ARITHMÉTIQUE ET ALGÈBRE

1ere année ESIL, département d'informatique
A. Bonnecaze

Table des matières

Chapitre 1

Rappels sur la théorie des ensembles

1.1 Constructions d'ensembles

Inclusion d'ensembles

On dit que l'ensemble E est inclus dans l'ensemble F si on a

$$\forall x, (x \in E) \Rightarrow (x \in F).$$

Si tel est le cas, on écrit $E \subset F$ et on dit que E est une **partie** de F.
L'ensemble des parties de E est noté $\mathcal{P}(E)$.
Il existe un seul ensemble qui ne contient aucun élément.
On l'appelle l'**ensemble vide** et on le note $\emptyset$.

Transitivité de l'inclusion

Soient E, F et G des ensembles tels que $E \subset F$ et $F \subset G$. Alors $E \subset G$.

Opérations sur les ensembles

Soient F et G deux parties d'un ensemble E. On définit alors
- le **complémentaire** de F dans E : ${}^cF = \{x \in E,\ x \notin F\}$,
- la **réunion** de F et G : $F \cup G = \{x \in F \text{ ou } x \in G\}$,
- l'**intersection** de F et G : $F \cap G = \{x \in F \text{ et } x \in G\}$,
- la **différence** de F et G : $F \setminus G = \{x \in F \text{ et } x \notin G\}$.

Produit cartésien

On appelle **produit cartésien** de deux ensembles E et F, l'ensemble des couples $(x,\ y)$ tels que $x \in E$ et $y \in F$ et on le note $E \times F$.

1.2 Relations et applications

Relations et applications

Soient E et F deux ensembles.
- On appelle **relation** (ou correspondance) de E vers F tout triplet $(G,\ E,\ F)$ où G est une partie de $E \times F$. Les ensembles $G,\ E,\ F$ sont respectivement appelés **graphe, ensemble de départ** et **ensemble d'arrivée** de la relation.

– On appelle application de E dans F toute relation $f = (G,\ E,\ F)$ de E vers F telle que, pour tout x de E, il existe un unique y tel que $(x,\ y) \in G$ et on note $f : E \to F$.
On note alors $y = f(x)$ et on appelle y l'**image** de x par f. On note $\mathcal{F}(E, F)$ l'ensemble des applications de E dans F.

Image directe et image réciproque d'une application

Soit f une application de E dans F.
– Pour toute partie A de E, on appelle **image directe** de A par f, l'ensemble des y de F pour lesquels il existe un x dans A tel que $y = f(x)$ et on la note $f(A)$.
– Pour toute partie B de F, on appelle **image réciproque** de B par f, l'ensemble des x de E dont l'image est dans B et on la note $f^{-1}(B)$.

Composée d'applications

Soient E, F, G trois ensembles et $f : E \to F$ et $g : F \to G$ deux applications. On appelle composée de f et g l'application $h : E \to G$ telle que $\forall x \in E,\ h(x) = g(f(x))$. On la note $h = g \circ f$.

Prolongement et restriction d'une application

Soient E et F deux ensembles et H une partie de E.
– Soit f une application de E dans F. On appelle restriction de f à H l'application notée $f_{|H}$ de H dans F définie par $\forall x \in H,\ f_{|H}(x) = f(x)$.
– Soit f une application de H dans F. On appelle prolongement de f à E toute application g de E dans F telle que $g_{|H} = f$.

1.3 Injectivité, surjectivité, bijectivité

Application InJective, surjective et bijective

Soit $f : E \to F$ une application. On dit que f est
– **injective** si l'égalité $f(x) = f(y)$ implique $x = y$.
– **surjective** si tout élément de F est l'image par f d'au moins un élément de E,
– **bijective** si f est à la fois injective et surjective, c'est-à-dire,

$$\forall y \in F,\ \exists! x \in E,\ y = f(x).$$

Composée d'applications

La composée de deux applications injectives (respectivement surjectives, bijectives) est injective (resp. surjective, bijective).

1.4 Familles

Familles et sous-familles

Soient I et E deux ensembles.
– On appelle famille d'éléments de E indexée par I toute application x de I dans E et on note la famille $(x_i)_{i \in I}$.
– On appelle sous-famille d'une famille $(x_i)_{i \in I}$ toute restriction de l'application x.
On peut alors généraliser les notions de réunion et d'intersection que l'on avait défini que pour les paires d'ensembles.

Opérations sur les familles

Soient E un ensemble et $(E_i)_{i\in I}$ une famille de parties de E. On définit alors
- la **réunion de la famille** $(E_i)_{i\in I}$: $\bigcup_{i\in I} E_i = \{x \in E,\ \exists i \in I,\ x \in E_i\}$
- l'**intersection de la famille** $(E_i)_{i\in I}$: $\bigcap_{i\in I} E_i = \{x \in E,\ \forall i \in I,\ x \in E_i\}$

Partition d'un ensemble

Soit $(X_i)_{i\in I}$ une famille de parties d'un ensemble E. On dit que cette famille est une partition de E si
- $\forall i \in I,\ X_i \neq \emptyset$
- $\forall (i,j) \in I^2,\ (i \neq j) \rightarrow X_i \cap X_j = \emptyset$
- $\bigcup_{i\in I} X_i = E$

1.5 Relation d'équivalence

Relation binaire

Soit E un ensemble. On appelle **relation binaire** sur E toute relation de E vers E. Si $\mathcal{R}$ est une relation binaire sur E, on écrira $x\mathcal{R}y$ au lieu de $(x,\ y) \in E^2$ et $(x,\ y) \in G$.

Relation d'équivalence (RST)

Soit $\mathcal{R}$ une relation binaire sur un ensemble E. On dit que $\mathcal{R}$ est une **relation d'équivalence** si elle est à la fois
- **Réflexive** $(\forall x \in E,\ x\mathcal{R}x)$
- **Symétrique** $(\forall (x,y) \in E^2,\ x\mathcal{R}y \Rightarrow y\mathcal{R}x)$
- **Transitive** $(\forall (x,y,z) \in E^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z)$

Classes d'équivalence

Soit E un ensemble muni d'une relation d'équivalence $\mathcal{R}$. On appelle **classe d'équivalence** d'un élément x de E **modulo** $\mathcal{R}$, l'ensemble $C(x)$ défini par

$$C(x) = \{y \in E,\ x\mathcal{R}y\}.$$

Ensemble des classes d'équivalence

L'ensemble des classes d'équivalence de la relation $\mathcal{R}$ forme une partition de E.

1.6 Relation d'ordre

Relation d'ordre (RAT)

Soit $\mathcal{R}$ une relation binaire sur un ensemble E. On dit que $\mathcal{R}$ est une relation d'ordre si elle est à la fois

- **Réflexive** $(\forall x \in E,\ x\mathcal{R}x)$
- **Antisymétrique** $(\forall (x,y) \in E^2,\ x\mathcal{R}y \text{ et } y\mathcal{R}x) \rightarrow x = y)$.
- **Transitive** $(\forall (x,y,z) \in E^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \Rightarrow x\mathcal{R}z)$

Ensemble ordonné

Un ensemble muni d'une relation d'ordre est dit **ordonné**.

Ordre total et ordre partiel

Un ordre $\leq$ sur un ensemble E est dit **total** si deux éléments quelconques de E sont comparables, c'est-à-dire si, étant donnés x et y dans E, on a $x \leq y$ ou $y \leq x$. Un ordre non total est dit **partiel**.

Maximaux, minimaux, majorants et minorants

Soient $(E, \leq)$ un ensemble ordonné et A une partie de E.

- Soit $M \in E$. On dit que M est un **majorant** de A dans E si $\forall x \in A,\ x \leq M$. Dans ce cas, on dit que A est majorée par M.
- Soit $m \in E$. On dit que m est un **minorant** de A dans E si $\forall x \in A,\ m \leq x$. Dans ce cas, on dit que A est minorée par m.
- On dit que A admet un **plus grand élément** s'il existe un majorant de A dans E qui appartienne à A.
- On dit que A admet un **plus petit élément** s'il existe un minorant de A dans E qui appartienne à A.

1.7 Problème

Rappels : Dans un ensemble ordonné, un élément maximal est un élément tel qu'il n'existe aucun autre élément de cet ensemble qui lui soit supérieur. Dans un ensemble ordonné, le plus grand élément (resp. plus petit élément) ou élément maximum (resp. élément minimum) d'une partie de cet ensemble est l'élément qui, quand il existe, appartient à cette partie et est supérieur (resp. inférieur) à tous autres éléments de la partie. Soit E un ensemble ordonné et F une partie de E, un majorant (resp. minorant) de F est un élément x de E tel que tous les éléments de F sont inférieurs (resp. supérieurs) à x. Dans un ensemble ordonné E, la borne supérieure (resp. borne inférieure) d'une partie majorée (resp. minorée) F de E est, s'il existe, le plus petit (resp. le plus grand) majorant (resp. minorant) de F.

Soit A un ensemble de cardinal $2n, \quad n > 2$. On note $\mathcal{P}(A)$ l'ensemble des parties de A. L'ensemble $\mathcal{P}_i(A)$ (resp $\mathcal{P}_p(A)$) représente l'ensemble des parties de A de cardinaux impairs (resp pairs). On considère maintenant la relation dans $\mathcal{P}(A)$ définie par

$$x\mathcal{R}y \text{ ssi } x \subseteq y$$

I Montrer que $\mathcal{R}$ est une relation d'ordre. Est-elle une relation d'ordre total ?

II Existe-t-il un plus grand (resp un plus petit) élément dans $\mathcal{P}(A)$?

III Existe-t-il un maximum (resp minimum) dans $\mathcal{P}_i(A)$, $\mathcal{P}_p(A)$?

IV Soit $a,\ b,\ c$ trois éléments de A deux à deux distincts :

a) Déterminer le cardinal des ensembles

$$\mathcal{P}_{3i}(A) = \{x \in \mathcal{P}_i(A) \quad | \quad \{a,\ b,\ c\} \subseteq x\}$$

$$\mathcal{P}_{3p}(A) = \{x \in \mathcal{P}_p(A) \quad | \quad \{a,\ b,\ c\} \subseteq x\}$$

b) Existe-t-il un élément minimum (resp maximum) dans $\mathcal{P}_{3i}(A)$?

c) Même question pour $\mathcal{P}_{3p}(A)$.

d) Déterminer l'ensemble $\mathcal{M}$ des minorants de $\mathcal{P}_{3p}(A)$; cet ensemble $\mathcal{M}$ admet-il une borne supérieure ?

V Soit f la fonction de l'ensemble $\mathcal{P}(\mathcal{P}_i(A)) \setminus \emptyset$ dans $\mathcal{P}(A) \setminus \emptyset$ définie par

$$f(E) = \bigcup_{X \in \mathcal{P}(A)} X \quad | \quad X \text{ est maximal dans } E$$

a) On suppose que $A = \{a,\ b\}$.

1) Déterminer la liste explicite des éléments de $\mathcal{P}(\mathcal{P}_i(A))$.

2) Expliciter $f(E)$ pour chaque E appartenant à $\mathcal{P}(\mathcal{P}_i(A)) \setminus \emptyset$.

b) On revient maintenant au cas général (on suppose que A est un ensemble de cardinal pair).

1) Montrer que f est une application. Est-elle surjective, injective ?

2) On suppose que l'ensemble d'arrivée est $\mathcal{P}_i(A) \setminus \emptyset$ au lieu de $\mathcal{P}(A) \setminus \emptyset$.
f est-elle une application ?

Chapitre 2

Propriétés des entiers

L'ensemble des nombres entiers est noté $\mathbb{Z}$:

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\},$$

et celui des entiers $n \geq 0$ est noté $\mathbb{N}$.
Dans la suite, les lettres désigneront toujours des entiers quelconques, sauf précision : ainsi, $a > 0$ signifiera $\forall a \in \mathbb{Z}$ et $a > 0$, et « il existe a tel que... » fera référence à un entier a vérifiant une certaine condition.

2.1 Division entière

Soit $a, b \in \mathbb{Z}$, b divise a si il existe $c \in \mathbb{Z}$ tel que $a = bc$. L'élément b est alors un **diviseur** de a et on écrit $b|a$. **Exemple.** $-6|30 \;\; 190|0 \;\; 11|759$

Théorème 2.1.1. *Quels que soient les entiers a, b, c, on a :*

a) $1|a$, $a|a$, $a|0$.

b) $0|a$ *SSI* $a = 0$.

c) Si $a|b$ *et* $b|c$, *alors* $a|c$.

d) Si $a|b$ *et* $a|c$, *alors* $a|(bx + cy)$, $\forall x, y \in \mathbb{Z}$.

e) $a|b$ *et* $b|a$ *SSI* $a = \pm b$.

Démonstration. de l'item e).
Si $a = \pm b$ alors $a|b$ et $b|a$.
Si $a|b$ et $b|a$, alors $b = ac$ et $a = bd$ pour $c, d \in \mathbb{Z}$. Donc $b = bdc$ et $dc = 1$. Donc $c = d = 1$ ou c=d=-1.
Donc $a = \pm b$. □

Théorème 2.1.2. *(Division entière) Si* $a, b \in \mathbb{Z}$, $b \geq 1$, *alors il existe un unique couple* $(q, r) \in \mathbb{Z}^2$ *tel que*

$$a = bq + r \quad \textit{avec } 0 \leq r < b$$

q *est appelé le* **quotient** *et* r *le* **reste** *de la division de* a *par* b.

$$\begin{cases} r = a \mod b \\ q = a \div b \end{cases}$$

De plus, on a $a \div b = \lfloor a/b \rfloor$ *et* $a \mod b = a - b\lfloor a/b \rfloor$.

