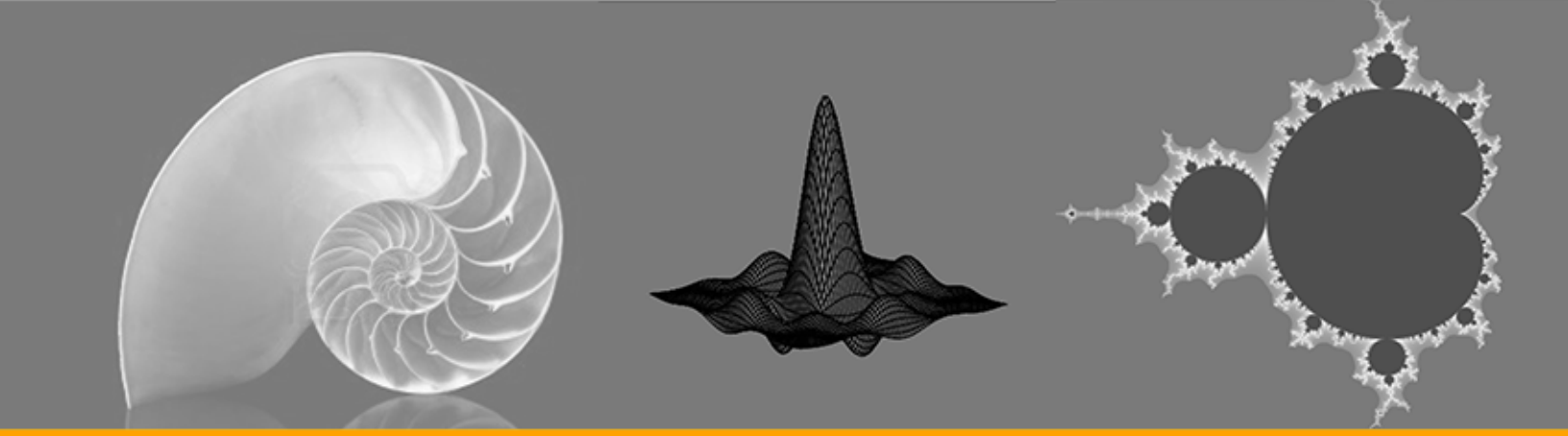


Théorie des nombres

Nicolas Bouffard

Université de Saint-Boniface
Une éducation supérieure depuis 1818

Dernière mise à jour :
8 septembre 2018 à 20:30

Table des matières

1 La divisibilité **5**
- 1.1 Historique . . . 5
- 1.2 Définition des nombres naturels et entiers . . . 7
- 1.3 Utilisation de l'induction . . . 9
- 1.4 Le théorème du binôme . . . 12
- 1.5 La divisibilité . . . 14
- 1.6 La division euclidienne . . . 14
- 1.7 Le plus grand commun diviseur . . . 15
- 1.8 Le plus petit commun multiple . . . 20
- 1.9 Les nombres premiers . . . 22
- 1.10 La crible d'Ératosthène . . . 24
- 1.11 Exercices . . . 25

2 Les modulos **27**
- 2.1 Les nombres modulos . . . 27
- 2.2 Les théorèmes de Fermat, Euler et Wilson . . . 32
- 2.3 L'équation $ax = b$ en modulo . . . 35
- 2.4 Le théorème du reste Chinois . . . 37
- 2.5 Les polynômes irréductibles . . . 41
- 2.6 La cryptographie RSA . . . 41
- 2.7 Exercices . . . 46

3 Les fonctions arithmétiques **49**
- 3.1 Introduction aux fonctions arithmétiques . . . 49
- 3.2 Les fonctions multiplicatives et le produit de Dirichlet . . . 50
- 3.3 La fonction $\tau(n)$ . . . 53
- 3.4 La fonction $\sigma(n)$ . . . 55
- 3.5 Les fonctions $\omega(n)$ et $\mu(n)$ . . . 57
- 3.6 La fonction $\phi(n)$ . . . 59
- 3.7 La fonction $\pi(n)$ . . . 61
- 3.8 Les nombres parfaits . . . 63
- 3.9 Exercices . . . 66

4 Les équations diophantiennes **67**
- 4.1 Introduction . . . 67
- 4.2 Les équations linéaires . . . 68
- 4.3 L'équation pythagoricienne . . . 70
- 4.4 La méthode de descente infinie de Fermat . . . 73
- 4.5 Le grand théorème de Fermat . . . 74
- 4.6 Le théorème des deux carrés de Fermat . . . 76
- 4.7 Le problème de Waring . . . 79
- 4.8 Exercices . . . 81

5 La réciprocité quadratique **83**
5.1 Les résidus quadratiques 83
5.2 Le symbole de Legendre 83
5.3 Le critère d'Euler 85
5.4 Les lois complémentaires 86
5.5 La loi de réciprocité quadratique 88
5.6 Exercices 94

Appendice 1 : Petit théorème de Fermat version algébrique **95**

Appendice 2 : Petit théorème de Fermat version combinatoire **99**

Appendice 3 : Différence finie **101**

Bibliographie **103**

Index **105**

Chapitre 1

La divisibilité

1.1 Historique

L'origine des mathématiques est très ancienne. Elle précède de plusieurs millénaires l'invention de l'écriture. En effet, l'un des plus anciens artefacts connus attestant de l'utilisation des mathématiques est le baton d'Ishango, retrouvé dans ce qui est aujourd'hui l'est du Congo, et qui est daté d'environ 35000 ans. Il s'agit d'un simple baton muni de trois rangés de traits, et qui semble avoir été utilisé pour compter.

Originalement, les mathématiques étaient principalement concentrés autour de deux disciplines : L'arithmétique et la géométrie. L'arithmétique étant l'étude des nombres, et la géométrie l'étude des figures. Au début, l'arithmétique était un simple outil comptable pour tenir un inventaire, faire un recensement, etc. L'évolution de l'arithmétique est ce qui deviendra plus tard la théorie des nombres. Il s'agit de l'étude des propriétés des nombres naturels, ou plus généralement des entiers.

On retrouve des traces de théorie des nombres dès l'époque babylonienne. En effet, des tablettes d'argile retrouvé nous montrent une liste de solutions entières à l'équation Pythagoricienne ($x^2 + y^2 = z^2$). À noter que le théorème de Pythagore était connu de l'époque des babyloniens, et ce bien avant la naissance de Pythagore.

À l'époque de Pythagore (environ 580 B.C. à 495 B.C.), l'arithmétique se transforme et devient une science des nombres proprement parlé avec un côté mystique important. On lui attribue souvent la citation suivante :

« Tout est nombres »

Pythagore

La vie de Pythagore reste encore aujourd'hui très peu connue. La plupart de ce qui est connu sur Pythagore fait plutôt référence à son école, et les textes qui lui sont attribués sont en fait apocryphes. Les pythagoriciens (5e siècle avant J.-C.) associaient à chaque nombre une signification mystique. Le nombre 1 était divin, 2 représentait le féminin, 3 le masculin, 5 le mariage (2+3=5), puis le nombre 6 était associé à la perfection car il est la somme de ses diviseur (1+2+3=6). Un nombre ayant cette propriété fut ensuite appellé nombre parfait dans les livres d'Euclide. C'est probablement ce côté mystique des nombres qui amena les pythagoriciens à les étudier plus un détail.

Vient ensuite Euclide (Environ 300 B.C.) qui fera une axiomatisation complète des mathématiques de son époque. Les démonstrations mathématiques deviennent de plus en plus importantes. Il écrit un ensemble de 13 volumes (Les éléments d'Euclide) qui contient encore aujourd'hui l'essentiel de la géométrie élémentaire, mais aussi de l'arithmétique. Ainsi, on retrouvera dans le cours MATH-2501 plusieurs résultats portant son nom, par exemple le lemme d'Euclide, l'algorithme d'Euclide qui sert à calculer le PGCD, ou bien un théorème sur l'infinitude des nombres premiers.

On peut ensuite noter le mathématicien Diophante d'Alexandrie (3e siècle) qui s'intéressa entre autres aux solutions entières de plusieurs équations algébriques. Il publia lui aussi une série de 13 volumes (Les arithmétiques) qui influenceront grandement l'évolution de la théorie des nombres. Il est cependant à noté que seul 10 des 13 livres ont survécu jusqu'à aujourd'hui. Autre fait important à noter, bien que ces livres traitent

d'équations algébriques, la notation algébrique n'existait pas encore et la formulation de ces problèmes était donc très différente de la notation moderne.

Au moyen-âge, l'Europe se désintéresse de la théorie des nombres, ou même des mathématiques en général. C'est du côté de l'Inde et de la Chine (entre autres) que la théorie des nombres continue à se développer rapidement. Brahmagupta (né en 598), un mathématicien indien, résout l'équation diophantienne linéaire $ax + by = c$. Par le 4e siècle, les mathématiciens chinois ont résolu plusieurs cas du théorème du reste chinois sur les solutions d'un ensemble de congruence linéaire.

La théorie des nombres reviendra en force en Europe avec entre autres Fermat (1601 - 1665). Ce dernier démontra un nombre considérable de résultats en théorie des nombres, et contribuera à faire connaitre le sujet en lançant des défis à la communauté mathématiques de l'époque. Le grand théorème de Fermat en est certainement le plus connu. Il affirme qu'il n'existe aucun entier (autre que 0 et 1) qui satisfont l'équation $x^n + y^n = z^n$ lorsque $n \geq 2$. Fermat écrit à ce sujet la remarque ci dessous dans la marge du livre Les Arithmétiques de Diophante.

> « Au contraire, il est impossible de partager soit un cube en deux cubes, soit un bicarré en deux bicarrés, soit en général une puissance quelconque supérieure au carré en deux puissances de même degré : j'en ai découvert une démonstration véritablement merveilleuse que cette marge est trop étroite pour contenir »
>
> Pierre de Fermat
> 1601 – 1665

Fermat n'a cependant laissé aucune trace de sa démonstration, et la communauté mathématiques a aujourd'hui de sérieux doutes que cette preuve, si elle a existé, ait pu être correcte. La première démonstration connue de ce théorème est due à Andrew Wiles (né en 1953) qui la publia en 1994. Sa démonstration est particulièrement difficile et est basée sur des outils mathématiques encore inexistants à l'époque de Fermat.

La théorie des nombres continua par la suite à se développer de plus en plus rapidement. Elle intéressa plusieurs des grands mathématiciens du 18e et 19e siècle qui y laisseront leur marque. On notera entres autres Euler, Lagrange, Legendre et Gauss. La théorie des nombres commence alors à se fractionner en différentes branches. Les plus importantes (à comprendre comme étant les plus connus) étant la théorie des nombres élémentaires, la théorie des nombres analytiques, et la théorie des nombres algébriques. Ces trois branches se différentient principalement par les outils qui y sont utilisés.

1. La théorie des nombres élémentaires est essentiellement l'étude des propriétés des nombres qui ne nécessite pas l'utilisation de mathématiques avancés tel que le calcul différentiel et intégral, ou bien les structures algébriques. On y étudie entre autre la divisibilité, du PGCD et PPCM, de la factorisation en nombres premiers, les congruences modulos, etc.
2. La théorie des nombres analytique utilise les techniques du calcul différentiel et intégral, ainsi que de l'analyse réel et/ou complexe pour déduire des propriétés des nombres. On y traite entre autres de la distribution des nombres premiers ou de la conjecture de Riemann (voir fonction zeta de Riemann).
3. La théorie des nombres algébriques utilise les techniques de l'algèbre moderne pour étudier les propriétés des nombres. Dans ce cas, on étudie certaines propriétés des groupes, des anneaux, des idéaux, etc, qui ont des propriétés semblables à des objets familiers de la théorie des nombres tel que les nombres premiers ou l'algorithme d'Euclide. Parmi les sujets d'intérêt en théorie algébrique des nombres on retrouve, par exemple, la démonstration du grand théorème de Fermat et plusieurs des outils qui ont été nécessaire pour développer la démonstration.

La théorie des nombres est à la fois l'un des sujets les plus faciles, et les plus difficiles des mathématiques. En effet, plusieurs des résultats que nous verrons dans ce cours sont particulièrement faciles à énoncer et à comprendre. Plusieurs des sujets traités ont déjà été mentionnés dans vos cours de mathématiques de l'école élémentaire. Plusieurs des grandes conjectures de la théorie des nombres peuvent être comprises par des gens ayant peu de connaissance en mathématiques. Pourtant, bien que plusieurs de ces conjectures sont particulièrement facile à énoncer, elles restent parmi les les problèmes les plus difficiles des mathématiques actuels. On peut penser par exemple au grand théorème de Fermat qui s'énonce de manière très simple, mais qui a pris plus de 350 ans pour être démontré.

Curieusement, bien que la théorie des nombres soit l'une des disciplines ayant été la plus étudiée dans l'histoire des mathématiques, elle ne possède que très peu d'applications (pour le moment). On retrouve bien sur plusieurs applications élémentaires permettant de simplifier quelques calculs comme le calcul du PGCD pour simplifier une fraction, ou bien faire la somme des chiffres d'un nombre pour savoir si ce dernier est divisible par 3 ou par 9. Par contre, les choses commencent à changer, et ce de manière très rapide. En effet, l'application la plus importante de la théorie des nombres est sans doute la cryptographie RSA qui est devenu particulèrement répandu avec l'utilisation d'internet. Cette technique que nous étudierons à la fin du chapitre 3 est en fait très récente. Elle a été décrite pour la première fois en 1977. Cette technique fait appel au concept de nombres premiers, la décomposition en facteurs premiers, les congruences modulos et le petit théorème de Fermat. La fonction ϕ d'Euler y joue aussi aussi un rôle particulièrement important. On remarque donc que la plupart des notions des trois premiers chapitres se retrouvent dans la cryptographie RSA.

Nous allons maintenant compléter cette section avec une citation attribuée au mathématicien Dedekind, et qui illustre en quelque sorte le point de départ de notre cours.

> « Dieu a donné à l'homme le nombre entier, l'homme a fait le reste. »
>
> Richard Dedekind
> 1831 - 1916

1.2 Définition des nombres naturels et entiers

La théorie des nombres est l'étude des nombres naturels, et de manière plus générale l'étude des nombres entiers. Plusieurs de leurs propriétés nous sont familières depuis l'école élémentaires. On peut parler entre autres de la divisibilité, du PGCD et PPCM, les nombres premiers et la décomposition en facteurs premiers, etc. Aucune de ces propriétés n'est particulièrement difficile à comprendre, mais pour pouvoir les étudier correctement, nous allons devoir commencer par établir des bases solides, en commençant par bien définir ce que sont les nombres naturels.

Pour ce faire, plusieurs approches sont possibles. Pendant longtemps, les nombres naturels et entiers étaient considéré comme acquis, sans aucune définition formelle, un peu comme dans la citation de Dedekind. Durant la crise des fondements mathématiques, il parut alors nécessaire d'en donner une définition formelle. Pour ce cours, nous allons commencer par définir les nombres naturels formellement à partir des axiomes de Peano, mais par la suite, seule une connaissance intuitive des nombres naturels et entiers sera nécessaire. Noter finalement que d'autres systèmes d'axiomes peuvent aussi être utilisé, mais nous n'en parlerons pas plus en détail ici.

Definition 1.2.1. (Axiomes de Peano) L'ensemble des nombres naturels (dénoté $\mathbb{N}$) est un ensemble satisfaisant les 5 axiomes suivants :

1. 1 est un nombre naturel
2. Pour chaque élément $x \in \mathbb{N}$, il existe exactement un nombre $x' \in \mathbb{N}$ appelé le successeur de x
3. Pour tout $x \in \mathbb{N}$, on a que $x' \neq 1$. En d'autre mots, le nombre 1 n'est pas le successeur d'un autre nombre naturel.
4. Si x et y sont des nombres naturels tel que $x' = y'$, alors $x = y$.
5. **(Axiome d'induction)** Si $\mathcal{M}$ est un ensemble de nombres naturels tel que $1 \in \mathcal{M}$ et tel que pour chaque $x \in \mathcal{M}$ on a que $x' \in \mathcal{M}$, alors $\mathcal{M} = \mathbb{N}$.

Notre définition des nombres naturels à partir de ces 5 axiomes peut sembler très compliqué, ce qui n'est pas très loin de la vérité. Nous allons donc, dans ce chapitre, nous concentrer sur certains points importants, et laisser la plupart des détails en exercice pour les étudiants les plus motivés. La première chose à remarquer est que notre définition ne parle absolument pas des nombres $2, 3, 4, ...$ Elle définit plutôt une fonction permettant de passer d'un nombre naturel x au nombre suivant que nous avons dénoté x'. Nous

allons donc établir la convention suivante :

$$1' = 2, \quad 2' = 3, \quad 3' = 4, \quad ..., \quad \text{etc}$$

Ceci va nous simplifier beaucoup l'écriture. De plus, un autre point important à remarquer est que notre définition ne nous parle absolument pas des opérations d'addition, de multiplication et d'ordre qui sont essentielles à l'étude de la théorie des nombres. Il faut donc en donner une définition.

Definition 1.2.2. Si x et y sont des nombres naturels, alors on définit une opération + appellée addition comme étant :

1. $x + 1 = x'$
2. $x + y' = (x + y)'$

Cette définition peut sembler particulièrement étrange, mais est, en fait, suffisante pour bien définir l'opération d'addition et en déduire ses propriétés élémentaires. Par exemple, à partir de cette définition nous pouvons maintenant démontrer formellement que $x + y = y + x$ pour tout nombre naturel x et y, et aussi que $(x + y) + z = x + (y + z)$ pour tout nombre naturel x, y, z. Bien que nous ne démontrons par les différentes propriétés de l'addition, regardons tout de même un exemple relativement simple pour illustrer notre définition.

Exemple 1.2.1. On veut calculer la valeur de $2 + 3$. Pour ce faire, on remarque que :

$$2 + 3 \quad = \quad 2 + 2' = (2 + 2)' = (2 + 1')' = ((2 + 1)')' = ((2')')' = (3')' = 4' = 5$$

ce qui est bien la valeur à laquelle nous nous attendions.

On peut ensuite donner une définition formelle de la multiplication. Pour ce faire, nous utiliserons une approche semblable à ce que nous avons fait pour l'addition.

Definition 1.2.3. Si x et y sont des nombres naturels, alors on définition une opération $\cdot$ appellé multiplication comme étant :

1. $x \cdot 1 = x$
2. $x \cdot y' = x \cdot y + x$

Cette approche est très technique, et vous pouvez trouver tous les détails dans le livre de Landau [5]. Pour notre cours, ce qui est important de comprendre est que les nombres naturels peuvent être définis de manière très formelle, et il est possible de faire de même avec les opérations d'addition, de multiplication et d'ordre. Par contre, pour le reste du texte, une approche plus intuitive sera suffisante. Nous allons donc définir l'ensemble des nombres naturels comme étant l'ensemble suivant :

$$\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$$

sur lequel nous pouvons définir les opérations d'addition, de multiplication et d'ordre habituel. Nous allons aussi supposer que les propriétés élémentaires de ces trois opérations sont correctes. Dans certain cas, nous allons nous permettre d'utiliser les opérations de soustraction et de division, mais dans tous les cas il faudra faire attention car ces deux opérations ne sont pas très bien définies dans les nombres naturels. Finalement, notons un résultat élémentaire, mais très important sur les nombres naturels : l'axiome du bon ordre. Cet axiome est en fait équivalent à l'axiome d'induction que nous avons énoncé précédemment, le terme axiome pourrait donc ici être remplacé par théorème.

Axiome du bon ordre : Tout ensemble non vide S de nombres naturels contient un plus petit élément (un minimum).

Les nombres naturels sont très pratiques, mais sont insuffisants pour définir la différence de n'importe quel deux nombres. On doit donc élargir $\mathbb{N}$, pour permettre de soustraire n'importe quels nombres. Ceci nous amène à définir les nombres entiers.

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

À noter qu'il est possible de donner une définition formelle des nombres entiers à partir des nombres naturels. Dans ce contexte, on définit l'ensemble des entiers de manière un peu différente. On écrira alors :

$$\mathbb{Z} = \{(a, b) : a, b \in \mathbb{N} \cup \{0\}\}$$

Puis on doit définir ce que nous entendons par l'égalité de deux nombres entiers. On aura donc :

$$(a, b) = (c, d) \text{ si et seulement si } a + d = b + c$$

Puis, on définit les opérations d'addition, de soustraction et de multiplication comme étant :

$$(a, b) + (c, d) = (a + c, b + d) \qquad (a, b) - (c, d) = (a + d, b + c) \qquad (a, b) \cdot (c, d) = (ac + bd, ad + bc)$$

Question de simplifier la notation, nous écrirons à la place de $(a, 0)$ le nombre a, puis à la place de $(0, a)$ le nombre $-a$. À partir de ces définitions, on peut démontrer les propriétés usuelles de l'addition, la soustraction et de la multiplication, ce que nous ne ferons pas ici.

Les nombres naturels et entiers sont suffisants pour l'étude de la théorie des nombres. Parmi les questions d'intérêt on notera la question de savoir quel entier peut être divisé par un entier donné (différent de 0). Par contre, pour d'autres applications, il est nécessaire de permettre la division de n'importe quel nombre (tant que le diviseur n'est pas 0). Ceci nous amène à définir l'ensemble des nombres rationnels.

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\}$$

Les nombres rationnels nous permettent de définir l'addition, la soustraction, la multiplication et la division. Par contre, il n'est toujours pas possible de faire du calcul différentiel et intégral. Pour ce faire, nous devons ajouter un nouvel axiome :

Axiome de complétude : Tout ensemble S borné supérieurement admet une plus petite borne supérieure.

On appelle compétition d'un ensemble, l'ajout à un ensemble de tout les nombres manquants pour que l'axiome de complétude soit satisfait, et c'est l'axiome de complétude qui nous amène à définir les nombres réels.

$$\mathbb{R} = \{\text{complétition de } \mathbb{Q}\}$$

Finalement, pour permettre de trouver des racines à tous les polynômes non constants, on doit aller plus loin et ajouter un nombre correspondant à $\sqrt{-1}$, ce qui nous amène à définir les nombres complexes.

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i^2 = -1\}$$

Les nombres complexes ont une particularité particulièrement importante. Ils sont algébriquement clos. La cloture algébrique est une propriété qui affirme que tout polynôme non constant et à coefficient complexe admet au moins une racine complexe.

1.3 Utilisation de l'induction

Dans la section précédente, nous avons donner une définition formelle des nombres naturels à partir des axiomes de Peano. Bien que la plupart des détails les concernant ont été omis, il est tout de même important d'étudier le 5e axiomes plus en détail avant d'aller plus loin. Le 5e axiome de Peano est appelé l'axiome d'induction. Il est particulièrement utile pour certaines démonstrations. Nous allons commencer par énoncer un théorème qui est une légère généralisation du 5e axiome.

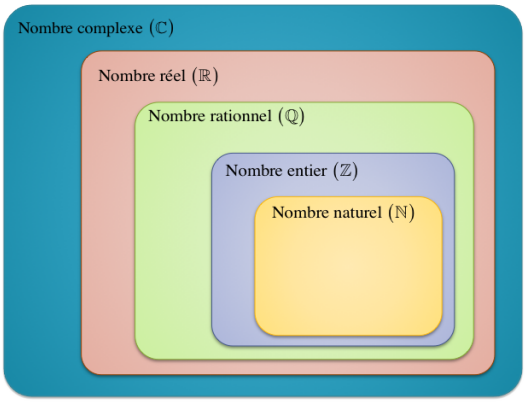


FIGURE 1.1 – Diagramme représentant les ensembles de nombres

Théorème 1.3.1. (Principe d'induction) Si P est une propriété satisfaisant les deux conditions suivantes :

1. La propriété P est vraie pour un entier a.
2. En faisant l'hypothèse que la propriété P est vraie pour un entier k (avec $k \geq a$), on peut démontrer qu'elle est aussi vraie pour l'entier $k+1$.

Alors on peut conclure que la propriété P est vraie pour tous les entiers plus grand ou égal à a.

À partir du théorème, on remarque donc qu'une démonstration par induction doit se faire en 3 étapes :

1. On commence par choisir l'entier de départ a. Il s'agit du premier entier pour lequel on veut montrer que la propriété est vraie. On doit alors démontrer que la propriété est vraie pour l'entier a.
2. On fait l'hypothèse que la propriété est vraie pour un entier $n \in \mathbb{Z}$
3. On démontre que la propriété est encore vraie pour $n+1$.

Si on parvient à compléter les trois étapes, on peut alors conclure que la propriété est vraie pour tout entier plus grand ou égal à a. Nous allons maintenant voir quelques exemples d'application du principe d'induction.

Exemple 1.3.1. On veut démontrer que pour tout nombre naturel n, on a :

$$1+2+3+4+\ldots+n = \frac{n(n+1)}{2}$$

Ou écrit de manière symbolique, on veut démontrer que :

$$\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$$

Pour ce faire, nous allons appliquer le principe d'induction.

1. On doit démontrer que la propriété est vraie lorsque $n = 1$. Pour ce faire, on remarque que :

$$\sum_{i=1}^{1} i = 1 \qquad \text{et} \qquad \frac{1(1+1)}{2} = 1$$

   donc la propriété est vraie lorsque $n = 1$.
2. Supposons maintenant que la propriété est vraie lorsque $n = k$, où k est un entier plus grand ou égal à 1. C'est à dire, on suppose que

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

3. On veut maintenant vérifier que la propriété est vraie pour $n = k+1$. On a donc :

$$\sum_{i=1}^{k+1} i = \Big(\sum_{i=1}^{k} i\Big) + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k^2+k+2k+2}{2} = \frac{(k+1)(k+2)}{2}$$

Donc à partir de notre hypothèse, on a bien que la propriété est vraie pour $n = k+1$.

Par le principe d'induction, on peut donc conclure que la propriété est vraie pour tout $n \in \mathbb{N}$.

Exemple 1.3.2. On veut utiliser l'induction pour démontrer que pour tout entier $n \geq 1$, on a que $n+4 < 7n^2$. Pour ce faire, nous allons suivre les 3 étapes d'une démonstration par induction :

1. On doit commencer par démontrer que la propriété est vraie si $n = 1$, en remplaçant dans l'équation on a : $1+4 < 7(1)^2$ ce qui est vrai car $5 < 7$. La propriété est donc vraie pour $n = 1$.
2. On fait maintenant l'hypothèse que l'inégalité est vraie pour $n = k$. C'est à dire on suppose que $k+4 < 7k^2$.
3. On veut maintenant démontrer que la propriété est encore vraie pour $n = k+1$ on a donc :

$$\begin{aligned}(k+1)+4 &= (k+4)+1\\ &< 7k^2+1 \quad \text{(hypothèse d'induction)}\\ &< (7k^2+1)+(14k+6)\\ &= 7k^2+14k+7\\ &= 7(k^2+2k+1)\\ &= 7(k+1)^2\end{aligned}$$

Ce qui est exactement ce que nous voulions montrer.

On peut donc conclure que $n+4 < 7n^2$ pour tout $n \geq 1$.

Exemple 1.3.3. On veut utiliser l'induction pour démontrer que $8^n - 3^n$ est divisible par 5 pour tout entier $n \geq 1$. Pour ce faire, commençons par nous rappeller qu'un entier a est divisible par 5 si on peut l'écrire sous la forme $a = 5b$ où b est aussi un entier. Nous allons maintenant appliquer l'induction.

1. Comme première étape on doit démontrer que la propriété est vraie si $n = 1$. Dans ce cas, on a $8^1 - 3^1 = 5$, ce qui est évidement divisible par 5. Donc la propriété est satisfaite pour une première valeur.
2. Nous faisons maintenant l'hypothèse que la propriété est vraie pour $n = k$. C'est à dire, on suppose que $8^k - 3^k$ est divisible par 5.
3. On veut maintenant montrer que la propriété est aussi vrai pour $n = k+1$, on a donc :

$$\begin{aligned}8^{k+1} - 3^{k+1} &= 8\cdot 8^k - 3\cdot 8^k + 3\cdot 8^k - 3\cdot 3^k\\ &= 5\cdot 8^k - 3(8^k - 3^k)\end{aligned}$$

Comme $8^k - 3^k$ est divisible par 5 par l'hypothèse de la seconde étape, il existe donc un entier m tel que $8^k - 3^k = 5m$. On obtient donc :

$$\begin{aligned}8^{k+1} - 3^{k+1} &= 5\cdot 8^k - 3(8^k - 3^k)\\ &= 5\cdot 8^k - 3(5m)\\ &= 5\big(8^k - 3m\big)\end{aligned}$$

Et donc $8^{k+1} - 3^{k+1}$ est aussi divisible par 5

On peut donc conclure que $8^n - 3^n$ est divisible par 5 pour tout entier $n \geq 1$.

Dans certain cas, le principe d'induction, tel que nous l'avons énoncé, n'est pas suffisant pour démontrer un résultat. Lorsqu'on applique de manière stricte le principe d'induction, on utilise uniquement la valeur précédente pour démontrer qu'une propriété est vraie pour une certaine valeur. Nous allons maintenant énoncer une version généralisée du principe d'induction qui nous permettra d'utiliser plusieurs valeurs précédentes pour démontrer un énoncé.

Théorème 1.3.2. **(Principe d'induction généralisé)** Si P est une propriété satisfaisant les deux conditions suivantes :

1. La propriété est vraie pour tous les entiers entre a et b (avec $a \leq b$).
2. En faisant l'hypothèse que la propriété est vraie pour tous les entiers entre a et k (avec $k \geq b$), on peut démontrer qu'elle est aussi vraie pour l'entier $k+1$.

Alors on peut conclure que la propriété P est vraie pour tous les entiers plus grand ou égal à a.

Exemple 1.3.4. Considérons la suite de nombres naturels définie par la relation

$$x_n = 7x_{n-1} - 10x_{n-2} \text{ avec } x_0 = 1 \text{ et } x_1 = 2$$

Utilisez l'induction pour démontrer que $x_n = 2^n$ pour tout $n \geq 0$.

1. Pour $n = 0$ et $n = 1$, on a bien l'égalité. Remarquez que l'on doit vérifier les deux premières valeurs car nous utilisons les deux valeurs précédentes dans notre troisième étape.
2. Supposons que $x_n = 2^n$ pour tout $n \leq k$
3. On veut maintenant montrer que l'équation est vrai pour $n = k+1$:

$$\begin{aligned} x_{k+1} &= 7x_k - 10x_{k-1} \\ &= 7(2^k) - 10(2^{k-1}) \\ &= 2^{k-1}(7 \cdot 2 - 10) \\ &= 2^{k-1}(2^2) \\ &= 2^{k+1} \end{aligned}$$

Ce qui complète la démonstration.

1.4 Le théorème du binôme

Nous allons maintenant utiliser l'induction pour démontrer le théorème du binôme qui nous sera utile plus tard, rendu au chapitre 3, pour démontrer la formule d'inversion de Mobiüs. L'idée du théorème est essentiellement de nous permettre de développer rapidement des expressions de la forme $(a+b)^n$.

Definition 1.4.1. Si $n \in \mathbb{N}$, alors on définit la factorielle, dénoté $n!$, comme étant :

$$n! = \begin{cases} 1 & \text{si } n = 0 \\ 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n & \text{si } n > 0 \end{cases} \tag{1.1}$$

Definition 1.4.2. Si $n, i \in \mathbb{N}$ avec $i \leq n$, alors on définit $\binom{n}{i}$ comme étant :

$$\binom{n}{i} = \frac{n!}{i!(n-i)!}$$

Lemme 1.4.1. *Si $n, i \in \mathbb{N}$ tel que $i \leq n$, alors on a :*

$$\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$$

Démonstration.

$$\begin{aligned} \binom{n}{i-1} + \binom{n}{i} &= \frac{n!}{(i-1)!(n-i+1)!} + \frac{n!}{i!(n-i)!} = \frac{n!i!(n-i)! + n!(i-1)!(n-i+1)!}{i!(i-1)!(n-i+1)!(n-i)!} \\ &= \frac{n!i! + n!(i-1)!(n-i+1)}{i!(i-1)!(n-i+1)!} = \frac{n!i + n!(n-i+1)}{i!(n-i+1)!} \\ &= \frac{n!(n+1)}{i!(n-i+1)!} = \frac{(n+1)!}{i!(n-i+1)!} = \binom{n+1}{i} \end{aligned}$$

□

Théorème 1.4.1. **(Théorème du binôme)** Pour tout $n \in \mathbb{N}$, on a

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$$

Démonstration. On fait la preuve par induction

1. Si $n = 0$, on a l'égalité $1 = 1$ qui est évidement vraie.
2. Supposons que l'égalité est vraie pour n
3. On doit montré que c'est toujours vrai pour $n+1$:

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n = (a+b)\sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i} = \sum_{i=0}^{n}\binom{n}{i}a^{i+1}b^{n-i} + \sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i+1} \\
&= \sum_{i=1}^{n+1}\binom{n}{i-1}a^i b^{n-i+1} + \sum_{i=0}^{n}\binom{n}{i}a^i b^{n-i+1} = a^{n+1} + b^{n+1} + \sum_{i=1}^{n}\left[\binom{n}{i-1} + \binom{n}{i}\right]a^i b^{(n+1)-i} \\
&= a^{n+1} + b^{n+1} + \sum_{i=1}^{n}\binom{n+1}{i}a^i b^{(n+1)-i} = \sum_{i=0}^{n+1}\binom{n+1}{i}a^i b^{(n+1)-i}
\end{aligned}$$

Ce qui complète la preuve. □

Nous pouvons maintenant utiliser ce théorème pour calculer rapidement certains produits. Pour ce faire, nous allons regarder premièrement le triangle de Pascal :

Triangle de Pascal

$n = 0$:					1					
$n = 1$:				1		1				
$n = 2$:			1		2		1			
$n = 3$:		1		3		3		1		
$n = 4$:	1		4		6		4		1	
$n = 5$:	1	5		10		10		5		1

La triangle est obtenu en plaçant premièrement un 1 sur la première ligne, et toutes les autres lignes sont obtenues en commençant et terminant par un 1, et les autres valeurs sont la somme des deux valeurs qui se trouve immédiatement au dessus. Le triangle de Pascal n'est en fait qu'une manière visuelle de représenter le lemme et est utilisé pour calculer rapidement les coefficients de la forme $\binom{n}{i}$. Par exemple, si on souhaite trouver la valeur de $\binom{4}{2}$, on regardera dans la ligne identifié $n = 4$, puis on prendra le 3^e élément. Attention, il ne s'agit pas d'un typo. Le premier élément de chaque ligne est l'élément $i = 0$. On aura donc :

$$\binom{4}{2} = 6$$

Ce qui correspond à la valeur que vous auriez obtenu en calculant les factoriels (vous devriez le vérifier!!!).

Exemple 1.4.1. On veut utiliser le triangle de Pascal pour calculer le produit $(x+2)^5$. On a donc :

$$\begin{aligned}
(x+2)^5 &= x^5 + 5x^4(2)^1 + 10x^3(2)^2 + 10x^2(2)^3 + 5x(2)^4 + 2^5 \\
&= x^5 + 10x^4 + 40x^3 + 80x^2 + 80x + 32
\end{aligned}$$

Exemple 1.4.2. On veut utiliser le triangle de Pascal pour calculer le produit $(4x-1)^3$. On a donc :

$$\begin{aligned}
(4x-1)^3 &= 1(4x)^3 + 3(4x)^2(-1)^1 + 3(4x)^1(-1)^2 + 1(-1)^3 \\
&= 64x^3 - 48x^2 + 12x - 1
\end{aligned}$$

1.5 La divisibilité

Dans les nombres naturels ($\mathbb{N}$), ou même dans les nombres entiers ($\mathbb{Z}$), il n'est pas toujours possible de diviser deux nombres. Si a et b sont deux nombres naturels avec $b \neq 0$, alors nous dirons intuitivement que b est divisible par a si le résultat de la division $b \div a$ est un nombre entier. Nous avons cependant besoin d'une définition plus formelle, qui n'utilise pas une opération qui n'est pas toujours définie dans les nombres naturels ou entiers.

Definition 1.5.1. Si $a, b \in \mathbb{Z}$, alors a divise b s'il existe un nombre $k \in \mathbb{Z}$ tel que $ak = b$. Nous écrirons alors $a|b$ (i.e. a divise b). De la même façon, si b n'est pas divisible par a, nous écrirons $a \nmid b$ (i.e. a ne divise pas b).

Exemple 1.5.1. Voici quelques exemples pour illustrer la définition précédente :

1. On a que $3|27$, car $3 \times 9 = 27$
2. On a que $7|49$, car $7 \times 7 = 49$
3. On a que $18 \nmid 38$, car $18 \times 2 = 36 < 38$ et $18 \times 3 = 54 > 38$

Voici maintenant un théorème énonçant certaines propriétés élémentaires de la divisibilité. Notez qu'ici les résultats du théorème sont relativement simples, et même peuvent sembler évident. Ce qui nous intéresse est surtout leur démonstration.

Théorème 1.5.1. Voici quelques propriétés de la divisibilité :

1. Si $a, b, c \in \mathbb{Z}$ sont tels que $a|b$, alors $a|(bc)$.
2. Si $a, b, c \in \mathbb{Z}$ sont tels que $a|b$ et $b|c$, alors $a|c$.
3. Si $a, b, c, d, e \in \mathbb{Z}$ sont tels que $a|b$ et $a|c$, alors $a|(bd + ce)$.

Démonstration.

