Update *25/02/2026* *February 21, 2026*

CONGRUENCE & CONVERGENCE:

A Conference in Celebration of Fidel Nemenzo's 65th Birthday

21-23 FEBRUARY 2026

UNIVERSITY OF THE PHILIPPINES DILIMAN

On multicyclotomic polynomials and binary forms

Michel Waldschmidt

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

Abstract

In a joint work in progress with Étienne Fouvry we define a multicyclotomic polynomial as a polynomial in one variable which is a product of distinct cyclotomic polynomials and has a positive leading coefficient. Hence a polynomial with integer coefficients is multicyclotomic if and only if it is monic with all its roots simple and roots of unity. It is equivalent to say that it is a divisor of a polynomial of the form $T^n - 1$, or that it is separable with Mahler's measure 1. A multicyclotomic form is a binary form obtained by homogenizing a multicyclotomic polynomial. We extend to this new setting some of the results known for cyclotomic polynomials and forms.

First meetings with Fidel

- 1993 The University of Hong Kong's Robert Black College
International Conference on Number Theory
Courses by Harold Stark and Hendrik Lenstra
Atle Selberg
Andrew Wiles' 1993 (June) announcement of his proof of
Fermat's last Theorem

- 2010 IMU Hyderabad project of a CIMPA School

- 2011 and 2012 Cambodia RUPP

RUPP Class Number Theory 2012

RUPP M.Sc. (Mathematics) Program

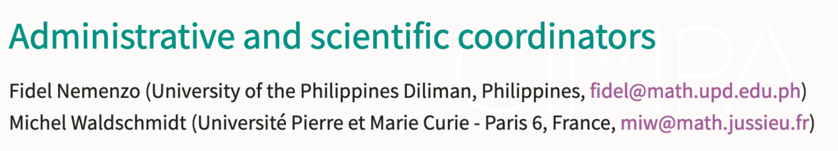
Number Theory (21 March – 06 April 2012)

Back(L-R): Ol Say, Yoeun Voline, Dohnbandit Bienthanong, Prokteab Sarun, Michel Waldschmidt, Fidel Nemenzo, Huot Sokloeun, Thy Chet
Front (L-R): Veng Sotheara, Seak Narith, Buoy Chamnan, Ick Phetyavong, Kim Sokun, Kum Romdoh

My previous visits to Diliman campus

Institute of Mathematics of the University of the Philippines,

July 14 – August 2, 2013, invited professor.
July 22 – August 2, 2013 ; CIMPA research school :
Algebraic Curves over Finite Fields and Applications.

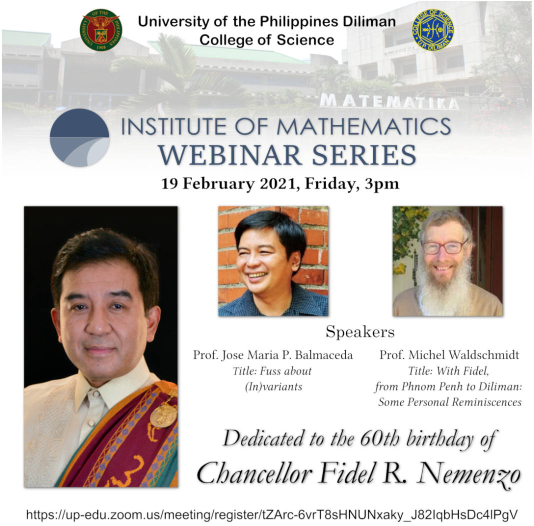


Administrative and scientific coordinators

Fidel Nemenzo (University of the Philippines Diliman, Philippines, fidel@math.upd.edu.ph)
Michel Waldschmidt (Université Pierre et Marie Curie - Paris 6, France, miw@math.jussieu.fr)

July 17 – 25, 2017
SEAMS School : Topics on elliptic curves.

January 9 – 20, 2023.
CIMPA School : Introduction to Galois Representations and Modular Forms and their Computational Aspects.



