ACTA ARITHMETICA
Online First version

Number of integers represented by families of binary forms (I)

by

Étienne Fouvry (Orsay) and Michel Waldschmidt (Paris)

Nous dédions ce travail à la mémoire d'André Schinzel
avec notre profond respect et notre affectueuse admiration

1. Introduction. Let $d \geq 3$ be an integer. We denote by $\mathrm{Bin}(d, \mathbb{Z})$ the set of binary forms $F = F(X, Y)$ with integer coefficients, of degree d and with discriminant different from zero. For

$$\gamma = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{Q}), \tag{1.1}$$

and $F \in \mathrm{Bin}(d, \mathbb{Z})$, $F \circ \gamma$ is the binary form with rational coefficients defined by

$$(F \circ \gamma)(X_1, X_2) = F(a_1X_1 + a_2X_2, a_3X_1 + a_4X_2).$$

Two elements F_1 and F_2 in $\mathrm{Bin}(d, \mathbb{Z})$ are said to be *isomorphic* if there is a $\gamma \in \mathrm{GL}(2, \mathbb{Q})$ such that

$$F_1 \circ \gamma = F_2.$$

To estimate the number of values simultaneously taken by F_1 and F_2, we introduce the counting function, for N an integer ≥ 1,

$$\begin{aligned} \mathcal{N}(F_1, F_2; N) &:= \sharp(F_1(\mathbb{Z}^2) \cap F_2(\mathbb{Z}^2) \cap [-N, +N]) \\ &= \sharp\{m : |m| \leq N, \text{ there exists } (x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 \\ &\qquad\qquad \text{such that } m = F_1(x_1, x_2) = F_2(x_3, x_4)\}. \end{aligned} \tag{1.2}$$

Our first result gives an upper bound for this function when the two forms are not isomorphic.

2020 *Mathematics Subject Classification*: Primary 11E76; Secondary 11D45, 11D85.
Key words and phrases: binary forms, representation of integers by binary forms, families of diophantine equations.
Received 6 June 2022; revised 13 January 2023.
Published online *.

Theorem 1.1. *For every $d \geq 3$, there is a constant $\vartheta_d < 2/d$ such that, for every $\varepsilon > 0$, for every pair (F_1, F_2) of non-isomorphic forms in* $\mathrm{Bin}(d, \mathbb{Z})$, *as $N \to \infty$, one has the bound*

$$\mathcal{N}(F_1, F_2; N) = O_{F_1,F_2,\varepsilon}(N^{\vartheta_d+\varepsilon}). \tag{1.3}$$

This theorem calls for the following comments:

Remark 1.2. The point of this theorem is that the constant ϑ_d defined in (2.1) satisfies $\vartheta_d < 2/d$ (see (2.3)). In fact, it is known that for any $F \in \mathrm{Bin}(d, \mathbb{Z})$, there exists $C_F > 0$ such that, for N tending to infinity, one has

$$\mathcal{N}(F, F; N) = (C_F + o_F(1))N^{2/d}$$

(see Theorem A in §1.1, due to Stewart and Xiao [SX, Theorem 1.1]).

Remark 1.3. The explicit value of ϑ_d given in (2.1) leads to the inequality $\vartheta_d > 1/d$ for all $d \geq 3$ (see (2.3)). It also shows that ϑ_d is asymptotic to $1/d$ as $d \to \infty$. This value is asymptotically optimal as shown by the forms

$$F_1(X, Y) = X^d + Y^d \quad \text{and} \quad F_2(X, Y) = X^d + 2Y^d.$$

These two forms are not isomorphic. From the equalities $F_1(n, 0) = F_2(n, 0) = n^d$, we deduce the lower bound

$$\mathcal{N}(F_1, F_2; N) \geq N^{1/d} (N \geq 1).$$

Remark 1.4. According to [FW, Corollaire 3.3], if the two forms F_1, F_2 are positive definite and not both divisible by a linear form with rational coefficients, then the exponent ϑ_d in the conclusion of Theorem 1.1 can be replaced by η_d with $\eta_d < \vartheta_d$ (see the definition of η_d and ϑ_d in §2.1).

Remark 1.5. We will show in §2.4 that ϑ_d can be replaced by η_d as in the previous remark when the binary form $F_1(X, Y)F_2(X, Y)$ has no real root.

Remark 1.6. Theorem 1.1 is no more valid for $d = 2$. This is well known: see for instance [FLW, Prop. 6.1, (6.3)], where, choosing $F_1(X, Y) = X^2+Y^2$ and $F_2(X, Y) = X^2 + XY + Y^2$, one has, for B tending to infinity, the asymptotic formula

$$\mathcal{N}(F_1, F_2; B) = (\beta_0 + o(1))B(\log B)^{-3/4}$$

for some constant $\beta_0 > 0$.

Remark 1.7. Theorem 1.1 immediately generalizes to binary forms with rational coefficients: it suffices to multiply by a common denominator.

Remark 1.8. The following proposition shows that if F_1 and F_2 are isomorphic, equality (1.3) never holds.

PROPOSITION 1.9. *Let $d \geq 3$ and let F_1 and F_2 be isomorphic binary forms in* $\mathrm{Bin}(d, \mathbb{Z})$. *Then there is a positive constant C_{F_1,F_2}, such that, for N tending to infinity, we have*

$$\mathcal{N}(F_1, F_2; N) \geq (C_{F_1,F_2} - o_{F_1,F_2}(1))N^{2/d}.$$

Proof. Let γ as in (1.1) be such that $F_1 = F_2 \circ \gamma$. Let $D \geq 1$ be an integer such that (Da_1, Da_2, Da_3, Da_4) belongs to $\mathbb{Z}^4$. By homogeneity, we deduce that the two forms

$$G_1(X_1, X_2) := F_1(DX_1, DX_2),$$
$$G_2(X_1, X_2) := F_2(Da_1X_1 + Da_2X_2, Da_3X_1 + Da_4X_2)$$

are equal. So we have the equality of their images

$$G_1(\mathbb{Z}^2) = G_2(\mathbb{Z}^2).$$

We also have the obvious inclusions

$$G_1(\mathbb{Z}^2) \subset F_1(\mathbb{Z}^2) \quad \text{and} \quad G_2(\mathbb{Z}^2) \subset F_2(\mathbb{Z}^2),$$

which leads to

$$G_1(\mathbb{Z}^2) \subset F_1(\mathbb{Z}^2) \cap F_2(\mathbb{Z}^2). \tag{1.4}$$

A new application of the result of Stewart and Xiao (see Theorem A below) gives, for some constant $C_{G_1} > 0$, the equality

$$\mathcal{N}(G_1, G_1; N) = (C_{G_1} + o_{G_1}(1))N^{2/d} \tag{1.5}$$

as N tends to infinity. Gathering (1.4) and (1.5) we obtain the inequality claimed in Proposition 1.9. ∎

Theorem 1.1 is an important tool for our generalization of our previous study in [FW], where we produced an asymptotic formula for the number of values m, with $|m| \leq B$, taken by some cyclotomic form Φ_n of degree $\varphi(n)$ greater than a fixed $d \geq 3$. Recall that φ is the Euler function and that to the nth cyclotomic polynomial $\phi_n(X)$, of degree $\varphi(n)$, is attached the *cyclotomic form* $\Phi_n(X, Y) := Y^{\varphi(n)} \cdot \phi_n(X/Y)$.

Our purpose is to study the following general problem:

Let $\mathcal{F}$ be an infinite subset of $\bigcup_{d\geq 3}\mathrm{Bin}(d, \mathbb{Z})$, *satisfying natural properties. Let A be a fixed non-negative integer. As B tends to infinity, estimate the counting function*

(1.6)

$$\mathcal{R}_{\geq d}(\mathcal{F}, B, A) := \sharp\,\{m : 0 \leq |m| \leq B, \textit{ and there are } F \in \mathcal{F} \textit{ with } \deg F \geq d \textit{ and } (x, y) \in \mathbb{Z}^2 \textit{ with } \max\{|x|, |y|\} \geq A \textit{ such that } F(x, y) = m\}.$$

The introduction of the parameter A may seem artificial. It is designed to prevent the following phenomenon encountered for instance in the case of the family of cyclotomic forms Φ_n, where, for every prime p, we have

$$\Phi_p(1,1) = p \tag{1.7}$$

(recall that $\Phi_p(X,Y) = (X^p - Y^p)/(X-Y)$). We wish to avoid counting these values, since the set of primes, by its cardinality, completely hides the set of other values $\Phi_n(x,y)$ when $\max\{|x|,|y|\} \geq 2$ and $\varphi(n) \geq d$.

Let $\mathcal{F}$ be a set of binary forms. We denote by $\mathcal{F}_d$ the subset of forms in $\mathcal{F}$ of degree d. We will study the set of values taken by forms belonging to some $(A, A_1, d_0, d_1, \kappa)$-*regular* families $\mathcal{F}$, which we define as follows.

Definition 1.10. Let A, A_1, d_0, d_1 be integers and let κ be a real number such that

$$A \geq 1,\ A_1 \geq 1,\ d_1 \geq d_0 \geq 0,\ 0 < \kappa < A. \tag{1.8}$$

Let $\mathcal{F}$ be a set of binary forms. We say that $\mathcal{F}$ is $(A, A_1, d_0, d_1, \kappa)$-*regular* if it satisfies the following conditions:

(i) The set $\mathcal{F}$ is infinite.

(ii) We have the inclusion

$$\mathcal{F} \subset \bigcup_{d \geq 3} \mathrm{Bin}(d, \mathbb{Z}).$$

(iii) For all $d \geq 3$, one has $\sharp\mathcal{F}_d \leq d^{A_1}$,

(iv) Two forms in $\mathcal{F}$ are isomorphic if and only if they are equal.

(v) For any $d \geq \max\{d_1, d_0+1\}$, the following holds:

$$\left.\begin{array}{l} F \in \mathcal{F}_d, \\ (x,y) \in \mathbb{Z}^2 \text{ and } F(x,y) \neq 0, \\ \max\{|x|,|y|\} \geq A \end{array}\right\} \Longrightarrow \max\{|x|,|y|\} \leq \kappa\, |F(x,y)|^{\frac{1}{d-d_0}}.$$

The upper bound on the right-hand side of (v) is trivial for $\max\{|x|,|y|\} \leq \kappa$; this is why we require $A > \kappa$.

The family of cyclotomic forms

$$\boldsymbol{\Phi} := \{\Phi_n : \varphi(n) \geq 4,\ n \not\equiv 2 \pmod 4\}$$

satisfies assumptions (i)–(iv), but is not $(1, A_1, d_0, d_1, \kappa)$-regular for any value of A_1, d_0, d_1 and κ, since (1.7) shows that (v) is not satisfied. However, $\boldsymbol{\Phi}$ is $(2, 2, 0, 4, 2/\sqrt{3})$-regular: this is a consequence of [FW, Théorème 4.10] and of the classical inequality $n/(\log\log n) < \varphi(n) < n$.

1.1. Some facts on a single form. Before stating our main result concerning $\mathcal{R}_{\geq d}(\mathcal{F}, B, A)$ defined in (1.6), we recall some fundamental objects attached to a binary form $F \in \mathrm{Bin}(d, \mathbb{Z})$ when $d \geq 3$:

- The *fundamental domain* of F is

$$\mathcal{D}(F) := \{(x,y) \in \mathbb{R}^2 : |F(x,y)| \leq 1\}.$$

- The *area* of the fundamental domain of F is the real number

$$A_F := \iint_{\mathcal{D}(F)} \mathrm{d}x\,\mathrm{d}y. \tag{1.9}$$

  We always have $0 < A_F < \infty$.
- The *group of automorphisms* of F is

$$\operatorname{Aut}(F,\mathbb{Q}) := \left\{ \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Q}) : F(X,Y) = F(a_1X + a_2Y, a_3X + a_4Y) \right\}.$$

This is a finite subgroup of $\mathrm{GL}(2,\mathbb{Q})$.

We now recall the important result of Stewart and Xiao [SX, Theorems 1.1 and 1.2], already mentioned above:

Theorem A. *For every $d \geq 3$, there is a constant $\kappa_d < 2/d$ such that, for all $F \in \operatorname{Bin}(d,\mathbb{Z})$ and all $\varepsilon > 0$, the equality*

$$\mathcal{N}(F,F;B) = A_F \cdot W_F \cdot B^{2/d} + O_{F,\varepsilon}(B^{\kappa_d+\varepsilon})$$

holds uniformly for $B \to \infty$, where $W_F = W(\operatorname{Aut}(F,\mathbb{Q}))$ depends only on the group $\operatorname{Aut}(F,\mathbb{Q})$.

For G a finite subgroup of $\mathrm{GL}(2,\mathbb{Q})$ which is the group of automorphisms of an element of $\operatorname{Bin}(d,\mathbb{Z})$, the constant $W(G)$ is a rational number which is defined in [SX, Theorem 1.2]. This definition is subtle since it depends on the denominators of the entries of the matrices belonging to G. However, for the families $\mathcal{F}$ that we will meet in this paper, we will only need the equalities

(1.10)

$$W(\{\mathrm{Id}\}) = 1, \quad W(\{\mathrm{Id},\, -\mathrm{Id}\}) = 1/2, \quad W\left(\left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\} \right) = 1/4.$$

Finally, the exponent κ_d in Theorem A is defined by

$$\kappa_d = \begin{cases} \frac{12}{19} & \text{if } d = 3, \\ \frac{3}{(d-2)\sqrt{d}+3} & \text{if } 4 \leq d \leq 8, \\ \frac{1}{d-1} & \text{if } d \geq 9. \end{cases} \tag{1.11}$$

Actually, the value of this exponent is improved when $F(X,Y)$ does not have a linear factor over $\mathbb{R}[X,Y]$; see [SX, (1.11)].

1.2. An asymptotic formula for $\mathcal{R}_{\geq d}(\mathcal{F},B,A)$. Our central result is the following. The exponent ϑ_d is defined in (2.1).

Theorem 1.11. *Let $(A, A_1, d_0, d_1, \kappa)$ satisfy conditions* (1.8)*. Let $\mathcal{F}$ be a $(A, A_1, d_0, d_1, \kappa)$-regular family of binary forms. Then for every $d \geq \max\{3, d_1\}$*

and every positive ε, one has

$$\mathcal{R}_{\geq d}(\mathcal{F},B,A)=\Big(\sum_{F\in\mathcal{F}_d}A_FW_F\Big)\cdot B^{2/d}+O_{\mathcal{F},A,d,\varepsilon}(B^{\vartheta_d+\varepsilon})+O_{\mathcal{F},A,d}(B^{2/d^\dagger})$$

uniformly for $B\to\infty$. The integer $d^\dagger$ is defined by

$$d^\dagger:=\inf\{d':d'>d \text{ such that } \mathcal{F}_{d'}\neq\emptyset\}.$$

Recall that $\mathcal{F}_d$ is not empty for infinitely many values of d since the set $\mathcal{F}$ is infinite.

Assumption (v) in Definition 1.10 of a regular family cannot be omitted, even in the case of totally imaginary forms (homogeneous versions of polynomials without real roots), as shown by the sequence of positive definite forms $(X-Y)^2(X-2Y)^2\cdots(X-dY)^2+dY^{2d}$, the value of which at the points $(x,y)=(n,1)$, $1\leq n\leq d$, is d.

The following is a direct application of (1.10):

Corollary 1.12. *Suppose that $\mathcal{F}$ satisfies the hypothesis of Theorem* 1.11 *and that, for every $d\geq 3$, $\mathcal{F}_d$ satisfies one of the following three conditions:*

(C1) *for all $F\in\mathcal{F}_d$, we have* $\mathrm{Aut}(F,\mathbb{Q})=\{\mathrm{Id}\}$,
(C2) *for all $F\in\mathcal{F}_d$, we have* $\mathrm{Aut}(F,\mathbb{Q})=\{\pm\mathrm{Id}\}$ (*cyclic group of order* 2),
(C3) *for all $F\in\mathcal{F}_d$, we have* $\mathrm{Aut}(F,\mathbb{Q})=\left\{\left(\begin{smallmatrix}\pm1&0\\0&\pm1\end{smallmatrix}\right)\right\}$ (*Klein group of order* 4).

Then

$$\mathcal{R}_{\geq d}(\mathcal{F},B,A)=C_d\cdot\Big(\sum_{F\in\mathcal{F}_d}A_F\Big)\cdot B^{2/d}+O_{\mathcal{F},A,d,\varepsilon}(B^{\vartheta_d+\varepsilon})+O_{\mathcal{F},A,d}(B^{2/d^\dagger}),\tag{1.12}$$

where the coefficient C_d is 1, 1/2 *or* 1/4 *according as condition* (C1), (C2), *or* (C3) *is satisfied by $\mathcal{F}_d$.*

1.3. Some applications. We now give a list of regular families $\mathcal{F}$ in order to illustrate our results.

The first example of course is given by the sequence of cyclotomic binary forms [FLW]. We do not repeat it.

Our second example is given by a family of binomials ax^d+by^d where d is even while a, b have the same sign: these restrictions allow us to check easily assumption (v) in Definition 1.10 of a regular family. Since the proof is easy, we give it right away.

The other three examples below will require more work; for them we restrict ourselves to families $\mathcal{F}$ satisfying the conditions of Corollary 1.12 in order to apply (1.12).

There are a lot of variations on these constructions.

1.3.1. *Binomial forms.* For each even integer $d \geq 4$, let $\mathcal{E}_d$ be a finite subset of $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$. Assume $\mathcal{E}_d$ is not empty for infinitely many d and has at most d^{A_1} elements for some $A_1 > 0$ and all d. Let $\mathcal{B}_d$ denote the family of binary forms $aX^d + bY^d$ with $(a,b) \in \mathcal{E}_d$ and let $\mathcal{B} = \bigcup_{d\geq 4} \mathcal{B}_d$. We assume that for $(a,b) \neq (a',b')$ in $\mathcal{E}_d$, at least one of a/a', b/b' is not a dth power of a rational number, and also at least one of a/b', b/a' is not a dth power of a rational number.

THEOREM 1.13. *The family $\mathcal{B}$ is $(2, A_1, 0, 4, 1)$-regular.*
Further, for every $d \geq 4$ and every $\varepsilon > 0$ we have

$$\mathcal{R}_{\geq d}(\mathcal{B}, B, 2) = \Big(\sum_{F\in\mathcal{B}_d} A_F W_F\Big) B^{2/d} + O_{\mathcal{B},d,\varepsilon}(B^{\max\{\vartheta_d+\varepsilon, 2/d^\dagger\}})$$

uniformly for $B \to \infty$. The integer $d^\dagger$ is defined by

$$d^\dagger := \inf\{d' : d' > d,\ \mathcal{B}_{d'} \neq \emptyset\}.$$

We will check hypothesis (iv) of Definition 1.10 by means of the following auxiliary result.

