April 18–20, 2018 4th Mini Symposium of the Roman Number Theory Association (RNTA)

Representation of integers by cyclotomic binary forms

by

Michel Waldschmidt

Abstract

The homogeneous form $\Phi_n(X,Y)$ of degree $\varphi(n)$ which is associated with the cyclotomic polynomial $\phi_n(t)$ is dubbed a cyclotomic binary form. A positive integer $m \geq 1$ is said to be representable by a cyclotomic binary form if there exist integers n, x, y with $n \geq 3$ and $\max\{|x|,|y|\} \geq 2$ such that $\Phi_n(x,y) = m$. These definitions give rise to a number of questions that we are going to address.

This is a joint work with Étienne Fouvry and Claude Levesque [FLW].

1 Cyclotomic polynomials

1.1 Definition

The sequence $(\phi_n(t))_{n\geq 1}$ can be defined by induction:

$$\phi_1(t) = t-1, \qquad t^n - 1 = \prod_{d|n} \phi_d(t).$$

Hence,

$$\phi_n(t) = \frac{t^n-1}{\displaystyle\prod_{\substack{d\neq n\\ d|n}} \phi_d(t)}\cdot$$

When p is prime, from

$$t^p - 1 = (t-1)(t^{p-1} + t^{p-2} + \cdots + t + 1) = \phi_1(t)\phi_p(t),$$

one deduces $\phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$. For instance

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

Further examples are

$$\phi_4(t) = \frac{t^4-1}{\phi_1(t)\phi_2(t)} = \frac{t^4-1}{t^2-1} = t^2+1 = \phi_2(t^2),$$

$$\phi_6(t) = \frac{t^6-1}{\phi_1(t)\phi_2(t)\phi_3(t)} = \frac{t^6-1}{(t+1)(t^3-1)} = \frac{t^3+1}{t+1} = t^2-t+1 = \phi_3(-t).$$

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

1.2 Cyclotomic polynomials and roots of unity

For $n \geq 1$, if ζ is a primitive n–th root of unity, we have, in $\mathbb{C}[t]$,

$$\phi_n(t) = \prod_{\gcd(j,n)=1} (t - \zeta^j).$$

For $n \geq 1$, $\phi_n(t)$ is the irreducible polynomial over $\mathbb{Q}$ of the primitive n–th roots of unity.

Let K be a field and let n be a positive integer. Assume that K has characteristic either 0 or else a prime number p prime to n. Then the polynomial $\phi_n(t)$ is separable over K and its roots in K are exactly the primitive n–th roots of unity which belong to K.

1.3 Properties of $\phi_n(t)$

• For $n \geq 2$ we have

$$\phi_n(t) = t^{\varphi(n)} \phi_n(1/t)$$

• Let $n = p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \dots, p_r$ are different primes, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \dots, r$ and $r \geq 1$. Denote by $R = p_1 \cdots p_r$ the radical of n. Then, $\phi_n(t) = \phi_R(t^{n/R})$. For instance $\phi_{2^e}(t) = t^{2^{e-1}} + 1$ for $e \geq 1$.

• Let $n = 2m$ with m odd ≥ 3. Then $\phi_n(t) = \phi_m(-t)$.

$\boxed{\phi_n(1)}$

For $n \geq 2$, we have $\phi_n(1) = e^{\Lambda(n)}$, where the von Mangoldt function Λ is defined for $n \geq 1$ as

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 0 & \text{otherwise.} \end{cases}$$

In other terms, for $n \geq 2$, we have

$$\phi_n(1) = \begin{cases} p & \text{if } n = p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise } (\omega(n) \geq 1). \end{cases}$$

$\boxed{\phi_n(-1)}$

For $n \geq 3$,

$$\phi_n(-1) = \begin{cases} 1 & \text{if } n \text{ is odd;} \\ \phi_{n/2}(1) & \text{if } n \text{ is even.} \end{cases}$$

In other terms, for $n \geq 3$,

$$\phi_n(-1) = \begin{cases} p & \text{if } n = 2p^r \text{ with } p \text{ prime and } r \geq 1; \\ 1 & \text{otherwise.} \end{cases}$$

Hence, $\phi_n(-1) = 1$ when n is odd or when $n = 2m$ where m has at least two distinct prime divisors.

