

International Conference on Diophantine Equations,
Polynomials and Related Areas (ICDEPRA) 2026,
to celebrate Professor Sudesh Kaur Khanduja's 75th Birthday

On the integers that are represented by multicyclotomic binary forms

Michel Waldschmidt

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

International Conference on Diophantine Equations, Polynomials & Related Areas

ICDEPRA - 2024

November 26 - 30, Indian Statistical Institute (ISI), Delhi.

On the number of integers represented by two non-isomorphic binary forms

ICDEPRA - 2025

October 13 - 17, Indian Statistical Institute (ISI) Delhi

On families of fewnomial binary forms

ICDEPRA - 2026

September 28 - October 2 : Chennai, IIT Madras,

On the integers that are represented by multicyclotomic binary forms

Abstract

For $n \geq 1$, let $\phi_n(t)$ be the cyclotomic polynomial of index n ; the degree $\varphi(n)$ of ϕ_n is given by Euler's totient function φ .

The cyclotomic binary form of index n is $\Phi_n(X, Y) := Y^{\varphi(n)} \phi_n(X/Y)$.

We define a *multicyclotomic binary form* as a product of distinct cyclotomic forms.

In a joint work with Etienne Fouvry we study the integers that are represented by one at least of these multicyclotomic forms.

In particular we give an asymptotic formula, as $N \rightarrow \infty$, for the number of m satisfying $|m| \leq N$ for which there exists a multicyclotomic form Φ of degree ≥ 3 and integers (x, y) with $\max\{|x|, |y|\} \geq 2$ satisfying $m = \Phi(x, y)$.

Our first example : cyclotomic forms

In 2018, with E. Fouvry and C. Levesque we studied the set of integers that 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

[math.NT]

arXiv: 1712.09019

Cyclotomic forms of small degree

$$\Phi_1(X, Y) = X - Y,$$

$$\Phi_2(X, Y) = X + Y,$$

$$\varphi(n) \geq 2 \text{ for } n \geq 3.$$

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

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

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

$$\varphi(n) \geq 4 \text{ otherwise.}$$

We say that an integer m is *represented by a binary form* $F \in \mathbb{Z}[X, Y]$ if there exists $(x, y) \in \mathbb{Z}^2$ such that $F(x, y) = m$.

Cyclotomic forms of degree ≥ 2 (with EF & CL)

The number of integers $m \leq N$ that are represented by one at least of the cyclotomic forms Φ_n with $\varphi(n) \geq 2$ is asymptotically

$$(C_{\Phi_3} + C_{\Phi_4}) \frac{N}{\sqrt{\log N}} + C_{\Phi_3, \Phi_4} \frac{N}{(\log N)^{3/4}} + O\left(\frac{N}{\log N}\right).$$

Represented by Φ_3 or Φ_6 :

$$C_{\Phi_3} N (\log N)^{-1/2} + O(N (\log N)^{-3/2}).$$

Represented by Φ_4 (sums of two squares) :

$$C_{\Phi_4} N (\log N)^{-1/2} + O(N (\log N)^{-3/2}).$$

Represented by Φ_3 and Φ_4 :

$$C_{\Phi_3, \Phi_4} N (\log N)^{-3/4} + O(N (\log N)^{-3/2}).$$

The error term $O(N (\log N)^{-1})$ arises from the contribution of the prime numbers $\Phi_p(1, 1) = p$.

The Landau – Ramanujan constant



Edmund Landau
1877 – 1938



Srinivasa Ramanujan
1887 – 1920

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

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

Refined asymptotic estimates (with EF and CL)

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

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

where C_{Φ_4} is Ramanujan's Constant.

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

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

The number of integers $\leq N$ that are represented by the quadratic form $X^2 + XY + Y^2$ and at the same time are sums of two squares is asymptotically

$$\frac{N}{(\log N)^{3/4}} \left(C_{\Phi_3, \Phi_4} + \frac{\beta_1}{\log N} + \cdots + \frac{\beta_M}{(\log N)^M} + O\left(\frac{1}{(\log N)^{M+1}}\right) \right).$$

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

$$\begin{aligned} C_{\Phi_4} &= \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \pmod{4}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \\ &= 0.764\,223\,653\,589\,220\dots \end{aligned}$$