LEMMA 1.14. *Let $d \geq 4$ be even and let a, b, a', b' be positive integers. Then the binary forms $aX^d + bY^d$ and $a'X^d + b'Y^d$ are isomorphic if and only if either a/a', b/b' are both dth powers of rational numbers, or a/b', b/a' are both dth powers of rational numbers.*

Proof. If $a/a' = u^d$ and $b/b' = v^d$, then the forms $aX^d+bY^d = a'(uX)^d + b'(vY)^d$ and $a'X^d + b'Y^d$ are isomorphic. Also, if $a/b' = u^d$ and $b/a' = v^d$, then the forms $aX^d + bY^d = a'(vY)^d + b'(uX)^d$ and $a'X^d + b'Y^d$ are isomorphic. It remains to prove the converse.

Assume $aX^d + bY^d$ and $a'X^d + b'Y^d$ are isomorphic. Let $\gamma = \left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Q})$ satisfy

$$a(a_1X + a_2Y)^d + b(a_3X + a_4Y)^d = a'X^d + b'Y^d.$$

We have

$$aa_1^d + ba_3^d = a', \qquad aa_2^d + ba_4^d = b'$$

and, for $i = 1, \dots, d-1$,

$$aa_1^i a_2^{d-i} + ba_3^i a_4^{d-i} = 0.$$

Assume $a_2 = 0$. From

$$a(a_1X)^d + b(a_3X + a_4Y)^d = a'X^d + b'Y^d$$

we deduce $ba_4^d = b'$, $a_4 \neq 0$, hence $a_3 = 0$, and therefore $aa_1^d = a'$.

Assume $a_1 = 0$. From

$$a(a_2Y)^d + b(a_3X + a_4Y)^d = a'X^d + b'Y^d$$

we deduce $ba_3^d = a'$, $a_3 \neq 0$, hence $a_4 = 0$, and therefore $aa_2^d = b'$.

Finally, let us check that the case $a_1a_2 \neq 0$ is not possible. Write

$$aa_1a_2^{d-1} + ba_3a_4^{d-1} = 0, \qquad aa_1^2a_2^{d-2} + ba_3^2a_4^{d-2} = 0.$$

We deduce $a_3a_4 \neq 0$,

$$\frac{a_1}{a_3} = -\frac{b}{a}\left(\frac{a_4}{a_2}\right)^{d-1}, \qquad \left(\frac{a_1}{a_3}\right)^2 = -\frac{b}{a}\left(\frac{a_4}{a_2}\right)^{d-2},$$

hence

$$\left(\frac{a_4}{a_2}\right)^d = -\frac{a}{b},$$

which is impossible for a, b positive and d even. ∎

Proof of Theorem 1.13. Conditions (i)–(iii) in Definition 1.10 are satisfied by hypothesis.

For $(a,b) \neq (a',b')$ in $\mathcal{E}_d$, the binary forms $aX^d + bY^d$ and $a'X^d + b'Y^d$ are not isomorphic, as shown by Lemma 1.14. Finally, for $(a,b) \in \mathcal{E}_d$ and $(x,y) \in \mathbb{Z}^2$, we have

$$ax^d + by^d \geq (\max\{|x|,|y|\})^d.$$

This completes the proof of the condition (v) in Definition 1.10.

The second assertion of Theorem 1.13 then follows from Theorem 1.11. ∎

Our assumptions do not allow any upper bound for $\mathcal{R}_{\geq d}(\mathcal{B}, B, 1)$ better than B: the set of all a, b and $a+b$ for (a,b) in $\bigcup_{d' \geq d} E_{d'}$ may contain all positive integers.

Explicit values for W_F and A_F for $F \in \mathcal{F}_d$ are given in [SX, Corollary 1.3]. The values of W_F and A_F are computed without the assumptions of a, b having the same sign and d being even, but none of these two hypotheses can be omitted from our theorem, as shown by the two sequences $X^d - (d^d - d)Y^d$ (d even) and $X^d + (d^d - d)Y^d$ (d odd).

1.3.2. *Products of positive quadratic forms.* Let $(\mu_n)_{n\geq 1}$ be an increasing sequence of positive squarefree integers; assume that there exists $\lambda > 0$ such that

$$\mu_n \leq \lambda n \quad \text{for all } n \geq 1. \tag{1.13}$$

If we choose $\mu_n = q_n$ where $(q_n)_{n\geq 1}$ is the full sequence

$$1,\ 2,\ 3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 13,\ 14,\ 15, \ldots$$

of positive squarefree integers, written in ascending order, then, as is well known (see [HW, Theorem 333] and https://oeis.org/A005117), we have

$$\sharp\{q_n \leq x\} = \sum_{n \leq x} \mu(n)^2 = \frac{6}{\pi^2}x + O(\sqrt{x}),$$

which implies that

$$q_n \sim \frac{\pi^2}{6} n \qquad (n \to \infty).$$

Since $\mu_{230} \geq q_{230} = 381$, we have $\lambda \geq \frac{381}{230}\cdot$ As a matter of fact, we have

$$\sup_{n \geq 1} \frac{q_n}{n} = \frac{381}{230}\cdot \tag{1.14}$$

Hence, in the special case $\mu_n = q_n$ $(n \geq 1)$, $\lambda = 381/230$ is an admissible value.

For $d \geq 2$ and $1 \leq \nu \leq d+1$, we denote by $Q^+_{d,\nu}$ the binary form of degree $2d$ defined by the formula

$$Q^+_{d,\nu}(X,Y) := \prod_{\substack{1 \leq n \leq d+1 \\ n \neq \nu}} (X^2 + \mu_n Y^2). \tag{1.15}$$

The associated family is

$$\mathcal{Q}^+ := \{Q^+_{d,\nu} : d \geq 2,\ 1 \leq \nu \leq d+1\}$$

with $\mathcal{Q}^+_d = \emptyset$ for d odd and $\mathcal{Q}^+_{2d} = \{Q^+_{d,\nu} : 1 \leq \nu \leq d+1\}$ for $d \geq 2$. With λ defined in (1.13), we have

Theorem 1.15. *The family* $\mathcal{Q}^+$ *is* $(2,1,0,4,1)$*-regular.*

Furthermore, for every $d \geq 2$, $\mathcal{Q}^+_{2d}$ *satisfies condition* (C3) *of Corollary* 1.12.

Finally, for every $d \geq 2$ *and every* $\varepsilon > 0$ *we have*

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^+, B, 0) = \frac{1}{4}\Big(\sum_{F \in \mathcal{Q}^+_{2d}} A_F\Big) B^{1/d} + O_{\lambda,d,\varepsilon}(B^{\max\{\vartheta_{2d}+\varepsilon, 1/(d+1)\}}) \tag{1.16}$$

uniformly for $B \to \infty$, *and*

$$\frac{\pi}{\sqrt{\lambda}} \cdot \sqrt{d} < \Big(\sum_{F \in \mathcal{Q}^+_{2d}} A_F\Big) < \pi\sqrt{\mathrm{e}}\,(\sqrt{d}+1). \tag{1.17}$$

See (2.5) for a simplification of the exponent in the error term of (1.16).

Remark 1.16 (*Thanks to Jean-Baptiste Fouvry*). Consider the quartic forms

$$Q^+_{2,3}(X,Y) = (X^2+Y^2)(X^2+2Y^2), \qquad Q^+_{2,1}(U,V) = (U^2+2V^2)(U^2+3V^2).$$

One checks

$$Q^+_{2,3}(X,Y) - Q^+_{2,1}(U,Y) = (-U^2+X^2-Y^2)(U^2+X^2+4Y^2).$$

The Pythagorean triples (y,u,x) which are the solutions of the equation $y^2+u^2=x^2$ produce solutions (m,x,y,u) to the equations

$$m = Q^+_{2,3}(x,y) = Q^+_{2,1}(u,y).$$

It follows that the exponent $\vartheta_4 = 0.448$ in Theorem 1.1 cannot be replaced with an exponent < 0.25.

1.3.3. *Products of indefinite quadratic forms.* With the above notations, including the definition of λ in (1.13), we assume $\mu_1 \geq 2$ and we consider, for $d \geq 2$ and $1 \leq \nu \leq d+1$, the binary form of degree $2d$ defined by

$$Q^-_{d,\nu}(X,Y) := \prod_{\substack{1\leq n\leq d+1 \\ n\neq\nu}} (X^2 - \mu_n Y^2).$$

The associated family is

$$\mathcal{Q}^- := \{Q^-_{d,\nu} : d \geq 2,\ 1 \leq \nu \leq d+1\}$$

with $\mathcal{Q}^-_d = \emptyset$ for d odd and $\mathcal{Q}^-_{2d} = \{Q^-_{d,\nu} : 1 \leq \nu \leq d+1\}$ for $d \geq 2$.

From (1.14) one deduces

$$\sup_{n\geq 1} \frac{q_{n+1}}{n} = 2,$$

hence $\lambda \geq 2$. In the special case $\mu_n = q_{n+1}$ $(n \geq 1)$, an admissible value for λ is $\lambda = 2$.

THEOREM 1.17. *For $A > 2\mathrm{e}\lambda$, the family $\mathcal{Q}^-$ is $(A, 1, 2, 2, 2\mathrm{e}\lambda)$-regular and satisfies condition* (C3) *of Corollary* 1.12.

Furthermore, for $d \geq 2$, we have

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, 0) = \frac{1}{4}\Big(\sum_{F\in\mathcal{Q}^-_{2d}} A_F\Big) B^{1/d} + O_{\lambda,A,d,\varepsilon}(B^{\max\{\vartheta_{2d}+\varepsilon, 1/(d+1)\}}),$$

uniformly for $B \to \infty$.

Finally,

$$\frac{\pi}{\sqrt{\lambda}} \cdot \sqrt{d} \leq \sum_{F\in\mathcal{Q}^-_{2d}} A_F \leq 22\lambda\sqrt{d}, \tag{1.18}$$

where the lower bound is valid for all $d \geq 2$ and the upper bound for d sufficiently large.

1.3.4. *Products of linear factors.* We reserve the letter p for prime numbers and we consider, for $5 \leq d \leq p$, the binary form $L_{d,p} \in \mathrm{Bin}(d,\mathbb{Z})$ defined by

$$L_{d,p}(X,Y) := (X - pY) \cdot \prod_{0\leq n\leq d-2} (X - nY).$$

The associated family is

$$\mathcal{L} := \{L_{d,p} : d \geq 5,\ d \leq p < 2d\}.$$

We have the following result:

THEOREM 1.18. *The family $\mathcal{L}$ is $(10, 1, 1, 5, 9)$-regular.*

Furthermore, for $d \geq 5$, $\mathcal{L}_d$ satisfies condition (C1) *of Corollary* 1.12 *for d odd and condition* (C2) *for d even.*

Finally, for every $d \geq 5$ and every $\varepsilon > 0$, one has

$$\mathcal{R}_{\geq d}(\mathcal{L}, B, 0) = \frac{1}{(2,d)}\Big(\sum_{d\leq p<2d} A_{L_{d,p}}\Big)B^{2/d} + O_{d,\varepsilon}(B^{\max\{\vartheta_d, 2/(d+1)\}}), \tag{1.19}$$

uniformly for $B \to \infty$, and

$$\frac{\mathrm{e}^2 - o(1)}{\log d} \leq \sum_{d\leq p<2d} A_{L_{d,p}} \leq \frac{5\mathrm{e}^2 + 2\mathrm{e} + o(1)}{\log d}$$

uniformly for $d \to \infty$.

The numerical values are $\mathrm{e}^2 = 7.389\ldots$ and $5\mathrm{e}^2 + 2\mathrm{e} = 42.381\ldots$.

See (2.6) for a simplification of the exponent in the error term of (1.19).

REMARK 1.19. We now give some hints on the construction of the family $\mathcal{L}$. More generally, consider the binary form of degree d defined by

$$L_{\mathbf{n},d}(X,Y) := \prod_{1\leq i\leq d}(X - n_iY),$$

where $\mathbf{n} := \{n_1 < \cdots < n_d\}$ is a set of d integers. Fix $d \geq 5$; then for almost all $\mathbf{n}$ (in the sense of Zariski topology), the group of automorphisms of $L_{\mathbf{n},d}$ is trivial, which means equal to $\{\mathrm{Id}\}$ or $\{\pm\mathrm{Id}\}$, according to the parity of d. Similarly, for fixed $d \geq 5$, for almost all $(\mathbf{m},\mathbf{n})$ the binary forms $L_{\mathbf{m},d}$ and $L_{\mathbf{n},d}$ are not isomorphic. For statements of that type, see [FK] for instance. The strategy of choosing $n_1 = 0$ and $n_d = p$, where p is a large prime, ensures that the group of automorphisms is trivial and that the binary forms that we meet are not isomorphic. These statements are proved by appealing to the classical properties of the cross-ratio (see §6.1 and §6.2).

Finally, we choose for $n_1, \ldots, n_{d-1}$ the first $d-1$ integers. This enables us to estimate the area $A_{L_{d,p}}$ (see §6.6) via Stirling's formula

$$N^N\mathrm{e}^{-N}\sqrt{2\pi N} < N! < N^N\mathrm{e}^{-N}\sqrt{2\pi N}\,\mathrm{e}^{1/(12N)}, \tag{1.20}$$

which is valid for all $N \geq 1$. In particular, as $N \to \infty$, we have

$$\log N - 1 < \frac{1}{N}\log(N!) < \log N - 1 + o(1).$$

It would be interesting to further investigate the explicit construction of other regular families of forms which are products of $\mathbb{Z}$-linear forms.

REMARK 1.20. A natural way to generalize the construction of the families $\mathcal{B}$, $\mathcal{Q}^-$ and $\mathcal{Q}^+$ is to consider sets of forms which are products of binomials of the shape

$$\mathrm{B}_{a,n}(X,Y) = X^a + nY^a.$$

The key point is to choose the integers n and the exponents $a \geq 2$ in such a way that we are able to control the homographies in $\mathrm{PGL}(2, \mathbb{Q})$ which exchange the set of zeroes of the products of $\mathrm{B}_{a,n}$.

2. Proof of Theorem 1.1

2.1. Beginning of the proof. The starting point is [FW, Théorème 3.1]. To state this result we use the following notations:

If F_1 and F_2 belong to $\mathrm{Bin}(d, \mathbb{Z})$ and if $B \geq 1$, we put

$$\mathcal{M}(F_1, F_2; B) = \sharp\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : \max |x_i| \leq B,\ F_1(x_1, x_2) = F_2(x_3, x_4)\},$$

$$\mathcal{M}^*(F_1, F_2; B) = \sharp\{(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4 : \max |x_i| \leq B,\ F_1(x_1, x_2) = F_2(x_3, x_4) \neq 0\}.$$

For $d \geq 3$, we introduce

$$\eta_d = \begin{cases} \frac{2}{9} + \frac{73}{108\sqrt{3}} & \text{for } d = 3, \\ \frac{1}{2d} + \frac{9}{4d\sqrt{d}} & \text{for } 4 \leq d \leq 20, \\ \frac{1}{d} & \text{for } d \geq 21 \end{cases}$$

and

$$\vartheta_d = \frac{d\eta_d}{d\eta_d + d - 2} \tag{2.1}$$

and

$$\eta'_{d,F_1,F_2} = \begin{cases} \eta_d & \text{if the binary form } F_1(X,Y)F_2(X,Y) \text{ has no zero in } \mathbb{P}^1(\mathbb{R}), \\ \vartheta_d & \text{otherwise.} \end{cases} \tag{2.2}$$

Here are the first approximate values for η_d, ϑ_d and κ_d (recall (1.11)):

d	η_d	ϑ_d	κ_d
3	0.612	0.647	0.631
4	0.406	0.448	0.428
5	0.301	0.334	0.309
6	0.236	0.261	0.234
7	0.192	0.211	0.184
8	0.161	0.177	0.150

For $d \geq 3$ and for F_1 and F_2 belonging to $\mathrm{Bin}(d, \mathbb{Z})$, one has the inequalities

$$1/d \leq \eta_d \leq \eta'_{d,F_1,F_2} \leq \vartheta_d < 2/d, \tag{2.3}$$

and in particular, for $d \geq 21$, we have $\eta_d = 1/d$ and $\vartheta_d = 1/(d-1)$.

Furthermore, by comparison with κ_d defined in (1.11), we check that

$$\begin{cases} \kappa_d < \vartheta_d & \text{if } 3 \le d \le 20, \\ \kappa_d = \vartheta_d & \text{if } d \ge 21. \end{cases} \tag{2.4}$$

Finally, by a direct computation we have the inequalities

$$\begin{cases} \vartheta_{2d} > 1/(d+1) & \text{if } d = 2,\ 3, \\ \vartheta_{2d} < 1/(d+1) & \text{if } d \ge 4, \end{cases} \tag{2.5}$$

and

$$\begin{cases} \vartheta_d > 2/(d+1) & \text{if } d = 4,\ 5, \\ \vartheta_d < 2/(d+1) & \text{if } d \ge 6. \end{cases} \tag{2.6}$$

We now recall (see [FW, Théorème 3.1])

PROPOSITION 2.1. *Let $d \ge 3$ and let F_1 and F_2 be non-isomorphic forms in* $\mathrm{Bin}(d, \mathbb{Z})$*, not both divisible by a linear form with rational coefficients. Then for all $\varepsilon > 0$ and all $B \ge 1$ one has*

$$\mathcal{M}(F_1, F_2; B) = O_{F_1,F_2,\varepsilon}(B^{d\eta_d+\varepsilon}).$$

As shown by [FW, Remarque 3.2], the above bound may not hold if one of the binary forms is divisible by a linear form over $\mathbb{Q}$. One eliminates this hypothesis by studying the counting function $\mathcal{M}^*$ rather than $\mathcal{M}$. In other words, one has the following variant for Proposition 2.1:

PROPOSITION 2.2. *Let $d \ge 3$ and let F_1 and F_2 be non-isomorphic forms in* $\mathrm{Bin}(d, \mathbb{Z})$*. Then for every $\varepsilon > 0$ and all $B \ge 1$ one has the bound*

$$\mathcal{M}^*(F_1, F_2; B) = O_{F_1,F_2,\varepsilon}(B^{d\eta_d+\varepsilon}).$$

Proof. We refer to the original proof of [FW, Théorème 3.1]. The hypothesis that F_1 or F_2 has no $\mathbb{Q}$-linear factor is only used in [FW, (22)] (which is equation (3.8) in the arXiv version). This case no longer has to be considered when one studies $\mathcal{M}^*$ instead of $\mathcal{M}$. ■

2.2. Lemmas in diophantine approximation. First we prove the following

LEMMA 2.3. *Let $f \in \mathbb{Z}[t]$ be a polynomial of degree $d \ge 1$ and with discriminant different from zero. Let $\xi_1, \dots, \xi_d$ be the complex roots of f. Then there are real constants $c_1 > 0$ and c_2 such that*

(i) *for every $t \in \mathbb{C}$, one has $\min_{1 \le j \le d} |t - \xi_j| \le c_2 |f(t)|$,*
(ii) *for every $t \in \mathbb{R}$, the condition $|f(t)| < c_1$ implies the existence of a real root ξ_i such that $|t - \xi_i| \le c_2 |f(t)|$.*

Proof. This statement is trivial when $d = 1$. We now suppose $d \ge 2$.

