Table des matières

1 Préliminaires **4**

1.1 Les propriétés des nombres premiers 4

1.2 Énoncés équivalents 5

1.3 Approximations asymptotiques 6

1.4 Quelques types des nombres premiers 7

2 Fonction zêta de Riemann et nombres premiers **12**

2.1 La conjecture de Riemann (Hypothèse de Riemann) 12

2.2 Fonction zêta de Riemann 13

2.2.1 Propriétés diverses de la fonction zêta de Riemann 14

2.2.2 Introduction aux séries de Dirichlet 15

2.2.3 Hypothèse de Riemann généralisée (HRG) 17

2.2.4 Liens avec quelques fonctions arithmétiques 17

2.2.5 Liens avec les nombres premiers 19

2.2.6 Conjecture de Hilbert-Pôlya 21

2.2.7 Connexion possible avec la mécanique quantique 22

2.3 Les nombres premiers 24

2.3.1 Existence d'une infinité des nombres premiers 24

2.3.2 **Petite chronologie** 25

2.3.3 Aperçu sur les nombres premiers 27

2.4 Sur la recherche des nombres premiers 28

2.5 Cryptographie à clé publique 29

3 Distribution des nombres premiers dans les grandes progressions arithmétiques. **32**

3.1 Théorème de la progression arithmétique 32

3.2 Quelques suites arithmétiques 32
3.3 Progressions arithmétiques dans les nombres premiers, d'après B. Green et T. Tao . 34
3.4 Conclusion 35

Introduction Générale

«*Si la mathématique est la reine des sciences, alors la théorie de nombres est la reine des mathématiques*» a dit Gauss, c'est-à-dire que les nombres premiers sont la base de la théorie des nombres. Les Grecs anciens sont les premiers qu'ont étudiés les nombres premiers et qu'ils sont trouvés leurs propriétés de bases. En 1640, Fermat a fait une petite théorie appelée nombres de Fermat, plus tard prouvé par Leibniz et Euler. Marin Mersenne a considérer les nombres premiers de la forme $2^p - 1$, ils sont appelés nombres premiers de Mersenne (dans son honneur). Aux début du 19éme siècle, Legendre et Gauss on conjectura que les nombres premiers jusqu'à x est asymptotique équivalent à $\frac{x}{\ln x}$, quand x tend vers l'infini, et Hadamard à complété ce conjecture. En 1859, Riemann a fait une relation entre le théorème des nombres premiers et la fonction zêta, c'est-à-dire qu'il a trouvé une correspondance entre la distribution des nombres premiers et les zéros de fonction zêta.

Dans ce mémoire, on va étudier la distribution des nombres premiers et leur relation avec la fonction zêta de Riemann. D'abord, on va commencer par quelques définitions de base des nombres premiers et leurs propriétés. Ensuite, on donnera quelques formules pour déterminer ces nombres. Ainsi, on va définir la fonction zêta de Riemann avec quelques propriétés, en trouvant la relation entre la distribution des nombres premiers et la fonction zêta de Riemann. En effet, on va démontrer l'infinité des nombres premiers et se rappeler de l'une des applications de ces nombres dans la cryptographie.

Enfin, on va donner la distribution des nombres premiers dans les grandes progressions arithmétiques (théorème de B. Green et T. Tao) et se rappeler de quelques fonctions arithmétiques.

Chapitre 1

Préliminaires

Dans ce chapitre, on va rappeler quelques définitions des nombres premiers et leurs propriétés. On va donner un peu d'information sur des nombres premiers, comme : le plus grande nombre premier connu et quelques formules a été trouvées pour déterminer ces nombres.

1.1 Les propriétés des nombres premiers

L'entier 1 a un seule diviseur qui est lui-même. Tous les autres entiers naturels sauf 1 ont au moins deux diviseurs ; lui-même et 1.

Exemple 1.1 10 *aux diviseurs* $1,\ 2,\ 5,\ 10$.
6 *aux diviseurs* $1,\ 2,\ 3,\ 6$.
5 *aux diviseurs* $1,\ 5$.

Définition 1.1 *Un entier n est un nombre premier si n est plus grande que 1 et n n'a pas de diviseurs positives sauf que 1 et lui-même. Sinon, n est appelé* ***composé****.*

Exemple 1.2 7 *est un nombre premier car tous les diviseurs de* 7 *sont* 1 *et* 7.

Définition 1.2 *La fonction de* ***compte*** *des nombres premiers est la fonction* ***comptant*** *le nombre de nombres premiers inférieurs ou égaux à un nombre réel x, notée par $\pi(x)$. C'est-à dire :*

$$\pi\left(x\right) = \#\left\{n \in \mathbb{N} \,|n \leq x \text{ et } n \text{ est un nombre premier}\right\}$$

Exemple 1.3 $\pi\left(10\right) = \#\left\{2,\ 3,\ 5,\ 7\right\} = 4, \pi\left(100\right) = 25$

Théorème 1.1 ***(Théorème des nombres premiers) :*** *Le nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à x est* ***équivalent****, lorsque le* ***réel*** *x tend vers $+\infty$, au quotient de x par son* ***logarithme népérien****. Soit*

$$\pi(x) \sim \frac{x}{\ln(x)}, \text{ quand } (x \to +\infty)$$

c'est-à-dire

$$\lim_{x \to +\infty} \pi(x) \frac{\ln x}{x} = 1$$

1.2 Énoncés équivalents

Le théorème des nombres premier équivaut à

$$\pi(x) \ln(\pi(x)) \sim x, \text{ quand } x \to +\infty$$

d'après [1], donc on a le **comportement asymptotique** suivant [1], [2], [3] pour le $n^{ième}$ nombre premier :

$$p_n \sim n \ln(n), \text{ quand } n \to +\infty$$

il équivaut aussi [4] à

$$\theta(x) \sim x, \text{ quand } x \to +\infty$$

et à

$$\Psi(x) \sim x, \text{ quand } x \to +\infty$$

puisque les deux fonctions de **Tchebycheff**

$$\theta(x) = \sum_{p \in P,\, p \leq x} \ln p$$

et

$$\Psi(x) = \sum_{p \in \mathbf{P},\, k \in \mathbb{N}^*,\, p^k \leq x} \ln p$$

où $\mathbf{P}$ est l'ensemble des nombres premiers sont équivalents [5] (quand $x \to +\infty$) à $\pi(x) \ln x$.

1.3 Approximations asymptotiques

Un **approximant** $\pi(x)$ nettement meilleur que $\frac{x}{\ln x}$ [1] est la fonction **logarithme intégrale** $li(x)$ ou sa variante, la fonction **d'écart logarithmique intégrale** $Li(x)$ [2] :

$$\pi(x) \sim li(x) \sim Li(x)$$

où

$$li(x) = \int_0^x \frac{dt}{\ln(t)} \text{ et } Li(x) = li(x) - li(2) = \int_2^x \frac{dt}{\ln(t)}$$

Le crible d'Eratosthène

On donne un entier N pour faire une liste des nombres premiers inférieurs à lui, **le crible d'Eratosthène** est très performant si N n'est pas très grand. Il est fondé sur le résultat déjà prouvé : Tout entier $n \geq 2$, qui n'est pas premier, possède un diviseur premier inférieur ou égal à $E(\sqrt{n})$ ($E(.)$ désigne la partie entière). En pratique, on écrit les entiers de 2 à N et on raye les multiples du plus petit nombre premier 2 et qui sont distincts de 2. L'entier 3 est premier car il n'est pas multiple d'un nombre premier plus petit que lui. On recommence avec les multiples de 3, distincts de 3. Le plus petit nombre > 3 non rayé est 5 qui de ce fait est premier. On raye ses multiples et on continue avec le plus petit entier non rayé et > 5. Supposons qu'a une certaine étape, on ait rayé les multiples de n distincts de n et soit $p > n$ le plus petit entier non rayé. Cet entier est premier car il n'est multiple d'aucun nombre premier plus petit que lui. Dès que p dépasse $E(\sqrt{N}) + 1$ il est inutile de continuer car tout nombre $\leq N$ qui n'est pas premier est rayé et donc tous ceux qui restent dans le tableau sont premiers. Par exemple ; si $N = 1000$ alors, après avoir rayé les multiples de 29, le plus petit entier non rayé est $31 = E(\sqrt{1000})$. On rayé les multiples de 31 et tout nombre non rayé est premier.

Donnons explicitement **le crible d'Eratosthène** pour $N = 100$. Après avoir rayé les multiples de 7, le plus petit entier non rayé est $11 > \sqrt{100} = 10$ et donc les entiers restants sont tous premiers.

Remarque 1.1 *Le record du plus grand nombre premier connu a presque toujours été trouvé parmi les nombres de Mersenne, comme le dernier en date,* $M_{74207281} = 2^{74207281} - 1$*, un nombre à* 22338618 *chiffres.*

[1] D'après l'estimation de développement asymptotique de $li(x)$ vaut aussi pour $\pi(x)$, à tout ordre. Or $\frac{x}{\ln x}$ n'en est que le premier terme.

