Ecole Supérieure Polytechnique
Laboratoire d'Informatique,
de Télécommunications et Applications
LITA

Outils mathématiques pour la cryptologie

Pr Gervais MENDY
gervais.mendy@esp.sn

Département Génie Informatique, École Supérieure Polytechnique ESP-UCAD

March 13, 2024

Plan du chapitre

Plan du chapitre

Plan du chapitre

Plan du chapitre

Plan du chapitre

Plan du chapitre

Plan du chapitre

Plan du chapitre

Groupes

Définitions

Un ensemble G muni d'une loi de composition interne (notée multiplicativement en général) est un **groupe** si:

- la loi est associative: $(\forall a, b, c \in G)$ $(ab)c = a(bc)$

Groupes

Définitions

Un ensemble G muni d'une loi de composition interne (notée multiplicativement en général) est un **groupe** si:

- la loi est associative: $(\forall a, b, c \in G) \qquad (ab)c = a(bc)$
- elle admet un élément neutre e: $(\forall a \in G) \qquad ae = ea = a$

Groupes

Définitions

Un ensemble G muni d'une loi de composition interne (notée multiplicativement en général) est un **groupe** si:

- la loi est associative: $(\forall a, b, c \in G) \qquad (ab)c = a(bc)$
- elle admet un élément neutre e: $(\forall a \in G) \qquad ae = ea = a$
- tout élément a de G admet un inverse a^{-1}: $aa^{-1} = a^{-1}a = e$

Groupe commutatif

Définitions

- Lorsque la loi est commutative, on dit que G est un **groupe commutatif**.

Presque tous les groupes que l'on rencontre en cryptographie sont abéliens.

Groupe commutatif

Définitions

- Lorsque la loi est commutative, on dit que G est un **groupe commutatif**.
- On note alors en général sa loi ***additivement*** (et le symétrique de a se nomme l'opposé de a et se note $-a$).

Presque tous les groupes que l'on rencontre en cryptographie sont abéliens.

Groupe commutatif

Définitions

- Lorsque la loi est commutative, on dit que G est un **groupe commutatif**.
- On note alors en général sa loi ***additivement*** (et le symétrique de a se nomme l'opposé de a et se note $-a$).
- Un groupe qui est commutatif est souvent appelé **groupe abélien**.

Presque tous les groupes que l'on rencontre en cryptographie sont abéliens.

Groupe commutatif

Générateur de groupe

Un groupe abélien est appelé cyclique s'il existe un élément spécial, appelé générateur, à partir duquel tous les autres éléments peuvent être obtenus soit par application (ou composition) répétée de l'opération de groupe, soit par l'utilisation de l'opération inverse.

- Par exemple, dans l'ensemble des entiers relatifs muni de la loi addition, chaque entier positif peut être obtenu par addition répétée de 1 à lui-même.

Groupe commutatif

Générateur de groupe

Un groupe abélien est appelé cyclique s'il existe un élément spécial, appelé générateur, à partir duquel tous les autres éléments peuvent être obtenus soit par application (ou composition) répétée de l'opération de groupe, soit par l'utilisation de l'opération inverse.

- Par exemple, dans l'ensemble des entiers relatifs muni de la loi addition, chaque entier positif peut être obtenu par addition répétée de 1 à lui-même.
- Chaque entier négatif peut être obtenu à partir d'un entier positif par application de l'opérateur inverse additif, $x \rightarrow -x$.

Groupe commutatif

Générateur de groupe

Un groupe abélien est appelé cyclique s'il existe un élément spécial, appelé générateur, à partir duquel tous les autres éléments peuvent être obtenus soit par application (ou composition) répétée de l'opération de groupe, soit par l'utilisation de l'opération inverse.

- Par exemple, dans l'ensemble des entiers relatifs muni de la loi addition, chaque entier positif peut être obtenu par addition répétée de 1 à lui-même.
- Chaque entier négatif peut être obtenu à partir d'un entier positif par application de l'opérateur inverse additif, $x \rightarrow -x$.
- On dit que 1 est un générateur des entiers relatifs sous la loi additive.

Groupe commutatif

Générateur de groupe

Si g est un générateur du groupe cyclique G, on écrit souvent $G = \langle g \rangle$.

- Si G est multiplicatif, alors tout élément h de G peut être écrit comme $h = g^x$.

Groupe commutatif

Générateur de groupe

Si g est un générateur du groupe cyclique G, on écrit souvent $G = \langle g \rangle$.

- Si G est multiplicatif, alors tout élément h de G peut être écrit comme $h = g^x$.
- Si G est additif, alors tout élément h de G peut être écrit comme $h = x \cdot g$

Groupe commutatif

Générateur de groupe

Si g est un générateur du groupe cyclique G, on écrit souvent $G = \langle g \rangle$.

- Si G est multiplicatif, alors tout élément h de G peut être écrit comme $h = g^x$.
- Si G est additif, alors tout élément h de G peut être écrit comme $h = x \cdot g$
- x est dans les deux cas un entier appelé le **logarithme discret** de h à la base g.

