ACTA ARITHMETICA
Online First version

Representation of integers by cyclotomic binary forms

by

Étienne Fouvry (Orsay), Claude Levesque (Québec)
and Michel Waldschmidt (Paris)

Dedicated to Robert Tijdeman on the occasion of his 75th birthday

1. Introduction. K. Győry [G] obtained many interesting results on the representation of integers (resp. algebraic integers) by binary forms. He obtained sharp estimates, in contrast with the exponential bounds previously obtained on Thue's equations by means of Baker's results on lower bounds for linear forms in logarithms of algebraic numbers. The bibliography of [G] contains a useful selection of articles dealing with these problems, including [N1] and [N2].

Most particularly, Győry considered binary forms of degree d with integral coefficients,

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

which are products of ℓ irreducible forms, assuming that the roots of $F(X,1)$ are totally imaginary quadratic numbers over a totally real number field, and he proved that for $m \neq 0$, the solutions $(x,y) \in \mathbb{Z}^2$ of $F(X,Y) = m$ satisfy

$$|x| \le 2|a_d|^{1-(2\ell-1)/d}|m|^{1/d} \quad \text{and} \quad |y| \le 2|a_0|^{1-(2\ell-1)/d}|m|^{1/d}.$$

In other words, the splitting field of each irreducible factor of $F(X,1)$ is a *CM-field*, i.e., a totally imaginary quadratic extension of a totally real number field. In particular, cyclotomic fields are such number fields.

2010 *Mathematics Subject Classification*: Primary 11E76; Secondary 12E10.
Key words and phrases: cyclotomic binary forms, cyclotomic polynomials, Euler's totient function, families of Diophantine equations, Thue Diophantine equations, representation of integers by binary forms.
Received 12 October 2017; revised 9 December 2017.
Published online *.

DOI: 10.4064/aa171012-24-12

Examples of such binary forms with $a_0 = a_d = 1$ are given by the cyclotomic binary forms, which we define as follows. For $n \geq 1$, denote by $\phi_n(X)$ the cyclotomic polynomial of index n and degree $\varphi(n)$ (Euler's totient function). Following [N2, Section 6], the *cyclotomic binary form* $\Phi_n(X,Y)$ is defined by $\Phi_n(X,Y) = Y^{\varphi(n)}\phi_n(X/Y)$. In particular, we have $\Phi_n(x,y) > 0$ for $n \geq 3$ and $(x,y) \neq (0,0)$ (see §4 below).

In the special case of cyclotomic binary forms, Győry [G] proves

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

for the integral solutions (x,y) of $\Phi_n(X,Y) = m$. In contrast with our Theorem 1.1 below, Győry gives an upper bound for n only if $\max\{|x|,|y|\} \geq 3$.

Here is our first main result, in which we exclude the cases $n = 1$ and $n = 2$, for which the cyclotomic polynomial ϕ_n is linear.

THEOREM 1.1. *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*

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

In particular, there is no solution when $m \in \{1,2\}$.

From the lower bound,

$$\varphi(n) > \left(\frac{n}{2.685}\right)^{1/1.161},$$

proved in six lines in [M–W], we deduce that the upper bound $\varphi(n) < 2(\log m)/\log 3$ of Theorem 1.1 implies

$$n < 5.383(\log m)^{1.161}. \tag{1.1}$$

Theorem 1.1 is a refinement of Győry's above-mentioned result for these cyclotomic binary forms. Subject to $\text{GCD}(x,y) = 1$, Nagell (see [N1, Lemma 1, p. 155]) comes up with a slightly larger bound than ours for $\varphi(n)$, namely he has $\varphi(n) < (4\log m)/(3\log 2)$, and he does not exhibit a bound for $\max\{|x|,|y|\}$.

The estimates of Theorem 1.1 are optimal because for $\ell \geq 1$,

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

If we assume $\varphi(n) > 2$, so $\varphi(n) \geq 4$, the conclusion of Theorem 1.1 can be replaced by

$$\varphi(n) \leq \frac{4}{\log 11}\log m \quad \text{and} \quad \max\{|x|,|y|\} \leq c_5^{-1/4} m^{1/\varphi(n)}$$

thanks to (5.1) (the constant c_5 is defined in Section 4). Again these estimates are best possible ([1]).

There are infinitely many integers n such that $\Phi_n(1,2) < 2^{\varphi(n)}$; for instance, $n = 2 \cdot 3^e$ with $e \geq 1$. We will prove the following.

THEOREM 1.2. *For $\theta \in]0,1[$, there are only finitely many triples (n,x,y) with $n \geq 3$ and $\max\{|x|,|y|\} \geq 2$ such that $\Phi_n(x,y) \leq 2^{\theta\varphi(n)}$; these triples can be effectively determined and they satisfy $\max\{|x|,|y|\} = 2$.*

As a matter of fact, we shall see that $\max\{|x|,|y|\} = 2$ follows from the weaker assumption

$$\Phi_n(x,y) < 7^{\varphi(n)/2},$$

which is optimal since $\Phi_3(1,-3) = 7$.

Theorem 1.1 shows that, for each integer $m \geq 1$, the set

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

is finite. The finiteness of the subset of (n,x,y) subject to the stronger condition $\max\{|x|,|y|\} \geq 3$ follows from [G], but not for $\max\{|x|,|y|\} \geq 2$. Let us denote by a_m the number of elements in the above set. The positive integers m such that $a_m \geq 1$ are the integers which are represented by a cyclotomic binary form. We will see in §7 that the sequence of integers $m \geq 1$ such that $a_m \geq 1$ starts with the following values of a_m [OEIS, A296095 and A299214]:

Table 1

m	3	4	5	7	8	9	10	11	12	13	16	17	18	19	20
a_m	8	16	8	24	4	16	8	8	12	40	40	16	4	24	8

The only result in this direction that we found in the literature is $a_1 = 0$: see [G, N1, N2].

For $N \geq 1$ and $n \geq 3$ let $\mathcal{A}(\Phi_n; N)$ be the set of positive integers $m \leq N$ which are in a restricted image of $\mathbb{Z}^2$ by Φ_n. In other words, for $n \geq 3$ we define

$$\mathcal{A}(\Phi_n; N) := \big\{m \in \mathbb{N} \bigm| m \leq N,\ m = \Phi_n(x,y) \text{ for some } (x,y) \in \mathbb{Z}^2 \text{ with } \max\{|x|,|y|\} \geq 2\big\}.$$

The following theorem describes the asymptotic cardinality of the set of values taken by the polynomials Φ_n for $n \geq 3$. Defining

$$\mathcal{A}(\Phi_{\{n\geq 3\}}; N) := \bigcup_{n\geq 3} \mathcal{A}(\Phi_n; N),$$

we have

([1]) We thank Peter Luschny for pointing out an inaccuracy in a previous version of this remark.

