Chapitre VI

Mathématiques pour la cryptographie

1 Introduction

Ce cours est un cours contenant des notions probablement déjà en partie déjà vues en cours de mathématiques pour l'informatique.

Le contenu général de cette leçon est le suivant :

- des rappels : PGCD, nombres premiers, algorithme d'Euclide.
- l'implémentation des calculs sur des grands nombres entiers,
- la propriété algébrique des ensembles,
- comment les utiliser pour construire des corps finis sur lesquels la multiplication et l'exponentiation sont inversibles.

Il s'agit de donner les notions nécessaires au cours de cryptographique à clef publique, contient les rappels permettant de comprendre la construction de l'ensemble $GF(2^8)$ dont l'algèbre est utilisée dans AES (cryptographie par bloc) et les méthodes calculs du RSA (cryptographie à clef privée).

2 Division, PGCD et nombres premiers

2.1 Division Euclidienne

Définition 42 (division Euclidienne)**.** Si a et b sont des entiers, la division Euclidienne de a par b donne un couple unique d'entiers (q, r) tel que $a = b.q + r$ et $0 \leq r \leq |b| - 1$.

q est appelé le quotient, r le reste de la division Euclidienne de a par b.

Exemples

- division euclidienne de 45 par 12 : $45 = 3 \times 12 + 9$
- division euclidienne -49 par 11 : $-49 = -5 \times 11 + 6$
  et non $-49 = -4 \times 11 - 5$ car r doit être positif.

Opérateurs: avec les notations ci-dessus, on introduit les deux opérateurs suivants

- la division entière | définit par $a \mid b = q$,
- le modulo mod définit par $a \bmod b = r$

Attention

sur un ordinateur, la division entière ne coïncide avec la division Euclidienne que si le numérateur et le dénominateur sont positifs.

2.2 Diviseur et PGCD

Définition 43 (Diviseur)**.** a est un diviseur de b s'il existe un entier m tel que $b = a.m$.

Remarques :

- on écrit $a \mid b$.
- on dit aussi que a divise b.
- de manière équivalente, $a \mid b$ si le reste de la division Euclidienne de a par b est nul.

Définition 44 (Diviseur commun)**.**
Un diviseur commun de a et b est un entier m tel que $m \mid a$ et $m \mid b$.

Définition 45 (Plus grand diviseur commun (PGCD))**.**
Le PGCD de deux entiers a et b est le plus grand diviseur commun de a et de b. Si $d = \text{PGCD}(a, b)$, alors pour tout m tel que $m \mid a$ et $m \mid b$, on a $m \mid d$.

Exemple:
$\text{PGCD}(18, 24) = 6$
$\text{PGCD}(12, 5) = 1$

2.3 Nombre premier

Définition 46 (Nombre premier)**.**
Un nombre entier naturel p est premier si et seulement si il admet exactement deux diviseurs distincts entiers et positifs (1 et lui-même).

Notes :
- 1 n'est pas premier parce qu'il n'admet qu'un seul diviseur (lui-même).
- 0 n'est pas premier parce qu'il est divisible par tous les entiers.

Théorème 25 (Nombres premiers entre eux)**.**
Deux nombres a et b sont premiers entre eux si PGCD$(a, b) = 1$.

A savoir, aucun des nombres qui divisent a ne divise b (sauf 1), et inversement, aucun des nombres qui divisent b ne divisent a.

Exemple : 35 et 6 sont premiers entre eux car PGCD$(35, 6) = 1$.

2.4 Algorithme d'Euclide

L'algorithme d'Euclide est un algorithme pratique permettant de calculer le PGCDde deux nombres a et b.

Algorithme 26 (Euclide)**.**
Soit la suite (r_i) telle que :
- **Initialisation :** $r_0 = a$ et $r_1 = b$ où $a \geq b$.
- **Récurrence :** pour $i \geq 2$, $r_i = r_{i-2} \bmod r_{i-1}$
- **Arret :** soit $k > 0$ tel que $r_k = 0$, alors PGCD$(a, b) = r_{k-1}$.

En pratique : seuls les deux derniers termes de la récurrence sont utiles au calcul.

Exemples d'exécution

$(a, b) = (24, 18) \Rightarrow \{r_i\} = \{24, 18, \mathbf{6}, 0, \ldots\}$
Donc, PGCD$(24, 18) = 6$

$(a, b) = (12, 5) \Rightarrow \{r_i\} = \{12, 5, 2, \mathbf{1}, 0, \ldots\}$
Donc, PGCD$(12, 5) = 1$

$(a, b) = (78, 32) \Rightarrow \{r_i\} = \{78, 32, 14, 4, \mathbf{2}, 0, \ldots\}$
Donc, PGCD$(78, 32) = 2$

Démonstration:
Montrons dans un premier temps que si $a = b.q + r$ avec $0 \leq r < b$, alors PGCD(a, b) = PGCD(b, r).
- Si $d \mid a$ et $d \mid b$, alors $d \mid r$ (puisque $a = b.q + r$).
  Comme $d \mid b$ et $d \mid r$, alors $d \mid$ PGCD(b, r).
  Donc PGCD$(a, b) \mid$ PGCD(b, r) (*i.e.* avec le plus grand d).
- Inversement, si $d' \mid b$ et $d' \mid r$, alors $d' \mid a$ (puisque $a = b.q + r$).
  Donc $d' \mid$ PGCD(a, b).
  En conséquence, PGCD$(a, b) \mid$ PGCD(b, r).

Soit $a > 0$ et $b \geq 0$.

On a deux cas :

- si $b = 0$, alors $\text{PGCD}(a, b) = \text{PGCD}(a, 0) = a$
- sinon soit $a = b.q + r$ with $0 \leq r < b$.
  $\text{PGCD}(a, b) = \text{PGCD}(b, r)$
  (b, r) est inférieur à (a, b).

□

On souhaiterait évaluer le nombre de division nécessaire lors de l'exécution de l'algorithme d'Euclide. On cherche le $\text{PGCD}(k, n)$ avec $k < n$
Le cas le plus lent correspond au cas où chacun des quotients r_i/r_{i+1} vaut 1. Si l'on remonte l'algorithme avec des quotients à 1, on a :

$$\begin{aligned} r_m &= r_{m-1} = 1 \\ r_{m-2} &= r_{m-1} + r_m \\ &\vdots \\ r_0 &= r_1 + r_2 \\ b &= r_0 + r_1 \\ a &= b + r_0 \end{aligned}$$

On reconnaît une suite de Fibonnaci ($F_0 = 0$, $F_1 = 1$ et $F_j = F_{j-1} + F_{j-2}$).

Théorème 27 (Lamé)**.**
Le nombre de division Euclidienne d nécessaire à la terminaison de l'algorithme d'Euclide appliquée à a et b (avec b < a) vérifie :

$$d \leq \log_\phi n$$

où $\phi = (1 + \sqrt{5})/2$ *et n le nombre de chiffres de b.*

3 Constructions algébriques

Les rappels d'algèbre faits ici ont pour but de clarifier :

- les propriétés des ensembles pour les opérations dont ils sont munis.
- les raisons pour lesquels certains ensembles sont construits.

L'ensemble des définitions et des propriétés a été réduit au strict minimum nécessaire dans le cadre de ce cours.

Il n'existe aucune difficulté à cette partie : il s'agit essentiellement de définir un vocabulaire.

Dans le cadre de la cryptographie, nous sommes intéressés à trouver des ensembles dans lesquels les éléments sont inversibles.

3.1 Semi-groupe

On muni un ensemble d'une opération :

Définition 47 (semi-groupe)**.** Un semi-groupe est une paire $(R, \circ)$ telle que R est un ensemble, et $\circ$ une opération associative sur cet ensemble (*i.e.* $\forall x, y, z \in R, (x \circ y) \circ z = x \circ (y \circ z)$).

Note : si l'opération $\circ$ est commutative (*i.e.* $\forall x, y, x \circ y = y \circ x$), il est dit commutatif ou abélien.
Exemple : $(\mathbb{Z}, +)$, $(\mathbb{Z}, .)$ sont des semi-groupes abélien.

Il ne peut pas y avoir d'inverse si l'ensemble n'a pas d'élément neutre :

Définition 48 (élément neutre d'un semi-groupe)**.** Un élément neutre e dans un semi-groupe $(R, \circ)$ est un élément $e \in R$ tel que $\forall a \in R, a \circ e = e \circ a = a$.

Note : on peut démontrer qu'il existe au plus un élément neutre.
Exemples :

- 0 est l'élément neutre de $(\mathbb{Z}, +)$,
- 1 est l'élément neutre de $(\mathbb{Z}, .)$.

3.2 Monoïde

On peut maintenant définir un ensemble muni d'une opération et qui contient un élément neutre :

Définition 49 (monoïde)**.** Un monoïde est un semi-groupe qui contient un élément neutre.

Exemples : $(\mathbb{Z}, +)$, $(\mathbb{Z}, .)$ sont des monoïdes abéliens.

Il devient donc possible de définir maintenant un inverse dans cet ensemble :

Définition 50 (élément inversible dans un monoïde)**.** dans un monoïde $(R, \circ)$ où l'élément neutre est noté e, si pour $a \in R$, il existe un $b \in R$ tel que $a \circ b = b \circ a = e$, alors a est inversible dans R, et son inverse est b.

Note : chaque élément a, au plus, un inverse.
Exemples :

- un élément a de $(\mathbb{Z}, +)$ est inversible, et $-a$ est son inverse.
- seul 1 est inversible dans $(\mathbb{Z}, .)$.

