Friable values of binary forms
Antal Balog, Valentin Blomer, Cécile Dartyge, Gérald Tenenbaum

To cite this version:
FRIABLE VALUES OF BINARY FORMS

ANTAL BALOG, VALENTIN BLOMER, CÉCILE DARTYGE, AND GÉRALD TENENBAUM

ABSTRACT. Let $F \in \mathbb{Z}[X,Y]$ be an integral binary form of degree $g \geq 2$, and let
$$\Psi_F(x,y) := \text{card}\{1 \leq a, b \leq x : P^+(F(a,b)) \leq y\}$$
where as usual $P^+(n)$ denotes the largest prime factor of $n$. It is proved that $\Psi_F(x,y) \asymp x^2$ for $y = x^{g-2+\varepsilon}$ in general, and $y = x^{1/2+\varepsilon}$ if $g = 3$. Better results are obtained if $F$ is reducible.

To the memory of our friend and colleague George Greaves

1. Introduction

For an integer $n$ let as usual $P^+(n)$ and $P^-(n)$ denote respectively the largest and smallest prime factor of $|n|$ with the conventions $P^+(\pm 1) = 1$, $P^-(1) = \infty$, $P^+(0) = 0$. Given a real number $y > 1$, an integer $n$ is called $y$-friable (or sometimes $y$-smooth) if $P^+(n) \leq y$. Friable numbers have proved to be very useful in many branches of number theory, both theoretically (e.g. in connection with Waring’s problem) and practically (e.g. for factoring algorithms). See [Gr] for a recent overview.

When the friability parameter $y$ exceeds a power of $x$, friable numbers occur with positive density among integers less than or equal to $x$. Indeed, for any fixed $\varepsilon > 0$, we have, as $x$ tends to infinity,
$$\Psi(x,x^\varepsilon) := \text{card}\{1 \leq a \leq x : P^+(a) \leq x^\varepsilon\} \sim g(1/\varepsilon)x$$
where $g$ is the Dickman function. It is, however, very often a hard problem to establish that a given sequence contains a positive proportion of friable numbers, even if we content ourselves with a relatively modest friability parameter $y$.

In this article, we consider integral binary forms $F \in \mathbb{Z}[X,Y]$, and define
$$\Psi_F(x,y) := \text{card}\{1 \leq a, b \leq x : P^+(F(a,b)) \leq y\}.$$ Without loss of generality we can assume that $F$ is “squarefree”, that is, its irreducible factors are distinct. We are interested in determining values of $y$ as small as possible such that we can still guarantee a bound of the type
$$\Psi_F(x,y) \leq x^2. \tag{1.1}$$

If $F$ is a linear form, one can trivially choose $y = x^\varepsilon$, and this is best possible. If $F = X^2 + Y^2$, Moree [Mo] (see also [BW, TW1, HTW]) showed that (1.1) holds again with $y = x^\varepsilon$. Actually the main result of [TW1] evaluates friable sums of fairly general multiplicative functions and furnishes corresponding asymptotic formulae in a much larger $(x,y)$-domain, certainly including $\exp((\log x)^\varepsilon) \leq y \leq x$. It is not hard to see that this result generalizes to arbitrary irreducible binary quadratic forms, noting that the representation function is a linear combination of multiplicative functions attached to certain ring class characters of the underlying quadratic number field. For higher degree, little has been known so far. We shall prove the following general theorem.

Theorem 1. Let $F = F(X,Y)$ be a binary form with integer coefficients, degree $t \geq 2$ and no repeated irreducible factor. Let $g$ be the largest degree of an irreducible factor of $F$ and let $k$ (resp.
\( \ell \) denote the number of distinct irreducible factors of \( F \) having degree \( g \) (resp. \( g - 1 \)). Given any positive real number \( \varepsilon \), the estimate

\[
\Psi_F(x, y) \asymp_{F, \varepsilon} x^2
\]

holds for all large \( x \) provided \( y \geq x^{\alpha_F + \varepsilon} \), where the exponent \( \alpha_F \) is defined by

\[
\alpha_F := \begin{cases} 
\frac{g - 2/k}{1 - 1/(\ell + 1)} & \text{if } k \geq 2, \\
\frac{g - 1}{\ell + 1} & \text{if } k = 1 \text{ and } (g, t) \neq (2, 3), \\
\frac{2}{3} & \text{if } (g, k, t) = (2, 1, 3).
\end{cases}
\]

As is well-known, irreducibility over \( \mathbb{Q} \) is the same as irreducibility over \( \mathbb{Z} \). Thus, distinct factors of \( F \) are understood as distinct up to a scalar. Irreducible binary forms correspond to the case \((k, \ell) = (1, 0)\). The theorem provides for these polynomials the exponent \( \alpha_F = g - 2 \). In the opposite direction, the theorem provides nontrivial results for simultaneous friable values of an arbitrary number of, say, binary linear forms. It also reproves the exponent \( \alpha_F = 0 \) for a reducible or irreducible quadratic form \( F \).

We obtain a better range for \( y \) when \( F \) is a cubic form. This is due to the fact that, when \( \deg(F) = t \leq 3 \), the level of distribution of the sequence \( \{F(a, b)\} \) for \( 1 \leq a, b \leq x \), given by Proposition 2 below, exceeds \( x^{1/2} \).

**Theorem 2.** Let \( F \in \mathbb{Z}[X, Y] \) be an integral binary cubic form. Let

\[
\alpha_F := \begin{cases} 
1/\sqrt{3}, & \text{if } F \text{ is irreducible; } \\
0, & \text{if } F \text{ is reducible.}
\end{cases}
\]

Then

\[
\Psi_F(x, y) \asymp_{F, \varepsilon} x^{2 + \varepsilon}
\]

provided \( y \geq x^{\alpha_F + \varepsilon} \).

We have \( 1/\sqrt{3} = 0.606\ldots \), so \( x^{1/\sqrt{3}} = (x^3)^{0.202}\ldots \). As a comparison, Theorem 1 yields \( \alpha_F = 1 \) if the cubic form \( F \) is irreducible and \( \alpha_F = 2/3 \) or \( 1/3 \) if \( F \) is reducible (depending on whether \( F \) decomposes into a quadratic and a linear form, or into three linear forms).

It is certainly also an interesting question how small \( y \) can be chosen if we drop the requirement to get a positive proportion of \( y \)-friable values. Here we only make the simple observation that \( \Psi_F(x, x^c) \gg x \) holds for any \( \varepsilon \) and any \( F \): just consider the values \( F(a, ca) \) for \( x^c \)-friable integers \( a \) and a suitable constant \( c \in \mathbb{Z} \) such that \( F(a, ca) \) is not constantly zero.

That friable values of binary forms play a central role in the number field sieve may provide further motivation for our results. Indeed, suppose we want to factorize a large integer \( N \). Let \( f \in \mathbb{Z}[X] \) be an integral polynomial of degree \( d \) and \( m \) such that \( N = f(m) \). Let \( F \) be the corresponding homogenized binary form \( F(a, b) = b^d f(a/b) \). An important step of the number field sieve is to find sufficiently many pairs \((a, b)\) such that \( F(a, b)(a - bm) \) is friable. Therefore the study of the function \( \Psi_F(x, y) \) yields information on the complexity of the factoring algorithm and will influence the choice of various parameters of the algorithm. The interested reader will find a detailed presentation of the number field sieve in the monograph of Crandall and Pomerance [CP, chapter 6].

The first key ingredient in the proof of both theorems is a result on the distribution of the values \( F(a, b) \) among arithmetic progressions, see section 2. Work of G. Greaves [G2] (see also [Dan]) shows that — at least for an irreducible form — the level of distribution of the set \( \{F(a, b) : 1 \leq a, b \leq x\} \) is \( x^{2-\varepsilon} \). The proof of Theorem 1 then follows along the lines of [DMT], although the details are somewhat more involved in the present case. For cubic forms, we have a little more elbow room, and we count solutions to \( F(a, b) = uvw \) where the integers \( u, v, w \) have restricted sizes and have their prime factors in certain prescribed intervals. In the reducible case, we need a generalization of a large sieve type inequality for roots of quadratic congruences due to Fouvry and Iwaniec [FI].
This may be useful in other situations, too, and we state and prove it in Section 5.

