On binomial binary forms

Michel Waldschmidt

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

Abstract (1/3)

Binomial binary forms are homogeneous polynomials with integer coefficients in two variables: $aX^d + bY^d$.

For $d = 2$, these are quadratic binary forms, the study of which goes back to Brahmagupta and Fermat (the so called Pell's equation). Sums of two squares have been investigated by Ramanujan and Landau. An asymptotic estimate for the number of representation of an integer by a positive definite quadratic form has been obtained by Bernays.

Abstract (2/3)

For $d \geqslant 3$, the fundamental result of Thue on diophantine approximation yields, for $m \neq 0$ and assuming $abm \neq 0$, the finiteness of the set of pairs of integers (x, y) such that $ax^d + by^d = m$. Among the many mathematicians who contributed to the study of representation of integers by binomial binary forms, we may quote Christopher Hooley, George R. H. Greaves, Christopher Skinner, Trevor Wooley, Roger Heath Brown, Michael Bean, Mike Bennett, Neil Dummigan, Timothy Browning, András Bazsó, Attila Bérczes, Kálmán Győry, Ákos Pintér, István Pink, Zsolt Rábai, until Cam Stewart and Stanley Yao Xiao found a very general theorem on the representation of integers by binary forms, producing a best possible asymptotic estimate. They gave a completely explicit version for binomial binary forms.

Abstract (3/3)

With Étienne Fouvry we recently investigated the number of integers which are represented by one form in a family of binary forms. In this lecture I will present the special case of binomial binary forms.

Étienne Fouvry and Michel Waldschmidt *Number of integers represented by families of binary forms (II): binomial forms.* Acta Arithmetica, to appear,
Online First, April 8, 2024 arXiv:2306.02462 [math.NT].

Étienne Fouvry

Binomial binary quadratic forms

$F(X,Y) = aX^2 + bY^2$, a, b in $\mathbb{Z}$, $ab \neq 0$.

Pierre de Fermat

1601 - 1665

Brahmagupta

598 – 668

- Indefinite forms: $ab < 0$.
  Example: $x^2 - Dy^2 = \pm 1$.
  Brahmagupta – Pell – Fermat equation.
- Positive definite forms: $ab > 0$.
  Finite number of solutions to $ax^2 + by^2 = m$.
  Example: sums of two squares.

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

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

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

Representation of integers by binary forms

Pierre de Fermat

1601 - 1665

Joseph-Louis Lagrange

1736 - 1813

Adrien-Marie Legendre

1752 - 1833

Carl Friedrich Gauss

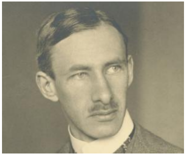
1777 - 1855

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

Peter Duren. Changing Faces: The Mistaken Portrait of Legendre.
www.ams.org/notices/200911/rtx091101440p.pdf

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 $m \in \mathbb{Z}$, $m \leqslant N$ 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/

Binary forms of degree $\geqslant 3$: Thue's Theorem

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $\geqslant 3$ with nonzero discriminant.

Axel Thue

1863 - 1922

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.*

Axel Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. **135** (1909), 284– 305.

Binary forms of degree $\geqslant 3$: Mahler's Theorem

Let $F \in \mathbb{Z}[X, Y]$ be a binary form of degree $\geqslant 3$ with nonzero discriminant.

Kurt Mahler

1903 - 1988

Mahler's result. *As $N \to \infty$, the number of $(x, y) \in \mathbb{Z}^2$ with $0 < |F(x, y)| \leqslant N$ is asymptotically $A_F N^{2/d}$ where*

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

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

Binomial binary forms of degree $\geqslant 3$

For a, b, d in $\mathbb{Z}$ satisfying $ab \neq 0$ and $d \geqslant 3$, set

$$F_{abd}(X, Y) := aX^d + bY^d.$$

Corollary [Thue] *For each $m \neq 0$ the equation $ax^d + by^d = m$ has only finitely many solutions.*

