Cours et activités en arithmétique pour les classes terminales - 2^{e} édition

Groupe de travail sur la liaison Lycées-Universités

IREM de Marseille

Table des matières

Chapitre 1

Introduction

L'arithmétique, qui étudie les différentes questions relatives aux nombres entiers, est un des secteurs scientifiques les plus anciens. Ses problèmes internes ont motivé durant des siècles des développements fondamentaux dans diverses parties des mathématiques. Plus récemment des problèmes concrets liés à l'informatique, l'electronique ainsi qu'à la représentation, la compression, l'intégrité et la confidentialité des données, ont été résolus dans le cadre de l'arithmétique. On peut ajouter que les méthodes de raisonnement et de démonstration utilisées dans cette discipline sont d'une grande richesse et d'une grande variété.
Ainsi, compte tenu de son aspect culturel, de son aptitude à la formation du raisonnement, de ses nombreuses applications concrètes récentes, aussi bien à l'intérieur qu'à l'extérieur du champ des mathématiques, convenait-il que l'arithmétique élémentaire ait une place dans la formation des élèves des lycées (tout au moins en spécialité mathématique).

Le programme des classes terminales scientifiques qui se met en place pour l'année scolaire 1998-1999 prévoit en spécialité mathématique un chapitre arithmétique. Le libellé du programme est clair et délimite parfaitement le contenu de l'enseignement.
Dans les grandes lignes, il s'agit de **présenter les notions élémentaires de l'arithmétique**, notamment la divisibilité, la division euclidienne, le pgcd, le ppcm, le théorème de Bezout, la décomposition en facteurs premiers, en faisant des démonstrations et des résolutions de problèmes "à la main", **en insistant sur l'aspect algorithmique**, et **en évitant toute dérive sur des aspects algébriques** (idéaux de $\mathbb{Z}$, étude de $\mathbb{Z}/n\mathbb{Z}$).

Divers thèmes liés à des applications peuvent être choisis pour illustrer les objets et faire fonctionner les résultats (codage, cryptage, etc ...).
Remarquons enfin que cette partie peut être utilisée avec profit pour faire réaliser aux élèves divers types de démonstrations.
Bien entendu, ce cours doit être conçu en tenant compte de ce qui sera fait en DEUG et années ultérieures, en mathématiques et en informatique. En particulier on pourra insister sur les principes de la numération avec des exemples concrets de changements de bases (décimal, binaire, octal, hexadécimal), les algorithmes de calcul du pgcd ou du ppcm (algorithmes d'Euclide, ou algorithmes utilisant la décomposition en facteurs premiers).

La brochure contient

- Un essai de cours de terminale écrit dans le respect du programme. Bien sûr, il ne s'agit que d'un document de travail qui offre **une présentation parmi d'autres** et qui de toutes façons **doit être adapté** au rythme, au niveau et aux centres d'intérêts de chaque classe.

- Des thèmes d'activités un peu larges, tournant autour d'interventions de l'arithmétique (clés de contrôle, correction d'erreurs, chiffrement, etc ...). Chacun des thèmes proposés fournit des exercices qui utilisent et illustrent les objets et les résultats du cours. Les sujets abordés sont assez longs, et il n'est évidemment pas question d'essayer de tout traiter. Nous nous sommes limités à des questions qui nous semblent abordables naturellement avec les connaissances du programme sans contorsion et sans artifice. Il y a déjà suffisamment à faire comme cela sans chercher à présenter des problèmes qui trouvent naturellement leur place dans des études ultérieures. Ces thèmes sont rédigés sous forme de questions parfois abruptes qu'il est nécessaire de détailler plus au niveau des élèves. C'est le propos du deuxième volet de cette partie, qui fournit également les solutions des exercices.

- Des compléments d'arithmétique à l'usage des enseignants, de niveau DEUG, préparation à l'agrégation interne.

Cette publication est le résultat du travail d'un groupe de **l'IREM de Marseille** (groupe de travail sur la liaison lycées- universités, année 1997-1998). Elle doit aussi beaucoup aux contacts que nous avons eus avec divers enseignants, en particulier avec le "Groupe Académique de Réflexion au niveau des

lycées" piloté par les inspecteurs pédagogiques régionaux de mathématiques de l'académie d'Aix-Marseille.
Les compléments d'arithmétique joints à ce travail sont une adaptation d'un cours de R. Rolland diffusé par ailleurs sur internet (http://www.irem.univ-mrs.fr).

Chapitre 2

Un projet de cours en classe de terminale

2.1 Introduction

Ce texte constitue un document de travail pour l'élaboration d'un cours d'arithmétique répondant aux spécifications du programme qui va se mettre en place en 1998-1999. Les notions développées sont les notions simples de base de l'arithmétique. Les démonstrations sont le plus souvent présentées sous forme algorithmique. Bien entendu, il faudra joindre à ce cours des exercices et thèmes de travail. De ce point de vue l'aspect algorithmique ainsi que des applications à l'informatique et à divers domaines de la vie courante, peuvent fournir de bonnes illustrations des bases de l'arithmétique.

2.2 La division dans $\mathbb{Z}$.

2.2.1 Définition

Définition 2.2.1 *Soient a et b deux éléments de $\mathbb{Z}$. Nous dirons que a* **est divisible par** *b ou encore que a est* **multiple** *de b s'il existe un élément q dans $\mathbb{Z}$ tel que $a = bq$. Dans ce cas nous noterons $b|a$.*

Remarquons que si $a \neq 0$ et si b divise a alors $b \neq 0$ et q est unique. On dira que q est le **quotient exact** de a par b et on le notera a/b. Dans ce cas a/b divise aussi a.

Exemples: 3 divise 18, -13 divise 39, -4 divise -16, 7 ne divise pas 22.

2.2.2 Propriétés élémentaires

Nous pouvons remarquer directement un certain nombre de propriétés élémentaires qui dérivent simplement de la définition.

Proposition 2.2.1 *Si un nombre divise a et b il divise tout nombre de la forme $ua + vb$. En particulier il divise la* **somme** *et la* **différence** *de a et de b.*

Voici une application simple de cette proposition: les nombres a et $a + 1$ n'ont que 1 comme diviseur positif commun. En effet la différence de ces deux nombres est 1.

Remarque: On dispose aussi des propriétés simples suivantes:
1) $a|a$.
2) $c|b$ et $b|a$ implique $c|a$.
3) $a|b$ et $b|a$ implique $|a| = |b|$.
4) $ac|ab$ et $a \neq 0$ implique $c|b$.
5) $1|a$.
6) $a|0$.
7) $0|a$ implique $a = 0$.
8) $b|a$ et $a \neq 0$ implique $0 < |b| \leq |a|$.

2.2.3 La division Euclidienne dans $\mathbb{Z}$.

Théorème 2.2.1 *Soit a un entier et b un entier* **non nul**. *Il existe un unique entier q et un unique entier r tels que*

$$a = qb + r$$

où r est soumis à la condition

$$0 \leq r < |b|.$$

Faire la **division euclidienne** de a par b consiste à déterminer q et r appelés respectivement le **quotient** et le **reste** de la division euclidienne.

Lorsque b divise a, q est le quotient exact de a par b et $r = 0$.

Preuve : La démonstration va consister tout d'abord à établir l'existence de q et r en donnant un algorithme produisant ces nombres.
Supposons dans un premier temps que $a \geq 0$ et $b > 0$.

Voici **l' algorithme d'Euclide** pour la division euclidienne, qui consiste à faire des soustractions successives:

$B := b$;
$R := a$;
$Q := 0$;
tant que $R \geq B$ *faire*
  début
    $R := R - B$;
    $Q := Q + 1$;
  fin;

A la fin on a dans la variable Q le quotient cherché et dans la variable R le reste.
En effet, remarquons qu'à l'entrée de la boucle, il y a b dans B, a dans R et 0 dans Q, donc $a = B * Q + R$. D'autre part si quand on commence un tour de boucle on a $a = B * Q + R$, à la fin du tour de boucle on a aussi cette même égalité puisque R a diminué de b alors que Q a augmenté de 1 ou encore $Q * B$ a augmenté de b. En fin de boucle on a donc $a = B * Q + R$ et $0 \leq R < B$.

Exemple: $a = 46$, $b = 15$.
On a successivement $R = 46, Q = 0$; $R = 46-15 = 31, Q = 1$; $R = 31-15 = 16, Q = 2$; $R = 16 - 15 = 1, Q = 3$.
Donc $46 = 3 \times 15 + 1$.

Etudions maintenant les cas où a et b ne sont pas nécessairement positifs. Le traitement de ces cas n'est qu'une adaptation technique de ce qu'il se passe sur les nombres positifs. On fera alors la division euclidienne entre nombres positifs de $|a|$ par $|b|$ sous la forme $|a| = q|b| + r$, et on calculera le quotient et le reste de la division de a par b en fonction de q et r. Plus précisément:

- $a \geq 0$ et $b < 0$. Dans ce cas on fait la division euclidienne de a par $-b$, ce qui donne $a = q(-b) + r$ ou encore $a = (-q)b + r$, si bien que le quotient cherché est $-q$ et le reste cherché est r.

- $a < 0$ et $b > 0$. Dans ce cas on fait la division euclidienne de $-a$ par b ce qui donne $-a = qb + r$ ou encore $a = -qb - r$ c'est-à-dire

$a = -(q+1)b + b - r$, si bien que le quotient cherché est $-(q+1)$, et le reste cherché est $b - r$.

- $a < 0$ et $b < 0$. Dans ce cas on fait la division euclidienne de $-a$ par $-b$ ce qui donne $-a = q(-b) + r$ ou encore $a = qb - r$ c'est-à-dire $a = (q+1)b - b - r$, si bien que le quotient cherché est $q+1$, et que le reste cherché est $-b - r$.

Quant à l'unicité, si on a une deuxième écriture sous la forme $a = q'b + r'$ avec $0 \leq r' < |b|$, alors $|r - r'| < |b|$, si bien que nécessairement $q = q'$ et donc $r = r'$.

2.3 La divisibilité dans $\mathbb{Z}$

2.3.1 Plus grand commun diviseur

Nous allons étudier les diviseurs d'un ou plusieurs nombres entiers. Comme les diviseurs de a sont les mêmes que ceux de $-a$ et que si d est un diviseur de a, il en est de même de $-d$, nous restreindrons dans un premier temps notre étude à $\mathbb{N}$. Elle s'étendra tout naturellement à $\mathbb{Z}$.

Considérons deux entiers naturels a et b dont l'un (b par exemple) est **strictement positif**. Faisons la division euclidienne de a par b:

$$a = qb + r \quad \text{avec } 0 \leq r < b.$$

Sur cette expression on voit que les diviseurs de a et de b sont les diviseurs de b et de r. On peut alors réitérer le procédé, en faisant la division euclidienne de b par r, et ainsi jusqu'à obtenir un reste nul, ce qui va nécessairement se produire puisque ces restes décroissent strictement et sont tous ≥ 0. Si nous appelons d le dernier reste non nul, nous en déduisons que les diviseurs de a et de b sont les diviseurs de d et de 0, c'est-à-dire les diviseurs de d. Ainsi d est un diviseur commun de a et b et tout autre diviseur commun de a et b divise d.

Théorème 2.3.1 *Soient a et b deux entiers dont l'un au moins est non nul. Il existe un plus grand entier > 0 qui soit diviseur commun de a et de b. Cet entier sera noté $pgcd(a,b)$ et appelé le* **plus grand commun diviseur** *de a et b. Les diviseurs communs de a et b sont les diviseurs de $pgcd(a,b)$.*

Ecrivons plus précisément l'algorithme (**algorithme d'Euclide** pour le calcul du pgcd):

$R0 := |a|;$
$R1 := |b|; \quad (b \neq 0)$
tant que $R1 > 0$ *faire*
début
$R := Reste\_Division(R0, R1);$
$R0 := R1;$
$R1 := R;$
fin;

Cet algorithme se termine car $R1$ décroît strictement à chaque tour de boucle. Comme de plus $R1 \geq 0$, la boucle se termine avec $R1 = 0$, et $R0 = pgcd(a, b)$. Remarquons qu'à chaque étape de la boucle, l'ensemble des diviseurs communs de $R0$ et $R1$ est le même.

Exemple: $a = 325$, $b = 145$.
On a successivement
$R0 = 325, R1 = 145, R0 = 2R1 + 35$; $R0 = 145, R1 = 35, R0 = 4R1 + 5$; $R0 = 35, R1 = 5, R0 = 7R1 + 0$; $R0 = 5, R1 = 0$.
Donc $pgcd(325, 145) = 5$.

Voici quelques propriétés élémentaires du pgcd.

Proposition 2.3.1
1) $pgcd(a, b) = pgcd(b, a)$.
2) $pgcd(a, (b, c)) = pgcd((a, b), c)$.
3) $pgcd(ca, cb) = |c| pgcd(a, b)$.
4) $pgcd(a, 1) = 1$.
5) Soit $a' = a/pgcd(a, b)$ *et* $b' = b/pgcd(a, b)$. *Alors* $pgcd(a', b') = 1$.

Exercice: Soient a et b deux entiers dont l'un au moins est non nul. Soit d un diviseur commun > 0 de a et b tel que $pgcd(a/d, b/d) = 1$. Montrer que $d = pgcd(a, b)$.

Définition 2.3.1 *Lorsque* $pgcd(a, b) = 1$, *nous dirons que les nombres* a *et* b *sont* **premiers entre eux**.

2.3.2 Conséquences, théorème de Bezout, applications

Reprenons l'algorithme qui nous a servi à déterminer le pgcd de deux nombres sur l'exemple précédent $a = 325$, $b = 145$. Cet algorithme nous conduit aux calculs

$$325 = 2 \times 145 + 35$$

et le reste 35 s'exprime en fonction de 325 et de 145

$$35 = 325 - 2 \times 145,$$

puis

$$145 = 4 \times 35 + 5$$

et le reste 5 s'exprime en fonction de 145 et de 35 et par suite en fonction de 325 et de 145

$$5 = 145 - 4 \times 35 = 9 \times 145 - 4 \times 325,$$

puis

$$35 = 7 \times 5 + 0$$

et l'algorithme s'arrête car le reste est nul. Ainsi $pgcd(325, 145) = 5$ et de plus on a pu exprimer ce pgcd 5 comme combinaison entière des nombres 325 et 145.

on dispose en fait du résultat suivant

Théorème 2.3.2 *Si $pgcd(a, b) = d$, il existe deux entiers u et v tels que $ua + vb = d$.*

Preuve : Là encore nous supposerons que $a \geq 0$ et $b > 0$. Le cas général s'en déduit.

Voici un algorithme (**algorithme d'Euclide étendu**, adaptation de l'algorithme précédent) qui permet de trouver explicitement un couple (u, v) qui convient.

$R0 := a; \quad (a \geq 0)$
$R1 := b; \quad (b > 0)$
$U0 := 1;$
$U1 := 0;$
$V0 := 0;$
$V1 := 1;$

tant que $R1 > 0$ *faire*
début
$Q := Quotient\_Division(R0, R1);$
$R := Reste\_Division(R0, R1);$
$U := U0 - Q * U1;$
$V := V0 - Q * V1;$
$R0 := R1;$
$R1 := R;$
$U0 := U1;$
$U1 := U;$
$V0 := V1;$
$V1 := V;$
fin;

En sortie $R0 = pgcd(a, b)$, $U0 = u$ et $V0 = v$. En effet, on constate que lors de l'initialisation

$$U0a + V0b = R0$$

et

$$U1a + V1b = R1.$$

De plus si à l'entrée de la boucle on a ces relations alors on les a aussi à la sortie de la boucle. La première est facile a vérifier car pendant la boucle la nouvelle valeur de U0 est l'ancienne valeur de U1, la nouvelle valeur de V0 est l'ancienne valeur de V1, la nouvelle valeur de R0 est l'ancienne valeur de R1. Quand à la seconde relation il suffit de se référer aux valeurs de U ,V ,R calculées dans la boucle pour voir que $Ua + Vb = aU0 + bV0 - Q * (aU1 + bV1) = R0 - Q * R1 = R$ (constater ici qu'on a travaillé sur les anciennes valeurs de U0,U1,V0,V1). Compte tenu des affectations qui suivent on obtient la relation attendue. Cet algorithme se termine puisque le contenu positif ou nul de $R1$ décroît strictement.

Théorème 2.3.3 *(Théorème de Bezout) Deux nombres entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.*

Preuve : L'existence des nombres u et v lorsque a et b sont premiers entre eux découle immédiatement du théorème 2.3.2.

Réciproquement s'il existe u et v tels que $au + bv = 1$ alors tout diviseur de a et b divise 1, ce qui montre que a et b sont premiers entre eux.

Théorème 2.3.4 *(Lemme d'Euclide Gauss) Si c divise ab et si c est premier avec b alors c divise a.*

Preuve : Si c est premier avec b alors on peut trouver u et v tels que $uc+bv = 1$. Par suite $auc+abv = a$. Mais auc est divisible par c et abv aussi, donc a est divisible par c.

2.3.3 Résolution complète de $ua+vb = d$ (où $d = pgcd(a, b)$)

Supposons tout d'abord a et b premiers entre eux. On sait qu'il existe un couple (u_0, v_0) tel que $u_0a + v_0b = 1$. En existe-t-il d'autres? Si oui, trouver tous les couples (u, v) tels que $ua + vb = 1$.
Soit (u, v) un couple quelconque répondant à la question. Alors

$$a(u - u_0) + b(v - v_0) = 0.$$

Donc b divise $a(u - u_0)$, et puisque b est premier avec a, b divise $u - u_0$.
Par suite u est nécessairement de la forme $u = u_0 + kb$. Si bien que

$$akb + b(v - v_0) = 0$$

ou encore

$$v = v_0 - ka.$$

Ainsi tout couple (u, v) répondant à la question vérifie

$$u = u_0 + kb$$

$$v = v_0 - ka$$

pour un certain $k \in \mathbb{Z}$. D'autre part on vérifie immédiatement, que pour tout $k \in \mathbb{Z}$, le couple (u, v) défini précédemment convient.

Remarque : Existe-t-il une solution (u, v), où u et v sont petits en valeur absolue? Supposons $a > 0, b = 1$. Alors $u_0 = 0, v_0 = 1$ convient. On a bien entendu un résultat analogue pour $a = 1, b > 0$.
Supposons maintenant $a > 1, b > 1$. Puisque pour tout couple (u, v) qui convient on a

$$u = u_0 + kb$$

où (u_0, v_0) est une solution particulière et que réciproquement si u est de cette forme, il existe v tel que le couple (u, v) convienne, on peut supposer, quitte à faire la division euclidienne par $-b$ que cette solution particulière u_0 vérifie $0 \leq u_0 < b$. De plus il n'y a qu'une solution telle que u_0 soit dans cet intervalle. On ne peut pas avoir $u_0 = 0$ car alors $v_0 b$ vaudrait 1 ce qui est impossible puisque $b > 1$. Donc

$$0 < u_0 < b.$$

Pour v_0 nous avons alors

$$v_0 = \frac{1 - au_0}{b},$$

d'où

$$1/b - a < v_0 < 0,$$

ce qui donne

$$-a < v_0 < 0.$$

Exercice : Modifier cette démonstration pour montrer que u_0 peut être choisi tel que $0 \leq |u_0| \leq b/2$. Trouver alors un encadrement pour $|v_0|$.

Supposons qu'on veuille maintenant résoudre

$$ua + vb = d$$

où $d = pgcd(a, b)$.
Dans ces conditions on a $ua' + bv' = 1$ avec $a' = a/pgcd(a, b)$ et $b' = b/pgcd(a, b)$. Mais on sait qu'alors a' et b' sont premiers entre eux. On est donc ramené au problème précédent.

2.3.4 Plus petit commun multiple

Soient a et b deux entiers. Si l'un est nul, alors tous les multiples communs de a et b sont nuls. Sinon, posons $d = pgcd(a, b)$. Alors

$$a = k_1 d, b = k_2 d \quad avec\ pgcd(k_1, k_2) = 1.$$

Dans ces conditions, si m est un multiple commun de a et de b on a

$$m = \alpha k_1 d = \beta k_2 d,$$

soit

$$\alpha k_1 = \beta k_2,$$

donc k_1 divise βk_2, et étant premier avec k_2 il divise β. Si bien que

$$m = uk_1k_2d.$$

Ainsi tout multiple commun de a et de b est de la forme uk_1k_2d c'est-à-dire $uab/pgcd(a,b)$. Réciproquement tout nombre de cette forme est à la fois multiple de a et de b ($uk_1k_2d = uk_2a = uk_1b$). En particulier le plus petit commun multiple > 0 de a et b est obtenu pour $u = 1$ ou $u = -1$ suivant les signes de a et b, c'est $|ab|/pgcd(a,b)$.