Exemple. Si $a = 73$ et $b = 17$, alors :

$$\begin{cases} q = 4, \; r = 5, \\ 73 \div 17 = 4, \\ 73 \mod 17 = 5\,. \end{cases}$$

Un entier c est un **diviseur commun** à a et b si $c|a$ et $c|b$.

2.2 Nombre premier

Un entier $p \geq 2$ est dit premier si ses seuls diviseurs positifs sont 1 et p. Sinon on dit que le nombre est composé.
Il existe dans $\mathbb{Z}$ une infinité de nombres premiers. Supposons en effet que leur ensemble soit fini : $\{p_1, \ldots, p_n\}$. Le nombre $q = p_1 \ldots p_n + 1$ n'est divisible par aucun des p_i, le reste étant toujours égal à 1. N'étant pas dans la liste, q n'est pas premier, et il est donc divible par un nombre premier, ce qui est absurde.

Théorème 2.2.1. *(Théorème fondamental de l'arithmétique) Tout entier $n \geq 2$ admet une factorisation unique comme produit de puissances de nombres premiers.*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Démonstration. L'existence de la factorisation se fait par induction sur n.
Si $n = 2$ OK. Supposons que la propriété soit vraie jusqu'à $n-1$, est-elle vraie pour n ?
Si n est premier OK. Sinon $n = ab$ avec $a < n$ et $b < n$. Donc la factorisation existe pour a et b et donc elle existe pour n. L'unicité sera démontrée plus tard. □

2.3 Idéaux, PGCD et PPCM

Un **idéal** de $\mathbb{Z}$ est un ensemble non vide d'entiers qui est clos par addition et par multiplication par un entier arbitraire .
Définition. Un ensemble $I \subseteq \mathbb{Z}$ non vide est un idéal si et seulement si pour tout $a, b \in I$ et pour tout $z \in \mathbb{Z}$, $a + b \in I$ et $az \in I$.
Remarques :

1. Si $a \in I$ alors $-a \in I$
2. $0 \in I$ car $a + (-a) \in I$
3. Si $1 \in I$ alors $I = \mathbb{Z}$.

Définition. $a\mathbb{Z} := \{az : z \in \mathbb{Z}\}$ est l'ensemble des multiples de a. $a\mathbb{Z}$ est un idéal généré par a. Tous les idéaux de la forme $a\mathbb{Z}$ sont appelés **idéaux principaux**.
Considérons maintenant $a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z} := \{a_1 z_1 + \cdots + a_k z_k : z_1, \cdots, z_k \in \mathbb{Z}\}$. Cet objet est un idéal engendré par les a_i. C'est le plus petit idéal contenant les a_i.
Exemple.

- $a = 3,\ aZ = \{\ldots, -9, -6, -3, 0, 3, 6, \ldots\}$
- $a_1 = 3, a_2 = 5,\ a_1\mathbb{Z} + a_2\mathbb{Z} = \mathbb{Z}$ car $2a_1 - a_2 = 1$
- $a_1 = 4, a_2 = 6,\ a_1\mathbb{Z} + a_2\mathbb{Z} = 2\mathbb{Z}$

Théorème 2.3.1. *Pour tout idéal $I \subset \mathbb{Z}$, il existe un unique entier positif d tel que $I = d\mathbb{Z}$.*

Démonstration.

- Si $I = \{0\}$, alors $d = 0$
- Si $I \neq \{0\}$, I contient un entier strictement positif. Soit d le plus petit entier positif de I. On veut montrer que $I = d\mathbb{Z}$.
    1. Montrons que $I \subseteq d\mathbb{Z}$. Soit $c \in I$, il faut montrer que $d|c$. On a $c = qd + r \in I$ avec $0 \leq r < d$, donc $r = c - qd \in I$. On en déduit que $r = 0$ car par hypothèse d est le plus petit élément de I. Donc $d|c$
    2. Montrer que $d\mathbb{Z} \subseteq I$ est immédiat puisque $d \in I$.

On a prouvé qu'il existe un $d > 0$ tel que $I = d\mathbb{Z}$.
Unicité : si $d\mathbb{Z} = d'\mathbb{Z}$, on a $d|d'$ et $d'|d$ donc $d = \pm d'$. □

Pour $a, b \in I$, on appelle $d \in \mathbb{Z}$ un diviseur commun de a et b si $d|a$ et $d|b$. L'élément d est le PGCD de a et b si $d \geq 0$. et tous les autres diviseurs communs de a et b divisent d.

Théorème 2.3.2. *Pour tout $a, b \in \mathbb{Z}$, il existe un unique PGCD d de a et b et de plus $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.*

Démonstration. D'après le théorème précédent, tout idéal s'écrit $d\mathbb{Z}$ avec $d > 0$. Il faut donc montrer que $d = PGCD(a, b)$. Posons $I = d\mathbb{Z}$, puisque $a, b \in I$, on a $d|a$ et $d|b$ et d est un diviseur commun de a et b. Puisque $I = a\mathbb{Z} + b\mathbb{Z}$, $\exists s, t \in Z$ tel que $d = as + bt$. Supposons que $a = a'd'$ et $b = b'd'$, alors l'équation $d = as + bt$ implique $d'(a's + b't) = d$. donc $d'|d$. Donc tout diviseur commun de a et b divise aussi d. Donc $d = PGCD(a, b)$.
Unicité : Si $d'' = PGCD(a, b)$, alors $d''|d$ et $d|d''$, donc $d = d''$ car d et d'' sont strictement positifs. □

Remarque : $PGCD(a, 0) = |a|$.
Calcul du PGCD : En pratique, on utilise l'algorithme d'Euclide :
Calcul de $PGCD(a, b)$
$R0 := |a|$;
$R1 := |b|$; $\quad (b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;
En sortie $R1 = 0$, et $R0 = pgcd(a, b)$.

Théorème 2.3.3. *(Bézout)*
$\forall a, b \in \mathbb{Z}, \exists s, t \in \mathbb{Z}$ *tel que* $as + bt = PGCD(a, b)$.
Si $PGCD(a, b) = 1$, a et b sont dits premiers entre eux. Il existe $s, t \in \mathbb{Z}$ tel que $as + bt = 1$.

Exemple. $PGCD(12, 42) = 6$ et on a
$(-3).12 + 1.42 = 6$
$4.12 + (-1).42 = 6$
Remarque : A partir d'un couple solution (x_0, y_0), il est possible d'obtenir toutes les autres solutions de la manière suivantes : $a(x_0 - k\frac{b}{d}) + b(y_0 + k\frac{a}{d}) = d$.

Théorème 2.3.4. *Pour $a, b, c \in \mathbb{Z}$ tel que $c|ab$ et $PGCD(a, c) = 1$, on a $a|b$.*

Démonstration. Supposons que $c|ab$ et $PGCD(a, c) = 1$.
$PGCD(a, c) = 1$ implique $as + ct = 1$ pour $s, t \in \mathbb{Z}$. On a $abs + cbt = b$ puisque c divise ab et $c|cbt$, on a $c|abs + cbt$ donc $c|b$. □

Théorème 2.3.5. *(Conséquence de la factorisation unique)*
Il existe une infinité de nombres premiers.

Démonstration. Supposons qu'il existe un nombre fini de nombres premiers : $p_1, \ldots, p_n$. Le nombre $q = p_1 \ldots p_n + 1$ n'est divisible par aucun des p_i, le reste étant toujours égal à 1. N'étant pas dans la liste, q n'est pas premier, et il est donc divible par un nombre premier, ce qui est absurde. □

Soit p un nombre premier. Soit $n \neq 0$ et $n = p^e m$ avec $p \nmid m$. On considère la fonction $\nu_p(n) := e$. On peut alors écrire

$$n = \pm \prod_p p^{\nu_p(n)}.$$

On peut étendre le domaine de définition de ν_p pour inclure 0 : $\nu_p(0) = \infty$.
On a ainsi

$$\nu_p(a.b) = \nu_p(a) + \nu_p(b) \ \ \forall p.$$

Pour tout $a, b \in \mathbb{Z}$ on a

$$b|a \Leftrightarrow \nu_p(b) \leq \nu_p(a) \ \ \forall p$$

et

$$\nu_p(PGCD(a,b)) = min(\nu_p(a), \nu_p(b)) \ \ \forall p.$$

Un entier m est un multiple commun de a et b si $a|m$ et $b|m$. Il est Plus Petit Multiple Commun (PPCM) s'il est positif et s'il divise tous les multiples communs de a et b. Le PPCM de deux entiers existe et est unique. On a $PPCM(a,0) = 0$
$PPCM(a,b)$ est le plus petit entier positif divisible par a et b. Pour tout a, bßß$\mathbb{Z}$, on a

$$\nu_p(PGCD(a,b)) = max(\nu_p(a), \nu_p(b)) \ \ \forall p.$$

On peut généraliser le PPCM à plusieurs entiers $a_1, \ldots, a_k$. Les éléments $a_1, \ldots, a_k$ sont premiers deux à deux si $PGCD(a_i, a_j) = 1$, pour tout i et j tel que $1 \leq i \neq j \leq k$.
Exercices. Si $PGCD(a_1, \ldots, a_k) = 1$, les entiers sont-ils premiers deux à deux ?
Soit $a, b \in /Z, p$ premier. Si $\nu_p(a) < \nu_p(b)$, alors a-t-on $\nu_p(a) + \nu_p(b) = \nu_p(a)$?

2.4 Exercices

1. L'algorithme de division entière le plus simple consiste à soustraire autant de fois b de a qu'il est possible, jusqu'à obtenir un reste $< b$. Mais il existe un autre algorithme appelé algorithme de division binaire.

Division:=proc(a,b)
local r, q, u ;

$r := a$;
$q := 0$;
while $(r >= b)$
. do
. $r := r - b$;
. $q := q + 1$;
. od ;
$u := [q, r]$;
return(u) ;
end ;

DivisionBinaire:=proc(a,b)
local r,q,aux,n,u ;
. $r := a$; $q := 0$; $n := 0$; $aux := b$;
. while $(aux <= a)$
. $aux := 2 * aux$;
. $n := n + 1$;
. while $(n > 0)$
. $aux := aux/2$;
. $n := n - 1$;
. if $(r < aux)$
. then
. $q := 2 * q$;
. else
. $q := 2 * q + 1$;
. $r := r - aux$;
. fi ; . $u := [q, r]$;
. return(u) ;
end ;

   (a) Faire tourner les deux algorithmes pour calculer $123/23$, puis $256/2$.

   (b) Comparer les deux algorithmes en terme d'efficacité (nombre de boucles)

2. Montrer que l'algorithme d'Euclide se termine et qu'il calcule le PGCD
Algorithme d'Euclide $R0 := |a|$;
$R1 := |b|$; $\quad (b \neq 0)$
Tantque $R1 > 0$ Faire
$R := Reste\_Division(R0, R1)$;
$R0 := R1$;
$R1 := R$;

3. Calculer $PGCD(79, 23)$

4. On note $a\mathbb{Z} := \{\ldots, -a, 0, a, 2a, 3a, 4a, \ldots\}$ et on définit pour $a_1, \ldots, a_k$

$$a_1\mathbb{Z} + \cdots + a_k\mathbb{Z} := \{a_1z_1 + \cdots + a_kz_k : z_1, \ldots, z_k \in \mathbb{Z}\}$$

   (a) Calculer $3\mathbb{Z} + 5\mathbb{Z}$, $6\mathbb{Z} + 9\mathbb{Z}$

   (b) Soit $a, b \in \mathbb{Z}$ et $d = PGCD(a, b)$, montrer que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$.

   (c) Que vaut $a\mathbb{Z} + b\mathbb{Z}$ si a et b sont premiers entre eux ?

5. Soit $a, b, c \in \mathbb{Z}$ tel que $c|ab$ et $PGCD(a, c) = 1$, montrer que $c|b$.

6. Si $PGCD(a_1, \ldots, a_k) = 1$, les entiers a_i sont-ils premiers deux à deux ?

7. Soit p un premier, $a, b \in \mathbb{Z}$. Montrer que $p|ab$ implique que $p|a$ ou $p|b$.

8. Soit $a_1, \ldots, a_k$ des entiers et p un premier. Montrer que si $p| \prod a_i$, alors $p|a_i$ pour un $i \in 1, \ldots, k$.

9. Montrer l'unicité de la factorisation d'un entier (théorème fondamental de l'arithmétique).

Chapitre 3

Congruences

3.1 Classes d'équivalence

Soit n un entier positif.

Définition. Rappelons la relation entre les entiers a et b : a est congru à b modulo n, ce qui s'écrit $a \equiv b \pmod{n}$, si $n|(a-b)$; n est le **module** de la congruence.

Exemples.

$$\begin{array}{rcll} 24 \equiv 9 & (\mathrm{mod}\ 5) & \text{puisque} & 24-9 = 3\,.\,5\,. \\ -11 \equiv 17 & (\mathrm{mod}\ 7) & \text{puisque} & -11-17 = -4\,.\,7\,. \end{array}$$

Propriétés de la congruence. $\forall\, a, a_1, b, b_1, c \in \mathbb{Z}$:

- $a \equiv b \pmod{n} \iff a$ et b ont le même reste dans la division par n.
- $a \equiv a \pmod{n}$ (réflexivité).
- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ (symétrie).
- $a \equiv b \pmod{n}$ et $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (transitivité).
- $a \equiv a_1 \pmod{n}$ et $b \equiv b_1 \pmod{n} \Rightarrow \begin{cases} a+b \equiv a_1+b_1 \pmod{n}\,, \\ ab \equiv a_1 b_1 \pmod{n}\,. \end{cases}$

Exemple : Résoudre $3x + 4 \equiv 6 \mod 7$.
On peut écrire $3x \equiv 2 \mod 7$ puis multiplier l'équation par 5 pour obtenir $x \equiv 3 \mod 7$.

