Compléments de Mathématiques Discrètes: Cours 3 .

Michaël Quisquater (Maître de Conférences,UVSQ)

Rappel du cours 2

- Notion de plus grand commun diviseur (pgcd)
- Calcul de pgcd (via la factorisation, algorithme d'Euclide)
- Théorème de Bezout et algorithme d'Euclide étendu
- Construction d'un groupe additif à deux éléments et généralisation?

Addition de classes de congruence modulo n

Rappelons qu'une classe de congruence (modulo n) de représentant **a** est définie par:

$$[a + n\mathbb{Z}] = \{x \in \mathbb{Z} \mid x \sim_n a\}.$$

où

$$x \sim_n y \text{ si et seulement si } x - y \text{ est un multiple de } n.$$

Notons l'ensemble des classes de congruence modulo n, $\{[a + n\mathbb{Z}] \mid a \in \mathbb{Z}\}$ par $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$

Addition de classes de congruence modulo n

- On souhaite définir une addition sur les classes d'équivalence $\mathbb{Z}/n\mathbb{Z}$ (comme on l'avait déjà fait sur les classe des nombres pairs et impairs qui ne sont rien d'autre que $\mathbb{Z}/2\mathbb{Z}$).
- Il s'agit d'associer à n'importe quelle paire de classes une troisième classe.
- Afin de bénéficier des propriétés du groupe $(\mathbb{Z}, +)$ nous allons définir cette association au moyen d'opérations dans $\mathbb{Z}$ (au niveau des représentant).

Addition de classes de congruence modulo n (suite)

Définition (Addition classe de congruence modulo n)

Pour tout $a, b \in \mathbb{Z}$ et tout entier $n \in \mathbb{Z}$, nous définissons le produit des classes de congruence $[a+n\mathbb{Z}]$ et $[b+n\mathbb{Z}]$ par

$$[a+n\mathbb{Z}]+[b+n\mathbb{Z}]=[(a+b)+n\mathbb{Z}]\,.$$

Cette opération est appelée "addition de classes de congruence modulo n".

Anneau des classes de congruence modulo n (suite)

Remarques:

1. Notons qu'il faudrait montrer que la définition de cette addition est bien définie et qu'en particulier elle ne dépend pas du choix des représentants des classes.
2. Notons que les sommes de n'importe quel nombre de $[a+n\mathbb{Z}]$ avec n'importe quel nombre de $[b+n\mathbb{Z}]$ couvre nécessairement tous les nombres de $[(a+b)+n\mathbb{Z}]$.
3. L'addition de classes de congruence modulo n est commutative.

Addition de classes de congruence modulo n (suite)

Exemple:

Nous avons $[1+7\mathbb{Z}]+[365+7\mathbb{Z}]=[366+7\mathbb{Z}]$.

Aussi, $[366+7\mathbb{Z}]=[2+7\mathbb{Z}]$ car $366=2+52\cdot 7$.

Finalement, $[1+7\mathbb{Z}]+[365+7\mathbb{Z}]=[2+7\mathbb{Z}]$.

Groupe des classes de congruence modulo n

Théorème

$(\mathbb{Z}/n\mathbb{Z},+)$ forme un groupe commutatif pour l'addition (définie au théorème précédent). L'élément neutre est $[n\mathbb{Z}]$. L'opposé d'une classe $[a+n\mathbb{Z}]$ est $-[a+n\mathbb{Z}]=[-a+n\mathbb{Z}]$.

Groupe des classes de congruence modulo n (exemple)

Exemple: Considérons $(\mathbb{Z}/4\mathbb{Z}, +)$.

Il s'agit des classes $[0 + 4\mathbb{Z}]$, $[1 + 4\mathbb{Z}]$, $[2 + 4\mathbb{Z}]$ et $[3 + 4\mathbb{Z}]$.

La table de l'opération d'addition modulo 4 est:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

Anneau des classes de congruence modulo n (suite)

But: Construire un anneau de classe de congruence modulo n.

Méthode: Ajouter une opération de multiplication au groupe des classes de congruences modulo n et vérifier que la structure ainsi construite satifasse bien la définition d'un anneau.

