On some families of binary forms and the integers they represent

Michel Waldschmidt

Sorbonne Université
Institut de Mathématiques de Jussieu
Paris

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

An asymptotic estimate for the number of integers which are represented by a given binary form is due to Landau, Ramanujan and Bernays for positive definite quadratic forms and more recently by Stewart and Xiao for binary forms of higher degree. The purpose of this lecture is to consider the same problem for families of binary forms. In a joint work with E. Fouvry and C. Levesque, we gave an asymptotic estimate for the number of integers which are represented by a cyclotomic form. With E. Fouvry we pursued this study for other families of binary forms.

Étienne Fouvry

Claude Levesque


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.

2, 5, 13, 17, 29, 37, 41, 53, 61, 73...

https://oeis.org/A002313

The product of a sum of two squares is a sum of two squares.

Identity of Brahmagupta:

\[(a^2 + b^2)(c^2 + d^2) = e^2 + f^2\]

with either

\[e = ac - bd, \quad f = ad + bc\]

or

\[e = ac + bd, \quad f = ad - bc.\]
Sums of two squares

A positive integer is a sum of two squares if and only if each prime divisor congruent to 3 modulo 4 occurs with an even exponent.

Sums of two squares
https://oeis.org/A001481

1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, 34, 36, 37...

Not sums of two squares
https://oeis.org/A022544

3, 6, 7, 11, 12, 14, 15, 19, 21, 22, 23, 24, 27, 28, 30, 31, 33, 35, 38...

For $N \geq 1$, the number of $(x, y)$ with $x^2 + y^2 \leq N$ is $> N$ (take $\max\{|x|, |y|\} \leq \sqrt{N}$). If an integer $m$ is a sum of two squares, there are many solutions $(x, y)$ to the equation $x^2 + y^2 = m$: if $m$ has $s$ prime divisors which are congruent to 1 modulo 4, there are at least $2^{s-1}$ solutions.
The Landau–Ramanujan constant

Edmund Landau
1877 – 1938

Srinivasa Ramanujan
1887 – 1920

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

\[
C_{\Phi_4} = \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \mod 4} \left( 1 - \frac{1}{p^2} \right)^{-\frac{1}{2}} = 0.764223653589220\ldots
\]

Asymptotic expansion for the number of sums of two squares:
There exist real numbers \( \alpha_1, \alpha_2, \ldots \) such that, for any \( M \geq 0 \), the number of positive integers \( \leq N \) which are sums of two squares is asymptotically

\[
\frac{N}{\sqrt{\log N}} \left\{ C_{\Phi_4} + \frac{\alpha_1}{\log N} + \cdots + \frac{\alpha_M}{(\log N)^M} + O \left( \frac{1}{(\log N)^{M+1}} \right) \right\}.
\]
Positive definite quadratic forms

Let \( F(X, Y) = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y] \) be a quadratic form with nonsquare positive discriminant \( b^2 - 4ac \). 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 \( C_F N (\log N)^{-\frac{1}{2}} \).


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

Earlier results on binary quadratic forms:

Fermat, Lagrange, Legendre, Gauss.
Paul Bernays (1888 – 1977)


- 1913, Habilitation, University of Zürich, *On complex analysis and Picard’s theorem*, advisor Ernst Zermelo.
- 1912 – 1917, Zürich ; work with Georg Pólya, Albert Einstein, Hermann Weyl.
- 1917 – 1933, Göttingen, with David Hilbert. Studied with Emmy Noether, Bartel Leendert van der Waerden, Gustav Herglotz.
- 1936 —, ETH Zürich.

Higher degree

If a positive integer $m$ is represented by a given quadratic form, there are many such representations.

A quadratic form has infinitely many automorphisms, an irreducible binary form of higher degree has a finite group of automorphisms:

$$U = \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \text{GL}_2(\mathbb{Q}), \quad F(X_1, X_2) = F(u_1 X_1 + u_2 X_2, u_3 X_1 + u_4 X_2).$$

Given an integer $k \geq 3$, that a positive integer is a sum of two $k$–th powers in more than one way (not counting symmetries) is

- rare for $k = 3$,
- extremely rare for $k = 4$,
- maybe impossible for $k \geq 5$.
1729 : the taxicab number

The smallest positive integer which is sum of two cubes in two essentially different ways:

\[ 1729 = 10^3 + 9^3 = 12^3 + 1^3. \]


Hardy (1917) : 1729 is a rather dull number.