University of the Philippines Diliman
College of Science

MATEMATIKA

INSTITUTE OF MATHEMATICS
WEBINAR SERIES

19 February 2021, Friday, 3pm

Speakers

Prof. Jose Maria P. Balmaceda
Title: Fuss about (In)variants

Prof. Michel Waldschmidt
Title: With Fidel, from Phnom Penh to Diliman: Some Personal Reminiscences

Dedicated to the 60th birthday of
Chancellor Fidel R. Nemenzo

https://up-edu.zoom.us/meeting/register/tZArc-6vrT8sHNUNxaky_J82IqbHsDc4lPgV

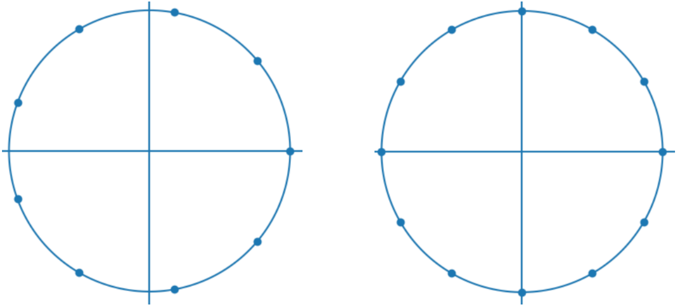
http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/FidelNemenzo60.pdf

Cyclo–tomy

Cyclo–tomy : cut the circle

Carl Friedrich Gauss

1777 – 1855



Cyclotomy

n equidistributed points on the circle : roots of $T^n - 1$

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}, \quad \zeta = \mathrm{e}^{2\mathrm{i}\pi/n}.$$

If d divides n, say $n = kd$, then $T^d - 1$ divides $T^n - 1$:

$$\frac{Z^k - 1}{Z - 1} = Z^{k-1} + \cdots + Z + 1, \quad Z = T^d.$$

New points : $\mathrm{e}^{2\mathrm{i}\pi\ell/n}$, $\gcd(\ell, n) = 1$: primitive roots of unity.

The sequence of cyclotomic polynomials

$$T^n - 1 = \prod_{d|n} \phi_d(T)$$

$$T - 1 = \phi_1(T), \qquad \boxed{\phi_1(T) = T - 1}$$

$$T^2 - 1 = (T-1)(T+1) = \phi_1(T)\phi_2(T) \qquad \boxed{\phi_2(T) = T + 1}$$

$$T^3 - 1 = (T-1)(T^2+T+1) = \phi_1(T)\phi_3(T)$$

$$\boxed{\phi_3(T) = T^2 + T + 1}$$

$$T^4 - 1 = (T-1)(T+1)(T^2+1) = \phi_1(T)\phi_2(T)\phi_4(T)$$

$$\boxed{\phi_4(T) = T^2 + 1}$$

$$T^5 - 1 = (T-1)(T^4+T^3+T^2+T+1) = \phi_1(T)\phi_5(T)$$

$$\boxed{\phi_5(T) = T^4 + T^3 + T^2 + T + 1}$$

$$T^6 - 1 = \phi_1(T)\phi_2(T)\phi_3(T)\phi_6(T)$$

$$\boxed{\phi_6(T) = T^2 - T + 1}$$

Roots of the cyclotomic polynomials

For any positive integer n, the polynomial $\phi_n(T)$ has its coefficients in $\mathbb{Z}$. Moreover, $\phi_n(T)$ is irreducible in $\mathbb{Z}[T]$.

$$T^n - 1 = \prod_{j=0}^{n-1} (T - \zeta_n^j), \quad \zeta_n = \mathrm{e}^{2\mathrm{i}\pi/n}.$$

$$\phi_n(T) = \prod_{\gcd(j,n)=1} (T - \zeta_n^j), \qquad T^n - 1 = \prod_{d|n} \phi_d(T).$$

Let K be a field of characteristic 0 and let n be a positive integer. Then the roots of the polynomial $\phi_n(T)$ are simple and are exactly the primitive n–th roots of unity which belong to K.

Euler totient function

The degree of ϕ_n is Euler totient function

Leonhard

1707 – 1783

$$\varphi(n) = \#\{j \mid 0 \leqslant j \leqslant n-1,\ \gcd(j,n)=1\}$$

$$n = \sum_{d|n} \varphi(d).$$

The sequence $\varphi(1), \varphi(2), \ldots$ is https://oeis.org/A000010

Euler totient function $\varphi(n)$: count numbers $\leqslant n$ and prime to n.

starting with

$$1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8, 16, 6, 18, 8, 12, 10, 22, \ldots$$

Euler totient function

$\varphi(1) = \varphi(2) = 1$.

For $n \geqslant 3$, $\varphi(n)$ is even.

$\varphi(3) = \varphi(4) = \varphi(6) = 2$, and $\varphi(n) \geqslant 4$ otherwise.

$\varphi(5) = \varphi(8) = \varphi(10) = \varphi(12) = 4$, and $\varphi(n) \geqslant 6$ otherwise.

Euler totient function is a multiplicative function

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ if } \gcd(a,b) = 1.$$

Since $\varphi(p^a) = (p-1)p^{a-1}$ for p prime and $a \geqslant 1$,

for $n = \prod_p p^{a_p}$ we have $\varphi(n) = \prod_{p|n} (p-1)p^{a_p-1}$.

