1. Les congruences

1.1. Introduction

Plusieurs mathématiciens sont à l'origine de ce domaine, parmi lesquels on peut citer Euler et surtout Gauss.

Pendant de nombreuses années, l'arithmétique modulaire a été un domaine sans application concrète. Depuis quelques années, le développement de l'électronique numérique et des transmissions ont engendré un intérêt croissant pour ce domaine et maintenant les techniques de chiffrement (on dit aussi cryptologie) font largement appel à l'arithmétique modulaire. Il en est de même des codes correcteurs d'erreurs largement utilisés dans des produits grand public comme les CD et les DVD et aussi dans les transmissions.

Si nous divisons 2 nombres entiers x et y par un entier n, nous obtenons 2 restes que nous appellerons x_1 et y_1. Si nous divisons $x - y$, $x + y$ ou xy par n, quels restes obtiendrons-nous ? Ces questions sont à l'origine de la notion de congruence et plus généralement de l'arithmétique modulaire.

D'une manière générale, pour l'étude des congruences, on utilise de préférence l'ensemble Z des entiers relatifs (négatifs ou positifs).

Ce chapitre aborde le sujet mais n'entre ni dans les détails ni dans toutes les démonstrations qui sont parfois un peu longues et sortent du cadre de ce livre.

Pour des raisons de commodité, tous les exemples numériques sont construits avec des entiers comportant peu de chiffres. Il faut cependant être conscient que diverses techniques, notamment les tests de primalité, ont été élaborées pour traiter des entiers comportant un grand nombre de chiffres (plus de 50 chiffres).

1.2. La notion de congruence

Si a et b admettent le même reste par division par l'entier p, on dit qu'ils sont congrus modulo p et on écrit :

$$a \equiv b \text{ modulo } p \quad \text{ou encore} \quad a \equiv b\ [p]$$

Tous les nombres donnant le même reste lors d'une division par l'entier p constituent un ensemble appelé congruence ou classe d'équivalence.

Si on divise des nombres par l'entier n, on pourra obtenir comme reste : 0, 1, 2, ... $(n - 1)$. Cela signifie que nous aurons au total n congruences dépendant de l'entier n.

Carl Friedrich Gauss a été un mathématicien très précoce : à l'âge de 10 ans, il avait trouvé la méthode pour calculer sans effort la somme des entiers de 1 à 100. Il n'avait que 24 ans, lorsque ses contemporains lui décernèrent le titre de « prince des mathématiques ». À 25 ans, il démontrait la loi de réciprocité quadratique sur laquelle Euler avait calé. Sa théorie des congruences est à la base de l'arithmétique modulaire qui a connu un grand développement, notamment pour les applications de cryptographie.

Notation : La réunion d'équivalence est souvent notée avec le symbole $\equiv$.

Les exemples suivants montrent que l'arithmétique modulaire fait partie de notre environnement :

L'horloge donne l'heure en modulo 12 : Si nous avons une horloge classique, elle nous donne l'heure modulo 12 sans indiquer la date. Nous devons lever l'indétermination par exemple entre 12 heures et minuit par la luminosité. Cela est aisé pour nous, mais peu commode dans un sous-marin !

Le jour de la semaine est donné modulo 7 : Par exemple, le 5 janvier 2009 est un lundi. Pour l'année 2009 les lundi seront tels que N° jour $\equiv 5$ modulo 7. Cela donne les 12, 19 et 26 janvier 2009.

Les longitudes sont données modulo 360 (car la Terre est sphérique).

Notation : Nous appelons $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes d'équivalences pour la congruence modulo n.

Quand on travaille avec des entiers relatifs, il faut tenir compte du signe dans la détermination de la congruence. Par exemple, si nous travaillons modulo 5, nous aurons 5 congruences :

- classe 0 qui contient : 0, 5, 10 etc.
- classe 1 qui contient : 1, 6, 11 etc.
- classe 2 qui contient : 2, 7, 12 etc.
- classe 3 qui contient : 3, 8, 13 etc.
- classe 4 qui contient : 4, 9, 14 etc.

Comment classer les nombres négatifs ?