Théorème 2.3.5 *Si a et b sont deux nombres entiers, il existe un plus petit entier ≥ 0 qui est multiple commun de a et de b. Cet entier sera noté $ppcm(a,b)$ et appelé le* **plus petit commun multiple** *de a et b. Si $a = 0$ ou $b = 0$ alors $ppcm(a,b) = 0$. Sinon, $ppcm(a,b) = |ab|/pgcd(a,b)$.*
Les multiples communs de a et b sont les multiples de $ppcm(a,b)$.

Remarque : ab est un multiple commun de a et b. Hormis le cas trivial où l'un des deux nombres est nul, peut-il se faire que $|ab| = ppcm(a,b)$? Du fait que dans ce cas $ppcm(a,b) = |ab|/pgcd(a,b)$, on peut dire que si $ab \neq 0$, $ppcm(a,b) = |ab|$ si et seulement si a et b sont premiers entre eux.

2.4 Les nombres premiers

2.4.1 Définition et premières propriétés

Définition 2.4.1 *Un nombre premier dans $\mathbb{Z}$ est un entier $n > 1$ dont les seuls diviseurs positifs sont 1 et n.*

Théorème 2.4.1 *Tout entier $n > 1$ est soit un nombre premier soit un produit de nombres premiers.*

Preuve : Le résultat est vrai pour 2. Supposons le vrai pour tout entier $< n$. Si n est non premier il a un diviseur positif $d > 1$, $d \neq n$. Donc $n = ab$ avec $2 \leq a < n$ et $2 \leq b < n$. En appliquant l'hypothèse de récurrence à a et b on obtient le théorème.

Théorème 2.4.2 *Le sous ensemble constitué par les nombres premiers est infini.*

Preuve : Supposons que ce sous ensemble soit fini. Notons alors $p_1, p_2, \cdots, p_n$ tous les nombres premiers. Soit $N = p_1 p_2 \cdots p_n + 1$. N n'est pas premier (il est plus grand que tous les p_i), et il n'est divisible par aucun des p_i, ce qui contredit le théorème précédent.

Proposition 2.4.1 *Si un nombre premier ne divise pas un entier, il est premier avec lui.*
Si un nombre premier p divise un produit d'entiers, il divise au moins l'un d'entre eux.

Preuve : Supposons que le nombre premier p ne divise pas l'entier a. Les seuls diviseurs positifs de p sont 1 et p. Donc le seul diviseur commun de p et a est 1.
Supposons que le nombre premier p divise le produit ab. Si p ne divise pas a alors p est premier avec a, donc d'après le lemme d'Euclide il divise b. Pour un produit de plus de deux entiers on raisonne par récurrence.

2.4.2 Décomposition en produit de nombres premiers

Théorème 2.4.3 *Tout entier $n > 1$ s'écrit de manière unique sous la forme*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où les α_i sont des entiers ≥ 1 et où les p_i sont des nombres premiers distincts tels que $p_i < p_{i+1}$.

Preuve : Nous avons déjà vu précédemment que la décomposition en nombre premier est toujours possible. Il nous reste à montrer l'unicité (résultat à admettre).

Une notation commode: Soit un entier $n > 1$. Pour tout nombre premier p, posons $\alpha_p = 0$ si p n'est pas présent dans la décomposition de n en facteurs premiers, et sinon, donnons à α_p la valeur de l'exposant de p dans cette décomposition de n en facteurs premiers. Avec ces notations on peut écrire

$$n = \prod_{p \ premier} p^{\alpha_p}.$$

Il faut comprendre ce produit qui semble porter sur une infinité de facteurs comme un produit fini n'impliquant que les facteurs distincts de 1.

2.4.3 Aspects algorithmiques

La détermination des nombres premiers est un problème important et difficile. Plus précisément il y a plusieurs problèmes distincts. Tout d'abord déterminer les nombres premiers plus petits qu'un nombre donné, c'est-à-dire construire une table; ensuite dire si un nombre donné est ou n'est pas premier; enfin, déterminer la décomposition en nombres premiers d'un nombre donné. Tous ces problèmes algorithmiques ont donné lieu à de longs développements et ne sont que partiellement résolus. Nous donnons ici un algorithme élémentaire pour construire des tables de nombres premiers, appelé le **crible d'Ératosthène**.

Pour avoir dans une table de résultats tous les nombres premiers $\leq n$, on écrit dans une table de départ et dans l'ordre habituel, tous les nombres de 2 à n. On itère jusqu'à épuisement de la table de départ l'action suivante: on met dans la table de résultats le premier nombre qui se trouve dans la table de départ et on supprime de cette dernière ce nombre ainsi que tous ses multiples.

2.4.4 Applications de la décomposition en facteurs premiers

Si a est un nombre entier > 1 on peut utiliser la décomposition de a en facteurs premiers pour caractériser les diviseurs de a.

Théorème 2.4.4 *Un nombre $b > 1$ divise le nombre $a > 1$ si et seulement si chaque nombre premier intervenant dans la décomposition de b intervient dans la décomposition de a affecté d'un exposant supérieur ou égal à celui qu'il a dans b. Ce qui peut s'écrire de la façon suivante: si*

$$a = \prod_{p \text{ premier}} p^{\alpha_p}$$

est la décomposition en facteurs premiers de a. Alors un nombre $b > 1$ divise a si et seulement si

$$b = \prod_{p \text{ premier}} p^{\beta_p}$$

où tous les β_p vérifient $\beta_p \leq \alpha_p$.

Exemple: Trouver tous les diviseurs de 360.

Soient a et b des nombres entiers > 1. Alors on peut utiliser la décomposition en facteurs premiers de a et de b pour calculer $pgcd(a, b)$ et $ppcm(a, b)$.

Théorème 2.4.5 *Soient a et b deux entiers > 1. Alors a et b sont premiers entre eux si et seulement si l'ensemble des nombres premiers présents dans la décomposition de a et l'ensemble des nombres premiers présents dans la décomposition de b sont disjoints.*

Preuve : Si a et b sont premiers entre eux, il ne peuvent pas avoir une puissance > 0 d'un même nombre premier p en commun dans leurs décompositions. Réciproquement, s'ils n'ont aucune puissance > 0 d'un même nombre premier en commun dans leurs décompositions, ils ne peuvent avoir en commun de diviseur > 1, car ce diviseur serait lui même divisible par un nombre premier qui devrait se retrouver dans les deux décompositions.

Théorème 2.4.6 *Soient*

$$a = \prod_{p \ premier} p^{\alpha_p} \ \ et \ b = \prod_{p \ premier} p^{\beta_p}$$

deux entiers > 1, décomposés en facteurs premiers. Alors

$$pgcd(a, b) = \prod_{p \ premier} p^{min(\alpha_p, \beta_p)}$$

et

$$ppcm(a, b) = \prod_{p \ premier} p^{max(\alpha_p, \beta_p)}.$$

Preuve : Pour le pgcd, on vérifie que

$$\prod_{p \ premier} p^{min(\alpha_p, \beta_p)}$$

est bien un diviseur de a et de b et que les quotients de a et de b par ce nombre sont premiers entre eux.
Pour le ppcm, puisque $a > 1$ et $b > 1$, $ppcm(a, b) = ab/pgcd(a, b)$. Compte tenu de l'expression déjà trouvée pour $pgcd(a, b)$ on trouve $ppcm(a, b)$ sous la forme indiquée.

Exemples: Prenons $a = 532$, $b = 246$. Alors

$$a = 2^2.7.19, \ \ b = 2.3.41, \ \ pgcd(532, 246) = 2,$$

$$ppcm(532, 246) = 4.7.19.3.41 = 65436.$$

2.5 Commentaires, compléments

2.5.1 Des exemples

Il est important de voir avant toute chose fonctionner les algorithmes et les autres notions sur des exemples concrets, notamment en ce qui concerne l'algorithme d'Euclide, l'algorithme d'Euclide étendu, le crible d'Erathostène, l'utilisation des décompositions en nombres premiers pour les calculs du pgcd, du ppcm, des diviseurs d'un nombre. Les représentations graphiques seront aussi très utiles à la bonne compréhension.

2.5.2 Compléments

Les congruences

En ce qui concerne les congruences, voici ce qu'il est dit dans le programme, dans la partie consacrée aux travaux pratiques:

La division euclidienne permet d'établir des compatibilités avec les opérations nécessaires pour les problèmes étudiés. Ceux-ci pourront être l'occasion de présenter et de mettre en œuvre la notion de congruence, au sujet de laquelle aucune connaissance spécifique ne peut être exigée.

Voici donc quelques résultats sur les congruences qu'on sera certainement amené à démontrer.
Considérons les nombres

$$\cdots \ -16 \ -10 \ -4 \ 2 \ 8 \ 14 \ 20 \ 26 \ \cdots$$

Le nombre 2 est le seul nombre de cet ensemble qui soit dans l'intervalle $[0, 6[$. Les éléments de cet ensemble sont tous les nombres y tels que

$$y = 6q + 2$$

c'est-à-dire, tous les nombres y dont la division euclidienne par 6 a pour reste 2.
Si x et y sont deux nombres de cet ensemble alors $y - x$ est un multiple de 6.

Plus généralement, si $n \geq 1$ et si $0 \leq r < n$, on cherche les éléments de $\mathbb{Z}$ dont la division euclidienne par n a pour reste r.

Théorème 2.5.1 *Les éléments de $\mathbb{Z}$ dont le reste de la division euclidienne par n est r sont les nombres de la forme*

$$x = nq + r.$$

Si x est un tel élément, les éléments y qui répondent à la question sont ceux pour lesquels $y - x$ est un multiple de n.
Il n'existe qu'un seul élément répondant à la question, qui soit ≥ 0 et $< n$, c'est r.

Il est donc équivalent de dire que x et y **ont le même reste** dans leur division euclidienne par n ou que $x - y$ **est un multiple de** n.

Définition 2.5.1 *Nous dirons que x est* **congru** *à y* **modulo** *n si x et y ont le même reste dans leur division euclidienne par n ou encore si $y - x$ est un multiple de n.*

Remarque 1 : La définition implique que si x est congru à y modulo n alors y est congru à x modulo n. On pourra donc dire que x et y sont congrus modulo n.
Remarque 2 : On trouve dans divers langages de programmation la notation

$$x \bmod n$$

pour désigner le seul élément $0 \leq r < n$ congru à x modulo n, c'est-à-dire le reste de la division de x par n.

La congruence est compatible avec l'addition et la multiplication:

Théorème 2.5.2 *Si x est congru à x_1 modulo n et si y est congru à y_1 modulo n alors $x + y$ est congru à $x_1 + y_1$ modulo n et xy est congru à x_1y_1 modulo n.*

Attention, le reste de la division par n d'une somme (respectivement d'un produit), n'est pas toujours la somme des restes (repectivement le produit des restes) de la division par n des termes.
Prendre par exemple $n = 5, x = 14, y = 12$. Dans ces conditions $x = 2n + 4$, $y = 2n + 2$, $x + y = 5n + 1$. Le reste 1 est différent de la somme $4 + 2$ des restes; ce qui est vrai c'est que ces deux nombres sont congrus modulo n.

La numération

Il est nécessaire aussi de *rappeler* quelques principes de numération. En particulier on peut indiquer la signification de l'écriture en base 10

$$9436 = 6 + 3 \times 10 + 4 \times 10^2 + 9 \times 10^3,$$

ou en base 2

$$101 = 1 + 0 \times 2 + 1 \times 2^2.$$

Plus généralement

Théorème 2.5.3 *Soit b un entier ≥ 2. Tout entier naturel $x > 0$ s'écrit d'une façon et d'une seule sous la forme*

$$x = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$$

où les nombres a_i vérifient $0 \leq a_i < b$, et où a_n est non nul.

Preuve : Les démonstrations de l'existence et de l'unicité du développement se font en utilisant l'algorithme d'Euclide.

Écriture : L'écriture en base b nécessite b symboles (**les chiffres**) $v_0, \cdots, v_{b-1}$ qui représentent les nombres entiers $0, \cdots, b-1$. Par exemple en base dix on utilise les chiffres $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, en base deux on utilise les chiffres $0, 1$, en base huit on utilise les chiffres $0, 1, 2, 3, 4, 5, 6, 7$, en base seize on utilise les chiffres $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$. Quand on travaille en général, et qu'on dispose de la décomposition $x = a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$, on écrit souvent le nombre x en base b sous la forme

$$x = (a_n a_{n-1} \cdots a_0)_b$$

en faisant l'abus qui consiste à noter de la même manière le nombre a_i de l'intervalle $[0, b-1]$ et le chiffre qui le représente.

Remarque 1 : L'écriture $(10 \cdots 0)_b$ (1 suivi de k symboles 0, représente le nombre b^k. L'écriture $(11 \cdots 1)_b$ (k symboles 1) représente le nombre $(b^k - 1)/(b-1)$.

Remarque 2 : Si on dispose de la table d'addition et de la table de multiplication des nombres à un chiffre en base b, on peut reproduire la technique habituelle qu'on connaît en base dix pour les opérations à la main. Sinon on peut transcrire en base dix et faire les opérations dans cette base, quitte à repasser en base b à la fin.

Remarque 3 : La comparaison des nombres développés en base b se fait de façon analogue à ce qu'on fait en base dix.

Des exemples de changements de bases sont proposés dans le chapitre suivant.

Chapitre 3

Quelques thèmes d'activités

3.1 Quelques exercices sur les changements de bases

Les notions concernant les changements de bases de numérations sont importantes, et sont utilisées fréquemment en informatique. Dès le début de la première année de DEUG, on en fait usage. Les thèmes choisis concernent des situations concrètes fort utiles: passage d'une écriture décimale à une écriture binaire, passage d'une écriture binaire à une écriture décimale, cas où une base est une puissance de l'autre (passage du binaire à l'octal ou à l'hexadécimal et réciproquement, utilisation de développements en base 10^n pour effectuer avec une calculette des opérations qui ne tiennent pas en mémoire. Nous donnons pour chaque thème un squelette permettant d'adapter à la classe des exercices correspondants.

3.1.1 Passage d'une écriture décimale à une écriture binaire

Données : le nombre $a > 0$ à traduire en binaire.
Sortie: le tableau A des digits binaires cherchés.

$Q := a;$
$R := 0;$
$I := 0;$
$Tant\ que\ Q \neq 0\ faire$
  $Debut$
    $A[I] := Q\ mod\ 2;$

$Q := Q\ div\ 2;$
$I := I + 1;$
$Fin;$

3.1.2 Passage d'une écriture binaire à une écriture décimale

(C'est l'occasion de présenter l'algorithme de Hörner. On pourra faire le rapprochement avec le calcul sur les polynômes).

$S := 0;$
$I := IMax;$
$Tant\ que\ I \geq 0\ faire$
$Debut$
$S := 2 * S + A[I];$
$I := I - 1;$
$Fin;$

3.1.3 Cas où une base est une puissance de l'autre

Le binaire, l'octal, l'hexadécimal

Exemple: Traduire le nombre écrit en binaire 1011101 en hexadécimal.
On découpe le nombre donné en blocs de 4 chiffres en partant de l'unité (en complétant éventuellement par des zéros) et on traduit chaque bloc de 4 chiffres binaires en un chiffre hexadécimal:

$$1011101 \to 0101\ 1101 \to 5\ D \to 5D.$$

Exemple: Traduire en binaire le nombre écrit en hexadécimal 6F.
Chaque chiffre haxadécimal est traduit par un bloc de 4 chiffres binaires.

$$6F \to 6\ F \to 0110\ 1111 \to 1101111.$$

Faire tenir sur une calculette des opérations sur des longs nombres (écriture en base 10^4 par exemple)

Exemple: faire la multiplication

$$39678472 \times 87752338.$$

Remarque: Les nombres étant écrits sous la forme

$$a_1 10^4 + a_0, b_1 10^4 + b_0$$

on peut se contenter de ne faire que 3 multiplications en utilisant la formule

$$(a_0 + a_1)(b_0 + b_1) = a_0 b_0 + a_1 b_1 + a_0 b_1 + a_1 b_0,$$

si bien que

$$a_0 b_1 + a_1 b_0 = (a_0 + a_1)(b_0 + b_1) - a_0 b_0 - a_1 b_1.$$

(méthode de Strassen)

3.2 Quelques exercices sur la divisibilité

Voici quelques situations concrètes d'utilisation de la divisibilité. Nous avons choisi trois thèmes: les clés de contrôle, la représentation des entiers en machine, les répartitions des termes d'une suite dans un tableau. Chaque thème donne lieu à des exercices dont nous donnons le squelette et qu'il convient, dans un travail ultérieur, d'adapter à la classe. Chaque exercice constitue au niveau d'une classe de terminale une séquence de travail assez longue. Aussi ces thèmes ne sont-ils pas prévus pour être tous traités.

3.2.1 Clés de contrôle

Dans la vie courante on est amené à manipuler des numéros d'identification, par exemple numéro I.N.S.E.E. (Institut National de la Statistique et de Etudes Economiques), numéros de comptes bancaires, numéros I.S.B.N. (International Standard Book Number), etc ... Ces numéros pouvant être assez longs, on les munit d'une clé qui permet de détecter (pas toujours) des erreurs de saisie éventuelles.

Numéro I.N.S.E.E.

Le numéro I.N.S.E.E. d'un individu est constitué de 15 chiffres. En lisant de gauche à droite, le premier est 1 ou 2 suivant qu'il s'agit d'un homme ou d'une femme. Les deux chiffres suivants désignent les deux derniers chiffres de l'année de naissance, les deux suivants le mois de naissance, les deux suivants le département, les trois suivants la commune de naissance, les trois suivants le numéro d'inscription sur le registre d'état civil, les deux derniers forment une clé K calculée de la manière suivante: désignons par A le nombre entier constitué par les 13 chiffres de gauche; soit r le reste de la division euclidienne de A par 97; on prend $K = 97 - r$.

a) Vérifiez pour votre numéro I.N.S.E.E.

b) Ecrivons A sous la forme

$$A = H \times 10^6 + L$$

avec

$$0 \leq L < 10^6.$$

Montrer que r est aussi le reste de la division euclidienne de $27 \times H + L$ par 97.

c) Soit A_1 le nombre constitué par un numéro I.N.S.E.E. (y compris la clé). Montrer que si un des chiffres de A_1 et un seul est erroné, l'erreur est détectée. Montrer que si deux chiffres consécutifs distincts sont permutés, l'erreur est détectée.

d) Donner un exemple d'erreur non détectée.

Clé de relevé d'identité bancaire (RIB)

Le relevé d'identité bancaire comporte de gauche à droite 5 chiffres pour le code de la banque, 5 chiffres pour le code du guichet, 11 chiffres pour le numéro de compte, 2 chiffres pour la clé. La clé K est calculée de la manière suivante: soit A le nombre constitué par les 21 chiffres de gauche; on calcule le reste r de la division euclidienne de $100 \times A$ par 97. On prend $K = 97 - A$.

a) Calculer la clé pour le relevé 14607 00052 05215075057 xx.

b) Comment mener le calcul avec une calculette?
(indication: écrire $100 \times A = H \times 10^{12} + M \times 10^6 + L$.)

c) Soit A_1 le nombre constitué par un RIB (y compris la clé). Montrer que si un des chiffres de A_1 et un seul est erroné, l'erreur est détectée. Montrer que si deux chiffres consécutifs distincts sont permutés, l'erreur est détectée.

Numéro I.S.B.N.

L'***I**nternational **S**tandard **B**ook **N**umber* utilise des mots de longueurs 10 constitués avec les chiffres $0, 1, ..., 9$ et le symbole X (qui représente le nombre 10); le symbole X ne sera utilisé, si nécessaire, que pour la clé.

Exemples: 2 84180 013 X, 2 84225 000 1, 0 471 62187 0, 0 12 163251 2.

Le premier chiffre représente le pays, un bloc de chiffres est attribué à un éditeur, un autre bloc est le numéro donné par l'éditeur, le dernier symbole est la clé, calculée de telle sorte que si $a_1a_2...a_{10}$ désigne un numéro I.S.B.N.

$$\sum_{i=1}^{10} ia_{11-i}$$

soit divisible par 11.

a) Vérifier les exemples donnés.

b) Montrer que si un chiffre (et un seul) est erroné, l'erreur est détectée.

c) Montrer que si deux chiffres distincts sont permutés, l'erreur est détectée.

d) Trouver toutes les valeurs de a et de b telles que $2842250ab1$ soit un code I.S.B.N. valide.

e) Pourquoi prendre la somme des ia_{11-i} et pas seulement la somme des a_i?

