Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département des Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématique Discrète

Thème

SUR LES FONCTIONS ARITHMÉTIQUES

Présentée par :
CHAMI Abde Ssamed

Soutenue publiquement le : 03/07/2022.

Devant le jury composé de :

Mr. N. Ghadbane	M.C.A,	Université de M'sila	**Président**.
Mr. A.BOUDAOUD	Prof,	Université de M'sila	**Encadreur**.
Mr. D. MIHOUBI	Prof,	Université de M'sila	**Examinateur**.
Mr. DJ. BELLAOUAR	M.C.A,	Université de Guelma	**Examinateur**.

Année universitaire 2021/2022.

Résume

Ce mémoire est formé de quatre chapitres. Le premier contient des notions fondamentales et nécessaires pour celui qui veut débuter à étudier un problème de théorie de nombres. Les concepts liés aux fonctions arithmétiques tels que : Multiplicativité, additivité, produit de convolution de Dirichlet, Inverses de Dirichlet et La formule d'inversion de Moebius, … font l'objet du deuxième chapitre. Le troisième chapitre est consacré aux méthodes de sommation, alors que le dernier chapitre est dévoué à la résolution de quelques problèmes liés au sujet et existant dans la littérature

.Mots clés: fonctions arithmétiques, Division Euclidienne, Parité entier, Nombre premier, Algorithme Euclidien, produit de convolution de Dirichlet, La formule d'inversion de Moebius, Sommation.

Abstract

This memoir consists of four chapters. The first one contains fundamental and necessary notions for those who want to start studying a number theory problem. Concepts related to arithmetic functions such as: Multiplicatively, additively, Dirichlet convolution product, Dirichlet inverses and the Moebius inversion formula, ... are the subject of the second chapter. The third chapter is devoted to summation methods, while the last chapter is devoted to the solution of some problems related to the subject and existing in the literature.

Keywords: Arithmetic functions, Euclidean Division, Prime number, Euclidean Algorithm, , Integer parity, Dirichlet convolution product, Moebius inversion formula Summation**.**

الملخص

تتكون هذه الرسالة من أربعة فصول .الأول يحتوي على مفاهيم أساسية وضرورية لأولئك الذين يريدون البدء في دراسة مشكلة نظرية الأعداد .المفاهيم المتعلقة بالوظائف الحسابية مثل: الضرب ، والجمع ، ومنتج التواء ديريتشليت ، ومعاكسات ديريتشليت وصيغة انعكاس موبيوس ... , هي موضوع الفصل الثاني .وقد خصص الفصل الثالث لطرق التجميع ، بينما خصص الفصل الأخير لحل بعض المشكلات المتعلقة بالموضوع والموجودة في الأدبيات الرياضية.

الكلمات المفتاحية: الدوال الحسابية, القسمة الاقليدية, العدد الأولي, الجزء الصحيح, خوارزمية إقليدس, منتج التواء ديريتشليتة, صيغة انعكاس موبيس, المجموع.

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 : Mr. 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'ils m'ont fais en acceptant de juger ce travail.

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

Merci

Table de matières

Notations

$\mathbb{N} = \{1,2,3, \ldots\}$, l'ensemble des nombres entiers positifs.

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

$\mathbb{Z} = \{\ldots, -2, -1,0,1,2, \ldots\}$, l'ensemble des nombres entiers.

$\mathbb{C}$ l'ensemble des nombres complexes.

Les lettres $n, m \; et \; a, b, c, d, k, r, \ldots$ désignent des nombres entiers, alors que la lettre p indique un nombre premier.

$d|n$: d est un diviseur de n.

$d \nmid n$: d ne divise pas n.

$[x]$ est la partie entière de x (x nombre réel).

$\{x\}$ désigne la partie fractionnaire de x (x nombre réel).

$\gamma = 0.577\ 2 \ldots$ La constante d'EULER.

$f(x) = \mathrm{O}(1)$ signifie que f est bornée pour tout $x \in [x_0, +\infty[$.

$\mu(n)$ est la fonction de Möbius.

$\sigma(n)$ est la fonction somme de diviseur de n..

$\tau(n)$ est la fonction de nombre de diviseurs de n.

$\varphi(n)$ est la fonction de Euler.

$\omega(n)$ est la fonction nombre de facteurs premiers distincts de n.

$\Omega(n)$ est la fonction nombre total de facteurs premiers de n.

$\Lambda(n)$ est la fonction de von Mangoldt.

Soit D un Domain quelconque et $f: D \to \mathbb{C}$. Soit $g: D \to \mathbb{R}$, telle que $g(x) > 0 \; \forall \; x \in D$. Alors.

• $f \ll g$ ou $g = \mathrm{O}(g)$ s'il existe un constant $C > 0$ telle que $|f(x)| \leq Cg(x)$ pout tout $x \in D$.

Introduction

Le travail de ce mémoire est intitulé " Sur les fonctions arithmétiques". L'intérêt de ce thème vient du fait que ces fonctions sont l'outil fondamental de la discipline mathématique appelées "Théorie des nombres" une spécialité ayant de différentes applications importantes dans le vie courante ; Nous citons par exemple la "cryptographie". Ce qui témoigne la place de cette branche c'est qu'elle s'appelle la "Reine des mathématiques".

Une fonction arithmétique est une fonction définie de $\mathbb{N}$ dans $\mathbb{C}$. Les fonctions se trouvent en deux familles importantes: fonctions multiplicatives et fonctions additives. Une fonction arithmétique f est dite multiplicative (resp. additive) si chaque fois que m et n sont des entier positifs premier entre eux , on a $f(mn) = f(m)f(n)$ (resp. $f(mn) = f(m) + f(n)$).

Une fonction multiplicative a la propriété que sa valeur en un nombre entier naturel n est le produit de ses valeurs en chacune des puissances de nombres premiers figurant dans la factorisation de n en un produit de nombres premiers élevés à des puissances. Nous étudions dans ce travail certaines fonctions qui sont très importantes, à savoir, $\tau, \varphi, \omega, \Omega, \mu, \sigma$ ....

Ce mémoire est formé par quatre chapitres. L'outils de base nécessaires pour tout le mémoire font l'objet de première chapitre. Dans le deuxième chapitre, on a cité quelques propriétés des fonctions multiplicatives et additives puis on a cité les notions de produit de convolution de Dirichlet, Inverses de Dirichlet et la formule d'inversion de Möbius. Le troisième chapitre est consacré aux méthodes de sommation et quelques applications. Le dernier chapitre est dévoué aux différents problèmes résolu.

Chapitre 1

Outils de base

Ce chapitre présente les théorèmes fondamentaux de l'arithmétique concernant la divisibilité, le plus grand commun diviseur, division Euclidienne, nombres premiers, congruences, parties entières et fractionnaires. Dans ce sens on trouve le théorème 1.2.1 qui prouve que deux entiers quelconques admet un plus grand commun diviseur, le théorème 1.3.1 (Algorithme de division) et le théorème 1.4.1 (théorème fondamental de l'arithmétiques), selon lequel tout nombre entier supérieur à 1 peut être écrit, d'une façon unique, comme un produit de facteurs premiers.

1.1 Divisibilité

Définition 1.1.1[3] Soient $a, b \in Z$ avec $a \neq 0$. On dit que a divise b,ou que b multiple de a, s'il existe $k \in Z$ tel que $b = ka$ et on noté $a|b$. Le cas où a ne divise pas b sera noté par $a \nmid b$

Dans ce cas, on dit aussi que a est divisible par b, ou que a est un diviseur de b ou que b est un multiple de a.

La proposition suivante établit plusieurs propriétés fondamentales de la divisibilité.

Proposition 1.1.1[1] Soient $d, n \in \mathbb{Z}$, avec $d \neq 0$. Nous listons dans le suite quelques propriétés les plus utilisés de la division

$(a)\ n\|n$	$(propriété\ réflexive)$
$(b)\ d\|n\ et\ n\|m\ implique\ d\|m$	$(propriété\ transitive)$
$(c)\ d\|n\ et\ d\|m\ implique\ d\|(an + bm)$	$(propriété\ de\ linéarité)$
$(d)\ d\|n\ implique\ ad\|an$	$(propriété\ de\ multiplication)$
$(e)\ ad\|an\ et\ a \neq 0\ implique\ d\|n$	$(loi\ d'annulation)$
$(f)\ 1\|n$	*(1 divise tout nombre entier)*
(g) $d\|n$ *and* $n \neq 0$ *implique* $\|d\| \leq \|n\|$	*(propriété de comparaison)*

Si $d|n$ alors n/d est appelé le diviseur conjugué de d.

1.2 Plus grand commun diviseur

Définition 1.2.1 Soient $a, b \in \mathbb{Z}$, le plus grand commun diviseur de a et b, qui ne sont pas tous les deux nuls, est le plus grand entier positif qui divise à la fois a et b.

Le plus grand commun diviseur de a et b s'écrit (a, b) ou $pgcd(a, b)$.

Exemple 1.2.1

$-\ pgcd(24,16) = 8, pgcd(21,28) = 7.$

$-\ pgcd(a, ak) = a, pour\ tout\ k \in \mathbb{Z}\ et\ a \geq 0.$

$-\ Cas\ particuliers. Pour\ tout\ a \geq 0 :\ pgcd(a, 0) = a\ et\ pgcd(a, 1) = 1.$

Citons dans le suite quelques théorèmes qui facilitent le calcul le plus grand commun diviseur.

Théorème 1.2.1[1] Étant donné deux entiers quelconques a et b, il existe un diviseur commun d de a et b de la forme

$$d = ax + by.$$

Preuve. Nous supposons d'abord que $a \geq 0$ et $b \geq 0$. Nous utilisons l'induction sur n, où $n = a + b$. $Si\ n = 0$ alors $a = b = 0$ et on peut prendre $d = 0$ avec $x = y = 0$. Supposons alors que le théorème a été démontré pour $0, 1, 2, \ldots, n - 1$. Par symétrie, on peut supposer $a \geq b$. Si $b = 0$ prendre $d = a, x = 1,\ y = 0$. Si $b \geq 1$ appliquer le théorème à $a - b$ et b. Puisque $(a - b) + b = a = n - b \leq n - 1$, l'hypothèse d'induction est applicable et il existe un diviseur commun d de $a - b$ et b de la forme $d = (a - b)x + by$. Ce d divise aussi $(a - b) + b = a$ donc d est un diviseur commun de a et b et nous avent $d = ax + (y - x)b$, la combinaison linéaire de a et b. Nous devons prouver que chaque diviseur commun divise d pour terminer la preuve. Cependant, un diviseur commun divise a et b, et donc divise d en raison de la linéarité.

Si a < 0 ou b < 0 (ou les deux), on peut appliquer le résultat qui vient d'être démontré à $|a|$ et $|b|$. Alors il existe un diviseur commun d de $|a|$ et $|b|$ de la forme

$$d=|a|x + |b|y.$$

Si $a \leq 0$, $|a|x = -ax = a(-x)$. De même , si $b < 0$, $|b|y = b(-y)$. D'où d est encore une combinaison linéaire de a et b. ■

Théorème 1.2.2[1] Soient $a, b \in \mathbb{Z}$, il n'existe qu'un seul entier d présentant les propriétés suivantes

(i) $d \geq 0$ $(d\ est\ non\ négatif)$.
(ii) $d|a\ et\ d|b$ $(d\ est\ un\ diviseur\ commun\ de\ a\ et\ b)$.
(iii) $e|a\ et\ e|b\ implique\ e|d$ $(chaque\ diviseur\ commun\ divise\ d)$.

Preuve. D'après le théorème 1.2.1, il existe au moins un d satisfaisant aux conditions (ii) et (iii) . De plus, $-d$ satisfait ces conditions. Mais si d' satisfait (ii) et (iii), alors $d|d'$ et $d'|d$, donc $|d| = |d'|$. Il y a donc exactement un $d \geq 0$ satisfaisant (ii) et (iii) . ■

Remarque 1.2.1[1] Dans le théorème 1.2.2, $d = 0$ si, et seulement si, $a = b = 0$. Sinon $d \geq 1$.

Théorème 1.2.3[1] Le pgcd a les propriétés suivantes :

a) $(a, b) = (b, a)$ (loi commutative)
b) $(a, (b; c)) = ((a, b), c)$ (loi associative)
c) $(ac, bc) = |c|(a, b)$ (loi distributive)
d) $(a, 1) = (1, a) = 1$, $(a, 0) = (0, a) = |a|$.
.