3.3 Groupe

Les ensembles qui nous intéressent sont donc ceux qui permettent d'inverser tous leurs éléments.

Définition 51 (groupe)**.** un groupe est un monoïde dans lequel tout élément est inversible.

Exemples :

- $(\mathbb{Z}, +)$ est un groupe abélien.
- Le monoïde $(\mathbb{Z}, .)$ n'est pas un groupe car tout élément n'est pas inversible.

Définition 52 (ordre d'un groupe)**.** L'ordre d'un groupe est le nombre de ses éléments.

Exemples :

- L'ordre de $(\mathbb{Z}, +)$ est infini.
- l'ordre de $\mathbb{Z}_n = \{0, ..., n-1\}$ est n.

On dispose d'un première définition formelle des propriétés que doivent respecter les ensembles qui nous conviendrait. Inconvénient : muni d'une seule opération, ces opérations sur les ensembles standards n'offrent qu'assez peu de complexité.

3.4 Anneau

Nous ajoutons donc une opération supplémentaire :

Définition 53 (anneau)**.** un anneau est un triplet $(R, \circ, \star)$ tel que $(R, \circ)$ est un groupe abélien et $(R, \star)$ est un semi-groupe.

Exemple : $(\mathbb{Z}, +, \times)$ est un anneau.

Définissons maintenant l'élément neutre pour cette opération supplémentaire :

Définition 54 (élément unité sur un anneau)**.** l'élément unité d'un anneau $(R, \circ, \star)$ est l'élément neutre pour le semi-groupe $(R, \star)$.

Exemple : 1 est l'élément unité de l'anneau $(\mathbb{Z}, +, \times)$.

3.5 Partition

Deuxième problème avec les ensembles classiques : ils sont infinis. Le partitionnement en un ensemble fini de parties est une possibilité.

Définition 55 (partition d'un ensemble)**.** soit E un ensemble non vide. Une partition de E est un ensemble de parties E_i non vides deux à deux disjointes et dont E est l'union (*i.e.* $E = \bigcup_i E_i$ tel que $i \neq j \Rightarrow E_i \cap E_j = \emptyset$).

Exemple : soit $\mathbb{E}$ (resp. $\mathbb{O}$) l'ensemble des éléments pairs (resp. impair) de $\mathbb{Z}$ [1]. $\mathbb{Z}$ est bien partitionné en deux : $\mathbb{Z} = \mathbb{E} \cup \mathbb{O}$ qui sont disjoints entre eux.

Mais comment faire pour définir le partitionnement d'un ensemble, et en particulier, savoir quels éléments mettre dans quelle partie ?

3.6 Relation d'équivalence

Dans le but de partitionner en un ensemble de partie, on définit une relation d'équivalence : cela permet de définir une condition qui permet de savoir si deux éléments se trouvent dans la même partie.

Définition 56 (relation d'équivalence sur un ensemble)**.** une relation d'équivalence R sur un ensemble E est un relation binaire réflexive ($\forall x \in E, xRx$), symétrique ($\forall (x, y) \in E^2, xRy \Rightarrow yRx$) et transitive ($\forall (x, y, z) \in E^3, xRy$ et $yRz \Rightarrow xRz$).

Exemple : on pourra vérifier que la relation binaire P définie par xPy si x a la même parité que y est bien une relation d'équivalence sur $\mathbb{Z}$.

3.7 Classe d'équivalence

On peut ainsi définir une classe d'équivalence comme une partie constituée de l'ensemble des éléments équivalents.

1. Noter que 0 est un nombre pair : entier multiple de 2 (condition suffisante, les arguments suivants sont pour vous en convaincre intuitivement), il est précédé et suivit d'un nombre impair, la somme de deux nombres pairs est bien paire si l'un de ces deux nombres est 0 (ou les deux), la somme d'un nombre pair et d'un nombre impair est bien impaire si le nombre paire est 0, ...

Définition 57 (classe d'équivalence)**.** soit E un ensemble et R une relation d'équivalence sur E. Pour tout $x \in E$, la classe d'équivalence de x pour R (notée $\overline{x}$) est l'ensemble des y de E en relation avec x (*i.e.* $\overline{x} = \{y \in E \mid xRy\}$).

Exemple : Pour $\mathbb{Z}$ et P la relation d'équivalence de parité (xPy si x et y ont la même parité), il y a deux classes d'équivalence, $\overline{0} = \overline{2} = ... = \mathbb{E}$, et $\overline{1} = \overline{3} = ... = \mathbb{O}$.

3.8 Ensemble quotient

Et à partir de cela, l'ensemble qui contient l'ensemble des classes d'équivalence :

Définition 58 (ensemble quotient)**.** L'ensemble des classes d'équivalence de E pour R est appelé ensemble quotient de E par R et noté E/R.

Exemple : $\mathbb{Z}/P = \{\mathbb{E}, \mathbb{O}\}$, à savoir l'ensemble quotient est l'ensemble des classes d'équivalence.

D'où l'on déduit naturellement la partition de l'ensemble :

Théorème 28 (partition d'un ensemble par une relation d'équivalence)**.** *si R est une relation d'équivalence sur un ensemble E non vide, alors l'ensemble des classes d'équivalence forment une partition de E.*

Exemple : on a bien $\mathbb{Z} = \mathbb{E} \cup \mathbb{O}$.

L'objectif de la construction est d'obtenir au final un corps :

Définition 59 (corps)**.** Un corps est un anneau abélien dans lequel tous les éléments non nuls sont inversibles.

Exemples :

- $(\mathbb{N}, +, .)$ n'est pas un corps parce que la plupart des entiers ne sont pas inversibles.
- $(\mathbb{Q}, +, .)$ et $(\mathbb{R}, +, \times)$ sont des corps, car pour tout $x \neq 0$, il existe y dans ce même corps tel que $x.y = 1$.

3.9 Groupe unitaire

On s'intéresse maintenant aux propriétés de l'ensemble des éléments possédant un inverse.

Définition 60 (élément unitaire)**.**
Sur un anneau R, soit 1_R l'élément identité pour la multiplication dans R, un élément $r \in R$ est dit unitaire si il existe $s \in R$ tel que $r.s = s.r = 1_R$.

Définition 61 (groupe unitaire)**.**
Sur un anneau R, le groupe unitaire de R, noté R^* est le groupe constitué de l'ensemble des éléments unitaires.

Notes :

- R^* contient l'élément identité pour la multiplication, et son inverse multiplicatif pour tout élément. Il est donc fermé par multiplication.
- Le groupe unitaire R^* d'un corps commutatif fini R contenant q éléments et d'ordre $q - 1$ car tous les éléments non nuls de R sont unitaires dans K.

En cryptographie, on utilisera la fonction d'exponentiation sur les éléments pour produire des résultats difficilement inversible. On s'intéresse donc à l'ordre des éléments dans ce groupe unitaire.

Définition 62 (ordre d'un élément)**.** L'ordre e d'un élément x dans un groupe unitaire R^* est le plus petit n tel que $x^n = 1_{R^*}$.

On définit l'indicatrice d'Euler qui joue un rôle dans le résultat qui suit.

Définition 63 (Indicatrice d'Euler)**.** L'indicatrice d'Euler est la fonction ϕ de $\mathbb{N}^*$ dans $\mathbb{N}^*$ qui associe à tout entier n le nombre d'entiers inférieurs ou égal à n premier avec n.
$\phi = card\,(\{m \leq n \mid \text{PGCD}(n, m) = 1\})$.

Théorème 29 (structure du groupe unité)**.**
Soit R un corps commutatif fini à q éléments. Alors, pour tout diviseur d de $q-1$, il y a exactement $\phi(d)$ éléments d'ordre d dans le groupe unité R^*.

Donc, si un nombre d divise $\phi(q)$, alors il existe un sous-groupe de R d'ordre d contenant $\phi(d)$ éléments.

Définition 64 (élément générateur d'un groupe fini R)**.**
Soit n l'ordre de R. Un élément $r \in R$ est un élément générateur si $R = \left\{r^k; 0 \leq k < n\right\}$.

Définition 65 (groupe fini cyclique)**.**
Un groupe fini R est cyclique s'il existe un élément générateur dans R.

Corollaire 30 (générateurs d'un groupe fini cyclique)**.**
Si R est un groupe fini d'ordre n, alors son groupe unité R^* est un groupe fini cyclique d'ordre $n-1$ et a exactement $\phi(n-1)$ générateurs, où ϕ est la fonction d'Euler.

Ce sont ces résultats qui seront utilisés pour :

- savoir si l'exponentielle cycle sur l'ensemble des éléments du groupe, et inverser l'exponentielle,
- montrer qu'un nombre entier B-friable (i.e. si tous ses facteurs premiers sont inférieurs à B pour un B raisonnable) est plus facile à factoriser. Voir l'algorithme $\rho - 1$ de Pollard dans le chapitre suivant.

3.10 Synthèse

Les étapes de la construction seront donc les suivantes :

- partir d'un anneau dont l'ordre est infini,
- choisir une relation d'équivalence permettant de construire un nombre fini de classes d'équivalence,
- trouver les conditions telles que le nouvel anneau constitué à partir des classes d'équivalence soit un corps.

Nous disposerons ainsi d'un ensemble discret dans lequel les éléments sont inversibles, et qui pourra servir de base à des méthodes cryptographiques.

Par ailleurs, l'opération d'exponentiation possède des propriétés intéressantes (cycle, inversion).