Remarque : $a \equiv b \mod n$ si et seulement si il existe c tel que $a = b + cn$.

3.2 Résoudre les congruences linéaires

Soit $n > 0, a \in \mathbb{Z}$, $a' \in \mathbb{Z}$ est l'inverse multiplicatif de $a \mod n$ si $a.a' \equiv 1 \mod n$. On note $a^{-1} \mod n$ l'inverse de a modulo n.

Théorème 3.2.1. *L'entier a admet un inverse multiplicatif modulo n si et seulement si $PGCD(a,n) = 1$*

Démonstration. $PGCD(a,n) = 1$ ssi il existe $s, t \in \mathbb{Z}$ tel que $as + nt = 1$, c'est à dire $as \equiv 1 \mod n$. □

Exemple : Calculer l'inverse de 2 modulo 7.
On a $2.4 - 7.1 = 1$ soit $2.4 \equiv 1 \mod 7$. Donc $2^{-1} \mod 7 \equiv 4 \mod 7$.
En pratique, pour calculer l'inverse d'un élément, on utilise l'algorithme d'Euclide étendu.

Théorème 3.2.2. *Soit $a, n, z, z' \in \mathbb{Z}, n > 0$. Si $PGCD(a, n) = 1$ alors*

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n$$

et si $PGCD(a, n) = d$ alors

$$az \equiv az' \mod n \Leftrightarrow z \equiv z' \mod n/d$$

Démonstration. Si $PGCD(a, n) = 1$ et a' est l'inverse de $a \mod n$, alors $az \equiv az' \mod n$ et en multipliant par a', on obtient $a'az \equiv a'az' \mod n$ et donc $z \equiv z' \mod n$.
Si $z \equiv z' \mod n$, alors $az \equiv az' \mod n$.
Supposons que $PGCD(a, n) = d$. Alors par définition des congruences $az \equiv az' \mod n$ si et seulement si $(a/d)z \equiv (a/d)z' \mod n/d$ si et seulement si $z \equiv z' \mod n/d$. □

Exemples :
a) $5.2 \equiv 5.(-4) \mod 6$.
On peut simplifier par 5 des deux cotés car $PGCD(5, 6) = 1$. On obtient $2 \equiv -4 \mod 6$.
b) $3.5 \equiv 3.3 \mod 6$.
On ne peut pas simplifier par 3 car $PGCD(3, 6) \neq 1$, mais on peut écrire $5 \equiv 3 \mod 2$.

Théorème 3.2.3. *Soit $a, b, n \in \mathbb{Z}, n > 0$ et $PGCD(a, n) = d$. Si $d|b$, $az \equiv b \mod n$ admet une solution z et tout z' est aussi solution si et seulement si $z \equiv z' \mod n/d$. Si $d \nmid b$, la congruence n'admet pas de solution.*

Exercices : Résoudre les équations suivantes
$2z \equiv 3 \mod 15$,
$3z \equiv 4 \mod 15$,
$3z \equiv 12 \mod 15$.

Théorème 3.2.4. *Soit $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ et des entiers arbitraires $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Si les entiers $n_1, n_2, \ldots, n_k$ sont deux à deux premiers entre eux, alors le système :*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \quad \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

a une solution unique modulo $n = n_1 n_2 \ldots n_k$.

Algorithme de Gauss. La solution x du système précédent peut s'écrire :

$$x = \sum_{i=1}^{k} a_i N_i M_i \mod n$$

avec $N_i = n/n_i$, $M_i = N_i^{-1} \mod n_i$.
Exemple. La solution unique du système :

$$\begin{cases} x \equiv 3 \mod 7 \\ x \equiv 7 \mod 13 \end{cases}$$

est $x \equiv 59 \mod 91$.
Proposition. Si pgcd$(n_1, n_2) = 1$, le système :

$$x \equiv a \pmod{n_1},\ x \equiv a \pmod{n_2}$$

admet l'unique solution $x \equiv a \pmod{n_1 n_2}$.
Remarque : Le logiciel magma permet de calculer de tels systèmes. Voir $http : //magma.maths.edu.au/calc/$ et taper l'exemple précédent : $CRT([3, 7], [7, 13])$;.

3.3 Classes résiduelles

Soit n un entier positif. La relation binaire $\equiv \pmod n$ est une relation d'équivalence. La **classe d'équivalence** de $a \in \mathbb{Z}$ est l'ensemble des entiers congrus à a modulo n. Notons-la $[a]_n$.

$$[a]_n = \{a + nz \ : z \in \mathbb{Z}\} = a + n\mathbb{Z}.$$

Les classes d'équivalence sont disjointes et forment une partition de $\mathbb{Z}$ en n sous-ensembles. Si $a = qn + r$, $0 \leq r < n$, alors $a \equiv r \pmod n$, r est son **résidu** modulo n, $[a]_n = [r]_n$. Ce résidu est utilisé pour représenter la classe d'équivalence $[a]_n$ de a.
On a $[1]_n = [1 + n]_n$.

Définition. L'ensemble des **entiers modulo n**, noté $\mathbb{Z}_n$ ou $\mathbb{Z}/n\mathbb{Z}$, est l'ensemble des n classes d'équivalence

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}.$$

L'addition et la multiplication respectant l'équivalence (donc aussi la soustraction, la division et l'exponentiation), elles induisent des opérations sur $\mathbb{Z}_n$: la somme des classes de a et b est la classe de $a + b$, leur produit est la classe de ab :
$[a]_n + [b]_n = [a + b]_n$,
$[a]_n[b]_n = [ab]_n$.
De plus,
$-[a]_n = [-1]_n.[a]_n = [-a]_n$
et
$[a]_n - [b]_n = [a]_n + (-[b]_n) = [a - b]_n$.
Exemple : Les quatre classes modulo 4 sont
$[0]_n = \{\ldots, -4, 0, 4, 8, \ldots\}$
$[1]_n = \{\ldots, -3, 1, 5, 9, \ldots\}$
$[2]_n = \{\ldots, -2, 2, 6, 10, \ldots\}$
$[3]_n = \{\ldots, -1, 3, 7, 11, \ldots\}$
On a par exemple $[1]_n + [3]_n = [0]_n$, $[2]_n.[2]_n = [0]_n$, $[2]_n.[3]_n = [2]_n$.

Définitions. Soit $[a]_n \in \mathbb{Z}_n$. L'**inverse** de $[a]_n$ est, s'il existe, $[x]_n \in \mathbb{Z}_n$ tel que $[ax]_n = [1]_n$. Il est unique, noté $[a]_n^{-1}$, et $[a]_n$ est dit **inversible**. La **division** de $[a]_n$ par $[b]_n \in \mathbb{Z}_n$, si $[b]_n$ est inversible, est égale à $[a]_n \left([b]_n\right)^{-1}$.

Proposition 3.3.1. *$[a]_n \in \mathbb{Z}_n$ est inversible* $\iff PGCD(a, n) = 1$.

Démonstration. D'après le théorème de Bézout, il existe des entiers x et y tels que $ax + ny = 1$, d'où : $[a]_n[x]_n = [1]_n$, $[x]_n = ([a]_n)^{-1}$. □

Exemple. Les éléments inversibles de $\mathbb{Z}_9$ sont les classes de $1, 2, 4, 5, 7$ et 8. Ainsi $\left([4]_9\right)^{-1} = [7]_9$ car $7 \,.\, 4 = 3 \,.\, 9 + 1$.

On a vu qu'on pouvait faire des additions et des multiplications dans $\mathbb{Z}_n$. En fait $(\mathbb{Z}_n, +, .)$ est une structure algébrique avec les propriétés suivantes : pour tout $\alpha, \beta, \gamma \in \mathbb{Z}_n$
$\alpha + \beta = \beta + \alpha$ (commutativité de $+$)
$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (associativité de $+$)
$\alpha + [0]_n = \alpha$ (neutre pour $+$)
$\alpha - \alpha = [0]_n$ (α est l'inverse additif de lui-même) $\alpha.\beta = \beta.\alpha$ (commutativité de .)
$(\alpha.\beta).\gamma = \alpha.(\beta.\gamma)$ (associativité de .)
$\alpha.(\beta + \gamma) = \alpha\beta + \alpha.\gamma$ (distributivité de .)
$\alpha.[1]_n = \alpha$ (existence du neutre de .)
Cette structure est appelée un **anneau commutatif**, sera développée plus tard.
Remarque : Dans $\mathbb{Z}_n$, tous les éléments ont un inverse additif mais pas forcément d'inverse multiplicatif.

Si un élément possède un inverse multiplicatif, celui-ci est unique.

Définitions. $\mathbb{Z}_n^*$ est l'ensemble des classes qui admettent un inverse multiplicatif.
Exemple. $\mathbb{Z}_6^* = \{[1]_6, [5]_6\}$

Soit $\alpha \in \mathbb{Z}_n^*$ et $k > 0$, alors $\alpha^k = \alpha \dots \alpha$ (k fois), $\alpha^0 = [1]_n$.

Remarque : Il est équivalent de travailler avec les congruences modulaires ou avec la structure algébrique $\mathbb{Z}_n$.
Par abus de notation, on écrit quelquefois pour simplifier :
$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ au lieu de
$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}$.

3.4 Exercices

1. Déterminer tous les entiers premiers inférieurs à 30 qui sont congrus à $3 \mod 4$.
2. Soit n un entier positif. Soit C_n le nombre de paires d'entiers (a, b) tel que $1 \leq a \leq n$, $1 \leq b \leq n$, et PGCD$(a, b) = 1$. Soit F_n le nombre de nombres rationnels *distincts* a/b, où $0 \leq a < b \leq n$.
   (a) Calculez F_i et C_i pour $i \leq 6$.
   (b) Montrez que $F_n = (C_n + 1)/2$.
3. Résoudre l'équation $65x \equiv 1 \mod 101$ en utilisant l'algorithme d'Euclide étendu.
4. Une bande de 17 pirates s'est emparée d'un butin composé de pièces d'or d'égale valeur. Ils décident de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci reçoit alors 3 pièces. Mais les pirates se querellent, et 6 d'entre eux sont tués. Après un nouveau partage du même butin, le cuisinier reçoit 4 pièces. Dans un naufrage ultérieur, seuls le butin, 6 pirates et le cuisinier sont sauvés, et le partage donne alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner les derniers pirates ?
5. Calculer dans $\mathbb{Z}_7$: $[2]_7 + [6]_7$, $[2]_7.[5]_7$
6. Déterminer x et y tel que $5x + 17y = 1$.
7. Déterminer Z_{14}^* et Z_{15}^*.
8. Quel est le dernier chiffre de $(257!)$?

1. Résoudre l'équation $2x \equiv 2y \mod 8$.
2. Résoudre $5x \equiv 20 \mod 25$ puis $4x \equiv 3 \mod 29$
3. Algorithme d'Euclide étendu :
   Calculer $11^{-1} \mod 26$, $18^{-1} \mod 35$, $7^{-1} \mod 33$, $7^{-1} \mod 26$, résoudre $7x = 1 \mod 35$.
4. Calculer x tel que $\begin{cases} x = & 12 \mod 21 \\ x = & 4 \mod 5 \\ x = & 6 \mod 22 \end{cases}$
5. Calculer x tel que $\begin{cases} x = & 12 \mod 18 \\ x = & 5 \mod 12 \end{cases}$

Chapitre 4

Propriétés des entiers modulaires

4.1 Fonction d'Euler

La fonction **indicatrice d'Euler**[1] fait correspondre à un entier positif n le nombre $\Phi(n)$ des entiers compris entre 1 et $n-1$ premiers avec n. On pose $\Phi(1)=1$.

- Si p est premier, $\Phi(p)=p-1$ et, si $n\geq 1$, $\Phi(p^n)=(p-1)\,p^{n-1}$.
- Si m et n sont premiers entre eux, $\Phi(mn)=\Phi(m)\,\Phi(n)$.
- Si les p_i sont les facteurs premiers de n, $\Phi(n)=n\prod_{i=1}^{k}(1-1/p_i)$.

Pour démontrer les deux premières propriétés, il suffit de dénombrer les entiers non premiers avec p^n ou mn et soustraire ce nombre à p^n-1 ou à $mn-1$.
Pour démontrer la troisième, on écrit :

$$\begin{aligned} n\prod_{i=1}^{k}(1-p_i^{-1}) &= p_1^{n_1}\dots p_k^{n_k}\,(1-p_1^{-1})\dots(1-p_k^{-1}) \\ &= p_1^{n_1}\,(1-p_1^{-1})\dots p_k^{n_k}\,(1-p_k^{-1}) \\ &= (p_1^{n_1}-p_1^{n_1-1})\dots(p_k^{n_k}-p_k^{n_k-1}) \\ &= \Phi(p_1^{n_1})\dots\Phi(p_k^{n_k}) \\ &= \Phi(n)\,. \end{aligned}$$

Si p est premier, $k\geq 1$ et $n\geq 1$, on a :

$$\begin{aligned} \Phi(p^k) &= p^{k-1}\,\Phi(p)\,, \\ &= p^k-p^{k-1} \\ \Phi(p\,n) &= p\,\Phi(n) \qquad \text{si } p|n\,, \\ &= (p-1)\,\Phi(n) \quad \text{sinon} \end{aligned}$$

et si $\prod_{i=1}^{k}p_i^{d_i}$ est la décomposition en facteurs premiers de n, on a :

$$\Phi(n)=\prod_{i=1}^{k}p_i^{d_i-1}\,\Phi(p_i)\,.$$

Ainsi, $4725=3^3.5^2.7$, et :

$$\begin{aligned} \Phi(4725) &= (3^2.\Phi(3)).(5.\Phi(5)).\Phi(7) \\ &= (9.2).(5.4).6 \\ &= 2160\,. \end{aligned}$$

[1] Leonhard Euler (1707-1783), immense mathématicien suisse.

