April 2025

Representation of integers by families of binary forms

Michel Waldschmidt

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

Abstract

The estimate for the asymptotic number of integers which are sums of two squares involves the Landau–Ramanujan constant. This result has been generalized by Paul Bernays in 1912 to quadratic forms with non square discriminant in place of $X^2 + Y^2$. A number of papers have been published, dealing with the asymptotic study of the number of integers which are represented by a binary form of degree at least 3, until Cam Stewart and Stanley Yao Xiao completely solved the problem in a paper published in 2019.
In this lecture we consider families of binary forms. The first example we studied in a joint paper with Claude Levesque and Etienne Fouvry is the family of cyclotomic forms. Next, in a series of papers with Étienne Fouvry, we considered more general families of binary forms. The proofs of our recent results rest on lower bounds for linear forms in logarithms and on the study of fractional linear transformations relating two binary forms.

Binary forms

A *binary form* is a homogeneous polynomial with integer coefficients in two variables:

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

We are interested in the representation of integers by such forms:

• Which are the values taken by F when the variables X,Y are replaced by rational integers?

• Given an integer m, are there solutions of the equation $F(x,y)=m$? If they exists, we say that m is *represented by* F.

• Are there finitely of infinitely many such (x,y)?

• If, for all m, there are only finitely many (x,y), how many m in an interval $[-N,N]$ are there for which such a solution exists?

Binary forms of degree 1 or 2

A binary form of degree 1 is nothing else than a linear form $a_0X + a_1Y$. The set of integers represented by this form is the set of multiples of the gcd of a_0, a_1 (Euclid algorithm).

A *quadratic form* is a binary form of degree 2:

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

Examples of quadratic forms are products of two linear forms, including the squares of binary linear forms (they are the quadratic binary form having a square discriminant), as well as the binomial binary quadratic forms $X^2 - dY^2$ (Pell–Fermat).

Cyclotomic binary forms

One defines a sequence Φ_n $(n \geqslant 1)$ of binary forms by the relation

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

Hence

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

and for p a prime

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

For $n \geqslant 1$, $\Phi_n(X,Y)$ it is the homogeneous version of the cyclotomic polynomial ϕ_n of index n:

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

when ζ_n is a primitive n-th root of unity.

Quadratic cyclotomic binary forms

The degree of the cyclotomic binary form $\Phi_n(X,Y)$ is given by Euler totient function:

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

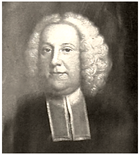
$$\Phi_n(X,Y) = Y^{\varphi(n)}\phi_n(X/Y) = \prod_{\substack{1\leqslant k\leqslant n \\ (k,n)=1}} (X - \zeta_n^k Y)$$

There are two linear cyclotomic binary forms Φ_1 and Φ_2, three quadratic cyclotomic binary forms Φ_3, Φ_4 and Φ_6:

$$\Phi_3(X,Y) = X^2 + XY + Y^2,$$
$$\Phi_4(X,Y) = X^2 + Y^2,$$
$$\Phi_6(X,Y) = X^2 - XY + Y^2 = \Phi_3(X,-Y).$$

The so–called Pell equation $x^2 - dy^2 = \pm 1$

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 between Pierre de Fermat and Lord Brouncker.

1657: letter of Fermat to Frenicle de Bessy (1604–1674).

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

Representation of integers by binary forms

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

The Landau–Ramanujan constant

Edmund Landau

1877 – 1938

Srinivasa Ramanujan

1887 – 1920

The number of positive integers $\leqslant N$ which are sums of two squares is asymptotically $\mathsf{C}_{\Phi_4} N(\log N)^{-\frac{1}{2}}$, where

$$\mathsf{C}_{\Phi_4} = \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

Online Encyclopedia of Integer Sequences

[OEIS A001481] `Numbers that are the sum of` 2 `squares.`

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

[OEIS A064533] `Decimal expansion of Landau-Ramanujan constant.`

$$\mathsf{C}_{\Phi_4} = 0.764\,223\,653\,589\,220\ldots$$

- 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.

The Landau–Ramanujan constant

References: 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

Sums of two squares

A prime number is a sum of two squares if and only either it is 2 or else if it is congruent to 1 modulo 4.