<https://oeis.org/A301429> :

$$\begin{aligned} C_{\Phi_3} &= \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \pmod{3}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \\ &= 0.638\,909\,405\,44\dots \end{aligned}$$

<https://oeis.org/A301430> :

$$\begin{aligned} C_{\Phi_3, \Phi_4} &= \frac{3^{\frac{1}{4}}}{2^{\frac{5}{4}}} \cdot \pi^{\frac{1}{2}} \cdot (\log(2 + \sqrt{3}))^{\frac{1}{4}} \cdot \frac{1}{\Gamma(1/4)} \cdot \prod_{p \equiv 5, 7, 11 \pmod{12}} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} \\ &= 0.302\,316\,142\,357\,065\,637\,94\dots \end{aligned}$$

Degree $\varphi(n) > 2$

In the previous estimate, the number of $m \leq N$ that can be written as $\Phi_n(x, y)$ with $\varphi(n) > 2$ and $\max\{|x|, |y|\} \geq 2$ does not contribute to the main terms.

When F is a binary form with nonzero discriminant, the number of integers m with $|m| \leq N$ that can be written as $F(x, y)$ follows a very different pattern whether F is a quadratic form or has degree > 2 .

For binary forms of degree ≥ 3 , there is no congruence, the asymptotic estimate does not depend on arithmetic but on geometry.

Forms of degree ≥ 3



Axel Thue
1863 - 1922



Kurt Mahler
1903 - 1988

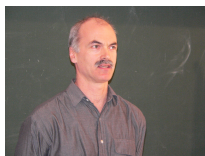
Let F be a binary form of degree ≥ 3 with nonzero discriminant.
Thue's Theorem. Let $m \in \mathbb{Z} \setminus \{0\}$. Then the set of $(x, y) \in \mathbb{Z}^2$ such that $F(x, y) = m$ is finite.

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

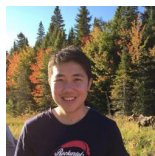
$$A_F := \iint_{|F(x,y)| \leq 1} dx dy$$

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

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

with $\beta_d < 2/d$ and where $W_F = W(\text{Aut} F)$ 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

[math.NT]

arXiv: 605.03427

The group $\text{Aut}F$ of a binary form F

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

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

A quadratic form has an infinite group of automorphisms. If an integer is represented by a quadratic form, it has many such representations.

If the degree of F is ≥ 3 , when an integer is represented by F , it has only finitely many such representations (*Thue's Theorem*).

Case of one cyclotomic form

Assume $d = \varphi(n) > 2$. Then the number of $m \leq N$ that are represented by the cyclotomic form Φ_n is asymptotically, as $N \rightarrow \infty$,

$$C_{\Phi_n} \cdot N^{2/d} + O_{n,\varepsilon}(N^{\beta_d+\varepsilon}),$$

with $\beta_d < 2/d$ and

$$C_{\Phi_n} = A_{\Phi_n} \cdot W_{\Phi_n}, \quad A_{\Phi_n} = \iint_{|\Phi_n(x,y)| \leq 1} dx dy,$$

$$W_{\Phi_n} = \frac{1}{|\text{Aut}\Phi_n|} = \begin{cases} 1/8 & \text{if } n \equiv 0 \pmod{4}, \\ 1/4 & \text{otherwise.} \end{cases}$$

Automorphisms of cyclotomic forms of degree ≥ 3

Let $n \geq 3$ be an integer. The group of automorphisms $\text{Aut} \Phi_n$ of $\Phi_n(X, Y)$ is

$$\text{Aut} \Phi_n = \begin{cases} \mathbb{D}_4 & \text{if } n \equiv 0 \pmod{4}, \\ \mathbb{D}_2 & \text{otherwise.} \end{cases}$$

where $\mathbb{D}_4$ (resp. $\mathbb{D}_2$) is the dihedral group of order 8 (resp. 4)

$$\mathbb{D}_4 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

$$\mathbb{D}_2 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}.$$



ETIENNE FOUVRY & MICHEL WALDSCHMIDT,

Sur la représentation des entiers par des formes cyclotomiques de grand degré, Bull. Soc. Math. France, **148** 2 (2020), 253 – 282.

arXiv: 1909.01892 [math.NT] Zbl 1455.11066

MR4124501

Corrigendum, **154** 2 (2026), 547–550.