Littlewood : every positive integer was one of Ramanujan’s personal friends.


Beginning at the 1729th decimal digit of the transcendental number e, the next ten successive digits are 0719425863. It is the first occurrence of all ten digits consecutively in the decimal representation of e.
The sequence of Taxicab numbers

[OEIS A001235] Taxi-cab numbers: sums of 2 cubes in more than 1 way.

\[ 1729 = 10^3 + 9^3 = 12^3 + 1^3, \quad 4104 = 2^3 + 16^3 = 9^3 + 15^3, \ldots \]

1729, 4104, 13832, 20683, 32832, 39312, 40033, 46683, 64232, 65728, 110656, 110808, 134379, 149389, 165464, 171288, 195841, 216027, 216125, 262656, 314496, 320264, 327763, 373464, 402597, 439101, 443889, 513000, 513856, 515375, 525824, 558441, 593047, \ldots

If \( n \) is in this sequence, then \( nk^3 \) also, hence this sequence is infinite.
Another sequence of Taxicab numbers (Fermat)

[OEIS A011541] Hardy-Ramanujan numbers: $Ta(n)$ is the smallest number that is the sum of 2 positive integral cubes in $n$ ways.

http://mathworld.wolfram.com/TaxicabNumber.html

$Ta(1) = 2$,
$Ta(2) = 1729 = 10^3 + 9^3 = 12^3 + 1^3$,
$Ta(3) = 87539319 = 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3$,
$Ta(4) = 6963472309248$,
$Ta(5) = 48988659276962496$.

2003 : C. S. Calude, E. Calude and M. J. Dinneen. With high probability,

$$Ta(6) = 24153319581254312065344.$$ 

Fermat proved that numbers expressible as a sum of two positive integral cubes in $n$ different ways exist for any $n$.

Hardy and Wright, *An Introduction to the Theory of Numbers*, 1938.
Cubefree taxicab numbers

\[ 15170835645 = 517^3 + 2468^3 = 709^3 + 2456^3 = 1733^3 + 2152^3. \]

The smallest cubefree taxicab number with three representations was discovered by Paul Vojta in 1981 while he was a graduate student.

Stuart Gascoigne and Duncan Moore (2003):
\[ 1801049058342701083 = 92227^3 + 1216500^3 = 136635^3 + 1216102^3 = 341995^3 + 1207602^3 = 600259^3 + 1165884^3. \]

[OEIS A080642] Cubefree taxicab numbers: the smallest cubefree number that is the sum of 2 cubes in \( n \) ways.

https://en.wikipedia.org/wiki/Taxicab_number
Taxicabs and Sums of Two Cubes

If the sequence \((a_n)\) of cubefree taxicab numbers with \(n\) representations is infinite, then the Mordell-Weil rank of the elliptic curve \(x^3 + y^3 = a_n\) tends to infinity with \(n\).

Leonhard Euler
1707 – 1783

The smallest integer represented by $x^4 + y^4$ in two essentially different ways was found by Euler, it is $635318657 = 41 \times 113 \times 241 \times 569$.

[OEIS A216284] Number of solutions to the equation $x^4 + y^4 = n$ with $x \geq y > 0$.
An infinite family with one parameter is known for non trivial solutions to $x_1^4 + x_2^4 = x_3^4 + x_4^4$ (N. Elkies).
Sums of two higher powers

A necessary and sufficient condition for a prime number to be a sum of two squares is given by a congruence. For $k \geq 3$, there are not enough primes of the form $x^k + y^k$.

[OEIS A334520] Primes that are the sum of two cubes.

$$2, 7, 19, 37, 61, 127, 271, 331, 397, 547, 631, 919, 1657, \ldots$$

$$(7 = 2^3 + (-1)^3).$$

We believe this list to be infinite, but this is not known.

For an odd integer which is a sum of two 4th powers, each prime number not congruent to 1 modulo 8 has an even exponent. This necessary condition is not sufficient.

[OEIS A004831] Numbers that are the sum of at most 2 nonzero 4th powers.

$$0, 1, 2, 16, 17, 32, 81, 82, 97, 162, 256, 257, 272, 337, 512, 625, \ldots$$
Quartan primes

[OEIS A002645] Quartan primes: primes of the form $x^4 + y^4$, $x > 0$, $y > 0$.