Nous constatons que les nombres d'une même congruence modulo p diffèrent les uns des autres d'un multiple de p. Nous appliquons le même décalage dans le sens négatif, ce qui donne le résultat suivant modulo 5.

classe 0 : $-10, -5, 0, 5, 10, 15,$ etc.

classe 1 : $-9, -4, 1, 6, 11, 16, 21,$ etc.

classe 2 : $-8, -3, 2, 7, 12, 17, 22,$ etc.

classe 3 : $-7, -2, 3, 8, 13, 18, 23,$ etc.

classe 4 : $-6, -1, 4, 9, 14, 19, 24,$ etc.

Les congruences conduisent parfois à des résultats étonnants, au moins pour le néophyte : par exemple si nous travaillons modulo 24, nous pouvons dire que :

1, 25, 49 et 121 sont équivalents.

Cela signifie aussi que, **modulo** 24**,** 5**,** 7 **et** 11 **sont des racines carrées de** 1 ! Ce résultat n'est pas absurde. Nous verrons qu'il conduit à la notion de ***résidu quadratique*** auquel un chapitre est consacré.

Comment transformer un nombre négatif ? Si nous travaillons modulo p, pour passer d'un nombre négatif x à son équivalent dans les classes $[0, 1, .. , p-1]$, il suffit de lui ajouter le nombre kp qui permet d'obtenir un nombre entre 0 et $p-1$.

Exemple : modulo 17, -84 est équivalent à $-84 + 5 \times 17 = 1$

donc $-84 \equiv 1$ modulo 17

Notation : On utilise souvent les notations -1 ou $-x$ pour désigner respectivement $p-1$ ou $p-x$ modulo p. Mais il faut faire attention à la parité : si p est impair, x et $-x$ sont de parités opposées (comme 1 et – 1).

Définition du résidu : **Modulo p, pour tout nombre n, il existe un entier $a < p$ tel que**

$n = a \bmod p$

***a* est appelé le résidu de *n* modulo *p*.**

Cette désignation n'a rien à voir avec la notion de résidu quadratique qui sera étudiée plus loin.

1.3. Quelques propriétés des congruences

Les relations d'équivalences sont **réflexives** : Quel que soit a entier, $a \equiv a$

Elles sont **symétriques** : si $a \equiv b$ alors $b \equiv a$

Elles sont **transitives** : si $a \equiv b$ et $b \equiv c$ alors $a \equiv c \mod n$

Si $a \equiv b$ et $c \equiv d$ modulo n, alors $a + c \equiv b + d$ modulo n

Il y a *n* classes modulo *n* que nous pouvons noter :

$0, 1, 2, \ldots , n-1$

Il s'agit des ensembles d'entiers dont les divisions par n donnent respectivement pour reste :

$0, 1, 2, \ldots , n-1$

Les nombres relatifs entrent aussi dans les classes par une « translation » :

Si nous travaillons modulo p, nous aurons :

$-1 \equiv p-1 \qquad -2 \equiv p-2 \qquad -3 \equiv p-3$ etc.

Notation : L'ensemble des classes d'équivalence modulo n est noté Z/nZ et s'appelle l'ensemble des entiers modulo n.

Si a,b,c et d sont des entiers relatifs, qui vérifient :
$a \equiv b$ et $c \equiv d$
alors :
$-a \equiv -b$
$a + c \equiv b + d$
$ac \equiv bd$

Démonstration : Si $a \equiv b$ et $c \equiv d \mod n$, cela signifie que a et b donnent le même reste quand on les divise par n. Même chose pour c et d.

Quand on additionne a et c, on obtient un nombre dont la somme des restes est la même que si on additionne b et d ; d'où les relations citées précédemment.

Si m et n sont premiers entre eux et si $a \equiv b \mod m$ et si $a \equiv b \mod n$ alors $a \equiv b \mod mn$.

Exemple : $73 \equiv 3 \mod 10$ et $73 \equiv 3 \mod 7$ donc $73 \equiv 3 \mod 70$

Démonstration : Nous pouvons écrire :

$$a - b \equiv 0 \mod m$$
$$a - b \equiv 0 \mod n$$

Cela signifie $(a - b)$ est multiple à la fois de m et de n et donc de mn puisque m et n sont premiers entre eux, donc $a \equiv b \mod mn$.