1.4 Lower bound for $\phi_n(t)$

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

Lemma 1. *For $n \geq 3$ and $t \in \mathbb{R}$, we have*

$$\phi_n(t) \geq 2^{-\varphi(n)}.$$

Consequence: from $\phi_n(t) = t^{\varphi(n)}\phi_n(1/t)$ we deduce, for $n \geq 3$ and $t \in \mathbb{R}$,

$$\phi_n(t) \geq 2^{-\varphi(n)} \max\{1, |t|\}^{\varphi(n)}. \tag{1.1}$$

Hence, $\phi_n(t) \geq 2^{-\varphi(n)}$ for $n \geq 3$ and $t \in \mathbb{R}$.

Proof of Lemma 1. Let ζ_n be a primitive n-th root of unity in $\mathbb{C}$; then

$$\phi_n(t) = \mathrm{Norm}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t - \zeta_n) = \prod_\sigma (t - \sigma(\zeta_n)),$$

where σ runs over the embeddings $\mathbb{Q}(\zeta_n) \to \mathbb{C}$. We have

$$|t - \sigma(\zeta_n)| \geq |\mathrm{Im}(\sigma(\zeta_n))| > 0 \quad \text{and} \quad (2i)\mathrm{Im}(\sigma(\zeta_n)) = \sigma(\zeta_n) - \overline{\sigma(\zeta_n)} = \sigma(\zeta_n - \overline{\zeta_n}).$$

Now $(2i)\mathrm{Im}(\zeta_n) = \zeta_n - \overline{\zeta_n} \in \mathbb{Q}(\zeta_n)$ is an algebraic integer, hence,

$$2^{\varphi(n)}\phi_n(t) \geq |\mathrm{Norm}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}((2i)\mathrm{Im}(\zeta_n))| \geq 1.$$

□

2 The cyclotomic binary forms

2.1 Definition

For $n \geq 2$, define

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

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

2.2 Lower bound for $\Phi_n(x, y)$

From (1.1) we deduce

Lemma 2 ([G])**.** *For $n \geq 3$ and $(x, y) \in \mathbb{Z}^2$,*

$$\Phi_n(x, y) \geq 2^{-\varphi(n)} \max\{|x|, |y|\}^{\varphi(n)}.$$

Therefore, if $\Phi_n(x, y) = m$, then

$$\max\{|x|, |y|\} \leq 2m^{1/\varphi(n)}. \tag{2.1}$$

As a consequence, if $\max\{|x|, |y|\} \geq 3$, then n is bounded:

$$\varphi(n) \leq \frac{\log m}{\log(3/2)}.$$

2.3 Generalization to CM fields

The same proof yields:

Proposition 3 ([GL, G]). *Let K be a CM field of degree d over $\mathbb{Q}$. Let $\alpha \in K$ be such that $K = \mathbb{Q}(\alpha)$; let f be the irreducible polynomial of α over $\mathbb{Q}$ and let $F(X,Y) = Y^d f(X/Y)$ the associated homogeneous binary form:*

$$f(t) = a_0 t^d + a_1 t^{d-1} + \cdots + a_d, \qquad F(X,Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_d Y^d.$$

For $(x,y) \in \mathbb{Z}^2$ we have

$$x^d \le 2^d a_d^{d-1} F(x,y) \quad \textit{and} \quad y^d \le 2^d a_0^{d-1} F(x,y).$$

The estimate of Proposition 3 is best possible: let $n \ge 3$, not of the form p^a nor $2p^a$ with p prime and $a \ge 1$, so that $\phi_n(1) = \phi_n(-1) = 1$. Then the binary form $F_n(X,Y) = \Phi_n(X, Y - X)$ has degree $d = \varphi(n)$ and $a_0 = a_d = 1$. For $x \in \mathbb{Z}$ we have $F_n(x, 2x) = \Phi_n(x,x) = x^d$. Hence, for $y = 2x$, we have

$$y^d = 2^d a_0^{d-1} F(x,y).$$

2.4 Improvement of Győry's estimate for binary cyclotomic forms [FLW]

We improve the upper bound (2.1) in order to have a non trivial result also for $\max\{|x|,|y|\} = 2$.