The sequence of totients

https://oeis.org/A014197

Number of numbers m with Euler $\varphi(m) = n$.

$$2, 3, 0, 4, 0, 4, 0, 5, 0, 2, 0, 6, 0, 0, 0, 6, 0, 4, 0, 5, 0, 2, 0, 10, \ldots$$

A *totient* is a value taken by Euler totient function φ. The sequence of totients https://oeis.org/A002202

Values taken by totient function $\varphi(m)$

starts with

$$1, 2, 4, 6, 8, 10, 12, 16, 18, 20, 22, 24, 28, 30, 32, 36, 40, 42, 44, \ldots$$

The sequence of totients

The sequence of totients contains all numbers $p-1$ with p prime but is still mysterious :

Kevin Ford

FORD, K, *The distribution of totients. Paul Erdős (1913–1996).* Ramanujan J. (**2**) (1998), no. 1–2, 67–151.

FORD, K, *The number of solutions of $\varphi(x)=m$.* Ann. of Math. (2) **150** (1999), no. 1, 283–311.

Sequence of even nontotients https://oeis.org/A005277

Nontotients: even numbers k such that $\varphi(m)=k$ has no solution.

$$14, 26, 34, 38, 50, 62, 68, 74, 76, 86, 90, 94, 98, 114, 118, \dots$$

Elementary properties of cyclotomic polynomials

In $n = p$ is a prime number, then from

$$T^p - 1 = (T-1)(T^{p-1} + \cdots + T + 1) = \phi_1(T)\phi_p(T)$$

we deduce

$$\phi_p(T) = T^{p-1} + \cdots + T + 1.$$

For $a \geqslant 2$, and m odd, $\varphi(2^a m) = 2^{a-1}\varphi(m)$ and

$\phi_{2^a}(T) = T^{2^{a-1}} + 1$ and $\phi_{2^a m}(T) = \phi_m(-T^{2^{a-1}})$ for $m \geqslant 3$.

Example : if m is odd, then $\varphi(2m) = \varphi(m)$ and if $m \geqslant 3$

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

Elementary properties of cyclotomic polynomials

For $m \geqslant 2$ the polynomial ϕ_m is reciprocal :

$$\phi_m(T) = T^{\varphi(m)}\phi_m(1/T).$$

When q is the radical of m (i.e. the product of all primes dividing n), we have

$$\phi_m(T) = \phi_q(T^{m/q}).$$

For p prime and m prime to p, $\varphi(pm) = (p-1)\varphi(m)$ and

$$\phi_m(T)\phi_{pm}(T) = \phi_m(T^p)$$

Möbius function

August Möbius

1790 – 1868

For $m \geqslant 1$,

$$\mu(m) = \begin{cases} 0 & \text{if } m \text{ is not squarefree,} \\ (-1)^{\omega(m)} & \text{if } m \text{ is squarefree,} \end{cases}$$

where $\omega(m)$ is the number of distinct prime factors of m

`https://oeis.org/A008683`

`Möbius (or Moebius) function` $\mu(n)$. $\mu(1) = 1$; $\mu(n) = (-1)^k$ `if` n `is the product of` k `different primes; otherwise` $\mu(n) = 0$.

$$1, -1, -1, 0, -1, 1, -1, 0, 0, 1, -1, 0, -1, 1, 1, 0, -1, 0, -1, 0, \ldots$$

Taylor expansion at $t = 0$

For m odd $\geqslant 3$ we have

$$\phi_m(t) = \begin{cases} 1 + t + t^2 + O(t^3) & \text{if } \mu(m) = -1, \\ 1 - t + O(t^3) & \text{if } \mu(m) = 1, \\ 1 + O(t^3) & \text{if } \mu(m) = 0 \end{cases}$$

while for m even $\geqslant 4$ we have

$$\phi_m(t) = \begin{cases} 1 + t + O(t^3) & \text{if } \mu(m) = -1, \\ 1 - t + t^2 + O(t^3) & \text{if } \mu(m) = 1, \\ 1 - \mu(m/2)t^2 + O(t^3) & \text{if } \mu(m) = 0. \end{cases}$$

Andrés Herrera-Poyatos & Pieter Moree. *Coefficients and higher order derivatives of cyclotomic polynomials : old and new (with an appendix by Pedro García-Sánchez)*. Expo. Math. 39, No. 3, 309-343 (2021). Zbl 1486.11041 https://arxiv.org/abs/1805.05207 https://doi.org/10.1016/j.exmath.2019.07.003

