

# Le théorème de Brun-Titchmarsh : une approche moderne

Olivier Ramaré

*Le 7 Avril 2005\**

## Résumé

Les dernières décennies ont vu des progrès immenses dans la compréhension des nombres premiers, presque tous dus à l'invention de la méthode du crible. Nous exposerons comment cette approche permet de majorer le nombre de premiers dans un intervalle  $[M + 1, M + N]$  uniformément en  $M$ .

## 1 Des nombres premiers

Commençons par rappeler que les nombres premiers sont ces entiers  $\geq 2$  qui ne sont divisibles par aucun entier  $\geq 1$ , sauf évidemment par 1 et par eux mêmes. 5 est un nombre premier. Ces entiers permettent de comprendre parfaitement tous les problèmes multiplicatifs grâce à la décomposition en facteurs premiers : tout entier  $n$  s'écrit comme un produit de nombres premiers et cette écriture est unique à l'ordre des facteurs près.

Dans la suite, la lettre  $p$  désignera toujours un nombre premier.

Donc nous comprenons bien la multiplication des entiers, bien leur addition et en conséquence nous maîtrisons aussi la soustraction et la division. Aussi nous tournons-nous vers le problème qui consiste à comparer ces deux structures. Il existe un lien : celui donné par la distributivité. Et si l'on ajoute (action du royaume additif) deux entiers divisibles pas 3 (propriété du royaume multiplicatif), on obtient un entier encore divisible par 3, c'est à dire que l'addition n'a pas détruit cette propriété additive ! Nous croyons à l'heure actuelle qu'il s'agit là du seul lien entre l'additif et le multiplicatif (excepté peut-être un autre lien ténu donné par la conjecture *abc*. Qui est largement hors sujet).

*Nombre premier et décomposition en facteurs premiers*

*Questions modernes : problèmes additifs/-multiplicatifs*

---

\*à Nantes (18/19h00) – VERSION 1

Parmi les problèmes de base, nous voulons connaître le plus précisément possible le nombre de nombres premiers dans les intervalles  $[M + 1, M + N]$ . Il s'agit encore d'un problème additif/multiplicatif, mais c'est un peu plus délicat à voir : être premier est bien une propriété multiplicative, et être inférieur à une borne donnée, disons  $X$ , est elle une propriété additive ! Il s'agit effectivement de la relation d'ordre liée à l'addition, et non celle liée à la multiplication qui est la divisibilité.

Le théorème des nombres premiers nous garantit que le nombre  $\pi(X)$  de nombres premiers  $\leq X$  est  $\simeq X/\text{Log } X$ .<sup>1</sup>

En fait, nous disposons d'une approximation encore meilleure

$$\pi(X) = \int_2^X \frac{dt}{\text{Log } t} + \mathcal{O}(X/\text{Log}^2 X)$$

Le 2 ci-dessus peut surprendre, et à voir la taille du terme d'erreur, nous pourrions le remplacer par n'importe quelle constante  $> 1$ . Comment dans ces conditions trouver une définition plus "canonique" que les autres ? En analyse classique et numérique, on prend comme borne initiale 0 ... Mais il faut réfléchir alors au sens de l'intégrale ! Ceci dit, le *logarithme intégral* est bien celui-ci, et c'est celui qui est tabulé, et non  $\int_2^X dt/\text{Log } t$ .

À interpréter comme "un nombre est premier avec probabilité  $1/\text{Log } t$ ".

Cela règle le cas de l'intervalle initial, où  $M = 0$ .

## 2 Une approche "crible"

La preuve donnant l'évaluation de  $\pi(X)$  est purement analytique. Si elle est précise dans son cas d'application, elle ne réussit pas à donner d'informations sur le nombre de nombres premiers dans un intervalle quelconque. Revenons donc aux bases.