Preuve. On prouve seulement (c). Soit $d = (a, b)$ et soit $e = (ac, bc)$. On veut prouver que $e = |c|d$. Écrire $d = ax + by$. Ensuite nous avons

$$cd = acx + bcy. \quad (1)$$

Donc $cd \mid e$ parce que cd divise à la fois ac et bc. De plus, l'équation (1) montre que $e \mid cd$ parce que $e \mid ac$ et $e \mid bc$. D'où $|e| = |cd|$, ou $e = |c|d$. ■

1.3 Division Euclidienne

L'algorithme de division est le fondement autour duquel s'articule tout notre développement. Il en résulte qu'un nombre entier a peut être divisé par un nombre entier positif b avec un résidu inférieur à b.

l'axiome 1.3.1 [1]Tout sous-ensemble S non vide de $\mathbb{Z}_{\geq 0}$ contient un élément minimal. De plus, si S est majoré, alors il contient aussi un élément maximal

Théorème 1.3.1[8] (Division algorithme) Soient $a, b \in \mathbb{Z}$ et $b \geq 1$. Il existe des entiers uniques q et r tels que

$$a = bq + r \quad (1.1)$$

et

$$0 \leq r < b - 1. \quad (2.2)$$

Dans la division de a par b, l'entier q est appelé le quotient, tandis que l'entier r est appelé le reste.

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

$$a - bx.$$

Avec $x \in \mathbb{Z}$. Si $a \geq 0$, alors $a = a - d.0 \in S$. Si $a < 0$, soit $x = -y$, où y est un entier positif. Puisque d est positif, on a $a - bx = a + by \in S$, si y est suffisamment grand. Par conséquent, S est un ensemble non vide d'entiers non négatifs. Par le principe du minimum, S contient un plus petit élément r, et . $0 \leq r = a - bq$ pour un certain $q \in Z$. Si $r \geq d$, alors

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

et $r - b \in S$, ce qui contredit la minimalité de r. Par conséquent, q et r satisfont les conditions (1.1) et (1.2). Soit q_1, r_1, q_2, r_2des entiers tels que

$$a = bq_1 + r_1 = bq_2 + r_2 \qquad \text{et} \qquad 0 \leq r_1, r_2 \leq b - 1.$$

Ensuite

$$|r_1, r_2| \leq b - 1$$

et

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

si $q_1 \neq q_2, alors$

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

et

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

ce qui est impossible. Par conséquent, $q_1 = q_2 et\ r_1 = r_2$ cela prouve que le quotient et le reste sont uniques. ■

Le théorème suivant est très important en mathématique est nous facilite le processus du calcul du plus grand commun diviseur et il s'appelle Algorithme d'Euclide.

Théorème 1.3.2[3]**(Algorithme d'Euclide).** On souhaite calculer le pgcd de $a, b \in \mathbb{N}$. On peut supposer $a \geq b$. On calcule des divisions euclidiennes successives. Le pgcd sera le dernier reste non nul. En effet :

– division de a par $b, a = bq_1 + r_1$.

$pgcd(a, b) = pgcd(b, r_1)\ et\ si\ r_1 = 0$, alors $pgcd(a, b) = b$

sinon on continue :

$$\begin{array}{rcll} b & = & r_1q_2 + r_2 & \text{pgcd(a, b)} = \text{pgcd(b}, r_1) = \text{pgcd}(r_1, r_2), \\ r_1 & = & r_2q_3 + r_3 & \text{pgcd(a, b)} = \text{pgcd} = (r_2, r_3) \\ \ldots & = & \ldots & \ldots \\ r_{k-2} & = & r_{k-1}q_k + r_k & \text{pgcd(a, b)} = \text{pgcd}(r_{k-1}, r_k) \\ r_{k-1} & = & r_kq_k + 0 & \text{pgcd(a, b)} = \text{pgcd}(r_k, 0) = r_k. \end{array}$$

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leq r_{i+1} < r$. Ainsi l'algorithme se termine car nous sommes sûr d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b \geq r_1 \geq r_2 \geq \ldots \geq 0$.

Exemple 1.3.1 Calculons le pgcd de a = 700 et b = 125

$$700 = 125 \times 5 + 75$$

$$125 = 75 \times 1 + 50$$

$$75 = 50 \times 1 + 25$$

$$50 = 25 \times 2 + 0$$

ainsi $pgcd(700,125) = 25$.

1.4 Nombres premiers

Les nombres premiers sont en quelque sorte les briques élémentaires des entiers car tout entier s'écrit comme produit de nombres premiers

Définition1.4.1[1] Un entier n est dit premier si $n > 1$ et si le seul nombre positif les diviseurs de n sont 1 et n. Si $n > 1$ et si n n'est pas premier, alors n est appelé composé.

Notation 1.4.2 Deux entiers a, b sont premiers entre eux si $pgcd(a, b) = 1$

Exemple 1.4.1 Les nombres premiers inférieurs à 100 sont 2 , 3 , 5 , 7,11, 13, 17, 19, 23, 29,31, 37, 41,43 , 47 , 53 , 59 , 61 , 67, 71 , 73 , 79 , 83 , 89 et 97.

Notation 1.4.1 Les nombres premiers sont généralement notés par p, p', p_i.

Théorème 1.4.1[1] (Le théorème fondamental de l'arithmétique) Tout entier $n \geq 2$ est soit un nombre premier soit un produit de nombres premiers

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

où p_i sont des nombres premiers et α_i sont des entiers positifs $(i = 1, \ldots, r)$.

Proposition 1.4.1[1] Soient $a, b, n, a_1, \ldots, a_n$ sont des entiers positifs et p est un nombre premier. Alors

1. $p|ab \Rightarrow p|a$ ou $p|b$.
2. $p|a_1, \ldots, a_n \Rightarrow p|a_i$pour certains $i \in \{1, \ldots, n\}$.
3. $p|a^n \Longrightarrow p|a$.

Maintenant nous sommes en mesure de prouver le théorème 1.4.1.

Preuve. Soit S l'ensemble des entiers composés ≥ 2 qui ne peuvent pas s'écrire comme un produit de facteurs premiers et supposons que $S = \emptyset$. En utilisant l'axiome 1.3.1, nous déduisons que S a un plus petit élément noté m. Puisque m n'est pas un nombre premier, nous avons $m = ab$ avec $a > 1$ et $b > 1$. Puisque $a < m$, $b < m$ et que m est le plus petit élément de S, on a $a, b \notin S$, et alors on peut écrire a et b comme un produit de facteurs premiers, et donc $m = ab$ peut aussi être écrit comme un produit de facteurs premiers, ce qui donne une contradiction. Par conséquent, nous avons prouvé que S = ∅.

Supposez que.

$$n = \prod_{i=1}^{r} {p_i}^{\alpha_i} = \prod_{i=1}^{s} {q_i}^{\beta_i}.$$

avec p_i , q_j nombres premiers et r, s, α_i , β_j entiers positifs. En utilisant la proposition 1.4.1, nous déduisons que chaque facteur p_i est un facteur q_j, et donc, en particulier, nous avons $r = s. r = s$, et sans perte de généralité, nous pouvons supposer que $p_i = q_j$ pour $i = 1, \ldots, r$. Enfin, si nous avions $\alpha_i < \beta_j$ pour tout entier $i \in \{1, \ldots, r\}$, alors le nombre $n/{p_i}^{\alpha_i}$ aurait deux décompositions, l'une impliquant p_i et l'autre non. l'autre non. Ceci est impossible par l'argument ci-dessus. Par symétrie, nous ne peut pas non plus avoir $\alpha_i > \beta_j$. Ainsi nous avons $\alpha_i = \beta_j$ pour tout i. ■

Exemple 1.4.2 Soit

1. $n = 3465 = 3^2 \times 7 \times 5 \times 11$
2. $m = 2695 = 5 \times 7^2 \times 11.$

Les résultats suivants résument certaines des utilisations du théorème 1.4.1.

Corollaire 1.4.1[2] Soit $n \in \mathbb{Z}$ avec $n \geq 2$. D'après la théorème 1.4.1 n s'écrire de la forme

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

1. Soit $d \in \mathbb{Z}$, avec $d > 0$, Alors nous avons

$$d | n \iff d = \prod_{i=1}^{r} {p_i}^{\beta_i} \ avec \ 0 \leq \beta_i \leq \alpha_i.$$

2. Soit $m = \prod_{i=1}^{r} {p_i}^{\beta_i}$ est entier positif. Alors nous avons

$$(n, m) = \prod_{i=1}^{r} {p_i}^{\min(\alpha_i, \beta_i)}.$$

3. Supposons que $(n, m) = 1$. Alors tout diviseur d de mn peut s'écrire $d = ab$ avec $a \mid m$, $b \mid n$ et $(a, b) = 1$.

Exemple 1.4.3 Trouver $(5187875,155925)$. On a

$5187875 = 5^3 \times 7^3 \times 11^2, \qquad 155925 = 3^4 \times 5^2 \times 7 \times 11.$

Donc $(5187875,155925) = 5^2 \times 7 \times 11 = 1925$

1.5 Congruences

Définition 1.5.1[1] Soient $a, b \ et \ n$ sont des entiers avec $n > 0$. Nous disons que a et b sont congruents modulo n si.

$$. a = kn + b , \quad k \in \mathbb{Z}.$$

Nous écrivons dans ce cas

$$a \equiv b(\ mod\ n).$$

Remarquons que n divise a si et seulement si $a \equiv 0\ (mod\ n)$.

Proposition 1.5.1[1] La congruence est une relation d'équivalence. C'est-à-dire que nous avons

a) Si $a \equiv a(mod\ n)$ (réflexive)
b) Si $a \equiv b(mod\ n)$ alors $b \equiv a(mod\ n)$ (symétrique)
c) Si $a \equiv b(mod\ n)$ et $b \equiv c(mod\ n)$ alors $a \equiv c(mod\ n)$ (transitive)

.

Preuve. Par la définition 1.5.1 on a
(a) $a = 0 \times n + \ a \Leftrightarrow a \equiv a[b]$.
(b) a − b = kn $\Longrightarrow b - a = -kn$.
(c)$a - b = kn\ , b - c = k'n \Rightarrow a - c = (a - b) + (b - c) = kn + k'n\ (k + k')n, (on\ pose\ (k + k') = k''alors\ a - c = k''n$.
Alors la relation «congru modulo n» est une relation d'équivalence. ■

Exemple 1.5.1
$-17 \equiv 7\ (mod\ 8)\ , 90 \equiv 0\ (mod\ 10)\ , 19 \equiv -2\ (mod\ 21)$,
$12^{20xx} \equiv 1^{20xx}\ (mod\ 11) \equiv 1\ (mod\ 11)$, où est l'année en cours.

Théorème 1.5.1[1] (théorème de Fermat). Soient a est un entier p est un nombre premier avec $p \nmid n$. Alors

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

d'une façon équivalente, si a est un entier, alors

$$a^p \equiv a\ (mod\ p)$$

Exemple 1.5.2 Soient $a = 12, p = 7$
$12^7 = 35831808 = 5118828 \times 7 + 12$.Alors

- $12^7 \equiv 12(mod\ 7)$. D'où $12^7 \equiv 5(mod\ 7)$..

$12^{7-1} = 12^6 = 426569 \times 7 + 1$. Alors

- $12^6 \equiv 1(mod\ 7)$.

1.6 Parties entières et fractionnaires

Pout tout $x\ \in\ \mathbb{R}$ on a

- Le partie entière de x est l'entier $[x]$ vérifiant :

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

- Le partie fractionnaire de *x* est la quantité $x\ -\ [x]$. Notée par $\{x\}$.

Proposition 1.6.1[2] Soient $x, y\ \in\ \mathbb{R}$. Les affirmations suivantes sont vraies

(i) $[x] = x + 0(1)$. Pour être plus précis, on peut écrire $x = [x] + \theta$ avec $\theta \in [0,1[$.
(ii) Soit $n\ \in\ \mathbb{Z}$. Alors $[x\ +\ n]\ =\ [x]\ +\ n$ et $\{x\ +\ n\}\ =\ \{x\}$.

(iii) $[x]+[y] \leq [x+y] \leq [x]+[y]+1$.

(iv) Supposons $x \geq 0$. Alors

$$\sum_{n \leq x} 1 = [x].$$

(v) Soit $d \in \mathbb{N}$ et supposons $x \geq 0$. $\left[\frac{x}{d}\right]$ est le nombre de multiples de d qui sont plus petits que x.