THEOREM 1.3. *There exist sequences* (α_h) *and* (β_h) *(with* $\alpha_0 > 0$ *and* $\beta_0 > 0$*) such that, for every* $M \geq 0$*, uniformly for* $N \geq 2$*,*

(1.2)
$$|\mathcal{A}(\Phi_{\{n\geq 3\}}; N)| = \frac{N}{(\log N)^{1/2}} \left\{ \left(\alpha_0 - \frac{\beta_0}{(\log N)^{1/4}}\right) + \frac{1}{\log N}\left(\alpha_1 - \frac{\beta_1}{(\log N)^{1/4}}\right) + \cdots + \frac{1}{(\log N)^M}\left(\alpha_M - \frac{\beta_M}{(\log N)^{1/4}}\right) + O\left(\frac{1}{(\log N)^{M+1}}\right)\right\}.$$

The proof of this theorem will be given in §6 with the precise definitions of the coefficients α_0 and β_0. This proof will show that the largest contribution to $|\mathcal{A}(\Phi_{\{n\geq 3\}}; N)|$ comes from the sets $\mathcal{A}(\Phi_3; N)$ and $\mathcal{A}(\Phi_4; N)$.

It follows from Theorem 1.3 that the set of integers m such that $a_m \neq 0$ has natural density 0. Combining Theorem 1.3 with Lemma 5.1, we will deduce that the average of the nonzero values of a_m grows like $\sqrt{\log m}$. More precisely, we have the following.

COROLLARY 1.4. *For* $N \geq 1$*, define*

$$A_N = |\mathcal{A}(\Phi_{\{n\geq 3\}}; N)| \quad \textit{and} \quad M_N = \frac{1}{A_N}(a_1 + \cdots + a_N).$$

Then there exists a positive absolute constant κ_1 *such that*

$$M_N \sim \kappa_1 \sqrt{\log N}.$$

In particular, the sequence $(a_m)_{m\geq 1}$ is unbounded; this follows from the fact that the number of representations of a positive integer by the quadratic form $\Phi_4(X,Y)$ is an unbounded sequence. The same is true for the quadratic forms $\Phi_3(X,Y)$ and $\Phi_6(X,Y)$.

In Lemma 5.1, we will prove that the number C_N of integers $\leq N$ which are represented by a binary form $\Phi_n(X,Y)$ with $\varphi(n) > 2$ and $\max\{|x|,|y|\} \geq 2$ is less than $\kappa_2 N^{1/2}$ where κ_2 is a positive absolute constant.

For $m \geq 1$, denote by b_m the number of elements in the set

$$\left\{(n,x,y) \in \mathbb{N} \times \mathbb{Z}^2 \;\middle|\; \varphi(n) > 2,\ \max\{|x|,|y|\} \geq 2,\ \Phi_n(x,y) = m\right\}.$$

We will see in the last section that for m between 1 and 100, there are exactly 16 values of m for which b_m is different from 0:

Table 2

m	11	13	16	17	31	32	43	55	57	61	64	73	80	81	82	97
b_m	8	8	24	8	8	4	8	8	8	16	24	16	4	24	8	8

LEMMA 1.5. *We have*

$$\limsup_{m\to\infty} \frac{b_m \log\log\log m}{\log\log m} \geq 8,$$

and therefore the sequence $(b_m)_{m\geq 1}$ *is unbounded.*

Proof. For the sth odd prime p_s, consider the integer

$$k_s = \varphi(3\cdot 5\cdots p_s),$$

the product being taken over all the primes between 3 and p_s. Set $m_s = 2^{k_s}$. Then $\Phi_n(x,y) = m_s$ for at least $8s$ values of (n,x,y), namely

$$(\ell, 0, \pm 2^t), \quad (\ell, \pm 2^t, 0), \quad (2\ell, 0, \pm 2^t), \quad (2\ell, \pm 2^t, 0),$$

for each prime ℓ between 3 and p_s with $t = k_s/\varphi(\ell)$. Therefore, by excluding $\ell = 3$ we have $b_{m_s} \geq 8(s-1)$.

Because

$$\log k_s = \sum_{3\leq p\leq p_s} \log(p-1),$$

the Prime Number Theorem implies that for $s\to\infty$ we have

$$\log k_s \sim p_s \sim s\log s,$$

hence

$$s \sim \frac{\log k_s}{\log\log k_s} \quad \text{with} \quad k_s = \frac{\log m_s}{\log 2}$$

and

$$s \sim \frac{\log\log m_s}{\log\log\log m_s}.$$

This completes the proof of Lemma 1.5. ∎

2. Positive definite binary forms. Consider a Thue equation $F(X,Y) = m$ associated with the polynomial $f(X)$ defined by $f(X) = F(X,1)$, where $f(X)$ has no real roots and has positive values on $\mathbb{R}$. This is the case for cyclotomic polynomials. Such a situation was also considered in [G]. The following result shows that the study of the associated Diophantine equation $F(X,Y) = m$ reduces to finding a lower bound for the values of $f(t)$ on $\mathbb{R}$.

LEMMA 2.1. *Let* $f(X)\in\mathbb{Z}[X]$ *be a nonzero polynomial of degree* d *which has no real root. Let* $g(X) = X^d f(1/X)$. *Assume that the leading coefficient of* $f(X)$ *is positive, so that the real numbers defined by*

$$\gamma_1 = \inf_{t\in\mathbb{R}} f(t), \qquad \gamma_2 = \inf_{t\in\mathbb{R}} g(t),$$

$$\gamma_1' = \inf_{-1\leq t\leq 1} f(t), \quad \gamma_2' = \inf_{-1\leq t\leq 1} g(t), \quad \gamma' = \min\{\gamma_1', \gamma_2'\}$$

are >0. *Let* $F(X,Y)$ *be the binary form* $Y^d f(X/Y)$ *associated with* $f(X)$.

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

$$F(x,y)\geq\gamma_1|y|^d,\qquad F(x,y)\geq\gamma_2|x|^d,\qquad F(x,y)\geq\gamma'\max\{|x|^d,|y|^d\}.$$

(2) *The following statements hold true:*

(i) *For any real number* c_1 *with* $c_1>\gamma_1$, *there exist infinitely many couples* (x,y) *in* $\mathbb{Z}^2$ *satisfying* $y>0$ *and*

$$F(x,y)<c_1y^d.$$

(ii) *For any real number* c_2 *with* $c_2>\gamma_2$, *there exist infinitely many couples* (x,y) *in* $\mathbb{Z}^2$ *satisfying* $x>0$ *and*

$$F(x,y)<c_2x^d.$$

(iii) *For any real number* c *with* $c>\gamma'$, *there exist infinitely many couples* (x,y) *in* $\mathbb{Z}^2$ *satisfying*

$$F(x,y)<c\max\{|x|^d,|y|^d\}.$$

Before proceeding to the proof, some remarks are in order. For $|t|>1$, from $g(t)=t^df(1/t)$ we deduce $f(1/t)\leq g(t)$. Hence

$$\inf_{-1\leq t\leq 1}|f(t)|\leq\inf_{|t|\geq 1}|g(t)|.$$

Therefore, if we set

$$\gamma_1''=\inf_{|t|\geq 1}f(t),\qquad\gamma_2''=\inf_{|t|\geq 1}g(t),$$

then

$$\gamma_1=\min\{\gamma_1',\gamma_1''\},\qquad\gamma_2=\min\{\gamma_2',\gamma_2''\},\qquad\gamma_2'\leq\gamma_1'',\qquad\gamma_1'\leq\gamma_2''.$$