[2] Dans la littérature scientifique, notamment anglo-saxonne, la fonction logarithme intégral $li(x)$ est parfois notée $Li(x)$ avec une majuscule, alors que cette dernière notation désigne plutôt la fonction d'écart logarithmique intégrale. En cas doute, il suffit de se souvenir que $Li(2) = 0$ alors que $li(2) = 1,045...$

	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~~

1.4 Quelques types des nombres premiers

Les formules intéressantes pour déterminer les nombres premiers par suivant :

Nombres additif

$$2,\ 3,\ 5,\ 7,\ 11,\ 23,\ 29,\ 41,\ 43,\ 47,\ 61,\ 67,\ 83,\ 89,\ 101,\ 113...$$

Nombres de Bell

$$2,\ 5,\ 877,\ 27644437,\ 35742549198872617291353508656626642567...$$

Nombres de Carol

Ces nombres de la forme :

$$(2^n - 1)^2 - 2$$

par exemple :

$$7,\ 47,\ 223,\ 3967,\ 16127...1298074214633706835075030044377087$$

Nombres Chanceux

$$3,\ 7,\ 13,\ 31,\ 37,\ 43,\ 67,\ 73,\ 79,\ 127,\ 151,\ 163,\ 193,\ 211,\ 223,\ 241,\ 283,\ 307,\ 331...$$

Double Mersenne première

C'est de la forme :

$$2^{2^p - 1} - 1$$

par exemples :

$$7,\ 127,\ 2147483647,\ 170141183460469231731687303715884105727...$$

Nombres d'Euclid

Ces nombres de la forme :

$$E_n = p_n\# + 1$$

où $p_n\#$ est le n-ième nombre primoriel (la primorielle $p_n\#$ est le produit de tous les nombres inférieurs ou égaux à n. Par exemple, $E_7 = 2 \times 3 \times 5 \times 7 = 210$).
par exemples :

$$2,\ 3,\ 7,\ 31,\ 211,\ 2311,\ 30031$$

Formule polynômial d'Euler

$$p(n) = n^2 - n + 41$$

Cette formule est toujours un nombre premier pour les n qui plus petite que 41.

Exemple 1.4 *Prenons la formule polynômial d'Euler,* $p(n) = n^2 - n + 41$

$$n = 1 \Rightarrow p(1) = 41,\ n = 2 \Rightarrow p(2) = 43$$

$$n = 7 \Rightarrow p(7) = 83,\ n = 8 \Rightarrow p(8) = 97$$

$$n = 11 \Rightarrow p(11) = 151,\ n = 12 \Rightarrow p(12) = 173$$

Nombre de Fermat

$$2^{2^n} + 1$$

où n est entier positif.

Factoriel première

$$p = n! + 1 \text{ ou } p = n! - 1$$

Gauss première

Ces nombres de la forme :

$$4n + 3$$

par exemple :

$$3,\ 7,\ 11,\ 19,\ 23,\ 31,\ 43,\ 47,\ 59,\ 67,\ 71,\ 79,\ 83,\ 103,\ 107,\ 127,\ 131...$$

Nombres joyeux

$$7,\ 13,\ 19,\ 23,\ 31,\ 79,\ 97,\ 103,\ 109,\ 139,\ 167,\ 193,\ 239,\ 263,\ 293,\ 313,\ 331...$$

Nombres irrégulier

$$37,\ 59,\ 67,\ 101,\ 103,\ 131,\ 149,\ 157,\ 233,\ 257,\ 263,\ 271,\ 283,\ 293,\ 307,\ 311...$$

Nombres de Kynea

Ces nombres de la forme :

$$(2n+1)^2 - 2$$

Nombres de Markov

Ces nombres de la forme :

$$x^2 + y^2 + p^2 = 3xyp$$

par exemple :

$$2,\ 5,\ 13,\ 29,\ 89,\ 233,\ 433,\ 1597,\ 2897,\ 5741,\ 7561,\ 28657,\ 33461,\ 43261,\ 96557,\ 426389,\ 514229...$$

Nombres de Mersenne

Les nombres premiers de **Mersenne** sont la forme :

$$2^p - 1$$

où p est un nombre premier.

Nombres de Newman–Shanks–Williams

$$7,\ 41,\ 239,\ 9369319,\ 63018038201,\ 489133282872437279,\ 19175002942688032928599$$

Pythagorean première

Ces nombres de la forme :

$$4n + 1$$

Exemple 1.5 *Prenons la pytagorean Première,* $p(n) = 4n + 1$

$$n = 1 \Rightarrow p(1) = 5,\ n = 3 \Rightarrow p(3) = 13$$

$$n = 4 \Rightarrow p(4) = 17,\ n = 7 \Rightarrow p(7) = 29$$

$$n = 9 \Rightarrow p(9) = 37,\ n = 10 \Rightarrow p(10) = 41$$

Ramanujan première

$$2,\ 11,\ 17,\ 29,\ 41,\ 47,\ 59,\ 67,\ 71,\ 97,\ 101,\ 107,\ 127,\ 149,\ 151,\ 167,\ 179,\ 181,\ 227,\ 229,\ 233...$$

Nombres ordinaire

$$3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 41,\ 43,\ 47,\ 53,\ 61,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97,\ 107,\ 109,\ 113,\ 127...$$

Nombres étoile

Ces de la forme :

$$6n(n-1)+1$$

par exemple :

$$13,\ 37,\ 73,\ 181,\ 337,\ 433,\ 541,\ 661,\ 937,\ 1093,\ 2053,\ 2281,\ 2521,\ 3037,\ 3313,\ 5581...$$

Nombres tripléts

Ces nombres de la forme :

$$(p,\ p+2,\ p+6) \text{ ou } (p,\ p+4,\ p+6)$$

par exemple :

$$(5,\ 7,\ 11),\ (7,\ 11,\ 13),\ (11,\ 13,\ 17),\ (13,\ 17,\ 19),\ (17,\ 19,\ 23),\ (37,\ 41,\ 43),\ (41,\ 43,\ 47)...$$

Nombres unique

$$3,\ 11,\ 37,\ 101,\ 9091,\ 9901,\ 333667,\ 909091,\ 99990001,\ 999999000001...1111111111111111111...$$

Wagstaff première

$$p=\frac{2^q+1}{3}$$

où q est un autre nombre premier.

Pour les nomber de Mersenne on a le tableau suivant qui donne the chiffre, l'année et la référence pour chaque nombre connu.

P	Chiffre	Année	référence	valeur
7	3	Antiquity		127
13	4	1461	Reguis (1536), Cataldi (1603)	8191
19	6	1588	Cataldi (1603)	524287
31	10	1750	Euler (1772)	2147483647
61	19	1883	Pervouchine (1883)	230...951
107	33	1913	Powers (1914)	1622...88127
2281	687	Oct. 9, 1952	Robinson (1954)	44608...36351
3217	969	Sep. 8, 1957	Riesel	25911...15071
4423	1332	Nov. 3, 1961	Hurwitz	28554...80607
11213	3376	Jan. 2, 1963	Gillies (1964)	28141...92191
19937	6002	Mar. 4, 1971	Tuckerman (1971)	43154...41471
23209	6987	Fiv. 9, 1979	Noll (Noll et Nickel 1980)	40287...64511
1257787	378632	Sep. 3, 1996	Slowinski et Gage	41224...66527
13466917	4053946	Nov. 14, 2001	Michael Cameron/GIMPS	92494...59071
42643801	12837064	Jan. 12, 2009	Odd Magnar Strindmo/GIMPS	16987...14751
43112609	12978189	Août. 23, 2008	Edson Smith/GIMPS	31647...52511
57885161	17425170	Jan. 25, 2013	Curtis Cooper/GIMPS	58188...85951
74207281	22338618	Jan. 7, 2016	Curtis Cooper/GIMPS	30037...36351

Tableau des nombres de Mersenne

Chapitre 2

Fonction zêta de Riemann et nombres premiers

2.1 La conjecture de Riemann (Hypothèse de Riemann)

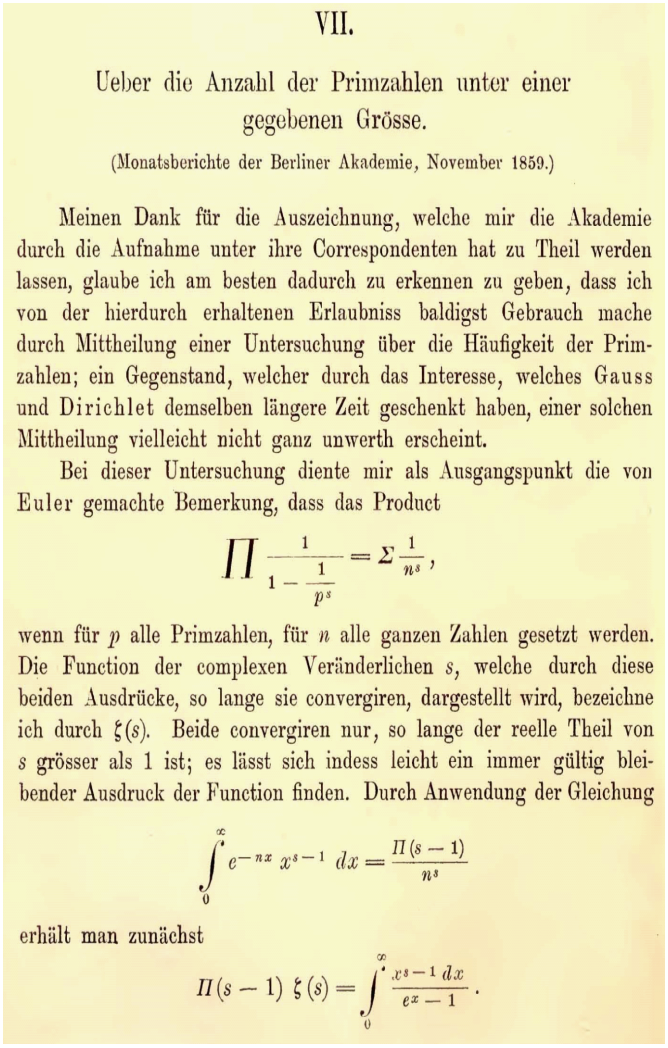
L'hypothèse de Riemann est une proposition mathématique selon laquelle il est possible de décomposer les nombres premiers en musique. Dire des nombres premiers qu'ils recèlent en eux une musique est une façon poétique de décrire ce théorème mathématique.