1. Comme $a|b$, alors il existe un entier k tel que $ak = b$. On a donc
$$bc = akc = a(kc)$$
Comme kc est un entier, alors $a|(bc)$.
2. Comme $a|b$ et $b|c$, alors il existe des entiers m, n tels que $am = b$ et $bn = c$. On obtient donc que :
$$c = bn = amn = a(mn)$$
Ce qui nous permet de conclure que $a|c$.
3. Comme $a|b$ et $a|c$, alors il existe des entiers m, n tels que $am = b$ et $an = c$. On obtient donc :
$$bd + ce = amd + and = a(md + nd)$$
ce qui nous donne $a|(bd + ce)$.

□

1.6 La division euclidienne

Nous allons maintenant introduire la division euclidienne. Il s'agit en quelque sorte d'effectuer la division avec reste que vous avez probablement déjà vu au primaire. Si a et b sont deux nombres naturels et $b \neq 0$, alors la division euclidienne de a par b est $a = br + q$ où r et q sont deux nombres naturels, et $0 \leq q < b$. On peut comprendre cette idée comme étant $a \div b = r$ reste q. N'oubliez pas que lorsque l'on parle d'entiers, il n'est pas question de travailler avec des fractions, celles ci n'existent pas en quelque sorte.

Théorème 1.6.1. **(Division euclidienne)** Si $a, b \in \mathbb{Z}$ avec $b > 0$, alors il existe des entiers q et r avec $0 \leq r < b$ tel que :

$$a = bq + r$$

Démonstration. Considérons l'ensemble

$$S = \{a - bq : q \in \mathbb{Z}, a - bq \geq 0\}$$

Comme $S \subseteq \mathbb{N}$ et $S \neq \emptyset$. Alors, il existe un plus petit élément $r_0 \in S$. Donc $r_0 = a - bq_0$, que l'on peut écrire sous la forme $a = bq_0 + r_0$. Il est clair que $r_0 \geq 0$, on doit donc montrer que $r_0 < b$. Supposons au contraire que $r_0 \geq b$. Alors

$$r_1 = a - b(q_0 + 1) = a - bq_0 - b = r_0 - b \geq 0$$

Donc $r_1 \in S$ et $r_1 < r_0$ ce qui est une contradiction. Donc $0 \leq r_0 < b$. □

Exemple 1.6.1. Effectuez la division euclidienne de 28 par 3. On doit donc trouver le plus grand entier r tel que $3r < 28$. Nous avons donc :

$$\begin{aligned}
3 \times 1 &= 3 \\
3 \times 2 &= 6 \\
3 \times 3 &= 9 \\
3 \times 4 &= 12 \\
3 \times 5 &= 15 \\
3 \times 6 &= 18 \\
3 \times 7 &= 21 \\
3 \times 8 &= 24 \\
3 \times 9 &= 27 \quad \longleftarrow \\
3 \times 10 &= 30 \\
3 \times 11 &= 33
\end{aligned}$$

On remarque donc que $r = 9$. On doit maintenant trouver le reste de la division. On a donc $28 - (3 \times 9) = 1$. On a donc que $q = 1$. Le résultat de la division euclidienne est donc $28 = 3(9) + 1$.

La division euclidienne est particulièrement utile pour démontrer des théorèmes en lien avec la divisibilité. Remarquer que si a est divisible par b, alors le reste de la division euclidienne doit obligatoirement être 0.

Exemple 1.6.2. On veut démontrer que le carré d'un nombre impair est toujours un nombre impair. Pour ce faire, remarquons que si n est un nombre impair, alors $n = 2k+1$ où k est un entier (Il s'agit de la définition d'un nombre impair). On obtient donc :

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

En posant $m = 2k^2 + 2k$, on remarque que m est un entier et $n^2 = 2m + 1$. On peut donc conclure que n^2 est aussi un nombre impair.

1.7 Le plus grand commun diviseur

Nous allons maintenant tourner notre attention sur le concept du plus grand commun diviseur, que l'on dénote habituellement par PGCD (ou GCD en anglais de greatest common divisor) ou tout simplement à l'aide de parenthèse.

Definition 1.7.1. Si a et b sont des nombres entiers non nuls, alors le PGCD de a et b, dénoté (a, b) ou $\text{PGCD}(a, b)$ est le plus grand nombre naturel qui divise à la fois a et b.

Exemple 1.7.1. On veut trouver le PGCD de 58 et 132. Nous allons donc commencer par énumérer tous les diviseurs de chacun de ces deux nombres. Les diviseurs de 58 sont :

$$\{1, 2, 29, 58\}$$

Et les diviseurs de 132 sont :

$$\{1, 2, 3, 4, 6, 11, 12, 22, 33, 44, 66, 132\}$$

On peut donc remarquer que le plus grand diviseur que les deux nombres ont en commun est 2.

Remarquez que bien que l'exemple précédent ne soit pas très difficile, énumérer tous les diviseurs peut prendre beaucoup de temps, en particulier si les nombres sont grands. Nous allons donc devoir d'ici la fin de cette section développer une méthode plus efficace pour calculer le PGCD.

Théorème 1.7.1. Si a et b sont deux entiers non nuls, alors il existe des entiers x, y tel que

$$ax + by = (a, b)$$

Démonstration. Considérons l'ensemble

$$S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$$

Par la propriété du bon ordre, il existe dans S un plus petit élément que nous appellerons s. Donc

$$s = ax_0 + by_0$$

On veut montrer que $s = (a, b)$. Supposons que s ne divise pas a. Alors par la division euclidienne on a $a = sq + r$ avec $0 < r < s$. Donc :

$$r = a - sq = a - (ax_0 + by_0)q = a - aqx_0 - bqy_0 = a(1 - qx_0) - b(qy_0)$$

Donc $r \in S$, et $r < s$ ce qui est une contradiction (s est le plus petit élément de S). Donc $s|a$. De la même manière, on montre que $s|b$. Donc s est bien un diviseur commun de a et b. On veut maintenant montrer qu'il s'agit du plus grand. Supposons que c est un diviseur quelconque de a et b, alors $c|(ax + by)$ pour tout $x, y \in \mathbb{Z}$, donc en particulier $c|s$, donc $c \leq s$. On peut donc conclure que $s = (a, b)$. □

Théorème 1.7.2. Si $a, b, k \in \mathbb{Z}$ et $d = (a, b)$ alors on a :

1. $\{ax + by : x, y \in \mathbb{Z}\}$ est l'ensemble des multiples de $d = (a, b)$
2. $(a, b + ka) = (a, b) = (a, -b)$
3. $(ka, kb) = |k|(a, b)$
4. $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

Démonstration.

1. Posons $d = (a, b)$ et
$$S = \{ax + by : x, y \in \mathbb{Z}\} \text{ et } T = \{kd : k \in \mathbb{Z}\}$$
Commençons par montrer que $S \subseteq T$. Pour ce faire, prenons $s \in S$, où $s = ax_1 + by_1$. Comme $d|a$ et $d|b$ par définition du PGCD, alors $d|(ax_1 + by_1)$ et donc $d|s$. On a donc $S \subseteq T$. Maintenant, pour l'autre

inclusion, prenons $t \in T$, donc $t = kd$. Comme d est le PGCD de a et b, alors il existe des entiers x_1, y_1 tels que $d = ax_1 + by_1$, ce qui nous donne :

$$t = kd = k(ax_1 + by_1) = a(kx_1) + b(ky_1) \in S$$

Donc $T \subseteq S$. On peut donc conclure que $S = T$, et donc l'ensemble S est bien l'ensemble des multiples de $d = (a, b)$.

2. Posons $d_1 = (a, b + ka)$. Par définition, on a donc que $d_1|a$ et $d_1|(b + ka)$. Il existe donc des entiers m, n tels que $d_1 m = a$ et $d_1 n = b + ka$ donc :

$$d_1 n = b + ka = b + k(d_1 m) = b + kd_1 m \Longrightarrow b = d_1 n - kd_1 m = d_1(n - km)$$

on a donc que $d_1|b$ et donc $d_1|(a, b)$. Maintenant, posons $d_2 = (a, b)$ donc par hypothèse, $d_2|a$ et $d_2|b$, ce qui nous donne que $d_2|b + ka$ et donc $d_2|(a + b + ka)$. Comme $d_1|d_2$, $d_2|d_1$ et que ces deux nombres sont positifs, alors $d_1 = d_2$, ce qui démontre la première égalité. La deuxième égalité est laissée en exercice.

3. Commençons par poser $d = (a, b)$ et supposons que $k \geq 0$. On a donc que $d|a$ et $d|b$ ce qui implique que $dk|ak$ et $dk|bk$. On a donc que $dk|(bk, ak)$. Il existe donc un entier s tel que $dks = (bk, ak)$, ce qui signifie que $dks|bk$ et $dks|ak$, et donc $ds|b$ et $ds|a$. Par définition du PGCD, on obtient donc que $s = 1$, ce qui signifie que

$$dk = (bk, ak)$$

La preuve lorsque $k < 0$ est semblable et est laissée en exercice.

4. En supposons que $d = (a, b)$ et $x = \left(\frac{a}{d}, \frac{b}{d}\right)$, on a donc :

$$dx = d\left(\frac{a}{d}, \frac{b}{d}\right) = |d|\left(\frac{a}{d}, \frac{b}{d}\right) = (a, b) = d$$

donc $dx = d$ ce qui implique que $x = 1$. On peut donc conclure que

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

□

L'algorithme d'Euclide est une méthode relativement simple pour calculer le PGCD de deux nombres. La méthode fait appel à la division euclidienne.

Théorème 1.7.3. (Algorithme d'Euclide) Si a et b sont des entiers non nuls tel que $a > b$. Posons $r_0 = b$ et $r_1 = a$, et on définie récursivement à l'aide de la division euclidienne :

$$r_{k-2} = q_k r_{k-1} + r_k, \quad \forall k \geq 2$$

Alors il existe un plus petit n tel que $r_n = 0$, et dans ce cas, $r_{n-1} = (a, b)$.

Démonstration. Par définition de la division euclidienne, chaque r_k doit être tel que $0 \leq r_k < r_{k-1}$. Il doit donc exister un plut petit n tel que $r_n = 0$. Maintenant, par le théorème précédant, nous avons aussi que :

$$(r_{k-1}, r_k) = (r_{k-1}, r_{k-2} - q_k r_{k-1}) = (r_{k-1}, r_{k-2}) = (r_{k-2}, r_{k-1})$$

Donc en particulier, nous avons que :

$$(a, b) = (r_{n-2}, r_{n-1}) = r_{n-1}$$

Car r_{n-2} est divisible par r_{n-1}. □

Nous allons illustrer la méthode à l'aide d'un exemple, il nous sera alors plus facile de l'expliquer.

Exemple 1.7.2. On veut à nouveau trouver le PGCD entre 58 et 132. On commence par trouver la division euclidienne entre ces deux nombres, ce qui nous donne :

$$132 = 2(58) + 16$$

On fait à nouveau la division euclidienne, mais cette fois ci en utilisant les nombres 58 et 16, ce qui nous donne :

$$58 = 3(16) + 10$$

Et on fait de même avec 16 et 10, ce qui nous donne :

$$16 = 1(10) + 6$$

Puis avec 10 et 6 :

$$10 = 1(6) + 4$$

Et avec 6 et 4 :

$$6 = 1(4) + 2$$

et finalement avec 4 et 2 :

$$4 = 2(2) + 0$$

La méthode se termine alors car nous avons obtenu un reste de 0. Le PGCD est alors le reste de la division qui précède la dernière. On remarque que la réponse est bien 2 comme nous avions déjà trouvé.

Bien que la méthode puisse sembler compliquée, elle est en fait beaucoup plus rapide (et facile) lorsque les nombres sont grands. Voici un autre exemple de calcul de PGCD :

Exemple 1.7.3. On veut trouver le PGCD de 1578 et 456. En appliquant l'algorithme d'Euclide on obtient :

$$\begin{aligned} 1578 &= 3(456) + 210 \\ 456 &= 2(210) + 36 \\ 210 &= 5(36) + 30 \\ 36 &= 1(30) + 6 \\ 30 &= 5(6) + 0 \end{aligned}$$

Le PGCD est donc le reste de l'avant dernière ligne. Le PGCD est donc 6. Vous pouvez vérifier en énumérant tous les diviseurs de chacun des deux nombres, mais vous verrez que ce sera beaucoup plus long.

Nous avons vu au début de cette section que si a et b sont des entiers non nuls et $d = (a, b)$, alors il existe des entiers x, y tels que

$$ax + by = d$$

Nous allons maintenant utiliser l'algorithme d'Euclide que nous venons de voir pour trouver une valeur de x et y qui satisfont cette équation. Il s'agit en fait de réécrire l'algorithme d'Euclide à l'envers comme l'illustre les deux exemples ci-dessous. Remarquez qu'il y a en général plus d'une solution possible pour x et y. Par contre, une seule solution nous sera suffisante pour le moment. Nous verrons plus tard comment faire pour trouver toutes les autres.

Exemple 1.7.4. On veut trouver des entiers m et n tels que $14m + 20n = (14, 20)$. L'algorithme d'Euclide nous donne :

$$\begin{aligned} 20 &= 1(14) + 6 \\ 14 &= 2(6) + 2 \\ 6 &= 3(2) + 0 \end{aligned}$$

Le PGCD est donc 2. En appliquant l'algorithme à l'envers, nous avons :

$$\begin{aligned} 2 &= 14 - 2(6) \\ &= 14 - 2(20 - 1(14)) \\ &= 14 - 2(20) + 2(14) \\ &= 3(14) - 2(20) \end{aligned}$$

Exemple 1.7.5. Trouvez des entiers m et n tels que $1144m+462n = (1144, 462)$. On commence par appliquer l'algorithme d'Euclide :

$$\begin{aligned} 1144 &= 2(462) + 220 \\ 462 &= 2(220) + 22 \\ 220 &= 10(22) + 0 \end{aligned}$$

Le PGCD est donc 22. Maintenant, pour trouver les valeurs de m et n, on a :

$$\begin{aligned} 22 &= 462 - 2(220) \\ &= 462 - 2(1144 - 2(462)) \\ &= 462 - 2(1144) + 4(462) \\ &= 5(462) - 2(1144) \end{aligned}$$

Ce qui nous donne : $m = -2$ et $n = 5$.

Théorème 1.7.4. (Lemme d'Euclide)

1. Si a, b sont des entiers non nuls pour lesquels il existe des entiers x, y tels que $ax + by = 1$, alors $(a, b) = 1$.
2. Si a, b, c sont des entiers tels que $a|bc$ et $(a, b) = 1$, alors $a|c$.

Démonstration.

1. Supposons que $ax + by = 1$ et posons $d = (a, b)$, alors $d|(ax + by)$, donc $d|1$. Maintenant, comme $d \geq 1$, alors on doit conclure que $d = 1$.
2. Comme $a|bc$, alors il existe un entier k tel que $ak = bc$. De plus, comme $(a, b) = 1$, alors il existe des entiers x, y tels que $ax + by = 1$, ce qui nous donne, en multipliant des deux côtés par c,

   $$acx + bcy = c$$

   On obtient donc finalement que :

   $$c = acx + bcy = acx + aky = a(cx + ky)$$

   on peut donc conclure que $a|c$.

□

Definition 1.7.2. Si a, b sont des entiers tel que $(a, b) = 1$, alors on dit que a et b sont des nombres copremiers.

Remarquez qu'il est aussi possible de parler du PGCD de plus que deux nombres. Par exemple, on définira le PGCD de a, b et c, dénoté (a, b, c) comme étant le plus grand entier d tel que $d|a, d|b$ et $d|c$. Les propriétés restent relativement semblables à celui du PGCD de deux nombres. Il vous est laissé en exercice de démontrer dans ce cas les différentes propriétés. Notez cependant une propriété importante qui peut être particulièrement utile. Si a, b et c sont des entiers, alors $(a, b, c) = ((a, b), c)$. Ceci jouera un rôle important dans l'étude des solutions entières de l'équation pythagoricienne $x^2 + y^2 = z^2$.

1.8 Le plus petit commun multiple

Une autre notion en lien avec le PGCD est celle du plus petit commun multiple, que l'on dénote habituellement par PPCM (en anglais on parlera de LCD pour least common multiple). Si n est un nombre entier, alors un multiple de n est un nombre de la forme kn où k est aussi un nombre entier.

Definition 1.8.1. Si a et b sont des entiers non nuls, alors on définit le plus petit commun multiple de a et b dénoté $PPCM(a,b)$ ou bien $[a,b]$ comme étant le plus petit entier positif (i.e. nombre naturel) qui est à la fois un multiple de a et de b.

Exemple 1.8.1. Les nombres suivants sont des multiples de 3 :

$$3, 6, 9, 12, 15, 18, 21, 24, ...$$

Si a et b sont deux entiers positifs non nuls, alors le plus petit commun multiple (PPCM) de a et b est le plus petit nombre qui est à la fois multiple de a et de b. Une première méthode pour trouver le PPCM est d'énumérer quelques multiples de chacun des nombres, et d'identifier le plus petit qui est commun. Ceci est illustré dans l'exemple suivant :

Exemple 1.8.2. On veut trouver le PPCM de 14 et 20. On va donc énumérer les premiers multiples de chacun de ces deux nombres. Pour 14 on a :

$$14, 28, 42, 56, 70, 84, 98, 112, 126, 140, 154, 168, 182, 196, 210, ...$$

et pour 20 nous avons :

$$20, 40, 60, 80, 100, 120, 140, 160, 180, 200, 220, 240, 260, 280, 300, ...$$

On remarque que le plus petit nombre que ces deux suites ont en commun est 140. Il s'agit donc du PPCM.

Remarquez que la méthode précédente n'est pas très efficace. Dans certain cas il peut être nécessaire d'énumérer une longue liste de multiples avant d'en trouver un en commun. Par contre, le théorème suivant nous aidera dans nos calculs

Théorème 1.8.1. Si a et b sont deux entiers positifs non nuls, alors :

1. Le PPCM de a et b est nécessairement plus petit ou égal au produit ab
2. Si k est un multiple commun de a et b, alors $[a,b]|k$
3. Si $k > 0$ alors $[ka, kb] = k[a,b]$
4. On a la relation suivante entre le PGCD et le PPCM de a et b :

$$[a,b] = \frac{|ab|}{(a,b)}$$

Démonstration.

1. Il s'agit de remarquer que $a|(ab)$ et $b|(ab)$. Le produit ab est donc un multiple commun à a et b. Le plus petit commun multiple doit donc être plus petit ou égal à ce dernier.
2. Supposons que m est le plus petit commun multiple de a et b, alors on peut calculer la division euclidienne de k par m, ce qui nous donne :

$$k = mq + r, \qquad 0 \leq r < m$$

ce qui peut être réécrit comme $r = k - mq$. Comme $a|k$ et $a|m$, alors $a|r$. De plus, comme $b|k$ et $b|m$, alors $b|r$. Donc r est un multiple commun de a et b qui est plus petit que le plus petit commun multiple m de a et b, ce qui est une contradiction si $r \neq 0$. Donc $k = mq$ pour un entier q, donc $m|k$.

3. Posons $m = [a, b]$ et $M = [ka, kb]$. Comme m est un multiple de a et b, alors km est un multiple de ka et kb, donc par la partie précédente $M|km$ et donc en particulier $M \leq km$. De plus, comme M est un multiple de ka et kb, alors $\frac{M}{k}$ est un multiple de a et b, donc $m\left|\frac{M}{k}\right.$, donc en particulier $m \leq \frac{M}{k}$, ou de façon équivalente : $mk \leq M$. On a donc :

$$M \leq km \text{ et } km \leq M$$

Ce qui implique que $M = km$.

4. Nous allons faire la démonstration seulement dans le cas où a et b sont positifs. Supposons premièrement que $(a, b) = 1$, et posons $[a, b] = m$. Donc m est un multiple de a, ce qui signifie qu'il existe un entier x tel que $m = ax$. De plus, m est aussi un multiple de b, donc $b|ax$. Comme par hypothèse $(a, b) = 1$, alors on a $b|x$, donc il existe un entier y tel que $by = x$ ce qui nous donne :

$$m = ax = aby$$

Maintenant par la première partie du théorème, on a que $m \leq ab$ et que $y \geq 1$, alors $y = 1$ ce qui nous donne $m = [a, b] = ab$. Ce qui démontre le théorème dans le cas ou a et b sont des entiers copremiers. Supposons maintenant que $(a, b) = d$. Dans ce cas, on a que $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, ce qui nous donne

$$[a, b] = d\left[\frac{a}{d}, \frac{b}{d}\right] = d\frac{ab}{d^2} = \frac{ab}{d} = \frac{ab}{(a, b)}$$

ce qui complète la démonstration si a et b sont positifs.

□

Exemple 1.8.3. Le PPCM de 14 et 20 est nécessairement plus petit (par le théorème précédent) que $14 \times 20 = 280$. Lorsque nous avons calculé la valeur exacte du PPCM, nous avons obtenu 140, ce qui est effectivement plus petit ou égal à 280.

Nous pouvons donc utiliser l'algorithme d'Euclide pour calculer le PPCM. Nous allons donc refaire l'exemple précédent, mais cette fois-ci en utilisant l'algorithme.

Exemple 1.8.4. On veut trouver le PPCM de 14 et 20. Pour ce faire, nous allons commencer par trouver le PGCD de ces deux nombres en utilisant l'algorithme d'Euclide :

$$\begin{aligned} 20 &= 1(14) + 6 \\ 14 &= 2(6) + 2 \\ 6 &= 3(2) + 0 \end{aligned}$$

Le PGCD est donc 2. En applicant la formule du théorème, on peut maintenant calculer le PPCM :

$$\begin{aligned} \text{PPCM}(14, 20) &= \frac{14 \times 20}{\text{PGCD}(14, 20)} \\ &= \frac{280}{2} \\ &= 140 \end{aligned}$$

Nous obtenons donc la même réponse.

Exemple 1.8.5. On veut trouver le PPCM de 786 et 524. En appliquant l'algorithme d'Euclide, on obtient :

$$\begin{aligned} 786 &= 1(524) + 262 \\ 524 &= 2(262) + 0 \end{aligned}$$

Le PGCD est donc 262. En appliquant la formule, on obtient maintenant :

$$\text{PPCM}(786, 524) = \frac{786 \times 524}{262} = 1572$$

Exemple 1.8.6. Supposez que a est un entier positif non nul. Si $\text{PGCD}(a, 598) = 23$ et $\text{PPCM}(a, 598) = 20930$, quelle est la valeur de a ? Pour ce faire, nous avons tout simplement à appliquer le théorème 1.8, ce qui nous donne :

$$\begin{aligned} \text{PPCM}(a, 598) &= \frac{598a}{\text{PGCD}(a, 598)} \\ 20930 &= \frac{598a}{23} \\ 20930 &= 26a \end{aligned}$$

Ce qui nous donne $a = 805$.

Finalement, remarquez que comme dans le cas du PGCD, il est aussi possible de définir le PPCM de plus que deux nombres. Par exemple, si a, b et c sont des entiers, alors on définit le PPCM de ces trois nombres, dénoté $[a, b, c]$ comme étant le plus petit nombre entier m tel que $a|m$, $b|m$ et $c|m$. Comme exercice, vous pouvez essayer de relier le PPCM de trois nombres avec le PGCD de ces mêmes trois nombres.

1.9 Les nombres premiers

Nous allons maintenant aborder le concept des nombres premiers. Ces derniers servent à construire n'importe quel nombre naturel plus grand ou égal à deux. Un nombre naturel a plus grand ou égal à deux est appelé un **nombre premier** si les seuls diviseurs de a sont 1 et a. Autrement dit un nombre est premier s'il a exactement deux diviseurs (les deux diviseurs doivent être différent). Un nombre naturel est dit composé, s'il a plus que deux diviseurs, autrement dit, un nombre naturel plus grand ou égal à deux est composé s'il n'est pas premier. Faites attention, les nombres naturels 0 et 1 sont différents. Ils ne sont ni composé, ni premier. Ils forment une classe à part dans l'ensemble des nombres naturels.

Nous allons commencer par réécrire le lemme d'Euclide (i.e. théorème 1.7) pour le cas des nombres premiers :

Théorème 1.9.1. Supposons que p est un nombre premier, et a, b sont des entiers non nul. Si $p|(ab)$ alors $p|a$ ou $p|b$.

Démonstration. Si $p|a$, alors le théorème est automatiquement vrai (il s'agit de l'une des conclusions du théorème), alors on va supposer que p ne divise pas a. Comme les seuls diviseurs de p sont 1 et p, alors le $\text{PGCD}(p, a) = 1$. Ceci est vrai car le PGCD doit obligatoirement par définition être un diviseur des deux nombres, et p n'est pas un diviseur de a par hypothèse. On a donc que $p|(ab)$ et $\text{PGCD}(a, p) = 1$. On peut donc appliquer le lemme d'Euclide ce qui nous donne que $p|b$. Le théorème est donc vrai. □

Remarquez que l'hypothèse que p est un nombre premier est très importante dans le théorème précédent. Si p n'est pas premier, le théorème ne fonctionne pas toujours. Par exemple, nous avons que 4 divise le produit 14×18, mais 4 ne divise pas 14 ni 18. Nous allons maintenant énoncer (et démontrer) l'un des résultats les plus importants de l'antiquité.

Théorème 1.9.2. **(Théorème fondamental de l'arithmétique)** Tout nombre naturel n plus grand ou égal à 2 peut s'écrire comme un produit de nombres premiers. De plus ce produit est unique si on ordonne les membres du produit en ordre croissant.

Démonstration. Nous voulons premièrement montrer que si n est un nombre naturel non nul, alors n peut s'écrire comme produit de nombre premier. Si n est déjà un nombre premier, alors nous avons terminé. Sinon, par définition d'un nombre composé, on peut écrire n sous la forme d'un produit $a_1 a_2$. Avec a_1, a_2 tous deux plus grand que 1, mais plus petit que n. Ensuite nous répétons la même étape avec les nombres a_1 et a_2.

S'ils sont tous deux premiers, alors nous avons terminé. Sinon, nous pouvons les écrire à nouveau comme un produit. En continuant de la même façon, nous obtiendrons éventuellement un produit de nombres premiers.

Maintenant, pour montrer que le produit est unique, nous allons supposer le contraire (preuve par contradiction). Supposons que le nombre n peut s'écrire des deux façons suivantes comme produit de nombres premiers :

$$n = p_1p_2p_3...p_r = q_1q_2q_3...q_s$$

Nous avons donc que p_1 doit diviser le produit $q_1q_2q_3...q_s$, et comme p_1 est un nombre premier, alors il doit diviser l'un des q_i. Par contre, comme ce q_i est aussi premier, nous n'avons pas le choix $p_1 = q_i$. En refaisant la même étape pour tous les p_j, nous obtenons alors que tous les membres du produit doivent être identiques, sauf peut être pour l'ordre dans lequel ils sont écrits. Si on les placent en ordre croissant, les deux produits seront alors identiques. □

La question qui se pose maintenant, est comment faire pour écrire un nombre donné sous forme d'un produit de nombres premiers. L'idée se trouve en fait dans le théorème précédent. Nous allons illustrer le processus par un exemple :

Exemple 1.9.1. On veut factoriser le nombre 1176 sous forme d'un produit de nombres premiers. Premièrement remarquons que 1176 peut être divisé par 4, on peut donc écrire

$$1176 = 4 \times 294$$

Maintenant, nous savons que $4 = 2 \times 2$ et on remarque que 294 peut être divisé par 3, nous avons donc :

$$1176 = (2 \times 2) \times (3 \times 98)$$

On remarque alors que 98 est encore une fois divisible par deux, ce qui nous donne :

$$1176 = 2 \times 2 \times 3 \times (2 \times 49)$$

En continuant de la même manière, on remarque que $49 = 7 \times 7$, ce qui nous donne finalement :

$$1176 = 2 \times 2 \times 3 \times 2 \times (7 \times 7)$$

Pour compléter, nous allons tout simplement ordonner les membres du produit en ordre croissant de sorte que la factorisation soit unique. Notre réponse finale est donc :

$$1176 = 2 \times 2 \times 2 \times 3 \times 7 \times 7$$

Dans le chapitre suivant, nous allons voir quelques critères pour tester la divisibilité, ce qui va nous aider à trouver la factorisation d'un nombre sous forme d'un produit de nombres premiers. Maintenant que nous avons vu que tout nombre naturel plus grand ou égal à 2 peut s'écrire comme un produit de nombres premiers, la question suivante qui se pose est combien y a-t-il de nombres premiers ? Encore une fois, la réponse a été fournie par Euclide et son école durant l'Antiquité.

Théorème 1.9.3. **(Euclide)** Il existe un infinité de nombre premier

Démonstration. Nous allons supposer le contraire. Supposons qu'il existe seulement un nombre fini de nombres premiers, c'est à dire que $p_1, p_2, p_3, ..., p_k$ sont les seuls nombres premiers existants. Considérons maintenant le nombre

$$N = p_1p_2...p_k + 1$$

Ce nombre est clairement plus grand que chacun des nombres $p_1, ..., p_k$. Si les p_i sont les seuls nombres premiers existants, alors N doit obligatoirement être divisible par certain d'entres eux, sinon il serait un

nombre premier. Pourtant nous allons montrer qu'aucun des p_i ne divise N. Supposons que p_i divise N, alors on peut trouver un entier m tel que $mp_i = N$, c'est à dire que nous avons :

$$mp_i = p_1p_2...p_k + 1$$

En déplaçant les termes, nous obtenons donc que

$$mp_i - p_1p_2...p_k = 1$$

puis en factorisant p_i à gauche, nous pouvons donc conclure que p_i doit diviser 1. Ce qui est bien entendu une contradiction. Donc aucun des p_i ne divise N. Il doit donc exister au moins un autre nombre premier. □

Remarquez que dans le théorème précédant, rien ne nous garanti que N est un nombre premier. Tout ce que nous avons montrer c'est qu'il doit exister un autre nombre premier que les $p_1, p_2, ..., p_k$. On appelle nombre premier d'Euclide un nombre premier de la forme

$$n = p_1p_2p_3...p_k + 1$$

Les premiers nombres premiers d'Euclide sont

$$3, 7, 31, 211, 2311, 30031, 510511, ...$$

On ne sait toujours pas à l'heure actuelle s'il existe une infinité de nombres premiers d'Euclide.

1.10 La crible d'Ératosthène

On est maintenant intéressé à savoir comment trouver une liste de nombres premiers, ou bien comment vérifier si un nombre est premier ou non. Le théorème suivant va nous aider dans cette direction.

Théorème 1.10.1. Si n est un entier plus grand ou égal à 2, et n n'est pas divisible par aucun nombre premier entre 2 et $\sqrt{n}$, alors n doit être premier.

Démonstration. Supposons que n n'est pas un nombre premier, alors il existe des entiers $a, b > 1$ tel que $n = ab$. Supposons que a, b sont tous deux plus grands que $\sqrt{n}$, alors on a :

$$n = ab > \sqrt{n}\sqrt{n} = n$$

ce qui est évidement une contradiction. Donc a ou b est plus petit ou égal à $\sqrt{n}$. □

Exemple 1.10.1. Nous allons maintenant utiliser cette méthode pour trouver tous les nombres premiers entre 2 et 25. Remarquez que $\sqrt{25} = 5$, donc un nombre entre 2 et 25 est premier s'il n'est pas divisible par un nombre premier entre 2 et 5. Il est facile de voir que les nombres premiers entre 2 et 5 sont $\{2, 3, 5\}$. Donc un nombre entre 2 et 25 est premier s'il n'est pas divisible par $2, 3$ ni 5. En éliminant tous les multiples de 2, 3 et 5, nous obtenons donc la liste suivante :

$$\{2, 3, 5, 7, 11, 13, 17, 19, 23\}$$

Exemple 1.10.2. Est ce que le nombre 223 est premier ? Pour ce faire, nous devons vérifier que 223 n'est pas divible par un nombre premier entre 2 et $\sqrt{223}$. Comme $\sqrt{223}$ est légèrement plus petit que 15, il nous suffit de vérifier que 223 n'est pas divisible par $2, 3, 5, 7, 11, 13$. Donc nous n'avons que 6 divisions à tester. Comme aucune de ces divisions nous donne un entier, on peut donc conclure que 223 est un nombre premier.

1.11 Exercices

Exercice 1.11.1. Utiliser l'induction pour démontrer chacune des égalités ci-dessous :

1. $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$
2. $\sum_{i=1}^{n} i^3 = \left[\sum_{i=1}^{n} i\right]^2$
3. $\sum_{i=1}^{n} i(i!) = (n+1)! - 1$
4. $\sum_{i=0}^{n} \binom{n}{i} = 2^n$

Exercice 1.11.2. Utiliser le théorème du binôme pour trouver le coefficient de x^3y^7 dans le développement de

$$(x+y)^{10}.$$

Exercice 1.11.3. Démontrer que le carré d'un nombre impair est toujours de la forme $4k+1$ où k est un entier.

Exercice 1.11.4. Démontrer que le carré d'un nombre impair est toujours de la forme $8k+1$ où k est un entier.

Exercice 1.11.5. Calculer la division euclidienne de :

1. 27 par 4
2. 279 par 7
3. 3054 par 18
4. 578 par 12

Exercice 1.11.6. Le théorème sur l'existence de la division Euclidienne nous garantit que tout entier peut s'écrire sous l'une des trois formes suivantes : $3k$, $3k+1$ ou $3k+2$. De plus, nous savons que k doit être pair ou impair. Utiliser ces résultats pour démontrer que le produit de 3 nombres consécutifs est toujours divisible par 6.

Exercice 1.11.7. Modifier votre démonstration de l'exercice précédent pour démontrer que le produit de 4 nombres consécutifs est toujours divisible par 24.

Exercice 1.11.8. Trouver le PGCD et le PPCM des nombres suivants :

1. 78 et 18
2. 198 et 52
3. 5946 et 93
4. 12854 et 8943

Exercice 1.11.9. Supposer que $a \in \mathbb{N}$ et $a \neq 0$. Si $(a, 70) = 14$ et $[a, 70] = 420$, trouver la valeur de a.

Exercice 1.11.10. Trouver tous les nombres naturels a, b non nul tel que $(a, b) = 7$ et $[a, b] = 42$.

Exercice 1.11.11. Écrire le nombre 484 comme produit de nombres premiers.

Exercice 1.11.12. Supposons que a et b sont des entiers non nuls tels que $a|b$ et $b|a$. Démontrez que $|a| = |b|$.

Exercice 1.11.13. On dit qu'une fraction $\frac{a}{b}$ est une fraction réduite si $(a, b) = 1$. Démontrer que si $\frac{a}{b}$ et $\frac{c}{d}$ sont des fractions réduites telles que

$$\frac{a}{b} + \frac{c}{d} = n$$

où n est un entier, alors $|b| = |d|$. Indice : Utiliser l'exercice précédent.

Exercice 1.11.14. Démontrer que si n est un entier tel que $2|n$ et $3|n$, alors $6|n$.

Exercice 1.11.15. Démontrer que si n est un entier positif, alors $6|(n^3 - n)$. Indice : factoriser le polynôme $n^3 - n$.

Exercice 1.11.16. Trouver la liste de tous les nombres premiers entre 2 et 100.

Exercice 1.11.17. Démontrer que le cube d'un entier positif peut toujours s'écrire comme la différence de deux carrés. C'est à dire que si n est un entier positif, alors il existe des entiers k et m tels que :

$$n^3 = m^2 - k^2$$

Indice : Commencer par écrire 1^3, 2^3, 3^3, 4^3 et 5^3 comme différence de deux carrés. formuler ensuite une hypothèse sur comment trouver m et k pour un entier positif n quelconque.

Exercice 1.11.18. Trouver des entiers m et n tel que

1. $910x + 1617y = (910, 1617)$
2. $52920x + 2275y = (52920, 2275)$

Exercice 1.11.19. Est-ce que les nombres ci dessous sont premiers ?

1. 281
2. 433
3. 323
4. 937

Exercice 1.11.20. Décomposer les nombres suivants comme un produit de nombre premier.

1. 484
2. 1755
3. 6480
4. 91

Exercice 1.11.21. Le but de cette question est d'étudier quelques propriétés du PGCD et PPCM de plus que deux nombres. Si a, b et c sont des entiers, alors on définit le PGCD de a, b et c, dénoté (a, b, c), comme étant le plus grand entier d tel que $d|a$, $d|b$ et $d|c$. De manière semblable, si a, b et c sont des entiers, alors on définit le PPCM de a, b et c, dénoté $[a, b, c]$, comme étant le plus petit entier positif m tel que $a|m$, $b|m$ et $c|m$.

1. Démontrez que pour tout $a, b, c \in \mathbb{Z}$, alors il existe $x, y, z \in \mathbb{Z}$ tel que
$$ax + by + cz = (a, b, c)$$
2. Si $a, b, c \in \mathbb{Z}$, démontrez que l'ensemble S ci-dessous est l'ensemble des multiples de $d = (a, b, c)$
$$S = \{ax + by + cz : x, y, z \in \mathbb{Z}\}$$
3. Démontrer que si a, b, c, d sont des entiers tel que $d|a, d|b$ et $d|c$, alors $d|(a, b, c)$
4. Démontrez que si $a, b, c \in \mathbb{Z}$, et $d = (a, b, c)$, alors
$$\left(\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right) = 1$$
5. Démontrer que dans ce cas nous avons :
$$(a, b, c) = (a, (b, c))$$
6. Démontrer que si a, b, c, m sont des entiers tel que $a|m, b|m$ et $c|m$, alors $[a, b, c]|m$
7. Démontrer que dans ce cas nous avons :
$$[a, b, c] = [a, [b, c]]$$
8. Utiliser les propriétés que vous venez de démontrer pour calculer $(360, 756, 2450)$
9. Utiliser les propriétés que vous venez de démontrer pour calculer $[360, 756, 2450]$

Chapitre 2

Les modulos

2.1 Les nombres modulos

Dans le chapitre précédent, nous avons mis beaucoup d'efforts à étudier le concept de la divisibilité. Ceci nous a amené à étudier des concepts tels que les nombres premiers et le plus grand commun diviseur pour n'en nommer que deux. Ce qui est important est que l'outil de base dans l'étude de la divisibilité a été la division euclidienne. Ce qui est encore plus important de remarquer est qu'en fait, même si la division euclidienne a été l'outil clé, c'est en fait le reste de la division qui était, en fait, le point clé. Il aurait donc été possible de démontrer plusieurs théorèmes du chapitre précédent en utilisant seulement des informations concernant le reste de la division. C'est la théorie des nombres modulos qui va nous permettre de mettre cette idée de manière un peu plus formelle.