The list of prime numbers which are sums of two 4th powers starts with 2, 17, 97, 257, 337, 641, 881, 1297, 2417, 2657, 3697, 4177, 4721, 6577, 10657, 12401, 14657, 14897, 15937, 16561, 28817, 38561, 39041, 49297, 54721, 65537, 65617, 66161, 66977, 80177, 83537, 83777, 89041, 105601, 107377, 119617, ...

It is not known whether this list is finite or not.

The largest known quartan prime is currently the largest known generalized Fermat prime: The 135365-digit $(145\,310^{65\,536})^4 + 1^4$.

[OEIS A002313] primes of the form $x^2 + y^2$,
[OEIS A002645] primes of the form $x^4 + y^4$,
[OEIS A006686] primes of the form $x^8 + y^8$,
[OEIS A100266] primes of the form $x^{16} + y^{16}$,
[OEIS A100267] primes of the form $x^{32} + y^{32}$. 
Primes of the form $X^2 + Y^4$ or $X^3 + 2Y^3$

However, it is known that there are infinitely many prime numbers of the form $X^2 + Y^4$ and also infinitely many prime numbers of the form $X^3 + 2Y^3$ – with the expected asymptotic order!


Representation of integers by a binary form of degree $\geq 3$

Let $F$ be a binary form of degree $d \geq 3$ with nonzero discriminant. For $N \geq 1$ denote by $R_F(N)$ the number of integers of absolute value at most $N$ which are represented by $F(X, Y)$.

Expected: $R_F(N) \sim C_F N^{2/d}$.

For $Z > 0$, the number $N_F(Z)$ of $(x, y) \in \mathbb{Z}^2$ such that $0 < |F(x, y)| \leq Z$ satisifies

$$N_F(Z) = A_F Z^{\frac{2}{d}} + O(Z^\theta)$$

as $Z \to \infty$, where $A_F$ is the area (Lebesgue measure) of the domain

$$\{(x, y) \in \mathbb{R}^2 \mid F(x, y) \leq 1\}.$$

$\theta = \frac{1}{d}$ if $F$ does not have a linear factor in $\mathbb{R}[X, Y]$,
$\theta = \frac{1}{d-1}$ otherwise.

Über die mittlere Anzahl der
Darstellungen grosser Zahlen durch
binäre Formen,

https://carma.newcastle.edu.au/
mahler/biography.html
Representation of integers by a binary form of degree 3 or 4

Cubic forms: $R_F(N) \sim C_F N^{2/3}$

  irreducible binary cubic forms, discriminant not a square: automorphism group $C_1$

  irreducible binary cubic forms, discriminant a square: automorphism group conjugate to $C_3$

Quartic forms: $R_F(N) \sim C_F N^{1/2}$

  irreducible binary quartic forms $ax^4 + bx^2y^2 + cy^4$: automorphism group conjugate to either $D_2$ or $D_4$. 

Christopher Hooley 1928 – 2018
Let $F$ be a binary form of degree $d \geq 3$ with nonzero discriminant. Recall

$$R_F(N) = \# \{ m \mid 1 \leq m \leq N, \text{ there exists } (x, y) \in \mathbb{Z}^2, F(x, y) = m \}.$$ 


Bennett, Dummigan and Wooley (1998) have obtained an asymptotic estimate for $R_F(N)$ when $F(X, Y) = aX^d + bY^d$ with $d \geq 3$ and $a$ and $b$ non-zero integers.
Let $F$ be a binary form of degree $d \geq 3$ with nonzero discriminant. There exists $C_F > 0$ and $\beta_d < \frac{2}{d}$ such that for $N \to \infty$, the number $R_F(N)$ of integers of absolute value at most $N$ which are represented by $F(X,Y)$ satisfies

$$R_F(N) = C_F N^{\frac{2}{d}} + O(N^{\beta_d}), \quad C_F = A_F W_F.$$

$W_F$ depends on the group of automorphisms of $F$ and $A_F$ is the area of the fundamental domain $\{(x,y) \in \mathbb{R}^2 \mid F(x,y) \leq 1\}$.


DOI: 10.4064/aa171012-24-12  

arXiv:1605.03427v2
Cameron L. Stewart, On integers represented by binary forms  
(University of Waterloo)

Thursday, October 15, 2020 (8am PDT, 11am EDT, 4pm BST, 5pm CEST, 6pm IDT, 8:30pm IST, 11pm China Standard Time)  
Friday, October 16, 2020 (2am AEDT, 4am NZDT)

Abstract: We shall discuss the following results which are joint work with Stanley Xiao.