Le code UPC (universal product code)

Le code I.S.B.N. a le désavantage d'utiliser pour la clé un symbole "parasite" (le X). Ceci provient du fait que l'on travaille modulo 11. Peut-on faire une étude analogue en travaillant modulo 10? Voici le code UPC, utilisé avec les codes barres, qui est basé sur ce principe.
Le code UPC utilise des nombres de 12 chiffres $a_1 \cdots a_{12}$ (11 chiffres pour désigner un produit, et une clé), de telle sorte que

$$\sum_{i=0}^{5} 3a_{2i+1} + \sum_{i=1}^{6} a_{2i}$$

soit divisible par 10.

a) Calculer la clé si le nombre formé par les 11 chiffres de gauche est 35602387190.

b) Montrer que si un chiffre (et un seul) est erroné, l'erreur est détectée.

c) Montrer que, sauf cas particulier à déterminer, la permutation de deux chiffres successifs distincts est détectée (hélas il y a des cas particuliers; personne n'est parfait!).

3.2.2 Représentation en machine des entiers

Position du problème

On veut **représenter** des nombres entiers en machine. Supposons par exemple que nous ayons **un octet** pour le faire. Avec un octet on dispose de $2^8 = 256$ écritures différentes, ces écritures pouvant être considérées comme les développements binaires des entiers de l'intervalle $\{0..255\}$. Comme on veut répartir équitablement les entiers que l'on représente entre des entiers positifs et des entiers négatifs, on décide de s'intéresser aux 256 entiers de l'intervalle $\{-128..127\}$. Il convient donc d'établir une bijection qui permette des calculs commodes, entre l'intervalle $\{-128..127\}$ des entiers qu'on veut représenter, et l'intervalle $\{0..255\}$ des représentations. En résumé, à tout entier x de l'intervalle $\{-128..127\}$ on va faire correspondre sa représentation $R(x)$ qui sera un entier de l'intervalle $\{0..255\}$. En outre comme $R(x)$ doit être stocké dans la mémoire d'une machine, on regardera plus spécialement les propriétés du développement binaire (sur un octet) de $R(x)$.

Représentation dite en "complément à 2"

Rappelons que si n est un entier, $n \bmod 256$ est le reste de la division de n par 256 ou encore l'unique entier m tel que $0 \leq m \leq 255$ et m congru à n modulo 256.

Notons I l'intervalle $\{-128..127\}$ et J l'intervalle $\{0..255\}$. Soit R l'application de I dans J définie par

$$R(x) = x \bmod 256.$$

a) Montrer que R est une application bijective.

b) Calculer $R(0), R(100), R(127), R(-1), R(-100), R(-128)$. Donner les développements binaires des résultats obtenus.

c) Calculer $R(x)$ en fonction de x.

d) Déterminer l'image par R de l'ensemble des $x \geq 0$ de I ainsi que l'image par R de l'ensemble des $x < 0$ de I. Comment reconnaître sur le développement binaire de $R(x)$ le signe de x?

e) On suppose que $x \in I \setminus \{-128, 0\}$. Calculer $R(-x)$ en fonction de $R(x)$. On constatera que $R(-x) = (255 - R(x)) + 1$. En déduire un algorithme simple permettant de calculer le développement binaire de $R(-x)$ à partir de celui de $R(x)$ (algorithme dit de complémentation à 2).

f) Pour écrire en binaire la représentation $R(x)$ d'un entier x de l'intervalle I on applique la stratégie suivante:

- Si $x \geq 0$, on développe x en binaire.
- Si $x < 0$, on développe $-x$ en binaire et on applique l'algorithme de complémentation à 2 (cf. e)).

Appliquer cette méthode pour calculer l'écriture binaire de $R(18)$, $R(-20)$.

Addition des entiers et représentation

Soit T l'application de $\mathbb{N}$ dans $\{0..255\}$ qui à tout $n = \sum_{j=0}^{\infty} a_j 2^j$ fait correspondre $T(n) = \sum_{j=0}^{7} a_j 2^j$ (troncature limitée aux 8 premiers bits).

a) Quel est le lien entre n mod 256 et $T(n)$?

b) Montrer que si $x_1, x_2, x_1 + x_2$ sont des éléments de I alors

$$R(x_1 + x_2) = (R(x_1) + R(x_2)) \bmod 256 = T(R(x_1) + R(x_2)).$$

Décrire un algorithme qui permette de calculer le développement binaire de $R(x_1 + x_2)$ connaissant ceux de $R(x_1)$ et de $R(x_2)$.

c)***Il est bien entendu que l'addition de deux éléments de I ne sera valide que si le résultat est aussi dans I. Comme la machine ne connaît que les représentants des nombres qu'on additionne, nous mettons en place ici une méthode (bien adaptée aux circuits électroniques) qui opère sur les représentations et permette à la fois de détecter si l'opération d'addition est valide et de calculer dans ce cas le résultat.

Nous allons prouver la pertinence de l'algorithme suivant:

Algorithme: Soient x_1 et x_2 deux éléments de I. Soit C le **carry**, retenue du 8^{e} bit vers l'exterieur, et α la retenue du 7^{e} bit vers le 8^{e}, obtenus en faisant l'addition $R(x_1) + R(x_2)$. On pose $V = C \oplus \alpha$.

- Si $V = 0$ l'addition est valide et $R(x_1+x_2)$ s'obtient en faisant en binaire l'addition de $R(x_1)$ avec $R(x_2)$ et en négligeant tout débordement au delà du huitième bit (cf. b)).
- Si $V = 1$ l'addition n'est pas valide.

c1) Supposons $0 \leq x_1 \leq 127$ et $0 \leq x_2 \leq 127$. Examiner les deux cas $x_1 + x_2 \leq 127$ (opération valide) et $x_1 + x_2 > 127$ (opération invalide), et dans chaque cas calculer C, α, V.

c2) Supposons $0 \leq x_1 \leq 127$ et $-128 \leq x_2 < 0$ (opération toujours valide). On examinera suivant les valeurs possibles de $R(x_1) + R(x_2)$ quelles sont les valeurs possibles de C, α, V.

c3) Supposons $-128 \leq x_1 < 0$ et $-128 \leq x_2 < 0$. Examiner les deux cas $x_1 + x_2 < -128$ (opération invalide) et $x_1 + x_2 \geq -128$ (opération valide), et dans chaque cas calculer C, α, V. (Indication: pour calculer α on pourra regarder si l'addition des deux nombres de 7 bits $(R(x_1)-128)$ et $(R(x_2)-128)$ a une retenue vers le huitième bit.)

c4) En conclure la validité de l'algorithme annoncé.

Extension des résultats

Que se passe-t-il si on dispose pour représenter les entiers de 2 octets (ou plus)?

3.2.3 Répartitions de termes d'une suite dans un tableau

Correspondance d'indices

Soient $u_1, u_2, \cdots, u_{3007}$ les termes d'une suite finie. On veut ranger ces nombres dans un tableau T_1 ayant 97 lignes et 31 colonnes en prenant les termes dans l'ordre et en remplissant successivement toutes les lignes à partir de la première colonne. Notons $a_{i,j}$ l'élément de la suite qui se trouve rangé à la ligne i et à la colonne j.
Dans quelle ligne i et quelle colonne j se trouve rangé le terme u_n?

Répartition dans deux tableaux

On transfère le tableau T_1 précédent dans un tableau T_2 ayant 31 lignes et 97 colonnes en parcourant les deux tableaux ligne par ligne à partir de la première colonne.
Montrer que deux éléments d'une même colonne dans T_1 sont rangés dans 2 colonnes différentes de T_2.

3.3 Quelques exercices autour du chiffrement affine

3.3.1 Principe du chiffrement affine

Les 26 lettres de l'alphabet étant numérotées de 0 à 25, on opère désormais sur l'ensemble $I = \{0, .., 25\}$. On fixe deux éléments a et b de I, et on considère la fonction $E_{(a,b)}$ de I dans I définie par

$$E_{(a,b)}(x) = (ax + b) \ mod \ 26$$

(où $u \ mod \ v$ désigne le reste de la division euclidienne de u par v). On espère utiliser $E_{(a,b)}$ comme **fonction de chiffrement** associée à la **clé** (a, b). Ainsi, un texte clair étant donné, le texte chiffré sera obtenu en transformant successivement toutes les lettres du texte clair par la fonction $E_{(a,b)}$. Encore faut-il s'assurer que cette fonction transforme bien deux lettres distinctes en deux lettres distinctes (sinon ça ne vas pas!) . Ceci n'est réalisé que pour certains couples (a, b). C'est ce que nous étudions dans le paragraphe suivant.

3.3.2 Les clés - Les fonctions de chiffrement

a) Calculer $E_{(7,4)}(8)$, $E_{(8,3)}(13)$, $E_{(8,3)}(0)$.

b) Montrer que si a n'est pas premier avec 26, il existe un élément x de I distinct de 0 tel que $E_{(a,b)}(x) = E_{(a,b)}(0)$. La fonction $E_{(a,b)}$ n'est donc pas bijective.

c) Montrer que si a est premier avec 26 alors $E_{(a,b)}$ est bijective.

d) Montrer que si (a_1, b_1) et (a_2, b_2) sont deux couples distincts (où a_1, b_1, a_2, b_2 sont des éléments de I) alors $E_{(a_1,b_1)} \neq E_{(a_2,b_2)}$.

e) Trouver tous les éléments de I premiers avec 26. Les clés seront les couples (a, b) où a est un élément de I premier avec 26 et b un élément quelconque de I. Combien a-t-on de clés (et donc de fonctions de chiffrement distinctes)?

Remarque: Ce nombre est trop petit pour que ce système cryptographique puisse servir réellement.

3.3.3 Fonctions de déchiffrement

a) Trouver z dans I et k dans $\mathbb{Z}$ tels que $7z + 26k = 1$.

b) Trouver z dans I tel que $E_{(7,4)}(z) = 5$.

c) Si (a, b) est une clé, nous avons vu que la fonction de chiffrement $E_{(a,b)}$ est bijective. Appelons $D_{(a,b)}$ la fonction réciproque de $E_{(a,b)}$ (**fonction de déchiffrement**).
Montrer qu'il existe un élément a' de I tel que $D_{(a,b)}$ soit définit sur I par

$$D_{(a,b)}(y) = \Big(a'(y - b) \; mod \; 26\Big).$$

On indiquera comment calculer a'.

3.3.4 Cryptanalyse

Le cryptanalyste qui voit passer un texte chiffré, essaye de retrouver la clé (a, b) qui lui est inconnue. Ici, le nombre de clés étant faible une façon de faire est de tester toutes les clés, jusqu'à trouver un texte compréhensible.
Voici une attaque plus astucieuse: compte tenu des fréquences d'apparition des lettres dans un texte, on peut faire des hypothèses sur les images de deux lettres, et à partir de là déterminer une clé probable qu'il ne reste plus qu'à essayer. Si on n'a pas trouvé la bonne clé on recommence avec d'autres hypothèses.
Ceci suppose qu'on sache résoudre le problème suivant: Trouver (a, b) connaissant $E_{(a,b)}(x_1)$ et $E_{(a,b)}(x_2)$ où x_1 et x_2 sont deux éléments connus de I.

a) On suppose que la clé (a, b) est telle que $E_{(a,b)}(8) = 20$ et $E_{(a,b)}(12) = 2$.
Montrer qu'il existe k tel que $4a + 26k = 8$, ou encore $2a + 13k = 4$.
Déterminer tous les couples (a, k) avec $a \in I$ vérifiant la condition précédente.
Trouver les clés (a, b) possibles.

b) Reprendre la question a) avec $E_{(a,b)}(15) = 17$ et $E_{(a,b)}(2) = 4$.

3.4 Une idée de la cryptographie à clé publique: Kid-RSA

Cet exemple indiqué à des fin pédagogiques par Neil Koblitz donne une idée de ce que peut être la cryptographie à clé publique. Évidemment il n'est pas réaliste dans la mesure où il est élémentairement cassable.

Les lettres $A, B, \cdots, Z$ sont représentées par les nombres $0, 1, \cdots, 25$. **A**lice choisit 4 entiers ≥ 3 notés a, b, a', b' et calcule successivement

$$M = ab - 1,$$
$$e = a'M + a,$$
$$d = b'M + b,$$
$$n = \frac{ed - 1}{M}.$$

Alice rend public (dans un annuaire par exemple) le couple (n, e) (sa clé publique) et maintient d secret (sa clé privée).

L'utilisation du système se fait de la façon suivante: si **B**ob désire envoyer un message à **A**lice, il chiffre successivement toutes les lettres de ce message en faisant correspondre à tout nombre m compris entre 0 et 25 le nombre $c = em \ mod \ n$.

a) Montrer que $n > 25$. Pourquoi est-il souhaitable qu'il en soit ainsi? Montrer que e et n sont premiers entre eux.

b) Comment **A**lice peut elle récupérer simplement m lorsqu'elle a reçu c?

c) Les espions **D**enis, **S**uzanne et **T**homas écoutent la ligne de communication entre **A**lice et **B**ob et disposent donc de c. Comment peuvent-ils attaquer le système et découvrir m?

d) Utiliser ce système pour signer un message.

3.5 Exemples sur les codes correcteurs d'erreurs

3.5.1 Un code correcteur de Hamming

Ici on se propose non plus seulement de détecter, mais de corriger une erreur éventuelle. Considérons les nombres de 10 chiffres (numéros de téléphone par exemple) $a_1a_2\cdots a_{10}$ où les a_i peuvent prendre les valeurs $0, 1, \cdots, 9$. On rajoute une clé constituée de deux chiffres $a_{11}a_{12}$ où a_{11} et a_{12} peuvent prendre les valeurs $0, 1, \cdots, 9$ et aussi la valeur X, représentant le nombre 10. La clé est calculée de telle sorte que

1) a_{11} soit le reste de la division de

$$\sum_{i=1}^{10} a_i$$

par 11,

2) a_{12} soit le reste de la division de

$$\sum_{i=1}^{10} ia_i$$

par 11.

a) Calculer la clé pour le numéro 0491413940.

b) On part d'un numéro muni de sa clé $a_1a_2\cdots a_{12}$. On se propose de montrer que si en communiquant ce numéro on fait **une erreur sur un chiffre** (et pas plus), on peut reconstituer le bon numéro.

Montrer que si l'erreur est faite sur un a_i avec $1 \leq i \leq 10$ alors aucune des relations 1) et 2) n'est vérifiée.

Montrer que si l'erreur est faite sur a_{11} la relation 1) n'est pas vérifiée, mais la relation 2) l'est.

Montrer que si l'erreur est faite sur a_{12} la relation 1) est vérifiée mais pas la relation 2).

Montrer qu'on peut corriger l'erreur. Indiquer comment.
Exemple: Soit le numéro 049132900000. Vérifier que ce numéro n'est pas correct. En supposant qu'un seul chiffre soit faux, retrouver le bon numéro.

3.5.2 ***Impossibilité de réaliser une correction du type précédent uniquement avec les chiffres décimaux

Le seul ennui du codage précédent est la présence éventuelle dans la clé du symbole "parasite" X. Mais on va voir qu'avec une clé de deux chiffres on ne peut pas se contenter des chiffres décimaux.

Soit E l'ensemble des nombres de dix chiffres $a_1a_2\cdots a_{10}$ où les a_i sont des chiffres décimaux habituels. Soit F l'ensemble des nombres de 12 chiffres décimaux.

a) Quel sont les nombres d'éléments de E et de F?

Si $x = x_1x_2\cdots x_{10}$ est un élément de E on calcule à partir de x une clé $K(x) = x_{11}x_{12}$ formée de 2 chiffres décimaux. Notons f l'application de E dans F qui à x associe $f(x) = x_1x_2\cdots x_{10}x_{11}x_{12}$ et $C = f(E)$ l'image de E.

b) Quel est le nombre d'éléments de C?

Si y est un élément de C on note B_y l'ensemble formé de y ainsi que de tous les éléments obtenus à partir de y en modifiant un (et un seul) chiffre de y.

c) Quel est le nombre d'éléments de B_y? Montrer qu'il existe au moins 2 éléments distincts z_1, z_2 dans C tels que $B_{z_1} \cap B_{z_2} \neq \emptyset$.

Si $t \in B_{z_1} \cap B_{z_2}$ il est impossible de savoir si t provient d'une erreur faite sur z_1 ou d'une erreur faite sur z_2. Cette obstruction montre qu'on ne peut pas réaliser un code correcteur du type de l'exemple précédent avec uniquement des digits décimaux. En essayant de faire ce même calcul sur l'exemple précédent (avec 11 digits), on verra évidemment que cette obstruction n'a pas lieu, mais que "ça passe juste".

3.6 Commentaires et solutions

3.6.1 Les changements de bases

Exercice : montrer que l'entier $(a_n\cdots a_0)_b$ ou $a_n \neq 0$ appartient à l'intervalle $[b^n, b^{n+1}[$.

Solution :

$$1 \times b^n \leq a_n \times b^n + \cdots + a_0 \leq (b-1)b^n + (b-1)b^{n-1} + \cdots + (b-1).$$

La somme de droite vaut

$$(b-1)(b^n + \cdots + 1) = b^{n+1} - 1.$$

Donc

$$b^n \leq (a_n\cdots a_0)_b < b^{n+1}.$$

Passage d'une écriture décimale à une écriture binaire : Dans l'algorithme décrit, $Q \ mod \ 2$ est le reste de la division euclidienne de Q par 2 et $Q \ div \ 2$ en est le quotient.

On peut faire tourner l'algorithme sur un exemple:

Q	I	$A[I]$
$a = 19$	0	1
9	1	1
4	2	0
2	3	0
1	4	1
0		

Ainsi l'entier $(19)_{10}$ s'écrit $(10011)_2$ en base 2.

Quant à l'algorithme, on constate qu'au début on a

$$Q = a, I - 1 = -1,$$

donc

$$2^I Q + \sum_{j=0}^{I-1} A[j]2^j = a.$$

Si cette dernière relation est vraie en entrée de boucle, puisque

$$Q = 2 * (Q \ div \ 2) + (Q \ mod \ 2)$$

alors après la première instruction de la boucle

$$a = 2^{I+1} * (Q \ div \ 2) + A[I]2^I \sum_{j=0}^{I-1} A[j]2^j$$

et puisqu'on met $Q \ div \ 2$ dans Q et $I+1$ dans I, la relation est encore vraie en sortie de boucle. Or en sortie de boucle $Q = 0$, donc $\sum_{j=0}^{I-1} A[j]2^j = a$, ce qui prouve que le tableau A contient le développement binaire de a.

Pour les petits nombres on peut chercher la plus grande puissance de 2 qui soit $\leq a$ et soustraire cette puissance à a. On réitère le procédé jusqu'à un nombre nul.
Exemple: $a = 87$.

$a = 2^6 + 23,\ 23 = 2^4 + 7,\ 7 = 2^2 + 3,\ 3 = 2 + 1$
Donc

$$a = 1 \times 2^6 + 0 \times 2^5 + 1 \times 2^4 + 0 \times 2^3 + 1 \times 2^2 + 1 \times 2 + 1 = (1010111)_2.$$

Utilisation de la base 2 pour accélérer le calcul de x^n.

En calculant directement $x.x\cdots.x$ on fait $n-1$ multiplications. Si on décompose n en base 2 on obtient

$$n = a_k 2^k + \cdots + a_1 2 + a_0.$$

Alors

$$x^n = x^{a_k 2^k + \cdots + a_1 2 + a_0} = x^{a_0} \times (x^2)^{a_1} \times \cdots \times ((x^{2^{k-1}})^2)^{a_k}.$$

Il y a donc au maximum $k-1$ carrés à effectuer de proche en proche et au maximum $k-1$ autres produits, donc au plus $2(k-1)$ multiplications.
Par exemple si $n = 15$ alors on calcule x^2 puis $x^4 = (x^2)^2$ puis $x^8 = (x^4)^2$ et enfin $x^{15} = x \times x^2 \times x^4 \times x^8$, soit 6 multiplications. Remarquons qu'une décomposition astucieuse de 15 en $6+9$ permet de ne faire que 5 multiplications.

