# UN COURS DE THÉORIE ANALYTIQUE DES NOMBRES

**Emmanuel Kowalski**

**Diffusion**

Maison de la SMF
B.P. 67
13274 Marseille Cedex 9
France
smf@smf.univ-mrs.fr

AMS
P.O. Box 6248
Providence RI 02940
USA
www.ams.org

EDP Sciences
17, avenue du Hoggar
91944 les Ulis cedex A
France
www.edpsciences.com

**Tarifs 2004**

*Vente au numéro :* 41 € ($ 59)
Des conditions spéciales sont accordées aux membres de la SMF.

**Secrétariat : Nathalie Christiaën**

Cours Spécialisés
Société Mathématique de France
Institut Henri Poincaré, 11, rue Pierre et Marie Curie
75231 Paris Cedex 05, France
Tél : (33) 01 44 27 67 99 • Fax : (33) 01 40 46 90 96
revues@smf.ens.fr • http://smf.emath.fr/



ISSN 1284-6090
ISBN 2-85629-161-9

Directeur de la publication : Marie-Françoise ROY

COURS SPÉCIALISÉS 13

# UN COURS DE THÉORIE ANALYTIQUE DES NOMBRES

Emmanuel Kowalski

Société Mathématique de France 2004

# TABLE DES MATIÈRES

# PRÉFACE

Ces notes ont été rédigées pour un cours de DEA donné à l'Université Bordeaux I au second semestre 2001/2002. L'idée était de présenter de manière motivée certaines des méthodes les plus modernes de théorie analytique des nombres par le biais d'un théorème très récent de Duke, Friedlander et Iwaniec. Pour que celui-ci soit présenté dans un contexte compréhensible, il a fallu tout naturellement développer les résultats fondamentaux concernant la distribution des nombres premiers, de sorte que le texte final peut aussi être considéré comme une introduction à toute la partie « multiplicative » de la théorie analytique des nombres. Il n'existe pas beaucoup de textes ayant cet objectif, ce qui peut rendre utiles ces notes au lecteur débutant ou non spécialiste.

Les choix de présentation ont été faits dans cette optique. En particulier, on remarquera l'insistance, parfois maniaque, sur les « sommes lisses » : si cela ne se justifie pas toujours pour ce qui est du contenu présent, il n'en est pas moins vrai que même des articles de recherche contiennent encore des énoncés plus faibles, ou des démonstrations plus complexes, que ce qu'ils (elles) pourraient être si leurs auteurs avaient songé à lisser ces sommes...

Il n'y a pas vraiment de résultats originaux dans ce cours, parfois simplement une présentation un peu différente de ce qu'on peut trouver habituellement. Cependant, dans la plupart des cas, je n'ai fait que reprendre et adapter certaines des notes de cours non publiées de H. Iwaniec.

Je dédie d'ailleurs à H. Iwaniec tout ce qu'il peut se trouver dans ce cours qui recevra son approbation, avec la plus grande admiration...

**Prérequis et notations**

Les prérequis formels sont assez minces : il faut essentiellement connaître les bases de la théorie de l'intégration, en particulier les propriétés de base de la transformée de Fourier sur $\mathbf{R}^n$ (bien que seules des fonctions très régulières soient utilisées), et

les bases de la théorie des fonctions holomorphes (formule des résidus[1], principe du maximum essentiellement). Plus que cela, c'est d'une certaine habitude et agilité dans le maniement des inégalités qu'il faut disposer : habitude qui devrait se renforcer à la lecture du cours, d'ailleurs, si celle-ci est attentive...

Les notations sont standard, à une exception près : en plus des symboles de Landau $f = O(g)$, $f = o(g)$ et $f \sim g$, on utilise souvent en théorie analytique des nombres le symbole de Vinogradov $f \ll g$ (et son opposé $f \gg g$), dont l'interprétation est subtilement différente.