Conjecture 2.1 *Les zéros non triviaux de la fonction zêta sont tous situés sur la droite* $x = \frac{1}{2}$.

Si cette hypothèse est vraie, ceci montre en particulier l'encadrement :

$$|\pi(N) - Li(N)| \leq C\sqrt{N}\ln(N)$$

D'après les travaux de H. Von Kock. En quoi cette hypothèse est-elle intéressante ?
Elle est liée à d'autres questions importantes par exemple une de ses formes généralisées entrainerait l'existence d'un algorithme polynomiale pour tester la primalité d'un nombre. Beaucoup de problèmes en théorie des nombres sont liés à cette hypothèse. Mais le plus important résultat de l'hypothèse de Riemann est la distribution des nombres premiers : *Si l'hypothèse de Riemann est vraie alors la distribution des nombres premiers est uniforme*.



VII.

Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse.

(Monatsberichte der Berliner Akademie, November 1859.)

Meinen Dank für die Auszeichnung, welche mir die Akademie durch die Aufnahme unter ihre Correspondenten hat zu Theil werden lassen, glaube ich am besten dadurch zu erkennen zu geben, dass ich von der hierdurch erhaltenen Erlaubniss baldigst Gebrauch mache durch Mittheilung einer Untersuchung über die Häufigkeit der Primzahlen; ein Gegenstand, welcher durch das Interesse, welches Gauss und Dirichlet demselben längere Zeit geschenkt haben, einer solchen Mittheilung vielleicht nicht ganz unwerth erscheint.

Bei dieser Untersuchung diente mir als Ausgangspunkt die von Euler gemachte Bemerkung, dass das Product

$$\prod \frac{1}{1-\frac{1}{p^s}} = \Sigma \frac{1}{n^s},$$

wenn für p alle Primzahlen, für n alle ganzen Zahlen gesetzt werden. Die Function der complexen Veränderlichen s, welche durch diese beiden Ausdrücke, so lange sie convergiren, dargestellt wird, bezeichne ich durch $\zeta(s)$. Beide convergiren nur, so lange der reelle Theil von s grösser als 1 ist; es lässt sich indess leicht ein immer gültig bleibender Ausdruck der Function finden. Durch Anwendung der Gleichung

$$\int_0^\infty e^{-nx}\, x^{s-1}\, dx = \frac{\Pi(s-1)}{n^s}$$

erhält man zunächst

$$\Pi(s-1)\, \zeta(s) = \int_0^\infty \frac{x^{s-1}\, dx}{e^x - 1}.$$

Figure1 : Article de Riemann de 1859 sur la fonction zêta.

2.2 Fonction zêta de Riemann

Nous présentons quelques-uns des résultats connus sur la nature arithmétique des valeurs aux entiers de la fonction zêta de Riemann, définie pour tout complexe s par :

$$\zeta(s) = \sum_{k=1}^{+\infty} \frac{1}{k^s}$$

cette série est divergente en toutes les autres valeurs réelles de s sauf les zéros.

2.2.1 Propriétés diverses de la fonction zêta de Riemann

Le développement de Laurent au voisinage de 1 de la fonction zêta de Riemann est donnée par :

$$\zeta(s) = \frac{s}{s-1} - s\int_1^{\infty} \frac{\{u\}}{u^{1+s}} du$$

comme $\{u\}$ est toujours compris entre 0 et 1, l'intégrale est convergente et le terme est borné. Le premier terme vaut aussi.

$$\frac{s}{s-1} = \frac{1}{s-1} + 1$$

ce qui montre que la fonction ζ admet un pôle d'ordre 1 en 1 et de résidu 1. Cela constitue le théorème de Dirichlet. Le développement en série de Laurent de la fonction $\zeta(s)$ s'écrit donc :

$$\zeta(s) = \frac{1}{s-1} + \gamma + \sum_{n=1}^{\infty} (-1)^n \frac{\gamma_n}{n!}(s-1)^n$$

où γ est la constante d'Euler Mascheroni et où l'on a :

$$\gamma_n = \lim_{k\to\infty} \left(\sum_{m=1}^{k} \frac{(\ln m)^n}{m} - \frac{(\ln k)^{n+1}}{n+1}\right)$$

ces nombres sont appelés constantes ou nombres de Stieltjes. Concernant ces nombres, Matsuoka, en 1985 [6], a montré que l'on avait pour $n > 4$:

$$|\gamma_n| \leq 10^{-4}(\ln n)^n$$

on sait aussi qu'il y a asymptotiquement la moitié de ces nombres qui sont positifs.
Le développement de Laurent à l'ordre 1 montre que ζ est négative sur l'axe réel juste avant 1 [1] (Elle est positive après 1 de manière élémentaire puisque tous les termes de la série de Dirichlet sont alors positifs). En effet, on a :

$$\zeta(s-1)\zeta(s) = 1 + \gamma(s-1) + O((s-1)^2)$$

or, en supposant $s - 1 < 0$ et suffisamment petit, on a $(s-1)\zeta(s) \geq 0$, donc $\zeta(s) \leq 0$.
La valeur principale de Cauchy de la fonction en 1 :

$$\lim_{\varepsilon\to 0} \frac{\zeta(1+\varepsilon) + \zeta(1-\varepsilon)}{2}$$

existe et égale la constante d'Euler-Mascheroni $\gamma = 0,5772...$

[1] L'expression : $\zeta(a) = \frac{\eta(a)}{(1-2)}$ pour $a \in]0, +\infty[\backslash\{1\}$ donne le même résultat puisque l'expression $\eta(a)$ de la fonction η de Dirichlet est positive par le théorème des séries alternées et que $1 - 2^{1-a}$ est du même signe que $a - 1$.

2.2.2 Introduction aux séries de Dirichlet

On va donner une brève introduction aux séries de Dirichlet pour déterminer la fonction zêta de Riemann. Une série de Dirichlet est une série de la forme :

$$f(s) = \sum_{n=1}^{\infty} a_n \exp(-\lambda_n s)$$

où λ_n est $\lambda_1 < \lambda_2 < \lambda_3 < \lambda_4 < \ldots$; $\lambda_n \to \infty$; et $a_n \in \mathbb{C}$ et $s = \{\sigma + it \mid \sigma, t \in \mathbb{R}\}$. Si $\lambda_n = \ln n$, on obtient la série de Dirichlet standard

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

Exemple 2.1 *Les séries de Dirichlet « classiques », celles de la première définition, figurent les séries L de Dirichlet, qui correspondent aux cas où la suite $(a_n)_{n\in\mathbb{N}}$ est totalement multiplicative ($a_n a_m = a_{n+m}$) et périodique ($\exists T > 0 : a_{n+T} = a_n$). L'exemple le plus simple d'une telle suite (appelée un caractère de Dirichlet) est la suite constante $a_n = 1$, qui correspond à la série de Riemann : $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$*

Exemple 2.2 *La théorie des séries de Dirichlet générales, en autorisant d'autres suites d'exposants λ_n que la suite $\log(n)$, permet d'inclure d'autres théories classiques : Si les valeurs λ_n vérifient $\lambda_n = n$ et que l'on note $z = \exp(-s)$, la série prend la forme :*

$$f(z) = a_0 + \sum_{n=1}^{\infty} a_n z^n$$

Exemple 2.3 *Dans le cas où $\lambda_n = 2\pi n$, le changement de variable $s = -it$ montre qu'une série de Fourier est aussi un cas particulier de série de Dirichlet.*

$$f(x) = A_0 + \sum_{n=1}^{\infty} (A_n \cos(nx) + B_n \sin(nx))$$

Définition 2.1 *On appelle suite géométrique une suite de nombres où on passe d'un terme au suivant en multipliant toujours par le même nombre (ce nombre est appelé la base de la suite géométrique et est souvent noté q).*

Formule permettant de calculer le $n^{ème}$ terme d'une suite géométrique :

$$n^{ème} \textbf{ terme} = \textbf{premier terme} \times q^{(n-1)}$$

Si on note u_0 le premier terme, on a : $u_n = (n+1)^{ème}$ terme $= u_0 q^n$. Si on note u_1 le premier terme, on a : $u_n = n^{ème}$ terme $= u_1 q^{n-1}$.