Passage d'une écriture binaire à une écriture décimale

Si $n = a_k 2^k + \cdots + a_0$, il suffit de calculer cette somme de manière "habituelle" pour avoir le développement décimal. Ce qui nous permet d'avoir le résultat, c'est bien sûr qu'on utilise les notations et les tables d'opérations du calcul décimal.
Le calcul peut être fait de manière astucieuse (surtout si ce calcul doit être programmé sur une machine) en utilisant l'algorithme de Hörner proposé, qui consiste à écrire le calcul sous la forme

$$n = (\cdots((a_n \times 2 + a_{n-1}) \times 2 + a_{n-2})\cdots) \times 2 + a_0.$$

Par exemple si $n = (10011)_2$ alors on calcule

$$n = ((((1 \times 2) + 0) \times 2 + 0) \times 2 + 1) \times 2 + 1,$$

et comme on calcule en base dix, on obtient le résultat 19 en base dix. Quand on calcule "à la main" sur des petits nombres, il est plus facile d'additionner directement les puissances de 2. Ainsi, dans notre exemple, $n = 2^4 + 2 + 1 = 19$.

Dans l'algorithme donné, on peut constater que

$$S + \sum_{J=0}^{I} A[J]2^J$$

a la même valeur à l'entrée et à la sortie de la boucle. Au début $S = 0$ $I = IMax$, donc cette valeur est le nombre n donné dans le tableau A par son développement binaire. À la fin du programme on a $S = n$, où S est un nombre entier qu'on peut faire désormais afficher en décimal.

Cas où une base est une puissance d'une autre

Ce cas est extrêmement important pour diverses applications, dont des applications à l'informatique. De plus dans ce cas, la traduction se fait très facilement.

Exemple du passage de l'écriture d'un nombre en base 2 à son écriture en base 8. Si en base 2 l'entier n s'écrit $(a_n a_{n-1} \cdots a_1 a_0)_2$, c'est que $n = a_n 2^n + a_{n-1}2^{n-1} + \cdots + a_1 2 + a_0$. Tout groupement de 3 termes consécutifs de la forme

$$a_{3i+2}2^{3i+2} + a_{3i+1}2^{3i+1} + a_{3i}2^{3i}$$

est égal à

$$(a_{3i+2}2^2 + a_{3i+1}2 + a_{3i})8^i.$$

De plus

$$0 \leq a_{3i+2}2^2 + a_{3i+1}2 + a_{3i} \leq 7.$$

Donc si l'écriture de n en base 8 est $(b_p b_{p-1} \cdots b_1 b_0)_8$, le terme b_i est égal à $a_{3i+2}2^2 + a_{3i+1}2 + a_{3i}$ d'après l'unicité de l'écriture dans une base donnée.
Pour écrire par exemple $(10010101110101)_2$ en base 8 on partage les chiffres en paquets de 3 à partir de la droite:

10 010 101 110 101.

Chaque paquet donne un digit octal

2 2 5 6 5,

donc le nombre écrit en octal est $(22565)_8$.

Exemple du passage de l'écriture d'un nombre en base 8 à son écriture en base 2. Si le nombre s'écrit $n = (b_p b_{p-1} \cdots b_1 b_0)_8$, c'est que $n = b_p 2^{3p} + b_{p-1}2^{3(p-1)} +$

$\cdots + b_1 2^3 + b_0$ avec $0 \leq b_i \leq 7$. Donc $b_i = (xyz)_2$ et $b_i 2^{3i} = x2^{3i+2} + y2^{3i+1} + z2^{3i}$. En remplaçant chaque b_i par son développement en base 2 et en concaténant tous les résultats on obtient le développement de n en base 2.
Par exemple si $n = (520761)_8$ alors en base 2 on obtient 101 010 000 111 110 001, c'est-à-dire $n = (101010000111110001)_2$.

Exemple de l'utilisation d'une base 10^m pour faire avec une calculette des opérations sur de longs nombres. Par exemple pour obtenir la valeur exacte de $\Pi = 39678472 \times 8752338$, on travaille en base 10^4, ce qui permet d'écrire

$$\Pi = (3967 \times 10^4 + 8472)(875 \times 10^4 + 2338),$$

puis la suite de calculs

$$\Pi = (3967 \times 875)10^8 + (3967 \times 2338 + 8472 \times 875)10^4 + (8472 \times 2338),$$

$$\Pi = 3471125 \times 10^8 + 16687846 \times 10^4 + 19807536,$$

$$\pi = 347 \times 10^12 + (1125 + 1668) \times 10^8 + (7846 + 1980) \times 10^4 + 7536,$$

$$\Pi = 347\ 2793\ 9826\ 7536.$$

Remarquons qu'on peut de la manière indiquée ne calculer que 3 produits au lieu de 4, mais cette façon de faire a plutôt une importance théorique que pratique.

3.6.2 La divisibilité, les congruences

Travail préliminaire sur la congruence modulo 97

Exercice : Montrer que 97 est un nombre premier. Montrer que si $1 \leq y \leq 9$ et si n est un entier, les nombres $y10^n$ et 97 sont premiers entre eux. Prouver que si $n = (a_5 a_4 \cdots a_0)_{10}$ alors n et $a_0 + 10a_1 + 3a_2 + 30a_3 + 9a_4 - 7a_5$ ont le même reste dans leur division par 97.

Solution : On peut établir la table des nombres premiers jusqu'à 100 par l'algorithme du crible.
97 étant premier il suffit de montrer que 97 ne divise pas $y10^n$. Les seuls diviseurs premiers de $y10^n$ sont les diviseurs premiers de y donc des nombres ≤ 9 et les diviseurs premiers de 10^n c'est-à-dire 2 et 5. Le nombre 97 ne figure pas parmi eux.
Il suffit d'appliquer la compatibilité de la congruence modulo 97 avec l'addition et la multiplication pour conclure, en remarquant que 100 est congru à

3 modulo 97, 1000 est congru à 30 modulo 97, 10000 est congru à 9 modulo 97 et 100000 est congru à 90 modulo 97, ou encore à -7.

Numéro I.N.S.E.E.

a) Il suffit de calculer.

b) Si $A = 10^6 H + L$ la compatibilité de la congruence modulo 97 avec l'addition et la multiplication permet de dire que si a est congru à 10^6 modulo 97 alors A et $aH + L$ ont le même reste dans leur division par 97. Or 10^6 est congru à 27 modulo 97.

c) Pour vérifier la cohérence de A_1 on peut procéder de la manière suivante: on écrit que $A_1 = 100A + K$, puis on pose $A_2 = A + K$ et on vérifie que A_2 est un multiple de 97 ($A_2 = 97q + r + 97 - r$).
Si l'un des chiffres de A_1 est modifié alors A_2 devient un nombre A_2' de telle sorte que $|A_2' - A_2| = a10^n$ où $1 \leq a \leq 9$. En utilisant l'exercice du paragraphe précédent on en conclut que $|A_2' - A_2|$ n'est pas congru à 0 modulo 97, et donc A_2' et A_2 ne sont pas congrus modulo 97. Le calcul de cohérence précédent produit alors un A_2' qui n'est pas divisible par 97.
Si deux chiffres **consécutifs distincts** sont permutés, une étude des trois cas: les deux chiffres sont dans la clé, un chiffre est dans la clé l'autre non, aucun des chiffres n'est dans la clé, montre que dans tous les cas

$$|A_2' - A_2| = |(xy)_{10} - (yx)_{10}|10^n = a10^n$$

où $1 \leq a \leq 81$ (le maximum pour $|(xy)_{10} - (yx)_{10}|$ est obtenu pour $90 - 09$). Par un raisonnement analogue au précédent on conclut que A_2' et A_2 ne sont pas congrus modulo 97 et donc A_2' n'est pas divisible par 97.

d) Ajouter par exemple un multiple de 97 à A.

Clé R.I.B.

Ce problème est à peu près identique au précédent.

b) on pose $100A = H \times 10^{12} + M \times 10^6 + L$ et on constate que 10^6 est congru à 27 modulo 97 et que 10^{12} est congru à 50 modulo 97. Donc r est le reste de la division euclidienne de

$$50 \times H + 27 \times M + L$$

par 97.

c) Dans ce cas,

$$A_1 = 100A + 97 - r = 97q + r + 97 - r = 97(q+1),$$

c'est-à-dire que A_1 est un multiple de 97. À partir de là on refait les raisonnements du problème précédent.

Numéro I.S.B.N.

a) Remarquons que $a_{10} = \sum_{i=1}^{9} ia_i$. Ceci simplifie un peu le calcul de la clé.

b) Soit A un numéro valide. Appelons A_1 le nombre $\sum_{i=1}^{10} ia_{11-i}$ obtenu à partir des chiffres de A. On sait que A_1 est divisible par 11. Si un chiffre de A est modifié, on obtient alors A' dont le nombre associé A'_1 vérifie

$$|A'_1 - A_1| = ia$$

où $0 \leq i \leq 10$, $1 \leq a \leq 9$. Le nombre ia est premier avec 11, donc A'_1 n'est pas divisible par 11, ce qui permet de détecter l'erreur.

c) Si deux chiffres distincts sont permutés, par exemples ceux d'indices i et j, le nombre A_1 devient A'_1 et

$$A'_1 - A_1 = i(a_j - a_i) + j(a_i - a_j) = a(i-j),$$

où $a = a_j - a_i$. On a $1 \leq |a| \leq 9$ et $1 \leq |i-j| \leq 9$. Donc $A'_1 - A_1$ n'est pas divisible par 11 et A'_1 n'est pas divisible par 11.

d) On cherche a et b tels que $2842250ab1$ soit un code I.S.B.N. valide. Cela revient à chercher a et b tels que

$$1 + 2b + 3a + 5 \times 5 + 6 \times 2 + 7 \times 2 + 8 \times 4 + 9 \times 8 + 10 \times 2$$

soit un multiple de 11 ou encore on cherche a et b tels que $3a + 2b$ soit un multiple de 11 avec $0 \leq a \leq 9$ et $0 \leq b \leq 9$. On remarque que $0 \leq 3a + 2b \leq 45$, donc on cherche les solutions a et b parmi les couples tels que $3a + 2b = 11k$ et $k = 0, 1, 2, 3, 4$.
Pour $k = 0$ on a un couple qui convient $a = 0$, $b = 0$.
Pour $k = 1$, $3a + 2b = 11$, donc a est impair et on trouve les couples suivants qui conviennent: $a = 1, b = 4$, $a = 3, b = 1$.

Pour $k = 2$, $3a + 2b = 22$, donc a est pair, et on trouve les couples suivants qui conviennent: $a = 2, b = 8$, $a = 4, b = 5$, $a = 6, b = 2$.
Pour $k = 3$, $3a + 2b = 33$, donc a est impair et on trouve les couples suivants qui conviennent: $a = 5, b = 9$, $a = 7, b = 6$, $a = 9, b = 3$.
Pour $k = 4$, $3a + 2b = 44$, il n'y a aucune solution valide.

e) La simple somme des chiffres aurait permis de détecter une erreur mais pas une permutation de deux chiffres distincts.

Le code U.P.C.

a) la clé associée au nombre 35602387190 est le nombre K compris entre 0 et 9 tel que $3(3+6+2+8+1+0)+(5+0+3+7+9+K)$ soit divisible par 10, c'est-à-dire tel que $4 + K$ soit divisible par 10. Donc $K = 6$.

b) Si un chiffre du nombre $A = a_1 a_2 \cdots a_{12}$ est modifié, la somme $A_1 = \sum_{i=0}^{5} 3a_{2i+1} + \sum_{i=1}^{6} a_{2i}$ associée à A est modifiée en A_1' de telle sorte que $|A_1' - A_1| = a$ ou que $|A_1' - A_1| = 3a$ avec $1 \leq a \leq 9$. Dans chacun de ces cas $A_1' - A_1$ n'est pas divisible par 10 et donc A_1' n'est pas divisible par 10 ce qui permet de détecter l'erreur.

c) Si le chiffre a_{2i} est permuté avec a_{2i+1}, la somme A_1 est transformée en A_1' de telle sorte que

$$A_1' - A_1 = a_{2i+1} - a_{2i} + 3(a_{2i} - a_{2i+1}).$$

Donc

$$A_1' - A_1 = 2(a_{2i} - a_{2i+1}).$$

En dehors des cas où $|a_{2i} - a_{2i+1}| = 5$, $A_1' - A_1$ n'est pas divisible par 10 donc l'erreur est détectée.

Représentation des entiers en machine

Représentation en complément à 2

a) Si x et y éléments de I ont le même reste dans leur division par 256 alors $x - y$ est un multiple de 256, donc $y = x + 256k$ ce qui n'est possible que si $x = y$. Donc deux éléments distincts ont deux images distinctes. De plus I et J ont le même nombre d'éléments, donc R est bijective.

b) $R(0) = 0 = (00000000)_2$; $R(100) = 100 = (01100100)_2$; $R(127) = 127 = (01111111)_2$; $R(-1) = 255 = (11111111)_2$; $R(-100) = 156 = (10011100)_2$; $R(-128) = 128 = (10000000)_2$

c) Si $x \geq 0$ alors $x = 0 \times 256 + R(x)$ et $R(x) = x$. Si $x < 0$ alors $x = (-1) \times 256 + R(x)$, et $R(x) = x + 256$.

d) Si $0 \leq x \leq 127$ alors $R(x) = x$, ce qui prouve que l'image de l'ensemble des éléments positifs de I est $\{0..127\}$. Comme R est une bijection, l'image de l'ensemble des éléments strictement négatifs de I est $\{128..255\}$. Le développement binaire de 128 est $(10000000)_2$. Par suite le développement binaire de $R(x)$ a son "bit de poids fort" égal à 1 si $x < 0$ et son bit de poids fort égal à 0 si $x \geq 0$.

e) Si $x < 0$ alors $-x > 0$ donc $R(-x) = -x$. De plus $R(x) = 256 + x$, donc $R(-x) = 256 - R(x)$.
Si $x > 0$ alors $-x < 0$ donc $R(-x) = 256 - x$, c'est-à-dire $R(-x) = 256 - R(x)$.
Dans tous les cas on a donc $R(-x) = 256 - R(x)$.
On peut alors écrire $R(-x) = 255 - R(x) + 1$, et comme $255 = (11111111)_2$, pour passer de la représentation binaire de $R(x)$ à celle de $R(-x)$ il suffit de retrancher la représentation binaire de $R(x)$ de $(11111111)_2$, ce qui se fait en changeant les 0 en 1 et les 1 en 0, puis ajouter 1.

f) Exemple: pour calculer $R(-20)$ on calcule $R(20) = 20 = (00010100)_2$, puis on change les 0 en 1 et les 1 en 0: $(11101011)_2$, enfin on ajoute 1 pour obtenir le résultat: $R(-20) = (11101100)_2$.
Pour calculer $R(18)$ il y a juste à développer 18 en binaire $R(18) = (00010010)_2$.

Addition des entiers et représentation

a) Quand on tronque n à partir du bit numéro 8 (neuvième bit), on enlève à n un multiple de 256, si bien que $n = 256q + T(n)$ où $0 \leq T(n) \leq 255$. Donc $T(n)$ est le reste de la division euclidienne de n par 256, c'est-à-dire $T(n) = n \bmod 256$.

b) En vertu de la compatibilité de la congruence par rapport à l'addition on peut écrire que x_1 et $R(x_1)$ ont le même reste dans la division par 256, x_2 et $R(x_2)$ ont le même reste dans la division par 256, donc $x_1 + x_2$ et $R(x_1) + R(x_2)$ on aussi le même reste. Ce reste est par définition $R(x_1 + x_2)$, c'est aussi d'après ce qu'on a vu précédemment $T(R(x_1) + R(x_2))$.

En conséquence pourvu que x_1, x_2 et $x_1 + x_2$ soient dans I, on obtient le développement binaire de $R(x_1 + x_2)$ en additionnant les développements binaires de $R(x_1)$ et $R(x_2)$, et en tronquant au delà du huitième bit.

c) Nous allons calculer dans différents cas C, α, V et regarder dans chaque cas la validité de l'opération.

c_1) $x_1 \geq 0$ et $x_2 \geq 0$.
Dans ce cas on a $R(x_1) = x_1$, $R(x_2) = x_2$, $R(x_1) + R(x_2) < 256$, donc $C = 0$.
• Si $x_1 + x_2 \leq 127$ (ou $R(x_1) + R(x_2) \leq 127$), l'opèration est valide, il n'y a pas non plus de retenue du septième bit vers le huitième (puisque le résultat ne dépasse pas 127). Dans ce cas on a $\alpha = 0$ et donc $V = 0$.
• Si $x_1 + x_2 \geq 128$ (ou $R(x_1) + R(x_2) \geq 128$), l'opération n'est pas valide, il y a une retenue du septième bit vers le huitième (puisque le résultat est ≥ 128). Dans ce cas $\alpha = 1$ et $V = 1$.

c_2) $x_1 \geq 0$ et $x_2 < 0$ (ou de façon symétrique $x_1 < 0$ et $x_2 \geq 0$).
L'opération est toujours valide. De plus le huitième bit de $R(x_1)$ est 0 alors que celui de $R(x_2)$ est 1. Par suite il y a une retenue du huitième bit vers l'extérieur si et seulement si il y a une retenue du septième bit vers le huitième. En conséquence ou bien $C = \alpha = 1$ ou bien $C = \alpha = 0$. Dans les deux cas $V = 0$.

c_3) $x_1 < 0$ et $x_2 < 0$.
Les développements binaires de $R(x_1)$ et $R(x_2)$ ont tous leur huitième bit valant 1. Donc $C = 1$.
On considère alors les 7 premiers bits de $R(x_1)$ et $R(x_2)$, ce qui revient à prendre $R(x_1) - 128$ et $R(x_2) - 128$. Or $R(x_1) = x_1 + 256$ et $R(x_2) = x_2 + 256$, donc

$$(R(x_1) - 128) + (R(x_2) - 128) = x_1 + x_2 + 256.$$

• Si $x_1 + x_2 < -128$ (opération invalide) alors $(R(x_1) - 128) + (R(x_2) - 128) < 128$, et il n'y a pas de retenue du septième bit vers le huitième. Donc $\alpha = 0$, $V = 1$.
• Si $x_1 + x_2 \geq -128$ (opération valide) alors $(R(x_1) - 128) + (R(x_2) - 128) \geq 128$, et il y a une retenue du septième bit vers le huitième. Donc $\alpha = 1$, $V = 0$.

c_4) En raisonnant par exhaustion on voit que l'opération est valide si et seulement si $V = 0$.

Extension des résultats Il suffit de remplacer 256 par 2^{16} si on travaille sur deux octets. On obtiendra les mêmes résultats.

Répartitions de termes d'une suite dans un tableau

Correspondance d'indices

Les termes étant rangés comme indiqué, le terme $a_{i,j}$ correpondant à la i^e ligne et la j^e colonne est le terme u_n avec $n = (i-1)31 + j$ et $1 \leq j \leq 31$. Si bien que $n - 1 = (i-1)31 + (j-1)$ avec $0 \leq j - 1 < 31$. Donc $(i-1)$ est le quotient euclidien de $n-1$ par 31 et $j-1$ est le reste de cette division.

Répartition dans deux tableaux

Deux éléments u_n et u_m de la suite sont rangés dans la même colonne pour les deux tableaux si et seulement si

$$n - m = 31k$$

et

$$n - m = 97r.$$

Mais 97 et 31 sont premiers entre eux, donc $n-m$ est multiple de $31 \times 97 = 3007$, ce qui est impossible car $|n-m| \leq 3006$.

On peut donner quelques activités plus détaillées autour de ce thème.

A) Soient $u_1, \cdots, u_{3071}$ donnés. On veut ranger ces 3071 nombres dans un tableau ayant 83 lignes et 37 colonnes en prenant les termes dans l'ordre et en remplissant successivement toutes les lignes à partir de la première colonne. Notons $a_{i,j}$ l'élément de la suite qui se trouve rangé dans la ligne i et la colonne j.
1) Dans quelle ligne et quelle colonne se trouve rangé le terme u_{35}? Le terme u_{38}? Le terme u_{74}? Quel est le terme rangé dans la ligne 78 et la colonne 28? Dans quelle ligne i et quelle colonne j se trouve rangé le terme u_{1245}? Quel lien y-a-t-il avec la division euclidienne par 37? Dans quelle ligne et quelle colonne se trouve rangé le terme u_n?

2) À quelle condition sur n et m les termes u_n et u_m sont ils dans la même ligne?
À Quelle condition sur n et m les termes u_n et u_m sont ils dans la même colonne?

B) On reprend les mêmes questions mais avec la suite $v_1, \cdots, v_{3072}$ à ranger dans un tableau de 64 lignes et de 48 colonnes. En quoi les réponses diffèrent elles de celle de l'exemple A)?