Hence

$$\gamma'=\min\{\gamma_1',\gamma_2'\}\leq\min\{\gamma_1'',\gamma_2''\}\leq\max\{\gamma_1,\gamma_2\}.$$

It follows that for a reciprocal polynomial f we have $\gamma_1=\gamma_2=\gamma_1'=\gamma_2'=\gamma'$; in particular, for a reciprocal f,

$$\inf_{t\in\mathbb{R}}f(t)=\inf_{|t|\leq 1}f(t).\tag{2.1}$$

Proof of Lemma 2.1. (1) The proof of the first two lower bounds is direct. Let us prove the third one. It is plain that

$$F(x,y)\geq\gamma_1'|y|^d\quad\text{for } |x|\leq|y|\quad\text{and}\quad F(x,y)\geq\gamma_2'|x|^d\quad\text{for } |x|\geq|y|,$$

and the third lower bound follows.

(2) Here we prove that the lower bounds of (1) are optimal.

(i) Let $t_0\in\mathbb{R}$ be such that $f(t_0)=\gamma_1$. There exists a real number $a>0$ such that, for $t\in\,]t_0-a,t_0+a[$,

$$|f(t)-\gamma_1|\leq(|f'(t_0)|+1)(t-t_0).$$

For $y > 0$, let x in $\mathbb{Z}$ be such that

$$|t_0 - x/y| \le 1.$$

For y sufficiently large, x/y is in $]t_0 - a, t_0 + a[$ and we have

$$|F(x,y) - y^d f(t_0)| \le (|f'(t_0)| + 1)y^{d-1}.$$

As a consequence, for y sufficiently large,

$$F(x,y) < c_1 y^d.$$

(ii) is proved in the same way.

(iii) Assume first $c > \gamma_1'$. Suppose $-1 \le t_0 \le 1$. Our argument above gives infinitely many couples (x,y) in $\mathbb{Z}^2$ with $F(x,y) < c|y|^d$ and $|y| \le |x|$. Hence

$$F(x,y) < c \max\{|x|^d, |y|^d\}.$$

The same argument, starting with $|t_0| \ge 1$, gives infinitely many couples (x,y) with $F(x,y) < c|x|^d$ and $|x| \le |y|$. The case $c > \gamma_2'$ is proved in the same way. ∎

Let us mention in passing that Győry [G, p. 364] exhibited Thue equations which have as many (nonzero) solutions as one pleases, by allowing the degree to be large enough. Let us give a similar example. Let c_j $(j = 1, \ldots, \ell)$ be different rational integers and let $c > 0$ be any fixed integer. Consider the binary form $F(X,Y)$ of degree 2ℓ defined by

$$F(X,Y) = \prod_{j=1}^{\ell} (X - c_j Y)^2 + cY^{2\ell}.$$

Here $F(x,y) > 0$ for all $(x,y) \in \mathbb{R}^2 \setminus \{(0,0)\}$. Moreover, for $j = 1, \ldots, \ell$, we have $F(c_j, 1) = c$, and the minimum value on the real axis of the associated polynomial $f(X)$, defined by $F(X,1)$, is c.

3. On cyclotomic polynomials. The cyclotomic polynomials $\phi_n(X) \in \mathbb{Z}[X]$, $n \ge 1$, are defined by the formula

$$\phi_n(X) = \prod_{\zeta \in E_n} (X - \zeta) \tag{3.1}$$

where E_n is the set of primitive roots of unity of order n. One can also define them via the recurrence provided by

$$X^n - 1 = \prod_{d \mid n} \phi_d(X). \tag{3.2}$$

The degree of $\phi_n(X)$ is $\varphi(n)$, where φ is Euler's totient function. We will always suppose that $n \ge 3$, so $\varphi(n)$ is always even. For $n \ge 3$, the polynomial $\phi_n(X)$ has no real root.

Two important formulas for cyclotomic polynomials are the following: when n is an integer ≥ 1 written as $n = p^r m$ with p a prime and $\mathrm{GCD}(p, m) = 1$, we have

$$\phi_n(X) = \frac{\phi_m(X^{p^r})}{\phi_m(X^{p^{r-1}})} \quad \text{and} \quad \phi_n(X) = \phi_{pm}(X^{p^{r-1}}). \tag{3.3}$$

We will use the following properties:

(i) The nth cyclotomic polynomial can be defined by

$$\phi_n(X) = \prod_{d|n} (X^d - 1)^{\mu(n/d)}, \tag{3.4}$$

where μ is the Möbius function.

(ii) 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,

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

Then

$$\phi_n(X) = \phi_R(X^{n/R}). \tag{3.5}$$

(iii) Let $n = 2m$ with m odd ≥ 3. Then

$$\phi_n(X) = \phi_m(-X). \tag{3.6}$$

4. The invariants c_n. The real number

$$c_n = \inf_{t \in \mathbb{R}} \phi_n(t)$$

is always > 0 for $n \geq 3$; this invariant c_n will play a major role in this paper. Since the cyclotomic polynomials are reciprocal, we deduce from (2.1) that

$$c_n = \inf_{-1 \leq t \leq 1} \phi_n(t). \tag{4.1}$$

PROPOSITION 4.1. *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*

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

Here are the first values of c_n for n odd and squarefree, with for each n a value of $t_n \in \,]-1, 1[$ such that $c_n = \phi_n(t_n)$:

Table 3

n	c_n	t_n	n	c_n	t_n	n	c_n	t_n
3	0.75	−0.5	19	0.562...	−0.822...	37	0.536...	−0.889...
5	0.673...	−0.605...	21	0.496...	0.723...	39	0.433...	0.808...
7	0.635...	−0.670...	23	0.553...	−0.844...	41	0.533...	−0.897...
11	0.595...	−0.747...	29	0.544...	−0.867...	43	0.531...	−0.900...
13	0.583...	−0.772...	31	0.541...	−0.873...	47	0.529...	−0.907...
15	0.544...	0.669...	33	0.447...	0.787...	51	0.414...	0.838...
17	0.567...	−0.808...	35	0.375...	0.782...	53	0.526...	−0.915...

Proof of Proposition 4.1. In view of the properties (3.5) and (3.6), we may restrict to the case where n is odd and squarefree.

We plan to prove

$$\phi_{p_1\cdots p_r}(t) \geq \frac{1}{p_1^{2^{r-2}}} \tag{4.2}$$

for $r \geq 1$ and $-1 \leq t \leq 1$.

