République Algérienne Démocratique et Populaire
Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de L'informatique
Département de Mathématiques

MEMOIRE DE FIN D'ETUDE

Présenté pour l'obtention du Diplôme de **MASTER**

Domaine : Mathématiques et Informatique

Filière : Mathématiques

Option : Algèbre et Mathématiques Discrètes

Par

AHLAM Hamlaoui

Sujet

Divisibilité et Congruence

Date de soutenance : 19/06/2018.

Devant le jury :

Mr. D. MIHOUBI	Prof. Univ de M'sila	Président
Mr. A. BOUDAOUD	Prof. Univ de M'sila	Rapporteur
Mr. S. MILLES	MCB. Univ de M'sila	Examinateur

Promotion : 2017 / 2018

Résumé :

Dans ce mémoire de Master on étudie la divisibilité et la congruence, on utilisé quelques principes fondamentaux que l'on trouve au début de la plupart des livres de théorie des nombres. Il s'agit, plus précisément, de l'Axiome de bon ordre, le Principe d'induction mathématique et le Principe de Tiroirs ainsi que les coefficients binomiaux.

Ensuit, on consacré à la notion de la divisibilité et les autres concepts connexes tels que : nombre premier, plus grand commun diviseur, plus petit commun multiple, algorithme d'Euclide, fractions continues et équations diophantiennes linéaires.

Enfin, on a étudié les grands théorèmes liés à la congruence tels que le théorème de Wilson, le théorème d'Euler, le théorème de Fermat (le petit théorème) et le théorème de reste Chinois.

Mots clés : **Arithmétique, Division euclidienne, Nombre premier, Algorithme d'Euclide.**

Abstract:

In this memoire of Master we have studied the divisibility and the congruence, we use some basic principles, which found at the beginning of most number theory books. It is, more precisely, the well-ordering principle, the mathematical induction principle, the pigeonhole principle and the binomial coefficients.

Next, is devoted to the notion of divisibility and other related concepts such as: prime number, greatest common divisor, least common multiple, Euclid's algorithm, continued fractions and linear diophantine equations.

Finally, we have studied the great theorems related to congruence such as Wilson's theorem, Euler's theorem, Fermat's theorem (the small theorem) and the Chinese remainder theorem.

Key words : **Arithmetic, Euclidean division, Prime number, Euclidean Algorithm.**

الملخص :

في هذه مذكرة الماستر قمنا بدراسة حول قابلية القسمة و الموافقات, استعملنا بعض الأساسيات المهمة التي نجدها في اغلب كتب نظرية الأعداد ويتعلق الأمر ببديهية الترتيب الجيد, مبدأ الرياضي للتراجع ومبدأ الدرج بالإضافة إلى المعاملات ذات حدين.

في التالي تطرقنا إلى مفهوم القسمة والمفاهيم المحيط بها منها الأعداد الأولية, القاسم المشترك الأكبر, المضاعف المشترك الأصغر, خوارزمية أوكليد , الكسور المستمرة, معادلات ديوفانتاين الخطية.

في الأخير درسنا النظريات الكبرى المتعلقة بالموافقات منها نظرية ويلسن, نظرية اولر, نظرية فارما الصغيرة, نظرية البواقي الصينية.

الكلمات المفتاحية : الحساب, القسمة الإقليدية, العدد الأولي , خوارزمية أوكليد.

Remerciements

Je remercie tout d'abord mon Dieu qui m'a donné la force pour terminer ce modeste travail.

*Je tiens à remercier mon promoteur : le docteur **A. Boudaoud** pour les conseils donnés et la confiance qu'il m'a témoignée en me proposant ce sujet, ses encouragements et sa patience.*

Je remercie tous les membres du jury pour l'honneur qu'il mon fait en acceptant de juger ce travail.

A la fin je remercie tous qui m'ont ceux aidé de prés ou de loin, et surtout ma famille qui m'a accompagné tout au long de mon étude.

Merci

Divisibilité et congruence

Hamlaoui Ahlam

29 juin 2018

Table des matières

Introduction

Dans la littérature mathématique la branche appelée « Théorie des nombres » s'intéresse à l'étude des entiers naturels et leurs propriétés. La notion la plus fondamentale dans cette branche est « Divisibilité » car toutes les autres notions sont définies moyennant cette dernière, par exemple on la trouve pour définir : nombre premier, la congruence, fonction arithmétique, équation diophantienne, ... La théorie des nombres s'applique dans des différents domaines, on cite ici, à titre d'exemple, le rôle essentiel que joue la congruence dans la cryptographie classique et moderne pour développer et sécuriser la communication électronique.

Les problèmes dans cette branche sont caractérisés par le fait qu'ils sont simples dans leurs formulation mais qui nécessitent beaucoup d'effort pour leur résolution. On cite ici, à titre d'exemple, le grand problème posé par *Pierre Fermat* $(1601-1665)$, à savoir l'équation $a^n + b^n = c^n$ qui n'a pas de solution en entiers naturels a, b, c, n dès que $n \geq 3$. Cette conjecture est devenue aujourd'hui un théorème après une longue démonstration par *Andrew Wiles* (Juin 1993).

L'objectif de ce mémiore est de présenter les notions élémentaires d'arithmétique.

Ce mémoire est réparti en trois chapitres :

Dans le premier chapitre : on présente des principes fondamentaux de raisonnement : axiome du bon ordre, principe d'induction mathématique, coefficients binomiaux, principe des Tiroirs. En plus on accompagne à ces notions quelques applications.

Dans le deuxième chapitre on traite les notions liées à la divisibilité telles que : nombre premier, plus grand commun diviseur, plus petit commun multiple, algorithme d'Euclide, fractions continues et équations diophantiennes linéaires.

Le troisième chapitre est consacré aux grands théorèmes liés à la congruence telle

que le théorème de Wilson, d'Euler, de Fermat (le petit théorème), de reste Chinois. Ce chapitre est aussi illustré par quelques applications.

Chapitre 1

Les principes fondamentaux de raisonnement

Dans tout la suite de ce travail nous noterons par $\mathbb{N}$ l'ensemble des entiers naturels $\{0, 1, 2, \ldots\}$. Et par $\mathbb{Z}$ l'ensemble des entiers $\{\ldots, -2, -1, 0, +1, +2, \ldots\}$.

1.1 Axiome du bon ordre

Axiome du bon ordre. Toute partie non vide de l'ensemble $\mathbb{N}$ a un plus petit élément.

Exemple 1.1 Démontrer qu'il n'existent pas d'entiers dans $]0, 1[$.

Solution 1.1 *Supposons le contraire i.e., qu'il existe un entiers dans* $]0, 1[$,

$$S = \{n \in \mathbb{N} \mid 0 < n < 1\} \neq \emptyset$$

avec $S \subset \mathbb{N}$. *Donc* S *a un plus petit élément* $m > 0$. *D'où* $0 < m^2 < m < 1$ *alors* m^2 *est un entier de* S *qui est inférieur strictement à* m, *contradiction.*

Exemple 1.2 Démontrer que $\sqrt{2}$ est un irrationnel.

Solution 1.2 *Supposons le contraire i.e.,* $\sqrt{2} = \dfrac{a}{b}$ *où* a *et* b *sont dans* $\mathbb{N}^*$. *Posons*

$$A = \left\{ n\sqrt{2} \mid n \text{ et } n\sqrt{2} \text{ sont des entiers positifs} \right\}.$$

$A \neq \emptyset$ car $a \in A$ et $A \subset \mathbb{N}$, par l'axiome du bon ordre A possède un plus petit élément $j = k\sqrt{2}$ où $k \in \mathbb{N}^*$

$$\begin{aligned} j(\sqrt{2}-1) &= j\sqrt{2} - j = j\sqrt{2} - k\sqrt{2}; \\ &= (j-k)\sqrt{2} \text{ est un entier positif.} \end{aligned}$$

Vu que $2 < 2\sqrt{2}$ implique $2 - \sqrt{2} < \sqrt{2}$ et $j\sqrt{2} = 2k$, nous avons

$$\begin{aligned} (j-k)\sqrt{2} &= (k\sqrt{2} - k)\sqrt{2} = (\sqrt{2}-1)k\sqrt{2}; \\ &= (2-\sqrt{2})k < k\sqrt{2} = j. \end{aligned}$$

D'où $(j-k)\sqrt{2} \in A$ et $(j-k)\sqrt{2} < j$, contradiction.

1.2 Principe d'induction mathématique

Théorème 1.3 (Principe d'induction mathématique) *Si S une partie d'entiers non négatifs contient 0, et aussi contient $n+1$ lorsque il contient l'entiers n. Alors $S = \mathbb{N}$.*

Preuve. Supposons que $S \neq \mathbb{N}$ ($S \subset \mathbb{N}$). Alors $\mathbb{N} \backslash S$ est un ensemble non vide d'entiers strictement positifs. D'après le principe de bon ordre $\mathbb{N} \backslash S$ admet un plus petit élément $k > 0$. Alors $k - 1 \geq 0$ appartient à S. Par hypothèse $(k-1) + 1 \in S$ i.e., $k \in S$, contradiction. Alors $S = \mathbb{N}$. ■

Corollaire 1.1 *Si A est un ensemble d'entier contient l'entier m et aussi contient $n+1$ lorsque il contient l'entiers n, où $n > m$, alors A contient tous les entiers positifs supérieur ou égal à m.*

Corollaire 1.2 *Si A est un ensemble d'entier contient l'entier m et aussi contient $n+1$ lorsque il contient $m+1, m+2, \ldots, n$, où $n > m$, alors A contient tous les entiers positifs supérieur ou égal à m.*

Exemple 1.3 Démontrer que si k est impair, alors 2^{n+2} divise $k^{2^n} - 1$ pour tout $n \geq 1$.

Solution 1.4 *Si* $n = 1$ *on a*

$$k^{2^1} - 1 = k^2 - 1 = (k-1)(k+1).$$

Comme k est impair, on pose $k = 2t + 1$, on distingue deux cas

a) $k = 2t + 1$ *où* $t = 2\tilde{t}$

$$\begin{aligned} k^2 - 1 &= (2t)(2t+1); \\ &= 4t(t+1); \\ &= 8\tilde{t}(t+1)\ . \end{aligned}$$

Donc $8 = 2^3 \mid k^2 - 1$.

b) $k = 2t + 1$ où $t = 2\tilde{t} + 1$

$$\begin{aligned} k^2 - 1 &= 2t(2t+1) = 4t(t+1); \\ &= 4t(2\tilde{t}+2) = 8t(\tilde{t}+1). \end{aligned}$$

Donc $8 = 2^3 \mid k^2 - 1$.
Supposons que $2^{n+2} \mid k^{2^n} - 1$ pour $n \geq 1$. Démontrons que $2^{n+3} \mid k^{2^{n+1}} - 1$ pour $n + 1$

$$\begin{aligned} k^{n+1} - 1 &= (k^{2^n})^2 - 1; \\ &= (k^{2^n} - 1)(k^{2^n} + 1). \end{aligned}$$

Par hypothèse $2^{n+2} \mid k^{2^n} - 1$;
d'autre par $2 \mid k^{2^n} + 1$, donc $(2^{n+2}) \times 2 \mid (k^{2^n} - 1)(k^{2^n} + 1)$
i.e., $2^{n+3} \mid k^{2^{n+1}} - 1$.