Isomorphism of binary forms

Two binary forms F and G in $\mathbb{Z}[X, Y]$ of degree ≥ 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 $d \geq 3$ and nonzero
discriminant,



Étienne Fouvry

the number of integers m with $|m| \leq N$ that are represented
by F and by G is bounded by $O(N^\beta)$ with $\beta < 2/d$.

Isomorphisms among two cyclotomic forms

Let n_1 and n_2 be two positive integers satisfying $n_1 < n_2$. The following statements are equivalent.

- (1) We have $\varphi(n_1) = \varphi(n_2)$ and the two binary cyclotomic forms Φ_{n_1} and Φ_{n_2} are $\mathbb{Q}$ -isomorphic.
- (2) We have $\Phi_{n_2}(X, Y) = \Phi_{n_1}(X, -Y)$.
- (3) n_1 is odd and $n_2 = 2n_1$.
- (4) The two binary forms Φ_{n_1} and Φ_{n_2} represent the same integers.

The proof uses the following auxiliary result :

Let n be a positive integer. The torsion group (= group of roots of unity) of the cyclotomic field $\mathbb{Q}(\zeta_n)$ is cyclic, of order n if n is even and $2n$ if n is odd.

Cyclotomic forms of degree $\geq d$

Let $d \geq 4$ be a totient. For $N \rightarrow \infty$, the number of integers m with $1 \leq m \leq N$ such that there exists integers (n, x, y) satisfying

$$\varphi(n) \geq d, \Phi_n(x, y) = m \text{ and } \max\{|x|, |y|\} \geq 2$$

is asymptotically

$$C_d N^{2/d} + O(N^{\beta_d})$$

with $\beta_d < 2/d$ and

$$C_d = \sum_{\substack{n \not\equiv 2 \pmod{4} \\ \varphi(n)=d}} C_{\Phi_n}$$



ETIENNE FOUVRY & MICHEL WALDSCHMIDT,

Sur la représentation des entiers par des formes cyclotomiques de grand degré, *Bull. Soc. Math. France*, **148** 2 (2020), 253 – 282.

arXiv: 1909.01892 [math.NT] Zbl 1455.11066

MR4124501

Corrigendum, **154** 2 (2026), 547 – 550.

Our new example : multicyclotomic forms

We now consider *multicyclotomic forms*, which are products of distinct cyclotomic polynomials.

$$\phi_{n_1}(T)\phi_{n_2}(T) \cdots \phi_{n_k}(T)$$

with $1 \leq n_1 < \cdots < n_k$.

For $n_1 \geq 3$ this is a positive definite form.

For $n_1 \geq 1$, this form has a positive definite factor of comparatively large degree.



Etienne Fouvry & Michel Waldschmidt

Number of integers represented by families of binary forms —

IV : Multicyclotomy.

In preparation.

Multicyclotomic polynomials and binary forms

When $k \geq 0$, and $n_1, \dots, n_k$, satisfy $1 \leq n_1 < \dots < n_k$, we write $\mathbf{n} = (n_1, \dots, n_k)$ and

$$\phi_{\mathbf{n}}(T) = \phi_{n_1}(T)\phi_{n_2}(T) \dots \phi_{n_k}(T).$$

Such an index $\mathbf{n}$ is called a *composition* of length k : it is a strictly increasing partition of $n_1 + \dots + n_k$.

The degree of the polynomial $\phi_{\mathbf{n}}(T)$ is

$$\varphi(\mathbf{n}) := \varphi(n_1) + \dots + \varphi(n_k).$$

The associated homogeneous binary form is

$$\begin{aligned}\Phi_{\mathbf{n}}(X, Y) &= \Phi_{n_1}(X, Y)\Phi_{n_2}(X, Y) \dots \Phi_{n_k}(X, Y) \\ &= Y^{\varphi(\mathbf{n})}\phi_{\mathbf{n}}(X/Y) = X^{\varphi(\mathbf{n})}\phi_{\mathbf{n}}(Y/X).\end{aligned}$$

Multicyclotomic polynomials

For a (nonzero) monic polynomial $f \in \mathbb{Z}[T]$, the following properties are equivalent :

- (i) There exist integers $k \geq 0$, $n_1, \dots, n_k$, satisfying $1 \leq n_1 < \dots < n_k$, such that $f = \phi_{n_1} \cdots \phi_{n_k}$.
- (ii) There exists $n \geq 1$ such that f is a divisor of $T^n - 1$ in $\mathbb{Z}[T]$.
- (iii) f is a separable polynomial with Mahler's measure 1 :

$$\prod_{\alpha \in \mathbb{C}, f(\alpha)=0} \max\{1, |\alpha|\} = 1.$$

- (iv) All roots of f in $\mathbb{C}$ are simple and are roots of unity.