We start with the case $r = 1$. Let p be an odd prime. For $-1 \leq t \leq 0$, we have $1 \leq 1 - t^p \leq 1 - t \leq 2$, hence

$$1/2 \leq \phi_p(t) \leq 1. \tag{4.3}$$

For $0 \leq t \leq 1$, we have $0 \leq 1-t \leq 1-t^p \leq 1$ and $\phi_p(t) = 1+t+t^2+\cdots+t^{p-1}$, so

$$1 \leq \phi_p(t) \leq p. \tag{4.4}$$

We deduce $1/2 \leq \phi_p(t) \leq p$ for $-1 \leq t \leq 1$. Since $c_3 = 3/4$, this completes the proof of (4.2) for $r = 1$.

Assume now $r \geq 2$. Using (3.4) for $n = p_1 \cdots p_r$, we express $\phi_n(t)$ as a product of 2^{r-1} factors, half of which are of the form $\phi_{p_1}(t^d)$, while the other half are of the form $1/\phi_{p_1}(t^d)$, where d is a divisor of $p_2 p_3 \cdots p_r$.

For $t \in [-1, 0]$, using (4.3), we have

$$1/2 \leq \phi_{p_1}(t) \leq 1 \quad \text{and} \quad 1/2 \leq \phi_{p_1}(t^d) \leq 1,$$

hence

$$\frac{1}{2^{2^{r-2}}} \leq \phi_{p_1\cdots p_r}(t) \leq 2^{2^{r-2}}. \tag{4.5}$$

For $t \in [0, 1]$, using (4.4), we have

$$1 \leq \phi_{p_1}(t) \leq p_1 \quad \text{and} \quad 1 \leq \phi_{p_1}(t^d) \leq p_1,$$

and so

$$\frac{1}{p_1^{2^{r-2}}} \leq \phi_{p_1\cdots p_r}(t) \leq p_1^{2^{r-2}}. \tag{4.6}$$

From (4.5) and (4.6), we conclude that (4.2) is true. Thanks to (4.1), inequality (4.2) can be written as

$$\log c_n \geq -2^{r-2} \log p_1. \ \blacksquare$$

We need an auxiliary result.

Lemma 4.2. *For any odd squarefree integer* $n = p_1 \cdots p_r$ *with* $p_1 < \cdots < p_r$ *satisfying* $n \geq 11$ *and* $n \neq 15$, *we have*

$$\varphi(n) > 2^{r+1} \log p_1. \tag{4.7}$$

Proof. If $r = 1$, then n is a prime ≥ 11 and (4.7) is true with $p_1 = n$. If $r = 2$, $n \neq 15$, we have $p_2 \geq 7$, hence

$$\varphi(p_1 p_2) = (p_1 - 1)(p_2 - 1) > 6(p_1 - 1) > 8 \log p_1,$$

so (4.7) is true.

Assume $r \geq 3$. Then

$$\begin{aligned}\varphi(n) &= (p_1 - 1)(p_2 - 1) \cdots (p_r - 1) \\ &> (p_1 - 1)2^{2(r-1)} \geq (p_1 - 1)2^{r+1} > 2^{r+1} \log p_1. \ \blacksquare\end{aligned}$$

We deduce the following consequence.

Proposition 4.3. *For* $n \geq 3$, *we have*

$$c_n \geq (\sqrt{3}/2)^{\varphi(n)}.$$

This lower bound is best possible, since there is equality for $n = 3$ (and for $n = 6$).

Proof of Proposition 4.3. It suffices to check the inequality when n is odd and squarefree, say $n = p_1 \cdots p_r$ where $p_1 < \cdots < p_r$ with $r \geq 1$. The lower bound is true for $n = 3$ (with equality, since $c_3 = 3/4$), and also for $n = 5$, for $n = 7$ and for $n = 15$, since

$$c_5 > 0.6 > (\sqrt{3}/2)^4, \quad c_7 > 0.6 > (\sqrt{3}/2)^6, \quad c_{15} > 0.5 > (\sqrt{3}/2)^8.$$

Using Proposition 4.1(ii) and Lemma 4.2, we have

$$8 \log c_n \geq -2^{r+1} \log p_1 \geq -\varphi(n),$$

which implies

$$c_n \geq e^{-\varphi(n)/8} \geq (\sqrt{3}/2)^{\varphi(n)}$$

since $\log(2/\sqrt{3}) > 1/8$. ■

Proposition 4.3 will be sufficient for the proofs of Theorems 1.1 and 1.2 and Lemma 5.1. However, it may be of independent interest to state further properties of c_n, which are easy to prove.

For p an odd prime number, the derivative $\phi_p'(t)$ has a unique real root; it lies in $]-1, -1/2]$ and will be denoted t_p.

- For $p = 3$, we have $t_3 = -1/2$.
- For p an odd prime number, one has $c_p = pt_p^{p-1}$.
- The sequence $(t_p)_{p \text{ odd prime}}$ is decreasing and converges to -1; in fact,

$$-1 + \frac{\log(2p)}{p} - \frac{(\log(2p))^2}{2p^2} < t_p < -1 + \frac{\log(2p)}{p} + \frac{\log(2p)}{p^2}.$$

- The sequence $(c_p)_{p \,\text{odd prime}}$ is decreasing and converges to $1/2$; in fact,

$$c_p = \frac{1}{2} + \frac{1 + \log(2p)}{4p} + \frac{\nu_p(\log p)^2}{p^2} \qquad \text{with } |\nu_p| \leq \frac{1}{4}\cdot$$

- Let p_1 and p_2 be primes. Then

$$c_{p_1 p_2} \geq \frac{1}{p_1}\cdot$$

Further, for any prime p_1,

$$\lim_{p_2 \to \infty} c_{p_1 p_2} = \frac{1}{p_1}\cdot$$

- We have $\liminf_{n\to\infty} c_n = 0$ and $\limsup_{n\to\infty} c_n = 1$.

5. Proofs of Theorems 1.1 and 1.2

Proof of Theorem 1.1. Assume

$$\Phi_n(x, y) = m$$

with $n \geq 3$ and $\max\{|x|, |y|\} \geq 2$. Using Lemma 2.1, we deduce

$$c_n \max\{|x|, |y|\}^{\varphi(n)} \leq m. \tag{5.1}$$

From Proposition 4.3 we get

$$\left(\frac{\sqrt{3}}{2} \max\{|x|, |y|\}\right)^{\varphi(n)} \leq m. \tag{5.2}$$

Since $\max\{|x|, |y|\} \geq 2$, we deduce the desired upper bound for $\varphi(n)$:

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

Using again (5.2), we arrive at

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

Proof of Theorem 1.2. We first prove that if the triple (n, x, y) satisfies

$$n \geq 3, \quad \max\{|x|, |y|\} \geq 2, \quad \Phi_n(x, y) < 7^{\varphi(n)/2},$$

then $\max\{|x|, |y|\} = 2$. Using Maple [M], we check that this property holds for $n \in \{3, 5, 7, 15\}$, namely, each of the inequalities

$$\Phi_3(x, y) < 7, \quad \Phi_5(x, y) < 7^2, \quad \Phi_7(x, y) < 7^3, \quad \Phi_{15}(x, y) < 7^4$$

implies $\max\{|x|, |y|\} = 2$.