**Acknowledgements.** The first two authors would like to thank for the invitation and excellent working conditions at the Université Nancy 1, where this paper was worked out.

## 2. Preliminaries

### 2.1. Generalities

Throughout the paper we shall (without loss of generality) always assume that all binary forms are primitive, that is, the greatest common divisor of their coefficients is 1. Given a binary form $F(X,Y)$, a real number $x \geq 1$ and a positive integer $d$, we define

$$A_d(x; F) := \text{card}\{1 \leq a, b \leq x : F(a, b) \equiv 0 \pmod{d}\}.$$ 

We consider the approximation

$$A_d(x; F) \approx \frac{\gamma_F(d)}{d^2} x^2 + r_d(x),$$

where

$$\gamma_F(d) := \text{card}\{0 \leq u, v < d : F(u, v) \equiv 0 \pmod{d}\}$$

is a multiplicative function and $r_d(x)$ is an error term. When $F(X,Y)$ is irreducible and not linear, Greaves [G1, G2] proved that the error term is small on average over $d$: for $x \geq 1$, $z \geq 1$ and any $\varepsilon > 0$ we have [G2, 2.4.4]

$$\sum_{d \leq z} |r_d(x)| \ll_{\varepsilon, F} (z + x)^{\varepsilon}.$$ 

A similar form of this relation is proved by S. Daniel [Dan, Lemma 3.3]: if $t := \text{deg } F$, we have

$$\sum_{d \leq z} \sup_{|\partial\mathcal{R}| \leq M} \left| \sum_{(a,b) \in \mathcal{R}} 1 - \frac{\gamma_F(d) \text{vol } \mathcal{R}}{d^2} \right| \ll_{\varepsilon, F} M^{1/2} \left\{ \log(2z) \right\}^{\nu_t} + z \{\log(2z)\}^{3\nu_t - 1},$$

where $\nu_t := t(1 + 2t)^{t+1}$, $\mathcal{R}$ is any compact subset of $\mathbb{R}^2$, $\text{vol } \mathcal{R}$ designates its volume and $|\partial\mathcal{R}|$ the length of its boundary.

Let us temporarily assume that $F$ is irreducible and set

$$\varrho_F(n) := \text{card}\{1 \leq a \leq n : F(a, 1) \equiv 0 \pmod{n}\}.$$ 

We then have (see [G2, 2.2.2, 2.2.5])

$$\gamma_F(p) = (p - 1)\varrho_F(p) + 1, \quad \gamma_F(p^2) = p(p - 1)\varrho_F(p^2) + p^2,$$

if $p$ does not divide the leading coefficient of $F(X,1)$; in particular $\gamma_F(p) \neq 0$, $\gamma_F(p^2) \neq 0$ in this case. For $t = 3$ and all primes $p$, the following general bounds hold

$$\gamma_F(p^\nu) \ll p^{1 + \nu/3} \quad (\nu \geq 1).$$

This follows by combining [Dan, (7.2)–(7.4)] on noting that Daniel's function $\varrho(d)$ is our function $\gamma_F(d)$. We also recall that $\gamma_F(p)$ is $p$ on average: indeed, we have [G2, 2.3.1]

$$\sum_{p \leq \xi} \frac{\gamma_F(p) \log p}{p^2} = \log \xi + O(1) \quad (\xi \geq 1).$$

More precisely, it is a classical result going back (at least) to Dedekind (see e.g. [Dan, pp. 126-7] or [T1, (3.35)]) that

$$\sum_{n \geq 1} \frac{\gamma_F(n)}{n^{s+1}} = \zeta_k(s)\varrho(s)$$

Note that these works employ a different normalization for the multiplicative function appearing in the main term of (2.1).
where $F$ is an Euler product, absolutely convergent in $\Re s > 1 - 1/t$, $K := \mathbb{Q}(\vartheta)$ for some root $\vartheta$ of $F(X, 1)$ and $\zeta_K$ is the Dedekind zeta function of the field $K$.

2.2. A summatory function linked to polynomial congruences. In the proof of Theorem 2, in the case when $F$ cubic and irreducible, we need an asymptotic formula for the sum of $\gamma_F(n)/n$ over integers without small prime factors. (This is needed for the evaluation of the $u$ and $w$-sums in (4.6) below.) We formulate the result in a somewhat more general context. Its full strength will not be needed for our present purposes, but it may be useful for further reference in similar situations.

Let $K/\mathbb{Q}$ be now an algebraic number field and $\zeta_K$ be the corresponding Dedekind zeta function. We let $\varrho$ and $\omega$ denote respectively the Dickman function and the Buchstab function, see [T2, pp. 366, 399] For $\varepsilon > 0$, we introduce the domain

$$H_{\varepsilon}(s) = \{\Re s > 1, \exp\{(\log\log x)^{5/3+\varepsilon}\} \leq z \leq x\}.$$ 

We also define, for $z \geq 2$,

$$L_{\varepsilon}(z) := \exp\{(\log z)^{3/5-\varepsilon}\}, \quad Z_{\varepsilon} := \exp\{(\log z)^{3/2-\varepsilon}\}.$$ 

For $x \geq z \geq 2$, we write systematically $u := (\log x)/\log z$ and define

$$H(u) := \exp\{u/(1 + \log u)^2\}.$$ 

We denote by $\zeta(s)$ the Riemann zeta function and introduce the partial Euler product

$$\zeta(s, z) := \prod_{p \leq z} (1 - p^{-s})^{-1} (\Re s > 0).$$ 

Proposition 1. Let $f$ be a multiplicative function with associated Dirichlet series $F(s) := \sum_{n \geq 1} f(n)n^{-s}$ absolutely convergent for $\Re s > 1$. Assume that

$$F(s) = \zeta_K(s)\varrho(s)$$

where $F$ is given by an Euler product that is absolutely convergent in a suitable half-plane $\Re s > 1 - \delta$ with $\delta > 0$. Then there exists an absolute constant $c > 0$ such that, for any given $\varepsilon > 0$ and uniformly in the domain $H_{\varepsilon}$, we have

$$\sum_{n \leq z} f(n) \sim x\omega(u) - z \frac{e^\gamma}{\zeta(1, z)} + O\left(\frac{x\varrho(u)}{(\log z)^2} \left\{H(u)^{-c} + Z_{\varepsilon}^{-1}\right\}\right).$$

Proof. Let $F(s; z)$ designate the subseries of $F(s)$ restricted to $z$-friable integers $n$. Let $\varphi$ denote the Laplace transform of the Dickman function $\varrho$, viz.

$$\varphi(u) := \int_0^\infty e^{-us}\varrho(u)\,du \quad (s \in \mathbb{C}).$$

From formula (3.35) of [T1], we see that Lemma 4.1 of [HTW] may be applied to $F$, providing the estimate

$$F(s; z) = F(s)(s - 1)(\log z)\varphi((s - 1)\log z)\left\{1 + O\left(\frac{1}{L_{\varepsilon}(z)}\right)\right\}$$

whenever $z \geq 2$, $\Re s > 1 - 1/(\log z)^{2/5+\varepsilon}$, $|\Im s| \leq L_{\varepsilon}(z)$. We obtain the stated result by reproducing step by step the computations of the proofs of Theorem III.6.7 and Corollary III.6.7.5 of [T2, pp. 408-417], simply replacing the function $\zeta(s)/\zeta(s, z)$ by $F(s)/F(s; z)$, which satisfies the same asymptotic formula, given by (2.8), in the same range $H_{\varepsilon}$. This is proved, in particular, by appealing to the fact that $\zeta_K(s)$ has a Vinogradov-type zero-free region analogous to that of $\zeta(s)$. We note that the necessary analogue of formula (III.6.72) of [T2], which follows from a simple form of the approximate functional equation for $\zeta(s)$, is provided by Lemma 3.4 of [HTW].
2.3. The level of distribution of the sequence \( \{F(a, b)\}_{a, b \in \mathbb{N}} \). In this section we adapt Greaves’ method to obtain a variant of (2.2) related to binary forms that need not be irreducible. We consider \( m \) distinct irreducible binary forms \( F_1, \ldots, F_m \), and write \( F = (F_1, \ldots, F_m) \). For all \( d = (d_1, \ldots, d_m) \in \mathbb{N}^m \) and \( x \geq 1 \), we write
\[
F(a, b) \equiv 0 \pmod{d}
\]
to mean that \( F_j(a, b) \equiv 0 \pmod{d_j} \) for \( 1 \leq j \leq m \), and define
\[
A(x; F, d) := \text{card}\{1 \leq a, b \leq x : F(a, b) \equiv 0 \pmod{d}\}.
\]
Our generalization is stated as follows.