Anneau des classes de congruence modulo n (suite)

Définition (Multiplication de classe de congruence modulo n)

Pour tout $a, b \in \mathbb{Z}$ et tout entier $n \in \mathbb{Z}$, nous définissons le produit des classes de congruence $[a + n\mathbb{Z}]$ et $[b + n\mathbb{Z}]$ par

$$[a + n\mathbb{Z}] \cdot [b + n\mathbb{Z}] = [(a \cdot b) + n\mathbb{Z}] .$$

Cette opération est appelée "multiplication de classes de congruence modulo n".

Anneau des classes de congruence modulo n (suite)

Remarques:

1. Notons qu'il faudrait montrer que la définition de ce produit soit bien définie et qu'en particulier il ne dépend pas du choix des représentants des classes.
2. Notons que les produits de n'importe quel nombre de $[a + n\mathbb{Z}]$ avec n'importe quel nombre de $[b + n\mathbb{Z}]$ ne couvre pas nécessairement tous les nombres de $[(a \cdot b) + n\mathbb{Z}]$.
3. La multiplication de classes de congruence modulo n est commutative.

Anneau des classes de congruence modulo n (suite)

Nous pouvons donc munir l'ensemble des classes de congruence modulo n d'une opération d'addition et de multiplication.

Il est possible de montrer le résultat suivant:

Théorème

Soit n un entier. $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$ ou encore $(\mathbb{Z}_n,+,\cdot)$ forme un anneau commutatif. Le neutre de l 'addition (resp. la multiplication) est la classe de congruences $[n\mathbb{Z}]$ (resp. $[1+n\mathbb{Z}]$).

Anneau des classes de congruence modulo n (exemple)

Exemple: Considérons le groupe additif $(\mathbb{Z}/4\mathbb{Z},+)$. Celui-ci se compose des classes $[0+4\mathbb{Z}]$, $[1+4\mathbb{Z}]$, $[2+4\mathbb{Z}]$ et $[3+4\mathbb{Z}]$.

Considérons de plus l'opération de multiplication de classes de congruence modulo 4.

La table de l'opération de multiplication modulo 4 est:

$\times$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Anneau des classes de congruence modulo n (suite)

Remarque:

- les classes de congruences $\overline{0}$ et $\overline{2}$ n'ont pas d'inverse multiplicatif
- $\overline{1}$ et $\overline{3}$ sont leur propre inverse multiplicatif
- $\mathbb{Z}_4^* = \{\overline{1}, \overline{3}\}$ (A^* dénote l'ensemble des éléments inversible de $(A, +, \cdot)$)

Caractérisation des classes de congruences inversibles modulo n

Comment savoir si une classe est inversible?

Considérons la classe de congruence $[a + n\mathbb{Z}]$. L'inverse de cette classe est une classe $[b + n\mathbb{Z}]$ satisfaisant la relation

$$[a + n\mathbb{Z}] \cdot [b + n\mathbb{Z}] = [1 + n\mathbb{Z}] = [b + n\mathbb{Z}] \cdot [a + n\mathbb{Z}] .$$

Comme la multiplication modulo n est commutative cette double égalité se réduit à

$$[a + n\mathbb{Z}] \cdot [b + n\mathbb{Z}] = [1 + n\mathbb{Z}] .$$

Par définition de la multiplication,

$$[a + n\mathbb{Z}] \cdot [b + n\mathbb{Z}] = [a \cdot b + n\mathbb{Z}] .$$

Caractérisation des classes de congruences inversibles modulo n (suite)

Par conséquent, le calcul d'inverse consiste à déterminer un représentant $b \in \mathbb{Z}$ tel $[a \cdot b + n\mathbb{Z}] = [1 + n\mathbb{Z}]$ ou encore

$$[a \cdot b + n\mathbb{Z}] + (-[1 + n\mathbb{Z}]) = [n\mathbb{Z}]$$

c-à-d

$$[(a \cdot b - 1) + n\mathbb{Z}] = [n\mathbb{Z}]$$

En d'autres termes, il faut déterminer $b \in \mathbb{Z}$ de telle façon que $a \cdot b - 1$ soit un multiple de n ou encore $a \cdot b - 1 = -k \cdot n$ pour un certain $k \in \mathbb{Z}$. On en déduit qu'il faut déterminer $b \in \mathbb{Z}$ pour lequel

$$k \cdot n + b \cdot a = 1\,,$$

pour un certain $k \in \mathbb{Z}$. $\rightarrow$ relation de Bezout!