Formule permettant de calculer la somme des n premiers termes d'une suite géométrique :
a)

$$S = \textbf{premier terme } (\frac{q^{\textbf{(nombre de termes)}}-1}{q-1})$$

b) Remarque : Si on note u_0 le premier terme, $u_0 + u_1 + u_2 + \ldots + u_n$ = somme des $(n+1)$ premiers termes

$$= u_0(\frac{q^{n+1}-1}{q-1})$$

si on note u_1 le premier terme, $u_1 + u_2 + u_3 + \ldots + u_n$ = somme des n premiers termes

$$u_1(\frac{q^{n}-1}{q-1})$$

Théorème 2.2 ***(La formule multiplicative d'Euler) :*** *La fonction zêta de Riemann est à la relation suivante :*

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1-p^{-s}}$$

Preuve. On va l'écrire en forme de multiplications

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^{+\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots \\
\frac{1}{2^s}\zeta(s) &= \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \ldots \\
(1-\frac{1}{2^s})\zeta(s) &= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \ldots \\
\frac{1}{3^s}(1-\frac{1}{2^s})\zeta(s) &= \frac{1}{3^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} + \ldots \\
(1-\frac{1}{3^s})(1-\frac{1}{2^s})\zeta(s) &= \frac{1}{3^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{217^s} + \ldots \\
&\ldots\ldots\ldots\ldots \\
\ldots(1-\frac{1}{11^s})(1-\frac{1}{7^s})(1-\frac{1}{5^s})(1-\frac{1}{3^s})(1-\frac{1}{2^s})\zeta(s) &= 1 \\
\zeta(s) &= \frac{1}{(1-\frac{1}{2^s})(1-\frac{1}{3^s})(1-\frac{1}{5^s})(1-\frac{1}{7^s})(1-\frac{1}{11^s})\ldots} \\
\zeta(s) &= \prod_{p \text{ premier}} \frac{1}{1-p^{-s}}
\end{aligned}$$

■

2.2.3 Hypothèse de Riemann généralisée (HRG)

L'hypothèse de Riemann généralisée a sans doute été formulée pour la première fois par Adolf Piltz en 1884.

Définition 2.2 *Un caractère de Dirichlet est une fonction arithmétique complètement multiplicative χ pour laquelle il existe un entier naturel $k > 0$ tel que, pour tout entier n, on ait $\chi(n+k) = \chi(n)$ et $\chi(n) = 0$ si n n'est pas premier avec k. On définit la fonction L de Dirichlet d'un tel caractère par :*

$$L(\chi,\ s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

pour tout nombre complexe s de partie réelle > 1. Par prolongement analytique, cette fonction peut être étendue à une fonction méromorphe définie sur tout le plan complexe.

Remarque 2.1 *Le cas du caractère trivial ($\chi(n) = 1$ pour tout n) correspond à l'hypothèse de Riemann ordinaire.*

Conséquences de l'hypothèse de Riemann généralisée

1) Soient a et d deux entiers naturels premiers entre eux, avec d non nul. D'après un théorème de Dirichlet, la progression arithmétique $a,\ a+d,\ a+2d,\ a+3d\ldots$ contient une infinité de nombres premiers. Notons $\pi(x,\ a,\ d)$ le nombre de nombres premiers appartenant à cette progression et inférieurs ou égaux à x. Si l'hypothèse de Riemann généralisée est vraie alors, pour tout réel $\varepsilon > 0$:

$$\pi(x,\ a,\ d) = \frac{1}{\varphi(d)} \int_2^x \frac{1}{\ln x} dx + O(x^{\frac{1}{2+\varepsilon}}), \text{ lorsque } x \to \infty$$

où φ désigne la fonction indicatrice d'Euler et O le symbole de Landau. C'est une version beaucoup plus forte du théorème des nombres premiers, et de la version quantitative du théorème de la progression arithmétique.
2) Si l'hypothèse de Riemann généralisée est vraie, alors le test de primalité de Miller-Rabin est assuré d'être exécuté en temps polynomial (temps fini).

2.2.4 Liens avec quelques fonctions arithmétiques

À partir de la série de Dirichlet de ζ on démontre les formules suivantes [7], [8] :

Carré de la fonction zêta

Si $\mathrm{Re}(s) > 1$:

$$\zeta^2(s) = \sum_{n=1}^{\infty} \frac{\tau(n)}{n^s}$$

où τ est la fonction nombre de diviseurs :

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

Si $\mathrm{Re}(s) > 2$:

$$\zeta(s)\zeta(s-1) = \sum_{n=1}^{\infty} \frac{\sigma(n)}{n^s}$$

où σ est la fonction somme des diviseurs :

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

les deux dernières formules sont des cas particuliers de l'égalité valide pour $\mathrm{Re}(s) > \max\{1,\ \mathrm{Re}(a)+1\}$ avec $a \in \mathbb{C}$:

$$\zeta(s)\zeta(s-a) = \sum_{n=1}^{\infty} \frac{\sigma_a(n)}{n^s}$$

où σ_a est la fonction diviseur à la puissance a :

$$\sigma_a(n) = \sum_{d|n} d^a$$

Inverse de la fonction zêta

Si $\mathrm{Re}(s) > 1$:

$$\frac{1}{\zeta(s)} = 1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \frac{1}{7^s} + \frac{1}{10^s} - \frac{1}{11^s} + \ldots = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$$

où μ est la fonction de Möbius.

Quotients de fonctions zêta par $\zeta(s)$

Si $\mathrm{Re}(s) > 2$:

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\varphi(n)}{n^s}$$

où φ est l'indicatrice d'Euler.

Si $\mathrm{Re}(s) > 1$:

$$\frac{\zeta(2s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\lambda(n)}{n^s}$$

où λ est la fonction de Liouville.
Si $\mathrm{Re}(s) > 1$:

$$\frac{\zeta'(s)}{\zeta(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$$

où Λ est la fonction de von Mangoldt.

2.2.5 Liens avec les nombres premiers

Le prolongement analytique de ζ

La fonction zêta a été considérée bien avant Riemann par Euler qui a par exemple montré formellement l'identité :

$$\zeta(s) = \prod_{p \text{ premier}} \frac{1}{1 - p^{-s}} \tag{2.1}$$

valable en fait pour $s > 1$. Euler a ainsi déduit de la divergence de $\zeta(1)$ une preuve analytique de l'existence d'une infinité de nombre premier. Pour explorer davantage ce lien entre nombres premiers et analyse, Riemann [9] a été le premier à considérer $\zeta(s)$ comme une fonction de la variable complexe s et l'a prolongée de façon unique en une fonction, toujours notée ζ, méromorphe sur $\mathbb{C}$, avec pôle simple en $s = 1$ de résidu 1. Il a aussi montré que ce prolongement vérifie l'équation fonctionnelle suivante, déjà devinée par Euler

$$\zeta(1-s) = 2(2\pi)^{-s} \cos(\frac{\pi s}{2}) \Gamma(s) \zeta(s) \tag{2.2}$$

Riemann a ainsi pu donner une formule, assez compliquée, liant les zéros de ζ à la fonction $\pi(x) = card\,\{p \text{ premier } | p \leq x\}$. Le succès de cette approche "complexe" arrivera en 1896 lorsque Hadamard et de la Vallée-Poussin prouvent indépendamment que ζ ne s'annule pas sur la droite verticale $\mathrm{Re}(s) = 1$ et en déduisent le théorème des nombres premiers :

$$\pi(x) \sim \int_2^x \frac{dt}{\log(t)} (\sim \frac{x}{\log(x)}), \text{ quand } x \to +\infty \tag{2.3}$$

l'estimation (2. 3) est même équivalente à la non-annulation de ζ sur $\mathrm{Re}(s) = 1$ ($\zeta(1 + it) \neq 0$, $\forall t \in \mathbb{R}$). Il n'est donc pas sur prenant que l'hypothèse de Riemann " *tous les zéros non triviaux de ζ sont sur la droite verticale* $\mathrm{Re}(s) = \frac{1}{2}$ " donnerait une version très précise de (2.3) si elle était

prouvée :

$$\pi(x) - \int_2^x \frac{dt}{\log(t)} = O(\sqrt{x}\log(x)), \text{ quand } x \to +\infty \tag{2.4}$$

La fonction Γ qui apparaît dans (2.2) est la fonction Gamma d'Euler défini sur $\mathrm{Re}(s) > 0$ par :

$$\Gamma(s) = \int_0^{+\infty} t^{s-1}\exp(-t)dt \tag{2.5}$$

L'équation fonctionnelle $\Gamma(s+1) = s\Gamma(s)$, que l'on prouve par intégration par parties, montre que $\Gamma(n) = (n-1)!$ pour tout entier $n \geq 1$ et prolonge Γ en une fonction méromorphe sur $\mathbb{C}$, avec des pôles simples aux entiers $-n \leq 0$, de résidu $\frac{(-1)^n}{n!}$ on pourra consulter [10], pp.114, pour plus de détails sur la fonction Γ.

Lemme 2.1 *Quelques soient les réels α et β tels que $\alpha > 1$ et $\beta \geq 0$, la série $\sum_{n\geq 1} \frac{\ln^\beta n}{n^\alpha}$ converge.*

Preuve. On sait que quel que soit $\beta \geq 0$, $\ln^\beta n = O(n^{\frac{\alpha-1}{2}})$, quand $n \to +\infty$ donc $\frac{\ln^\beta n}{n^\alpha} = O(n^{-\frac{\alpha+1}{2}})$. La série $n^{-\frac{\alpha+1}{2}}$ est une série de Riemann absolument convergente puisque $\frac{\alpha+1}{2} > \frac{1+1}{2} = 1$ ce qui implique, par les critères usuelles de domination des séries, la convergence de la série $\sum_{n\geq 1} \frac{\ln^\beta n}{n^\alpha}$. ■

Proposition 2.1 ***1)*** *La fonction zêta restreinte à $]1, +\infty[$ est une fonction de classe C^∞ et sa dérivée $K^{ème}$ est donnée par :*

$$\zeta^{(k)}(s) = \sum_{n=1}^{+\infty} \frac{(-1)^k \ln^k n}{n^s} \tag{2.6}$$

en outre, pour tout entier $k \geq 0$, la convergence de la série $\sum_{n\geq 1} \frac{(-1)^k \ln^k n}{n^s}$ est normale sur tout intervalle de la forme $[\alpha, +\infty[$ avec $\alpha > 1$.