C) On transfère le tableau T_1 de l'exemple A) dans un tableau T_2 ayant 37 lignes et 83 colonnes en parcourant les deux tableaux ligne par ligne à partir de la première colonne.
1) Si u_n et u_m sont dans la même colonne du tableau T_1, peuvent ils être dans la même colonne du tableau T_2?
2) Un élément peut il être rangé dans la même colonne dans T_1 et T_2?

D) On transfère le tableau T_3 de l'exemple B) dans un tableau T_4 ayant 48 lignes et 64 colonnes. Répondre aux mêmes questions que dans C).

3.6.3 Le chiffrement affine

Les clés - Les fonctions de chiffrement

a) $E_{(7,4)}(8) = 8$; $E_{(8,3)}(13) = 3$; $E_{(8,3)}(0) = 3$.

b) Si a n'est pas premier avec 26 soit d diviseur commun > 1. Alors $a = da'$ et $26 = db'$. Prenons $x = b'$, alors $ax = da'b' = 26a'$. Donc $(ax + b) \bmod 26 = b$. Par suite $E_{(a,b)}(b') = E_{(a,b)}(0)$ ce qui prouve que $E_{(a,b)}$ n'est pas bijective.

c) Supposons $E_{(a,b)}(x) = E_{(a,b)}(y)$. Alors $a(x - y)$ est un multiple de 26. Comme a est premier avec 26, $x-y$ est un multiple de 26 (théorème d'Euclide Gauss). Mais $|x - y| < 26$,donc $x = y$. Comme de plus l'ensemble de départ I a le même nombre d'éléments que l'ensemble d'arrivée (qui est aussi I), l'application est bijective.

d) Supposons que $E_{(a_1,b_1)} = E_{(a_2,b_2)}$ alors en prenant $x = 0$ on a $b_1 = b_2$. Prenons maintenant $x = 1$ alors $a_1 - a_2$ est divisible par 26. Comme $|a_1 - a_2| < 26$ on a $a_1 = a_2$.

e) Les éléments de I premiers avec 26 sont $1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25$. On dispose donc de $12 \times 26 = 312$ clés.

Fonctions de déchiffrement

a) 7 et 26 étant premiers entre eux on peut trouver z et k tels que $7z+26k = 1$. Si de plus on impose à z d'être dans I, il y a unicité. $z = 15, k = -4$.

b) On cherche z tel que $7z + 4 = 5 + 26k$, ou encore $7z - 26k = 1$. En vertu du a) on a $z = 15$.

c) Si $D_{(a,b)}(y) = x$ alors $y = ax + b + 26k$, $ax = (y - b) + 26k$. Soit $a' \in I$ tel que $aa' = 1 + 26u$ (cf. question précédente). Alors $aa'x = a'(y - b) + 26ka'$ ou encore $x + 26ux = a'(y - b) + 26ka'$, c'est-à-dire $x = a'(y - b) + 26k_1$.

Cryptanalyse

a) On a les deux conditions

$$8a + b = 20 + 26k_1$$

et

$$12a + b = 2 + 26k_2.$$

On en déduit que $4a = -18+26(k_2-k_1)$ ou encore que $4a = -18+26+26(k_2-k_1-1)$, ce qui donne $4a+26k = 8$, puis $2a+13k = 4$. On a nécessairement k pair, et $k \leq 0$. Essayons $k = 0$ on obtient $a = 2$ et $b = 4$, et cette solution ne convient pas car 2 n'est pas premier avec 26. Essayons $k = -2$, on obtient $a = 15$ donc $b = 4$ et cette solution convient. À partir de $k = -4$ on obtient un a trop grand.

b) On a les deux conditions

$$15a + b = 17 + 26k_1$$

et

$$2a + b = 4 + 26k_2.$$

On en déduit que $13a = 13 + 26(k_1 - k_2)$ ou encore $a = 1 + 2k$.
Les solutions admissibles sont $a = 1, b = 2$; $a = 3, b = 24$; $a = 5, b = 20$; $a = 7, b = 16$; $a = 9, b = 12$; $a = 11, b = 8$; $a = 15, b = 0$; $a = 17, b = 22$; $a = 19, b = 18$; $a = 21, b = 14$; $a = 23, b = 10$; $a = 25, b = 6$. Pour choisir la bonne clé il faut faire des essais jusqu'à obtenir un texte compréhensible.

3.6.4 Une idée de la cryptographie à clé publique: Kid-RSA

a) $ed - 1 = (a'M + a)(b'M + b) = a'b'M^2 + M(a'b + ab') + ab - 1 = M(a'b'M + a'b + ab' + 1)$. Donc $n = a'b'M + a'b + ab' + 1$. Par suite si les nombres a, a', b, b' sont $geq 3$ alors $M \geq 8$ et $n \geq 91$.
Il est important que n soit > 25 car comme on travaille modulo n si on veut avoir une chance que deux messages m et m' distincts $(0 \leq m, m' \leq 25)$ soient toujours chiffrés différemment il est nécessaire que cette condition soit réalisée.
Remarquons que $nM - ed = 1$ et donc que tout nombre qui divise n et e divise 1. Donc e et n sont premiers entre eux.

b) Alice calcule

$$cdmodn = edmmodn = mmodn = n.$$

c) Il suffit à D.S.T. de trouver un nombre d_1 tel que

$$ed_1 = 1 + kn$$

et comme e est premier avec n ceci revient à la résolution d'un problème de Bezout.

d) Pour signer un message m Alice utilise sa clé privé pour calculer $s = mdmodn$ et joint la signature s au message m. Celui qui reçoit le message m signé avec s n'a plus qu'à utiliser la clé publique d'Alice pour calculer $semodn$ et vérifier qu'il obtient bien m.

3.6.5 Exemples sur les codes correcteurs d'erreurs

Un code correcteur de Hamming

a) Il suffit de calculer pour trouver la clé 27.

b) Soit A le numéro (muni de sa clé) dont on part. Soit $A_1 = \sum_{i=1}^{10} a_i - a_{11}$ et $A_2 = \sum_{i=1}^{10} ia_i - a_{12}$. Alors A_1 et A_2 sont divisibles par 11. Si on modifie un chiffre de A d'indice $1 \leq j \leq 10$, alors A_1 est transformé en A'_1 de telle sorte que $A'_1 - A_1 = e \neq 0$ où $-9 \leq e \leq 9$, ce qui prouve que A'_1 n'est pas divisible par 11. De même A_2 est transformé en A'_2 de telle sorte que $A'_2 - A_2 = je$. Le nombre je n'est pas divisible par 11, donc A'_2 ne l'est pas non plus.
Si la modification porte sur a_{11} alors A_1 est transformé en A'_1 et ce dernier nombre n'est pas divisible par 11, alors que A_2 n'est pas modifié.
Si la modification porte sur a_{12} c'est A_1 qui n'est pas modifié alors que A_2 est transformé en un nombre A'_2 qui n'est pas divisible par 11.

La correction de l'erreur se fait alors de la façon suivante:

si seule la relation 2) n'est pas vérifiée, alors l'erreur porte sur a_{12} et le bon a_{12} est déterminé par un calcul direct de la clé comme au a) puisque les 10 premiers chiffres sont corrects;

si seule la relation 1) n'est pas vérifiée alors l'erreur porte sur a_{11}, et comme précédemment par le calcul de la clé utilisant les 10 premiers chiffres on reconstitue a_{11};

si aucune des relations 1) et 2) n'est vérifiée, c'est que l'erreur se situe en une position j où $1 \leq j \leq 10$. Si a_j est modifié en $a'_j = a_j + e$, $(-9 \leq e \leq 9)$ On a $A'_1 - A_1 = e$. Alors e est congru à A'_1 modulo 11 $(e = A_1 + 11k_1)$. Ceci nous permet de déterminer au plus deux valeurs possibles pour e, l'une positive qu'on notera e_1 (reste de la division de A_1 par 11), l'autre négative (puisque $-9 \leq e \leq 9$).
De même $A'_2 - A_2 = je$ et par suite je_1 est congru à A'_2 modulo 11 $(je_1 = A_2 + 11k_2)$.
Le nombre e_1 est premier avec 11, donc on peut trouver s et k_3 tels que $se_1 + 11k_3 = 1$. Par suite $je_1s = j - 11jk_3 = sA_2 + 11sk_2$, ce qui donne $j = sA_2 + 11k$. j est donc congru à sA_2 modulo 11, et comme $1 \leq j \leq 10$, on détermine la position j de manière unique. Maintenant on a la valeur de a'_j et parmi les deux valeurs possibles de e il n'y en a qu'une telle que $0 \leq a'_j - e = a_j \leq 9$.

Exemple: on a le numéro 049132900000. On calcule le reste e_1 de la division de A'_1 par 11 et on trouve $e_1 = 6$; on peut donc prendre $s = 2$ (car $2 \times 6 - 11 = 1$). On calcule le reste de la division de A'_2 par 11 et on trouve 8. Par suite j doit être tel que $6j = 8 + 11k$, ce qui donne en multipliant par s, j congru à 16 modulo 11, c'est-à-dire $j = 5$. Comme $a_5 + e = 3$ et que e est congru à 6 modulo 11, c'est que $e = -5$ et $a_5 = 8$.

Impossibilité de réaliser une correction de type précédent uniquement avec des chiffres décimaux

a) E a 10^{10} éléments et F en a 10^{12}.

b) C a le même nombre d'éléments que E c'est-à-dire 10^{10}.

c) Le nombre d'éléments pouvant être obtenus à partir de $y \in C$ par modification d'un chiffre est 12×9. Si on rajoute l'élément y lui même on voit que B_y a 109 éléments.
Si les ensembles B_y $(y \in C)$ étaient disjoints, leur réunion comporterait $10^{10} \times 109$ éléments, ce qui est strictement plus que le nombre total d'éléments de F (car $10^{10} \times 109 > 10^{12}$). Par suite il existe au moins deux éléments de C, distincts, z_1 et z_2, tels que $B_{z_1} \cap B_{z_2} \neq \emptyset$.

Si on fait le calcul dans le cadre de l'exercice précédent (on permet 11 chiffres au lieu de 10) alors E et C ont 11^{10} éléments, F a 11^{12} éléments, B_y a 121 éléments et on constate que $121 \times 11^{10} = 11^{12}$, ouf!

Chapitre 4

Compléments d'arithmétique élémentaire

4.1 Introduction - Notations.

Ce texte est une étude élémentaire de l'arithmétique. Nous essayons à travers le cas particulier important de l'anneau $\mathbb{Z}$ de mettre en place une étude généralisable à d'autres anneaux, en mettant l'accent sur les méthodes de base de l'algèbre commutative. Ainsi la relation de divisibilité est étudiée à travers la relation d'inclusion entre idéaux. Nous regardons aussi le passage au quotient par un idéal (dans notre cas, les classes résiduelles modulo n).

4.2 Etude élémentaire de $\mathbb{Z}$.

4.2.1 Ensembles majorés et minorés de $\mathbb{Z}$.

Rappelons que dans un ensemble ordonné A, une partie B est dite **majorée** (resp. **minorée**) s'il existe un élément de A plus grand (resp. plus petit) que tous les éléments de B.

Dans $\mathbb{Z}$ les ensembles majorés et les ensembles minorés ont un comportement très simple et répondent au comportement suivant

Tout ensemble majoré de $\mathbb{Z}$ a un plus grand élément. Tout ensemble minoré de $\mathbb{Z}$ a un plus petit élément.

4.2.2 Quelques fonctions élémentaires liées aux entiers

Il existe quelques fonctions classiques simples définies sur $\mathbb{R}$, qui prennent des valeurs entières:

trunc(x) : cette fonction associe à x l'entier situé entre x et 0 le plus proche de x.

$$trunc(-3.1) = -3,$$

$$trunc(2.6) = 2,$$

$$trunc(3) = 3.$$

round(x) : cette fonction associe à x l'entier le plus proche de x. Dans le cas où on tombe exactement entre deux entiers on choisit celui de plus grande valeur absolue.

$$round(2.1) = 2,$$

$$round(-3.8) = -4,$$

$$round(5.5) = 6,$$

$$round(-3.5) = -4.$$

frac(x) : cette fonction associe à x sa partie fractionnaire, c'est-à-dire

$$frac(x) = x - trunc(x).$$

$$frac(2.3) = 0.3,$$

$$frac(-4.7) = -0.7.$$

floor(x) : cette fonction associe à x le plus grand entier $\leq x$.

$$floor(4.6) = 4,$$

$$floor(5) = 5,$$

$$floor(-3.1) = -4.$$

ceil(x) : cette fonction associe à x le plus petit entier $\geq x$.

$$ceil(4.6) = 5,$$

$$ceil(5) = 5,$$

$$ceil(-3.1) = -3.$$

4.2.3 La division dans $\mathbb{Z}$.

Définition et propriétés élémentaires

Définition 4.2.1 *Soient a et b deux éléments de $\mathbb{Z}$. Nous dirons que a* **est divisible par** *b s'il existe un élément q dans $\mathbb{Z}$ tel que $a = bq$. Dans ce cas nous noterons $b|a$.*

Remarquons que si $a \neq 0$ et si b divise a alors $b \neq 0$ et q est unique. On dira que q est le **quotient exact** de a par b et on le notera a/b. Dans ce cas a/b divise aussi a.

Nous pouvons remarquer directement un certain nombre de propriétés élémentaires qui dérivent simplement de la définition.

Proposition 4.2.1
1) $a|a$.
2) $c|b$ et $b|a$ implique $c|a$.
3) $a|b$ et $b|a$ implique $|a| = |b|$.
(On a presque une relation d'ordre; si on restreint la relation à $\mathbb{N}$ on a une relation d'ordre).
4) $c|a$ et $c|b$ implique $c|(ua + vb)$.
5) $ac|ab$ et $a \neq 0$ implique $c|b$.
6) $1|a$.
7) $a|0$.
8) $0|a$ implique $a = 0$.
9) $b|a$ et $a \neq 0$ implique $|b| \leq |a|$.

La division Euclidienne dans $\mathbb{Z}$.

Soit b un nombre entier distinct de 0. Pour tout entier k définissons l'intervalle I_k par

$$I_k = [kb, kb + |b|[= \{x \in \mathbb{Z} \mid kb \leq x < kb + |b|\}.$$

En utilisant le fait que tout ensemble majoré de $\mathbb{Z}$ a un plus grand élément on peut montrer que les intervalles I_k constituent une partition de $\mathbb{Z}$ et aussi que pour tout entier $a \in \mathbb{Z}$ il existe un entier q unique appelé **quotient euclidien** de a par b tel que a soit dans l'intervalle I_q. On peut donc écrire a sous la forme

$$a = qb + r$$

avec

$$0 \leq r < |b|,$$

et cette écriture est unique sous ces conditions. L'entier r est appelé le **reste** de la division euclidienne de a par b.

Lorsque b divise a, q est le quotient exact de a par b et $r = 0$.

Voici **l'algorithme d'Euclide** qui permet d'obtenir effectivement q et r et qui peut servir aussi de démonstration à l'existence du couple (q, r). Cet Algorithme consiste à faire des soustractions successives:

$B :\ = b$;
$R :\ = a$;
$Q :\ = 0$;
tant que $R \geq B$ *faire*
  début
    $R :\ = R - B$;
    $Q :\ = Q + 1$;
  fin;

A la fin on a dans la variable Q le quotient cherché et dans la variable R le reste.
En effet, remarquons qu'à l'entrée de la boucle, il y a b dans B, a dans R et 0 dans Q, donc $a = B * Q + R$. D'autre part si quand on commence un tour de boucle on a $a = B * Q + R$, à la fin du tour de boucle on a aussi cette même égalité puisque R a diminué de b alors que Q a augmenté de 1 ou encore $Q * B$ a augmenté de b. En fin de boucle on a donc $a = B * Q + R$ et $0 \leq R < B$. (Puisque tout ensemble minoré de $\mathbb{Z}$ a un plus petit élément, le programme s'arrête).

4.2.4 La divisibilité dans $\mathbb{Z}$

Divisibilité et inclusion

Nous allons étudier la relation de divisibilité dans $\mathbb{Z}$, et pour cela nous faisons une remarque préliminaire très simple:

pour que b divise a il faut et il suffit que l'ensemble des multiples de a soit inclus dans l'ensemble des multiples de b.

Ainsi la relation de divisibilité s'exprime simplement à travers la relation d'inclusion entre certaines parties de $\mathbb{Z}$. Ce sont ces parties (ensembles de multiples) que nous allons donc étudier dans un premier temps.

Idéaux et ensembles de multiples

Soit $a \in \mathbb{Z}$. Notons $a\mathbb{Z}$ l'ensemble des multiples de a. Il est très facile de vérifier que l'ensemble $a\mathbb{Z}$ possède les propriétés suivantes:

- $a\mathbb{Z}$ est un sous groupe de $\mathbb{Z}$;
- le produit d'un élément quelconque de $a\mathbb{Z}$ par un élément quelconque de $\mathbb{Z}$ appartient à $a\mathbb{Z}$.

Ces deux propriétés définissent ce qu'on appelle un **idéal** de $\mathbb{Z}$.
Ainsi, **dans $\mathbb{Z}$, tout ensemble de multiples est un idéal de $\mathbb{Z}$.**

Réciproquement, tout idéal de $\mathbb{Z}$ est l'ensemble des multiples d'un élément a de $\mathbb{Z}$. En effet, Soit $\mathcal{I}$ un idéal de $\mathbb{Z}$. Si $\mathcal{I} = \{0\}$ le résultat est bien vrai avec $a = 0$. Sinon, il existe dans $\mathcal{I}$ un plus petit entier strictement positif a. Alors, si $b \in \mathcal{I}$, par division euclidienne on obtient $b = aq + r$ avec $0 \leq r < a$. Comme a et b sont dans $\mathcal{I}$, il en est de même pour r; donc en vertu du choix de a on conclut $r = 0$, ce qui prouve le résultat. En conclusion on a le théorème

Théorème 4.2.1 *la classe des idéaux de $\mathbb{Z}$ est la classe des sous ensembles de $\mathbb{Z}$ de la forme $a\mathbb{Z}$. (On dit que dans $\mathbb{Z}$* **tout idéal est principal** *ou encore que $\mathbb{Z}$ est* **principal***).*

Remarque : La démonstration du théorème 4.2.1 est importante car elle reflète une démarche très fréquente dans ce type de situations.
Si $\mathcal{I}$ est un idéal il existe **un et un seul** $a \geq 0$ tel que $\mathcal{I} = a\mathbb{Z}$.

Conséquences, théorème de Bezout, applications

Nous nous intéressons maintenant à la somme de deux idéaux $\mathcal{I}_1 = a\mathbb{Z}$ et $\mathcal{I}_2 = b\mathbb{Z}$

$$\mathcal{I}_1 + \mathcal{I}_2 = \{i = i_1 + i_2 \mid i_1 \in \mathcal{I}_1,\ i_2 \in \mathcal{I}_2\} = \{au + bv \mid u \in \mathbb{Z},\ v \in \mathbb{Z}\}$$

ainsi qu'à leur intersection $\mathcal{I}_1 \cap \mathcal{I}_2$.

Théorème 4.2.2 *La somme et l'intersection de deux idéaux sont des idéaux.*

Preuve : Il suffit de revenir à la définition d'un idéal. On vérifie aisément les propriétés attendues.

Par application du théorème 4.2.1 nous obtenons le résultat suivant

Théorème 4.2.3 *Il existe un et un seul entier $d \geq 0$ tel que $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ et un seul entier $m \geq 0$ tel que $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$.*

Théorème 4.2.4 *Si $a \neq 0$ ou $b \neq 0$ alors $d \neq 0$ et d est le plus grand diviseur commun de a et b, et tout diviseur commun de a et b est un diviseur de d. Dans tous les cas m est le plus petit commun multiple ≥ 0 de a et b et tout multiple commun de a et b est un multiple de m.*

Preuve : On voit que $a\mathbb{Z} \subset d\mathbb{Z}$ et que $b\mathbb{Z} \subset d\mathbb{Z}$. Donc $d|a$ et $d|b$. Il est clair que si $c|a$ et $c|b$ alors $a\mathbb{Z} \subset c\mathbb{Z}$ et $b\mathbb{Z} \subset c\mathbb{Z}$, donc $d\mathbb{Z} \subset c\mathbb{Z}$. On voit aussi que $m\mathbb{Z} \subset a\mathbb{Z}$ et que $m\mathbb{Z} \subset b\mathbb{Z}$. Donc m est multiple de a et de b. Si c est multiple de a et de b alors $c\mathbb{Z} \subset a\mathbb{Z}$ et $c\mathbb{Z} \subset b\mathbb{Z}$, donc $c\mathbb{Z} \subset m\mathbb{Z}$.