Anneaux

Définitions

Soit $(A, +, \cdot)$ un ensemble muni de deux lois de composition interne. On dit que $(A, +, \cdot)$ est un **anneau** si

- $(A, +)$ est un groupe commutatif

Anneaux

Définitions

Soit $(A, +, \cdot)$ un ensemble muni de deux lois de composition interne. On dit que $(A, +, \cdot)$ est un **anneau** si

- $(A, +)$ est un groupe commutatif
- $(A, \cdot)$ est un magma associatif

Anneaux

Définitions

Soit $(A, +, \cdot)$ un ensemble muni de deux lois de composition interne. On dit que $(A, +, \cdot)$ est un **anneau** si

- $(A, +)$ est un groupe commutatif
- $(A, \cdot)$ est un magma associatif
- la loi multiplicative $\cdot$ est distributive par rapport à la loi additive $+$

Anneaux

Définitions

- Si la deuxième loi est commutative, on dit que l'anneau est commutatif.

En fait, dans la cryptographie, on considère la plupart du temps les anneaux finis, comme l'anneau commutatif des classes résiduelles modulo n, $\mathbb{Z}/n\mathbb{Z}$.

Anneaux

Définitions

- Si la deuxième loi est commutative, on dit que l'anneau est commutatif.
- Dans le cas où la loi multiplicative admet un élément neutre (noté en général 1), on dit l'anneau est **unifère** (ou **unitaire**).

En fait, dans la cryptographie, on considère la plupart du temps les anneaux finis, comme l'anneau commutatif des classes résiduelles modulo n, $\mathbb{Z}/n\mathbb{Z}$.

Anneaux

Définitions

- Si la deuxième loi est commutative, on dit que l'anneau est commutatif.
- Dans le cas où la loi multiplicative admet un élément neutre (noté en général 1), on dit l'anneau est **unifère** (ou **unitaire**).
- On appelle **corps** un anneau unifère où tout élément non nul est inversible. Un corps commutatif est appelé **champ**.

En fait, dans la cryptographie, on considère la plupart du temps les anneaux finis, comme l'anneau commutatif des classes résiduelles modulo n, $\mathbb{Z}/n\mathbb{Z}$.

Théorie des nombres

Introduction

Aujourd'hui, les algorithmes de la théorie des nombres sont largement utilisés, notamment en raison de la création de modèles cryptographiques fondés sur les grands nombres premiers. La faisabilité de ces modèles dépend de notre capacité à trouver facilement de grands nombres premiers, alors que leur sécurité dépend de notre incapacité à factoriser le produit de grands nombres premiers.

Propriètès de divisibilitè

Notions de divisibilité

- On dit que l'entier b divise l'entier a s'il existe un entier k tel que $b \cdot k = a$. On note $b|a$

Thèorème

Pour tout entier a et tout entier positif n, il existe deux entiers q et r uniques tels que $0 \leq r < n$ et $a = qn + r$.

Propriètès de divisibilitè

Notions de divisibilité

- On dit que l'entier b divise l'entier a s'il existe un entier k tel que $b \cdot k = a$. On note $b|a$
- On dit d'un entier $a > 1$ dont les seuls diviseurs sont les diviseurs triviaux 1 et a que c'est un **nombre premier**.

Thèorème

Pour tout entier a et tout entier positif n, il existe deux entiers q et r uniques tels que $0 \leq r < n$ et $a = qn + r$.

Propriètès de divisibilitè

Notions de divisibilité

- On dit que l'entier b divise l'entier a s'il existe un entier k tel que $b \cdot k = a$. On note $b|a$
- On dit d'un entier $a > 1$ dont les seuls diviseurs sont les diviseurs triviaux 1 et a que c'est un **nombre premier**.
- On dit d'un entier $a > 1$ qui n'est pas premier qu'il est **composé**.

Thèorème

Pour tout entier a et tout entier positif n, il existe deux entiers q et r uniques tels que $0 \leq r < n$ *et* $a = qn + r$.

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.
- Si $a - b$ est un multiple de n, on dit que a est ***congru*** à b ***modulo*** n et on écrit $a \equiv b \pmod{n}$.

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.
- Si $a - b$ est un multiple de n, on dit que a est ***congru*** à b ***modulo*** n et on écrit $a \equiv b \pmod{n}$.
- La relation $a \equiv b \pmod{n}$ est une **relation d'équivalence**.

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.
- Si $a - b$ est un multiple de n, on dit que a est ***congru*** à b ***modulo*** n et on écrit $a \equiv b \pmod{n}$.
- La relation $a \equiv b \pmod{n}$ est une **relation d'équivalence**.
- Chaque classe d'équivalence contient un unique entier r vérifiant $0 \leq r < n$;

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.
- Si $a - b$ est un multiple de n, on dit que a est ***congru*** à b ***modulo*** n et on écrit $a \equiv b \pmod{n}$.
- La relation $a \equiv b \pmod{n}$ est une **relation d'équivalence**.
- Chaque classe d'équivalence contient un unique entier r vérifiant $0 \leq r < n$;
- c'est le **résidu** commun à tous les éléments de la classe.

