler

Si $p \wedge q = 1$ **alors :**

$$\Phi(pq) = \Phi(p)\Phi(q)$$

On dit que la fonction Φ **est une fonction multiplicative.**

Si p **et** q **sont deux nombres premiers alors :**

$$\Phi(pq) = (p-1)(q-1)$$

Enfin si $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ **alors**

$$\Phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_n})$$

Calcul de la puissance modulaire

❶ $10^7 \equiv 130 \pmod{257}$

❷ $10^{15} \equiv 130 \times 130 \times 10 \equiv 151 \pmod{257}$

❸ $10^{31} \equiv 151 \times 151 \times 10 \equiv 51 \pmod{257}$

❹ $10^{62} \equiv 51 \times 51 \equiv 31 \pmod{257}$

❺ $10^{124} \equiv 31 \times 3 \equiv 190 \pmod{257}$

❻ $10^{249} \equiv 190 \times 190 \times 10 \equiv 172 \pmod{257}$

❼ $10^{499} \equiv 172 \times 172 \times 10 \equiv 33 \pmod{257}$

❽ $10^{999} \equiv 33 \times 33 \times 10 \equiv 96 \pmod{257}$

Calcul de la puissance modulaire (2)

Il faut tout d'abord calculer les deux fonction suivantes :

- ✔ `modulo(a,b,d)` **:** $a = b \pmod d$**. Si on remarque que :** $b = qd + a$**, le modulo est le reste de la divison de** b **par** d**.**
- ✔ `multmod(a,b,c,d)` **:** $a = b \times c \pmod d$**. On calcule le produit** $b \times c$ **et on prend le résultat modulo** d**.**

La fonction `powermod(a,b,c,d)` **:** $a = b^c \pmod d$ **se calcule alors au moyen de la procédure suivante :**

$$x^n = \begin{cases} (x^2)^{n/2} & \text{si } n \text{ est pair,} \\ x(x^2)^{n/2} & \text{si } n \text{ est impair.} \end{cases}$$

Calcul de la puissance modulaire (3)

Calcule $y = x^n \pmod{m}$

<u>if</u> $n \bmod 2 \neq 0$ **<u>then</u>** $y \Leftarrow x$ **<u>else</u>** $y \Leftarrow 1$ **<u>fi</u>**
<u>do</u>
    $n \Leftarrow \lfloor n/2 \rfloor$
    <u>if</u> $n = 0$ **<u>then</u>** **<u>exit</u>** **<u>fi</u>**
    $x \Leftarrow x \times x \pmod{m}$
    <u>if</u> $n \bmod 2 \neq 0$ **<u>then</u>** $y \Leftarrow y \times x \pmod{m}$ **<u>fi</u>**
<u>od</u>
y

Le théorème chinois des restes

Soit $m_1, m_2, \ldots, m_r$ une suite d'entiers positifs premiers entre eux deux à deux. Alors le système de congruences :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

a une solution unique x modulo $M = m_1 \times m_2 \times \cdots \times m_r$:

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_r M_r y_r$$

avec

$$M_i = M/m_i \qquad y_i M_i \equiv 1 \pmod{m_i}$$

Un exemple

Cherchons à résoudre le système de congruences suivant :

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 3 \pmod{7} \end{cases}$$

On pose $M = 3 \times 5 \times 7 = 105$

$$\begin{array}{lll} M_1 = 105/3 = 35 & y_1 \times 35 \equiv 1 \pmod{3} & y_1 = 2 \\ M_2 = 105/5 = 21 & y_2 \times 21 \equiv 1 \pmod{5} & y_2 = 1 \\ M_3 = 105/7 = 15 & y_3 \times 15 \equiv 1 \pmod{7} & y_3 = 1 \end{array}$$

$$x \equiv 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1 \equiv 157 \equiv 52 \pmod{105}$$

Un exemple (2)

Quand les modulos ne sont pas premiers entre eux

$$\left\{\begin{array}{lcll} x & \equiv & 1 & \pmod{6} \\ x & \equiv & 4 & \pmod{15} \end{array}\right. \iff \left\{\begin{array}{lcll} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 1 & \pmod{3} \\ x & \equiv & 4 & \pmod{5} \end{array}\right.$$

$$x \equiv 1 \pmod{6} \iff \left\{\begin{array}{lcll} x & \equiv & 1 & \pmod{2} \\ x & \equiv & 1 & \pmod{3} \end{array}\right.$$

$$x \equiv 4 \pmod{15} \iff \left\{\begin{array}{lcll} x & \equiv & 1 & \pmod{3} \\ x & \equiv & 4 & \pmod{5} \end{array}\right.$$