Caractérisation des classes de congruences inversibles modulo n (suite)

Par conséquent, si $pgcd(a, n) = 1$, on peut calculer les coefficients de Bezout (k et b).

b est un représentant de la classe de congruence inverse de la classe $[a + n\mathbb{Z}]$

D'autre part, si $pgcd(a, n) \neq 1$ cela signifie qu'il existe $k' \in \mathbb{Z}$ (avec k' différent de 1 ou -1) tel que $n = k' \cdot n'$ et $a = k' \cdot a'$. En particulier, cela signifie que $k \cdot n + b \cdot a = k' \cdot (k \cdot n' + b \cdot a')$. Il s'agit donc d'un multiple de k' et cette expression ne peut jamais être égale à 1. On en déduit donc que si $pgcd(a, n) \neq 1$, la classe $[a + n\mathbb{Z}]$ n'est pas inversible. De cette discussion resulte le théorème de caractérisation :

Caractérisation des classes de congruences inversibles modulo *n* (suite)

Théorème

Soit n un naturel supérieur ou égal à 2. $[a + n\mathbb{Z}]$ *(avec* $a \in \mathbb{Z}$*) est inversible pour la multiplication modulo n si et seulement si* $pgcd(a, n) = 1$.

Calcul de l'inverse d'une classe de congruence

Donnons à présent un exemple de calcul d'inverse d'une classe de congruence.

Cherchons l'inverse de la classe $\overline{3} \in \mathbb{Z}_{40}$.

La classe $\overline{3}$ est inversible. En effet, $pgcd(3, 40) = 1$ (voir ci-dessous)

Calculons un représentant de la classe inverse de $\overline{3}$. Pour ce faire, calculons les coefficients de Bezout $a, b \in \mathbb{N}$ tel que $a \cdot 40 + b \cdot 3 = 1$.

L'algorithme d'Euclide étendu donne les valeurs suivantes:

Calcul de l'inverse d'une classe de congruence (suite)

k	0	1	2	3
r_k	40	3	1	0
q_k	-	13	3	-
x_k	1	0	1	-
y_k	0	1	-13	-

Nous déduisons que $a = 1$ et $b = -13$.

On vérifie que l'on a bien $3 \cdot (-13) + 1 \cdot 40 = 1$.

Un représentant de la classe inverse de $\overline{3}$ est donc -13.

Le représentant minimal de la classe $\overline{-13}$ de $\mathbb{Z}_{40}$ est 27. En effet, $[-13 + 40\mathbb{Z}] = [27 + 40\mathbb{Z}]$. Par conséquent,

$$\overline{3}^{-1} = \overline{-13} = \overline{27}\,.$$

Groupe multiplicatif de $(\mathbb{Z}_n,+,\cdot)$

Critère d'inversibilité: $[a + n\mathbb{Z}]$ est inversible pour la multiplication si son représentant a est relativement premier avec n.

Cela signifie qu'il existe en général des éléments non-inversibles dans $(\mathbb{Z}_n,+,\cdot)$.

Considérons l'ensemble des éléments inversibles (pour la multiplication) de $(\mathbb{Z}_n,+,\cdot)$. Notons cet ensemble $\mathbb{Z}_n^*$.

Groupe multiplicatif de $(\mathbb{Z}_n, +, \cdot)$ (suite)

$(\mathbb{Z}_n^*, \cdot)$ est un groupe car

- $\cdot : \mathbb{Z}_n^* \times \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ (le produit d'éléments inversibles est inversible)
- la multiplication des classes de congruence est associative
- $[1 + n\mathbb{Z}] \in \mathbb{Z}_n^*$ ($[1 + n\mathbb{Z}]$ est son propre inverse)
- l'inverse de tout élément inversible est inversible et donc appartient à $(\mathbb{Z}_n^*, \cdot)$

Cardinalité de $(\mathbb{Z}_n^*, \cdot)$

Objectif: Calculer le nombre d'éléments de $(\mathbb{Z}_n^*, \cdot)$.