(vi) Soient $a < b$ des nombres réels. Alors le nombre d'entiers dans l'intervalle $[a, b]$ est

$$[b-1] \quad ou \quad [b-1]+1.$$

(vii) Soit $0 \leq \delta < \frac{1}{2}$ un nombre réel. Alors

$$\begin{cases} [x+\delta]-[x]=1 & \Leftrightarrow \quad \{x\} \geq 1-\delta, \\ [x]-[x+\delta]=1 & \Leftrightarrow \quad \{x\} \geq 1. \end{cases}$$

CHAPITRE 2
Fonctions arithmétiques

2.1 fonctions arithmétiques : Quelques exemples

Une fonction $f: \mathbb{N} \to \mathbb{C}$ est dit arithmétique ; dans la suite de cette section ou en donne quelques exemples

Définition 2.1.1[2] ($\omega(n)$ nombre de facteurs premiers distincts de n) définie par ω(1)=0 et pour tout $n \geq 2$,avec $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $\omega(n) = k$. C'est - à – dire

$$\omega(n) = \begin{cases} 0 & si\ n = 1, \\ k & si\ n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}. \end{cases}$$

Exemple 2.1.1

- $\omega(53) = 1 \quad (53\ est\ nombre\ premier\ )$.
- $\omega(450) = 3 \quad (450 = 2 \times 3^2 \times 5^2\ alors\ k = 3)$.
- $\omega(539) = 2 \quad (539 = 7^2 \times 11\ alors\ k = 2)$.
- $\omega(25200) = 4 \quad (25200 = 2^4 \times 3^2 \times 5^2 \times 7\ alors\ k = 4)$

Définition 2.1.2[4] ($\Omega(n)$ nombre total de facteurs premiers de n) définie par $\Omega(1) = 0$ est pour tout $n \geq 2$, avec $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, $\Omega(n) = a_1 + a_2 \dots a_k$. C'est - à – dire

$$\Omega(n) = \begin{cases} 0 & si\ n = 1, \\ a_{1+}a_2 + \cdots + a_k & si\ n \geq 2. \end{cases}$$

Exemple 2.1.2 Soit p un nombre premier, alors

- $\omega(p) = 1 = \Omega(p)$
- $\omega(p^2) = 1,\ \Omega(p^2) = 2$

Exemple 2.1.3

- $\Omega(450) = 5 \quad (450 = 2 \times 3^2 \times 5^2\ alors\ a_i = 5)$.
- $\Omega(539) = 3 \quad (539 = 7^2 \times 11\ alors\ a_i = 3)$.
- $\Omega(25200) = 9 \quad (25200 = 2^4 \times 3^2 \times 5^2 \times 7\ alors\ a_i = 9)$

Définition 2.1.3 [7] (Fonction Möbius) $\mu(n)$ est définie par

$$\mu(n) = \begin{cases} 1 & si \quad n = 1 \\ 0 & si \quad p^2|n \\ (-1)^k & autrement \end{cases}$$

Exemple 2.1.4

- $\mu(2) = -1$.
- $\mu(44) = 0$ ($car\ 2^2|44$).
- $\mu(154) = (-1)^3 = -1$ ($car\ 154 = 2 \times 7 \times 11$).
- $\mu(65) = (-1)^2 = 1$ ($car\ 65 = 5 \times 13$).

Définition 2.1.4[4] (Fonction d'Eluer) Pour $n \geq 1$ un entier $\varphi(n)$ est le nombre d'entiers positifs ne dépassent pas n est qui relativement premier avec n . C'est - à - dire

$$(1) \qquad \varphi(n) = \sum_{\substack{m \leq n \\ (m,n)=1}} 1,$$

Exemple 2.1.5

n	10	11	12	13	14	15	16	17	18	19
$\varphi = (n)$	4	10	4	12	6	8	8	16	7	18

Définition 2.1.5[4] (Fonction de von Mangoldt) $\Lambda(n)$ est définie par

$$\Lambda(n) = \begin{cases} \log(p). & si\ n = p^a, pour\ p\ est\ nombre\ premier\ et\ a \in \mathbb{N} \\ 0 & autrement. \end{cases}$$

Exemple 2.1.6.

n	49	121	125	289	361	841	1369	4913	50653
$\Lambda(n)$	$\log(7)$	$\log(11)$	$\log(5)$	$\log(17)$	$\log(19)$	$\log(29)$	$\log(37)$	$\log(17)$	$\log(37)$

Définition 2.1.6[2] (Fonctions somme des diviseurs de n) Soient $k \geq 0$ et $n \geq 1$ deux entiers. Nous définissions σ_k par

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Si $k = 1$ on note $\sigma_1(n)\ par\ \sigma(n)$. Donc

$$\sigma_1(n) = \sigma(n) = \sum_{d|n} d\,.$$

est la somme des diviseurs de n.

Si $k = 0$ on note $\sigma_0(n)\ par\ \tau(n)\ ou\ d(n)$. Donc

$$\sigma_0(n) = d(n) = \tau(n) = \sum_{d|n} 1$$

est le nombre des diviseurs de n.

Exemple 2.1.7

n	10	11	12	13	14	15	16	17	18
$\sigma_k(n)\ k=2$	130	122	210	14	250	260	341	18	455
$\sigma(n)$	18	12	28	1	24	24	31	18	39
$\tau(n)$	4	2	6	2	4	4	5	2	6

Définition 2.1.7[2] (Fonction constante) définie par $f(n) = c$ pour tout $n \in \mathbb{N}$. En particulier, $\mathbf{1}(n)$ désigne le fonction égale à 1 pour tout n.

Définition 2.1.8[4] **(**Fonction d'identité) définie par $id(n) = n$ pour tout $n \in \mathbb{N}$.

Définition 2.1.9[4] **(**Fonction unité) pour tout $n \in \mathbb{N}$, définie par

$$e(n) = \begin{cases} 1 & si\ n = 1, \\ 0 & sinon. \end{cases}$$

2.2 Fonctions multiplicatives et additives

Les fonctions arithmétiques se divisent en deux types : Les fonctions qui sont multiplicatives et celles qui sont additives, ci après on donne leurs définitions .

Définition 2.2.1[2] Soit f une fonction arithmétique

- f est multiplicatif si $f(1) \neq 0$ et si , pour m , n deux entiers positifs tels que $(m,n) = 1$, on a
$$f(mn) = f(m)f(n). \qquad (2.1)$$

Remarque 2.2.1 [2]

- f est complètement multiplicative si $f(1) \neq 0$ et si $f(m,n) = f(m)f(n)$ pour tous les entiers positifs m , n.
- f est fortement multiplicative si f est multiplicative et $f(p^a) = f(p)$ si pour tout a $a \geq 1$ entier et p premier.

Lemme 2.2.1[2] Soit f une fonction arithmétique, f est multiplicative si et seulement si $f\ (1) = 1$ et pour tout $n = p_1^{a_1} \dots\ p_r^{a_r}$ où les p_i $(i = 1,2,3 \dots ., r)$ sont des nombres premiers distincts, on a

$$f(n) = \prod_{k=1}^{r} f\left(p_k^{a_k}\right). \qquad (2.2)$$

Preuve. Soient $m = p_1^{a_1} \dots p_r^{a_r}$, $n = q_1^{b_1} \dots q_r^{b_r}$ deux entiers positifs premiers entre eux. En utilisant (2.2) et le fait que $p_i \neq q_j$on obtient

$$f(mn) = f\left(p_1^{a_1} \dots p_r^{a_r} q_1^{b_1} \dots q_r^{b_r}\right) = \prod_{k=1}^{r} f(p_k^{a_k}) \prod_{k=1}^{r} f\left(q_k^{b_k}\right) = f(m)f(n).$$

et donc f satisfait (2.1) car $f\,(1) = 1 \neq 0$, on en déduit que f est multiplicative. Inversement, soit f une fonction multiplicative. L'utilisation de (2.1) avec $m = n = 1$ donne $f\,(1) = f\,(1)f\,(1)$ de sorte que $f\,(1) = 1$ puisque $f\,(1) \neq 0$. Soit maintenant $n_1, \dots, n_k$ des entiers qui sont deux à deux premiers entre eux. Par induction en utilisant (2.1), on obtient

$$f(n_1 \dots n_k) = f(n_1) \dots f(n_k).$$

Ainsi, si $n = p_1^{a_1} \dots p_r^{a_r}$ où les p_i sont des nombres premiers distincts, on en déduit que f satisfait (2.2) . ■

Exemple 2.2.1 Soit $f_a(n) = n^a$ où a est un nombre réel . Cette fonction est complètement multiplicatif.

On a

$$f_a(mn) = (mn)^a \qquad avce\ a \in \mathbb{R}$$

$$f_a(mn) = m^a n^a$$

$$f_a(mn) = f_a(m)f_a(n).$$

Exemple 2.2.2 La fonction möbius μ est une fonction multiplicative. En effet soient

$$m = p_1' p_2' \dots \dots p_r' \quad et \quad n = q_1' q_2' \dots \dots q_s'$$

On a

$$\mu(1) = 1 \neq 0 \qquad \text{par définition.}$$

Si

$$p^2 | m \Rightarrow \mu(m) = 0$$

$$p^2 | n \Rightarrow \mu(n) = 0$$

Donc

$$\mu(mn) = \mu(m)\mu(n) = 0.$$

Si $n = \prod_{i=1}^{r} p_1 p_2 \dots p_r$ et $m = \prod_{i=1}^{s} q_1 q_2 \dots q_s$, alors

$$\mu(mn) = \mu(p_1 p_2 \dots\dots p_r\, q_1 q_2 \dots \dots\dots q_{s)}$$

r+s fois

$$\mu(mn) = (-1)^{r+s}$$

$$\mu(mn) = (-1)^r\,(-1)^s$$

$$\mu(mn) = \mu(p_1 p_2 \dots\dots p_r)\mu(q_1 q_2 \dots \dots\dots q_s)$$

$$\mu(mn) = \mu(m)\mu(n).$$

Exemple 2.2.3 La fonction τ est multiplicative

Clairement $\tau(1) = 1 \neq 0$.

Soient $m > 1$, $n > 1$; alors $m = p_1^{k_1} \dots p_r^{k_r}$, $n = p_1^{j_1} \dots p_s^{j_s}$.

$$mn = (p_1^{k_1} \dots p_r^{k_r})(p_1^{j_1} \dots p_s^{j_s})$$
$$\tau(mn) = (k_1 + 1)(k_2 + 1) \dots (k_r + 1)(j_1 + 1)(j_2 + 1) \dots (j_s + 1),$$
$$\tau(mn) = \tau(m)\tau(n) .$$

Définition 2.2.2[2] f est additive si, pour m , n deux entiers positifs tel que $(m, n) = 1$, on a

$$f(mn) = f(m) + f(n). \qquad (2.3)$$

Remarque 2.2.2[2]

- f est complètement additive si la condition $f(mn) = f(m) + f(n)$ est vraie pour tout entiers positifs m, n.
- f est fortement additive si f est additive et $si\ f(p^a) = f(p)$ pour toutes les puissances premières p^a.

Lemme 2.2.2[2] Soit f une fonction arithmétique, f est additive si et seulement si $f(1) = 0$ et pour tout $n = p_1^{a_1} \dots p_r^{a_r}$ où les p_i $(i = 1,2,3, \dots, r)$ sont des nombres premiers distincts, on a

$$f(n) = \sum_{k=1}^{r} f\left(p_k^{a_k}\right). \qquad (2.4)$$

Exemple 2.2.5 Calculons $\omega(120)$

$120 = 3 \times 5 \times 2^3$

$\omega(120) = \omega((3 \times 5) \times 2^3)$

$= \omega(3 \times 5) + \omega(2^3)$

$= 2 + 1 = 3.$

2.3 Quelques propriétés des fonctions multiplicatives et additives

Nous donnons ci-dessous dans le reste de cette section , quelques propriétés des fonctions multiplicatives et additives citées précédemment.