[OEIS A002313] `Primes congruent to` 1 `or` 2 `modulo` 4`; or, primes of form` $x^2 + y^2$`; or,` -1 `is a square` $\bmod p$. $2, 5, 13, 17, 29, 37, 41, \dots$

Pierre de Fermat

1601 – 1665

Identity of Brahmagupta:

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

with

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

Brahmagupta

598 – 668

Sums of two squares

When a and q are two positive integers, denote $N_{a,q}$ any integer $\geqslant 1$ which satisfies

$$p \mid N_{a,q} \Longrightarrow p \equiv a \bmod q.$$

An integer $m \geqslant 1$ is of the form

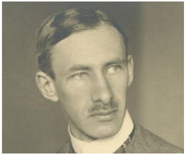
$$m = \Phi_4(x, y) = x^2 + y^2$$

if and only if there exist integers $a \geqslant 0$, $N_{3,4}$ and $N_{1,4}$ satisfying

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

Quadratic forms with non square discriminant

Let $F \in \mathbb{Z}[X, Y]$ be a quadratic form with determinant which is not a square. There exists a positive constant C_F such that, for $N \to \infty$, the number of positive integers $m \in \mathbb{Z}$, $m \leqslant N$ which are represented by F is asymptotically $\mathsf{C}_F N(\log N)^{-\frac{1}{2}}$.



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. in mathematics, Göttingen University, *On the analytic number theory of binary quadratic forms* (Advisor: E. Landau).
- 1913, Habilitation, Zürich University, *On complex analysis and Picard's theorem*, advisor E. Zermelo.
- 1912 – 1917, Zürich; works with Georg Pólya, Albert Einstein, Hermann Weyl.
- 1917 – 1933, Göttingen, with David Hilbert. Study with Emmy Noether, van der Waerden, G. Herglotz,
- 1935 – 1936, Institute for Advanced Study, Princeton. Lectures on mathematical logic and axiomatic theory of sets.
- 1936 —, ETH Zürich.
- With Hilbert, "Grundlagen der Mathematik" (1934 – 39) 2 vol. — Hilbert–Bernays paradox.
- Axiomatic Set Theory (1958). — Von Neumann–Bernays–Gödel set theory.

Generalizations

- Sums of cubes, biquadrates,. . .

Notice that $X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2)$.

The binary form $\Phi_3(X, Y) = X^2 + XY + Y^2$ is the homogeneous version of the cyclotomic polynomial $\phi_3(t) = t^2 + t + 1$.
We have

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

and

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

The quadratic form X^2+XY+Y^2

A prime number is represented by the quadratic cyclotomic binary form X^2+XY+Y^2 if and only if either it is 3, or else it is congruent to 1 modulo 3.

Product of two numbers represented by the quadratic form X^2+XY+Y^2:

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

with

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

The field $\mathbb{Q}(\sqrt{-3})=\mathbb{Q}(\zeta_3)$, $1+\zeta_3+{\zeta_3}^2=0$ is one of the two quadratic cyclotomic fields (the other is $\mathbb{Q}(\mathrm{i})$):

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

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

An integer $m \geqslant 1$ can be written

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

if and only if there exist integers $b \geqslant 0$, $N_{2,3}$ and $N_{1,3}$ such that

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

[OEIS A003136] `Loeschian numbers: numbers of the form` $x^2 + xy + y^2$`; norms of vectors in` $A2$ `lattice.`

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

Cyclotomic forms

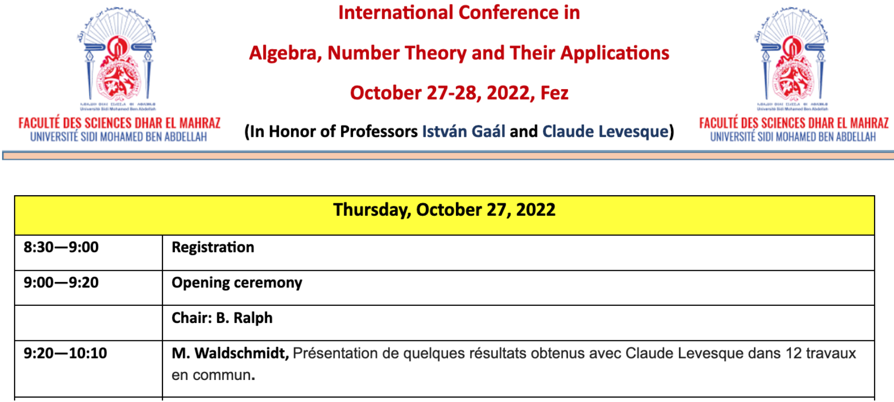
In a joint work with E. Fouvry and C. Levesque we gave an asymptotic estimate for the number of integers represented by one of the cyclotomic forms of degree $\geqslant 2$.