Let $F(x,y)$ be a binary form with integer coefficients, degree $d(>2)$ and non-zero discriminant. There is a positive number $C(F)$ such that the number of integers of absolute value at most $Z$ which are represented by $F$ is asymptotic to $C(F)Z^{d/2}$.

Let $k$ be an integer with $k>1$ and suppose that there is no prime $p$ such that $p^k$ divides $F(a,b)$ for all pairs of integers $(a,b)$. Then, provided that $k$ exceeds $7d/18$ or $(k,d)$ is $(2,6)$ or $(3,8)$, there is a positive number $C(F,k)$ such that the number of $k$-free integers of absolute value at most $Z$ which are represented by $F$ is asymptotic to $C(F,k)Z^{d/2}$.

Link to recording (118MB)

Link to lecture notes (PDF)
ON THE REPRESENTATION OF INTEGERS BY BINARY FORMS

C.L. Stewart
cstewart@uwaterloo.ca

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

Number Theory Web Seminar, October 15, 2020
ON THE REPRESENTATION OF INTEGERS BY BINARY FORMS

C.L. Stewart
cstewart@uwaterloo.ca

Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada

Number Theory Web Seminar, October 15, 2020
Cyclotomic polynomials

Recall the cyclotomic polynomials, defined by induction:

\[ \phi_1(t) = t - 1, \quad t^n - 1 = \prod_{d \mid n} \phi_d(t), \quad \phi_n(t) = \frac{t^n - 1}{\prod_{d \neq n \mid n} \phi_d(t)} \]

\[ \phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1, \]

\[ \phi_2(t) = t + 1, \quad \phi_3(t) = t^2 + t + 1, \quad \phi_5(t) = t^4 + t^3 + t^2 + t + 1, \]

\[ \phi_4(t) = t^2 + 1, \quad \phi_6(t) = t^2 - t + 1, \quad \phi_8(t) = t^4 + 1, \quad \phi_{12}(t) = t^4 - t^2 + 1. \]

Also, for \( m \) odd,

\[ \phi_{2m}(t) = \phi_m(-t). \]

The degree of \( \phi_n(t) \) is \( \varphi(n) \), where \( \varphi \) is the Euler totient function.
Cyclotomic forms

For $n \geq 1$, define

$$\Phi_n(X, Y) = Y^{\varphi(n)} \phi_n(X/Y).$$

This is a binary form in $\mathbb{Z}[X, Y]$ of degree $\varphi(n)$.

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

$$\Phi_3(X, Y) = X^2 + XY + Y^2, \quad \Phi_4(X, Y) = X^2 + Y^2,$$

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

$$\Phi_5(X, Y) = X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4,$$

$$\Phi_8(X, Y) = X^4 + Y^4, \quad \Phi_{12}(X, Y) = X^4 - X^2Y^2 + Y^4,$$

$$\Phi_{10}(X, Y) = \Phi_5(X, -Y) = X^4 - X^3Y + X^2Y^2 - XY^3 + Y^4.$$
Integers represented by a given cyclotomic form $\Phi_n$

The result of Stewart and Xiao gives, for the number $R_{\Phi_n}(N)$ of integers $m \leq N$ represented by $\Phi_n$ for a given $n$ with $\varphi(n) = d \geq 4$,

$$R_{\Phi_n}(N) = C_{\Phi_n}N^{\frac{2}{d}} + O_\varepsilon(N^{\beta_d + \varepsilon}) \quad \text{with} \quad C_{\Phi_n} = w_n A_{\Phi_n}.$$ 

Here

$$\beta_d = \begin{cases} \frac{3}{d\sqrt{d}} & \text{for } d = 4, 6, 8, \\ \frac{1}{d} & \text{for } d \geq 10 \end{cases} \quad \text{and} \quad A_{\Phi_n} = \iint_{\Phi_n(x,y) \leq 1} dx dy.$$ 

The group of automorphisms of $\Phi_n$ is isomorphic either to the dihedral group $\mathbb{D}_2$ with 4 elements or to the dihedral group $\mathbb{D}_4$ with 8 elements:

$$\text{Aut } \Phi_n = \begin{cases} \mathbb{D}_4 & \text{if } 4 \text{ divides } n, \\ \mathbb{D}_2 & \text{otherwise}, \end{cases} \quad w_n = \begin{cases} \frac{1}{8} & \text{if } 4 \text{ divides } n, \\ \frac{1}{4} & \text{otherwise}. \end{cases}$$
The cyclotomic fundamental domain