Propriètès de divisibilitè

Congruences

Soient a et b deux entiers relatifs.

- La valeur $r = a \mod n$ est le reste de la division.
- Si $a - b$ est un multiple de n, on dit que a est ***congru*** à b ***modulo*** n et on écrit $a \equiv b \pmod{n}$.
- La relation $a \equiv b \pmod{n}$ est une **relation d'équivalence**.
- Chaque classe d'équivalence contient un unique entier r vérifiant $0 \leq r < n$;
- c'est le **résidu** commun à tous les éléments de la classe.
- L'ensemble des classes d'équivalence s'appelle l'ensemble des ***entiers modulo n*** et on le note $\mathbb{Z}/n\mathbb{Z}$ ou $\mathbb{Z}_n$

Propriétés de divisibilité

Relation et classe d'équivalence

- Les entiers peuvent être divisés en n **classes d'équivalence** en fonction du reste de leur division par n.

Propriétés de divisibilité

Relation et classe d'équivalence

- Les entiers peuvent être divisés en n **classes d'équivalence** en fonction du reste de leur division par n.
- La classe d'équivalence modulo n qui contient un entier a est $[a]_n = \{a + kn : k \in \mathbb{Z}\}$

Propriétés de divisibilité

Relation et classe d'équivalence

- Les entiers peuvent être divisés en n **classes d'équivalence** en fonction du reste de leur division par n.
- La classe d'équivalence modulo n qui contient un entier a est $[a]_n = \{a + kn : k \in \mathbb{Z}\}$
- Par exemple, $[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$; cet ensemble se note aussi $[-4]_7$ ou $[10]_7$.

Propriétés de divisibilité

Relation et classe d'équivalence

- Les entiers peuvent être divisés en n **classes d'équivalence** en fonction du reste de leur division par n.
- La classe d'équivalence modulo n qui contient un entier a est $[a]_n = \{a + kn : k \in \mathbb{Z}\}$
- Par exemple, $[3]_7 = \{\ldots, -11, -4, 3, 10, 17, \ldots\}$; cet ensemble se note aussi $[-4]_7$ ou $[10]_7$.
- On peut dire qu'écrire $a \in [b]_n$ est la même chose qu'écrire $a \equiv b \pmod{n}$.

Propriétés de divisibilité

Relation et classe d'équivalence

- Les entiers peuvent être divisés en n **classes d'équivalence** en fonction du reste de leur division par n.
- La classe d'équivalence modulo n qui contient un entier a est $[a]_n = \{a + kn : k \in \mathbb{Z}\}$
- Par exemple, $[3]_7 = \{..., -11, -4, 3, 10, 17, ...\}$; cet ensemble se note aussi $[-4]_7$ ou $[10]_7$.
- On peut dire qu'écrire $a \in [b]_n$ est la même chose qu'écrire $a \equiv b \pmod{n}$.
- L'ensemble de toutes ces classes d'équivalence est

$$\mathbb{Z}_n = \{[a]_n : 0 \leq a \leq n - 1\} \tag{1}$$

Propriétés de divisibilité

Relation et classe d'équivalence (suite)

- ou

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{2}$$

Propriétés de divisibilité

Relation et classe d'équivalence (suite)

- ou

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{2}$$

- la définition $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ sera comprise comme étant équivalente à l'équation 1 en gardant à l'esprit que 0 représente $[0]_n$, 1 représente $[1]_n$, etc ;

Propriétés de divisibilité

Relation et classe d'équivalence (suite)

- ou

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{2}$$

- la définition $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ sera comprise comme étant équivalente à l'équation 1 en gardant à l'esprit que 0 représente $[0]_n$, 1 représente $[1]_n$, etc ;
- chaque classe est représentée par son plus petit élément positif ou nul.

Propriétés de divisibilité

Relation et classe d'équivalence (suite)

- ou

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{2}$$

- la définition $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ sera comprise comme étant équivalente à l'équation 1 en gardant à l'esprit que 0 représente $[0]_n$, 1 représente $[1]_n$, etc ;
- chaque classe est représentée par son plus petit élément positif ou nul.
- Toutefois, il ne faut pas oublier les classes d'équivalence correspondantes.

Propriétés de divisibilité

Relation et classe d'équivalence (suite)

- ou

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\} \tag{2}$$

- la définition $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ sera comprise comme étant équivalente à l'équation 1 en gardant à l'esprit que 0 représente $[0]_n$, 1 représente $[1]_n$, etc ;
- chaque classe est représentée par son plus petit élément positif ou nul.
- Toutefois, il ne faut pas oublier les classes d'équivalence correspondantes.
- Par exemple, une référence à -1 comme membre de $\mathbb{Z}_n$ est une référence à $[n-1]_n$, puisque $-1 \equiv n-1 \pmod{n}$.