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]`

Fez Octobre 2022



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.

With E. Fouvry and C. Levesque

The number of integers $\leqslant N$ which are sums of two integers is asymptotically

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

The number of integers $\leqslant N$ which are represented by the quadratic form X^2+XY+Y^2 is asymptotically

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

where

$$\mathsf{C}_{\Phi_3}=\frac{1}{2^{\frac{1}{2}}3^{\frac{1}{4}}}\cdot\prod_{p\equiv 2 \bmod 3}\left(1-\frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

Intersection

An integer $m \geqslant 1$ is at the same time of the form

$m = \Phi_4(x, y) = x^2+y^2$ and of the form $m = \Phi_3(u, v) = u^2+uv+v^2$

if and only if there exist integers $a,\ b \geqslant 0$, $N_{5,12}$, $N_{7,12}$, $N_{11,12}$ and $N_{1,12}$ such that

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

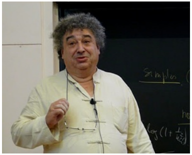
The number of integers $\leqslant N$ which are sums of two squares and are also represented by the quadratic form $X^2 + XY + Y^2$ is asymptotically

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

where

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

Development of zeta functions of classical constants



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

Connection with Euler constants

Alessandro Languasco Pieter Moree

Euler constants from primes in arithmetic progression.
Math. Comp. **95** (2026), 363–387.

Jean-Pierre Serre.
Quelques applications du théorème de densité de Chebotarev.
Publ. Math., Inst. Hautes Étud. Sci. **54** (1981), 123–202.

Jean-Pierre Serre

Online Encyclopedia of Integer Sequences

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

$$\mathsf{C}_{\Phi_3} = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} = 0.638\,909\,405\,445\,343\,88\ldots$$

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

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

$$= 0.302\,316\,142\,357\,065\,637\,94\ldots$$

Cyclotomic forms of degree > 2

Lemma (EF-CL-MW). *Let $d > 2$. There exists an effectively computable constant $C(d)$ such that the number of (n, x, y) in $\mathbb{Z}_{>0} \times \mathbb{Z}^2$ which satisfy $\varphi(n) \geqslant d$, $\max\{|x|, |y|\} \geqslant 2$ and $\Phi_n(x, y) < N$ is bounded above by $C(d)N^{2/d}$.*

Consequence: the number of integers $\leqslant N$ which are represented by one of the forms Φ_n of degree $\geqslant 2$ is asymptotically the number of integers $\leqslant N$ which are represented by one of the cyclotomic quadratic forms Φ_3, Φ_4: the cyclotomic forms of degree $\geqslant 4$ contribute only to the remainder term.

Remark on the assumption $\max\{|x|, |y|\} \geqslant 2$:
$\Phi_p(1, 1) = p$ for any prime p.

Cyclotomic forms of higher degree

It is natural to ask how many integers $\leqslant N$ are represented by one of the cyclotomic forms of degree $\geqslant d$, when d is a given integer > 2.

Theorem (with EF). *Let $d \geqslant 4$. Assume that there exists an integer n such that $\varphi(n) = d$. Then the number of integers $\leqslant N$ which are represented by one of the cyclotomic binary forms Φ_n of degree $\geqslant d$ is asymptotically the number of integers $\leqslant N$ which are represented by one of the cyclotomic binary forms Φ_n of degree d: the cyclotomic forms of degree $> d$ contribute only to the remainder term.*

We also give an asymptotic estimate for the number of integers $\leqslant N$ which are represented by one of the cyclotomic forms Φ_n of degree d.