**Proposition 2.** Let \( \varepsilon > 0 \) and \( 0 \leq s \leq m \). Assume that \( F_1, \ldots, F_s \) are linear forms and that \( F_{s+1}, \ldots, F_m \) are forms of degree \( \geq 2 \). Then, uniformly for \( D_1 \geq 1, \ldots, D_m \geq 1, x \geq 1 \), we have
\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu^2(\Delta_m) |A(x; F, d) - x^2 \prod_{1 \leq j \leq m} \frac{\gamma_{F_j}(d_j)}{d_j^2}| \ll \left( xD_s + \Delta_s^2 + D \right) D^\varepsilon,
\]
with
\[
\Delta_m := \prod_{1 \leq j \leq m} d_j, \quad \Delta_s := \prod_{1 \leq j \leq s} D_j, \quad \hat{D}_s := \prod_{s \leq j \leq m} D_j, \quad D := \prod_{1 \leq j \leq m} D_j.
\]

When \( F \) has no linear factor, we have \( s = 0 \), and our definition of \( \hat{D}_s \) ensures that \( \hat{D}_s \neq 0 \) even in this case. The upper bound in (2.9) is then \((x + D)D^\varepsilon\).

We confined ourselves to proving a simple result which is sufficient for the proof of Theorem 1. With a little more work, the condition that the \( d_j \) are squarefree and pairwise coprime could be relaxed.

**Proof.** We detect congruences via exponential sums. We have
\[
A(x; F, d) = \frac{1}{\Delta_m^2} \sum_{0 \leq g, h < \Delta_m, \frac{F(u, v)}{d} \equiv 0 \pmod{d}} \sum_{0 \leq u, v \leq \Delta_m} \sum_{\substack{1 \leq a, b \leq x, 0 \leq a, \nu \leq \Delta_m \leq \Delta_m}} e \left( \frac{g(u - a) + h(v - b)}{\Delta_m} \right).
\]
The main contribution arises from \( g = h = 0 \). Since \( (d_i, d_j) = 1 \) for all \( i \neq j \), this yields a term
\[
x^2 \prod_{1 \leq j \leq m} \frac{\gamma_{F_j}(d_j)}{d_j^2}.\]
To estimate the remaining terms, we consider separately those pairs \((g, h)\) such that \( g = 0 \) or \( h = 0 \). Writing
\[
S(d; g, h) := \sum_{0 \leq u, v \leq \Delta_m, \frac{F(u, v)}{d} \equiv 0 \pmod{d}} e \left( \frac{gu + hv}{\Delta_m} \right),
\]
we have
\[
A(x; F, d) = x^2 \prod_{1 \leq j \leq m} \frac{\gamma_{F_j}(d_j)}{d_j^2} + R_1(d) + R_2(d),
\]
with
\[
R_1(d) := \frac{x}{\Delta_m} \sum_{1 \leq h \leq \Delta_m} (S(d; 0, h) + S(d; h, 0)) \sum_{1 \leq a \leq x} e \left( \frac{-ha}{\Delta_m} \right) \ll \frac{x}{\Delta_m} \sum_{1 \leq h \leq \Delta_m} \min(h, \Delta_m - h) \ll \frac{x}{\Delta_m} \sum_{1 \leq h \leq \Delta_m/2} \frac{|S(d; 0, h)| + |S(d; h, 0)|}{h},
\]
\[
R_2(d) := \frac{1}{\Delta_m^2} \sum_{1 \leq g, h \leq \Delta_m} S(d; g, h) \sum_{1 \leq a, b \leq x} e \left( \frac{-ga - hb}{\Delta_m} \right) \ll \sum_{1 \leq g, h \leq \Delta_m/2} \frac{|S(d; g, h)| + |S(d; -g, h)|}{gh}.
\]
We proceed to bound the exponential sums $S(d; g, h)$. Put $\Delta'_m := \Delta_m/d_1$. Since $(d_1, \Delta'_m) = 1$, the Chinese remainder theorem implies that each pair $\{u, v\}$ with $1 \leq u, v \leq \Delta_m$ has a representation in the form $u = u_1 \Delta'_m + u_2 d_1$, $v = v_1 \Delta'_m + v_2 d_1$ with $0 \leq u_1, v_1 < d_1$ and $0 \leq u_2, v_2 < \Delta'_m$. Since the forms $F_j$ are homogeneous, the congruence conditions become
\[
F_j(u, v) \equiv 0 \pmod{d_j} \quad \Leftrightarrow \quad \begin{cases} 
F_j(u_2 d_1, v_2 d_1) \equiv 0 \pmod{d_j} & \text{if } j \neq 1 \\
F_j(u_1, v_1) \equiv 0 \pmod{d_1} & \text{if } j = 1
\end{cases}
\]
Thus we obtain
\[
S(d; g, h) = \prod_{1 \leq j \leq m} \sum_{\substack{0 \leq u, v < d_j \\ F_j(u,v) \equiv 0 \pmod{d_j}}} e\left(\frac{gu + hv}{d_j}\right) =: \prod_{1 \leq j \leq m} S_j(d_j; g, h),
\]
say. When $d_j = p$ is a prime and $\deg(F_j) \geq 2$, Greaves (see [G1] or [G2]) proved that
\[
S_j(p; g, h) \ll (F_j(h, g), p).
\]
This inequality is also satisfied when $\deg(F_j) = 1$, i.e. $F_j$ is of type $F_j(X, Y) = \alpha_j X + \beta_j Y$ with $(\alpha_j, \beta_j) = 1$. Indeed, if $(\alpha_j, p) = 1$, we have
\[
S_j(p; g, h) = \sum_{0 \leq u, v < p} e\left(\frac{gu + hv}{p}\right),
\]
where $\overline{\alpha_j}$ is defined modulo $p$ by the equation $\alpha_j \overline{\alpha_j} \equiv 1 \pmod{p}$. Thus
\[
S_j(p; g, h) = \sum_{0 \leq v < p} e\left(\frac{v\overline{h} - \alpha_j \beta_j}{p}\right) = \begin{cases} 
p & \text{if } -\alpha_j h + \beta_j g \equiv 0 \pmod{p}, \\
0 & \text{otherwise}
\end{cases}
\]
and (2.12) is still satisfied (with implicit constant 1) in this case. If $p \mid \alpha_j$ and therefore $p \nmid \beta_j$, then $F_j(u, v) \equiv 0 \pmod{p}$ if and only if $v = 0$, so
\[
S_j(p; g, h) = \begin{cases} 
p & \text{if } p \mid g, \\
0 & \text{otherwise.}
\end{cases}
\]
Thus (2.12) holds unconditionally. Successive applications of the Chinese remainder theorem (using the fact that the $d_j$ are squarefree) and (2.12) yield
\[
S_j(d_j; g, h) = \prod_{p \mid d_j} S_j(p; g, h) \ll C_j^{\omega(d_j)} (F_j(-h, g), d_j),
\]
where $C_j > 0$ depends only of $F_j$. Thus, there exists $C = C(F) > 0$ such that
\[
S(d, g, h) \ll C^{\omega(\Delta_m)} \prod_{1 \leq j \leq m} (F_j(-h, g), d_j).
\]
Moreover, we bear in mind that when $F_j$ is linear we also have from the Chinese remainder theorem, (2.13) and (2.14), that
\[
S_j(d_j; g, h) = \begin{cases} 
d_j & \text{if } F_j(-h, g) \equiv 0 \pmod{d_j}, \\
0 & \text{otherwise.}
\end{cases}
\]
We are now in a position to estimate the contributions to (2.9) of the error terms $R_j(d)$ in (2.10). Let $0 < \varepsilon_1 < \varepsilon$. The case of $R_2(d)$ is typical. We observe that when $\deg F_j \geq 2$, we always have $F_j(-h, g) \neq 0$ in (2.15). Indeed $(0, 0)$ is the only solution in $\mathbb{Z}^2$ of the equation $F_j(a, b) = 0$ because $F_j$ is irreducible and non-linear. (See [Dar, p. 51] for a proof of this assertion.) We also remark (in the case $s \neq 0$) that if $(g, h)$ satisfy $F_j(-h, g) = 0$ for some $1 \leq i \leq s$ then $F_j(-h, g) \neq 0$ for all $1 \leq j \leq s$ such that $j \neq i$.