2) *Plus généralement la fonction zêta est une fonction holomorphe sur le demi-plan $\{s \in \mathbb{C}$ tel que $\mathrm{Re}(s) > 1\}$ Et sa dérivée $K^{ème}$ est donnée par la formule(2.6). La convergence de la série $\sum_{n\geq 1} \frac{(-1)^k \ln^k n}{n^s}$ est normale sur tout demi-plan $\{s \in \mathbb{C}$ tel que $\mathrm{Re}(s) \geq \alpha\}$ avec $\alpha > 1$ d'après le **Lemme 2.1**.*

Proposition 2.2 ***(Développement Eulérien) :*** *Soient $\mathbf{P}$ l'ensemble des nombres premiers de $\mathbb{N}$ et s un nombre complexe tel que $\mathrm{Re}(s) > 1$. Le produit $\zeta(s) = \prod_{p\in\mathbf{P}} \frac{1}{1-p^{-s}}$ converge uniformément sur*

tout demi-plan de la forme $\{s \in \mathbb{C}$ *tel que* $\mathrm{Re}(s) \geq \alpha\}$ *avec* $\alpha > 1$ *et*

$$\forall s \in \mathbb{C} \text{ tel que } \mathrm{Re}(s) > 1,\ \zeta(s) = \prod_{p \in \mathbf{P}} \frac{1}{1 - p^{-s}}$$

Corollaire 2.1 *Quel que soit le nombre complexe* s *tel que* $\mathrm{Re}(s) > 1$*, on a* $\zeta(s) \neq 0$.

On a le développement asymptotique suivant :

$$\sum_{p \in \mathbf{P}} \frac{1}{p^s} = -\ln(s-1) + A + O(1), \text{ quand } s \to 1^+,\ s \in \mathbb{R}$$

où A est une certaine constante réelle. En particulier, la série $\sum_{p \in \mathbf{P}} \frac{1}{p}$ diverge.

Continuité de ζ sur $]1, +\infty[$

Soit α un réel strictement supérieur à 1 donné. Pour $n \geq 1$ donné, la fonction $s \longmapsto \frac{1}{n^s}$ est continue sur $[\alpha, +\infty[$. De plus, pour tout réel s de $[\alpha, +\infty[$, $\left|\frac{1}{n^s}\right| = \frac{1}{n^s} \leq \frac{1}{n^\alpha}$ avec égalité pour $s = \alpha$ ou encore

$$\sup\left\{\left|\frac{1}{n^s}\right|,\ s \in [\alpha,\ +\infty[\right\} = \frac{1}{n^\alpha}$$

puisque la série numérique de terme général $\frac{1}{n^\alpha}$ converge (série de Riemann d'exposant $\alpha > 1$), la série de fonctions de terme général $s \longmapsto \frac{1}{n^s}$, $n \geq 1$, est normalement convergente et donc uniformément convergente sur $[\alpha, +\infty[$. La somme ζ est donc continue sur $[\alpha, +\infty[$ en tant que limite uniforme sur $[\alpha, +\infty[$ d'une suite de fonctions continues sur $[\alpha, +\infty[$. Ceci étant vrai pour tout réel α de $]1, +\infty[$, on a montré que la fonction ζ est continue sur $]1, +\infty[$.

2.2.6 Conjecture de Hilbert-Pôlya

Hilbert et Pôlya ont pensé sur ce conjecture que les valeurs de t telles que $\frac{1}{2} + it$ soit un zéro de la fonction zêta de Riemann doivent être les valeurs propres d'un operateurs hermitien à l'aide de la théorie spectrale. En 1950, Néanmoins Selberg a démontré la formule des traces de Selberg qui est représenté la dualité entre les spectres des longueurs d'une surface de Riemann et les valeurs propres de son laplacien [11]. En 1972, Hugh Montgomery conjectura des propriétés de la distribution statistique des zéros, tel que Freeman Dyson fit remarquer à Montgomery que la distribution des zéros de la fonction de zêta de Riemann est maintenant reconnue pour satisfaire les mêmes statistiques que les valeurs propres d'une matrice hermitienne aléatoire, ce que l'on

appelle l'ensemble unitaire gaussien. En 1996, Alain connes a énoncé une formule de trace qui est actuellement équivalente à l'hypothèse de Riemann généralisée. Ceci a, par conséquent affermi la correspondance avec la formule de trace de Selberg.

2.2.7 Connexion possible avec la mécanique quantique

Une connexion possible de l'opérateur de Hilbert-Pólya avec la mécanique quantique a été donnée par Pôlya. L'opérateur de Hilbert-Pôlya est de la forme $\frac{1}{2} + iH$ où H est le Hamiltonien d'une particule de masse m c'est-à-dire se déplaçant sous l'influence d'un potentiel $V(x)$. La conjecture de Riemann est équivalente à l'affirmation que le Hamiltonien est un opérateur hermitien, ou de manière équivalente que V est réel.

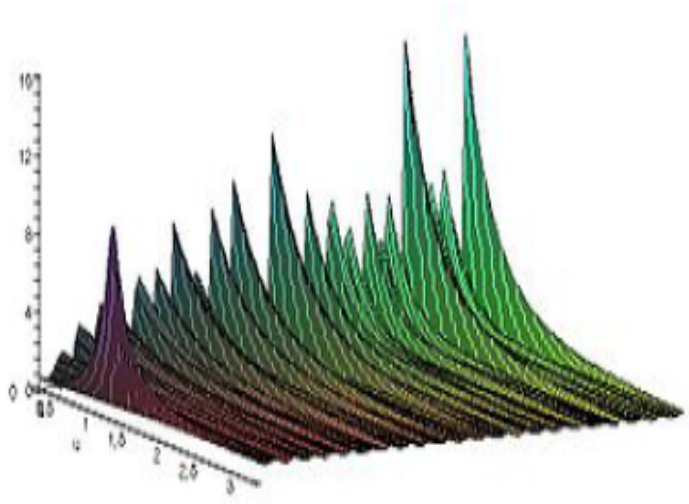


Figure 2 : Le module de la fonction $(u, t) \mapsto \zeta(u + it)$ de Riemann pour $0 \leq u \leq 3$ et $0.1 \leq t \leq 200$. On notera la pointe due au pôle en 1 et la très grande irrégularité du module.

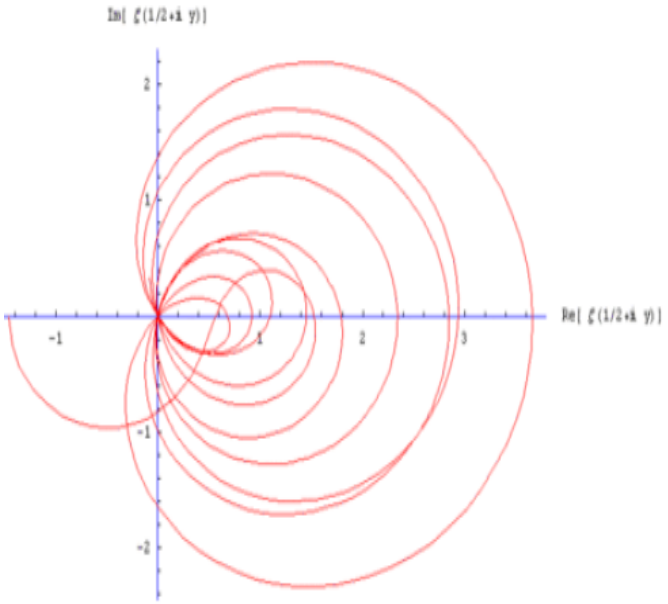


Figure 3 : Trajectoire de $\zeta(\frac{1}{2}+iy)$ pour y de 0 à 50.