La cardinalité de $(\mathbb{Z}_n, +, \cdot)$ est n. Les representants minimaux des différentes classes sont les entiers compris entre 0 et $n - 1$. Notons que $[n\mathbb{Z}]$ n'a pas d'inverse multiplicatif.

Les classes inversibles sont celles dont les représentants sont relativement premiers avec n.

Par conséquent, le nombre de classe inversible pour $n \geq 2$ est la cardinalité de

$$\{k \mid 1 \leq k \leq n \text{ et } pgcd(k, n) = 1\}.$$

Remarque: cette cardinalité ne dépend que de n. Notons que si $n = 0$, $\mathbb{Z}_n = \mathbb{Z}$ et si $n = 1$ $\mathbb{Z}_n = \{0\}$.

Fonction totient d'Euler

Définissons la fonction totient d'Euler par

$$\Phi : \mathbb{N} \to \mathbb{N} : n \mapsto \Phi(n) = \mid \{k \mid 1 \leq k \leq n \text{ et } pgcd(k,n) = 1\} \mid .$$

Si $n \geq 2$, Cette fonction représente la cardinalité de $\mathbb{Z}_n^*$, i.e.

$$\mid \mathbb{Z}_n^* \mid = \Phi(n) .$$

Comment calculer efficacement $\Phi(n)$?

Par définition, $\Phi(0) = 0$ et $\Phi(1) = 1$.

Evaluons $\phi(p^\alpha)$ où p est un nombre premier et α un naturel non-nul.

Evaluation de $\phi(p^\alpha)$

Il s'agit d'évaluer le nombre d'entiers compris entre 1 et p^α relativement premiers avec p^α. Autrement dit, il s'agit de tous les nombres compris entre 1 et p^α à l'exception des multiples de p.

- Il y a p^α nombres entre 1 et p^α et
- Il y a $p^{\alpha-1}$ qui sont multiples de p et compris entre 1 et p^α.

Nous avons donc que $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Propriété de la fonction totient d'Euler

Théorème

Soit $\Phi : \mathbb{N} \to \mathbb{N}$ *la fonction totient d'Euler. Alors,*

1. $\Phi(0) = 0$,
2. $\Phi(1) = 1$,
3. $\Phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ *pour tout premier* p *et tout naturel* α *non-nul* ,
4. $\Phi(m \cdot n) = \Phi(m) \cdot \Phi(n)$ *pour tout naturel* m, n *relativement premiers* .

Calcul de $\Phi(n)$ pour un natrurel n quelconque

Par le théorème fondamental de l'arithmétique $n = \prod_{i \in I} p_i^{\alpha_i}$ avec p_i des premiers distincts et α_i des naturels strictement positifs.

Observons que $pgcd(p_i^{\alpha_i}, p_j^{\alpha_j}) = 1$ si $i \neq j$.

Par conséquent,

$$\Phi(n) = \Phi(\prod_{i \in I} p_i^{\alpha_i}) = \prod_{i \in I} \Phi(p_i^{\alpha_i}) = \prod_{i \in I} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) .$$

Calcul de $\Phi(n)$ pour un natrurel n quelconque (suite)

Corollaire

Soit un nombre naturel non-nul $n \in \mathbb{N}$ dont la factorisation est $n = \prod_{i\in I} p_i^{\alpha_i}$ avec p_i des premiers distincts et α_i des naturels strictement positifs. Alors,

$$\Phi(n) = \prod_{i\in I}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}),$$

En particulier, si $n = p \cdot q$ avec p et q des nombres premiers distincts, nous avons

$$\Phi(n) = (p-1)\cdot(q-1).$$

Remarque: cette formule nécessite de factoriser n.

Corps commutatif fini

Nous savons que $(\mathbb{Z}_p,+,\cdot)$ est un anneau commutatif.