4 Application : arithmétique de $\mathbb{Z}_n$

On veut maintenant appliquer ce principe de partitionnement de manière à :

- partir de l'anneau $(\mathbb{Z}, +, \times)$,
- créer une partition de cet ensemble en n parties en choisissant une relation d'équivalence

et voir ainsi :

- quelles sont les propriétés de ces opérations sur les ensembles quotients,
- si on arrive ainsi (et sous quelles conditions) à construire des opérations inversibles,
- comment l'on calcule les inverses.

Note : Par la suite, on utilisera aussi le point pour noter la multiplication (= on écrit $a.b$ à la place de $a \times b$).

4.1 Construction de $\mathbb{Z}/n\mathbb{Z}$

4.1.1 Définition

On se place donc sur l'anneau $(\mathbb{Z}, +, \times)$.

Définissons tout d'abord la relation :

Définition 66 (relation divise)**.**
soit $n \in \mathbb{Z}^*$, et $a \in \mathbb{Z}$.
On dit que n divise a si $\exists k \in \mathbb{Z}$ tel que $a = k.n$.
Si n divise a, on note $n \mid a$.

Notons que ceci n'est pas une relation d'équivalence.

Utilisons maintenant cette relation pour définir la congruence :

Définition 67 (relation de congruence)**.**
Soit $n > 0$, et $a, b \in \mathbb{Z}$.
On dit que a est congruent à b modulo n si $n \mid (a - b)$.
Si a est congruent à b modulo n, on note $a \equiv b \bmod n$.

Notons tout d'abord que par définition, $a \equiv b \bmod n$ signifie que $n \mid (a - b)$. Par conséquent : $\exists k \in \mathbb{Z}$ tel que que $a - b = k.n$.

D'où on tire : $(a \equiv b \bmod n) \Leftrightarrow (\exists k / a = b + k.n)$

Proposition 31. *La congruence modulo n est une relation d'équivalence.*

Démonstration:
La relation est :

- réflexive : $a \equiv a \bmod n$ car $a - a = 0$ est divisible par tout n.
- symétrique : $a \equiv b \bmod n \Leftrightarrow b \equiv a \bmod n$ car $n \mid (a - b) \Leftrightarrow n \mid (b - a)$.
- transitive : $a \equiv b \bmod n$ et $b \equiv c \bmod n \Rightarrow a \equiv c \bmod n$ car $\exists k_1, k_2$ tel que $a - b = k_1.n$ et $b - c = k_2.n$, donc $a - c = (k_1 + k_2).n$.

□

Nous avons donc une relation d'équivalence candidate pour partitionner l'ensemble $\mathbb{Z}$.

Théorème 32. *Soit $n > 0$. Pour tout entier a, il existe un unique entier $0 \leq r < n$ tel que a est congruent à r modulo n.*

Exemples

$2 \equiv 8 \bmod 3$ car $3 \mid (8 - 2)$.
$12 \equiv 2 \bmod 5$ car $5 \mid (12 - 2)$.

Autrement dit, deux nombres a et b sont équivalents si et seulement si, ils ont le même reste lors de la division euclidienne par n.

Note : ne pas confondre la fonction `%` en C++ avec le reste de la division euclidienne (identique seulement si a et b sont positifs).

On définit ainsi l'ensemble des représentants des classes d'équivalence associées :

Définition 68 (Classe d'équivalence)**.**
L'ensemble représentant des classes d'équivalence engendré par $\bmod n$ sur $\mathbb{Z}$ (= ensemble des classes de congruence modulo n) est noté $\mathbb{Z}_n$.

à savoir $\mathbb{Z}_n = \{0, \ldots, n-1\}$ (modulo n, il ne peut y avoir que n restes r possibles, donc $0 \leq r < n$).

Ainsi que l'ensemble quotient :

Définition 69 (Ensemble quotient)**.**
L'ensemble quotient (=ensemble des classes d'équivalence) pour la relation congruence modulo n est noté $\mathbb{Z}/n\mathbb{Z}$

L'ensemble des classes d'équivalence est donc :
$\mathbb{Z}/n\mathbb{Z} = \bigcup_{p=0}^{n-1} \overline{p}$
où $\overline{p}$ est la classe d'équivalence $\{x / p \equiv x \bmod n\}$ dont le représentant est p.

4.1.2 Propriétés

Regardons maintenant les propriétés de cette relation d'équivalence vis-à-vis des opérations + et × sur l'anneau.

Proposition 33.

1. *si* $a \equiv a' \bmod n$ *et* $b \equiv b' \bmod n$*, alors* $a + b \equiv (a' + b') \bmod n$
2. *si* $a \equiv a' \bmod n$ *et* $b \equiv b' \bmod n$*, alors* $a \times b \equiv (a' \times b') \bmod n$

Démonstration:

1. si $a = a' + k_a.n$ et $b = b' + k_b.n$, alors on a : $a + b = a' + b' + n.(k_a + k_b)$.
2. si $a = a' + k_a.n$ et $b = b' + k_b.n$, alors on a : $a.b = a'.b' + n.(a'.k_b + b'.k_a + k_a.k_b)$.

□

4.1.3 Inverse multiplicatif

L'inverse pour l'addition étant trivial dans $\mathbb{Z}/n\mathbb{Z}$, intéressons nous à l'inverse pour la multiplication.

Définition 70 (Inverse multiplicatif)**.**
Soit $n > 0$ et $p \in \mathbb{Z}$.
q est l'inverse multiplicatif de p modulo n si :
$p.q \equiv 1 \bmod n$.

Théorème 34 (Existence d'un inverse multiplicatif)**.**
Soit $n > 0$, $p \in \mathbb{Z}$ avec $n > 0$.
p a un inverse multiplicatif modulo n si et seulement si $\text{PGCD}(p, n) = 1$.

Démonstration:
Ce théorème est une conséquence du théorème de Bézout (voir ci-après). □

Exemples

L'inverse multiplicatif de 5 modulo 7 est 3 parce que $3 \times 5 = 15 \equiv 1 \bmod 7$.

2 n'a pas d'inverse multiplicatif modulo 6 :

$2 \times 0 = 0 \equiv 0 \bmod 6$ $\quad$ $2 \times 3 = 6 \equiv 0 \bmod 6$
$2 \times 1 = 2 \equiv 2 \bmod 6$ $\quad$ $2 \times 4 = 8 \equiv 2 \bmod 6$
$2 \times 2 = 4 \equiv 4 \bmod 6$ $\quad$ $2 \times 5 = 10 \equiv 4 \bmod 6$

4.1.4 Conséquences

Nous avons donc trouvé une relation d'équivalence qui permet de partitionner $\mathbb{Z}$ en n parties. Si n est premier, tout élément est alors inversible.

Afin d'utiliser de cette propriété, nous définissons maintenant une opération arithmétique de "réduction modulo n" qui va nous permettre de de considérer $\mathbb{Z}_n$ comme un ensemble à n éléments sur lequel on peut :

- effectuer tout calcul arithmétique,
- ramener tout calcul de $\mathbb{Z}$ dans $\mathbb{Z}_n$,
- calculer des inverses,
- les utiliser pour résoudre des équations (congruence linéaire, restes chinois)
- calculer des exponentielles

4.2 Arithmétique de base dans $\mathbb{Z}_n$

Pour un entier $n > 1$ appelé le module :

Définition 71 (Réduction modulaire)**.**
$r = a \bmod n$ est le reste de la division de a par n, où $0 \leq r < n$.

Exemple : $11 \bmod 8 = 3$, $15 \bmod 5 = 0$.

Attention

Ne pas confondre la congruence et la réduction modulaire.
La congruence est la relation d'équivalence sur $\mathbb{Z}$ définie par :
$a \equiv b \bmod n$ si $n \mid (a - b)$.
Exemple : $11 \equiv 19 \bmod 8$.

Proposition 35 (Lien entre réduction modulaire et congruence)**.**
• *$a \equiv b \bmod n$ si et seulement si $a \bmod n = b \bmod n$.*
• *si $r = a \bmod n$ alors $r \equiv a \bmod n$.*

Démonstration : conséquence des définitions. □

Définition 72 (Entiers modulo n)**.**
L'ensemble des entiers modulo n est l'ensemble $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Proposition 36 (Arithmétique modulaire dans $\mathbb{Z}_n$)**.**
L'arithmétique avec les opérateurs $+$, $-$, $\times$ dans $\mathbb{Z}_n$ est définie en effectuant les calculs dans $\mathbb{Z}$, puis en réduisant le résultat modulo n.

Démonstration:
On avait vu que si $a \equiv b \bmod n$ et $a' \equiv b' \bmod n$,
$(a + a') \equiv (b + b') \bmod n$,
$(a - a') \equiv (b - b') \bmod n$ (même démonstration qu'avec $+$),
$(a \times a') \equiv (b \times b') \bmod n$.
Donc, tous ces opérateurs sont définis sur $\mathbb{Z}_n$ en ramenant le résultat par réduction modulaire dans $\mathbb{Z}_n$ car tout élément de $\mathbb{Z}$ possède une membre de sa classe d'équivalence dans $\mathbb{Z}_n$. □

Exemple dans $\mathbb{Z}_7$

$6 + 4 = 3$
$3 - 4 = 6$
$3 \times 6 = 4$

Conséquence

Lorsque l'on effectue un calcul modulo n, on peut substituer tout x par x' tel que $x' = x \bmod n$.

Par exemple, on cherche $0 \leq a < 7$, tel que $a \equiv (83 \times 72) \bmod 7$.

Solution 1

On effectue $83 \times 72 = 5976$.
On calcule le reste de la division Euclidienne par 7.
On trouve $a = 5$.