A *multicyclotomic polynomial* is a polynomial satisfying these properties.

Multicyclotomic forms of small degree

Degree 1

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

Degree 2

$$\begin{aligned} \Phi_3(X, Y) &= X^2 + XY + Y^2, & \Phi_6(X, Y) &= X^2 - XY + Y^2, \\ \Phi_4(X, Y) &= X^2 + Y^2, & \Phi_{1,2}(X, Y) &= X^2 - Y^2. \end{aligned}$$

Degree 3

$$\begin{aligned} \Phi_{1,3}(X, Y) &= X^3 - Y^3, & \Phi_{2,6}(X, Y) &= \Phi_{1,3}(X, -Y) \\ \Phi_{1,4}(X, Y) &= X^3 - X^2Y + XY^2 - Y^3, & \Phi_{2,4}(X, Y) &= \Phi_{1,4}(X, -Y), \\ \Phi_{1,6}(X, Y) &= X^3 + 2X^2Y + 2XY^2 + Y^3 & \Phi_{2,6}(X, Y) &= \Phi_{1,6}(X, -Y) \end{aligned}$$

Examples of multicyclotomic polynomials

$$\phi_{1,2}(T) = (T - 1)(T + 1) = T^2 - 1.$$

More generally, for m odd ≥ 1 ,

$$\phi_{m,2m}(T) = \phi_m(T)\phi_{2m}(T) = \phi_m(T^2).$$

For $m \geq 1$,

$$\prod_{d|m} \phi_d(T) = T^m - 1 \text{ and } \prod_{\substack{d|2m \\ d \nmid m}} \phi_d(T) = T^m + 1.$$

For $a_1 < \cdots < a_s$ powers of 2,

$$\phi_{2^{a_1}, \dots, 2^{a_s}}(T) = (T^{a_1} + 1) \cdots (T^{a_s} + 1).$$

Multicyclotomic forms of degree ≥ 2

The number of integers m with $m \leq N$ that are represented by one at least of the multicyclotomic forms $\Phi_{\mathbf{n}}$ with $\varphi(\mathbf{n}) \geq 2$ is asymptotically

$$\frac{3}{2}N + O\left(\frac{N}{\sqrt{\log N}}\right).$$

Indeed, an integer m is a difference of two squares if and only if it is not congruent to 2 modulo 4 :

If $m = 2\ell + 1$, then $m = (\ell + 1)^2 - \ell^2$

If $m = 4\ell$, then $m = (\ell + 1)^2 - (\ell - 1)^2$,

If $m = x^2 - y^2$, then $m \not\equiv 2 \pmod{4}$.

Hence the form $\Phi_{1,2}(X, Y) = X^2 - Y^2$ contributes to the main term, the other forms $\Phi_{\mathbf{n}}$ with $\varphi(\mathbf{n}) \geq 2$ (including Φ_3 , Φ_4 , Φ_6) only to the error term.

Diophantine equations $\Phi_{\mathbf{n}}(x, y) = m$ for $\varphi(\mathbf{n}) \geq d$

Main result for multicyclotomy (with EF) Let $d \geq 3$.

1. For each $m \in \mathbb{Z}$, the set of $(\mathbf{n}, x, y)$ with $\max\{|x|, |y|\} \geq 2$ and $\varphi(\mathbf{n}) \geq d$ such that $\Phi_{\mathbf{n}}(x, y) = m$ is finite; moreover, as $|m|$ tends to infinity, this number of $(\mathbf{n}, x, y)$ is bounded by

$$O_{d,\epsilon}(|m|^\epsilon).$$

2. The number of integers $m \in \mathbb{Z}$ with $|m| \leq N$ such that there exists $(x, y) \in \mathbb{Z}^2$ and $\mathbf{n}$ satisfying $\max\{|x|, |y|\} \geq 2$, $\varphi(\mathbf{n}) \geq d$ and $\Phi_{\mathbf{n}}(x, y) = m$ is asymptotically

