



Représentation des entiers par des familles de formes binaires.

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris

<http://www.imj-prg.fr/~michel.waldschmidt/>

Résumé

L'estimation asymptotique du nombre d'entiers qui sont sommes de deux carrés fait intervenir la constante de [Landau–Ramanujan](#). Ce résultat a été étendu par [Paul Bernays](#) en 1912 aux formes binaires quadratiques de discriminant non carré à la place de $X^2 + Y^2$. De nombreux travaux ont été consacrés à l'étude asymptotique du nombre d'entiers représentés par une forme binaire de degré au moins 3, jusque quand [Cam Stewart](#) et [Stanley Yao Xiao](#) ont complètement résolu la question dans un article publié en 2019. Dans cet exposé nous nous intéressons à des familles de formes binaires. Le premier exemple que nous avons étudié dans un article avec [Claude Levesque](#) et [Etienne Fouvry](#) est celui de la famille des formes cyclotomiques. Ensuite, dans une série d'articles avec [Étienne Fouvry](#), nous avons considéré des familles plus générales de formes binaires. Nos résultats récents reposent sur des minoration de formes linéaires de logarithmes et sur l'étude des homographies entre deux formes binaires.

Formes binaires

Une *forme binaire* est un polynôme homogène à coefficients entiers en deux variables :

$$F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d \in \mathbb{Z}[X, Y].$$

Nous nous intéressons à la représentation des entiers par de telles formes :

- Quelles sont les valeurs prises par F quand les variables X, Y sont remplacés par des entiers rationnels ?
- Étant donné m , quelles sont les solutions de l'équation $F(x, y) = m$? S'il en existe, on dit que m est *représenté par* F .
- Y a-t-il un nombre fini ou infini de (x, y) ?
- Si, pour tout m , il n'y en a qu'un nombre fini, combien y a-t-il de m dans un intervalle $[-N, N]$ pour lesquels une telle solution existe ?

Formes binaires de degré 1 ou 2

Une forme binaire de degré 1 est une forme linéaire $a_0X + a_1Y$. L'ensemble des entiers représentés par une telle forme est l'ensemble des multiples du pgcd de a_0, a_1 (algorithme d'Euclide).

Une *forme quadratique* est une forme binaire de degré 2 :

$$a_0X^2 + a_1XY + a_2Y^2.$$

Des exemples de formes quadratiques sont les produits de deux formes binaires linéaires, en particulier les carrés des formes binaires linéaires (celles dont le discriminant est un carré), ainsi que les formes $X^2 - dY^2$ (équation de Pell–Fermat).

Formes binaires cyclotomiques

On définit une suite Φ_n ($n \geq 1$) de formes binaires par la relation

$$X^n - Y^n = \prod_{d|n} \Phi_d(X, Y).$$

$$\Phi_1(X, Y) = X - Y, \quad \Phi_2(X, Y) = X + Y,$$

et pour p premier

$$\Phi_p(X, Y) = X^{p-1} + X^{p-2}Y + \dots + XY^{p-2} + Y^{p-1}.$$

Pour $n \geq 1$, $\Phi_n(X, Y)$ est la version homogène du polynôme cyclotomique ϕ_n d'indice n :

$$\Phi_n(X, 1) = \phi_n(X) := \prod_{\substack{1 \leq k \leq n \\ (k, n) = 1}} (X - \zeta_n^k)$$

quand ζ_n est une racine primitive de l'unité d'ordre n .

Formes binaires cyclotomiques quadratiques

Le degré de la forme binaire $\Phi_n(X, Y)$ est donné par l'indicatrice d'Euler

$$\varphi(n) = \#\{k \mid 1 \leq k \leq n, (k, n) = 1\}.$$

$$\Phi_n(X, Y) = Y^{\varphi(n)} \phi_n(X/Y) = \prod_{\substack{1 \leq k \leq n \\ (k, n) = 1}} (X - \zeta_n^k Y)$$

Les deux formes cyclotomiques linéaires sont Φ_1 et Φ_2 , les trois formes cyclotomiques quadratiques sont Φ_3 , Φ_4 et Φ_6 :

$$\Phi_3(X, Y) = X^2 + XY + Y^2,$$

$$\Phi_4(X, Y) = X^2 + Y^2,$$

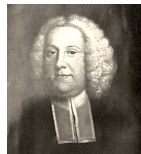
$$\Phi_6(X, Y) = X^2 - XY + Y^2 = \Phi_3(X, -Y).$$

Équation dite de Pell $x^2 - dy^2 = \pm 1$

Brahmagupta (598 – 670) $d = 92$.