Solution 2

On remarque que $83 \equiv 6 \bmod 7$ et que $72 \equiv 2 \bmod 7$.
Or, si $a \equiv a' \bmod n$ et $b \equiv b' \bmod n$, alors $a \times b \equiv (a' \times b') \bmod n$.
Donc, on effectue $6 \times 2 = 12 \equiv 5 \bmod 7$.
On trouve $a = 5$.

Exercice 38: Propriétés de la congruence

On se place dans $\mathbb{Z}_{13}$.

1. Calculer 45 et 99 modulo 13.
2. Calculer le résultat de 45 + 99 modulo 13 en utilisant l'arithmétique modulaire. On vérifiera le résultat avec une machine à calculer.
3. Calculer le résultat de 45 × 99 modulo 13 en utilisant l'arithmétique modulaire. On vérifiera le résultat avec une machine à calculer.

4.3 Inversion dans $\mathbb{Z}_n$

4.3.1 Calcul de l'inverse

On veut maintenant disposer de méthode pratiques pour calculer les inverses dans $\mathbb{Z}_n$.

Nous rappelons :

- le théorème de Bachet-Bézout.
- l'algorithme d'Euclide étendu qui permet de trouver, en plus du PGCD, les solutions (x, y) de l'identité de Bézout.
- la méthode qui permet, si le PGCD est égal à 1, de calculer l'inverse de tout élément de $\mathbb{Z}_n$ modulo n.

Théorème de Bachet-Bézout

Théorème 37 ((Bachet-Bézout))**.**
Pour tout $(a, b) \in \mathbb{Z}^2$*, il existe* $(x, y) \in \mathbb{Z}^2$ *tel que* $x.a + y.b = \text{PGCD}(a, b)$.
Et donc, si a et b sont premiers entre eux, $x.a + y.b = 1$.

Notons que $x.a + y.b = 1$ peut s'écrire :

- $x.a = 1 - y.b$. Donc, $x.a \equiv 1 \bmod b$.
  Donc, x est l'inverse multiplicatif de a modulo b (*i.e.* $x \equiv a^{-1} \bmod b$).

- $y.b = 1 - x.a$. Donc, $y.b \equiv 1 \bmod a$.
  Donc, y est l'inverse multiplicatif de b modulo a (*i.e.* $y \equiv b^{-1} \bmod a$).

et que ceux-ci existent si PGCD$(a, b) = 1$.

Exemples

PGCD$(35, 7) = 7$, et on trouve : $-1 \times 35 + 6 \times 7 = 7$

PGCD$(152, 541) = 2$, et on trouve : $-82 \times 152 + 23 \times 542 = 2$

PGCD$(35, 6) = 1$, et on trouve : $-1 \times 35 + 6 \times 6 = 1$.

PGCD$(152, 541) = 1$, et on trouve : $210 \times 152 - 59 \times 541 = 1$

Algorithme d'Euclide étendu

Nous abordons maintenant l'algorithme d'Euclide étendu qui permet de calculer, pour deux nombres (a, b) le PGCD ainsi que les valeurs de (x, y).

Algorithme 38 (Euclide étendu)**.**
Soit trois suites (r_i), (u_i), (v_i) et deux entiers $0 < b \leq a$ tels que :

- **Initialisations :**
  $r_0 = a$, $r_1 = b$
  $u_0 = 1$, $u_1 = 0$
  $v_0 = 0$, $v_1 = 1$
- **Récurrence :** (pour $k \geq 2$)
  $r_k = r_{k-2} \bmod r_{k-1}$
  $q_k = r_{k-2}/r_{k-1}$
  $u_k = u_{k-2} - q_k.u_{k-1}$
  $v_k = v_{k-2} - q_k.v_{k-1}$
- **Arret :** soit $k > 0$ tel que $r_k = 0$, alors PGCD$(a, b) = r_{k-1} = u_{k-1}.a + v_{k-1}.b$

En pratique : seuls les deux derniers termes de la récurrence sont utiles au calcul.

Démonstration:
Montrons par récurrence que l'on a toujours $r_k = u_k.a + v_k.b$.

- pour $k = 0$, $r_0 = a = 1.a + 0.b$.
- pour $k = 1$, $r_1 = b = 0.a + 1.b$.
- supposons que la propriété est vérifiée au rang $k-2$ et $k-1$, alors au rang k :

$$\begin{aligned} u_k.a + v_k.b &= (u_{k-2} - q_{k-2}.u_{k-1}).a + (v_{k-2} - q_{k-2}.v_{k-1}).b \\ &= (u_{k-2}.a + v_{k-2}.b) - q_{k-2}.(u_{k-1}.a + v_{k-1}.b) \\ &= r_{k-2} - q_{k-2}.r_{k-1} \\ &= r_k \end{aligned}$$

Car $r_k = r_{k-2} \bmod r_{k-1}$ et $q_k = r_{k-2}/r_{k-1}$, donc $r_k = r_{k-2} - q_{k-2}.r_{k-1}$.

Donc la propriété est vraie pour tout $k \geq 0$.

Comme pour l'algorithme d'Euclide, r_k décroît strictement vers 0. □

Exemple 1 : pour $a = 986$ et $b = 290$

k	r_k	q_k	u_k	v_k
0	986		0	1
1	290		1	0
2	116	3	-3	1
3	58	2	7	-2
4	0	2	-17	5

Rappel :

$r_k = r_{k-2} \bmod r_{k-1}$
$q_k = r_{k-2}/r_{k-1}$
$u_k = u_{k-2} - q_k.u_{k-1}$
$v_k = v_{k-2} - q_k.v_{k-1}$

$\text{PGCD}(986, 290) = 58 = 7 \times 290 - 2 \times 986$

Exemple 2 : pour $a = 995$ et $b = 942$

k	r_k	q_k	u_k	v_k
0	995		0	1
1	942		1	0
2	53	1	-1	1
3	41	17	18	-17
4	12	1	-19	18
5	5	3	75	-71
6	2	2	-169	160
7	1	2	413	-391
8	0	2	-995	942

$\text{PGCD}(995, 942) = 1 = 413 \times 942 - 391 \times 995$

Calcul de l'inverse multiplicatif

En conséquence, pour calculer l'inverse multiplicatif de a dans $\mathbb{Z}_n$, on procède de la manière suivante :

1. d'après Bachet-Bézout, il existe (x, y) tels que $x.a + y.n = PGCD(a, n)$.
2. calculer (x, y) et le PGCD en utilisant l'algorithme d'Euclide étendu.
3. si PGCD $\neq 1$, alors il n'existe pas d'inverse de a dans $\mathbb{Z}_n$.
4. sinon $x.a + y.n = 1$ implique $(x.a + y.n) \bmod n = 1 \bmod n$, et $x.a \bmod n = 1$.

On en déduit que x est l'inverse multiplicatif de a.

Notons que l'on retrouve ici la conditions d'existence de l'inverse : $(\mathbb{Z}_n, \times)$ est

un monoïde si et seulement si n est premier.

Exercice 39: Algorithme d'Euclide

Calculer le PGCD des nombres suivants avec l'algorithme d'Euclide étendu.

1. 27 et 5.
2. 57 et 21.
3. Duquel de ces deux calculs peut-on déduire les inverses multiplicatifs ?

Division modulaire

On peut ainsi définir la division modulaire :

Définition 73 (Division modulaire)**.**
Soit n un module. Soit $(a, b) \in \mathbb{Z}^2$ tel que $\text{PGCD}(a, n) = 1$.
Alors la division modulaire b/a modulo n est définie par :

$$b/a \bmod n \equiv b.a^{-1} \bmod n$$

où a^{-1} est l'inverse multiplicatif de a modulo n.

Remarque

Si $c \equiv b/a \bmod n$ alors $a \times c \equiv b \bmod n$.
Autrement dit, c est la solution de $a \times x \equiv b \bmod n$.

Exemple

$x = 5/3 \bmod 7 \equiv 5.3^{-1} \bmod 7$.
Or $3 \times 5 \equiv 15 \equiv 1 \bmod 7$.
Ainsi $3^{-1} = 5 \bmod 7$.
Donc, $5/3 \bmod 7 \equiv 5 \times 5 \equiv 25 \equiv 4 \bmod 7$.
En conséquence, $5/3 \bmod 7 = 4$.

4.3.2 Congruence linéaire

Théorème 39 (Résolution de la congruence linéaire)**.**
Soit $n > 0$. Soit $(a, b) \in \mathbb{Z}$ tel que $\text{PGCD}(a, n) = 1$.
L'équation $a \times x \equiv b \bmod n$ a une solution x unique modulo n.

Démonstration:

Soit a^{-1} l'inverse multiplicatif de a modulo n.
Alors $(a^{-1}.b) \bmod n \equiv a^{-1}.a.x \equiv x$.
Donc, $x = (a^{-1}.b) \bmod n$.

Exemple Trouver x tel que $5 \times x = 6 \bmod 7$

3 est l'inverse de 5 modulo 7 parce que $5 \times 3 \equiv 1 \bmod 7$.
$3 \times 5 \times x \equiv 15 \times x \equiv 1 \times x \equiv 3 \times 6 \equiv 4 \bmod 7$.
Donc $x \equiv 4 \bmod 7$.

4.3.3 Reste chinois

Théorème 40 (du reste chinois)**.**
Soit deux entiers $n_1 > 1$ *et* $n_2 > 0$ *tels que* $\text{PGCD}(n_1, n_2) = 1$.
$\forall (a1, a2) \in \mathbb{Z}^2$*, le système d'équation :*

$z \equiv a_1 \bmod n_1$
$z \equiv a_2 \bmod n_2$

a une solution z unique modulo $n1 \times n2$.