Special values of the cyclotomic polynomials

We have $\phi_1(0) = -1$, $\phi_n(0) = 1$ for $m \geqslant 2$,

$$\phi_m(1) = \begin{cases} 0 & \text{if } m = 1, \\ p & \text{if } m = p^k \ (k \geq 1), \\ 1 & \text{if } \omega(m) \geq 2, \end{cases}$$

and

$$\phi_n(-1) = \begin{cases} -2 & \text{if } m = 1, \\ 0 & \text{if } n = 2, \\ p & \text{if } n = 2p^r \text{ with } p \text{ a prime and } r \geqslant 1, \\ 1 & \text{otherwise, if } n \text{ is odd or if } n = 2m \text{ where } m \\ & \text{has at least two distinct prime divisors.} \end{cases}$$

Coefficients of the cyclotomic polynomials

If m has at most two odd prime divisors, then the coefficients of ϕ_m belong to $\{0, 1, -1\}$.

The first instance of another coefficients is with $105 = 3 \cdot 5 \cdot 7$:

$$\begin{aligned}\Phi_{105}(t) = 1 &+ t + t^2 - t^5 - t^6 - \mathbf{2}t^7 - t^8 - t^9 + t^{12} \\ &+ t^{13} + t^{14} + t^{15} + t^{16} + t^{17} - t^{20} - t^{22} - t^{24} \\ &- t^{26} - t^{28} + t^{31} + t^{32} + t^{33} + t^{34} + t^{35} + t^{36} \\ &- t^{39} - t^{40} - \mathbf{2}t^{41} - t^{42} - t^{43} + t^{46} + t^{47} + t^{48}.\end{aligned}$$

Cyclotomic binary forms

$$\Phi_n(X,Y) = Y^{\varphi(n)}\phi_n(X/Y) = X^{\varphi(n)}\phi_n(Y/X)$$
$$X^n - Y^n = \prod_{d|n} \Phi_d(X,Y).$$

$$\begin{aligned}
\Phi_1(X,Y) &= X - Y,\\
\Phi_2(X,Y) &= X + Y,\\
\Phi_3(X,Y) &= X^2 + XY + Y^2,\\
\Phi_4(X,Y) &= X^2 + Y^2,\\
\Phi_5(X,Y) &= X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4,\\
\Phi_6(X,Y) &= X^2 - XY + Y^2,\\
\Phi_7(X,Y) &= X^6 + X^5Y + X^4Y^2 + X^3Y^3 + X^2Y^4 + XY^5 + Y^6,\\
\Phi_8(X,Y) &= X^4 + Y^4,\\
\Phi_9(X,Y) &= X^6 + X^3Y^3 + Y^6,\\
\Phi_{10}(X,Y) &= X^4 - X^3Y + X^2Y^2 - XY^3 + Y^4.
\end{aligned}$$

Multicyclotomic polynomials

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

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

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

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

Multicyclotomic polynomials and binary forms

When $k \geqslant 0$, and $n_1, \ldots, n_k$, satisfy $1 \leqslant n_1 < \cdots < n_k$, we write $\mathbf{n} = (n_1, \ldots, n_k)$ and

$$\phi_{\mathbf{n}}(T) = \phi_{n_1}(T)\phi_{n_2}(T) \ldots \phi_{n_k}(T),$$

Such an index $\mathbf{n}$ is called a *composition* of length k : it is a strictly increasing partition of $n_1 + \cdots + n_k$.
The degree of the polynomial $\phi_{\mathbf{n}}(T)$ is

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

The associated homogeneous binary form is

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

Multicyclotomic forms of small degree

Degree 1

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

Degree 2

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

Degree 3

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

Examples of multicyclotomic polynomials

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

More generally, for m odd $\geqslant 1$,

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

For $m \geqslant 1$,

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

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

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

Goldbach's Conjecture

Question : *Does there exists, for each integer $d \geqslant 3$, a composition $\mathbf{n}$ such that $2 \leqslant n_1 < \cdots < n_k$ with $k \leqslant 3$ and $\varphi(\mathbf{n}) = d$?*

Christian Goldbach

1690 – 1764

- if d is even and $d+2$ is a sum of two distinct primes, say $d+2 = p_1 + p_2$, then $d = \varphi(p_1) + \varphi(p_2)$.
- if d is even and $d+2 = 2p$, then $d = \varphi(3p)$.
- if d is odd and $d+1$ is a sum of two distinct primes, say $d+2 = p_1 + p_2$, then $d = \varphi(p_1) + \varphi(p_2) + \varphi(2)$.
- if d is odd and $d+1 = 2p$, then $d = \varphi(3p) + \varphi(2)$.

The number 15 is not a sum of two totients but $15 = \varphi(2) + \varphi(3) + \varphi(13)$.