1.4. Opérations sur les congruences

1.4.1. L'addition

L'addition de 2 nombres appartenant à des classes d'équivalences différentes se fait normalement, mais la question est la suivante : dans quelle classe devra aller le résultat ? Le calcul est simple à obtenir :

Par exemple, si nous travaillons modulo 7, et que nous additionnons 8 à 10, le résultat est 18, mais 8 est dans la classe 1, 10 est dans la classe 3 et le résultat est dans la classe 4. Si nous additionnons 12 et 9, 12 est dans la classe 5, 9 est dans la classe 2 et le résultat 21 est dans la classe 0. Cela nous conduit à élaborer une table d'addition pour les congruences.

Attention : Additionner 5 modulo 7 avec 15 modulo 19 n'a pas de sens ! **D'une manière générale, les opérations d'addition, de soustraction, de multiplication, etc. n'ont de sens que modulo un même nombre**.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Table d'addition modulo 7

L'addition bénéficie de diverses propriétés :

- elle est commutative : $a + b \equiv b + a$
- elle est associative : a + (b + c) ≡ (a + b) + c
- elle a un élément neutre (la congruence zéro)
- tout élément a un inverse : pour tout a, il existe b tel que : $a + b \equiv 0$

Avec l'opération d'addition, les congruences ont donc une structure de groupe commutatif (on dit aussi abélien).

1.4.2. La soustraction

Cette opération est comparable à l'addition.

Exemples :

Si $x \equiv 5$ modulo 12 et si $y \equiv 2$ modulo 12 alors nous aurons :

$x - y \equiv 3$ modulo 12

$2 - 5 \equiv 9$ modulo 12

1.4.3. La multiplication

La multiplication bénéficie également de différentes propriétés :

- elle est commutative,
- elle est associative,
- elle a un élément neutre (congruence 1),
- elle est distributive par rapport à l'addition.

Mais tout élément n'a pas systématiquement un inverse.

Comme pour l'addition, on peut construire, par exemple, la table de multiplication :

×	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

Table de multiplication modulo 7

Remarque : Nous avons vu que modulo n :

$$n - 1 \equiv -1$$

Cela signifie que $(n-1)^q \equiv (-1)^q$ et d'une manière générale que :

$$(n-x)^q \equiv (-x)^q$$

La seconde écriture est souvent pratique pour certains calculs.

1.4.4. Multiplication modulaire rapide

La multiplication modulaire est facile lorsque les nombres sont petits mais quand on s'intéresse aux techniques de cryptographie, il faut pouvoir effectuer plusieurs multiplications modulaires portant sur des grands nombres et surtout modulo un grand nombre. La technique classique devient alors pénible.

On peut alléger un peu le calcul en utilisant la fonction modulo à chaque fois que cela est possible :

Par exemple, soit à calculer : $X = (a \times b \times c) \bmod n$

Le calcul suivant est souvent préférable :

$$X = (((a \bmod n) \times b \bmod n) \times c \bmod n) \bmod n$$

A priori, il semble qu'il y ait plus d'opérations à effectuer, ce qui est vrai, mais cela évite de travailler sur des grands nombres (sauf si n est très grand).

L'algorithme de Montgomery permet d'effectuer ce type de calcul plus rapidement surtout lorsqu'il est répétitif. Il est spécialement conçu pour être utilisé sur des ordinateurs qui calculent en base 2.

1.4.5. Les nombres négatifs et les inégalités

Dans les mathématiques classiques, nous considérons qu'un nombre négatif a une représentation précise, notamment sur une droite orientée et qu'un tel nombre est inférieur à un nombre positif.

En arithmétique modulaire, **il n'y a ni nombre négatif, ni nombre positif** :

Si a est un entier noté positivement, nous pouvons toujours parler de $-a$, mais modulo p, $-a$ représente en fait $p-a$ qui est positif.

Les signes < et > n'ont plus de signification en arithmétique modulaire comme nous allons le voir sur les 3 exemples suivants **:**

Exemple 1 : Modulo 19, -3 est équivalent à 16 car $19-3=16$.