We handle separately the contribution of those pairs $(g, h)$ such that $F_j(-h, g) = 0$ for some $1 \leq j \leq s$. We write

\begin{equation}
R_2(d) = T_0(d) + \sum_{1 \leq j \leq s} T_j(d)
\end{equation}

where in $T_0(d)$ the summation comprises all $1 \leq g, h \leq \Delta_m$ such that $F(-h, g) \neq 0$ and in $T_j(d)$ with $1 \leq j \leq s$, the summation is defined by the conditions $1 \leq g, h \leq \Delta_m$ and $F_j(-h, g) = 0$.

We first consider the contribution of $T_0(d)$ to the left-hand side of (2.9). We have

\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 T_0(d) \ll \sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \Delta_m^2 \sum_{1 \leq g, h \leq \Delta_m \neq 0} \frac{1}{gh} \prod_{1 \leq j \leq m} |(F_j(-h, g), d_j)| \ll D^\varepsilon \sum_{1 \leq g, h \leq \Delta_m \neq 0} \frac{1}{gh} \prod_{1 \leq j \leq m} |(F_j(-h, g), d_j)|.
\]

Now we note that for all integers $D \geq 1$, $N \geq 1$, we have

\begin{equation}
\sum_{d \leq D} (N, d) = \sum_{d \leq D} \sum_{l | (N, d)} \varphi(t) \leq \sum_{l | N, t \leq D} \varphi(t)D/t \leq D\tau(N),
\end{equation}

where $\tau(N)$ denotes the number of divisors of $N$. Inserting this in the above bound yields

\begin{equation}
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 T_0(d) \ll D^{1+\varepsilon} \sum_{1 \leq g, h \leq \Delta_m \neq 0} \frac{1}{gh} \prod_{1 \leq j \leq m} \tau(|F_j(-h, g)|) \ll D^{1+\varepsilon}.
\end{equation}

Next, we estimate the contributions to (2.9) of the quantities $T_j(d)$ for $1 \leq j \leq s$. Since in these summations we have $F_j(-h, g) = -\alpha_j h + \beta_j g = 0$, we may replace the variable $h$ by $g\beta_j/\alpha_j$. Note that we must have $\alpha_j \neq 0$ since $gh\beta_j \neq 0$. We define $\Delta_s := \prod_{1 \leq i \leq s} d_i$. By (2.16) we have

\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 T_j(d) \ll \sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \Delta_m^2 \sum_{1 \leq g, h \leq \Delta_m \neq 0} \frac{1}{gh} \prod_{s < r \leq m} |(F_r(-h, g), d_r)|.
\]

Let $\varepsilon_2 \in \varepsilon_1, \varepsilon_1$, where $\varepsilon$ is given in Proposition 2 and $\varepsilon_1$ was defined after (2.16). First, we use (2.18) to estimate the $d_j$-partial sums for $s < j \leq m$ in the same way as we did for the terms $T_0(d)$. We obtain

\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 T_j(d) \ll \tilde{D}_s D^{\varepsilon_2} \sum_{d_1 \leq D_1} \cdots \sum_{d_s \leq D_s} \mu^s(\Delta_m) \sum_{1 \leq g, h \leq \Delta_m \neq 0} \frac{\Delta_s}{g^2}.
\]

For $1 \leq i \leq s$, $i \neq j$, the congruence $F_i(-g\beta_j/\alpha_j, g) \equiv 0 \pmod{d_i}$ is equivalent to

\[
g \beta_j \equiv 0 \pmod{(d_i, \alpha_j \beta_i - \alpha_i \beta_j)}.
\]

Since the $d_i$ are mutually coprime we have

\[
\text{lcm}_{j \neq i \leq s} \left\{ \frac{d_i}{(d_i, \alpha_j \beta_i - \alpha_i \beta_j)} \right\} = \frac{\Delta_s}{Kd_j}.
\]
where \( K = K(d) \) satisfies
\[
K \mid \prod_{1 \leq i, j \leq s, i \neq j} (\alpha_j \beta_i - \alpha_i \beta_j)
\]
and is therefore bounded uniformly with respect to \( d \). Thus there exists \( K_0(d) \in \mathbb{N} \), \( K_0(d) \ll 1 \), such that, whenever \( g \) satisfies the conditions \( d_i \mid F_i(-g \beta_j / \alpha_j, g) \) for \( 1 \leq i \leq s, i \neq j \), then \( \Delta_s/\{K_0(d)d_j\} \mid g \). Writing \( g = \Delta_s g' / \{K_0(d)d_j\} \), we infer that
\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 T_j(d) \ll D_1 D^2 \sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_s)^2 \sum_{1 \leq \Delta_s g' / \{K_0(d)d_j\} \leq \Delta_s \hat{D}_s} \frac{d_j^2}{\Delta s g'^2} \ll D_1^2 \hat{D}_s D^2.
\]

The contribution to (2.9) of the terms \( R_1(d) \) may be handled similarly. We appeal to (2.11), (2.15) and (2.16). If there are no defective factors \( F_j(X, Y) = \pm X \) or \( F_j(X, Y) = \pm Y \), then we have \( F_j(-h, 0) \neq 0 \) and \( F_j(0, h) \neq 0 \) for all \( h \neq 0 \) and all \( 1 \leq j \leq m \). With computations parallel to those employed to estimate the contribution to (2.9) of the terms \( T_0(d) \), we obtain
\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 |R_1(d)| \ll x D^\epsilon.
\]
If, for instance, we have \( F_1(X, Y) = X \) then \( S_1(d_1; g, 0) = d_1 \) for all \( g \) and \( d_1 \). We obtain
\[
R_1(d) \ll \frac{xd_1 C_{\Delta_m}^\epsilon}{\Delta_m} \sum_{1 \leq h \leq \Delta_m/2} \frac{1}{h} \prod_{2 \leq j \leq m} |(F_j(-h, 0), d_j)|.
\]
Arguing as for the estimation of the terms \( T_j(d) \) \((j \neq 0)\), we obtain
\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 |R_1(d)| \ll D^\epsilon D_1 x.
\]
Similarly, if \( F_1(X, Y) = X, F_2(X, Y) = Y \), we have
\[
\sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 |R_1(d)| \ll D^\epsilon (D_1 + D_2)x,
\]
and so in any case
\[
(2.21) \sum_{d_1 \leq D_1} \cdots \sum_{d_m \leq D_m} \mu(\Delta_m)^2 |R_1(d)| \ll D^\epsilon \hat{D}_s x
\]
Combining (2.19), (2.20) (summed over \( 1 \leq j \leq s \)) and (2.21) completes the proof of Proposition 2.