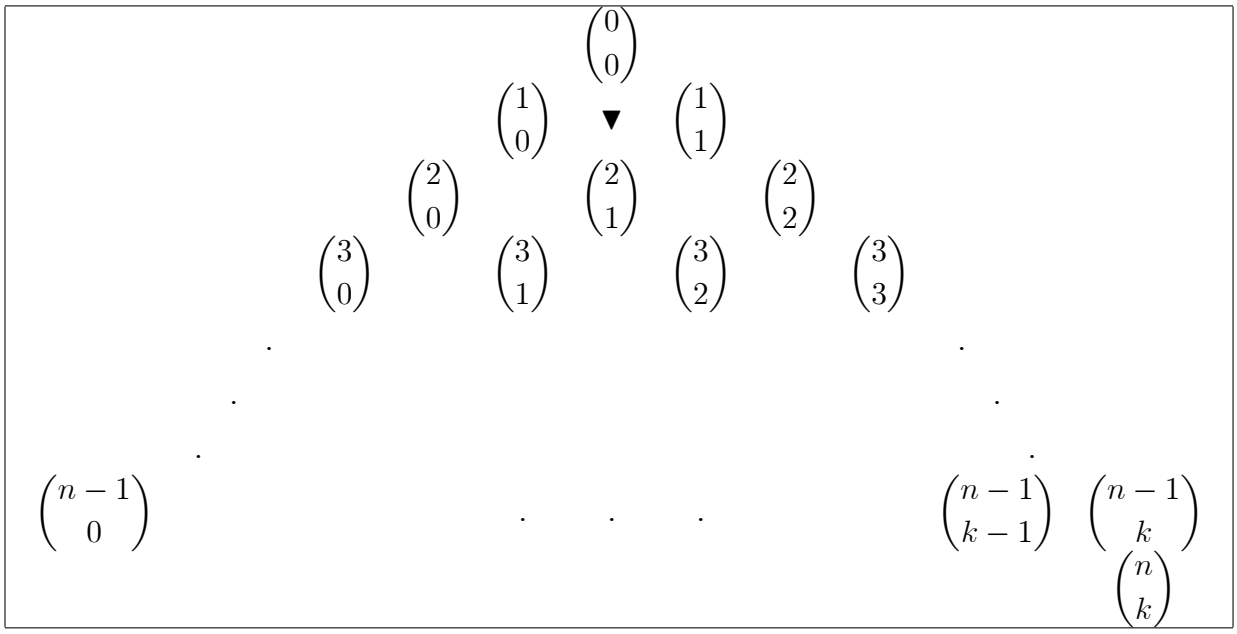
1.3 Coefficients binomiaux

Définition 1.1 (Coefficients binomiaux) Soit n un entier positif et k un entier satisfaisant $0 \leq k \leq n$. On définit

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

où $0! = 1$ et $n! = n(n-1)\cdots 3 \cdot 2 \cdot 1$.

Triangle de Pascal. Les différents coefficients binomiaux $\binom{n}{k}$, où $0 \leq k \leq n$, peuvent être disposés sous la forme d'un triangle, appelé triangle de Pascal, comme indique dans la figure suivant.



Théorème 1.5 (Binôme de Newton) *Soit a, $b \in \mathbb{R}$ et $n \in \mathbb{N}$. Alors*

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

Preuve. On démontre ce théorème par récurrence.

Pour $n = 0$

$$\begin{aligned}(a+b)^n &= (a+b)^0 = 1;\\ \sum_{k=0}^{0}\binom{0}{k}a^{0-k}b^k &= \binom{0}{0}a^0b^0 = 1.\end{aligned}$$

Supposons que le théorème est vrai pour n et démontrons-le pour $n+1$

$$\begin{aligned}(a+b)^n &= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k;\\ &= \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n.\end{aligned}$$

$$\begin{aligned}(a+b)^{n+1} &= (a+b)^n \cdot (a+b)\,;\\ &= \left[\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k\right]\cdot(a+b)\,;\\ &= \sum_{k=0}^{n}\binom{n}{k}a^{n+1-k}b^k + \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^{k+1};\\ &= \binom{n}{0}a^{n+1} + \binom{n}{1}a^nb + \cdots + \binom{n}{n}ab^n + \binom{n}{0}a^nb + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n}b^{n+1};\\ &= \binom{n}{0}a^{n+1} + \left[\binom{n}{0} + \binom{n}{1}\right]a^nb + \cdots + \left[\binom{n}{n-1} + \binom{n}{n}\right]ab^n + \cdots + \binom{n}{n}b^{n+1}.\end{aligned}$$

D'après le triangle de Pascal on a

$$\begin{aligned}\binom{n}{0} &= \binom{n+1}{0} = 1;\\ \binom{n}{n} &= \binom{n+1}{n+1} = 1;\\ \binom{n-1}{k-1} + \binom{n-1}{k} &= \binom{n}{k};\end{aligned}$$

où $0 \leq k \leq n$.

Donc

$$\begin{aligned}(a+b)^{n+1} &= \binom{n+1}{0}a^{n+1}b^0 + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}a^0 b^{n+1};\\ &= \sum_{k=0}^{n+1}\binom{n+1}{k}a^{(n+1)-k}b^k.\end{aligned}$$

■

Corollaire 1.3 *Soit n un entier non nul. Alors*

$$2^n = \sum_{k=0}^{n}\binom{n}{k}.$$

Preuve. On utilise le théorème 1.5 avec $x = 1$ et $y = 1$, donc

$$2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k}1^k = \sum_{k=0}^{n}\binom{n}{k}.$$

■

1.4 Principe des Tiroirs

Théorème 1.6 (Principe des Tiroirs) *Si plus de n objets sont distribués parmi n boîtes, alors une des boîtes contient au moins deux objets.*

Preuve. Nous prouvons le principe des Tiroirs en utilisant une preuve par contraposition. Supposons que chaque boîte contient au plus un objet. Alors le nombre total d'objet serait au plus n, contradiction. Car il y a au plus n objets. ■

Exercice 1.7 *Montrer que parmi* 51 *entiers positifs arbitraires, on peut en trouver deux dont la différence est divisible par* 50.

Solution 1.8 *Il y a exactement* 50 *restes possibles lorsqu'on divise les nombres par* 50 *et ce sont les nombres*: $0, 1, 2, \ldots, 49$. *Puisque l'on a* 51 *entiers et seulement* 50 *restes possibles, alors d'après le principe des tiroirs, il y a au moins deux nombres parmi ces* 51 *entiers qui ont le même reste. Alors la différence de ces deux entiers a pour reste* 0 *et est donc divisible par* 50.

Théorème 1.9 (Dirichlet, début XIXème) *Pour tout nombre réel x et tout entier $N \geq 2$ il existe deux entiers relatifs p et q tels que*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{qN}$$

avec $1 \leq q \leq N$.

Preuve. On considère l'ensemble finie suivant :

$$E = \{0 \cdot x - [0 \cdot x], 1.x - [1 \cdot x], \ldots, N \cdot x - [N \cdot x]\}$$

qui peut aussi être écrit comme suit $E = \{\{0 \cdot x\}, \{1 \cdot x\}, \ldots, \{N \cdot x\}\} \subset [0, 1]$. Dans ce cas on a N intervalles $\left[\frac{i}{N}, \frac{i+1}{N}\right]$ quand $0 \leq i \leq N-1$ et dans E on a $N+1$ réels. Alors d'après le principe des Tiroirs, il y a deux réels $px - [px]$ et $qx - [qx]$ de E qui sont dans le même intervalle. D'où

$$|px - [px] - (qx - [qx])| = |(p-q)\, x - l| \leq \frac{1}{N}, \text{ avec } l = [qx] - [px].$$

Ce qui implique

$$\begin{aligned} \left| x - \frac{l}{(p-q)} \right| &\leq \frac{1}{(p-q)\, N} \\ &= \left| x - \frac{P}{Q} \right| \leq \frac{1}{QN}, \text{ où } P = l,\ Q = p - q. \end{aligned}$$

■

Chapitre 2

Divisibilité

Diviseurs, multiples d'entiers, nombres premiers et composites, ... sont des notions qui ont été connus et étudies au moins depuis l'epoque d'Euclide, qui vivait à environ 350 B.C.

2.1 Division

Définition 2.1 Soient a et b deux entiers relatifs. On dit que a divise b (ou b est un multiple de a), et on note $a \mid b$, s'il existe un entier n tel que $b = an$. Si a ne divise pas b, on note $a \nmid b$.

Exemple 2.1 56 est un multiple de -8 car $56 = (-7) \times (-8)$.

Proposition 2.1 *Soient a, b et c trois entiers relatifs. Si a divise b et b divise c alors a divise c.*

Preuve. Si a divise b et b divise c alors il existe deux entiers k et $\tilde{k}$ tel que $b = ka$ et $c = \tilde{k}b$. Donc il existe un entier relatif $l = k\tilde{k}$ tel que $c = la$. D'où a divise c. ■

Exemple 2.2 3 divise 12 et 12 divise 36 alors 3 divise 36.

Proposition 2.2 (Combinaisons linéaires) *Soient a, b et c trois entiers relatifs. Si c divise a et b alors c divise $ma + nb$ où m et n sont deux entiers relatifs.*

Preuve. Si c divise a et b alors il existe deux entiers relatifs k et $\tilde{k}$ tel que $a = kc$ et $b = \tilde{k}c$. Donc il existe un entier relatif $l = mk + n\tilde{k}$ tel que $ma + nb = lc$. ■

Exemple 2.3 Soit un entier relatif N qui divise les entiers relatifs n et $n+1$. Alors N divise $n+1-n=1$. Donc $N=1$ ou $N=-1$.

2.2 Division euclidienne

Théorème 2.1 (Division euclidienne) *Soient a et d deux entiers avec $d \geq 1$. Il existe des entiers uniques q et r tels que*

$$a = dq + r \tag{2.1}$$

et

$$0 \leq r \leq d-1. \tag{2.2}$$

L'entier q est appelé le quotient et l'entier r appelé le reste dans la division de a par d.