Remarque : Le cas où $a = b = 0$ est spécial car alors on a $d = 0$. Dans ce cas il n'y a pas de plus grand diviseur commun à a et b (tout élément de $\mathbb{Z}$ est diviseur commun).

Le nombre d sera noté $\mathrm{pgcd}(a, b)$. Le nombre m sera noté $\mathrm{ppcm}(a, b)$.

Voici quelques propriétés élémentaires du pgcd (et du ppcm).

Proposition 4.2.2
1) $pgcd(a, b) = pgcd(b, a)$.
2) $pgcd(a, (b, c)) = pgcd((a, b), c)$.
3) $pgcd(ca, cb) = |c| pgcd(a, b)$.
4) $pgcd(a, 1) = 1$.
5) Soit $a' = a/pgcd(a, b)$ et $b' = b/pgcd(a, b)$. Alors $pgcd(a', b') = 1$.
6) $|ab| = pgcd(a, b) ppcm(a, b)$.

Définition 4.2.2 *Lorsque $pgcd(a, b) = 1$, nous dirons que les nombres a et b sont* **premiers entre eux**.

Théorème 4.2.5 (**Théorème de Bezout**) *Deux nombres entiers a et b sont premiers entre eux si et seulement s'il existe des entiers u et v tels que $au + bv = 1$.*

Preuve : Ce théorème découle immédiatement du théorème 4.2.3.

Théorème 4.2.6 *(Lemme d'Euclide) Si c divise ab et si c est premier avec b alors c divise a.*

Preuve : Si c est premier avec b alors on peut trouver u et v tels que $uc + bv = 1$. Par suite $auc + abv = a$. Mais auc est divisible par c et abv aussi, donc a est divisible par c.

Aspects algorithmiques

Voici un algorithme (**algorithme d'Euclide étendu**) qui permet de calculer le pgcd d de deux nombres a et b, ainsi que des coefficients u et v tels que $au + bv = d$.

Posons $t_0 = a$, $t_1 = b$ et par récurrence pour $i > 1$

$$t_i = t_{i-2} - q_i t_{i-1}$$

où q_i est le quotient de t_{i-2} par t_{i-1}. Ainsi t_i est le reste de la division précédente.

1) Montrer qu'il existe un plus petit entier k tel que $t_k = 0$.

2) Montrer que t_{k-1} est le pgcd de a et de b.

On pose $u_0 = 1$, $v_0 = 0$, $u_1 = 0$, $v_1 = 1$. Et on définit par récurrence pour $i > 1$

$$u_i = u_{i-2} - q_i u_{i-1},$$

$$v_i = v_{i-2} - q_i v_{i-1}.$$

3) Montrer que pour tout $0 \leq i \leq k-1$ on a $t_i = au_i + bv_i$.

4) En conclure l'existence et le calcul de u et v tels que $au + bv = d$.

Aspects relation d'ordre

Si on se restreint à $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, la relation de divisibilité est une relation d'ordre et pour cette relation d'ordre les intervalles sont finis. On peut vouloir étudier des fonctions arithmétiques, c'est-à-dire des fonctions définies sur $\mathbb{N}^*$

à valeurs dans $\mathbb{Z}$, $\mathbb{R}$, $\mathbb{C}$, ou plus généralement dans un groupe abélien. Si f est une telle fonction définissons la fonction

$$g(n) = \sum_{d|n} f(d).$$

Est il possible d'exprimer f en fonction de g? Pour cela définissons la fonction de Möbius arithmétique par

$$\mu(1) = 1,$$

$$\mu(p_1p_2\cdots p_k) = (-1)^k \text{ si les nombres premiers } p_i \text{ sont distincts,}$$

$$\mu(n) = 0 \text{ sinon.}$$

Dans ces conditions on obtient la formule d'inversion

$$f(n) = \sum_{d|n} \mu(d)g(\frac{n}{d}).$$

Nous renvoyons à l'annexe I pour une étude plus générale et plus détaillée des fonctions de Möbius.

4.2.5 Les nombres premiers

Définition et premières propriétés

Définition 4.2.3 *Un nombre premier dans $\mathbb{Z}$ est un entier $n > 1$ dont les seuls diviseurs positifs sont 1 et n.*

Théorème 4.2.7 *Tout entier $n > 1$ est soit un nombre premier soit un produit de nombres premiers.*

Preuve : Le résultat est vrai pour 2. Supposons le vrai pour tout entier $< n$. Si n est non premier il a un diviseur positif $d > 1$, $d \neq n$. Donc $n = ab$ avec $2 \leq a < n$ et $2 \leq b < n$. En appliquant l'hypothèse de récurrence à a et b on obtient le théorème.

Théorème 4.2.8 *Le sous ensemble constitué par les nombres premiers est infini.*

Preuve : Supposons que ce sous ensemble soit fini. Notons alors $p_1, p_2, \cdots, p_n$ tous les nombres premiers. Soit $N = p_1p_2 \cdots p_n + 1$. N n'est pas premier (il est plus grand que tous les p_i), et il n'est divisible par aucun des p_i, ce qui contredit le théorème précédent.

Proposition 4.2.3 *Si un nombre premier ne divise pas un entier, il est premier avec lui.*
Si un nombre premier p divise un produit d'entiers, il divise au moins l'un d'entre eux.

Preuve : Supposons que le nombre premier p ne divise pas l'entier a. Les seuls diviseurs positifs de p sont 1 et p. Donc le seul diviseur commun à p et a est 1.
Supposons que le nombre premier p divise le produit ab. Si p ne divise pas a alors p est premier avec a, donc d'aprés le lemme d'Euclide il divise b. Pour un produit de plus de deux entiers on raisonne par récurrence.

Décomposition en produit de nombres premiers

Théorème 4.2.9 *Tout entier $n > 1$ s'écrit de manière unique sous la forme*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

où les α_i sont des entiers ≥ 1 et où les p_i sont des nombres premiers distincts tels que $p_i < p_{i+1}$.

Preuve : Nous avons déjà vu précédemment que la décomposition en nombre premier est toujours possible. Il nous reste à montrer l'unicité. Le Résultat est vrai pour 2. Supposons le vrai pour tout entier $< n$. Supposons alors que

$$n = p_1 \cdots p_u = q_1 \cdots q_v$$

alors p_1 divise $q_1 \cdots q_v$, et donc divise au moins l'un des q_i, par exemple q_1; comme q_1 est premier, $p_1 = q_1$. Il s'en suit que toute décomposition de n est de la forme $p_1 a$. En appliquant l'hypothèse de récurrence à a on obtient le résultat voulu.

Aspects algorithmiques

La détermination des nombres premiers est un problème important et difficile. Plus précisément il y a plusieurs problèmes distincts. Tout d'abord déterminer les nombres premiers plus petits qu'un nombre donné, c'est-à-dire construire une table; ensuite dire si un nombre donné est ou n'est pas premier; enfin, déterminer la décomposition en nombres premiers d'un nombre donné. Tous ces problèmes algorithmiques ont donné lieu à de longs développements et ne sont que partiellement résolus. Nous donnons ici un algorithme élémentaire pour construire des tables de nombres premiers, appelé le **crible d'Ératosthène**.

Pour avoir dans une table de résultats tous les nombres premiers $\leq n$, on écrit dans une table de départ et dans l'ordre habituel, tous les nombres de 2 à n. On itère jusqu'à épuisement de la table de départ l'action suivante: on met dans la table de résultats le premier nombre qui se trouve dans la table de départ et on supprime de cette dernière ce nombre ainsi que tous ses multiples.

Liens avec les idéaux

Un **idéal premier** d'un anneau A est un idéal I distinct de A et tel que si un produit ab d'éléments de A est dans I, alors l'un des deux éléments a ou b est dans I.

Les idéaux premiers de $\mathbb{Z}$ sont l'idéal $\{0\}$ et les idéaux $p\mathbb{Z}$ où p est premier.

Un **idéal maximal** d'un anneau A est un idéal M distinct de A tel que A soit le seul idéal qui contienne strictement M. Tout idéal maximal est premier.

Les idéaux maximaux de $\mathbb{Z}$ sont les idéaux $p\mathbb{Z}$ où p est premier.

Nous renvoyons à l'annexe III pour des informations plus précises sur ces notions.

4.3 Les classes résiduelles: $\mathbb{Z}/n\mathbb{Z}$

4.3.1 Définition

Soit $n \geq 0$. Dans $\mathbb{Z}$ définissons la relation $x\mathcal{R}y$ si et seulement si $x - y \in n\mathbb{Z}$. Cette relation est une relation d'équivalence dans $\mathbb{Z}$. Si x et y sont dans la même classe (i.e. équivalents), nous dirons que x **est congru à** y **modulo** n et nous noterons

$$x \equiv y \quad (n).$$

Remarquons que si $n \geq 1$, x est congru à y modulo n si et seulement si les divisions euclidiennes de x par n et de y par n ont le même reste.

Sur l'ensemble quotient on définit une addition et une multiplication en posant

$$\overline{x} + \overline{y} = \overline{x+y}$$

$$\overline{x}\overline{y} = \overline{xy}$$

où $\overline{x}$ représente la classe de x. Il est facile de vérifier tout d'abord que ces définitions sont cohérentes c'est-à-dire que la classe résultat ne dépend pas des représentants choisis. Ensuite puisque les opérations sur les classes se définissent à partir d'un représentant de chaque classe, on montre que les propriétés des opérations sur $\mathbb{Z}$ se transmettent aux opérations sur les classes. L'ensemble quotient est ainsi un anneau que l'on note $\mathbb{Z}/n\mathbb{Z}$.

Si $n = 0$ alors $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}$.
Si $n = 1$ alors $\mathbb{Z}/n\mathbb{Z} = \{0\}$.

Théorème 4.3.1 *Si $n \geq 1$ l'anneau $\mathbb{Z}/n\mathbb{Z}$ a n éléments, et chaque classe a un représentant et un seul x tel que $0 \leq x \leq n-1$.*

Dans la suite lorsque $n \geq 1$ nous noterons les éléments de l'anneau $\mathbb{Z}/n\mathbb{Z}$ par $0, 1, \cdots, n-1$. Ainsi nous pourrons noter dans $\mathbb{Z}/3\mathbb{Z}$, $2 + 2 = 1$, ou encore si nous voulons préciser mieux que nous sommes dans $\mathbb{Z}/3\mathbb{Z}$, nous pourrons écrire $2 + 2 \equiv 1 \quad (3)$.

4.3.2 Idéaux et noyaux d'homomorphismes

Identification des noyaux avec les idéaux

Soit f un homomorphisme de $\mathbb{Z}$ dans un anneau A. Il est immédiat de vérifier le résultat suivant.

Théorème 4.3.2 *Le noyau de f est un idéal de $\mathbb{Z}$. Ainsi il existe un et un seul $a \geq 0$ tel que*

$$Ker\ f = a\mathbb{Z}.$$

Théorème 4.3.3 *Soit I un idéal de $\mathbb{Z}$. Alors il existe un homomorphisme de $\mathbb{Z}$ dans un anneau dont le noyau est I.*

Preuve : Si I est un idéal de $\mathbb{Z}$ alors il existe un et un seul $a \geq 0$ tel que $I = a\mathbb{Z}$. Soit f la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/a\mathbb{Z}$ (i.e. l'application qui a un élément x fait correspondre sa classe). Alors Ker $f = a\mathbb{Z}$.

Ainsi la classe des idéaux de $\mathbb{Z}$ s'identifie avec la classe des noyaux des homomorphismes de $\mathbb{Z}$ dans un anneau.

Factorisation des homomorphismes

Théorème 4.3.4 *Soit f un homomorphisme surjectif de $\mathbb{Z}$ sur un anneau B. Il existe une application bijective g et une seule de $\mathbb{Z}/Ker\ f$ sur B telle que $f = g \circ s$ où s est la surjection canonique de $\mathbb{Z}$ sur $\mathbb{Z}/Ker\ f$.*

Preuve : Si g existe elle est nécessairement définie par $g(\overline{x}) = f(x)$. Une telle définition est cohérente car si x et y sont dans la même classe alors $f(x) = f(y)$. L'application g est surjective à cause de la surjectivité de f, de plus Ker $g = \{0\}$ donc g est aussi injective.

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d, "s"'] & B \\ \mathrm{A/Ker\ f} \arrow[ur, "g"'] & \end{tikzcd}$$

Structure de corps

On peut se demander si l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps. La réponse est donnée par le théorème suivant

Théorème 4.3.5 *L'anneau $\mathbb{Z}/n\mathbb{Z}$ (avec $n \geq 0$) est un corps si et seulement si n est premier.*

Preuve : Si $n = 0$ ou si $n = 1$, $\mathbb{Z}/n\mathbb{Z}$ n'est pas un corps. Si $n \geq 2$ n'est pas premier il existe deux éléments a et b tels que $2 \leq a \leq n-1$, $2 \leq b \leq n-1$ et $n = ab$ donc tels que $ab \equiv 0 \quad (n)$. Ainsi $\mathbb{Z}/n\mathbb{Z}$ a des diviseurs de 0 et donc n'est pas un corps. Si n est premier et si $1 \leq a \leq n-1$, alors a est premier avec n et on peut trouver u et v tels que $au+nv=1$. En passant aux classes on conclut que $au \equiv 1 \quad (n)$, et donc que a est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

En fait on a redémontré ici, dans un cas particulier, le théorème énoncé dans l'annexe III, qui dit que le quotient d'un anneau par un idéal est un corps si et seulement si cet idéal est maximal.

Remarque sur la structure de groupe de $\mathbb{Z}/n\mathbb{Z}$

Les groupes finis commutatifs ont une description très simple:

Théorème 4.3.6 *Tout groupe abélien fini G est isomorphe à un produit de groupes $\mathbb{Z}/n_i\mathbb{Z}$. En outre les n_i peuvent être pris comme des puissances de nombres premiers.*

4.3.3 Application à la représentation des entiers en machine

Soit E le sous ensemble de $\mathbb{Z}$ constitué des entiers $\{-2^{15}, \cdots, 2^{15}-1\}$. Soit i l'application de E dans $\mathbb{Z}/2^{16}\mathbb{Z}$ qui à x associe sa classe. On note q l'application de $\mathbb{Z}/2^{16}\mathbb{Z}$ dans $\{0, \cdots, 2^{16}-1\}$ qui à toute classe fait correspondre son unique représentant compris entre 0 et $2^{16}-1$. On pose alors $R = q \circ i$.

a) Montrer que R est une application bijective.

b) Calculer $R(x)$ en fonction de x.

c) Donner un algorithme permettant de calculer $R(-x)$ à partir de $R(x)$ (algorithme dit de complémentation à 2).

Soit T l'application de $\mathbb{N}$ dans $\{0, \cdots, 2^{16}-1\}$ qui à tout $n = \sum_{j=0}^{\infty} a_j 2^j$ fait correspondre $T(n) = \sum_{j=0}^{15} a_j 2^j$ (troncature limitée aux 16 premiers bits).

Quel est le lien entre la classe de n modulo 2^{16} et $T(n)$?

e) Montrer que si x_1, x_2, x_1+x_2 sont des éléments de E alors $R(x_1+x_2) = T(R(x_1)+R(x_2))$.

f) Soient x_1 et x_2 deux éléments de E. Soit C le carry, retenue du 16$^{\text{e}}$ bit vers l'exterieur, et α la retenue du 15$^{\text{e}}$ bit vers le 16$^{\text{e}}$, obtenus en faisant l'addition $R(x_1)+R(x_2)$. On pose $V = C \oplus \alpha$. Montrer que x_1+x_2 est élément de E si et seulement si $V=0$.

4.3.4 Théorème chinois

Rappelons que l'anneau produit de deux anneaux A et B est défini comme étant l'ensemble produit $A \times B$ sur lequel on définit l'addition

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$

et la multiplication

$$(a_1, b_1).(a_2, b_2) = (a_1 \times a_2, b_1 \times b_2).$$

L'élément neutre pour l'addition est alors $(0_A, 0_B)$, et celui de la multiplication est $(1_A, 1_B)$.
Les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ ont le même nombre d'éléments. Sont ils isomorphes? Si $x \in \mathbb{Z}$ nous noterons $s(x)$ la classe de x modulo ab, $s_1(x)$ la classe de x modulo a et $s_2(x)$ la classe de x modulo b. La réponse à la question posée se trouve dans le théorème suivant.

Théorème 4.3.7 *Les anneaux $\mathbb{Z}/ab\mathbb{Z}$ et $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ sont isomorphes si et seulement si a et b sont premiers entre eux. Dans ce cas l'application*

$$s(x) \longrightarrow (s_1(x), s_2(x)),$$

définit un isomorphisme de $\mathbb{Z}/ab\mathbb{Z}$ sur $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$.

Preuve : Soient a et b premiers entre eux. Remarquons que si x et y sont dans la même classe modulo ab alors x et y sont dans la même classe modulo a et dans la même classe modulo b.
Ceci permet de définir l'application ϕ de $\mathbb{Z}/ab\mathbb{Z}$ dans $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$, en posant $\phi(s(x)) = (s_1(x), s_2(x))$. Cette application est un homomorphisme. Si $s(x)$ est dans le noyau de ϕ alors x est à la fois multiple de a et multiple de b, et donc multiple de ab puisque a et b sont premiers entre eux. Par suite dans ce cas $s(x) = 0$. Par suite le noyau de ϕ est réduit à $\{0\}$ et ϕ est injective. De plus le nombre d'éléments de $\mathbb{Z}/ab\mathbb{Z}$ est égal au nombre d'éléments de $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$. Donc ϕ est bijective.
Si a et b ne sont pas premiers entre eux. Si on note m le plus petit commun multiple de a et de b, alors $m \neq ab$. L'unité $(1_A, 1_B)$ de $A \times B = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ est d'ordre m, alors que l'unité de $\mathbb{Z}/ab\mathbb{Z}$ est d'ordre ab.

Soient a et b deux entiers premiers entre eux, et u et v deux entiers. Soit à résoudre le système

$$x \equiv u \quad (a)$$

$$x \equiv v \quad (b).$$

Grâce au théorème précédent, nous pouvons affirmer que ce problème a dans l'intervalle $\{0, \cdots, ab-1\}$, une solution unique x_0, et que toutes les solutions sont alors de la forme

$$x = x_0 + kab.$$

Le problème qui reste est de savoir comment déterminer effectivement x_0. Pour cela on peut envisager par exemple de tester les nombres compris entre 0 et ab. Une autre possibilité consiste à calculer par l'algorithme d'Euclide étendu des nombres s et t tels que $sa + tb = 1$. On a alors

$$sa \equiv 1 \quad (b),$$

$$tb \equiv 1 \quad (a)$$

et

$$x_0 \equiv sav + tbu \quad (ab).$$

4.3.5 La fonction indicatrice d'Euler

Soit n un entier ≥ 1. Nous étudions le sous ensemble E_n de $\mathbb{Z}/n\mathbb{Z}$ constitué des éléments inversibles. E_n est un groupe pour la multiplication.

Proposition 4.3.1 *Les éléments de E_n sont les classes des m tels que $0 < m \leq n-1$ et m premier avec n.*

Preuve : Désignons chaque classe par son unique représentant m tel que $0 \leq m \leq n-1$. Alors m est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement s'il existe un entier u tel que $mu \equiv 1 \quad (n)$, ce qui s'exprime encore en disant qu'il existe u et v tels que $mu + nv = 1$. Donc m est inversible dans $\mathbb{Z}/n\mathbb{Z}$ si et seulement si m est premier avec n.

La **fonction indicatrice d'Euler** est la fonction arithmétique ϕ qui à tout entier $n \in \mathbb{N}^*$ fait correspondre le nombre d'éléments de E_n.

Il résulte immédiatement du théorème précédent que:

$$\phi(1) = 1,$$

$$\text{Si } p \text{ est premier, alors } \phi(p) = p - 1.$$

Proposition 4.3.2 *Si p est un nombre premier et α un entier ≥ 1 alors $\phi(p^\alpha) = (p-1)p^{\alpha-1}$.*

Preuve : Il nous faut chercher le nombre d'entiers x tels que $1 \leq x \leq p^{\alpha-1}$ qui sont premiers avec $p^{\alpha-1}$, c'est-à- dire avec p. Les entiers qui ne conviennent pas sont les multiples de p qui se trouvent dans l'intervalle considéré: $p, 2p, \cdots, p^{\alpha-1}p$. Il y en a exactement $p^{\alpha-1}$. Ceux qui conviennent sont les $p^\alpha - p^{\alpha-1}$ restants.