Counting multicyclotomic polynomials

For $d \geqslant 1$, let $S(d)$ be the number of multicyclotomic polynomials of degree d. The generating series of the sequence $(S(d))_{d \geqslant 0}$ is

$$\sum_{d \geqslant 0} S(d) x^d = \prod_{q \geqslant 1} (1 + x^{\varphi(q)}).$$

The sequence $(S(d))_{d \geqslant 0}$ starts with

$$1, 2, 4, 6, 10, 14, 24, 34, 52, 70, 102, 134, 194, 254, 352, 450, \ldots$$

This is the sequence `https://oeis.org/A280611` :

`Number of degree` d `products of distinct cyclotomic polynomials.`

Partitions

For $d \geqslant 1$, $S(d)$ is the number of partitions of d into distinct parts of the form $\varphi(q)$:

$$d = \sum_{q \geqslant 1} \epsilon_q \varphi(q), \quad \epsilon_q \in \{0, 1\}.$$

Asymptotics :

$$S(d) = A d^{-3/4} \mathrm{e}^{B\sqrt{d}} \left(1 + O(1/\log d)\right),$$

where

$$A = \frac{1}{4\pi}(105\zeta(3)/2)^{1/4} = 0.2249\ldots$$

and

$$B = \frac{1}{\pi}(105\zeta(3)/2)^{1/2} = 2.52867\ldots$$

Cyclotomic partitions

David Boyd

Hugh Montgomery[1]

David W. Boyd & Hugh L. Montgomery. *Cyclotomic partitions.* In Number theory, Ed. Richard Mollin, Proceedings of the First Conference of the Canadian Number Theory Association held at the Banff Center, Banff, Alberta, April 17–27, 1988, 7-25. Walter de Gruyter & Co., Berlin, 1990.

`Zbl 0697.10040` `MR1106647`.

[1] Credit photo : Renate Schmid — Mathematisches Institut Oberwolfach (MFO),

Circle method : Ramanujan, Hardy, Littlewood

Srinivasan Ramanujan

1887 – 1920

Godfrey Harold Hardy

1877 – 1947

John Edensor Littlewood

1885 – 1977

Hardy, ICM Stockholm, 1916

Hardy and Ramanujan (1918) : partitions

Hardy and Littlewood (1920 – 1928) :
Some problems in Partitio Numerorum

Circle method

This method was further developed by Hardy, Littlewood, Rademacher, Vinogradov, Davenport,. . .
This gave rise to :

- Large Sieve
- Ternary Goldbach Conjecture
- Progress on binary Goldbach Conjecture
- Waring's problem

All these problems looked beyond reach before the birth of Circle method.

Hardy and Littlewood

References

H. W. Lenstra, Jr.
Vanishing sums of roots of unity, (1976)
Zbl 0411.12003

R. C. Vaughan
Coefficients of cyclotomic polynomials and related topics, (1989).
MR1203320

R. Thangadurai
On the coefficients of cyclotomic polynomials, (2000).
MR1802391

Carlo Sanna
A Survey on Coefficients of Cyclotomic Polynomials
https://arxiv.org/abs/2111.04034

section 11.2 Divisors of $X^n - 1$

Number of integers represented by a form

On the number of integers which are represented by a cyclotomic form (joint work with É. Fouvry and C. Levesque) (Acta Arithmetica 2018).

Étienne Fouvry

Claude Levesque

The number of integers $\leqslant N$ which are sums of two squares is asymptotically

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

where C_{Φ_4} is Ramanujan's Constant.

Number of integers represented by a form

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

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

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

$$\frac{N}{(\log N)^{3/4}}\left(\beta_0+\frac{\beta_1}{\log N}+\cdots+\frac{\beta_M}{(\log N)^M}+O\left(\frac{1}{(\log N)^{M+1}}\right)\right)$$

Forms of degree $\geqslant 3$

Axel Thue

1863 – 1922

Kurt Mahler

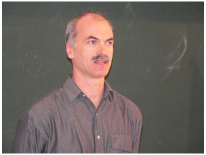
1903 – 1988

Let F be a binary form of degree $\geqslant 3$ with nonzero discriminant.
Thue's Theorem. Let $m \in \mathbb{Z} \setminus \{0\}$. Then the set of $(x, y) \in \mathbb{Z}^2$ such that $F(x, y) = m$ is finite.
Mahler's result. The number of $(x, y) \in \mathbb{Z}^2$ with $0 < |F(x, y)| \leqslant N$ is asymptotically $A_F N^{2/d}$ where

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

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

Stewart & Xiao



Cam L. Stewart

Stanley Yao Xiao

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $d \geqslant 3$ and non-zero discriminant.