Exemple. $\Phi(60) = 60.(1-1/2).(1-1/3).(1-1/5) = 16.$

Théorème 4.1.1. *Quel que soit $n \geq 1$ on a :*

$$n = \sum_{d|n} \Phi(d)\,.$$

Démonstration. Cela est trivial si $n = 1$ ou est premier. Supposons la propriété vraie pour un produit n de k puissances de nombres premiers (égaux ou différents) et prouvons-la pour le nombre $p\,n$, p étant premier quelconque, pour passer à $k+1$. Si p ne divise pas n, il ne divise aucun des d, les diviseurs de $p\,n$ sont les diviseurs d_i de n et les produits $p\,d_i$ et on a :

$$\begin{aligned} \sum_{d|p\,n} \Phi(d) &= \sum_{d|n} \Phi(d) + (p-1)\sum_{d|n} \Phi(d) \\ &= p\,n \end{aligned}$$

ce qui achève la récurrence dans ce cas.

Si $p|n$, $n = p^h q$ avec $(p,q) = 1$, et, d'après l'hypothèse de récurrence, et ce qui précède :

$$p^h q = \sum_{d|p^h q} \Phi(d)\,.$$

Quand on passe de $p^h q$ à $p^{h+1} q$ les diviseurs que l'on rajoute sont de la forme $p^{h+1} d$, $d|q$. On a donc :

$$\sum_{d|p\,n} \Phi(d) = \sum_{d|n} \Phi(d) + \sum_{d|q} \Phi(p^{h+1}\,d)$$

puis :

$$\begin{aligned} \Phi(p\,d) &= (p-1)\Phi(d) \\ \Phi(p^{h+1}\,d) &= p^h(p-1)\Phi(d) \end{aligned}$$

et enfin

$$\begin{aligned} \sum_{d|p\,n} \Phi(d) &= p^h q + p^h(p-1)\Phi(d) \\ &= p^{h+1}\,d \\ &= p\,n \end{aligned}$$

ce qui achève la récurrence dans ce dernier cas. □

4.2 Théorème d'Euler et petit théorème de Fermat

Soit $\alpha \in \mathbb{Z}_n^*$. On considère les puissances successives de α : $\alpha^0, \alpha^1, \alpha^2, \ldots$. Tous ces éléments appartiennent à $\mathbb{Z}_n^*$ et comme $\mathbb{Z}_n^*$ est fini, il existe des entiers $k, i > 0$ tels que

$$\alpha^k \equiv \alpha^i \mod n$$

soit $\alpha^{k-i} \equiv 1 \mod n$.

L'ordre multiplicatif de α est le plus petit entier positif t tel que $\alpha^t \equiv 1 \mod n$.

Exemple. $n = 7$

i		1	2	3	4	5	6
1^i	mod 7	1	1	1	1	1	1
2^i	mod 7	2	4	1	2	4	1
3^i	mod 7	3	2	6	4	5	1
4^i	mod 7	4	2	1	4	2	1
5^i	mod 7	5	4	6	2	3	1
6^i	mod 7	6	1	6	1	6	1

Ainsi 3 et 5 sont d'ordre 6, 2 et 4 sont d'ordre 3, 6 est d'ordre 2 et 1 est d'ordre 1. On remarque que tous les ordres des éléments divisent 6 qui est le nombre d'éléments dans $\mathbb{Z}_7^* = \Phi(7)$.

Théorème 4.2.1 (d'Euler)**.** *Si $n \geq 2$ et $a \in \mathbb{Z}_n^*$, alors $a^{\Phi(n)} \equiv 1 \pmod{n}$.*

Démonstration. Soit $\alpha \in \mathbb{Z}_n^*$. Considérons l'application f :
$\mathbb{Z}_n^* \to \mathbb{Z}_n^*$
$\beta \mapsto \alpha\beta$
La fonction f est injective de $\mathbb{Z}_n^*$ dans $\mathbb{Z}_n^*$ car si $\alpha\beta = \alpha\beta'$, on a $\alpha = \beta'$. $\mathbb{Z}_n^*$ étant un ensemble fini, f est aussi surjective et donc bijective. Ainsi, lorsque β parcourt $\mathbb{Z}_n^*$, $\alpha\beta$ parcourt $\mathbb{Z}_n^*$. On a

$$\prod_{\beta \in \mathbb{Z}_n^*} \beta = \prod_{\beta \in \mathbb{Z}_n^*} (\alpha\beta) = \alpha^{\Phi(n)} (\prod_{\beta \in \mathbb{Z}_n^*} \beta).$$

En simplifiant, on obtient

$$\alpha^{\Phi(n)} = [1]_n$$

donc $\alpha^{\Phi(n)} = 1 \mod n$. □

Théorème 4.2.2 (Petit théorème de Fermat[2])**.** *Soit p un nombre premier. Quel que soit a premier avec p, c'est-à-dire non multiple de p, on a : $a^{p-1} \equiv 1 \mod p$.*

Le petit théorème de Fermat est un cas particulier du théorème d'Euler.

Corollaire : Dans $\mathbb{F}_p$, on travaille modulo $p-1$ sur les exposants. ▽

Théorème 4.2.3. *Quel que soit a, $a^p \equiv a \mod p$.*

Soit $n \in \mathbb{Z}^+, a \in \mathbb{Z}$, $PGCD(a,n) = 1$, a est un élément **primitif** modulo n si l'ordre multiplicatif de $a \mod n$ est $\Phi(n)$.
Les seuls entiers positifs n pour qui il existe une racine primitive sont

$$n = 1, 2, 4p^e, 2p^e, \quad p \text{ premier }, e \geq 1.$$

Exercices
Déterminer les ordres des éléments de $\mathbb{Z}_{21}^*$. Idem avec $\mathbb{Z}_{14}^*$.
Calculer $8^{11} \mod 11, 5^8 \mod 7, 7^8 \mod 30$.

4.3 Application du théorème d'Euler : le cryptosystème RSA

Le théorème d'Euler est utilisé dans le chiffrement RSA (1977). Bob souhaite chiffrer un message pour Alice. Alice choisit des paramètres entiers premiers p et q et pose $n = pq$. Notons que connaissant p et q, il est facile de calculer n mais si n est grand, il est difficile de retrouver p et q à partir de n. Il n'existe en effet pas d'algorithme rapide de factorisation.
Alice choisit alors un entier $d < n$ puis calcule e tel que $ed \equiv 1 \mod \Phi(n)$. Ces deux valeurs s'appellent des clés. La première clé est privée (d) et la seconde (e) est publique. Connaissant e il est facile de calculer d si on connaît $\Phi(n)$ en utilisant l'algorithme d'Euclide étendu. Mais si on ne connaît pas $\Phi(n)$, le calcul de d est difficile. Or si n est suffisamment grand, le calcul de $\Phi(n)$ est un problème difficile lorsqu'on ne connaît pas la factorisation de n.
Alice rend publique n, e. Pour chiffrer un message $m < n$ (le message est codé en un nombre inférieur à n), Bob utilise la clé publique e, calcule $c = m^e \mod n$ et envoie la valeur à Alice. Alice reçoit c et retrouve la valeur du message m en utilisant la clé privée d. Elle calcule $c^d \mod n = (m^e)^d \mod n = m^{e.d \mod \Phi(n)} \mod n = m$. Bien sur, il faut que $PGCD(m,n) = 1$ pour pouvoir réduire les exposants modulo $\Phi(n)$.
Application numérique
Alice choisit $p = 3, q = 11, d = 7$. Calculer la clé publique. Si $m = 15$, qu'elle est la valeur de c ? Comment Bob va-t-il déchiffrer ?
La pratique : Dans la pratique, les paramètres sont à choisir avec précaution. Par exemple, p et q doivent être très grands (supérieurs à 1024 bits) et pour obtenir une sécurité satisfaisante, le cryptosystème ne peut pas être utilisé en l'état car il est déterministe (pour plus de détail, voir http ://www.rsa.com/rsalabs/).

[2]Pierre de Fermat (1601-1665), mathématicien français.

4.4 Résidus quadratiques

Soit $a \in \mathbb{Z}_n^*$; a est un **résidu quadratique** modulo n, ou un **carré** modulo n, s'il existe $x \in \mathbb{Z}_n^*$ tel que $x^2 = a$ ($x^2 \equiv a \pmod{n}$). Si un tel x n'existe pas, a est un **non-résidu quadratique** modulo n.
L'ensemble de tous les résidus quadratiques modulo n est noté Q_n et celui des non-résidus quadratiques, $\overline{Q}_n$.
Par définition $0 \notin \mathbb{Z}_n^*$, et donc $0 \notin Q_n$ et $0 \notin \overline{Q}_n$.

Proposition 4.4.1. *Soient $p > 2$ un nombre premier et a un élément primitif de $\mathbb{Z}_p^*$ (c.a.d d'ordre $p-1$). Alors $b \in \mathbb{F}_p$ est un résidu quadratique modulo p s'il existe un entier pair i tel que : $b = a^i$ ($b \equiv a^i \pmod{p}$). Il s'ensuit que :*

$$|Q_p| = |\overline{Q}_p| = \frac{p-1}{2}\,.$$

La moitié des éléments sont des résidus et l'autre moitié des non-résidus.

Démonstration. Un élément primitif a ne peut être un carré. On a en effet $a^{p-1} = 1$ et $a^{(p-1)/2} = -1$. S'il existait b tel que $b^2 = a$, on aurait $b^{p-1} = -1$ et $b^p = -b$, ce qui est absurde. les a^{2k} sont évidemment des carrés. Si un a^{2k+1} était un carré, $a^{2k+1} = c^2$, on aurait $a = c^2/a^2 = (c/a)^2$ et a serait un carré. Les résidus quadratiques sont donc les a^{2k} de $k = 0$ à $k = (p-3)/2$. Pour $k = (p-1)/2$, $a^{2k} = 1 = a^0$. Il y en a donc $(p-1)/2$. Les non-résidus quadratiques sont les a^i avec $i = 1, 3, \ldots, p-2$. Il y en a donc $(p-1)/2$. □

Critère d'Euler : x est un résidu quadratique modulo p, premier, ssi :

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p}\,.$$

Exemple. 6 est un élément primitif de $\mathbb{Z}_{13}^*$. Les puissances de 6 sont :

i	0	1	2	3	4	5	6	7	8	9	10	11
6^i	1	6	10	8	9	2	12	7	3	5	4	11

Les résidus quadratiques sont les 6^{2i}. Ainsi $Q_{13} = \{1, 3, 4, 9, 10, 12\}$ et $\overline{Q}_{13} = \{2, 5, 6, 7, 8, 11\}$.

Proposition 4.4.2. *Soit $n = p\,q$, p et q étant premiers distincts. Alors $a \in \mathbb{Z}_n$ est un résidu quadratique modulo n ssi la classe de a modulo p appartient à Q_p et celle de a modulo q à Q_q.*

Démonstration. Si $a \in Q_n$, $a = b^2$ et dans $\mathbb{Z}$ $a = b^2 + kp\,q$. On a donc $a \equiv b^2$ modulo p et modulo q. Réciproquement, si $a \equiv b^2 \pmod{p}$, $a = b^2 + hp$, et si $a \equiv b^2 \pmod{q}$, $a = b^2 + kq$, ce qui impose que $hp = kq$, donc que $q|h$, $h = rq$, $a = b^2 + rp\,q$, et enfin que $a \equiv b^2 \pmod{p\,q}$. □

Proposition 4.4.3. *Dans la situation précédente on a :*

$$\begin{aligned} |Q_n| &= |Q_p|.|Q_q| \\ &= \frac{(p-1)(q-1)}{4} \\ |\overline{Q}_n| &= 3\,\frac{(p-1)(q-1)}{4}\,. \end{aligned}$$

Démonstration. C'est une conséquence immédiate de la proposition précédente. □

Exemple. $Q_{21} = \{1, 4, 16\}$, $\overline{Q}_{21} = \{2, 5, 8, 10, 11, 13, 17, 19, 20\}$.

Définition. Soit $a \in Q_n$. Si $x \in \mathbb{Z}_n^*$ est tel que $x^2 = a$ ($x^2 \equiv a \pmod{n}$), alors x est une **racine carrée** de a modulo n.

Théorème 4.4.1. *Nombre de racines carrées :*

(a) Si $p > 2$ est premier, $a \in Q_p$ a exactement deux racines modulo p.

(b) Si $n = p\,q$, p et q premiers, impairs, distincts, alors, si $a \in Q_n$, a possède exactement 4 racines carrées distinctes modulo n.

