Representation of integers
by cyclotomic binary forms

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://www.imj-prg.fr/~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 plan to address.
This is a joint work with
Étienne Fouvry and Claude Levesque

Representation of integers by cyclotomic binary forms.
arXiv: 712.09019 [math.NT]
Cyclotomic polynomials

Definition by induction:

\[ \phi_1(t) = t - 1, \quad t^n - 1 = \prod_{d|n} \phi_d(t). \]

For \( p \) prime,

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

so

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

For instance

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

Definition by induction:

\[ \phi_1(t) = t - 1, \quad t^n - 1 = \prod_{d|n} \phi_d(t). \]

For prime \( p \),

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

so

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

For instance

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

Definition by induction:

\[ \phi_1(t) = t - 1, \quad t^n - 1 = \prod_{d|n} \phi_d(t). \]

For \( p \) prime,

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

so

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

For instance

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

$$\phi_n(t) = \frac{t^n - 1}{\prod_{d\neq n, d|n} \phi_d(t)}.$$ 

For instance

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

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

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

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

For instance

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

\[ \phi_6(t) = \frac{t^6 - 1}{(t^3 - 1)(t + 1)} = \frac{t^3 + 1}{t + 1} = t^2 - t + 1 = \phi_3(-t). \]

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

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

For instance

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

\[ \phi_6(t) = \frac{t^6 - 1}{(t^3 - 1)(t + 1)} = \frac{t^3 + 1}{t + 1} = t^2 - t + 1 = \phi_3(-t). \]

The degree of \( \phi_n(t) \) is \( \varphi(n) \), where \( \varphi \) is the Euler totient function.
Cyclotomic polynomials and roots of unity

For \( n \geq 1 \), if \( \zeta \) is a primitive \( n \)-th root of unity,

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

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 \( K \).
Cyclotomic polynomials and roots of unity

For $n \geq 1$, if $\zeta$ is a primitive $n$–th root of unity,

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

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 $K$. 
Cyclotomic polynomials and roots of unity

For \( n \geq 1 \), if \( \zeta \) is a primitive \( n \)-th root of unity,

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

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 \( K \).
Properties of $\phi_n(t)$

• For $n \geq 2$ we have

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

• Let $n = 2^{e_0}p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are different odd primes, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \ldots, r$ and $r \geq 1$. Denote by $R$ the radical of $n$, namely

$$R = \begin{cases} 2p_1 \cdots p_r & \text{if } e_0 \geq 1, \\ p_1 \cdots p_r & \text{if } e_0 = 0. \end{cases}$$

Then,

$$\phi_n(t) = \phi_R(t^{n/R}).$$

• Let $n = 2m$ with $m$ odd $\geq 3$. Then

$$\phi_n(t) = \phi_m(-t).$$
Properties of $\phi_n(t)$

- For $n \geq 2$ we have
  \[ \phi_n(t) = t^{\varphi(n)} \phi_n(1/t) \]

- Let $n = 2^{e_0}p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are different odd primes, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \ldots, r$ and $r \geq 1$. Denote by $R$ the radical of $n$, namely
  \[
  R = \begin{cases} 
  2p_1 \cdots p_r & \text{if } e_0 \geq 1, \\
  p_1 \cdots p_r & \text{if } e_0 = 0. 
  \end{cases}
  \]

  Then,
  \[ \phi_n(t) = \phi_R(t^{n/R}). \]

- Let $n = 2m$ with $m$ odd $\geq 3$. Then
  \[ \phi_n(t) = \phi_m(-t). \]
Properties of $\phi_n(t)$

- For $n \geq 2$ we have
  $$\phi_n(t) = t^{\varphi(n)}\phi_n(1/t)$$

- Let $n = 2^{e_0}p_1^{e_1} \cdots p_r^{e_r}$ where $p_1, \ldots, p_r$ are different odd primes, $e_0 \geq 0$, $e_i \geq 1$ for $i = 1, \ldots, r$ and $r \geq 1$. Denote by $R$ the radical of $n$, namely
  $$R = \begin{cases} 
2p_1 \cdots p_r & \text{if } e_0 \geq 1, \\
p_1 \cdots p_r & \text{if } e_0 = 0.
\end{cases}$$
  Then,
  $$\phi_n(t) = \phi_R(t^{n/R}).$$