Bhāskara II = Bhāskarāchārya (1114 - 1185) $d = 61$.

Narayaṇa Paṇḍit ($\sim 1340 - \sim 1400$) $d = 103$.



John Pell
1610 – 1685



Lord William Brouncker
1620–1684



Pierre de Fermat
1601–1665

Correspondence entre Pierre de Fermat et Lord Brouncker.
1657 : lettre de Fermat à Frenicle de Bessy (1604–1674).

<https://mathshistory.st-andrews.ac.uk/Biographies/>

Représentation des entiers par des formes binaires



Pierre de Fermat
1601 - 1665



Joseph-Louis Lagrange
1736 - 1813



Adrien-Marie Legendre
1752 - 1833



Carl Friedrich Gauss
1777 - 1855

<https://mathshistory.st-andrews.ac.uk/Biographies/>

Peter Duren. Changing Faces: The Mistaken Portrait of Legendre.

www.ams.org/notices/200911/rtx091101440p.pdf

La constante de Landau–Ramanujan



Edmund Landau

1877 – 1938



Srinivasa Ramanujan

1887 – 1920

Le nombre d'entiers positifs $\leq N$ qui sont sommes de deux carrés est asymptotiquement $C_{\Phi_4} N(\log N)^{-\frac{1}{2}}$, où

$$C_{\Phi_4} = \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

Online Encyclopedia of Integer Sequences

[[OEIS A001481](#)] Numbers that are the sum of 2 squares.

0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, ...

[[OEIS A064533](#)] Decimal expansion of Landau-Ramanujan constant.

$$C_{\Phi_4} = 0.764\,223\,653\,589\,220\dots$$

- [Philippe Flajolet](#) and [Ivan Vardi](#), Zeta function expansions of some classical constants, Feb 18 1996.
- [Xavier Gourdon](#) and [Pascal Sebah](#), Constants and records of computation.
- [David E. G. Hare](#), [125 079](#) digits of the [Landau–Ramanujan](#) constant.

La constante de Landau–Ramanujan

Références : <https://oeis.org/A064533>

- B. C. Berndt, *Ramanujan's notebook part IV*, Springer-Verlag, 1994
- S. R. Finch, *Mathematical Constants*, Cambridge, 2003, pp. 98-104.
- G. H. Hardy, "Ramanujan, Twelve lectures on subjects suggested by his life and work", Chelsea, 1940.
- Institute of Physics, Constants - Landau-Ramanujan Constant
- Simon Plouffe, Landau Ramanujan constant
- Eric Weisstein's World of Mathematics, Ramanujan constant
- https://en.wikipedia.org/wiki/Landau-Ramanujan_constant

Sommes de deux carrés

Quand a et q sont deux entiers positifs, on désigne par $N_{a,q}$ tout entier ≥ 1 qui vérifie

$$p \mid N_{a,q} \implies p \equiv a \pmod{q}.$$

Un entier $m \geq 1$ peut être écrit

$$m = \Phi_4(x, y) = x^2 + y^2$$

si et seulement s'il existe des entiers $a \geq 0$, $N_{3,4}$ et $N_{1,4}$ satisfaisant

$$m = 2^a N_{3,4}^2 N_{1,4}.$$

Formes quadratiques de discriminant non carré

Soit $F \in \mathbb{Z}[X, Y]$ une forme quadratique dont le discriminant n'est pas un carré. Il existe une constante positive C_F telle que, pour $N \rightarrow \infty$, le nombre d'entiers positifs $m \in \mathbb{Z}$, $m \leq N$ qui sont représentés par F est asymptotiquement $C_F N (\log N)^{-\frac{1}{2}}$.



Paul Bernays
1888 – 1977

P. BERNAYS, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven, binären quadratischen Formen einer nicht quadratischen Diskriminante,*

Ph.D. dissertation, Georg-August-Universität, Göttingen, Germany, 1912.

http://www.ethlife.ethz.ch/archive_articles/120907_bernays_fm/

Paul Bernays (1888 – 1977)

<https://www.thefamouspeople.com/profiles/paul-bernays-7244.php>

- 1912, Ph.D. en mathématiques, Université de Göttingen, *On the analytic number theory of binary quadratic forms* (Directeur de thèse : [E. Landau](#)).
- 1913, Habilitation, Université de Zürich, *On complex analysis and [Picard's theorem](#)*, advisor [E. Zermelo](#).
- 1912 – 1917, Zürich ; travaille avec [Georg Pólya](#), [Albert Einstein](#), [Hermann Weyl](#).
- 1917 – 1933, Göttingen, avec [David Hilbert](#). Étudie avec [Emmy Noether](#), [van der Waerden](#), [G. Herglotz](#),
- 1935 – 1936, Institute for Advanced Study, Princeton. exposés sur la logique mathématique et la théorie axiomatique des ensembles.
- 1936 —, ETH Zürich.
- Avec Hilbert, “Grundlagen der Mathematik” (1934 – 39) 2 vol. — Paradoxe de [Hilbert–Bernays](#).
- Axiomatic Set Theory (1958). — [Von Neumann–Bernays–Gödel set theory](#).