Definition 2.1.1. Si a, b sont deux entiers, et n est un entier plus grand ou égal à 2, alors on écrit

$$a \equiv b \text{ (mod n) si et seulement si } n|(a-b)$$

De plus, lorsqu'il n'y a pas de danger de confusion, on remplace le symbol $\equiv$ par une simple égalité $=$.

Exemple 2.1.1. On a que $25 \equiv 19 \pmod 3$, car $25 - 19 = 6$ et $3|6$.

De manière générale, si $a \in \mathbb{Z}$, et n est un entier plus grand ou égal à 2, ce que nous souhaitons est de trouver le plus petit entier positif b tel que $a \equiv b$ (mod n). C'est ce que nous appelons le **résidu modulo**. Le résidu modulo n d'un nombre a n'est en fait rien d'autre que le reste de la division de a par n. Par abus de language, lorsque nous demanderons qu'elle est la valeur de $a \pmod n$, nous voudrons dire quel est le résidu modulo n de l'entier a. Le résidu modulo n d'un entier a n'est en fait rien d'autre que l'entier le plus simple qui est congru à l'entier a. Vous pouvez imaginer les nombres modulos un peu comme un horloge. Sur un horloge après 12, nous revenons à 1. Lorsqu'il est 11h sur un horloge, alors 2h plus tard il sera 1h.

Exemple 2.1.2. Trouver la valeur de 25 modulo 3, ou si vous préférez de manière plus correcte, quel est le résidu modulo 3 du nombre 25 ? Comme nous avons $25 = 8(3) + 1$, alors 25 modulo 3 est 1.

Les nombres modulos nous permettent de diviser les entiers en classes d'équivalence. Si nous travaillons avec les nombres modulos n, où n est un nombre naturel non nul, alors nous aurons n classes d'équivalence. Nous dirons par exemple que des entiers a et b sont dans la même classe modulo n si a (mod n) = b (mod n). Nous utiliserons la notation $\mathbb{Z}_n$ pour dénoter les nombres modulos n, et nous utiliserons la notation $\overline{a}$ pour dénoter l'ensemble des entiers b pour lesquels b (mod n) = a (mod n).

Par exemple, dans $\mathbb{Z}_3$ nous avons 3 classes d'équivalences, c'est à dire $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Ce qui nous donne :

$$\begin{aligned}
\overline{0} &= \{..., -6, -3, 0, 3, 6, 9, ...\} \\
\overline{1} &= \{..., , -5, -2, 1, 4, 7, 10, ...\} \\
\overline{2} &= \{..., -4, -1, 2, 5, 8, 11, ...\}
\end{aligned}$$

Théorème 2.1.1. Si a, b, c et d sont des entiers et n est un nombre naturel non nul. Alors on a les propriétés suivantes :

1. $a = a \pmod{n}$
2. $a = b \pmod{n} \iff b = a \pmod{n}$
3. $a = b \pmod{n}$ et $c = d \pmod{n} \Rightarrow a + c = b + d \pmod{n}$
4. $a = b \pmod{n}$ et $c = d \pmod{n} \Rightarrow ac = bd \pmod{n}$
5. $ab = ac \pmod{n} \iff b = c \left(\mod \frac{n}{(a,n)}\right)$

Démonstration.

1. Il s'agit de vérifier que $n|(a-a)$ ce qui est vrai car $n|0$.
2. Si $a = b \pmod{n}$, alors cela signifie que $n|(a-b)$, il existe donc un entier k tel que $nk = a - b$, et donc $n(-k) = b - a$ ce qui implique que $n|(b-a)$ et donc $b = a \pmod{n}$.
3. Comme $a = b \pmod{\text{n}}$ et $c = d \pmod{\text{n}}$, alors $n|(a-b)$ et $n|(c-d)$, il existe donc des entiers k, m tels que $nk = (a-b)$ et $nm = (c-d)$, ce qui nous donne
$$(a+c) - (b+d) = (a-b) + (c-d) = nk + nm = n(k+m)$$
ce qui signifie que $n|[(a+c) - (b+d)]$ et donc $a + c = b + d \pmod{\text{n}}$.
4. Comme $a = b \pmod{\text{n}}$ et $c = d \pmod{\text{n}}$, alors $n|(a-b)$ et $n|(c-d)$ et donc il existe des entiers k, m tels que $nk = a - b$ et $nm = c - d$ ce qui nous donne :
$$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b) = anm + dnk = n(am + dk)$$
et donc $n|(ac - bd)$ ce qui nous donne $ac = bd \pmod{\text{n}}$.
5. Commençons par démontrer ($\Rightarrow$). Par hypothèse, on a que
$$ab = ac \pmod{\text{n}} \text{ donc } n|a(b-c)$$
Supposons que $(a, n) = d$, il existe donc des entiers x, y tels que $xd = a$ et $yd = n$ avec $(x, y) = 1$, ce qui nous donne :
$$yd|xd(b-c) \Longrightarrow y|x(b-c)$$
Comme $(x, y) = 1$, on obtient donc :
$$y|(b-c)$$
Comme $y = \dfrac{n}{(a,n)}$, on peut donc conclure que
$$b = c \left(\mod \frac{n}{(a,n)}\right)$$
Maintenant pour l'autre direction ($\Leftarrow$). Par définition, on a que
$$\frac{n}{(a,n)} \Big| b - c$$
il existe donc un entier x tel que :
$$\frac{n}{(a,n)} x = b - c$$
En multipliant des deux côtés par a, on obtient donc :
$$\frac{n}{(a,n)} ax = a(b-c) \Longrightarrow n\left(\frac{a}{(a,n)}\right) x = a(b-c)$$
Comme $(a, n)|a$, on obtient donc
$$n|a(b-c) \Longrightarrow ab = ac \pmod{n}$$

□

Exemple 2.1.3. On veut trouver la valeur de 34×55 modulo 3. Nous pourrions, bien entendu, calculer le produit 34×55 et ensuite calculer la valeur du modulo. Par contre il est plus simple de calculer les modulos en premier. Nous savons que $34 = 11(3) + 1$ et $55 = 18(3) + 1$ ce qui nous donne que $34 \equiv 1 \pmod 3$ et $55 \equiv 1 \pmod 3$. Et donc :

$$34 \times 55 \equiv 1 \times 1 \pmod 3 \equiv 1 \pmod 3$$

De la même façon, nous avons que :

$$34 + 55 \equiv 1 + 1 \pmod 3 \equiv 2 \pmod 3$$

Exemple 2.1.4. On veut trouver le dernier chiffre du produit 876×254. On remarque que le dernier chiffre du produit, n'est en fait rien d'autre que la valeur de $876 \times 254 \pmod{10}$, ce qui nous donne :

$$876 \times 254 \pmod{10} \equiv 6 \times 4 \pmod{10} \equiv 24 \pmod{10} \equiv 4 \pmod{10}$$

Le dernier chiffre est donc 4.

Supposons maintenant que n est un entier positif non nul et que a, b, c, d sont des entiers tels que $a \equiv b \pmod{\text{n}}$ et $c \equiv d \pmod{\text{n}}$. Alors nous avons déjà vu que

$$a^c \equiv b^c \pmod{\text{n}}$$

par contre, en général il est **faux** de dire que a^c est égal à $a^d \pmod{\text{n}}$.

Exemple 2.1.5. Trouver le dernier chiffre de l'expression 342^{18}. Pour ce faire, remarquons premièrement que $342 = 2 \pmod{10}$, et donc :

$$342^{18} \pmod{10} \equiv 2^{18} \pmod{10}$$

Maintenant, pour calculer 2^{18} nous allons utiliser une petite astuce. Nous avons :

$$\begin{aligned}
2^1 &\equiv 2 \pmod{10} \\
2^2 &\equiv 2 \times 2 \pmod{10} \equiv 4 \pmod{10} \\
2^4 &\equiv 2^2 \times 2^2 \pmod{10} \equiv 16 \pmod{10} \equiv 6 \pmod{10} \\
2^8 &\equiv 2^4 \times 2^4 \pmod{10} \equiv 36 \pmod{10} \equiv 6 \pmod{10} \\
2^{16} &\equiv 2^8 \times 2^8 \pmod{10} \equiv 36 \pmod{10} \equiv 6 \pmod{10}
\end{aligned}$$

Finalement, on remarque que $18 = 16 + 2$, et donc $2^{18} = 2^{16} \times 2^2$, ce qui nous donne finalement :

$$\begin{aligned}
342^{18} \pmod{10} &\equiv 2^{18} \pmod{10} \equiv 2^{16} \times 2^2 \pmod{10} \equiv 6 \times 4 \pmod{10} \\
&\equiv 24 \pmod{10} \equiv 4 \pmod{10}
\end{aligned}$$

Nous pouvons donc affirmer que le dernier chiffre est 4.

Dans l'exemple précédant, nous aurions pu calculer directement la valeur de 342^{18}, ce qui nous aurais donné

$$342^{18} = 4097037216620966201473718623746777319410499584$$

Par contre, il est plutôt difficile de trouver ce dernier à la main, et même la plupart des calculatrices ne vous donneront pas cette valeur.

Exemple 2.1.6. Trouvez le dernier chiffre de 4583^{934}. Premièrement, on a que

$$4583^{934} \equiv 3^{934} \pmod{10}$$

Ensuite, pour calculer $3^{934} \pmod{10}$, on utilise la même astuce que précédemment :

$$\begin{aligned}
3^1 &\equiv 3 \pmod{10} \\
3^2 &\equiv 9 \pmod{10} \\
3^4 &\equiv 3^2 \times 3^2 \equiv 9 \times 9 \equiv 81 \equiv 1 \pmod{10} \\
3^8 &\equiv 3^4 \times 3^4 \equiv 1 \times 1 \equiv 1 \pmod{10} \\
3^{16} &\equiv 3^8 \times 3^8 \equiv 1 \times 1 \equiv 1 \pmod{10} \\
3^{32} &\equiv 1 \pmod{10} \\
3^{64} &\equiv 1 \pmod{10} \\
3^{128} &\equiv 1 \pmod{10} \\
3^{256} &\equiv 1 \pmod{10} \\
3^{512} &\equiv 1 \pmod{10} \\
3^{1024} &\equiv 1 \pmod{10}
\end{aligned}$$

Ensuite, on remarque que $934 = 512 + 256 + 128 + 32 + 4 + 2$, ce qui nous donne :

$$\begin{aligned}
3^{934} &= 3^{512} \times 3^{256} \times 3^{128} \times 3^{32} \times 3^4 \times 3^2 \\
&\equiv 1 \times 1 \times 1 \times 1 \times 1 \times 9 \pmod{10} \\
&\equiv 9 \pmod{10}
\end{aligned}$$

Et donc le dernier chiffre est un 9.

Exemple 2.1.7. On veut trouver les deux derniers chiffres de 99^{2453}. Pour ce faire, nous allons devoir travailler modulo 100. Si nous utilisons exactement la même astuce que précédemment, on peut facilement remarquer que le calcul sera long. En effet, nous devons calculer :

$$\begin{aligned}
99^1 &\equiv 99 \pmod{100} \\
99^2 &\equiv ??? \pmod{100} \\
99^4 &\equiv ??? \pmod{100} \\
99^8 &\equiv ??? \pmod{100} \\
99^{16} &\equiv ??? \pmod{100} \\
99^{32} &\equiv ??? \pmod{100} \\
99^{64} &\equiv ??? \pmod{100} \\
99^{128} &\equiv ??? \pmod{100} \\
99^{256} &\equiv ??? \pmod{100} \\
... &\equiv .....
\end{aligned}$$

Bien entendu, aucun de ces calculs n'est particulièrement difficile, par contre c'est effectivement long à calculer. Pour simplifier les choses, remarquons que $99 \equiv -1 \pmod{100}$. Et donc trouver les deux derniers chiffres de 99^{2453} revient à trouver les deux derniers chiffres de $(-1)^{2452}$. Nous savons que $(-1)^a = 1$ si a est pair, et $(-1)^a = -1$ si a est impair. Comme dans notre exemple, l'exposant est impair, nous avons donc :

$$99^{2453} \pmod{100} \equiv (-1)^{2453} \pmod{100} \equiv -1 \pmod{100} \equiv 99 \pmod{100}$$

Remarquez que la dernière étape ci-dessus est nécessaire car la réponse finale doit obligatoirement être entre 0 et 99. Les deux derniers chiffres sont donc 99.

Nous allons maintenant compléter cette section en regardant quelques tests permettant de vérifier rapidement si un nombre est divisible par un autre.

Théorème 2.1.2. **(Critères de divisibilités)** Si n est un entier non nul, alors :

1. n est divisible par 2 si le dernier chiffre de n est divisible par 2
2. n est divisible par 3 si la somme des chiffres qui le composent est divisible par 3
3. n est divisible par 4 si le nombre formé des deux derniers chiffres de n est divisible par 4
4. n est divisible par 5 si le dernier chiffre de n est divisible par 5
5. n est divisible par 6 s'il est divisible par 2 et par 3
6. n est divisible par 9 si la somme des chiffres qui le composent est divisible par 9
7. n est divisible par 10 si son dernier chiffre est un 0.

Démonstration.

1. On peut écrire n sous la forme :

$$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$$

avec $0 \leq a_i \leq 9$. En calculant le tout modulo 2, on obtient donc :

$$n = 0^n a_n + 0^{n-1} a_{n-1} + ... + 0^2 a_2 + 0^1 a_1 + a_0 = a_0 \pmod 2$$

Comme n est divisible par 2 si et seulement si $n = 0 \pmod 2$, on a donc que n est divisible par 2 si et seulement si $a_0 = 0 \pmod 2$, c'est à dire si et seulement si a_0 est divisible par 2.

2. On utilise la même idée que précédemment. On peut écrire n sous la forme :

$$n = 10^n a_n + 10^{n-1} a_{n-1} + ... + 10^2 a_2 + 10 a_1 + a_0$$

avec $0 \leq a_i \leq 9$. En calculant le tout modulo 3, on obtient donc :

$$n = 1^n a_n + 1^{n-1} a_{n-1} + ... + 1^2 a_2 + 1^1 a_1 + a_0 = a_n + a_{n-1} + ... + a_2 + a_1 + a_0 \pmod 3$$

Donc un nombre est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.

3. Exercice
4. Exercice
5. Exercice
6. Exercice
7. Exercice

□

Exemple 2.1.8. Est-ce que le nombre 100100100 est divisible par 3 ? Le vérifier en calculant la division peut nous prendre un certain temps à la main, rien de très compliqué, juste un peu long. Par contre, en appliquant le critère de divisibilité que nous venons de démontrer, on remarque qu'il s'agit d'additionner les chiffres qui le composent. On obtient donc $1 + 0 + 0 + 1 + 0 + 0 + 1 + 0 + 0 = 3$. Comme $3|3$, le nombre est donc divisible par 3.

Nous pouvons aussi, bien sûr, utiliser la technique que nous avons vue dans la démonstration précédente pour créer nos propres tests de divisibilité, comme le montre l'exemple ci-dessous.

Exemple 2.1.9. Est-ce que le nombre 784 est divisible par 7 ? Pour ce faire, écrivons le nombre sous la forme $(7 \times 10^2) + (8 \times 10^1) + (4 \times 10^0)$. Et maintenant trouvons la valeur de 10^k modulo 7.

$$\begin{aligned} 10^0 &= 1 \\ 10^1 &= 3^1 \pmod 7 = 3 \pmod 7 \\ 10^2 &= 10^1 \times 10^1 \pmod 7 = 3 \times 3 \pmod 7 = 9 \pmod 7 = 2 \pmod 7 \end{aligned}$$

Nous avons donc que

$$\begin{aligned} 784 &= (7\times 10^2)+(8\times 10^1)+(4\times 10^0) \\ &= (7\times 2)+(8\times 3)+(4\times 1) \pmod 7 \ = 14+24+4 \pmod 7 \\ &= 42 \pmod 7 \ = 0 \pmod 7 \end{aligned}$$

On peut donc conclure que 784 est bien divisible par 7.

Remarquez qu'il aurait sans doute été plus facile d'effectuer directement la division pour vérifier que 784 est effectivement divisible par 7. Par contre, la méthode ci-dessous est très générale. Par exemple, si on vous demande ensuite si le nombre 598 est divisible par 7, vous pourriez directement écrire :

$$598 \equiv (5\times 2)+(9\times 3)+(8\times 1) \pmod 7 \ \equiv 45 \pmod 7 \ \equiv 3 \pmod 7$$

Donc il n'est pas divisible par 7.

Exemple 2.1.10. Est-ce que le nombre 57823 est divisible par 11 ? Nous avons que $10 = -1 \pmod{11}$ et donc :

$$\begin{aligned} 57823 &= (5\times 10^4)+(7\times 10^3)+(8\times 10^2)+(2\times 10^1)+(3\times 10^0) \\ &\equiv (5\times(-1)^4)+(7\times(-1)^3)+(8\times(-1)^2)+(2\times(-1)^1)+(3\times(-1)^0) \pmod{11} \\ &\equiv (5\times 1)+(7\times(-1))+(8\times 1)+(2\times(-1))+(3\times 1) \pmod{11} \\ &\equiv 5-7+8-2+3 \pmod{11} \\ &\equiv 7 \pmod{11} \end{aligned}$$

Et donc 57823 n'est pas divisible par 11.

Exemple 2.1.11. Pouvez-vous construire un test de divisibilité par 11 ? On commence par écrire un nombre n sous la forme :

$$n = 10^n a_n + 10^{n-1}a_{n-1} + ... + 10^2 a_2 + 10a_1 + a_0$$

avec $0 \le a_i \le 9$. On remarque que $10 = -1 \pmod{11}$, ce qui nous donne :

$$n = (-1)^n a_n + (-1)^{n-1}a_{n-1} + ... + 1^2 a_2 - 1^1 a_1 + a_0 \pmod{11}$$

Donc un nombre est divisible par 11 si les unités moins les dizaines plus les centaines moins les milliers .... est divisible par 11.

2.2 Les théorèmes de Fermat, Euler et Wilson

Dans ce chapitre, nous allons étudier 3 théorèmes particulièrement important en théorie des nombres. Le théorème de Fermat, entre autre, joue un rôle particulièrement important en cryptographie, et reviendra à plusieurs reprises d'ici la fin du cours.

Definition 2.2.1.

1. Si $x = y \pmod{\text{n}}$ alors on dit que y est un résidu de x modulo n
2. Un ensemble $\{x_1, x_2, ..., x_n\}$ est appelé un système complet de résidu modulo n si pour chaque entier y, il existe un seul x_i tel que $x_i = y \pmod{\text{n}}$.
3. Un ensemble $\{x_1, x_2, ...x_k\}$ est appelé un système réduit de résidu modulo n si $(x_i, n) = 1$ pour tout i et si pour chaque entier y tel que $(y, n) = 1$, il existe un seul x_i tel que $x_i = y \pmod{\text{n}}$.

Definition 2.2.2. Si n est un entier plus grand ou égal à 2, alors on définit $\phi(n)$ comme étant le nombre d'éléments dans un système réduit de résidus modulo n. C'est à dire que $\phi(n)$ est le nombre d'entiers m tels que $0 \le m < n$ et $(m, n) = 1$.

Théorème 2.2.1. **(Théorème d'Euler)** Si $a, n \in \mathbb{Z}$ sont tels que $(a, n) = 1$, alors :

$$a^{\phi(n)} = 1 (\text{mod } n)$$

Démonstration. Supposons que $\{x_1, x_2, ..., x_{\phi(n)}\}$ est un système réduit modulo n et supposons que $(a, n) = 1$. On va commencer par démontrer que $\{ax_1, ax_2, ..., ax_{\phi(n)}\}$ est aussi un système réduit modulo n. Comme ces deux ensembles ont le même nombre d'éléments, il s'agit de démontrer que $ax_i \neq ax_j$ (mod n) si $i \neq j$.

$$\begin{aligned} ax_i = ax_j \text{ (mod n)} &\Rightarrow n | a(x_i - x_j) \\ &\Rightarrow n | (x_i - x_j) \text{ car } (a, n) = 1 \\ &\Rightarrow x_i = x_j \text{ (mod n)} \\ &\Rightarrow i = j \text{ car } \{x_1, x_2, ..., x_n\} \text{ est un système réduit modulo n} \end{aligned}$$

Il s'agit donc bien d'un système réduit modulo n. Le produit des éléments de ces deux systèmes réduits modulo n doit donc être égal modulo n. On a donc :

$$\prod_{i=1}^{\phi(n)} ax_i = \prod_{i=1}^{\phi(n)} x_i \text{ (mod n)}$$

Et maintenant, en sortant le a du produit, on obtient un facteur $a^{\phi(n)}$, ce qui nous donne :

$$a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} x_i \text{ (mod n)}$$

Finalement, comme $(n, x_i) = 1$ pour tout i, on a donc que

$$\left(n, \prod_{i=1}^{\phi(n)} x_i\right) = 1$$

En utilisant les propriétés des modulos, on peut donc simplifier le produit de chaque côté, ce qui nous laisse l'égalité que nous recherchions :

$$a^{\phi(n)} = 1 \text{ (mod n)}$$

□

Nous somme maintenant prêt à énoncer le petit théorème de Fermat. Dans cette section, nous allons le regarder comme un simple corollaire au théorème d'Euler, mais vous devriez regarder en appendice deux autres démonstrations qui sont particulièrement instructives. L'une utilisant des techniques de combinatoire, et l'autre des techniques de la théorie des groupes. La démonstration utilisant la théorie des groupes donne en fait une indication des techniques utilisées dans le domaine de la théorie des nombres algébriques.

Théorème 2.2.2. **(Petit théorème de Fermat)** Si p est un nombre premier et $a \in \mathbb{N}$ tel que $p \nmid a$. Alors :

$$a^{p-1} = 1 (\text{mod } p)$$

Démonstration. Il s'agit d'une conséquence directe du théorème d'Euler. Si p est un nombre premier, alors $\phi(p) = p - 1$. On obtient donc :

$$a^{p-1} = a^{\phi(n)} = 1 \text{ (mod } n)$$

□

Le petit théorème de Fermat est souvent utilisé comme technique probabiliste pour déterminer si un nombre est premier ou non. L'idée est la suivante. Si on veut vérifier si un nombre naturel n est premier, on peut calculer

$$a^{n-1} \pmod{n}$$

pour différentes valeurs de a. Du moment qu'on trouve un entier a pour lequel $a^{n-1} \neq 1 \pmod{n}$, on peut affirmer que le nombre n n'est pas un nombre premier. D'un autre côté, si après avoir testé plusieurs valeurs de a, on obtient toujours $a^{n-1} = 1 \pmod{n}$, alors on est presque certain que le nombre n est premier. Il faut cependant faire très attention car le petit théorème de Fermat ne peut absolument pas nous garantir que le nombre est premier. En effet, il existe quelques entiers, appelé nombres de Carmichael, qui satisfont le petit théorème de Fermat pour tout entier a, mais qui ne sont pas premiers. Le plus petit nombre de Carmichael est 561. Plusieurs questions restent encore ouvertes concernant les nombres de Carmichael. Nous n'irons cependant pas plus loin dans cette direction. Pour compléter cette section, nous allons finalement voir un théorème qui cette fois nous permettra d'affirmer qu'un nombre est premier. Il s'agit cette fois d'un si et seulement si. Bien que les calculs nécessaires pour vérifier qu'un nombre est premier à l'aide du théorème de Wilson sont trop longs pour être d'un grand intérêt, le théorème est particulièrement utile pour son côté théorique.

Théorème 2.2.3. **(Théorème de Wilson)** Si $n \in \mathbb{N}$ tel que $m > 1$. Alors :

$$n \text{ est premier } \iff (n-1)! = -1 (\text{mod } n)$$

Démonstration.
(⇒) Supposons que n est un nombre premier. Si $n = 2$ ou $n = 3$, le résultat est facile à démontrer, il suffit de remplacer dans l'équation. Nous allons donc supposons que n est un nombre premier plus grand ou égal à 5. D'après le petit théorème de Fermat, pour chaque $x \in \{1, 2, ..., (n-1)\}$, il existe un $y = x^{n-2}$ tel que $xy = 1$ (mod n). Supposons que z est un autre entier dans $\{1, 2, ..., (n-1)\}$ tel que $xz = 1$, alors on a :

$$xz = xy \text{ (mod n)} \Longrightarrow z = y \text{ (mod n) car } (x, n) = 1$$

En d'autres mots, pour chaque $x \in \{1, 2, ..., (n-1)\}$, il existe un unique $y \in \{1, 2, ..., (n-1)\}$ tel que $xy = 1 \pmod{n}$.

Maintenant, si on suppose que $x = y$, alors on a $x^2 = 1 \pmod{n}$, ce qui signifie que $n|(x^2 - 1) \Rightarrow n|(x-1)(x+1)$. Comme n est, par hypothèse, un nombre premier, alors on obtient que $n|(x-1)$ ou $n|(x+1)$. De plus, on remarque que $n|(x-1)$ est possible seulement si $x = 1$. De plus, la condition que $n|(x+1)$ est possible seulement si $x = n-1$. En d'autres mots, pour chaque $x \in \{2, 3, ..., n-2\}$, il existe un unique $y \in \{2, 3, ..., n-2\}$ tel que $x \neq y$ et $xy = 1 \pmod{n}$. C'est à dire que tous les nombres dans l'ensemble $\{2, 3, ..., n-2\}$ peuvent être groupés en pairs pour lesquels le produit est 1 modulo n.

Ensuite, il est facile de remarquer que $1 = 1 \pmod{n}$ et $n - 1 = -1 \pmod{n}$. Ceci nous permet d'affirmer que :

$$\prod_{k=1}^{n-1} k = (n-1)! = -1 \pmod{n}$$

Ce qui est exactement ce que nous voulions démontrer.

(⇐) Supposons que n n'est pas un nombre premier. Alors il existe a et b tel que $ab = n$ avec $a, b < n$. Si $a \neq b$, alors le produit $(n-1)!$ contient les facteurs a et b, et donc est un multiple de n. On peut donc conclure que si n est composé et n'est pas un carré parfait, alors $(n-1)! = 0 \pmod{n}$. Si au contraire $n = p^2$ où p est un nombre premier, alors p et $2p$ sont tous deux des facteurs de $(n-1)!$, donc en particulier, en multipliant p et $2p$ on remarque de $(n-1)!$ est un multiple de $(n-1)!$, ce qui signifie que $(n-1)! = 0 \pmod{n}$. Donc si $(n-1)! = -1 \pmod{n}$, alors n ne peut pas être composé, et donc n doit être un nombre premier. □

2.3 L'équation $ax = b$ en modulo

Nous allons maintenant nous intéresser à la résolution des équations algébriques en modulo. Lorsque vous avez commencé à étudier l'algèbre au secondaire, l'une des premières équations que vous avez rencontré avait la forme $ax = b$. Il semble donc approprié de commencer par cette équation dans le contexte des modulos. Remarquez cependant que la solution n'est pas aussi simple que celle que vous connaissez pour les nombres réels. En effet, dans la plupart des cas il n'est pas possible de tout simplement diviser par a étant donné que la division n'est pas bien définie. Le théorème d'Euler, ainsi que le petit théorème de Fermat peuvent cependant nous permettre de contourner ce problème.

Théorème 2.3.1. Si a, b, n sont des entiers, $n > 1$, et $(a, n) = 1$, alors l'équation

$$ax = b \pmod{n}$$

possède exactement une solution.

Démonstration. Premièrement, par le théorème de Euler, si $(a, n) = 1$, alors

$$a \cdot (a^{\phi(n)-2}b) = a^{\phi(n)-1}b = b \pmod{n}$$

donc $x = a^{\phi(n)-2}b$ est une solution de l'équation. Maintenant, supposons que y est aussi une solution de l'équation, alors on a :

$$ax = ay \pmod{n} \Rightarrow x = y \pmod{n} \text{ car } (a, n) = 1$$

Donc la solution est unique. □

Exemple 2.3.1. On veut trouver la solution de l'équation

$$5x = 8 \pmod{13}$$

Premièrement, on remarque que $(5, 13) = 1$, donc par le théorème précédent, il doit y avoir exactement une solution. Il y a deux méthode pour trouver cette solution.
Première méthode : Comme 13 est un nombre premier, par le petit théorème de Fermat on a que :

$$5^{12} = 1 \pmod{13}$$

Ce qui nous donne :

$$\begin{aligned} 5x &= 8 \pmod{13} \\ 5^{11} \cdot 5x &= 5^{11}8 \pmod{13} \\ 5^{12}x &= 5^{11}8 \pmod{13} \\ x &= 5^{11}8 \pmod{13} \\ x &= 12 \pmod{13} \end{aligned}$$

Deuxième méthode : On commence par utiliser l'algorithme d'Euclide pour trouver une solution de l'équation $5x + 13y = 1$. Comme $(5, 13) = 1$, nous savons déjà que cette équation possède une solution, mais nous allons tout de même utiliser l'algorithme d'Euclide pour le calculer :

$$13 = 2(5) + 3$$

$$5 = 1(3) + 2$$

$$3 = 1(2) + 1$$

$$2 = 2(1) + 0$$

Maintenant, en réécrivant l'algorithme d'Euclide à l'envers, on obtient :

$$1 = 3 - 1(2) = 3 - 1[5 - 1(3)] = 3 - 1(5) + 1(3) = 2(3) - 1(5)$$

$$= 2[13 - 2(5)] - 1(5) = 2(13) - 4(5) - 1(5) = 2(13) - 5(5)$$

Donc une solution de l'équation $5x + 13y = 1$ est donnée par $5(-5) + 13(2) = 1$. Maintenant, en multipliant le tout par 8, on obtient :

$$5(-40) + 13(16) = 8$$

Finalement, en calculant le tout modulo 13, on obtient :

$$5(-40) = 8 \pmod{13}$$

La solution est donc $x = -40 = -40 + 4(13) = 12 \pmod{13}$.

Théorème 2.3.2. Si a, b, n sont des entiers et $n > 1$, alors l'équation

$$ax = b \pmod{n}$$

possède au moins une solution si et seulement si $(a, n)|b$. Dans ce cas, elle a exactement (a, n) solutions qui sont données par :

$$x = x_0 + \frac{kn}{(a, n)} \pmod{n}, \quad k \in \mathbb{Z}$$

où x_0 est une solution particulière de l'équation

$$\frac{a}{(a, n)}x = \frac{b}{(a, n)} \left(\mod \frac{n}{(a, n)}\right)$$

Démonstration. Premièrement, notons que $ax = b \pmod{n}$ a une solution si et seulement si il existe un entier x tel que $n|(ax - b)$, ce qui est le cas si et seulement s'il existe des entiers x et y tels que $(ax - b) = (-n)y$, ce qui nous donne finalement qu'il existe une solution si et seulement s'il existe des entiers x et y tels que

$$ax + ny = b$$

Maintenant, nous avons déjà vu que l'ensemble $\{ax + ny\}$ est l'ensemble de tous les multiples de (a, n). Il existe donc une solution si et seulement si $(a, n)|b$, c'est à dire si b est un multiple de (a, n).

On va donc supposer que $(a, n)|b$, c'est à dire que nous sommes dans le cas où il y a une solution. Donc a, b et n sont tous les 3 divisibles par (a, n). En utilisant le théorème du début du chapitre sur les propriétés des modulos, on a donc :

$$\begin{aligned} ax = b \pmod{n} &\iff (a, n)\frac{ax}{(a, n)} = (a, n)\frac{b}{(a, n)} \pmod{n} \\ &\iff \frac{a}{(a, n)}x = \frac{b}{(a, n)} \left(\mod \frac{n}{(a, n)}\right) \end{aligned}$$

Donc si x_0 est une solution de cette dernière équation, alors toutes les autres solutions sont données en ajoutant ou soustrayant des multiples de $\frac{n}{(a, n)}$, c'est à dire que toutes les autres x qui satisfont l'équation sont de la forme :

$$x = x_0 + \frac{kn}{(a, n)} \pmod{n}$$

car seules les solutions modulos n nous intéressent (les autres étant équivalentes). □

Exemple 2.3.2. On veut trouver les solutions de l'équation

$$21x = 6 \pmod{96}$$

Pour ce faire, commençons par calculer le PGCD de 96 et 21 :

$$\begin{aligned} 96 &= 4(21) + 12 \\ 21 &= 1(12) + 9 \\ 12 &= 1(9) + 3 \\ 9 &= 3(3) + 0 \end{aligned}$$

On a donc : $(96, 21) = 3$. Comme $3|6$, il doit donc y avoir des solutions. Nous allons donc commencer par trouver une solution particulière x_0 à l'équation :

$$7x = 2 \ (\mod 32)$$

Comme $(7, 32) = 1$, alors on peut appliquer le théorème d'Euler qui nous donne :

$$7^{\phi(32)} = 1 \pmod{32}$$

Comme $\phi(32) = 16$, on a donc :

$$\begin{aligned} 7x_0 &= 2 \ (\mod 32) \\ 7^{15} \cdot 7x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ 7^{16}x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ x_0 &= 7^{15} \cdot 2 \ (\mod 32) \\ x_0 &= 14 \ (\mod 32) \end{aligned}$$

Par le théorème, on a donc que les solutions de l'équation originale sont :

$$x = 14 \ (\mod 96)$$

$$x = 14 + \frac{96}{3} \ (\mod 96) = 14 + 32 \ (\mod 96) = 46 \ (\mod 96)$$

$$x = 14 + \frac{96 \cdot 2}{3} \ (\mod 96) \ (\mod 96) = 14 + 64 = 78 \ (\mod 96)$$

2.4 Le théorème du reste Chinois

Nous allons maintenant nous intéresser à un problème relativement appliqué et qui nous servira de motivation pour le théorème du reste chinois. Supposons qu'un éleveur de poulet récolte un matin un nombre inconnu d'oeufs. Lorsqu'il groupe les oeufs en paquet de 12, il lui en reste 3. En essayant plutôt de les regrouper en paquets de 7, il lui en reste 5. Combien d'oeufs a récolté l'éleveur ? Le but de cette section est bien sûr de trouver une méthode efficace pour résoudre ce type de problème, mais comme première approche, nous allons utiliser une méthode élémentaire qui consiste à énumérer les différentes possibilités, puis on compare les résultats en commun. En considérant uniquement la condition qu'en faisant des paquets de 12, il nous reste 3 oeuf, on obtient que les différentes possibilités sont :

$$\{3, 15, 27, 39, 51, 63, 75, 87, 99, 111, 123, 135, 147, 159, 171, 183, 195, 207, 219, 231, 243, ...\}$$

Maintenant, en considérant uniquement la seconde condition, c'est à dire qu'en faisant des paquets de 7, il reste 5 oeufs, on obtient que les différentes possibilités sont :

$$\{5, 12, 19, 26, 33, 40, 47, 54, 61, 68, 75, 82, 89, 96, 103, 110, 117, 124, 131, 138, 145, 152, 159, 166, 173, 180, 187$$

$$194, 201, 208, 215, 222, 229, 236, 243, 250, ...\}$$

Maintenant, on cherche les éléments communs aux deux listes que nous venons de trouver, on obtient :

$$\{75, 159, 243, ...\}$$

Bien que nous ayons obtenu seulement 3 solutions, il semble raisonnable de faire l'hypothèse que l'ensemble des solutions est donné par :

$$\{75 + 84k : k \in \mathbb{N} \cup \{0\}\}$$

Il est maintenant possible de démontrer que l'ensemble des solutions que nous avons obtenu est bel et bien correct, ce que nous ne ferons pas ici. Nous allons plutôt utiliser le théorème du reste chinois (que nous allons démontrer) pour recalculer l'ensemble des solutions. Ce qui est important de remarquer, c'est que le problème n'est en fait rien d'autre qu'un système d'équations linéaires en modulo. En effet, le problème aurait pu être tout simplement de demander à trouver l'ensemble des nombres naturels x satisfaisant les équations suivantes :

$$\begin{cases} x = 3 \pmod{12} \\ x = 5 \pmod{7} \end{cases}$$

C'est ce type de problème que le théorème du reste chinois nous permet de résoudre. Question de nous donner un peu d'intuition sur comment aborder une méthode générale de solution, nous allons essayer une seconde approche. Une réécriture du système d'équations nous affirme qu'il existe des entiers k_1 et k_2 tels que :

$$\begin{cases} x = 3 + 12k_1 \\ x = 5 + 7k_2 \end{cases}$$

Comme il s'agit du même x dans les deux cas, on obtient donc :

$$3 + 12k_1 = 5 + 7k_2 \qquad \Rightarrow \qquad 12k_1 - 7k_2 = 2$$

En posant $z = k_1$ et $w = -k_2$, l'équation peut se réécrire sous la forme $12z + 7w = 2$, que nous pouvons résoudre à partir de l'algorithme d'Euclide. On va donc commencer par résoudre l'équation $12z' + 7w' = (12, 7)$.

$$\begin{aligned} 12 &= 1(7) + 5 \\ 7 &= 1(5) + 2 \\ 5 &= 2(2) + 1 \end{aligned}$$

Ce qui nous donne :

$$1 = 5 - 2(2) = 5 - 2[7 - 5] = 3(5) - 2(7) = 3[12 - 7] - 2(7) = 3(12) - 5(7)$$

Et donc en multipliant par deux, on obtient $12(6) + 7(-10) = 2$, ce qui nous donne $z = k_1 = 6$ et $w = -k_2 = -10$, donc $k_2 = 10$. On peut maintenant calculer une première valeur de x en remplaçant k_1 et k_2 dans l'équations, ce qui nous donne :

$$\begin{cases} x = 3 + 12(6) = 75 \\ x = 5 + 7(10) = 75 \end{cases}$$

Maintenant, en remarquant que si y est un autre solution, alors $x - y$ est 0 modulo 12 et aussi 0 modulo 7. Comme $(12, 7) = 1$, on peut donc conclure que $x - y$ est divisible par 84. C'est à dire que l'ensemble des solutions est donné par :

$$\{75 + 84k : k \in \mathbb{Z}\}$$

Si on se concentre sur le problème des oeufs, on doit alors considérer seulement les valeurs de $k \geq 0$. Cette deuxième approche est certainement meilleure que la première, mais il y a encore un obstacle majeur. Cette méthode s'applique seulement dans le cas ou on a seulement un système de deux équations. La question demeure encore entière sur comment résoudre ce type de problème lorsque l'on a plusieurs équations. Nous allons maintenant essayer encore une fois une nouvelle approche, qui cette fois sera facilement généralisable et va nous amener au théorème du reste chinois. Pour ce faire, nous allons résoudre les deux équations suivantes :

$$7x = 1 \pmod{12} \qquad \text{et } 12x = 1 \pmod{7}$$

Nous avons vu dans la section précédente comment résoudre chacune de ces deux équations, mais avant de le faire, nous allons essayer de comprendre comment les solutions de ces équations peuvent nous aider. Pour ce faire, supposons que b_1 est une solution de la première équation, et b_2 est une solution de la seconde équation. Dans ce cas, on obtient :

$$\begin{cases} 7b_1 = 1 \pmod{12} \\ 7b_1 = 0 \pmod{7} \end{cases} \quad \text{et} \quad \begin{cases} 12b_2 = 1 \pmod{7} \\ 12b_2 = 0 \pmod{12} \end{cases}$$

En multipliant les équations de gauche par 3, et les équations de droite par 5, on obtient donc :

$$\begin{cases} 7(3)b_1 = 3 \pmod{12} \\ 7(3)b_1 = 0 \pmod{7} \end{cases} \quad \text{et} \quad \begin{cases} 12(5)b_2 = 5 \pmod{7} \\ 12(5)b_2 = 0 \pmod{12} \end{cases}$$

Maintenant, si on pose la somme des deux équations comme étant x, on obtient :

$$x = 7(3)b_1 + 12(5)b_2$$

Il est facile de voir qu'il s'agit d'une solution du problème original. De plus, les mêmes commentaires que nous avons fait à la fin de notre seconde approche s'appliquent et nous affirme que les solutions seront congrues modulo 84. Nous allons maintenant réécrire notre solution de manière générale sous la forme du théorème du reste chinois, puis nous complèterons ensuite la solution du problème.