The cyclotomic fundamental domain of the binary form $\Phi_n$ is

$$O_n = \{(x, y) \in \mathbb{R}^2 \mid \Phi_n(x, y) \leq 1\}.$$

Let $\varepsilon > 0$. There exists $n_0 = n_0(\varepsilon)$ such that, for $n \geq n_0$, $O_n$ contains the square centered at the origin with side $2 - n^{-1+\varepsilon}$ and is contained in the square centered at the origin with side $2 + n^{-1+\varepsilon}$. Hence

$$\lim_{n \to \infty} A_{\Phi_n} = 4.$$

The cyclotomic fundamental domain $O_n$ is convex if and only if $n$ is either a prime, or twice a prime, or a power of 2.
Numbers represented by cyclotomic forms of degree $\geq 2$

**Theorem 1.** The number of integers $m \leq N$ which are represented by at least one of the binary cyclotomic forms $\Phi_n(X, Y)$ with $n \geq 3$ is asymptotically

$$
\alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O \left( \frac{N}{\log N} \right)
$$

as $N \to \infty$.

The main term

$$
\alpha \frac{N}{\sqrt{\log N}} \quad \text{with} \quad \alpha = C_{\Phi_4} + C_{\Phi_3} = 1.403\,133\,059\,034 \ldots
$$

occurs from the contributions of the quadratic forms $\Phi_4$ and $\Phi_3$.

The next term

$$
-\beta \frac{N}{(\log N)^{\frac{3}{4}}} \quad \text{with} \quad \beta = 0.302\,316\,142\,357 \ldots
$$

occurs from the contribution of the numbers which are represented by the form $\Phi_4$ and also by the form $\Phi_3$.

The error term is sharp; it takes into account all binary cyclotomic forms of degree $\geq 4$. 
The quadratic form $\Phi_3(X, Y) = X^2 + XY + Y^2$

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. The quadratic form $X^2 + 3Y^2$ represents the same numbers.

Primes of the form $3m + 1$:

https://oeis.org/A002476

7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97, 103, 109 \ldots

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 $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, $1 + \zeta_3 + \zeta_3^2 = 0$:

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

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 the prime divisors of $m$ congruent to 2 modulo 3 occur with an even exponent.

Numbers represented by the quadratic form $X^2 + XY + Y^2$:

https://oeis.org/A003136

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

Numbers not represented by the quadratic form $X^2 + XY + Y^2$:

https://oeis.org/A034020

2, 5, 6, 8, 10, 11, 14, 15, 17, 18, 20, 22, 23, 24, 26, 29, 30…
Asymptotic expansion for Loeschian numbers

The number of positive integers \( \leq N \) which are represented by the quadratic form \( X^2 + XY + Y^2 \) is asymptotically \( C_{\Phi_3} N (\log N)^{-\frac{1}{2}} \), where

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

[OEIS A301429] Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers. The first decimal digits of \( C_{\Phi_3} \) are

\[
C_{\Phi_3} = 0.638909405445343882254942674\ldots
\]

There exist real numbers \( \alpha'_1, \alpha'_2, \ldots \) such that, for any \( M \geq 0 \), the number of positive integers \( \leq N \) which are represented by the form \( X^2 + XY + Y^2 \) is asymptotically

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


https://arxiv.org/abs/1908.06808v1
Loeschian numbers which are sums of two squares

An integer \( m \geq 1 \) is simultaneously of the forms

\[
m = \Phi_4(x, y) = x^2 + y^2 \text{ and } m = \Phi_3(u, v) = u^2 + uv + v^2
\]

if and only if its prime divisors not congruent to 1 modulo 12 occur with an even exponent.

Sequence: \( \text{https://oeis.org/A155563} \)

\[
1, 4, 9, 13, 16, 25, 36, 37, 49, 52, 61, 64, 73, 81, 97, 100 \ldots
\]

The number of Loeschian integers \( \leq N \) which are sums of two squares is asymptotically

\[
\frac{N}{(\log N)^{\frac{3}{4}}} \left\{ \beta + \frac{\alpha'_{1}}{\log N} + \cdots + \frac{\alpha'_{M}}{(\log N)^{M}} + O \left( \frac{1}{(\log N)^{M+1}} \right) \right\}.
\]

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

\[
\beta = 0.302316142357065637947769900\ldots \quad \text{[OEIS A301430]}
\]


\( \text{https://arxiv.org/abs/1908.06808v1} \)
The error term in Theorem 1

Recall Theorem 1 which gives an asymptotic estimate for the number of integers \( m \leq N \) which are represented by one at least of the binary cyclotomic forms \( \Phi_n(X, Y) \) of degree \( \geq 2 \).