Proposition 2.3.1[1] Pour $n \geq 1$, la fonction de Möbius satisfait aux conditions suivantes

(a) $\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1\ si\ n = 1, \\ 0\ si\ n \geq 2. \end{cases}$

(b) $\mu(n)$ est multiplicative

preuve. (a) Si $n = 1$, la formule est toute à fait correcte. Supposons que $n > 1$, et écrivons $n = p_1^{a1} \dots p_k^{ak}$. Les seuls termes non nuls dans la somme $\sum_{d|n} \mu(d)$ proviennent de $d = 1$ et des diviseurs de n qui sont des produits de nombres premiers séparés.

$$\sum_{d|n}\mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2 \ldots p_k)$$

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

(b) Ceci est montré dans Exemple 2.2.2 ■

Exemple 2.3.1 Soit $n = 525 = 3 \times 5^2 \times 7$, l'ensemble des diviseurs est $= \{1,3,5,7,15,21,25,35,75,105,175,525\}$

$$\sum_{d|525}\mu(d) = \mu(1) + \mu(3) + \mu(5) + \mu(7) + \mu(15) + \mu(21) + \mu(25) + \mu(35) + \mu(75) + \mu(105) + \mu(175) + \mu(525)$$

$$= \mu(1) + [\mu(3) + \mu(5) + \mu(7)] + [\mu(3\times5) + \mu(3\times7) + \mu(5^2) + \mu(5\times7)] + [\mu(3\times5^2) + \mu(3\times5\times7) + \mu(5^2\times7)] + \mu(3\times5^2\times7)$$

$$= 1 + [(-1) + (-1) + (-1)] + [1 + 1 + 0 + 1] + [0 + (-1) + 0 + 0] + 0$$

$$= 0.$$

Théorème 2.3.1[1] La fonction d'Euler satisfait aux conditions suivantes :

(i) $\sum_{d|n}\varphi(d) = n, \ \forall\, n \in \mathbb{N}.$

(ii) $\varphi(n) = \sum_{d|n}\mu(d)\left(\frac{n}{d}\right).$

(iii) $\varphi(n)$ est multiplicative.

Preuve.(ii) La somme (1) définissant $\varphi(n)$ peut être réécrite sous la forme

$$\varphi(n) = \sum_{k=1}^{n}\left[\frac{1}{(n,k)}\right],$$

où maintenant k parcourt tous les entiers $\leq n$ Maintenant nous utilisons la proposition 2.3.1 (a) en remplaçant par (n,k) pour obtenir

$$\varphi(n) = \sum_{k=1}^{n}\sum_{d|(n,k)}\mu(d) = \sum_{k=1}^{n}\sum_{\substack{d|n\\ d|k}}\mu(d).$$

Pour un diviseur fixé d de n, nous devons additionner tous les k dans l'intervalle $1 \leq k \leq n$ qui sont des multiples de d. Si on écrit $k = qd$ alors $1 \leq k \leq n$ si et seulement si $1 \leq k \leq n/d$. Par conséquent, la dernière somme pour $\varphi(n)$ peut être écrite comme

$$\varphi(n) = \sum_{d|n}\sum_{q=1}^{n|d}\mu(d) = \sum_{d|n}\mu(d)\sum_{q)1}^{n|d}1 = \sum_{d|n}\mu(d)\frac{n}{d}.$$

Cela prouve (ii). ■

(iii) Voir [1]. ■

Théorème 2.3.2 [5]

(a) Soit p un nombre premier, et soit e un entier positif. Alors

$$\varphi(p^e) = (p-1)p^{e-1} = p^e - p^{e-1} = p^e\left(1-\frac{1}{p}\right).$$

(b) Soit $p_1 \dots p_r$ les facteurs premiers distincts de n, alors

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right).$$

Preuve . Soit p nombre premier, alors

(a) A partir de l'ensemble $\{1,2,\dots,p^e\}$ les nombres non relativement premiers à p^e sont exactement ceux divisibles par p, c'est-à-dire l'ensemble $\{p, 1p, 3p, \dots, p^e\}$. Il y en a p^{e-1} , donc le nombre total de nombres relativement premiers est

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

(b) Pour cette partie, nous utilisons la partie (a) et le Théorème 2.3.1(iii) . Étant donné $n = p_1^{e_1} \dots p_r^{e_r}$, nous calculons

$$\begin{aligned}\varphi(n) &= \varphi\left(p_1^{e_1}\dots p_r^{e_r}\right)\\ &= \varphi\left(p_1^{e_1}\right)\dots\varphi(p_r^{e_r})\\ &= p_1^{e_1}\left(1-\frac{1}{p_1}\right)\dots p_r^{e_r}\left(1-\frac{1}{p_r}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\dots\left(1-\frac{1}{p_r}\right).\end{aligned}$$

Nous pouvons maintenant calculer la fonction d'Euler pour tout entier que nous pouvons factoriser. C'est beaucoup plus rapide que de vérifier le plus grand commun diviseur pour tout entier positif inférieur à n. ■

Exemple 2.3.2

(a) Pour $n = 343$

$$\varphi(343) = \varphi(7^3) = 7^2(7-1) = 294.$$

(b) Pour $n = 15$

$$\varphi(15) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)$$
$$\varphi(15) = 15 \times \frac{2}{3} \times \frac{4}{5} = 8.$$

Théorème 2.3.3 [1] Si n≥1 on a

(3) $$\log(n) = \sum_{d|n} \Lambda(d).$$

Preuve. Le théorème est vrai si n = 1 puisque les deux membres sont nuls. Par conséquent, supposons que n > 1 d'après (théorème 1.4.1) nous écrivons

$$n = \prod_{k=1}^{r} p_k^{a_k}.$$

En prenant les logarithmes, nous avons

$$\log(n) = \sum_{k=1}^{r} a_k log(p_k)\,.$$

Considérons maintenant la somme à droite de (3) Les seuls termes non nuls dans la somme proviennent de ces diviseurs d de la forme p_k^m pour $m = 1, 2, \ldots, a_k \; et \; k = 1,2,\ldots,r$. Ainsi

$$\sum_{d|n} \Lambda(n) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log(p_k) = \sum_{k=1}^{r} a_k \log(p_k) = \log(n)\,,$$

Ce qui termine la prouve ■

Proposition 2.3.2 Soit p un nombre premier. Alors

(a) $\sigma(p) = 1 + p$.
(b) $\tau(p) = 2$.
(c) $\sigma_k(p) = 1 + p^k$.

Théorème 2.3.4[5] Soit p un nombre premier et soit m un entier positif. Alors

$$\sigma_k(p^m) = \sum_{i=0}^{m} p^{ki} = \begin{cases} m+1 & k = 0, \\ \dfrac{p^{k(m+1)} - 1}{p^k - 1} & k \geq 1. \end{cases}$$

Preuve. Les seuls diviseurs de p^m sont les puissances de p, $\{1, p^1, p^2, p^3, \ldots, p^{m-1}, p^m\}$. Ainsi,

$$\sigma_k(p^m) = 1 + p^k + p^{2k} + \cdots + p^{km} = \frac{p^{k(m+1)} - 1}{p^k - 1}.$$

Si $k = 0$, $\sigma_0(p^m) = \tau(p^m) = m + 1$. ■

2.4 Le produit de convolution de Dirichlet

Définition 2.4.1[2] Soient f et g deux fonctions arithmétiques. le produit de convolution de Dirichlet de f et g est la fonction arithmétique $f \star g$ définie par

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

Il faut remarquer que la seconde égalité ci-dessus découle du fait que l'application $d \rightarrow d'$ tel que $dd' = n$ est bijective.

Exemple 2.4.1 Pour $n = 18$. calculer la valeur de $(\mu \star \tau)(18)$. On détermine d'abord l'ensemble des diviseurs de 18 qui est $\{1,2,3,6,9,18\}$. Pour chaque facteur d , calculer la valeur de $\mu(d)$, $\tau\left(\frac{18}{d}\right)$ et leurs produit :

Facteur d	$\mu(d)$	Cofacteur $18/d$	$\tau\left(\frac{18}{d}\right)$	$\mu(d)\,\tau\left(\frac{18}{d}\right)$
1	1	18	6	6
2	-1	9	3	-3
3	-1	6	4	-4
6	1	3	2	2
9	0	2	2	0
18	0	1	1	0

enfin, additionnez les valeurs de la dernière colonne: 6-3-4+2=1 .

$(\mu \star \tau)(18) = 1$.

Le théorème suivant décrit les propriétés algébriques de la multiplication de Dirichlet.

Théorème 2.4.1[2] Le produit de convolution de Dirichlet est commutatif, associatif et possède un élément neutre qui est la fonction e_1. De plus, si $f\,(1) \neq 0$, alors f est inversible. Alors pour les fonction arithmétiques $f, g\ et\ h$ on a

$f \star g = g \star f$ (commutatif)

$(f \star g) \star h = f \star (g \star h)$ (associatif)

$f \star e_1 = e_1 \star f = f$ (élément neutre)

Preuve. La commutativité découle immédiatement de la Définition 2.4.1.Soient maintenant $f\ , g\ et\ h$ être trois fonctions arithmétiques et n un entier positif. Nous avons.

$$\big((f \star g) \star h\big)(n) = \sum_{d|n} (f \star g)(d) h\left(\frac{n}{d}\right) = \sum_{d|n} \left(\sum_{\delta|d} f(\delta) g\left(\frac{d}{\delta}\right) \right) h\left(\frac{n}{d}\right)$$

et

$$\big(f \star (g \star h)\big)(n) = \sum_{n|d} f(d)(g \star h)\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \sum_{\delta|(n|d)} g(\delta) h\left(\frac{n}{d\delta}\right).$$

Mettons $d = d\delta$ dans la dernière somme nous obtenons

$$\big(f \star (g \star h)\big)(n) = \sum_{d'|n} \sum_{d|d'} f(d) g\left(\frac{d'}{d}\right) h\left(\frac{n}{d'}\right) = \big((f \star g) \star h\big)(n)$$

Ce que établit l'associativité. Concernant l'élément neutre on a

$$(e_1 \star f)(n) = \sum_{d|n} e_1(d) f\left(\frac{n}{d}\right) = f(n).$$

Aussi, d'une façon analogue,

$$(f \star e_1)(n) = \sum_{d|n} f(d)\, e_1\left(\frac{n}{d}\right) = f(n).$$

D'où $$f \star e_1 = e_1 \star f = f.$$

Enfin, on prouve l'inversibilité en construisant par récurrence l'inverse g d'un f(-onction arithmétique f satisfaisant $f(1) \neq 0$. La fonction g est l'inverse de f si et seulement si $(f \star g)(1) = 1$ et $(f \star g)(n) = 0$ pour tout n>1. Cela équivaut à

$$\begin{cases} f(1)g(1) = 1 \\ \sum_{d|n} g(d) f\left(\frac{n}{d}\right) = 0 \quad (n \geq 2). \end{cases}$$

Puisque $f(1) \neq 0$, on a $g(1) = f(1)^{-1}$ par la première équation. Soit maintenant $n > 1$ et supposons que l'on ait prouvé qu'il existe des valeurs uniques $g(1), \ldots, g(n-1)$ satisfaisant les équations ci-dessus. Puisque $f(1) \neq 0$, la deuxième équation ci-dessus est équivalente à

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n \\ d \neq n}} g(d) f\left(\frac{n}{d}\right)$$

qui détermine $g(n)$ de manière unique par l'hypothèse d'induction, et cette définition de $g(n)$ montre que les équations ci-dessus sont satisfaites, ce qui complète preuve. ■

Notation 2.4.1 [2]

(i) Donc la condition $f(1) \neq 0$ est nécessaire et suffisante pour l'inversibilité . D'après (ii) du lemme 2.2.1, on déduit que toute fonction multiplicative est inversible. Le résultat suivant est d'une importance cruciale.