We further suppose that a_0 (the leading coefficient of f) is ≥ 1 and we factor f into

$$f(t) = a_0 \prod_{j=1}^{d} (t - \xi_j).$$

Let $\delta := \min_{1 \leq i < j \leq d} |\xi_i - \xi_j|$. Since the discriminant of f is different from zero, we have $\delta > 0$. Let i be an index such that $|t - \xi_i| = \min_{1 \leq j \leq d} |t - \xi_j|$. The triangular inequality gives, for $j \neq i$, the lower bound

$$|t - \xi_j| \geq \frac{|t - \xi_j| + |t - \xi_i|}{2} \geq \frac{1}{2} |\xi_j - \xi_i| \geq \frac{\delta}{2}.$$

We write the sequence of inequalities

$$|f(t)| \geq \prod_{1 \leq j \leq d} |t - \xi_j| \geq |t - \xi_i| \left(\frac{\delta}{2}\right)^{d-1},$$

which leads to point (i) with $c_2 = (2/\delta)^{d-1}$.

For item (ii), we now suppose that t is real. We decompose the proof into three cases.

If all the ξ_j are real, there is nothing to prove as a consequence of (i). We choose $c_1 = 1$ for instance.

If no ξ_j is real, we set

$$c_1 := \inf_{x \in \mathbb{R}} |f(x)|,$$

which is > 0.

If f has at least one real root and at least one non-real root, we put

$$c_1 = \frac{1}{c_2} \min \{|\mathrm{Im}(\xi_i)| : 1 \leq i \leq d,\ \xi_i \notin \mathbb{R}\}.$$

Applying item (i), we notice that for $t \in \mathbb{R}$ the inequality $|f(t)| < c_1$ implies the existence of a root ξ_j such that

$$|t - \xi_j| < c_1 c_2 = \min \{|\mathrm{Im}(\xi_i - t)| : 1 \leq i \leq d,\ \xi_i \notin \mathbb{R}\}.$$

If ξ_j were not real, we would deduce that $|t - \xi_j| < |\mathrm{Im}(t - \xi_j)|$, which is impossible. Hence ξ_j is real. ∎

The following lemma provides an upper bound for the tail of the series defining the Riemann ζ-function.

Lemma 2.4. *For all real $\delta > 1$ and all positive integer B, one has*

$$\sum_{n \geq B} \frac{1}{n^\delta} \leq \zeta(\delta) B^{1-\delta}.$$

Proof. By dividing the interval of summation into intervals with length B and by using the inequality $Bq + r \ge Bq$, we write

$$\sum_{n\ge B} \frac{1}{n^\delta} = \sum_{q\ge 1}\sum_{r=0}^{B-1} \frac{1}{(Bq+r)^\delta} \le B^{1-\delta}\sum_{q\ge 1}\frac{1}{q^\delta} = \zeta(\delta)B^{1-\delta}. \ \blacksquare$$

The next lemma was inspired by [Ho, pp. 34–36].

Lemma 2.5. *Let ξ, κ, s, Q_1 and Q_2 be real numbers such that $s > 2$, $\kappa > 0$, $Q_2 > Q_1 \ge 1$. Then the number of rational numbers $\frac{p}{q}$ such that*

$$\left|\xi - \frac{p}{q}\right| \le \frac{\kappa}{q^s} \quad \textit{and} \quad Q_1 \le q \le Q_2$$

is bounded by

$$\frac{2^{s+1}\kappa}{(2^{s-2}-1)Q_1^{s-2}} + \left\lceil \frac{\log\frac{Q_2}{Q_1}}{\log 2}\right\rceil.$$

Proof. First we consider the case when $Q_2 \le 2Q_1$ and we prove the result with the coefficient $\frac{2^{s+1}}{2^{s-2}-1}$ replaced by 8. Two distinct rational numbers $\frac{p}{q}$, $\frac{p'}{q'}$ such that $Q_1 \le q, q' \le Q_2$ satisfy the inequalities

$$\left|\frac{p}{q} - \frac{p'}{q'}\right| \ge \frac{1}{qq'} \ge \frac{1}{Q_2^2} \ge \frac{1}{4Q_1^2}.$$

If they also satisfy

$$\left|\xi - \frac{p}{q}\right| \le \frac{\kappa}{q^s} \quad \text{and} \quad \left|\xi - \frac{p'}{q'}\right| \le \frac{\kappa}{q'^s},$$

then they belong to the interval

$$\left[\xi - \frac{\kappa}{Q_1^s}, \xi + \frac{\kappa}{Q_1^s}\right],$$

the length of which is $2\kappa/Q_1^s$. So the number of such $\frac{p}{q}$ is less than

$$4Q_1^2\frac{2\kappa}{Q_1^s} + 1 = \frac{8\kappa}{Q_1^{s-2}} + 1.$$

In the case where $Q_2 > 2Q_1$, we cover the interval $[Q_1, Q_2]$ by ℓ intervals $[2^hQ_1, 2^{h+1}Q_1]$, $0 \le h \le \ell - 1$, with $2^{\ell-1}Q_1 < Q_2 \le 2^\ell Q_1$; thus ℓ satisfies the inequalities

$$\frac{\log\frac{Q_2}{Q_1}}{\log 2} \le \ell < 1 + \frac{\log\frac{Q_2}{Q_1}}{\log 2}.$$

As we have seen, in the interval $[2^hQ_1, 2^{h+1}Q_1]$, the number of rational numbers $\frac{p}{q}$ satisfying our assumption is bounded by

$$\frac{8\kappa}{2^{h(s-2)}Q_1^{s-2}} + 1.$$

The total number of fractions $\frac{p}{q}$ satisfying our assumption is less than

$$\sum_{h=0}^{\ell-1}\left(\frac{8\kappa}{2^{h(s-2)}Q_1^{s-2}}+1\right)=\frac{8\kappa}{Q_1^{s-2}}\sum_{h=0}^{\ell-1}\frac{1}{2^{h(s-2)}}+\ell$$
$$<\frac{8\kappa}{Q_1^{s-2}}\cdot\frac{2^{s-2}}{2^{s-2}-1}+\left\lceil\frac{\log\frac{Q_2}{Q_1}}{\log 2}\right\rceil. \blacksquare$$

2.3. On the set of values taken by a binary form when one of the variables is large. As a consequence of the three lemmas proved in §2.2 we will deduce

PROPOSITION 2.6. *Let $d \geq 3$ and let $F \in \mathrm{Bin}(d,\mathbb{Z})$. Then there are constants c_3 and c_4, effectively computable and depending on F only, such that, for all $\Delta > c_3$ and all $A > 0$, one has*

$$\sharp\{(x,y)\in\mathbb{Z}^2 : 0<|F(x,y)|\leq A,\ |y|\geq A^{1/d}\Delta\}\leq c_4(A^{2/d}\Delta^{2-d}+A^{1/(d-1)}).$$

The proof of this proposition will use the following effective refinement of Liouville's inequality, due to N. I. Fel'dman [F]:

LEMMA 2.7. *Let ξ be an algebraic number of degree $d \geq 3$. There are effectively computable positive constants $c_5 = c_5(\xi)$ and $c_6 = c_6(\xi)$ such that, for every fraction $p/q \in \mathbb{Q}$ with $q \geq 1$, one has*

$$\left|\xi-\frac{p}{q}\right|\geq\frac{c_5}{q^{d-c_6}}.$$

A completely explicit version of this inequality can be found in [GP, (13), p. 248].

We deduce from this lemma the following one.

LEMMA 2.8. *Let $P(X) \in \mathbb{Z}[X]$ be a polynomial of degree $d \geq 3$. There are effectively computable positive constants $c_5' = c_5'(P)$ and $c_6' = c_6'(P)$ such that, for every root ξ of P, and every rational number p/q such that $q \geq 1$ and $p/q \neq \xi$, we have*

$$\left|\xi-\frac{p}{q}\right|\geq\frac{c_5'}{q^{d-c_6'}}. \tag{2.7}$$

We stress that there is no assumption on whether the polynomial P is irreducible or not, nor on whether the root ξ is real or not.

Proof of Lemma 2.8. Let δ be the degree of ξ. We split the argument according to the value of δ and to the nature of ξ.

If ξ is not real, inequality (2.7) is trivial since $|\xi - p/q| \geq |\mathrm{Im}\,\xi|$ for every rational number p/q.

We now suppose that ξ is a real number.

If $\delta = 1$, we put $\xi = a/b$ with a and b integers and $b \geq 1$. We have $|a/b-p/q| = |aq-bp|/(bq) \geq 1/(bq)$, since ξ is different from p/q. We obtain (2.7) with the choices $c'_5 = 1/b$ and $c'_6 = 1$ since $d \geq 3$.

If $\delta = 2$, the real number ξ is quadratic. Liouville's inequality for quadratic real numbers is optimal: there exists $\alpha = \alpha(\xi) > 0$ such that

$$\left|\xi - \frac{p}{q}\right| \geq \frac{\alpha}{q^2}\cdot$$

By the hypothesis $d \geq 3$, we deduce (2.7) with the choice $c'_5 = \alpha$ and $c'_6 = 1/2$.

If $\delta \geq 3$, we apply Lemma 2.7 in the form

$$\left|\xi - \frac{p}{q}\right| \geq \frac{c_5}{q^{\delta - c_6}}\cdot$$

Since $\delta \leq d$, we obtain (2.7) with the choice $c'_5 = c_5$ and $c'_6 = c_6$.

To complete the proof, we choose for $c'_5 = c'_5(P)$ and for $c'_6 = c'_6(P)$ the least values c'_5 and c'_6 corresponding to the various ξ that we met above ■

Proof of Proposition 2.6. Let $f(t) = F(t,1)$, so $F(x,y) = y^d f(x/y)$. Let d' be the degree of f. Since the discriminant of F is different from zero, we have

$$d' = d \quad \text{or} \quad d-1.$$

If f has no real root, then, for sufficiently large $\varDelta$ (more precisely, for $\varDelta > (\inf_{t\in\mathbb{R}} |f(t)|)^{-1/d}$), the set

$$\{(x,y) \in \mathbb{Z}^2 : 0 < |F(x,y)| \leq A,\ |y| \geq A^{1/d}\varDelta\}$$

is empty.

Let $r \geq 1$ be the number of real roots of f, denoted by $\xi_1, \dots, \xi_r$. By hypothesis these roots are simple. Let $(x,y) \in \mathbb{Z}^2$ with $y \neq 0$. The condition $0 < |F(x,y)| \leq A$ implies

$$0 < \left| f\left(\frac{x}{y}\right)\right| \leq \frac{A}{|y|^d}\cdot$$

We suppose $|y| \geq A^{1/d}\varDelta$ and $\varDelta > c_1^{-1/d}$, and we apply Lemma 2.3(ii). We deduce the existence of some $i \in \{1, \dots, r\}$ such that

$$0 < \left|\frac{x}{y} - \xi_i\right| \leq \frac{c_2 A}{|y|^d}, \tag{2.8}$$

which is equivalent to

$$0 < |x - y\xi_i| \leq \frac{c_2 A}{|y|^{d-1}}\cdot \tag{2.9}$$

When the integer y is fixed, the number of integers x satisfying (2.9) is equal to

$$\frac{2c_2A}{|y|^{d-1}}+O(1).$$

We fix $Y_0=A^{1/(d-1)}$ and we sum over $i=1,\dots,r$. We apply Lemma 2.4 with $B=A^{1/d}\varDelta$ and $\delta=d-1$ to deduce that the number of (x,y) with $0<|F(x,y)|\le A$ and $A^{1/d}\varDelta\le|y|\le Y_0$ is bounded by

$$O\bigl(A^{2/d}\varDelta^{2-d}\bigr)+O(Y_0). \tag{2.10}$$

To complete the proof, we use Lemma 2.8, which implies the lower bound

$$\left|\xi_i-\frac{p}{q}\right|\ge\frac{c_5'}{q^{d'-c_6'}}\ge\frac{c_5'}{q^{d-c_6'}}. \tag{2.11}$$

Combining (2.8) with (2.11), we deduce the upper bound $|y|\le Y_1$ with $Y_1=\bigl(\frac{c_2}{c_5'}A\bigr)^{1/c_6'}$. It remains to compute the number of solutions of (2.8) satisfying $Y_0<|y|\le Y_1$. We use Lemma 2.5, with $s=d$, $\kappa=c_2A$, $Q_1=Y_0$, $Q_2=Y_1$ to see that this number is bounded by

$$O(A/Y_0^{d-2})+O(\log Y_1)=O(A^{1/(d-1)}).$$

By adding (2.10) we obtain the upper bound announced in Proposition 2.6. ∎

2.4. End of the proof of Theorem 1.1. We split the argument into two different cases.

Assume first the binary form $F_1(X,Y)F_2(X,Y)$ has no zero in $\mathbb{P}^1(\mathbb{R})$. This holds true if and only if the polynomial

$$F_1(t,1)F_1(1,t)F_2(t,1)F_2(1,t)$$

has no real root. By homogeneity, there is a constant $c_7>0$ such that for all $(x_1,x_2,x_3,x_4)\in\mathbb{R}^4$, one has

$$|F_1(x_1,x_2)|\ge c_7\max\{|x_1|^d,|x_2|^d\}\quad\text{and}\quad|F_2(x_3,x_4)|\ge c_7\max\{|x_3|^d,|x_4|^d\}.$$

This leads to the existence of a constant c_8 such that the inequalities

$$|F_1(x_1,x_2)|\le N\quad\text{and}\quad|F_2(x_3,x_4)|\le N$$

imply $\max(|x_1|,|x_2|,|x_3|,|x_4|)\le B$ with $B:=(c_8N)^{1/d}$. We apply Proposition 2.2 in the form

$$\mathcal{N}(F_1,F_2;N)\le 1+\mathcal{M}^*(F_1,F_2;B)=O_{F_1,F_2}(B^{d\eta_d+\varepsilon})=O_{F_1,F_2}(N^{\eta_d+\varepsilon}).$$

By inequality (2.3), the proof of Theorem 1.1 is complete in that case, including the refinement stated in Remark 1.5.

Assume now that $F_1(X,Y)F_2(X,Y)$ has at least one zero in $\mathbb{P}^1(\mathbb{R})$. This is equivalent to the assumption that $F_1(t,1)F_1(1,t)F_2(t,1)F_2(1,t)$ has at least one real root. The constant η'_{d,F_1,F_2} is now defined by the second formula of (2.2), that is, $\eta'_{d,F_1,F_2} = \vartheta_d$. Let

$$\tau := \frac{\frac{2}{d} - \eta_d}{d\eta_d + d - 2},$$

so we have

$$\frac{2}{d} - (d-2)\tau = \eta_d(1 + d\tau) = \eta'_{d,F_1,F_2}.$$

Let $\varDelta := N^\tau$. To bound from above the number $\mathcal{N}(F_1, F_2; N)$ of $m \in \mathbb{Z}$, $|m| \le N$, such that there is at least one $(x_1, x_2, x_3, x_4) \in \mathbb{Z}^4$ satisfying

$$F_1(x_1, x_2) = F_2(x_3, x_4) = m, \tag{2.12}$$

we first consider those m such that at least one of (x_1, x_2, x_3, x_4) associated to m by (2.12) satisfies

$$\max\{|x_1|, |x_2|, |x_3|, |x_4|\} < N^{1/d}\varDelta.$$

Proposition 2.2 with $B = N^{1/d+\tau}$ shows that the number of those m is bounded by

$$O_{F_1,F_2,\varepsilon}(B^{d\eta_d+\varepsilon}) = O_{F_1,F_2,\varepsilon}(N^{\eta_d(1+d\tau)+\varepsilon}) = O_{F_1,F_2,\varepsilon}(N^{\eta'_{d,F_1,F_2}+\varepsilon}). \tag{2.13}$$

Next, we estimate the number of those m such that all the 4-tuples (x_1, x_2, x_3, x_4) associated to m by (2.12) satisfy

$$\max\{|x_1|, |x_2|, |x_3|, |x_4|\} \ge N^{1/d}\varDelta.$$

For simplicity, we study the case where $|x_1| \ge N^{1/d}\varDelta$, since the other cases are similar. We only consider the values taken by the binary form F_1 and we apply Proposition 2.6. With the choices $F = F_1$ and $A = N$, using $\vartheta_d \ge 1/(d-1)$, we deduce that the number of the relevant m's is bounded by

$$O_{F_1,F_2}(N^{2/d}\varDelta^{2-d} + N^{1/(d-1)}) = O_{F_1,F_2}(N^{\eta'_{d,F_1,F_2}}).$$

By (2.13), this completes the proof of Theorem 1.1.