Joint work with E. Fouvry

EF+MW,

• *Sur la représentation des entiers par des formes cyclotomiques de grand degré.*
Bull. Soc. Math. France, **148** (2020), 253–282.
`DOI: 0.24033/bsmf.2805          arXiv:  1909.01892 [math.NT]`

• *Number of integers represented by families of binary forms (I).*
Acta Arithmetica, **209** (2023), 219–267.
`DOI: 10.4064/aa220606-16-2   arXiv:  2206.03733 [math.NT].`

• *Number of integers represented by families of binary forms (II): binomial forms.*
Acta Arithmetica, **214** (2024), 271–287.
`DOI: 10.4064/aa230525-6-9      arXiv:2306.02462 [math.NT].`

• *Number of integers represented by families of binary forms (III): lacunary forms (fewnomials).* In preparation.

The group $\mathrm{Aut}F$

When $F \in \mathbb{Z}[X,Y]$ is a binary form of degree $\geqslant 2$ with nonzero discriminant, *the group* $\mathrm{Aut}F$ *of automorphisms of* F is the subgroup of $\mathrm{GL}_2(\mathbb{Q})$ which consists of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that

$$F(aX+bY, cX+dY) = F(X,Y).$$

Forms of degree $\geqslant 3$

A quadratic form has an infinite group of automorphisms. If an integer is represented by a quadratic form, it has many such representations. This explains the occurence of the denominator $(\log N)^{1/2}$ in the estimate by Bernays of the number of integers $\leqslant N$ which are represented by a given quadratic form.

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $d \geqslant 3$ and non-zero discriminant. The group of automorphisms of F is finite (an automorphism permutes the roots of $F(t,1)$).

If an integer is represented by F, it has only finitely many such representations (*Thue's Theorem*).

Forms of degree $\geqslant 3$

Axel Thue

1863 - 1922

Kurt Mahler

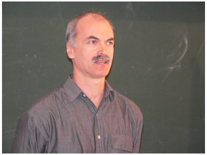
1903 - 1988

Let F be a binary form of degree $\geqslant 3$ with nonzero discriminant.
Thue's Theorem. Let $m \in \mathbb{Z} \setminus \{0\}$. Then the set of $(x, y) \in \mathbb{Z}^2$ such that $F(x, y) = m$ is finite.
Mahler's result. The number of $(x, y) \in \mathbb{Z}^2$ with $0 < |F(x, y)| \leqslant N$ is asymptotically $A_F N^{2/d}$ where

$$A_F := \iint_{|F(x,y)| \leqslant 1} \mathrm{d}x\mathrm{d}y$$

Mahler, K.: *Zur Approximation algebraischer Zahlen. III.* Acta Math. **62**, 91–166 (1933). `DOI: 10.1007/BF02393603` `JFM 60.0159.04`

Stewart & Xiao



Cam L. Stewart

Stanley Yao Xiao

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $d \geqslant 3$ and non-zero discriminant.
The number of integers $m \in \mathbb{Z}$ with $|m| \leqslant N$ of the form $m = F(x, y)$ with $(x, y) \in \mathbb{Z}^2$ is asymptotically

$$A_F \cdot W_F \cdot N^{2/d} + O_{F,\varepsilon}\left(N^{\kappa_d+\varepsilon}\right),$$

with $\kappa_d < 2/d$ and where $W_F = W(\mathrm{Aut} F)$ depends only on the group of automorphisms of F.

C.L. Stewart and S. Yao Xiao, *On the representation of integers by binary forms*, Math. Ann. **375** (2019), 133–163.
DOI: 10.4064/aa171012-24-12 arXiv:1605.03427v2

Tools: analytic number theory, algebraic geometry

Christopher Hooley

Roger Heath-Brown

Jean-Louis Colliot-Thélène

Per Salberger

Automorphisms of binary forms

Let G_1 and G_2 be subgroups of $\mathrm{GL}_2(\mathbb{Q})$. We say that they are *equivalent under conjugation* if there is an element T in $\mathrm{GL}_2(\mathbb{Q})$ such that $G_1 = TG_2T^{-1}$.

There are 10 equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ under $\mathrm{GL}_2(\mathbb{Q})$–conjugation to which $\mathrm{Aut}F$ might belong.