Proposition 4.3.3 *Si a et b sont premiers entre eux, $\phi(ab) = \phi(a)\phi(b)$.*

Preuve : Ce résultat est une conséquence du théorème chinois. Reprenons les notations utilisées dans la partie consacrée à ce théorème. Les éléments $s(x)$ inversibles de $\mathbb{Z}/ab\mathbb{Z}$ sont ceux qui correspondent aux couples $(s_1(x), s_2(x))$ où $s_1(x)$ est inversible dans $\mathbb{Z}/a\mathbb{Z}$ et $s_2(x)$ inversible dans $\mathbb{Z}/b\mathbb{Z}$.

Théorème 4.3.8 *Si un entier $n > 1$ a pour décomposition en nombre premiers*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

alors

$$\phi(n) = n(1 - \frac{1}{p_1}) \cdots (1 - \frac{1}{p_k}).$$

Preuve : En utilisant les théorèmes précédents on voit que

$$\phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdots (p_k - 1)p_k^{\alpha_k - 1}.$$

En mettant $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ en facteur dans cette dernière quantité on obtient le résultat annoncé.

Théorème 4.3.9 *Si $n \geq 1$, alors*

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

Preuve : Soit $S_n = \{\frac{1}{n}, \frac{2}{n}, \cdots, \frac{n}{n})$. Notons T_n le sous ensemble de S_n constitué des fractions irréductibles. Il est clair que si $r \neq s$ alors $T_r \cap T_s = \emptyset$. De plus,

$$S_n = \cup_{d|n} T_d.$$

Mais le nombre d'éléments de T_d est $\phi(d)$ et celui de S_n est n. Donc

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

Théorème 4.3.10 *Si* $n \geq 1$, *alors*

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Preuve : Il suffit d'introduire la fonction g définie par

$$g(n) = \sum_{d|n} \phi(d).$$

Alors $g(n) = n$ et le théorème d'inversion de Möbius nous donne le résultat.

Théorème 4.3.11 *Si* $n \geq 1$ *et si* a *est premier avec* n *alors*

$$a^{\phi(n)} \equiv 1 \quad (n).$$

Preuve : L'ensemble des éléments inversibles de $\mathbb{Z}/n\mathbb{Z}$ est un groupe E pour la multiplication. Si a est premier avec n la classe de a est un élément de E. Les puissances de a engendrent un sous groupe cyclique de E dont l'ordre r divise l'ordre de E c'est-à-dire $\phi(n)$. Or on sait que $a^r \equiv 1 \quad (n)$, donc on a aussi $a^{\phi(n)} \equiv 1 \quad (n)$.

Remarque: En particulier si a est premier avec n alors a est inversible dans $\mathbb{Z}/n\mathbb{Z}$ et $a^{-1} = a^{\phi(n)-1}$ dans $\mathbb{Z}/n\mathbb{Z}$.

4.4 Equations ax+by =c

Soient a, b, c des entiers. Nous cherchons tous les couples d'entiers (x, y) tels que

$$ax + by = c.$$

Eliminons tout d'abord les cas triviaux où l'un au moins des deux nombres a et b est nul.
Si $a = b = 0$ alors si $c = 0$ tout couple (x, y) est solution, sinon il n'y a pas de solution.
Si $a = 0$ et $b \neq 0$, si b divise c il y a une solution, sinon il n'y en a pas.

Maintenant supposons $a \neq 0$ et $b \neq 0$.

1) Supposons a et b premiers entre eux.

Il s'agit donc de trouver des couples (x, y) tels que $ax + by = c$. On sait que ceci est possible d'après le théorème de Bezout. Plus précisément en se plaçant dans $\mathbb{Z}/b\mathbb{Z}$, on doit résoudre

$$\overline{ax} = \overline{c}.$$

Puisque a est premier avec b, la classe de a est inversible et on a donc une classe solution unique

$$\overline{c}(\overline{a})^{-1}$$

dont on notera x_0 un représentant. Ainsi toutes les solutions sont données par $x = x_0 + kb$, $y = \frac{c-a(x_0+kb)}{b}$.

2) Supposons maintenant que a et b ne soient pas premiers entre eux.

Notons d le pgcd de a et de b. Si d ne divise pas c il n'y a pas de solutions. Si d divise c alors on est amené à résoudre

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d},$$

et comme $\frac{a}{d}$ est premier avec $\frac{b}{d}$, on est ramené au problème précédent.

4.5 Annexe I: Fonctions de Möbius - Formule de Rota

4.5.1 Chaînes dans les ensembles finis ordonnés

Soit $\mathbb{L}$un ensemble **fini ordonné** par une relation notée $\leq$.

Définition 4.5.1 *Pour tout entier $p \geq 0$ et tout couple (x, y) d'éléments de $\mathbb{L}$tels que $x \leq y$ on appelle chaîne de longueur p joignant x à y toute suite finie $(x_0, x_1, \cdots, x_p)$ d'éléments de $\mathbb{L}$tels que*

$$x = x_0 < x_1 < \cdots < x_p = y.$$

On note $c_p(x, y)$ le nombre de ces chaînes.

Il est clair que

- $c_0(x, x) = 1$
- $c_0(x, y) = 0$ pour $x < y$
- $c_p(x, x) = 0$ pour $p > 0$
- $c_1(x, y) = 1$ pour $x < y$

Proposition 4.5.1 *On dispose des relations de récurrence suivantes entre les nombres $c_p(x, y)$:*

$$c_{p+1}(x, y) = \sum_{x \leq z < y} c_p(x, z)$$

$$c_{p+1}(x, y) = \sum_{x < z \leq y} c_p(z, y)$$

Preuve : Toute chaîne de longueur $p+1$ joignant x à y est constituée d'une chaîne de longueur p joignant x à un certain $z < y$ à laquelle on adjoint comme point x_{p+1} le point extrémité y. Ceci nous donne la première relation. La deuxième relation se démontre de manière analogue.

4.5.2 Fonction de Möbius

Définition 4.5.2 *La fonction de Möbius $\mu_{\mathbb{L}}$ de l'ensemble ordonné $\mathbb{L}$est la fonction définie sur $\mathbb{L} \times \mathbb{L}$ à valeurs dans $\mathbb{Z}$ par*

$$\mu_{\mathbb{L}}(x,y) = \sum_{p \geq 0} (-1)^p c_p(x,y)$$

si $x \leq y$ et par

$$\mu_{\mathbb{L}}(x,y) = 0$$

sinon.

Proposition 4.5.2 *La fonction $\mu_{\mathbb{L}}$ vérifie*

$$\mu_{\mathbb{L}}(x,x) = 1$$

et si $x < y$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x,z) = 0$$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(z,y) = 0.$$

Preuve : La première relation est une conséquence du fait que $\mu_{\mathbb{L}}(x,x) = c_0(x,x)$.
En ce qui concerne la deuxième relation en utilisant la définition de $\mu_{\mathbb{L}}$ et la proposition 4.5.1 on obtient la suite de calculs

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x,z) = \sum_{x \leq z \leq y} \sum_{p \geq 0} (-1)^p c_p(x,z)$$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x,z) = \sum_{p \geq 0} (-1)^p \sum_{x \leq z \leq y} c_p(x,z)$$

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x,z) = \sum_{p \geq 0} (-1)^p (c_{p+1}(x,y) + c_p(x,y))$$

donc

$$\sum_{x \leq z \leq y} \mu_{\mathbb{L}}(x,z) = 0.$$

La dernière relation s'obtient de manière analogue.

Remarque 1: Si on considère la relation d'ordre $\geq$ au lieu de $\leq$ sur $\mathbb{L}$, on obtient une fonction de Möbius $\mu'_{\mathbb{L}}$ qui vérifie

$$\mu'_{\mathbb{L}}(x, y) = \mu_{\mathbb{L}}(y, x).$$

Remarque 2: Toute cette étude reste encore valable sur un ensemble infini pourvu que pour tout couple x, y tel que $x \leq y$ il n'y ait qu'un ensemble fini de z tels que $x \leq z \leq y$. Tout ce qui est fait par la suite reste aussi valable dans ce cas.

4.5.3 Formule sommatoire de Rota

Soit f une fonction définie sur $\mathbb{L}$à valeurs dans un groupe abélien G. Posons

$$g(x) = \sum_{y \leq x} f(y).$$

Théorème 4.5.1 (Inversion de Rota) *Il est possible de retrouver la fonction f connaissant la fonction g grâce à la formule*

$$f(x) = \sum_{y \leq x} \mu_{\mathbb{L}}(y, x) g(y).$$

Preuve :

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x) g(y) = \sum_{y \leq x} \mu_{\mathbb{L}}(y, x) \sum_{z \leq y} f(z)$$

et par un autre regroupement des termes

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x) g(y) = \sum_{z \leq x} f(z) \sum_{z \leq y \leq x} \mu_{\mathbb{L}}(y, x)$$

or le seul cas où la somme $\sum_{z \leq y \leq x} \mu_{\mathbb{L}}(y, x)$ est non nulle est quand $z = x$ auquel cas cette somme vaut 1, donc

$$\sum_{y \leq x} \mu_{\mathbb{L}}(y, x) g(y) = f(x).$$

Remarquons que dans la formule d'inversion de Rota les $\mu_{\mathbb{L}}(y, x)$ sont dans $\mathbb{Z}$ alors que les $g(y)$ sont dans G. La signification des produits $\mu_{\mathbb{L}}(y, x) g(y)$

est claire; c'est la signification classique, à l'aide d'une itération d'additions, de la multiplication d'un élément d'un groupe par un entier.

Remarquons aussi que cette formule d'inversion, en raison de la remarque faite à la fin de la section précédente, peut aussi s'écrire, lorsque la fonction h est définie par

$$h(x) = \sum_{x \leq y} f(y),$$

sous la forme

$$f(x) = \sum_{x \leq y} \mu(x, y) h(y).$$

Si on remplace G par un corps K de caractéristique nulle alors $\mathbb{Z} \subset K$ et dans ce cas on peut énoncer le résultat suivant

Théorème 4.5.2 *Si pour tout couple (x, y) de points de $\mathbb{L}$tels que $x \leq y$ il existe un $a(x, y)$ dans K, de telle sorte que pour toute fonction f de $\mathbb{L}$dans K et tout x de $\mathbb{L}$on ait*

$$f(x) = \sum_{y \leq x} a(x, y) g(y)$$

où

$$g(y) = \sum_{z \leq y} f(z)$$

alors

$$a(x, y) = \mu_{\mathbb{L}}(x, y)$$

pour tout $x \leq y$.

Preuve : Notons s la cardinalité de $\mathbb{L}$. Indexons les éléments de $\mathbb{L}$sous la forme $\mathbb{L} = \{l_1, l_2, \cdots, l_s\}$ de telle sorte que l_1 soit minimal dans $\mathbb{L}$et que pour $k > 1$ l_k soit minimal dans $\mathbb{L} \setminus \{l_1, l_2, \cdots, l_{k-1}\}$. Soient $f_1, f_2, \cdots, f_s$ des fonctions de $\mathbb{L}$dans K linéairement indépendantes et $g_1, g_2, \cdots, g_s$ les fonctions correspondantes. On sait donc que

$$g_j(l_i) = \sum_{l \leq l_i} f_j(l)$$

Si bien que si on note F la matrice dont les coefficients sont les $f_j(l_i)$ et G celle dont les coefficients sont les $g_j(l_i)$ alors $G = BF$ où B est une matrice

triangulaire inférieure (à cause de l'indexation des éléments de $\mathbb{L}$) ayant des 1 sur la diagonale. Donc la matrice B est inversible et comme F aussi par le choix des fonctions f_j, il en découle que G est inversible.
Par hypothèse on sait que $F = AG$ où les coefficients de A sont des zéros ou des a(x,y). Alors $A = FG^{-1}$. On en conclut que A est entièrement déterminée par F et G ce qui montre le résultat.

Pour calculer la fonction de Möbius d'un ensemble concret L on peut donc penser aux diverses démarches suivantes:

- Calculer tous les coefficients $c_p(x, y)$.
- Utiliser la proposition 4.5.2 pour calculer par récurrence les $\mu_{\mathbb{L}}(x, y)$.
- Utiliser une formule d'inversion connue par d'autres moyens pour en déduire grâce au théoreme 4.5.2 la fonction de Möbius.

4.5.4 Exemples

Intervalles finis d'entiers

Prenons $\mathbb{L} = \{1, 2, \cdots, n\}$ muni de l'ordre habituel. La fonction de Möbius dans ce cas est donnée par

$$\mu_{\mathbb{L}}(i, i) = 1$$

$$\mu_{\mathbb{L}}(i, i+1) = -1$$

et pour $j > i + 1$

$$\mu_{\mathbb{L}}(i, j) = 0.$$

Preuve : Nous avons dejà vu que la relation $\mu_{\mathbb{L}}(x, x) = 1$ a lieu dans tous les cas.
Pour la deuxième égalité il suffit de voir que le coefficient $c_r(i, i+1)$ est nul sauf pour $r = 1$ auquel cas il vaut 1.
Enfin quand $j > i + 1$

$$\mu_{\mathbb{L}}(i, j) = \sum_{p=1}^{j-i} (-1)^p c_p(i, j)$$

et comme $c_p(i, j)$ est égal au coefficient binomial C_{j-i-1}^{p-1} la somme considérée est nulle.

Ainsi si $g(i) = \sum_{j=1}^{i} f(j)$ alors par la formule d'inversion de Rota on trouve la relation bien claire

$$f(i) = g(i) - g(i-1).$$

On aurait pu partir de cette relation visiblement vraie et utiliser le théorème 4.5.2 pour en déduire la fonction de Möbius.

Diviseurs d'un entier

On se place dans l'ensemble $\mathbb{N}$ des nombres naturels. Soit $n \in \mathbb{N}$ et $\mathbb{L}$l'ensemble des diviseurs de n ordonné par la relation de divisibilité. La fonction de Möbius dans ce cas est

$$\mu_{\mathbb{L}}(r,s) = \mu(s/r)$$

où μ est la fonction de Möbius classique donnée par

$$\mu(1) = 1$$

si $p_1, p_2, \cdots, p_k$ sont des nombres premiers distincts

$$\mu(p_1.p_2 \cdots p_k) = (-1)^k$$

et dans tous les autres cas

$$\mu(r) = 0.$$

Preuve : Remarquons tout d'abord que $\mu_{\mathbb{L}}(r,s) = \mu_{\mathbb{L}}(1, r/s)$. Si on considère la fonction de Möbius arithmétique il est facile de voir que $\sum_{z|y} \mu(z) = 0$ ou encore $\mu(y) = -\sum_{z|y, z \neq y} \mu(z)$. Comme $\mu_{\mathbb{L}}(1,y)$ vérifie la même relation de récurence et que $\mu_{\mathbb{L}}(1,1) = \mu(1)$ on conclut que $\mu_{\mathbb{L}}(1,y) = \mu(y)$. D'où le résultat annoncé. Ici on a pu déterminer la fonction de Möbius sans faire appel au nombre de chaînes.

Parties d'un ensemble fini

Soit S un ensemble fini et $\mathbb{L} = \mathcal{P}(S)$ l'ensemble des parties de S ordonné par inclusion. La fonction de Möbius dans ce cas est

$$\mu_{\mathbb{L}}(A,B) = (-1)^{\sharp B - \sharp A}$$

(où $\sharp X$ désigne le nombre d'éléments de X) si $A \subset B$ et

$$\mu_{\mathbb{L}}(A, B) = 0$$

sinon.

Preuve : La démonstration se fait par récurrence sur $\sharp(B-A)$. Si $\sharp(B-A) = 0$ (cas où A=B) le résultat est vrai (on obtient bien $\mu_{\mathbb{L}}(A, A) = 1$). Supposons le résultat vrai pour toutes les parties $A \subset B$ telles que $\sharp(B-A) = k$ et montrons le résultat pour un couple B, A , où $A \subset B$ et $\sharp(B-A) = k+1$. Alors

$$\sum_{A \subset T \subset B} \mu_{\mathbb{L}}(A, T) = 0$$

et par hypothèse de récurrence

$$\sum_{A \subset T \subsetneq B} (-1)^{\sharp T - \sharp A} + \mu_{\mathbb{L}}(A, B) = 0.$$

Or il y a autant de parties entre A et B ayant un nombre pair d'éléments que de parties ayant un nombre impair d'éléments par suite

$$\sum_{A \subset T \subset B} (-1)^{\sharp T - \sharp A} = 0$$

donc

$$\mu_{\mathbb{L}}(A, B) = (-1)^{\sharp B - \sharp A}.$$

Transformation de Reed et Müller

Soit $\mathbb{L} = \{0, 1\}^m$. Si $u = (u_1, u_2, \cdots, u_m) \in \mathbb{L}$ notons

$$supp(u) = \{i | u_i \neq 0\}.$$

Sur $\mathbb{L}$on considère la relation d'ordre

$$(u \leq v) \Longleftrightarrow (supp(u) \subset supp(v)).$$

Dans ce cas la fonction de Möbius est

$$\mu_{\mathbb{L}}(u, v) = (-1)^{\sharp supp(u) - \sharp supp(v)}.$$

Preuve : On se ramène clairement à l'exemple précédent des parties d'un ensemble fini.

Remarquons qu'on sait que si f est une fonction booléenne de m variables booléennes et si on pose

$$g(u) = \sum_{v \le u} f(v)$$

alors

$$f(u) = \sum_{v \le u} g(v).$$

On est ici dans un cas où une formule d'inversion (transformation de Reed Müller) ne nous permet pas de retrouver la fonction de Mobius (bien sûr à partir de la fonction de Mobius on retrouve cette formule puisque dans $\{0,1\}$ 1=-1).

Formule d'inclusion exclusion

Soit E un ensemble fini non vide, $P_1, P_2, \cdots, P_n$, des sous ensembles de E. Notons S l'ensemble $\{1, \cdots, n\}$ et $\mathcal{P}(S)$ l'ensemble de ses parties, ordonné par inclusion. Définissons les fonctions f et g de $\mathcal{P}(S)$ dans $\mathbb{Z}$ par

$$f(I) = \sharp\Big(\bigcap_{i \in I} P_i \bigcap_{i \notin I} \overline{P_i}\Big)$$

$$g(I) = \sharp\Big(\bigcap_{i \in I} P_i\Big).$$

Rappelons que si $I = \emptyset$ alors $\bigcap_{i \in I} P_i = E$.
On vérifie que

$$g(I) = \sum_{I \subset J} f(J),$$

et donc par inversion

$$f(I) = \sum_{I \subset J} (-1)^{\sharp J - \sharp I} g(J).$$

En particulier si $I = \emptyset$ alors

$$\sharp\Big(\bigcap_{1 \le i \le n} \overline{P_i}\Big) = \sum_{k \ge 0} (-1)^k \sum_{\sharp J = k} g(J),$$

ou encore par passage au complémentaire

$$\sharp\Big(\bigcup_{1\leq i\leq n} P_i\Big) = \sharp E - \sum_{k\geq 0}(-1)^k \sum_{\sharp J=k} g(J) = \sum_{k\geq 1}(-1)^{k+1} \sum_{\sharp J=k} g(J).$$

Familles d'hyperplans

Soit $\mathcal{A}$ un arrangement d'hyperplans (nombre fini d'hyperplans d'un espace vectoriel de dimension finie V). Soit $\mathbb{L} = L(\mathcal{A})$ l'ensemble des intersections d'éléments de $\mathcal{A}$. Sur $\mathbb{L}$on met la relation d'ordre $(X \leq Y) \Longleftrightarrow (Y \subset X)$. La fonction de Möbius obtenue est appelée fonction de Möbius de l'arrangement. Cette fonction dépend de l'arrangement. Dans certains cas particulier on sait calculer cette fonction.

Remarquons que V qui peut être considéré comme l'intersection de zéro éléments de $\mathcal{A}$ est dans $\mathbb{L}$, et avec la relation d'ordre considérée, V est le plus petit élément de $\mathcal{A}$. On définit alors

$$\mu(X) = \mu(V, X).$$

Dans le cas où $V = \mathbb{F}_q^n$ on obtient la formule

$$\sharp\Big(\bigcup_{H\in\mathcal{A}} H\Big) = q^n - \sum_{X\in\mathbb{L}} \mu(X) q^{dim(X)}.$$

Pour démontrer cette formule il suffit de montrer que

$$\sharp\Big(\bigcap_{H\in\mathcal{A}} \overline{H}\Big) = \sum_{X\in\mathbb{L}} \mu(X) q^{dim(X)}.$$

Ceci se fait comme pour la formule d'inclusion exclusion. Soit $X \subset \mathbb{L}$, et $\mathcal{B}(X)$ le sous ensemble de $\mathcal{A}$ constitué des hyperplans qui contiennent X. définissons

$$f(X) = \sharp\Big(X \bigcap_{H\notin\mathcal{B}(X)} \overline{H}\Big)$$

et

$$g(X) = \sharp X.$$

Alors on vérifie que

$$g(X) = \sum_{X\leq Y} f(Y)$$

et donc
$$f(X) = \sum_{X \leq Y} \mu(X,Y) g(Y).$$
Si on prend $X = V$ on trouve la formule annoncée.