**Theorem 1.** The number of integers \( m \leq N \) which are represented by at least one of the binary cyclotomic forms \( \Phi_n(X, Y) \) with \( n \geq 3 \) is asymptotically

\[
\alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O \left( \frac{N}{\log N} \right)
\]

as \( N \to \infty \).

\[\alpha = C_{\Phi_4} + C_{\Phi_3} = 1.403\ 133\ 059\ 034\ \ldots\]

\[\beta = 0.302\ 316\ 142\ 357\ \ldots\]
The error term

Any prime number \( p \) is represented by a cyclotomic binary form:

\[
\Phi_{pr}(1, 1) = \phi_{pr}(1) = \phi_{2pr}(-1) = p \quad \text{for} \quad r \geq 1 \quad \text{and} \quad p \quad \text{an odd prime.}
\]

For any \( d \geq 4 \) the number of integers \( \leq N \) represented by one at least of the cyclotomic binary forms of degree \( \geq d \) is asymptotic to the number \( \pi(N) \) of primes \( \leq N \).

We now count the representations \( \Phi_n(x, y) \) with \( \max\{|x|, |y|\} \geq 2 \).

**Theorem 1'.** The number of integers \( m \leq N \) for which there exists \( n \geq 3 \) and \( (x, y) \in \mathbb{Z}^2 \) with \( \max(|x|, |y|) \geq 2 \) and \( m = \Phi_n(x, y) \), is asymptotically

\[
\alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O \left( \frac{N}{(\log N)^{\frac{3}{2}}} \right)
\]

as \( N \to \infty \).
\( \mathcal{A}_d(N) \) and \( \mathcal{A}_{\geq d}(N) \)

Define, for \( d \geq 4 \),

\[
\mathcal{A}_d(N) = \#\{m \mid 1 \leq m \leq N, \text{ there exists } n \geq 3 \text{ and } (x, y) \in \mathbb{Z}^2 \text{ with } \varphi(n) = d \text{ and } \Phi_n(x, y) = m\}
\]

and

\[
\mathcal{A}_{\geq d}(N) = \#\{m \mid 1 \leq m \leq N, \text{ there exists } n \geq 3 \text{ and } (x, y) \in \mathbb{Z}^2 \text{ with } \max\{|x|, |y|\} \geq 2, \varphi(n) \geq d \text{ and } \Phi_n(x, y) = m\}.
\]

Theorem 1’ states: \textit{Asymptotically, as } N \rightarrow \infty,\textit{ }

\[
\mathcal{A}_{\geq 2}(N) = \alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right).
\]
Contribution of the forms of degree $\geq 4$

It remains to be shown that

$$A_{\geq 4}(N) = O\left(\frac{N}{(\log N)^{3/2}}\right).$$

Each individual form $\Phi_n(X, Y)$ with $\varphi(n) = d \geq 4$ contributes only to the error term in Theorem 1’ with $O(N^{2/d})$.

But there are infinitely many such forms. We need a uniform estimate; the next one will be good enough.

**Proposition 2.** Let $d \geq 4$. For $d \geq 2$ and $N \to \infty$, the number $A_{\geq d}(N)$ of $m \leq N$ for which there exists $n$ and $(x, y) \in \mathbb{Z}^2$ with $\varphi(n) \geq d$, $\max(|x|, |y|) \geq 2$ and $m = \Phi_n(x, y)$ is bounded by

$$29N^{2/d}(\log N)^{1.161}.$$
Lower bound for norm forms of CM fields

For $n \geq 3$, the polynomial $\phi_n(t)$ has integer coefficients, hence real coefficients, and no real root, hence it takes only positive values (and its degree $\varphi(n)$ is even).

For $n \geq 3$ and $t \in \mathbb{R}$,
\[
\phi_n(t) \geq 2^{-\varphi(n)} \max\{1, |t|\} \varphi(n).
\]

K. Győry, L. Lovász, 


For $n \geq 3$ and $(x, y) \in \mathbb{Z}^2$,
\[
\Phi_n(x, y) \geq 2^{-\varphi(n)} \max\{|x|, |y|\} \varphi(n).
\]
Lower bound for $\phi_n(t)$

The lower bound $\Phi_n(x, y) \geq 2^{-\varphi(n)} \max\{|x|, |y|\} \varphi(n)$ is useful only if $\max\{|x|, |y|\} \geq 3$. We need a refinement of the result of K. Győry & L. Lovász for the special case of cyclotomic forms.