The number of integers $m \in \mathbb{Z}$ *with* $|m| \leqslant N$ *of the form* $m = F(x,y)$ *with* $(x,y) \in \mathbb{Z}^2$ *is asymptotically*

$$\mathsf{C}_F \cdot N^{2/d} + O_{F,\varepsilon}\left(N^{\kappa_d+\varepsilon}\right),$$

with $\kappa_d < 2/d$, *where* $\mathsf{C}_F = A_F \cdot W_F$ *while* $W_F = W(\mathrm{Aut}F)$ *depends only on the group of automorphisms of* F.

C.L. Stewart & S. Yao Xiao, *On the representation of integers by binary forms*, Math. Ann. **375** (2019), 133–163.

`DOI: 10.4064/aa171012-24-12` `arXiv:1605.03427v2`

Isomorphism of binary forms

Two binary forms F and G in $\mathbb{Z}[X,Y]$ of degree $\geqslant 3$ with nonzero discriminant are *isomorphic* if there exists a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(\mathbb{Q})$ such that

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

With *Etienne Fouvry* :
if F and G are two non-isomorphic binary forms of degree $d \geqslant 3$ and nonzero discriminant,

Étienne Fouvry

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

Isomorphisms among two cyclotomic forms

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

The proof uses the following auxiliary result :

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

Number of integers represented by a cyclotomic form of degree $\geqslant d$

With Étienne Fouvry (Bull. Soc. Math. France 2020).

Let $d \geqslant 4$ be a totient. For $N \geqslant 2$, let $\mathcal{A}_d(N)$ be the number of integers m with $1 \leqslant m \leqslant N$ such that there exists integers (n, x, y) satisfying

$$\varphi(n) \geqslant d,\ \Phi_n(x,y) = m \textit{ and } \max\{|x|,|y|\} \geqslant 2.$$

Then as $N \to \infty$,

$$\mathcal{A}_d(N) = C_d N^{2/d} + O(N^{\beta_d})$$

with $\beta_d < 2/d$ and

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

Isomorphisms of multicyclotomic forms

The set of cyclotomic forms $\Phi_n(X,Y)$ with n not congruent to 2 modulo 4 is a complete set of isomorphism classes of cyclotomic forms.

Examples of isomorphisms of multicyclotomic forms :

For m_1 and m_2 odd positive integers

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

are isomorphic.
Also

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

are isomorphic.

Isomorphisms among two multicyclotomic forms

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

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

Write $\mathbf{n} = (n_1, \ldots, n_k)$ and $\tilde{\mathbf{n}} = (\tilde{n}_1, \ldots, \tilde{n}_{\tilde{k}})$.
We say that $\mathbf{n} \neq \tilde{\mathbf{n}}$ are *equivalent* if either they are equal, or if $k = \tilde{k}$ and there exists a permutation σ of $\{1, 2, \ldots, k\}$ such that, for all $j \in \{1, \ldots, k\}$, we have either $\tilde{n}_j = 2n_{\sigma(j)}$ with $n_{\sigma(j)}$ odd, or $\tilde{n}_j = n_{\sigma(j)}/2$ with $\tilde{n}_j$ odd.

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

A complete set of isomorphism classes of multicyclotomic forms

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

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

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

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

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

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

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

Automorphisms of forms of degree $\geqslant 3$

Let $F \in \mathbb{Z}[X,Y]$ be a binary form of degree $d \geqslant 3$ and non-zero discriminant. The group $\mathrm{Aut}F$ of automorphisms of F is a finite subgroup of $\mathrm{GL}_2(\mathbb{Q})$ (an automorphism permutes the roots of $F(t,1)$).

Let G_1 and G_2 be subgroups of $\mathrm{GL}_2(\mathbb{Q})$. We say that they are *equivalent under conjugation* if there is an element T in $\mathrm{GL}_2(\mathbb{Q})$ such that $G_1 = TG_2T^{-1}$.

Stewart & Xiao : There are 10 equivalence classes of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ under $\mathrm{GL}_2(\mathbb{Q})$–conjugation to which $\mathrm{Aut}F$ might belong.

Automorphisms of multicyclotomic forms

In $\mathrm{GL}(2,\mathbb{Q})$, there are 6 groups (and 4 classes) of automorphisms of multicyclotomic forms of degree $\geqslant 3$: one cyclic of order 2 and 5 dihedral groups of order 2, 4 or 8.