Theorem 4 ([FLW]). *Let m be a positive integer and let n, x, y be rational integers satisfying $n \ge 3$, $\max\{|x|,|y|\} \ge 2$ and $\Phi_n(x,y) = m$. Then*

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

These estimates are optimal, since for $\ell \ge 1$, we have $\Phi_3(\ell, -2\ell) = 3\ell^2$. If we assume $\varphi(n) > 2$, which means $\varphi(n) \ge 4$, then

$$\varphi(n) \le \frac{4}{\log 11} \log m$$

which is best possible since $\Phi_5(1,-2) = 11$.

2.5 Lower bound for the cyclotomic polynomials

Theorem 4 is equivalent to the following result:

Proposition 5 ([FLW]). *For $n \ge 3$ and $t \in \mathbb{R}$,*

$$\phi_n(t) \ge \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

2.6 The sequence $(c_n)_{n\geq 3}$

Define

$$c_n = \inf_{t\in\mathbb{R}} \phi_n(t) \qquad (n \geq 3).$$

Hence, for x and y in $\mathbb{Z}$ and for $n \geq 3$ we have

$$\Phi_n(x,y) \geq c_n \max\{|x|,|y|\}^{\varphi(n)}.$$

According to Proposition 5, for $n \geq 3$ we have

$$c_n \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$

Let $n \geq 3$. Write $n = 2^{e_0} p_1^{e_1} \cdots p_r^{e_r}$ where $p_1,\ldots,p_r$ are odd primes with $p_1 < \cdots < p_r$, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1,\ldots,r$ and $r \geq 0$. Then

(i) For $r = 0$, we have $e_0 \geq 2$ and $c_n = c_{2^{e_0}} = 1$.

(ii) For $r \geq 1$ we have

$$c_n = c_{p_1\cdots p_r} \geq p_1^{-2^{r-2}}.$$

The main step in the proof of Proposition 5 is the following:

Lemma 6 ([FLW])**.** *For any odd squarefree integer $n = p_1\cdots p_r$ with $p_1 < p_2 < \cdots < p_r$ satisfying $n \geq 11$ and $n \neq 15$, we have*

$$\varphi(n) > 2^{r+1} \log p_1.$$

Further properties of the sequence $(c_n)_{n\geq 3}$.

- $\liminf_{n\to\infty} c_n = 0$ and $\limsup_{n\to\infty} c_n = 1$.
- The sequence $(c_p)_{p \text{ odd prime}}$ is decreasing from 3/4 to 1/2.
- For p_1 and p_2 primes, $c_{p_1p_2} \geq \dfrac{1}{p_1}\cdot$
- For any prime p_1, $\lim_{p_2\to\infty} c_{p_1p_2} = \dfrac{1}{p_1}\cdot$

3 The sequence $(a_m)_{m\geq 1}$

For each integer $m \geq 1$, the set

$$\big\{(n,x,y) \in \mathbb{N}\times\mathbb{Z}^2 \;\mid\; n \geq 3,\ \max\{|x|,|y|\} \geq 2,\ \Phi_n(x,y) = m\big\}$$

is finite. Let a_m the number of its elements.