Théorème 2.4.2[2] Si f et g sont multiplicatives, alors $f \star g$ est multiplicative. .

preuve. Soient f et g deux fonctions multiplicatives et soit m, n des entiers positifs premiers enter aux. D'après Corollaire 1.4.1 (3) chaque diviseur d de mn peut s'écrire de manière unique sous la forme $d = ab$ avec $a \mid m, b \mid n$ et $(a,b) = 1$ de sorte que

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

et puisque f et g sont multiplicatives et $(a,b) = (m/a, n/b) = 1$, on en déduit que

$$(f \star g)(mn) = \sum_{a|m} \sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) = (f \star g)(m)(f \star g)(n)$$

Cela termine la preuve. ■

Exemple2.4.2

(1) $(\mathbf{1} \star \mathbf{1})(n) = \tau(n)$. En utilisant la définition on a

$$(\mathbf{1} \star \mathbf{1})(n) = \sum_{d|n} \mathbf{1}(d)\mathbf{1}\left(\frac{n}{d}\right)$$

$$= \sum_{d|n} 1 \cdot 1$$

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

(2) $(id \star \mathbf{1})(n) = \sigma(n)$. En effet

$$(id \star \mathbf{1})(n) = \sum_{d|n} id(d)\mathbf{1}\left(\frac{n}{d}\right).$$

Comme $\mathbf{1}\left(\frac{n}{d}\right) = 1 \ et \ id(d) = d$, on a

$$(id \star \mathbf{1})(n) = \sum_{n|d} d \cdot 1$$

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

2.5 Inverses de Dirichlet et La formule d'inversion de Möbius

Théorème 2.5.1[1] Si f est une fonction arithmétique avec $f(1) \neq 0$, il existe unique fonction arithmétique f^{-1}, appelée l'inverse de Dirichlet de *f*, tel que

$$f \star f^{-1} = f^{-1} \star f = e_1.$$

De plus, f^{-1} est donné par les formules de récurrence

$$f^{-1}(1) = \frac{1}{f(1)}, \qquad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(n) \qquad pour\ n > 1.$$

Preuve. Étant donné *f*, nous montrerons que l'équation $(f * f^{-1})(n) = e_1(n)$ a une solution unique pour les valeurs $f^{-1}(n)$. Pour $n = 1$, nous devons résoudre le équation

$$(f \star f^{-1})(1) = e_1(n)$$

qui se réduit à

$$f(1)f^{-1}(1) = 1.$$

Puisque $f(1) \neq 0$ il existe une seule et unique solution, à savoir $f^{-1}(1) = 1/f(1)$. Supposons maintenant que les valeurs de la fonction $f^{-1}(k)$ ont été déterminées de manière unique pour tout $k < n$. Alors nous devons résoudre l'équation

$(f \star f^{-1})(n) = I(n)$, ou

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0\,.$$

Cela peut être écrit comme suit

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Si les valeurs $f^{-1}(d)$ sont connues pour tous les diviseurs $d < n$, il il y'aura une seul valeur $f^{-1}(n)$, à savoir,

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d).$$

Ceci établit l'existence et l'unicité de f^{-1} . ■

Théorème 2.5.2[2] (Formule d'inversion de Möbius) Soient f et g deux fonctions arithmétiques. Alors on a

$$f = g \star 1 \iff g = f \star \mu$$

c'est-à-dire pour tous les entiers positifs n

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

Pour la preuve voir [2].

Chapitre 3

Méthodes de sommation

3.1 Valeurs moyennes des fonctions arithmétiques

Definition3.1.1[8] (Fonction unimodale) $f(t)$ est une fonction unimodale sur un intervalle I. S'il existe un nombre t_0 I tel que $f(t)$ est croissante pour $t \leq t_0$ et décroissante pour $t \geq t_0$.

Exemple 3.1.1 La fonction $f(t) = e^{-2(t-2)^2}$ est unimodale sur l'intervalle $[1\ , 4]$ avec $t_0 = 2$.

Trouvé t_0.

On calcule la dérivée $f'(t)$

$$f'(t) = -2(t-2)e^{-2(t-2)^2}.$$

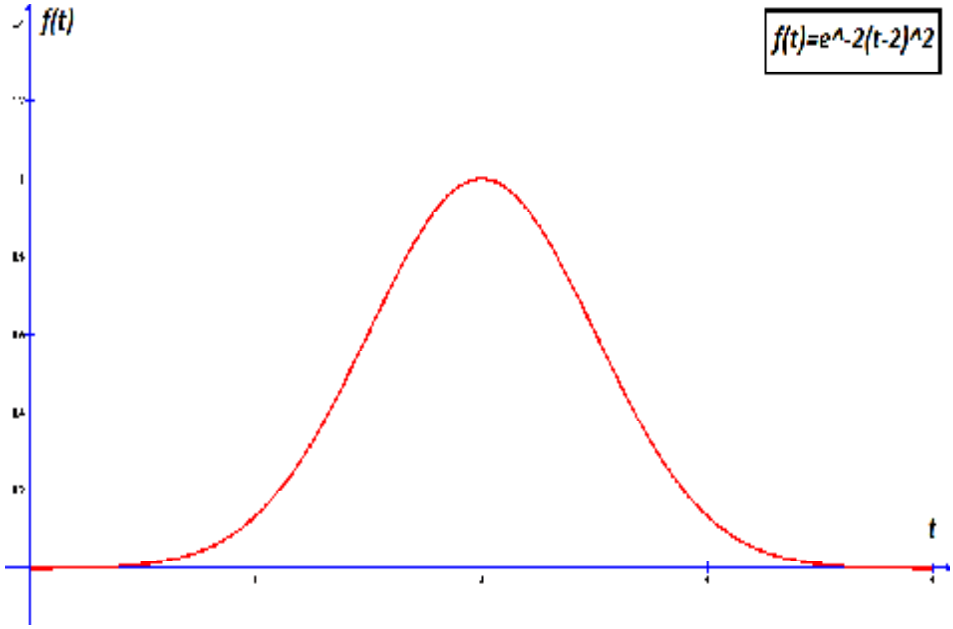
Calcule $f'(t) = 0$, alors

$$-2(t-2)e^{-2(t-2)^2} = 0$$

Donc

$$t_0 = 2.$$

La fonction f est croissante si $t \leq t_0$ et décroissante si $t \geq t_0$ donc la fonction f est unimodale sur intervalle $[1\ , 4]$ avec $t_0 = 2$.



la figure 3.1 Graphique de f.

Définition 3.1.2[8] La valeur moyenne F(x) d'une fonction arithmétique $f(n)$ est définie par

$$F(x) = \sum_{n \le x} f(n)$$

où la somme est sur tous les entiers positifs $n \le x$. En particulier, $F(x) = 0$ pour $x < 1$. La fonction $F(x)$ est aussi appelée fonction somme de f.

Nous allons citer deux outils simples mais puissants pour estimer les fonctions somme en théorie des nombres. Le premier est l'intégration et le second est la sommation partielle.

Théorème 3.1.1[8] Soient a, b deux entiers positives avec $a < b$ et $f(t)$ comme une fonction monotone sur l'intervalle $[a, b]$. Alors

1.

$$\min(f(a), f(b)) \le \sum_{n=a}^{b} f(n) - \int_a^b f(t)dt \le \max\big(f(a), f(b)\big). \qquad (3.1)$$

2. Soient x, y des nombres réels avec $y < [x]$, et $f(t)$ une fonction monotone non négative sur $[y, x]$. Alors

$$\left| \sum_{y<n\le x} f(n) - \int_a^b f(t)dt \right| \le \max\big(f(y), f(x)\big). \qquad (3.2)$$

3. Si $f(t)$ est une fonction unimodale non négative sur [1,∞], alors

$$F(x) = \sum_{n \le x} f(n) = \int_1^x f(t)dt + O(1). \tag{3.3}$$

Preuve .

1. Si $f(t)$ est croissante sur l'intervalle $[n, n+1]$, alors

$$f(n) \le \int_n^{n+1} f(t)dt \le f(n+1).$$

Si $f(t)$ est croissante sur l'intervalle [a, b], alors

$$a \le b \Leftrightarrow f(a) \le f(b)$$

et donc on a

$$f(a) + \int_a^b f(t)dt \le \sum_{n=a}^{b} f(n) \le f(b) + \int_a^b f(t)dt.$$

De même, si $f(t)$ est décroissante sur l'intervalle $[n, n+1]$, alors

$$f(n+1) \le \int_n^{n+1} f(t)dt \le f(n).$$

Si $f(t)$ est décroissante sur l'intervalle $[a, b]$, alors

$$a < b \Leftrightarrow f(b) < f(a)$$

et donc on a

$$f(b) + \int_a^b f(t)dt \le \sum_{n=a}^{b} f(t)dt \le f(a) + \int_a^b f(t)dt.$$

Ceci démontre (3.1).

2. Soit $f(t)$ une fonction non négative et monotone sur l'intervalle [y, x]. mettons $a = [y] + 1$ et $b = [x]$. On a $y < a \le b \le x$. Si $f(t)$ est croissante, alors .

$$\sum_{y<n\le x} f(n) = \sum_{a\le n\le b} f(n),$$

$$\le \int_a^b f(t)dt + f(b)$$

$$\le \int_y^x f(t)dt + f(b)$$

$$\le \int_y^x f(t)dt + f(x).$$

Comme

$$f(a) \geq \int_y^a f(t)dt$$

et

$$f(x) \geq \int_b^x f(t)dt,$$

il en résulte que

$$\sum_{y<n<x} f(n) \geq \int_a^b f(t)dt + f(a)$$

$$\geq \int_y^x f(t)dt - \int_b^x f(t)dt + f(a) - \int_y^a f(t)dt$$

$$\geq \int_y^x f(t)dt - f(x).$$

Par conséquent,

$$\left| \sum_{y<n\leq x} f(n) - \int_x^y f(t)dt \right| \leq f(x).$$

Maintiennent si $f(t)$ est décroissante, alors

$$\sum_{y<n\leq x} f(n) = \sum_{a<n\leq b} f(n)$$

$$\leq \int_a^b f(t)dt + f(a)$$

$$\leq \int_a^b f(t)dt + f(y).$$

Vu que

$$f(b) \geq \int_b^x f(t)dt$$

et

$$f(y) \geq \int_y^x f(t)dt$$

Il s'ensuit que

$$\sum_{y<n\leq x} f(n) \geq \int_a^b f(t)dt + f(b)$$

$$\geq \int_a^b f(t)dt + f(b) - \int_y^a f(t)dt - \int_y^a f(t)dt$$

$$\geq \int_a^b f(t)dt + f(y)$$

et donc

$$\left| \sum_{y<n\leq x} f(n) - \int_x^y f(t)dt \right| \leq f(y).$$

Cela prouve (3.2).

3. Si $f(t)$ est non négative et unimodale sur $[1,\infty]$ elle est bornée, alors (3.3) suit (3.2). Dans ce cas on remplace y par 1 on aura

$$\sum_{1<n\leq x} f(n) - \int_1^x f(t)dt = O(1)$$

$$\sum_{n\leq x} f(n) + f(1) - \int_x^y f(t)dt = O(1)$$

$$\sum_{n\leq x} f(n) = \int_1^y f(t)dt + O(1).$$

Cela prouve (3.3). ■

Maintenant comme application nous donne le résulte suivant.

Théorème 3.1.3[8] Pour $x \geq 2$,

$$\sum_{n\leq x} log\, n = x\, log\, x - x + O(log\, x).$$

Preuve. La fonction $f(t) = log\, t$ est croissante sur $[1, x]$. Par le théorème 3.1.1 (3.1),

$$\min\big(f(1), f(x)\big) \leq \sum_{n=1}^{x} f(n) - \int_1^x f(t)dt \leq \max\big(f(1), f(x)\big).$$

$$\log 1 = 0 \leq \sum_{n=1}^{x} \log n - \int_1^x \log t\, dt \leq \log x$$

$$\int_1^x \log t\, dt \leq \sum_{n\leq x} \log n \leq \log x + \int_1^x \log t\, dt\ .$$

Donc

$$\sum_{n\le x}\log n = x\log x - x + O(\log x).$$

Cela termine la prouve. ■

Théorème 3.1.4[8] (Sommation partielle) Soient les fonctions arithmétiques f et g. Posons

$$F(x) = \sum_{n\le x} f(n).$$

1. Soient a et b sont des entiers positive avec $a < b$. Alors

$$\sum_{n=a+1}^{b} f(n)g(n) = F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b-1} F(n)\big(g(n+1) - g(n)\big). \qquad (3.4)$$

2. Soient x et y des nombres réels positifs avec $[y] < [x]$ et $g(t)$ une fonction ayant la dérivée continue sur l'intervalle $[y, x]$. Alors

$$\sum_{n=a+1}^{b} f(n)g(n) = F(x)g(x) - F(y)g(y) - \int_1^x F(t)g'(t)dt. \qquad (3.5)$$

3. En particulier, si $x \ge 2$ et $g(t)$ est continument différentiable sur $[1, x]$. Alors

$$\sum_{n\le x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)dt. \qquad (3.6)$$

Preuve.

1. L'identité (3.4) est un calcul simple.

$$\sum_{n=a+1}^{b} f(n)g(n)$$

$$= \sum_{n=a+1}^{b} \big(F(n) - F(n-1)\big)g(n)$$

$$= \sum_{n=a+1}^{b} (F(n)g(n) - \sum_{n=a}^{b-1} F(n)g(n+1)$$

$$= F(b)g(b) - F(a)g(a+1) - \sum_{n=a+1}^{b+1} F(n)\big(g(n+1) - g(n)\big).$$

Cela prouve (3.4).