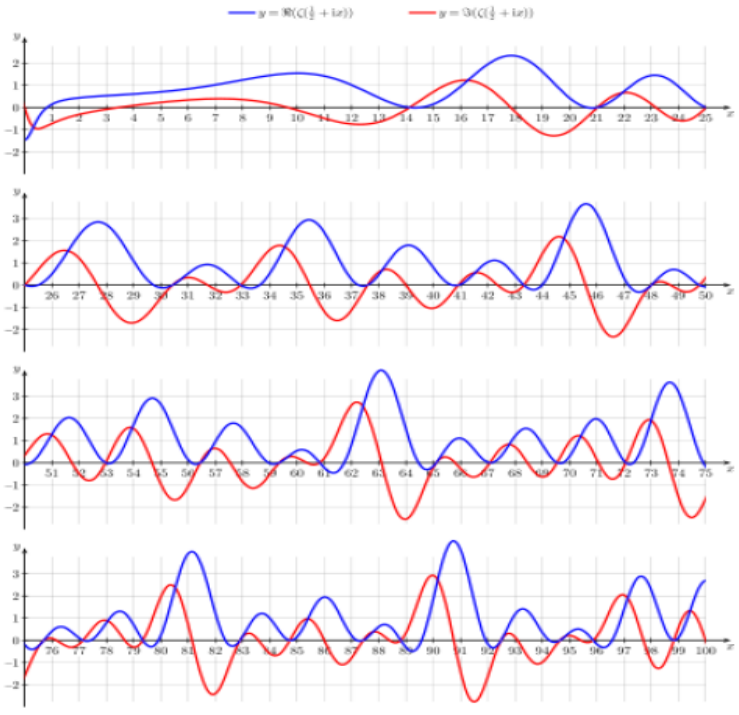


Figure 4 : Représentation en bleu de la partie réelle et en rouge de la partie imaginaire de la fonction $\zeta(\frac{1}{2}+ix)$ sur l'intervalle $[0,\ 100]$ où l'on voit clairement apparaître les premiers zéros non triviaux lorsque les deux courbes se croisent sur l'axe des abscisses.

2.3 Les nombres premiers

On sait depuis Euclide que l'ensemble P des nombres premiers est infini.
En effet, si p est premier, le plus petit diviseur premier de $1 + p!$ dépasse p.
La répartition des nombres premiers a été étudiée par des générations de mathématiciens, mais il a fallu attendre 1896 pour que le résultat asymptotique suivant soit en n démontré.

2.3.1 Existence d'une infinité des nombres premiers

Euclide a démontré dans ces **éléments** que les nombres premiers sont en plus grande quantité que toute quantité proposée de nombres premiers. Autrement dit, il existe **une infinité** de nombres premiers.
Pour montrer qu'il existe une infinité des nombres premiers, on a besoin le lemme suivant :

Lemme 2.2 *Tous les entiers plus que* 1 *à un diviseur premier.*

Théorème 2.3 *Il existe une infinité des nombres premiers.*

Preuve. Supposons que $p_1, p_2, ..., p_n$ sont tous les nombres premiers où n est une entier positif et $p_1 < p_2 < .... < p_n$. On considère un entier Q_n

$$Q_n = p_1 p_2 ....p_n + 1$$

on sait que tous les entiers a un diviseur premier par le lemme précédent, alors il doit exister un autre nombre premier que les p_n qui divise Q_n, car p_i ne divise pas Q_n pour tout $i \in \{1, ..., n\}$. ■

Proposition 2.3 *Tout entier* $n \geq 2$ *admet un diviseur premier. Si* n *n'est pas premier alors il possède un diviseur premier* p *tel que* $p \leq E(\sqrt{n})$ *(*$E(.)$ *désigne la partie entière).*

Proposition 2.4 *L'ensemble des nombres premiers est infini.*

Preuve. Soit $p_1, ..., p_n$ une suite finie de n nombres premiers et $N = p_1 ... p_n$. D'après la proposition précédente $N + 1$ possède un diviseur premier p qui ne peut être l'un des p_i car le reste de la division euclidienne de $N + 1$ par p_i est 1. Donc pour tout entier n, il existe plus de n nombres premiers. Leur ensemble est infini. ■

Remarque 2.2 *La proposition précédente peut être considérée comme un cas particulier du* ***théorème de Dirichlet :*** *Si* a *et* b *sont deux entiers premiers entre eux alors il existe une infinité de nombres premiers de la forme* $a + bn$, $n \in \mathbb{N}$. *La démonstration de ce théorème est très difficile.*

2.3.2 Petite chronologie

On peut dresser une liste (non exhaustive) de mathématiciens célèbres ayant contribué à cette étude :

Euclide (Grec 330-275 avant JC) montre que P est infini.

Leonhard Euler (Suisse 1707-1783) démontre que : $\sum_{p} \frac{1}{p}$ diverge.

Adrien Legendre (Français 1752-1833) consacre un ouvrage à la théorie des nombres.

Carl Gauss (Allemand 1777-1855) est le premier à conjecturer le **TNP**.

August Möbius (Allemand 1790-1868) introduit la fonction qui porte son nom.

Pafnouti Tchebychev (Russe 1821-1894) prouve que : $(\forall x \geq 30),\ 0.9 \leq \frac{\pi(x)\ln x}{x} \leq 1.2$.

Bernhard Riemann (Allemand 1826-1866) introduit la fonction $\zeta(z) = \sum_{n=1}^{+\infty} \frac{1}{n^z}$.

Jacques Hadamard (Français 1865-1963) et Charles de la **Vallée-Poussin** (Belge 1866-1962) Démontrent indépendamment l'un de l'autre le **TNP** en 1896. Leurs démonstrations reposent en grande partie sur la fonction de Riemann.

Paul Erdös (Hongrois 1913-1996) et Atle Selberg (Norvégien 1917) publient en 1949, et à la surprise générale, une démonstration dite «élémentaire» du **TNP**, qui n'utilise ni la fonction, ni plus généralement les fonctions d'une variable complexe.

Notations

Conventions

x désignera toujours un nombre réel supérieur ou égal à 1, p un nombre premier, et k, l, m, n, v..., des nombres entiers naturels non nuls. On allègera les notations en ne précisant pas les ensembles. Ainsi, par exemple, le produit des diviseurs premiers de l'entier n pourra être noté $\prod_{p/n} p$ ou $\prod_{pk=n} p$.

Ensembles de référence

P est l'ensemble des nombres entiers premiers.

P' est l'ensemble des entiers qui n'ont pas de diviseur carré supérieur à 1. (**Nombres de Möbius**)

$P'' = \{p^v / p \in P \text{ et } v \in \mathbb{N}^*\}$ est l'ensemble des nombres premiers.

On a :

$$P = P' \cap P''$$

Fonctions de la variable entière n

$$\tau(n) = card\,\{p/p \text{ divise } n\}$$

$$\mu(n) = \begin{cases} 0, \text{ si } n \notin P' \\ (-1)^{\tau(n)}, \text{ si } n \in P' \end{cases}, \textbf{ (fonction de Möbius)}$$

Exemple 2.4 $\mu(10) = 1$, $\mu(8) = 0$

$$\delta(n) = \sum_{k/n} \mu(k)$$

$$\Lambda(n) = \begin{cases} 0, \text{ si } n \notin P'' \\ \ln(p), \text{ si } n = p^v \end{cases}, \text{ (fonction de von Mangoldt)}$$

Exemple 2.5 $\Lambda(8) = \ln 2$

n	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(n)$	$+1$	-1	-1	0	-1	$+1$	-1	0	0	$+1$	-1	0	-1
$\Lambda(n)$	0	$\ln 2$	$\ln 3$	$\ln 2$	$\ln 5$	0	$\ln 7$	$\ln 2$	$\ln 3$	0	$\ln 11$	0	$\ln 13$

Fonctions de la variable réelle x

$$M(x) = \sum_{k \leq x} \mu(k), \textbf{ (fonction de Merten)}$$

$$\varphi(x) = |M(x)| \ln^2 x - 2x \ln x$$

$$\sigma(x) = \sup_{t \geq x} \left| \frac{M(t)}{t} \right|$$

$$\Psi(x) = \sum_{p \leq x} v_P \ln(p) = \sum_{n \leq x} \Lambda(n), \textbf{ (fonction de Tchebycheff)}$$

$$v_p = \left[\frac{\ln(x)}{\ln(p)} \right] = \begin{cases} 0, \text{ si } p > x \\ \max \{v / p^v \leq x\}, \text{ si } p \leq x \end{cases}$$

On définit :

$$\lambda_d = \lambda_{d,\,x} = \mu(d) \log^2 \frac{x}{d}$$

Définition 2.3 ***(La fonction*** $v(x)$***) :*** *La fonction* $v(x)$ *est définie ainsi :*

$$v(x) = \sum_{p \leq x} \log p$$

Exemple 2.6 $v(10) = \log 2 + \log 3 + \log 5 + \log 7$

Définition 2.4 ***(Comparaison asymptotique ou O notation)*** *Soient f et g sont deux fonctions qui sont définie dans $\mathbb{R}$, on écrit :*

$$f(x) = O(g(x))$$

si est seulement s'il existe une constant positif M, tel que

$$|f(x)| \leq M\,|g(x)|$$

pour x assez grande.

Exemple 2.7 $4x^3 + 2014x^2 = O(x^3)$ *car il existe une M assez grande que $4x^3 + 2014x^2 \leq Mx^3$ où $M = 5$.*

Définition 2.5 ***(La fonction θ_n) :*** *La θ_n est une fonction qui est définie ainsi :*

$$\theta_n = \theta_{n,\,x} = \sum_{d|n} \lambda_n$$

Proposition 2.5 ***(La fonction θ_n)*** *On a la définition suivante de la fonction θ_n :*

$$\theta_n\,(x) = \begin{cases} \log^2 x, \text{ pour } n = 1 \\ \dfrac{\log p \log x^2}{p}, \text{ pour } n = p^\alpha,\ \alpha \geq 1 \\ 2 \log p \log q, \text{ pour } n = p^\alpha q^\beta,\ \alpha \geq 1,\ \beta \geq 1 \\ 0, \text{ sinon} \end{cases}$$

2.3.3 Aperçu sur les nombres premiers

Un nombre premier est un nombre entier $p \geq 2$ dont les seuls diviseurs positifs sont 1 et p. Les nombres 0 et 1 ne sont ni premiers ni composés. La liste des vingt premier : 2, 3 , 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71. Tout nombre entier naturel se décompose de manière unique en un produit de nombres premiers. Par exemple, $3192290292037 = 7 \times 11^2 \times 37^4 \times 2011$.