Preuve. Considérons l'ensemble S des entiers non négatifs qui sont de la forme

$$a - dx$$

avec $x \in \mathbb{Z}$. Si $a \geq 0$, alors $a = a - d \cdot 0 \in S$. Si $a < 0$, soit $x = -y$, lorsque y est un entier positif. Puisque d est positif, nous avons $a - dx = a + dy \in S$ si y est suffisamment grand. Donc, S est un ensemble non vide d'entiers non négatifs. Par le principe de bon ordre, S contient un plus petit élément r, et $r = a - dq \geq 0$ pour certains $q \in \mathbb{Z}$. Si $r \geq d$, alors

$$0 \leq r - d = a - d(q+1) < r.$$

Et $r - d \in S$, ce qui contredit la minimalité de r. Donc, q et r satisfont aux conditions (2.1) et (2.2).

Soit q_1, r_1, q_2, r_2 des entiers tels que

$$a = dq_1 + r_1 = dq_2 + r_2 \qquad \text{et} \qquad 0 \leq r_1,\ r_2 \leq d-1.$$

Alors

$$| r_1 - r_2 | \leq d - 1$$

et

$$d(q_1 - q_2) = r_2 - r_1.$$

Si $q_1 \neq q_2$, alors

$$| q_1 - q_2 | \geq 1$$

et

$$d \leq d \mid q_1 - q_2 | = | r_2 - r_1 | \leq d - 1,$$

ce qui est impossible. Donc, $q_1 = q_2$ et $r_1 = r_2$. Alors le quotient et le reste sont uniques. ■

Exemple 2.4 La division euclidienne de 4412 par 15 est

$$4412 = 15 \times 294 + 2,$$

alors $q = 294$ et $r = 2$.

Définition 2.2 (Partie entière, partie fractionnaire) Soit $x \in \mathbb{R}$. La partie entière de x est l'unique entier, noté $[x]$ satisfaisant

$$x - 1 < [x] \leq x.$$

La partie fractionnaire de x est le réel, noté $\{x\}$, défini par $\{x\} = x - [x]$. D'après l'encadrement ci-dessus, on a donc

$$0 \leq \{x\} < 1.$$

Remarque 2.1 Cette définition de la partie entière est équivalente à

$$[x] \leq x \leq [x] + 1.$$

Exemple 2.5 $[2.5] = 2, \{8\} = 0,\ [-3.9] = -4, \left[\frac{3}{4}\right] = 0, \left\{\frac{3}{4}\right\} = \frac{3}{4},$
$[-\pi] = -4, \{-\pi\} = 0.8584073\ldots$

Théorème 2.2 *Soient x, $y \in \mathbb{R}$. Alors on a*

(i) $x = [x] + \theta$ *avec* $\theta \in [0, 1[$;

(ii) Soit $n \in \mathbb{Z}$. *Alors on a*

$$[x + n] = [x] + n \text{ et } \{x + n\} = \{x\} ;$$

(iii)

$$[x] + [y] \leq [x + y] \leq [x] + [y] + 1.$$

Preuve. *(i)* Il suffit d'écrire $x = [x] + \{x\}$ avec $0 \leq \{x\} < 1$.
(ii) On a $[x + n] = x + n + \theta_1$ et $[x] = x + \theta_2$ avec $-1 < \theta_i \leq 0$. Alors

$$[x + n] - ([x] + n) = \theta_1 - \theta_2 \in]-1, 1[,$$

et comme $[x + n] - ([x] + n) \in \mathbb{Z}$, on obtient $[x + n] - ([x] + n) = 0$.
Pour l'autre égalité, on utilise ce qui précède

$$\{x + n\} = x + n - [x + n] = x - [x] = \{x\} .$$

(iii) D'une part, d'après *(ii)*, on a

$$[x] + [y] = [[x] + y] \leq [x + y].$$

D'autre part, si $x = [x] + \theta_1$ et $y = [y] + \theta_2$ avec $0 \leq \theta_i < 1$, alors on a

$$[x + y] = [[x] + [y] + \theta_1 + \theta_2] = [x] + [y] + [\theta_1 + \theta_2] \leq [x] + [y] + 1,$$

puisque $0 \leq \theta_1 + \theta_2 < 2$. Ceci implique $[\theta_1 + \theta_2] = 0$ ou 1. ■

2.3 Nombre premier et plus grand commun diviseur

2.3.1 Nombre premier

Définition 2.3 (Nombre premier) Un nombre premier est un entier strictement supérieur à 1 qui n'est divisible que par 1 et par lui-même.

Exemple 2.6 Ainsi, 2 est le plus petit nombre premier et l'unique qui est pair.

Théorème 2.3 (Euclide) *Il existe une infinité d'entiers premiers.*

Preuve d'Euclide. Supposons que

$$p_1 = 2 < p_2 = 3 < \cdots < p_r.$$

Sont tous les nombres premiers, posons $p = p_1 p_2 \dots p_r + 1$. Alors ou bien p est premier et donc $p > p_i$, pour tout $i = \{1, 2, \dots, r\}$, ou p n'est pas premier et dans ce cas il existe un premier $\tilde{p} \mid p$ et $\tilde{p}$ différent de tous les p_i $(i = 1, 2, \dots, r)$. D'ou la liste $p_1, p_2, \dots, p_r$ ne contient pas tous les premiers. ■

Remarque 2.2 Comme il y a plusieurs preuves pour le théorème d'Euclide on va proposer dans la suite une autre preuve.

Preuve de Pólya. (voir Pólya & Szegö, 1924) Utilise l'idée suivante : il suffit de trouver une suite infinie des nombres naturels $1 < a_1 < a_2 < \cdots$ qui sont deux à deux premiers entre eux, dans ce cas si p_1 premier divise a_1, si p_2 premier divise a_2, etc., alors on a une infinité d'entiers premiers $p_1, p_2, \dots, ..$ qui sont tous différents.

Pour cette preuve, les nombres a_n que l'on choisis sont ceux de Fermat donnés par $F_n = 2^{2^n} + 1$ $(n \geq 0)$. En effet, il est facile de voir, par récurrence sur m, que $F_m - 2 = F_0 F_1 \cdots F_{m-1}$. D'où si $n < m$, alors F_n divise $F_m - 2$.

Si p premier divisant à la fois F_n et F_m, alors p divise $F_m - 2$ et F_m. Par conséquent p doit être égale à 2. Mais comme F_n est impair, F_n ne peut être divisible par 2. Ce qui montre que les nombres de Fermat sont deux à deux premiers entre eux. ■

2.3.2 Crible d'Eratosthène

Méthode crible d'Eratosthène. Soit n un entier donné. On écrit la liste des n premiers entiers naturels non nuls. On éliminé 1, les multiples de 2 plus grand que 2. Dans une étape intermédiaire on éliminé les multiples du plus petit nombre premier p restant et qui est supérieur à p. Il suffit faire ceci par $p^2 < n$. Ainsi, les multiples de $2, 3, 5, 7 < \sqrt{100}$ sont éliminés. Alors les premiers inférieurs à 100 sont $2, 3, 5, 7$.

Exemple 2.7 $n = 100$

1	**2**	**3**	4	**5**	6	**7**	8	9	10
11	12	**13**	14	15	16	**17**	18	**19**	20
21	22	**23**	24	25	26	27	28	**29**	30
31	32	33	34	35	36	**37**	38	39	40
41	42	**43**	44	45	46	**47**	48	49	50
51	52	**53**	54	55	56	57	58	**59**	60
61	62	63	64	65	66	**67**	68	69	70
71	72	**73**	74	75	76	77	78	**79**	80
81	82	**83**	84	85	86	87	88	**89**	90
91	92	93	94	95	96	**97**	98	99	100

Les nombres en gras sont les nombres premiers inférieurs ou égaux à 100.

2.3.3 Plus grand commun diviseur et plus petit commun multiple

Plus grand commun diviseur

Définition 2.4 Soient a et b deux entiers non nuls. Le plus grand commun diviseur de a et b, noté par $pgcd(a, b)$ ou simplement (a, b), est le plus grand entier d tel que $d \mid a$ et $d \mid b$.

Exemple 2.8 $pgcd(4, 12) = pgcd(12, 4) = pgcd(-4, -12) = pgcd(-4, -12) = 4$, $pgcd(3, 5) = 1$, $pgcd(12, 15) = 3$.

Définition 2.5 Les entiers $a_1, a_2, \ldots, a_k$ sont appelés relativement premiers si

$$(a_1, a_2, ..., a_k) = 1.$$

Les entiers $a_1, a_2, \ldots, a_k$ sont appelés deux à deux relativement premiers si

$$(a_i, a_j) = 1, \ \forall i \neq j.$$

Exemple 2.9 $(6, 10, 15) = 1$, mais $(6, 10) = 2$, $(10, 15) = 5$, $(6, 15) = 3$.

Théorème 2.4 (Bachet-Bézout) *Le plus grand commun diviseur de deux entiers non nuls a et b peut s'écrire comme combinaisons linéaire de a et b, i.e., il existe deux entiers x et y tel que*

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

Preuve. Soit $A = \{ax + by \mid ax + by > 0, \ x, \ y \in \mathbb{Z}\}$. Il est claire que l'on $\pm a, \pm b$ est dans A, avec a et b non nul. Par le principe de bon ordre, A contient un plus petit élément d. Donc, il existe x_0, y_0 tel que $d = ax_0 + by_0$. Nous prouvons que $d = (a, b)$. Nous prouvons que $d \mid a$, $d \mid b$ et que $t \mid a$, $t \mid b$ alors $t \mid d$.

Premièrement nous montrons que $d \mid a$. Par la division euclidienne, peut être trouvé des entiers q, r avec $0 \leq r < d$ tel que $a = dq + r$. Alors

$$r = a - dq = a(1 - qx_0) - bqy_0.$$

Si $r > 0$, donc $r \in A$. Si $r \in A$, alors r est le plus petit élément de A, contradiction. Donc $r = 0$. On écrit $dq = a$, i.e., $d \mid a$. De même manière on démontre que $d \mid b$.

Supposons que $t \mid a$, $t \mid b$. Alors $a = tm$, $b = tn$ pour m, n des entiers. Donc $d = ax_0 + by_0 = t(mx_0 + ny_0)$, ce qui implique $t \mid d$. ■

Théorème 2.5 (Lemme d'Euclide) *Soient a, b et c des entiers si a divise bc et $(a, b) = 1$ alors a divise c.*

Preuve. Si $(a, b) = 1$, par le théorème de Bézout il existe des entiers x, y avec $ax + by = 1$. Puisque $a \mid bc$, il existe un entier s tel que $as = bc$. Alors $c = c \cdot 1 = cax + cby = cax + asy$, donc il découle que $a \mid c$. ■

Théorème 2.6 *Soit $k \geq 2$, et soient $a, b_1, b_2, \ldots, b_k$ des entiers. Si $(a, b_i) = 1$ pour tout $i = 1, \ldots, k$, alors $(a, b_1 b_2 \cdots b_k) = 1$.*

Preuve. Soit $k = 2$ et $d = (a, b_1 b_2)$. Nous montrons que $d = 1$. Du fait que d divise a et $(a, b_1) = 1$, il découle que $(d, b_1) = 1$. Du fait que d divise $b_1 b_2$, on a d'après lemme d'Euclide d divise b_2. Donc, d est un diviseur commun de a et b_2. Vu que $(a, b_2) = 1$ et alors $d = 1$.