Propriétés de divisibilité

PGCD, Factorisation

Thèorème

Si a et b sont deux entiers quelconques, non nuls en même temps, alors $pgcd(a, b)$ est le plus petit élément positif de l'ensemble $\{ax + by : x, y \in \mathbb{Z}\}$ des combinaisons linéaires de a et b.

Thèorème

Un entier composé a peut s'écrire d'une seule façon comme un produit de la forme

$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$$

où les p_i sont premiers, $p_1 < p_2 < \cdots < p_r$, et les e_i sont des entiers positifs.

Arithmétique modulaire

Opération sur $\mathbb{Z}_n$

La classe d'équivalence de deux entiers détermine de manière unique la classe d'équivalence de leur somme ou de leur produit:

- si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $a + b \equiv a' + b' \pmod{n}$ et $ab \equiv a'b' \pmod{n}$

Arithmétique modulaire

Opération sur $\mathbb{Z}_n$

La classe d'équivalence de deux entiers détermine de manière unique la classe d'équivalence de leur somme ou de leur produit:

- si $a \equiv a' \pmod{n}$ et $b \equiv b' \pmod{n}$, alors $a + b \equiv a' + b' \pmod{n}$ et $ab \equiv a'b' \pmod{n}$
- On peut donc définir l'addition et la multiplication modulo n, notée $+_n$ et $\cdot_n$, de la manière suivante:
  1. $$[a]_n +_n [b]_n = [a + b]_n \tag{3}$$
  2. $$[a]_n \cdot_n [b]_n = [ab]_n \tag{4}$$
  3. Chaque résultat x d'opération effectuée par les représentants, est remplacé par le représentant de sa classe $x \mod n$.

Arithmétique modulaire

Groupe additif $(\mathbb{Z}_n, +_n)$

- Avec l'addition modulo n, on définit le ***groupe additif modulo*** n par $(\mathbb{Z}_n, +_n)$.

Thèorème

Le système $(\mathbb{Z}_n, +_n)$ est un groupe abélien fini.

Arithmétique modulaire

Groupe additif $(\mathbb{Z}_n, +_n)$

- Avec l'addition modulo n, on définit le ***groupe additif modulo*** n par $(\mathbb{Z}_n, +_n)$.
- La taille du groupe additif modulo n est $|\mathbb{Z}_n| = n$.

Thèorème

Le système $(\mathbb{Z}_n, +_n)$ est un groupe abélien fini.

Arithmétique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$

- Avec la multiplication modulo n, on définit le ***groupe multiplicatif modulo*** n par $(\mathbb{Z}_n^*, \cdot_n)$.

Arithmétique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$

- Avec la multiplication modulo n, on définit le ***groupe multiplicatif modulo*** n par $(\mathbb{Z}_n^*, \cdot_n)$.
- Les éléments de ce groupe forment l'ensemble $\mathbb{Z}_n^*$ des éléments de $\mathbb{Z}_n$ qui sont premiers avec n:

$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \quad pgcd(a, n) = 1\}$$

Arithmétique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$

- Avec la multiplication modulo n, on définit le ***groupe multiplicatif modulo*** n par $(\mathbb{Z}_n^*, \cdot_n)$.
- Les éléments de ce groupe forment l'ensemble $\mathbb{Z}_n^*$ des éléments de $\mathbb{Z}_n$ qui sont premiers avec n:

$$\mathbb{Z}_n^* = \{[a]_n \in \mathbb{Z}_n : \quad pgcd(a, n) = 1\}$$

- Exemple: $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$, où l'opération de groupe est la multiplication modulo 15. Ici, un élément $[a]_{15}$ est noté a ; par exemple, $[7]_{15}$ est noté 7. Par exemple, $8 \cdot 11 \equiv 13 \pmod{15}$, si l'on se place dans $\mathbb{Z}_{15}^*$. L'élément neutre pour ce groupe est 1.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 1)

Thèorème

Le système $(\mathbb{Z}_n^*, \cdot_n)$ est un groupe abélien fini.

- On dit que $\overline{x} \in \mathbb{Z}_n^*$ est ***inversible*** si et seulement si, il existe $\overline{y} \in \mathbb{Z}_n^*$ vérifiant

$$\overline{x} \cdot \overline{y} = \overline{1} \Longleftrightarrow x \cdot y \equiv 1 \pmod{n}$$

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 1)

Thèorème

Le système $(\mathbb{Z}_n^*, \cdot_n)$ est un groupe abélien fini.