- Let $n = 2m$ with $m$ odd $\geq 3$. Then
  $$\phi_n(t) = \phi_m(-t).$$
\( \phi_n(1) \)

For \( n \geq 2 \), we have \( \phi_n(1) = e^{\Lambda(n)} \), where the von Mangoldt function 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 we have

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

For \( n \geq 2 \), we have \( \phi_n(1) = e^{\Lambda(n)} \), where the von Mangoldt function 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 we have

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

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 \( n \geq 3 \),

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

Hence \( \phi_n(-1) = 1 \) when \( n \) is odd or when \( n = 2m \) where \( m \) has at least two distinct prime divisors.
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 $n \geq 3$, \[
\phi_n(-1) = \begin{cases} 
p & \text{if } n = 2p^r \text{ with } p \text{ a prime and } r \geq 1 ; \\
1 & \text{otherwise}. 
\end{cases}
\]

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

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

For $n \geq 3$ and $t \in \mathbb{R}$, 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 $t \in \mathbb{R}$,

$$\phi_n(t) \geq 2^{-\varphi(n)} \max\{1, |t|\}^{\varphi(n)}.$$
Lower bound for $\phi_n(t)$

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

For $n \geq 3$ and $t \in \mathbb{R}$, 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 $t \in \mathbb{R}$,

$$\phi_n(t) \geq 2^{-\varphi(n)} \max\{1, |t|\}^{\varphi(n)}.$$
Lower bound for $\phi_n(t)$

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

For $n \geq 3$ and $t \in \mathbb{R}$, 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 $t \in \mathbb{R}$,

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

**Proof.**

Let \( \zeta_n \) be a primitive \( n \)-th root of unity in \( \mathbb{C} \);

\[ \phi_n(t) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t - \zeta_n) = \prod_{\sigma}(t - \sigma(\zeta_n)), \]

where \( \sigma \) runs over the embeddings \( \mathbb{Q}(\zeta_n) \rightarrow \mathbb{C} \). We have

\[ |t - \sigma(\zeta_n)| \geq |\text{Re}(\sigma(\zeta_n))| > 0, \]

\[ (2i)\text{Re}(\sigma(\zeta_n)) = \sigma(\zeta_n) - \overline{\sigma(\zeta_n)} = \sigma(\zeta_n - \overline{\zeta_n}). \]

Now \((2i)\text{Re}(\zeta_n) = \zeta_n - \overline{\zeta_n} \in \mathbb{Q}(\zeta_n)\) is an algebraic integer:

\[ 2^{\varphi(n)}\phi_n(t) \geq |N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}((2i)\text{Re}(\zeta_n))| \geq 1. \]
\[ \phi_n(t) \geq 2^{-\varphi(n)} \text{ for } n \geq 3 \text{ and } t \in \mathbb{R} \]

**Proof.**
Let \( \zeta_n \) be a primitive \( n \)-th root of unity in \( \mathbb{C} \);

\[
\phi_n(t) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t - \zeta_n) = \prod_{\sigma}(t - \sigma(\zeta_n)),
\]

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

\[
|t - \sigma(\zeta_n)| \geq |\Im(\sigma(\zeta_n))| > 0,
\]

\[
(2i)\Im(\sigma(\zeta_n)) = \sigma(\zeta_n) - \overline{\sigma(\zeta_n)} = \sigma(\zeta_n - \overline{\zeta_n}).
\]

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

\[
2^{\varphi(n)}\phi_n(t) \geq |N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}((2i)\Im(\zeta_n))| \geq 1.
\]
\[ \phi_n(t) \geq 2^{-\varphi(n)} \text{ for } n \geq 3 \text{ and } t \in \mathbb{R} \]

Proof.