Dans  $I = [M + 1, M + N]$ , il y a  $N/2 + \mathcal{O}(1)$  nombres pairs. En langage un peu flou, la probabilité qu'un entier de cet intervalle soit divisible par 2 est  $\frac{1}{2}$  et celle qu'il ne soit pas divisible par 2 vaut  $1 - \frac{1}{2}$ . Pour la divisibilité par 3, nous constatons que la probabilité qu'un entier de cet intervalle ne soit pas divisible par 3 vaut  $1 - \frac{1}{3}$ . Et en supposant ces deux événements indépendants, la probabilité pour qu'un entier ne soit divisible ni par 2, ni par 3, vaut  $(1 - \frac{1}{2})(1 - \frac{1}{3})$ . Pour obtenir les nombres premiers, il nous faut ôter les multiples de 2, de 3, ... de  $p$ , pour tous les  $p \leq ?$ , où il n'est pas

---

<sup>1</sup>Oui, l'auteur note  $\text{Log } x$  le logarithme népérien de  $x$  ...

clair jusqu'où nous devrions aller. Dans le cas de l'intervalle initial, il faudrait aller jusqu'à  $\sqrt{X}$  et cela donnerait

$$\pi(X) \stackrel{?}{\simeq} \prod_{p \leq \sqrt{X}} \left(1 - \frac{1}{p}\right) X.$$

Mais le théorème de Mertens nous dit que le produit est asymptotique à  $2e^{-\gamma}/\text{Log } X \simeq 1.122 \dots / \text{Log } X$ . La constante n'est par conséquent pas la bonne! Le problème dans cette approche vient de ce que nous considérons que le fait d'être divisible par  $p_1$  ou de l'être par un autre nombre premier  $p_2$  sont deux événements indépendants, ce qui n'est manifestement pas! Enfin, presque, puisque nous obtenons toutefois une expression proche de la vérité.

L'argument qui ne fonctionne pas concerne l'indépendance des événements. Et cette indépendance sera d'autant plus caduque que le nombre de modules considérés sera grand. Nous allons donc restreindre ce nombre de modules, mais du coup, nous n'allons plus avoir accès qu'à une borne supérieure.

*Utilisation  
ailleurs*

En contrepartie, cette approche va fonctionner dans le cas général d'un intervalle, là où le théorème des nombres premiers ne s'applique pas!

### 3 L'inégalité de Brun-Titchmarsh

**Théorème de Brun-Titchmarsh simplifié.** *Pour  $M$  et  $N$  deux entiers  $\geq 1$ , le nombre  $Z$  de nombres premiers dans l'intervalle  $[M + 1, M + N]$  est au plus  $2N/\text{Log } N$ .*

Si  $M = 1$ , le théorème des nombres premiers nous donne un meilleur résultat, puisqu'il nous permet de remplacer le 2 par un  $1 + o(1)$ . L'avantage de cette borne est ailleurs, et précisément dans le fait que nous pouvons l'appliquer lorsque  $M$  est très grand par rapport à  $N$ . Nous trouvons par exemple qu'entre  $10^{100}$  et  $10^{100} + 10\,000$ , il y a moins de 2 200 nombres premiers.

La version du théorème que nous proposons est due à (Montgomery & Vaughan, 1973). C'est Linnik qui dans les années 40 a baptisé ce genre de résultat des théorèmes de Brun-Titchmarsh à cause d'un lemme allant dans cette direction de Titchmarsh dans les années 30 où il utilisait une méthode de crible due au père des méthodes de crible : Viggo Brun. Nous avons ajouté l'adjectif "simplifié" ci-dessus, parce que la version non simplifiée traite des nombres premiers en progressions arithmétiques. L'adaptation énoncée plus loin est sans difficulté.

Par contre, le facteur 2 est lui vital, et toute amélioration aurait des répercussions énormes sur notre connaissance des nombres premiers.

Nous allons démontrer une version un peu plus faible avec  $4 + o(1)$  au lieu de la constante 2 ; et aussi imposer  $M \geq N^{1/4}$ , mais un peu plus de soin dans la preuve permettrait d'obtenir  $2 + o(1)$  sans condition sur  $M$ . Par contre, montrer que le  $o(1)$  peut être pris égal à 0 est plus difficile.

Nous allons prouver une version légèrement affaiblie de ce théorème en passant par une petite série de quatre lemmes. Nous y posons

$$\mathcal{Q} = \{q \leq Q, q \text{ sans facteurs carrés}\} \quad (1)$$

où  $Q$  est un paramètre que nous choisirons plus loin. La route que nous prenons est bien loin a priori des considérations de divisibilité et d'indépendance que nous avons utilisées pour la motiver. Il serait trop long de refaire ici le chemin qui va d'une approche à l'autre. Contentons de dire ici que ce chemin existe, les deux méthodes ne sont effectivement pas étrangères l'une à l'autre, et celle que nous présentons est franchement moderne.