- On dit que $\overline{x} \in \mathbb{Z}_n^*$ est ***inversible*** si et seulement si, il existe $\overline{y} \in \mathbb{Z}_n^*$ vérifiant

$$\overline{x} \cdot \overline{y} = \overline{1} \Longleftrightarrow x \cdot y \equiv 1 \pmod{n}$$

- Dans ce cas on dit que y est un ***inverse multiplicatif*** de x modulo n

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 2)

- L'***inverse multiplicatif*** d'un élément a est noté $(a^{-1} \mod n)$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 2)

- L'***inverse multiplicatif*** d'un élément a est noté $(a^{-1} \mod n)$.
- La division dans $\mathbb{Z}_n^*$ est définie par l'équation $a/b \equiv ab^{-1} \pmod{n}$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 2)

- L'***inverse multiplicatif*** d'un élément a est noté ($a^{-1} \mod n$).
- La division dans $\mathbb{Z}_n^*$ est définie par l'équation $a/b \equiv ab^{-1} \pmod{n}$.
- Par exemple, dans $\mathbb{Z}_{15}^*$ on a $7^{-1} \equiv 13 \pmod{15}$, puisque $7 \cdot 13 \equiv 91 \equiv 1 \pmod{15}$, de sorte que $4/7 \equiv 4 \cdot 13 \equiv 7 \pmod{15}$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 3)

- La taille de $\mathbb{Z}_n^*$ se note $\phi(n)$. Cette fonction, connue sous le nom de ***fonction phi d'Euler***, satisfait à l'équation

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) \tag{5}$$

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 3)

- La taille de $\mathbb{Z}_n^*$ se note $\phi(n)$. Cette fonction, connue sous le nom de ***fonction phi d'Euler***, satisfait à l'équation

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p}) \tag{5}$$

- où p parcourt l'ensemble des nombres premiers qui divisent n (y compris n lui-même, si n est premier).

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 4)

- Si n est premier, alors $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$, et

$$\phi(n) = n - 1. \tag{6}$$

Thèorème

(Théorème de Lagrange)
Si $(G, +)$ est un groupe fini et $(H, +)$ est un sous-groupe de $(G, +)$, alors $|H|$ est un diviseur de $|G|$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 4)

- Si n est premier, alors $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$, et

$$\phi(n) = n - 1. \tag{6}$$

- Si n est composé, alors $\phi(n) < n - 1$.

Thèorème

(Théorème de Lagrange)
Si $(G, +)$ est un groupe fini et $(H, +)$ est un sous-groupe de $(G, +)$, alors $|H|$ est un diviseur de $|G|$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 5)

- Dans le groupe $\mathbb{Z}_n$, on a: $a^{(k)} = ka \mod n$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 5)

- Dans le groupe $\mathbb{Z}_n$, on a: $a^{(k)} = ka \mod n$.
- Dans le groupe $\mathbb{Z}_n^*$, on a: $a^{(k)} = a^k \mod n$.

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 5)

- Dans le groupe $\mathbb{Z}_n$, on a: $a^{(k)} = ka \mod n$.
- Dans le groupe $\mathbb{Z}_n^*$, on a: $a^{(k)} = a^k \mod n$.
- Le sous-groupe engendré par a, noté $\langle a \rangle$ est défini par

$$\langle a \rangle = \{a^{(k)} : k \geq 1\}$$

Arithmètique modulaire

Groupe multiplicatif $(\mathbb{Z}_n^*, \cdot_n)$ (suite 5)

- Dans le groupe $\mathbb{Z}_n$, on a: $a^{(k)} = ka \mod n$.
- Dans le groupe $\mathbb{Z}_n^*$, on a: $a^{(k)} = a^k \mod n$.
- Le sous-groupe engendré par a, noté $\langle a \rangle$ est défini par

$$\langle a \rangle = \{a^{(k)} : k \geq 1\}$$

- L'***ordre*** de a, noté $ord(a)$, est le plus petit $t > 0$ tel que $a^{(t)} = e$, e étant l'***élément neutre*** du groupe.

Arithmètique modulaire

Ordre et taille de sous-groupe

Thèorème

Pour un groupe fini G quelconque, et pour tout $a \in G$, l'ordre de l'élément a est égal à la taille du sous-groupe qu'il engendre, c'est-à-dire $ord(a) = |\langle a \rangle|$.

Corollaire

La séquence $a^{(1)}, a^{(2)}, \ldots$ est périodique de période $t = ord(a)$; autrement dit, $a^{(i)} = a^{(j)}$ si et seulement si $i \equiv j \pmod{t}$.

Arithmètique modulaire

Ordre et taille de sous-groupe (suite)

Il est cohérent avec le corollaire précédent de définir $a^{(0)}$ comme étant égal à e et $a^{(i)}$ comme étant égal à $a^{(i \mod t)}$, avec $t = ord(a)$, pour tout entier i.

Corollaire

Si G est un groupe fini ayant pour élément neutre e, alors pour tout $a \in G$,

$$a^{(|G|)} = e.$$

Rèsolution èquations linèaires modulaires

Équation

Soit l'équation

$$ax \equiv b \pmod{n}, \tag{7}$$

où $a > 0$ et $n > 0$.

- Il existe plusieurs applications pour ce problème ; notamment dans une partie de la procédure de calcul de clé du cryptosystème à clé publique RSA.