Théorème 2.4.1. (Théorème du reste chinois) Si $n_1, n_2, ..., n_m$ sont des entiers positifs non nuls relativement premiers et $a_1, a_2, ..., a_m$ sont des entiers. Alors l'ensemble des solutions du système d'équation :

$$\begin{cases} x = a_1 \pmod{n_1} \\ x = a_2 \pmod{n_2} \\ ... \\ x = a_m \pmod{n_m} \end{cases}$$

est donnée par :

$$x = \left(\sum_{i=1}^{m} \frac{n_1 n_2 ... n_m}{n_i} b_i a_i \right) + k n_1 n_2 ... n_m, \qquad k \in \mathbb{Z}$$

où b_i est une solution de l'équation :

$$\frac{n_1 n_2 ... n_m}{n_i} x_i = 1 \pmod{n_i}$$

Démonstration. Posons $n = n_1 n_2 ... n_m$. Comme $(n_1, n_2, ..., n_m) = 1$, alors

$$\left(n_i, \frac{n}{n_i} \right) = 1$$

Donc pour chaque i, il existe x_i tel que

$$\frac{n}{n_i} x_i = 1 \pmod{n_i}$$

ce qui nous donne :

$$\begin{cases} \dfrac{n a_i}{n_i} x_i = a_i \pmod{n_i} \\ \dfrac{n a_i}{n_i} x_i = 0 \pmod{n_j} \text{ si } i \neq j \end{cases}$$

Donc si on pose

$$x = \sum_{i=1}^{m} \frac{n a_i}{n_i} x_i$$

alors les équations précédentes nous permettent de vérifier facilement que x est une solution du système d'équation. Supposons maintenant que y est aussi une solution du système. On a donc que $x = y \pmod{n_i}$ pour tout i, donc $n_i|(x-y)$ pour tout i. Il s'ensuit que $(x-y)$ est un multiple commun de tous les n_i, donc $(x-y)$ est un multiple de $[n_1, n_2, ..., n_m]$. En d'autres termes, $[n_1, n_2, ..., n_m]|(x-y)$ ce qui nous donne $x = y \pmod{[n_1, n_2, ..., n_m]}$. Comme les n_i sont relativement premiers, on a que $[n_1, n_2, ..., n_m] = n_1 n_2 ... n_m$, ce qui nous donne finalement que

$$x = y \pmod{n}$$

□

Nous allons maintenant utiliser le théorème pour résoudre le problème des oeufs du début de la section.

Exemple 2.4.1. On veut résoudre le système suivant :

$$\begin{cases} x = 3 \pmod{12} \\ x = 5 \pmod{7} \end{cases}$$

En utilisant le théorème, on remarque que la première étape consiste à trouver une solution de l'équation $7x = 1 \pmod{12}$. Pour ce faire, nous allons appliquer l'algorithme d'Euclide pour chercher une solution entière à l'équation $7x + 12y = 1$.

$$\begin{aligned} 12 &= 1(7) + 5 \\ 7 &= 1(5) + 2 \\ 5 &= 2(2) + 1 \end{aligned}$$

Ce qui nous donne :

$$1 = 5 - 2(2) = 5 - 2[7 - 5] = 3(5) - 2(7) = 3[12 - 7] - 2(7) = 3(12) - 5(7)$$

On obtient donc qu'une solution de l'équation $7x = 1 \pmod{12}$ est donnée par $x = b_1 = -5$. Ensuite, nous devons trouver une solution de l'équation $12x = 1 \pmod{7}$. Pour ce faire, on trouver une solution entière à l'équation $12x + 7y = 1$. On remarque qu'ici il s'agit essentiellement du même problème que nous venons de résoudre. On obtient donc la solution $x = b_2 = 3$. Ce qui nous donne finalement la solution suivante du problème original :

$$\begin{aligned} x &= 3(7)(-5) + 5(12)(3) + 12(7)k, \quad k \in \mathbb{Z} \\ &= 75 + 84k, \quad k \in \mathbb{Z} \end{aligned}$$

Ce qui est exactement la même solution que nous avions obtenue précédemment.

Exemple 2.4.2. On veut résoudre le système suivant :

$$\begin{cases} x = 2 \pmod{3} \\ x = 4 \pmod{7} \\ x = 3 \pmod{11} \end{cases}$$

Pour ce faire, on doit commencer par trouver des x_1, x_2 et x_3 qui satisfont les équations suivantes :

$$\begin{cases} 77x_1 = 1 \pmod{3} \\ 33x_2 = 1 \pmod{7} \\ 21x_3 = 1 \pmod{11} \end{cases} \Longrightarrow \begin{cases} 2x_1 = 1 \pmod{3} \\ 5x_2 = 1 \pmod{7} \\ 10x_3 = 1 \pmod{11} \end{cases} \Longrightarrow \begin{cases} x_1 = 2^1 \pmod{3} \\ x_2 = 5^5 \pmod{7} \\ x_3 = 10^9 \pmod{11} \end{cases}$$

$$\Longrightarrow \begin{cases} x_1 = 2 \pmod{3} \\ x_2 = 3 \pmod{7} \\ x_3 = 10 \pmod{11} \end{cases}$$

Nous obtenons donc que

$$x = 77 \cdot 2 \cdot 2 + 33 \cdot 3 \cdot 4 + 21 \cdot 10 \cdot 3 = 1334$$

Nous obtenons donc que l'ensemble des solutions du système est donné par $x = 1334 \pmod{231}$ ce qui nous donne, en simplifiant, que l'ensemble des solutions est donné par :

$$x = 179 \pmod{231} \Longrightarrow x = 179 + 231k, \ k \in \mathbb{Z}$$

2.5 Les polynômes irréductibles

Nous allons maintenant utiliser la théorie des nombres modulos pour montrer que certains polynômes sont irréductibles. Ici il faut comprendre irréductible dans le sens qu'il est impossible de factoriser le polynôme en utilisant uniquement des entiers. L'idée est relativement simple. Si un polynôme $p(x)$ est au contraire réductible, alors il doit exister un entier n tel que $p(n) = 0$, et donc $p(n)$ doit aussi être égal à 0 modulo n'importe quel entier plus grand ou égal à 2.

Exemple 2.5.1. On veut montrer qu'il n'existe aucun entier x tel que

$$p(x) = x^2 + x + 1 = 0$$

pour ce faire, nous allons essayer de travailler modulo 2. Donc s'il existe une solution entière, alors $p(0)$ ou $p(1)$ doit être égal à 0 modulo 2. On a donc :

$$p(0) = 0^2 + 0 + 1 = 1 (\text{mod } 2)$$

$$p(1) = 1^2 + 1 + 1 = 1 (\text{mod } 2)$$

On peut donc conclure que $p(x)$ n'a aucune solution entière, et donc que $p(x)$ est irréductible.

Exemple 2.5.2. On veut montrer qu'il n'existe aucun entier x tel que

$$p(x) = x^2 + x + 2 = 0$$

pour ce faire, nous allons commencer par essayer de travailler modulo 2 comme dans l'exemple précédent. Donc s'il existe une solution entière, alors $p(0)$ ou $p(1)$ doit être égal à 0 modulo 2. On a donc :

$$p(0) = 0^2 + 0 + 2 = 0 (\text{mod } 2)$$

$$p(1) = 1^2 + 1 + 2 = 4 = 0 (\text{mod } 2)$$

On ne peut donc rien conclure en travaillant modulo 2. On va donc essayer modulo 3. On a donc :

$$p(0) = 0^2 + 0 + 2 = 2 (\text{mod } 3)$$

$$p(1) = 1^2 + 1 + 2 = 4 = 1 (\text{mod } 3)$$

$$p(2) = 2^2 + 2 + 2 = 8 = 2 (\text{mod } 3)$$

Comme l'équation n'a aucune solution modulo 3, on peut donc conclure que $p(x) = 0$ n'a aucune solution entière, et donc que $p(x)$ est irréductible.

Remarquez que nous pouvons travailler modulo de n'importe quel nombre naturel supérieur ou égal à 2.

2.6 La cryptographie RSA

Depuis le début de ce chapitre, nous avons vu plusieurs résultats nous permettant de calculer rapidement certaines valeurs. Par contre, il ne semble pas y avoir beaucoup d'applications concrètes à ce que nous avons vu jusqu'à présent. Dans cette section, les choses vont changer. Nous allons voir que les résultats vus depuis le début du chapitre sont en fait très utilisés dans la pratique. L'application que nous allons voir s'appelle la cryptographie, autrement dit le codage des messages secrets. La cryptographie n'est pas un sujet nouveau. Elle est utilisé depuis au moins l'Antiquité. Par contre, trouver une façon efficace de coder un message est relativement complexe. Avec les ordinateurs modernes, la plupart des codes utilisés dans l'Antiquité ou au moyen-âge peuvent être décryptés en quelques minutes tout au plus. La méthode que nous allons voir s'appelle la cryptographie RSA. Il s'agit de l'une des techniques de codage les plus couramment utilisées entre autres sur internet. La technique repose sur la difficulté de factoriser un grand nombre. Plus le nombre est grand, plus un ordinateur prendra de temps à le factoriser (ici on ne parle pas en minutes, mais bien

en mois ou années). Donc, le temps de décrypter le message, son contenu devient souvent inutile, car trop vieux.

Remarquez ici qu'il n'est pas impossible de décrypter le message. Donc si vous envoyez, par exemple, votre numéro de carte de crédit sur internet, et que quelqu'un intercepte le numéro (qui a été bien entendu crypté), il pourra le décoder. Par contre si la méthode pour coder le numéro a été bien choisie, un ordinateur moderne pourrait prendre facilement 100 ans à le décrypter. Donc le temps que mettra la personne qui a intercepté le message à le décoder et à obtenir votre numéro de carte de crédit, il est pratiquement certain que le numéro ne sera plus utilisable de toute façon.

La technique que nous allons voir est pratiquement identique à ce qu'on utilise sur internet. Nous allons cependant tricher un peu en choisissant des nombres relativement petit pour simplifier les calculs. Vous devez cependant vous rappeler que pour que votre code soit sécuritaire, vous devez en pratique choisir des nombres les plus grands possible. Voici maintenant les étapes de la méthode :

Étape 1 : Choisir deux nombres premiers p et q les plus grands possible

Étape 2 : Calculer les valeurs n et ϕ de la façon suivante :

$$n = pq \quad \text{et} \quad \phi(n) = (p-1)(q-1)$$

La formule pour le calcul de $\phi(n)$ sera justifiée à la fin de ce chapitre. Pour le moment, notez seulement que ce $\phi(n)$ est le même que nous avons utilisé dans le théorème d'Euler.

Étape 3 : Choisir un nombre naturel non nul a qui est copremier avec ϕ. C'est à dire un entier positif a tel que $(a, \phi(n)) = 1$.

Étape 4 : Trouver un nombre b tel que $ab = 1 (\text{mod } \phi)$. Pour trouver ce b, on remarque que parce que $(a, \phi(n)) = 1$, alors il existe b et k tels que

$$ab + k\phi(n) = 1$$

que l'on peut trouver en utilisant l'algorithme d'Euclide. En calculant le tout modulo $\phi(n)$, on obtient donc

$$ab = 1 \pmod{\phi(n)}$$

Étape 5 : Envoyez la clé de codage (a, n) à votre correspondant. Il encodera son message à l'aide de la formule suivante :

$$x^a \pmod{\text{n}}$$

Ici x représente la valeur à coder. Il vous envoie alors le message codé.

Étape 6 : Vous décodez le message à l'aide de la clé (b, n), c'est à dire à l'aide de la formule suivante :

$$y^b \pmod{\text{n}}$$

où y représente le message codé que vous avez recu. Nous allons démontrer à la fin de cette section que cette formule permet bien de décrypter le message.

Remarquez que n'importe quelle personne interceptant la clé (a, n) pourrait coder un message et vous l'envoyer. Par contre, vous êtes le seul à connaître la clé (b, n) pour décoder le message. Si les nombres p et q sont petits, il est facile de factoriser n, et donc de trouver la clé pour décoder le message. Par contre, si p et q sont très grands, il est pratiquement impossible de factoriser n dans un temps raisonnable, et donc on ne peut pas calculer la clé pour décoder le message.

Exemple 2.6.1. Votre correspondant souhaite vous envoyer un message crypté. Il vous demande donc de lui envoyer une clé de cryptage. Vous devez donc choisir deux nombres premiers (en théorie le plus grand possible). Ici nous allons choisir $p = 5$ et $q = 13$. On calcule ensuite $n = 5 \times 13 = 65$ et $\phi = 4 \times 12 = 48$. On doit maintenant choisir un nombre copremier avec 48. Pour ce faire, il s'agit de choisir un nombre premier différent de 5 et 13. Choisissons $a = 11$. Puis, on doit trouver un nombre b tel que $ab = 1 \pmod{48}$. Pour ce faire il y a un astuce. Commençons par appliquer l'algorithme d'Euclide aux nombres 11 et 48, ce qui nous donne :

$$\begin{aligned} 48 &= 4(11) + 4 \\ 11 &= 2(4) + 3 \\ 4 &= 1(3) + 1 \\ 3 &= 3(1) + 0 \end{aligned}$$

Nous allons maintenant appliquer l'algorithme d'Euclide à l'envers pour trouver des entiers b et m tels que $48m + 11b = 1$. Nous avons donc :

$$\begin{aligned} 1 &= 4 - 1(3) \\ &= 4 - 1(11 - 2(4)) = 4 - 1(11) + 2(4) = 3(4) - 1(11) \\ &= 3(48 - 4(11)) - 1(11) = 3(48) - 12(11) - 1(11) = 3(48) - 13(11) \end{aligned}$$

Le coefficient du nombre 11 est dans la même classe modulo 48 que le nombre b que nous cherchons. On peut donc trouver b en calculant $-13 + 48 = 35 = b$.

La clé que nous devons envoyer à notre correspondant est $(11, 65)$. La clé de décryptage est $(35, 65)$. Nous devons bien entendu garder cette dernière secrète. Nous devons être les seuls à la connaître. Même notre correspondant ne la connait pas. Prenons maintenant la place de notre correspondant qui souhaite vous envoyer le mot "Bonjour". Commençons par coder chacune des lettres en valeur numérique en utilisant la grille suivante :

a	1	n	14
b	2	o	15
c	3	p	16
d	4	q	17
e	5	r	18
f	6	s	19
g	7	t	20
h	8	u	21
i	9	v	22
j	10	w	23
k	11	x	24
l	12	y	25
m	13	z	26

Donc le mot "Bonjour" peut s'écrire numériquement par :

$$2 - 15 - 14 - 10 - 15 - 21 - 18$$

Nous devons maintenant crypter chacune de ces valeurs à l'aide de la clé $(11, 65)$

On veut premièrement calculer $2^{11} \pmod{65}$.

$$\begin{aligned} 2^1 &= 2 \pmod{65} \\ 2^2 &= 4 \pmod{65} \\ 2^4 &= 2^2 \times 2^2 = 16 \pmod{65} \\ 2^8 &= 2^4 \times 2^4 = 16 \times 16 = 256 = 61 \pmod{65} \\ 2^{11} &= 2^8 \times 2^2 \times 2^1 = 61 \times 4 \times 2 \pmod{65} = (-4) \times 4 \times 2 \pmod{65} \\ &= -16 \times 2 = -32 \pmod{65} = 33 \pmod{65} \end{aligned}$$

On fait maintenant de même avec $15^{11} \pmod{65}$.

$$\begin{aligned} 15^1 &= 15 \\ 15^2 &= 225 = 30 \\ 15^4 &= 15^2 \times 15^2 = 30 \times 30 = 900 = 55 \pmod{65} \\ 15^8 &= 15^4 \times 15^4 = 55 \times 55 = (-10) \times (-10) \pmod{65} = 100 \pmod{65} \\ &= 35 \pmod{65} \\ 15^{11} &= 15^8 \times 15^2 \times 15^1 = 35 \times 30 \times 15 \pmod{65} = (-30) \times 30 \times 15 \pmod{65} \\ &= -900 \times 15 \pmod{65} = 10 \times 15 \pmod{65} = 150 \pmod{65} = 20 \pmod{65} \end{aligned}$$

Puis avec $14^{11} \pmod{65}$.

$$\begin{aligned}
14^1 &= 14 \\
14^2 &= 196 = 1 \pmod{65} \\
14^4 &= 14^2 \times 14^2 = 1 \times 1 \pmod{65} = 1 \pmod{65} \\
14^8 &= 14^4 \times 14^4 = 1 \times 1 \pmod{65} = 1 \pmod{65} \\
14^{11} &= 14^8 \times 14^2 \times 14^1 = 1 \times 1 \times 14 \pmod{65} = 14 \pmod{65}
\end{aligned}$$

En continuant de la même façon, nous obtenons :

$$\begin{aligned}
10^{11} &= 30 \pmod{65} \\
15^{11} &= 20 \pmod{65} \\
21^{11} &= 31 \pmod{65} \\
18^{11} &= 47 \pmod{65}
\end{aligned}$$

Donc le message que vous recevez de votre correspondant est :

$$33 - 20 - 14 - 30 - 21 - 31 - 47$$

Nous voulons maintenant décrypter le message reçu. Commençons par $33^{35} \pmod{65}$:

$$\begin{aligned}
33^1 &= 33 \\
33^2 &= 1089 = 49 \pmod{65} \\
33^4 &= 33^2 \times 33^2 = 49 \times 49 \pmod{65} = 2401 \pmod{65} = 61 \pmod{65} \\
33^8 &= 33^4 \times 33^4 = 61 \times 61 \pmod{65} = (-4) \times (-4) \pmod{65} = 16 \pmod{65} \\
33^{16} &= 33^8 \times 33^8 = 16 \times 16 \pmod{65} = 256 \pmod{65} = 61 \pmod{65} \\
33^{32} &= 33^{16} \times 33^{16} = 61 \times 61 \pmod{65} = 16 \pmod{65} \\
33^{35} &= 33^{32} \times 33^2 \times 33^1 = 16 \times 49 \times 33 \pmod{65} = 25872 \pmod{65} = 2 \pmod{65}
\end{aligned}$$

Ce qui correspond bien à la lettre "b", et en continuant de la même façon, on peut donc retrouver le message complet : "Bonjour".

Nous allons maintenant compléter cette section en démontrant que la formule pour décrypter le message est bel et bien valide, mais avant, nous allons justifier la formule que nous avons utilisée pour calculer $\phi(n)$.

Théorème 2.6.1. Supposons que p et q sont des nombres premiers, alors

$$\phi(pq) = (p-1)(q-1)$$

Démonstration. Posons $n = pq$, alors les seuls diviseurs de n sont $1, p, q, n$. Donc si a est un entier tel que $(a, n) \neq 1$, alors a doit être un multiple de p ou de q. On a donc que $\frac{n}{q} = p$ est le nombre de multiples de q et $\frac{n}{p} = q$ est le nombre de multiples de p. Aussi, comme p et q sont des nombres premiers distincts, alors $[p, q] = n$, il y a donc 1 seul multiple commun de p et q qui est inférieur ou égal à n. Il y a donc $p + q - 1$ entier a tel que $(a, n) \neq 1$, ce qui nous donne finalement :

$$\phi(n) = n - (p + q - 1) = pq - p - q + 1 = p(q-1) - (q-1) = (p-1)(q-1)$$

□

Théorème 2.6.2. Supposons que p et q sont des nombres premiers et $n = pq$. Supposons aussi que a est un entier tel que $(a, \phi(n)) = 1$, et b est un entier tel que $ab = 1 \pmod{\phi(n)}$. Supposons finalement que x est un entier et $y = x^a \pmod{n}$, alors on a :

$$x = y^b \pmod{n}$$

Démonstration. Par hypothèse, on a que $ab = 1 \pmod{\phi(n)}$, on a donc que $\phi(n)|(ab-1)$, c'est à dire qu'il existe un entier k tel que :

$$k\phi(n) = ab - 1 \Longrightarrow ab = k\phi(n) + 1$$

Par le théorème d'Euler, on a que $x^{\phi(n)} = 1 \pmod{n}$. On obtient donc que :

$$y^b = (x^a)^b = x^{ab} = x^{k\phi(n)+1} = (x^{\phi(n)})^k x = 1^k x = x \pmod{n}$$

□

2.7 Exercices

Exercice 2.7.1. Dans chacun des cas, trouver le résidu. C'est à dire, trouver le plus petit entier positif congru (égal) à

1. 98 modulo 8
2. 105 modulo 3
3. 67 modulo 4
4. 2976 modulo 2
5. 1884 modulo 7

Exercice 2.7.2. Trouver le dernier chiffre des sommes et produit suivant :

1. 2987×3474
2. 12986×23652
3. $2365 + 23546$

Exercice 2.7.3. Trouver le dernier chiffre de chacune des expressions suivantes :

1. 768^{212}
2. $16 \times (893^{53} + 212)$
3. $758^{47} + 719^{63}$
4. $152^{129} \times 4365^{259}$

Exercice 2.7.4. Trouver les 2 derniers chiffres de chacune des expressions suivantes :

1. $97^{87} + 3^{43}$
2. $74699^{3623} + 1$
3. $784(327^{129})$
4. $691^{52} + 803^{92}$

Exercice 2.7.5. Démontrer les critères de divisibilité suivant :

1. Un nombre naturel n est divisible par 2 si et seulement si son dernier chiffre est pair.
2. Un nombre naturel n est divisible par 3 si et seulement si la somme de ses chiffres est divisible par 3.
3. Un nombre naturel n est divisible par 4 si et seulement si les unités plus 2 fois les dizaines sont divisibles par 4.
4. Un nombre naturel n est divisible par 4 si et seulement si le nombre formé des deux derniers chiffres est divisible par 4.
5. Un nombre naturel n est divisible par 5 si et seulement si son dernier chiffre est un 0 ou un 5.
6. Un nombre naturel n est divisible par 6 si et seulement si il est divisible par 2 et par 3.
7. Un nombre naturel n inférieur à 1000 est divisible par 7 si et seulement si ses unités plus 3 fois ses dizaines plus 2 fois ses centaines est divisible par 7.
8. Un nombre naturel n est divisible par 8 si et seulement si ses unités, plus deux fois les dizaines, plus quatre fois les centaines est divisible par 8.
9. Un nombre naturel n est divisible par 8 si et seulement si le nombre formé des 3 derniers chiffres de n est divisible par 8.
10. Un nombre naturel n est divisible par 9 si et seulement si la somme de ses chiffres est divisible par 9.
11. Un nombre naturel n est divisible par 11 si et seulement si la somme alterné de ses chiffres est divisible par 11. Ici la somme alterné signifie les unités moins les dizaines plus les centaines moins les milliers, etc.
12. Un nombre naturel n est divisible par 12 si et seulement si la somme de ses chiffres est divisible par 3 et le nombre formé de ses 2 derniers chiffres est divisible par 4.

Exercice 2.7.6. Utilisez les critères de divisibilité que nous avons développé dans ce chapitre pour répondre aux questions suivantes :

1. Est ce que 100 100 100 100 100 100 est divisible par 3 ?
2. Est ce que 12 345 678 910 est divisible par 4 ?

Exercice 2.7.7. Dans chacun des cas, dites si le nombre est divisible par le nombre donné :

1. $762^{613} + 1$ divisible par 7 ?
2. $866^{52} + 32^{18}$ divisible par 3 ?
3. $643^{43} + 7$ divisible par 11 ?
4. $412^{52} - 213^{29}$ divisible par 13 ?

Exercice 2.7.8. Si n est un entier, démontrer que $5n^3 + 7n^5$ est divisible par 12.

Exercice 2.7.9. Démontrer que la différence entre deux cubes consécutifs n'est jamais divisible par 3.

Exercice 2.7.10. Trouver tout les entiers x pour lesquels le reste de la division de $7x$ par 19 est 3.

Exercice 2.7.11. Trouver tous les entiers qui satisfont les congruences suivantes :

1. $x = 2 \pmod 7$
2. $5x = 4 \pmod{11}$
3. $9x = 5 \pmod{19}$
4. $8x = 12 \pmod{20}$
5. $6x = 5 \pmod 9$
6. $14x = 28 \pmod{21}$
7. $2080x = 571 \pmod{33957}$
8. $378x = 93 \pmod{875}$
9. $1105x = 4992 \pmod{8424}$

Exercice 2.7.12. Calculer les valeurs de la fonction ϕ d'Euler suivante :

1. $\phi(653)$
2. $\phi(67)$
3. $\phi(55)$

4. $\phi(40)$
5. $\phi(19512)$

Exercice 2.7.13. Trouver le plus petit entier positif qui est congru à 95! modulo 97. Indice : 97 est un nombre premier.

Exercice 2.7.14. Un matin, un éleveur de poule récole une quantité inconnu d'oeuf. En faisant des paquets de 12, il lui en reste 5. En faisant des paquets de 5, il lui en reste 1. En faisant des paquet de 13, il lui en reste 8. Combien d'oeuf a récolté l'éleveur ? Trouver toutes les possibilités.

Exercice 2.7.15. Trouver l'ensemble des solutions des systèmes d'équations modulos suivants :

1. $$\begin{cases} x = 3 \pmod 7 \\ x = 5 \pmod{11} \end{cases}$$
2. $$\begin{cases} x = 4 \pmod 9 \\ x = 7 \pmod{10} \end{cases}$$
3. $$\begin{cases} x = 18 \pmod{67} \\ x = 45 \pmod{137} \end{cases}$$
4. $$\begin{cases} 5x = 3 \pmod 9 \\ 2x = 19 \pmod{35} \end{cases}$$
5. $$\begin{cases} x = 2 \pmod 3 \\ x = 4 \pmod 5 \\ x = 3 \pmod 7 \end{cases}$$
6. $$\begin{cases} x = 5 \pmod 7 \\ x = 2 \pmod{11} \\ x = 4 \pmod{13} \end{cases}$$

Exercice 2.7.16. Démontrer que les polynômes suivants sont irréductibles :

1. $x^2 + 5x + 2$
2. $x^2 - 3x + 1$

Exercice 2.7.17. Pour que la cryptographie RSA soit sécuritaire, nous avons vu que les nombres utilisés doivent être très grands. En d'autres mots, si les nombres sont relativement petits, il doit être possible de décrypter un message que vous auriez intercepté. Pour illustrer cette idée, supposer que vous interceptez la clé de cryptage $(4493, 5561)$. Pouvez-vous trouver la clé de décryptage ?

Exercice 2.7.18. Vous souhaiter transmettre un message crypter via une ligne qui n'est pas très sécuritaire. Pour ce faire, vous demander à votre correspondant de vous envoyer un clé de cryptage (RSA). Il vous envoie la clé $(91, 1147)$

1. Utiliser la clé que votre correspondant vous a envoyé pour crypter le mot MATH.
2. Une personne malhonnête intercepte votre conversation et cherche la clé de décryptage. Sera-t-il en mesure de la trouver ? Pourquoi ?
3. Quelle est la clé de décryptage ?
4. Utiliser la clé de décryptage que vous avez trouvé dans la partie précédente pour décrypter votre réponse de la première partie. Retrouvez-vous le mot MATH ?

Chapitre 3

Les fonctions arithmétiques

3.1 Introduction aux fonctions arithmétiques

Une fonction arithmétique est une fonction définie sur les nombres naturels. Il existe plusieurs fonctions arithmétiques naturels. On peut chercher par exemple le nombre de diviseurs d'un nombre, la somme des diviseurs, etc. Dans ce chapitre, nous sommes intéressé à étudier plusieurs de ces fonctions, et en particulier établir des formules simples pour les évaluer.

Definition 3.1.1. Une fonction f est dite arithmétique si $f : \mathbb{N} \to \mathbb{R}$.

Remarquez la similarité entre les fonctions arithmétiques et une suite de nombres réels. Techniquement, il s'agit en fait de la même chose. La différence réside dans l'approche que nous allons prendre pour les étudier. Il existe plusieurs fonctions arithmétiques importantes en théorie des nombres. Le tableau ci-dessous présente les principales que nous allons étudier.

Fonctions arithmétiques importantes

$\tau(n)$	Le nombre de diviseurs de n
$\sigma(n)$	La somme des diviseurs de n.
$\omega(n)$	Le nombre de facteurs premiers distincts de n.
$\phi(n)$	La fonction d'Euler définie par : $\phi(n) = \#\{x \in \mathbb{Z} : 1 \leq x < n \text{ et } (x, n) = 1\}$
$\pi(n)$	Le nombre de nombres premiers inférieur ou égal à n.
$\mu(n)$	La fonction de Mobius définie par $\mu(n) = \begin{cases} 0 \text{ si } n \text{ est divisible par un carré parfait différent de 1} \\ (-1)^{\omega(n)} \text{ autrement} \end{cases}$
$1(n)$	La fonction constante $1(n) = 1$
$I(n)$	La fonction identité $I(n) = n$
$\varepsilon(n)$	La fonction définie par $\varepsilon(n) = \begin{cases} 1 \text{ si } n = 1 \\ 0 \text{ autrement} \end{cases} = \left[\frac{1}{n}\right]$

De plus, on a la fonction ci-dessous qui n'est pas une fonction arithmétique, mais qui est souvent utile en théorie des nombres.

Definition 3.1.2. On définit la fonction $[\cdot] : \mathbb{R} \to \mathbb{Z}$ comme étant

$$[x] = \text{ plus petit entier inférieur ou égal à } x$$

Théorème 3.1.1. Si n est un nombre naturel et p un nombre premier, alors le plus grand entier α tel que $p^\alpha | n!$ est :

$$\alpha = \sum_{i=1}^{\infty} \left[\frac{n}{p^i} \right]$$

Exemple 3.1.1. Combien y a-t-il de 0 à la fin de 100! ? Pour ce faire, on doit trouver le plus grand entier α tel que $10^\alpha | 100!$. Comme 10 n'est pas un nombre premier, on ne peut cependant pas utiliser directement le théorème précédent. Cependant, on peut décomposer 10 en produit de nombres premiers : $10 = 2 \times 5$. Donc on doit donc trouver les plus grands entiers β et γ tels que $2^\beta | 100!$ et $5^\gamma | 100!$. On remarque que dans ce cas, $\beta \geq \gamma$, et donc on a que $\alpha = \gamma$. On va donc utiliser le théorème précédent avec $p = 5$:

$$\begin{aligned} \alpha = \gamma &= \left[\frac{100}{5}\right] + \left[\frac{100}{5^2}\right] + \left[\frac{100}{5^3}\right] + \left[\frac{100}{5^4}\right] + \ldots \\ &= \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] + \left[\frac{100}{125}\right] + \left[\frac{100}{5^6 25}\right] + \ldots \\ &= 20 + 4 + 0 + 0 + \ldots \\ &= 24 \end{aligned}$$

Il y a donc 24 zéro à la fin de 100!.

Exemple 3.1.2. On veut calculer $\tau(100)$ et $\sigma(100)$. Pour ce faire, commençons par trouver la liste de tous les diviseurs de 100. On a donc :

$$\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$$

On obtient donc que

$$\tau(100) = 9$$

et

$$\sigma(100) = 1 + 2 + 4 + 5 + 10 + 20 + 25 + 50 + 100 = 217$$

Remarquez qu'heureusement pour nous, le nombre 100 n'est pas très grand, et il nous a donc été relativement facile d'énumérer la liste de tous les diviseurs de 100. Par contre, plus le nombre de diviseurs d'un nombre augmente, plus il sera facile d'oublier un certain nombre de diviseurs. Il nous sera donc nécessaire de trouver une façon de calculer τ et σ sans devoir énumérer la liste de tous les diviseurs. Nous allons faire ceci en utilisant le théorème fondamental de l'arithmétique, c'est à dire en décomposant un nombre en facteurs premiers. Pour que le théorème fondamental nous soit d'une certaine utilité, nous allons cependant avoir besoin de l'aide des fonctions multiplicatives et du produit de Dirichlet que nous allons voir dans la section suivante.

3.2 Les fonctions multiplicatives et le produit de Dirichlet

Nous allons maintenant nous lancer dans une section particulièrement technique, peut-être l'une des plus techniques du cours. Nous allons définir une forme de produit entre deux fonctions arithmétiques, appelé produit de Dirichlet. Ce produit est en fait la clé qui nous permettra, après avoir établie ses propriétés de base, d'établir relativement facilement les propriétés des différentes fonctions arithmétiques.

Definition 3.2.1. Si f est une fonction arithmétique alors :

1. f est **multiplicative** si $f(1) = 1$, et si pour tout entier m, n tel que $(m, n) = 1$ alors $f(mn) = f(m)f(n)$.

2. f est **complètement multiplicative** si $f(1) = 1$, et si pour tout entier m, n alors $f(mn) = f(m)f(n)$.
3. f est **additive** si $f(mn) = f(m) + f(n)$ si $(m, n) = 1$.
4. f est **complètement additive** si $f(mn) = f(m) + f(n)$ pour tout m, n.

Exemple 3.2.1. Les fonctions $1(n)$ et $I(n)$ sont des fonctions complètement multiplicatives. De plus, la fonction $I(n)$ est une fonction complètement additive, mais pas la fonction $1(n)$.

Definition 3.2.2. Si f et g sont des fonctions arithmétiques, alors on définit le produit de Dirichlet "*" comme étant :

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right)$$

Exemple 3.2.2. Le produit de Dirichlet nous permet d'écrire les fonctions $\tau(n)$ et $\sigma(n)$ sous les formes suivantes :

$$\tau = 1 * 1$$
$$\sigma = I * 1$$

Théorème 3.2.1. (Propriétés du produit de Dirichlet)

1. La fonction ε est une identité pour le produit de Dirichlet. C'est à dire que si f est une fonction arithmétique, alors $f * \varepsilon = f$.
2. Le produit de Dirichlet est commutatif. C'est à dire que si f et g sont des fonctions arithmétiques, alors $f * g = g * f$.
3. Le produit de Dirichlet est associatif. C'est à dire que si f, g, h sont des fonctions arithmétiques, alors $(f * g) * h = f * (g * h)$.
4. Si f et g sont des fonctions arithmétiques multiplicatives, alors le produit $f * g$ est aussi une fonction arithmétique multiplicative.

Démonstration.

1. Supposons que f est une fonction arithmétique, et n est un entier positif. Alors on a :

$$(f * \varepsilon)(n) = \sum_{d|n} f(d)\varepsilon\left(\frac{n}{d}\right) = f(n)\varepsilon\left(\frac{n}{n}\right) = f(n)$$

   ce qui confirme que ε est une identité pour le produit de Dirichlet.