$$\sum_{\mathbf{n} \in \mathcal{E}_d} |\text{Aut}(\Phi_{\mathbf{n}})|^{-1} A_{\Phi_{\mathbf{n}}} \cdot N^{2/d} + O_d(N^{\beta_d})$$

where $\beta_d < 2/d$ and $\mathcal{E}_d$ is a complete set of representative of the classes of compositions $\mathbf{n} = (n_1, \dots, n_k)$ satisfying $\varphi(\mathbf{n}) = d$, where $\mathbf{n}$ and $\tilde{\mathbf{n}}$ are in the same class if and only if the two binary forms $\Phi_{\mathbf{n}}(X, Y)$ and $\Phi_{\tilde{\mathbf{n}}}(X, Y)$ are $\mathbb{Q}$ -isomorphic.

Automorphisms of multicyclotomic forms

The group of automorphisms of a multicyclotomic form of degree ≥ 3 is a subgroup of the dihedral group $\mathbb{D}_4$ of order 8.

$$\mathbb{D}_4 = \left\{ \pm \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \pm \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

Number Theory Web Seminar. Thursday, April 16, 2026

Multicyclotomy

<https://www.ntwebseminar.org/previous-talks>

Link to recording (YouTube)

Link to slides

Isomorphisms of multicyclotomic forms

Examples of isomorphisms of multicyclotomic forms :

For m_1 and m_2 odd positive integers

$$\Phi_{m_1}(X, Y)\Phi_{m_2}(X, Y) \text{ and } \Phi_{2m_1}(X, Y)\Phi_{2m_2}(X, Y)$$

are isomorphic.

Also

$$\Phi_{m_1}(X, Y)\Phi_{2m_2}(X, Y) \text{ and } \Phi_{2m_1}(X, Y)\Phi_{m_2}(X, Y)$$

are isomorphic.

Isomorphisms among two multicyclotomic forms

Let $n_1, \dots, n_k$ and $\tilde{n}_1, \dots, \tilde{n}_{\tilde{k}}$ be positive integers satisfying

$$1 \leq n_1 < n_2 < \dots < n_k, \quad 1 \leq \tilde{n}_1 < \tilde{n}_2 < \dots < \tilde{n}_{\tilde{k}}.$$

Write $\mathbf{n} = (n_1, \dots, n_k)$ and $\tilde{\mathbf{n}} = (\tilde{n}_1, \dots, \tilde{n}_{\tilde{k}})$.

We say that $\mathbf{n}$ and $\tilde{\mathbf{n}}$ are *equivalent* if either they are equal, or if $k = \tilde{k}$ and there exists a permutation σ of $\{1, 2, \dots, k\}$ such that, for all $j \in \{1, \dots, k\}$, we have either $\tilde{n}_j = 2n_{\sigma(j)}$ with $n_{\sigma(j)}$ odd, or $\tilde{n}_j = n_{\sigma(j)}/2$ with $\tilde{n}_j$ odd.

Assume $\mathbf{n} \neq \tilde{\mathbf{n}}$. The following assertions are equivalent.

- (i) The two binary forms $\Phi_{\mathbf{n}}$ and $\Phi_{\tilde{\mathbf{n}}}$ are $\mathbb{Q}$ -isomorphic.
- (ii) We have $\Phi_{\tilde{\mathbf{n}}}(X, Y) = \Phi_{\mathbf{n}}(X, -Y)$.
- (iii) The two compositions $\mathbf{n}$ and $\tilde{\mathbf{n}}$ are equivalent.
- (iv) The two binary forms $\Phi_{\mathbf{n}}$ and $\Phi_{\tilde{\mathbf{n}}}$ represent the same integers.

A complete set of isomorphism classes of multicyclotomic forms

The set of multicyclotomic binary forms $\Phi_{\mathbf{n}}$ indexed by the following compositions $\mathbf{n} = (n_1, \dots, n_k)$ (with $k \geq 1$, $1 \leq n_1 < \dots < n_k$) is a complete system of representatives of the classes of multicyclotomic binary forms for the equivalence relation induced by the $\mathrm{GL}(2, \mathbb{Q})$ -isomorphism of binary forms :

- ▶ either one at least of the n_i is a multiple of 4,
- ▶ or all the even n_i are $\equiv 2 \pmod{4}$ and the number of indices $i \in \{1, \dots, k\}$ with $n_i \equiv 2 \pmod{4}$ is $< k/2$
- ▶ or else $k = 2\ell$ is even, $\mathbf{n}$ has ℓ odd components $a_1, \dots, a_\ell$ and ℓ even components $2b_1, \dots, 2b_\ell$ with $(a_1, \dots, a_\ell) \leq (b_1, \dots, b_\ell)$ for the lexicographic order.