The sequence of integers $m \geq 1$ such that $a_m \geq 1$ starts with the following values of a_m

m	3	4	5	7	8	9	10	11	12	13	16	17
a_m	8	16	8	24	4	16	8	8	12	40	40	16

3.1 Online Encyclopedia of Integer Sequences [OEIS]

`Number of representations of integers by cyclotomic binary forms.`
OEIS A299214

The sequence $(a_m)_{m\geq 1}$ starts with

$$0, 0, 8, 16, 8, 0, 24, 4, 16, 8, 8, 12, 40, 0, 0, 40, 16, 4, 24, 8, 24, 0, 0, 0, 24, 8, 12, 24, 8, 0, 32, 8, 0,$$
$$8, 0, 16, 32, 0, 24, 8, 8, 0, 32, 0, 8, 0, 0, 12, 40, 12, 0, 32, 8, 0, 8, 0, 32, 8, 0, 0, 48, 0, 24, 40, 16, 0, \ \dots$$

`Integers represented by cyclotomic binary forms`
OEIS A296095

$a_m \neq 0$ for $m =$

$$3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19, 20, 21, 25, 26, 27, 28, 29, 31, 32, 34, 36, 37, 39, 40,$$
$$41, 43, 45, 48, 49, 50, 52, 53, 55, 57, 58, 61, 63, 64, 65, 67, 68, 72, 73, 74, 75, 76, 79, 80, 81, 82, \ \dots$$

`Integers not represented by cyclotomic binary forms`
OEIS A293654

$a_m = 0$ for $m =$

$$1, 2, 6, 14, 15, 22, 23, 24, 30, 33, 35, 38, 42, 44, 46, 47, 51, 54, 56, 59, 60, 62, 66, 69, 70, 71, 77,$$
$$78, 83, 86, 87, 88, 92, 94, 95, 96, 99, 102, 105, 107, 110, 114, 115, 118, 119, 120, 123, 126, 131, \ \dots$$

4 Integers represented by cyclotomic binary forms

For $N \geq 1$, let $\mathcal{A}(N)$ be the number of $m \leq N$ which are represented by cyclotomic binary forms: there exists $n \geq 3$ and $(x, y) \in \mathbb{Z}^2$ with $\max(|x|, |y|) \geq 2$ and $m = \Phi_n(x, y)$. This means

$$\mathcal{A}(N) = \#\{m \in \mathbb{N} \ \mid \ m \leq N, \ a_m \neq 0\}.$$

Theorem 7 ([FLW]). *We have*

$$\mathcal{A}(N) = \alpha \frac{N}{(\log N)^{\frac{1}{2}}} - \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right) \qquad \text{as } N \to \infty.$$

The number of positive integers $\leq N$ represented by Φ_4 (namely the sums of two squares) is

$$\alpha_4 \frac{N}{(\log N)^{\frac{1}{2}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right).$$

The number of positive integers $\leq N$ represented by Φ_3 (namely $x^2 + xy + y^2$: Loeschian numbers) is

$$\alpha_3 \frac{N}{(\log N)^{\frac{1}{2}}} + O\left(\frac{N}{(\log N)^{\frac{3}{2}}}\right).$$

The number of positive integers $\leq N$ represented by Φ_4 and by Φ_3 is

$$\beta \frac{N}{(\log N)^{\frac{3}{4}}} + O\left(\frac{N}{(\log N)^{\frac{7}{4}}}\right).$$

Theorem 7 holds with $\alpha = \alpha_3 + \alpha_4$.

4.1 The Landau–Ramanujan constant

The number of positive integers $\le N$ which are sums of two squares is asymptotically $\alpha_4 N(\log N)^{-1/2}$, where

$$\alpha_4 = \frac{1}{2^{\frac{1}{2}}} \cdot \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

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

$$\alpha_4 = 0.764\,223\,653\,589\,220\ \ldots$$

References from OEIS A064533:

- 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, 125 079 digits of the Landau-Ramanujan constant.
- 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`.

4.2 Sums of two squares

If a and q are two integers, we denote by $\mathcal{P}_{a,q}$ the set of primes $p \equiv a \bmod q$ and by $N_{a,q}$ any integer ≥ 1 satisfying the condition $p \mid N_{a,q} \Longrightarrow p \equiv a \bmod q$.

An integer $m \ge 1$ is of the form $m = \Phi_4(x,y) = x^2 + y^2$ if and only if there exist integers $a \ge 0$, $N_{3,4}$ and $N_{1,4}$ such that $m = 2^a\, N_{3,4}^2\, N_{1,4}$.