3. Proof of Theorem 1.11. By similarity with (1.6), we put

$$\mathcal{R}_{=d}(\mathcal{F}, B, A) := \sharp\{m : 0 \le |m| \le B, \text{ and there are } F \in \mathcal{F}_d,\ (x,y) \in \mathbb{Z}^2, \text{ such that } \max\{|x|,|y|\} \ge A \text{ and } m = F(x,y)\}.$$

The lower bound for $\mathcal{R}_{\ge d}(\mathcal{F}, B, A)$ is obtained as follows:

$$\begin{aligned}\mathcal{R}_{\ge d}(\mathcal{F}, B, A) &\ge \mathcal{R}_{=d}(\mathcal{F}, B, A)\\ &\ge \sum_{F\in\mathcal{F}_d} \mathcal{N}(F, F; B) - \sum_{\substack{F,F'\in\mathcal{F}_d\\ F\ne F'}}\sum \mathcal{N}(F, F'; B) - (2A+1)^2 d^{A_1},\end{aligned}$$

where the counting function $\mathcal{N}$ is defined by (1.2). Condition (iii) in Definition 1.10 of a regular family implies $\sharp\mathcal{F}_d = O_d(1)$; thanks to condition (iv) and to the inequality $\kappa_d \le \vartheta_d$ (see (2.4)), Theorems 1.1 and A give

$$\mathcal{R}_{\ge d}(\mathcal{F}, B, A) \ge \Big(\sum_{F \in \mathcal{F}_d} A_F W_F \Big) \cdot B^{2/d} - O_{\mathcal{F},A,\varepsilon}(B^{\vartheta_d + \varepsilon}). \tag{3.1}$$

For the upper bound, we recall that the parameters d_0, κ and A_1 appear in Definition 1.10. We start from the inequality

$$\begin{aligned} \mathcal{R}_{\ge d}(\mathcal{F}, B, A) \le \sum_{F \in \mathcal{F}_d} \mathcal{N}(F, F; B) + \sum_{n=d^\dagger}^{d^\dagger + d_0} \sum_{F \in \mathcal{F}_n} \mathcal{N}(F, F; B) \\ + \sharp\Big(\bigcup_{n > d^\dagger + d_0} \bigcup_{F \in \mathcal{F}_n} (F(\mathcal{Z}_A) \cap [-B, B]) \Big) \end{aligned} \tag{3.2}$$

with

$$\mathcal{Z}_A = \mathbb{Z}^2 \setminus ([-A, A] \times [-A, A]).$$

Applying Theorem A one more time, we have

$$\sum_{F \in \mathcal{F}_d} \mathcal{N}(F, F; B) = \Big(\sum_{F \in \mathcal{F}_d} A_F W_F \Big) \cdot B^{2/d} + O_{\mathcal{F},d,\varepsilon}(B^{\kappa_d + \varepsilon}), \tag{3.3}$$

and

$$\mathcal{N}(F, F; B) = O_F(B^{2/d^\dagger}) \quad \text{if } \deg F \ge d^\dagger. \tag{3.4}$$

Hence the second term on the right-hand side of (3.2) is bounded as follows:

$$\sum_{n=d^\dagger}^{d^\dagger + d_0} \sum_{F \in \mathcal{F}_n} \mathcal{N}(F, F; B) = O_{\mathcal{F},d}(B^{2/d^\dagger}).$$

To deal with the third term on the right-hand side of (3.2), we interchange the summations to write

$$\begin{aligned} \sharp\Big(\bigcup_{n > d^\dagger + d_0} \bigcup_{F \in \mathcal{F}_n} (F(\mathcal{Z}_A) \cap [-B, B]) \Big) \\ \le \sharp\{(n, F, x, y) : n > d^\dagger + d_0,\ F \in \mathcal{F}_n,\ (x, y) \in \mathcal{Z}_A,\ |F(x, y)| \le B\}. \end{aligned} \tag{3.5}$$

Condition (v) in Definition 1.10 of the $(A, A_1, d_0, d_1, \kappa)$-regularity of $\mathcal{F}$ produces a bound for n, by the sequence of inequalities

$$\kappa < A \le \max\{|x|, |y|\} \le \kappa |F(x, y)|^{\frac{1}{n - d_0}} \le \kappa B^{\frac{1}{n - d_0}} \le \kappa B^{\frac{1}{d^\dagger + 1}}, \tag{3.6}$$

which implies

$$n \le d_0 + \frac{\log B}{\log(A/\kappa)}.$$

Furthermore, inequalities (3.6) imply

$$\max\{|x|, |y|\} \le \kappa B^{1/(d^\dagger + 1)}.$$

Combining the above inequalities, we deduce that the number of quadruples (n, F, x, y) on the right-hand side of (3.5) is bounded from above by

$$\left(d_0 + \frac{\log B}{\log(A/\kappa)}\right)^{A_1} (1 + 2\kappa B^{1/(d^\dagger+1)})^2 = o_{\mathcal{F}}(B^{2/d^\dagger}). \tag{3.7}$$

Gathering (3.2), (3.3), (3.4) and (3.7), we finally obtain the upper bound

(3.8)
$$\mathcal{R}_{\geq d}(\mathcal{F}, B, A) \leq \Big(\sum_{F \in \mathcal{F}_d} A_F W_F\Big) \cdot B^{2/d} + O_{\mathcal{F},A,d,\varepsilon}(B^{\kappa_d+\varepsilon}) + O_{\mathcal{F},d}(B^{2/d^\dagger}).$$

Comparing (3.1) and (3.8) and recalling (2.4), we complete the proof of Theorem 1.11.

4. Proof of Theorem 1.15

4.1. The family $\mathcal{Q}^+$ is $(2, 1, 0, 4, 1)$-regular. Our first purpose is to prove the following

PROPOSITION 4.1. *The family $\mathcal{Q}^+$ is $(2, 1, 0, 4, 1)$-regular.*

Proof. Several times, we will use the following property satisfied by two positive distinct squarefree numbers:

$$n \neq n' \implies \mathbb{Q}(i\sqrt{\mu_n}) \neq \mathbb{Q}(i\sqrt{\mu_{n'}}). \tag{4.1}$$

We now check each of the items of Definition 1.10 of a regular family.

Items (i) and (ii) are trivial.

The family $\mathcal{Q}^+$ contains no element with odd degree d. By contrast, if this degree $d \geq 4$ is even, the family contains $d/2 + 1$ binary forms of degree d. Thus item (iii) is verified with $A_1 = 1$.

For item (iv) we proceed as follows. Suppose that there are two distinct isomorphic forms F and F' in $\mathcal{Q}^+$. Necessarily they have the same degree $2d$. So there exist $1 \leq \nu < \nu' \leq d+1$ and a matrix $\gamma \in \mathrm{GL}(2, \mathbb{Q})$, written as in (1.1), such that

$$Q^+_{d,\nu} = Q^+_{d,\nu'} \circ \gamma.$$

Let $\tilde{\gamma}$ be the homography attached to γ. This homography,

$$\tilde{\gamma} : \mathbb{P}^1(\mathbb{C}) \ni z \mapsto \frac{a_1 z + a_2}{a_3 z + a_4}, \tag{4.2}$$

induces a bijection between the set of zeroes $\mathcal{Z}(Q^+_{d,\nu})$ (in $\mathbb{P}^1(\mathbb{C})$) of $Q^+_{d,\nu}$ and the set of zeroes $\mathcal{Z}(Q^+_{d,\nu'})$. So, $\tilde{\gamma}(i\sqrt{\mu_{\nu'}})$ is a zero of $Q^+_{d,\nu'}$, hence is one of $\pm i\sqrt{\mu_n}$ with $n \neq \nu'$, which contradicts (4.1).

For item (v), the definition (1.15) implies that $Q^+_{d,\nu}(x, y) = 0$ if and only if $(x, y) = (0, 0)$. Furthermore, by positivity, we have the lower bound

$$|Q^+_{d,\nu}(x, y)| \geq (\max\{|x|^2, |y|^2\})^d = (\max\{|x|, |y|\})^{\deg Q^+_{d,\nu}}.$$

The above inequality implies

$$\max\{|x|,|y|\} \le |Q^+_{d,\nu}(x,y)|^{1/\deg Q^+_{d,\nu}},$$

which means (v) is satisfied for $A=2$, $d_0=0$, $d_1=4$ and $\kappa=1$. ∎

4.2. Triviality of the group $\mathrm{Aut}(Q^+_{d,\nu},\mathbb{Q})$**.** We now prove

PROPOSITION 4.2. *For every* $d\ge 2$ *and* $1\le \nu\le d+1$*, one has*

$$\mathrm{Aut}(Q^+_{d,\nu},\mathbb{Q}) = \left\{\begin{pmatrix}\pm 1 & 0\\ 0 & \pm 1\end{pmatrix}\right\}$$

(*Klein group of order* 4).

Proof. The four elements

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

in $\mathrm{GL}(2,\mathbb{Q})$ clearly belong to $\mathrm{Aut}(Q^+_{d,\nu},\mathbb{Q})$. Conversely, let $\gamma = \left(\begin{smallmatrix}a_1 & a_2\\ a_3 & a_4\end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{Q})$ and let $Q^+_{d,\nu}$ be such that

$$Q^+_{d,\nu}\circ\gamma = Q^+_{d,\nu}. \tag{4.3}$$

The set of zeroes $\mathcal{Z}(Q^+_{d,\nu})$ is stable by the homography $\tilde\gamma$ attached to γ. Appealing to (4.1), we deduce

$$\tilde\gamma(i\sqrt{\mu_n}) = \varepsilon_n i\sqrt{\mu_n} \quad (1\le n\le d+1,\ n\ne\nu),$$

where $\varepsilon_n=\pm 1$. We now prove that the value of ε_n is independent of n. Indeed, suppose that there exist m and n such that $\varepsilon_m=1$ and $\varepsilon_n=-1$. Returning to the explicit expression of $\tilde\gamma$ (see (4.2)), we obtain

$$a_1 i\sqrt{\mu_m}+a_2 = i\sqrt{\mu_m}\,(a_3 i\sqrt{\mu_m}+a_4),$$
$$a_1 i\sqrt{\mu_n}+a_2 = -i\sqrt{\mu_n}\,(a_3 i\sqrt{\mu_n}+a_4).$$

Since a_1, a_2, a_3 and a_4 are rational numbers, we deduce the four equalities

$$a_2=-a_3\,\mu_m,\quad a_2=a_3\,\mu_n,\quad a_1=a_4,\quad a_1=-a_4.$$

They imply $(a_1,a_2,a_3,a_4)=(0,0,0,0)$, which is forbidden. So $\tilde\gamma(z)=\varepsilon z$ for some fixed $\varepsilon\in\{\pm 1\}$. This means that for some $\tau\in\mathbb{Q}$, we have

$$\gamma = \begin{pmatrix}\varepsilon\tau & 0\\ 0 & \tau\end{pmatrix}.$$

By the identification in (4.3), we find that $\tau=\pm 1$. ∎

4.3. Estimating the number of images by $\mathcal{Q}^+$ **of** (x,y) **with** $\max\{|x|,|y|\}\ge 2$**.** For the family $\mathcal{Q}^+$, one has $(2d)^\dagger = 2d+2$. Combining Corollary 1.12, Propositions 4.1 and 4.2 and equality (1.10), we obtain the following

Proposition 4.3. *For every $d \geq 2$, one has*

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^+, B, 2) = \frac{1}{4}\Big(\sum_{F \in \mathcal{Q}^+_{2d}} A_F\Big) \cdot B^{1/d} + O_{\lambda,d,\varepsilon}(B^{\vartheta_{2d}+\varepsilon}) + O_{\lambda,d}(B^{1/(d+1)}).$$

4.4. Estimating the number of images by $\mathcal{Q}^+$ of (x, y) with $\max\{|x|, |y|\} < 2$. The difference

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^+, B, 0) - \mathcal{R}_{\geq 2d}(\mathcal{Q}^+, B, 2) \tag{4.4}$$

is bounded from above by the cardinality of the set

$$\begin{aligned} &\{m : 0 \leq m \leq B,\, m = Q^+_{d',\nu}(\pm 1, \pm 1),\, d' \geq d,\, 1 \leq \nu \leq d' + 1\} \\ &\cup \{m : 0 \leq m \leq B,\, m = Q^+_{d',\nu}(0, \pm 1),\, d' \geq d,\, 1 \leq \nu \leq d' + 1\} \cup \{0, 1\}. \end{aligned} \tag{4.5}$$

For every d' and $1 \leq \nu \leq d' + 1$, one has

$$Q^+_{d',\nu}(\pm 1, \pm 1) \geq \prod_{1 \leq n \leq d'} (1 + n^2) \geq (d'\,!)^2.$$

This implies that the inequality $Q^+_{d',\nu}(\pm 1, \pm 1) \leq B$ can only hold if $d' = O(\log B)$. So the cardinality of the first set in (4.5) is bounded by $O(\log^2 B)$. The same bound also applies to the second set. Combining Proposition 4.3 with (4.4) we obtain

Proposition 4.4. *For every $d \geq 2$ and every $\varepsilon > 0$, one has*

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^+, B, 0) = \frac{1}{4}\Big(\sum_{F \in \mathcal{Q}^+_{2d}} A_F\Big) \cdot B^{1/d} + O_{\lambda,d,\varepsilon}(B^{\vartheta_{2d}+\varepsilon}) + O_{\lambda,d}(B^{1/(d+1)}).$$

4.5. Some results on A_F for $F \in \mathcal{Q}^+$. By the definition (1.9), the fundamental domain attached to $Q^+_{d,\nu}$ is

$$\mathcal{D}(Q^+_{d,\nu}) := \Big\{(x, y) \in \mathbb{R}^2 : \prod_{\substack{1 \leq n \leq d+1 \\ n \neq \nu}} (x^2 + \mu_n y^2) \leq 1\Big\}. \tag{4.6}$$

Our purpose is to estimate the sum

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) := \sum_{F \in \mathcal{Q}^+_{2d}} A_F$$

as $d \to \infty$. We use integration techniques to express this sum of fundamental areas as follows.

Lemma 4.5. *For any $d \geq 2$ and $1 \leq \nu \leq d + 1$, one has*

$$A_{Q^+_{d,\nu}} = \int_{-\infty}^{\infty} \frac{(u^2 + \mu_\nu)^{1/d}}{G_d(u)^{1/d}}\, \mathrm{d}u,$$

where

$$G_d(u) := \prod_{n=1}^{d+1} (u^2 + \mu_n).$$

Hence

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) = \int_{-\infty}^{\infty} \frac{\sum_{1 \le n \le d+1} (u^2 + \mu_n)^{1/d}}{G_d(u)^{1/d}}\, \mathrm{d}u.$$

Proof. By (4.6) and by the change of variables $x = uv$, $y = v$ we have

$$A_{Q^+_{d,\nu}} = \iint_{\mathcal{D}(Q^+_{d,\nu})} \mathrm{d}x\, \mathrm{d}y = \iint_{v^{2d} \prod_{1 \le n \le d+1,\, n \ne \nu} (u^2 + \mu_n) \le 1} |v|\, \mathrm{d}u\, \mathrm{d}v$$
$$= \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{1 \le n \le d+1,\, n \ne \nu} (u^2 + \mu_n)^{1/d}}.$$

Compare with [B, p. 122]. Summing over all the $Q^+_{d,\nu} \in \mathcal{Q}^+_{2d}$, we obtain the second formula of Lemma 4.5. ∎

We first give a lower bound of $\mathrm{Coef}(\mathcal{Q}^+, 2d)$. We have

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) \ge (d+1) \int_{-\infty}^{\infty} \frac{(u^2 + \mu_1)^{1/d}}{G_d(u)^{1/d}}\, \mathrm{d}u \tag{4.7}$$
$$\ge (d+1) \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{2 \le n \le d+1} (u^2 + \mu_n)^{1/d}}$$
$$\ge (d+1) \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{u^2 + \mu_{d+1}} \ge \pi \cdot \frac{d+1}{\sqrt{\mu_{d+1}}}.$$

From our assumption $\mu_{d+1} \le \lambda(d+1)$ we deduce from (4.7) the lower bound

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) > \frac{\pi}{\sqrt{\lambda}} \sqrt{d}. \tag{4.8}$$

For the upper bound, we write

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) \le (d+1) \int_{-\infty}^{\infty} \frac{(u^2 + \mu_{d+1})^{1/d}}{G_d(u)^{1/d}}\, \mathrm{d}u$$
$$\le (d+1) \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{1 \le n \le d} (u^2 + \mu_n)^{1/d}}.$$

Using Hölder's inequality we deduce

$$\begin{aligned}\mathrm{Coef}(\mathcal{Q}^+, 2d) &\le (d+1)\prod_{n=1}^{d}\left(\int_{-\infty}^{\infty}\frac{\mathrm{d}u}{u^2+\mu_n}\right)^{1/d}\\ &\le \pi(d+1)\prod_{n=1}^{d}\mu_n^{-1/(2d)} \le \pi\frac{d+1}{D}\end{aligned}$$

with $D := (d\,!)^{1/(2d)}$. Using the Stirling formula (1.20), we deduce

$$\mathrm{Coef}(\mathcal{Q}^+, 2d) \le \pi\sqrt{\mathrm{e}}\,(\sqrt{d}+1).$$

Combining with (4.8) we complete the proof of (1.17). Recalling Propositions 4.2 and 4.4, we conclude that the proof of Theorem 1.15 is now complete.

5. Proof of Theorem 1.17. Recall that for $d \ge 2$ and $1 \le \nu \le d+1$, $Q^-_{d,\nu}$ denotes the following binary form of degree $2d$:

$$Q^-_{d,\nu}(X,Y) = \prod_{\substack{1\le n\le d+1\\ n\ne\nu}}(X^2-\mu_n Y^2),$$

and $\mathcal{Q}^-$ denotes the family

$$\mathcal{Q}^- = \{Q^-_{d,\nu} : d \ge 2,\ 1 \le \nu \le d+1\}.$$

5.1. The family $\mathcal{Q}^-$ is $(A, 1, 2, 2, 2\mathrm{e}\lambda)$-regular. Our goal in this subsection is to prove the following

PROPOSITION 5.1. *For $A>2\mathrm{e}\lambda$, the family $\mathcal{Q}^-$ is $(A, 1, 2, 2, 2\mathrm{e}\lambda)$-regular.*

The proofs of items (i)–(iv) in Definition 1.10 of a regular family are the same as for Proposition 4.1: one only replaces (4.1) with the remark that for positive squarefree numbers n, n' we have

$$n \ne n' \implies \mathbb{Q}(\sqrt{\mu_n}) \ne \mathbb{Q}(\sqrt{\mu_{n'}}).$$

It remains to check condition (v) in Definition 1.10. We start with an auxiliary lemma

LEMMA 5.2. *For m and d integers satisfying $1 \le m < d$, we have*

$$\left(\frac{d}{m}-1\right)^{d-m} \ge \mathrm{e}^{-\mathrm{e}^{-1}m};$$

further, for n an integer in the range $1 \le n \le d$, we have

$$\frac{n!(d-n)!}{n^d} \ge \mathrm{e}^{-(1+\mathrm{e}^{-1})d}.$$

The numerical value of $\mathrm{e}^{1+\mathrm{e}^{-1}}$ is $3.927\cdots < \frac{79}{20}$.