2. Il s'agit de remarquer que l'on peut réécrire le produit de Dirichlet sous la forme :

$$(f * g)(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{ab=n} f(a)g(b) = \sum_{ab=n} g(b)f(a) = (g * f)(n)$$

   ce qui confirme que le produit de Dirichlet est commutatif.

3. Supposons que f, g, h sont des fonctions arithmétiques, alors on a :

$$\begin{aligned}
[(f * g) * h](n) &= \sum_{dc=n} (f * g)(d) \cdot h(c) = \sum_{dc=n} \left(\sum_{ab=d} f(a)g(b) \right) h(c) \\
&= \sum_{abc=n} f(a)g(b)h(c) = \sum_{ad=n} f(a) \left(\sum_{bc=d} g(b)h(c) \right) \\
&= \sum_{ad=n} f(a) \cdot (g * h)(d) = [f * (g * h)](n)
\end{aligned}$$

   ce qui confirme que le produit de Dirichlet est associatif.

4. Supposons que m, n sont des entiers tels que $(m,n) = 1$ et $d|(mn)$. Par le théorème fondamental de l'arithmétique, il existe des nombres premiers p_i tels que

$$d = p_1 p_2 ... p_k$$

Comme $d|(mn)$, alors pour chaque i on a que $p_i|m$ ou $p_i|n$, de plus comme $(m,n) = 1$, alors p_i ne peut pas diviser m et n en même temps. On peut donc séparer ces p_i en deux ensembles. Le premier contenant les p_i qui divisent m et l'autre les p_i qui divisent n. Finalement, on remarque que ces deux ensembles doivent être disjoints (i.e. n'avoir aucun élément en commun) sinon cela contredirait la condition $(m,n) = 1$. On va donc noter par d_m le produit des p_i qui divisent m et par d_n le produit des p_i qui divisent n. On a donc :

$$d = d_1 d_2, \qquad (d_1, d_2) = 1$$

Si on revient maintenant à nos fonctions multiplicatives f et g et au produit de Dirichlet. On a donc :

$$\begin{aligned}
(f * g)(mn) &= \sum_{d|(mn)} f(d) g\left(\frac{mn}{d}\right) \\
&= \sum_{(d_m d_n)|(mn)} f(d_m d_n) g\left(\frac{mn}{d_m d_n}\right) \\
&= \sum_{d_m|m} f(d_m) g\left(\frac{m}{d_m}\right) \sum_{d_n|m} f(d_n) g\left(\frac{n}{d_n}\right) \\
&= (f * g)(m) \cdot (f * g)(n)
\end{aligned}$$

La fonction $(f * g)$ est donc multiplicative.

□

Le théorème précédent, bien que purement théorique pour le moment, nous sera d'une très grande utilité dans les sections suivantes pour démontrer que plusieurs des fonctions arithmétiques que nous avons présentées dans la section précédente sont en fait multiplicatives, ce qui nous permettra d'établir des formules relativement simples pour les évaluer.

Théorème 3.2.2. **(Formule d'inversion de Mobiüs)**

$$F(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

Démonstration. Avant de commencer la démonstration, nous allons commencer par rappeler un résultat que nous avons vu au premier chapitre. Rappelons que la théorème du binôme nous dit que si k est un entier positif non nul, alors

$$(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^i y^{k-i}$$

Maintenant, si n est un entier plus grand que 1, on veut évaluer la somme suivante :

$$\sum_{d|n} \mu(d)$$

Par le théorème fondamental de l'arithmétique, on peut décomposer n en produit de nombres premiers. On peut donc écrire :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} ... p_k^{\alpha_k}$$

donc si $d|n$, alors $d = p_1^{\beta_1} p_2^{\beta_2} p_3^{\beta_3} ... p_k^{\beta_k}$. Si l'un des $\beta_i > 1$, alors $\mu(d) = 0$. On peut donc supposer que d est un produit de nombres premiers distincts. On a donc :

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \mu(p_2) + ... + \mu(p_k) + \mu(p_1p_2) + \mu(p_1p_3) \\ &\quad +... + \mu(p_{k-1}p_k) + \mu(p_1p_2p_3) + ... + \mu(p_1p_2...p_k) \\ &= 1 + \binom{k}{1}(-1) + \binom{k}{2}(1) + \binom{k}{3}(-1) + ... + \binom{k}{k}(-1)^k \\ &= (1 + (-1))^k \\ &= 0\end{aligned}$$

D'un autre côté si $n = 1$, alors $\sum_{d|n} \mu(d) = 1$. On obtient donc que :

$$(\mu * 1)(n) = \varepsilon(n), \quad \forall n \in \mathbb{N}\backslash\{0\}$$

Supposons que f est une fonction arithmétique multiplicative, et posons

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

Par définition du produit de Dirichlet, on a donc que $F = f * 1$. On obtient donc :

$$\mu * F = \mu * (f * 1) = f * (1 * \mu) = f * \varepsilon = f$$

Ce qui peut être réécrit sous forme de somme comme étant :

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

Pour l'autre direction, supposons que F est une fonction arithmétique et posons

$$f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$$

En réécrivant le tout sous forme d'un produit de Dirichlet, on a donc posé que $f = \mu * F$. On obtient donc :

$$f * 1 = (\mu * F) * 1 = F * (\mu * 1) = F * \varepsilon = F$$

Ce qui revient à écrire que :

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

□

3.3 La fonction $\tau(n)$

On se rappelle que la fonction $\tau(n)$ est la fonction arithmétique comptant le nombre de diviseurs d'un nombre naturel n. Nous allons utiliser le produit de Dirichlet pour en établir quelques propriétés importantes.

Théorème 3.3.1. La fonction $\tau(n)$ a les propriétés suivantes :

1. $\tau = 1 * 1$
2. $\tau(n)$ est une fonction multiplicative
3. $\tau(p) = 2$ si p est un nombre premier
4. $\tau(p^\alpha) = \alpha + 1$ si p est un nombre premier et $\alpha \geq 2$
5. $\tau(n) = \prod_{i=1}^{k} (\alpha_i + 1)$ si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$
6. $\tau(n)$ est impair si et seulement si n est un carré parfait.

Démonstration.

1. Il s'agit d'utiliser la définition du produit de Dirichlet :
$$1 * 1(n) = \sum_{d|n} 1(d)1\left(\frac{n}{d}\right) = \sum_{d|n} 1 = \tau(n)$$
2. Comme la fonction 1 est une fonction arithmétique multiplicative, alors le produit de Dirichlet $1 * 1$ est aussi une fonction multiplicative. Donc par la première partie du théorème on a que τ est une fonction multiplicative.
3. Si p est un nombre premier, alors par définition il doit avoir exactement 2 diviseurs. On a donc $\tau(p) = 2$.
4. Si p est un nombre premier et α un entier plus grand ou égal à 2, alors les seuls diviseurs de p^α sont : $\{1, p, p^2, p^3, ..., p^\alpha\}$. Il y a donc exactement $\alpha + 1$ diviseurs de p^α, d'où $\tau(p^\alpha) = (\alpha + 1)$.
5. Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Comme τ est une fonction multiplicative, alors on a :
$$\begin{aligned} \tau(n) &= \tau(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) \\ &= \tau(p_1^{\alpha_1})\tau(p_2^{\alpha_2})...\tau(p_k^{\alpha_k}) \\ &= (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) \\ &= \prod_{i=1}^{k}(\alpha_i + 1) \end{aligned}$$
6. Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, donc par la partie précédente, on a que :
$$\tau(n) = \prod_{i=1}^{k}(\alpha_i + 1)$$
donc $\tau(n)$ est impair si et seulement $(\alpha_i + 1)$ est impair pour tout i, ce qui est le cas si et seulement tous les α_i sont pairs. On a donc que $\tau(n)$ est impair si et seulement $\alpha_i = 2\beta_i$ pour tout i ce qui est finalement le cas si et seulement si
$$n = p_1^{2\beta_1} p_2^{2\beta_2} ... p_k^{2\beta_k} = (p_1^{\beta_1} p_2^{\beta_2} ... p_k^{\beta_k})^2$$
c'est à dire si et seulement si n est un carré parfait.

□

Exemple 3.3.1. Nous voulons, à nouveau, calculer $\tau(100)$, mais cette fois en utilisant le théorème précédent. Comme $100 = 2^2 \cdot 5^2$, alors on a :
$$\tau(100) = (2 + 1)(2 + 1) = 3 \cdot 3 = 9$$
ce qui est plus simple que d'énumérer tous les diviseurs de 100.

Exemple 3.3.2. On veut trouver le plus petit entier n ayant exactement 10 diviseurs. C'est à dire qu'on cherche le plus petit entier n tel que $\tau(n) = 10$. Supposons que la décomposition en nombres premiers de n est $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, alors par le théorème précédent nous avons que :
$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)...(\alpha_k + 1) = 10$$
Nous allons donc chercher tous les produits qui donnent 10. Les seuls produits sont donc 10 et 2×5. On va donc tester les deux options pour essayer de trouver le plus petit n. Considérons premièrement que le produit est seulement 10. On a donc :
$$\alpha_1 + 1 = 10 \Longrightarrow \alpha_1 = 9$$
Comme le plus petit nombre premier est 2, on obtient donc que $n = 2^9 = 512$. Nous allons maintenant considérer la seconde option, c'est à dire le produit 2×5. Dans ce cas on a :
$$\begin{cases} (\alpha_1 + 1) = 2 \\ (\alpha_2 + 1) = 5 \end{cases} \Longrightarrow \begin{cases} \alpha_1 = 1 \\ \alpha_2 = 4 \end{cases}$$

Comme les deux plus petits nombres premiers sont 2 et 3, on obtient donc dans ce cas que $n = 2^4 \cdot 3^1 = 48$. En comparant les deux options que nous avons obtenues, on remarque donc que le plus petit n tel que $\tau(n) = 10$ est $n = 48$. On peut maintenant énumérer tous les diviseurs de 48 pour confirmer qu'il a bien exactement 10 diviseurs (remarquez que cette étape n'est bien sur pas vraiment nécessaire). On a donc que les diviseurs de 48 sont :

$$\{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$$

3.4 La fonction $\sigma(n)$

On se rappelle que la fonction $\sigma(n)$ est la fonction arithmétique qui calcule la somme des diviseurs d'un nombre naturel n. Nous allons utiliser le produit de Dirichlet pour en établir quelques propriétés importantes. La procédure est en fait très semblable à ce que nous avons fait dans la section précédente.

Théorème 3.4.1. La fonction $\sigma(n)$ a les propriétés suivantes :

1. $\sigma = I * 1$
2. $\sigma(n)$ est une fonction multiplicative
3. $\sigma(p) = p + 1$ si p est un nombre premier
4. $\sigma(p^\alpha) = \dfrac{1 - p^{\alpha+1}}{1 - p}$ si p est un nombre premier et $\alpha \geq 2$
5. $\sigma(n) = \displaystyle\prod_{i=1}^{k} \left(\frac{1 - p^{\alpha+1}}{1 - p} \right)$ si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$

Démonstration.

1. Il s'agit d'utiliser la définition du produit de Dirichlet :

$$I * 1(n) = \sum_{d|n} I(d) 1\left(\frac{n}{d}\right) = \sum_{d|n} d = \sigma(n)$$

2. Comme I et 1 sont toutes deux des fonctions arithmétiques multiplicatives, alors $I * 1$ est aussi une fonction multiplicative. Par la première partie, on a donc que σ est une fonction multiplicative.

3. Supposons que p est un nombre premier. Alors les seuls diviseurs de p sont 1 et p. On a donc que $\sigma(p) = p + 1$.

4. Supposons que p est un nombre premier et α est un entier positif non nul. Alors les diviseurs de p^α sont : $1, p, p^2, p^3, ..., p^\alpha$. On a donc que :

$$\sigma(p^\alpha) = 1 + p + p^2 + p^3 + ... + p^\alpha$$

Pour compléter la démonstration, remarquons que

$$(1 + p + p^2 + p^3 + ... + p^\alpha)(1 - p) = 1 - p^{\alpha+1}$$

Ce qui nous permet finalement d'obtenir que :

$$\sigma(p^\alpha) = \frac{1 - p^{\alpha+1}}{1 - p}$$

5. Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers. Comme σ est une fonction arithmétique multiplicative, alors on a :

$$\begin{aligned}
\sigma(n) &= \sigma(p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}) \\
&= \sigma(p_1^{\alpha_1}) \cdot \sigma(p_2^{\alpha_2}) \cdot ... \cdot \sigma(p_k^{\alpha_k}) \\
&= \left(\frac{1-p_1^{\alpha_1+1}}{1-p_1}\right) \cdot \left(\frac{1-p_2^{\alpha_2+1}}{1-p_2}\right) \cdot ... \cdot \left(\frac{1-p_k^{\alpha_k+1}}{1-p_k}\right) \\
&= \prod_{i=1}^{k} \left(\frac{1-p_i^{\alpha_i+1}}{1-p_i}\right)
\end{aligned}$$

□

Exemple 3.4.1. Nous voulons à nouveau calculer $\sigma(100)$, mais cette fois en utilisant le théorème précédent. Comme $100 = 2^2 \cdot 5^2$, alors on a :

$$\sigma(100) = \left(\frac{1-2^3}{1-2}\right)\left(\frac{1-5^3}{1-5}\right) = \left(\frac{1-8}{1-2}\right)\left(\frac{1-125}{1-5}\right) = \frac{-7}{-1} \cdot \frac{-124}{-4} = 7 \cdot 31 = 217$$

ce qui est plus simple que d'énumérer tous les diviseurs de 100.

Exemple 3.4.2. On veut trouver tous les entiers n pour lesquels la somme de tous les diviseurs de n est 10. Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ est la décomposition en facteurs premiers du nombre n. Alors on a :

$$\prod_{i=1}^{k} (1 + p_i + p_i^2 + p_i^3 + ... + p_i^{\alpha_i}) = 10$$

Comme les seules façons de décomposer 10 est 10 et 2×5, alors on doit trouver des nombres premiers p tels que $(1 + p + p^2 + p^3 + ... + p^{\alpha_i})$ égal 2, 5 ou 10. Nous avons bien sûr à tester seulement des nombres premiers inférieurs à 10. On a donc si $p = 2$:

$$1$$

$$1 + 2^1 = 3$$

$$1 + 2^1 + 2^2 = 7$$

$$1 + 2^1 + 2^2 + 2^3 > 10$$

Donc aucun des p_i ne peut être 2. Maintenant essayons avec $p = 3$:

$$1$$

$$1 + 3^1 = 4$$

$$1 + 3^1 + 3^2 > 10$$

Donc aucun des p_i ne peut être 3. On va donc essayer avec $p = 5$:

$$1$$

$$1 + 5^1 = 6$$

$$1 + 5^1 + 5^2 > 10$$

Donc aucun des p_i ne peut être 5. On va finalement essayer avec $p = 7$:

$$1$$

$$1 + 7^1 = 8$$

$$1 + 7^1 + 7^2 > 10$$

Donc aucun des p_i ne peut être 7. Comme la somme $(1 + p + p^2 + p^3 + ... + p^{\alpha_i})$ n'est jamais $2, 5$ ou 10, on est donc forcé de conclure qu'il n'existe aucun n tel que $\sigma(n) = 10$.

Exemple 3.4.3. On veut trouver tous les entiers n pour lesquels la somme de tous les diviseurs de n est 13. C'est à dire qu'on cherche un entier n tel que $\sigma(n) = 13$. Supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers. On a donc :

$$\prod_{i=1}^{k} (1 + p_i + p_i^2 + p_i^3 + ... + p_i^{\alpha_i}) = 13$$

Comme 13 est un nombre premier, il n'est pas possible de le décomposer en un produit. On a donc :

$$(1 + p + p^2 + p^3 + ... + p^{\alpha}) = 13$$

On va donc chercher un nombre premier p qui satisfait cette condition en testant un par un tous les nombres premiers inférieurs à 13. Commençons avec le nombre 2 :

$$1$$

$$1 + 2^1 = 3$$

$$1 + 2^1 + 2^2 = 7$$

$$1 + 2^1 + 2^2 + 2^3 > 13$$

Donc $p \neq 2$. Maintenant essayons avec 3 :

$$1$$

$$1 + 3^1 = 4$$

$$1 + 3^1 + 3^2 = 13$$

Donc une première possibilité est $p = 3$ et $\alpha = 2$. On va continuer à essayer quand même afin de voir s'il s'agit de la seule option. Essayons que 5

$$1$$

$$1 + 5^1 = 6$$

$$1 + 5^1 + 5^2 > 13$$

En continuant de la même manière avec 7 et 11, on remarque qu'il s'agissait effectivement de la seule option. On a donc que la seule possibilité est :

$$n = 3^2 = 9$$

Bien que ce ne soit pas vraiment nécessaire, pour se convaincre que notre solution est vraiment correcte on peut maintenant vérifier que $\sigma(9) = 13$. Pour ce faire, énumérons la liste de tous les diviseurs de 9 :

$$\{1, 3, 9\}$$

en calculant leur somme, on obtient donc :

$$\sigma(9) = 1 + 3 + 9 = 13$$

3.5 Les fonctions $\omega(n)$ et $\mu(n)$

Nous voulons maintenant étudier les fonctions $\omega(n)$ et $\mu(n)$. On se rappelle que si n est un nombre naturel, alors on définit $\omega(n)$ comme étant le nombre de facteurs premiers distincts de n, et $\mu(n)$ est définit par :

$$\mu(n) = \begin{cases} 0 \text{ si } n \text{ est divisible par un carré parfait différent de 1} \\ (-1)^{\omega(n)} \text{ autrement} \end{cases}$$

Théorème 3.5.1. Les fonctions $\omega(n)$ et $\mu(n)$ ont les propriétés suivantes :

1. $\omega(n)$ est une fonction additive, c'est à dire que $\omega(mn) = \omega(m) + \omega(n)$ si $(m,n) = 1$.
2. $\mu(n)$ est une fonction multiplicative
3. $\sum_{d|n} \mu(d) = 0$ si $n > 1$
4. $\sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1$
5. $\sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = n$

Démonstration.

1. Supposons que $m = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ et $n = q_1^{\beta_1}q_2^{\beta_2}...q_l^{\beta_l}$ sont les décompositions en facteurs premiers de m et n. Comme $(m,n) = 1$ alors $p_i \neq q_j$ pour tout i,j. On a donc :

$$\omega(mn) = k + l = \omega(m) + \omega(l)$$

   La fonction ω est donc additive.

2. Supposons que m,n sont des entiers plus grands positifs tels que $(m,n) = 1$. Si m ou n est divisible par un carré parfait, alors mn l'est aussi, donc dans ce cas $\mu(mn) = \mu(m)\mu(n) = 0$. D'un autre côté, si mn est divisible par un carré parfait, alors il existe un nombre premier p tel que $p^2|mn$. Dans ce cas on obtient que $p^2|m$ ou $p^2|n$, ce qui veut dire qu'on obtient à nouveau que $\mu(mn) = \mu(m)\mu(n) = 0$. On va donc supposer que m, n et mn ne sont pas divisibles par un carré parfait. Dans ce cas, on obtient :

$$\mu(mn) = (-1)^{\omega(mn)} = (-1)^{\omega(m)+\omega(n)} = (-1)^{\omega(m)}(-1)^{\omega(n)} = \mu(m)\mu(n)$$

   ce qui confirme que μ est une fonction multiplicative.

3. La preuve est incluse dans celle du théorème d'inversion de Mobiüs.

4. Définissons une fonction arithmétique $f(n)$ comme étant :

$$f(n) = (\mu * \tau)(n) = \sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right)$$

   par le théorème d'inversion de Mobius on a donc :

$$\tau(n) = (f * 1)(n) = \sum_{d|n} f(d)$$

   par définition de la fonction τ, ou si vous préférez par les propriétés de la fonction τ on obtient donc que $f = 1$. On obtient donc :

$$\sum_{d|n} \mu(d)\tau\left(\frac{n}{d}\right) = 1$$

5. Définissons une fonction arithmétique $f(n)$ comme étant :

$$f(n) = (\mu * \sigma)(n) = \sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right)$$

   par le théorème d'inversion de Mobiüs on a donc :

$$\sigma(n) = (f * 1)(n) = \sum_{d|n} f(d)$$

par définition de la fonction σ, ou si vous préférez par les propriétés de la fonction σ on obtient donc que $f(n) = I(n)$. On obtient donc :

$$\sum_{d|n} \mu(d)\sigma\left(\frac{n}{d}\right) = I(n) = n$$

□

3.6 La fonction $\phi(n)$

Nous allons maintenant étudier les propriétés de la fonction ϕ d'Euler que nous avons définie dans le chapitre précédent. Rappelons nous qu'elle a joué un rôle important dans le théorème d'Euler, mais que nous avons, jusqu'à présent, aucune façon de la calculer de manière efficace. Cela va changer avec le théorème ci dessous :

Théorème 3.6.1. La fonction $\phi(n)$ a les propriétés suivantes :

1. $I = \phi * 1$ en d'autre terme : $\sum_{d|n} \phi(d) = n$
2. $\phi = \mu * I$
3. La fonction $\phi(n)$ est une fonction multiplicative
4. $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$ où p est un nombre premier.
5. $\phi(n)$ est pair pour tout $n > 2$
6. Si $m|n$, alors $\phi(m)|\phi(n)$
7. $\phi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)$ si $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$

Démonstration.

1. Considérons n un entier plus grand ou égal à 2, et d un entier positif tel que $d|n$. Posons

   $$E_d = \{k \in \mathbb{Z}, 1 \leq k \leq n : (k, n) = d\}$$

   nous voulons trouver combien d'éléments se trouvent dans l'ensemble E_d. Donc si k est un entier tel que $(k, d) = d$, alors il existe des entiers k' et d' tels que $dk' = k$ et $dn' = n$ avec $(k', n') = 1$, autrement d ne serait pas le PGCD. Maintenant, par définition de la fonction ϕ, on a donc qu'il y a $\phi(n')$ entier k' tel que $(k', n') = 1$. Maintenant, on a que $\phi(n') = \phi(\frac{n}{d})$, ce qui veut dire qu'il y a $\phi(\frac{n}{d})$ entiers k tel que $(k, n) = d$. On peut donc conclure qu'il y a $\phi(\frac{n}{d})$ éléments dans l'ensemble E_d. Maintenant on remarque que tous les entiers m tels que $1 \leq m \leq n$ doivent être dans l'un des ensembles E_d où $d|n$. On a donc que :

   $$n = \sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$$

2. Il s'agit d'appliquer la formule d'inversion de Mobius. Comme $I = \phi * 1$, alors la formule nous donne que

   $$\phi = \mu * I$$

   C'est à dire que :

   $$\phi(n) = \sum_{d|n} \mu(d) I\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d)\frac{n}{d}$$

3. Nous avons déjà démontré que les fonctions μ et I sont des fonctions multiplicatives, donc la fonction $\mu * I$ est aussi une fonction multiplicative, donc par la partie précédente on obtient que ϕ est une fonction multiplicative.

4. $\phi(p^\alpha)$ est le nombre d'entiers m tel que $1 \leq m \leq p^\alpha$ et $(m, p^\alpha) = 1$. Comme p est un nombre premier, les seuls entiers m tels que $(m, p^\alpha) \neq 1$ sont les multiples de p. Il est facile de voir qu'il y a $\dfrac{p^\alpha}{p}$ multiples de p, ce qui nous donne :
$$\phi(p^\alpha) = p^\alpha - \frac{p^\alpha}{p} = p^\alpha - p^{\alpha-1}$$

5. Supposons que n est un entier supérieur à 2, alors on peut décomposer n en facteurs premiers $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Comme la fonction ϕ est multiplicative, on a donc :
$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})...\phi(p_k^{\alpha_k})$$
Pour montrer que $\phi(n)$ est pair, il s'agit donc seulement de démontrer qu'au moins un des $\phi(p_i^{\alpha_i})$ est pair. Supposons que l'un des p_i est impair, disons p_k, alors on a :
$$\phi(p_k^{\alpha_k}) = p^k - p^{k-1}$$
avec p^k et p^{k-1} tous deux impairs. Comme la différence entre deux nombres impairs est toujours pair, alors $\phi(p^k)$ est pair. Supposons maintenant qu'aucun des p_i est impair, alors dans ce cas $n = 2^\alpha$. On a donc que $\phi(n) = 2^n - 2^{n-1}$ avec $n \geq 2$ car $n > 2$. $\phi(n)$ est donc la différence entre deux nombres pairs, qui est aussi un nombre pair. On obtient donc que $\phi(n)$ est un nombre pair pour tout entier $n > 2$.

6. Supposons que m et n sont des entiers tels que $m|n$, et supposons que $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ et $m = p_1^{\beta_1} p_2^{\beta_2} ... p_r^{\beta_r}$ sont les décompositions en facteurs premiers de m et n. Comme ϕ est une fonction multiplicative, on a donc :
$$\phi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) \qquad \phi(m) = \prod_{i=1}^{r}(p_i^{\beta_i} - p_i^{\beta_i - 1})$$
On obtient donc que :
$$\begin{aligned}
\frac{\phi(n)}{\phi(m)} &= \frac{\prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i-1})}{\prod_{i=1}^{r}(p_i^{\beta_i} - p_i^{\beta_i-1})} \\
&= \left(\frac{p_1^{\alpha_1} - p_1^{\alpha_1-1}}{p_1^{\beta_1} - p_1^{\beta_1-1}}\right)\left(\frac{p_2^{\alpha_2} - p_2^{\alpha_2-1}}{p_1^{\beta_2} - p_2^{\beta_2-1}}\right)...\left(\frac{p_r^{\alpha_r} - p_r^{\alpha_r-1}}{p_1^{\beta_r} - p_r^{\beta_r-1}}\right)\prod_{i=r+1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i-1}) \\
&= \left[\frac{p^{\alpha_1-1}}{p^{\beta_1-1}}\left(\frac{p-1}{p-1}\right)\right]\left[\frac{p^{\alpha_2-1}}{p^{\beta_2-1}}\left(\frac{p-1}{p-1}\right)\right]...\left[\frac{p^{\alpha_r-1}}{p^{\beta_r-1}}\left(\frac{p-1}{p-1}\right)\right]\prod_{i=r+1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i-1}) \\
&= p^{\alpha_1-\beta_1}p^{\alpha_2-\beta_2}...p^{\alpha_r-\beta_k}\prod_{i=r+1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i-1})
\end{aligned}$$
Comme le quotient nous donne bien un entier, on obtient donc que $\phi(m)|\phi(n)$.

7. Comme ϕ est une fonction multiplicative, si $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ est la décomposition de n en facteurs premiers, alors on a :
$$\begin{aligned}
\phi(n) &= \prod_{i=1}^{k}\phi(p_i^{\alpha_i}) = \prod_{i=1}^{k}(p^{\alpha_i} - p^{\alpha_i-1}) = \prod_{i=1}^{k}p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right) \\
&= \left(\prod_{i=1}^{k}p_i^{\alpha_i}\right)\left[\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)\right] = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right)
\end{aligned}$$

□

Exemple 3.6.1. On veut évaluer la valeur de $15^{74} \pmod{52}$. Commençons par calculer $\phi(52)$. Pour ce faire, remarquons que $52 = 2^2 \cdot 13$. On a donc :

$$\phi(52) = 52\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{13}\right) = 52\left(\frac{1}{2}\right)\left(\frac{12}{13}\right) = \frac{52 \cdot 12}{26} = 24$$

Comme $(15, 52) = 1$, par le théorème d'Euler, on a donc que :

$$15^{24} = 1 \pmod{52}$$

De plus, comme $74 = 3(24) + 2$, alors on a :

$$15^74 = 15^{3(24)+2} = (15^{24})^3 \cdot 15^2 = 15^2 = 225 = 17 \pmod{52}$$

3.7 La fonction $\pi(n)$

Nous allons maintenant nous intéresser à la fonction $\pi(n)$ qui compte le nombre de nombres premiers inférieur ou égal à n. Notons que cette fonction n'est pas additive ni multiplicative, ce qui la rend beaucoup plus compliquée à étudier que les autres fonctions que nous avons étudiées depuis le début du chapitre. Notons aussi que bien que nous allons regarder la plupart du temps cette fonction comme une fonction arithmétique, rien ne nous empêche de traiter la fonction comme une fonction sur les nombres $\mathbb{R}$. Dans ce cas, si $x \in \mathbb{R}$, on définit $\pi(x)$ comme étant le nombre de nombres premiers inférieur ou égal à x.

Théorème 3.7.1. La fonction $\pi(n)$ a les propriétés suivantes :

1. $\lim_{n\to\infty} \pi(n) = \infty$
2. $\pi(n) \geq \ln(\ln(n))$
3. $\frac{\ln(2)}{4}\frac{n}{\ln(n)} < \pi(n) < 9\ln(2)\frac{n}{\ln(n)}$ (Inégalités de Tchebycheff)
4. $\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$ (Théorème fondamental des nombres premiers)

Démonstration.

1. Cette propriété est seulement une réécriture du fait qu'il existe une infinité de nombres premiers. Comme la fonction $\pi(n)$ est croissante par définition, on doit donc avoir que :

$$\lim_{n\to\infty} \pi(n) = \infty$$

2. Premièrement, on doit se rappeler de la preuve de l'infinitude des nombres premiers que si $\{p_1, p_2, p_3, ...\}$ est l'ensemble des nombres premiers, alors

$$p_{k+1} \leq p_1 p_2 p_3 ... p_k + 1, \qquad \forall k \in \mathbb{N}$$

Nous allons maintenant montrer par induction que $p_{r+1} \leq 2^{2^r}$. Remarquons premièrement que si $r = 0$, alors on a l'égalité, donc l'inégalité est satisfaite. On va donc supposer (hypothèse d'induction) que $p_{k+1} \leq 2^{2^k}$ pour tout $k \leq r$. On obtient donc pour $r + 1$:

$$\begin{aligned} p_{r+2} &\leq p_1 p_2 p_3 ... p_r p_{r+1} + 1 \\ &\leq 2^{2^0} 2^{2^1} 2^{2^2} ... 2^{2^{r-1}} 2^{2^r} + 1 \\ &= 2^{(\Sigma_{i=0}^{r} 2^i)} + 1 \\ &= 2^{2^{(r+1)}-1} + 1 \\ &\leq 2^{2^{r+1}} \end{aligned}$$

Ce qui complète la preuve par induction. Maintenant, remarquons que si n est un nombre entier, alors il existe un entier r tel que :

$$e^{e^{r-1}} < n \leq e^{e^r}$$

La seconde inégalité nous permet d'obtenir que $r \geq \ln(\ln(n))$. De plus, comme $2 < e$ et que la fonction π est croissante, on obtient donc les inégalités suivantes :

$$\pi(n) \geq \pi(e^{e^{r-1}}) \geq \pi(2^{2^{r-1}}) \geq \pi(p_r) = r \geq \ln(\ln(n))$$

ce qui complète la démonstration.

3. La démonstration est trop compliquée pour le niveau du cours, elle ne sera donc pas donnée ici. Vous êtes encouragé à chercher dans la littérature pour en trouver une démonstration.
4. Idem au point précédent. Notez cependant qu'il existe plusieurs démonstrations de ce résultat, certaines utilisant uniquement des outils élémentaires, d'autres du calcul et des nombres complexes, ou encore des notions encore plus avancées.

□

Théorème 3.7.2. **(Postulat de Bertrand)** Pour tout entier positif n, il existe un nombre premier p satisfaisant

$$n < p \leq 2n$$

Le résultat précédent est une conséquence des inégalités de Tchebycheff. Comme nous n'avons pas fait la démonstration de ces dernières inégalités, nous ne ferons pas non plus la démonstration du Postulat de Bertrand.

Exemple 3.7.1. On veut utiliser le théorème fondamental des nombres premiers pour trouver une approximation du nombre de nombre premier inférieur à 1000. C'est à dire qu'on veut approximer $\pi(1000)$. Pour ce faire, remarquons que :

$$\lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1$$

signifie que si n est grand, alors $\pi(n) \approx \dfrac{n}{\ln(n)}$. On obtient donc que :

$$\pi(1000) \approx \frac{1000}{\ln(1000)} \approx 145$$

Il y a donc approximativement 145 nombres premiers qui sont inférieurs à 1000. En réalité, si on fait une énumération complète de tous les nombres premiers inférieurs à 1000, on remarque qu'il y en a 168. L'approximation est donc loin d'être parfaite, mais on obtient au moins un ordre de grandeur correct.

Exemple 3.7.2. On veut utiliser les inégalités de Tchebycheff pour trouver une borne minimale et une borne maximale pour la valeur de $\pi(1000)$. Pour la borne minimale, on a donc :

$$\pi(1000) > \frac{\ln(2)}{4} \cdot \frac{1000}{\ln(1000)} \approx 25$$

Maintenant, pour la borne maximale, on obtient :

$$\pi(1000) < 9\ln(2)\frac{1000}{\ln(1000)} \approx 903$$

On peut donc affirmer de manière certaine qu'il y a entre 25 et 903 nombres premiers inférieurs à 1000. La valeur correct $\pi(1000) = 168$ ce trouve bien dans cet intervalle.

3.8 Les nombres parfaits

On se rappelle de notre introduction que l'une des raisons qui ont motivé les débuts de la théorie des nombres a été la forme de mythologie que Pythagore attribuait aux nombres. À chaque nombre, il associait une signification. En particulier, il disait du nombre 6 qu'il était parfait, car il était la somme de ses diviseurs ($6 = 1 + 2 + 3$). Techniquement, en se basant sur notre définition d'un diviseur, il aurait plutôt fallu dire que 6 est la somme de ses diviseurs propres. Autrement dit il aurait fallu ajouter 6 à notre somme.

Bien que le côté mystique des nombres disparu peu à peu, l'idée de trouver des nombres parfait subsista. On peut en effet retrouver la définition d'un nombre parfait dans le 7e livre d'Euclide.

Definition 3.8.1. Si n est un entier, alors on dit que n est un nombre parfait si $\sigma(n) = 2n$.

Notez qu'il est néssaire d'écrire $2n$ dans notre définition, car la somme des diviseurs de n inclura obligatoirement lui même. Les 4 premiers nombres parfaits étaient connus dès l'époque des Grecques, il fallut ensuite attendre l'an 1456 pour qu'un cinquième nombre parfait soit trouvé. En 2013, il y a présentement 48 nombres parfaits connus. Nous ne savons cependant toujours pas s'il existe une infinité de nombres parfaits, nous ne savons pas non plus s'il existe un nombre parfait impair. La but de cette section sera d'essayer de caractériser les nombres parfaits, et ce dans le but de pouvoir calculer (facilement) les 4-5 premiers nombres parfait. Comme nous ne savons toujours pas s'il existe un nombre parfait impair, nous allons nous concentrer ici uniquement sur les nombres parfaits pairs.

Théorème 3.8.1. Si n est un nombre parfait pair, alors n peut s'écrire sous la forme :

$$n = 2^{k-1}(2^k - 1)$$

où $2^k - 1$ est un nombre premier. De plus, tous les nombres de cette forme sont des nombres parfaits.

Démonstration. Supposons que n est un nombre parfait pair. Alors par définition d'un nombre parfait, on a :

$$\sigma(n) = 2n$$

De plus, comme n est par hypothèse pair, on peut écrire n sous la forme

$$n = 2^k m, \quad k \geq 1, \quad (2, m) = 1$$

En remplaçant dans la définition d'un nombre parfait, et en utilisant la multiplicativité de la fonction σ, on obtient donc :

$$\sigma(n) = \sigma(2^k m) = \sigma(2^k)\sigma(m) = (2^{k+1} - 1)\sigma(m) \quad \text{et} \quad \sigma(n) = 2n = 2^{k+1} m$$

En particulier, on obtient l'égalité :

$$(2^{k+1} - 1)\sigma(m) = 2^{k+1} m$$

Maintenant, comme le nombre $2^{k+1} - 1$ est impair, on doit avoir par le lemme d'Euclide que $(2^{k+1} - 1) | m$, c'est à dire qu'il existe un entier y tel que $(2^{k+1} - 1)y = m$ ou de manière équivalente :

$$y = \frac{m}{2^{k+1} - 1}$$

En particulier, m et y sont tout deux des diviseurs de m, ce qui signifie que $\sigma(m) \geq m + y$. On obtient donc :

$$\sigma(m) = \frac{2^{k+1} m}{2^{k+1} - 1} = 2^{k+1} y \quad \text{et} \quad \sigma(m) \geq m + y = (2^{k+1} - 1)y + y = 2^{k+1} y$$

Ce qui signifie que l'inégalité dans l'équation de droite doit en fait être un égalité, c'est à dire que m et y doivent être les deux seuls diviseurs de m. Comme 1 est toujours un diviseur, on doit donc avoir $y = 1$, et de plus, comme m possède seulement deux diviseurs, il doit être premier. On a donc :

$$m = (2^{k+1} - 1)y) = 2^{k+1} - 1 \quad \text{et} \quad m \text{ est un nombre premier}$$

Et finalement, on obtient que :

$$n = 2^k(2^{k+1}-1) \quad \text{avec} \quad 2^{k+1}-1 \text{ un nombre premier}$$

où de manière équivalente (en remplaçant k par $k-1$, on obtient :

$$n = 2^{k-1}(2^k-1) \quad \text{avec} \quad 2^k-1 \text{ un nombre premier}$$

D'un autre côté, supposons que 2^p-1 est un nombre premier, alors on a :

$$\begin{aligned}\sigma(2^{p-1}(2^p-1)) &= \sigma(2^{p-1})\sigma(2^p-1)\\ &= \left(\frac{1-2^p}{1-2}\right)2^p\\ &= (2^p-1)2^p\\ &= 2\left(2^{p-1}(2^p-1)\right)\end{aligned}$$

On obtient donc que $2^{p-1}(2^p-1)$ est un nombre parfait. □

Les nombres premiers de la forme 2^n-1 sont donc important pour bien comprendre les nombres parfait, ce qui nous amène à leur donner un nom.