Démonstration. Remarquons d'abord que si x est une racine de a dans $\mathbb{Z}_n$, x modulo p est une racine de a modulo p, et de même pour q.
(a) Si $a = x^2 = y^2$ dans $\mathbb{F}_p$, avec $y \neq x$, on a : $x^2 - y^2 = 0$, $(x - y)\,(x + y) = 0$, et, comme on est dans un corps, $x + y = 0$ et $y = -x$. Il ya deux racines.
(b) Si $n = p\,q$, on résoud modulo p : $y^2 \equiv a \pmod{p}$, puis modulo q : $z^2 \equiv a \pmod{q}$. La solution doit s'écrire : $x = y + hp = z + kq$, d'où : $hp - kq = z - y$. Soit u et v tels que $up - vq = 1$. Chacun des 4 couples (y, z) donne une valeur $t = z - y$, d'où $h = tu$, $k = tv$, et enfin x. Ces valeurs sont distinctes, car $t = t'$ équivaut à $z - z' = y - y'$, or $z - z' = \lambda q$, $y - y' = \mu p$, et donc λ est multiple de p, de sorte que $y - y'$ et $z - z'$ sont nuls (dans $\mathbb{Z}_n$) et que $y = y'$ et $z = z'$. □

Exemple. Cherchons les racines carrées de 16 dans $\mathbb{Z}_{65}$. Comme $65 = 5.13$, commençons par $p = 5$. Les solutions sont ± 1 car $16 \equiv 1 \pmod{5}$. Pour $q = 13$, $16 \equiv 3 \pmod{13}$ et nous avons les solutions ± 4. L'identité de Bézout s'écrit : $-5.5 - (-2).13 = 1$, soit $u = -5$ et $v = -2$. Voici les solutions en fonction de (y, z) :

$$\begin{cases} (y,z) = (1,4) \quad \Rightarrow t = 3 \Rightarrow h = -15,\ x = 1 - 15.5 \mod 65 = -9\,, \\ (y,z) = (-1,4) \Rightarrow t = 5 \Rightarrow h = -25,\ x = -1 - 25.5 \mod 65 = 4\,, \end{cases}$$

et, en changeant les signes : $(-1, -4)$ donne $x = 9$, et $(1, -4)$ donne $x = -4$. ▽

4.5 Symbole de Legendre

Le **symbole de Legendre** rend compte si un entier a est un résidu quadratique modulo un premier p ou non.

Définition. Soit $p > 2$ un premier. Le symbole de Legendre $(\frac{a}{p})$ est ainsi défini :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ si } p|a\,, \\ 1 \text{ si } a \in Q_p\,, \\ -1 \text{ si } a \in \overline{Q}_p\,. \end{cases}$$

Ainsi, l'entier a est un résidu quadratique modulo p si et seulement si le symbole de Legendre est égal à 1.
Propriétés du symbole de Legendre. Soit p un premier impair, et $a, b \in \mathbb{Z}$.

(a) $(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod{p}$. En particulier, $(\frac{1}{p}) = 1$ et $(\frac{-1}{p}) = (-1)^{(p-1)/2}$. Ainsi, $-1 \in Q_p$ si $p \equiv 1 \pmod{4}$ et $-1 \in \overline{Q}_p$ si $p \equiv 3 \pmod{4}$.

(b) $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$. Donc, si $a \in \mathbb{Z}_n$, $a \neq 0$, alors $(\frac{a^2}{p}) = 1$.

(c) $a \equiv b \pmod{p} \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$.

(d) $(\frac{2}{p}) = (-1)^{(p^2-1)/8}$. Donc, $(\frac{2}{p}) = 1$ si $p \equiv \pm 1 \pmod{8}$ et $(\frac{2}{p}) = -1$ si $p \equiv \pm 3 \pmod{8}$.

(e) Loi de réciprocité quadratique : si $q \neq p$ est premier impair, alors :

$$(\frac{p}{q}) = (-1)^{\frac{(p-1)(q-1)}{4}}\ (\frac{q}{p})\,.$$

En d'autres termes, $(\frac{p}{q}) = (\frac{q}{p})$ sauf si p et q sont congrus à 3 modulo 4, auquel cas, $(\frac{p}{q}) = -(\frac{q}{p})$.

4.6 Symbole de Jacobi

Le **symbole de Jacobi** est une généralisation du symbole de Legendre à des entiers n impairs premiers ou non.

Soit $n \geq 3$ un entier impair dont la factorisation en puissances de premiers est :

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} .$$

Alors le symbole de Jacobi est ainsi défini :

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \dots \left(\frac{a}{p_k}\right)^{e_k}$$

de sorte que si n est premier on retrouve le symbole de Legendre.

Propriétés du symbole de Jacobi. Soient $n \geq 3$, $m \geq 3$ et $a, b \in \mathbb{Z}$. Alors le symbole de Jacobi a les propriétés suivantes :

(a) $(\frac{a}{n}) = 0, 1$ ou -1. De plus, $(\frac{a}{n}) = 0$ ssi $d(a, n) \neq 1$.

(b) $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$. Si $a \in \mathbb{Z}_n$, $a \neq 0$, alors $(\frac{a^2}{n}) = 1$.

(c) $(\frac{a}{mn}) = (\frac{a}{m})(\frac{a}{n})$.

(d) $a \equiv b \pmod{n} \Rightarrow (\frac{a}{n}) = (\frac{b}{n})$.

(e) $(\frac{1}{n}) = 1$.

(f) $(\frac{-1}{n}) = (-1)(n-1)/2$. Donc, $(\frac{-1}{n}) = 1$ si $n \equiv 1 \pmod 4$, et $(\frac{-1}{n}) = -1$ si $n \equiv 3 \pmod 4$.

(g) $(\frac{2}{n}) = (-1)^{(n^2-1)/8}$. Donc $(\frac{2}{n}) = 1$ si $n \equiv \pm 1 \pmod 8$ et $(\frac{2}{n}) = -1$ si $n \equiv \pm 3 \pmod 8$.

(h) $(\frac{n}{m}) = (\frac{m}{n})(-1)^{\frac{(n-1)(m-1)}{4}}$. En d'autres termes, $(\frac{n}{m}) = (\frac{m}{n})$ sauf si m et n sont congrus à 3 modulo 4, auquel cas $(\frac{n}{m}) = -(\frac{m}{n})$.

Il découle de ces propriétés que si $a = 2^e a_1$, c impair, on a :

$$(\frac{a}{n}) = (\frac{2^e}{n})(\frac{a_1}{n}) = (\frac{2}{n})^e (\frac{n \bmod a_1}{a_1})^{\frac{(n-1)(m-1)}{4}} .$$

Cette remarque mène à l'algorithme récursif suivant pour le calcul de $(\frac{a}{n})$ qui ne nécessite pas la factorisation de n en puissances de premiers.

Algorithme de calcul du symbole de Jacobi (ou de Legendre).

JACOBI(a, n)
Entrée : les entiers $n \geq 3$, impair, et a, $0 \leq a < n$.
Sortie : $(\frac{a}{n})$.
si $a = 0$ Retourner 0.
si $a = 1$ Retourner 1.
Ecrire $a = 2^e a_1$ avec a_1 impair.
si e est pair **alors** $s \leftarrow 1$.
sinon
  si $n \equiv \pm 1 \pmod 8$ **alors** $s \leftarrow 1$
  si $n \equiv \pm 3 \pmod 8$ **alors** $s \leftarrow -1$
si $n \equiv 3 \pmod 4$ et $a_1 \equiv 3 \pmod 4$ **alors** $s \leftarrow -s$.
$n_1 \leftarrow n \pmod{a}_1$.
si $a_1 = 1$ sort s.
sinon Retourner $s \,.\, JACOBI(n_1, a_1)$.

La complexité de cet algorithme est $O((\lg n)^2)$.

Remarque. Soit p un premier impair. On sait que la moitié des éléments de $\mathbb{Z}_n^*$ sont des résidus quadratiques ($|Q_p| = |\overline{Q}_p|$), mais on ne dispose pas d'algorithme en temps polynomial pour en trouver un. On peut en fait, pour obtenir un non-résidu, choisir un $a \in [1, p-1]$ tel que $(\frac{a}{p}) = (-1)$. Le nombre d'itérations est 2, et la procédure nécessite donc un temps polynomial.

Exemple. Pour $a = 134$ et $n = 215$ l'algorithme précédent calcule :

$$\begin{aligned}
\Big(\frac{134}{215}\Big) &= \Big(\frac{2}{215}\Big)\Big(\frac{67}{215}\Big) \\
&= (+1)\Big(\frac{215}{67}\Big)(-1)^{214\,.\,66/4} \\
&= (-1)\Big(\frac{14}{67}\Big) \\
&= (-1)\Big(\frac{2}{67}\Big)\Big(\frac{7}{67}\Big) \\
&= \Big(\frac{4}{7}\Big)(-1) \\
&= -1\,.
\end{aligned}$$

Contrairement au symbole de Legendre, le symbole de Jacobi ne dit pas si un nombre est résidu quadratique modulo n (non premier). Il est vrai que si a est un résidu quadratique $(\frac{a}{n}) = 1$, mais la réciproque est fausse.

Exemple. La table suivante liste les a tels que $a \in \mathbb{Z}_{21}$, $PGCD(a, 21) = 1$, et leur symbole de Jacobi. Souvenons-nous que $Q_{21} = \{1, 4, 16\}$ et remarquons que $(\frac{5}{21}) = 1$ bien que $5 \notin Q_{21}$. De même pour 17 et 20.

a	1	2	4	5	8	10	11	13	16	17	19	20
$a^2 \bmod n$	1	4	16	4	1	16	16	1	4	16	4	1
$(\frac{a}{3})$	1	-1	1	-1	-1	1	-1	1	1	-1	1	-1
$(\frac{a}{7})$	1	1	1	-1	1	-1	1	-1	1	-1	-1	-1
$(\frac{a}{21})$	1	-1	1	1	-1	-1	-1	-1	1	1	-1	1

Définition. Soient $n = p\,q$ (p et q premiers impairs), $a \in \mathbb{Z}_n$. On pose $J_n = \{a \in \mathbb{Z}_n^* \,|\, (\frac{a}{n}) = 1\}$. Si $a \in J_n$, on peut avoir $(\frac{a}{p}) = (\frac{a}{q}) = -1$, et $a \notin \mathbb{Q}_n$. De tels éléments sont des **pseudo-racines-carrées**. Leur ensemble est noté $\widetilde{Q}_n$. Il est égal à $J_n \setminus Q_n$. la moitié des éléments de J_n sont des résidus quadratiques et l'autre moitié sont des pseudo-racines-carrées. On a donc :

$$|Q_n| = \frac{(p-1)(q-1)}{4}\,,\ |\overline{Q}_n| = 3\,|Q_n|\,, |J_n| = 2\,|Q_n|\,,\ |\widetilde{Q}_n| = |Q_n|\,.$$

4.7 Exercices

1. Calculer $51 * 25 \mod 91$, $25^{71} \mod 91$.
2. Calculer $\phi(85),\ \phi(1024),\ \phi(759), \phi(105),\ \phi(1155),\ \phi(48)$.
3. Soit n le produit de deux entiers premiers et $\phi(n)$ la fonction indicatrice d'Euler de n. Connaissant n et $\phi(n)$, comment peut-on faire pour factoriser n (c'est à dire trouver p et q tel que $n = pq$) ?
4. Soit p premier, a est un résidu quadratique modulo p (RQ) si $a < p$ et si $x^2 = a \mod p$ pour un certain x. Calculer tous les RQ modulo 7 puis modulo 23.
5. Combien l'entier 2 admet-il de racines carrées modulo 23 ? Combien l'entier 4 admet-il de racines carrées modulo 1155 ?
6. Le symbole de Legendre $L(a, p),\ p > 2$ est défini comme suit
   $L(a, p) = 0$ si a est divisible par p ; $L(a, p) = 1$ si a est un RQ modulo p ; $L(a, p) = -1$ si a n'est pas un RQ modulo p
   L'entier 2 est-il un RQ modulo 101 ? Calculer $L(4, 7),\ L(18, 23),\ L(3, 11),\ L(4, 101),\ L(97, 101)$.
7. Calculer $8^{11} \mod 11,\ 7^{11} \mod 11,\ 5^8 \mod 7,\ 14^{16} \mod 17,\ 67^{258} \mod 68,\ 3^{45} \mod 5,\ 7^{31} \mod 11,\ 4^{25} \mod 35,\ 7^8 \mod 30$.
8. Attaque sur RSA : Théorème du reste chinois :
   Stephane doit envoyer le même message M à Alice, Claire et Corinne dont les clés publiques sont respectivement $(n_1 = 26, e = 7),\ (n_2 = 35, e = 7),\ (n_3 = 33, e = 7)$, (où n_i sont les modules RSA).
   Stephane envoie les valeurs $C_1 = 24,\ C_2 = 23,\ C_3 = 29$.
   Comment Estelle va-t-elle procéder pour retrouver M après avoir intercepté les trois valeurs et les clés publiques ?
9. Soit $g < p$, p premier. 2 est-il un élément primitif modulo 11 ? 3 est-il un élément primitif modulo 11 ?
   Soit Z_5 l'ensemble des entiers modulo 5, $Z_5 = \{0, 1, 2, 3, 4\}$. Montrer que Z_5 peut s'écrire sous la forme $Z_5 = \{0\} \cup \{g^0, g^1, g^2, g^3\}$.

Chapitre 5

Structures algébriques

Une structure algébrique est un ensemble muni d'une ou plusieurs opérations. Certaines structures se rencontrent fréquemment dans notre environnement. Par exemple, l'ensemble des nombres entiers muni de $+$ ou l'ensemble des nombres réels muni de $+$ et . forme une structure qui admet certaines propriétés (associativité, commutativité, inversibilité, distributivité, etc).
Nous allons nous intéresser aux trois structures mathématiques les plus importantes : les structures de groupe, d'anneau et de corps. Chaque structure admet des propriétés qui induisent des méthodes de calcul spécifiques.