**Proposition 3.** For $n \geq 3$,

$$\inf_{t \in \mathbb{R}} \phi_n(t) \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

Hence

$$\Phi_n(x, y) \geq \left(\frac{\sqrt{3}}{2} \max\{|x|, |y|\}\right)^{\varphi(n)}.$$

**Corollary.** Let $m$ be a positive integer and let $n, x, y$ be rational integers satisfying $n \geq 3$, $\max(|x|, |y|) \geq 2$ and $\Phi_n(x, y) = m$. Then

$$\max\{|x|, |y|\} \leq \frac{2}{\sqrt{3}} m^{1/\varphi(n)}, \text{ hence } \varphi(n) \leq \frac{2}{\log 3} \log m.$$

As a consequence, $n$ is bounded

$$n < 5.383(\log m)^{1.161}.$$
Numbers represented by two nonisomorphic binary forms of the same degree

Two binary forms $F_1$ and $F_2$ are isomorphic if there exists $\begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix}$ in $\text{GL}_2(\mathbb{Q})$ such that $F_1(X_1, X_2) = F_2(u_1 X_1 + u_2 X_2, u_3 X_1 + u_4 X_2)$. For $B \geq 2$, let $\mathcal{N}_{F_1, F_2}(B)$ be the number of elements in the set

$$\left\{ (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \mid \max_{i=1,2,3,4} |x_i| \leq B, \ F_1(x_1, x_2) = F_2(x_3, x_4) \right\}.$$ 

**Theorem 2.** Let $F_1$ and $F_2$ be two nonisomorphic binary forms of the same degree $d \geq 3$. Assume that their discriminants are nonzero. Then for any $\varepsilon > 0$ we have

$$\mathcal{N}_{F_1, F_2}(B) = O(B^{\gamma_d + \varepsilon}),$$

with

$$\gamma_d = \begin{cases} \frac{2}{3} + \frac{73}{36\sqrt{3}} & \text{if } d = 3, \\ \frac{1}{2} + \frac{9}{4\sqrt{d}} & \text{if } 4 \leq d \leq 20, \\ 1 & \text{for } d \geq 21. \end{cases}$$
Sketch of proof of Theorem 2.

The proof is based on results and ideas of Heath-Brown, Hooley, Salberger, Stewart and Xiao.

Salberger, P. – *Rational points of bounded height on projective surfaces.*

The goal is to give an upper bound for the number of integral points \((x_1, x_2, x_3, x_4) \in \mathbb{Z}^4\) with \(\max_{i=1,2,3,4} |x_i| \leq B\) on the hypersurface

\[
X : \quad F_1(X_1, X_2) = F_2(X_3, X_4).
\]

One estimates the number of such points for which the projective point \((x_1 : x_2 : x_3 : x_4)\) does not lie on a complex projective line contained in \(X\) by using a result due to P. Salberger. This produces the main term in the estimate.

Next one estimates the number of points for which the projective point \((x_1 : x_2 : x_3 : x_4)\) lies on a projective line contained in \(X\), and one uses an upper bound for the number of these lines. This produces an error term \(O(B)\).
Corollary. Let \( n_1 \) and \( n_2 \) be two positive integers such that \( \varphi(n_1) = \varphi(n_2) = d \geq 4 \). Assume that the two cyclotomic binary forms \( \Phi_{n_1} \) and \( \Phi_{n_2} \) are not isomorphic. Then for any \( \varepsilon > 0 \) the number of \( m \leq N \) such that there exists \( (a, b) \) and \( (c, d) \) with

\[
m = \Phi_{n_1}(a, b) = \Phi_{n_2}(c, d)
\]

is bounded by

\[
O_{d, \varepsilon}(N^{\eta_d + \varepsilon})
\]

with

\[
\eta_d = \frac{\gamma_d}{d} = \begin{cases} 
\frac{1}{2d} + \frac{9}{4d\sqrt{d}} & \text{if } 4 \leq d \leq 20, \\
\frac{1}{d} & \text{for } d \geq 22.
\end{cases}
\]
Isomorphic cyclotomic binary forms

**Corollary.** For $n_1$ and $n_2$ positive integers with $n_1 < n_2$, the following conditions are equivalent:

1. $\varphi(n_1) = \varphi(n_2)$ and the two binary forms $\Phi_{n_1}$ and $\Phi_{n_2}$ are isomorphic.
2. The two binary forms $\Phi_{n_1}$ and $\Phi_{n_2}$ represent the same integers.
3. $n_1$ is odd and $n_2 = 2n_1$.