Généralisations

- Sommes de cubes, de bicarrés,...

Remarquer que $X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2)$

La forme binaire $\Phi_3(X, Y) = X^2 + XY + Y^2$ est la version homogène du polynôme cyclotomique $\phi_3(t) = t^2 + t + 1$.

On a

$$\Phi_6(X, Y) = \Phi_3(X, -Y) = X^2 - XY + Y^2$$

et

$$\Phi_8(X, Y) = X^4 + Y^4.$$

La forme quadratique $X^2 + XY + Y^2$

Un nombre premier est représenté par la forme quadratique $X^2 + XY + Y^2$ si et seulement si, ou bien il est égal à 3, ou bien il est congruent à 1 modulo 3.

Produit de deux nombres représentés par la forme quadratique $X^2 + XY + Y^2$:

$$(a^2 + ab + b^2)(c^2 + cd + d^2) = e^2 + ef + f^2$$

avec

$$e = ac - bd, \quad f = ad + bd + bc.$$

Le corps $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, $1 + \zeta_3 + \zeta_3^2 = 0$ est un corps quadratique cyclotomique ;

$$a^2 + ab + b^2 = \text{Norm}_{\mathbb{Q}(\zeta_3)/\mathbb{Q}}(a - \zeta_3 b).$$

Loeschian numbers : $m = x^2 + xy + y^2$

Un entier $m \geq 1$ peut être écrit

$$m = \Phi_3(x, y) = \Phi_6(x, -y) = x^2 + xy + y^2$$

si et seulement s'il existe des entiers $b \geq 0$, $N_{2,3}$ et $N_{1,3}$ tels que

$$m = 3^b N_{2,3}^2 N_{1,3}.$$

[[OEIS A003136](#)] Loeschian numbers: numbers of the form $x^2 + xy + y^2$; norms of vectors in A_2 lattice.

0, 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, 25, 27, 28, 31, 36, 37, ...

Formes cyclotomiques

Dans un travail en commun avec E. Fouvry et C. Levesque nous avons étudié le nombre d'entiers représentés par une des formes cyclotomiques de degré ≥ 2 .



Étienne Fouvry



Claude Levesque

EF+CL+MW,

Representation of integers by cyclotomic binary forms.

Acta Arithmetica, **184.1** (2018), 67 – 86.

DOI: 10.4064/aa171012-24-12

arXiv: 712.09019 [math.NT]



FACULTÉ DES SCIENCES DHAR EL MAHRAZ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH

International Conference in Algebra, Number Theory and Their Applications

October 27-28, 2022, Fez

(In Honor of Professors István Gaál and Claude Levesque)



FACULTÉ DES SCIENCES DHAR EL MAHRAZ
UNIVERSITÉ SIDI MOHAMED BEN ABDELLAH

Thursday, October 27, 2022

8:30—9:00	Registration
9:00—9:20	Opening ceremony
	Chair: B. Ralph
9:20—10:10	M. Waldschmidt, Présentation de quelques résultats obtenus avec Claude Levesque dans 12 travaux en commun.

Avec E. Fouvry et C. Levesque

Le nombre d'entiers $\leq N$ qui sont sommes de deux carrés est asymptotiquement

$$\frac{N}{(\log N)^{1/2}} \left(C_{\Phi_4} + \frac{\alpha_1}{\log N} + \cdots + \frac{\alpha_M}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right).$$

Le nombre d'entiers $\leq N$ représentés par la forme quadratique $X^2 + XY + Y^2$ est asymptotiquement

$$\frac{N}{(\log N)^{1/2}} \left(C_{\Phi_3} + \frac{\alpha'_1}{\log N} + \cdots + \frac{\alpha'_M}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right)$$

où

$$C_{\Phi_3} = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \pmod{3}} \left(1 - \frac{1}{p^2} \right)^{-\frac{1}{2}}.$$