Definition 3.8.2. On appelle un nombre premier de Mersenne un nombre premier de la forme 2^n-1 où n est un entier.

Donc si on souhaite trouver des nombres parfaits, on devra en premier essayer de trouver des nombres premiers de Mersenne. Historiquement, certaine personne on cru que tout les nombres de la forme 2^n-1 était premier, malheureusement, ce n'est absolument pas le cas. Le théorème suivant va cependant nous aider dans notre recherche.

Théorème 3.8.2. Supposons que 2^n-1 est un nombre premier de Mersenne, alors n est un nombre premier.

Démonstration. Supposons qu'au contraire n n'est pas un nombre premier. Alors $n = pq$ où p et q sont des entiers strictement plus grands que 1. On a donc :

$$\begin{aligned}(1+2^p+(2^p)^2+(2^p)^3+\ldots+(2^p)^{q-1})(2^p-1) &= \left(\sum_{i=0}^{q-1}(2^p)^i\right)(2^p-1)\\ &= \left(\frac{2^{pq}-1}{2^p-1}\right)(2^p-1)\\ &= 2^{pq}-1\end{aligned}$$

Donc si n n'est pas un nombre premier, alors $2^n-1 = 2^{pq}-1$ est un nombre composé. On peut donc conclure que si 2^n-1 est un nombre premier, alors n doit être un nombre premier. □

À partir des deux résultats précédents, il devient relativement facile de trouver les 4 premiers nombres parfait. Avec un peu de patience, le 5e est aussi à votre porté. Il faut cependant faire attention. Même si n est un nombre premier, il n'y a aucune garantie que le nombre 2^n-1 soit un nombre premier. En particulier, si on prend $n = 11$, on obtient :

$$2^{11}-1 = 2047 = 23 \times 89$$

En lien avec les nombres parfaits, on peut définir ce qu'on appelle les nombres déficients, les nombres abondants et les nombres amicaux.

Definition 3.8.3. Si n est un entier, alors on dit que n est

1. parfait si $\sigma(n) = 2n$
2. déficient si $\sigma(n) < 2n$
3. abondant si $\sigma(n) > 2n$

Definition 3.8.4. Si m et n sont des entiers alors on dit que m et n sont des nombres amicaux si la somme des diviseurs propres de m est égale à n et la somme des diviseurs propres de n est égale à m.

Il faut faire attention ici de faire la distinction entre la somme des diviseurs propres d'un nombre et la somme de ses diviseurs. Lorsque l'on parle d'un diviseur propre d'un nombre n, on exclut le nombre n de la somme. Par contre, la somme des diviseurs l'inclut. La fonction σ représente la somme de tout les diviseurs. Ceci nous amène au résultat suivant :

Théorème 3.8.3. Si n et m sont des entiers, alors n et m sont amicaux si et seulement si

$$\sigma(m) = \sigma(n) = m + n$$

Démonstration. Un diviseur propre d'un nombre k est un diviseur de k différent de k. On obtient donc que la somme des diviseurs propres de m et la somme des diviseurs propres de n sont donnés respectivement par :

$$\sigma(m) - m \qquad \text{et} \qquad \sigma(n) - n$$

Par définition des nombres amicaux, on doit donc avoir :

$$\sigma(m) - m = n \qquad \text{et} \qquad \sigma(n) - n = m$$

En isolant $\sigma(m)$ et $\sigma(n)$ de chacune des expressions, on obtient donc :

$$\sigma(m) = \sigma(n) = m + n$$

□

Il est facile de voir que si $n = m$ est un nombre parfait, alors m et n sont des nombres amicaux. Le plus petit couple de nombres (m, n) qui sont amicaux avec $m \neq n$ est $(220, 284)$.

Exemple 3.8.1. On veut montrer que $(220, 284)$ est un couple de nombre amicaux. Pour ce faire, commençons par décomposer ces deux nombres en facteurs premiers :

$$220 = 2^2 \cdot 5 \cdot 11, \qquad 284 = 2^2 \cdot 71$$

On obtient donc :

$$\sigma(220) = \left(\frac{1-2^3}{1-2}\right)\left(\frac{1-5^2}{1-5}\right)\left(\frac{1-11^2}{1-11}\right) = 7 \cdot 6 \cdot 12 = 504$$

$$\sigma(284) = \left(\frac{1-2^3}{1-2}\right)\left(\frac{1-71^2}{1-71}\right) = 7 \cdot 72 = 504$$

De plus, on a que $220 + 284 = 504$. On obtient donc :

$$\sigma(220) = \sigma(284) = 220 + 284$$

Il s'agit donc bien de nombres amicaux.

3.9 Exercices

Exercice 3.9.1. Dans chacun des cas ci dessous, trouver le plus grand entier α qui satisfait la propriété :

1. $7^{\alpha}|100!$
2. $6^{\alpha}|200!$

Exercice 3.9.2. Calculer les valeurs ci dessous :

1. $\tau(1\ 225)$
2. $\tau(313\ 632)$
3. $\tau(432\ 575)$
4. $\tau(1\ 123\ 632)$

Exercice 3.9.3.

1. Quel est le plus petit nombre ayant exactement 20 diviseurs ?
2. Quel est le plus petit nombre ayant exactement 100 diviseurs ?

Exercice 3.9.4. Calculer les valeurs ci dessous :

1. $\sigma(1\ 000)$
2. $\sigma(14\ 625)$
3. $\sigma(36\ 936)$
4. $\sigma(4\ 159\ 375)$

Exercice 3.9.5. Trouver tous les nombres pour lesquels la somme de leurs diviseurs est exactement 183.

Exercice 3.9.6. Trouver tous les nombres n tels que :

1. $\tau(n) = 3$ et $\sigma(n) = 1407$
2. $\tau(n) = 4$ et $\sigma(n) = 252$
3. $\tau(n) = 5$ et $\sigma(n) = 2801$

Exercice 3.9.7. Identifier quelle fonction arithmétique est représentée par chacun des produits de Dirichlet suivants :

1. $1 * 1$
2. $1 * I$
3. $1 * \mu$
4. $1 * \phi$
5. $\tau * \mu$
6. $\sigma * \mu$
7. $\varepsilon * \mu$
8. $I * \mu$
9. $\phi * \varepsilon$

Exercice 3.9.8. Dans cette question, nous allons étudier certaines propriétés de la fonction Ω et de la fonction λ de Liouville. Si $n > 1$, et

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

est la décomposition de n en facteurs premiers, alors on définit $\Omega(n)$ comme étant :

$$\Omega(n) = \alpha_1 + \alpha_2 + ... + \alpha_k$$

et on définit $\lambda(n)$ comme étant :

$$\lambda(n) = (-1)^{\Omega(n)}$$

De plus, on définit $\lambda(1) = 1$ et $\Omega(1) = 0$.

1. Démontrer que la fonction Ω est une fonction additive. C'est à dire que si $m, n \geq 1$, $(m, n) = 1$, alors

$$\Omega(mn) = \Omega(m) + \Omega(n)$$

2. Démontrer que la fonction λ est multiplicative
3. Démontrer que la fonction

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

est aussi une fonction multiplicative

4. Démontrer que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 \text{ si n est un carré parfait} \\ 0 \text{ autrement} \end{cases}$$

5. Si g et λ sont les fonctions définies dans la question 5, démontrer que :

$$\lambda = \mu * g$$

Exercice 3.9.9. Évaluer les valeurs suivantes :

1. $\phi(1\ 000)$
2. $\phi(4\ 725)$
3. $\phi(47\ 432)$
4. $\phi(102\ 752)$

Exercice 3.9.10. Trouver tous les nombres naturels n tels que

$$\phi(n) = \frac{n}{2}$$

Exercice 3.9.11. Répondez aux questions suivantes :

1. Utilisez les inégalités de Tchebycheff pour trouver une borne inférieure et une borne supérieure pour $\pi(1000000)$.
2. Utilisez le théorème fondamental des nombres premiers pour donner une approximation de $\pi(1000000)$.

Pour vous aider à vérifier si vos réponses sembles correctes, notez que la valeur exacte est $\pi(1000000) = 78498$.

Exercice 3.9.12. Répondez aux deux questions suivantes :

1. Trouver quels sont les 4 premiers nombre premier de Mersenne. Si vous êtes courageux, vous pouvez aussi essayer de trouver le 5e.
2. Utiliser votre réponse à la question précédente pour trouver quels sont les 4 premiers nombre parfait (ou 5 si vous avez été courageux).

Exercice 3.9.13. Démontrer qu'un multiple strict d'un nombre parfait ou abondant est un nombre abondant.

Exercice 3.9.14. Démontrer que tous les diviseurs strict d'un nombre parfait ou déficient est un nombre déficient.

Exercice 3.9.15. Démontrer que si p est un nombre premier, alors p^{α} est un nombre déficient pour tout entier $\alpha \geq 1$.

Exercice 3.9.16. Supposons que p est un nombre premier impair qui n'est pas un nombre premier de Mersenne, et supposons que n est le plus grand entier tel que $2^n < p$. Démontrer que $2^n p$ est un nombre abondant.

Chapitre 4

Les équations diophantiennes

4.1 Introduction

Dans ce chapitre, nous sommes intéressé à étudier certaines équations diophantiennes. Nous avons déjà rencontrer quelques équations de ce type depuis le début du cours, mais nous allons en faire une étude plus approfondie dans ce chapitre.

Definition 4.1.1. Une équation est dite diophantienne s'il s'agit d'une équation algébrique pour laquelle on cherche des solutions entières.

La première chose à remarquer est que les techniques que vous avez appris dans votre étude d'algèbre classique au secondaire sont très différentes des méthodes nécessaires dans le cas des équations diophantiennes. De plus, les solutions peuvent être dans certains cas particulièrement curieuses. Voici un exemple que nous avons déjà rencontré au chapitre 2 sous une forme légèrement différente.

Exemple 4.1.1. Quelles sont les conditions nécessaires pour que l'équation suivante possèdent des solutions entières :

$$(n-1)! + 1 = nk$$

En regardant l'équation modulo n, on obtient :

$$(n-1)! + 1 = 0 \pmod{n} \qquad \Rightarrow \qquad (n-1)! = -1 \pmod{n}$$

Par le théorème de Wilson, on remarque donc que n doit être un nombre premier, et que pour chaque nombre premier, il existe un entier k qui satisfait l'équation. En particulier, si n est un nombre premier, alors on peut calculer k par l'équation :

$$k = \frac{(n-1)! + 1}{n}$$

Il existe beaucoup d'équations diophantiennes ayant été étudié. Parmi celles-ci, nous allons dans ce chapitre nous concentrer principalement sur deux types d'équations particulièrement importantes. Dans un premier temps, nous allons regarder l'équation linéaire. Si a, b et c sont des entiers, nous allons chercher l'ensemble de toutes les solutions (s'il y en a) à l'équation

$$ax + by = c$$

Nous allons ensuite étudier l'équation de Pythagore, c'est à dire que nous allons chercher l'ensemble des solutions entières à l'équation

$$x^2 + y^2 = z^2$$

Dans ce cas, il est facile de voir que $3^2 + 4^2 = 5^2$ est une solution, ainsi que tous les multiples de cette dernière, par exemple $6^2 + 8^2 = 10^2$. Par contre, trouver d'autres solutions est moins évident. Les outils que nous avons développés jusqu'à présent vont cependant nous permettre de trouver l'ensemble de toutes les solutions entières à cette équation.

Notre étude va ensuite nous amener à regarder une équation diophantienne très célèbre qui est en fait un généralisation de l'équation de Pythagore. Quelles sont les solutions entières à l'équation

$$x^n + y^n = z^n \ ?$$

Cette équation est l'un des problèmes les plus connus et des plus difficiles de la théorie des nombres. Il s'agit du grand théorème de Fermat. Ce dernier nous affirme qu'il n'y a aucune solution entière non triviale lorsque $n > 2$.

4.2 Les équations linéaires

Tel que mentionné dans l'introduction du chapitre, le premier type d'équations diophantiennes que nous allons étudier est l'équation linéaire $ax + by = c$ où a, b et c sont des constantes. On se rappelle que nous avons déjà rencontré un cas particulier de cette équation. Le cas ou $c = (a, b)$. C'est à dire que nous avons déjà vu comment trouver une solution à l'équation

$$ax + by = (a, b)$$

Dans ce cas, nous avons utilisé l'algorithme d'Euclide qui nous a permis de trouver une seule solution. Nous allons maintenant voir comment traiter le cas général.

Théorème 4.2.1. Si a, b, c sont des entiers, alors l'équation diophantienne

$$ax + by = c$$

possède des solutions entières si et seulement si

$$(a, b)|c$$

Dans ce cas, l'ensemble des solutions est donné par :

$$x = x_0 + \frac{bk}{(a, b)}, \qquad y = y_0 - \frac{ak}{(a, b)}, \qquad k \in \mathbb{Z}$$

où x_0, y_0 est une solution particulière de l'équation que l'on peut obtenir à partir de l'algorithme d'Euclide.

Démonstration. Premièrement, comme nous avons vu au chapitre 1 que l'ensemble $\{ax + by : x, y \in \mathbb{Z}\}$ est l'ensemble de tous les multiple de $d = (a, b)$, alors l'équation $ax + by = c$ a une solution si et seulement si $(a, b)|c$. Nous allons donc supposer que l'équation a au moins une solution, c'est à dire que $d = (a, b)$ divise c. Supposons, pour commencer, que $d = 1$. En prenant l'équation modulo $|b|$, on obtient donc :

$$ax = c \pmod{|b|} \qquad \text{avec } (a, |b|) = 1$$

D'après le chapitre 2, cette dernière équation n'a qu'une seule solution en modulo, disons x_0. L'ensemble des x qui satisfont l'équation originale sera donc de la forme :

$$x = x_0 + kb, \quad b \in \mathbb{Z}$$

Maintenant, en remplaçant ce x dans l'équation originale, on obtient :

$$a(x_0 + kb) + by = c \Longrightarrow ax_0 + abk + by = c \Longrightarrow by = c - ax_0 - abk \Longrightarrow y = \frac{c - ax_0}{b} - ak$$

Donc si on pose $y_0 = \dfrac{c - ax_0}{b}$ qui est la valeur de y qui satisfait l'équation correspondant à x_0, alors on obtient que l'ensemble des solutions est de la forme :

$$\begin{cases} x = x_0 + bk \\ y = y_0 - ak \end{cases}$$

où x_0, y_0 est une solution particulière.

Supposons maintenant que $d = (a, b)$ est un entier quelconque, alors on peut diviser l'équation originale par d, ce qui nous donne :

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

avec $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$. Donc on peut appliquer la première partie, qui nous donne que l'ensemble des solutions est de la forme

$$\begin{cases} x = x_0 + \dfrac{b}{d}k \\ \\ y = y_0 - \dfrac{a}{d}k \end{cases} \qquad k \in \mathbb{Z}$$

□

Exemple 4.2.1. On veut trouver l'ensemble des entiers (s'il y en a) qui satisfont l'équation suivante :

$$440x + 700y = 120$$

Pour ce faire, on va commencer par calculer $(440, 700)$:

$$\begin{aligned} 700 &= 1(440) + 260 \\ 440 &= 1(260) + 180 \\ 260 &= 1(180) + 80 \\ 180 &= 2(80) + 20 \\ 80 &= 4(20) + 0 \end{aligned}$$

On a donc $(440, 700) = 20$. Comme $20|120$, l'équation admet donc des solutions. On va commencer par diviser l'équation par 20 pour obtenir une équation équivalente qui sera un peu plus simple à résoudre. On obtient donc l'équation :

$$22x + 35y = 6$$

Comme $(22, 35) = 1$, on va commencer par appliquer l'algorithme d'Euclide pour trouver une solution à l'équation $22x + 35y = 1$, puis on va multiplier notre solution par 6 pour obtenir une solution de l'équation originale.

$$\begin{aligned} 35 &= 1(22) + 13 \\ 22 &= 1(13) + 9 \\ 13 &= 1(9) + 4 \\ 9 &= 2(4) + 1 \\ 4 &= 4(1) + 0 \end{aligned}$$

En réécrivant l'algorithme à l'envers, on obtient donc :

$$\begin{aligned} 1 &= 9 - 2(4) \\ &= 9 - 2[13 - 1(9)] \\ &= 3(9) - 2(13) \\ &= 3[22 - 1(13)] - 2(13) \\ &= 3(22) - 5(13) \\ &= 3(22) - 5[35 - 1(22)] \\ &= 8(22) - 5(35) \end{aligned}$$

Donc une solution de l'équation originale est donnée par $x_0 = 8 \cdot 6 = 48$ et $y_0 = -5 \cdot 6 = -30$. Donc l'ensemble des solutions est :

$$x = 48 + 35k, \qquad y = -30 - 22k, \qquad k \in \mathbb{Z}$$

4.3 L'équation pythagoricienne

Dans cette section, nous voulons trouver l'ensemble de toutes les solutions entières de l'équations pythagore

$$x^2 + y^2 = z^2$$

Pour ce faire, nous allons caractériser l'ensemble de toutes les solutions primitives.

Definition 4.3.1. Une solution primitive de l'équation pythagoricienne est une solution telle que $(x, y, z) = 1$.

Nous connaissons tous le triplet pythagoricien $3, 4, 5$ qui est la solution primitive la plus simple de l'équation pythagoricienne. Nous aimerions maintenant trouver quelles sont les autres. Pour ce faire, nous allons trouver plusieurs propriétés des triplets pythagoriciens que nous appellerons lemme, et qui vont culminer à la fin de cette section par un théorème qui va caractériser tous les triplets pythagoriciens.

Lemme 4.3.1. *Si x, y, z est une solution primitive, alors $(x, y) = (x, z) = (y, z) = 1$.*

Démonstration. Supposons $(x, y) = d$, alors $x = dm$ et $y = dn$. Donc

$$z^2 = x^2 + y^2 = (dm)^2 + (dn)^2 = d^2(m^2 + n^2)$$

On obtient donc que $d^2 | z^2$, et donc $d | z$. On en déduit donc que $1 = (x, y, z) \geq d$. Donc $d = 1$.

Supposons maintenant que $(x, z) = d$, alors $x = dm$ et $z = dn$. Donc

$$y^2 = z^2 - x^2 = (dn)^2 - (dm)^2 = d^2(n^2 - m^2)$$

On obtient donc que $d^2 | y^2$, et donc $d | y$. On en déduit donc que $1 = (x, y, z) \geq d$. Donc $d = 1$.

La démonstration que $(y, z) = 1$ se fait de la même façon et est laissée en exercice. □

Lemme 4.3.2. *Si x, y, z est une solution primitive, alors z est impair, et x, y sont de parité opposée (l'un est pair, l'autre est impair).*

Démonstration. Supposons premièrement que x, y sont tous deux pairs. Donc $x = 2m$ et $y = 2n$. On obtient donc :

$$z^2 = x^2 + y^2 = 4m^2 + 4n^2 = 2^2(m^2 + n^2)$$

Donc $2^2 | z^2$ et donc $2 | z$, ce qui contredit l'hypothèse qu'il s'agit d'une solution primitive. x, y ne peuvent donc pas être tous deux pairs.

Supposons maintenant que x, y sont tous deux impairs. Donc $x = 2m + 1$ et $y = 2n + 1$, ce qui nous donne :

$$z^2 = x^2 + y^2 = 4(m^2 + m + n^2 + n) + 2$$

On obtient donc que $z^2 = 2 \pmod 4$, et en particulier z doit aussi être pair. D'un autre côté, si z est pair, alors $z = 2k$. Donc $z^2 = 4k^2$, et donc $z^2 = 0 \pmod 4$, ce qui est une contradiction. Donc x, y ne peuvent pas être tous deux impairs.

On peut donc conclure que si x, y, z est une solution primitive, alors x, y doivent être de parité opposée (l'un est pair, l'autre est impair). De plus, z doit obligatoirement être impair, car la somme d'un nombre pair avec un nombre impair est toujours un nombre impair. □

Lemme 4.3.3. *Si x, y, z est une solution primitive tel que x est impair, alors*

$$(z + x, z - x) = 2$$

Démonstration. Premièrement, comme x et z sont tous deux impairs, leur somme et leur différence doivent être paires. Donc $2|(z+x)$ et $2|(z-x)$. Il s'en suit donc que $2|(z+x, z-x)$. Maintenant, supposons que $d = (z+x, z-x)$, donc $d|(z+x)$ et $d|(z-x)$, et donc

$$d|[(z+x)+(z-x)] \Rightarrow d|(2z)$$

$$d|[(z+x)-(z-x)] \Rightarrow d|(2x)$$

Il s'en suit que $d|2$. Comme $2|d$ et $d|2$, on obtient finalement que $d = 2$. □

Lemme 4.3.4. *Supposons que m, n, z sont des entiers tels que*

$$(m,n) = 1 \text{ et } mn = z^n$$

alors il existe des entiers r, s tels que

$$m = r^n \text{ et } n = s^n$$

Démonstration. En utilisant le théorème fondamental de l'arithmétique, on peut décomposer z en facteurs premiers. On a donc :

$$z = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$$

Ce qui nous donne :

$$mn = z^n = p_1^{n\alpha_1} p_2^{n\alpha_2} ... p_k^{n\alpha_k}$$

Maintenant, comme $(m,n) = 1$, alors chacun des $p_i^{n\alpha_i}$ est un diviseur de m ou un diviseur de n (mais pas des deux). On peut obtient donc que :

$$m = p_1^{n\alpha_1} p_2^{n\alpha_2} ... p_j^{n\alpha_j} \text{ et } n = p_{j+1}^{n\alpha_{j+1}} p_{j+2}^{n\alpha_{j+2}} ... p_k^{n\alpha_k}$$

Ce qui nous donne finalement :

$$\begin{aligned} m &= r^n = (p_1^{\alpha_1} p_2^{\alpha_2} ... p_j^{\alpha_j})^n \\ n &= s^n = (p_{j+1}^{\alpha_{j+1}} p_{j+2}^{\alpha_{j+2}} ... p_k^{\alpha_k})^n \end{aligned}$$

□

Théorème 4.3.1. À l'ordre près des termes x, y, les solutions primitives de l'équation $x^2 + y^2 = z^2$ sont donné par :

$$\begin{cases} x = r^2 - s^2 \\ y = 2rs \\ z = r^2 + s^2 \end{cases}, \qquad r, s \in \mathbb{Z}$$

où r et s sont de parités différentes (l'un est pair et l'autre impair), $(r,s) = 1$ et $r > s > 0$.

Démonstration. Supposons que x est impair. Comme $(z+x, z-x) = 2$, on a donc que $2|(z+x)$ et $2|(z-x)$. Il existe donc des entiers u et v tels que :

$$z + x = 2u \text{ et } z - x = 2v$$

En additionnant et soustrayant ces deux équations, on obtient donc :

$$z = u + v \text{ et } x = u - v$$

En utilisant l'équation de Pythagore, on peut maintenant calculer la valeur de y :

$$y^2 = z^2 - x^2 = (z+x)(z-x) = (2u)(2v) = 4uv$$

ce qui nous donne en réarrangeant les termes que :

$$\left(\frac{y}{2}\right)^2 = uv$$

par le lemme précédent, il existe donc des entiers r, s tels que $r^2 = u$ et $s^2 = v$, ce qui nous donne :

$$\begin{cases} x = r^2 - s^2 \\ y = 2rs \\ z = r^2 + s^2 \end{cases}, \qquad r, s \in \mathbb{Z}$$

Maintenant, comme x est impair par hypothèse, alors r et s doivent être de parités opposées. De plus, comme $(z - x, z + x) = 2$, alors

$$\left(\frac{z-x}{2}, \frac{z+x}{2}\right) = (v, u) = 1$$

De plus, comme $v = s^2$ et $u = r^2$, on obtient donc $(r, s) = 1$. Finalement, pour compléter la démonstration, il ne nous reste plus qu'à démontrer que tous les x, y, z de cette forme sont des solutions primitives de l'équation Pythagoricienne. Supposons que $(r, s) = 1$ avec r et s de parités opposées. Il est facile de voir que dans ce cas, $x^2 + y^2 = z^2$, et donc il s'agit d'une solution de l'équation. De plus, on a :

$$(r, s) = 1 \Rightarrow (u, v) = 1 \Rightarrow \left(\frac{z-x}{2}, \frac{z+x}{2}\right) = 1 \Rightarrow (z - x, z + x) = 2$$

Posons $(x, z) = d$. Donc $d|x$ et $d|z$ ce qui implique que $d|(z-x)$ et $d|(z+x)$. Ce qui nous donne $d|(z-x, z+x) \Rightarrow d|2$. On a donc que $d = 1$ ou $d = 2$. Comme r et s sont de parité opposée, alors x est impair, donc $2 \nmid x$. On obtient donc finalement que $d = 1$, ou en d'autres termes $(x, z) = 1$. On a donc que $x^2 + y^2 = z^2$ est une solution primitive de l'équation Pythagoricienne. □

Exemple 4.3.1. On veut trouver une solution primitive de l'équation $x^2 + y^2 = z^2$ pour laquelle $z = 113$. Pour ce faire, nous pourrions commencer par calculer $z^2 = 12769$ et chercher à décomposer ce dernier comme une somme de carrés, ce qui risquerait d'être un peu long. Nous allons donc utiliser une approche différente en utilisant le théorème précédent. Pour ce faire, plutôt que de décomposer $z^2 = 12769$ comme une somme de deux carrés, nous allons plutôt décomposer directement le nombre $z = 113$ en une somme de deux carrés.

$$\begin{aligned} 113 - 1^2 &= 112 \text{ n'est pas un carré parfait} \\ 113 - 2^2 &= 109 \text{ n'est pas un carré parfait} \\ 113 - 3^2 &= 104 \text{ n'est pas un carré parfait} \\ 113 - 4^2 &= 97 \text{ n'est pas un carré parfait} \\ 113 - 5^2 &= 88 \text{ n'est pas un carré parfait} \\ 113 - 6^2 &= 77 \text{ n'est pas un carré parfait} \\ 113 - 7^2 &= 64 = 8^2 \end{aligned}$$

Comme $8^2 + 7^2 = 113$, 8 et 7 sont de parités différentes et $(8, 7) = 1$, on peut donc prendre $r = 8$ et $s = 7$ dans le théorème ce qui nous donne :

$$\begin{cases} x = 15 \\ y = 112 \\ z = 113 \end{cases}$$

On peut ensuite vérifier que $15^2 + 112^2 = 113^2$ comme souhaité.

Exemple 4.3.2. On veut trouver toutes les solutions primitives de l'équation $x^2 + y^2 = z^2$ pour lesquelles $y = 140$. Pour ce faire, remarquons que $140 = 2^2 \cdot 5 \cdot 7$. On doit donc trouver des nombres r et s tels que $rs = 70$. Pour ce faire, on a les options suivantes :

$$\begin{aligned} 35 \times 2 &= 70 \\ 14 \times 5 &= 70 \\ 10 \times 7 &= 70 \end{aligned}$$

Remarquez que dans chacun des cas, les nombres sont de parités différentes et leur PGCD est toujours 1, ce qui nous garantie que les solutions que nous allons obtenir seront bien des solutions primitives. On a donc les solutions suivantes :

1. Si $r = 35$ et $s = 2$, alors $x = 35^2 - 2^2 = 1221$, $y = 2 \cdot 35 \cdot 2 = 140$ et $z = 35^2 + 2^2 = 1229$. On obtient donc la solution
$$1221^2 + 140^2 = 1229^2$$
2. Si $r = 14$ et $s = 5$, alors $x = 14^2 - 5^2 = 171$, $y = 2 \cdot 14 \cdot 5 = 140$ et $z = 14^2 + 5^2 = 221$. On obtient donc la solution
$$171^2 + 140^2 = 221^2$$
3. Si $r = 10$ et $s = 7$, alors $x = 10^2 - 7^2 = 51$, $y = 2 \cdot 10 \cdot 7 = 140$ et $z = 10^2 + 7^2 = 149$. On obtient donc la solution
$$51^2 + 140^2 = 149^2$$

Il y a donc un total de 3 solutions primitives possibles.

4.4 La méthode de descente infinie de Fermat

Jusqu'à présent, nous nous sommes concentrés sur deux équations diophantiennes pour lesquels il est possible, du moins sous certaines conditions, de trouver des solutions. Il s'agit de l'équation linéaire et pythagoricienne. Nous allons maintenant regarder une méthode particulièrement ingénieuse et popularisée par Fermat : La méthode de descente infinie. Il s'agit d'une méthode qui dans plusieurs cas peut nous permettre de démontrer qu'une équation diophantienne ne possède pas de solution.

L'idée est relativement simple. On commence par supposer que l'équation possède une solution avec des nombres naturels, puis on démontre que dans ce cas, on peut construire une autre solution qui est plus petite. Cette nouvelle solution aura donc encore une fois une solution qui est encore plus petite, et ainsi de suite. On obtient donc une infinité de solutions, ce qui est une contradiction. En effet, il existe seulement un nombre fini de nombres naturels inférieurs à un nombre donné. On peut alors conclure qu'il ne peut pas y avoir de solution.

Alternativement, on peut voir la méthode de descente infinie comme étant une application du principe du bon ordre, combiner avec une démonstration par contradiction. Si on suppose qu'une solution existe, le principe du bon ordre affirme qu'il existe une plus petite solution. Si à partir de cette solution on peut en construire une autre qui est encore plus petite, on obtient alors une contradiction et on peut affirmer que l'équation diophantienne n'admet aucune solution.

Nous allons maintenant regarder un exemple relativement simple d'application de la méthode de descente infinie.

Exemple 4.4.1. On veut montrer que l'équation diophantienne $x^2 = 2y^2$ ne possède aucune solution (où x et y sont des nombres entiers). Pour ce faire, supposons au contraire qu'il existe des nombres naturels x_0, y_0 tel que $x_0^2 = 2y_0^2$, alors x_0^2 doit être un nombre pair. Par le lemme d'Euclide, si $2|x_0^2$, alors $2|x_0$, c'est à dire que x_0 est un nombre pair. Il existe donc un nombre naturel k tel que $x_0 = 2k$. En revenant à l'équation de départ, on a donc que $x_0^2 = 2y_0^2$ devient $4k^2 = 2y_0^2$, qui peut être simplifier comme étant $2k^2 = y_0^2$. En applicant à nouveau la même méthode, on peut donc affirmer que y_0 est aussi pair, et donc il existe un nombre naturel m tel que $y_0 = 2m$. En revenant à nouveau à notre équation, on obtient donc que l'équation $2k^2 = y_0^2$ devient $2k^2 = 4m^2$, qui en simplifiant devient $k^2 = 2m^2$. Maintenant, en remarquant que $k < x_0$ et $m < y_0$, on a donc obtenue une équation ayant des coefficients plus petits que notre première solution. En répétant la même procédé, on peut donc obtenir une infinité de solutions ayant chacune des coefficients en nombres naturels, et plus petite l'une que l'autre. On a donc obtenue une contradiction, car il ne peut y avoir plus qu'un nombre fini de solutions en nombres naturels plus petite qu'une équation donné. L'équation diophantienne ne possède donc aucune solution en nombres naturels.

Pour compléter notre démonstration, il faut maintenant traiter le cas des nombres entier négatif. Supposons qu'il existe des nombres entiers x_1, y_1 pour lesquels $x_1^2 = 2y_1^2$. Alors on obtient que $|x_1|^2 = 2|y_1|^2$ est aussi une solution, mais cette fois $|x_1|$ et $|y_1|$ sont des nombres naturels. Comme nous avons montré plus tôt qu'il n'y a aucune solution en nombres naturels, il ne peut donc pas y avoir de solution entière.

Remarquez que le résultat que nous venons de démontrer est en fait très semblable à la démonstration que $\sqrt{2}$ n'est pas un nombre rationnel. Dans ce cas, on suppose qu'il existe des entiers p, q tels que $\sqrt{2} = \frac{p}{q}$. En élevant le tout au carré, et en ramenant le p^2 du côté gauche on obtient la même équation que précédemment. Comme nous savons que cette équation ne possède aucune solution entière, on peut donc conclure que $\sqrt{2}$ n'est pas un nombre rationnel.

4.5 Le grand théorème de Fermat

L'équation de Pythagore $x^2 + y^2 = z^2$ que nous avons étudiée dans la section précédente nous amène à nous poser la question de l'existance de solutions entières à l'équation

$$x^n + y^n = z^n$$

pour n strictement plus grand que 2. Ce problème porte le nom de grand théorème de Fermat (aussi appelé dernier théorème de Fermat, ou bien théorème de Fermat-Wiles). Ce théorème a été énoncé pour la première fois par Pierre de Fermat qui l'énonça dans la marge d'un livre (une traduction de l'arithmétique de Diophante) avec le commentaire suivant :

> « ... J'ai trouvé une merveilleuse démonstration de cette proposition. Mais la marge est trop étroite pour la contenir. »

Depuis ce temps, le problème porte le nom de théorème. Fermat ne laissa cependant aucune trace de sa démonstration, et la recherche d'une telle démonstration s'avéra l'un des problèmes les plus difficiles des mathématiques. En 1993, Andrew Wiles en fit une première démonstration lors d'une conférence de 3 jours. Le théorème de Fermat est alors un corollaire de ses résultats. Le secret avait été gardé sur l'importance de la conférence et des recherches de Wiles. Dans les mois qui suivirent, on découvrit cependant une faille importante dans la démonstration, et ce n'est finalement qu'en 1995 que Wiles publia une preuve correcte, c'est à dire environ 350 ans après que Fermat eut énoncé le problème. La preuve de Wiles fait plus de 100 pages et pris près de 7 ans d'effort de la part de Wiles. Aujourd'hui, la question de savoir si Fermat avait vraiment trouvé une démonstration de son théorème reste ouverte, bien que la plupart des mathématiciens croient que sa preuve était probablement incorrecte.

Théorème 4.5.1. **(Grand théorème de Fermat)** Il n'existe aucune solution entière à l'équation

$$x^n + y^n = z^n$$

où $n > 2$ et $xyz \neq 0$.

La démonstration du théorème étant particulièrement compliquée, nous ne la présenterons pas ici. Nous allons cependant démontrer le théorème dans le cas où $n = 4$. Ce résultat sera une conséquence du théorème ci dessous :

Théorème 4.5.2. Il n'existe aucun solution entière à l'équation

$$x^4 + y^4 = z^2$$

avec $xyz \neq 0$.

Démonstration. Supposons au contraire qu'il existe des entiers x, y, z tels que $x^4 + y^4 = z^2$ et $xyz \neq 0$, alors il existe une solution pour laquelle z est minimale. Nous allons donc supposer que x, y, z est cette solution. Remarquons que dans ce cas, nous obtenons aussi une solution de l'équation Pythagoricienne car

$$(x^2)^2 + (y^2)^2 = z^2$$

Cette solution est obligatoirement une solution primitive de l'équation autrement cela contredirait la minimalisé de z. En utilisant le théorème de la section précédente, il existe donc des entiers r et s tels que :

$$\begin{cases} x^2 = r^2 - s^2 \\ y^2 = 2rs \\ z^2 = r^2 + s^2 \end{cases}$$

où r et s sont de parités différentes et $(r, s) = 1$. Nous allons maintenant montrer que s doit être pair. Pour ce faire, supposons au contraire que s est impair. Dans ce cas, r soit être pair, on obtient donc que

$$x^2 = r^2 - s^2 = -s^2 \pmod 4$$

Comme le carré d'un nombre impair est toujours congru à 1 modulo 4, on obtient donc une contradiction : $1 = -1 \pmod 4$. On peut donc supposer que s est pair et r est impair. Maintenant, remarquons que :

$$s^2 + x^2 = s^2 + (r^2 - s^2) = r^2$$

Donc (s, x, r) forme un triplet Pythagoricien. Il s'agit d'une solution primitive, car $(r, s) = 1$. Donc on peut à nouveau appliquer le théorème de la section précédente. Il existe donc des entiers a et b de parités différentes tels que $(a, b) = 1$ et :

$$\begin{cases} x = a^2 - b^2 \\ s = 2ab \\ r = a^2 + b^2 \end{cases}$$

Remarquez que nous avons ici utilisé le fait que s est pair. On a donc que :

$$y^2 = 2rs = 2(a^2 + b^2)(2ab) = 4ab(a^2 + b^2)$$

On veut montrer que a, b et a^2+b^2 sont tous des carrés parfaits. Pour ce faire, on doit montrer que $(a, a^2+b^2) = (b, a^2 + b^2) = 1$. Supposons que $d = (a, a^2 + b^2)$ avec $d > 1$. Il existe donc un nombre premier p tel que $p|a$ et $p|(a^2+b^2)$. Il existe donc des entiers k et l tels que : $kp = a$ et $lp = a^2+b^2$. Donc $b^2 = lp-a^2 = lp-k^2p^2 = p(l-k^2p)$. On a donc que $p|b^2$ et comme p est premier on a $p|b$, ce qui contredit le fait que $(a, b) = 1$. Donc aucun nombre premier p ne peut diviser d. On peut donc conclure que $d = 1$. On a donc $(a, a^2+b^2) = 1$. De la même manière, on peut montrer que $(b, a^2 + b^2) = 1$. On en déduit donc que $(a, b, a^2 + b^2) = 1$ ce qui nous permet d'obtenir que a, b et $a^2 + b^2$ sont tous des carrés parfaits. Il existe donc des entiers u, v, w tels que :

$$\begin{cases} a = u^2 \\ b = v^2 \\ a^2 + b^2 = w^2 \end{cases}$$

On obtient donc que :

$$u^4 + v^4 = a^2 + b^2 = w^2$$

On a donc que u, v, w est aussi une solution de l'équation $x^4 + y^4 = z^2$. De plus, nous avons que :

$$w^2 = a^2 + b^2 = r < r^2 + s^2 = z^2$$

Remarquez qu'ici nous avons utilisé l'hypothèse que $xyz \neq 0$ et donc que $rs \neq 0$. On obtient donc que $w < z$ ce qui contredit la minimalité de la solution x, y, z. On peut donc conclure qu'il n'y a aucune solution entière non nulle à l'équation $x^4 + y^4 = z^2$. □

On peut maintenant utiliser le résultat ci-dessus pour démontrer que l'équation

$$x^4 + y^4 = z^4$$

n'a pas de solution entière si $xyz \neq 0$. Ceci est laissé en exercice.