Soit $k \geq 3$, supposons que le résultat détient pour $k-1$. Soient $a, b_1, b_2, \ldots, b_k$ sont des entiers tel que $(a, b_i) = 1$ pour $i = 1, \ldots, k$. De hypothèse on a $(a, b_1 b_2 \cdots b_{k-1}) = 1$. Comme nous avons aussi $(a, b_k) = 1$, il découle à partir le cas $k = 2$ que $(a, b_1 b_2 \cdots b_{k-1} b_k) = 1$. ■

Théorème 2.7 *Si p un nombre premier divise un produit d'entiers, alors p divise l'un des facteurs.*

Preuve. Soient $b_1, b_2, \ldots, b_k$ des entiers tels que p divise $b_1 b_2 \cdots b_k$. Par le théorème 2.6**,** on a $(p, b_i) > 1$ pour certains i. Puisque p est premier, donc p divise b_i. ■

Théorème 2.8 (Théorème fondamental de l'arithmétique) *Tout entier positif peut être écrit uniquement (à ordre prés) comme le produit des nombres premiers.*

Preuve. D'abord, nous prouvons que l'entier positif peut être écrit comme un produit de nombres premiers. Puisqu'un produit vide est égal à 1, nous pouvons écrire 1 comme le produit vide des nombres premiers. Soit $n \geq 2$, supposons que tout entier positif inférieur à n est un produit des nombres premiers. Si n est premier, nous avons fini. Si n est composite, alors $n = d\tilde{d}$, où $1 < d \leq \tilde{d} < n$. Par l'hypothèse de récurrence, d et $\tilde{d}$ sont tous deux des produits de nombres premiers, et donc $n = d\tilde{d}$ est un produit de nombres premiers.

Dans la suite nous allons utiliser le principe de récurrence pour démontrer que cette représentation est unique. La représentation 1 comme le produit de l'ensemble vide des premiers est unique.
Soit $n \geq 2$, supposons que la représentation est unique pour tout entier positif inférieur ou égal à n. Maintenant nous montrons que si

$$n = p_1 \cdots p_k = \tilde{p}_1 \cdots \tilde{p}_l,$$

où $p_1, \ldots, p_k$, $\tilde{p}_1, \ldots, \tilde{p}_l$ sont des premiers, donc $k = l$ et il existe une permutation σ de $\{1, \ldots, k\}$ telle que $p_i = \tilde{p}_{\sigma(i)}$ pour $i = 1, \ldots, k$. Par le théorème 2.7, du fait que p_k divise $\tilde{p}_1 \cdots \tilde{p}_l$, il existe un entier $j_0 \in \{1, \ldots, l\}$ tel que p_k divise $\tilde{p}_{j_0}$, d'où $p_k = \tilde{p}_{j_0}$ du fait que $\tilde{p}_{j_0}$ est premier. Donc

$$\frac{n}{p_k} = p_1 \cdots p_{k-1} = \prod_{\substack{j=1 \\ j \neq j_0}}^{l} \tilde{p}_j < n.$$

Il découle, de l'hypothèse de récurrence $k - 1 = l - 1$, et il existe une application injectif de

$$\sigma : \{1, \ldots, k-1\} \longrightarrow \{1, \ldots, k\} \setminus \{j_0\}$$

telle que $p_i = \tilde{p}_{\sigma(i)}$ pour $i = 1, \ldots, k-1$. Posons $\sigma(k) = j_0$. Ceci déterminer la permutation σ, et terminer la preuve. ■

Exercice 2.9 *Ecrivez les nombres 3850 et 1911 sous forme de produits de nombres premiers.*

Solution 2.10 $3850 = 2 \times 5^2 \times 7 \times 11$,

$1911 = 3 \times 7^2 \times 13$.

Plus petit commun multiple

Définition 2.6 (Plus petit commun multiple) Soit $a_1, a_2, \ldots, a_r \in \mathbb{Z} \setminus \{0\}$. Le plus petit commun multiple (ou simplement ppcm*)* de $a_1, a_2, \ldots, a_r$ noté $[a_1, a_2, \ldots, a_r]$ est le plus petit entier positif, parmi tous les commun multiple de $a_1, a_2, \ldots, a_r$.

Exemple 2.10 $102 = 2 \cdot 3 \cdot 17$ et $138 = 2 \cdot 3 \cdot 23$, donc $ppcm(102, 138) = 2 \cdot 3 \cdot 17 \cdot 23 = 2346$.

Théorème 2.11 *Si $q_1, q_2, \ldots, q_r$ sont des nombres premiers et si $a = \Pi_{i=1}^{r} q_i^{\alpha_i}$ et $b = \Pi_{i=1}^{r} q_i^{\beta_i}$, avec $\alpha_i \geq 0$ et $\beta_i \geq 0$ pour $i = 1, 2, \ldots, r$, alors*

$$(a, b) = \prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i)} \text{ et } [a, b] = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i)}.$$

De même, si $a = \Pi q_i^{\alpha_i}$, $b = \Pi q_i^{\beta_i}$, $c = \Pi q_i^{\gamma_i}$ *avec* $\alpha_i \geq 0$, $\beta_i \geq 0$ *et* $\gamma_i \geq 0$ *pour* $i = 1, 2, \ldots, r$, *alors*

$$(a, b, c) = \prod_{i=1}^{r} q_i^{\min(\alpha_i, \beta_i, \gamma_i)} \text{ et } [a, b, c] = \prod_{i=1}^{r} q_i^{\max(\alpha_i, \beta_i, \gamma_i)}.$$

Exemple 2.11 Si $a = 108$ et $b = 225$, alors

$a = 2^2 3^3 5^0$, $b = 2^0 3^2 5^2$,

$(a, b) = 2^0 3^2 5^0 = 9$, $[a, b] = 2^2 3^3 5^2 = 2700$.

Théorème 2.12 *Soient* a, b, c, $k \in \mathbb{Z}^*$

(1) $ppcm(a, b) = ppcm(b, a)$ ou bien on écrit $[a, b] = [b, a]$;

(2) $ppcm(ka, kb) = |k| \cdot ppcm(a, b)$;

(3) Si a divise M et b divise M, alors

$$ppcm(a, b) \mid M.$$

Preuve. (1) Claire d'après la définition.

(2) Soient $m_1 = ppcm(a, b)$ et $m_2 = ppcm(ka, kb)$. Puisque $|k| m_1$ est un multiple commun de ka et kb, on a donc $|k| m_1 \geq m_2$ d'une part. D'autre part, m_2 est un multiple commun de ka et kb, donc $m_2 \mid |k|$ est un multiple commun de a et b et ainsi $m_2 \mid |k| \geq m_1$, ou encore $|k| m_1 \leq m_2$.

(3) Posons $m = ppcm(a, b)$ et supposons que $m \nmid M$. La division euclidienne de M par m s'écrit

$$M = qm + r \quad avec \quad 0 \leq r < m.$$

Et comme a, b divisent m et M, ils divisent $M - qm = r$. Ainsi r est un multiple commun de a et b, et donc $r \geq m$, donnant ainsi une contradiction. ■

2.4 Algorithme d'Euclide et les fractions continues

Théorème 2.13 (Algorithme d'Euclide) *Soit a, $b \in \mathbb{Z}$, $a > 0$. En appliquant successivement la division euclidienne (Théorème 2.1), on obtient la suite d'équations*

$$\begin{aligned}
b &= aq_1 + r_1, \quad 0 < r_1 < a \ ; \\
a &= r_1q_2 + r_2, \ 0 < r_2 < r_1; \\
r_1 &= r_2q_3 + r_3, \ 0 < r_3 < r_2; \\
&\vdots \qquad\qquad \vdots \\
r_{j-2} &= r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}; \\
r_{j-1} &= r_jq_{j+1};
\end{aligned}$$

où $r_j = (a, b)$.

Exemple 2.12 Trouver le $pgcd(42823, 6406)$.

Solution 2.14 *En appliquant l'algorithme d'Euclide pour trouver le $pgcd(42823, 6406)$.*

On a $b = 42823$ et $a = 6406$

$$\begin{aligned}
42823 &= 6406 \cdot 6 + 4369 \\
6406 &= 4369 \cdot 1 + 2040 \\
4369 &= 2040 \cdot 2 + 289 \\
2040 &= 289 \cdot 7 + 17 \\
289 &= 17 \cdot 17 + 0.
\end{aligned}$$

Donc $pgcd(42823, 6406) = 17$.

Définition 2.7 (Les fractions continues) Etant donné un nombre rationnel $\frac{a}{b}$, avec $(a,b) = 1$ et $b > 0$, d'après l'algorithme d'Euclide, il existe un entier positif n tel que

$$\begin{aligned}
a &= a_1 b + b_1, && 0 < b_1 < b;\\
b &= a_2 b_1 + b_2, && 0 < b_2 < b_1;\\
b_1 &= a_3 b_2 + b_3, && 0 < b_3 < b_2;\\
&\vdots\\
b_{n-3} &= a_{n-1} b_{n-2} + b_{n-1}, && 0 < b_{n-1} < b_{n-2};\\
b_{n-2} &= a_n b_{n-1}.
\end{aligned}$$

En utilisant successivement chacune de ces équations, on peut écrire

$$\begin{aligned}
\frac{a}{b} &= a_1 + \frac{1}{\left(\frac{b}{b_1}\right)} = a_1 + \frac{1}{a_2 + \frac{1}{\left(\frac{b_1}{b_2}\right)}}\\
&\vdots\\
&= a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}} \overset{déf}{=} \langle a_1, a_2, \ldots, a_n \rangle .
\end{aligned}$$

L'expression à plusieurs étage s'appelle le développement du nombre $\frac{a}{b}$ en fraction continue finie.