Pour clarifier cela, nous reprenons la définition (celle de Bourbaki, par exemple) de $f = O(g)$, qui est de nature topologique. Ainsi, étant donné un espace topologique $X$, un point $x_0 \in X$, des fonctions $f$ et $g$ définies sur un voisinage de $x_0$ (pas forcément en $x_0$ même), on dit que $f = O(g)$ *quand* $x \to x_0$, s'il existe un voisinage $V$ de $x_0$ et une constante $C \geqslant 0$, dépendant *a priori* de $V$ et de $x_0$, telle que

$$|f(x)| \leqslant Cg(x) \quad \text{pour } x \in V.$$

Par contre, si $X$ est un ensemble quelconque, $f$ et $g$ des fonctions sur $X$, on dit que $f \ll g$ pour $x \in Y \subset X$ s'il existe $C$ telle que

$$|f(x)| \leqslant Cg(x) \quad \text{pour tout } x \in Y.$$

La différence est que, dans ce second cas, l'ensemble $Y$ doit être exactement spécifié (bien que souvent il soit clair dans le contexte), alors que le voisinage $V$ de $f = O(g)$ peut être remplacé par tout autre voisinage $W \subset V$ de $x_0$. Dans l'écriture $f \ll g$ sur $Y$, une constante $C$ convenable est appelée « constante implicite » dans le symbole $\ll$ (souvent, elle dépendra d'autres paramètres, qui seront explicitement mentionnés ou indiqués en indice $\ll_\varepsilon$, *etc.*)

Un exemple suffit à expliquer cela : on a

$$\frac{1}{x} = O\Big(\frac{1}{x+1}\Big) \quad \text{quand } x \to +\infty.$$

mais certainement pas

$$\frac{1}{x} \ll \frac{1}{x+1} \quad \text{pour } x > 0.$$

Les lecteurs sont prévenus qu'une grande partie de la littérature en théorie analytique des nombres utilise $f = O(g)$ comme synonyme de $f \ll g$, et parle donc de constante implicite. Mais c'est aussi une source de nombreuses erreurs et malentendus...

Il est pratique d'introduire un nouveau symbole $f = \underline{O}(g)$ (appelé « grand O uniforme ») tel que $f = \underline{O}(g)$ soit exactement synonyme de $f \ll g$.

[1] En pratique, seulement pour un rectangle !

Finalement, le symbole $\approx$ n'a pas de signification mathématique précise. Il est utilisé dans les raisonnements heuristiques, et $f \approx g$ indique que $f$ est, ou devrait être, proche de $g$, en un sens qui peut dépendre du contexte.

Rappelons que la notation $p^k \,||\, n$ pour $p$ premier et $k \geqslant 0$ signifie que $p^k$ divise $n$ mais $p^{k+1}$ ne divise pas $n$.

On écrit aussi $n \mid m^\infty$ pour dire que tous les facteurs premiers de $n$ sont des facteurs premiers de $m$.

Si $m \geqslant 1$ et $x \in (\mathbf{Z}/m\mathbf{Z})^\times$, on note $\overline{x}$ l'inverse de $x$ modulo $m$, c'est-à-dire que $x\overline{x} \equiv 1 \pmod{m}$. Le module $m$ est toujours clair dans le contexte.

Sauf mention explicite du contraire $p$ désigne toujours un nombre premier et $n$ un entier $\geqslant 0$.

Enfin, si $G$ est un groupe quelconque agissant *à gauche* sur un ensemble $X$, de sorte que $g \cdot (h \cdot x) = (gh) \cdot x$, on note

$$G\backslash X$$

le quotient de $X$ par $G$, c'est-à-dire l'ensemble des orbites $Gx$, $x \in X$ ; si par contre $G$ agit *à droite*, avec $(x \cdot g) \cdot h = x \cdot (gh)$, on note

$$X/G$$

l'ensemble des orbites $xG$. Et si $G_1$ agit à gauche et $G_2$ à droite, le double quotient

$$G_1\backslash X/G_2$$

est l'ensemble des double classes $G_1xG_2$, $x \in X$.