For n an odd squarefree integer $\notin \{3,5,7,15\}$, according to (4.7), we have

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

Since $\log(3/\sqrt{7}) > 1/8$, we deduce from (5.1) and Proposition 4.1 that the assumption $\Phi_n(x,y) < 7^{\varphi(n)/2}$ implies

$$\begin{aligned}\varphi(n)\log\max\{|x|,|y|\} \le \log\Phi_n(x,y) - \log c_n &< \frac{\varphi(n)}{2}\log 7 + 2^{r-2}\log p_1\\ &< \left(\frac{1}{2}\log 7 + \frac{1}{8}\right)\varphi(n) < \varphi(n)\log 3,\end{aligned}$$

hence $\max\{|x|,|y|\} < 3$ and therefore $\max\{|x|,|y|\} = 2$. Since $2\log 2 < \log 7$, we deduce that the assumptions $n \ge 3$, $\max\{|x|,|y|\} \ge 2$, and $\Phi_n(x,y) \le 2^{\varphi(n)}$ imply $\max\{|x|,|y|\} = 2$.

Let $\theta \in\,]0,1[$ and let $n \ge 3$, $\max\{|x|,|y|\} \ge 2$, and $\Phi_n(x,y) \le 2^{\theta\varphi(n)}$. Then

$$c_n \le 2^{(\theta-1)\varphi(n)}.$$

Proposition 4.1 implies

$$(1-\theta)(\log 2)\varphi(n) \le 2^{r-2}\log p_1.$$

It remains to check that the set of odd squarefree integers n satisfying this condition is bounded. Indeed, if $r = 1$, then $n = p_1$ satisfies

$$2(\log 2)(1-\theta)(p_1-1) \le \log p_1,$$

hence p_1 is bounded. If $r \ge 2$, then the condition

$$(1-\theta)(\log 2)(p_1-1)(p_2-1)(p_3-1)\cdots(p_r-1) \le 2^{r-2}\log p_1$$

shows that $p_1\cdots p_r$ is bounded. ∎

The proofs of Theorem 1.3 and Corollary 1.4 will use the following result, the proof of which rests on Proposition 4.3.

Lemma 5.1. *Let $d > 2$. There exists an effectively computable positive constant $C(d)$ such that the number of triples (n,x,y) in $\mathbb{N}\times\mathbb{Z}^2$ which satisfy $\varphi(n) \ge d$, $\max\{|x|,|y|\} \ge 2$ and $\Phi_n(x,y) < N$ is bounded by $C(d)N^{2/d}$.*

Given a positive integer N and a binary form $F(X,Y)$ of degree d, with integer coefficients and nonzero discriminant, denote by $R_F(N)$ the number of integers of absolute value at most N which are represented by $F(X,Y)$. In [S–X], the authors quote the foundational work of Fermat, Lagrange, Legendre and Gauss concerning the case where F is a binary quadratic form, and a result of Erdős and Mahler (1938) for forms of higher degrees. They prove that for $d \ge 3$, there exists a positive constant $C_F > 0$ such that

$R_F(N)$ is asymptotic to $C_F N^{2/d}$. Lemma 5.1 concerns a sequence of forms having no real zero, a situation which is easier to deal with.

Proof of Lemma 5.1. If $m < N$ is represented by $\Phi_n(x, y)$ with $\varphi(n) \geq d$, then $\Phi_n(x, y) < N$, hence by (5.1) we have $c_n 2^{\varphi(n)} < N$. From Proposition 4.3 we deduce $3^{\varphi(n)/2} < N$, so $\varphi(n) < (2 \log N)/\log 3$. Next, from (5.2) we deduce

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

which proves that for each n, the number of (x, y) is bounded by $(16/3)N^{2/d}$. From (1.1) we deduce that the number of triples (n, x, y) in $\mathbb{N} \times \mathbb{Z}^2$ which satisfy $\varphi(n) \geq d$, $\max\{|x|, |y|\} \geq 2$ and $\Phi_n(x, y) < N$ is bounded by $29N^{2/d}(\log N)^{1.161}$.

Now we consider two cases. If there is no n with $\varphi(n) = d$, then we deduce the sharper upper bound $29N^{2/(d+1)}(\log N)^{1.161}$. If the set $\{n_1, \dots, n_k\}$ of integers n satisfying $\varphi(n) = d$ is not empty, for $1 \leq j \leq k$ the number of couples (x, y) in $\mathbb{Z}^2$ satisfying $\max\{|x|, |y|\} \geq 2$ and $\Phi_{n_j}(x, y) < N$ is bounded by $(16/3)N^{2/d}$, while the number of triples (n, x, y) in $\mathbb{N} \times \mathbb{Z}^2$ with $\varphi(n) > d$, $\max\{|x|, |y|\} \geq 2$ and $\Phi_n(x, y) < N$ is bounded by $29N^{2/(d+1)}(\log N)^{1.161}$. Since k is bounded in terms of d, Lemma 5.1 follows. ■

6. Proofs of Theorem 1.3 and Corollary 1.4. We start from an easy inequality concerning the cardinality of the union of finite sets:

(6.1)
$$\Big||\mathcal{A}(\Phi_{\{n\geq 3\}}; N)| - \big(|\mathcal{A}(\Phi_3; N)| + |\mathcal{A}(\Phi_4; N)| - |\mathcal{A}(\Phi_3; N) \cap \mathcal{A}(\Phi_4; N)|\big)\Big| \leq \Big|\bigcup_{\varphi(n)\geq 4} \mathcal{A}(\Phi_n; N)\Big|.$$

By Lemma 5.1 the right-hand side of (6.1) is $O(N^{1/2})$, which is absorbed by the error term of (1.2). So we are led to study the cardinalities of three sets: $\mathcal{A}(\Phi_3; N)$, $\mathcal{A}(\Phi_4; N)$ and $\mathcal{A}(\Phi_3; N) \cap \mathcal{A}(\Phi_4; N)$. For algebraic reasons, it is better to consider for $k \in \{3, 4\}$ the larger sets

$$\tilde{\mathcal{A}}(\Phi_k; N) := \big\{m \in \mathbb{N} \mid m \leq N, m = \Phi_n(x, y) \text{ for some } (x, y) \in \mathbb{Z}^2 \setminus \{(0, 0)\}\big\},$$

which differ from $\mathcal{A}(\Phi_k; N)$ by at most two terms. In conclusion, the proof of Theorem 1.3 will be complete (with $\alpha_h = \alpha_h^{(3)} + \alpha_h^{(4)}$, $h \geq 0$) as soon as we prove