- $\mathbf{C}_2$ the cyclic subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 2 :

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \begin{pmatrix}-1 & 0\\ 0 & -1\end{pmatrix}, \qquad (X,Y) \longmapsto \pm(X,Y),$$

- $\mathbf{D}_1$ the dihedral subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 2 :

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}, \qquad (X,Y) \longmapsto (X,Y),\ (Y,X),$$

- $\mathbf{D}_1'$ dihedral subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 2 :

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \quad \begin{pmatrix}0 & -1\\ -1 & 0\end{pmatrix}, \qquad (X,Y) \longmapsto (X,Y),(-Y,-X).$$

Automorphisms of multicyclotomic forms

Two dihedral groups of order 4, one of order 8.

- $\mathbf{D}_2$ dihedral subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 4 :

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \pm\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\qquad (X,Y)\longmapsto \pm(X,Y),\ \pm(Y,X),$$

- $\mathbf{D}'_2$ dihedral subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 4 :

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \pm\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\qquad (X,Y)\longmapsto \pm(X,Y),\ \pm(X,-Y),$$

- $\mathbf{D}_4$ dihedral subgroup of $\mathrm{GL}(2,\mathbb{Q})$ of order 8 :

$$\pm\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \pm\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad \pm\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

corresponding to the transformations

$$(X,Y)\longmapsto \pm(X,Y),\ \pm(Y,X),\ \pm(X,-Y),\ \pm(Y,-X).$$

Automorphisms of cyclotomic forms of degree $\geqslant 3$

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

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

Etienne Fouvry & Michel Waldschmidt,
Sur la représentation des entiers par des formes cyclotomiques de grand degré, Bull. Soc. Math. France, **148** 2 (2020), 253-282.
arXiv: 1909.01892 [math.NT] Zbl 1455.11066 MR4124501
Corrigendum, to appear.

$\mathbf{D}_2$ $\qquad (X,Y) \longmapsto \pm(X,Y),\ \pm(Y,X)$

Let $\mathbf{n} = (n_1, \dots, n_k)$ with $k \geqslant 1$ and $1 \leqslant n_1 < \cdots < n_k$. When $n_1 \geqslant 3$, we have

$$\Phi_{\mathbf{n}}(X,Y) = \Phi_{\mathbf{n}}(-X,-Y) = \Phi_{\mathbf{n}}(Y,X) = \Phi_{\mathbf{n}}(-Y,-X),$$

hence the group of automorphisms $\mathrm{Aut}(\Phi_{\mathbf{n}}) \subset \mathrm{GL}(2,\mathbb{Q})$ contains the dihedral group $\mathbb{D}_2$ of order 4 which consists of the matrices

$$\pm\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \pm\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Examples with $\mathrm{Aut}(\Phi_{\mathbf{n}}) = \mathbf{D}_2$:

$$\Phi_5(X,Y) = X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4,$$
$$\Phi_{3,4}(X,Y) = X^4 + X^3Y + 2X^2Y^2 + XY^3 + Y^4.$$

$\mathbf{D}_4$ $\pm(X,Y)$, $\pm(Y,X)$, $\pm(X,-Y)$, $\pm(Y,-X)$

Condition $(\star)$:

$\{n_1,\dots,n_k\}=\{a_1,\dots,a_h,2a_1,\dots,2a_h,c_1,\dots,c_\ell\}$ with $a_1,\dots,a_h$ odd, $c_1,\dots,c_\ell$ multiples of 4, and $h\geqslant 0$, $k\geqslant 0$, $k=2h+\ell$.

If condition $(\star)$ is satisfied, then we also have

$$\Phi_{\mathbf{n}}(X,-Y)=\Phi_{\mathbf{n}}(-X,Y)=\Phi_{\mathbf{n}}(Y,-X)=\Phi_{\mathbf{n}}(-Y,X),$$

and therefore $\mathrm{Aut}(\Phi_{\mathbf{n}})$ also contains

$$\pm\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix},\quad \pm\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

hence contains the dihedral group $\mathbb{D}_4$ of order 8.

Examples with $\mathrm{Aut}(\Phi_{\mathbf{n}})=\mathbf{D}_4$:

$$\Phi_8(X,Y)=X^4+Y^4,\quad \Phi_{12}(X,Y)=X^4-X^2Y^2+Y^4,$$
$$\Phi_{3,6}(X,Y)=X^4-X^2Y^2+Y^4=\Phi_6(X^2,Y^2).$$

Automorphisms of a multicyclotomic form

Assume $\varphi(\mathbf{n}) \geqslant 3$. The group of automorphisms of $\Phi_{\mathbf{n}}$ is

• The dihedral group $\mathbb{D}_4$ of order 8 if $n_1 \geqslant 3$, and condition $(\star)$ is satisfied,

• The dihedral group $\mathbb{D}_2$ of order 4 if $n_1 \geqslant 3$ and condition $(\star)$ is not satisfied,

• The dihedral group $\mathbf{D}_1$ of order 2 if $n_1 = 2$,

• The dihedral group $\mathbf{D}_1'$ of order 2 if $n_1 = 1$ and $n_2 \geqslant 3$,

• The dihedral group $\mathbf{D}_1'$ of order 2 if $n_1 = 1$, $n_2 = 2$ and $\mathbf{n}$ satisfies $(\star)$,

• The cyclic group $\mathbf{C}_2$ of order 2 if $n_1 = 1$, $n_2 = 2$ and $\mathbf{n}$ does not satisfy $(\star)$.