5.1 Groupes

Un ensemble G muni d'une opération $*$ associative possédant un élément e, dit **neutre** ($\forall g \in G\ e * g = g * e = g$) tel que, quel que soit $g \in G$, il existe un élément y de G vérifiant : $x * y = e$ est un **groupe**. L'élément y est l'**inverse** de x, et il est noté x^{-1}. Ceci est la notation multiplicative, pour laquelle e est aussi noté 1_G, voire 1, et $a * b$ est souvent noté $a.b$, ou encore ab.
Si l'opération $*$ est commutative, le groupe est dit **commutatif**.
On utilise aussi la notation additive (équivalente) $a + b$, pour laquelle le neutre est noté 0_G, ou simplement 0. L'inverse, s'appelle alors l'**opposé**, noté $-x$. Le choix entre ces deux notations est justifié par le contexte.
Le nombre d'éléments d'un groupe fini G, son cardinal, est son **ordre** $|G|$ (noté aussi $\#G$).
Un groupe se note comme un couple $(G, *)$ (ou un triplet $(G, *, e)$, e étant l'élément neutre) où le premier élément est l'ensemble et le second la loi qui agit sur les éléments. Lorsqu'il n'y a pas d'ambiguïté sur la loi, le groupe se note simplement G.
Exemple de groupes : $(\mathbb{Z}, +)$, $(n\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\{\pm 1\}, *)$ et $(\mathbb{Z}_n^*, *)$ appelé le groupe multiplicatif de $\mathbb{Z}_n$. Notons que $(\mathbb{Z}, *)$ ne forme pas un groupe car les éléments différent de ± 1 n'ont pas d'inverse.

Proposition 5.1.1. *Un groupe G n'admet qu'un seul élément neutre.*

Démonstration. Supposons que e et e' soient deux éléments neutres de G, on a $e = e.e' = e'$. □

Proposition 5.1.2. *L'inverse d'un élément de G est unique.*

Démonstration. Supposons que a' et a'' soient deux inverses de a. Alors $a.a'' = a.a' = e$. Donc en multipliant par a' à gauche, on obtient $a'' = a'$. □

Autres exemples de groupes :
- L'ensemble des chaînes de n bits avec XOR
- Les permutations sur trois éléments S_3 (groupe non commutatif)
- $\mathbb{Z}_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$.

Exercice : Calculer l'ordre du groupe $\mathbb{Z}_{77}^*$.
Définition. L'ordre d'un élément g de G est le plus petit entier non nul n tq $g^n = e$. Si n n'existe pas, g est d'ordre infini.

Proposition 5.1.3. *Soit $g \in G$ un élément d'ordre n, alors g^{-1} est aussi d'ordre n.*

5.1.1 Groupes cycliques

Un groupe fini G est **cyclique** s'il est constitué des puissances successives de l'un de ses éléments, g, appelé alors **générateur** :

$$G = \{g, g^2, \ldots, g^{|G|} = e\}.$$

Exemple : $\mathbb{Z}_{14}^* = \{1, 3, 5, 9, 11, 13\} = \{3^6, 3, 3^5, 3^2, 3^4, 3^3\}$. $\mathbb{Z}_{14}^*$ est donc un groupe cyclique et 3 est un générateur du groupe (aussi appelé élément primitif).

Le nombre de générateurs dans un groupe cyclique d'ordre n est $\Phi(n)$.

Exemples :
- $(\mathbb{Z}, +)$ est engendré par 1
- $(\mathbb{Z}_n, +)$ est engendré par 1 (en fait il s'agit de $[1]_n$)

5.2 Sous-groupe

Un sous ensemble H de G est un sous-groupe de G s'il est non vide et si on a
- pour tout $g, h \in H$, $g * h \in H$ ou $*$ est la loi de G
- pour tout $g \in H$, $g^{-1} \in H$.

Attention, il faut bien vérifier que la loi est bien la même. Par exemple, $(\mathbb{Z}_3, +_3)$ n'est pas un sous groupe de $(\mathbb{Z}_{15}, +_{15})$ car le premier groupe est muni de l'addition modulo 3 alors que le deuxième groupe est muni de l'addition modulo 15.
Exercice : Soit $G = (\mathbb{Z}_3 \times \mathbb{Z}_3, +, (0, 0))$. Soit $(a, b), a \neq b$, un générateur de G. $< (a, b) >$ est-il un sous groupe strict de G ? G est-il un groupe cyclique ?

Si H est l'ensemble des puissances d'un élément h d'un groupe cyclique fini G. Cet ensemble étant fini, il existe un couple d'entiers distincts (r, s) tel que $a^r = a^s$, et alors $a^{r-s} = e$; H est donc un groupe cyclique pour la même opération que G et avec le même neutre : c'est un sous-groupe de G, différent de G si h n'est pas un générateur de G. L'ordre d'un élément de G est l'ordre du groupe cyclique qu'il engendre (ses puissances).
Remarque : Dans un groupe cyclique fini, l'ordre d'un générateur est égal à l'ordre du groupe.

Théorème 5.2.1 (Lagrange)**.** *Soit G fini, $H \subset G$ un sous groupe, alors l'ordre de H divise l'ordre de G.*

Proposition 5.2.1. *Soit $g \in G$, l'ordre de g divise $|G|$. En particulier*

$$|H| \mid |G|, \quad \textit{avec } < g >= H$$

En conséquence, $g^{|G|} = e$, pour tout $g \in G$. En particulier si $a \in \mathbb{Z}_n^*$, alors

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

5.3 Homomorphismes de groupes

Considérons deux groupes $(G, \perp)$ et $(H, \top)$ et leur neutre respectif e_G et e_H.
Définition Une application $f : G \to H$ est un homomorphisme de groupe si :

- $f(e_G) = e_H$
- Si x et y sont éléments de G, $f(x \perp y) = f(x) \top f(y)$.

De plus :

- Si $G = H$, f est un **endomorphisme**.
- Si f est bijective, f est un **isomorphisme**. Si il existe un isomorphisme entre G et H, G et H sont isomorphes et on note $G \simeq H$
- Si f est à la fois un isomorphisme et un endomorphisme, f est un **automorphisme**.

L'image de f est

$$Im(f) := \{f(a) \ : \ a \in G\}$$

et le noyau de f est

$$Ker(f) := \{a \in G \ : \ f(a) = e_H\}.$$

On peut montrer que $Im(f)$ et $Ker(f)$ sont des sous groupes de respectivement G et H.

Proposition 5.3.1. *Soit f un homomorphisme. f est injective si et seulement si $Ker(f) = \{e_G\}$. f est surjective si et seulement si $Im(f) = H$.*

Exemples :

1. Soit $f : (\mathbb{Z}_6, +, 0) \to (\mathbb{Z}_{12}, +, 0)$, définie par $f([1]_6) = [4]_{12}$. f est bien définie car $[1]_6$ est générateur de $\mathbb{Z}_6$ et $[4]_{12}$ est d'ordre 3.
   Par la suite, on simplifie les notations en écrivant des entiers au lieu de classes.
   $f(1) = 4, f(2) = 8, f(3) = 0, f(4) = 4, f(5) = 8, f(0) = 0$.
   $Ker(f) = \{0, 3\}$, donc f n'est pas injective.
   $Im(f) = \{0, 4, 8\}$. $Im(f)$ est un sous-groupe de $(\mathbb{Z}_{12}, +, 0)$.
2. $(\mathbb{Z}_6, +, 0)$ et $(\mathbb{Z}_7^*, ., 1)$ sont isomorphe. L'isomorphisme est $f : \ i \to 3^i$.

5.4 Exercices

1. Quel est l'ordre du groupe additif Z_n ? Quel est celui du groupe multiplicatif Z_n^* ?
2. Montrer que Z_{11}^* est cyclique. $(Z_{15}^*, ., 1)$ est-il un groupe cyclique ? pourquoi ? et $(Z_{18}^*, ., 1)$?
3. Soit G un groupe abélien et soit m un entier. Montrer que $mG := \{ma \ : \ a \in G\}$ est un sous groupe de G.
4. Soit $G = (Z_6, +)$, déterminez un sous groupe propre de G (sous groupe différent de G).
5. Montrez qu'un groupe où tous les éléments sont involutifs (cad $a^2 = e$) est abélien.
6. Cherchez le groupe des inversibles de R^2 muni de la loi

$$(a, b)(c, d) = (ac, bc + d).$$

7. Soit H_1 et H_2 deux sous groupes d'un groupe G abélien. Montrer que $H_1 + H_2$ est un sous groupe avec $H_1 + H_2 := \{h_1 + h_2 \ : \ h_1 \in H_1, h_2 \in H_2\}$.
8. Le groupe $(Z_3, +, 0)$ est-il un sous groupe de $(Z_{15}, +, 0)$?
9. Soit G un groupe abélien. Soit m un entier, montrer que la fonction qui envoie $a \in G$ vers $ma \in G$ est un homomorphisme de groupe de G dans lui-même.
10. Le groupe $(Z_8, +, 0)$ est-il isomorphe à $(Z_{30}^*, ., 1)$? idem avec $(Z_6, +, 0)$ et $(Z_{14}^*, ., 1)$.
11. Quels sont les générateurs du groupe cyclique additif Z ?
12. Sachant que tous les éléments de Z_{15}^* ont un ordre multiplicatif qui divise 4, est-il possible de savoir si Z_{15}^* est cyclique ?
13. Soit $G = \{0, a, b, c\}$ un ensemble muni d'une loi additive définie par sa table :

$+$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Cette structure est-elle un groupe ?
Soit $H = \{0, a\}$ un ensemble muni d'une loi additive définie par sa table :

$+$	0	a
0	0	a
a	a	0

Montrer que $(H, +)$ est un groupe isomorphe à Z_2.
$(H, +)$ est-il un sous-groupe de $(G, +)$?
$(G, +)$ est-il isomorphe au groupe $(G', *)$ de quatre éléments dont la loi $*$ est telle que $x * x = 0, \ \forall x \in G'$?

14. Soit $\phi \ : \ G_1 \to G_2$ un morphisme de groupes (finis). Montrer que $Im(\phi)$ est un sous-groupe de G_2.
15. Montrer que $C_x = \{y \in G | \ xy = yx\}, \ x \in G$, est un groupe de G (G étant un groupe fini).

5.5 Corps et anneaux

On a souvent besoin d'avoir deux opérations binaires distinctes : l'addition et la multiplication. On peut alors construire des structures algébriques plus complexes comme les corps ou les anneaux. Ce sont ces structures qui nous intéressent maintenant.
Un corps F est un ensemble d'éléments dans lequel il est possible de faire des additions, soustractions, multiplications et divisions (à l'exception de zero !).
$+$ et $*$ doivent satisfaire les lois de commutativité, associativité et distributivité.
De plus, pour tout $\alpha \in F$, il doit exister $0,\ 1,\ -\alpha,\ \alpha^{-1}$ tel que

$$\begin{array}{cc} 0+\alpha=\alpha & (-\alpha)+\alpha=0 \\ 1*\alpha=\alpha & 0*\alpha=0 \\ \text{et si } \alpha\neq 0 & (\alpha^{-1})*\alpha=1 \end{array}$$

Un corps fini contient un nombre fini d'éléments : C'est son **ordre**. Les corps finis sont appelés **Corps de Galois**.
Un anneau $(F,+,\cdot)$ admet une structure semblable au corps à ceci près que les éléments de $F^\star$ n'admettent pas forcément un inverse multiplicatif. L'ensemble des inversibles d'un anneau forme un groupe (multiplicatif) appelé le groupe des inversible de R.

Exemple 5.5.1. *L'anneau des entiers modulo p avec p premier :*

$$\mathbb{Z}_p = \{0, 1, \ldots,\ p-1\}.$$

0 est l'élément neutre additif et 1 l'élément neutre multiplicatif. L'ordre de $\mathbb{Z}_p$ est p puisque $\mathbb{Z}_p$ contient p éléments.

La caractéristique d'un anneau est le plus petit entier n tel que $n.1 = 0$. La caractéristique de $\mathbb{Z}_p$ est donc p. Si la caractéristique m d'un corps est non nulle, alors m est premier.
On a vu que $(\mathbb{Z}_n, +, 0)$ et $(\mathbb{Z}_p^\star, *, 1)$ forment des groupes commutatifs pour tout n et tout p premier. On a donc

Proposition 5.5.1. *$(\mathbb{Z}_p, +, \cdot)$ est un corps si p est premier. Si p n'est pas premier, $(\mathbb{Z}_p, +, \cdot)$ est une anneau.*

Définition 5.5.1. *Un sous-ensemble F d'un corps E est un sous-corps de E si F est un corps pour les lois de E. Dans ce cas, E est une extension de F.*

5.5.1 Polynômes

Soit A un anneau, un polynôme f est une expression de la forme

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n,$$

où n est un entier positif, les coefficients $a_i,\ 0 \leq i \leq n$ sont des éléments de A et x un symbole appelé une indeterminée.

Définition 5.5.2. *Soit $f = \sum_{i=0}^{n} a_i x^i$ un polynôme tel que $a_n \neq 0$. Alors f est de degré n (on note $\deg(f) = n$), a_0 est le terme constant et a_n le coefficient de plus haut degré (leading coefficient en anglais).*

On peut définir la somme et le produit de deux polynômes $f = \sum_{i=0}^{n} a_i x^i$ et $g = \sum_{i=0}^{m} b_i x^i$ $(m \leq n)$:

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i) x^i,$$

et

$$f(x)g(x) = \sum_{k=0}^{n+m} c_k x^k, \text{ où } c_k = \sum_{i+j=k} a_i b_j,$$

où $0 \leq i \leq n$ et $0 \leq j \leq m$.
L'ensemble des polynômes sur A muni de ces deux opérations admet une structure d'anneau noté $A[x]$.
On montre facilement que pour tout $f, g \in F[x]$ (F étant un corps)

$$\deg(f+g) \leq max\{\deg(f), \deg(g)\}, \text{ et } \deg(fg) = \deg(f) + \deg(g).$$

Le polynôme g divise le polynôme f si il existe un polynôme h tel que $f = gh$. Pour éviter tout problème, on ne considère ici que des polynômes à coefficients dans un corps.