Aussi, si p est premier $\Phi(p) = p - 1$. Cela signifie que tous les classes de congruence non-nulles de $\mathbb{Z}_p$ sont inversibles. Par conséquent,

Corollaire

$(\mathbb{Z}_p,+,\cdot)$ est un corps commutatif si p est premier.

Ce corollaire signifie que $(\mathbb{Z}_p,+,\cdot)$ a une structure algébrique similaire à celles de $(\mathbb{R},+,\cdot)$ et $(\mathbb{Q},+,\cdot)$.

Théorème d'Euler et de Fermat

... ou la vrai raison de l'usage en cryptographie des anneaux de classes de congruence modulo n

Cette section nous informe que si on multiplie une classe inversible par elle-même un certain nombre de fois on tombe sur le neutre multiplicatif.

Les deux résultats suivants nous donne une indication sur ce nombre de fois.

Théorème d'Euler

Théorème

Soit n un naturel supérieur ou égal à deux. Soit $a \in \mathbb{Z}$ tel que $pgcd(a,n) = 1$, alors

$$a^{\Phi(n)} = 1 \bmod n$$

De façon équivalente, si $\overline{a}$ dénote la classe de congruence $[a + n\mathbb{Z}]$ alors pour tout $\overline{a} \in \mathbb{Z}_n^*$,

$$\overline{a}^{\Phi(n)} = \overline{1}\,.$$

Remarque: $\Phi(n)$ n'est pas nécessairement le nombre minimal de fois qu'il faut multiplier une classe inversible par elle-même pour tomber sur le neutre. $\Phi(n)$ est un multiple du nombre minimal (à montrer!).

Preuve du théorème d'Euler

Considérons le groupe multiplicatif $\mathbb{Z}_n^*$. Considérons l'application

$$\Gamma_{\overline{\alpha}} : \mathbb{Z}_n^* \to \mathbb{Z}_n^* : \overline{x} \mapsto \overline{\alpha} \cdot \overline{x},$$

où $\overline{\alpha} \in \mathbb{Z}_n^*$.

Cette application est une bijection, en effet l'application inverse est

$$\Gamma_{\overline{\alpha}}^{-1} : \mathbb{Z}_n^* \to \mathbb{Z}_n^* : \overline{x} \mapsto \overline{\alpha}^{-1} \cdot \overline{x}\,.$$

Notons que le produit des éléments de $\mathbb{Z}_n^*$ est égal au produit des éléments permutés de ce groupe.

Preuve du théorème d'Euler (suite)

En particulier, nous avons que

$$\prod_{\overline{x}\in\mathbb{Z}_n^*} \overline{x} = \prod_{\overline{x}\in\mathbb{Z}_n^*} \Gamma(\overline{x}) = \prod_{\overline{x}\in\mathbb{Z}_n^*} \overline{\alpha}\cdot\overline{x} = \overline{\alpha}^{|\mathbb{Z}_n^*|} \prod_{\overline{x}\in\mathbb{Z}_n^*} \overline{x} = \overline{\alpha}^{\Phi(n)} \prod_{\overline{x}\in\mathbb{Z}_n^*} \overline{x}\,.$$

Comme $\prod_{\overline{x}\in\mathbb{Z}_n^*} \overline{x}$ est le produit d'éléments inversibles, cet élément est inversible. On peut donc simplifier l'équation précédente et on obtient:

$$\overline{\alpha}^{\Phi(n)} = \overline{1}\,.$$

□

Petit théorème de Fermat

Corollaire

(Petit théorème de Fermat) Soit p un nombre premier. Alors pour tout entier a non multiple de p

$$a^{p-1} = 1 \bmod p\,.$$

Autrement dit, pour tout élément $\overline{a} \in \mathbb{Z}_p \setminus \overline{0}$ *(c'est-à-dire* $\mathbb{Z}_p^*$*), nous avons*

$$\overline{a}^{p-1} = \overline{1}\,.$$

Preuve. Il suffit d'appliquer le théorème d'Euler au naturel $n = p$ où p est premier. □

Conclusion

- Classes de congruence, relation d'équivalence
- Groupe additif des classes de congruence modulo n
- Anneau des classes de congruence modulo n
- Caractérisation des classes de congruence inversibles
- Calcul de l'inverse d'une classe de congruence inversible