Remarque 2.3 2011 *est un nombre premier. On essaye en vain de le diviser par* $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$ *cela suffit car* 47 *est le premier suivant et* $47^2 = 2209 > 2011$.

Question de la répartition des nombres premiers : C'est une question très large, aux multiples facettes. Premier exemple, le théorème de Tchebycheff (ca 1850), Ex-Postulat de Bertrand : *Pour tout entier naturel* n*, l'intervalle* $[n,\ 2n]$ *contient au moins un nombre premier.* Second exemple : On dit que deux nombres premiers sont **jumeaux** si leur différence vaut 2. Premier exemple. On ne sait pas s'il existe une infinité de nombres premiers **jumeaux**. Les trois plus petits couples de nombres premiers jumeaux sont $(3, 5)$, $(5, 7)$ et $(11, 13)$. Le 25 décembre 2011, le plus grand connu est $3756801695685 \times 2^{666669} \pm 1$; les deux nombres possèdent 200700 chiffres. Il est conjecturé qu'il existe une infinité de nombres premiers jumeaux.
La fonction π : Pour tout nombre réel $x > 0$, on note $\pi(x)$ le nombre de nombres premiers p qui vérifient $p \leq x$. Pour tout entier naturel $n \geq 1$, on notera p_n le $n^{ième}$ nombre premier. Début du tableau ci-dessous :

n	p_n	$n \ln n$	$\frac{p_n}{n \ln n}$
1	2	0	$-$
2	3	~ 1	~ 2.164
3	5	~ 3	~ 1.517
4	7	~ 5	~ 1.262
10	29	~ 23	~ 1.259
100	541	~ 460	~ 1.174
1000	7919	~ 6907	~ 1.146

En 1896, Hadamard et de la Vallée-Poussin démontrent indépendamment le difficile théorème des nombres premiers : $p_n \sim n \ln n$ lorsque n tend vers $+\infty$, ce qui signifie que la limite en $+\infty$ de $\dfrac{p_n}{n \ln n}$ égale 1.
Une formulation équivalente :

$$\pi(x) \sim \frac{x}{\ln x}, \text{ lorsque } x \text{ tend vers } +\infty$$

ce qui signifie que :

$$\lim_{x \to +\infty} \frac{\pi(x) \ln x}{x} = 1$$

2.4 Sur la recherche des nombres premiers

Les techniques modernes de codage exigent la connaissance de grands nombres premiers d'où l'intérêt d'algorithmes permettant de trouver des nombres premiers. Avant de décrire le premier

algorithme, notons que la répartition des nombres premiers semble très irrégulière. On peut apporter à l'appui de cette affirmation les faits suivants :
1) Il existe deux nombreux couples $(p,\ p+2)$ formés de nombres premiers dits **jumeaux**. On ne sait pas s'il y en a une infinité mais on en connait de très grands.
2) Il existe des intervalles de $\mathbb{N}$ de longueurs arbitrairement grandes ne contenant aucun nombre premier. Par exemple, pour tout entier n, $[n!+2,\ n!+n]$ ne contient aucun nombre premier car $n!+k$, $2 \leq k \leq n$, est divisible par k.
3) Tout intervalle $[n,\ 2n]$, $n \geq 1$, contient au moins un nombre premier (théorème de Bertrand ou de Tchebycheff).
4) (**Conjecture**) : Pour chaque nombre naturel $d \geq 2$ et pair, il existe une infinité des nombres premiers p_i et p_j tel que $p_i - p_j = d$
Notons aussi les différents objectifs que peut présenter la recherche de nombre premier :
- Trouver tous les nombres premiers compris entre 2 et n.
- Trouver un très grand nombre premier sans propriété particulière (par exemple pour utiliser ce nombre en cryptographie).

2.5 Cryptographie à clé publique

Le principe de la **cryptographie symétrique** est le premier système public qui décrive en 1978 par **Ronald Rivest, Adi Shamir** et **Leonard Adleman** (nommé d'après leurs initiales **RSA**), tel que ce système basé sur les propriétés des nombres premiers et de la factorisation [12]. Dans un tel système, deux clés sont utilisées : L'une sert à chiffrer, l'autre à déchiffrer. La clé permettant de chiffrer est accompagnée d'un grand nombre entier premier, le produit de deux grands nombres premiers gardés secrètes (de l'ordre de 200 chiffres).
Pour calculer la clé de déchiffrement, la seul méthode connue nécessite de connaître les deux facteurs premier. La sécurité du système est basée sur le fait qu'il est facile de trouver deux grands nombres premiers (en utilisant des tests de primalité la méthode de Lehmer) et de les multiplier entre eux, mais qu'il serait difficile pour un attaquant de retrouver ces deux nombres. Ce système permet également de créer des signatures numériques, et a révolutionné le monde de la cryptographie.
La méthode R.S.A
La méthode **RSA** (pour Rivest, Shamir, Adleman) permet de coder un message numérique M puis de le décoder. Tout message littéral peut être transformé en un message numérique : Par exemple, on remplace a par 01, b par 02,..., z par 26.

Cette méthode de codage exige la connaissance de grands nombres premiers. La taille de ces nombres va en croissant avec les progrès de l'informatique d'où l'intérêt des tests de primalité.

Préparation du code

1) On choisit deux nombres premiers p et q.

2) On effectue leur produit $n = pq$ et on calcule $\phi(n) = (p-1)(q-1)$.

3) On choisit un nombre d premier avec $\phi(n)$.

4) On calcule e tel que $0 < e < \phi(n)$ et $ed \equiv 1(\mathrm{mod}\,\phi(n))$. C'est possible car d et $\phi(n)$ étant premier entre eux, il existe deux entiers u et v tels que $ud + v\phi(n) = 1$ (théorème de Bézout). On a donc $ud \equiv 1(\mathrm{mod}\,\phi(n))$ et e est le reste de la division euclidienne de u par $\phi(n)$.

Codage et décodage

Soit M un entier tel que $0 < M < n$, M n'étant pas multiple de p ou de q (M est premier avec n). On calcule C vérifiant $0 < C < n$ et $C \equiv M^e(\mathrm{mod}(n))$. L'entier C code le message M. On a $M \equiv C^d(\mathrm{mod}(n))$. En effet : $C^d \equiv M^{ed}(\mathrm{mod}(n))$ et il existe un entier k tel que $ed - 1 = k\phi(n)$ d'où $M^{ed} \equiv MM^{k\phi(n)}(\mathrm{mod}(n))$.

L'entier M étant premier avec n, le théorème d'Euler entraine $M^{\phi(n)} \equiv 1(\mathrm{mod}(n))$ d'où $C^d \equiv M(\mathrm{mod}(n))$. Comme $0 < M < n$ cette congruence détermine M et permet de décoder le message C.

Le codage des suites finies d'entiers

L'unicité de la décomposition en facteurs premiers entraine que l'application ϕ qui a une suite finie d'entiers n_1,..., n_k fait correspondre l'entier $p_1^{n_1+1}...p_k^{n_k+1} = 2^{n_1+1}3^{n_2+1}...p_k^{n_k+1}$ est injective. On dit que ϕ est le codage des suites finies d'entiers et cette technique a de nombreuses applications, en général abstraites car les valeurs de ϕ sont de très grands entiers ($\phi(1, 1, 1, 1, 1) = 2^2 3^2 5^2 7^2 11^2 = 5336100$).

Application aux cardinaux

Il résulte de l'injectivité de ϕ que l'ensemble des suites finies de $\mathbb{N}$ est dénombrable. Plus généralement, l'ensemble des suites finies d'éléments d'un ensemble dénombrable est dénombrable et donc le produit cartésien d'un nombre fini d'ensembles dénombrables est dénombrable.

En particulier, $\mathbb{N}^2$ est dénombrable et donc aussi l'ensemble des nombres rationnels positifs. On en déduit facilement que $\mathbb{Q}$ est aussi dénombrable.

Application en logique

Le chiffrement des suites finies d'entiers par un entier est attribué au logicien **Kurt Gödel** qui l'a utilisé dans les années trente pour démontrer ses célèbres théorèmes concernant l'incomplétude de l'arithmétique et les problèmes posés par sa consistance.Ce logicien **K. Gödel** commence par remplacer chaque symbole figurant dans une formule de l'arithmétique par un entier bien déterminé et ainsi toute formule devient une suite finie d'entiers n_1,..., n_k. A cette suite il fait corres-

pondre l'entier $\phi(n_1,..., n_k)$ appelé depuis le nombre de **Gödel** de la formule. Plus généralement, une démonstration de l'arithmétique, qui est une suite finie de formules, devient aussi un entier et, par exemple, l'affirmation de l'existence d'une démonstration est remplacée par l'affirmation de l'existence d'un entier.

Chapitre 3

Distribution des nombres premiers dans les grandes progressions arithmétiques.