Démonstration:

1. **Existence de la solution :** soit $m_1 = n_2^{-1} \bmod n_1$ et $m_2 = n_1^{-1} \bmod n_2$.
   soit $z = n_2.m_1.a_1 + n_1.m_2.a_2$, alors :
   $z \bmod n_1 \equiv n_2.m_1.a_1 \equiv a_1 \bmod n_1$ car $n_2.m_1 = 1 \bmod n_1$
   $z \bmod n_2 \equiv n_1.m_2.a_2 \equiv a_2 \bmod n_2$ car $n_1.m_2 = 1 \bmod n_2$
   Donc z est solution du système.
2. **Unicité modulo** $n_1 \times n_2$ **:**
   Supposons qu'il existe deux solutions z et z'.
   soit $z" = z - z'$. Alors $n_1|z"$ et $n_2|z"$.
   Puisque $\text{PGCD}(n1, n2) = 1$, alors $(n1 \times n2) \mid z"$.
   Ainsi $(n1 \times n2)|z'$ et $(n1 \times n2)|z$.
   Par conséquent, $z \equiv z' \bmod (n1 \times n2)$.

□

Exemple

Supposons que $z \equiv 2 \bmod 7$ et $z \equiv 4 \bmod 5$.

Calculons :

- $n_2^{-1}.5 = 1 \bmod 7 \Rightarrow m_1 = n_2^{-1} = 3$
- $n_1^{-1}.7 = 1 \bmod 5 \Rightarrow m_2 = n_1^{-1} = 3$

$z = n_2.m_1.a_1 + n_1.m_2.a_2 = 5.3.2 + 7.3.4 = 114 = 9 \bmod 35$

car la solution est dans $\mathbb{Z}_{5\times7}$.

On vérifie $9 \bmod 7 = 2$ et $9 \bmod 5 = 4$. Donc $z = 9$ est bien la solution recherchée.

Application : $391 = 19 \times 17$ et on veut calculer $1704 \bmod 391$.

on a $17 \times 19 \bmod 23 = 1$ (l'inverse de 17 modulo 23 est 19).

on a $23 \times 3 \bmod 17 = 1$ (l'inverse de 23 modulo 17 est 3).

on calcule : $1704 \bmod 17 = 2$ et $1704 \bmod 23 = 4$.

$z = n_2.n_2^{-1}.a_1 + n_1.n_1^{-1}.a_2 = 17.19.2 + 23.3.4 = 922 = 140 \bmod 391$.

Exercice 40: Congruence linéaire

Résoudre les équations suivantes :

1. $8 \times x = 9 \bmod 11$.
2. $9 = 7 \times x \bmod 11$.
3. Quel est l'inverse multiplicatif de 8 dans $\mathbb{Z}_{11}$.
4. Quel est l'inverse multiplicatif de 7 dans $\mathbb{Z}_{11}$.

On pourra utiliser, soit l'algorithme d'Euclide étendu, soit la table de multiplication suivante modulo 11 :

×	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	4	6	8	10	1	3	5	7	9
3	3	6	9	1	4	7	10	2	5	8
4	4	8	1	5	9	2	6	10	3	7
5	5	10	4	9	3	8	2	7	1	6
6	6	1	7	2	8	3	9	4	10	5
7	7	3	10	6	2	9	5	1	8	4
8	8	5	2	10	7	4	1	9	6	3
9	9	7	5	3	1	10	8	6	4	2
10	10	9	8	7	6	5	4	3	2	1

4.4 Exponentiation dans $\mathbb{Z}_n$

On s'intéresse maintenant au calcul de puissances modulo n. A savoir, soit a et b, quel est le résultat de $a^b \bmod n$?

Il s'avère que cette opération est très intéressante pour la cryptographie, comme nous le verrons dans le chapitre suivant, car elle nous permettra de construire

une fonction de chiffrement assez facile à calculer, et difficile à inverser.

Nous verrons les résultats suivants :

- la fonction d'Euler qui a la propriété remarquable de lier le nombre d'entiers premiers avec n à la décomposition de n en facteurs premiers,
- le théorème d'Euler et le petit théorème de Fermat qui exposent les simplifications possibles lors du calcul d'une puissance modulo n si a et premier avec n, ils permettront de déduire les règles de calcul lors d'une exponentiation modulaire.
- pour s'assurer que l'exponentiation engendrera bien une fonction complexe, nous étudierons l'ordre des éléments et les éléments primitifs. Ces propriétés seront utilisées pour les méthodes d'attaque des chiffres utilisant ces propriétés.

4.4.1 Fonction d'Euler

Définition 74 ($\mathbb{Z}_n^*$)**.**
$\mathbb{Z}_n^*$ est l'ensemble des entiers $p < n$ de $\mathbb{Z}_n$ tels que PGCD$(n, p) = 1$.
i.e. $\mathbb{Z}_n^* = \{p \in \mathbb{Z}_n, p < n \mid \text{PGCD}(n, p) = 1\}$

Exemple

$\mathbb{Z}_2^* = \{1\}$
$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$
$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$
$\mathbb{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$

Définition 75 (Fonction d'Euler $\phi(n)$)**.**
La fonction d'Euler est le nombre d'entiers $p < n$ de $\mathbb{Z}_n$ tels que PGCD$(n, p) = 1$.
i.e. $\phi(n) = |\mathbb{Z}_n^*|$

Exemple

$\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$
$\phi(12) = 4$, $\phi(13) = 12$

Remarque : si n est premier, $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$.

Proposition 41 (Propriété de la fonction d'Euler)**.**

1. *si $p \geq 2$ est premier, alors $\phi(p) = p - 1$.*
2. *si $p \geq 2$ est premier, pour tout $e \geq 1$, $\phi(p^e) = p^{e-1}.(p - 1)$.*
3. *pour $n, m > 0$ tel que* PGCD$(n, m) = 1$*, on a : $\phi(n.m) = \phi(n).\phi(m)$*

Démonstration:

1. Si p est premier, pour tout entier $1 \leq a < p$, PGCD$(a, p) = 1$. Donc, $\phi(p) = p - 1$.
2. Les entiers entre 1 et p^e qui ne sont pas premier avec p^e sont tous les multiples de p à savoir $p, 2.p, \ldots, (p^{e-1} - 1).p$.
   Il n'y en a pas d'autre car p est premier.
   Il y a donc $p^{e-1} - 1$ entiers qui ne sont pas premier avec p^e.
   Donc, $\phi(p^e) = (p^e - 1) - (p^{e-1} - 1) = p^e - p^{e-1} = p^{e-1}(p - 1)$.
3. D'après le th. des restes chinois, l'application $f : \mathbb{Z}^*_{nm} \rightarrow \mathbb{Z}^*_n \times \mathbb{Z}^*_m$ telle que $f(a) = (a \bmod n, a \bmod m)$ est une bijection.
   De plus, PGCD$(a, n.m) = 1$ ssi PGCD$(a, n) = 1$ et PGCD$(a, m) = 1$.
   Donc, $|\mathbb{Z}^*_{nm}| = |\mathbb{Z}^*_n|.|\mathbb{Z}^*_m|$, ce qui implique $\phi(n.m) = \phi(n).\phi(m)$.

□

Exemples

1. $\mathbb{Z}^*_7 = \{1, 2, 3, 4, 5, 6\}$, donc $\phi(7) = |\mathbb{Z}^*_7| = 6$.
2. $\phi(8) = \phi(2^3) = 2^{3-1}.(2 - 1) = 4$. Or, $\mathbb{Z}^*_8 = \{1, 3, 5, 7\}$, donc on a bien $\phi(8) = |\mathbb{Z}^*_8| = 4$.
3. $\mathbb{Z}^*_4 = \{1, 3\}$ et $\mathbb{Z}^*_9 = \{1, 2, 4, 5, 7, 8\}$.
   On a bien PGCD$(4, 9) = 1$.
   $\mathbb{Z}^*_{36} = \{1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35\}$.
   Tous les nombres p de $\mathbb{Z}^*_{36}$ sont bien tels que PGCD$(p, 4) = 1$ et PGCD$(p, 9) = 1$.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1
0	1	2	3	4	5	6	7	8	0	1	2	3	4	5	6	7	8

18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
2	3	0	1	2	3	0	1	2	3	0	1	2	3	0	1	2	3
0	1	2	3	4	5	6	7	8	0	1	2	3	4	5	6	7	8

   On a donc bien : $|\mathbb{Z}^*_{36}| = |\mathbb{Z}^*_4|.|\mathbb{Z}^*_9| = 2 \times 6 = 12$.
   Et $\phi(36) = \phi(4) \times \phi(9)$.

Théorème 42 (fonction d'Euler d'un nombre factorisé)**.**
Soit $n = p_1^{e_1}.p_2^{e_2} \ldots p_r^{e_r}$ la factorisation de n en nombres premiers, alors :

$$\phi(n) = \prod_{i=1}^{r} p_i^{e_i - 1}.(p_i - 1) = n.\prod_{i=1}^{r}(1 - 1/p_i)$$

Démonstration:
C'est la conséquence immédiate des propriétés précédentes.

$$\phi(n) = \phi(\prod_{i=1}^{r} p_i^{e_i}) = \prod_{i=1}^{r} \phi(p_i^{e_i}) = \prod_{i=1}^{r} p_i^{e_i-1}.(p_i - 1).$$

Et en remarquant que :

$\prod_{i=1}^{r} p_i^{e_i-1}.(p_i - 1) = \prod_{i=1}^{r} p_i^{e_i}.(1 - 1/p_i) = \prod_{i=1}^{r} p_i^{e_i}. \prod_{i=1}^{r}(1 - 1/p_i)$. □

Exemple

$\phi(36) = \phi(2^2.3^2) = \phi(2^2).\phi(3^2) = 2^1.(2-1) \times 3^1.(3-2) = 2 \times 6 = 12$.
On retrouve bien les résultats de l'exemple précédent.