3. Proof of Theorem 1

If \( G(X, Y) \) is an irreducible factor of \( F \) with degree \( < \alpha_F \), then we have
\[
P^\epsilon(G(a, b)) \ll x^{O_F} = o(y)
\]
for all \( 1 \leq a, b \leq x \). Thus, irreducible factors of \( F \) having small degree may be discarded. Let \( m \) be the integer defined by
\[
m := \begin{cases} k & \text{if } k \geq 2 \\ \ell + 1 & \text{if } k = 1. \end{cases}
\]
Then \( m \) is the number of distinct irreducible factors of \( F \) having degree \( \geq \alpha_F \). If \( m = k \), we write the factorization of \( F \) in the form:
\[
F(X, Y) = G(X, Y) \prod_{1 \leq j \leq k} F_j(X, Y)^{\beta_j},
\]
where $F_1, \ldots, F_k$ are the distinct (up to scalars) irreducible factors of degree $g$ of $F$ and all irreducible factors of $G$ have degree at most $g - 1$. If $m > k$ (i.e. $k = 1$, $\ell \geq 1$, $m = \ell + 1$), then we write the factorization of $F$ as

$$F(X, Y) = H(X, Y) \prod_{1 \leq i \leq m} F_i(X, Y)^{\delta_i},$$

where $F_1, \ldots, F_k$ are the distinct irreducible factors of $F$ of degree $g - 1$ and $F_m$ is the (only) irreducible factor of $F$ of degree $g$.

The arguments of the various proofs in [DMT] were based on properties of arithmetic functions related to the number of divisors of polynomial values in prescribed intervals. Here we adapt the ideas, and retain the main notations, of [DMT]. For $\Psi$ of (3.1) that follows from (3.1). When (3.2) whenever $|d_j'| \leq |F_j(a, b)| |(Kx)^{\delta_j}| < y$, and so $P^+(F(a, b)) \leq y$.

Indeed, if $(a, b)$ is counted by $H_J(x; w, z)$, then $F_j(a, b) = d_j d_j'$ with $Kx^\delta/y < d_j \leq y$ for each $j$, whence $|d_j' | \leq |F_j(a, b) y/(Kx)^{\delta_j} < y$, and so $P^+(F(a, b)) \leq y$.

In the case $k = 1$, there exists $K > 0$, depending only on $F$, such that (3.1) holds provided

$$Kx^\delta/y < w_j \leq z_j \leq y \quad (1 \leq j \leq k).$$

Indeed, if $(a, b)$ is counted by $H_J(x; w, z)$, then $F_j(a, b) = d_j d_j'$ with $Kx^\delta/y < d_j \leq y$ for each $j$, whence $|d_j' | \leq |F_j(a, b) y/(Kx)^{\delta_j} < y$, and so $P^+(F(a, b)) \leq y$.

Let $\delta \in \{0, 1/(1 + m^2)\}$. Using Proposition 2, we shall show that

$$H_J(x; w, z) \geq x^2$$

for

$$z_j := \begin{cases} x^{(2-\delta)/k-(j-1)\delta} & \text{if } k \geq 2 \text{ and } 1 \leq j \leq k, \\ x^{(1-\delta)/m-(j-1)\delta} & \text{if } k = 1 \text{ and } 1 \leq j \leq \ell, \\ x^{\delta+(1-\delta)/m} & \text{if } k = 1 \text{ and } j = m. \\ \end{cases}$$

We note that, with the above choice of parameters, the intervals $[w_j, z_j]$ are disjoint.

Let us first assume $\deg(F) \geq 4$. When $k \geq 2$, conditions (3.2) are fulfilled for $y = x^{\alpha_F + \varepsilon}$ with $\alpha_F$ as in Theorem 1, if $\delta$ is sufficiently small in terms of $\varepsilon$ and $k$. The required lower bound hence follows from (3.1). When $k = 1$, $g \geq 3$, we arrive at the same conclusion by noting that (3.3) holds for small enough $\delta$. In the case $k = 1$, $g = 2$, we have $\ell \geq 2$. Therefore $m \geq 3$, and so the first set of conditions in (3.3) holds for small enough $\delta$. However, the inequality $z_m \leq y$ is not necessarily satisfied and we adapt the definition of $H_J(x; w, z)$ by requiring that the divisor $d_m$ is itself friable. We postpone this case as well as the discussion of the cases $\deg(F) = 2, 3$ to the end of the proof.

Let us first assume $(g, k) \neq (2, 1)$ (and $\deg(F) \geq 4$), and prove (3.4) in this case. Let $w, z$ be as above. We observe that

$$B_F(a, b) := \prod_{1 \leq j \leq m} \sum_{p_j | F_j(a, b)} 1 \leq \left( \frac{\max_{1 \leq j \leq m} \log(Kx^\delta)}{\log w_j} \right)^m \ll \left( \frac{m^2g}{1 - \delta(1 + m^2)} \right)^m$$

for $1 \leq a, b \leq x$. Hence

$$H_J(x; w, z) \geq \sum_{1 \leq a, b \leq x} B_F(a, b) = \sum_{w_1 \leq p_1 \leq z_1} \cdots \sum_{w_m \leq p_m \leq z_m} \sum_{1 \leq a, b \leq x} 1.$$
Our choice of $x$ guarantees that $z_1 \cdots z_m < x^{2-\eta}$ for sufficiently small $\eta > 0$. Moreover, the primes $p_1, \ldots, p_m$ in (3.6) are distinct since $[w_j, z_j]w_i, z_i] = \emptyset$ if $j \neq i$. By Proposition 2 it follows that

$$H_F(x; w, z) \gg x^2 \prod_{1 \leq j \leq m} \frac{\gamma_{F_j}(p_j)}{p_j^2} + O(x^{-\eta/2}).$$

By (2.6) and partial summation we have for all $1 \leq j \leq m$,

$$\sum_{w_j < p_j \leq z_j} \frac{\gamma_{F_j}(p_j)}{p_j^2} = \log \left( \frac{\log z_j}{\log w_j} \right) + O\left( \frac{1}{\log w_j} \right),$$

Inserting (3.8) in (3.7) confirms (3.4) and completes the proof of Theorem 1 in the case $(g, k) \neq (2, 1)$.

To handle the case $(g, k) = (2, 1)$ (still assuming $\deg(F) \geq 4$), we replace the weights $B_F(a, b)$ by

$$B_F^*(a, b) := \left( \sum_{s_m < p_m \leq t_m} \prod_{u_m < q_m \leq v_m} \prod_{p_m q_m | F_m(a, b)} 1 \right),$$

where $p_j$, $q_m$ denote primes and $t_m = u_m := x^{\frac{1}{2} - \delta + (1-\delta)/(2m)}$, $s_m := t_m x^{-\delta}$, $v_m := u_m x^\delta$.

If $B_F^*(a, b) \neq 0$, then the divisor $d_m = p_m q_m$ of $F_m(a, b)$ is $y$-friable and hence $F_m(a, b)$ is also $y$-friable. The last steps are as in the previous case. We have

$$\Psi_F(x, y) \gg \sum_{1 \leq a, b \leq x} B_F^*(a, b) \gg \sum_{w_1 < p_1 \leq z_1} \cdots \sum_{s_m < p_m \leq t_m} \sum_{u_m < q_m \leq v_m} \sum_{p_m q_m | F_m(a, b)} 1.$$

Applying Proposition 2 and using the fact that $\gamma_{F_m}$ is multiplicative to separate the summations over $p_m$ and $q_m$, we obtain the lower bound $\Psi_F(x, y) \gg x^2$ as before. This ends the proof of Theorem 1 in the case $\deg(F) \geq 4$.

It remains to handle the cases $\deg(F) = 2, 3$. Then, in (3.9), the divisors $d_j = p_j q_j \in [w_j, z_j]$ may not be $y$-friable, and we modify the weights accordingly. Since the corresponding results will be improved in Theorem 2 for cubic forms and are essentially known for quadratic forms, we only provide a brief description.