**Proof.**

We may assume $n_1 \geq 3$.

1. $\Rightarrow$ 3 If $\Phi_{n_1}$ and $\Phi_{n_2}$ are isomorphic, the primitive roots of unity $\zeta_{n_1}$ and $\zeta_{n_2}$ are related by

$$\zeta_{n_1} = \frac{u_1 \zeta_{n_2} + u_2}{u_3 \zeta_{n_2} + u_4} \quad \text{with} \quad \begin{pmatrix} u_1 & u_2 \\ u_3 & u_4 \end{pmatrix} \in \text{GL}_2(\mathbb{Q}),$$

hence $\mathbb{Q}(\zeta_{n_1}) = \mathbb{Q}(\zeta_{n_2})$. The torsion subgroup of $\mathbb{Q}(\zeta_n)^\times$ is cyclic of order $n$ (resp. $2n$) if $n$ is even (resp. odd).

3. $\Rightarrow$ 2 For $m$ odd, $\phi_{2m}(t) = \phi_m(-t)$.

2. $\Rightarrow$ 1 Follows from the corollary above on $\Phi_{n_1}(a, b) = \Phi_{n_2}(c, d)$. □
Even integers not represented by Euler totient function

Let us call *totient* a positive integer which is a value of Euler totient function $\varphi$. Let $d$ be a totient and $d^{\dagger}$ the next totient $> d$.

Always $d + 2 \leq d^{\dagger} < 2d$.

The list of even integers which are not values of Euler $\varphi$ function (i.e., for which $C_d = 0$) starts with

14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98, 114, 118, 122, 124, 134, 142, 146, 152, 154, 158, 170, 174, 182, 186, 188, 194, 202, 206, 214, 218, 230, 234, 236, 242, 244, 246, 248, 254, 258, 266, 274, 278, 284, 286, 290, 298, 302, 304, 308, 314, 318, ...  

[OEIS A005277] Nontotients: even $n$ such that $\varphi(m) = n$ has no solution.


**Ford, K**, *The number of solutions of $\varphi(x) = m$*, Ann. of Math. (2) (150) (1999), no. 1, 283–311.
Theorem 3. Let $d \geq 4$. As $N \to \infty$, the number $A_{\geq d}(N)$ of integers $m \leq N$ for which there exist $n$ and $(x, y)$ with $\Phi_n(x, y) = m$, $\varphi(n) \geq d$ and $\max\{|x|, |y|\} \geq 2$, is asymptotically

$$A_{\geq d}(N) = C_d N^{\frac{2}{d}} + \begin{cases} O_\varepsilon(N^{\frac{13}{32} + \varepsilon}) & \text{for } d = 4, \\ O(N^{\frac{2}{d^\dagger}}) & \text{for } d \geq 6, \end{cases}$$

with

$$C_d = \sum_n C_{\Phi_n},$$

where the sum is over the set of integers $n$ such that $\varphi(n) = d$ and $n$ is not congruent to $2$ modulo $4$.

If $d \geq 6$ and $d^\dagger = d + 2$, then the error term is sharp.
Optimality of the error term when $d^\dagger = d + 2$

Assume $d \geq 4$ and $d + 2$ are totients. Then, among the $\Phi_m(u, v)$ with $\varphi(m) = d + 2$, a positive proportion of them is not of the form $\Phi_n(a, b)$ with $\varphi(n) = d$: there exists $v_d > 0$ such that, for sufficiently large $N$,

$$A_{\geq d}(N) \geq A_d(N) + v_d N^{\frac{2}{d+2}}.$$

**Lemma (Confinement).** Let $n \geq 2$ and let $p$ be a prime number dividing $n$. Then for all $a, b$ in $\mathbb{Z}$, we have

$$\Phi_n(a, b) \equiv 0, 1 \mod p.$$ 

Further similar results are needed modulo 4 and 9.

On some families of binary forms and the integers they represent

Michel Waldschmidt

Sorbonne Université
Institut de Mathématiques de Jussieu
Paris

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