Proposition 6.1. *There exist sequences* $(\alpha_h^{(3)})$, $(\alpha_h^{(4)})$ *and* (β_h) $(h \geq 0)$ *of real numbers, with* $\alpha_0^{(3)}, \alpha_0^{(4)}, \beta_0 > 0$, *such that for every for* $M \geq 0$, *uniformly for* $N \geq 2$,

$$(6.2)\qquad |\tilde{\mathcal{A}}(\Phi_k;N)| = \frac{N}{(\log N)^{1/2}}\biggl\{\alpha_0^{(k)} + \frac{\alpha_1^{(k)}}{\log N} + \cdots + \frac{\alpha_M^{(k)}}{(\log N)^M} + O\biggl(\frac{1}{(\log N)^{M+1}}\biggr)\biggr\} \qquad (k=3,4)$$

and

$$(6.3)\qquad |\tilde{\mathcal{A}}(\Phi_3;N) \cap \tilde{\mathcal{A}}(\Phi_4;N)| = \frac{N}{(\log N)^{3/4}}\biggl\{\beta_0 + \frac{\beta_1}{\log N} + \cdots + \frac{\beta_M}{(\log N)^M} + O\biggl(\frac{1}{(\log N)^{M+1}}\biggr)\biggr\}.$$

The proof of this proposition occupies the next three subsections. We will exploit the fact that Φ_3 and Φ_4 are binary quadratic forms, which also are the norms of integers of imaginary quadratic fields with class number 1. Finally, the characteristic functions of the sets $\tilde{\mathcal{A}}(\Phi_k;\infty)$ for $k \in \{3,4\}$ are studied by analytic methods via the theory of Dirichlet series.

6.1. Algebraic background. We fix some notation. The letter p is reserved for primes. If a and q are two integers, we denote by $N_{a,q}$ any integer ≥ 1 satisfying the condition

$$p \mid N_{a,q} \;\Rightarrow\; p \equiv a \bmod q.$$

PROPOSITION 6.2. *The following equivalences hold true:*

(i) *An integer* $n \geq 1$ *is of the form*

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

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

$$n = 2^a N_{3,4}^2 N_{1,4}.$$

(ii) *An integer* $n \geq 1$ *is of the form*

$$n = \Phi_3(u,v) = \Phi_6(u,-v) = u^2 + uv + v^2$$

if and only if there exist integers $b \geq 0$, $N_{2,3}$ *and* $N_{1,3}$ *such that*

$$n = 3^b N_{2,3}^2 N_{1,3}.$$

(iii) *An integer* $n \geq 1$ *is simultaneously of the forms*

$$n = \Phi_3(u,v) = u^2 + uv + v^2 \quad \text{and} \quad n = \Phi_4(x,y) = x^2 + y^2$$

if and only if there exist integers $a, b \geq 0$, $N_{5,12}$, $N_{7,12}$, $N_{11,12}$ *and* $N_{1,12}$ *such that*

$$n = (2^a 3^b N_{5,12} N_{7,12} N_{11,12})^2 N_{1,12}.$$

Proof. Part (i) is well known (see [H–W, Theorem 366] for instance). It can be proved by detecting primes in the ring $\mathbb{Z}[i]$ of Gaussian integers of the quadratic field $\mathbb{Q}(i)$. This ring is principal and the norm of an element $x+iy$ is given by the quadratic form $\Phi_4(x,y)=x^2+y^2$. The quadratic field $\mathbb{Q}(\sqrt{-3})$ has similar properties: its associated ring of integers is a principal domain equal to $\mathbb{Z}[j]$ with $j=(-1+\sqrt{-3})/2$. The primes of $\mathbb{Z}[j]$ (also called *Eisenstein primes*) are detected by the values of the Kronecker symbol $(-3/p)$ and the norm of the element $u+vj$ of $\mathbb{Z}[j]$ is equal to $\Phi_3(u,-v)=\Phi_6(u,v)=u^2+uv+v^2$. This gives part (ii). Also, this statement is a particular case of [B–Ch, Théorème 3, p. 267] and it is implicitly contained in [H–W, Theorem 254], [H, Exercise 2, p. 308].

Combining (i) and (ii), we deduce part (iii) directly. ∎

6.2. Analytic background. Our main tool is based on the Selberg–Delange method. The following version is a weakened form of the quite general result due to Tenenbaum [T, Theorem 3, p. 185]. It gives an asymptotic expansion of the summatory function of a sequence (a_n) when the associated Dirichlet series can be approached by some power of the ζ-function in a domain slightly larger than the half-plane $\{s\in\mathbb{C}\mid \Re s\geq 1\}$.

PROPOSITION 6.3. *Let $s=\sigma+it$ be the complex variable and let*

$$F(s):=\sum_{n\geq 1}a_n n^{-s}$$

be a Dirichlet series such that

- *the coefficients a_n are real nonnegative numbers,*
- *there exist $z\in\mathbb{C}$ and $c_0,\delta,K>0$ such that the function*

$$G(s):=F(s)\zeta(s)^{-z}$$

has a holomorphic continuation in the domain $\mathcal{D}$ of the complex plane defined by

$$\sigma>1-\frac{c_0}{1+\log(1+|t|)}, \tag{6.4}$$

and satisfies

$$|G(s)|\leq K(1+|t|)^{1-\delta} \tag{6.5}$$

for every $s\in\mathcal{D}$.

Then there exists a sequence (λ_k) $(k\geq 0)$ of real numbers such that for all $M\geq 1$, uniformly for $x\geq 2$,

$$\sum_{1\leq n\leq x}a_n=x(\log x)^{z-1}\bigg\{\sum_{0\leq k\leq M}\frac{\lambda_k}{(\log x)^k}+O\bigg(\frac{1}{(\log x)^{M+1}}\bigg)\bigg\}.$$

In particular,

$$\lambda_0=\frac{1}{\Gamma(z)}G(1).$$

6.3. Proof of Proposition 6.1. We restrict ourselves to the proof of (6.3) since the proof of (6.2) is simpler. Let ξ_n be the characteristic function of the set of integers $n \geq 1$ which are simultaneously represented by Φ_3 and Φ_4. Let $F(s) = \sum_n \xi_n n^{-s}$ be the associated Dirichlet series. Note that

$$|\tilde{\mathcal{A}}(\Phi_3; N) \cap \tilde{\mathcal{A}}(\Phi_4; N)| = \sum_{n \leq N} \xi_n.$$

By Proposition 6.2(iii), $F(s)$ factorizes into the product

$$F(s) = H(s)\Pi(s) \tag{6.6}$$

with

$$H(s) = \left(1 - \frac{1}{4^s}\right)^{-1}\left(1 - \frac{1}{9^s}\right)^{-1} \prod_{p \equiv 5,7,11 \bmod 12} \left(1 - \frac{1}{p^{2s}}\right)^{-1}, \tag{6.7}$$

$$\Pi(s) = \prod_{p \equiv 1 \bmod 12} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{6.8}$$