(a) $F$ is a cubic form. If $F$ is irreducible, we replace the weights $B_F(a, b)$ defined in (3.5) by

$$B_F(a, b) := \sum_{p_1, p_2 \mid F(a, b)} 1.$$

The proof may then be completed by computations very similar to those described in the case $(g, k) = (2, 1)$, $\deg(F) \geq 4$. If $F = F_1 F_2$ where $F_j$ is, for $j = 1, 2$, an irreducible binary form of degree $j$, we choose

$$B_F(a, b) := \sum_{p_1 \mid F_1(a, b)} 1 \sum_{p_2 \mid F_2(a, b)} 1,$$

where the primes $p_1, p_2, q_2$ are subject to the conditions

$$x^{(1/3) - \delta} < p_1 < x^{1/3}, \quad x^{(2/3) - \delta} < p_2 < x^{2/3}, \quad x^{(2/3) - 2\delta} < q_2 < x^{(2/3) - \delta}.$$
When $F = F_1 F_2 F_3$ is a product of three linear factors we select
\[ B_F(a, b) := \prod_{1 \leq j \leq 3} p_{j|F(a, b)} \sum_{1 \leq j \leq 3} 1, \]
subject to the conditions $x^{(1/3) - (j - 1/2)\delta} < p_j \leq x^{(1/3) - (j - 1)\delta}$ and $x^{(1/3) - j\delta} < q_j \leq x^{(1/3) - (j - 1/2)\delta}$.

(b) $F$ is a quadratic form. When $F$ is irreducible we take
\[ B_F(a, b) := \sum_{x^{2-2\delta} < d \leq x^{2-\delta}} \sum_{\substack{P^+(d) < y, P^-(d) > x^\eta \atop d|F(a, b)}} 1 \ll 2^{2/\eta}, \]
where $\delta$ and $\eta$ are sufficiently small parameters and $x$ is sufficiently large. The lower bound
\[ \sum_{x^{2-2\delta} < d \leq x^{2-\delta}} \sum_{\substack{P^+(d) < y, P^-(d) > x^\eta \atop d|F(a, b)}} \frac{\gamma_F(d)}{d^2} \gg 1 \]
is then derived from the inequality
\[ \sum_{x^{2-2\delta} < d \leq x^{2-\delta}} \sum_{\substack{P^+(d) < y, P^-(d) > x^\eta \atop d|F(a, b)}} \frac{\gamma_F(d)}{d^2} \geq \prod_{1 \leq j \leq J, x^{(j-1)\eta} < p_j} \frac{\gamma_F(p_j^{\eta_j})}{p_j^\eta_j}, \]
where $J$ is chosen in such a way that
\[ 2 - 2\delta < \frac{1}{2} J(J + 1)\eta, \quad \frac{1}{2} J(J + 3)\eta < 2 - \delta. \]
This is indeed possible provided $\delta$ and $\eta/\delta$ are small enough, for instance $\eta = \delta^2$. It then only remains to apply (3.8) to the sums over $p_j$. The last case, i.e. $F = F_1 F_2$ is a product of two linear forms, is essentially trivial, as explained in the proof of Theorem 2, and we skip the details here.

4. Cubic forms — the irreducible case

4.1. The combinatorial setup. Let $F$ be a primitive irreducible cubic form. By [G2, p. 37] the form $F$ cannot have a fixed divisor other than 1 and 2, i.e. $\gamma_F(p) < p^2$ if $p > 2$. If $\gamma_F(2) = 2^2$, then $F^*(X, Y) := \frac{1}{2} F(X, 2Y)$ is an integral primitive irreducible form without fixed prime divisor, and Theorem 2 for $F^*$ implies the result for $F$. Thus we can assume henceforth
\[ \gamma_F(p) < p^2 \]
for all $p$. Let $\mathcal{S}_0$ be the set of primes dividing the discriminant or the leading coefficients of $F$, and let $\mathcal{S}$ denote the union of $\mathcal{S}_0$ and the set of those primes satisfying $\gamma_F(p) = 0$. Then $\mathcal{S}_0$ is a finite set depending only on $F$, and by Hensel’s lemma we have
\[ \gamma_F(p^\eta) \neq p\gamma_F(p) \]
for all $p \notin \mathcal{S}$. For this and the following sections we use the notation
\[ \mathcal{P}_z := \prod_{p \leq z} p, \quad \mathcal{P}_z^\ast := \prod_{p \leq z, p \notin \mathcal{S}} p, \quad \mathcal{P}_0^\ast := \prod_{p \leq z, p \notin \mathcal{S}_0} p. \]
We study $y$-friable values of $F(a, b)$ by considering factorizations $|F(a, b)| = uvw$, where $u$ and $v$ vary in prescribed ranges (so eventually $w$ as well), and $P^+(uvw) \leq y$, $(uvw, \mathcal{P}_z) = 1, 2 \leq z \leq y \leq x$. We choose
\[ z = x^{\eta}. \]
\[3\] The discriminant of $F$ is in fact the discriminant of the polynomial $F(X, 1)$. 
levels of small parameters and put

$$\epsilon > \delta := \epsilon^2 > \eta := \epsilon^3 > 0.$$

For parameters $U, V$ to be fixed later, we have

$$\text{card}\{1 \leq a, b \leq x : P^+(F(a, b)) \leq y\} \gg S := \sum_{\substack{1 \leq a, b \leq x \\mid F(a, b) = uv \\mid \mathcal{P}_z}} 1.$$

This last sum counts all five-tuples $(a, b, u, v, w)$ satisfying the long list of conditions. The condition $P^+(w) \leq y$ is controlled by counting all $w$ first and subtracting the contribution of those having $P^+(w) > y$; when doing this second stage we can drop the condition $P^+(u) \leq y$ as we only need a lower bound. In other words

$$S \geq \sum_{U^{-\epsilon} < u \leq U} \sum_{V^{-\epsilon} < v \leq V} \sum_{1 \leq a, b \leq x \mid F(a, b) \equiv 0 (\text{mod } uv)} 1 - \sum_{P^+(w) > y} \sum_{u \mid \mathcal{P}_z} \sum_{w, v \mid \mathcal{P}_z} 1.$$

First realize that the innermost sum in the second term is obviously empty if

$$w > W := x^{3+\epsilon+2\delta}/(UV).$$

On the other hand, for any given $W_0$, the contribution of those terms with $w \leq W_0$ can be bounded by (2.3): they contribute at most

$$\ll \sum_{w \leq W_0} \sum_{v \leq V} \sum_{\substack{1 \leq a, b \leq x \\mid F(a, b) \equiv 0 (\text{mod } uv)}} 1$$

$$\ll \sum_{w \leq W_0} \sum_{v \leq V} \gamma_F(v)\gamma_F(u)(uvU)^{2/3} + O(x^\eta(VW_0 + (UVW_0)^{1/3}(VW_0)^{1/2})))$$

$$\ll (UVW_0)^{2/3} + x^\eta(VW_0 + U^{1/3}(VW_0)^{5/6}).$$

By choosing the parameters, we have to provide that the above bound is $\ll x^{2-\eta}$, as well as we need that $UV \leq x^{2-\eta}$, $VW \leq x^{2-\eta}$ (to leave room for a sieving). The best choice is

$$W = U := x^{1+\epsilon+4\delta}, \quad V := U/x^\epsilon$$

$$V_0 := V/x^\delta$$

$$W_0 := x^{1+\delta} = W/x^{\epsilon+3\delta}.$$
characteristic function of \((n, \mathcal{P}) = 1\). Using these weights in the appropriate place we arrive at
\[
S \geq \sum_{\substack{U_0 < u \leq U \atop (u, \mathcal{P}) = 1}} \sum_{V_0 < v \leq V \atop (v, \mathcal{P}) = 1} \sum_{d \leq D \atop d \mid \mathcal{P}} \lambda_d^+ \sum_{1 \leq a, b \leq x \atop F(a, b) \equiv 0 \pmod{ud}} 1
- \sum_{\substack{W_0 < w \leq W \atop (w, \mathcal{P}) = 1}} \sum_{V_0 < v \leq V \atop (v, \mathcal{P}) = 1} \sum_{d \leq D \atop d \mid \mathcal{P}} \lambda_d^+ \sum_{1 \leq a, b \leq x \atop F(a, b) \equiv 0 \pmod{vw}} 1 + O(x^{2-\eta}).
\]