Exercice 41: Fonction d'Euler

En utilisant les propriétés de la fonction d'Euler, montrer que :

1. Calculer la fonction d'Euler des nombres suivants : 11, 77, 81, 770.
2. Calculer la fonction d'Euler de 5400.

4.4.2 Ordre multiplicatif

Définition 76 (Ordre multiplicatif)**.**
L'ordre multiplicatif d'un entier a modulo n est défini comme étant le plus petit entier $k > 0$ tel que $a^k \equiv 1 \bmod n$.

Exemple

Pour $n = 5$:

i	1	2	3	4
1^i	1	1	1	1
2^i	2	4	3	1
3^i	3	4	2	1
4^i	4	1	4	1

Pour $n = 6$:

i	1	2	3	4	5
1^i	1	1	1	1	1
2^i	2	4	2	4	2
3^i	3	3	3	3	3
4^i	4	4	4	4	4
5^i	5	1	5	1	5

Ordres multiplicatifs modulo 5 : 1 pour 1.
2 pour 4.
4 pour 2 et 3.

Ordres multiplicatifs modulo 6 : 1 pour 1.
2 pour 5.
Les autres ne sont pas inversibles car non premier avec 6.

4.4.3 Théorème d'Euler

Théorème 43 ((Euler))**.**
Pour tout $n > 1$ *et a tel que* PGCD$(a, n) = 1$,
$a^{\phi(n)} \equiv 1 \bmod n$.

Démonstration:
Soit l'application $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ tel que $f(b) = a.b$ pour tout $b \in \mathbb{Z}_n$.
Comme PGCD$(a, n) = 1$, remarquons que f est une permutation.
Exemple : $n = 5$, $a = 2$, alors $\{f(0), f(1), f(2), f(3), f(4)\} = \{0, 2, 4, 1, 3\}$.
Donc, $\prod_{b\in\mathbb{Z}_n^*} b = \prod_{b\in\mathbb{Z}_n^*} a.b = a^{|\mathbb{Z}_n^*|}. \prod_{b\in\mathbb{Z}_n^*} b = a^{\phi(n)}. \prod_{b\in\mathbb{Z}_n^*} b$.
En conséquence, $a^{\phi(n)} \equiv 1 \bmod n$. □

Théorème 44 ((petit théorème de Fermat))**.**
Pour tout nombre premier p,

1. *pour tout* $a \neq 0$*, on a :* $a^{p-1} \equiv 1 \bmod p$.
2. *pour tout a, on a :* $a^p \equiv a \bmod p$.

Démonstration:
1. Conséquence du théorème d'Euler, car si p est premier, $\phi(p) = p - 1$.
2. Multiplier le résultat précédent par a.

□

Conséquences du petit théorème de Fermat

Si p est premier, lorsque l'on travaille modulo p sur les éléments non nuls de $\mathbb{Z}_p^*$, on travaille modulo $p - 1$ sur les exposants.

En effet, tout exposant d peut s'écrire $d = d' + k.(p - 1)$ avec $0 \leq d' < (p - 1)$ *i.e.* $d' = d \bmod (p - 1)$, alors :

$$a^d \bmod p = a^{d'+k.(p-1)} \bmod p = a^{d'} .a^{k.(p-1)} \bmod p = a^{d'} \bmod p$$

car $a^{p-1} \equiv 1 \bmod p$.

Donc, pour tout exposant entier d, on a : $a^d \bmod p = a^{d \bmod (p-1)} \bmod p$

Rappel : $a^d \bmod = (a \bmod p)^d \bmod p$ car $(\prod_i a_i) \bmod n = (\prod_i (a_i \bmod p)) \bmod p$ par propriété du modulo.

Exemple

Soit $p = 31$ (premier),

$$4812^{768} \bmod 31 = (4812 \bmod 31)^{768 \bmod (31-1)} \bmod 31 = 7^{18} \bmod 31.$$

Le nombre de bits nécessaires pour les calculs de puissance n'est donc jamais supérieur à p^2 (voir le calcul de rapide de l'exponentiation modulaire).

Exercice 42: Exponentiation modulaire

1. Dans quel cas $a^n \bmod p = (a \bmod p)^n \bmod p$?
2. Dans que cas $a^n \bmod p = a^{n \bmod \phi(p)} \bmod p$?
3. Calculer $1080^{706} \bmod 7$
4. Calculer $580^{203} \bmod 9$.

4.4.4 Éléments primitifs

On regarde maintenant l'ensemble des valeurs engendrés par l'élévation à la puissance d'un nombre a modulo n ?

Théorème 45 (éléments primitifs)**.**
Si n est premier, alors il existe au moins un élément primitif α qui génère $\mathbb{Z}_n^*$, à savoir :

$$\exists \alpha \in \mathbb{Z}_n^* \mid \mathbb{Z}_n^* = \left\{1, \alpha, \alpha^2, \dots \alpha^{n-2}\right\}$$

Théorème 46 (nombre d'éléments primitifs)**.**
Le nombre d'éléments primitifs de $\mathbb{Z}_n^*$ est $\phi(n-1)$.

Exemple

Pour $n = 5$,

α	α^2	α^3	α^4
1	$1^2 = 1$	$1^3 = 1$	$1^4 = 1$
2	$2^2 = 4$	$2^3 = 3$	$2^4 = 1$
3	$3^2 = 4$	$3^3 = 2$	$3^4 = 1$
4	$4^2 = 1$	$4^3 = 4$	$4^4 = 1$

Donc, $\mathbb{Z}_5^*$ possède 2 éléments primitifs : 2 et 3.
Le nombre d'éléments primitifs est bien $\phi(5-1) = \phi(4) = 2$.

Démonstrations : non données.

L'ordre multiplicatif d'un élément primitif est donc $n - 1$.

Définition 77 (ordre d'un élément)**.**
L'ordre d'un élément a de $\mathbb{Z}_n$ est le plus petit entier k tel que $a^k \bmod n = 1$.

Mais, il est possible d'en dire plus sur les différentes valeurs que peuvent prendre l'ordre des éléments dans $\mathbb{Z}_n$:

Théorème 47 (ordre des éléments dans $\mathbb{Z}_n^*$)**.**
- *(e est l'ordre d'un élément de $\mathbb{Z}_n^*$) $\Leftrightarrow$ ($e \mid n-1$).*
- *$e \mid n-1 \Rightarrow$ il y a exactement $\phi(e)$ éléments d'ordre e.*

Exemple

On reprend l'exemple précédent.
Pour $n = 5$, $\{1, 2, 4\}$ divisent $n - 1 = 4$.
Or $\phi(1) = 1$, $\phi(2) = 1$ et $\phi(4) = 2$.
Il y a 1 élément d'ordre 1, c'est 1.
Il y a 1 élément d'ordre 2, c'est 4.
Il y a 2 élément d'ordre 4, ce sont 2 et 3.

Mais comment trouver un élément primitif ?

On peut utiliser la définition (i.e. tester tous les α^k avec $2 < k < p - 2$), mais évidemment, la complexité est exponentielle.

Théorème 48 (élément générateur de $\mathbb{Z}_n$)**.**
Soit $n - 1 = \prod_i p_i^{n_i}$ la décomposition en facteurs premiers de $n - 1$.
α est un primitif si et seulement si pour tout $1 \leq i \leq k$, on a $\alpha^{(n-1)/p_i} \neq 1$.

Démonstration : Un élément est primitif si $\alpha^i \neq 1$ pour tout $1 \leq i \leq p - 2$. □

Ceci exige de savoir factoriser $p - 1$, et permet de tester plus rapidement si l'élément est primitif.

La construction d'un élément primitif lorsque p est grand ne se fait pas indépendamment de la construction du nombre premier lui-même.

Exemple

Pour $n = 5$, $n - 1 = 4 = 2^2$.
Donc, $k = 1$, $p_1 = 2$, $n_1 = 2$.
On a : $(n - 1)/p_1 = 4/2 = 2$.
Ainsi, un élément α est primitif si $\alpha^2 \neq 1$.
On avait : $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ et $4^2 = 1$.
En conséquence, 2 et 3 sont des éléments primitifs.

Mais comment calculer l'ordre d'un élément quelconque ?

Théorème 49.
Soit $n - 1 = \prod_i p_i^{n_i}$ la décomposition en facteurs premiers de $n - 1$.
Soit $g \in \mathbb{Z}_n^*$. Soit k_i le plus grand entier tel que $g^{(n-1)/p_i^{k_i}} = 1$.
Alors, l'ordre de g est $\prod_i p_i^{n_i - k_i}$.

Exemple

Soit $\mathbb{Z}_{101}$. $n-1 = 100 = 5^2.2^2$. On cherche l'ordre de 2.

$p_1 = 2$	$p_2 = 5$
$k_1 = 2, 2^{100/2^2} = 2^{25} \equiv 10$	$k_2 = 2, 2^{100/5^2} = 2^4 \equiv 16$
$k_1 = 1, 2^{100/2^1} = 2^{50} \equiv 100$	$k_2 = 1, 2^{100/5^1} = 2^{20} \equiv 95$
$k_1 = 0, 2^{100/2^0} = 2^{100} \equiv 1$	$k_2 = 0, 2^{100/5^0} = 2^{100} \equiv 1$

D'où on tire que l'ordre de 2 est $2^{n_1-k_1}.5^{n_2-k_2} = 2^{2-0}.5^{2-0} = 100$.