2. Si $g(t)$ est une fonction ayant le dérivée continue sur $[y, x]$, alors

$$g(n+1)-g(n)=\int_n^{n+1} g'(t)dt.$$

Puisque F(t) = F(n) pour $n \le t < n+1$, on aura

$$F(t)=\sum_{i\le t} f(i)$$

$$F(n)=\sum_{i\le n} f(i)$$

et $n \le t < n+1$,donc $F(t)=F(n)$.

il s'ensuit que .

$$F(n)\big(g(n+1)-g(n)\big)=\int_n^{n+1} g'(t)dt.$$

Posons $a=[y]$ et $b=[x]$. Puisque $a \le y < a+1 \le b \le x < b+1$, on a

$$\sum_{y<n\le x} f(n)g(n)=\sum_{n=a+1}^{b} f(n))g(n)$$

$$=F(x)g(b)-F(a)g(a+1)-\sum_{n=a+1}^{b-1} F(n)(g(n+1)-g(n))$$

$$=F(x)g(b)-F(y)g(a+1)-\sum_{n=a+1}^{b-1} F(n)(g(n+1)-g(n))$$

$$=F(x)g(b)-F(y)g(a+1)-\sum_{n=a+1}^{b-1}\int_n^{n+1} F(t)g'(t)dt$$

$$=F(x)g(x)-F(y)g(y)-F(x)\big(g(x)-g(b)\big)-F(y)\big(g(a+1)-g(y)\big)-\int_{a+1}^{b} F(t)g'(t)dt$$

$$=F(x)g(x)-F(y)g(y)-\int_y^x F(t)g'(t)dt.$$

Cela prouve (3.5).

3. Si $x \ge 2$ et $g(t)$ est continument différentiable sur $[1,x]$, alors

$$\sum_{n\le x} f(n)g(n)=f(1)g(1)+\sum_{1<n\le x} f(n)g(n)$$

$$= f(1)g(1) + F(x)g(x) - F(1)g(1) - \int_1^x F(t)g'(t)dt$$

$$= F(x)g(x) - \int_1^x F(t)g'(t)dt.$$

Cela prouve (3.6). ■

Maintenant comme application du théorème nous citons les résultats suivants.

Théorème 3.1.5[8] Si $x \geq 1$,

$$\sum_{n \leq x} \frac{1}{n} = \log x + \gamma + r(x),$$

où

$$0 < \gamma = 1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt < 1$$

et

$$|r(x)| < \frac{1}{x}.$$

Preuve. Puisque $0 \leq \{t\} < 1$ pour tout t, nous avons

$$0 < \int_1^{\infty} \frac{\{t\}}{t^2} dt < \int_1^{\infty} \frac{1}{t^2} dt = 1$$

et donc $\gamma \in (0, 1)$.

Nous appliquons la théorème 3.1.4 avec fonctions $f(n) = 1$ et $g(t) = 1/t$. Alors $F(t) = \sum_{n \leq t} 1 = [t]$. Comme $[x] = x - \{x\}$ on a

$$\sum_{n \leq x} \frac{1}{n} = \sum_{n \leq x} f(n)g(n)$$

$$= \frac{[x]}{x} + \int_1^x \frac{[t]}{t^2} dt$$

$$= \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{t\}}{t^2} dt$$

$$= 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{t} dt - \int_1^x \frac{\{t\}}{t^2} dt$$

$$= \log x + \left(1 - \int_1^{\infty} \frac{\{t\}}{t^2} dt\right) - \int_x^{\infty} \frac{\{t\}}{t^2} dt - \frac{\{x\}}{x}$$

$$= \log x + \gamma + r(x).$$

Où on a utilisé le fait que $\int_1^x \frac{\{t\}}{t^2} dt = \int_1^{\infty} \frac{\{t\}}{t^2} dt - \int_x^{\infty} \frac{\{t\}}{t^2} dt$.

$$r(x) = \int_x^{\infty} \frac{\{t\}}{t^2} dt - \frac{\{x\}}{x}$$

De plus, $|r(x)| < 1/x$ car $0 \leq \{x\}/x < 1$ et

$$0 < \int_x^{\infty} \frac{\{t\}}{t^2} dt < \int_x^{\infty} \frac{1}{t^2} dt = \frac{1}{x}.$$

Ainsi on termine la preuve du théorème. ■

Théorèmes 3.1.6 [8]Si $x \geq 2$,

$$\sum_{n \leq x} \log^2 n = x \log^2 x - 2x \log x + 2x + O(\log^2 x).$$

Preuve. Nous utilisons le théorème 3.1.4 avec $f(n) = 1$ et $g(t) = \log^2 t$. Alors $F(t) = [t]$ et $g'(t) = 2 \log t / t$. Donc

$$\sum_{n \leq x} \log^2 n = [x] \log^2 x - \int_1^x \frac{[t](2 \log^2 t)}{t} dt$$

$$= (x - \{x\}) \log^2 x - 2 \int_1^x \frac{(t - \{t\}) \log t}{t} dt$$

$$= x \log^2 x - \{x\} \log^2 x - 2 \int_1^x \frac{t \log t}{t} dt + 2 \int_1^x \frac{\{t\} \log^2 t}{t} dt$$

$$= x \log^2 x - O(\log^2 x) - 2 \int_1^x \log t \, dt + 2 \int_1^x \frac{\{t\} \log^2 t}{t} dt$$

$$= x \log^2 x - 2x \log^2 x + 2x + O(\log^2 x).$$

La preuve est ainsi terminée. ■

3.2 Quelque sommation des fonctions arithmétique

Dans cette sous-section, fournissons encore quelques outils pour estimer des sommes de la forme

$$S(x) = \sum_{n \leq x} (f \star g)(n) = \sum_{n \leq x} \sum_{d | n} f(d) g\left(\frac{n}{d}\right).$$

Proposition 3.2.1[2] Soit $x \geq 1$ un nombre réel et f et g sont deux fonctions arithmétiques. Alors

$$S(x) = \sum_{d \leq x} f(d) \sum_{k \leq \frac{x}{d}} g(k).$$

Exemple 3.2.1 On a $\tau = 1 \star 1$, nous obtenons en utilisant la proposition 3.2.1

$$\sum_{n \leq x} \tau(n) = \sum_{d \leq x} \sum_{k \leq \frac{x}{d}} 1$$

Apres la proposition 1.6.1 (v), on a

$$\sum_{k \leq \frac{x}{d}} 1 = \left[\frac{x}{d}\right].$$

Alors,

$$\sum_{n \leq x} \tau(n) = \sum_{d \leq x} \left[\frac{x}{d}\right].$$

On applique l'égalité $[x] = x + O(1)$, nous obtenons

$$\begin{aligned} \sum_{n \leq x} \tau(n) &= \sum_{n \leq x} \left(\frac{x}{d}\right) + O(1) \\ &= x \sum_{d \leq x} \frac{1}{d} + O(x) \\ &= x \log x + O(x). \end{aligned}$$

Proposition 3.2.2[2] (Principe de l'hyperbole de Dirichlet) Soient T et x des réels avec $1 \leq T \leq x$ et soient f et g deux fonctions arithmétiques. Alors

$$\sum_{n \leq x} (f \star g)(n) = \sum_{n \leq T} f(n) \sum_{k \leq x/n} g(k) + \sum_{k \leq x/T} g(k) \sum_{n \leq x/k} f(n) - \sum_{n \leq T} f(n) \sum_{k \leq x/T} g(k).$$

Preuve. En fractionnant la somme du côté droit de la proposition 3.2.1, nous obtenons

$$\sum_{n \leq x} (f \star g)(n) = \sum_{d \leq T} f(d) \sum_{k \leq x/d} g(k) + \sum_{T < d \leq x} f(d) \sum_{k \leq x/d} g(k)$$

et

$$\sum_{T < d \leq x} f(d) \sum_{k \leq x/d} g(k) = \sum_{k \leq x/T} g(k) \sum_{T < d \leq x/k} f(d)$$

et

$$\sum_{T<d\leq x/k} f(d) = \sum_{d\leq x/k} f(d) - \sum_{d<T} f(d)$$

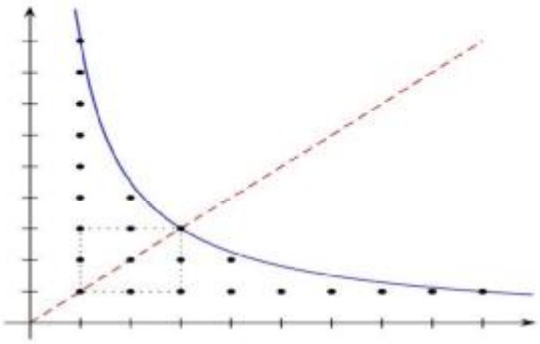
Alors

$$\sum_{T<d\leq x} f(d) \sum_{k\leq \frac{x}{d}} g(k) = \sum_{k\leq x/T} g(k) \left(\sum_{d\leq \frac{x}{k}} f(d) - \sum_{d<T} f(d) \right)$$

En remplaçant on termine le preuve eu question. ■

Remarque 3.2.1[2] Historiquement, c'est Dirichlet qui a découvert ce principe lorsqu'il a réussi à améliorer le terme d'erreur dans la somme

$$\sum_{n\leq x} \tau(n).$$



la figure 3.2 Hyperbole de Dirichlet principe.

Le nom vient de l'observation suivante. Puisque

$$\sum_{n\leq x} \tau(n) = \sum_{d\leq x} \left[\frac{x}{d}\right]$$

on est amené à compter le nombre de points entiers (m, n) avec $1 \leq m \leq x$ situés sous l'hyperbole $mn = x$.

Dirichlet utilisa la symétrie de l'hyperbole pour déduire que le nombre de points entiers est égal à celui de l'intérieur du carré $[1, \sqrt{x}]^2$ plus deux fois le nombre de points entiers (m, n) tels que $\sqrt{x} < m \leq x$, voir la figure 3.2. Cela donne

$$\sum_{n\leq x} \tau(n) = \left[\sqrt{x}\right]^2 + 2 \sum_{\sqrt{x}<m\leq x} \left[\frac{x}{m}\right]$$

$$= \left[\sqrt{x}\right]^2 + 2 \sum_{m\leq x} \left[\frac{x}{m}\right] - 2 \sum_{m\leq \sqrt{x}} \left[\frac{x}{m}\right]$$

$$= \left[\sqrt{x}\right]^2 + 2\sum_{m\le x}\tau(n) - 2\sum_{m\le\sqrt{x}}\left[\frac{x}{m}\right]$$

$$\sum_{m\le x}\tau(n) - 2\sum_{m\le x}\tau(n) = \left[\sqrt{x}\right]^2 - 2\sum_{m\le\sqrt{x}}\left[\frac{x}{m}\right]$$

et donc on obtient

$$\sum_{m\le x}\tau(n) = 2\sum_{m\le\sqrt{x}}\left[\frac{x}{m}\right] - \left[\sqrt{x}\right]^2. \qquad (3.4)$$

On voit facilement que l'utilisation de la proposition 3.2.2 avec $f = g = 1$ donne (3.4), de sorte que ce résultat généralise la méthode géométrique de Dirichlet. Nous sommes maintenant en mesure de montrer l'estimation suivante qui est le premier résultat dans le problème du diviseur de Dirichlet.

Théorème 3.2.1[2] (Dirichlet) Pour x suffisamment grand, on a

$$\sum_{n\le x}\tau(n) = x(\log x + 2\gamma - 1) + O\left(\sqrt{x}\right).$$

Avec γ est la constante d'Euler.