At this stage, we derive from (2.2) the following relation
\[
(4.5) \quad S \geq \sum_{\substack{U_0 < u \leq U \atop (u, \mathcal{P}) = 1}} \sum_{V_0 < v \leq V \atop (v, \mathcal{P}) = 1} \sum_{d \leq D \atop d \mid \mathcal{P}} \lambda_d^+ \gamma_F(uvd)x^2 \quad (uvd)^2 - \sum_{\substack{W_0 < w \leq W \atop (w, \mathcal{P}) = 1}} \sum_{V_0 < v \leq V \atop (v, \mathcal{P}) = 1} \sum_{d \leq D \atop d \mid \mathcal{P}} \lambda_d^+ \gamma_F(uvd)x^2 \quad (uvd)^2 + O(x^{2-\eta}).
\]

We plainly have \((uv, vd) = 1\). Hence we have to compute
\[
T^+ := \sum_{\substack{V_0 < v \leq V \atop (v, \mathcal{P}) = 1}} \sum_{d \leq D \atop d \mid \mathcal{P}} \lambda_d^+ \gamma_F(vd) \quad (vd)^2,
\]
and (4.5) becomes
\[
(4.6) \quad S \geq x^2 T^- \sum_{\substack{U_0 < u \leq U \atop (u, \mathcal{P}) = 1}} \frac{\gamma_F(u)}{u^2} - x^2 T^+ \sum_{\substack{W_0 < w \leq W \atop (w, \mathcal{P}) = 1}} \frac{\gamma_F(w)}{w^2} + O(x^{2-\eta}).
\]

**Remark.** Although a big chunk of computation is still ahead, we have at this point a flash of the final result. Suppose that \(y = x^\alpha\). Since \(z = x^\gamma = D^\delta\), we expect that, for suitable constants \(c > 0\), \(\kappa(\varepsilon)\), we have
\[
T^- \sim T^+ \sim \frac{c}{\log z} \sum_{\substack{V_0 < v \leq V \atop (v, \mathcal{P}) = 1}} \frac{\gamma_F(v)}{v^2} \sim \kappa(\varepsilon) > 0.
\]

Indeed, it is expected that an interval, the endpoints of which being two fixed, distinct powers of \(z\), captures a positive proportion of the friable sum
\[
\sum_{v \mid \mathcal{P}} \frac{\gamma_F(v)}{v^2} \approx \log z.
\]

Bearing in mind that \(\gamma_F(q)/q\) is 1 on average, we similarly expect that, with a suitable constant \(b > 0\), we have
\[
\sum_{\substack{U_0 < u \leq U \atop (u, \mathcal{P}) = 1}} \frac{\gamma_F(u)}{u^2} \sim b \left(1 - \log \left(\frac{\log U}{\log y}\right)\right) \frac{\log(U/U_0)}{\log z} \sim b \varepsilon^2 \left(1 - \log \frac{1}{\varepsilon}\right),
\]
and, much in the same way,
\[
\sum_{\substack{W_0 < w \leq W \atop (w, \mathcal{P}) = 1}} \frac{\gamma_F(w)}{w^2} \sim b \log \left(\frac{\log W}{\log y}\right) \frac{\log(W/W_0)}{\log z} \sim b \varepsilon^2 \log \frac{1}{\varepsilon}.
\]

Finally these expectations lead to
\[
S \geq \left\{1 - 2 \log \frac{1}{\varepsilon} + o(1)\right\} \frac{b \kappa(\varepsilon)x^2}{\varepsilon^2}.
\]
This exceeds a positive constant times $x^2$ precisely when $\theta > 1/\sqrt{e}$.

4.2. Estimation of the main term. We return to (4.6). For any fixed $v \not| \mathcal{P}_z^*$ we note that $\gamma_F(v) \neq 0$ by (2.4) and (4.2), and we define

$$g_v(p) := \frac{\gamma_F(p^v)}{p^\gamma_F(v)} = \begin{cases} \frac{\gamma_F(p)}{p} & \text{if } p \nmid v, \\ \frac{\gamma_F(p^2)}{p^\gamma_F(p)} & \text{if } p \mid v. \end{cases}$$

By (4.1), (2.4) and (2.5) we conclude (see also [G2, 2.2.11]) that, uniformly in $v$,

$$g_v(p) = O(1), \quad g_v(p) < p.$$

This last inequality needs the condition $v \not| \mathcal{P}_z^*$, as it is not true for $g_F(p) = 0$, $p \mid v$, for example.

Next we check that the function $g_v(d) := \gamma_F(vd)/(d\gamma_F(v))$ is multiplicative. This follows from the well-known general fact that, for any multiplicative function $f$ and any fixed integer $m$ such that $f(m) \neq 0$, the function $f_m(n) = f(mn)/f(m)$ is multiplicative. Indeed, writing $\mu_p$ for the $p$-adic valuation of $m$, we have

$$f_m(n) = \prod_{p^\nu || n} \frac{f(p^{\nu+\mu_p})}{f(p^{\nu})} \quad (n \geq 1).$$

We can now apply a fundamental lemma type sieve estimate for $T^\pm$. What we need is implicit in [HR, Theorem 7.1]. We get

$$T^\pm = \sum_{\substack{V_0 < v \leq V \\ v \mid \mathcal{P}_z^*}} \frac{\gamma_F(v)}{v^2} \sum_{\substack{d \leq D \\ d \mid \mathcal{D}_z}} \frac{\lambda_d^F g_v(d)}{d}$$

$$= \sum_{\substack{V_0 < v \leq V \\ v \mid \mathcal{P}_z^*}} \frac{\gamma_F(v)}{v^2} \left\{1 + O(e^{-D}/\log z)\right\} \prod_{p \leq z} \left(1 - \frac{g_v(p)}{p}\right)$$

$$= \left\{1 + O(e^{1/\varepsilon})\right\} \prod_{p \leq z} \left(1 - \frac{\gamma_F(p)}{p^2}\right) \sum_{\substack{V_0 < v \leq V \\ v \mid \mathcal{P}_z^*}} \frac{\gamma_F^*(v)}{v^2},$$

where, for shorter reference we have written

$$(4.7) \quad \gamma^*_F(v) := \gamma_F(v) \prod_{p \mid v} \frac{p^2 - \gamma_F(p^2)/\gamma_F(p)}{p^2 - \gamma_F(p)}.$$

This is still a multiplicative function. Note that by (2.4) we have $\gamma^*_F(p) = 0$ if $g_F(p) = 0$, but $p$ does not divide the leading coefficient of $F(X, 1)$. Thus, we can include those primes into the $v$-sum, and only need to exclude the primes in $\mathcal{D}_0$, that is

$$T^\pm = \left\{1 + O(e^{1/\varepsilon})\right\} \prod_{p \leq z} \left(1 - \frac{\gamma_F(p)}{p^2}\right) \sum_{\substack{V_0 < v \leq V \\ v \mid \mathcal{P}_z^*}} \frac{\gamma_F^*(v)}{v^2}.$$

By (2.7), the product is $\asymp A/\log z$ where $A$ is a positive constant. Moreover, by [TW2, Theorem 3.2], the $v$-sum is

$$\{1 + o(1)\} e^{-\gamma} \int_{(1-\varepsilon,1-\varepsilon z)} e^\gamma \prod_{p \mid \mathcal{P}_0} \left(1 + \frac{\gamma_F^*(p)}{p^2}\right) = (\kappa_0(\varepsilon) + o(1)) \log z,$$

say.
Put $\kappa(\varepsilon) := A\kappa_0(\varepsilon)$. Substituting into (4.6), we arrive at

$$
S \geq \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \left\{ x^2 \kappa(\varepsilon) \left( \sum_{u_0 < u \leq U} \frac{\gamma_F(u)}{u^2} - \sum_{W_0 < w \leq W} \frac{\gamma_F(w)}{w^2} \right) + O(x^{2-\eta}) \right\}
$$

(4.8)

as the interval $[U_0, U]$ is contained in the interval $[W_0, W]$. We evaluate the sums over $u$ and $w$ by Proposition 1. By (2.5) and (2.7), the arithmetic function $n \mapsto \gamma_F(n)/n$ satisfies the hypotheses of Proposition 1. We recall the choices (4.4) of the relevant parameters as well as $D = \varepsilon^\delta$, $z = \varepsilon^\gamma = D^\delta$.