Proof of Lemma 5.2. Set $t = d - m$, $f_m(t) = \left(\frac{t}{m}\right)^t$, $g_m(t) = \log f_m(t) = t\log t - t\log m$. The derivative $g'_m(t) = 1 + \log t - \log m$ of g_m vanishes at $t = m/\mathrm{e}$, so the minimum of $f_m(t)$ on the interval $0 < t \le d-1$ is reached at $t = m/\mathrm{e}$, giving the value $(t/m)^t = \mathrm{e}^{-t} = \mathrm{e}^{-m/\mathrm{e}}$.

The last part of Lemma 5.2 follows from the first one thanks to Stirling's formula (1.20):

$$\frac{n!(d-n)!}{n^d} \ge \frac{n^n}{\mathrm{e}^n}\cdot\frac{(d-n)^{d-n}}{\mathrm{e}^{d-n}}\cdot\frac{1}{n^d} = \frac{(d-n)^{d-n}}{n^{d-n}\mathrm{e}^d} \ge \mathrm{e}^{-d}\mathrm{e}^{-\mathrm{e}^{-1}n} \ge \mathrm{e}^{-(1+\mathrm{e}^{-1})d}. \ \blacksquare$$

The last inequality of Lemma 5.2 implies

$$(5.1)\qquad (n!(d-n)!)^{1/d} \ge \mathrm{e}^{-1-\mathrm{e}^{-1}}\max\{n, d-n\} \ge \frac{d}{2\mathrm{e}^{1+\mathrm{e}^{-1}}} \ge \frac{d}{2\mathrm{e}^2}.$$

End of the proof of Proposition 5.1. Let $d \ge 2$, $1 \le \nu \le d+1$, $(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. Set $Q = Q^-_{d,\nu}(x,y)$. Our goal it to prove

$$(5.2)\qquad |Q| > (2\mathrm{e}\lambda)^{-2d+2}(\max\{|x|,|y|\})^{2d-2}.$$

We consider three cases depending on the sign of the factors $x^2 - \mu_n y^2$.

If $x^2 < \mu_1 y^2$, all factors are negative. For $2 \le n \le d+1$ we have

$$|x^2 - \mu_n y^2| = \mu_n y^2 - x^2 > (\mu_n - \mu_1)y^2.$$

When $\nu \ge 2$, we use the lower bound $\mu_1 y^2 - x^2 \ge 1$ and obtain

$$|Q| > (\mu_2 - \mu_1)\cdots(\mu_{d+1} - \mu_1)(\mu_\nu - \mu_1)^{-1} y^{2d-2} \ge (d-1)!y^{2d-2}.$$

For $\nu = 1$ the stronger lower bound $|Q| > (d-1)!y^{2d}$ holds. Hence for $1 \le \nu \le d+1$ we have

$$|Q| > \frac{(d-1)!}{\mu_1^{d-1}} x^{2d-2} \ge \frac{(d-1)!}{\lambda^{d-1}} x^{2d-2}.$$

The desired estimate (5.2) follows.

If $x^2 > \mu_{d+1}y^2$, all factors are positive and $\max\{|x|,|y|\} = |x|$. For $m = 1, \dots, d$ we have

$$x^2 - \mu_m y^2 > (\mu_{d+1} - \mu_m)\frac{x^2}{\mu_{d+1}},$$

while for $m = d+1$ we have $x^2 - \mu_{d+1}y^2 \ge 1$. Hence for $1 \le \nu \le d$ we have

$$\begin{aligned}|Q| &= Q \\ &> (\mu_{d+1} - \mu_1)(\mu_{d+1} - \mu_2)\cdots(\mu_{d+1} - \mu_d)(\mu_{d+1} - \mu_\nu)^{-1}\frac{x^{2d-2}}{\mu_{d+1}^{d-1}} \ge \frac{d!x^{2d-2}}{\mu_{d+1}^{d-1}}.\end{aligned}$$

The lower bound $|Q| > d!x^{2d-2}/\mu_{d+1}^{d-1}$ is also true when $\nu = d+1$ since in this case we have

$$|Q| = Q > (\mu_{d+1} - \mu_1)(\mu_{d+1} - \mu_2)\cdots(\mu_{d+1} - \mu_d)\frac{x^{2d}}{\mu_{d+1}^d} \ge \frac{d!x^{2d}}{\mu_{d+1}^d}$$

and $x^2 > \mu_{d+1} y^2 \geq \mu_{d+1}$. Since $d! > d^d \mathrm{e}^{-d}$ (see (1.20)) and $\mu_{d+1} \leq \lambda(d+1)$, we have

$$\frac{d!}{\mu_{d+1}^{d-1}} > \frac{d}{\mathrm{e}\left(1+\frac{1}{d}\right)^{d-1}(\lambda\mathrm{e})^{d-1}} > \frac{1}{(2\mathrm{e}\lambda)^{2d-2}}.$$

This implies (5.2).

Finally, assume that there is an n in the interval $1 \leq n \leq d$ such that

$$x^2 - \mu_{n+1} y^2 < 0 < x^2 - \mu_n y^2.$$

Hence $y \neq 0$ and $\max\{|x|,|y|\} = |x|$. We have

$$\begin{aligned} |Q| = {} & (x^2-\mu_1 y^2)(x^2-\mu_2 y^2)\cdots(x^2-\mu_n y^2) \\ & \times (\mu_{n+1}y^2 - x^2)\cdots(\mu_{d+1}y^2-x^2)|x^2-\mu_\nu y^2|^{-1} \end{aligned} \tag{5.3}$$

with

$$\begin{aligned} & (x^2-\mu_1 y^2)(x^2-\mu_2 y^2)\cdots(x^2-\mu_{n-1} y^2) \\ & \quad > (\mu_n-\mu_1)(\mu_n-\mu_2)\cdots(\mu_n-\mu_{n-1})y^{2n-2} \geq (n-1)!y^{2n-2} \end{aligned} \tag{5.4}$$

and

$$\begin{aligned} & (\mu_{n+2}y^2-x^2)\cdots(\mu_{d+1}y^2-x^2) \\ & \quad > (\mu_{n+2}-\mu_{n+1})\cdots(\mu_{d+1}-\mu_{n+1})y^{2d-2n} \geq (d-n)!y^{2d-2n}. \end{aligned} \tag{5.5}$$

For $1 \leq \nu \leq n-1$, we use the lower bound

$$(x^2-\mu_1 y^2)(x^2-\mu_2 y^2)\cdots(x^2-\mu_{n-1} y^2)(x^2-\mu_\nu y^2)^{-1} > (n-2)!y^{2n-4}, \tag{5.6}$$

while for $n+2 \leq \nu \leq d+1$, we use the lower bound

$$(\mu_{n+2}y^2-x^2)\cdots(\mu_{d+1}y^2-x^2)(\mu_\nu y^2-x^2)^{-1} > (d-n-1)!y^{2d-2n-2}. \tag{5.7}$$

It remains to estimate the product $(x^2-\mu_n y^2)(\mu_{n+1}y^2-x^2)$ of the two terms in the middle of (5.3). We consider two cases.

Assume first $|y| \geq 2$. If $\nu \in \{n, n+1\}$, we use the trivial lower bound

$$(x^2-\mu_n y^2)(\mu_{n+1}y^2-x^2)|x^2-\mu_\nu y^2|^{-1} \geq 1, \tag{5.8}$$

while if $\nu \leq n-1$ or $\nu \geq n+2$ we use the lower bound

$$\begin{aligned} (x^2-\mu_n y^2)(\mu_{n+1}y^2-x^2) & \geq (x^2-\mu_n y^2)+(\mu_{n+1}y^2-x^2)-1 \\ & = (\mu_{n+1}-\mu_n)y^2-1 \geq y^2-1 \geq \frac{3}{4}y^2. \end{aligned} \tag{5.9}$$

For $\nu \in \{n, n+1\}$, from (5.3), (5.4), (5.5), (5.8) we deduce

$$|Q| \geq (n-1)!(d-n)!y^{2d-2}.$$

For $1 \leq \nu \leq n-1$, from (5.3), (5.5), (5.6), (5.9) we deduce

$$|Q| \geq \frac{3}{4}(n-2)!(d-n)!y^{2d-2}.$$

For $n+2 \le \nu \le d+1$, from (5.3), (5.4), (5.7), (5.9) we deduce

$$|Q| \ge \frac{3}{4}(n-1)!(d-n-1)!y^{2d-2}.$$

In all three cases, that is, for all $1 \le \nu \le d+1$, we have, thanks to Lemma 5.2,

$$|Q| \ge \frac{3n!(d-n)!}{4n(d-1)}y^{2d-2} \ge \frac{3n^{d-1}}{4(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}}y^{2d-2}.$$

From $x^2 < \mu_{n+1}y^2 \le \lambda(n+1)y^2 \le 2\lambda n y^2$ we deduce

$$|Q| > \frac{3}{4(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}(2\lambda)^{d-1}}x^{2d-2}.$$

Finally, since $\lambda \ge 2$, we have

$$\frac{3}{4(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}} > \frac{1}{(2\mathrm{e}^2\lambda)^{d-1}} \tag{5.10}$$

for $d \ge 2$, and (5.2) follows.

Assume now that $y^2 = 1$. Hence $\mu_n < x^2 < \mu_{n+1}$, because of the trivial lower bound

$$(x^2-\mu_n)(\mu_{n+1}-x^2) \ge 1,$$

and a combination of the above lower bounds (5.3)–(5.7) yields

$$|Q| \ge \begin{cases} (n-1)!(d-n)! & \text{if } \nu \in \{n, n+1\},\\ (n-2)!(d-n)! & \text{if } 1 \le \nu \le n-1,\\ (n-1)!(d-n-1)! & \text{if } n+2 \le \nu \le d+1. \end{cases}$$

For $1 \le \nu \le d+1$, we obtain, thanks to Lemma 5.2,

$$|Q| \ge \frac{n!(d-n)!}{n(d-1)} \ge \frac{n^{d-1}}{(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}}.$$

If $x^2 \le 2\lambda$, using $n \ge 1$, we deduce

$$|Q| \ge \frac{n^{d-1}}{(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}}\left(\frac{x^2}{2\lambda}\right)^{d-1},$$

while if $x^2 \ge 2\lambda$ we have, by (1.13), the inequalities $n > \frac{x^2}{\lambda} - 1 \ge \frac{x^2}{2\lambda}$, hence again

$$|Q| \ge \frac{x^{2d-2}}{(d-1)\mathrm{e}^{(1+\mathrm{e}^{-1})d}(2\lambda)^{d-1}}.$$

From (5.10) we deduce the estimate (5.2) also when $|y| = 1$.

This completes the proof of Proposition 5.1. ∎

5.2. Triviality of the group $\mathrm{Aut}(Q^-_{d,\nu}, \mathbb{Q})$**.** The following result is the analog of Proposition 4.2. The proof is the same, since $\mu_1 \ge 2$ and the roots of $Q^-_{d,\nu}$ are all irrational numbers.

Proposition 5.3. *For every $d \geq 2$ and $1 \leq \nu \leq d+1$, one has*

$$\mathrm{Aut}(Q^-_{d,\nu}, \mathbb{Q}) = \left\{ \begin{pmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{pmatrix} \right\}$$

(*Klein group of order* 4).

5.3. Estimating the number of images by $\mathcal{Q}^-$ of (x, y) with $\max\{|x|, |y|\} \geq A$. From Corollary 1.12, equalities (1.10) and Propositions 5.1 and 5.3, we deduce

Proposition 5.4. *For every $A > 2\mathrm{e}\lambda$, every $d \geq 2$ and every $\varepsilon > 0$, one has*

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, A) = \frac{1}{4}\Big(\sum_{F \in \mathcal{Q}^-_{2d}} A_F \Big) \cdot B^{1/d} + O_{\lambda, A, d, \varepsilon}(B^{\vartheta_{2d} + \varepsilon}) + O_{\lambda, A, d}(B^{1/(d+1)}).$$

5.4. Estimating the number of images by $\mathcal{Q}^-$ of (x, y) with $\max\{|x|, |y|\} < A$. The difference

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, 0) - \mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, A)$$

is at most the cardinality of the set

$$\big\{ m : 0 \neq |m| \leq B,\, m = Q^-_{d',\nu}(x, y),\, d' \geq d,\\ 1 \leq \nu \leq d' + 1,\, \max\{|x|, |y|\} \leq A \big\}.$$

Given d', the number of such m in this set is bounded by $(d'+1)(2A+1)^2$. Hence we only need to bound from above the value of d' when $|m| \geq 2$.

We first consider the integers of the form $Q^-_{d',\nu}(x, 0)$. As $Q^-_{d',\nu}(\pm 1, 0) = 1$, we may assume $|x| \geq 2$. From

$$Q^-_{d',\nu}(x, 0) = x^{2d'} \leq B$$

we deduce that d' is bounded by $O(\log B)$.

Next let $m = Q^-_{d',\nu}(x, y)$ with $d' \geq d$, $1 \leq \nu \leq d' + 1$, $\max\{|x|, |y|\} \leq A$, $|y| \geq 1$ and $0 < |m| \leq B$. Without loss of generality we may assume $d' > 2A^2$. We split the product

$$\prod_{\substack{1 \leq n \leq d'+2 \\ n \neq \nu}} |x^2 - \mu_n y^2|,$$

the value of which is $|m|$, as $P_1 P_2$ where

$$P_1 = \prod_{\substack{1 \leq n \leq 2A^2 \\ n \neq \nu}} |x^2 - \mu_n y^2|, \qquad P_2 = \prod_{\substack{2A^2 < n \leq d'+2 \\ n \neq \nu}} |x^2 - \mu_n y^2|.$$

The product P_1 is ≥ 1. For $2A^2 < n \leq d' + 2$, since $\mu_n > n$, $|x| \leq A$ and $|y| \geq 1$, we have $\mu_n y^2 - x^2 \geq A^2$, hence

$$(A^2)^{d'-2A^2} \leq P_2 \leq P_1 P_2 = |m| \leq B,$$

which yields

$$d' \leq 2A^2 + \frac{\log B}{2\log A} = O_A(\log B).$$

Hence

$$\mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, 0) - \mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, A) = O_A((\log B)^2).$$

Thanks to Proposition 5.4, this completes the proof of the estimate for $\mathcal{R}_{\geq 2d}(\mathcal{Q}^-, B, 0)$ in Theorem 1.17.

5.5. Some results on A_F for $F \in \mathcal{Q}^-$. By the definition (1.9), the fundamental domain attached to $Q^-_{d,\nu}$ is

$$\mathcal{D}(Q^-_{d,\nu}) := \Big\{(x,y) \in \mathbb{R}^2 : \prod_{\substack{1\leq n\leq d+1\\ n\neq \nu}} |x^2 - \mu_n y^2| \leq 1\Big\}.$$

Our purpose is to estimate the sum

$$\operatorname{Coef}(\mathcal{Q}^-, 2d) := \sum_{F\in\mathcal{Q}^-_{2d}} A_F$$

as $d \to \infty$ by proving (1.18).

Repeating the proof of Lemma 4.5, we obtain

Lemma 5.5. *For any $d \geq 2$ and $1 \leq \nu \leq d+1$, one has*

$$A_{Q^-_{d,\nu}} = \int_{-\infty}^{\infty} \frac{|u^2 - \mu_\nu|^{1/d}}{\prod_{1\leq n\leq d+1} |u^2 - \mu_n|^{1/d}}\, \mathrm{d}u.$$

Hence

$$\operatorname{Coef}(\mathcal{Q}^-, 2d) = \int_{-\infty}^{\infty} \frac{\sum_{1\leq n\leq d+1} |u^2 - \mu_n|^{1/d}}{\prod_{n=1}^{d+1} |u^2 - \mu_n|^{1/d}}\, \mathrm{d}u.$$

Since $|u^2 - \mu_n| \leq u^2 + \mu_n$, the lower bound on $\operatorname{Coef}(\mathcal{Q}^-, 2d)$ is a consequence of the lower bound on $\operatorname{Coef}(\mathcal{Q}^+, 2d)$. More precisely, we have, by Lemma 5.5,

$$A_{Q^-_{d,\nu}} = \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} |u^2 - \mu_n|^{1/d}} \geq \int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} (u^2 + \mu_n)^{1/d}},$$

hence

$$\operatorname{Coef}(\mathcal{Q}^-,2d) \geq (d+1)\int_{-\infty}^{\infty} \frac{\mathrm{d}u}{\prod_{2\leq n\leq d+1}(u^2+\mu_n)^{1/d}}$$

$$\geq (d+1)\int_{-\infty}^{\infty} \frac{\mathrm{d}u}{u^2+\mu_{d+1}} = \pi\cdot\frac{d+1}{\sqrt{\mu_{d+1}}}.$$

This proves the lower bound

$$\operatorname{Coef}(\mathcal{Q}^-,2d) > \frac{\pi}{\sqrt{\lambda}}\sqrt{d}. \tag{5.11}$$

For the upper bound, we use Lemma 5.5 once more. By the change of variable $u^2=v$ we have

$$A_{Q^-_{d,\nu}} = 2\int_0^{\infty} \frac{\mathrm{d}u}{\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} |u^2-\mu_n|^{1/d}} = \int_0^{\infty} \frac{\mathrm{d}v}{\sqrt{v}\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} |v-\mu_n|^{1/d}}.$$

We split the integral as the sum of $d+3$ terms

$$A_{Q^-_{d,\nu}} = \sum_{j=0}^{d+2} A_j$$

with

$$A_0 = \int_0^{\mu_1} \frac{\mathrm{d}v}{\sqrt{v}\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} (\mu_n-v)^{1/d}},$$

$$A_j = \int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{\sqrt{v}\prod_{\substack{1\leq n\leq j\\ n\neq\nu}} (v-\mu_n)^{1/d}\prod_{\substack{j+1\leq n\leq d+1\\ n\neq\nu}} (\mu_n-v)^{1/d}} \quad (1\leq j\leq d+1),$$

$$A_{d+2} = \int_{\mu_{d+2}}^{\infty} \frac{\mathrm{d}v}{\sqrt{v}\prod_{\substack{1\leq n\leq d+1\\ n\neq\nu}} (v-\mu_n)^{1/d}}.$$