Exemple 5.5.2. *Dans $\mathbf{F}_2[x]$, considérons les deux polynômes*
$f = x^7 + x^6 + x^3 + x^2 + x + 1$ *et*
$g = x^4 + x^3 + x^2 + 1$.
Le polynôme g divise f car $f = gh$ avec $h = x^3 + x + 1$.

Théorème 5.5.1. *Soit g un polynôme non nul dans $F[x]$. Alors pour tout $f \in F[x]$ il existe deux polynômes q et r de $F[x]$ tels que*

$$f = qg + r, \text{ où } \deg(r) < \deg(q).$$

Toujours dans $F[x]$, si d divise f et g et si tout polynôme divisant f et g divise aussi d, alors d est le plus grand diviseur commun de f et g. On note $d = pgcd(f, g)$. Si $pgcd(f, g) = 1$, on dit que f et g sont premiers entre eux.

Exemple 5.5.3. *Les polynômes de $\mathbf{F}_2[x]$*
$f = x^2 + x + 1$ *et* $g = x^5 - 1$ *sont-ils premiers entre eux ?*

Théorème 5.5.2. *Avec les mêmes notations, il existe $u, v \in F[x]$ tels que*

$$d(x) = u(x)f(x) + g(x)v(x), \text{ avec } u, v \in F[x].$$

Exemple 5.5.4. *Prenons $f := x^6 + x^5 + 2\,x^4 + 2\,x^2 + 2$, et $g := x^2 + 2\,x + 1$, deux polynômes sur $\mathbf{F}_3$. Alors, on a*

$$f = q_1 g + r_1 \text{ avec } q_1 = x^4 + 2\,x^3 + x \text{ et } r_1 = 2x + 2$$
$$g = q_2 r_1 + r_2 \text{ avec } q_2 = 2x + 2 \text{ et } r_2 = 0.$$

On trouve, $d = 2f + q_1 g = x + 1$.

Définition 5.5.3. *un polynôme non constant $f \in F[x]$ est dit irréductible sur F si les seuls polynômes ($\neq f$) qui le divisent sont constants. Sinon, le polynôme f est réductible.*

Exemple 5.5.5. *Le polynôme de $\mathbf{F}_2[x]$*
$f = x^4 - 1$ *est-il irreductible ? même question avec $f = x^3 - 1$.*

Théorème 5.5.3. *Tout polynôme $f \in F[x]$ peut s'écrire*

$$f = a f_1^{e_1} f_2^{e_2} \dots f_k^{e_k},$$

où $a \in F$, les f_i sont des polynômes irréductibles unitaires de $F[x]$ et les exposants e_i des entiers positifs. Cette factorisation est unique.

Rappelons qu'un polynôme unitaire a son coefficient de plus haut degré égal à 1.

Définition 5.5.4. *Un élément a est une racine (ou un zéro) du polynôme f si $f(a) = 0$.*

5.6 Construction d'un corps fini

Jusqu'à présent, nous n'avons introduit qu'un corps ayant p éléments (p premier). Il s'agit de $\mathbf{F}_p$. Dans $\mathbf{F}_p$ les opérations ($+$ et $\cdot$) sont effectuées modulo p.
Comment construire un corps qui admet p^m éléments ? En fait, construire un corps qui contient peu d'éléments n'est pas difficile : il suffit de construire les tables de multiplication et d'addition en respectant les contraintes déjà vues. Par exemple, dans la table de multiplication, chaque ligne doit avoir l'élément neutre. Cela traduit l'existance d'un inverse pour tout élément non nul.
Dans ce qui suit, nous donnons une méthode générale de construction. Nous allons construire le corps $\mathbf{F}_{p^m}$ qui admet p^m éléments.
Soit m un entier positif et $f(x)$ un polynôme irréductible sur $\mathbf{F}_p$ de degré m. On considère un élément α satisfaisant $f(\alpha) = 0$. Posons

$$\mathbf{F}_{p^m} = \{a_0 + a_1\alpha + \cdots + a_{m-1}\alpha^{m-1} \mid a_i \in \mathbf{F}_p\},$$

l'ensemble de tous les polynômes en α de degrés inférieurs à m et à coefficients dans F_p. On peut alors munir cet ensemble des opérations $+$ et $\cdot$.
L'opération $+$ est définie comme l'addition de polynômes dans $\mathbf{F}_p$.
L'opération multiplicative se fait en deux étapes : supposons que l'on veuille calculer $g_1 \cdot g_2$, on va d'abord effectuer une multiplication de polynômes usuelle

$$g_1(\alpha) \cdot g_2(\alpha) = h(\alpha)$$

puis, si le degré de h est supérieur à m, on va le réduire en effectuant une division par f et en considérant le reste r de cette division. Si $\deg(r) < m$ alors $g_1(\alpha) \cdot g_1(\alpha) = r(\alpha)$ sinon on redivise $r(\alpha)$ jusqu'à obtenir un reste dont le degré est inférieur à m. En d'autres termes, on fait les caluls "modulo" le polynôme f, modulo p.

Remarque 1. *Il est important de voir que puisque f est irréductible sur F_p, la racine α n'est pas un élément de F_p.*

Remarque 2. *Pour simplifier, on note souvent $f \cdot g$ par fg.*

Exemple 5.6.1. *Calculer $f * g \mod h$ dans $\mathbf{F}_2$ avec $f = x^3 + x^2 + 1$, $g = x^4 + x + 1$ et $h = x^5 + x + 1$.*

Théorème 5.6.1. *$(\mathbf{F}_{p^m}, +, \cdot)$ est un corps de taille p^m*

Preuve Il est facile de montrer que $(\mathbf{F}_{p^m}, +, \cdot)$ est un anneau contenant p^m éléments. Il reste à montrer que tout élément non nul admet un inverse. Puisque g appartient à $\mathbf{F}_{p^m}$, son degré est inférieur ou égal à $m - 1$. Et puisque f est irréductible, les deux polynômes f et g sont premiers entre eux. On peut donc utiliser Bezout : il existe deux polynômes $u(x)$ et $v(x)$ de $\mathbf{F}_{p^m}[x]$ tels que

$$u(x)f(x) + v(x)g(x) = 1.$$

Si l'on écrit cette égalité en α, puisque $f(\alpha) = 0$, on obtient

$$v(\alpha)g(\alpha) = 1,$$

et en supposant que $\deg(v(\alpha)) < m$ (sinon on réduit modulo f comme précédemment) on a $g^{-1} = v(\alpha)$. □

Le corps $\mathbf{F}_{p^m}$ est appelé une extension finie de $\mathbf{F}_p$ et $\mathbf{F}_p$ est le corps de base. Le corps se note aussi $\mathbf{F}_p[x]/(f(x))$. Si f est réductible, il existe deux polynômes non nuls f_1 et f_2 de $\mathbf{F}_p[x]$ tels que $f = f_1 f_2$. Cela signifie que f_1 et f_2 sont des diviseurs de zéro (donc non inversibles) et $\mathbf{F}_p[x]/(f(x))$ n'est pas un corps.

Exemple 5.6.2. *Soit $p = 2$ et $f(x) = x^3 + x + 1$ un polynôme irréductible sur $\mathbf{F}_2$. Soit β une racine de $f(x)$. Le corps fini $\mathbf{F}_{2^3}$ est défini par*

$$\mathbf{F}_{2^3} = \{a_0 + a_1\beta + a_2\beta^2 | a_i \in \mathbf{F}_2\}.$$

Les éléments de $\mathbf{F}_{2^3}$ peuvent donc s'écrire comme des triplets (a_0, a_1, a_2) ou des polynômes. De plus, puisque $\mathbf{F}_{2^3}$ est un corps, $\mathbf{F}_{2^3}^\star$ forme un groupe multiplicatif.

On peut montrer que tout corps fini peut être construit comme nous venons de le voir. Cela signifie que tout corps fini F de caractéristique p admet p^m éléments (m étant un entier strictement positif).

Exemple 5.6.3. *On veut construire le corps à quatre éléments. On sait que $4 = 2^2$ donc le corps de base est $\mathbf{F}_2$ et pour construire le corps, il suffit d'obtenir un polynôme irreductible de degré $m = 2$ sur $\mathbf{F}_2$ (pour cela il existe des tables de polynômes irreductibles dans la littérature).*
Soit $f(x) = x^2 + x + 1$ un polynôme irréductible sur $\mathbf{F}_2$ et soit β une racine de $f(x)$. La caractéristique du corps est égale à 2, c'est la caractéristique du corps de base. Les éléments de F_4 peuvent être représentés par les polynômes de la forme $a_1 + a_2\beta$, a_1 et a_2 étant binaires. On obtient : $F_4 = \{0, 1, \beta, \beta + 1\}$. Le corps est totalement défini par sa table d'addition et de multiplication que nous construisons maintenant en notant $\beta + 1 = \overline{\beta}$

$+$	0	1	β	$\overline{\beta}$
0	0	1	β	$\overline{\beta}$
1	1	0	$\overline{\beta}$	β
β	β	$\overline{\beta}$	0	1
$\overline{\beta}$	$\overline{\beta}$	β	1	0

$\cdot$	0	1	β	$\overline{\beta}$
0	0	1	0	0
1	0	1	β	$\overline{\beta}$
β	0	β	$\overline{\beta}$	1
$\overline{\beta}$	0	$\overline{\beta}$	1	β

Considérons maintenant un corps fini F muni de p^m éléments et $\beta \in F^\star = F \setminus \{0\}$. Alors toute puissance de β appartient aussi à $F^\star$ et comme F est fini, il existe un k et un l tel que $\beta^k = \beta^l$. Cela signifie que $\beta^{k-l} = 1$.

Exemple 5.6.4. $F = \mathbb{Z}_{11},\ \beta = 2$. *$F^\star$ s'écrit*

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	5	10	9	7	3	6	1	2

Donc $\beta^{10} = 1$: β est une racine dixième de l'unité.

Définition 5.6.1. *L'***ordre** *d'un élément β non nul dans un corps fini est le plus petit entier $r \geq 1$ tel que $\beta^r = 1$.*

Théorème 5.6.2. *(de l'élément primitif) Tout corps fini F de taille p^m contient un élément β d'ordre $p^m - 1$, appelé* **élément primitif** *de F.*

Preuve On sait que puisque F est un corps, $F^\star$ est un groupe multiplicatif d'ordre $p^m - 1$. On va montrer plus précisément que c'est un groupe cyclique engendré par un élément β.
Soit $\beta \in F^\star$ un élément dont l'ordre r est le plus grand parmi tous les éléments du groupe. On a trivialement $r < p^m$. Il est facile de montrer que l'ordre l de tout élément b du groupe divise r. Ainsi, puisque β est racine de l'equation $x^r - 1$, tous les éléments du groupe sont aussi racines de cette même equation et $\prod_{\alpha \in F^\star}(x - \alpha)$ divise $x^r - 1$. Ce qui signifie que $r \geq p^m - 1$. Comme on sait que $r \leq p^m - 1$ on a $r = p^m - 1$. Donc β est d'ordre $p^m - 1$ qui est la taille du groupe multiplicatif $F^\star$ et $F^\star = \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\}$. □

Corollaire 5.6.1. *Tout corps fini de taille p^m est de la forme*

$$F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m - 2}\},\ \beta \in F.$$

Exemple 5.6.5. $F = \mathbb{Z}_{11} = \{0\} \cup \{1, 2, 2^2, 2^3, 2^4, 2^5, 2^6, 2^7, 2^8, 2^9\}$.

Un polynôme primitif est un polynôme qui contient une racine primitive. Il faut noter que tous les polynômes irréductibles ne sont pas primitifs. Par exemple dans $\mathbf{F}_2[x]$, $P = x^{11}+x^9+x^7+x^6+x^5+x+1$ est irréductible de degré 11 et racine de $x^{23}-1$. Soit β une racine de P, β est d'ordre 23 et non $2^{11}-1 = 2047$ donc β n'est pas une racine primitive de $\mathbf{F}_{2^{11}}$. La donnée de P permet de construire le corps : c'est l'ensemble des polynômes de $\mathbf{F}_2[x]$ "modulo" $P(x)$.
Cependant, d'après le théorème précédent, il existe un élément α d'ordre $2^{11}-1 = 2047$ dont les puissances forment $\mathbf{F}^{\star}_{2^{11}}$. On sait que l'ordre de β divise l'ordre de α. On a $\beta = \alpha^{89}$ car $89 * 23 = 2047$. En résumé, voici deux représentations du corps en fonction de β ou α :

$$\begin{aligned}\mathbf{F}_{2^{11}} &= \{\textstyle\sum_{i=1}^{11} a_i\beta^i,\ a_i \in \mathbf{F}_2\} \\ &= \{0\} \cup \{1, \alpha, \alpha^2, \ldots, \alpha^{2^{11}-2}\}.\end{aligned}$$

Théorème 5.6.1. *(Fermat) Tout élément β d'un corps F d'ordre p^m satisfait $\beta^{p^m} = \beta$. Ainsi, β est racine de $x^{p^m} = x$ et*

$$x^{p^m} - x = \prod_{\beta \in F} (x - \beta).$$

Définition 5.6.2. *Le polynôme minimal sur $\mathbf{F}_p$ de β est le polynôme unitaire de plus bas degré $M(x)$ dont les coefficients sont dans $\mathbf{F}_p$ tel que $M(\beta) = 0$.*

Exemple 5.6.6. *Construction du corps $F_8 = F_{2^3}$. Le corps admet huit éléments donc il contient un élément β d'ordre 7 qui est une racine primitive de l'unité. $F_8 = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^6\}$, et β est racine du polynôme $(x^7 - 1) \mod 2$. On a $x^7 - 1 = \prod_{i=1}^{7}(x - \beta^i) = (x^3 + x + 1)(x^3 + x^2 + 1)(x + 1)$. Notons P_1 le polynôme $x^3 + x + 1$ et P_2 son réciproque et choisissons comme générateur β une racine de P_1. Cela veut dire que $P_1(\beta) = 0$ et $\beta^3 = \beta + 1$. Tout élément du corps peut être représenté par un triplet (s'il est vu comme un espace vectoriel de dimension 3 sur F_2) ou un polynôme de degré (au plus) 2 avec $\beta^3 = \beta + 1$.*

triplet $(\beta^2, \beta, 1)$	*polynôme*	*puissance de* β
$(0,0,0)$	0	0
$(0,0,1)$	1	1
$(0,1,0)$	β	β
$(1,0,0)$	β^2	β^2
$(0,1,1)$	$1+\beta$	β^3
$(1,1,0)$	$\beta+\beta^2$	β^4
$(1,1,1)$	$1+\beta+\beta^2$	β^5
$(1,0,1)$	$1+\beta^2$	β^6
$(0,0,1)$	1	$\beta^7 = 1$

En choisissant β racine de P_2, on aurait obtenu un corps isomorphe. Rappelons que deux corps sont dits isomorphes si il existe une application bijective ϕ de E dans F qui preserve l'arithmétique du corps (c.a.d. $\phi(a + b) = \phi(a) + \phi(b)$ et $\phi(ab) = \phi(a)\phi(b)$, $a,\ b \in E$).