The constant W_F of Stewart and Xiao is a rational number that depends only on the conjugacy class of $\mathrm{Aut}F$.

Numbers essentially represented by a form

Let F be a binary form and m a nonzero integer. We say that m is *essentially represented by* F if m is represented by F and whenever (x_1, y_1), (x_2, y_2) are in $\mathbb{Z}^2$ and

$$F(x_1, y_1) = F(x_2, y_2) = m,$$

then there exists A in $\mathrm{Aut}F$ such that

$$A \begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_2 \\ y_2 \end{pmatrix}.$$

Stewart and Xiao: the number of integers m with $|m| \leqslant N$ which are represented by F not essentially is bounded by $O(N^\beta)$ with $\beta < 2/d$.

Isomorphism of binary forms

Two binary forms F and G in $\mathbb{Z}[X,Y]$ of degree $\geqslant 3$ with nonzero discriminant are *isomorphic* if there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(\mathbb{Q})$ such that

$$F(aX+bY, cX+dY) = G(X,Y).$$

With Etienne Fouvry: if F and G are two non isomorphic binary forms of degree $d \geqslant 3$ and nonzero discriminant, the number of integers m with $|m| \leqslant N$ which are represented by F and by G is bounded by $O(N^\beta)$ with $\beta < 2/d$.

Regular family of binary forms

Let $\mathcal{F}$ be an infinite set of binary forms with discriminants different from zero and with degrees $\geqslant 3$. We assume that for each $d \geqslant 3$, the subset $\mathcal{F}_d$ of $\mathcal{F}$ of forms with degree d is finite. We will say this set $\mathcal{F}$ is *regular* if there exists a positive integer A satisfying the following two conditions
(i) Two forms of the family $\mathcal{F}$ are $\mathrm{GL}(2,\mathbb{Q})$–isomorphic if and only if they are equal,
(ii) For all $\epsilon > 0$, there exist two positive integers $N_0 = N_0(\epsilon)$ and $d_0 = d_0(\epsilon)$ such that, for all $N \geqslant N_0$, the number of integers m in the interval $[-N, N]$ for which there exists $d \in \mathbb{Z}$, $(x, y) \in \mathbb{Z}^2$ and $F \in \mathcal{F}_d$ satisfying

$$d \geqslant d_0, \quad \max\{|x|, |y|\} \geqslant A \quad \text{and} \quad F(x, y) = m$$

is bounded by N^ϵ.

Main result for a regular family

Let $\mathcal{F}$ be a regular family of binary forms. Then for every $d \geqslant 3$, the quantity

$$\mathcal{R}_{\geqslant d}(\mathcal{F}, N, A) := \sharp \Big\{ m : 0 \leqslant |m| \leqslant N, \text{ there is } F \in \mathcal{F} \text{ with } \deg F \geqslant d \text{ and } (x,y) \in \mathbb{Z}^2 \text{ with } \max\{|x|,|y|\} \geqslant A, \text{ such that } F(x,y) = m \Big\}$$

satisfies

$$\mathcal{R}_{\geqslant d}(\mathcal{F}, N, A) = \left(\sum_{F \in \mathcal{F}_d} A_F W_F \right) \cdot N^{2/d} + O\big(N^{\beta}\big),$$

uniformly as $N \to \infty$.

Examples of regular families

- Cyclotomic forms Φ_n, $\varphi(n) \geqslant 3$.

- Products of linear forms $\displaystyle\prod_{j=1}^{d}(X + a_jY)$, $d \geqslant 3$.

- Products of quadratic forms $\displaystyle\prod_{j=1}^{d/2}(X^2 + a_jY^2)$, d even $\geqslant 4$.

- Binary binomial forms $aX^d + bY^d$, $d \geqslant 3$.