The function H is holomorphic for $\sigma > 1/2$ and uniformly bounded for $\sigma \geq 3/4$. The infinite product $\Pi(s)$ is absolutely convergent for $\sigma > 1$ and we want to study the behavior of this product in the vicinity of the singularity $s = 1$. To detect among the primes $p \geq 5$ those which are congruent either to 1 modulo 12 or to $5, 7, 11$ modulo 12, we use the formula

$$\frac{1}{4}\left(1 + \left(\frac{-3}{p}\right) + \left(\frac{-4}{p}\right) + \left(\frac{12}{p}\right)\right) = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 12, \\ 0 & \text{if } p \equiv 5, 7, 11 \bmod 12. \end{cases} \tag{6.9}$$

Inserting (6.9) into (6.8), we deduce that for $\sigma > 1$ we have

$$\Pi(s) = \prod_{p \geq 5} \left\{ \left(1 - \frac{1}{p^s}\right)\left(1 - \frac{(-3/p)}{p^s}\right)\left(1 - \frac{(-4/p)}{p^s}\right)\left(1 - \frac{(12/p)}{p^s}\right) \right\}^{-1/4} \times \prod_{p \equiv 5,7,11 \bmod 12} \left(1 - \frac{1}{p^{2s}}\right)^{1/2}.$$

Completing the first infinite product with the factors associated with the primes $p = 2$ and $p = 3$ to obtain the ζ-function and some L-functions, we deduce that for $\sigma > 1$,

$$\Pi(s) = H_1(s)\zeta(s)^{1/4} L(s, (-3/\cdot))^{1/4} L(s, (-4/\cdot))^{1/4} L(s, (12/\cdot))^{1/4}, \tag{6.10}$$

with

$$H_1(s) = \left(1 - \frac{1}{4^s}\right)^{1/4}\left(1 - \frac{1}{9^s}\right)^{1/4} \prod_{p \equiv 5,7,11 \bmod 12} \left(1 - \frac{1}{p^{2s}}\right)^{1/2}.$$

By (6.6)–(6.8) and (6.10), we deduce that for $\sigma > 1$,

$$F(s) = H_2(s)\zeta(s)^{1/4}L(s,(-3/\cdot))^{1/4}L(s,(-4/\cdot))^{1/4}L(s,(12/\cdot))^{1/4}, \tag{6.11}$$

with

$$H_2(s) = \left(1 - \frac{1}{4^s}\right)^{-3/4}\left(1 - \frac{1}{9^s}\right)^{-3/4} \prod_{p\equiv 5,7,11 \bmod 12}\left(1 - \frac{1}{p^{2s}}\right)^{-1/2}.$$

The function H_2 is holomorphic for $\sigma > 1/2$ and uniformly bounded for $\sigma \geq 3/4$.

By the classical zerofree region of the Dirichlet L-functions, there exists $c_0 > 0$ such that in the domain $\mathcal{D}$ defined in (6.4) the function

$$L(s,(-3/\cdot))\, L(s,(-4/\cdot))\, L(s,(12/\cdot))$$

does not vanish. This implies that the function

$$G(s) := F(s)\zeta(s)^{-1/4} = H_2(s)L(s,(-3/\cdot))^{1/4}L(s,(-4/\cdot))^{1/4}L(s,(12/\cdot))^{1/4}$$

can be extended to a holomorphic function on $\mathcal{D}$ satisfying (6.5) with $\delta = 1/2$, as a consequence of the functional equation and the Phragmén–Lindelöf convexity principle (see [I–K, Exercise 3, p. 100] for instance).

All the conditions of Proposition 6.3 are satisfied with $z = 1/4$ and we obtain (6.3) with

$$\beta_0 = H_2(1)\, L(1,(-3/\cdot))^{1/4}L(1,(-4/\cdot))^{1/4}L(1,(12/\cdot))^{1/4}/\Gamma(1/4),$$

which can be written as

$$\beta_0 = \left(\frac{3}{2}\right)^{3/4}\frac{1}{\Gamma(1/4)}L(1,(-3/\cdot))^{1/4}L(1,(-4/\cdot))^{1/4}L(1,(12/\cdot))^{1/4} \times \prod_{p\equiv 5,7,11 \bmod 12}\left(1 - \frac{1}{p^2}\right)^{-1/2}.$$

Since [OEIS, A101455, A073010, A196530]

$$L(1,(-4/\cdot)) = \frac{\pi}{4}, \qquad L(1,(-3/\cdot)) = \frac{\pi}{3^{3/2}}, \qquad L(1,(12/\cdot)) = \frac{\log(2+\sqrt{3})}{\sqrt{3}},$$

we deduce

$$\beta_0 = \frac{3^{1/4}}{2^{5/4}}\pi^{1/2}(\log(2+\sqrt{3}))^{1/4}\frac{1}{\Gamma(1/4)}\prod_{p\equiv 5,7,11 \bmod 12}\left(1 - \frac{1}{p^2}\right)^{-1/2}.$$

The proof of (6.2) for $k = 3$ and $k = 4$ is simpler since the formula to detect the congruences $p \equiv 1 \bmod 3$ and $p \equiv 1 \bmod 4$ contains only two terms instead of four as in (6.9). In both cases $k = 3$ and $k = 4$, the parameter z is $1/2$. This gives (6.2) with

$$\alpha_0^{(3)} = \frac{1}{2^{1/2}3^{1/4}} \prod_{p \equiv 2 \bmod 3} \left(1 - \frac{1}{p^2}\right)^{-1/2},$$

$$\alpha_0^{(4)} = \frac{1}{2^{1/2}} \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right)^{-1/2}.$$

Finally, (6.2) is a detailed version of Landau's formula which states that for N tending to infinity, we have

$$|\tilde{\mathcal{A}}(\Phi_4; N)| \sim C \frac{N}{\sqrt{\log N}},$$

where $C = \alpha_0^{(4)} = 0.764\,223\,653\,589\,220\ldots$ is the Landau–Ramanujan constant (cf. [L, pp. 257–263] and [OEIS, A000404, A064533]). Using Pari/GP [P], one checks that the first decimal digits of $\alpha_0^{(3)}$ are $0.638\,909$, while the first decimal digits of β_0 are $0.302\,316$. ∎

6.4. Proof of Corollary 1.4. For $N \geq 1$, $a_1 + \cdots + a_N$ counts the number of triples (n, x, y) with $n \geq 3$, $\max\{|x|, |y|\} \geq 2$ and $\Phi_n(x, y) \leq N$. The number of such triples with $n = 4$ is asymptotically πN. The number of such triples with $n = 3$ is asymptotically $(\pi/\sqrt{3})N$, and the same for $n = 6$. The number of such triples with $\varphi(n) > 2$ is $o(N)$, as shown by Lemma 5.1. Hence

$$a_1 + \cdots + a_N \sim \left(1 + \frac{2}{\sqrt{3}}\right)\pi N,$$

and Corollary 1.4 with

$$\kappa_1 = \frac{\pi}{\alpha_0}\left(1 + \frac{2}{\sqrt{3}}\right)$$

follows from Theorem 1.3. ∎

7. Numerical computations. From (5.2), we deduce that the assumptions $n \geq 3$, $\Phi_n(x, y) \leq 20$ and $\max\{|x|, |y|\} \geq 2$ imply

$$\left(\frac{\sqrt{3}}{2}\max\{|x|, |y|\}\right)^{\varphi(n)} \leq 20.$$

We deduce firstly $3^{\varphi(n)/2} \leq 20$, hence $\varphi(n) \leq 4$, and secondly

$$\max\{|x|, |y|\} \leq 2\sqrt{20/3},$$

hence $\max\{|x|, |y|\} \leq 5$. It is now again a simple matter of computation with Maple [M] to complete the rest of Table 1. For instance, one can find in

Table 4 the values of (x, y) which are the only ones satisfying the stronger condition $\Phi_n(x, y) \leq 10$.