Conséquence : si $g^{n/p} \neq 1$ pour tous les diviseurs premiers de p, alors l'ordre de g est n.

Exercice 43: Exponentiation entière

Soit $q = 11$ et $p = 7$.

1. Soit $n = p.q$. Calculer $\phi(n)$.
2. Choisir le plus petit a possible tel que PGCD$(a, \phi(n)) = 1$.
3. Calculer b tel que $a.b \equiv 1 \bmod \phi(n)$, à savoir calculer l'inverse multiplicatif de a. On utilisera l'algorithme d'Euclide étendu.
4. Calculer $x = 30^a \bmod n$ en utilisant l'algorithme d'exponentiation modulaire.
5. Calculer $y = x^b \bmod n$ en utilisant l'algorithme d'exponentiation modulaire.
6. Pourquoi ce résultat était-il prévisible ?
7. Supposons maintenant que p ou q divisent x, que se passe-t-il ?
8. Dans le cas où p ou q divisent x (prendre par exemple $x = 33$), calculer alors $x^{ab} \bmod p$ et $x^{ab} \bmod q$, en déduire $x^{ab} \bmod n$.

5 Application : arithmétique sur $GF(2^n)$

5.1 Polynomes sur un corps commutatif

5.1.1 Définitions

Définition 78 (Polynôme sur **R**)**.**
Un polynôme à une variable **R** est une application :
$f(x) = a_n.x^n + a_{n-1}.x^{n-1} + ... + a_1.x + a_0$
où la variable x et les coefficients $a_0, ..., a_n$ sont des éléments **R**.

Notation : L'ensemble des polynômes de variable x sur **R** est noté **R**$[x]$.

On définit :

- le degré d'un polynôme est le coefficient non nul d'ordre le plus élevé.
- la somme et le produit de deux polynômes $f(x) = \sum_{i=0}^{n} a_i.x^i$ et $g(x) = \sum_{i=0}^{m} b_i.x^i$ sont définis de la manière usuelle.
  Les coefficients c_i de :
  - ◇ l'addition $(f + g)(x)$ sont $c_i = a_i + b_i$.
  - ◇ la multiplication $(f.g)(x)$ sont $c_i = \sum_{j,k \mid j+k=i} a_j.b_k$ et $\deg(f.g) = \deg f + \deg g$.

  où les coefficients a_i et b_i non définis sont égaux à 0.
- ainsi, $(\mathbf{R}[X], +, .)$ est un anneau commutatif avec pour élément unité 1.

5.1.2 Division euclidienne et modulo

Si maintenant **R** est un corps commutatif, on a les propriétés suivantes :

Lemme 50 (Diviseur de 0 dans $\mathbf{R}[x]$)**.**
*$R[x]$ des polynômes sur **R** ne contient aucun diviseur de 0 (i.e. $\forall f \in \boldsymbol{R}[x], \nexists a \neq 0 \mid a.f = 0$).*

D'où la possibilité de définir la division euclidienne et le modulo :

Lemme 51 (Division euclidienne dans $\mathbf{R}[x]$)**.** *Soit $f, g \in \boldsymbol{R}[x]$, $g \neq 0$. Alors il existe des polynômes $q, r \in \boldsymbol{R}[x]$ tels que : $f = q.g + r$ avec $r = 0$ ou $\deg r < \deg g$.*

Notes : naturellement, on définit l'opération mod entre deux polynômes comme le reste de leur division euclidienne (*i.e.* $r = f \bmod g$ où $f = q.g + r$ aux conditions ci-dessus).

On note $C_{\max}(g)$ le coefficient de plus haut degré de g. Par exemple, si $g(x) = 3x^4 + 2.x^2 + 5$, $C_{\max}(g) = 3$.

Remarque

On utilise l'algorithme itératif suivant sur les polynômes afin d'effectuer les calculs.

Pour calculer la division euclidienne de $f(x)$ par $g(x)$, on part avec $f_0 = f$

- soit $d_{i+1} = \deg f_i - \deg g$,
- soit $q_{d_i} = C_{\max}(f_i)/C_{\max}(g)$
- calculer $f_{i+1} = f_i - q_{d_i}.x^{d_i}.g$
- tant que $d_i \geq 0$, itéré i et recommencer.

On obtient $q = \sum q_i.x^i$ et $r = f - q.g$.

Exemple

sur $\mathbb{Z}/2\mathbb{Z}[x]$, soient $f(x) = x^3 + x + 1$ et $g(x) = x^2 + x$

i	d_i	q_{d_i}	f_i
0			$x^3 + x + 1$
1	3-2 = 1	1/1 = 1	$(x^3 + x + 1) - 1.x^1.(x^2 + x) = x^2 + x + 1$
2	2-2 = 0	1/1 = 1	$(x^2 + x + 1) - 1.x^0.(x^2 + x) = 1$

on en déduit $q(x) = x + 1$ et $r(x) = 1$.

5.1.3 Irréductibilité

Définition 79 (Zéro d'un polynôme)**.**
Un zéro d'un polynôme f est un $r \in \mathbf{R}$ tel que $f(r) = 0$.

Conséquences

soit $f \in \mathbf{R}[x]$ et $f \neq 0$

- si a est un zéro de f (*i.e.* $f(a) = 0$), alors f est divisible par $(x - a)$. Donc, il existe un polynôme q de $\mathbf{R}[x]$ tel que $f = (x - a).q$.
- f a au plus deg f zéros.

Exemple sur $\mathbb{Z}/2\mathbb{Z}[x]$,

- $x^2 + x$ a deux zéros : 0 et 1.
- $x^2 + 1$ a un zéro : 1
- $x^2 + x + 1$ n'a aucun zéro.

Définition 80 (Polynôme irréductible dans $\mathbf{R}[x]$)**.**
Un polynôme f est dit irréductible s'il ne peut pas s'écrire comme $f = g.h$ où g et h sont des polynômes de $\mathbf{R}[x]$ de degré strictement positif.

Notes : On parle aussi de polynôme premier. Ils jouent exactement le même rôle que les nombres premiers dans $\mathbb{Z}/n\mathbb{Z}$ lorsque l'on définit des corps de Galois $GF(p^n)$.

Un polynôme réductible est un polynôme qui n'est pas irréductible.

Exemples sur $\mathbb{Z}/2\mathbb{Z}[x]$,

- $f(x) = x^2 + x + 1$ est irréductible (s'il était réductible, étant de degré 2, il serait divisible par un polynôme de degré 1, et il aurait donc des zéros).
- $g(x) = x^2 + 1$ n'est pas réductible car $g(x) = (x + 1)^2$.
- noter que $f(x)^2$ est évidemment réductible, mais n'a pas de zéro.

5.2 Construction d'un corps de Galois

5.2.1 Corps de Galois

Définition 81 (Corps de Galois)**.** Un corps commutatif fini s'appelle un corps de Galois.
On le note $GF(q)$.

Exemples

- si p est premier, l'anneau $\mathbb{Z}/p\mathbb{Z}$ $GF(p)$ est un corps de Galois $GF(p)$. On dit que c'est un corps premier.
- si p est premier, le corps $\mathbb{Z}/p\mathbb{Z}[x]$ (construction détaillée ci-après) est un corps de Galois $GF(p^n)$.

Dans le cadre de la cryptographie, nous sommes particulièrement intéressés par les corps de Galois $GF(2^n)$, puisqu'ils nous permettent d'associer un nombre binaire à tout polynôme, et de lui associer un inverse non trivial. Voir la section sur AES pour des exemples concrets.

5.2.2 Principe de construction

Considérons maintenant la construction suivante :

- l'anneau $\mathbb{Z}/p\mathbb{Z}$ (entiers pris modulo p) est un corps commutatif si et seulement si p est un nombre premier (car 0 n'est pas produit par deux entiers non nuls modulo p, et assure l'existence d'un inverse).
- on considère un polynôme irréductible f de $\mathbb{Z}/p\mathbb{Z}[x]$.
- on considère maintenant l'ensemble des classes des résidus des polynômes de $\mathbb{Z}/p\mathbb{Z}[x]$ par la division par f.
- la classe g consiste en tous les polynômes $h \in \mathbb{Z}/p\mathbb{Z}[x]$ tels que $(g - h)$ est un multiple de f.
  Cette classe se note $g + f(\mathbb{Z}/p\mathbb{Z})[x]$.
- comme les représentants de classe de résidus sont constitués de la totalité des polynômes de degré $<$ deg f. En notant $n = \deg f$, p étant premier, il y a donc p coefficients différents possibles pour chaque degré, ce qui conduit à un nombre de classe de résidus possible égal à p^n.
- le polynôme f est irréductible, $\mathbb{Z}/p\mathbb{Z}[x]$ est un corps, et tous ses éléments sont inversibles.

Cette méthode permet donc de construire un corps fini de taille p^n. C'est un corps de Galois $GF(p^n)$.p est appelé la caractéristique du corps.

Exemple :

Soit $f(x) = 1 + x + x^2$ (donc $n = 2$) dans $\mathbb{Z}/2\mathbb{Z}[x]$ (donc $p = 2$).

Les classes des restes de f sont :

- $f(\mathbb{Z}/2\mathbb{Z})$
- $1 + f(\mathbb{Z}/2\mathbb{Z})$
- $x + f(\mathbb{Z}/2\mathbb{Z})$
- $x + 1 + f(\mathbb{Z}/2\mathbb{Z})$

Le corps de Galois construit est donc $GF(2^2) = GF(4)$.