Let \( \zeta_n \) be a primitive \( n \)-th root of unity in \( \mathbb{C} \);

\[ \phi_n(t) = N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}(t - \zeta_n) = \prod_{\sigma}(t - \sigma(\zeta_n)), \]

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

\[ |t - \sigma(\zeta_n)| \geq |\text{Im}(\sigma(\zeta_n))| > 0, \]

\[ (2i) \text{Im}(\sigma(\zeta_n)) = \sigma(\zeta_n) - \sigma(\zeta_n) = \sigma(\zeta_n - \overline{\zeta_n}). \]

Now \( (2i) \text{Im}(\zeta_n) = \zeta_n - \overline{\zeta_n} \in \mathbb{Q}(\zeta_n) \) is an algebraic integer:

\[ 2^{\varphi(n)}\phi_n(t) \geq |N_{\mathbb{Q}(\zeta_n)/\mathbb{Q}}((2i)\text{Im}(\zeta_n))| \geq 1. \]
The cyclotomic binary forms

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 \( \varphi(n) \).

Consequence of the lower bound for \( \phi_n(t) \): 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

\[
\max\{|x|, |y|\} \leq 2m^{1/\varphi(n)}.
\]

If \( \max\{|x|, |y|\} \geq 3 \), then \( n \) is bounded:

\[
\varphi(n) \leq \frac{\log m}{\log(3/2)}.
\]
The cyclotomic binary forms

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 \( \varphi(n) \).

Consequence of the lower bound for \( \phi_n(t) \): 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

\[
\max\{|x|, |y|\} \leq 2m^{1/\varphi(n)}.
\]

If \( \max\{|x|, |y|\} \geq 3 \), then \( n \) is bounded:

\[
\varphi(n) \leq \frac{\log m}{\log(3/2)}.
\]
The cyclotomic binary forms

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 \( \varphi(n) \).

Consequence of the lower bound for \( \phi_n(t) \) : 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

\[
\max\{|x|, |y|\} \leq 2m^{1/\varphi(n)}.
\]

If \( \max\{|x|, |y|\} \geq 3 \), then \( n \) is bounded :

\[
\varphi(n) \leq \frac{\log m}{\log(3/2)}.
\]
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 $\alpha$ over $\mathbb{Q}$ and let $F(X, Y) = Y^df(X/Y)$ the associated homogeneous binary form:

$$f(t) = a_0t^d + a_1t^{d-1} + \cdots + a_d,$$

$$F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_dY^d.$$

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

$$x^d \leq 2^da_d^{d-1}F(x, y) \quad \text{and} \quad y^d \leq 2^da_0^{d-1}F(x, y).$$
Let \( n \geq 3 \), not of the form \( p^a \) nor \( 2p^a \) with \( p \) prime and \( a \geq 1 \), 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

\[
y^d = 2^d a_0^{d-1} F(x, y).
\]
Best possible for CM fields

Let $n \geq 3$, not of the form $p^a$ nor $2p^a$ with $p$ prime and $a \geq 1$, 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

$$y^d = 2^d a_0^{d-1} F(x, y).$$
Best possible for CM fields

Let $n \geq 3$, not of the form $p^a$ nor $2p^a$ with $p$ prime and $a \geq 1$, 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

$$y^d = 2^d a_0^{d-1} F(x, y).$$
Let $n \geq 3$, not of the form $p^a$ nor $2p^a$ with $p$ prime and $a \geq 1$, 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

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

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

These estimates are optimal, since for $\ell \geq 1$,

$$\Phi_3(\ell, -2\ell) = 3\ell^2.$$ 

If we assume $\varphi(n) > 2$, namely $\varphi(n) \geq 4$, then

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

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

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

These estimates are optimal, since for $\ell \geq 1$,

$$\Phi_3(\ell, -2\ell) = 3\ell^2.$$ 

If we assume $\varphi(n) > 2$, namely $\varphi(n) \geq 4$, then

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

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


Binary cyclotomic forms (EF–CL–MW 2018)