Rèsolution èquations linèaires modulaires

Équation

Soit l'équation

$$ax \equiv b \pmod{n}, \tag{7}$$

où $a > 0$ et $n > 0$.

- Il existe plusieurs applications pour ce problème ; notamment dans une partie de la procédure de calcul de clé du cryptosystème à clé publique RSA.
- On suppose que a, b et n sont donnés, et on doit trouver toutes les valeurs de x modulo n qui vérifient l'équation (7).

Rèsolution èquations linèaires modulaires

Équation

Soit l'équation

$$ax \equiv b \pmod{n}, \tag{7}$$

où $a > 0$ et $n > 0$.

- Il existe plusieurs applications pour ce problème ; notamment dans une partie de la procédure de calcul de clé du cryptosystème à clé publique RSA.
- On suppose que a, b et n sont donnés, et on doit trouver toutes les valeurs de x modulo n qui vérifient l'équation (7).
- Il peut y avoir zéro, une ou plusieurs solutions.

Rèsolution èquations linèaires modulaires

Équation (suite)

- Soit $\langle a \rangle$ le sous-groupe de $\mathbb{Z}_n$ engendré par a.

Rèsolution èquations linèaires modulaires

Équation (suite)

- Soit $\langle a \rangle$ le sous-groupe de $\mathbb{Z}_n$ engendré par a.
- Comme $\langle a \rangle = \{a^{(x)} : x > 0\} = \{ax \mod n : x > 0\}$, l'équation (7) a une solution si et seulement si $b \in \langle a \rangle$.

Rèsolution èquations linèaires modulaires

Équation (suite)

- Soit $\langle a \rangle$ le sous-groupe de $\mathbb{Z}_n$ engendré par a.
- Comme $\langle a \rangle = \{a^{(x)} : x > 0\} = \{ax \mod n : x > 0\}$, l'équation (7) a une solution si et seulement si $b \in \langle a \rangle$.
- Le théorème de Lagrange nous dit que $|\langle a \rangle|$ doit être un diviseur de n. Le théorème suivant nous donne une caractérisation précise de $\langle a \rangle$.

Rèsolution èquations linèaires modulaires

Quelques théorèmes et corollaires

Thèorème

Pour deux entiers quelconques strictement positifs a et n, si $d = pgcd(a, n)$, *alors*

$$\langle a \rangle = \langle d \rangle = \{0, d, 2d, \ldots, ((n/d) - 1)d\}, \tag{8}$$

dans $\mathbb{Z}_n$, *et donc*

$$|\langle a \rangle| = n/d$$

Corollaire

L'équation $ax \equiv b \pmod{n}$ *a une solution pour l'inconnue x si et seulement si* $pgcd(a, n)|b$.

Rèsolution èquations linèaires modulaires

Quelques théorèmes et corollaires (suite 1)

Corollaire

L'équation $ax \equiv b \pmod{n}$ *possède soit* d *solutions distinctes modulo* n, *où* $d = pgcd(a, n)$, *soit aucune solution.*

Thèorème

Soit $d = pgcd(a, n)$, *et supposons que* $d = ax' + ny'$ *pour deux entiers* x' *et* y' *particuliers (calculés, par exemple, par EUCLIDE-ETENDU). Si* $d|b$, *l'une des solutions de l'équation* $ax \equiv b \pmod{n}$ *est* x_0 , *où* $x_0 = x'(b/d) \mod n$.

Rèsolution èquations linèaires modulaires

Quelques théorèmes et corollaires (suite 2)

Thèorème

On suppose que l'équation $ax \equiv b \pmod{n}$ *admet une solution (autrement dit,* $d|b$*, avec* $d = pgcd(a, n)$*) et que* x_0 *est une des solutions de cette équation. Alors, cette équation possède exactement* d *solutions distinctes, modulo* n*, données par* $x_i = x_0 + i(n/d)$ *pour* $i = 1, 2, \ldots, d - 1$.

Corollaire

Pour tout $n > 1$*, si* $pgcd(a, n) = 1$*, alors l'équation* $ax \equiv b \pmod{n}$ *possède une solution unique modulo* n.

Rèsolution èquations linèaires modulaires

Quelques théorèmes et corollaires (suite 3)

Si $b = 1$, cas fréquent d'un intérêt considérable, l'inconnue x que nous cherchons est un inverse multiplicatif de a, modulo n.

Corollaire

Pour tout $n > 1$, si $pgcd(a, n) = 1$, alors l'équation

$$ax \equiv 1 \pmod{n}$$

possède une solution unique, modulo n. Sinon, elle n'a pas de solution.

Rèsolution èquations linèaires modulaires

Quelques théorèmes et corollaires (suite 4)

Le corollaire 16 ci-haut nous permet d'utiliser la notation $(a^{-1} \mod n)$ pour désigner l'unique inverse multiplicatif de a modulo n, quand a et n sont premiers entre eux. Si $pgcd(a, n) = 1$, alors une solution à l'équation $ax \equiv 1 \mod n$ est l'entier x retourné par EUCLIDE-ETENDU (qui sera étudié à la section suivante), puisque l'équation $pgcd(a, n) = 1 = ax + ny$ implique $ax \equiv 1 \pmod n$. Donc, $(a^{-1} \mod n)$ peut être calculé efficacement à l'aide de EUCLIDE-ETENDU.