Upper bound for A_0. For $\nu=1$, we use the lower bound

$$\prod_{2\leq n\leq d+1} (\mu_n-\mu_1) \geq d! \geq \frac{d^d}{e^d},$$

which follows from Stirling's estimate (1.20), and one deduces

$$A_0 \leq \frac{1}{\prod_{2\leq n\leq d+1}(\mu_n-\mu_1)^{1/d}} \int_0^{\mu_1} \frac{\mathrm{d}v}{\sqrt{v}} \leq \frac{2\mathrm{e}\sqrt{\mu_1}}{d} \leq \frac{2\mathrm{e}\sqrt{\lambda}}{d}.$$

Similarly, for $2\leq\nu\leq d+1$ we have

$$A_0 \leq \frac{1}{\prod_{2\leq n\leq d+1,\, n\neq\nu}(\mu_n-\mu_1)^{1/d}} \int_0^{\mu_1} \frac{\mathrm{d}v}{\sqrt{v}(\mu_1-v)^{1/d}}$$

and

$$\prod_{\substack{2\le n\le d+1\\ n\ne\nu}}(\mu_n-\mu_1)\ge(d-1)!=\frac{d!}{d},$$

hence

$$\prod_{\substack{2\le n\le d+1\\ n\ne\nu}}(\mu_n-\mu_1)^{1/d}\ge\frac{d}{\mathrm{e}\sqrt{2}}\cdot$$

From the upper bounds (recall $\lambda\ge 2$ and $2\le\mu_1\le\lambda$)

$$\begin{aligned}\int_0^{\mu_1}\frac{\mathrm{d}v}{\sqrt{v}\,(\mu_1-v)^{1/d}}&\le\int_0^{\mu_1}\frac{\mathrm{d}v}{\sqrt{v}}+\int_0^{\mu_1}\frac{\mathrm{d}v}{(\mu_1-v)^{1/d}}\\&=2\sqrt{\mu_1}+\frac{d}{d-1}\mu_1^{1-(1/d)}<(2+\sqrt{2})\lambda,\end{aligned}$$

we deduce

$$A_0<\frac{5\mathrm{e}\lambda}{d}\cdot$$

Upper bound for A_j, $1\le j\le d+1$. If $\nu\notin\{j,j+1\}$, we have

$$\begin{aligned}A_j\le&\frac{1}{\sqrt{\mu}_j\prod_{1\le n\le j-1,\,n\ne\nu}(\mu_j-\mu_n)^{1/d}\prod_{j+2\le n\le d+1,\,n\ne\nu}(\mu_n-\mu_{j+1})^{1/d}}\\&\times\int_{\mu_j}^{\mu_{j+1}}\frac{\mathrm{d}v}{(v-\mu_j)^{1/d}(\mu_{j+1}-v)^{1/d}}.\end{aligned}$$

We use (5.1): for $1\le j\le d$ we have

$$\begin{aligned}\prod_{\substack{1\le n\le j-1\\ n\ne\nu}}(\mu_j-\mu_n)\prod_{\substack{j+2\le n\le d+1\\ n\ne\nu}}(\mu_n-\mu_{j+1})&\ge\begin{cases}\frac{(j-1)!(d-j)!}{j-\nu}&\text{for }1\le\nu\le j-1\\ \frac{(j-1)!(d-j)!}{\nu-j-1}&\text{for }j+1\le\nu\le d+1\end{cases}\\&\ge\frac{j!(d-j)!}{d^2}\ge\frac{1}{d^2}\left(\frac{d}{2\mathrm{e}^{1+\mathrm{e}^{-1}}}\right)^d,\end{aligned}$$

while for $j=d+1$ this lower bound becomes

$$\prod_{\substack{1\le n\le d\\ n\ne\nu}}(\mu_{d+1}-\mu_n)\ge\frac{d!}{d+1-\nu}\ge\frac{1}{d^2}\left(\frac{d}{2\mathrm{e}^{1+\mathrm{e}^{-1}}}\right)^d.$$

Next we use the following estimate:

$$\int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}(\mu_{j+1}-v)^{1/d}} \le \frac{2^{1/d}}{(\mu_{j+1}-\mu_j)^{1/d}}\left(\int_{\mu_j}^{(\mu_j+\mu_{j+1})/2} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}} + \int_{(\mu_j+\mu_{j+1})/2}^{\mu_{j+1}} \frac{\mathrm{d}v}{(\mu_{j+1}-v)^{1/d}}\right).$$

We have

$$\int_{\mu_j}^{(\mu_j+\mu_{j+1})/2} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}} = \int_{(\mu_j+\mu_{j+1})/2}^{\mu_{j+1}} \frac{\mathrm{d}v}{(\mu_{j+1}-v)^{1/d}} = \frac{d}{d-1}\left(\frac{\mu_{j+1}-\mu_j}{2}\right)^{1-(1/d)}.$$

Hence

$$\int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}(\mu_{j+1}-v)^{1/d}} \le \frac{d}{d-1}2^{2/d}(\mu_{j+1}-\mu_j)^{1-(2/d)}.$$

For $\nu \notin \{j, j+1\}$, we deduce that

$$A_j \le (4d^2)^{1/d} 2\mathrm{e}^{1+\mathrm{e}^{-1}} \frac{(\mu_{j+1}-\mu_j)^{1-(2/d)}}{(d-1)\sqrt{\mu_j}}.$$

If $\nu = j$, we have

$$A_j \le \frac{1}{\sqrt{\mu}_j \prod_{1\le n\le j-1}(\mu_j-\mu_n)^{1/d} \prod_{j+2\le n\le d+1}(\mu_n-\mu_{j+1})^{1/d}} \times \int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(\mu_{j+1}-v)^{1/d}}$$

and we use the formula

$$\int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(\mu_{j+1}-v)^{1/d}} = \frac{d}{d-1}(\mu_{j+1}-\mu_j)^{1-(1/d)}.$$

If $\nu = j+1$, we have

$$A_j \le \frac{1}{\sqrt{\mu}_j \prod_{1\le n\le j-1}(\mu_j-\mu_n)^{1/d} \prod_{j+2\le n\le d+1}(\mu_n-\mu_{j+1})^{1/d}} \times \int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}}$$

and we use the formula

$$\int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}v}{(v-\mu_j)^{1/d}} = \frac{d}{d-1}(\mu_{j+1}-\mu_j)^{1-(1/d)}.$$

We deduce that for $1 \le j \le d+1$ and $1 \le \nu \le d+1$, we have

$$A_j \le (2\mathrm{e}^{1+\mathrm{e}^{-1}} + o(1)) \frac{\mu_{j+1}-\mu_j}{d\sqrt{\mu_j}}\cdot \tag{5.12}$$

For $j \ge 1$, we also have

$$\mu_j \ge j+1 \ge \frac{1}{\lambda}\,\mu_{j+1},$$

and we deduce that

$$\sum_{j=1}^{d+1} \frac{\mu_{j+1}-\mu_j}{\sqrt{\mu_j}} \le \sqrt{\lambda} \sum_{j=1}^{d+1} \frac{\mu_{j+1}-\mu_j}{\sqrt{\mu_{j+1}}}\cdot$$

Using the inequality

$$\sum_{j=1}^{d+1} \frac{\mu_{j+1}-\mu_j}{\sqrt{\mu_{j+1}}} \le \sum_{j=1}^{d+1} \int_{\mu_j}^{\mu_{j+1}} \frac{\mathrm{d}t}{\sqrt{t}} = \int_{\mu_1}^{\mu_{d+2}} \frac{\mathrm{d}t}{\sqrt{t}} \le 2\sqrt{\mu_{d+2}} \le 2\sqrt{\lambda(d+2)},$$

we deduce from (5.12) that

$$\sum_{j=1}^{d+1} A_j \le \big((2\mathrm{e}^{1+\mathrm{e}^{-1}} + o_\lambda(1))/d\big)\cdot\sqrt{\lambda}\cdot\big(2\sqrt{\lambda(d+2)}\big) \le (4\mathrm{e}^{1+\mathrm{e}^{-1}} + o_\lambda(1))\frac{\lambda}{\sqrt{d}}\cdot$$

Upper bound for A_{d+2}. For $v \ge \mu_{d+2}$ and $1 \le n \le d+1$, we have

$$v - \mu_n \ge v\left(1 - \frac{\mu_n}{\mu_{d+2}}\right),$$

hence

$$A_{d+2} \le \frac{1}{\prod_{1\le n\le d+1,\, n\ne\nu}(1-\mu_n/\mu_{d+2})^{1/d}} \int_{\mu_{d+2}}^{\infty} \frac{\mathrm{d}v}{v^{3/2}}$$

with

$$\int_{\mu_{d+2}}^{\infty} \frac{\mathrm{d}v}{v^{3/2}} = \frac{2}{\sqrt{\mu_{d+2}}} \le \frac{2}{\sqrt{d+2}}$$

and (using Stirling's estimate (1.20) once more)

$$\prod_{\substack{1\le n\le d+1\\ n\ne\nu}} \left(1-\frac{\mu_n}{\mu_{d+2}}\right)^{1/d} \ge \frac{d!^{1/d}}{\mu_{d+2}} \ge \frac{d!^{1/d}}{\lambda(d+2)} \ge \frac{1}{\lambda\mathrm{e}}\left(1+\frac{2}{d}\right)^{-1}.$$

We deduce

$$A_{d+2} \le (2\mathrm{e} + o(1))\frac{\lambda}{\sqrt{d}}\cdot$$

Combining the estimates, we obtain

$$A_{Q^-_{d,\nu}} = \sum_{j=0}^{d+2} A_j \le (4\mathrm{e}^{1+\mathrm{e}^{-1}} + 2\mathrm{e} + o_\lambda(1))\frac{\lambda}{\sqrt{d}}.$$

Summing over all the $Q^-_{d,\nu} \in \mathcal{Q}^-_{2d}$ we conclude

$$\mathrm{Coef}(\mathcal{Q}^-, 2d) \le (4\mathrm{e}^{1+\mathrm{e}^{-1}} + 2\mathrm{e} + o_\lambda(1))\lambda\sqrt{d}.$$

Combining this with (5.11) and with the upper bound $4\mathrm{e}^{1+\mathrm{e}^{-1}} + 2\mathrm{e} < 22$, we complete the proof of (1.18), hence of Theorem 1.17.

6. Proof of Theorem 1.18. We now use the notations of §1.3.4. Our first purpose is to check that the family $\mathcal{L}$ satisfies the conditions of Definition 1.10 of a regular family. Items (i), (ii) are obvious. Item (iii) is trivially satisfied with $A_1 = 1$. Items (iv) and (v) are more subtle.

6.1. Isomorphisms between two elements in $\mathcal{L}$. We will prove the following more general statement which implies that item (iv) is satisfied by $\mathcal{L}$.

PROPOSITION 6.1. *Let $d \ge 4$ be an integer, $\{a_i : 1 \le i \le d-1\}$ and $\{b_j : 1 \le j \le d-2\}$ two sets of integers and p a prime number such that*

$$0 < a_1 < \cdots < a_{d-1} < p, \tag{6.1}$$

$$0 < b_1 < \cdots < b_{d-2} < p. \tag{6.2}$$

Then the binary forms

$$X\prod_{i=1}^{d-1}(X - a_iY) \quad \text{and} \quad (X - pY)X\prod_{j=1}^{d-2}(X - b_jY) \tag{6.3}$$

are not isomorphic.

Proof. The proof is based on classical properties of the cross-ratio of points on $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Recall that if (x_1, x_2, x_3, x_4) is a quadruple of distinct complex numbers, the associated *cross-ratio* is the complex number $[x_1, x_2, x_3, x_4]$ defined by

$$[x_1, x_2, x_3, x_4] := \frac{x_3 - x_1}{x_3 - x_2} \Big/ \frac{x_4 - x_1}{x_4 - x_2}.$$

This definition is naturally extended to $\mathbb{P}^1(\mathbb{C})$ when exactly one of the elements x_1, x_2, x_3, x_4 is equal to ∞. The cross-ratio is invariant by any homography of $\mathbb{P}^1(\mathbb{C})$. In other words, for any homography $\mathfrak{h}$, for any quadruple (x_1, x_2, x_3, x_4) of distinct points of $\mathbb{P}^1(\mathbb{C})$, one has

$$[x_1, x_2, x_3, x_4] = [\mathfrak{h}(x_1), \mathfrak{h}(x_2), \mathfrak{h}(x_3), \mathfrak{h}(x_4)]. \tag{6.4}$$

Let a be a non-zero integer. The canonical decomposition of $|a|$ into prime factors

$$|a| = \prod_p p^{v_p(a)}$$

defines, for each prime number p, the *p-adic valuation* $v_p(a) \in \mathbb{Z}$ of a. Let $t = a/b \neq 0$ be a rational number, written in its irreducible form. The *p-adic valuation* of t is the non-negative integer

$$v_p(t) := \begin{cases} v_p(a) & \text{if } p \nmid b, \\ -v_p(b) & \text{if } p \nmid a. \end{cases}$$

We now begin the proof of Proposition 6.1 proper. We argue by contradiction. Let $F_1(X,Y)$ and $F_2(X,Y)$ be the two binary forms introduced in (6.3). Suppose that there is $\gamma \in \mathrm{GL}(2,\mathbb{Q})$, written as in (1.1), such that

$$F_1 = F_2 \circ \gamma.$$

Then the homography $\mathfrak{h}$ associated with γ has the shape

$$z \mapsto \mathfrak{h}(z) = \frac{az+b}{cz+d}\cdot$$

This homography induces a bijective map between the sets of the polynomials $f_1(X) := F_1(X,1)$ and $f_2(X) := F_2(X,1)$. These sets are $\mathcal{Z}(f_1) := \{0, a_1, \dots, a_{d-1}\}$ and $\mathcal{Z}(f_2) = \{0, b_1, \dots, b_{d-2}, p\}$, treated as subsets of $\mathbb{P}^1(\mathbb{C})$. Consider, for $j = 1, 2$, the subsets of $\mathbb{Q} \setminus \{0\}$ defined by

$$\mathrm{Bir}(f_j) := \{[x_1, x_2, x_3, x_4] : x_i \in \mathcal{Z}(f_j),\ x_i \text{ distinct}\}. \tag{6.5}$$

Equality (6.4) implies that

$$\mathrm{Bir}(f_1) = \mathrm{Bir}(f_2),$$

and also

$$\{v_p(y) : y \in \mathrm{Bir}(f_1)\} = \{v_p(z) : z \in \mathrm{Bir}(f_2)\}.$$

As a consequence of (6.1), we have $\{v_p(y) : y \in \mathrm{Bir}(f_1)\} = \{0\}$. However, we also have $1 \in \{v_p(z) : z \in \mathrm{Bir}(f_2)\}$ by considering the cross-ratio $[0, b_1, p, b_2]$ and (6.2). So we reach a contradiction: the element γ does not exist and the binary forms F_1 and F_2 are not isomorphic. ∎

6.2. Triviality of the group $\mathrm{Aut}(L_{d,p},\mathbb{Q})$**.** In order to determine the value of the coefficient W appearing in Theorem A, we prove the following.

PROPOSITION 6.2. *Let $d \geq 5$ be an integer. For every prime $p \geq d$, the automorphism group of the binary form $L_{d,p}$ is* $\{\mathrm{Id}\}$ *if d is odd, and* $\{\pm\mathrm{Id}\}$ *if d is even. In particular, the set $\mathcal{L}_d$ satisfies condition* (C1) *or* (C2) *of Corollary* 1.12*, according to the parity of d.*

6.2.1. *Two preliminary results.* The proof of the following lemma is based on the analytic properties of the homography on each of its intervals of definition.

LEMMA 6.3. *Let* $\mathfrak{h}$ *be a homography belonging to* $\mathrm{PGL}(2,\mathbb{R})$*,* $M > 0$ *be a real number,* $t \geq 1$ *be an integer,* $x_1, \dots, x_t$ *be* t *real numbers satisfying* $0 < x_1 < \cdots < x_t < M$*, and* $y_1, \dots, y_t$ *be* t *real numbers satisfying* $0 < y_1 < \cdots < y_t < M$*. Assume*

$$\begin{cases} \mathfrak{h}(\{x_i : 1 \leq i \leq t\}) = \{y_j : 1 \leq j \leq t\}, \\ \mathfrak{h}(0) = 0 \text{ and } \mathfrak{h}(M) = M. \end{cases}$$

Then, for every $1 \leq i \leq t$*, one has* $\mathfrak{h}(x_i) = y_i$*.*

Proof. We split the proof into several cases depending on the nature of the homography $\mathfrak{h}$.

If $\mathfrak{h}(\infty) = \infty$, the restriction of $\mathfrak{h}$ to the real affine line has the shape $\mathfrak{h}(x) = ax + b$, where $a \neq 0$ and b are real numbers. The conditions $\mathfrak{h}(0) = 0$ and $\mathfrak{h}(M) = M$ imply $a = 1$ and $b = 0$. Hence the result follows since $\mathfrak{h}$ is the identity.

If $\mathfrak{h}(\infty) \neq \infty$, then $\mathfrak{h}$ has a unique expansion as

$$\mathfrak{h}(x) = a + \frac{b}{x - c}, \tag{6.6}$$

where a, b and c are real numbers such that $c \notin \{0, x_1, \dots, x_t, M\}$ and $b \neq 0$. We now consider the respective values of b and c.

- If $b > 0$, the function $x \mapsto \mathfrak{h}(x)$ is decreasing on the two intervals $(-\infty, c)$ and $(c, +\infty)$. We consider the value of c.
  - If $c < x_t$ $(< M)$, we have $\mathfrak{h}(x_t) > \mathfrak{h}(M) = M$, since $\mathfrak{h}$ is decreasing. This contradicts the hypothesis $\mathfrak{h}(x_t) < M$.
  - If $c > x_t$ (> 0), we have $0 = \mathfrak{h}(0) > \mathfrak{h}(x_t)$. This contradicts the hypothesis $\mathfrak{h}(x_t) > 0$. We conclude that $\mathfrak{h}$ is not of the form (6.6) with $b > 0$.
- If $b < 0$, the function $x \mapsto \mathfrak{h}(x)$ is increasing on both $(-\infty, c)$ and $(c, +\infty)$. We now consider the value of c.
  - If $c \notin [0, M]$, the function $x \mapsto \mathfrak{h}(x)$ is increasing on $(0, M)$, so $\mathfrak{h}(x_i) = y_i$ for $1 \leq i \leq t$.
  - If $0 < c < M$, the hyperbola $\{(x, \mathfrak{h}(x)) \in \mathbb{R}^2 : x \in \mathbb{R}, x \neq c\}$ has two asymptotes: one with abscissa c and the other one with ordinate a. Elementary considerations lead to

    $$\mathfrak{h}(0) > a > \mathfrak{h}(M).$$

    This contradicts the hypothesis $\mathfrak{h}(0) = 0$ and $\mathfrak{h}(M) = M$. In conclusion, $\mathfrak{h}$ is not of the form (6.6) with $b < 0$ and $0 < c < M$. ∎

We will require the following variant of Lemma 6.3.