Exemple 2.13

$$\begin{aligned}
\frac{574}{252} &= 2+\frac{70}{252}\\
&= 2+\cfrac{1}{3+\cfrac{42}{70}}\\
&= 2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{28}{42}}}\\
&= 2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{14}{28}}}}\\
&= 2+\cfrac{1}{3+\cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{2}}}}\\
&= \langle 2,3,1,1,2\rangle\,.
\end{aligned}$$

Théorème 2.15 *Soient a et b deux entiers avec $b \geq 1$. Si l'algorithme d'Euclide pour a et b a une longueur n avec une suite de quotients $q_0, q_1, \ldots, q_{n-1}$, alors*

$$\frac{a}{b} = \langle q_0, q_1, \ldots, q_{n-1}\rangle\,.$$

Preuve. Soient $r_0 = a$ et $r_1 = b$. On démontre par récurrence sur n. Si $n = 1$, alors

$$r_0 = r_1 q_0$$

et

$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 = \langle q_0\rangle\,.$$

Si $n = 2$, alors

$$\begin{aligned}
r_0 &= r_1 q_0 + r_2\\
r_1 &= r_2 q_1
\end{aligned}$$

et

$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{r_2}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{q_1} = \langle q_0, q_1 \rangle .$$

Soit $n \geq 2$, et supposons que le théorème est vrai pour les entiers a et $b \geq 1$ avec l'algorithme d'Euclide a une longueur n. Soient a et $b \geq 1$ deux entiers avec l'algorithme d'Euclide a une longueur $n+1$ et dont la suite de quotients partiels est $\langle q_0, q_1, \ldots, q_{n-1} \rangle$. Soit

$$\begin{aligned} r_0 &= r_1 q_0 + r_2 \\ r_1 &= r_2 q_1 + r_3 \\ &\vdots \\ r_{n-1} &= r_n q_{n-1} + r_{n+1} \\ r_n &= r_{n+1} q_n. \end{aligned}$$

Soit les $n+1$ équations dans l'algorithme d'Euclide pour $a = r_0$ et $b = r_1$. L'algorithme d'Euclide pour deux entiers positifs r_1 et r_2 a une longueur n avec la suite de quotient partiels $q_1, \ldots, q_n$. Il résulte de l'hypothèse de récurrence que

$$\frac{r_1}{r_2} = \langle q_1, \ldots, q_n \rangle$$

et donc

$$\frac{a}{b} = \frac{r_0}{r_1} = q_0 + \frac{1}{\frac{r_1}{r_2}} = q_0 + \frac{1}{\langle q_1, \ldots, q_n \rangle} = \langle q_0, q_1, \ldots, q_n \rangle .$$

■

2.5 Equations diophantiennes

Lemme 2.1 *Soient $a, b, c \in \mathbb{Z}$ tels que $ab \neq 0$ et $d = pgcd(a, b)$. L'équation diophantienne $ax + by = c$ possède au moins une solution dans $\mathbb{Z}^2$ si et seulement si d divise c.*

Preuve. Si $c = 0$, on a $d \mid c$ et $(x, y) = (0, 0)$ est solution dans $\mathbb{Z}^2$. On suppose que $c \neq 0$. On note aussi u et v des entiers relatifs tels que $d = au + bv$.

Supposons d'abord que $d \nmid c$ et que l'équation possède une solution (x, y) dans $\mathbb{Z}^2$. Puisque $d \mid a$ et $d \mid b$, on a $d \mid (ax + by) = c$, d'où une contradiction.

Réciproquement, supposons que $d \mid c$. On pose $x_0 = \dfrac{cu}{d}$ et $y_0 = \dfrac{cv}{d}$. Notons que l'on a bien $(x_0, y_0) \in \mathbb{Z}^2$ puisque $d \mid c$. Alors

$$ax_0 + by_0 = \frac{acu + bcv}{d} = \frac{c}{d}(au + bv) = c.$$

Ainsi, le couple $(x_0, y_0) = \left(\dfrac{cu}{d}, \dfrac{cv}{d}\right)$ est une solution de l'équation. ■

Théorème 2.16 *Soient $a, b, c \in \mathbb{Z}$ tels que $ab \neq 0$ et $d = pgcd(a, b)$. On suppose que $d \mid c$ et on note (x_0, y_0) une solution particulière de équation diophantienne*

$$ax + by = c.$$

Alors, tout (x, y) est solution si et seulement si elle est donnée par

$$\begin{cases} x = x_0 + \dfrac{kb}{d}; \\ y = y_0 - \dfrac{ka}{d}. \end{cases} \tag{2.3}$$

Où $k \in \mathbb{Z}$.

Preuve. On note $a = d\tilde{a}, b = d\tilde{b}$ et $c = d\tilde{c}$ de sort $pgcd(\tilde{a}, \tilde{b}) = 1$. L'équation équivalant à $\tilde{a}x + \tilde{b}y = \tilde{c}$. Soit (x, y) une solution de $ax + by = c$ est que (x_0, y_0). De l'égalité
$\tilde{a}x + \tilde{b}y = \tilde{a}x_0 + \tilde{b}y_0$
on tire
$\tilde{a}(x - x_0) = \tilde{b}(y_0 - y)$
donc $\tilde{b}$ divise $\tilde{a}(x - x_0)$. Comme $pgcd(\tilde{a}, \tilde{b}) = 1$ on a d'après lemme d'Euclide $\tilde{b} \mid x - x_0$, et ainsi il existe $k \in \mathbb{Z}$ tel que $x = x_0 + \tilde{b}k$.
En remplaçant $x - x_0$ par $\tilde{b}k$ dans (2.4), on obtient $y = y_0 - \tilde{a}k$.

Réciproquement, on vérifie que les couples $(x, y) = (x_0 + \tilde{b}k, y_0 - \tilde{a}k)$, où $k \in \mathbb{Z}$, sont des solutions de (2.3). ■

Exemple 2.14 Résoudre dans $\mathbb{Z}^2$ l'équation

$$18459x + 3809y = 879.$$

Solution 2.17 *D'après l'algorithme d'Euclide, on a* $pgcd(18459, 3809) = 293$ *et comme* $879 = 3 \times 293$, *on déduit que l'équation possède au moins une solution. Après simplification par* 293, *l'équation équivalente à*

$$63x + 13y = 3. \tag{2.4}$$

Toujours d'après l'algorithme d'Euclide, on a $63(6) + 13(-29) = 1$, *donc le couple* $(x_0, y_0) = (18, -87)$ *est une solution particulière de* (2.4). *Soit* (x, y) *une solution. Alors*

$$63x + 13y = 63(18) + 13(-87) \Longleftrightarrow 63(x - 18) = 13(-y - 87).$$

Et ainsi $13 \mid 63(x - 18)$. *Puisque* $pgcd(63, 13) = 1$, *on a d'après lemme d'Euclide*
$13 \mid (x - 18)$,
et donc il existe $k \in \mathbb{Z}$ *tel que* $x = 18 + 13k$. *En remplaçant, on obtient*
$y = -87 - 63k$.

Réciproquement, on vérifie que les couples $(18+13k, -87-63k)$ *sont bien solutions de* (2.4). *Ainsi*

$$S = \{(18 + 13k, -87 - 63k),\ k \in \mathbb{Z}\}.$$

On peut résoudre cette équation par d'autre méthode comme l'exemple suivant.

Exemple 2.15 **[10]**Trouver les solutions de $999x - 49y = 5000$.

Solution 2.18 *Par la division euclidienne nous observons que* $999 = 20 \cdot 49 + 19$. *Cela suggère d'écrire l'équation dans la forme*

$$19x - 49(y - 20x) = 5000.$$

On remplace $\tilde{x} = x$, $\tilde{y} = y - 20x$, *nous trouvons que l'équation*

$$19\tilde{x} - 49\tilde{y} = 5000.$$

C'est plus simple car les coefficients sont plus petits. Du fait que $49 = 2 \cdot 19 + 11$, *nous écrivons cette équation comme*

$$19(\tilde{x} - 2\tilde{y}) - 11\tilde{y} = 5000.$$

Où, $19\hat{x} - 11\hat{y} = 5000$ *tel que* $\hat{x} = \tilde{x} - 2\tilde{y}$ *et* $\hat{y} = \tilde{y}$. *Puisque* $19 = 2 \cdot 11 - 3$, *nous écrivons l'équation comme*

$$-3\hat{x} - 11(-2\hat{x} + \hat{y}) = 5000.$$

Où, $-3x^{(3)} - 11y^{(3)} = 5000$. *Tel que* $x^{(3)} = \hat{x}$, $y^{(3)} = -2\hat{x} + \hat{y}$. *Comme* $11 = 4 \cdot 3 - 1$, *nous écrivons l'équation comme*

$$-3(x^{(3)} + 4y^{(3)}) + y^{(3)} = 5000.$$

Où, $-3x^{(4)} + y^{(4)} = 5000$ *tel que* $x^{(4)} = x^{(3)} + 4y^{(3)}$, $y^{(4)} = y^{(3)}$. *On fait changement de variable* $x^{(5)} = x^{(4)}, y^{(5)} = -3x^{(4)} + y^{(4)}$, *on devient*

$$y^{(5)} = 5000.$$

Ici la valeur de $y^{(5)}$ *est un entier fixe, et* $x^{(5)}$ *est un entier arbitraire. Du fait que les paires d'entiers* (x, y) *sont en correspondance biunivoque avec les paires d'entiers* $\left(x^{(5)}, y^{(5)}\right)$, *il suit que l'équation originale a une infinité de solutions entières. Pour exprimer* x *et* y *explicité en termes de* $x^{(5)}$ *et* $y^{(5)}$, *nous déterminons d'abord* x *et* y *en termes de* $\tilde{x}$ *et* $\tilde{y}$, *puis en termes de* $\hat{x}$ *et* $\hat{y}$, *et ainsi de suit. Ces transformations peuvent être développées en même temps que l'originale d'équation est simplifiée. Nous commençons par*

$$\begin{aligned} 999x - 49y &= 5000; \\ x &= x; \\ y &= y. \end{aligned} \tag{2.5}$$

Nous écrivons cette équation sous la forme

$$\begin{aligned} 19x - 49(y - 20x) &= 5000; \\ x &= x; \\ 20x + (-20x + y) &= y. \end{aligned}$$

Donc,

$$\begin{aligned} 19\tilde{x} - 49\tilde{y} &= 5000; \\ \tilde{x} &= x; \\ 20\tilde{x} + \tilde{y} &= y. \end{aligned} \tag{2.6}$$

Nous réécrivons ces équations

$$\begin{aligned} 19(\tilde{x} - 2\tilde{y}) - 11\tilde{y} &= 5000; \\ \tilde{x} - 2\tilde{y} + 2\tilde{y} &= x; \\ 20\,(\tilde{x} - 2\tilde{y}) + 41 &= y. \end{aligned}$$

Donc,

$$\begin{aligned} 19\hat{x} - 11\hat{y} &= 5000; \\ \hat{x} + 2\hat{y} &= x; \\ 20\hat{x} + 41\hat{y} &= y. \end{aligned} \tag{2.7}$$

Nous réécrivons ces équations

$$\begin{aligned} -3\hat{x} - 11(-2\hat{x} + \hat{y}) &= 5000; \\ 5\hat{x} + 2(-2\hat{x} + \hat{y}) &= x; \\ 102\hat{x} + 41(-2\hat{x} + \hat{y}) &= y. \end{aligned}$$