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

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

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

if and only if there exist integers $b \ge 0$, $N_{2,3}$ and $N_{1,3}$ such that $m = 3^b\, N_{2,3}^2\, N_{1,3}$.

The number of positive integers $\le N$ which are represented by the quadratic form $X^2 + XY + Y^2$ is asymptotically $\alpha_3 N(\log N)^{-1/2}$ where

$$\alpha_3 = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.$$

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

$$\alpha_3 = \frac{1}{2^{\frac{1}{2}}3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} = 0.638\,909\,405\,44\ \ldots$$

Hence,

$$\alpha = \alpha_3 + \alpha_4 = 1.403\,133\,059\,034\ \ldots$$

Using the method of Flajolet and Vardi, Bill Allombert (private communication, April 2018) computed

$$\begin{aligned}\alpha_3 =\,& 0.63890940544534388225494267492824509375497550802912334542l\\ & 6923657080763100276496582468971791125286643881416875191074 24\ldots\end{aligned}$$

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

$$\beta = \frac{3^{\frac{1}{4}}}{2^{\frac{5}{4}}} \cdot \pi^{\frac{1}{2}} \cdot (\log(2+\sqrt{3}))^{\frac{1}{4}} \cdot \frac{1}{\Gamma(1/4)} \cdot \prod_{p \equiv 5,7,11 \bmod 12} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}} = 0.302\,316\,142\,35\ \ldots$$

Using the method of Flajolet and Vardi, Bill Allombert (private communication, April 2018) computed

$$\begin{aligned}\beta =\,& 0.302316142357065637947769900480199715602412795189369645458 8\\ & 67841288865448752410510899487467813979272708567765913272591 0\ldots\end{aligned}$$

4.4 Further developments

• Prove similar estimates for the number of integers represented by other binary forms (done for quadratic forms); e.g.: prove similar estimates for the number of integers which are sums of two cubes, two biquadrates,...

• Prove similar estimates for the number of integers which are represented by Φ_n for a given n.

• Prove similar estimates for the number of integers which are represented by Φ_n for some n with $\varphi(n) \geq d$.

5 Representation of integers by positive definite quadratic forms

5.1 Quadratic forms

Theorem 8 (P. Bernays [B])**.** *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 $\mathsf{C}_F N(\log N)^{-\frac{1}{2}}$.*

5.2 Higher degree

Theorem 9 (Stewart - Xiao [S–Y])**.** *Let F be a binary form of degree $d \geq 3$ with nonzero discriminant.*

There exists a positive constant $C_F > 0$ such that the number of integers of absolute value at most N which are represented by $F(X,Y)$ is asymptotic to $C_F N^{2/d}$.

Proposition 10 (K. Mahler [M]). *Let F be a binary form of degree $d \geq 3$ with nonzero discriminant. Denote by A_F the area (Lebesgue measure) of the domain*

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

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

$$N_F(Z) = A_F Z^{2/d} + O(Z^{1/(d-1)})$$

as $Z \to \infty$.

The situation for positive definite forms of degree ≥ 3 is different for the following reason: if a positive integer m is represented by a positive definite quadratic form, it usually has many such representations; while if a positive integer m is represented by a positive definite binary form of degree $d \geq 3$, it usually has few such representations. If F is a positive definite quadratic form, the number of (x,y) with $F(x,y) \leq N$ is asymptotically a constant times N, but the number of $F(x,y)$ is much smaller.

If F is a positive definite binary form of degree $d \geq 3$, the number of (x,y) with $F(x,y) \leq N$ is asymptotically a constant times $N^{1/d}$, the number of $F(x,y)$ is also asymptotically a constant times $N^{1/d}$.

5.3 Sums of k–th powers

If a positive integer m is a sum of two squares, there are many such representations.

Indeed, the number of (x,y) in $\mathbb{Z}\times\mathbb{Z}$ with $x^2+y^2 \leq N$ is asymptotic to πN, while the number of values $\leq N$ taken by the quadratic form Φ_4 is asymptotic to $\alpha_4 N/\sqrt{\log N}$ where α_4 is the Landau–Ramanujan constant. Hence, Φ_4 takes each of these values with a high multiplicity, on the average $(\pi/\alpha)\sqrt{\log N}$.