Lower bound for $|\Phi_{\mathbf{n}}(x, y)|$ with $\varphi(\mathbf{n}) = d \geq 3$

What is specific to multicyclotomic forms?

When $\varphi(\mathbf{n}) = d \geq 3$ and $(x, y) \in \mathbb{Z}^2$ with $\Phi_{\mathbf{n}}(x, y) \neq 0$, we have

$$|\Phi_{\mathbf{n}}(x, y)| \geq \max\{|x|, |y|\}^{d/2}.$$

Our method works when we replace the set of multicyclotomic forms of degree ≥ 3 with any family $\mathcal{F}$ of binary forms of degree ≥ 3 and nonzero discriminant satisfying a similar lower bound.

Families of binary forms

Let $\mathcal{F}$ be a family of binary forms with nonzero discriminants and degree ≥ 3 . For $d \geq 3$, we denote by $\mathcal{F}_d$ the subset of $\mathcal{F}$ containing the forms of degree d (we always assume $\mathcal{F}_d$ to be finite) and by $\mathcal{F}_{\geq d}$ the subset of $\mathcal{F}$ containing the forms of degree $\geq d$.

We consider two Diophantine questions

1. Given $m \in \mathbb{Z}$ and $d \geq 3$, how many solutions are there to the equation $F(x, y) = m$ where the unknowns are $F \in \mathcal{F}_{\geq d}$ and $(x, y) \in \mathbb{Z} \times \mathbb{Z}$?
2. What is the asymptotic estimate, as $N \rightarrow \infty$, for the number of $m \in \mathbb{Z}$ satisfying $|m| \leq N$ such that there exists $F \in \mathcal{F}_{\geq d}$ and $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ with $\max\{|x|, |y|\} \geq 2$ satisfying $F(x, y) = m$?

Further examples

Binomials : $aX^d + bY^d$ with varying a, b, d .

Fewnomials :

$$a_0X^{kr} + a_1X^{k(r-1)}Y^k + \cdots + a_{r-1}X^kY^{k(r-1)} + a_rY^{kr}$$

with fixed $r \geq 1$ and varying $k, a_0, a_1, \dots, a_r$.

ICDEPRA - 2025 *On families of fewnomial binary forms*

October 13 - 17, Indian Statistical Institute (ISI) Delhi



Etienne Fouvry ; & Michel Waldschmidt

Number of integers represented by families of binary forms. I.

Acta Arith. 209, 219-267 (2023).

Zbl 1536.11071 arXiv: 2206.03733 [math.NT]



— II : Binomial forms.

Acta Arith. 214, 271-287 (2024).

Zbl 1557.11027 arXiv: 2306.02462 [math.NT]



— III : fewnomials.

Analysis Mathematica 2026. Published online 23 September 2026.

DOI: 10.1007/s10476-026-00192-y arXiv: 2509.08335 [math.NT]



— IV : Multicyclotomy In preparation.

Main result

Let μ be a real numbers such that $0 < \mu \leq 1$. Assume that, for all $d \geq 3$, all $F \in \mathcal{F}_d$ and all $(x, y) \in \mathbb{Z}^2$ with $\max\{|x|, |y|\} \geq 2$ and $F(x, y) \neq 0$, we have

$$|F(x, y)| \geq \max\{|x|, |y|\}^{\mu d}.$$

Then

(i) for all $d \geq 3$ and all $m \in \mathbb{Z}$, the set

$$\mathcal{G}_{\geq d}(\mathcal{F}, m) = \# \left\{ (F, x, y) \mid F \in \mathcal{F}_{\geq d}, (x, y) \in \mathbb{Z}^2, \right. \\ \left. \max\{|x|, |y|\} \geq 2, m = F(x, y) \right\}$$

is finite,

(ii) for all $d \geq 3$ and all $\epsilon > 0$, we have, as $|m| \rightarrow \infty$,

$$\mathcal{G}_{\geq d}(\mathcal{F}, m) = O_{\mathcal{F}, d, \epsilon}(|m|^{\epsilon}).$$

