#### 31/01/2024

#### Diophantine conference, TSIMF (Tsinghua Sanya International Mathematics Forum)

# Representation of integers by binary forms

Michel Waldschmidt

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

#### Abstract

An asymptotic estimate for the number of integers below a given bound which are sums of two squares has been given by Ramanujan, it involves the so-called Landau Ramanujan constant. Similar estimates, due to P. Bernays, are known for quadratic forms with nonzero discriminant. Only recently C.L. Stewart and S.Y. Xiao proved such an estimate for the number of integers which are represented by a binary form of degree  $\geq 3$ .

With E. Fouvry we investigated the number of integers which are represented by two nonisomorphic binary form of the same degree  $\geq 3$ . This enables us to give asymptotic estimates for the number of integers which are represented by at least one form in some families of forms.

## **Binary forms**

A binary form is a homogeneous polynomial in two variables  $a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d \in \mathbb{Z}[X, Y].$ 

A binary form of degree 1 is a linear form  $a_0X + a_1Y$ . The set of integers which are represented by such a form is the set of multiples of the gcd of  $a_0, a_1$  (Euclid algorithm). *Quadratic forms* are binary forms of degree 2 :

 $a_0 X^2 + a_1 X Y + a_2 Y^2.$ 

We first consider the *cyclotomic* forms  $\Phi_4(X, Y) = X^2 + Y^2$ and  $\Phi_3(X, Y) = X^2 + XY + Y^2$ . Notice that  $\Phi_6(X, Y) = X^2 - XY + Y^2$ . Here  $\Phi_d$  are the homogeneous versions of the cyclotomic polynomials

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

3/36

・ロト ・ 同ト ・ ヨト ・ ヨト ・ りゅう

# Cyclotomic forms

We shall start with a joint work with E. Fouvry and C. Levesque on the number of integers which are represented by a cyclotomic form.



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]

# Joint work with E. Fouvry

Next we shall present joint works with E. Fouvry where we study other families of binary forms of degree  $\geq 3$ .

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.2805hfill 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, to appear. arXiv:2306.02462 [math.NT].

# Representation of integers by binary forms



Pierre de Fermat 1601 - 1665



#### Joseph-Louis Lagrange 1736 - 1813



Adrien-Marie Legendre 1752 - 1833 R

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

6/36

# The Landau-Ramanujan constant



The number of positive integers  $\leq N$  which are sums of two squares is asymptotically  $C_{\Phi_4}N(\log N)^{-\frac{1}{2}}$ , 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.

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

• Ph. Flajolet and I. 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, 125079 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 if it is either 2 or else 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 mod p. 2, 5, 13, 17, 29, 37, 41, ...

Identity of Brahmagupta :

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

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



Pierre de Fermat 1601 – 1665



Brahmagupta 598 – 668

### Sums of two squares

If a and q are two integers, we denote by  $N_{a,q}$  any integer  $\geq 1$  satisfying the condition

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

An integer  $m \geq 1$  can be written as

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

if and only if there exist integers  $a\geq 0$  ,  $N_{3,4}$  and  $N_{1,4}$  such that

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

・ロ ・ ・ 一部 ・ く 言 ・ く 言 ・ う へ (や 11 / 36

#### Positive definite quadratic forms

Let  $F \in \mathbb{Z}[X, Y]$  be a positive definite quadratic form. There exists a positive constant  $C_F$  such that, for  $N \to \infty$ , the number of positive integers  $m \in \mathbb{Z}$ ,  $m \leq N$  which are represented by F is asymptotically  $C_F N(\log N)^{-\frac{1}{2}}$ .



Paul Bernays 1888 – 1977

P. BERNAYS, Uber 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, University of Göttingen, *On the analytic number theory of binary quadratic forms* (Advisor : E. Landau).

• 1913, Habilitation, University of Zürich, *On complex analysis and Picard's theorem*, advisor E. Zermelo.

- 1912 1917, Zürich; work with Georg Pólya, A. Einstein, Hermann Weyl.
- 1917 1933, Göttingen, with D. Hilbert. Studied with Emmy Noether, van der Waerden, G. Herglotz,
- 1935 1936, Institute for Advanced Study, Princeton. Lectures on mathematical logic and axiomatic set theory
- 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  $X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2)$ 

We start with the quadratic form  $\Phi_3(X, Y) = X^2 + XY + Y^2$ which is the homogeneous version of the cyclotomic polynomial  $\phi_3(t) = t^2 + t + 1$ . Notice that

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

Also

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

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

A prime number is represented by the quadratic form  $X^2 + XY + Y^2$  if and only if it is either 3 or else 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 quadratic cyclotomic field  $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ ,  $1 + \zeta_3 + \zeta_3^2 = 0$ :

$$a^{2} + ab + b^{2} = \operatorname{Norm}_{\mathbb{Q}(\zeta_{3})/\mathbb{Q}}(a - \zeta_{3}b).$$

<ロ > < 部 > < き > くき > き や え の Q (C) 15 / 36 Loeschian numbers :  $m = x^2 + xy + y^2$ 

An integer  $m \geq 1$  can be written as

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

if and only if there exist integers  $b\geq 0,~N_{2,3}$  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, ...