Un exemple (3)

$$\left\{ \begin{array}{rcll} x & \equiv & 1 & \pmod 9 \\ x & \equiv & 4 & \pmod{15} \end{array} \right. \quad \Longleftrightarrow \quad \left\{ \begin{array}{rcll} x & \equiv & 1 & \pmod 9 \\ x & \equiv & 1 & \pmod 3 \\ x & \equiv & 4 & \pmod 5 \end{array} \right.$$

$$x \equiv 1 \pmod 9 \quad \Longrightarrow \quad x \equiv 1 \pmod 3$$

$$\Longrightarrow \quad \left\{ \begin{array}{rcll} x & \equiv & 1 & \pmod 9 \\ x & \equiv & 4 & \pmod 5 \end{array} \right.$$

Le théorème chinois des restes (2)

Soit $m = m_1 \times m_2 \times \cdots \times m_r$ **alors l'application**

$$\mathbb{Z}/m\mathbb{Z} \leftrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_r\mathbb{Z}$$

est bijective. Le théorème des restes chinois permet de construire l'application réciproque.

Si $x = (x_1, x_2, \ldots, x_r)$ **et** $y = (y_1, y_2, \ldots, y_r)$ **alors :**

- $x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_r + y_r)$
- $x \times y = (x_1 \times y_1, x_2 \times y_2, \ldots, x_r \times y_r)$

Le théorème chinois des restes (3)

Un exemple avec $3 \times 5 = 15$.

$$
\begin{array}{lcl}
0 & \rightarrow & (0,0) \\
1 & \rightarrow & (1,1) \\
2 & \rightarrow & (2,2) \\
3 & \rightarrow & (0,3) \\
4 & \rightarrow & (1,4) \\
5 & \rightarrow & (2,0) \\
6 & \rightarrow & (0,1) \\
7 & \rightarrow & (1,2)
\end{array}
\qquad\qquad
\begin{array}{lcl}
8 & \rightarrow & (2,3) \\
9 & \rightarrow & (0,4) \\
10 & \rightarrow & (1,0) \\
11 & \rightarrow & (2,1) \\
12 & \rightarrow & (0,2) \\
13 & \rightarrow & (1,3) \\
14 & \rightarrow & (2,4)
\end{array}
$$

Ex1 : $3 + 8 = (0,3) + (2,3) = (2,6) = (2,1) = 11$

Ex2 : $2 \times 6 = (2,2) \times (0,1) = (0,2) = 12$

Application aux grands nombres

Comment additionner et multiplier : $x = 3589$ **et** $y = 11235$ **en ne faisant que des opérations sur des nombres de deux chiffres. On a :**

$$\begin{aligned} x &\equiv 25 \pmod{99} & \qquad y &\equiv 48 \pmod{99} \\ x &\equiv 61 \pmod{98} & y &\equiv 63 \pmod{98} \\ x &\equiv 0 \pmod{97} & y &\equiv 80 \pmod{97} \\ x &\equiv 74 \pmod{95} & y &\equiv 25 \pmod{95} \end{aligned}$$

$$\begin{aligned} x+y &\equiv 73 \pmod{99} & \qquad x \times y &\equiv 12 \pmod{99} \\ x+y &\equiv 26 \pmod{98} & x \times y &\equiv 21 \pmod{98} \\ x+y &\equiv 80 \pmod{97} & x \times y &\equiv 0 \pmod{97} \\ x+y &\equiv 4 \pmod{95} & x \times y &\equiv 45 \pmod{95} \\ x+y &= 14824 & x \times y &= 40322415 \end{aligned}$$

Une petite propriété

Si $a = bq + r$ **avec** $r < b$ **alors :**

$$2^a - 1 = 2^{bq+r} - 1 = 2^{bq}2^r + 2^r - 2^r - 1 = 2^r(2^{bq} - 1) + 2^r - 1$$

$$2^{bq} - 1 = (2^b)^q - 1^q = (2^b - 1)Q'$$
$$2^a - 1 = (2^b - 1)Q + 2^r - 1$$

En appliquant l'algorithme d'Euclide aux exposants on en déduit que :

$$(2^a - 1) \wedge (2^b - 1) = (2^{a \wedge b} - 1)$$

puis que si a **et** b **sont premiers entre eux alors :**

$$(2^a - 1) \wedge (2^b - 1) = 1$$

Des tests de divisibilité

Test 1 : **Un nombre est divisible par 2^k si ses k derniers chiffres sont divisibles par 2^k.**

$$10 \equiv 0 \pmod 2 \qquad\qquad 10^j \equiv 0 \pmod{2^j}$$

Test 2 : **Un nombre est divisible par 5^k si ses k derniers chiffres sont divisibles par 5^k.**