Table 4

$m = 3$:	$n = 3$,	$(x, y) = (1, -2), (-1, 2), (2, -1), (-2, 1)$
$m = 3$:	$n = 6$,	$(x, y) = (1, 2), (-1, -2), (2, 1), (-2, -1)$
$m = 4$:	$n = 3$,	$(x, y) = (0, 2), (0, -2), (2, 0), (2, -2), (-2, 0), (-2, 2)$
$m = 4$:	$n = 4$,	$(x, y) = (0, 2), (0, -2), (2, 0), (-2, 0)$
$m = 4$:	$n = 6$,	$(x, y) = (0, 2), (0, -2), (2, 0), (2, 2), (-2, 0), (-2, -2)$
$m = 5$:	$n = 4$,	$(x, y) = (1, 2), (1, -2), (-1, 2), (-1, -2), (2, 1), (2, -1), (-2, 1), (-2, -1)$
$m = 7$:	$n = 3$,	$(x, y) = (1, 2), (1, -3), (-1, 3), (-1, -2), (-3, 1), (3, -1), (2, 1), (2, -3), (-2, 3), (-2, -1), (3, -2), (-3, 2)$
$m = 7$:	$n = 6$,	$(x, y) = (1, 3), (1, -2), (-1, 2), (-1, -3), (3, 1), (-3, -1), (2, 1), (2, -1), (2, 3), (-2, -3), (3, 2), (-3, -2)$
$m = 8$:	$n = 4$,	$(x, y) = (2, 2), (2, -2), (-2, 2), (-2, -2)$
$m = 9$:	$n = 3$,	$(x, y) = (0, 3), (0, -3), (3, 0), (3, 3), (-3, 0), (-3, 3)$
$m = 9$:	$n = 4$,	$(x, y) = (0, 3), (0, -3), (3, 0), (-3, 0)$
$m = 9$:	$n = 6$,	$(x, y) = (0, 3), (0, -3), (3, 0), (3, 3), (-3, 0), (-3, 3)$
$m = 10$:	$n = 4$,	$(x, y) = (1, 3), (1, -3), (-1, 3), (-1, -3), (3, 1), (3, -1), (-3, 1), (-3, -1)$

With similar calculations, we obtain Table 2. The triples (n, x, y) which contribute to Table 2 satisfy $\varphi(n) \in \{4, 6\}$ and $\max\{|x|, |y|\} \in \{2, 3\}$.

Notice that given $h \geq 3$, the smallest value m_h of m for which there exists (n, x, y) with $n \geq 2$, $\max\{|x|, |y|\} \geq h$ and $\Phi_n(x, y) = m$ is

$$m_h = \begin{cases} \Phi_3\left(\dfrac{h-1}{2}, -h\right) = \Phi_3\left(\dfrac{h+1}{2}, -h\right) = \dfrac{3h^2+1}{4} & \text{if } 2 \nmid h, \\ \Phi_3\left(\dfrac{h}{2}, -h\right) = \dfrac{3h^2}{4} & \text{if } 2 \mid h. \end{cases}$$

Acknowledgments. This work was initiated in Lecce in June 2016, and was pursued at the University of the Philippines at Diliman during a SEAMS school; the second and third authors are grateful to Fidel Nemenzo for the stimulating environment. Last but not least, many thanks to Kálmán Győry for drawing our attention to his paper [G] and for his valuable remarks.

The second author was supported by an NSERC grant.

References

[B–Ch] Z. I. Borevitch et I. R. Chafarevitch, *Théorie des nombres*, Monogr. Internat. Math. Modernes 8, Gauthier-Villars, Paris, 1967.

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

[H–W] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Clarendon Press, New York, 1979.

[H] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.

[I–K] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc. Colloq. Publ. 53, Amer. Math. Soc., Providence, RI, 2004.

[L] W. J. LeVeque, *Topics in Number Theory*, Vol. 2, Dover, Mineola, NY, 2002.

[M] *Maple* software, Univ. of Waterloo, Waterloo, ON.

[M–W] M. Mignotte and M. Waldschmidt, *Linear forms in two logarithms and Schneider's method, III,* Ann. Fac. Sci. Toulouse Math. (5), 1989, suppl., 43–75.

[N1] T. Nagell, *Contributions à la théorie des corps et des polynômes cyclotomiques*, Ark. Mat. 5 (1963), 153–192.

[N2] T. Nagell, *Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang*, Ark. Mat. 5 (1965), 477–521.

[OEIS] N. J. A. Sloane, *The On-line Encyclopedia of Integer Sequences*, https://oeis.org/.

[P] *Pari/GP* software, Univ. Bordeaux I, https://pari.math.u-bordeaux.fr/.

[S–X] C. L. Stewart and S. Y. Xiao, *On the representation of integers by binary forms*, arXiv:1605.03427 (2016).

[T] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, Cambridge Stud. Adv. Math. 46, Cambridge Univ. Press, Cambridge, 1995.

Étienne Fouvry
Institut de Mathématique d'Orsay
Université Paris-Sud
CNRS, Université Paris-Saclay
F-91405 Orsay, France
E-mail: etienne.fouvry@u-psud.fr

Michel Waldschmidt
Sorbonne Université
UPMC Univ Paris 06
UMR 7586 IMJ-PRG
F-75005 Paris, France
E-mail: michel.waldschmidt@imj-prg.fr

Claude Levesque
Département de mathématiques et de statistique
Université Laval
Québec, QC, Canada G1V 0A6
E-mail: cl@mat.ulaval.ca

Abstract (will appear on the journal's web site only)

The homogeneous form $\Phi_n(X,Y)$ of degree $\varphi(n)$ which is associated with the cyclotomic polynomial $\phi_n(X)$ 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 $\Phi_n(x,y) = m$. We prove that the number a_m of such representations of m by a cyclotomic binary form is finite. More precisely, we have $\varphi(n) \leq (2/\log 3)\log m$ and $\max\{|x|,|y|\} \leq (2/\sqrt{3})\, m^{1/\varphi(n)}$. We give a description of the asymptotic cardinality of the set of values taken by the forms for $n \geq 3$. This will imply that the set of integers m such that $a_m \neq 0$ has natural density 0. We will deduce that the average value of the nonzero values of a_m grows like $\sqrt{\log m}$.