Intersection

Un entier $m \geq 1$ est simultanément de la forme

$m = \Phi_4(x, y) = x^2 + y^2$ et de la forme $m = \Phi_3(u, v) = u^2 + uv + v^2$

si et seulement s'il existe des entiers $a, b \geq 0$, $N_{5,12}$, $N_{7,12}$, $N_{11,12}$ et $N_{1,12}$ tels que

$$m = \left(2^a 3^b N_{5,12} N_{7,12} N_{11,12} \right)^2 N_{1,12}.$$

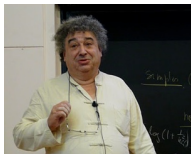
Le nombre d'entiers $\leq N$ qui sont représentés par la forme quadratique $X^2 + XY + Y^2$ et qui sont aussi sommes de deux carrés est asymptotiquement

$$\frac{N}{(\log N)^{3/4}} \left(\beta_0 + \frac{\beta_1}{\log N} + \cdots + \frac{\beta_M}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right)$$

où

$$\beta_0 = \frac{3^{\frac{1}{4}}}{2^{\frac{5}{4}}} \cdot \pi^{\frac{1}{2}} \cdot (\log(2 + \sqrt{3}))^{\frac{1}{4}} \cdot \frac{1}{\Gamma(1/4)} \cdot \prod_{p \equiv 5, 7, 11 \pmod{12}} \left(1 - \frac{1}{p^2} \right)^{-\frac{1}{2}}.$$

Développement de fonctions Zeta de constantes classiques,



Philippe Flajolet
1948–2011



Ilan Vardi



Bill Allombert



Olivier Ramare

S. Ettahri, O. Ramare, L.Surel. *Fast multi-precision computation of some Euler products.*
<https://arxiv.org/abs/1908.06808v1>

Online Encyclopedia of Integer Sequences

[[OEIS A301429](#)] Decimal expansion of an analog of the [Landau--Ramanujan](#) constant for Loeschian numbers.

$$C_{\Phi_3} = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \pmod{3}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} = 0.638\,909\,405\,445\,343\,88\dots$$

[[OEIS A301430](#)] Decimal expansion of an analog of the [Landau--Ramanujan](#) constant for Loeschian numbers which are sums of two squares.

$$\begin{aligned} \beta_0 &= \frac{3^{\frac{1}{4}}}{2^{\frac{5}{4}}} \cdot \pi^{\frac{1}{2}} \cdot (\log(2 + \sqrt{3}))^{\frac{1}{4}} \cdot \frac{1}{\Gamma(1/4)} \cdot \prod_{p \equiv 5, 7, 11 \pmod{12}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \\ &= 0.302\,316\,142\,357\,065\,637\,94\dots \end{aligned}$$

Formes cyclotomiques de degré > 2

Lemme (EF-CL-MW). Soit $d > 2$. Il existe une constante effectivement calculable $C(d)$ telle que le nombre de triplets (n, x, y) dans $\mathbb{Z}_{>0} \times \mathbb{Z}^2$ qui satisfont $\varphi(n) \geq d$, $\max\{|x|, |y|\} \geq 2$ et $\Phi_n(x, y) < N$ est majoré par $C(d)N^{2/d}$.

Conséquence : le nombre d'entiers $\leq N$ représentés par une des formes cyclotomiques Φ_n de degré ≥ 2 est asymptotiquement le nombre d'entiers $\leq N$ représentés par une des formes cyclotomiques Φ_3, Φ_4 : les formes cyclotomiques de degré ≥ 4 ne contribuent qu'au terme reste.

Remarque : on impose $\max\{|x|, |y|\} \geq 2$ car $\Phi_p(1, 1) = p$ pour tout p premier.

Formes cyclotomiques de degré supérieur

Il est naturel de se poser la question du nombre d'entiers représentés par une des formes cyclotomiques de degré $\geq d$, quand d est donné > 2 .

Théorème (avec EF). Soit $d \geq 4$. On suppose qu'il existe un entier n tel que $\varphi(n) = d$. Alors le nombre d'entiers $\leq N$ représentés par une des formes cyclotomiques Φ_n de degré $\geq d$ est asymptotiquement le nombre d'entiers $\leq N$ représentés par une des formes cyclotomiques de degré d : les formes cyclotomiques de degré $> d$ ne contribuent qu'au terme reste.

On donne aussi une estimation asymptotique du nombre d'entiers $\leq N$ représentés par une des formes cyclotomiques Φ_n de degré d .



Représentation des entiers par des familles de formes binaires.

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris
<http://www.imj-prg.fr/~michel.waldschmidt/>