Exemple 5.6.7. *Construction du corps $F_{16} = F_{2^4}$.*
On sait que F_{16} peut s'écrire $F_{16} = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{14}\}$, où β est un élément primitif de F_{16}.

5.6.1 Logarithme de Zech

Lorsque l'on fait des calculs dans les corps finis, il est facile de calculer $\alpha^i\alpha^j$. Il suffit d'additionner les puissances. Par contre, $\alpha^i + \alpha^j$ est plus difficile à déterminer. On peut alors utiliser le logarithme de Zech. Supposons que $i < j$. Alors

$$\alpha^i + \alpha^j = \alpha^i(1 + \alpha^{j-i}).$$

Posons $r = j - i$. On veut calculer $(1 + \alpha^r) = \alpha^s$.
L'entier s est appelé le logarithme de Zech de r, noté $Zech(r)$:

$$\alpha^{Zech(r)} = \alpha^r + 1.$$

Il existe bien sur des tables de logarithmes pour les corps finis les plus utilisés.

Exercice 5.6.1. *Calculer les tables pour* $\mathbf{F}_8$ *et* $\mathbf{F}_{16}$.

Par cette méthode, il suffit de stocker les $p^m - 2$ logarithmes de Zech pour pouvoir effectuer toutes les additions nécessaires.

5.6.2 Classes cyclotomiques

Les classes cyclotomiques (cyclotomic cosets en anglais) permettent de déterminer le nombre de facteurs irréductibles de $x^{p^m-1} - 1$ sur F. Connaissant le polynôme minimal d'une racine de $x^{p^m-1} - 1$, elles permettent de trouver tous les polynômes minimaux des racines de $x^{p^m-1} - 1$, c'est à dire tous les facteurs de $x^{p^m-1} - 1$.

Théorème 5.6.3. *$\beta \in F_{p^m}$ et β^p ont le même polynôme minimal.*

Preuve Soit $M_\beta(x)$ le polynôme minimal de β. $M_\beta(x) = \sum_{i=0}^{d} a_i x^i$, où $d = \deg(M_\beta(x))$ et $a_i \in F_p$. Notons que $a_i = a_i^p$ car a_i est racine de $x^p - x = 0$. On a $M_\beta(\beta) = 0$ et $M_\beta(\beta) = \sum_{i=0}^{d} a_i \beta^i = (\sum_{i=0}^{d} a_i \beta^i)^p = \sum_{i=0}^{d} a_i^p (\beta^p)^i = M(\beta^p)$. Donc β^p est une racine de M_β. Puisque M_β est irreductible, $M_\beta = M_{\beta^p}$. □

Définition 5.6.3. *Soit $\beta \in F_{p^m}$. Alors les éléments $\beta,\ \beta^p, \ldots,\ \beta^{p^{m-1}}$ sont appelés les conjugués de β pour le corps F_p.*

Tous les conjugués de β ont donc le même polynôme minimal.

Exemple 5.6.8. *On considère le corps F_{16} avec $p = 2$, $m = 4$ et β admettant pour polynôme minimal $\beta^4 + \beta + 1$. Alors*

$$\left.\begin{array}{ll} \beta & \text{est un zéro de } x^4 + x + 1 \\ \beta^2 & \text{idem} \\ \beta^4 & \text{idem} \\ \beta^8 & \text{idem} \\ \beta^{16} = \beta & \end{array}\right\} \text{4 racines distinctes}$$

Finalement, on peut vérifier par le calcul que

$$x^4 + x + 1 = (x - \beta)(x - \beta^2)(x - \beta^4)(x - \beta^8).$$

Trouver l'ensemble des conjugués de toutes les racines revient à partitionner l'ensemble des puissances de β. Le corps F s'écrit $F = \{0\} \cup \{1, \beta, \beta^2, \ldots, \beta^{p^m-2}\}$ et l'ensemble des puissances de β est tout simplement Z_{p^m-1}.

Définition 5.6.4. *Soit $a,\ b \in Z_{p^m-1}$. a et b sont dits equivalents (notés $a \equiv b$) si $b = p^i a \mod (p^m - 1)$.*

La relation d'equivalence est reflexive, symétrique et transitive. C_s représente une classe cyclotomique où s est le plus petit entier de la classe :

$$\{s,\ sp,\ sp^2, \ldots,\ sp^{m_s-1}\},$$

où m_s est l'entier le plus petit tel que $p^{m_s} = s \pmod{p^m - 1}$. L'entier s est quelquefois appelé le chef de classe ou en anglais coset leader.

Exemple 5.6.9. *Quelles sont les classes cyclotomiques modulo* 15 *pour* $p = 2$ *?*

$$\begin{aligned} C_0 &= \{0\} \\ C_1 &= \{1, 2, 4, 8\} \\ C_3 &= \{3, 6, 12, 9\} \\ C_5 &= \{5, 10\} \\ C_7 &= \{7, 14, 13, 11\}. \end{aligned}$$

Théorème 5.6.4. *Soit* $\alpha \in \mathbf{F}_{p^m}$ *un élément primitif.*

$$M(\alpha^s)(x) = \prod_{i \in C_s} (x - \alpha^i)$$

Preuve Ce résultat est admis. □

Exercice 5.6.2. *Soit* α *une racine primitive de* $x^4 + x + 1$ *sur* $\mathbf{F}_{16}$.
Déterminer les polynômes minimaux de $1, 3, 5, 7$.

5.7 Exercices

1. Calculer $(x+1)(x+2)(x^2+1)$ dans $F_3[x]$. Montrer que x^2+1 est irréductible. Construire un corps de neuf éléments. Soit α un élément de ce corps, calculer α^4.
2. Soit R un anneau. Un idéal de R est un sous-groupe I du sous-groupe additif de R qui est clos par multiplication avec un éléments de R (pour tout $a \in I$ et $r \in R$, on a $ar \in I$).
   Soit $m \in Z$.
   Montrer que l'ensemble mZ est un sous-groupe additif du groupe Z et un idéal de l'anneau Z.
3. Soit $f(x) = x^4 + x + 1 \in F_2[x]$. Soit α une racine de f.
   (a) Calculer α^5, α^6, α^7, α^8, α^9, α^{10}, ...
   (b) Calculer $(\alpha^4 + \alpha + 1)^2$.
   (c) Calculer les inverse de $\alpha^{12}, \alpha^8, \alpha^{14}$
   (d) Construire le corps $F_2[x]/(f(x))$.
4. Montrer (par contradiction) que la caractéristique d'un anneau intègre est soit 0 soit un entier premier.
5. Soit p un entier premier. On considère le polynôme $a := x^p + x \in Z_p[x]$. Déterminer $a(\alpha)$ pour tout $\alpha \in Z_p$.
6. Donner un exemple où le degré du produit de deux polynômes a et b est strictement inférieur à $\deg(a) + \deg(b)$.
7. Calculer $a \mod b$ dans F_3, avec $a = x^4 + 2x^3 + x + 2$, $b = x^3 - 1$.
8. Calculer $a.a' \mod b$ dans F_5, avec $a' = 2x^2 + x + 2$
9. Montrer qu'un idéal propre d'un anneau A ne peut contenir d'éléments inversibles.
10. Montrer qu'un anneau est un corps si et seulement si il n'a pas d'idéal propre non nul.
11. Soit α une racine de $x^3 + x^2 + 1 \in F_2[x]$. Quelles sont les autres racines de ce polynôme (en fonction de α) ?
12. Soit f un polynome irréductible primitif dans $GF(3)$. $f = x^2 + 2x + 2$. Factoriser $X^8 - 1$ dans $GF(3)[x]$.
13. Il existe plusieurs façons de construire $GF(16)$. La première est de considérer $GF(16)$ comme une extension de $GF(2)$:
    $$GF(16) = GF(2)[x]/(x^4 + x + 1).$$
    Quelle est la deuxième ?
14. Soit α une racine de $(x^4 + x + 1)$. Quel est le polynôme minimal M de α^3 (polynôme unitaire de plus bas degré tel que $M(\alpha^3) = 0$) ?
15. Trouver un polynôme binaire de degré 9 qui factorise $x^{15} - 1$.
16. Combien existe-t-il de polynomes binaires de degré 10 qui factorise $x^{15} - 1$?
17. On considère l'anneau $GF(2)[x]/(x^{15}-1)$. Dans cet anneau, combien l'idéal engendré par x^4+x+1 admet-il d'éléments ?

5.7.1 Exercice supplémentaire

Considérons un corps commutatif F. Une courbe elliptique E sur F est définie comme étant l'ensemble des couples (x, y), $x, y \in F$, vérifiant l'équation

$$y^2 = x^3 + ax + b$$

et augmenté artificiellement d'un élément supplémentaire que l'on notera O et qu'on appelle le "point à l'infini". Une droite qui passe par deux points d'une courbe elliptique la recoupe en exactement un point supplémentaire. On peut munir une courbe d'une structure de groupe commutatif. Les éléments du groupes sont les points de la courbe et la loi de groupe est notée $+$. On convient que

1. Le point à l'infini O est l'élement neutre,
2. Soit $P, Q,\ R$ trois points de E. $P + Q + R = O$ si les points P, Q, R sont alignés.

La loi de groupe, notée $+$, peut être définie géométriquement. Si $P \neq O$ est le point (x, y) et Q est le point $(x, -y)$ symétrique par rapport à l'axe des x, on convient que $P + Q = O$. P et Q sont donc des points opposés.
Soient deux points $P_1 = (x_1, y_1)$ et $P_2 = (x_2, y_2)$ de E différents de O et tels que $x_1 \neq x_2$. Alors la somme $P_1 + P_2 = P_3 = (x_3, y_3)$ est un point de la courbe vérifiant

$$\begin{cases} x_3 = & (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 = & -y_1 + (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) \end{cases}$$

Si $P_2 = P_1$, le point $P_3 = P_1 + P_1$ noté $2.P_1$ a pour coordonnées x_3 et y_3 avec

$$\begin{cases} x_3 = & (\frac{3{x_1}^2 + a}{2y_1})^2 - 2x_1 \\ y_3 = & -y_1 + (\frac{3{x_1}^2 + a}{2y_1})(x_1 - x_3) \end{cases}$$

Soit E la courbe elliptique d'équation $y^2 = x^3 + x + 1$ sur F_{17}.

1. Montrer que $P = (0, 1)$ est un point de la courbe E.
   On constate que le groupe de la courbe est un groupe cyclique à 18 éléments et que P en est un générateur. Ainsi $15.P = (4, 1)$, $17.P = (0, -1)$ et $18.P = O$ appartiennent à la courbe.
2. Calculer $2.P$, $3.P$ et $(0, 1) + (-4, 1)$
3. Le point $A = (-4, -1)$ appartient-il à la courbe E ? Si oui, calculer k tel que $k.P = A$.

Alice et Bob désirent communiquer de manière confidentielle et décident d'utiliser la courbe elliptique pour chiffrer leur communication. Bob rend publics la courbe E, le corps F_{17}, le point P et un point $\Pi = s.P$. L'entier s est la clé secrète de Bob. Un message M est un élément de F_{17} transformé en un point de la courbe et pour le chiffrer, Alice choisit un entier aléatoire k, calcule $k.P$ et transmet le point (C_1, C_2) ou $C_1 = k.P$ et $C_2 = M + k.\Pi$. Pour déchiffrer, Bob calcule $M = C_2 - s.C_1$.

4 Alice veut chiffrer $M = (-4, 1)$. Elle choisit $k = 3$. La valeur de Π est $(-1, 4)$. Quelle est la valeur du chiffré ?

5 Calculer $5.P$

L'inconvénient majeur de cette méthode est qu'il faut d'abord précoder chaque message en un point de la courbe E, ce qui n'est pas très commode.
Pour corriger ce défaut, Menezes et Vanstone ont proposé cette variante : chaque message en clair M est un couple $M = (M_1, M_2)$ d'éléments de F_{17}.
Pour le chiffrement, Alice choisit un entier k, calcule $k.P$ et $k.\Pi = (x, y)$.
Le message chiffré est le couple $C = (C_1, C_2)$ où $C_1 = k.P$ et $C_2 = (M_1 x, M_2 y)$ est un couple d'éléments de F_{17}.

6 Comment Bob va-t-il déchiffrer ?

7 Quelle est la longueur du chiffré par rapport à celle du texte clair ?