4.5.5 Aspect fonctionnel

Soit $\mathbb{L}$un ensemble **fini ordonné** par une relation notée $\leq$. Notons $\mathbb{A}(\mathbb{L})$ l'espace des fonctions f de $\mathbb{L} \times \mathbb{L}$ dans $\mathbb{R}$ telles que $f(x,y) = 0$ si $x \not\leq y$. Définissons en outre la multiplication dans $\mathbb{A}(\mathbb{L})$ par
$$f \star g(x,y) = \sum_{x \leq z \leq y} f(x,z) g(z,y).$$
On obtient ainsi une algèbre dont l'unité est
$$\delta(x,y) = \begin{cases} 1 & \text{si } x = y, \\ 0 & \text{sinon.} \end{cases}$$

Théorème 4.5.3 *Un élément f de l'algèbre $\mathbb{A}(\mathbb{L})$ a un inverse si et seulement si $f(x,x) \neq 0$.*

La condition est nécessaire car dans ce cas
$$\sum_{x \leq z \leq y} f(x,z) g(z,y) = \delta(x,y),$$
ce qui donne pour $x = y$, $f(x,x)g(x,x) = 1$. Réciproquement, l'égalité précédente définit $g(x,y)$ lorsque $\sharp[x,y] = 1$. Par récurrence en supposant $g(x,y)$ défini lorsque $\sharp[x,y] = k$, montrons qu'on peut définir $g(x,y)$ lorsque $\sharp[x,y] = k+1$. Pour cela puisque $x \neq y$ il suffit de voir qu'en prenant
$$f(x,x)g(x,y) = -\sum_{x < z \leq y} f(x,z) g(z,y)$$
on obtient ce qu'il faut (on obtient un inverse à gauche, mais comme pour tout h on a $\delta \star h = h \star \delta = h$, c'est aussi un inverse à droite).

Définition 4.5.3 *La fonction ζ définie par*
$$\zeta(x,y) = \begin{cases} 1 & \text{si } x \leq y, \\ 0 & \text{sinon.} \end{cases}$$
est la **fonction zeta**.

Théorème 4.5.4 *La fonction zeta a un inverse qui est la fonction de Möbius.*

Pour le montrer il suffit d'effectuer la convolution $\mu \star \zeta$ ou la convolution $\zeta \star \mu$. Dans les deux cas on trouve facilement δ.

Ce dernier résultat permet en fait de rétablir la formule d'inversion de Rota. Pour ce faire il faut tout d'abord remarquer que puisqu'on suppose $\mathbb{L}$ fini, on peut toujours lui rajouter un élément noté 0 plus petit que tous les autres. Dans ces conditions si on définit

$$G = F \star \zeta$$

on a alors

$$F = G \star \mu.$$

En posant $g(x) = G(0, x)$ et $f(x) = F(0, x)$ et en plus en posant $F(0, 0) = 0$ (ce qui implique $G(0, 0) = 0$) on obtient d'une part

$$g(x) = G(0, x) = F \star \zeta(0, x) = \sum_{0 \leq z \leq x} F(0, z)\zeta(z, x),$$

$$g(x) = \sum_{z \leq x} f(z),$$

d'autre part

$$f(x) = F(0, x) = G \star \mu(0, x) = \sum_{z \leq x} \mu(z, x) f(z).$$

4.5.6 Produit d'ensembles ordonnés

Soient $\mathbb{L}_1, \cdots, \mathbb{L}_n$ des ensembles ordonnés finis. On considère l'ensemble $\mathbb{L} = \prod_{i=1}^n \mathbb{L}_i$ ordonné par l'ordre produit ($x \leq y$ si et seulement si $x_i \leq y_i$ pour tout i).

Théorème 4.5.5 *La fonction de Möbius du produit* $\mathbb{L}$ *est le produit des fonctions de Möbius des* $\mathbb{L}_i$.

Ceci se voit facilement en utilisant la fonction zeta qui vérifie clairement

$$\zeta(x,y) = \prod_{i=1}^{m} \zeta_i(x_i,y_i)$$

en conséquence de quoi la fonction

$$\prod_{i=1}^{m} \mu_i(x_i,y_i)$$

est l'inverse pour la convolution de la fonction zeta. Cest donc la fonction de Möbius.

Exemple: Définissons pour tout nombre premier p l'ensemble

$$E_p = \{1, p, p^2, \cdots, p^k, \cdots\}$$

que nous munissons de l'ordre naturel. Ainsi la fonction de Möbius de E_p est

$$\mu_p(p^i,p^j) = \begin{cases} 1 & \text{si } i = j, \\ -1 & \text{si } j = i+1, \\ 0 & \text{dans les autres cas.} \end{cases}$$

Le produit des ensembles ordonnés E_p (limité aux suites formées de 1 à partir d'un certain rang) n'est rien d'autre que $\mathbb{N}$ ordonné par la divisibilité. On obtient ainsi la fonction de Möbius classique comme produit des fonctions de Möbius des E_p.

4.6 Annexe II: Fonctions définies sur $\mathbb{Z}/n\mathbb{Z}$

On fixe un entier $n \geq 2$. Notons G le groupe $\mathbb{Z}/n\mathbb{Z}$ et $\mathcal{F}$ l'espace des fonctions définies sur G à valeurs dans le corps des nombres complexes $\mathbb{C}$.

4.6.1 L'espace des fonctions définies sur $\mathbb{Z}/n\mathbb{Z}$

A tout élément a de G on associe la fonction e_a définie par

$$e_a(x) = \begin{cases} 1 & si \quad x = a, \\ 0 & si \quad x \neq a. \end{cases}$$

1) Montrer que la famille $(e_a)_{0\leq a\leq n-1}$ est une base de $\mathcal{F}$. Ainsi $\mathcal{F}$ est un espace vectoriel sur $\mathbb{C}$, de dimension n.

2) Soit $f \in \mathcal{F}$. Quelles sont les composantes de f sur la base $(e_a)_{0\leq a\leq n-1}$.

3) Décrire la base duale de la base $(e_a)_{0\leq a\leq n-1}$.

4.6.2 Les caractères de G

A tout élément u de G on associe la fonction χ_u définie par

$$\chi_u(v) = e^{\frac{2i\pi uv}{n}}.$$

1) Montrer que les fonctions χ_u vérifient

$$\chi_u(x+y) = \chi_u(x)\chi_u(y), \tag{4.1}$$

$$\chi_u(0) = 1. \tag{4.2}$$

2) Montrer qu'on obtient ainsi toutes les fonctions complexes définies sur G vérifiant (1) et (2).

4.6.3 Produit scalaire hermitien sur $\mathcal{F}$

1) Montrer qu'on définit sur $\mathcal{F}$ un produit scalaire hermitien en posant

$$< f, g >= \sum_{u\in G} f(u)\overline{g(u)}.$$

2) Montrer que la base $(e_a)_{0\leq a\leq n-1}$ est orthonormée.

3) Calculer pour tout u et tout v dand G le produit scalaire $< \chi_u, \chi_v >$. En conclure que la famille $(\chi_u)_{0\leq u\leq n-1}$ est une base de $\mathcal{F}$, et que cette base est orthogonale.

4) Calculer en fonction des valeurs prises par f, les composantes de f dans la base $(\chi_u)_{0\leq u\leq n-1}$.

4.6.4 Transformation de Fourier

Pour toute fonction $f \in \mathcal{F}$, on définit la fonction $\widehat{f} \in \mathcal{F}$, par

$$\widehat{f}(v) = \sum_{u\in G} f(u)e^{-\frac{2i\pi uv}{n}}.$$

1) Montrer que

$$f(u) = \frac{1}{n}\sum_{v\in G}\widehat{f}(v)e^{\frac{2i\pi uv}{n}}.$$

En conclure que

$$\widehat{\widehat{f}}(u) = nf(-u).$$

2) Comparer $< f, g >$ et $< \widehat{f}, \widehat{g} >$. Comparer la norme de f avec celle de $\widehat{f}$.

3) Notons F l'opérateur de $\mathcal{F}$ qui à f associe $\widehat{f}$. Quelle est la norme de l'opérateur F.

4) Calculer $\widehat{f}$ lorsque $f = e_u$ et lorsque $f = \chi_u$.

4.6.5 Matrices associées aux objets précédents

1) Quelle est la matrice de F si $\mathcal{F}$ est muni de la base $(e_a)_{0\leq a\leq n-1}$?

2) Quelle est la matrice de F si $\mathcal{F}$ est muni de la base $(\chi_u)_{0\leq u\leq n-1}$?

3) Calculer Det(F).

4) Calculer la matrice de passage P ainsi que son inverse, de la base $(e_a)_{0\leq a\leq n-1}$ à la base $(\chi_u)_{0\leq u\leq n-1}$.

4.6.6 Fonctions de $\mathcal{F}$ et polynômes formels

A tout fonction $f \in \mathcal{F}$ on associe le polynôme $P_f \in \mathbb{C}[X]$ de degré $\leq n-1$ défini par

$$P_f(X) = f(0) + f(1)X + \cdots + f(n-1)X^{n-1}.$$

Montrer que

$$\widehat{f}(v) = P_f(e^{-\frac{2i\pi v}{n}}),$$

et que

$$f(u) = \frac{1}{n}P_{\widehat{f}}(e^{\frac{2i\pi u}{n}}).$$

En conclure un algorithme pour trouver le polynôme P d'interpolation de Lagrange, de degré $\leq n-1$, qui prend des valeurs données aux n points $e^{\frac{2i\pi u}{n}}$.

4.6.7 Convolution et filtres stationnaires

On définit la convolée $f_1 * f_2$ de deux fonctions de $\mathcal{F}$ par

$$f_1 * f_2(x) = \sum_{y \in G} f_1(x+y) f_2(-y).$$

1) Montrer que

$$f_1 * f_2(x) = f_2 * f_1(x) = \sum_{u+v=x} f_1(u) f_2(v).$$

2) Calculer $\widehat{f1 * f_2}$ et $\widehat{f_1 f_2}$.

3) Etudier $P_{f_1 * f_2}$ en fonction de P_{f_1} et P_{f_2}.

4) Pour tout $t \in G$ soit T_t l'opérateur de translation qui à la fonction f fait correspondre la fonction $T_t(f)$ telle que $T_t(f)(x) = f(x+t)$. Soit H un opérateur qui commute avec T_t pour tout t. Montrer que les χ_u forment une base de vecteurs propres de H. Quelles sont les valeurs propres associées? Montrer qu'il existe une fonction $h \in \mathcal{F}$ telle que pour tout $f \in \mathcal{F}$, on ait $H(f) = h * f$.

4.7 Annexe III: Définitions de base de l'algèbre commutative

4.7.1 Anneaux

Un **anneau** A est un ensemble non vide muni de deux opérations internes (**addition** et **multiplication**) telles que

A-1) A est un **groupe abélien** pour l'addition.

A-2) La multiplication est **associative** et **distributive** par rapport à l'addition.

Dans la suite les anneaux seront

A-3) **commutatifs**

A-4) **unitaires** (l'élément unité est noté 1).

Remarque: On peut avoir $1 = 0$, (0 est l'élément neutre de l'addition) et dans ce cas $A = \{0\}$.

4.7.2 Homomorphismes

Un **homomorphisme** d'anneaux est une application f d'un anneau A dans un anneau B telle que

H-1) $f(x+y) = f(x) + f(y)$ (et donc $f(0) = 0$ et aussi $f(-x) = -f(x)$)

H-2) $f(xy) = f(x)f(y)$

H-3) $f(1) = 1$.

4.7.3 Sous Anneaux

Un **sous anneau** B de l'anneau A est un sous ensemble B de A tel que

SA-1) B est fermé pour l'addition

SA-2) B est fermé pour la multiplication

SA-3) B contient l'unité 1 de l'anneau A.

Remarque: B a une structure d'anneau pour les opérations induites par celles de A.

4.7.4 Idéaux

Un **idéal** d'un anneau A est un un sous ensemble $\mathcal{I}$ de A tel que

I-1) $\mathcal{I}$ est un sous groupe de A

I-2) $A\mathcal{I} \subset \mathcal{I}$.

4.7.5 Anneaux quotients

$\mathcal{I}$ étant un idéal de A on définit sur A la relation

$$x \equiv y \Longleftrightarrow x - y \in \mathcal{I}$$

Cette relation est une relation d'équivalence, $A/\mathcal{I}$ est l'ensemble des classes.

Remarque: On notera $\overline{x}$ la classe de x.
Sur $A/\mathcal{I}$ on définit une structure d'anneau en posant

AQ-1) $\overline{x} + \overline{y} = \overline{x+y}$

AQ-2) $\overline{x}\ \overline{y} = \overline{xy}$.

L'anneau $A/\mathcal{I}$ est appelé **anneau quotient** de l'anneau A par l'idéal $\mathcal{I}$. L'application s de A sur $A/\mathcal{I}$ qui à tout élément x fait correspondre sa classe est un homomorphisme surjectif dont le **noyau** est $\mathcal{I}$. C'est la **surjection canonique**.

De plus si f est un homomorphisme de A dans B alors le noyau $Ker(f) = f^{-1}(0)$ de f est un idéal de A.

Ainsi les **idéaux** sont les **noyaux** des **homomorphismes**.

4.7.6 Factorisation des homomorphismes

Soit f un homomorphisme surjectif de A sur B. Il existe une application bijective g et une seule de $A/Ker(f)$ sur B telle que $f = g \circ s$ où s est la surjection canonique de A sur $A/Ker(f)$.

$$\begin{tikzcd} \mathrm{A} \arrow[r, "\mathrm{f}"] \arrow[d, "\mathrm{s}"'] & \mathrm{B} \\ \mathrm{A/Ker(f)} \arrow[ur, "\mathrm{g}"'] & \end{tikzcd}$$

4.7.7 Diviseurs de zéro

Un **diviseur de zéro** est un élément x non nul tel qu'il existe un y non nul réalisant xy=0.

Un anneau sans diviseurs de zéro est un anneau **intègre**.

Une **unité** est un élément x inversible (il existe y tel que xy=1). L'ensemble des unités est un groupe multiplicatif.
Un élément x est **nilpotent** s'il existe un entier $n > 0$ tel que $x^n = 0$. Dans ce cas x est un diviseur de zéro.

Un **corps** est un anneau dans lequel $1 \neq 0$ et tout élément non nul est inversible.

4.7.8 Idéaux premiers - Idéaux maximaux

Un idéal **premier** dans A est un idéal $\mathcal{P}$ différent de A vérifiant

$$xy \in \mathcal{P} \Longrightarrow x \in \mathcal{P} \; ou \; y \in \mathcal{P}.$$

Un idéal **maximal** est un idéal $\mathcal{M}$ différent de A tel que pour tout idéal $\mathcal{I}$

$$\mathcal{M} \subset \mathcal{I} \Longrightarrow \mathcal{I} = \mathcal{M} \; ou \; \mathcal{I} = A.$$

On dispose des deux résultats suivants

$$\mathcal{P} \; premier \Longleftrightarrow A/\mathcal{P} \; est \; integre$$
$$\mathcal{M} \; maximal \Longleftrightarrow A/\mathcal{M} \; est \; un \; corps.$$

En conséquence **tout idéal maximal est premier**.

- Tout anneau $\neq \{0\}$ a un idéal maximal.
- Tout idéal $\mathcal{I} \neq A$ est contenu dans un idéal maximal.
- Tout élément non unitaire de A est contenu dans un idéal maximal.

4.7.9 Radical

L'ensemble $\mathcal{N}$ de tous les éléments nilpotents dans l'anneau A est un idéal et $A/\mathcal{N}$ n'a aucun élément nilpotent non nul.

L'idéal $\mathcal{N}$ est appelé le **nilradical** de A.

Le **nilradical** de A est **l'intersection de tous les idéaux premiers** de A. Le **radical de Jacobson** $\mathcal{R}$ de A est **l'intersection de tous les idéaux maximaux** de A.

L'idéal $\mathcal{R}$ est caractérisé par

$$x \in \mathcal{R} \Longleftrightarrow 1 - xy \; est \; une \; unité \; de \; A \; pour \; tout \;\; y.$$

Soit $\mathcal{A}$ un idéal. On appelle **radical** de $\mathcal{A}$

$$r(\mathcal{A}) = \{x \in A | x^n \in \mathcal{A} \; pour \; un \; n > 0\}$$

Le **radical** d'un **idéal** $\mathcal{A}$ est **l'intersection des idéaux premiers** contenant $\mathcal{A}$.

4.7.10 Opérations sur les idéaux

On définit pour deux idéaux $\mathcal{A}$ et $\mathcal{B}$

- Leur **somme** $\mathcal{A}+\mathcal{B}$ (ensemble des $a+b$ ou $x \in \mathcal{A}$ et $b \in \mathcal{B}$).
- Leur **intersection** $\mathcal{A} \cap \mathcal{B}$.
- Leur **produit** $\mathcal{A}\mathcal{B}$ (idéal engendré par les produits xy).

4.7.11 Localisation d'un anneau

Un sous ensemble S de A est **multiplicativement clos** si

MC-1) $1 \in S$

MC-2) $a \in S$ et $b \in S \Longrightarrow ab \in S$.

Sur $A \times S$ on définit la relation d'équivalence
$(a,s) \equiv (b,t) \Longleftrightarrow \exists u \in S$ tel que $(at-bs)u=0$.
On note $S^{-1}A$ l'ensemble des classes d'équivalence, qu'on munit d'une structure d'anneau en posant

$a/s + b/t = (at+bs)/st$

$(a/s)(b/t) = (ab/st)$

(où a/s dénote la classe de (a,s)).

Remarque: On identifiera $x/1$ avec x pour tout $x \in A$.
Dans $S^{-1}A$, les éléments de S sont **inversibles**.

Si A est **intègre** et si $S = A \setminus \{0\}$ alors $S^{-1}A$ est le **corps des fractions** de A.

Si $\mathcal{P}$ est un **idéal premier** alors $S = A \setminus \mathcal{P}$ est multiplicativement clos. La **localisation** de A en $\mathcal{P}$ est

$$A_{\mathcal{P}} = S^{-1}A$$

tout élément de $A_{\mathcal{P}}$ s'écrit a/s où $a \in A$ et $s \notin \mathcal{P}$.
Les éléments a/s où $a \in \mathcal{P}$ et $s \notin \mathcal{P}$ forment un idéal $\mathcal{M}$ de $A_{\mathcal{P}}$.

$\mathcal{M}$ est **l'unique idéal maximal** de $A_{\mathcal{P}}$.

L'anneau $A_{\mathcal{P}}$ est un **anneau local** (anneau ayant un seul idéal maximal).

4.7.12 Décomposition primaire

Un idéal **primaire** dans A est un idéal $\mathcal{Q}$ différent de A vérifiant

$$xy \in \mathcal{Q} \Longrightarrow x \in \mathcal{Q} \text{ ou } y^n \in \mathcal{Q} \text{ pour un certain } n.$$

Donc $\mathcal{Q}$ est primaire si et seulement si $A/\mathcal{Q} \neq \{0\}$ et si tout diviseur de zéro dans $A/\mathcal{Q}$ est nilpotent.

• Si $\mathcal{Q}$ est un idéal primaire de A, le radical $r(\mathcal{Q})$ est le plus petit idéal premier contenant $\mathcal{Q}$.

Si $\mathcal{P} = r(\mathcal{Q})$ on dira que l'idéal $\mathcal{Q}$ est $\mathcal{P} - primaire$.

• Si $\mathcal{A}$ est un idéal tel que $r(\mathcal{A})$ soit maximal, alors $\mathcal{A}$ est primaire.

Bibliographie

[1] **T.M. Apostol,** *Introduction to analytic number theory.* Springer-Verlag, 1976

[2] **L. Chambadal,** *Calcul pratique.* Hachette, 1983

[3] **COMAP,** *Principles and practice of Mathmatics.* Springer-Verlag, 1997

[4] **M. Demazure,** *Cours d'algèbre.* Cassini, 1997

[5] **M. Mignotte,** *Mathématiques pour le calcul formel.* Puf, 1989