## 4 Considérations hermitiennes

Notre premier lemme prend place dans un espace de Hilbert  $\mathcal{H}$ .

**Lemme 1 (Parseval approché).** *Soit  $(\varphi_q)_{q \in \mathcal{Q}}$  une famille finie de points de  $\mathcal{H}$ . Soit  $f$  un autre point de  $\mathcal{H}$ . Alors*

$$\sum_{q \in \mathcal{Q}} |[f|\varphi_q]|^2 / M_q \leq \|f\|^2$$

où  $M_q$  est une borne supérieure pour  $\sum_{q' \in \mathcal{Q}} |[\varphi_q|\varphi_{q'}]|$ .

Pour comprendre ce lemme, il suffit de considérer le cas où les  $\varphi_q$  sont deux à deux orthogonaux. Dans ce cas, nous pouvons prendre  $M_q = \|\varphi_q\|^2$  et l'inégalité proposée est simplement celle de Parseval. Ce lemme permet de se dispenser de l'hypothèse d'orthogonalité, mais est construit en pensant que notre système est "presque orthogonal", i.e. que  $M_q$  vaut "presque"  $\|\varphi_q\|^2$ .

Inégalité due à Selberg dans les années 70. On dit souvent que c'est le mathématicien hongrois Hálász qui a introduit un peu avant dans la théorie ce genre d'inégalités générales, mais l'histoire n'est pas claire à ce sujet.

## 5 Un peu d'arithmétique

Notre second lemme concerne les sommes de Ramanujan :

$$c_q(n) = \sum_{\substack{a=1, \\ \text{pgcd}(a,q)=1}}^q \exp(2i\pi an/q). \quad (2)$$

Bien sûr,  $c_q(n)$  ne dépend que de la classe de  $n$  modulo  $q$ . Notons dès à présent que cette somme porte sur  $\phi(q)$  entiers  $a$ , où  $\phi(q)$  désigne l'indicateur d'Euler, et ce parce que  $\phi(q)$  est précisément le nombre d'entiers  $\leq q$  premiers à  $q$ .

À titre d'exemple, pour  $q = p$  un nombre premier, la condition  $\text{pgcd}(a, p) = 1$  se réduit à  $a \neq 0$  et

$$c_p(n) = \sum_{a=1}^p \exp(2i\pi an/p) - 1 = \begin{cases} p-1 & \text{si } p|n, \\ -1 & \text{si } p \nmid n. \end{cases} \quad (3)$$

Voilà qui règle le cas où  $q$  est un nombre premier. En utilisant le lemme chinois, nous montrons que

$$c_{q_1 q_2}(n) = c_{q_1}(n) c_{q_2}(n) \quad \text{si } \text{pgcd}(q_1, q_2) = 1. \quad (4)$$

Comme dans notre application,  $q$  sera un produit de nombres premiers distincts, la conjugaison de (3) et de (4) suffit pour calculer  $c_q(n)$ . Voici la propriété qui nous intéresse particulièrement :

**Lemme 2.** *Si  $q \in \mathcal{Q}$  et  $n$  est premier à  $q$ , alors  $c_q(n)$  vaut  $(-1)^{\omega(q)}$  où  $\omega(q)$  est le nombre de facteurs premiers de  $q$ .*

En particulier, il s'agit d'un nombre indépendant de  $n$  et de module 1.

Notre troisième lemme donne une évaluation pour la fonction sommatoire d'une fonction multiplicative positive, un sujet très classique en théorie analytique des nombres.

**Lemme 3.** *Nous avons*

$$\sum_{q \in \mathcal{Q}} 1/\phi(q) \geq \text{Log } Q.$$

## 6 Preuve de l'inégalité de Brun-Titchmarsh

Nous prenons pour  $\varphi_q$  la fonction suivante :

$$\varphi_q(n) = \begin{cases} c_q(n) & \text{si } M+1 \leq n \leq M+N \\ 0 & \text{sinon,} \end{cases} \quad (5)$$

pour  $q$  variant dans  $\mathcal{Q}$ .