3.1 Théorème de la progression arithmétique

En mathématique, et plus particulièrement en théorie des nombres, le théorème de la progression arithmétique, dû au mathématicien allemand Gustav Lejeune Dirichlet, est une généralisation du théorème d'Euclide sur les nombres premiers qui s'énonce de la façon suivante :

Théorème 3.1 *(Théorème de Dirichlet) Si m et n sont deux entiers premier entre eux et si n est strictement positif, il existe une infinité de nombres premiers de la forme $m + an$ avec a entier.*

Ce qui est équivalent à l'énoncé suivant :

Théorème 3.2 *Si m et n sont entiers premier entre eux et si n est strictement positif, il existe une infinité de nombres premiers dans la classe de m modulo n.*

Ce théorème utilise à la fois les résultats de l'arithmétique modulaire et ceux de la théorie analytique des nombres.

3.2 Quelques suites arithmétiques

Définition 3.1 *On appelle suite arithmétique une suite de nombres où on passe d'un terme au suivant en ajoutant toujours le même nombre (ce nombre est appelé la base de la suite arithmétique et est souvent noté r).*

Exemple 3.1 *Suite arithmétique de premier terme 2 et de la base 3 :* $2 \quad 5 \quad 8 \quad 11 \quad 14 \quad 17$ *etc.*

Notations possibles : Si on note u_0 le premier terme, on a : $u_0 = 2$, $u_1 = 5$, $u_2 = 8$, etc. et, dans ce cas, u_n est le $(n+1)^{ème}$ terme. Si on note u_1 le premier terme, on a : $u_1 = 2$, $u_2 = 5$, $u_3 = 8$, etc. et, dans ce cas, u_n est $n^{ème}$ le terme. Dans les deux cas, $u_{n+1} = u_n + r$.
Formule permettant de calculer le $n^{ème}$ d'une suite arithmétique :

$$n^{ème} \textbf{ terme} = \textbf{premier terme} + (n-1)r$$

Remarque 3.1 *Si on note u_0 le premier terme, on a : $u_n = (n+1)^{ème}$ terme $= u_0 + nr$.*
Si on note u_1 le premier terme, on a : $u_n = n^{ème}$ terme $= u_1 + (n-1)r$.

Exemple 3.2 *Le $12^{ème}$ terme de la suite arithmétique de premier terme 2 et de la base 3 vaut $2+11\times3$ soit 35.*
Formule permettant de calculer la somme du premier terme d'une suite arithmétique :

a)

$$S = \textbf{nombre de terme } (\frac{\textbf{premier terme } + \textbf{ dernier terme}}{2})$$

b) Remarque : Si on note u_0 le premier terme, $u_0 + u_1 + u_2 + \ldots + u_n =$ somme des $(n+1)$ premiers termes

$$= (n+1)(\frac{u_0 + u_n}{2})$$

Si on note u_1 le premier terme, $u_1 + u_2 + u_3 + \ldots + u_n =$ somme des n premiers termes

$$= n(\frac{u_1 + u_n}{2})$$

c) Exemple concernant la suite arithmétique de premier terme 2 et de la base 3 :

$$2 + 5 + 8 + 11 + 14 + 17 = 6(\frac{2+17}{2}) = 57$$

d) Exemple « classique » (avec la suite des entiers naturels qui est la suite arithmétique de premier terme 1 et de la base 1) :

$$1 + 2 + 3 + 4 + 5 + ... + (n-1) + n = n(\frac{1+n}{2}) = \frac{n(n+1)}{2}$$

donc

$$1 + 2 + 3 + 4 + 5 + \ldots + 67 + 68 = \frac{68 \times 69}{2} = 2346$$

e) Remarque : Une formule analogue est utilisable pour trouver la somme de termes consécutifs d'une suite arithmétique quand le premier terme considéré n'est pas le premier terme de la suite arithmétique : $u_{12} + u_{13} + u_{14} + \ldots + u_{33} + u_{34} = 23(\frac{u_{12} + u_{34}}{2})$. Il y a $(34 - 12 + 1)$ soit 23 termes. Exemple « Classique » (avec la suite des entiers naturels qui est la suite arithmétique de premier terme 1 et de la base 1) : $25 + 26 + 27 + \ldots + 57 + 58 = 34(\frac{25+58}{2}) = 1411$. Il y a $(58 - 25 + 1)$ soit 34 termes.

3.3 Progressions arithmétiques dans les nombres premiers, d'après B. Green et T. Tao

Théorème 3.3 *[13] L'ensemble des nombres premiers contient des progressions arithmétiques de toutes longueurs.*

La méthode employée permet de déterminer explicitement pour tout k un entier N (très grand) tel que l'ensemble des nombres premiers plus petits que N contienne une progression arithmétique de longueur $k+1$.
Le **théorème 3.3** répond à une question forte ancienne bien que difficile à dater exactement. Très peu de résultats partiels étaient connus jusqu'ici ; citons celui de van der Corput **[14]** qui a montré en 1939 l'existence d'une infinité de progressions de longueur 3 dans les nombres premiers.
En 1923, Hardy et Littlewood **[15]** ont proposé une conjecture très générale sur la répartition de certaines configurations dans les nombres premiers, qui entraînerait une version quantitative précise du **Théorème 3.3** si elle s'avérait exacte. Ce même théorème suivrait aussi d'une résolution positive donnée à une conjecture proposée par Erdös et Turan [16] en 1936 :

Conjecture 3.4 *Tout sous-ensemble E de $\mathbb{N}^*$ vérifiant*

$$\sum_{n\in E}\frac{1}{n}=+\infty$$

contient des progressions arithmétiques de toutes longueurs.

Cette conjecture reste totalement ouverte et les méthodes de Green et Tao ne permettent pas de s'en approcher. Dans une direction voisine, Szemerédi a montré en 1975 l'existence de progressions sous l'hypothèse plus forte de la densité positive. Rappelons que la densité d'un ensemble d'entiers $E\subset\mathbb{N}$ est :

$$d^*(E)=\lim\sup_{N\to\infty}\frac{1}{N}card(E\cap[0,\,N-1])$$

Le théorème de Szemerédi s'énonce :

Théorème 3.5 ***Théorème de Szemerédi [17].*** *Tous ensemble d'entiers de densité positive $(d^*(E)>0)$ contient des progressions arithmétiques de toutes longueurs.*

Il peut aussi s'exprimer en termes d'ensembles finis d'entiers :

Théorème 3.6 ***Version finie du théorème de Szemerédi :*** *Pour tout entier $k\geq 2$ et tout réel $\delta>0$ il existe un entier $N=N(k,\,\delta)$ tel que tout sous-ensemble E de $[0,\,N[$ ayant au moins δN éléments contienne une progression arithmétique de longueur $k+1$.*

Ce théorème ne peut évidemment pas être utilisé directement puisque les nombres premiers ont une densité nulle. Cependant il tient une place centrale dans la démonstration.

3.4 Conclusion

Les nombres premiers sont considérés d'une part comme la pierre de la construction des nombres entiers, d'autre part, ils sont importants dans les applications géométriques et arithmétiques. Dans notre mémoire, on a expliqué avec des détails la relation entre les nombres premiers et la fonction zêta de Riemann, tel que ces nombres sont distribués uniformément suivant l'hypothèse de Riemann tant qu'elle est vraie. Alors, on déduit qu'il y a une conformité entre les zéros de la fonction zêta de Riemann et la distribution des nombres premiers.

Bibliographie

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976, pp. 80, th. 4.5.

[2] G. H. Hardy et E. M. Wright, *Introduction à la théorie des nombres* [*An Introduction to the Theory of Numbers*], Vuibert-Springer, 2007, pp. 11.

[3] G. Tenenbaum et M. Mendès France, *Les Nombres premiers, Que sais-je 571*, Paris, PUF, 1997, pp. 11.

[4] Apostol 1976, pp. 79, th. 4. 4.

[5] Hardy et Wright 2007, pp. 444, th. 420.

[6] Y. Matsuoka, *Generalized Euler Constants Associated with the Riemann Zeta Function, Number Theory and Combinatorics*, World Scientific, 1985, pp. 279295.

[7] G. H. Hardy et E. M. Wright pp. 321-330.

[8] Ellison et Mendès France, pp. 75.

[9] B. Riemann, *Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse*, Monatsberichte der Berliner Akademie, November 1859. Traduction en anglais sur le site http ://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zêta/.

[10] P. Eymard, J. P. Lafon, *Autour du nombre π*, Actualités Scientifiques et Industrielles no. 1443, Hermann, Paris, 1999.

[11] A. Connes, *Trace formula in noncommutative geometry and the zeros of the Riemann zeta function*, Selecta Math. (N. S.) 5 (1999), pp. 29–106.

[12] RL. Rivest, A. Shamir et L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Communications of the ACM, volume 21 Issue 2, Feb. 1978, pp. 120-126.

[13] B. Green, T. Tao, (2008).*The primes contain arbitrarily long arithmetic progressions*. Annals of Mathematics.167 (2) : pp. 481-547.

[14] J. G. van der Corput. *Uber Summen von Primzahlen und Primzahlquadraten*. Math. Ann. 116 (1939), 1–50.

[15] G. H. Hardy & J. E. Littlewood. *Some problems of "partition numerorum" III : on the expression of a number as a sum of primes*. Acta. Math., 44 (1923), pp. 1–70.

[16] P. Erdös & T. Turán. *On some sequences of integers*. J. London Math. Soc. 11 (1936), pp. 261–264.

[17] E. Szemerédi. *On sets of integers containing no k elements in arithmetic progression*. Acta Arith. 27 (1975), pp. 199–245.