Family of binary binomial forms $aX^d + bY^d$

For each $d \geqslant 3$, let $\mathcal{E}_d$ be a finite set of $(a,b) \in \mathbb{Z}^2$ with $ab \neq 0$ and $\mathcal{F}_d$ the set of binary binomial forms $aX^d + bY^d$ with $(a,b) \in \mathcal{E}_d$.
For $m \in \mathbb{Z}$, let

$$\mathcal{G}_{\geqslant d}(m) = \Big\{(d', a, b, x, y) \ \mid \ m = ax^{d'} + by^{d'} \ \text{ with } \\ d' \geqslant d,\ (a,b) \in \mathcal{E}_{d'},\ (x,y) \in \mathbb{Z}^2 \ \text{ and } \ \max\{|x|, |y|\} \geqslant 2\Big\}.$$

For $d \geqslant 3$, let

$$\mathcal{R}_{\geqslant d} = \{m \in \mathbb{Z} \ \mid \ \mathcal{G}_{\geqslant d}(m) \neq \emptyset\}$$

and for $N \geqslant 1$, let $\mathcal{R}_{\geqslant d}(N) = \mathcal{R}_{\geqslant d} \cap [-N, N]$. So $\#\mathcal{R}_{\geqslant d}(N)$ is the number of $m \leqslant N$ which are represented by one of the forms $aX^{d'} + bY^{d'}$ with $d' \geqslant d$ and $(a,b) \in \mathcal{E}_{d'}$.

Isomorphisms between two binary binomial forms

Let $(a, b) \in \mathbb{Z}^2$ and $(a, b) \in \mathbb{Z}^2$ satisfy $ab \neq 0$ and $a'b' \neq 0$ and let $d \geqslant 2$. If the two conditions

(C1): For every $(a, b) \neq (a', b') \in \mathcal{E}_d$, at least one of ratios a/a' and b/b' is not the d–th power of a rational number,

(C2): For every $(a, b) \neq (a', b') \in \mathcal{E}_d$, at least one of ratios a/b' and b/a' is not the d–th power of a rational number

are satisfied, then the two forms $aX^d + bY^d$ and $a'X^d + b'Y^d$ are not isomorphic (and conversely).

Family of positive definite binary binomial forms

Assume $a>0$, $b>0$ for all $(a,b)\in\mathcal{E}_d$ for all $d\geqslant 4$ and $\mathcal{E}_d=\emptyset$ for odd d. Assume further

$$\frac{1}{d}\log(\sharp\mathcal{E}_d+1)\to 0 \quad \text{as} \quad d\to\infty.$$

Then

(a) For all $m\in\mathbb{Z}\smallsetminus\{0,1\}$ and all $d\geqslant 4$, the set $\mathcal{G}_{\geqslant d}(m)$ is finite. Furthermore, for all $d\geqslant 4$ and all $\epsilon>0$, we have, as $|m|\to\infty$,

$$\sharp\mathcal{G}_{\geqslant d}(m)=O\left(|m|^{(1/d)+\epsilon}\right).$$

(b) Let $d\geqslant 4$ be an integer such that the above conditions *(C1)* and *(C2)* hold. We have, as $N\to\infty$,

$$\sharp\mathcal{R}_{\geqslant d}(N)=\left(\sum_{(a,b)\in\mathcal{E}_d} C_{a,b,d}\right)N^{2/d}+O\Big(N^{\beta}\Big).$$

Family of binary binomial forms (general case)

Let $\epsilon > 0$. There exists a constant $\eta > 0$ depending only on ϵ with the following property. Assume that there exists $d_0 > 0$ such that, for all $d \geqslant d_0$, we have the inequality

$$\max_{(a,b)\in\mathcal{E}_d} \{|a|, |b|\} \leqslant \exp(\eta d/\log d).$$

Then

(a) For all $m \in \mathbb{Z} \smallsetminus \{-1, 0, 1\}$ and all $d \geqslant 3$, the set $\mathcal{G}_{\geqslant d}(m)$ is finite. Furthermore, for all $d \geqslant 3$, we have, as $|m| \to \infty$,

$$\sharp\mathcal{G}_{\geqslant d}(m) = O\left(|m|^{(1/d)+\epsilon}\right).$$

(b) Let $d \geqslant 3$ be an integer such that the above conditions *(C1)* and *(C2)* hold. We have, as $N \to \infty$,

$$\sharp\mathcal{R}_{\geqslant d}(N) = \left(\sum_{(a,b)\in\mathcal{E}_d} C_{a,b,d}\right) N^{2/d} + O\Big(N^\beta\Big).$$

Avril 2025

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/