Corollary [Mahler] *The number of integers $(x, y) \in \mathbb{Z}^2$ such that $0 < [ax^d + by^d| \leqslant N$ is asymptotically $A_{F_{abd}} N^{2/d}$ where*

$$A_{F_{abd}} := \iint_{|ax^d + by^d| \leqslant 1} \mathrm{d}x\mathrm{d}y.$$

Value of $A_{F_{abd}}$: C.L. Stewart and S.Y. Xiao

If d is odd then

$$A_{F_{abd}} = \frac{1}{d|ab|^{1/d}} \left(\frac{2\Gamma(1-2/d)\Gamma(1/d)}{\Gamma(1-1/d)} + \frac{\Gamma^2(1/d)}{\Gamma(2/d)} \right)$$

while if d is even

$$A_{F_{abd}} = \frac{2}{d|ab|^{1/d}} \frac{\Gamma^2(1/d)}{\Gamma(2/d)} \quad \text{if} \quad ab > 0$$

and

$$A_{F_{abd}} = \frac{4}{d|ab|^{1/d}} \frac{\Gamma(1-2/d)\Gamma(1/d)}{\Gamma(1-1/d)} \quad \text{if} \quad ab < 0.$$

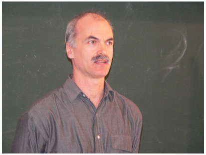
Number of integers represented by F

Mahler's result deals with the number of (x, y) with $0 < |F(x, y)| \leqslant N$. We are interested with the number of integers m with $|m| \leqslant N$ which are represented by F.

If any number $m \neq 0$ represented by F were represented exactly w_F times, with w_F depending on F but not on m, then we would deduce that the number of m with $|m| \leqslant N$ which are represented by F is asymptotically $(1/w_F)A_F N^{2/d}$.

This is asking too much, but the conclusion on the existence of w_F is the right one: this constant w_F depends on the automorphisms of F. The number of integers which are represented by F more than w_F times contributes only to the error term. This is the remarkable result of Stewart and Xiao.

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*

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

with $\kappa_d < 2/d$ *and where* $W_F = W(\mathrm{Aut} F) \leqslant 1$ *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. arXiv:1605.03427v2

Value of $W_{F_{abd}}$ for binomial binary forms

Let a, b and d be non-zero integers with $d \geqslant 3$ and let $F_{abd}(x,y) = ax^d + by^d$.
If a/b is not the d-th power of a rational number then

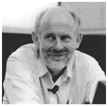
$$W_{F_{abd}} = \begin{cases} 1 & \text{if } d \text{ is odd,} \\ \frac{1}{4} & \text{if } d \text{ is even.} \end{cases}$$

If $\frac{a}{b} = \left(\frac{A}{B}\right)^d$ with A and B coprime integers then

$$W_{F_{abd}} = \begin{cases} 1 - \frac{1}{2|AB|} & \text{if } d \text{ is odd,} \\ \frac{1}{4}\left(1 - \frac{1}{2|AB|}\right) & \text{if } d \text{ is even.} \end{cases}$$

Reference: C.L. Stewart & S.Y. Xiao, op. cit., Corollary 1.3.

Some of the earlier results


Christopher Hooley George R. H. Greaves Christopher Skinner



Trevor Wooley Roger Heath Brown Mike Bennett




Neil Dummigan Timothy Browning András Bazsó Attila Bérczes



Kálmán Győry Ákos Pintér István Pink

Some of the earlier results

Hooley, C. – *On binary cubic forms.* J. Reine Angew. Math. **226**, 30–87 (1967)

Hooley, C. – *On another sieve method and the numbers that are a sum of two hth powers.* Proc. Lond. Math. Soc. **43**, 73–109 (1981)

Hooley, C. – *On binary quartic forms.* J. Reine Angew. Math. **366**, 32–52 (1986)

Greaves, G. – *Representation of a number by the sum of two fourth powers.* Mat. Zametki **55**, 47–58 (1994)

Skinner, C., Wooley, T.D. – *Sums of two kth powers.* J. Reine Angew. Math. **462**, 57–68 (1995)

Wooley, T.D. – *Sums of two cubes.* Int. Math. Res. Notices. **4**, 181–185 (1995)

Hooley, C. – *On another sieve method and the numbers that are a sum of two hth powers, II.* J. Reine Angew. Math. **475**, 55–75 (1996)

Bennett, M.A., Dummigan, N.P., Wooley, T.D. – *The representation of integers by binary additive forms.* Compos. Math. **111**, 15–33 (1998)

Hooley, C. – *On binary cubic forms. II.* J. Reine Angew. Math. **521**, 185-240 (2000)

Browning, T.D. – *Equal sums of two kth powers.* J. Number Theory **96**, 293–318 (2002)

Families of binary forms I

Joint work with

Étienne Fouvry

Number of integers represented by families of binary forms I
Acta Arithmetica, **209** (2023), 219–267.
arXiv: 2206.03733 [math.NT].