On the opposite, it is extremely rare that a positive integer is a sum of two biquadrates in more than one way (not counting symmetries).

$635\,318\,657 = 158^4 + 59^4 = 134^4 + 133^4$. Leonhard Euler1707 − 1783

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

`Number of solutions to the equation` $x^4 + y^4 = n$ `with` $x \geq y > 0$ [OEIS A216284]

An infinite family with one parameter is known for non trivial solutions to $x_1^4 + x_2^4 = x_3^4 + x_4^4$.

`http://mathworld.wolfram.com/DiophantineEquation4thPowers.html`

Sums of k–th powers

One conjectures that given $k \geq 5$, if an integer is of the form $x^k + y^k$, there is essentially a unique such representation. But there is no value of k for which this has been proved.

The situation for positive definite forms of degree ≥ 3 is different also for the following reason. A necessary and sufficient condition for a number m to be represented by one of the quadratic forms Φ_3, Φ_4, is given by a congruence. By contrast, consider the quartic binary form $\Phi_8(X,Y) = X^4 + Y^4$. On the one hand, an integer represented by Φ_8 is of the form

$$N_{1,8}(N_{3,8}N_{5,8}N_{7,8})^4.$$

On the other hand, there are many integers of this form which are not represented by Φ_8.

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

The list of prime numbers represented by Φ_8 start with

$$2, 17, 97, 257, 337, 641, 881, 1297, 2417, 2657, 3697, 4177, 4721, 6577, 10657, 12401, 14657,$$
$$14897, 15937, 16561, 28817, 38561, 39041, 49297, 54721, 65537, 65617, 66161, 66977, 80177, \dots$$

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 1353265-digit $(145310^{65536})^4 + 1^4$.

Primes of the form $x^{2^k}+y^{2^k}$

[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` $x^{32}+y^{32}$.

But it is known that there are infinitely many prime numbers of the form X^2+Y^4 [FI].

References

[B] 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/

[FLW] É. Fouvry, C. Levesque & M. Waldschmidt. *Representation of integers by cyclotomic binary forms.* Acta Arithmetica, **184**.1 (2018), 67 – 86.
http://arxiv.org/abs/1701.01230

[FI] J. Friedlander & H. Iwaniec. *The polynomial X^2+Y^4 captures its primes.* Ann. of Math. (2) **148** (1998), no. 3, 945 –1040.
https://arxiv.org/pdf/math/9811185.pdf

[G] K. Győry. *Représentation des nombres entiers par des formes binaires*, Publ. Math. Debrecen **24 (3–4)**, 363 – 375, (1977).

[GL] K. Győry & L. Lovász. *Representation of integers by norm forms II*, Publ. Math. Debrecen **17**, 173 – 181, (1970).

[M] K. Mahler. *Über die mittlere Anzahl der Darstellungen grosser Zahlen durch binäre Formen.* Acta Math. **62** (1933), 91–166.
https://carma.newcastle.edu.au/mahler/biography.html

[OEIS] N.J. Sloane. *The On–line Encyclopedia of Integer Sequences*,
https://oeis.org/
OEIS A296095 Integers represented by cyclotomic binary forms.
OEIS A293654 Integers not represented by cyclotomic binary forms.
OEIS A299214 Number of representations of integers by cyclotomic binary forms.
OEIS A301429 Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers.
OEIS A301430 Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers which are sums of two squares.

[S–Y] C.L. Stewart & S. Yao Xiao. *On the representation of integers by binary forms*,
http://arxiv.org/abs/1605.03427

Michel WALDSCHMIDT
Sorbonne Université
Faculté Sciences et Ingenierie
CNRS, Institut Mathématique de Jussieu Paris Rive Gauche, IMJ-PRG
F – 75005 Paris, France
michel.waldschmidt@imj-prg.fr
http://www.imj-prg.fr/~michel.waldschmidt