# With E. Fouvry and C. Levesque

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

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

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

$$\frac{N}{(\log N)^{1/2}} \left( \mathsf{C}_{\Phi_3} + \frac{\alpha_1'}{\log N} + \dots + \frac{\alpha_M'}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right)$$

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  $m \ge 1$  is simultaneously of the forms

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

if and only if there exist integers  $a,\,b\geq 0$  ,  $N_{5,12}$  ,  $N_{7,12}$  ,  $N_{11,12}$  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  $\leq N$  which are represented by the quadratic form  $X^2 + XY + Y^2$  and at the same time are sums of two squares is asymptotically

$$\frac{N}{(\log N)^{3/4}} \left( \beta_0 + \frac{\beta_1}{\log N} + \dots + \frac{\beta_M}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right)$$
  
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 \text{ mod } 12} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}} \left( \frac{1-\frac{1}{p^2}}{p^2} \right)^{-\frac{1}{2}} \cdot \sum_{\substack{n < n \\ 18/3}}$$

#### Zeta function expansions of some 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://arxiy.org/abs/1908.06808u1

#### Online Encyclopedia of Integer Sequences [OEIS A301429] Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers.

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

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

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

# The group $\operatorname{Aut} F$

When  $F \in \mathbb{Z}[X, Y]$  is a binary form of degree  $\geq 2$  with nonzero discriminant, the group  $\operatorname{Aut} F$  of automorphisms of Fis the subgroup of  $\operatorname{GL}_2(\mathbb{Q})$  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 $\geq 3$

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

Let  $F \in \mathbb{Z}[X, Y]$  be a binary form of degree  $d \geq 3$  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 $\geq 3$



Axel Thue 1863 - 1922



Kurt Mahler 1903 - 1988

Let F be a binary form of degree  $\geq 3$  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  $0 < |F(x, y)| \leq N$  is asymptotically  $A_F N^{2/d}$  where

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

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  $d \geq 3$  and non-zero discriminant.

The number of integers  $m \in \mathbb{Z}$  with  $|m| \leq N$  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  $W_F = W(\operatorname{Aut} F)$  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  $\operatorname{GL}_2(\mathbb{Q})$ . We say that they are *equivalent under conjugation* if there is an element T in  $\operatorname{GL}_2(\mathbb{Q})$  such that  $G_1 = TG_2T^{-1}$ .

There are 10 equivalence classes of finite subgroups of  $GL_2(\mathbb{Q})$  under  $GL_2(\mathbb{Q})$ -conjugation to which AutF might belong.

The constant  $W_F$  of Stewart and Xiao is a rational number that depends only on the conjugacy class of AutF.

#### 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 AutF 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  $|m| \leq N$ 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  $\geq 3$  with nonzero discriminant are *isomorphic* if there exists a matrix  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$  in  $\operatorname{GL}_2(\mathbb{Q})$  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  $d \ge 3$  and nonzero discriminant, the number of integers m with  $|m| \le N$  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  $\geq 3$ . We assume that for each  $d \geq 3$ , 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  $N \ge N_0$ , 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

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

is bounded by  $N^{\epsilon}$ .

#### Main result for a regular family

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

 $\begin{aligned} \mathcal{R}_{\geq d}\left(\mathcal{F}, N, A\right) &:= \sharp \left\{ m : 0 \leq |m| \leq N, \text{ there is } F \in \mathcal{F} \text{ with} \\ \deg F \geq d \text{ and } (x, y) \in \mathbb{Z}^2 \text{ with } \max\{|x|, |y|\} \geq A, \\ \text{ such that } F(x, y) = m \right\} \end{aligned}$ 

satisfies

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

uniformly as  $N \to \infty$ .

# Examples of regular families

• Cyclotomic forms  $\Phi_n$ ,  $\varphi(n) \geq 3$ .

• Products of linear forms 
$$\prod_{j=1}^{d} (X + a_j Y)$$
,  $d \ge 3$ .

• Products of quadratic forms  $\prod_{j=1}^{d/2} (X^2 + a_j Y^2)$ , d even  $\geq 4$ .

• Binary binomial forms  $aX^d + bY^d$ ,  $d \ge 3$ .

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

For each  $d \geq 3$ , 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

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

For  $d \geq 3$ , let

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

and for  $N \ge 1$ , let  $\mathcal{R}_{\ge d}(N) = \mathcal{R}_{\ge d} \cap [-N, N]$ . So  $\#\mathcal{R}_{\ge d}(N)$ is the number of  $m \le N$  which are represented by one of the forms  $aX^{d'} + bY^{d'}$  with  $d' \ge d$  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  $d \geq 2$ . 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 $d \ge 4$ 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

1

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

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

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

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

34 / 36

Family of binary binomial forms (general case) Let  $\epsilon > 0$ . There exists a constant  $\eta > 0$  depending only on  $\epsilon$ with the following property. Assume that there exists  $d_0 > 0$ such that, for all  $d \ge d_0$ , we have the inequality

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

Then

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

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

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

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

35 / 36

#### 31/01/2024

36 / 36

#### Diophantine conference, TSIMF (Tsinghua Sanya International Mathematics Forum)

# Representation of integers by binary forms

Michel Waldschmidt

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