Lemma 6.4. *Let* $\mathfrak{h}$ *be a homography belonging to* $\mathrm{PGL}(2,\mathbb{R})$*,* $M>0$ *be a real number,* $t\geq 1$ *be an integer,* $x_1,\dots,x_t$ *be* t *real numbers satisfying* $0<x_1<\dots<x_t<M$*, and* $y_1,\dots,y_t$ *be* t *real numbers satisfying* $0<y_1<\dots<y_t<M$*. Assume*

$$\begin{cases}\mathfrak{h}(\{x_i : 1\leq i\leq t\})=\{y_j : 1\leq j\leq t\},\\ \mathfrak{h}(0)=M \text{ and } \mathfrak{h}(M)=0.\end{cases}$$

Then for every $1\leq i\leq t$*, one has* $\mathfrak{h}(x_i)=y_{t+1-i}$*.*

Proof. Introduce the homography $\mathfrak{g}=\mathfrak{s}\circ\mathfrak{h}$, where $\mathfrak{s}$ is the symmetry $\mathfrak{s}(x)=M-x$. Then $\mathfrak{g}$ meets the hypotheses of Lemma 6.3 provided that we replace the points y_i $(1\leq i\leq t)$ by the points $y_i':=M-y_{t+1-i}$. We deduce that for all i one has $\mathfrak{g}(x_i)=y_i'$, which gives $\mathfrak{h}(x_i)=y_{t+1-i}$. ∎

6.2.2. *Proof of Proposition 6.2.* Consider the polynomial

$$f(X)=L_{d,p}(X,1)$$

and its set of zeroes $\mathcal{Z}(f)=\{0,1,\dots,d-2,p\}$. In order to prove that the group of automorphisms of $L_{d,p}$ is trivial, it suffices to prove that the unique homography $\mathfrak{h}\in\mathrm{PGL}(2,\mathbb{Q})$ such that

$$\mathfrak{h}(\mathcal{Z}(f))=\mathcal{Z}(f), \tag{6.7}$$

is the identity as long as $p\geq d$.

As in the proof of Proposition 6.1, we will play with the p-adic valuation of the elements in $\mathrm{Bir}(f)$, defined in (6.5). We first notice that for x and y two distinct integers in $\{1,\dots,d-2\}$, the elements

$$\alpha:=[0,x,p,y],\ [p,x,0,y],\ [x,0,y,p],\ [x,p,y,0]$$

belong to $\mathrm{Bir}(f)$ and satisfy $v_p(\alpha)=1$. These are the only such elements in $\mathrm{Bir}(f)$. In particular, if four distinct elements x,y,z,t in $\mathcal{Z}(f)$ satisfy $v_p([x,y,z,t])=1$, then $\{0,p\}\subset\{x,y,z,t\}$.

By (6.4), we have

$$v_p([\mathfrak{h}(x),\mathfrak{h}(0),\mathfrak{h}(y),\mathfrak{h}(p)])=1,$$

where x and y are integers as above. Since $d\geq 5$, there exists an integer x in $\{1,\dots,d-2\}$ such that $\mathfrak{h}(x)\notin\{0,p\}$. We claim that there is another integer $y\neq x$ in $\{1,\dots,d-2\}$ with the same property, namely such that $\mathfrak{h}(y)\notin\{0,p\}$. This is plain for $d\geq 6$; for $d=5$, the only case where this would not be true is when $\{1,2,3\}=\{x,y,z\}$ with $\{\mathfrak{h}(y),\mathfrak{h}(z)\}=\{0,p\}$, but this case is not possible since it would not be compatible with our requirement that

$$\{0,p\}\subset\{\mathfrak{h}(x),\mathfrak{h}(0),\mathfrak{h}(y),\mathfrak{h}(p)\}.$$

This proves our claim that there are two distinct integers x and y in the set $\{1,\ldots,d-2\}$ such that $\{\mathfrak{h}(x),\mathfrak{h}(y)\}\cap\{0,p\}=\emptyset$. Therefore

$$\{\mathfrak{h}(0),\mathfrak{h}(p)\}=\{0,p\}.$$

We consider two cases.

Assume first

$$\mathfrak{h}(0)=0 \quad \text{and} \quad \mathfrak{h}(p)=p.$$

Since $\mathfrak{h}$ induces by restriction a bijective map of $\mathcal{Z}(f)$ onto itself, we may apply Lemma 6.3. We deduce that $\mathfrak{h}(t)=t$ for $0\le t\le d-2$ and $\mathfrak{h}(p)=p$. Since a homography is determined by its restriction to a set with three elements, we deduce that $\mathfrak{h}=\mathrm{Id}$.

If in turn

$$\mathfrak{h}(0)=p \quad \text{and} \quad \mathfrak{h}(p)=0, \tag{6.8}$$

we apply Lemma 6.4 to deduce that $\mathfrak{h}(i)=d-1-i$ for $1\le i\le d-2$. The unique homography $\mathfrak{h}$ satisfying this property is the symmetry defined by $\mathfrak{h}: z\mapsto d-1-z$. But such a formula is not compatible with the fact that $\mathfrak{h}(0)=p$. So there is no homography $\mathfrak{h}$ satisfying (6.7) and (6.8).

We conclude that the set of $\mathfrak{h}$ satisfying (6.7) is reduced to the identity. The proof of Proposition 6.2 is complete. ∎

6.3. The family $\mathcal{L}$ is regular (continued). We now investigate condition (v) of Definition 1.10. We will prove

PROPOSITION 6.5. *For every $d\ge 5$, every p with $p\ge d-1$, and all $(x,y)\in\mathbb{Z}^2$ such that $L_{d,p}(x,y)\ne 0$. the following inequality holds:*

$$\max\{|x|,|y|\}\le 9|L_{d,p}(x,y)|^{\frac{1}{d-1}}. \tag{6.9}$$

Inequality (6.9) is equivalent to the lower bound

$$|L_{d,p}(x,y)|\ge \left(\tfrac{1}{9}\max\{|x|,|y|\}\right)^{d-1}, \tag{6.10}$$

under the hypotheses of Proposition 6.5. We will rather work with (6.10).

The proof of (6.10) depends on the relative sizes of $|x|$ and $|y|$. However, if we suppose that $xy\le 0$ and $L_{d,p}(x,y)\ne 0$, it is straightforward that

$$|L_{d,p}(x,y)|\ge (\max\{|x|,|y|\})^{d-1}.$$

Hence we may assume that x and y are not zero and have the same sign. Further, since $|L_{d,p}(-x,-y)|=|L_{d,p}(x,y)|$, we will assume that both x and y are positive.

The basic equality is the following:

$$|L_{d,p}(x,y)|=x\cdot|x-y|\cdot|x-2y|\cdots|x-(d-2)y|\cdot|x-py|. \tag{6.11}$$

We split the argument according to the relative sizes of x and y.

6.3.1. *Assume* $1 \le x \le y$. Let x and y be positive integers such that $L_{d,p}(x,y) \neq 0$ with $y \ge x$. Hence $y \ge x+1$. From (6.11) we deduce

$$\begin{aligned}|L_{d,p}(x,y)| &= x\cdot(y-x)\cdot(2y-x)\cdots((d-2)y-x)\cdot(py-x)\\ &> x\cdot(y-x)\cdot y\cdot(2y)\cdots((d-3)y)\cdot((p-1)y)\\ &= x\cdot(y-x)\cdot(d-3)\,!\cdot(p-1)\,y^{d-2}.\end{aligned}$$

If $y \ge 2x$, we have $x(y-x) \ge y-x \ge y/2$, while for $x < y \le 2x$ we have $x(y-x) \ge x \ge y/2$. Hence

$$|L_{d,p}(x,y)| > \tfrac{1}{2}(d-3)!(p-1)(\max\{|x|,|y|\})^{d-1}.$$

So we have proved

Proposition 6.6. *For every $d \ge 3$, every $p \ge d-1$, and all integers x and y such that $L_{d,p}(x,y) \neq 0$ and $|x| \le |y|$, one has*

$$|L_{d,p}(x,y)| \ge (\max\{|x|,|y|\})^{d-1}.$$

6.3.2. *Assume* $(d-2)y \le x$. Let x and y be positive integers such that $L_{d,p}(x,y) \neq 0$ with $x \ge (d-2)y$, hence $x \ge (d-2)y+1$. From (6.11) we deduce

$$|L_{d,p}(x,y)| = x\cdot(x-y)\cdot(x-2y)\cdots(x-(d-2)y)\cdot|x-py|.$$

If $y=1$, then since $x \ge d-1$, we have

$$x-n = x\left(1-\frac{n}{x}\right) \ge x\left(1-\frac{n}{d-1}\right) = x\left(\frac{d-n-1}{d-1}\right)$$

for $0 \le n \le d-2$; using the trivial lower bound $|x-p| \ge 1$ together with Stirling's formula (1.20), we deduce

$$|L_{d,p}(x,1)| \ge x\cdot(x-1)\cdot(x-2)\cdots(x-(d-2)) \ge \frac{(d-1)!}{(d-1)^{d-1}}\,x^{d-1} \ge \frac{x^{d-1}}{\mathrm{e}^{d-1}}.$$

We assume now $y \ge 2$. As a consequence of $y \le x/(d-2)$, we have

$$x\cdot(x-y)\cdot(x-2y)\cdots(x-(d-3)y) \ge \frac{(d-2)!}{(d-2)^{d-2}}\,x^{d-2}.$$

If $x > py$, then

$$x-(d-2)y \ge x\left(1-\frac{d-2}{p}\right) \ge x\left(1-\frac{d-2}{d-1}\right) = \frac{x}{d-1}$$

and the trivial lower bound $x-py \ge 1$ suffices to deduce

$$L_{d,p}(x,y) \ge \frac{(d-2)!}{(d-1)(d-2)^{d-2}}\,x^{d-1}.$$

If $py > x$, then from $x-(d-2)y \ge 1$ and $py-x \ge 1$ we deduce

$$(x-(d-2)y)\cdot(py-x) \ge (x-(d-2)y)+(py-x)-1 \ge y(p-d+2)-1.$$

If $p = d-1$, then we use the assumption $y \geq 2$, which yields

$$y(p-d+2)-1 = y-1 \geq \frac{y}{2} > \frac{x}{2p} = \frac{x}{2(d-1)},$$

while for $p \geq d$ we use the lower bounds

$$y(p-d+2)-1 \geq y(p-d+1) \geq py\left(1-\frac{d-1}{p}\right) > x\left(1-\frac{d-1}{d}\right) = \frac{x}{d}.$$

Therefore, for $(d-2)y \leq x$ and $y \geq 2$, we have

$$|L_{d,p}(x,y)| \geq \frac{(d-2)!}{2(d-1)(d-2)^{d-2}}\, x^{d-1} \geq \frac{x^{d-1}}{2d\mathrm{e}^{d-2}}.$$

We deduce

Proposition 6.7. *For $d \geq 3$, p prime $\geq d-1$ and $(x,y) \in \mathbb{Z}^2$ such that $|x| \geq (d-2)|y|$ and $L_{d,p}(x,y) \neq 0$, we have*

$$|L_{d,p}(x,y)| \geq \frac{1}{d\mathrm{e}^d}(\max\{|x|,|y|\})^{d-1}.$$

6.3.3. *Assume $(n-1)y \leq x \leq ny$ for some n with $2 \leq n \leq d-2$.* From (6.11) we deduce

$$|L_{d,p}(x,y)| = x\cdot(x-y)\cdots(x-(n-1)y)\cdot(ny-x)\cdots((d-2)y-x)\cdot(py-x).$$

We have

$$x\cdot(x-y)\cdots(x-(n-2)y) \geq (n-1)!y^{n-1}$$

and

$$\begin{aligned}((n+1)y-x)\cdots((d-2)y-x)\cdot(py-x) &\geq (d-n-2)!(p-n)y^{d-n-1}\\ &\geq (d-n-1)!y^{d-n-1}.\end{aligned}$$

For the product of the two terms in the middle, if $y = 1$, then we use the trivial lower bound $(x-(n-1)y)(ny-x) \geq 1$, which yields

$$|L_{d,p}(x,y)| \geq (n-1)!(d-n-1)!y^{d-2} \geq \frac{(n-1)!(d-n-1)!}{n^{d-2}}x^{d-2},$$

while for $y \geq 2$ we use

$$(x-(n-1)y)(ny-x) \geq (x-(n-1)y)+(ny-x)-1 = y-1 \geq y/2,$$

which yields

$$|L_{d,p}(x,y)| \geq \frac{1}{2}(n-1)!(d-n-1)!y^{d-1} \geq \frac{(n-1)!(d-n-1)!}{2n^{d-1}}x^{d-1}.$$

We now use Lemma 5.2:

$$\frac{(n-1)!(d-n-1)!}{n^{d-1}} = \frac{n!(d-n)!}{n^d(d-n)} \geq \mathrm{e}^{-(1+\mathrm{e}^{-1})d}\frac{1}{d-n},$$

from which we deduce

$$|L_{d,p}(x,y)| \geq \mathrm{e}^{-(1+\mathrm{e}^{-1})d}\frac{1}{2(d-n)}x^{d-1}.$$

This proves the following result:

PROPOSITION 6.8. *For $d \geq 3$, $2 \leq n \leq d-2$, p prime $\geq d-1$ and x and y such that $(n-1)|y| \leq |x| \leq n|y|$ and $L_{d,p}(x,y) \neq 0$, we have*

$$|L_{d,p}(x,y)| \geq \frac{1}{2(d-2)} \cdot \frac{\max\{|x|,|y|\}^{d-1}}{\mathrm{e}^{(1+\mathrm{e}^{-1})d}}.$$

For $d \geq 5$, we have

$$2(d-2)\cdot \mathrm{e}^{(1+\mathrm{e}^{-1})d} < 9^{d-1}.$$

We may now gather Propositions 6.6–6.8 to deduce (6.10), which completes the proof of Proposition 6.5.

6.4. Estimating the number of images by $\mathcal{L}$ of (x,y) with $\max\{|x|,|y|\} \geq 10$. Gathering Propositions 6.1 and 6.5, we find that the family $\mathcal{L}$ is $(10,1,1,5,9)$-regular. Furthermore, according to the parity of d, the set $\mathcal{L}_d$ satisfies condition (C1) or (C2) of Corollary 1.12, by Proposition 6.2. As a consequence of Corollary 1.12 we have the following

PROPOSITION 6.9. *For any $d \geq 5$, for every $\varepsilon > 0$, one has*

$$\mathcal{R}_{\geq d}(\mathcal{L}, B, 10) = \frac{1}{(2,d)}\Big(\sum_{d \leq p < 2d} A_{L_{d,p}}\Big) B^{2/d} + O_{d,\varepsilon}(B^{\vartheta_d+\varepsilon}) + O_d(B^{2/(d+1)}).$$

6.5. Estimating the number of images by $\mathcal{L}$ of (x,y) with $\max\{|x|,|y|\} < 10$. The difference

$$\mathcal{R}_{\geq d}(\mathcal{L}, B, 0) - \mathcal{R}_{\geq d}(\mathcal{L}, B, 10) \tag{6.12}$$

is bounded from above by twice the cardinality of the set

$$\mathfrak{Er}_{\geq d}(B) := \{m : 0 < m = |L_{d',p}(x,y)| \leq B,\ d \leq d' \leq p < 2d',\ \max\{|x|,|y|\} \leq 9\}.$$

There are 19^2 pairs (x,y) with $\max\{|x|,|y|\} \leq 9$. We first count the number of m in $\mathfrak{Er}_{\geq d}(B)$ of the form $|L_{d',p}(x,0)|$, that is, with $y=0$. For $x = \pm 1$ and $y=0$ we have $m=1$; for $2 \leq |x| \leq 9$ and $y=0$, we have $2^{d'} \leq B$, hence there are at most $O_d(\log B)$ such values of m.

We now count the number of m in $\mathfrak{Er}_{\geq d}(B)$ of the form $|L_{d',p}(x,y)|$ with $|y| \geq 1$. We have $|x-ny| \geq n - |x| \geq n-9 \geq 2$ for $n \geq 11$, hence

$$B \geq m \geq \prod_{11 \leq n \leq d'-2} (n-9) \geq 2^{d'-12},$$

and therefore $d' \leq O(\log B)$. It follows that the number of pairs (d',p) as above is bounded by $O_d(\log^2 B)$. So we have proved

$$\sharp\mathfrak{Er}_{\geq d}(B) = O_d(\log^2 B).$$

Combining this bound with (6.12) and with Proposition 6.9, we obtain equality (1.19) of Theorem 1.18.

6.6. Some results on A_F for $F \in \mathcal{L}$. The area of the fundamental domain associated to $L_{d,p}$ is, by the definition (1.9), equal to

$$A_{L_{d,p}} = \iint\limits_{\mathcal{D}(L_{d,p})} \mathrm{d}x\,\mathrm{d}y$$

with

$$\mathcal{D}(L_{d,p}) := \{(x,y) \in \mathbb{R}^2 : |x(x-y)(x-2y)\cdots(x-(d-2)y)(x-py)| \le 1\}.$$

By the change of variables $u = x$ and $v = y/x$, we obtain

$$A_{L_{d,p}} = \iint\limits_{\mathcal{D}^*(L_{d,p})} |u|\,\mathrm{d}u\,\mathrm{d}v$$

with

$$\mathcal{D}^*(L_{d,p}) := \{(u,v) \in \mathbb{R}^2 : |u|^d \cdot |(1-v)(1-2v)\cdots(1-(d-2)v)(1-pv)| \le 1\}.$$

Some elementary calculations transform $A_{L_{d,p}}$ into a single integral.