Thèorème du reste chinois

Théorème du reste chinois

Soit $n = n_1 n_2 \cdots n_k$, où les n_i sont premiers entre eux deux à deux. On considère la correspondance

$$a \longleftrightarrow (a_1, a_2, \ldots, a_k), \tag{9}$$

avec $a \in \mathbb{Z}_n$, $a_i \in \mathbb{Z}_{n_i}$ et $a_i = a \pmod{n_i}$ pour $i = 1, 2, \ldots, k$. Alors, la correspondance 9 est une bijection entre $\mathbb{Z}_n$ et le produit cartésien $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$. Les opérations sur les éléments de $\mathbb{Z}_n$ peuvent être effectuées de manière équivalente sur les $k-uplets$ correspondants via application indépendante sur chaque composante de coordonnée.

Thèorème du reste chinois

Théorème du reste chinois (suite)

Autrement dit, si

$$a \longleftrightarrow (a_1, a_2, \ldots, a_k)$$

$$b \longleftrightarrow (b_1, b_2, \ldots, b_k)$$

Alors

$$(a + b) \bmod n \longleftrightarrow ((a_1 + b_1) \bmod n_1, \ldots, (a_k + b_k) \bmod n_k) \quad (10)$$

$$(a - b) \bmod n \longleftrightarrow ((a_1 - b_1) \bmod n_1, \ldots, (a_k - b_k) \bmod n_k) \quad (11)$$

$$(ab) \bmod n \longleftrightarrow ((a_1 b_1) \bmod n_1, \ldots, (a_k b_k) \bmod n_k) \quad (12)$$

Puissance modulo

Exemple

On considère la séquence des puissances de a modulo n, où $a \in \mathbb{Z}_n^*$:

$$a^0, a^1, a^2, a^3, \ldots, \tag{13}$$

modulo n.

En indexant à partir de 0, la 0^{eme} valeur de cette séquence est $a^0 \mod n = 1$ et la i^{eme} est $a^i \mod n$.

Par exemple, les puissances de 3 modulo 7 sont

i	0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
$3^i \mod 7$	1	3	2	6	4	5	1	3	2	6	4	5	$\cdots$

Puissance modulo

Exemple (suite)

tandis que les puissances de 2 modulo 7 sont

i		0	1	2	3	4	5	6	7	8	9	10	11	$\cdots$
2^i	mod 7	1	2	4	1	2	4	1	2	4	1	2	4	$\cdots$

Nous considérons $\langle a \rangle$ le sous-groupe de $\mathbb{Z}_n^*$ généré par a et $ord_n(a)$ (l'« ordre de a modulo n ») l'ordre de a dans $\mathbb{Z}_n^*$.

Par exemple,$\langle 2 \rangle = \{1, 2, 4\}$ dans $\mathbb{Z}_7^*$ et $ord_7(2) = 3$. En utilisant la fonction d'Euler $\phi(n)$ pour la taille de $\mathbb{Z}_n^*$,

Puissance modulo

Théorèmes d'Euler, de Fermat

Thèorème

(Théorème d'Euler) Pour un entier $n > 1$ quelconque, $a^{\phi(n)} \equiv 1 \mod n$ pour tout $a \in \mathbb{Z}_n^*$.

Thèorème

(Théorème de Fermat) Si p est premier, $a^{p-1} \equiv 1 \pmod p$ pour tout $a \in \mathbb{Z}_p^*$.

- Si $ord_n(g) = |\mathbb{Z}_n^*|$, alors tout élément de $\mathbb{Z}_n^*$ est une puissance de g modulo n, et on dit que g est une ***racine primitive*** ou encore un ***générateur*** de $\mathbb{Z}_n^*$.

Puissance modulo

Théorèmes d'Euler, de Fermat (suite)

- Si $\mathbb{Z}_n^*$ possède une racine primitive, on dit que le groupe $\mathbb{Z}_n^*$ est cyclique.

Puissance modulo

Théorèmes d'Euler, de Fermat (suite)

- Si $\mathbb{Z}_n^*$ possède une racine primitive, on dit que le groupe $\mathbb{Z}_n^*$ est cyclique.
- Si g est une racine primitive de $\mathbb{Z}_n^*$ et si a est un élément quelconque de $\mathbb{Z}_n^*$, alors il existe un z tel que $g^z \equiv a \pmod{n}$. Ce z est appelé ***logarithme discret*** ou ***indice*** de a modulo n, dans la base g; on représente cette valeur par $ind_{n,g}(a)$.