$\mathbf{D}_1$ $\qquad (X,Y) \longmapsto (X,Y),\ (Y,X)$

$n_1 = 2$

Examples with $\mathrm{Aut}(\Phi_{\mathbf{n}}) = \mathbf{D}_1$:

$$\Phi_{2,3}(X,Y) = X^3 + 2X^2Y + 2XY^2 + Y^3,$$
$$\Phi_{2,4}(X,Y) = X^3 + X^2Y + XY^2 + Y^3,$$
$$\Phi_{2,5}(X,Y) = X^5 + 2X^4Y + 2X^3Y^2 + 2X^2Y^3 + 2XY^4 + Y^5.$$

$\mathbf{D}_1'$ $\qquad (X,Y) \longmapsto (X,Y),\ (-Y,-X)$

$n_1 = 1$ and $n_2 \geqslant 3$,
$n_1 = 1$, $n_2 = 2$ and $\mathbf{n}$ satisfies $(\star)$,

Examples with $\mathrm{Aut}(\Phi_{\mathbf{n}}) = \mathbf{D}_1'$:

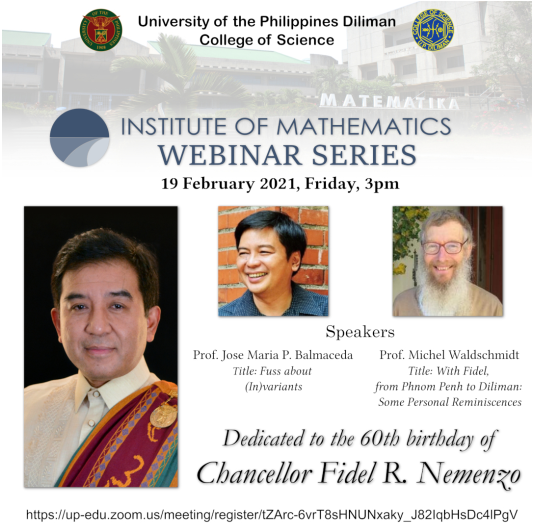
$$\Phi_{1,3}(X,Y) = X^3 - Y^3, \quad \Phi_{1,4}(X,Y) = X^3 - X^2Y + XY^2 + Y^3,$$
$$\Phi_{1,2,4}(X,Y) = X^4 - Y^4, \quad \Phi_{1,2,3,6}(X,Y) = X^6 - Y^6,$$

$\mathbf{C}_2$ $\qquad (X,Y) \longmapsto \pm(X,Y),$

$n_1 = 1$, $n_2 = 2$ and $\mathbf{n}$ does not satisfy $(\star)$.

Examples with $\mathrm{Aut}(\Phi_{\mathbf{n}}) = \mathbf{C}_2$:

$$\begin{aligned}\Phi_{1,2,3}(X,Y) &= X^4 + X^3Y - XY^3 - Y^4,\\ \Phi_{1,2,5}(X,Y) &= X^6 + X^5Y - XY^5 - Y^6\end{aligned}$$



University of the Philippines Diliman
College of Science

MATEMATIKA

INSTITUTE OF MATHEMATICS
WEBINAR SERIES

19 February 2021, Friday, 3pm

Speakers

Prof. Jose Maria P. Balmaceda
Title: Fuss about (In)variants

Prof. Michel Waldschmidt
Title: With Fidel, from Phnom Penh to Diliman: Some Personal Reminiscences

Dedicated to the 60th birthday of
Chancellor Fidel R. Nemenzo

https://up-edu.zoom.us/meeting/register/tZArc-6vrT8sHNUNxaky_J82IqbHsDc4IPgV

http://www.imj-prg.fr/~michel.waldschmidt/articles/pdf/FidelNemenzo60.pdf

Update *25/02/2026* *February 21, 2026*

CONGRUENCE & CONVERGENCE:

A Conference in Celebration of Fidel Nemenzo's 65th Birthday

21-23 FEBRUARY 2026
UNIVERSITY OF THE PHILIPPINES DILIMAN

On multicyclotomic polynomials and binary forms

Michel Waldschmidt

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