Donc,

$$\begin{aligned} -3x^{(3)} - 11y^{(3)} &= 5000; \\ 5x^{(3)} + 2y^{(3)} &= x; \\ 102x^{(3)} + 41y^{(3)} &= y. \end{aligned} \tag{2.8}$$

Nous réécrivons ces équations

$$\begin{aligned} -3(x^{(3)} + 4y^{(3)}) + y^{(3)} &= 5000; \\ 5(x^{(3)} + 4y^{(3)}) - 18y^{(3)} &= x; \\ 102(x^{(3)} + 4y^{(3)}) - 367y^{(3)} &= y. \end{aligned}$$

Donc,

$$\begin{aligned} -3x^{(4)} + y^{(4)} &= 5000; \\ 5x^{(4)} - 18y^{(4)} &= x; \\ 102x^{(4)} - 367y^{(4)} &= y. \end{aligned} \tag{2.9}$$

Nous réécrivons ces équations

$$\begin{aligned} -3x^{(4)} + y^{(4)} &= 5000; \\ -49x^{(4)} - 18\left(-3x^{(4)} + y^{(4)}\right) &= x; \\ -999x^{(4)} + 367\left(-3x^{(4)} + y^{(4)}\right) &= y. \end{aligned}$$

Donc,

$$\begin{aligned} y^{(5)} &= 5000; \\ -49x^{(5)} - 18y^{(5)} &= x; \\ -999x^{(5)} - 367y^{(5)} &= y. \end{aligned} \tag{2.10}$$

On remplace $y^{(5)}$ par cette valeur, et nous écrivons k à la place de $x^{(5)}$, nous obtenons

$$\begin{aligned} x &= -49k - 90000; \\ y &= -999k - 1835000. \end{aligned}$$

Nous notons que les coefficients en (2.6) sont obtenus de ceux de (2.5) par soustraire 20 fois la deuxième colonne de la première colonne. Similairement, les coefficients en (2.7) sont obtenus à partir de ceux de (2.6) nous ajoutons deux fois la première colonne à la deuxième. En (2.7) nous ajoutons -4 fois la première colonne à la deuxième pour obtenir (2.8), et en (2.8) nous ajoutons 3 fois la première colonne à la deuxième pour obtenir (2.9).

En général, nous pouvons ajouter un multiple d'une des deux premières colonnes à l'autre. En plus nous pouvons permuter les deux premières colonnes de multiplier tous les éléments de l'une de ces colonnes par -1. Ainsi nous pouvons modifier les coefficients au moyen des trois opérations suivantes.

C_1) Ajouter un multiple m de l'une des deux premiers colonnes à l'autre.

C_2) Echanger les deux premiers colonnes.

C_3) Multiplier tous les éléments de l'une des deux premiers colonnes par -1.

Exemple 2.16 [10]Trouver les entiers x et y tel que $147x + 258y = 369$.

Solution 2.19 *Nous écrivons*

$$\begin{array}{ccccccccccccccc} 147 & 258 & 369 & & 147 & 111 & 369 & & 36 & 111 & 369 & & 36 & 3 & 369 \\ 1 & 0 & & \longrightarrow & 1 & -1 & & \longrightarrow & 2 & -1 & & \longrightarrow & 2 & -7 & \\ 0 & 1 & & & 0 & 1 & & & -1 & 1 & & & -1 & 4 & \end{array}$$

$$\begin{array}{ccccc} & 0 & 3 & 369 & \\ \longrightarrow & 86 & -7 & & \\ & -49 & 4 & & \end{array}$$

Notons les variables par u et v. Du fait que $3v = 369$, nous déduisons $v = 123$, et que l'ensemble des solutions originales données par $x = 86u - 861$, $y = -49u + 492$. Les variables u et v ont été obtenu des variables originales x et y par un changement de coordonnés homogène. Nous pouvons réduire la taille des entiers figurant dans la

solution moyennant un changement de variable non homogène. Par exemple, si nous mettons $u = t + 10$, alors nous trouvons que $x = 86t - 1$, $y = -49t + 2$.

Chapitre 3

Congruence

Dans ce chapitre on étudie la congruence qui a été introduit par Carl Friedrich Gauss $(1777-1855)$, l'un des plus grands mathématiciens de tous les temps.

3.1 Congruence linéaire

Soit n un entier strictement positif.

Définition 3.1 Soit a et b deux entiers relatifs. On dit que a est congru à b modulo n si $a-b$ est un multiple de n.

Cette relation se note $a \equiv b \bmod n$ ou bien $a \equiv b\ [n]$.

Exemple 3.1 $141 \equiv 9 \bmod 11$, car $141-9=132$ est un multiple de 11.

Théorème 3.1 *Soit $n>0$ un entier. Alors*

$$a \equiv b \mod n \Longleftrightarrow n \mid (a-b).$$

Preuve. $\Longrightarrow$) Supposons $a \neq b$. Par l'Algorithme d'Euclide il existe deux entiers $q_1 \neq q_2$ tels que $a=q_1n+r$ et $b=q_2n+r$, comme a et b ont le même reste quand on la divise par n. Donc $a-b=q_1n-q_2n=(q_1-q_2)n$. Ce qui implique $n \mid (a-b)$.
$\Longleftarrow$) Si $n \mid (a-b)$ alors il existe un entier t tel que $nt=a-b$. Supposons que $a=m_1n+r_1$ et $b=m_2n+r_2$ avec $0 \leq r_1, r_2 < n$. Alors
$nt=a-b=(m_1-m_2)n+r_1-r_2 \Rightarrow n(t-m_1+m_2)=r_1-r_2 \Rightarrow n \mid (r_1-r_2)$.

Puisque $|r_1 - r_2| < n$ nous avons $r_1 - r_2 = 0$ et donc a et b ont le même reste quand on les divise par n. ■

Théorème 3.2 *Soient a, b, c, d, $n \in \mathbb{Z}$, $k \in \mathbb{N}^*$ avec $a \equiv b \bmod n$ et $c \equiv d \bmod n$. Alors*

1. $a + c \equiv b + d \bmod n$
2. $a - c \equiv b - d \bmod n$
3. $ac \equiv bd \bmod n$
4. $a^k \equiv b^k \bmod n$.

Preuve. Comme $a \equiv b \bmod n$ et $c \equiv d \bmod n$, il existe k_1, $k_2 \in \mathbb{Z}$ avec $a = b + k_1 n$ et $c = d + k_2 n$. Donc $a \pm c = b \pm d + n(k_1 \pm k_2)$. Aussi on a $ac = bd + n(dk_1 + bk_2)$.
On démontre par récurrence $a^k \equiv b^k \bmod n$. Pour $k = 1$
$a^1 = a$ et $b^1 = b$ donc $a^1 \equiv b^1 \bmod n$.
Supposons que pour $k \geq 1$ on a $a^k \equiv b^k \bmod n$ et montrons $a^{k+1} \equiv b^{k+1} \bmod n$.
On a $a^k \equiv b^k \bmod n$ et $a \equiv b \bmod n$. Alors, en multipliant membre à membre, on obtient

$$a^{k+1} \equiv b^{k+1} \bmod n.$$

■

Définition 3.2 (Relation d'équivalence) Une relation $\Re$ sur un ensemble E est une relation d'équivalence si elle est

i) Réflexive ; $\forall a \in E$, $a \Re a$;

ii) Symétrique ; $\forall a, b \in E$, $(a \Re b) \Rightarrow (b \Re a)$;

iii) Transitive ; $\forall a, b, c \in E$, $(a \Re b$ *et* $b \Re c) \Rightarrow (a \Re c)$.

Théorème 3.3 *Pour tout n positif, la congruence modulo n est une relation d'équivalence sur un ensemble des entiers.*

Preuve. Réflexivité ; si a un entier, alors $a \equiv a \bmod n$ car $n \mid (a - a) = 0$.
Symétrie ; si $a \equiv b \bmod n$, alors $n \mid (a - b)$, donc $n \mid (b - a)$ et donc $b \equiv a \bmod n$.
Transitivité ; si $a \equiv b \bmod n$ et $b \equiv c \bmod n$, alors $n \mid (a - b)$ et $n \mid (b - c)$, puisque $n \mid [(a - b) + (b - c)] = (a - c)$, donc $a \equiv c \bmod n$. ■

Théorème 3.4 *Soient n, a, b des entiers avec $n \geq 1$. Posons $d = (a, n)$. La congruence*

$$ax \equiv b \bmod n \tag{3.1}$$

a une solution si et seulement si,

$$b \equiv 0 \bmod d.$$

Si $b \equiv 0 \mod d$, alors la congruence (3.1) a exactement d solutions en entiers qui sont deux à deux incongrues modulo n.
En particulier, si $(a, n) = 1$, la congruence (3.1) a une solution unique modulo n.

Preuve. D'après le théorème 2.16 nous savons que la solution de l'équation diophantienne linéaire $ax + ny = b$ est donnée par $x = x_0 + \frac{nt}{d}$, $y = y_0 - \frac{at}{d}$, $d = (a, n)$, $t \in \mathbb{Z}$, où x_0, y_0 satisfont $ax_0 + ny_0 = b$.
Soit $t = 0, 1, 2, \ldots, d-1$, nous obtenons d solutions mutuellement incongrues, du fait que la valeur absolue de la différence entre deux de ces solutions plus petit que d. Si $x = x_0 + \frac{n\tilde{t}}{d}$ est moindre que tout autre solution, nous écrivons $\tilde{t}$ comme $\tilde{t} = qd + r_0$, $0 \leq r_0 < d$. Alors

$$\begin{aligned} x &= x_0 + \frac{n(qd + r_0)}{d}; \\ &= x_0 + nq + \frac{nr_0}{d}; \\ &\equiv x_0 + \frac{nr_0}{d} \mod n. \end{aligned}$$

Ainsi toute solution de la congruence $ax \equiv b \mod n$ est congrue mod n à une et une seul solution de la forme $x_0 + \frac{nt}{d}$ de d valeurs avec $0 \leq t \leq d-1$. Ainsi s'il y a une solution de la congruence, donc il existe d solutions incongrue mod n. ■

Lemme 3.1 *Si p un nombre premier. Alors $x^2 \equiv 1 \mod p$, si et seulement si, $x \equiv \pm 1 \mod p$.*

Preuve. Si $x \equiv \pm 1 \mod p$, alors $x^2 \equiv 1 \mod p$.