With Étienne Fouvry, we are investigating the representation of integers by families of binary forms. Given a family of binary forms $\mathcal{F}$ having nonzero discriminant and with only finitely many forms in $\mathcal{F}$ of a given degree, under suitable assumptions, we prove that the number of integers which are represented by elements of degree $\geqslant d$ in $\mathcal{F}$ is asymptotically the number of integers which are represented by elements of degree $= d$ in $\mathcal{F}$: the forms of degree $> d$ contribute only to the error term.

Non isomorphic binary forms

Two binary forms F_1 and F_2 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

$$F_1(aX+bY, cX+dY) = F_2(X,Y).$$

Two isomorphic binary forms have the same degree.

Auxiliary result: *If two binary forms in $\mathbb{Z}[X,Y]$ of degree $d \geqslant 3$ with nonzero discriminant are not isomorphic, then, as $N \to \infty$, the number of integers m with $|m| \leqslant N$ which are represented by both forms*

$$m = F_1(x_1, y_1) = F_2(x_2, y_2)$$

is $o(N^{2/d})$.

Families of binary forms II: binomial forms

Joint work with

Étienne Fouvry

Number of integers represented by families of binary forms II: binomial forms.
Acta Arithmetica, to appear.
Online First, April 8, 2024
arXiv:2306.02462 [math.NT].

For each $d \geqslant 3$, let $\mathcal{F}_d$ be a finite set of binomial binary forms

$$aX^d + bY^d$$

with $ab \neq 0$. Let $\mathcal{F}$ be the union of $\mathcal{F}_d$ for $d \geqslant 3$. Given $d \geqslant 3$, we wish to give an asymptotic formula, as $N \to \infty$, for the number of $m \in \mathbb{Z}$ with $|m| \leqslant N$ for which there exists $d' \geqslant d$, $F \in \mathcal{F}_{d'}$ and $(x, y) \in \mathbb{Z}^2$ such that $F(x, y) = m$.

Families of binomial binary forms

Let
$$F_{abd}(X,Y) = aX^d + bY^d.$$
Since
$$\begin{aligned} F_{abd}(1,0) &= a, & F_{abd}(-1,0) &= (-1)^d a,\\ F_{abd}(0,1) &= b, & F_{abd}(0,-1) &= (-1)^d b,\\ F_{abd}(1,1) &= a+b, & F_{abd}(-1,1) &= (-1)^d a + b,\\ F_{abd}(1,-1) &= a+(-1)^d b, & F_{abd}(-1,-1) &= (-1)^d a + (-1)^d b,\end{aligned}$$
by investigating $F_{abd}(x,y) = m$ it is natural to assume $\max\{|x|,|y|\} \geqslant 2$.

Families of binomial binary forms

Expected result: given $d \geqslant 3$ with $\mathcal{F}_d \neq \emptyset$,

> *The number of* $m \in \mathbb{Z}$ *with* $|m| \leqslant N$ *for which there exists* $d' \geqslant d$, $F_{abd'} \in \mathcal{F}_{d'}$ *and* $(x, y) \in \mathbb{Z}^2$ *with* $\max\{|x|, |y|\} \geqslant 2$ *such that* $F_{abd'}(x, y) = m$

is asymptotic to

> *the number of* $m \in \mathbb{Z}$ *with* $|m| \leqslant N$ *for which there exists* $F_{abd} \in \mathcal{F}_d$ *and* $(x, y) \in \mathbb{Z}^2$ *with* $\max\{|x|, |y|\} \geqslant 2$ *such that* $F_{abd}(x, y) = m$*, namely*

$$\left(\sum_{F_{abd} \in \mathcal{F}_d} A_{F_{abd}} W_{F_{abd}} \right) N^{2/d}.$$

Auxiliary results

To prove such a result, we need

- For the main term, to make sure we do not count several times the same m.
- To prove that the numbers $m \in \mathbb{Z}$ with $|m| \leqslant N$ which are represented by forms in $\mathcal{F}_{d'}$ for large d' contribute only to the error term.