Notre Hilbert est simplement l'ensemble des fonctions sur les entiers de  $[M+1, M+N]$  muni du produit hermitien standard :

$$[g|h] = \sum_{M+1 \leq n \leq M+N} f(n) \overline{g(n)}. \quad (6)$$

Le dernier lemmes dont nous aurons besoin mesure la quasi-orthogonalité de la famille  $(\varphi_q)_{q \in \mathcal{Q}}$ .

**Lemme 4.**

$$\sum_{q' \in \mathcal{Q}} |[\varphi_q | \varphi_{q'}]| \leq M_q = \phi(q)(N + Q^4).$$

Nous prenons tout simplement pour  $f$  la fonction caractéristique des nombres premiers de l'intervalle  $[M + 1, M + N]$  et nous supposons que  $Q$ , qui intervient dans la définition de  $\mathcal{Q}$  est  $\leq M$ . Dans ce cas, nous obtenons directement *Appliquons l'inégalité hermitienne*

$$[f | \varphi_q] = \sum_{M+1 \leq n \leq M+N} f(n) \overline{\varphi_q(n)} = (-1)^{\omega(q)} \sum_{M+1 \leq n \leq M+N} f(n) \quad (7)$$

tout simplement parce que  $\varphi_q(n) = (-1)^{\omega(q)}$  pour tous les nombres premiers de notre intervalle. En rappelant que  $Z$  désigne le nombre de ces nombres premiers, nous pouvons réécrire l'équation ci-dessus sous la forme

$$[f | \varphi_q] = (-1)^{\omega(q)} Z. \quad (8)$$

Notre lemme nous donne alors

$$\sum_{q \in \mathcal{Q}} |(-1)^{\omega(q)} Z|^2 / \phi(q) \leq Z(N + Q^4),$$

soit encore

$$Z \sum_{q \in \mathcal{Q}} 1/\phi(q) \leq N + Q^4. \quad (9)$$

Le lemme 3 nous permet alors d'atteindre la majoration  $Z \leq (N + Q^4) / \text{Log } Q$  où il nous faut à présent optimiser  $Q$ . Nous prenons

$$Q = N^{1/4} / \text{Log } N \quad (10)$$

ce qui nous donne le résultat annoncé.

## 7 Compléments

Tout d'abord, en remarquant que dans l'ensemble  $\{a/q, \text{pgcd}(a, q) = 1, q \leq Q\}$ , deux points sont distants d'au moins  $1/Q^2$ , il est assez facile de montrer qu'en fait, nous avons

$$\sum_{q' \in \mathcal{Q}} |[\varphi_q | \varphi_{q'}]| = \phi(q)N + \mathcal{O}(\phi(q)Q^2 \text{Log } Q) \quad (11)$$

ce qui nous donnerait  $Z \leq (2 + o(1))N/\text{Log } N$ .

Il nous faut ensuite éliminer la condition  $Q \leq M$  : pour cela, il suffit de prendre pour  $f$  la fonction caractéristique des nombres premiers de notre intervalle, mais qui sont aussi  $> Q$ . Du coup,  $\sum_n f(n)$  ne vaut plus  $Z$ , mais  $Z + \mathcal{O}(Q)$ , ce qui nous suffit largement.

Cette preuve est récente : je l'ai mise au point l'été dernier ! En fait, cela m'a permis de montrer la majoration

$$Z \leq 2N/(\text{Log } N + 2.88 + o(1)). \quad (12)$$

Qui n'est d'ailleurs pas encore publiée. Qu'une telle inégalité soit possible, mais avec une constante non spécifiée est dû à (van Lint & Richert, 1965) bien que (Selberg, 1949) mentionne un tel résultat sans démonstration. (Bombieri, 1971) obtenait le première valeur avec la majoration  $Z \leq 2N/(\text{Log } N - 3 + o(1))$ . (Montgomery & Vaughan, 1973) ont ensuite affiné ce  $-3$  en  $5/6$  et dans la section 22 de (Selberg, 1991) se trouve une preuve donnant  $c = 2.81$ , preuve à laquelle nous empruntons certains éléments.