Réciproquement, si $x^2 \equiv 1 \mod p$, alors p divise $x^2 - 1 = (x+1)(x-1)$, et donc p divise $x + 1$ ou $x - 1$. Ce qui implique $x \equiv \pm 1 \mod p$. ■

Théorème 3.5 (Wilson) *Si p est premier, alors*

$$(p-1)! \equiv -1 \mod p.$$

Preuve. C'est vrai pour $p = 2$ et $p = 3$, comme $1! \equiv -1 \bmod 2$ et $2! \equiv -1 \bmod 3$.
Soit $p \geq 5$. Par le théorème 3.4, pour tout entier $a \in \{1, 2, \ldots, p-1\}$ il existe un unique entier $a^{-1} \in \{1, 2, \ldots, p-1\}$ tel que $aa^{-1} \equiv 1 \bmod p$.
Par le lemme 3.1, $a = a^{-1}$ si et seulement si $a = 1$ ou $a = p-1$. Donc, nous partitionnons l'ensemble $\{2, 3, \ldots, p-2\}$ à $p-3$ nombres entre $(p-3)/2$ paire d'entiers $\left\{a_i, a_i^{-1}\right\}$ tel que $a_i a_i^{-1} \equiv 1 \bmod p$ pour $i = \{1, \ldots, (p-3)/2\}$. Alors

$$\begin{aligned}
(p-1)! &\equiv 1 \cdot 2 \cdot 3 \cdots (p-2)(p-1) \\
&\equiv (p-1) \prod_{i=1}^{(p-3)/2} a_i a_i^{-1} \\
&\equiv p-1 \\
&\equiv -1 \mod p.
\end{aligned}$$

■

Exercice 3.6 *Soit p un nombre premier et soit r un entier tel que $1 \leq r < p$. Si $(-1)^r r! \equiv 1 \bmod p$, montrer que*

$$(p-r-1)! \equiv -1 \mod p.$$

Déduire de ce résultat que $259! \equiv -1 \bmod 269$ et $463! - 1 \bmod 479$.

Solution 3.7 *D'après le théorème de Wilson,*

$$(p-1)! = (p-1)(p-2)\cdots(p-r)(p-r-1)! \equiv (-1)^r r!\,(p-r-1)! \equiv -1 \bmod p.$$

Puisque $(-1)^r r! \equiv 1 \bmod p$, on obtient le résultat.
Pour la deuxième partie, on observe que 269 et 479 sont premiers et donc il suffit de remarquer $(-1)^9 9! \equiv 1 \bmod 269$ et que $(-1)^{15} 15! \equiv 1 \bmod 479$.

3.2 Fonction d'Euler

Définition 3.3 (Fonction d'Euler) La fonction ϕ d'Euler est définie par

$$\phi(n) = \#\{0 < m \leq n \mid (n,m) = 1\}.$$

Exemple 3.2 $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = \phi(4) = 2$, $\phi(5) = 4$.

Remarque 3.1 Si p est premier, on a $(a,p) = 1$ pour $a = 1, 2, 3, \ldots, p-1$ donc

$$\phi(p) = p - 1.$$

Exemple 3.3 Si $p = 1001$ est premier, $\phi(1001) = 1001 - 1 = 1000$.

Théorème 3.8 *Soit p est un nombre premier et r est un entier positif. Alors*

$$\phi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right).$$

Preuve. Soit un entier k tel que $1 \leq k \leq p^r$ sera relativement premier à p^r, si et seulement si, k ne divise pas par p puisque, par le théorème 2.7, les seuls diviseurs de p^r sont les puissances de p. Les entiers k tel que $1 \leq k < p^r$ et k est divisible par p sont ceux de la liste $p, 2p, 3p, \ldots,(p^{r-1}-1)p$. On déduit que le nombre de ces entiers égale à $p^{r-1}-1$. Ainsi les nombres des entiers positifs inférieurs aux p^r et relativement premier à p est $p^r - 1 - (p^{r-1}-1) = p^r - p^{r-1}$. Donc $\phi(p^r) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$. ■

Théorème 3.9 *Si p et q deux premiers, alors*

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

Preuve. D'après le lemme d'Euclide, un entier k satisfait $(k,pq) > 1$, si et seulement si, $p \mid k$ ou $q \mid k$. Le nombre de tels k avec $1 \leq k < pq$ est $(q-1)$(à partir des multiples de p qui sont inférieurs à pq) plus $(p-1)$(à partir des multiples de p qui sont inférieurs à pq). Ainsi le nombre de k tel que $1 \leq k < pq$ et $(k,pq) = 1$ est $pq - 1 - (q-1) - (p-1) = pq - q - p + 1 = (p-1)(q-1)$. ■

3.3 Théorème du reste Chinois

Théorème 3.10 (Théorème Chinois) *Soit $m_1, m_2, \ldots, m_r$ des entiers positifs relativement premiers deux à deux. Soit $a_1, a_2, \ldots, a_r$ des entiers quelconques. Alors le système de congruences*

$$\begin{cases} x \equiv a_1 \mod m_1 \\ x \equiv a_2 \mod m_2 \\ \quad \vdots \\ x \equiv a_r \mod m_r \end{cases}$$

possède une unique solution modulo $m_1 m_2 \cdots m_r$.

Preuve. Considérons les entiers

$$P_j = \frac{m_1 m_2 \cdots m_r}{m_j}.$$

Où $1 \leq j \leq r$.

On considère les équations diophantiennes $P_j x \equiv 1 \,[m_j]$, pour $1 \leq j \leq r$. Chacune de ces équations possède une unique solution modulo m_j car $(P_j, m_j) = 1$, pour $j = 1, \ldots, r$.

Notons par Q_j la solution de $P_j x \equiv 1 \,[m_j]$, avec $j = 1, \ldots, r$.

L'entier

$$x = a_1 P_1 Q_1 + a_2 P_2 Q_2 + \cdots + a_r P_r Q_r$$

est une solution car

$$\begin{aligned} x &= a_1 (1 + k m_1) + \sum_{i=2}^{r} a_i P_i Q_i \\ x &= a_1 + a_1 k m_1 + \sum_{i=2}^{r} a_i P_i Q_i \\ x &= a_1 + \tilde{k} m_1 \\ x &= a_1 \,[m_1]. \end{aligned}$$

De la même manière on obtient que $x = a_j \,[m_j]$ pour $j = 2, \ldots, r$.

Supposons qu'il existe deux solution x et $\overline{x}$ tels que

$$\begin{aligned} x &\equiv a_i\,[m_i] = a_i + lm_i; \\ \overline{x} &\equiv a_i\,[m_i] = a_i + \tilde{l}m_i. \end{aligned}$$

Pour $j = 1, \ldots, r$, donc $x - \overline{x} \equiv 0\,[m_i]$ on applique le théorème 3.1, nous obtenons

$$\begin{aligned} x - \overline{x} &\equiv 0\,[m_1] \Longleftrightarrow m_1 \mid x - \overline{x}; \\ x - \overline{x} &\equiv 0\,[m_2] \Longleftrightarrow m_2 \mid x - \overline{x}; \\ &\vdots \qquad\qquad\qquad\quad \vdots \\ x - \overline{x} &\equiv 0\,[m_r] \Longleftrightarrow m_r \mid x - \overline{x}. \end{aligned}$$

Comme les entiers $m_1, m_2, \ldots, m_r$ sont deux à deux premiers entre eux, alors $m_1 m_2 \cdots m_r \mid x - \overline{x}$ i.e., $\overline{x} \equiv x\,[m_1 m_2 \cdots m_r]$. D'où la solution est unique modulo $m_1 m_2 \cdots m_r$. ■

Exemple 3.4

$$\begin{cases} x \equiv 3\,[5] \\ x \equiv 7\,[11] \end{cases}$$

on a $m_1 = 5$, $m_2 = 11$,
et on a $P_1 = 11$, $P_2 = 5$, $Q_1 \equiv 1\,[5]$ car $11Q_1 \equiv 1\,[5]$ i.e., $Q_1 = 1 + 5t$, $Q_2 \equiv 9\,[11]$ puisque $5Q_2 \equiv 1\,[11]$ i.e., $Q_2 = 9 + 11t$.

$$\begin{aligned} x &= a_1 P_1 Q_1 + a_2 P_2 Q_2 \\ &= 3 \cdot 11\,(1 + 5t) + 7 \cdot 5\,(9 + 11t) \\ &= 348 + 165t + 385t \\ &= 348 + 550t \\ &= 293 + 55 + 10 \cdot 55t \\ &= 293 + 55\,(1 + 10t) \end{aligned}$$

d'autre part $293 \equiv 18\,[55]$ nous obtenons

$$\begin{aligned} x &= 293 + 55\tilde{t} \\ &\equiv 18\,[55]\,. \end{aligned}$$

Donc la solution est $x \equiv 18\,[55]$.

Exemple 3.5 Résoudre le système suivant $\begin{cases} 5x \equiv 7 \bmod 12 \\ 4x \equiv 12 \bmod 14. \end{cases}$

Solution 3.11 *On a* $\begin{cases} 5x \equiv 7 \bmod 12 \\ 4x \equiv 12 \bmod 14. \end{cases}$
Multiplions la première équation par 5 *on obtient*

$$x \equiv 11 \bmod 12.$$

La deuxième équation devient $2x \equiv 6 \bmod 7$, *et devient aussi*

$$x \equiv 3 \bmod 7.$$

$$\begin{cases} x \equiv 11 \bmod 12 \\ x \equiv 3 \bmod 7. \end{cases}$$

Donc $m_1 = 12, m_2 = 7, P_1 = 7, P_2 = 12$, *et on a* $7Q_1 \equiv 1 \bmod 12$ *ce qui implique* $Q_1 = 7 + 12t$, *d'autre part* $12Q_2 \equiv 1 \bmod 7$ *ce qui implique* $Q_2 = 3 + 7\tilde{t}$. *Alors*

$$\begin{aligned} x &= 11 \cdot 7 \cdot 7 + 3 \cdot 12 \cdot 2 \\ &= 647 \\ &\equiv 59 \mod 84. \end{aligned}$$

3.4 Théorème d'Euler et théorème de Fermat

Définition 3.4 (Système réduit de résidus) Un système réduit de résidus modulo m est un ensemble d'entiers r_i tel que $(r_i, m) = 1$, $r_i \not\equiv r_j \bmod m$ lorsque $i \neq j$,

et tel que chaque entier x relativement premier avec m est congru à un certain r_i modulo m.

Exemple 3.6 $\{1,2,3,4,5,6\}$ et $\{2,4,6,\ldots,12\}$ sont des système réduit de résidu modulo 7.