Remarquons les lois d'additions et du multiplications :

+	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

.	1	x	x+1
1	1	x	x+1
x	x	x+1	1
x+1	x+1	1	x

Donc, l'ensemble des classes de résidus munies de l'addition et de la multiplication est un anneau commutatif avec que élément unité $1 + f(\mathbb{Z}/2\mathbb{Z})$.

C'est également un corps commutatif puisque tout élément non nul a un inverse multiplicatif.

Remarques :

- cette construction est possible en raison de l'unicité du reste de la division polynomiale.
- on peut utiliser l'algorithme d'Euclide étendu sur les classes de résidu des polynômes afin de calculer l'inverse multiplicatif.
  L'existence d'un inverse sur est garantie si le polynôme f est irréductible.
- les corps commutatifs produits par deux polynômes irréductibles différents de même degré sont isomorphes.
  c'est la raison pour laquelle la notation $GF(n^p)$ suffit pour décrire le corps (= construit sur les polynômes de $\mathbb{Z}/n\mathbb{Z}$ à partir d'un polynôme irréductible de degré p).

5.2.3 Inversion dans un corps de Galois

L'algorithme d'Euclide étendu peut être directement utilisé pour calculer les inverses.

Exemple

Soit le polynôme irréductible $f(x) = x^7 + x^3 + 1$.

On veut calculer l'inverse de $g(x) = x^5 + x^4 + 1$ modulo $f(x)$.

r_k	q_k	u_k	v_k
$x^7 + x^3 + 1$		1	0
$x^5 + x^4 + 1$		0	1
$x^4 + x^3 + x^2 + x$	$x^2 + x + 1$	1	$x^2 + x + 1$
$x^3 + x^2 + 1$	x	x	$x^3 + x^2 + x + 1$
x^2	x	$x^2 + 1$	$x^4 + x^3 + 1$
1	$x + 1$	$x^3 + x^2 + 1$	$x^5 + x^2$
0	x^2	$x^5 + x^4 + 1$	$x^7 + x^3 + 1$

Donc, l'inverse de $x^5 + x^4 + 1$ modulo $x^7 + x^3 + 1$ est $x^5 + x^2$.

6 Calcul avec les grands nombres entiers

Rappel

Les types entiers utilisables sur une machine sont `int8_t`, `int16_t`, `int32_t`, `int64_t` (existent aussi en `uint*_t`).

Ces types sont standards et définis dans `stdint.h`.

Portabilité 32/64bit : initialiser un entier x 64 bits avec les macros `__I64(x)` (resp. `__U64(x)` si non signé) car le nombre de `L` change.

Nous allons effectuer des calculs sur des grands nombres entiers dont la précision dépasse largement des types simples sur les machines.

Typiquement sur 128, 192, 256, ... bits.

Comment réaliser de tels calculs sur un ordinateur ?

6.1 Réprésentation des grands entiers

Réprésentation des grands entiers

Un entier est représenté comme un entier de chiffres en base B, avec un bit de signe :

$$a = \pm \sum_{i=0}^{k-1} a_i.B^i = \pm(a_{k-1} \dots a_0)_B$$

avec $0 \leq a_i < B$.

Si on prend :

- $B = 2$, c'est la décomposition en binaire du nombre en entier sur k bits.
- $B = 2^v$ (par exemple, $v = 32$), permet de coder a avec des mots de 32 bits, donc sur $k \times 32$ bits.

Exemples

- $147 = (10010011)_2 = 1.2^7 + 0.2^6 + 0.2^5 + 1.2^4 + 0.2^3 + 0.2^2 + 1.2^1 + 1.2^0$
- $147 = (93)_{16} = 9.16 + 3$

6.2 Addition/multiplication

Addition $c = a + b$ **avec** $a, b > 0$

$a = (a_{k-1} \dots a_0)_B$ et $b = (b_{\ell-1} \dots b_0)_B$ avec $k \geq \ell \geq 1$,
$c = (c_k c_{k-1} \dots c_0)_B$.

Algorithme :

$q = 0$
pour $i = 0, \dots, k-1$
si $(i \leq \ell - 1)$ alors $s = a_i + b_i + q$
si $(i \geq \ell)$ alors $s = a_i + q$
$c_i = s \bmod B$
$q = s/B$
si $(r = 1)$ alors $c_k = 1$

Complexité : $c_+ \times \log_2(\max(a, b))$.

Multiplication $c = a.b$ **avec** $a, b > 0$

$a = (a_{k-1} \dots a_0)_B$ et $b = (b_{\ell-1} \dots b_0)_B$ avec $k \geq \ell \geq 1$,
$c = (c_{k+\ell-1} \dots c_0)_B$.

Algorithme :

$r = 0$
pour $i = 0, \dots, k + \ell - 1$
$c_i = 0$
pour $i = 0, \dots, k-1$
$r = 0$
pour $j = 0, \dots, \ell - 1$
$s = a_i \times b_j + c_{i+j} + r$
$r = s/B$
$c_{i+j} = s \bmod B$
$c_{i+\ell} = r$

Complexité : $c_\times \times \log_2 a \times \log_2 b$

Exercice 44: Calcul sur des grands nombres

1. Soit $a = (101)_2$ et $b = (1101)_2$. Calculer $a + b$ en utilisant l'algorithme pour les grands nombres.
2. Soit $a = (a4f)_{16}$ et $b = (b4)_{16}$. Calculer $a \times b$ en utilisant l'algorithme pour les grands nombres.

6.3 Division Euclidienne

Division avec reste $a = b.q + r$ **avec** $a > b > 0$

But : calculer q et r tel que $a = b.q + r$ et $0 \leq r < b$.
On note $a = (a_{k-1} \dots a_0)_B$, $b = (b_{\ell-1} \dots b_0)_B$
$q = (q_{m-1} \dots q_0)_B$, avec $m := k - \ell + 1$, $r = (r_{k-1} \dots r_0)_B$.

Algorithme :

$r = a$
pour $i = m - 1$ à 0
  $q_i = r/(B^i.b)$
  $r = r - B^i.q_i.b$

Mais comment calculer $q_i = r/(B^i.b)$?

$q_i = 0$
tant que $r \geq 0$
  $r = r - (B^i.b)$
  $q_i = q_i + 1$
$q_i = q_i - 1$

Complexité : $c_/ \times \log_2 a \times \log_2(a/b)$

6.4 Exponentiation

Exponentiation

On veut calculer $c = a^d$.

Méthode naïve : multiplier d fois a par lui-même.
mauvaise idée, si d fait 128 bits, $2^{128} - 1$ multiplications !

Remarquons que $b = b^{2^0}$, $b.b = b^{2^1}$, $b^2.b^2 = b^{2^2}$, $b^4.b^4 = b^{2^3}$, ...
En conséquence, si l'on écrit en binaire $d = \sum_{i \geq 0} d_i.2^i$, on a :
$a^d = a^{\sum_{i \geq 0} d_i.2^i} = \prod_{i \text{ tel que } d_i = 1} a^{2^i}$ car si $d_i = 0$, $a^{d_i.2^i} = 1$.

Algorithme : calculer $c = a^d$ où $\ell = \lceil \log_2 d \rceil$

$c = 1$
pour $i = \ell - 1$ à 0
  $c = c^2$
  si $d_i = 1$ alors $c = c \times a$

Complexité : $2 \times \ell \times$ multiplication

Exemple : si $c = a^{10}$, $10 = 1010_2$

i	c	d_i	maj c
3	1	1	$1.a$
2	a^2	0	
1	a^4	1	$a^4.a$
0	a^{10}	0	

C'est l'algorithme à utiliser pour implémenter la fonction `pow` sur des entiers.

6.5 Exponentiation modulaire

Exponentiation modulaire

On veut calculer $c = a^d \bmod n$.

On reprend l'algorithme précédent de l'exponentiation simple, mais en effectuant la réduction modulaire chaque fois que possible (= on fait une multiplication modulaire).

Algorithme : calculer $c = a^d \bmod n$ où $\ell = \lceil \log_2 d \rceil$
  $c = 1$
  pour $i = \ell - 1$ à 0
    $c = c^2 \bmod n$
    si $d_i = 1$ alors $c = (c \times a) \bmod n$

Complexité : $2 \times \ell \times$ multiplication modulaire

Exercice 45: Exponentiation

En utilisant l'algorithme d'exponentiation :

1. Calculer 3^{11}.
2. Calculer $q = 2^{57} \bmod 11$.

7 Conclusion

La compréhension de cette leçon est importante car elle présente une partie des bases nécessaires afin de comprendre pourquoi les différentes méthodes de

cryptographie moderne que nous étudions fonctionnent.

Nous avons vu dans cette leçon :

- un rappel des définitions de la division euclidienne, du pgcd, des nombres premiers et de l'algorithme d'euclide,
- un présentation générale sur la façon d'implémenter les calculs sur de grand nombres entiers sur une machine,
- un rappel d'algèbre sur les propriétés des ensembles qui explique comment construire des corps finis sur lesquels l'inversion et l'exponentiation sont possibles,
- l'application de ce principe à la construction de $\mathbb{Z}/n\mathbb{Z}$, ainsi que l'ensemble des propriétés pour des calculs sur $\mathbb{Z}_n$.
- l'application de ce principe, en partant de l'ensemble $\mathbb{Z}/n\mathbb{Z}[x]$, définir un nombre fini de classes d'équivalence par réduction modulaire à un polynôme irréductible, afin d'obtenir des corps de Galois.