## 8 Optimalité ?

Si nous savons que les méthodes de preuves dont nous disposons à l'heure actuelle ne sauraient améliorer notablement le théorème de Brun-Titchmarsh, si ce n'est sous la forme de petites améliorations comme dans (12), il n'est absolument pas clair que ce théorème ne soit pas optimal en soi. Il serait très intéressant de déterminer un intervalle  $[M + 1, M + N]$  où le nombre de nombres premiers divisé par  $N/\text{Log } N$  soit  $> 1$  et où  $M \geq 2N$ . Et en fait le plus grand possible et même proche de 2 ... À l'heure actuelle, je ne connais que des exemples :

$M + 1$	$M + N$	$N$	$Z$	rapport
5 639	5 659	21	7	1.0148 ...
113 143	113 177	35	10	1.0158 ...
21 817 283 854 511 261	21 817 283 854 511 311	51	14	1.0793 ...

Ce dernier exemple date de 1982.

Ceci est à rapprocher de la conjecture de Hardy & Littlewood de 1923 qui affirme que  $\pi(M + 1) - \pi(M + N) \leq \pi(N - 1)$ . Voir à ce sujet (Dusart, 1998), (Hensley & Richards, 1974), (Schinzel & Sierpiński, 1958) et (Schinzel, 1961).

Pour déterminer des exemples permettant de s'approcher plus près de la borne donnée par le théorème de Brun-Titchmarsh, il convient peut être de se tourner vers sa formulation la plus générale :

**Théorème de Brun-Titchmarsh.** Soit  $q \geq 1$  un entier et  $a$  un entier premier à  $q$ . Pour  $M$  et  $N$  deux entiers  $\geq 1$ , le nombre  $Z$  de nombres premiers congrus à  $a$  modulo  $q$  et dans l'intervalle  $[M + 1, M + N]$  est au plus

$$\frac{2N}{\phi(q) \operatorname{Log}(N/q)}.$$

Je ne crois pas qu'une telle approche ait été tentée, par exemple avec des nombres premiers = 2[3].

## 9 Annexe

### 9.1 Preuve du lemme 1

La preuve du lemme 1 est très simple. Considérons l'inégalité

$$\left\| f - \sum_{q \in \mathcal{Q}} \xi_q \varphi_q \right\|^2 \geq 0$$

où les  $\xi_q$  sont des paramètres que nous souhaitons choisir au mieux, c'est à dire de façon à rendre cette norme aussi petite que possible. Le mieux serait bien sûr de prendre pour  $\sum_{q \in \mathcal{Q}} \xi_q \varphi_q$  la projection orthogonale de  $f$  sur l'espace engendré par les  $\varphi_q$ , mais nous ne savons pas calculer de tels coefficients  $\xi_q$  en général. Nous nous contenterons de ce que nous espérons être une approximation, mais que nous savons exprimer. Le développement de la norme nous donne

$$\|f\|^2 - 2\Re \sum_{q \in \mathcal{Q}} \overline{\xi_q} [f | \varphi_q] + \sum_{q, q' \in \mathcal{Q}} \xi_q \overline{\xi_{q'}} [\varphi_q | \varphi_{q'}] \geq 0,$$

où nous séparons  $q$  et  $q'$  à l'aide de  $|\xi_q| |\xi_{q'}| \leq \frac{1}{2} (|\xi_q|^2 + |\xi_{q'}|^2)$ . Nous réorganisons nos termes et injectons  $M_q$  dans l'inéquation résultante. Il vient

$$\|f\|^2 - 2\Re \sum_{q \in \mathcal{Q}} \overline{\xi_q} [f | \varphi_q] + \sum_{q \in \mathcal{Q}} |\xi_q|^2 M_q \geq 0. \quad (13)$$

Maintenant que la forme quadratique en  $\xi_q$  est remplacée par une forme diagonale, il est facile de déterminer les  $\xi_q$  qui minimisent (13) :

$$\xi_q = [f | \varphi_q] / M_q.$$

En injectant ces valeurs dans (13), nous obtenons bien l'inégalité annoncée.