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

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

These estimates are optimal, since for $\ell \geq 1$,

$$\Phi_3(\ell, -2\ell) = 3\ell^2.$$ 

If we assume $\varphi(n) > 2$, namely $\varphi(n) \geq 4$, then

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

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

Lower bound for the cyclotomic polynomials

The upper bound

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

for $\Phi_n(x, y) = m$ is equivalent to the following result:

For $n \geq 3$ and $t \in \mathbb{R}$,

$$\phi_n(t) \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}.$$
The sequence \((c_n)_{n \geq 3}\)

\[ c_n = \inf_{t \in \mathbb{R}} \phi_n(t) \quad (n \geq 3). \]

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 \(r \geq 0\).

(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

\[ c_n = c_{p_1 \cdots p_r} \geq p_1^{-2^{r-2}}. \]
End of the proof of $\phi_n(t) \geq \left(\frac{\sqrt{3}}{2}\right)^{\varphi(n)}$.

**Lemma.** 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

$$\varphi(n) > 2^{r+1} \log p_1.$$
The sequence  \( (c_n)_{n \geq 3} \)

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

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

• \( \liminf_{n \to \infty} c_n = 0 \) 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, \( c_{p_1 p_2} \geq \frac{1}{p_1} \).

• For any prime \( p_1 \), \( \lim_{p_2 \to \infty} c_{p_1 p_2} = \frac{1}{p_1} \).
The sequence \((c_n)_{n \geq 3}\)

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

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

- \(\liminf_{n \to \infty} c_n = 0\) 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, \(c_{p_1p_2} \geq \frac{1}{p_1}\).

- For any prime \(p_1\), \(\lim_{p_2 \to \infty} c_{p_1p_2} = \frac{1}{p_1}\).
The sequence $\left( c_n \right)_{n \geq 3}$

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

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

- $\liminf_{n \to \infty} c_n = 0$ 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, $c_{p_1p_2} \geq \frac{1}{p_1}$.

- For any prime $p_1$, $\lim_{p_2 \to \infty} c_{p_1p_2} = \frac{1}{p_1}$.
The sequence \((c_n)_{n \geq 3}\)

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

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

- \(\liminf_{n \to \infty} c_n = 0\) 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, \(c_{p_1p_2} \geq \frac{1}{p_1}\).

- For any prime \(p_1\), \(\lim_{p_2 \to \infty} c_{p_1p_2} = \frac{1}{p_1}\).
The sequence \((a_m)_{m \geq 1}\)

For each integer \(m \geq 1\), the set

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

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 \(a_m\):

<table>
<thead>
<tr>
<th>(m)</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a_m)</td>
<td>8</td>
<td>16</td>
<td>8</td>
<td>24</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>40</td>
<td>40</td>
<td>16</td>
</tr>
</tbody>
</table>
The sequence $(a_m)_{m \geq 1}$

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

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

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 $a_m$

<table>
<thead>
<tr>
<th>$m$</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>16</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>$a_m$</td>
<td>8</td>
<td>16</td>
<td>8</td>
<td>24</td>
<td>4</td>
<td>16</td>
<td>8</td>
<td>8</td>
<td>12</td>
<td>40</td>
<td>40</td>
<td>16</td>
</tr>
</tbody>
</table>
OEIS A299214

https://oeis.org/A299214
Number of representations of integers by cyclotomic binary forms.

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

\[
0, 0, 8, 16, 8, 0, 24, 4, 16, 8, 8, 12, 40, 0, 0, 40, 16, 4, 24, 8, 24, 0, 0, 24, 8, 12, 24, 8, 0, 32, 8, 0, 8, 0, 16, 32, 0, 24, 8, 8, 0, 32, 0, 8, 0, 0, 12, 40, 12, 0, 32, 8, 0, 8, 0, 32, 8, 0, 0, 48, 0, 24, 40, 16, 0, 24, 8, 0, 0, 0, 4, 48, 8, 12, 24, \ldots
\]
OEIS A296095

https://oeis.org/A296095
Integers represented by cyclotomic binary forms.