Puissance modulo

Théorème du logarithme discret

Thèorème

(Théorème du logarithme discret) Si g est une racine primitive de $\mathbb{Z}_n^*$, alors l'équation $g^x \equiv g^y \pmod{n}$ est satisfaite si et seulement si l'équation $x \equiv y \pmod{\phi(n)}$ l'est aussi.

- L'opération en théorie des nombres consistant à élever un nombre à une puissance modulo un autre nombre s'appelle ***exponentiation modulaire***.

Puissance modulo

Théorème du logarithme discret (suite)

- Quel est moyen efficace de calculer $a^b \mod n$, où $a, b \geq 0$ et $n > 0$?

Puissance modulo

Théorème du logarithme discret (suite)

- Quel est moyen efficace de calculer $a^b \mod n$, où $a, b \geq 0$ et $n > 0$?
- L'exponentiation modulaire est une opération fondamentale pour de nombreuses routines de test de primarité, ainsi que pour le cryptosystème à clé publique RSA.

Puissance modulo

Théorème du logarithme discret (suite)

- Quel est moyen efficace de calculer $a^b \mod n$, où $a, b \geq 0$ et $n > 0$?
- L'exponentiation modulaire est une opération fondamentale pour de nombreuses routines de test de primarité, ainsi que pour le cryptosystème à clé publique RSA.
- La méthode des ***élévations répétées au carré*** résout ce problème efficacement en utilisant la représentation binaire de b.

Algorithmes présentés

Algorithmes numériques fondamentaux

- Algorithme d'Euclide

Algorithmes présentés

Algorithmes numériques fondamentaux

- Algorithme d'Euclide
- Algorithme d'Euclide étendu

Algorithmes présentés

Algorithmes numériques fondamentaux

- Algorithme d'Euclide
- Algorithme d'Euclide étendu
- Algorithme de Résolution d'équations linéaires modulaires

Algorithmes présentés

Algorithmes numériques fondamentaux

- Algorithme d'Euclide
- Algorithme d'Euclide étendu
- Algorithme de Résolution d'équations linéaires modulaires
- Exponentiation modulaire

Algorithmes numériques fondamentaux

Algorithme d'Euclide

Thèorème

(Théorème de récursivité pour le PGCD) Quel que soit l'entier a positif ou nul, et quel que soit l'entier positif b,

$$pgcd(a, b) = pgcd(b, a \mod b).$$

EUCLIDE (a, b)

```
1   si b = 0
2       alors retourner a
3       sinon retourner EUCLIDE(b, a mod b)
```

Algorithmes numériques fondamentaux

Algorithme d'Euclide étendu

Nous généralisons l'algorithme l'algorithme d'Euclide pour lui permettre de calculer les coefficients entiers x et y tels que

$$d = pgcd(a, b) = ax + by. \tag{14}$$

EUCLIDE-ETENDU (a, b)

1 ***si*** $b = 0$
2 ***alors retourner*** $(a, 1, 0)$
3 $(d', x', y') \longleftarrow$ *EUCLIDE-ETENDU* $(b, a \mod b)$
4 $(d, x, y) \longleftarrow (d', y', x' - \lfloor a/b \rfloor y')$
5 ***retourner*** (d, x, y)

Algorithmes numériques fondamentaux

Algorithme de Résolution d'équations linéaires modulaires

Pour la résolution de l'équation linéaire modulaire $ax \equiv b \pmod{n}$, l'algorithme suivant imprime toutes les solutions de cette équation. Les entrées a et n sont des entiers strictement positifs arbitraires, et b est un entier arbitraire.

Résolution-Equations-Linéaires-Modulaires (a, b, n)

1 $(d, x', y') \longleftarrow$ *EUCLIDE-ETENDU* (a, n)
2 ***si*** $d|b$
3 ***alors*** $x_0 \longleftarrow x'(b/d) \mod n$
4 ***pour*** $i \longleftarrow 0$ à $d-1$ ***faire***
5 imprimer $(x_0 + i(n/d)) \mod n$
6 ***sinon*** imprimer « pas de solution »

Algorithmes numériques fondamentaux

Exponentiation modulaire

Soit b et sa représentation binaire $\langle b_k, b_{k-1}, \ldots, b_1, b_0 \rangle$. Autrement dit, la représentation binaire a une longueur $k+1$, b_k est le bit le plus significatif et b_0 est le bit le moins significatif. La procédure suivante calcule $a^c \mod n$ pour c croissant par doublements et incrémentations de 0 à b.

Algorithmes numériques fondamentaux

Exponentiation modulaire (suite)

EXPONENTIATION-MODULAIRE (a, b, n)

```
1   c ⟵ 0
2   d ⟵ 1
3   Soit ⟨b_k, b_{k−1}, ..., b_1, b_0⟩ lareprésentation binaire de b
4   pour i ⟵ k decr jusqu'à 0 faire
5       c ⟵ 2c
6       d ⟵ (d · d) mod n
7       si b_i = 1
8           alors c ⟵ c + 1
9                 d ⟵ (d · a) mod n
10  retourner d
```

Fin du chapitre

Merci de votre Attention