Théorème 3.12 (Euler) *Soit $m \in \mathbb{N}$ et $a \in \mathbb{Z}$ tels que $(a,m)=1$. Alors*

$$a^{\phi(m)} \equiv 1 \mod m.$$

Preuve. Soit $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ un système réduit de résidus modulo m. Vu que $(a,m)=1$, on a $(ar_i, m)=1$ pour $i=\{1,\ldots,\phi(m)\}$. D'où, pour $i=\{1,\ldots,\phi(m)\}$ il existe $\sigma(i) \in \{1,\ldots,\phi(m)\}$ tel que

$$ar_i \equiv r_{\sigma(i)} \mod m.$$

De plus $ar_i \equiv ar_j \bmod m$ si et seulement si $i=j$, et donc σ est une permutation de $\{1,\ldots,\phi(m)\}$ et $\{ar_1, ar_2, \ldots, ar_{\phi(m)}\}$ est aussi un système réduit de résidus modulo m. Alors

$$\begin{aligned} a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} &\equiv (ar_1)(ar_2)\cdots(ar_{\phi(m)}) \mod m \\ &\equiv r_{\sigma(1)} r_{\sigma(2)} \cdots r_{\sigma(\phi(m))} \mod m \\ &\equiv r_1 r_2 \cdots r_{\phi(m)} \mod m. \end{aligned}$$

Divisons par $r_1 r_2 \cdots r_{\phi(m)}$, nous obtenons

$$a^{\phi(m)} \equiv 1 \mod m.$$

■

Exemple 3.7 $m=11$ et $a=2$, tel que $(11,2)=1$
$\phi(11)=10$, ce qui implique $2^{10}=1024 \equiv 1 \bmod 11$.

Théorème 3.13 (Le petit théorème de Fermat) *Soit p un nombre premier. Si a est un entier non divisible par p, alors*

$$a^{p-1} \equiv 1 \mod p.$$

De plus,

$$a^p \equiv a \mod p$$

pour tout entier a.

Preuve. Si p est premier et $p \nmid a$, alors $(a,p) = 1$, $\phi(p) = p - 1$, et

$$a^{p-1} = a^{\phi(p)} \equiv 1 \mod p.$$

Aussi on a $a^p \equiv a \bmod p$.
Si $p \mid a$ c'est évident

$$a^p \equiv a \mod p.$$

■

3.5 Fonctions arithmétiques

Définition 3.5 Une fonction arithmétique est une application de $\mathbb{N}$ dans $\mathbb{C}$. Une fonction arithmétique f est dite multiplicative si $f(1) = 1$ et si $f(mn) = f(m) f(n)$ lorsque $(m,n) = 1$. Une fonction arithmétique f est dite totalement multiplicative (ou complètement multiplicative) si $f(1) = 1$ et si $f(mn) = f(m) f(n)$ pour tous les entiers m et n.

Définition 3.6 Une fonction arithmétique f est dite additive si $f(1) = 0$ et si $f(mn) = f(m) + f(n)$ lorsque $(m,n) = 1$. Une fonction arithmétique f est dit totalement additive (ou complètement additive) si $f(1) = 0$ et si $f(mn) = f(m) + f(n)$ pour tous les entiers m et n.

Exemple 3.8 Voici quelques-unes fonctions arithmétiques

1. $\tau(n)$: le nombre de diviseurs de n;

2. $\sigma(n)$: la somme des diviseurs de n, pour chaque nombre réel $r, \sigma_r(n) = \sum_{d|n} d^r$;
3. $\omega(n)$: le nombre de facteurs premiers distincts de n, ou en d'autres termes $\omega(n) = \sum_{p|n} 1$ et $\omega(1) = 0$;
4. $\Omega(n)$: le nombre total de facteurs premiers de n, ou en d'autres termes $\Omega(n) = \sum_{p^\alpha \| n} \alpha$ et $\Omega(1) = 0$.

Exemple 3.9 En appliquant ces exemples

1. Pour $n = 14$ on a les diviseurs de 14 sont $1, 2, 7, 14$. Donc $\tau(14) = 4$.
2. Pour $n = 6$, $\sigma(6) = 1 + 2 + 3 + 6 = 12$.
3. Pour $n = 18$, $\omega(18) = 2$.
4. Pour $n = 36$, $\Omega(n) = 4$ car $36 = 2^2 \times 3^2$.

Théorème 3.14 *Une fonction arithmétique f est multiplicative si et seulement si $f(1) = 1$ et, lorsque $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers distincts, on a*

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r}). \tag{3.2}$$

Preuve. Supposons d'abord que f vérifie $f(1) = 1$ et l'égalité (3.2). Soient alors $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ et $m = q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}$ deux entiers premiers entre eux. Ainsi, $p_i \neq q_j$ pour tout $(i, j) \in \{1, \ldots, r\}^2$. D'après (3.2),

$$f(n) f(m) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r}) f\left(q_1^{\beta_1}\right) f\left(q_2^{\beta_2}\right) \cdots f\left(q_r^{\beta_r}\right)$$

et

$$\begin{aligned} f(nm) &= f\left(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1} q_2^{\beta_2} \cdots q_r^{\beta_r}\right); \\ &= f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r}) f\left(q_1^{\beta_1}\right) f\left(q_2^{\beta_2}\right) \cdots f\left(q_r^{\beta_r}\right); \end{aligned}$$

et donc $f(nm) = f(n)f(m)$. D'où f est multiplicative.
Réciproquement, supposons que soit f multiplicative. Alors

$$f(1) = 1.$$

Aussi, si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où les p_i sont premiers distincts, alors par récurrence on démontre que

$$f(n) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_r^{\alpha_r}).$$

■

Théorème 3.15 *Une fonction arithmétique f est additive si et seulement si $f(1) = 0$ et, lorsque $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ où les p_i sont des nombres premiers distincts, on a*

$$f(n) = f(p_1^{\alpha_1}) + f(p_2^{\alpha_2}) + \cdots + f(p_r^{\alpha_r}). \tag{3.3}$$

3.6 Des applications

Exercice 3.16 *Montrer que si f et g sont des fonctions multiplicatives, alors le produit fg est aussi une fonction multiplicative. Si f est une fonction multiplicative, peut-on dire que kf, $k \in \mathbb{R}$, est aussi une fonction multiplicative? Qu'en est-il de $f + g$?*

Solution 3.17 *On a f et g sont des fonctions multiplicatives, alors*

$$\begin{aligned} fg(1) &= f(1) g(1) = 1. \\ fg(mn) &= f(mn) g(mn); \\ &= f(m) f(n) g(m) g(n); \\ &= fg(m) fg(n). \end{aligned}$$

Donc fg est une fonction multiplicative.
kf, $k \in \mathbb{R}$ est une fonction multiplicative?
On a $kf(1) = k$

$$\begin{aligned} \text{si } k &= 1, \text{ donc } kf \text{ est une fonction multiplicative;} \\ \text{si } k &\neq 1, \text{ donc } kf \text{ n'est pas une fonction multiplicative.} \end{aligned}$$

$f+g$ est une fonction multiplicative?

$$f+g\left(1\right)=f\left(1\right)+g\left(1\right)=2\neq 1.$$

Alors $f+g$ n'est pas une fonction multiplicative.

Exercice 3.18 *Démontrer que*

$$\sum_{n=1}^{\infty}\frac{\tau\left(n\right)}{2^{n}}=\sum_{n=1}^{\infty}\frac{1}{2^{n}-1}.$$

Solution 3.19 *En développant le membre de droite, on obtient*

$$\begin{aligned}
\sum_{n=1}^{\infty}\frac{1}{2^{n}-1} &= \sum_{n=1}^{\infty}\left(\frac{1}{2^{n}}\cdot\frac{1}{1-\frac{1}{2^{n}}}\right)\\
&= \sum_{n=1}^{\infty}\frac{1}{2^{n}}\left(1+\frac{1}{2^{n}}+\frac{1}{2^{2n}}+\cdots\right)\\
&= \sum_{n=1}^{\infty}\left(\frac{1}{2^{n}}+\frac{1}{2^{2n}}+\frac{1}{2^{3n}}+\cdots\right)\\
&= \sum_{d_{2}=1}^{\infty}\sum_{d_{1}=1}^{\infty}\frac{1}{2^{d_{1}d_{2}}}\\
&= \sum_{m=1}^{\infty}\frac{1}{2^{m}}\sum_{d_{1}d_{2}=m}^{\infty}1\\
&= \sum_{m=1}^{\infty}\frac{\tau\left(m\right)}{2^{m}}.
\end{aligned}$$

Exercice 3.20 *Démonter que $\tau\left(n\right)\leq 2\sqrt{n}$.*

Solution 3.21 *Chaque diviseur positif a de n peut être apparie avec son diviseur $\frac{n}{a}$. Comme $n=a\cdot\frac{n}{a}$, un de ces diviseurs doit être $\leq\sqrt{n}$. Ce donné la plupart $2\sqrt{n}$ diviseurs.*

Conclusion

La lecture des notions présentées dans ce mémoire mettre le lecteur dans une situation commode qui lui permet d'entamer et de faire pas mal de recherches dans le domaine de la théorie des nombres. Ceci parce qu'il s'agit des notions clefs comme nous avons dit dans l'introduction.

Dans ce sens et on se basant sur ce modeste mémoire on peut étudier la réciprocité quadratique et les formes quadratique, quelque fonctions de la théorie des nombres, quelque équations diophantiennes linéaires et non linéaires, cryptographie . . . .

Bibliographie

[1] **O. Bordellés**, *Thème d'arithmétique*, Ellipses, Mars 2006.

[2] **J. M. De koninck et A. Mercier**, *1001 problèmes en théorie classique des nombres*, Ellipses, 2004.

[3] **J. R. Durbin**, *Modern algebra*, Sixth Edition, John Wiley & Sons, Inc, 2009.

[4] **X. Gourdon**, *Les maths en tête*, Ellipses, Juillet 1996.

[5] **C. Guyeux**, *Mathématiques pour l'informatique*, Site Internet : guyeux@iut-bm.univ-fcomte.fr, 21 avril 2008.

[6] **F. Liret**, *Arithmétique*, Licence capes, Août 2011.

[7] **J. P. Marco et L. Lazzarini**, *Mathématique* L_1, Pearson Education France, 2007.

[8] **Y. Monka**, *Divisibilité et congruence*, Académie de Strasbourg, Site Internet : www.maths-et-tiques.fr.

[9] **M. B. Nathason**, *Elementary methods in number theory*, Springer, 2000.

[10] **I. Niven et H. S. Zuckerman et H. L. Montgomery**, *An introduction to the theory of numbers*, Fifth Edition, John Wiley & Sons, Inc, 1991.

[11] **R. Pass**, *A course in discrete structures*, Wei-Lung Dustin Tseng, Site Internet : www.freechbooks.com.

[12] **P. Ribenboim**, *The little book of big primes*, Springer-Verlag, 1991.

[13] **K. H. Rosen**, *Discrete mathematics and its applications*, Seventh Edition, The McGraw-Hill Companies, Inc, 2012.

[14] **D. A. Santos**, *Elementary number theory notes,* Site internet :\\www.course-hero.com/file/8359327/Santos David Elementary Number Theory Notes//, January 15, 2004.

[15] **D. A. Santos**, *Discrete mathematics notes*, Site Internet : dsantos@ccp.edu, July 3, 2006.