\[ a_m \neq 0 \text{ for } m = 3, 4, 5, 7, 8, 9, 10, 11, 12, 13, 16, 17, 18, 19, 20, 21, 25, 26, 27, 28, 29, 31, 32, 34, 36, 37, 39, 40, 41, 43, 45, 48, 49, 50, 52, 53, 55, 57, 58, 61, 63, 64, 65, 67, 68, 72, 73, 74, 75, 76, 79, 80, 81, 82, 84, 85, 89, 90, 91, 93, 97, 98, 100, 101, 103, 104, 106, 108, 109, 111, 112, 113, 116, 117, 121, 122, \ldots \]
OEIS A293654

https://oeis.org/A293654
Integers not represented by cyclotomic binary forms.

\(a_m = 0\) for \(m =\)
For \( N \geq 1 \), let \( A(N) \) be the number of \( m \leq N \) which are represented by cyclotomic binary forms:

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

We have

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

as \( N \to \infty \).
Integers represented by cyclotomic binary forms

For $N \geq 1$, let $A(N)$ be the number of $m \leq N$ which are represented by cyclotomic binary forms:

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

We have

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

as $N \to \infty$. 
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:

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

We have

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

as $N \to \infty$. 

\[ \alpha = \alpha_3 + \alpha_4 \]

The number of positive integers \( \leq N \) represented by \( \Phi_4 \) (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 \( \Phi_3 \) (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 \( \Phi_4 \) and by \( \Phi_3 \) is

\[ \beta \frac{N}{(\log N)^{\frac{3}{4}}} + O \left( \frac{N}{(\log N)^{\frac{7}{4}}} \right). \]
The Landau–Ramanujan constant

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

\[
\alpha_4 = \frac{1}{2^{1/2}} \cdot \prod_{p \equiv 3 \mod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2}.
\]
OEIS A064533

OEIS A064533 Decimal expansion of Landau-Ramanujan constant.

\[ \alpha_4 = 0.764223653589220 \ldots \]

- Ph. Flajolet and I. Vardi, Zeta function expansions of some classical constants, Feb 18 1996.
- Xavier Gourdon and Pascal Sebah, Constants and records of computation.
- David E. G. Hare, 125079 digits of the Landau-Ramanujan constant.
The Landau–Ramanujan constant

References: https://oeis.org/A064533

- 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.
Sums of two squares

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

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

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

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

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

$$m = 2^a N_{3,4}^2 N_{1,4}.$$
Sums of two squares

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

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

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

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

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

$$m = 2^a N_{3,4}^2 N_{1,4}.$$
Loeschian numbers: \( m = x^2 + xy + y^2 \)

An integer \( m \geq 1 \) 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 \( b \geq 0, N_{2,3} \) and \( N_{1,3} \) such that

\[
m = 3^b N_{2,3}^2 N_{1,3}.
\]

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

\[
\alpha_3 = \frac{1}{2^{1/2} 3^{1/4}} \cdot \prod_{p \equiv 2 \mod 3} \left( 1 - \frac{1}{p^2} \right)^{-1/2}.
\]
Loeschian numbers: \( m = x^2 + xy + y^2 \)

An integer \( m \geq 1 \) 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 \( b \geq 0 \), \( N_{2,3} \) and \( N_{1,3} \) such that

\[
m = 3^b N_{2,3}^2 N_{1,3}.
\]

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

\[
\alpha_3 = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \mod 3} \left(1 - \frac{1}{p^2}\right)^{-\frac{1}{2}}.
\]
OEIS A301429

OEIS A301429 Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers.

\[ \alpha_3 = \frac{1}{2^{\frac{1}{2}} 3^{\frac{1}{4}}} \cdot \prod_{p \equiv 2 \text{ mod } 3} \left( 1 - \frac{1}{p^2} \right)^{-\frac{1}{2}}. \]

\[ \alpha_3 = 0.638 \, 909 \, 405 \, 44 \ldots \]

\[ \alpha = \alpha_3 + \alpha_4 = 1.403 \, 133 \, 059 \ldots \]
OEIS A301429

OEIS A301429 Decimal expansion of an analog of the Landau-Ramanujan constant for Loeschian numbers.