Lemma 6.10. *For $d \ge 5$ and $p \ge d-1$, the following equalities hold:*

$$A_{L_{d,p}} = \int_{-\infty}^{\infty} \frac{\mathrm{d}v}{(|1-v|\cdot|1-2v|\cdots|1-(d-2)v|\cdot|1-pv|)^{2/d}}$$

and

$$A_{L_{d,p}} = \int_{-\infty}^{\infty} \frac{\mathrm{d}t}{|t|\cdot|t-1|\cdot|t-2|\cdots|t-(d-2)|\cdot|t-p|)^{2/d}}.$$

We will only work with the second expression of $A_{L_{d,p}}$. So we introduce the function

$$\lambda_{d,p}(t) := t(t-1)\cdots(t-(d-2))(t-p),$$

which is the product of d linear factors in t. We split the interval of integration into d intervals of length 1 around the singularities $0,\dots,d-2$ and p and three remaining intervals to write

$$A_{L_{d,p}} = \Big(\int_{-\infty}^{-1/2} + \int_{-1/2}^{1/2} + \cdots + \int_{d-5/2}^{d-3/2} + \int_{d-3/2}^{p-1/2} + \int_{p-1/2}^{p+1/2} + \int_{p+1/2}^{\infty}\Big)\frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}}. \tag{6.13}$$

We will give an upper bound and a lower bound for each of these positive integrals in order to prove

Proposition 6.11. *Uniformly for $d\to\infty$ and $d\le p<2d$, one has*
$$\frac{\mathrm{e}^2-o(1)}{d}\le A_{L_{d,p}}\le\frac{5\mathrm{e}^2+2\mathrm{e}+o(1)}{d}\cdot$$

The last part of Theorem 1.18 is obtained from this proposition after a summation over $d\le p<2d$ and an application of the Prime Number Theorem.

6.6.1. *An auxiliary lemma.*

Lemma 6.12. *For $d\to\infty$, we have*
$$(1\cdot3\cdot5\cdots(2d-3))^{1/d}=(2\mathrm{e}^{-1}+o(1))d.$$

Proof. We write
$$1\cdot3\cdot5\cdots(2d-3)=\frac{(2d-3)!}{2^{d-2}(d-2)!}=\frac{(2d)!}{(2d-1)2^d d!}$$
and we use Stirling's formula (1.20), which gives
$$\left(\frac{2d}{\mathrm{e}}\right)^d\frac{\sqrt{2}}{(2d-1)\cdot\mathrm{e}^{1/12d}}\le1\cdot3\cdot5\cdots(2d-3)\le\left(\frac{2d}{\mathrm{e}}\right)^d\frac{\sqrt{2}\cdot\mathrm{e}^{1/24d}}{2d-1}\cdot\ \blacksquare$$

6.6.2. *Study of $\int_{-\infty}^{-1/2}$ and of $\int_{p+1/2}^{\infty}$*

Lemma 6.13. *For $d\to\infty$ and $p\ge d$, one has*
$$0\le\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}}\le\frac{\mathrm{e}+o(1)}{d}\cdot$$

Proof. Using Hölder's inequality and Lemma 6.12, we obtain
$$\begin{aligned}\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}}&\le\left(\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|t|^2}\right)^{1/d}\left(\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|t-1|^2}\right)^{1/d}\\&\qquad\times\cdots\times\left(\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|t-(d-2)|^2}\right)^{1/d}\left(\int_{-\infty}^{-1/2}\frac{\mathrm{d}t}{|t-p|^2}\right)^{1/d}\\&\le\left(\frac{2}{1}\cdot\frac{2}{3}\cdot\frac{2}{5}\cdots\frac{2}{2d-3}\cdot\frac{2}{2p+1}\right)^{1/d}\\&\le\left(\frac{2^d}{1\cdot3\cdot5\cdots(2d-3)\cdot(2p+1)}\right)^{1/d}\le\frac{\mathrm{e}+o(1)}{d}\cdot\ \blacksquare\end{aligned}$$

Similarly, one proves

Lemma 6.14. *For $d\to\infty$ and $p\ge d$, one has*
$$0\le\int_{p+1/2}^{\infty}\frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}}\le\frac{\mathrm{e}+o(1)}{d}\cdot$$

Proof. For $t > p+1/2$, we have

$$|\lambda_{d,p}(t)| = \lambda_{d,p}(t) = t(t-1)\cdots(t-(d-2))(t-p).$$

Using Hölder's inequality and Lemma 6.12, we obtain

$$\begin{aligned}\int_{p+1/2}^{\infty} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}} &\le \Big(\int_{p+1/2}^{\infty} \frac{\mathrm{d}t}{t^2}\Big)^{1/d}\Big(\int_{p+1/2}^{\infty} \frac{\mathrm{d}t}{(t-1)^2}\Big)^{1/d} \\ &\quad \times\cdots\times \Big(\int_{p+1/2}^{\infty} \frac{\mathrm{d}t}{(t-(d-2))^2}\Big)^{1/d}\Big(\int_{p+1/2}^{\infty} \frac{\mathrm{d}t}{(t-p)^2}\Big)^{1/d} \\ &\le \Big(\frac{2}{2p+1}\cdot\frac{2}{2p-1}\cdot\frac{2}{2p-3}\cdots\frac{2}{2p-2d+5}\cdot\frac{2}{1}\Big)^{1/d} \\ &\le \Big(\frac{2^d}{1\cdot 3\cdot 5\cdots(2d-3)}\Big)^{1/d} \le \frac{\mathrm{e}+o(1)}{d}\cdot \ \blacksquare\end{aligned}$$

6.6.3. *Study of* $\int_{d-3/2}^{p-1/2}$

LEMMA 6.15. *For $d\to\infty$ and $d\le p<2d$, one has*

$$0 \le \int_{d-3/2}^{p-1/2} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}} \le \frac{\mathrm{e}^2+o(1)}{d}.$$

Proof. For t in the interval $(d-3/2, p-1/2)$, we have $p-t>1/2$,

$$|\lambda_{d,p}(t)| = t(t-1)\cdots(t-(d-2))(p-t)$$

and, for $0\le n\le d-2$,

$$t-n > \frac{2d-2n-3}{2},$$

hence

$$|\lambda_{d,p}(t)| \ge \frac{(2d-3)\cdot(2d-5)\cdots 3\cdot 1}{2^d}$$

and therefore

$$|\lambda_{d,p}(t)|^{2/d} \ge (\mathrm{e}^{-2}+o(1))d^2$$

by Lemma 6.12. Since $d\le p<2d$, the interval of integration has length at most $d+1$, and so we deduce

$$\int_{d-3/2}^{p-1/2} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}} \le \frac{\mathrm{e}^2+o(1)}{d}\cdot \ \blacksquare$$

6.6.4. *Study of* $\int_{p-1/2}^{p+1/2}$

LEMMA 6.16. *For $d \geq 5$ and $d \leq p < 2d$, one has*

$$0 \leq \int_{p-1/2}^{p+1/2} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}} = O\Big(\frac{1}{d^2}\Big).$$

We introduce the polynomial

$$\mathcal{M}(t) := t(t-1)\cdots(t-(d-2))$$

of degree $d-1$. It is easy to see that

$$\min_{|t-p|\leq 1/2} |\mathcal{M}(t)| = |\mathcal{M}(p-1/2)| \geq \mathcal{M}(d-3/2)$$
$$= \frac{1}{2}\cdot\frac{3}{2}\cdot\frac{5}{2}\cdots\frac{2d-5}{2}\cdot\frac{2d-3}{2},$$

hence by Lemma 6.12, we have

$$\min_{|t-p|\leq 1/2} |\mathcal{M}(t)|^{2/d} \geq (\mathrm{e}^{-2}+o(1))d^2.$$

Since

$$\int_{p-1/2}^{p+1/2} \frac{\mathrm{d}t}{|t-p|^{2/d}} = O(1),$$

we conclude

$$\int_{p-1/2}^{p+1/2} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}}$$
$$\leq \Big(\int_{p-1/2}^{p+1/2} \frac{\mathrm{d}t}{|t-p|^{2/d}}\Big)\cdot\Big(\frac{1}{\min_{|t-p|\leq 1/2}|\mathcal{M}(t)|}\Big)^{2/d} = O\Big(\frac{1}{d^2}\Big).$$

6.6.5. *Study of the remaining integrals.* We are now concerned, for $\nu = 0, 1, \ldots, d-2$, with the integrals

$$\mathcal{I}_\nu = \mathcal{I}_{d,p,\nu} = \int_{\nu-1/2}^{\nu+1/2} \frac{\mathrm{d}t}{|\lambda_{d,p}(t)|^{2/d}},$$

for which we want to find an upper and a lower bound. We split the product defining $\lambda_{d,p}(t)$ into four pieces:

$$\lambda_{d,p}(t) = (t-\nu)\cdot(t-p)\cdot\lambda_\nu^-(t)\cdot\lambda_{d,\nu}^+(t) \tag{6.14}$$

with

$$\lambda_\nu^-(t) := \prod_{0\leq k<\nu}(t-k) \quad\text{and}\quad \lambda_{d,\nu}^+(t) := \prod_{\nu<k\leq d-2}(t-k).$$

We have

$$(6.15)\qquad \mathcal{I}_\nu \le \Big(\int_{\nu-1/2}^{\nu+1/2} \frac{\mathrm{d}t}{|t-\nu|^{2/d}} \Big) \cdot (\min|\lambda_\nu^-(t)|)^{-2/d} \cdot (\min|\lambda_{d,\nu}^+(t)|)^{-2/d} \cdot (\min|t-p|)^{-2/d}$$

and

$$(6.16)\qquad \mathcal{I}_\nu \ge \Big(\int_{\nu-1/2}^{\nu+1/2} \frac{\mathrm{d}t}{|t-\nu|^{2/d}} \Big) \cdot (\max|\lambda_\nu^-(t)|)^{-2/d} \cdot (\max|\lambda_{d,\nu}^+(t)|)^{-2/d} \cdot (\max|t-p|)^{-2/d},$$

where all the maxima and minima are taken for $\nu - 1/2 \le t \le \nu + 1/2$. Direct computations transform (6.15) and (6.16) into

$$(1-o(1))(\max|\lambda_\nu^-(t)|)^{-2/d} \cdot (\max|\lambda_{d,\nu}^+(t)|)^{-2/d} \le \mathcal{I}_\nu \le (1+o(1))(\min|\lambda_\nu^-(t)|)^{-2/d} \cdot (\min|\lambda_{d,\nu}^+(t)|)^{-2/d},$$

which is also

$$(6.17)\qquad (1-o(1))|\lambda_\nu^-(\nu+1/2)|^{-2/d} \cdot |\lambda_{d,\nu}^+(\nu-1/2)|^{-2/d} \le \mathcal{I}_\nu \le (1+o(1))|\lambda_\nu^-(\nu-1/2)|^{-2/d} \cdot |\lambda_{d,\nu}^+(\nu+1/2)|^{-2/d}$$

uniformly for $d \to \infty$ and $d \le p < 2d$.

For $1 \le \nu \le d-2$, we have the equalities

$$\lambda_\nu^-(\nu+1/2) = \frac{(2\nu+1)(2\nu-1)\cdots 3}{2^\nu} = \frac{(2\nu+1)\,!}{2^{2\nu}\cdot \nu\,!} = \frac{(2\nu)\,!}{2^{2\nu}\cdot \nu\,!}\cdot\frac{1}{2\nu+1},$$
$$\lambda_\nu^-(\nu-1/2) = \frac{(2\nu-1)(2\nu-3)\cdots 1}{2^\nu} = \frac{(2\nu-1)\,!}{2^{2\nu-1}\cdot(\nu-1)\,!} = \frac{(2\nu)\,!}{2^{2\nu}\cdot \nu\,!},$$

and for $0 \le \nu \le d-3$, we have

$$|\lambda_{d,\nu}^+(\nu+1/2)| = \frac{(2d^*-1)(2d^*-3)\cdots 3\cdot 1}{2^{d^*}} = \frac{(2d^*-1)!}{2^{2d^*-1}\cdot(d^*-1)!} = \frac{(2d^*)!}{2^{2d^*}\cdot d^*!},$$
$$|\lambda_{d,\nu}^+(\nu-1/2)| = \frac{(2d^*+1)(2d^*-1)\cdots 5\cdot 3}{2^{d^*}} = \frac{(2d^*+1)!}{2^{2d^*}\cdot d^*!} = \frac{(2d^*)!}{2^{2d^*}\cdot d^*!}\cdot(2d^*+1),$$

with the notation $d^* = d-2-\nu$. Furthermore, since we have empty products in the decomposition (6.14), we see that

$$(6.18)\qquad \lambda_0^-(1/2) = \lambda_0^-(-1/2) = \lambda_{d,d-2}^+(d-3/2) = \lambda_{d,d-2}^+(d-5/2) = 1.$$

The following lemma shows that inequalities (6.17) are sharp.

Lemma 6.17. *Uniformly for $0 \le \nu \le d-2$ and $d \to \infty$, one has*

$$1 - o(1) \le \left(\frac{|\lambda_\nu^-(\nu - 1/2)| \cdot |\lambda_{d,\nu}^+(\nu + 1/2)|}{|\lambda_\nu^-(\nu + 1/2)| \cdot |\lambda_{d,\nu}^+(\nu - 1/2)|} \right)^{-2/d} \le 1 + o(1)$$

Proof. Obvious consequence of the explicit formulas given above. ∎

For $0 \le \nu \le d-2$, let

$$\Lambda = \Lambda(d,\nu) := |\lambda_\nu^-(\nu - 1/2)|^{-2/d} \cdot |\lambda_{d,\nu}^+(\nu + 1/2)|^{-2/d}.$$

A consequence of the explicit formulas for λ_ν^- and $\lambda_{d,\nu}^+$ is the equality

$$\log \Lambda = -\frac{2}{d}\{\log((2\nu)!) + \log((2d^*)!) - \log(\nu!) - \log(d^*!) - 2d\log 2 + o(d)\}$$

uniformly for $1 \le \nu \le d-3$ and $d \to \infty$. Using Stirling's formula (1.20), we deduce

$$\begin{aligned} -\frac{d}{2} \cdot \log \Lambda &= \nu \log \nu + d^* \log d^* - d + o(d) \\ &= \nu \log \nu + (d-\nu)\log(d-\nu) - d + o(d), \end{aligned}$$

hence

$$\log \Lambda = -\frac{2}{d}(\nu \log \nu + (d-\nu)\log(d-\nu)) + 2 + o(1) \tag{6.19}$$

uniformly for $1 \le \nu \le d-3$ and $d \to \infty$. By a direct study of the function f_d defined by

$$f_d : [1, d-1] \ni t \mapsto f_d(t) = t\log t + (d-t)\log(d-t),$$

we deduce that, for all $1 \le t \le d-1$, the function f_d satisfies

$$f_d(d/2) = d\log(d/2) \le f_d(t) \le f_d(1) = f_d(d-1) = (d-1)\log(d-1).$$

Inserting this bound into (6.19), we obtain

$$-2\log d + 2 - o(1) \le \log \Lambda(d,\nu) \le -2\log d + 2\log 2 + 2 + o(1) \tag{6.20}$$

uniformly for $1 \le \nu \le d-3$. Actually, this formula also holds for $\Lambda(d,0)$ and $\Lambda(d,d-2)$ thanks to (6.18).

Combining (6.17), (6.20) and Lemma 6.17, we obtain

Lemma 6.18. *Uniformly for $d \to \infty$, $0 \le \nu \le d-2$ and $d \le p < 2d$, one has*

$$\frac{\mathrm{e}^2 - o(1)}{d^2} \le \mathcal{I}_{d,p,\nu} \le \frac{4\mathrm{e}^2 + o(1)}{d^2}.$$

6.6.6. *End of the proof of Proposition 6.11.* We split the end of the proof into two parts.

For the lower bound, we use positivity to write

$$A_{L_{d,p}} \geq \sum_{\nu=0}^{d-2} \mathcal{I}_\nu \geq (d-1) \cdot \frac{\mathrm{e}^2 - o(1)}{d^2} \geq \frac{\mathrm{e}^2 - o(1)}{d},$$

as a consequence of (6.13) and Lemma 6.18.

For the upper bound, we respectively apply Lemmas 6.13–6.16 and 6.18 to bound each of the terms in (6.13), and we obtain

$$A_{L_{d,p}} \leq \frac{5\mathrm{e}^2 + 2\mathrm{e} + o(1)}{d}.$$

The proof of Proposition 6.11 is now complete. This concludes the proof of Theorem 1.18.

Acknowledgements. We are thankful to the referee for his valuable comments.

References

[B] M. A. Bean, *An isoperimetric inequality for the area of plane regions defined by binary forms*, Compos. Math. 92 (1994), 115–131.

[F] N. I. Fel'dman, *An effective refinement of the exponent in Liouville's theorem*, Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971), 973–990 (in Russian).

[FK] É. Fouvry and P. Koymans, *Binary forms with the same value set*, in preparation.

[FLW] É. Fouvry, C. Levesque and M. Waldschmidt, *Representation of integers by cyclotomic binary forms*, Acta Arith. 184 (2018), 67–86.

[FW] É. Fouvry et M. Waldschmidt, *Sur la représentation des entiers par les formes cyclotomiques de grand degré*, Bull. Soc. Math. France 148 (2020), 253–282; arXiv: 1909.01892.

[GP] K. Győry and Z. Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, in: Studies in Pure Mathematics. To the memory of Paul Turán, Akadémiai Kiadó, Budapest, and Birkhäuser, Basel, 1983, 245–257.

[HW] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford Univ. Press, Oxford, 2008.

[Ho] C. Hooley, *On binary cubic forms*, J. Reine Angew. Math. 226 (1967), 30–87.

[SX] C. L. Stewart and S. Y. Xiao, *On the representation of integers by binary forms*, Math. Ann. 375 (2019), 133–163.

Étienne Fouvry
Université Paris-Saclay, CNRS
Laboratoire de Mathématiques d'Orsay
91405 Orsay, France
E-mail: Etienne.Fouvry@universite-paris-saclay.fr

Michel Waldschmidt
Sorbonne Université
and Université de Paris
CNRS, IMJ-PRG
75005 Paris, France
E-mail: michel.waldschmidt@imj-prg.fr

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

We extend our previous results on the number of integers which are values of some cyclotomic form of degree larger than a given value, to more general families of binary forms with integer coefficients. Our main ingredient is an asymptotic upper bound for the cardinality of the set of values which are common to two non-isomorphic binary forms of degree greater than 3. We apply our results to some typical examples of families of binary forms.