Test 3 : **Un nombre est divisible par 3 ou 9 si la somme de ses chiffres est divisible par 3 ou par 9.**

$$10 \equiv 1 \pmod 3 \qquad\qquad 10 \equiv 1 \pmod 9$$

c'est la preuve par 9.

Des tests de divisibilité (2)

Test 4 : Un nombre est divisible par 11 si la somme alternée de ses chiffres est divisible par 11.

$$10 \equiv -1 \pmod{11}$$

Ex : 723160823 est divisible par 11 car :
7-2+3-1+6-0+8-2+3 = 22

Test 5 : Un nombre est divisible par 7, 11 ou 13 si la somme alternée des blocs de 3 chiffres est divisible par 7, 11 ou 13.

$$7 \times 11 \times 13 = 1001 \qquad 1000 \equiv -1 \pmod{1001}$$

Ex 59358208 est divisible par 7 et 13 mais pas par 11 car :
59 - 358 + 208 = -91 = 910 = 13*7*10.

Calcul du jour de la semaine

On veut savoir à quel jour de la semaine correspond une date donnée. On va représenter les jours avec les entiers suivants :

Dimanche = 0	**Jeudi = 4**
Lundi = 1	**Vendredi = 5**
Mardi = 2	**Samedi = 6**
Mercredi = 3	

Pour Jules César l'année avait 365,25 jours ce qui ne correspond pas à la valeur exacte qui est de 365,2422 jours. Il y a donc une erreur d'environ 8 jours au bout de 1000 ans.

En 1582, il y avait 10 jours de retard

Calcul du jour de la semaine (2)

Le pape Grégoire décida donc de passer du 5 Octobre 1582 au 15 Octobre 1582, et il donna la règle du calendrier grégorien qui est encore utilisé aujourd'hui.

- **Les années bissextiles sont les années divisibles par 4 sauf les siècles**
- **Les siècles divisibles par 400 sont cependant bissextiles (Ex : 2000)**

Cela donne une durée d'année de 365,2425 jours ce qui donne encore une erreur de 1 jour pour 3000 ans.

Remarque : ce changement de calendrier a été effectué au Japon en 1873 et en Grèce en 1923.

Excel de Microsoft

27 février 1900	27 février 2000
28 février 1900	28 février 2000
29 février 1900	29 février 2000
1 mars 1900	1 mars 2000
2 mars 1900	2 mars 2000

Calcul du jour de la semaine (3)

Pour simplifier les calculs on va supposer que l'année commence le 1er Mars. C'est à dire que Février est le 12ème mois de l'année. On écrira l'année sous la forme $S \times 100 + A$.

Première étape : On va calculer le jour de la semaine du 1er Mars d'une année :

$$D \equiv 3 - 2 \times S + A + \lfloor S/4 \rfloor + \lfloor A/4 \rfloor \pmod 7$$

Ex : 1er Mars 2002 :

$$D \equiv 3 - 40 + 2 + 5 + 0 = -30 = 5 \pmod 7$$

C'est donc un Vendredi (prochain cours ! ! ! !).

Calcul du jour de la semaine (4)

Deuxième étape : **Il ne reste plus qu'a s'occuper du jour dans l'année. On remarque que**

$$31 \equiv 3 \pmod 7 \qquad 30 \equiv 2 \pmod 7$$

Il suffit alors de construire la table correspondante : $(3, 2, 3, 2, 3, 3, 2, 3, 2, 3, 3)$**. Mais on peut exprimer cette table avec la formule :** $\lfloor 2, 6 \times M - 0.2 \rfloor - 2$ **d'ou la formule finale :**

$$j \equiv J + \lfloor 2.6 \times M - 0.2 \rfloor - 2 \times S + A + \lfloor S/4 \rfloor + \lfloor A/4 \rfloor \pmod 7$$

Ex : 22 Février 2002 (22/12/2001)

$$j \equiv 22 + 31 - 40 + 1 + 5 + 0 = 19 = 5 \pmod 7$$

C'est donc un Vendredi