Preuve. Par (3.4), l'estimation $[x] = x + O(1)$ et le théorème 3.1.5, on a

$$\sum_{n\le x}\tau(n) = 2\sum_{m\le\sqrt{x}}\frac{x}{m} + O\left(\sqrt{x}\right) - \left(\sqrt{x} - O(1)\right)^2$$

$$= 2x\sum_{m\le\sqrt{x}}\frac{1}{m} + O\left(\sqrt{x}\right) - \left(\sqrt{x} - O(1)\right)^2$$

$$= 2x\left(\log\sqrt{x} + \gamma + O\left(x^{-1/2}\right)\right) - x + O\left(\sqrt{x}\right)$$

$$= 2x\log\sqrt{x} + x(2\gamma - 1) + O\left(\sqrt{x}\right)$$

$$= x\log x + x(2\gamma - 1) + O\left(\sqrt{x}\right).$$

Ce qui termine la preuve**.** ■

Chapitre 4

Résolution de quelques problèmes impliquant des fonctions multiplicatives et additives

Dans ce chapitre, nous aborderons certains des problèmes qui ont été résolus pour certaines fonctions arithmétiques

Problème 4.1[10] Soit $n \in \mathbb{N}$, n est nombre composé, alors

$$\sigma(n) > n + \sqrt{n}.$$

Preuve. Soit n est nombre composé, a un diviseur d tel que $1 < d < n$. Donc $1 < n/d < n$, si $d < \sqrt{n}$, alors $n/d > \sqrt{n}$. Mais puisque n/d est aussi un diviseur de n (pas nécessairement différent de d) et $1 < n/d < n$, nous voyons que $\sigma(n) \geq n + \sqrt{n+1}$, d'où $\sigma(n) \geq n + \sqrt{n}$, qui doit être prouvé ■

Exemple 4.1.1 Soit $n = 729 = 3^6$, alors

$$n + \sqrt{n} = 3^6 + \sqrt{3^6} = 756$$

$$\sigma(729) = \sigma(3^6) = 3^0 + 3^1 + 3^2 + 3^3 + 3^4 + 3^5 + 3^6 = 1092 > 756.$$

Problème 4.2[7]

$$\varphi(n) \leq n - \sqrt{n}.$$

Preuve. Soient $n \in \mathbb{Z}$ un nombre composé et $p_1$son plus petit diviseur premier . Comme nous le savons, $p_1 < \sqrt{n}$, donc, par le théorème 2.3.2 (b).

$$\varphi(n) \leq n\left(1-\frac{1}{p_1}\right).$$

Et

$$\begin{gathered} p_1 < \sqrt{n}, \\ \frac{1}{p_1} > \frac{1}{\sqrt{n}}, \\ -\frac{1}{p_1} < -\frac{1}{\sqrt{n}}, \\ n-\frac{n}{p_1} < n-\frac{n}{\sqrt{n}}, \\ \varphi(n) < n\left(1-\frac{1}{p_1}\right) < n-\sqrt{n}. \end{gathered}$$

ce qui prouve l'inégalité ■

Exemple 4.1.2 Pour $n = 2116$=$2^2 \times 23^2$, alors

$$n-\sqrt{n} = 2^2 \times 23^2 - \sqrt{2^2 \times 23^2} = 2116 - 46 = 2070.$$

et

$$\begin{aligned} \varphi(2116) = \varphi(2^2 \times 23^2) &= 2^2 \times 23^2\left(1-\frac{1}{2}\right)\left(1-\frac{1}{23}\right) = 2^2 \times 23^2\left(\frac{1}{2}\right)\left(\frac{22}{23}\right) \\ &= \frac{2^2 \times 23^2 \times 22}{2 \times 23} = 2 \times 23 \times 22 = 1012 < 2070. \end{aligned}$$

Problème 4.3 [7] Soit $n \in \mathbb{N}$, on a

$$2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}.$$

Preuve. Puisque les trois expressions de la chaîne d'inéquations sont des fonctions multiplicatives, il est évident qu'il suffit de prouver que les inéquations sont vraies lorsque n est une puissance d'un premier . Par conséquent, démontrer simplement que est suffisant.

Alors prenons $n = p^a$. Dans ce cas on a

$$\omega(p^a) = 1 \ , \tau(p^a) = a+1 \ \ , \Omega(p^a) = a,$$

Par remplacement on a $2^{\omega(n)} = 2, \tau(n) = a$.

Nous montrons que

$$2 \leq a+1 \leq 2^a, \text{pout tout } a \geq 1.$$

Appliqué la méthode par récurrence pour $a \geq 1$

Pour $a = 1$, on a

$2 \leq 2 \leq 2$ est vrai

On supposent $2 \leq a + 1 \leq 2^a$ est vrai pour $a \geq 1$ est démontre que pour $a + 1$

$$2 \leq a + 2 \leq 2^{a+1}$$

On a

$$2 \leq a + 2 \qquad (a \geq 1) \qquad (*)$$

Et

$$a + 1 \leq 2^a$$

$$2(a + 1) \leq 2 \times 2^a$$

$$a + 2 \leq 2a + 2 \qquad (**)$$

D'après (*) et (**), on a

$$2 \leq a + 2 \leq 2^{a+1}$$

Alors pour tout $a \geq 1$, on a

$$2 \leq a + 1 \leq 2^a \qquad \Leftrightarrow \qquad 2^{\omega(n)} \leq \tau(n) \leq 2^{\Omega(n)}.$$

qui doit être prouvé ■

Exemple 4.1.3 Prendre $n = 25200 = 2^4 \times 3^2 \times 5^2 \times 7$, alors

$\omega(25200) = 4$,

$\tau(25200) = 5 \times 3 \times 3 \times 2 = 90$,

$\Omega(25200) = 4 + 2 + 2 + 1 = 9$,

donc

$$2^4 = 16 \leq 18 \leq 2^9 = 512.$$

Problème 4.4[7] Soit $n \in \mathbb{N}$, alors

$$\frac{1}{2}\sqrt{n} \leq \varphi(n) \leq n.$$

Preuve. Il est évident que $\varphi(n) \leq n$. Donc, nous avons seulement besoin de prouver l'inégalité de gauche.

Pour $n = 1$, on a

$$\frac{1}{2}\sqrt{1} = \frac{1}{2} \leq \varphi(1) = 1,$$

Pour $n > 1$ de la forme $n = 2^{a_0} \times q_1^{a_1} \times \ldots \times q_r^{a_r}$, où $2 < q_1 < \cdots < q_r$ sont des nombres premiers et le a_i est des entiers positifs. on a alors

$$\varphi(n) = 2^{a_0-1} \prod_{i=1}^{r} q_i^{a_i-1}(q_i - 1)$$

on a pour $p \geq 3$

$$p(p-3) + 1 = (p-1)^2 - p > 0$$

donc

$$\otimes \qquad \text{s}(p-1)^2 > p \Rightarrow p - 1 > \sqrt{p} \Rightarrow \frac{p-1}{\sqrt{p}} > 0.$$

¨Par contre, pour chaque nombre entier positif a_i, on a $a_i - \frac{1}{2} > \frac{1}{2}a_i$, c'est pour cela que

$$\varphi(n) = 2^{a_0-1} \times q_1^{a_1-1} \times \ldots \times q_r^{a_r-1}(q_1 - 1) \times \ldots \times (q_r - 1)$$

d'âpres $\otimes$ on a

$$(q_1 - 1) \times \ldots \times (q_r - 1) > q_1^{\frac{1}{2}} \times \ldots \times q_r^{\frac{1}{2}}$$

et

$$2^{a_0-1} \times q_1^{a_1-1} \times \ldots \times q_r^{a_r-1} q_1^{\frac{1}{2}} \times \ldots \times q_r^{\frac{1}{2}} = 2^{a_0-1} \times q_1^{a-\frac{1}{2}} \times \ldots \times q_r^{a-\frac{1}{2}}.$$

Donc

$$\begin{aligned} 2^{a_0-1} \times q_1^{a_1-1} \times \ldots \times q_r^{a_r-1}(q_1 - 1) \times \ldots \times (q_r - 1) &> 2^{a_0-1} \times q_1^{a-\frac{1}{2}} \times \ldots \times q_r^{a-\frac{1}{2}} \\ &\geq 2^{a_0-1} \times q_1^{\frac{1}{2}a_1} \times \ldots \times q_r^{\frac{1}{2}a_r}, \\ &\geq 2^{-1}\sqrt{n} = \frac{1}{2}\sqrt{n}. \end{aligned}$$

Qui doit être prouvé ■

Exemple 4.1.4 Soit $n = 256036 = 2^2 \times 11^2 \times 23^2$, alors

$\frac{1}{2}\sqrt{n} = \frac{1}{2}\sqrt{256036} = 253,$

$\varphi(256036) = 2^2 \times 11^2 \times 23^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{23}\right) = 111320$,alors

$$253 \leq 111320 \leq 256036.$$

Problème 4.5[6] Soit $n \in \mathbb{N}$, on a

$\Omega(\varphi(n)) = \varphi(\Omega(n))$ est valable si $n = 2^p, n = 3\ ou\ n = 2^y \times 3^{p-y}$, où p est un nombre premier et $1 \leq y \leq p-1$.

Preuve.

suffisance :

Si $n = 2^p$, par théorème 2.3.2 (b) , on a

$$\varphi(2^p) = (2-1)2^{p-1} = 2^{p-1}$$

alors

$$\Omega(\varphi(2^p)) = \Omega(2^{p-1}) = p - 1$$

et

$$\varphi(\Omega(2^p)) = \varphi(p) = p - 1.$$

Si $n = 3$, on a $\Omega(3) = 1$, $\varphi(3) = 2$, alors $\Omega(\varphi(3)) = \Omega(3) = 1$ et $\varphi(\Omega(3)) = \varphi(1) = 1$.

Si $n = 2^y \times 3^{p-y}$, alors

$$\Omega(\varphi(2^y \times 3^{p-y})) = \Omega(2^{y-1} \times 2 \times 3^{p-y-1}) = y - 1 + 1 + p - y - 1 = p - 1$$

et

$$\begin{aligned}\varphi(\Omega(2^y \times 3^{p-y})) &= \varphi(y + p - y),\\ &= \varphi(p),\\ &= p - 1.\end{aligned}$$

■

Remarque 4.1.1 Pour la nécessité voir [6].

Exemple 4.1.5 Soit $n = 72 = 2^3 \times 3^2$, alors

$\Omega(\varphi(n)) = \Omega(\varphi(2^3 \times 3^2)) = 2^3 \times 3^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4,$

$\varphi(\Omega(n)) = \varphi(\Omega(2^3 \times 3^2)) = \varphi(5) = 4.$

Problème 4.6[7] Soit $n \in \mathbb{N}$. Si $\omega(n) = r\ avec\ r \leq 9$

$$\varphi(n) > \frac{n}{7}.$$

Preuve. Ecrivant n selon factorisation canonique $n = q^{a_1} \times \ldots \times q_r^{a_r}, r \leq 9$, est la représentation de n comme produit de puissances premières distinctes. Donc $\omega(n) = 9$, et appliqué théorème 2.3.2 (b) alors

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{q_i}\right)$$

Puisque $q_I > p_I$ pour $i = 1,2,\ldots,r$, nous avons

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{r} \left(1 - \frac{1}{q_i}\right)$$

$$\geq \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

$$\geq \prod_{i=1}^{9} \left(1 - \frac{1}{p_i}\right)$$

$$\prod_{i=1}^{9} \left(1 - \frac{1}{p_i}\right) = \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{7}\right)\left(1 - \frac{1}{11}\right)\left(1 - \frac{1}{13}\right)\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{19}\right)\left(1 - \frac{1}{23}\right) = \frac{36495360}{223092870} \simeq 0.16 > \frac{1}{7} = 0.14.$$

Donc

$$\frac{\varphi(n)}{n} > \frac{1}{7}$$

$$\varphi(n) > \frac{n}{7}.$$

Ce que nous devons démontrer. ■

Exemple 4.1.6 Soit $n = 256036 = 2^2 \times 11^2 \times 23^2$, alors

$\omega(256036) = \omega(2^2 \times 11^2 \times 23^2) = 6 < 9.$

Donc

$$\varphi(256036) = \varphi(2^2 \times 11^2 \times 23^2) = 111320 = \frac{779240}{7} > \frac{n}{7} = \frac{256036}{7}.$$

Problème 4.7[7] Soient $n, r \in \mathbb{Z}^+$ et $\omega(n) = r$, alors

$$\varphi(n) \geq \frac{n}{2^r}.$$

Preuve. En utilisant la formule (b) du théorème 2.3.2

$$\varphi(n) = n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

$$\frac{\varphi(n)}{n} = \prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

$$\geq \prod_{i=1}^{r}\left(1-\frac{1}{2}\right) = \frac{1}{2^r}.$$

Ce qui termine le preuve ■

Exemple 4.1.7 Soient $n = 3^r$ et $r \in \mathbb{N}$ avec $r > 2$, alors

$$\omega(n) = \omega(3^r) = r \quad et \quad \frac{n}{2^r} = \frac{3^r}{2^r}$$

et

$$\varphi(n) = \varphi(3^r) = 2 \times 3^{r-1} = 2 \times \frac{3^r}{3}$$

on a

$$3^{r-1} = \frac{3^r}{3}$$

$$\frac{3^r}{3} > \frac{3^r}{2^{r-1}}$$

$$2 \times \frac{3^r}{3} > 2 \times \frac{3^r}{2^{r-1}}$$

$$\varphi(n) > \frac{3^r}{2^r}.$$

Ce qui termine la preuve .