## 9.2 Preuve du lemme 3

Commençons par remarquer que, si  $q = p$  est un nombre premier, alors

$$\frac{1}{\phi(p)} = \frac{1}{p-1} = \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \dots$$

Une fois cela acquis, regardons ce qui se passe si  $q = p_1 p_2$  un produit de deux nombres premiers distincts :

$$\begin{aligned} \frac{1}{\phi(p_1 p_2)} &= \frac{1}{(p_1 - 1)(p_2 - 1)} \\ &= \left( \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \dots \right) \left( \frac{1}{p_2} + \frac{1}{p_2^2} + \frac{1}{p_2^3} + \dots \right) \\ &= \sum_n \frac{1}{n} \end{aligned}$$

où la somme porte sur tous les entiers dont les facteurs premiers sont exactement  $p_1$  et  $p_2$ . En poursuivant ce raisonnement, nous constatons que notre somme initiale est celle des  $1/n$  où  $n$  est un entier dont le produit de tous les facteurs premiers est  $\leq Q$ . Ensemble qui contient au moins tous les entiers  $\leq Q$ , soit la minoration

$$\sum_{q \in Q} 1/\phi(q) \geq \sum_{1 \leq n \leq Q} 1/n \geq \text{Log } Q.$$

Ce qu'il fallait démontrer.

## 9.3 Preuve du lemme 4

Ce lemme va être une conséquence facile du suivant.

**Lemme 5.** *Nous avons  $|\varphi_q | \varphi_q - \phi(q)N| \leq \phi(q)q^3$ . De plus, si  $q' \neq q$ , nous avons aussi*

$$|\varphi_q | \varphi_{q'}| \leq \phi(q)qq'^2.$$

PREUVE : Il vaut mieux raccourcir un peu les notations et écrire  $e(\alpha) = \exp(2i\pi\alpha)$ . Nous obtenons alors, que  $q'$  soit premier à  $q$  ou non,

$$|\varphi_q | \varphi_{q'}| = \sum_{M+1 \leq n \leq M+N} \left( \sum_{\substack{1 \leq a \leq q, \\ \text{pgcd}(a,q)=1}} e(na/q) \right) \left( \sum_{\substack{1 \leq a' \leq q', \\ \text{pgcd}(a',q')=1}} e(-na'/q') \right).$$

En mettant les sommations sur  $a$  et  $a'$  devant, cela donne

$$[\varphi_q | \varphi_{q'}] = \sum_{\substack{1 \leq a \leq q, \\ \text{pgcd}(a,q)=1}} \sum_{\substack{1 \leq a' \leq q', \\ \text{pgcd}(a',q')=1}} \sum_{M+1 \leq n \leq M+N} e\left(n\left(\frac{a}{q} - \frac{a'}{q'}\right)\right).$$

La somme interne est en fait la somme d'une progression arithmétique. Si  $a/q \neq a'/q'$ , elle vaut au plus en module

$$1/|\sin\left(\pi\left(\frac{a}{q} - \frac{a'}{q'}\right)\right)| \leq qq'/2$$

en utilisant l'inégalité classique  $\sin x \geq 2x/\pi$  si  $0 \leq x \leq \pi/2$ . ◇◇◇

Tout cela résulte en le lemme 4.

## Références

- Bombieri, E. 1971. A note on the large sieve method. *Acta Arith.*, **18**, 401–404.
- Dusart, P. 1998. *Autour de la fonction qui compte le nombre de nombres premiers*. Ph.D. thesis, Limoges, [http://www.unilim.fr/laco/theses/1998/T1998\\_01.pdf](http://www.unilim.fr/laco/theses/1998/T1998_01.pdf). 173 pp.
- Hensley, D., & Richards, I. 1974. Primes in intervals. *Acta Arith.*, **4**(25), 375–391.
- Montgomery, H.L., & Vaughan, R.C. 1973. The large sieve. *Mathematika*, **20**(2), 119–133.
- Schinzel, A. 1961. Remarks on the paper : Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, **7**(1), 1–8.
- Schinzel, A., & Sierpiński, W. 1958. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.*, **4**(3), 185–208.
- Selberg, A. 1949. On elementary problems in prime number-theory and their limitations. *C.R. Onzième Congrès Math. Scandinaves, Trondheim, Johan Grundt Tanums Forlag*, 13–22.
- Selberg, A. 1991. Collected papers. *Springer-Verlag*, **II**, 251pp.
- van Lint, J.E., & Richert, H.E. 1965. On primes in arithmetic progressions. *Acta Arith.*, **11**, 209–216.