Main result (continued)

(iii) Assume further that two forms in the family $\mathcal{F}$ are $\mathbb{Q}$ -isomorphic if and only if they are equal. Then for every $d \geq 3$, there exists $\beta_d < 2/d$ such that, uniformly as $N \rightarrow \infty$, the number

$$\begin{aligned}\mathcal{R}_{\geq d}(\mathcal{F}, N) &:= \# \{m : 0 \leq |m| \leq N, \mathcal{G}_{\geq d}(\mathcal{F}, m) \neq 0\} \\ &= \# \{m : 0 \leq |m| \leq N, \text{ there exists} \\ &\quad F \in \mathcal{F}_{\geq d} \text{ and } (x, y) \in \mathbb{Z}^2 \text{ satisfying} \\ &\quad \max\{|x|, |y|\} \geq 2 \text{ and } F(x, y) = m\}\end{aligned}$$

satisfies

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

Forms with a large definite positive factor

Let μ_1 and μ_2 be two real numbers satisfying $0 < \mu_1 < 1$ and $0 < \mu_2 \leq 1$. Assume that each form F in the family $\mathcal{F}$ can be written $F = F_1 F_2$ where $\deg F_2 = d_2 \geq \mu_2 \deg F$ and F_2 is totally positive : $F_2(t, 1) > 0$ for all $t \in \mathbb{R}$. Assume F_2 satisfies

$$\min\{F_2(t, 1), F_2(1, t)\} \geq 2^{-\mu_1 d_2}$$

for all real numbers t in the range $-1 \leq t \leq 1$. Then the condition

$$|F(x, y)| \geq \max\{|x|, |y|\}^{\mu d}$$

is satisfied with $\mu = (1 - \mu_1)\mu_2$.

Examples of sequences of binary forms

It is easy to produce sequences of binary forms with a large positive definite factor for which the behavior of the above quantities $\mathcal{R}_{\geq d}(\mathcal{F}, N)$ satisfy prescribed almost arbitrary conditions.

Sequences of positive definite forms, d even ≥ 4 :

- ▶ The sequence of forms $X^d + \ell_d Y^d$
- ▶ The sequence of forms $(X - dY)^d + \ell_d Y^d$
- ▶ Sequence of forms $(v_d X - u_d Y)^d + \ell_d (h_d X - k_d Y)^d$

Sequences indexed by all $d \geq 3$:

- ▶ Forms with a large positive definite factor

$$(v_d X - u_d Y)^d + \ell_d (h_d X - k_d Y)^{d-1} (v_d X - u_d Y)$$

References

<https://webusers.imj-prg.fr/~michel.waldschmidt/>



Etienne Fouvry, Claude Levesque & Michel Waldschmidt
Representation of integers by cyclotomic binary forms.
Acta Arith. 184, No. 1, 67-86 (2018).
Zbl 1417.11028



Etienne Fouvry & Michel Waldschmidt
On the representation of integers by cyclotomic forms with large degree.
Bull. Soc. Math. Fr. 148, No. 2, 253-282 (2020).
Zbl 1455.11066



—
Number of integers represented by families of binary forms. I.
Acta Arith. 209, 219-267 (2023).
Zbl 1536.11071



— II : Binomial forms.
Acta Arith. 214, 271-287 (2024).
Zbl 1557.11027



— III : fewnomials.
Analysis Mathematica 2026. Published online 23 September 2026.
DOI: 10.1007/s10476-026-00192-y
arXiv: 2509.08335 [math.NT] HAL 05247823.



— IV : Multicyclotomy. In preparation.

Happy Birthday to my dear cousin Professor Sudesh Kaur Khanduja



Abu 'Ali al-Husayn ibn Sina (Avicenne)

⋮

Michel Chasles

H. A. (Hubert Anson) Newton

George David Birkhoff

Clarence Raymond Adams

Mahlon Marsh Day

Indar Singh Luthar

Sudesh Kaur Kanduja

Gaston Darboux

Émile Picard

Arnaud Denjoy

Charles Pisot

Yvette Amice

Jean Fresnel

Michel Waldschmidt