Annexe

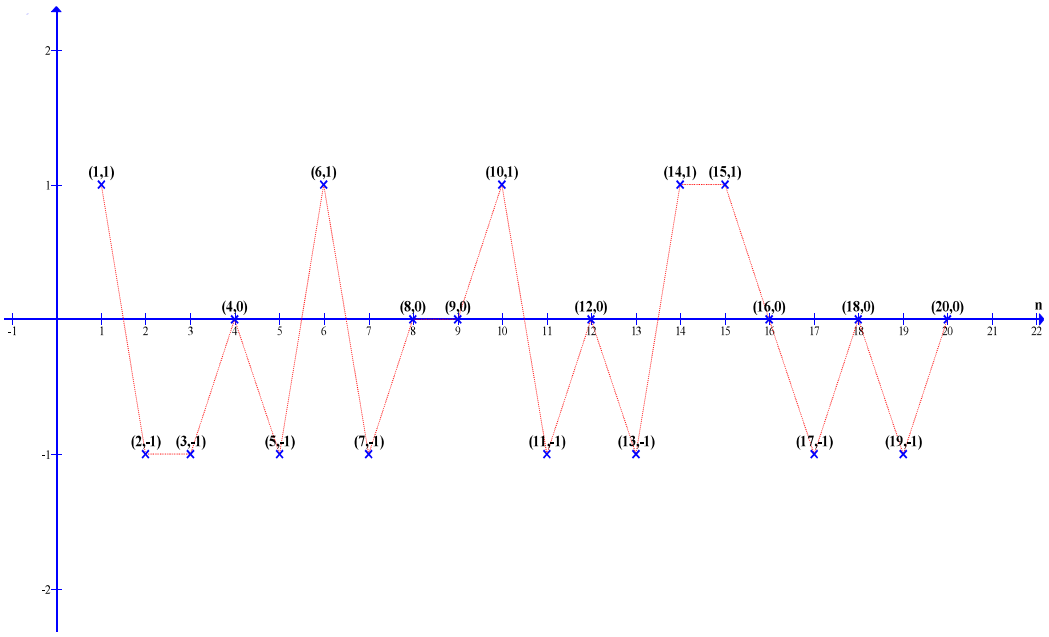


fig1. Graphe de fonction de Möbius.

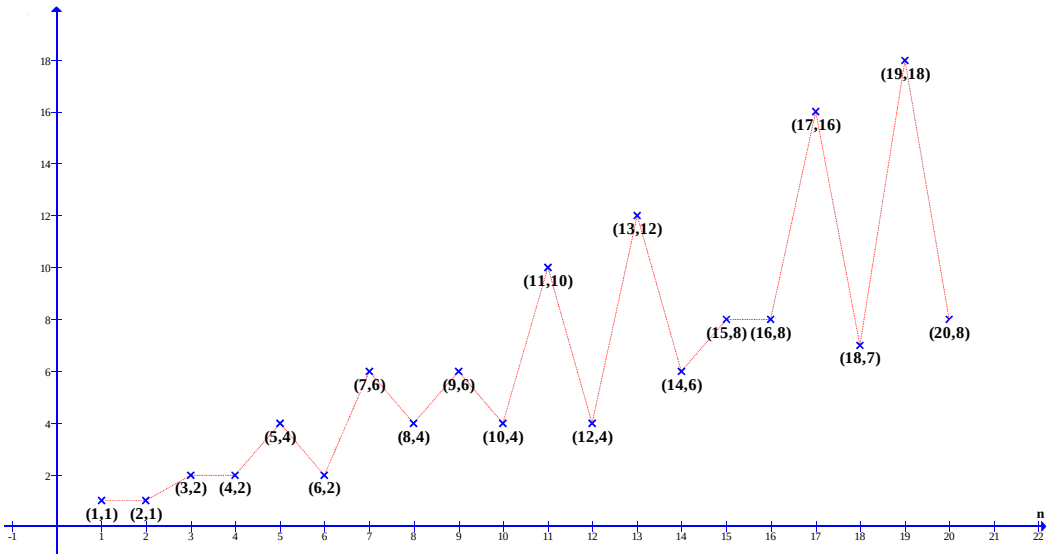


Fig2. graphe de fonction de Euler

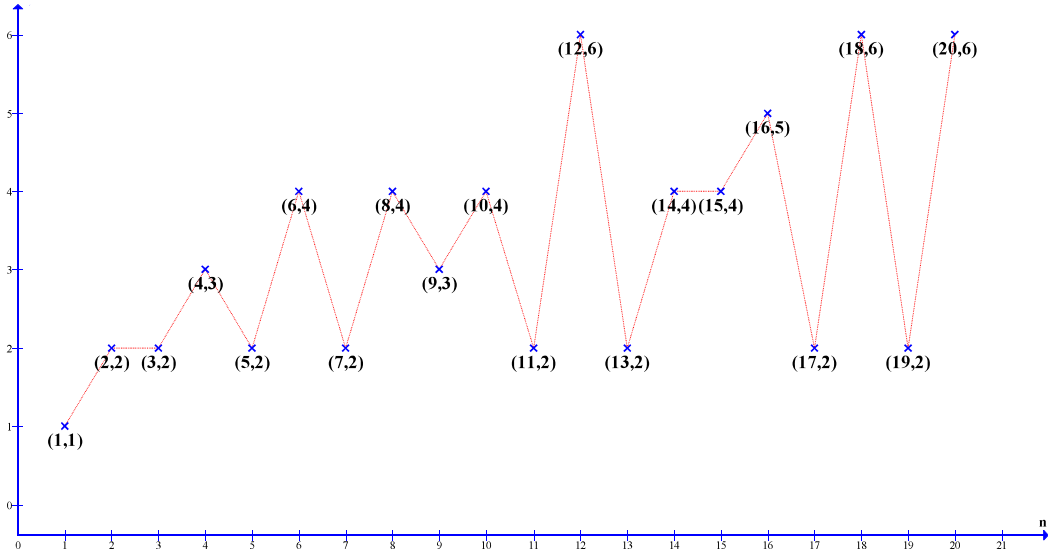


fig3. Graphe de la fonction nombre des diviseurs de n .

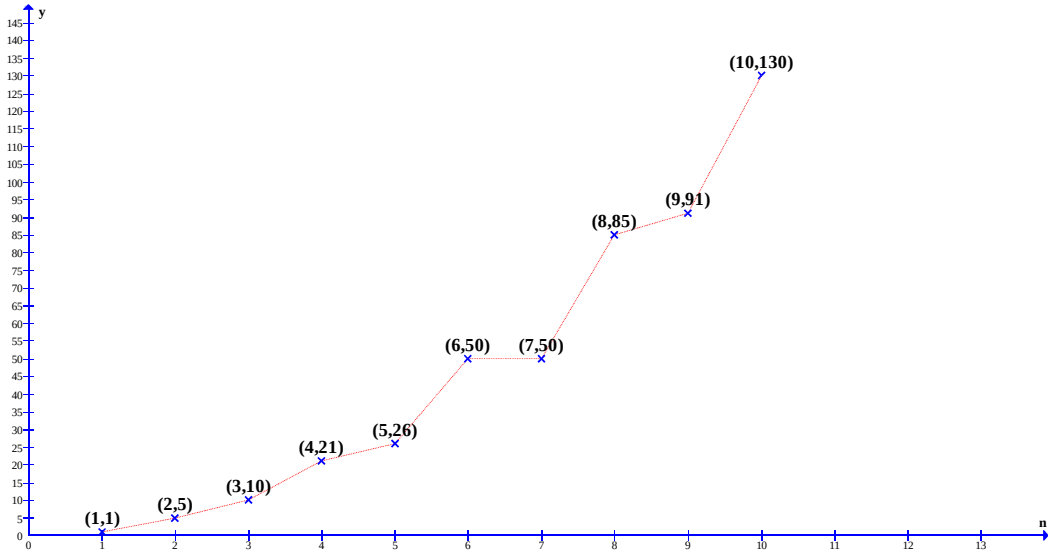


fig4. Graphe de la fonction somme des diviseurs de n.

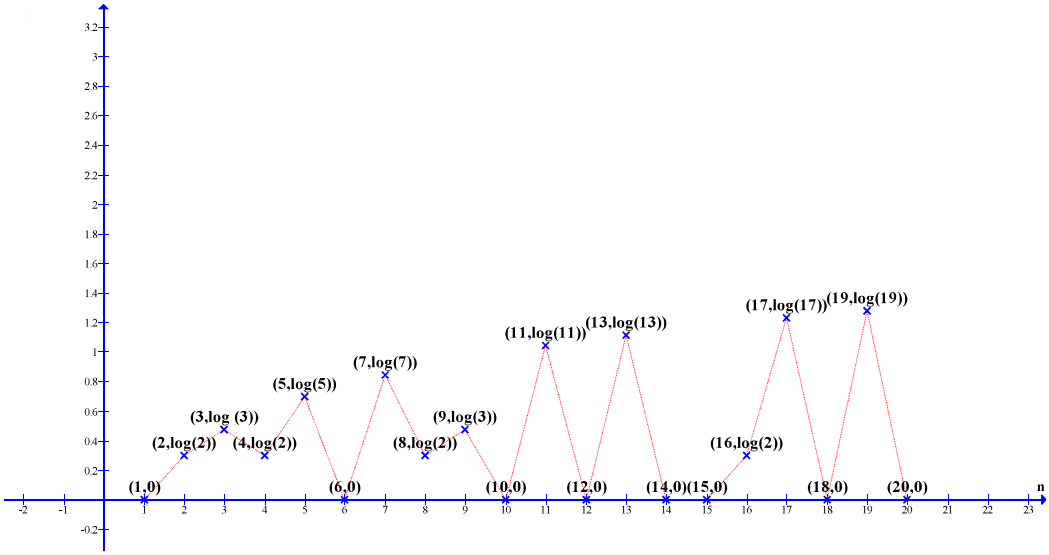


fig5. Graphe de la fonction Mangoldt .

Conclusion

Ce mémoire contient un minimum de connaissance concernant les fonctions arithmétiques. Nous pensons que ce modeste travail permet aux débutants de comprendre un bon aperçu sur les fonctions arithmétiques et leurs propriétés sur tout que l'on a discuté dans notre mémoire.

D'autre part nous avons terminé notre travail par résoudre a nouveau certains problèmes de la littérature et ceci pour approfondie la compréhension des notions.

Bibliographies

1. Apostol. T. M. (1998). Introduction to Analytic Number Theory. Springer Science & Business Media.
2. Bordellès. O. (2012). Arithmetic Tales(p. 1). London. Springer.
3. Boudaoud, A. (2020-2021). cour théorie de nombre 1er master algèbre et mathématique discret , université Mohamed Boudiaf M'sila.
4. Hildebrand, A. J. (2006). Inroduction to Analyitic Number Theory Math 531 Lecture Notes, Fall 2005. URL: http//www. Math. Uiuc.edu/hildebr/ant. Version. 1.
5. Hutz, B. (2018). An Experimental Introduction to Number Theory (vol. 31). American Mathematical Society.
6. Kézér, I. (2018). On some problems on composition of arithmetic functions. Teaching Mathematics and Computer Science, 16(2), 161-181.
7. Mercier, A. (2007). 1001 problems in classical number theory. American Mathematical Society.
8. Nathanson. M. B. (2008). Elementary Methods in number theory. (Vol. 195). Springer Science & Business Media.
9. Rosen. K. H. (2011). Elementary number theory and its applications. London Perason Education.
10. Sierpinski, W. (1988). Elementary Theory of Numbers: Second English Edition (edited by A. Schinzel). Elsevier

.

Faculté des Mathématiques et de l'Informatique
Département des Mathématiques
قسم الرياضيات

المسيلة في: / /

تصريح بتصحيح مذكرة الماستر 2

أنا الممضي أسفله الأستاذ: مواود عبدالمجيد

مؤطر الطلبة الآتية أسماؤهم:

1- قاسي عبدالحميد

2-

3-

أصرح بأنهم قد قاموا بتصحيح مذكرتهم المعنونة بـ:

Sur les fonctions arithmétiques

وذلك تبعا للنصائح الموجهة لهم من طرف لجنة التقييم.

إمضاء الأستاذ المؤطر