En fait, il n'y a plus de nombres mais uniquement des classes d'équivalences

Exemple 2 : Si nous pouvons écrivons :

$$3 < 17 \bmod 19$$

alors en additionnant 2 à chaque terme, nous obtenons :

$$3+2=5 > 17+2=0 \bmod 19$$

Exemple 3 : En arithmétique classique, la forme simplifiée de l'inégalité de Young est :

$$ab \le \frac{a^2}{2}+\frac{b^2}{2}$$

Prenons $a=4$ et $b=10$. En arithmétique classique nous aurons :

$$40 \le 8+50$$

Si maintenant nous travaillons modulo 43, nous aurons :

$$40 > 8+50 \equiv 15$$

Ces exemples montrent qu'il faut être très prudent quand on manie des inégalités.

La conclusion est que la méthode habituelle de comparaison des nombres n'a plus de sens.

En revanche les signes = et ≠ ont maintenant la signification suivante :

***x* = *y* signifie que *x* et *y* appartiennent à la même classe d'équivalence,**

***x* ≠ *y* signifie que *x* et *y* sont dans 2 classes d'équivalence différentes.**

En arithmétique modulaire, on préfère donc utiliser une autre métrique qui est la métrique p-adique qui sort du cadre de ce livre.

1.5. Les puissances en arithmétique modulaire

Le calcul se fait de façon similaire à celui des multiplications. Le tableau suivant montre les résultats modulo 13. Ce tableau se lit de la façon suivante : la valeur de a^x modulo 13 se trouve au croisement de la ligne horizontale correspondant à la valeur de a et de la verticale correspondant à x. Par exemple, 5^7 se trouve au croisement de la verticale 5 et de la ligne 7.

```
    Calcul de puissance modulo  p
table modulo :? 13
a   2   3   4   5   6   7   8   9  10  11  12  13  14  15  16  17
2   4   8   3   6  12  11   9   5  10   7   1   2   4   8   3   6
3   9   1   3   9   1   3   9   1   3   9   1   3   9   1   3   9
4   3  12   9  10   1   4   3  12   9  10   1   4   3  12   9  10
5  12   8   1   5  12   8   1   5  12   8   1   5  12   8   1   5
6  10   8   9   2  12   7   3   5   4  11   1   6  10   8   9   2
7  10   5   9  11  12   6   3   8   4   2   1   7  10   5   9  11
8  12   5   1   8  12   5   1   8  12   5   1   8  12   5   1   8
9   3   1   9   3   1   9   3   1   9   3   1   9   3   1   9   3
10  9  12   3   4   1  10   9  12   3   4   1  10   9  12   3   4
11  4   5   3   7  12   2   9   8  10   6   1  11   4   5   3   7
12  1  12   1  12   1  12   1  12   1  12   1  12   1  12   1  12
13  0   0   0   0   0   0   0   0   0   0   0   0   0   0   0   0
14  1   1   1   1   1   1   1   1   1   1   1   1   1   1   1   1
15  4   8   3   6  12  11   9   5  10   7   1   2   4   8   3   6
16  9   1   3   9   1   3   9   1   3   9   1   3   9   1   3   9
```

Puissances modulo p = 13

Cet exemple montre que la verticale 5 contient tous les entiers de 0 à 11. Cela signifie que modulo 13, 5 est un élément générateur que nous étudierons plus loin.

1.6. Congruence inverse

Nous avons vu que la multiplication avait un « élément neutre » qui est la congruence dont le reste est 1.

1.6.1. Inverse d'un nombre

Par définition, l'inverse d'un nombre x est un nombre x' tel que :

$$xx' = 1$$

Avec les nombres réels (ou complexes), à l'exception de 0, tout nombre est inversible.

En arithmétique classique, aucun nombre, à l'exception de 1 n'est inversible.

En arithmétique modulaire, la définition est la suivante :

Définition : 2 entiers *a* et *b* sont dits associés ou inverses modulo *n* si leur produit *ab* est congru à 1 modulo *n*. On dit aussi que *b* est l'inverse de *a* modulo *n*.

Exemples : si $n = 17$, 3 et 6 sont associés car $3 \times 6 = 18 \equiv 1 \bmod 17$

4 est l'inverse de 7 modulo 9 car :

$7 \equiv 4$ modulo 9, $4 \equiv 4$ modulo 9 mais $7 \times 4 = 28 \equiv 1$ modulo 9.

De même 16 est également l'inverse de 4 modulo 9.