4.6 Le théorème des deux carrés de Fermat

Un peu plus tôt dans le chapitre, nous avons vu que ci x, y, z est une solution primitive de l'équation $x^2 + y^2 = z^2$, alors il existe des entiers r, s tels que r et s sont de parités différentes, $(r, s) = 1$ pour lesquels $z = r^2 + s^2$. Nous allons maintenant nous intéresser à savoir quel entier z peut s'écrire sous la forme d'une somme de deux carrés. Nous allons commencer par nous intéresser au cas ou z est un nombre premier impair.

Théorème 4.6.1. (Théorème des deux carrés de Fermat pour les nombres premiers) Un nombre premier impair peut s'écrire sous la forme

$$p = x^2 + y^2$$

où x et y sont des entiers si et seulement si

$$p = 1 \pmod 4$$

Démonstration. Commençons par démontrer $\Rightarrow$. Prenons p un nombre premier impair et supposons que $p = x^2 + y^2$, où x, y sont des entiers. Alors, x et y doivent être de parité opposée (autrement $x^2 + y^2$ serait un nombre pair). Sans perte de généralité, supposons que x est pair, et y est impair. Il existe donc des entiers m et n tels que $x = 2m$ et $y = 2n + 1$. On a donc :

$$p = x^2 + y^2 = (2m)^2 + (2n+1)^2 = 4m^2 + 4n^2 + 4n + 1 = 4(m^2 + n^2 + n) + 1$$

En calculant le tout modulo 4, on obtient donc :

$$p = 4(m^2 + n^2 + n) + 1 = 1 \pmod 4$$

La condition est donc belle et bien nécessaire. Nous allons maintenant démontrer $\Leftarrow$. Nous allons faire cette partie de la démonstration en 5 étapes :

1. Supposons que p et n sont des entiers qui peuvent s'écrire comme une somme de deux carrés telle que $p|n$ et p est un nombre premier. Alors il existe des entiers a, b, c, d tels que

$$\begin{cases} p = a^2 + b^2 \\ n = c^2 + d^2 \end{cases}$$

Comme $p|n$, alors

$$p \Big| \Big(a^2(p^2 + q^2) - p^2(a^2 + b^2) \Big)$$

Maintenant, on remarque que :

$$\begin{aligned} a^2(c^2 + d^2) - c^2(a^2 + b^2) &= a^2c^2 + a^2d^2 - a^2c^2 - b^2d^2 \\ &= a^2d^2 - b^2c^2 \\ &= (aq + bp)(aq - bp) \end{aligned}$$

On obtient donc que :

$$p \Big| \Big((ad - bc)(ad + bc) \Big)$$

Comme p est un nombre premier, alors on a :

$$p|(ad - bc) \text{ ou } p|(ad + bc)$$

On aura donc deux cas à traiter. Remarquons premièrement que :

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (a^2c^2 + 2abcd + b^2d^2) + (b^2c^2 - 2abcd + a^2d^2) \\ &= (ac + bd)^2 + (bc - ad)^2 \\ &= (ac + bd)^2 + (ad - bc)^2 \end{aligned}$$

Donc si $p|(ad-bc)$, alors $p|(ac+bd)$. Dans ce cas, on obtient donc :

$$\frac{a^2+b^2}{c^2+d^2} = \left(\frac{ac+db}{c^2+d^2}\right)^2 + \left(\frac{ad-bc}{c^2+d^2}\right)^2$$

donc $\frac{n}{p}$ est donc une somme de deux carrés. Supposons maintenant que $p|(ad+bc)$, alors on remarque que :

$$\begin{aligned}(a^2+b^2)(c^2+d^2) &= a^2c^2+a^2d^2+b^2c^2+b^2d^2\\ &= (a^2c^2-2abcd+b^2d^2)+(b^2c^2+2abcd+a^2d^2)\\ &= (ac-bd)^2+(bc+ad)^2\\ &= (ac-bd)^2+(ad+bc)^2\end{aligned}$$

Donc si $p|(ad+bc)$ alors $p|(ac-bd)$. On obtient donc :

$$\frac{a^2+b^2}{c^2+d^2} = \left(\frac{ac-bd}{c^2+d^2}\right)^2 + \left(\frac{ad+bc}{c^2+d^2}\right)^2$$

Donc dans ce cas, on obtient encore une fois que $\frac{n}{p}$ est la somme de deux carrés. On peut donc conclure que si n et p sont des entiers qui peuvent s'écrire comme somme de deux carrés et si $p|n$ et p est un nombre premier, alors $\frac{n}{p}$ est aussi la somme de deux carrés.

2. Supposons que m et n sont des entiers tels que $m|n$, n est la somme de deux carrés, mais m n'est pas la somme de deux carrés. Posons $\frac{n}{m} = y$, et on décompose y en facteurs premiers, disons $y = p_1p_2p_3...p_k$. On obtient donc :

$$n = mp_1p_2p_3...p_k$$

Supposons que tous les facteurs p_i sont la somme de deux carrés, alors en utilisant la partie précédente on a que :

$$\frac{n}{p_k} = mp_1p_2...p_{k-1}$$

est la somme de deux carrés. En répétant la même opération, on obtient donc que :

$$\frac{n}{p_{k-1}p_k} = mp_1p_2...p_{k-2}$$

est aussi la somme de deux carrés. En continuant de la même manière, on obtient donc finalement que :

$$\frac{n}{p_1p_2...p_k} = m$$

est la somme de deux carrés, ce qui est une contradiction. On peut donc conclure que si m et n sont des entiers tels que $m|n$ et tels que n est la somme de deux carrés, mais m ne l'est pas, alors $\frac{n}{m}$ contient un facteur premier qui n'est pas la somme de deux carrés.

3. Supposons maintenant que a et b sont des entiers tels que $(a,b) = 1$ et pour lesquels il existe un entier x, $x|(a^2+b^2)$ qui n'est pas la somme de deux entiers. En modifiant légèrement la division Euclidienne que nous avons vu au chapitre 1, on peut donc trouver des entiers m,n,c,d tels que :

$$\begin{cases} a = mx \pm c \\ b = nx \pm d \end{cases}$$

avec

$$c,d \leq \frac{x}{2}$$

On obtient donc :

$$a^2+b^2 = m^2x^2 \pm 2cmx + c^2 + n^2x^2 \pm 2dnx + d^2 = Ax + (c^2+d^2)$$

où $A = m^2x \pm 2cm + n^2x \pm 2dn$. Comme $x|(a^2+b^2)$, on obtient donc que $x|(c^2+d^2)$. Il existe donc un entier y tel que

$$xy = c^2 + d^2$$

Supposons maintenant que qu'il existe un nombre premier $p|(c,d)$, alors $p|(c^2+d^2)$, alors $p|x$ ou $p|y$. On remarque cependant que p ne peut pas diviser x, car autrement p diviserait a et b (car $a = mx \pm c, b = nx \pm d$), ce qui est impossible car $(a,b) = 1$. Donc $p|y$. Donc si $(c,d) \neq 1$, alors $(c,d)|y$. Ce qui nous donne :

$$x\left(\frac{y}{(c,d)^2}\right) = \left(\frac{c}{(c,d)}\right)^2 + \left(\frac{d}{(c,d)}\right)^2$$

On va donc poser $e = \dfrac{c}{(c,d)}$ et $f = \dfrac{d}{(c,d)}$. On obtient donc que :

$$x|(e^2+f^2)$$

Il existe donc un entier z tel que :

$$xz = e^2 + f^2$$

Maintenant, on remarque que :

$$xz = e^2 + f^2 \leq c^2 + d^2 \leq \left(\frac{x}{2}\right)^2 + \left(\frac{x}{2}\right)^2 \leq \frac{1}{2}x^2$$

Donc $z \leq \dfrac{1}{2}x$. Finalement, comme x est un facteur de e^2+f^2 qui n'est pas la somme de deux carrés, alors par la partie précédente $\dfrac{e^2+f^2}{x} = z$ contient un facteur qui n'est pas la somme de deux carrés. Appelons ce facteur de z par la lettre w. Ce dernier est donc encore une fois nécessairement inférieur à $\dfrac{1}{2}x$.

4. Supposons que que a, b sont des entiers tels que $(a,b) = 1$, et supposons qu'il existe un entier x tel que $x|(a^2+b^2)$ et x ne peut pas s'écrire comme somme de deux carrés. Alors par la partie précédente, on peut donc trouver des entiers c, d, w tels que $(c,d) = 1$, $w|(c^2+d^2)$, w n'est pas la somme de deux carrés et $w \leq \dfrac{x}{2}$. Posons $x_2 = w$, $a_2 = c$ et $b_2 = d$. En répétant la même étape à répétition, on peut donc obtenir des suites $\{x_i\}, \{a_i\}$ et $\{b_i\}$. À chaque étape $x_{i+1} \leq \dfrac{1}{2}x_i$. Éventuellement, ces x_i devront donc être inférieurs à 1 ce qui est impossible. L'hypothèse de départ doit donc être fausse. x est la somme de deux carrés. On a donc que si a, b sont des entiers tels que $(a,b) = 1$, alors tous les facteurs de a^2+b^2 sont la somme de deux carrés.
5. Supposons que p est un nombre premier de la forme $p = 4n+1$. Alors par le petit théorème de Fermat, on a que :

$$1^{4n}, 2^{4n}, 3^{4n}, 4^{4n}, ..., (4n)^{4n}$$

sont tous congrus à 1 modulo p. On a donc que :

$$2^{4n} - 1^{4n}, 3^{4n} - 2^{4n}, 4^{4n} - 3^{4n}, ...(4n)^{4n} - (4n-1)^{4n}$$

sont tous divisibles par p (car il sont congrus à 0 modulo p). Maintenant, remarquons que chacune des expressions ci-dessus peuvent être factorisées sous la forme :

$$k^{4n} - (k-1)^{4n} = (k^{2n} + (k-1)^{2n})(k^{2n} - (k-1)^{2n})$$

Pour chaque $k \in \{1, ...4n\}$, comme $p|(k^{4n} - (k-1)^{4n})$, alors $p|(k^{2n} - (k-1)^{2n})$ ou $p|(k^{2n} + (k-1)^{2n})$. Supposons que pour au moins un k on a que $p|(k^{2n} + (k-1)^{2n})$, alors p divise une somme de deux carrés, et donc par la partie précédente on a que p est lui-même une somme de deux carrés. Si au contraire $p|(k^{2n} - (k-1)^{2n})$ pour tout k, alors on a que les $2n$-différences finies de

$$1^{2n}, 2^{2n}, 3^{2n}, 4^{2n}, ..., (4n)^{2n}$$

sont toutes égales à $(2n)!$ (Voir le théorème des différences finies en annexe). De plus, comme à partir de la première différence finie ces dernières sont divisibles par p, alors on a que

$$p|(2n)!$$

ce qui est une contradiction. Donc nous sommes dans le cas où $p|(k^{2n}+(k-1)^{2n})$ pour au moins un k, et donc que p est une somme de deux carrés.

□

Théorème 4.6.2. **(Théorème des deux carrés de Fermat cas général)** Un nombre naturel n peut s'écrire sous la forme

$$n = x^2 + y^2$$

où x, y sont des entiers si et seulement si chaque facteur premier de la forme $4k+3$ intervient à une puissance paire.

Démonstration. Premièrement, on va montrer que si a et b sont deux nombres naturels qui peuvent s'écrire comme une somme de deux carrés, alors le produit ab peut aussi s'écrire comme un somme de deux carrés. Pour ce faire, supposons que

$$a = x^2 + y^2 \quad \text{et} \quad b = z^2 + w^2$$

alors on a :

$$\begin{aligned} ab &= (x^2+y^2)(z^2+w^2) \\ &= x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 \\ &= (x^2z^2 + y^2w^2) + (x^2w^2 + y^2z^2) \\ &= (xz+yw)^2 - 2xyzw + (xw-yz)^2 + 2xyzw \\ &= (xz+yw)^2 + (xw-yz)^2 \end{aligned}$$

Donc ab peut aussi s'écrire comme un somme de deux carrés. Maintenant, notons que si $n = 0$ ou $n = 1$ alors le résultat est trivial. On va donc supposer que $n \geq 2$. Dans ce cas, on peut écrire n comme un produit de nombres premiers. On a donc :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} ... p_k^{\alpha_k}$$

On va montrer que chacun des $p_i^{\alpha_i}$ est la somme de deux carrés.

1. Si $p_i = 2$, alors p_i est la somme de deux carrés, et donc par la première partie de la démonstration, $p_i^{\alpha_i}$ est aussi une somme de deux carrés.
2. Si $p_i = 1 \pmod 4$, alors par le théorème précédent p_i est une somme de deux carrés, et donc par la première partie de cette démonstration $p_i^{\alpha_i}$ est aussi la somme de deux carrés.
3. Si $p_i = 3 \pmod 4$, alors p_i^2 est trivialement une somme de deux carrés $(p_i^2 + 0^2)$, comme α_i est paire par hypothèse, alors on obtient que $p_i^{\alpha_i}$ est un produit de p_i^2, donc une somme de deux carrés.

Finalement, comme chaque $p_i^{\alpha_i}$ est une somme de deux carrés, en appliquant à nouveau la première partie de la démonstration, on obtient que n doit être une somme de deux carrés, ce qui complète la démonstration. □

4.7 Le problème de Waring

Dans la section précédente, nous avons vu que certains nombres naturels peuvent s'écrire comme une somme de deux carrés, mais pas tous. Nous pouvons maintenant nous demander si tous les nombres naturels

peuvent s'écrire comme une somme de 3 carrés ?

$$\begin{aligned} 1 &= 1^2 \\ 2 &= 1^2 + 1^2 \\ 3 &= 1^2 + 1^2 + 1^2 \\ 4 &= 2^2 \\ 5 &= 2^2 + 1^2 \\ 6 &= 2^2 + 1^2 + 1^2 \end{aligned}$$

Donc à première vue, il semble possible d'écrire tous les nombres naturels comme une somme de trois carrés, par contre, en continuant, on remarque vite que ce n'est pas le cas pour le nombre 7

$$7 = 2^2 + 1^2 + 1^2 + 1^2$$

On en vient donc à se demander si tout nombre naturel peut s'écrire comme une somme de 4 carrés ? Cette fois-ci, la réponse est oui comme nous l'affirme de théorème suivant dû à Lagrange.

Théorème 4.7.1. **(4 carrés de Lagrange)** Tout nombre naturel n peut s'écrire comme une somme de 4 carrés.

Le problème de Waring va plus loin. Nous voulons savoir combien de carrés sont nécessaires pour écrire n'importe quel nombre naturel. Combien de cubes ? Combien de nombres à la puissance 4 ? etc... Le problème est particulièrement compliqué et n'est toujours pas entièrement résolu. Pour le moment seules quelques valeurs sont connues.

4.8 Exercices

Exercice 4.8.1. Trouver l'ensemble de toutes les solutions des équations Diophantienne linéaires suivantes :

1. $5x + 3y = 4$
2. $6x + 15y = 21$
3. $6x + 9y = 7$
4. $1652x + 714y = 70$
5. $1375x + 484y = 819$
6. $5256x + 2457y = 1107$

Exercice 4.8.2. Trouver toutes les solutions primitives de l'équation Pythagoricienne $x^2 + y^2 = z^2$ qui satisfont les conditions ci-dessous. Dans chaque cas, on suppose que x est impair et y est pair.

1. $z = 65$
2. $z = 493$
3. $y = 884$
4. $z = 25$
5. $y = 294$
6. $y = 380$

Exercice 4.8.3. Si x, y, z est une solution primitive de l'équation Pythagoricienne $x^2 + y^2 = z^2$, démontrer les trois propriétés suivantes :

1. x ou y est divisible par 4.
2. x ou y est divisible par 3.
3. x, y ou z est divisible par 5.

Exercice 4.8.4. Répondez aux deux questions suivantes :

1. Démontrer qu'il existe une infinité de solutions primitives de l'équation Pythagoricienne pour laquelle $z - y = 1$.
2. Donner au moins 4 exemples de solutions primitives de l'équation Pythagoricienne tel que $z - y = 1$.

Exercice 4.8.5. Démontrer qu'il n'existe aucune solution entière à l'équation $x^4 + y^4 = z^4$ si $xyz \neq 0$.

Exercice 4.8.6. Démontrer que la seule solution entière à l'équation $3x^2 - y^2 = 0$ est $x = y = 0$.

Exercice 4.8.7. Démontrer que l'équation

$$x^3 + 5y^3 = 25z^3$$

ne possède aucune solution autre que $x = y = z = 0$.

Chapitre 5

La réciprocité quadratique

5.1 Les résidus quadratiques

Dans ce chapitre, nous allons chercher à développer une méthode pour vérifier quels nombres, modulo un nombre premier p, est un carré. C'est à dire que nous allons nous intéresser aux équations de la forme :

$$x^2 = m \text{ (mod p)}$$

La question est de savoir pour quelles valeurs de m l'équation peut être résolue. Ceci revient essentiellement à chercher quels nombres entiers possèdent une racine carré.

Definition 5.1.1. On dit que m est un résidu quadratique modulo p s'il existe un x tel que

$$x^2 = m \text{ (mod p)}$$

Autrement, on dit que m est un non-résidu quadratique.

Attention à ne pas confondre la définition d'un résidu quadratique modulo p avec celle d'un résidu modulo p. Question de nous donner une idée de la saveur du problème, nous allons commencer avec une méthode empirique pour résoudre les problèmes de cette section. Supposons que nous sommes intéressé à travailler modulo 13, alors on peut écrire :

$1^2 = 1 \text{ (mod 13)}$	$5^2 = 25 = 12 \text{ (mod 13)}$	$9^2 = 81 = 3 \text{ (mod 13)}$
$2^2 = 4 \text{ (mod 13)}$	$6^2 = 36 = 10 \text{ (mod 13)}$	$10^2 = 100 = 9 \text{ (mod 13)}$
$3^2 = 9 \text{ (mod 13)}$	$7^2 = 49 = 10 \text{ (mod 13)}$	$11^2 = 121 = 4 \text{ (mod 13)}$
$4^2 = 16 = 3 \text{ (mod 13)}$	$8^2 = 64 = 12 \text{ (mod 13)}$	$12^2 = 144 = 1 \text{ (mod 13)}$

Un phénomène intéressant se remarque automatiquement, il y a une forme de symétrie. En effet, si on énumère dans l'ordre les différentes valeurs, on obtient :

$$\{1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1\}$$

On remarque donc que les 6 premières valeurs obtenues $\{1, 4, 9, 3, 12, 10\}$, se répètent ensuite dans le sens inverse : $\{10, 12, 3, 9, 4, 1\}$. Donc chaque résidu quadratique se répète deux fois. De plus, si on exclut le 0 qui n'est pas d'un très grand intérêt, on remarque qu'il y a autant de résidus quadratiques que de non résidus quadratiques. En effet, les résidus quadratiques sont $\{1, 3, 4, 9, 10, 12\}$, alors que les non résidus quadratiques sont $\{2, 5, 6, 7, 8, 11\}$.

5.2 Le symbole de Legendre

Question d'améliorer un peu notre efficacité à travailler avec ce type de problème, nous allons introduire une notion qui va nous être particulièrement utile jusqu'à la fin du chapitre. Il s'agit du symbole de Legendre [1].

1. Le symbole de Legendre est définie uniquement pour des nombres premiers p. Il existe aussi une généralisation appelé symbol de Jacobi qui est définie pour tout entier positif. Nous n'allons cependant pas étudier le symbol de Jacobi ici.

Definition 5.2.1. Si p est un nombre premier impair et $n \in \mathbb{Z}$, alors on définit le symbole de Legendre comme étant :

$$\left(\frac{n}{p}\right) = \begin{cases} 0 \text{ si } n = 0 \pmod{\text{p}} \\ 1 \text{ si } n \neq 0 \pmod{\text{p}} \text{ et n est un résidu quadratique modulo p} \\ -1 \text{ si } n \neq 0 \pmod{\text{p}} \text{ et n n'est pas un résidu quadratique modulo p} \end{cases}$$

Remarquez qu'ici le cas de $0 \pmod{p}$ est considéré comme un cas particulier qui est exclu de la plupart des théorèmes du chapitre, ce qui inclut le théorème ci-dessous.

Théorème 5.2.1. Si p est un nombre premier impair, alors il existe autant de résidus quadratiques modulo p que de non-résidus quadratiques. De plus, l'ensemble des résidus quadratiques modulo p est donné par :

$$\left\{1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2\right\}$$

Démonstration. Premièrement, remarquons que l'ensemble

$$\left\{1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2\right\}$$

contient uniquement des résidus quadratiques, et remarquons que tous ces nombres sont dans des classes différentes modulo p. Pour le montrer, supposons que $i^2 = j^2$ avec $0 \leq i, j \leq \frac{p-1}{2}$. Alors on a :

$$i^2 - j^2 = (i-j)(i+j) = 0 \pmod{p}$$

donc $p|(i-j)$ ou $p|(i+j)$. De plus remarquons que :

$$0 \leq i + j \leq \left(\frac{p-1}{2}\right) + \left(\frac{p-1}{2}\right) = p - 1 < p$$

il est donc impossible que $p|(i+j)$, on doit donc avoir $p|(i-j)$, ce qui nous donne :

$$i = j \pmod{p}$$

Il y a donc au moins $\frac{p-1}{2}$ résidus quadratiques modulo p. On veut maintenant montrer qu'il n'y en a pas d'autres. Supposons donc que $\frac{p+1}{2} \leq k < p$. On veut montrer que k^2 appartient déjà à l'une des classes d'équivalence de l'ensemble. Pour ce faire, il s'agit tout simplement de remarquer que :

$$k^2 = (p-2k)p + k^2 = (p-k)^2 \pmod{p}$$

Il ne peut donc pas y avoir d'autres résidus quadratiques modulo p. On doit donc avoir $\frac{p-1}{2}$ résidus quadratiques modulo p, et $\frac{p-1}{2}$ non-résidus. □

Exemple 5.2.1. On veut trouver l'ensemble de tous les résidus quadratiques modulo 11. Par le théorème précédent, on a donc que les résidus quadratiques sont donnés par $\{1^2, 2^2, 3^2, 4^2, 5^2\}$. Il s'agit maintenant de les simplifier modulo 11 :

$$\begin{aligned} 1^2 &= 1 \pmod{11} \\ 2^2 &= 4 \pmod{11} \\ 3^2 &= 9 \pmod{11} \\ 4^2 &= 16 = 5 \pmod{11} \\ 5^2 &= 25 = 3 \pmod{11} \end{aligned}$$

L'ensemble des résidus quadratiques modulo 11 est donc : $\{1, 3, 4, 5, 9\}$, et l'ensemble des non résidus est donné par : $\{2, 6, 7, 8, 10\}$.

Remarquez maintenant que même si le théorème précédent nous donne certaines informations intéressantes sur les résidus et non résidus quadratiques, si p est un nombre premier relativement grand, il peut être très long trouver l'ensemble des résidus quadratiques. Le théorème nous est donc d'une utilité très limitée.

5.3 Le critère d'Euler

Nous allons maintenant faire un grand pas en avant dans notre étude des résidus quadratiques. Le critère d'Euler, que nous allons étudier dans cette section, peut, en effet, nous permettre d'évaluer, relativement facilement, le symbole de Legendre pour n'importe quel nombre premier impair p. Le critère d'Euler est en fait une application du petit théorème de Fermat et du théorème de Wilson que nous avons vus au chapitre 2.

Théorème 5.3.1. **(Critère d'Euler)** Si p est un nombre premier impair, alors pour tout n on a :

$$\left(\frac{n}{p}\right) = n^{(p-1)/2} \pmod{p}$$

Démonstration. Premièrement, remarquons que le résultat est évident si $n = 0 \pmod{p}$, c'est à dire si $\left(\frac{n}{p}\right) = 0$. On va donc s'intéresser aux deux autres cas :

Cas 1 : Supposons donc que $\left(\frac{n}{p}\right) = 1$. Dans ce cas, il existe un x tel que $x^2 = n \pmod{p}$. On obtient donc :

$$n^{(p-1)/2} = (x^2)^{(p-1)/2} = x^{p-1} = 1 \pmod{p}$$

d'après le petit théorème de Fermat, ce qui démontre le théorème dans le premier cas.

Cas 2 : On va supposer que $\left(\frac{n}{p}\right) = -1$. C'est à dire qu'il n'existe aucun x tel que $x^2 = n \pmod{p}$. Dans ce cas, pour chaque entier a tel que $1 \leq a < p$, il existe un unique b tel que $1 \leq b < p$ satisfaisant :

$$ab = n \pmod{p}$$

de plus, $a \neq b$ car autrement a serait un résidu quadratique. Donc chaque entier dans l'intervalle $[1, p-1]$ peut être regroupé en pair pour laquelle le produit est n. On obtient donc que

$$(p-1)! = a^{(p-1)/2} \pmod{p}$$

Maintenant, en appliquant le théorème de Wilson, on peut conclure que :

$$(p-1)! = a^{(p-1)/2} = -1 \pmod{p}$$

Ce qui complète la démonstration du second cas. □

Exemple 5.3.1. On veut savoir s'il existe un entier x tel que $x^2 = 4 \pmod{17}$. En appliquant le critère d'Euler on a donc :

$$\left(\frac{4}{17}\right) = 4^8 = (4^2)^4 = 16^4 = (-1)^4 = 1 \pmod{17}$$

Il existe donc une valeur de x qui satisfait l'équation.

Remarquez que le critère d'Euler ici ne nous donne aucune identification de la valeur de x qui satisfait l'équation. On aurait cependant pu vérifier facilement que $x = 2$ doit être une solution. Remarquez aussi que le problème que nous avions pour les grandes valeurs de p se pose toujours. Si p est grand, le calcul risque de devenir long.

Exemple 5.3.2. Existe-t-il un entier x tel que $x^2 = 17 \pmod{101}$? En utilisant le critère d'Euler à nouveau, on a donc :

$$\left(\frac{17}{101}\right) = 17^{50} \pmod{101}$$

Pour ce faire, on a donc :

$$\begin{aligned} 17^2 &= 289 = 87 \pmod{101} \\ 17^4 &= 87^2 = 7569 = 95 \pmod{101} \\ 17^8 &= 95^2 = (-6)^2 = 36 \pmod{101} \\ 17^{16} &= 36^2 = 1296 = 84 \pmod{101} \\ 17^{32} &= 84^2 = 7056 = 87 \pmod{101} \end{aligned}$$

De plus, comme $50 = 32 + 16 + 2$, alors on a :

$$17^{50} = 17^{32} \cdot 17^{16} \cdot 17^2 = 87 \cdot 84 \cdot 87 = 7308 \cdot 87 = 36 \cdot 87 = 3132 = 1 \pmod{101}$$

Il existe donc encore une fois un x qui satisfait l'équation.

Le théorème le plus important de ce chapitre est la loi de réciprocité quadratique que nous allons voir plus loin dans le chapitre. Il s'agit d'un théorème qui va nous permettre de calculer, de manière beaucoup plus efficace, le symbole de Legendre que ce que nous permet de faire le critère d'Euler. Par contre, le critère d'Euler reste une étape incontournable dans l'étude du symbole de Legendre car il nous permet d'affirmer que le symbole de Legendre est en fait une fonction complètement multiplicative. C'est ce que nous allons démontrer immédiatement.

Théorème 5.3.2. Le symbole de Legendre est une fonction complètement multiplicative. C'est à dire que si p est un nombre premier impair, et m, n sont des entiers, alors :

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

Démonstration. Il s'agit d'appliquer le critère d'Euler. On a donc :

$$\begin{aligned} \left(\frac{mn}{p}\right) &= (mn)^{(p-1)/2} \pmod{p} \\ &= m^{(p-1)/2} n^{(p-1)/2} \pmod{p} \\ &= \left(\frac{m}{p}\right)\left(\frac{n}{p}\right) \end{aligned}$$

□

Aux vues de ce dernier théorème, on remarque donc que l'étude des résidus quadratiques et du symbol de Legendre peut donc se ramener à l'étude du symbol de Legendre $\left(\frac{q}{p}\right)$ où p et q sont des nombres premiers. Les autres cas peuvent alors être résolus facilement en utilisant la multiplicité du symbole de Legendre.

5.4 Les lois complémentaires

Avant d'énoncer la loi de réciprocité de Gauss, nous allons commencer par énoncer les deux lois complémentaires, qui avec la loi de réciprocité, vont nous permettre de résoudre la plupart des problèmes.

Théorème 5.4.1. **(Première loi complémentaire)** Si p est un nombre premier impair, alors :

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 \text{ si } p = 1 \pmod 4 \\ -1 \text{ si } p = 3 \pmod 4 \end{cases}$$

Démonstration. La première partie n'est en fait qu'une simple application du critère d'Euler. On obtient donc directement que :

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$$

Maintenant, pour la seconde partie, remarquons que si p est un nombre (premier) impair, alors p doit avoir la forme $4k+1$ ou $4k+3$. Dans un premier temps, si $p = 4k+1$, on obtient :

$$\frac{p-1}{2} = \frac{4k+1-1}{2} = \frac{4k}{2} = 2k \qquad \Rightarrow \qquad \frac{p-1}{2} \text{ est pair}$$

Donc si $p = 1 \pmod 4$, alors on obtient :

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{\text{nombre pair}} = 1$$

Dans un second temps, si $p = 4k+3$, on obtient :

$$\frac{p-1}{2} = \frac{4k+3-1}{2} = \frac{4k+2}{2} = 2k+1 \qquad \Rightarrow \qquad \frac{p-1}{2} \text{ est impair}$$

Donc si $p = 3 \pmod 4$, alors on obtient :

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{\text{nombre impair}} = -1$$

Ce qui complète la démonstration de la première loi complémentaire. □

Théorème 5.4.2. **(Deuxième loi complémentaire)** Si p est un nombre premier impair, alors :

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 \text{ si } p = \pm 1 \pmod 8 \\ -1 \text{ si } p = \pm 3 \pmod 8 \end{cases}$$

Démonstration. Premièrement notons que par le critère d'Euler on a :

$$\left(\frac{2}{p}\right) = 2^{\frac{p-1}{2}}$$

Maintenant, considérons l'ensemble des $\dfrac{p-1}{2}$ congruences suivantes :

$$\begin{cases} p-1 = 1(-1)^1 \pmod p \\ 2 = 2(-1)^2 \pmod p \\ p-3 = 3(-1)^3 \pmod p \\ 4 = 4(-1)^4 \pmod p \\ p-5 = 5(-1)^5 \pmod p \\ \ldots = \ldots \\ \dfrac{p-1}{2} \text{ ou } p - \dfrac{p-1}{2} = \dfrac{p-1}{2}(-1)^{\frac{p-1}{2}} \pmod p \end{cases}$$

Remarquons que tous les membres de gauche sont des nombres pairs. En calculant le produit des termes de gauche et le produit des termes de droite, on obtient donc :

$$2 \cdot 4 \cdot 6 \cdot 8 \cdot \ldots \cdot (p-1) = \prod_{i=1}^{\frac{p-1}{2}} i(-1)^i \pmod{p}$$

$$2^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdot \ldots \cdot \frac{p-1}{2}\right) = \left(\frac{p-1}{2}\right)! \prod_{i=1}^{\frac{p-1}{2}} (-1)^i \pmod{p}$$

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = \left(\frac{p-1}{2}\right)! (-1)^{1+2+3+\ldots+\frac{p-1}{2}} \pmod{p}$$

$$2^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! = \left(\frac{p-1}{2}\right)! (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

Maintenant, comme $\left(\frac{p-1}{2}\right)! \neq 0 \pmod{p}$ et que p est un nombre premier, on obtient donc :

$$2^{\frac{p-1}{2}} = (-1)^{\frac{p^2-1}{8}} \pmod{p}$$

Maintenant, en utilisant le critère d'Euler tel que nous l'avons mentionné au début de la démonstration, on obtient finalement :

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

□

Exemple 5.4.1. Existe-t-il un entier x tel que $x^2 = 11 \pmod{13}$? Comme $11 = -2 \pmod{13}$, on obtient donc :

$$\left(\frac{11}{13}\right) = \left(\frac{-2}{13}\right) = \left(\frac{-1}{13}\right)\left(\frac{2}{13}\right) = (-1)^6(-1)^{21} = -1$$

Il n'existe donc aucun entier x qui satisfait l'équation.

5.5 La loi de réciprocité quadratique

Nous sommes maintenant pratiquement prêt à énoncer et à démontrer la loi de réciprocité quadratique. Il ne nous reste qu'à énoncer et à démontrer le lemme de Gauss avant de pouvoir le faire. Ce dernier est en quelque sorte une autre façon de calculer le symbole de Legendre comme pour le critère d'Euler, à la différence que le lemme de Gauss est très inefficace pour les calculs, mais qui nous sera essentielle à la démonstration de la loi de réciprocité quadratique.

Théorème 5.5.1. **(Lemme de Gauss)** Si p est un nombre premier impair et a est un entier tel que $(a, p) = 1$. Considérons l'ensemble

$$\left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

et posons n le nombre de ces entiers qui sont congrus à un entier entre $\frac{p}{2}$ et p modulo p. Alors

$$\left(\frac{a}{p}\right) = (-1)^n$$

Démonstration. Posons

$$A = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2}a\right\}$$

Il est facile de voir que tous les éléments de A sont distincts modulo p car $(a,p)=1$. On sépare maintenant l'ensemble A en deux sous-ensembles :

$$R=\{r_1,r_2,r_3,...,r_k\} \quad \text{et} \quad S=\{s_1,s_2,s_3,...,s_n\}$$

où l'ensemble R contient les éléments de A qui sont congrus modulo p à un entier entre 0 et $\frac{p}{2}$ et l'ensemble S contient les éléments de A qui sont congrus à un entier entre $\frac{p}{2}$ et p. On a donc nécessairement que $A=R\cup S$. À partir de l'ensemble S, on construit maintenant un autre ensemble T comme étant :

$$T=\{p-s_1,p-s_2,p-s_3,...,p-s_n\}$$

On remarque donc que tous les éléments de T sont congrus modulo p à un entier entre 0 et $\frac{p}{2}$. On veut maintenant montrer que R et T sont disjoints. Pour ce faire, supposons le contraire, c'est à dire qu'il existe i,j tel que

$$r_i=p-s_j \pmod p$$

Dans ce cas, on obtient que

$$r_i+s_j=0 \pmod p$$

il existe donc des entiers u,v tels que $r_i=ua$ et $s_j=va$ avec u,v entre 1 et $\frac{p-1}{2}$, ce qui nous donne :

$$r_i+s_j=ua+va=(u+v)a=0 \pmod p$$

comme $(a,p)=1$, on obtient donc que $p|(u+v)$. Cependant, on a aussi que :

$$0<u+v<\frac{p-1}{2}+\frac{p-1}{2}=p-1<p$$

on obtient donc une contradiction. On a donc que $R\cap T=\emptyset$. On a donc que $R\cup T$ contient exactement $\frac{p-1}{2}$ élément congru à des entiers entre 1 et $\frac{p-1}{2}$, ce qui signifie que $R\cup T$ contient tous les entiers entre 1 et $\frac{p-1}{2}$ modulo p. En multipliant tous les éléments de $R\cup S$, on obtient donc :

$$r_1r_2r_3...r_k(p-s_1)(p-s_2)(p-s_3)...(p-s_n)=\left(\frac{p-1}{2}\right)! \pmod p$$

ce qui nous donne en simplifiant :

$$\begin{aligned}
r_1r_2r_3...r_k(-s_1)(-s_2)(-s_3)...(-s_n) &= \left(\frac{p-1}{2}\right)! \pmod p\\
(-1)^n r_1r_2r_3...r_ks_1s_2s_3...s_n &= \left(\frac{p-1}{2}\right)! \pmod p\\
(-1)^n a\cdot 2a\cdot 3a\cdot ...\cdot \frac{p-1}{2}a &= \left(\frac{p-1}{2}\right)! \pmod p\\
(-1)^n a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! &= \left(\frac{p-1}{2}\right)! \pmod p\\
(-1)^n a^{\frac{p-1}{2}} &= 1 \pmod p\\
a^{\frac{p-1}{2}} &= (-1)^n \pmod p
\end{aligned}$$

Maintenant, d'après le critère d'Euler on a que $\left(\frac{a}{p}\right)=a^{\frac{p-1}{2}}$, ce qui nous donne finalement :

$$\left(\frac{a}{p}\right)=(-1)^n \pmod p$$

□

Nous allons maintenant illustrer le lemme de Gauss à l'aide d'un exemple :

Exemple 5.5.1. On veut savoir s'il existe un entier x tel que $x^2 = 6 \pmod{19}$. On veut utiliser le lemme de Gauss. Pour ce faire, commençons par consider l'ensemble :

$$\{6, 2\cdot 6, 3\cdot 6, 4\cdot 6, 5\cdot 6, 6\cdot 6, 7\cdot 6, 8\cdot 6, 9\cdot 6\}$$

En effectuant les produits, on obtient :

$$\{6, 12, 18, 24, 30, 36, 42, 48, 54\}$$

Puis en réduisant au plus petit résidu positif modulo 19, on obtient :

$$\{6, 12, 18, 5, 11, 17, 4, 10, 17\}$$

Maintenant, on remarque qu'il y a exactement 6 nombres dans l'ensemble ci-dessus qui sont supérieurs à $\frac{19}{2} = 8,5$. On a donc d'après le lemme de Gauss :

$$\left(\frac{6}{19}\right) = (-1)^6 = 1$$

Il existe donc un x qui satisfait l'équation.