Isomorphisms between binomial binary forms

Lemma. *Let* $d \geqslant 3$ *and* a, b, a' *and* b' *be integers different from zero. Then the two binary forms* $aX^d + bY^d$ *and* $a'X^d + b'Y^d$ *are isomorphic if and only if at least one of the following two conditions hold*

1. *the ratios* a/a' *and* b/b' *are both* d*–th powers of a rational number,*
2. *the ratios* a/b' *and* b/a' *are both* d*–th powers of a rational number.*

Recall that if $aX^d + bY^d$ and $a'X^d + b'Y^d$ are not isomorphic, then as $N \to \infty$, the number of m with $|m| \leqslant N$ which are represented by both binary forms is $o(N^{2/d})$.

Asymptotic result

Two methods are available;

- Assume the forms in $\mathcal{F}$ are definite positive. We merely need an assumption on the number of forms in $\mathcal{F}$. The proof is elementary.
- Lower bounds for linear forms in logarithms allow us to deal with more general families of binomial binary forms, assuming an upper bound for the coefficients a, b for the forms in $\mathcal{F}_d$.

Our setting

For each integer $d \geqslant 3$, let $\mathcal{E}_d$ be a finite subset of $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$.

Let $\mathcal{F}_d$ denote the family of binary forms $aX^d + bY^d$ with $(a,b) \in \mathcal{E}_d$ and let $\mathcal{F} = \cup_{d\geqslant 3}\mathcal{F}_d$.

The number of m with $|m| \leqslant N$ which are represented by one of the forms of degree $\geqslant d$ in the family $\mathcal{F}$ is

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

We assume that two forms in the family $\mathcal{F}$ are isomorphic if and only if they are equal.

Our two results

• **Family of positive definite binomial binary forms**

Assume $a > 0$, $b > 0$, $\mathcal{E}_d = \emptyset$ *for odd* d *and*

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

• **General case** (Stonger hypothesis)

Assume, for all ϵ *and for sufficiently large* d,

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

Conclusion

For every $d \geqslant 3$ *we have the equality*

$$\mathcal{R}_{\geqslant d}(N) = \left(\sum_{F\in\mathcal{F}_d} A_F W_F\right) N^{2/d} + o(N^{2/d})$$

uniformly for $N \to \infty$.

Two examples

• *The assumption* $\max\{|x|,|y|\} \geqslant 2$ *cannot be omitted.*
For each even $d \geqslant 4$, let $\mathcal{F}_d = \{F_d\}$ with $F_d = a_d X^d + Y^d$, where $(a_4, a_6, a_8, a_{10}, \dots)$ is the sequence

$$(1, 2, 1, 2, 3, 1, 2, 3, 4, \dots)$$

Then each integer m is represented infinitely often by one of the forms of the family $\mathcal{F}$:

$$F_d(1,0) = a_d, \quad F_d(1,1) = a_d + 1.$$

• *The assumptions on* $\sharp\mathcal{E}_d$ *and on* $\max_{(a,b)\in\mathcal{E}_d}\{|a|,|b|\}$ *cannot be omitted.*
Take $\mathcal{F}_d = \{aX^d + Y^d \mid 1 \leqslant a \leqslant 2^d\}$. For $N = 2^{2d} + 1$ there are 2^d positive integers $m \leqslant N$ of the form $F(2,1)$ for some $F \in \mathcal{F}_d$.

Conjectures

Using either the abc Conjecture or conjectures on lower bounds for linear forms in logarithms, one may replace the assumption

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

in the general case with

$$\max_{(a,b)\in\mathcal{E}_d} \{|a|, |b|\} \leqslant \mathrm{e}^{\epsilon d}.$$

SCHOLAR II –
A SCIENTIFIC CELEBRATION
HIGHLIGHTING OPEN LINES
OF ARITHMETIC RESEARCH
In honour of M. Ram Murty

On binomial binary forms

Michel Waldschmidt

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