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

\[ \alpha_3 = 0.638 \, 909 \, 405 \, 44 \ldots \]

\[ \alpha = \alpha_3 + \alpha_4 = 1.403 \, 133 \, 059 \ldots \]
Zeta function expansions of some classical constants, Feb 18 1996.

Philippe Flajolet

Ilan Vardi

Bill Allombert

\[ \alpha_3 = 0.63890940544534388 \\
22549426749282450937 \\
54975508029123345421 \\
69236570807631002764 \\
96582468971791125286 \\
64388141687519107424 \ldots \]
OEIS A301430

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

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

\[
\beta = 0.30231614235 \ldots
\]

Only 11 digits after the decimal point are known.
OEIS A301430

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

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

\[
\beta = 0.30231614235 \ldots
\]

Only 11 digits after the decimal point are known.
Zeta function expansions of some classical constants, Feb 18 1996.

Philippe Flajolet

$\beta = 0.302316142357065637$
$94776990048019971560$
$24127951893696454588$
$67841288865448752410$
$51089948746781397927$
$27085677659132725910 \ldots$

Ilan Vardi

Bill Allombert
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,\ldots

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

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

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

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

- Prove similar estimates for the number of integers which are represented by $\Phi_n$ for some $n$ with $\varphi(n) \geq d$. 
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 $\Phi_n$ for a given $n$.

- Prove similar estimates for the number of integers which are represented by $\Phi_n$ for some $n$ with $\varphi(n) \geq d$. 
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 $C_F N^{2/d}$. 


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 $Z \to \infty$. 

K. Mahler (1933)
Kurt Mahler

1903 – 1988

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

Higher degree

The situation for positive definite forms of degree $\geq 3$ 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 $N^{1/d}$. 
Higher degree

The situation for positive definite forms of degree $\geq 3$ 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 $N^{1/d}$. 
Higher degree

The situation for positive definite forms of degree $\geq 3$ 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 $N^{1/d}$. 
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 $\pi N$, while the number of values $\leq N$ taken by the quadratic form $\Phi_4$ is asymptotic to $\alpha_4 N / \sqrt{\log N}$ where $\alpha_4$ is the Landau–Ramanujan constant. Hence $\Phi_4$ 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).
$$635318657 = 158^4 + 59^4 = 134^4 + 133^4.$$  

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

Leonhard Euler  
1707 – 1783

[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 $x_1^4 + x_2^4 = x_3^4 + x_4^4$.  

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.
Higher degree

The situation for positive definite forms of degree \( \geq 3 \) 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 \( \Phi_3, \Phi_4 \), 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 \( \Phi_8 \) 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 \( \Phi_8 \).
Higher degree

The situation for positive definite forms of degree \( \geq 3 \) 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 \( \Phi_3, \Phi_4 \), 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 \( \Phi_8 \) 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 \( \Phi_8 \).
Higher degree

The situation for positive definite forms of degree $\geq 3$ 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 $\Phi_3$, $\Phi_4$, 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 $\Phi_8$ 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 $\Phi_8$.  


Quartan primes

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

The list of prime numbers represented by $\Phi_8$ 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, 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 1353265-digit $(145310^{65536})^4 + 1^4$. 
Quartan primes

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

The list of prime numbers represented by $\Phi_8$ 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, 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 1353265-digit $(145310^{65536})^4 + 1^4$. 
Quartan primes

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

The list of prime numbers represented by $\Phi_8$ 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, 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 1353265-digit $(145310^{65536})^4 + 1^4$. 
Quartan primes

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

The list of prime numbers represented by $\Phi_8$ 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, 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
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 $x^{32} + y^{32}$.
Primes of the form $X^2 + Y^4$

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


Representation of integers by cyclotomic binary forms

Michel Waldschmidt

Institut de Mathématiques de Jussieu — Paris VI
http://www.imj-prg.fr/~michel.waldschmidt/