Théorème 5.5.2. **(Loi de réciprocité quadratique de Gauss)** Si p et q sont des nombres premiers impairs distincts, alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

Avant de commencer, notez que la preuve ci-dessus utilise la démonstration du lemme de Gauss (incluant la notation). Il est donc nécessaire de bien comprendre la démonstration du lemme de Gauss avant d'entreprendre la démonstration de la loi de réciprocité.

Démonstration. Nous allons faire la démonstration en deux parties :
Première partie : Si p est un nombre premier impair, et a un entier tel que $(a, p) = 1$, alors le lemme de Gauss nous affirme que :

$$\left(\frac{a}{p}\right) = (-1)^n$$

où n est défini dans le lemme de Gauss. Dans un premier temps, nous allons chercher à trouver un expression nous permettant de calculer la valeur de ce n. Premièrement, rappelons nous que pour utiliser le lemme de Gauss, nous avons besoin de trouver les plus petits résidus positifs des éléments de l'ensemble $\left\{a, 2a, 3a, ..., \frac{p-1}{2}a\right\}$. Pour ce faire, remarquons que :

$$\frac{ma}{p} = \left[\frac{ma}{p}\right] + b_m, \text{ avec } 0 \leq b_m < 1$$

où la fonction $[\cdot]$ représente le plus grand entier inférieur ou égal à la valeur entre crochet. En multipliant des deux côtés par p, on obtient donc :

$$ma = p\left[\frac{ma}{p}\right] + pb_m = p\left[\frac{ma}{p}\right] + a_m, \text{ avec } 0 \leq a_m < p$$

donc a_m est le plus petit résidu de ma modulo p. En réduisant les éléments de l'ensemble $\{a, 2a, 3a, ..., \frac{p-1}{2}\}$ modulo p, on obtient donc l'ensemble :

$$\left\{a_1, a_2, a_3, ..., a_{\frac{p-1}{2}}\right\} = \{r_1, r_2, ..., r_k, s_1, s_2, ..., s_n\}$$

où les r_i et s_i sont définis dans la démonstration du lemme de Gauss. En additionnant tous les termes de ces deux ensembles, on obtient donc :

$$\sum_{i=1}^{\frac{p-1}{2}} a_i = \sum_{i=1}^{k} r_i + \sum_{i=1}^{n} s_i \tag{5.1}$$

De plus, dans la démonstration du lemme de Gauss nous avons montré que :

$$\left\{1, 2, 3, ..., \frac{p-1}{2}\right\} = \{r_1, r_2, ..., r_k, p - s_1, p - s_2, ..., p - s_n\}$$

maintenant, on additionne à nouveau les éléments de ces deux ensembles. On obtient donc :

$$\sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{k} r_i + \sum_{i=1}^{n} (p - s_i)$$

qui nous donne en simplifiant :

$$\frac{p^2-1}{8} = \sum_{i=1}^{k} r_i + np - \sum_{i=1}^{n} s_i \tag{5.2}$$

Maintenant, en additionnant les équations 5.1 et 5.2, on obtient :

$$\sum_{i=1}^{\frac{p-1}{2}} a_i + \frac{p^2-1}{8} = 2\sum_{i=1}^{k} r_i + np$$

Comme nous avons montré au début de la démonstration que $a_i = ia - p\left[\frac{ia}{p}\right]$, on obtient donc :

$$\sum_{i=1}^{\frac{p-1}{2}} \left(ia - p\left[\frac{ia}{p}\right]\right) + \frac{p^2-1}{8} = 2\sum_{i=1}^{k} r_i + np$$

ce qui nous donne en simplifiant :

$$a\left(\frac{p^2-1}{8}\right) - p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] + \frac{p^2-1}{8} = 2\sum_{i=1}^{k} r_i + np$$

$$(a+1)\left(\frac{p^2-1}{8}\right) - p\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] = 2\sum_{i=1}^{k} r_i + np$$

On calcule ensuite le tout modulo 2, puis on simplifie :

$$(a+1)\left(\frac{p^2-1}{8}\right) - \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] = n \pmod 2$$

remarquez que nous avons utilisé ci-dessus le fait que p est un nombre impair. Remarquons maintenant que si a est un nombre impair, l'équation peut ce simplifier encore plus et on obtient :

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ia}{p}\right] = n \pmod 2$$

Deuxième partie : Si p et q sont tous deux des nombres premiers impairs, et $p \neq q$, alors en utilisant le lemme de Gauss en combinaison avec la formule que nous venons d'obtenir, on obtient les deux formules suivantes :

$$\left(\frac{p}{q}\right) = (-1)^{\Sigma_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right]} \quad \text{et} \quad \left(\frac{q}{p}\right) = (-1)^{\Sigma_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]}$$

Et en multipliant ces deux équations on obtient :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\Sigma_{i=1}^{\frac{q-1}{2}}\left[\frac{ip}{q}\right]+\Sigma_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]} \tag{5.3}$$

Nous allons donc chercher à évaluer l'exposant de droite. Pour ce faire, considérons l'ensemble S de tous les couples (x, y) avec x et y entiers, $1 \leq x \leq \frac{p-1}{2}$ et $1 \leq y \leq \frac{q-1}{2}$. Il est donc facile de voir qu'on a exactement $\frac{(p-1)(q-1)}{4}$ éléments dans S. Nous allons maintenant séparer les éléments de S en deux ensembles :

$$S_1 = \{(x, y) \in S : qx > py\} \text{ et } S_2 = \{(x, y) \in S : qx < py\}$$

On remarque donc que $S = S_1 \cup S_2$. Maintenant, il s'agit de compter combien il y a d'éléments dans chacun de ces deux ensembles. Comme $qx > py$ implique que $y < \frac{qx}{p}$, il y a donc

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right]$$

élément dans l'ensemble S_1. De la même manière, comme $qx < py$ implique que $x < \frac{py}{q}$, il y a donc :

$$\sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right]$$

éléments dans l'ensemble S_2. On obtient donc en comparant le nombre d'éléments dans S, S_1 et S_2 :

$$\sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\frac{q-1}{2}} \left[\frac{py}{q}\right] = \frac{(p-1)(q-1)}{4}$$

Finalement, en remplaçant le tout dans l'équation 5.3, on a :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\Sigma_{x=1}^{\frac{p-1}{2}}\left[\frac{qx}{p}\right]+\Sigma_{y=1}^{\frac{q-1}{2}}\left[\frac{py}{q}\right]} = (-1)^{\frac{(p-1)(q-1)}{4}}$$

ce qui complète la démonstration. □

Ici, une remarque un peut curieuse s'impose. Comme le symbol de Legendre prend seulement les valeurs $0, 1$ ou -1, alors la loi de réciprocité quadratique peut être réécrite de différente façon :

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \iff \left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right) \iff \left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{p}{q}\right)$$

En particulier, il n'est absolument pas nécessaire d'avoir recourt à la division.

Exemple 5.5.2. On veut savoir s'il existe un entier x tel que

$$x^2 = 797 \pmod{1499}$$

Comme les nombres 797 et 1499 sont des nombres premiers, le problème revient donc à calculer la valeur de $\left(\frac{797}{1499}\right)$. Par la loi de réciprocité quadratique, on a donc :

$$\left(\frac{797}{1499}\right) = \left(\frac{1499}{797}\right)(-1)^{\frac{796\cdot 1498}{4}} = \left(\frac{702}{797}\right)(-1)^{298102} = \left(\frac{702}{797}\right)$$

car 1499 mod 797 = 702. Maintenant, on factorise le nombre 702 et on utilise le fait que le symbole de Legendre est complètement multiplicatif.

$$\left(\frac{702}{797}\right) = \left(\frac{2}{797}\right)\left(\frac{3}{797}\right)^3\left(\frac{13}{797}\right)$$

Pour calculer $\left(\frac{2}{797}\right)$ on utilise la deuxième loi complémentaire, ce qui nous donne :

$$\left(\frac{2}{797}\right) = (-1)^{\frac{797^2-1}{8}} = (-1)^{79401} = -1$$

Maintenant, pour calculer $\left(\frac{3}{797}\right)$, on utilise la loi de réciprocité quadratique, suivi de la deuxième loi complémentaire :

$$\left(\frac{3}{797}\right) = \left(\frac{797}{3}\right)(-1)^{\frac{796\cdot 2}{4}} = \left(\frac{2}{3}\right)(-1)^{398} = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = (-1)^1 = -1$$

Puis, pour calculer $\left(\frac{13}{797}\right)$, on applique encore une fois la loi de réciprocité quadratique suivie de la multiplicité complète du symbole de Legendre :

$$\left(\frac{13}{797}\right) = \left(\frac{797}{13}\right)(-1)^{\frac{796\cdot 12}{4}} = \left(\frac{4}{13}\right)(-1)^{2388} = \left(\frac{2}{13}\right)^2 = 1$$

En combinant c'est 3 dernières équations, on obtient finalement que :

$$\left(\frac{702}{797}\right) = \left(\frac{2}{797}\right)\left(\frac{3}{797}\right)^3\left(\frac{13}{797}\right) = (-1)(-1)^3(1) = 1$$

On peut donc conclure qu'il existe bien un x qui satisfait l'équation

$$x^2 = 797 \pmod{1499}$$

Par contre, la méthode ne nous donne aucune information pour trouver ce x. À l'aide d'un ordinateur, il nous est possible de trouver que les deux valeurs de x qui satisfont cette équation sont 332 et 1167.

Exemple 5.5.3. On veut utiliser la théorie développée dans ce chapitre pour savoir si l'équation

$$x^2 + 7x + 5 = 0 \pmod{11}$$

possède au moins une solution. Pour ce faire, nous devons commencer par compléter le carré du polynôme, c'est à dire écrire le polynôme sous la forme :

$$(x-b)^2 = c \pmod{11} \quad \Longrightarrow \quad x^2 - 2bx + b^2 = c \pmod{11}$$

On doit donc résoudre l'équation $-2b = 7 \pmod{11}$. En appliquant le petit théorème de Fermat, on obtient donc :

$$\begin{aligned} -2b &= 7 \pmod{11} \\ (-2)^{10}b &= (-2)^9 \cdot 7 \pmod{11} \\ b &= (-2)^9 \cdot 7 = (-2)\cdot(((-2)^2)^2)^2 \cdot 7 = (-2)\cdot(4^2)^2 \cdot 7 \pmod{11} \\ &= (-2)\cdot 5^2 \cdot 7 = (-2)\cdot 3 \cdot 7 = (-2)\cdot(-1) = 2 \pmod{11} \end{aligned}$$

On obtient donc :

$$(x-2)^2 + 5 = 4 \pmod{11} \Longrightarrow (x-2)^2 = -1 \pmod{11}$$

En posant $y = x-2$. On obtient donc que l'équation $x^2+7x+5 = 0 \pmod{11}$ possède au moins une solution si et seulement si l'équation $y^2 = -1 \pmod{11}$ possède au moins une solution. On est donc ramené à calculer :

$$\left(\frac{-1}{11}\right) = (-1)^5 = -1$$

L'équation n'a donc pas de solution.

5.6 Exercices

Exercice 5.6.1. Trouver la liste de tous les résidues quadratiques différents de 0

1. modulo 7
2. modulo 19

Exercice 5.6.2. Trouver tous les entiers x (s'il y en a) tel que

1. $x^2 = 9 \pmod{11}$
2. $x^2 = 3 \pmod{13}$

Exercice 5.6.3. En utilisant le critère d'Euler, calculer les valeurs des symboles de Legendre suivants :

1. $\left(\frac{8}{11}\right)$
2. $\left(\frac{52}{97}\right)$

Exercice 5.6.4. Répondez aux deux questions suivantes :

1. Si a est un nombre naturel non nul, p est un nombre premier et $(a, p) = 1$. Démontrer que
$$\left(\frac{a^2}{p}\right) = 1$$
2. Existe-t-il des entiers x qui satisfont l'équation suivante ?
$$x^2 = -25 \pmod{1429}$$
Indice : 1429 est un nombre premier.

Exercice 5.6.5. Répondez aux deux questions suivantes :

1. Si p est un nombre premier impair. En utilisant les lois complémentaires et la multiplicité du symbole de Legendre, trouver un expression permettant de calculer $\left(\frac{-2}{p}\right)$
2. Utiliser la première partie pour évaluer $\left(\frac{59}{61}\right)$

Exercice 5.6.6. Utiliser le lemme de Gauss pour calculer les symboles de Legendre suivants :

1. $\left(\frac{7}{13}\right)$
2. $\left(\frac{3}{17}\right)$

Exercice 5.6.7. Utiliser la loi de réciprocité quadratique et tous les outils que nous avons vus dans ce chapitre pour évaluer les symboles de Legendre suivants :

1. $\left(\frac{5}{17}\right)$
2. $\left(\frac{5}{11}\right)$
3. $\left(\frac{68}{101}\right)$
4. $\left(\frac{143}{173}\right)$

Exercice 5.6.8. Dans chacun des cas, indiquer s'il existe un entier x qui satisfait l'équation :

1. $x^2 = 24 \pmod{67}$
2. $x^2 = 5 \pmod{73}$

Exercice 5.6.9. Trouver l'ensemble des solutions des équations suivantes :

1. $x^2 + 5x + 3 = 0 \pmod{13}$
2. $x^2 + 31x + 99 = 0 \pmod{113}$

Exercice 5.6.10. Est-ce que l'équation suivante admet une solution ?

$$x^2 + 7x + 24 = 0 \pmod{53}$$

Exercice 5.6.11. Démontrer que si p est un nombre premier, $p \geq 5$, alors on a :

$$\left(\frac{3}{p}\right) = \begin{cases} 1 \text{ si } p = 1 \text{ ou } 11 \pmod{12} \\ -1 \text{ si } p = 5 \text{ ou } 7 \pmod{12} \end{cases}$$

Appendice 1 : Petit théorème de Fermat version algébrique

Nous allons dans cet appendice donner une autre démonstration du petit théorème de Fermat, mais cette fois en utilisant la théorie des groupes. Il s'agit en quelque sorte du point de départ de la théorie algébrique des nombres.

Definition 6.6.1. On dit que $(G, *)$ est un groupe si G est un ensemble, et $*$ est un opération binaire $* : G \times G \to G$ tel que :

1. Il existe un élément $e \in G$ tel que $e * g = g * e = g$ pour tout $g \in G$
2. Pour tout $a, b, c \in G$ on a : $a * (b * c) = (a * b) * c$
3. Pour tout $g \in G$, il existe un élément dénoté $g^{-1} \in G$ tel que $g * g^{-1} = g^{-1} * g = e$

Remarquez qu'il est sous entendu dans la définition d'un groupe que si $g, h \in G$, alors $g * h \in G$.

Definition 6.6.2. Si p est un nombre premier, alors on définit $(\mathbb{Z}_p^\times, \times)$ comme étant l'ensemble

$$\mathbb{Z}_p^\times = \{1, 2, 3, ..., p-1\}$$

muni de l'opération de multiplication modulo p.

Théorème 6.6.1. *Si p est un nombre premier, alors $(\mathbb{Z}_p^\times, \times)$ est un groupe.*

Démonstration. Premièrement, il est facile de voir que $e = 1$ est un identité, et que l'opération de multiplication modulo p est associative. Il ne nous reste donc qu'à démontrer l'existence d'inverse. Prenons $a \in \mathbb{Z}_p^\times$, alors comme p est premier, $(a, p) = 1$. Donc par l'identité de Bézout, il existe $m, n \in \mathbb{Z}$ tel que :

$$ma + bp = 1$$

Maintenant, en calculant le tout modulo p, on obtient :

$$ma = 1 \pmod{p}$$

ce qui nous donne $a^{-1} = m$ dans $(\mathbb{Z}_p^\times, \times)$. On peut donc conclure que $(\mathbb{Z}_p^\times, \times)$ est un groupe. □

Definition 6.6.3. Supposons que $(G, *)$ est un groupe, alors on dit que $(H, *)$ est un sous groupe de $(G, *)$ si H est un sous-ensemble de G et $(H, *)$ est un groupe.

Théorème 6.6.2. *Supposons que p est un nombre premier et prenons $x \in \{1, 2, 3, ..., p-1\}$. Alors l'ensemble*

$$\langle x \rangle = \{1, x, x^2, x^3, x^4, ...\}$$

muni de l'opération de multiplication modulo p est un sous-groupe de $(\mathbb{Z}_p^\times, \times)$.

Démonstration. Premièrement, commençons par noter que l'ensemble $\langle x \rangle$ n'est pas vraiment infini comme le suggère sa définition. Comme nous travaillons modulo p, l'ensemble $\langle x \rangle$ ne peut pas avoir plus de p éléments. Il doit donc exister $a, b \in \mathbb{Z}$, $a > b$ tel que :

$$x^a = x^b$$

On obtient donc :

$$x^b \times x^{a-b} = x^b \times 1$$

Comme il s'agit d'élément de $\mathbb{Z}_p^\times$, on obtient donc que :

$$x^{a-b} = 1$$

Il existe donc un plus petit entier n, $n > 1$ tel que $x^n = 1$. De plus, on remarque que $\{1, x^2, x^3, ..., x^{n-1}\}$ sont tous des éléments distincts, autrement, cela contredirait la minimalité de n. Maintenant, notons que l'ensemble $\langle x \rangle$ contient une identité et est associatif, donc pour démontrer qu'il s'agit d'un sous-groupe, nous n'avons qu'à démontrer l'existence d'inverse. Prenons $x^a \in \langle x \rangle$, alors $(x^a)^{-1} = x^{n-a}$, car

$$x^a x^{n-a} = x^n = 1$$

Donc l'ensemble $\langle x \rangle$ est bien un sous groupe de $\mathbb{Z}_p^\times$. □

Definition 6.6.4. Si $(G, *)$ est un groupe, alors on définit la cardinalité de G, dénoté $|G|$ comme étant le nombre d'élément (distinct) de G.

Théorème 6.6.3 (Lagrangre)**.** *Supposons que $(G, *)$ est un groupe, et $(H, *)$ un sous-groupe. Alors $|H| \Big| |G|$.*

Démonstration. Prenons $x \in G$. On veut montrer que H et $xH = \{x \times h : h \in H\}$ ont le même nombre d'éléments. Pour ce faire, définissons la fonction

$$f : H \to xH$$

$$f(h) = xh$$

Comme f est une fonction, à chaque élément de H on associe un élément de xH. Pour ce faire, commençons par remarquer que si $f(h_1) = f(h_2)$, alors on a :

$$\begin{aligned} f(h_1) &= f(h_2) \\ xh_1 &= xh_2 \\ x^{-1}xh_1 &= x^{-1}xh_2 \\ h_1 &= h_2 \end{aligned}$$

De plus, si $a \in xH$, alors il existe un h tel que $a = xh$. On obtient donc que $f(h) = xh = a$. On peut donc conclure que la fonction f associe à chaque élément de H un élément de xH, mais aussi que chaque élément de xH associe un seul élément de H. On peut donc conclure que H et xH ont le même nombre d'élément. Maintenant, considérons $\{x_1, x_2, x_3, ..., x_n\}$ l'ensemble de tous les éléments de G, et considérons l'ensemble

$$\{x_1H, x_2H, x_3H, ..., x_nH\}$$

Supposons que $x_iH \cap x_jH \neq \emptyset$. On veut montrer que dans ce cas, ces deux ensembles sont en fait égaux. Supposons que $a \in x_iH \cap x_jH$, alors il existe h_i et h_j tels que :

$$a = x_ih_i = x_jh_j$$

Maintenant prenons $b \in x_iH$, alors il existe $h \in H$ tel que $b = x_ih$. On obtient donc :

$$\begin{aligned} b &= x_ih \\ &= (x_jh_jh_i^{-1})h \\ &= x_j(h_jh_i^{-1}h) \\ &= x_jh' \text{ avec } h' = h_jh_i^{-1}h \end{aligned}$$

Comme H est un groupe, alors $h' \in H$. On a donc que $b \in x_jH$. On peut donc conclure que $x_iH = x_jH$. De plus, n'importe quel élément $g \in g$ fait partie de l'ensemble gH. On peut donc partitionner G en ensembles disjoints

$$\{x_1H, x_2H, ..., x_kH\}$$

Comme tous ces ensembles ont le même nombre d'éléments, qu'ils sont disjoints, et contiennent ensemble tous les éléments de G, on peut donc conclure que le nombre d'éléments d'un ensemble $x_i H$ est donné par :

$$\frac{|G|}{k} = |x_i H| = |H|$$

en d'autres mots, on obtient :

$$|H| \Big| |G|$$

□

Théorème 6.6.4 (Fermat)**.** *Supposons que p est premier, et $x \in \mathbb{Z}$ tel que $(x,p) = 1$. Alors*

$$x^{p-1} = 1 \ (mod\ p)$$

Démonstration. Premièrement, par définition du groupe $\mathbb{Z}_p^\times$, nous savons que $|\mathbb{Z}_p^\times| = p-1$. De plus, nous savons que si $x \in \{1,2,3,...,p-1\}$, alors nous avons vu que $\langle x \rangle$ est un sous groupe de $\mathbb{Z}_p^\times$. Nous allons chercher combien d'éléments sont dans $\langle x \rangle$. Nous avons déjà vu qu'il existe un plus petit entier $n > 1$ tel que $x^n = 1 \pmod p$. On veut maintenant montrer que tous les éléments de $\{1, x, x^2, x^3, ..., x^{n-1}\}$ sont distincts. Pour ce faire, remarquons que si $x^i = x^j$ avec $0 < i, j < n$, $i > j$, alors on a :

$$\begin{aligned} x^i &= x^j \\ x^j x^{i-j} &= x^j \cdot 1 \\ x^{i-j} &= 1 \end{aligned}$$

On a donc trouvé un élément x^{i-j} tel que $x^{i-j} = 1$ et $0 < i - j < n$, ce qui contredit la minimalité de n. On peut donc conclure que $\langle x \rangle$ contient exactement n éléments. Maintenant par le théorème de Lagrange, on sait que le nombre d'éléments de $\langle x \rangle$ divise le nombre d'éléments de $\mathbb{Z}_p^\times$. En d'autre mot, $n|(p-1)$. Il existe donc un entier k tel que $nk = p-1$, ce qui nous permet d'obtenir :

$$x^{p-1} = x^{nk} = (x^n)^k = 1^k = 1 \pmod p$$

Ce qui complète la démonstration. □

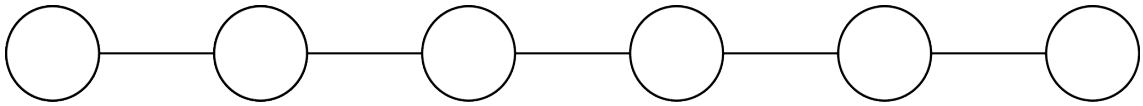
Ce que nous avons vu dans cet appendice n'est en fait qu'un aperçu de l'utilisation de l'algèbre en théorie des nombres. Nous pouvons en fait aller beaucoup plus loin et montrer que l'ensemble des nombres modulo p, où p est un nombre premier forme en fait ce que l'on appelle un corps commutatif (une sorte de groupe ayant 2 opérations plutôt qu'une seule). Nous pouvons définir un concept similaire à celui des nombres premiers que l'on appelle les idéaux premiers. Nous pouvons alors faire correspondre plusieurs idées de théorie des nombres en concept algébrique (i.e. groupe, anneaux, corps,...).

Appendice 2 : Petit théorème de Fermat version combinatoire

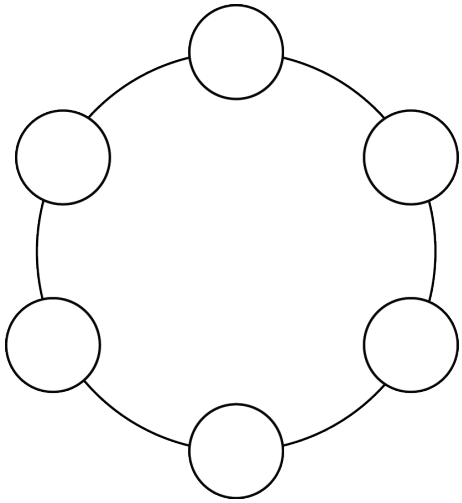
Dans cet appendice, nous allons maintenant regarder une 3e démonstration du petit théorème de Fermat (La première ayant été donné dans le chapitre 2, et la seconde dans l'appendice précédent). Cette fois, nous allons cependant regarder une approche très différente. Il s'agit d'une approche combinatoire, en comptant des colliers.

Théorème 7.6.5. *Si p est un nombre premier, et $x \in \{1, 2, 3, ..., p-1\}$, alors $p|(x^p - x)$.*

Démonstration. On veut savoir combien de colliers différents on peut faire de colliers contenant p perles sachant qu'on a des perles de x couleurs différentes. Pour ce faire, commençons par calculer le nombre de chaines que l'on peut faire :



On a donc x^p chaines que l'on peut faire. Exactement x d'entre elles sont d'une seule couleur. Maintenant considérons des colliers proprement dit en réunissant les deux extrémités.



Nous avons bien sûr x colliers différents ayant une unique couleur. Nous allons donc supposer que nos colliers sont d'au minimum 2 couleurs différentes. Dans ce cas, on remarque qu'en appliquant une rotation à notre collier, il s'agit toujours du même collier, même si sur papier il peut sembler différent. Donc pour chacun des $x^p - x$ colliers ayant au minimum deux couleurs, p d'entre eux sont identiques (les p rotations). Ici on a utilisé le fait que p est un nombre premier, autrement il y aurait plus que p colliers identiques. Il doit donc y avoir

$$\frac{x^p - x}{p}$$

colliers ayant au minimum deux couleurs. Le nombre $x^p - x$ doit donc être divisible par p. □

Théorème 7.6.6. *Si p est un nombre premier et $(x,p) = 1$, alors $x^{p-1} = 1$ $(mod\ p)$.*

Démonstration. En travaillant modulo p, on peut supposer que $x \in \{1,2,3,...,p-1\}$. Par le théorème précédent, nous savons que $p|(x^p - x)$. On a donc que $x^p = x \pmod p$. Ce qui nous donne $x^{p-1}x = x \pmod p$. Maintenant, comme $(x,p) = 1$, on peut simplifier le x, ce qui nous donne finalement le résultat :

$$x^{p-1} = 1 \pmod p$$

□

Appendice 3 : Différence finie

Supposons que f est une fonction $f : \mathbb{R} \to \mathbb{R}$. Si $h \in \mathbb{R}$ est une constante, alors on appelle $\Delta_h f(x)$ la différence finie et on définit $\Delta_h f(x)$ comme étant :

$$\Delta_h f(x) = f(x+h) - f(x)$$

Notons que si p est un polynôme, alors $\Delta_h p(x)$ est aussi un polynôme. Maintenant, si k est un entier, alors on définit $\Delta_h^k f(x)$ récursivement comme étant :

$$\Delta_h^k f(x) = \Delta_h \left(\Delta_h^{k-1} f(x)\right) \text{ où } \Delta_h^1 f(x) = \Delta_h f(x)$$

On appelle cette dernière k-ième différence finie.

Lemme 8.6.1. *Supposons que $p(x)$ est un polynôme de degré n, alors $\Delta_h p(x)$ est un polynôme de degré $n-1$*

Démonstration. Prenons $p(x)$ un polynôme de degré n tel que :

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 = a_n x^n + q(x)$$

où $q(x)$ est un polynôme de degré $n-1$. Alors on a :

$$\begin{aligned}
\Delta_h p(x) &= p(x+h) - p(x) \\
&= (a_n(x+h)^n + q(x+h)) - (a_n x^n + q(x)) \\
&= a_n\left((x+h)^n - x^n\right) + (q(x+h) - q(x)) \\
&= a_n\left[\left(\sum_{i=0}^{n}\binom{n}{i}x^i h^{n-i}\right) - x^n\right] + (q(x+h) - q(x)) \\
&= a_n\left(\sum_{i=0}^{n-1}\binom{n}{i}x^i h^{n-i}\right) + (q(x+h) - q(x))
\end{aligned}$$

Comme la partie de gauche est un polynôme de degré $n-1$ et la partie de droite est la différence entre deux polynôme de degré $n-1$, qui est un polynôme de degré $n-1$. On obtient donc la conclusion. □

Lemme 8.6.2. *Supposons que $p(x)$ est un polynôme de degré n, alors $\Delta_h^k p(x)$ est un polynôme de degré $n-k$. En particulier $\Delta_h^n p(x)$ est une constante.*

Démonstration. La preuve se fait par induction. Nous avons déjà démontrer que si $p(x)$ est un polynôme de degré n, alors $\Delta_h^1 p(x)$ est un polynôme de degré $n-1$. Supposons maintenant que $\Delta_h^k p(x)$ est un polynôme de degré $n-k$, alors

$$\Delta_h^{k+1} p(x) = \Delta_h\left(\Delta_h^k p(x)\right)$$

est un polynôme de degré $n-k-1$ en utilisant le lemme précédent car $\Delta_h^k p(x)$ est un polynôme de degré $n-k$. □

Lemme 8.6.3. *Supposons que $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ est un polynôme de degré n, alors $\Delta_h^n p(x) = a_n n!$.*

Démonstration. Prenons $p(x)$ un polynôme de degré n tel que :

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0 = a_n x^n + q(x)$$

où $q(x)$ est un polynôme de degré $n-1$. Alors on a :

$$\begin{aligned}
\Delta_h p(x) &= p(x+h) - p(x) \\
&= (a_n(x+h)^n + q(x+h)) - (a_n x^n + q(x)) \\
&= a_n\left((x+h)^n - x^n\right) + (q(x+h) - q(x)) \\
&= a_n\left((x+h)^n - x^n\right) + \Delta_h q(x) \\
&= a_n\left[\left(\sum_{i=0}^{n}\binom{n}{i}x^i h^{n-i}\right) - x^n\right] + \Delta_h q(x) \\
&= a_n\left(\sum_{i=0}^{n-1}\binom{n}{i}x^i h^{n-i}\right) + \Delta_h q(x) \\
&= a_n n x^{n-1} + a_n\left(\sum_{i=0}^{n-2}\binom{n}{i}x^i h^{n-i}\right) + \Delta_h q(x) \\
&= a_n n x^{n-1} + r(x) + \Delta_h q(x)
\end{aligned}$$

où $r(x)$ et $\Delta_h q(x)$ sont des polynômes de degré $n-2$. En répétant les mêmes étapes, on obtient donc :

$$\Delta_h^2 p(x) = \Delta_h(\Delta_h p(x)) = \Delta_h(a_n n x^{n-1} + r(x) + \Delta_h q(x)) = a_n n(n-1)x^{n-2} + w(x)$$

où $w(x)$ est un polynôme de degré $n-3$. On continue ensuite de la même manière (preuve par induction) pour obtenir :

$$\Delta_h^n p(x) = a_n n(n-1)(n-2)(n-3)...3\cdot 2\cdot 1 = a_n n!$$

□

Considérons maintenant un ensemble

$$S = \{a_1, a_2, a_3, ..., a_n\}$$

Alors on définit un ensemble ΔS comme étant :

$$\Delta S = \{a_2 - a_1, a_3 - a_2, a_4 - a_3, a_5 - a_4, ..., a_n - a_{n-1}\}$$

Et on définit à nouveau récursivement $\Delta^k S$ comme étant :

$$\Delta^k S = \Delta(\Delta^{k-1}S), \qquad \Delta^1 S = \Delta S$$

Théorème 8.6.7. (Théorème des différences finies) Supposons que k et n sont des entiers tels que $n \geq k$, et considérons l'ensemble

$$S = \{1^k, 2^k, 3^k, 4^k, ..., n^k\}$$

Alors

$$\Delta^k S = \{k!, k!, k!, ..., k!\}$$

Démonstration. Considérons le polynôme $p(x) = x^k$. On remarque que $p(x)$ est un polynôme de degré k et que l'ensemble S peut alors s'écrire sous la forme :

$$S = \{p(1), p(2), p(3), p(4), ..., p(n)\}$$

On obtient donc que :

$$\Delta S = \{2^k - 1^k, 3^k - 2^k, ..., n^k - (n-1)^k\} = \{\Delta_1 p(1), \Delta_1 p(2), ..., \Delta_1 p(n-1)\}$$

Par induction, on peut donc obtenir que :

$$\Delta^m S = \{\Delta_1^m p(1), \Delta_1^m p(2), ..., \Delta_1^m p(n-m)\}$$

En particulier si $m = k$, par le lemme précédent on obtient :

$$\Delta^k S = \{\Delta_1^k p(1), \Delta_1^k p(2), ..., \Delta_1^k p(n-k)\} = \{k!, k!, k!, ..., k!\}$$

□

Remarquons maintenant qu'il y a une analogie importante à faire entre la dérivée d'une fonction et les différences finies. Si $f(x)$ est une fonction, alors il est facile de voir que :

$$f'(x) = \lim_{h \to 0} \frac{f(x+h) - f(x)}{h} = \lim_{h \to 0} \frac{1}{h} \Delta_h f(x)$$

En particulier, si $h = 1$, on a que :

$$f'(x) \approx \Delta_1 f(x)$$

Supposons maintenant que $p(x)$ est un polynôme de degré n,

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0,$$

alors on se souvient des cours de calcul que :

$$\begin{aligned}
p'(x) &= a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + ... + 2a_2 x + a_1 \\
p''(x) &= a_n n(n-1)x^{n-2} + a_{n-1}(n-1)(n-2)x^{n-3} + ... + 3 \cdot 2x + 2a_2 \\
p'''(x) &= a_n n(n-1)(n-2)x^{n-3} + a_{n-1}(n-1)(n-2)(n-3)x^{n^4} + ... + 4!x + 3!a_3 \\
... &= ... \\
p^{(n)}(x) &= n! a_n
\end{aligned}$$

On remarque donc que

$$p^{(n)}(x) = \Delta_h^n p(x)$$

Donc le théorème que nous avons démontré n'est en fait rien d'autre qu'une analogie entre la n-ième dérivée d'un polynôme de degré n et la n-ième différence finie de ce même polynôme.

Bibliographie

[1] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, New York, 1976. Undergraduate Texts in Mathematics.

[2] Jean-Marie De Koninck and Armel Mercier. *Introduction à la théorie des nombres.* Modulo, 1994.

[3] Jean-Marie De Koninck and Armel Mercier. *1001 problems in classical number theory.* American Mathematical Society, Providence, RI, 2007. Translated from the 2004 French original by De Koninck.

[4] Euclid. *Euclid's Elements.* Green Lion Press, Santa Fe, NM, 2002. All thirteen books complete in one volume, The Thomas L. Heath translation, Edited by Dana Densmore.

[5] Edmund Landau. *Foundations of analysis.* AMS Chelsea Publishing, 1966.

[6] Calvin T. Long. *Elementary introduction to number theory.* Prentice Hall Inc., Englewood Cliffs, NJ, third edition, 1987.

[7] James E. Shockley. *Introduction to number theory.* Holt, Rinehart and Winston, Inc., New York, 1967.

Index

Algorithme d'Euclide, 18
Axiome d'induction, 8
Axiome de complétude, 10
Axiome de Peano, 8
Axiome du bon ordre, 9

Babylonien, 5
Baton d'Ishango, 5
Brahmagupta, 6

Cloture algébrique, 10
Crible d'Ératosthène, 25

Diophante, 5
Division euclidienne, 15

Euclide, 5

Fermat, 6
Fonctions additives, 53
Fonctions complètement additives, 53
Fonctions complètement multiplicatives, 53
Fonctions multiplicatives, 53
Formule d'inversion de Mobiüs, 54

Inégalités de Tchebycheff, 64

Lemme d'Euclide, 20
Lemme de Gauss, 91
Loi complémentaire (Deuxième), 90
Loi complémentaire (Première), 89
Loi de réciprocité quadratique de Gauss, 93

Mathématiques chinoise, 6
Mathématiques indienne, 6

Nombre abondant, 67
Nombre copremier, 20
Nombre déficient, 67
Nombre parfait, 65, 67
Nombre premier d'Euclide, 25
Nombre premier de Mersenne, 66
Nombres amicaux, 67
Nombres complexes, 10
Nombres entiers, 9
Nombres naturels, 8
Nombres réels, 10
Nombres rationnels, 9

Plus grand commun diviseur, 17
Plus petit commun multiple, 21
Postulat de Bertrand, 65
Principe d'induction, 10
Principe d'induction généralisé, 12
Produit de Dirichlet, 53
Pythagore, 5

Théorème des 4 carrés de Lagrange, 83
Théorème des deux carrés de Fermat, 78, 81
Théorème des différences finies, 106
Théorie des nombres élémentaires, 6
Théorie des nombres algébriques, 6
Théorie des nombres analytiques, 6