From Proposition 1, we obtain

$$
\sum_{n \leq \xi \atop (n, \mathcal{P}_2) = 1} \frac{\gamma_F(n)}{n} = \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \frac{\xi}{\log z},
$$

whenever $D < \xi \leq U$, while an elementary argument using (2.6) furnishes

$$
\sum_{n \leq \xi \atop (n, \mathcal{P}_2) = 1} \frac{\gamma_F(n)}{n} \ll \frac{\xi}{\log z} + 1
$$

for all $\xi \geq 1$. By partial summation, we infer that

$$
\sum_{U_0 < u \leq U \atop (u, \mathcal{P}_2) = 1} \frac{\gamma_F(u)}{u^2} = \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \frac{\log(U/U_0)}{\log z},
$$

and

$$
\sum_{W_0 < w \leq W \atop (w, \mathcal{P}_2) = 1} \frac{\gamma_F(w)}{w^2} = \sum_{y < p \leq W} \frac{\gamma_F(p)}{p^2} \sum_{W_0 < w \leq W/p \atop (w, \mathcal{P}_2) = 1} \frac{\gamma_F(w)}{w^2}
$$

$$
= \sum_{y < p \leq W} \frac{\gamma_F(p)}{p^2} \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \frac{\log(W/W_0)}{\log z}
$$

$$
= \left\{ 1 + O(\varepsilon) \right\} \frac{\log W}{\log y} \frac{\log(W/W_0)}{\log z}.
$$

Suppose that $y = \varepsilon^\delta$. Substituting the last two displays into (4.8), we arrive at

$$
S \geq \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \left\{ x^2 \kappa(\varepsilon) \left( \frac{\log(U/U_0)}{\log z} - 2 \log \left( \frac{\log W}{\log y} \frac{\log(W/W_0)}{\log z} \right) \right) + O(x^{2-\eta}) \right\}
$$

$$
= \left\{ 1 + O(e^{-1/\varepsilon}) \right\} \left\{ 2(\varepsilon + 3\delta) \frac{\log \left( \frac{1 + \varepsilon + 4\delta}{\delta} \right)}{\varepsilon^3} x^2 + O(x^{2-\eta}) \right\}
$$

$$
\geq \left\{ 1 - 2 \log \frac{1}{\varepsilon^3} + O(\varepsilon) \right\} x^2 + O(x^{2-\eta}).
$$

This completes the proof of Theorem 2 in case the form is irreducible.
5. Cubic forms — the reducible case

There are two possibilities for a reducible cubic form $F$: either $F = F_1 F_2$ where $F_1$ is linear and $F_2$ is quadratic, or $F = F_1 F_2 F_3$ for three linear forms $F_1, F_2, F_3$.

5.1. Three linear forms. Let us start with the second case, and let us assume that two of the three linear forms

$$F_i(a, b) = \alpha_i a + \beta_i b, \quad \alpha_i, \beta_i \in \mathbb{Z}, \quad 1 \leq i \leq 3,$$ 

say $F_1$ and $F_2$, are linearly independent over $\mathbb{Q}$. Let $A = \left( \begin{array}{cc} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{array} \right) \in \text{GL}_2(\mathbb{Q})$, and set $\Delta := \det A \neq 0$.

If we write $r = F_1(a, b)$, $s = F_2(a, b)$, then $(r) = A(\langle a \rangle)$, and therefore

$$F_3(a, b) = \alpha_3 r + \beta_3 s,$$

where $(\alpha_3', \beta_3') := (\alpha_3, \beta_3) A^{-1} \in \left( \frac{1}{\Delta} \mathbb{Z} \right)^2$.

Thus

$$S := \text{card}\{ (r, s) : \Delta \mid r, \Delta \mid s, A^{-1}(\langle s \rangle) = [1, x]^2, P^+(rs(\alpha_3' r + \beta_3' s)) \leq y \}$$

is a lower bound for the number of $1 \leq a, b \leq x$ such that $F(a, b)$ is $y$-friable. Fix $\varepsilon > 0$ and assume $y = x^\varepsilon$. Notice that $[c_1 x, c_2 x] \times [c_3 x, c_4 x] \subseteq A([1, x]^2)$ for suitable (positive or negative) constants $c_1 \neq c_2, c_3 \neq c_4$, and let

$$\mathcal{A} := \{ \alpha_3' r : r \in [c_1 x, c_2 x], \Delta \mid r, P^+(r) \leq y \}, \quad \mathcal{B} := \{ \beta_3' s : s \in [c_3 x, c_4 x], \Delta \mid s, P^+(s) \leq y \}.$$

Then $|\mathcal{A}| \cdot |\mathcal{B}| \gg x^2$ and $\mathcal{A}, \mathcal{B} \subseteq [-c_5 x, c_5 x]$ for some constant $c_5 > 0$. By a result of La Bretèche [Br, Théorème 2] (which holds in the same way and with the same proof for $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}$, not only for $\mathcal{A}, \mathcal{B} \subseteq \mathbb{N}$), we obtain

$$S \gg \text{card}\{ (a, b) \in \mathcal{A} \times \mathcal{B} : P^+(a + b) \leq y \} \gg |\mathcal{A}| \cdot |\mathcal{B}| \gg x^2.$$

If all three linear forms are linearly dependent, La Bretèche’s theorem gives the same result immediately. It is clear that the same result holds for a reducible quadratic form.

5.2. A linear and a quadratic form. Let us now turn to the harder case $F = F_1 F_2$ where

$$F_1(a, b) = \alpha_1 a + \beta_1 b, \quad F_2(a, b) = \alpha_2 a^2 + \beta_2 a b + \gamma_2 b^2$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2, \gamma_2 \in \mathbb{Z}$ and $F_2$ is irreducible of discriminant $\Delta = \beta_2^2 - 4\alpha_2 \gamma_2$ which is not a perfect square. In particular, $\alpha_2 \neq 0$. Since not both $\alpha_1$ and $\beta_1$ are 0, we can assume that $\alpha_1 \neq 0$. Let $A = \left( \begin{array}{cc} \alpha_1 & \beta_1 \\ 0 & 1 \end{array} \right)$, and change variables $(\langle s \rangle) := A(\langle a \rangle)$. Then

$$\alpha_1^2 F_2(a, b) = \alpha_1^2 + \beta_2 a b + \gamma_2 b^2 =: \tilde{F}(r, s)$$

where $\alpha = \alpha_2 \neq 0$, $\beta = \alpha_1 \beta_2 - 2\beta_1 \alpha_2$, $\gamma = \beta_2^2 - \beta_1^2 \alpha_2 + 2\beta_1 \alpha_1$, and the discriminant of $\tilde{F}$ is $\Delta := \alpha_1^2 \Delta$. By the same argument as above,

$$\text{card}\{ (r, s) : r \equiv \beta_1 s \mod(\alpha_1), A^{-1}(\langle s \rangle) \subseteq [1, x]^2, P^+(r \tilde{F}(r, s)) \leq y \}$$

is a lower bound for the number of $1 \leq a, b \leq x$ such that $F(a, b)$ is $y$-friable. Again as above, this is

$$\gg \text{card}\{ (r, s) \in [c_1 x, c_2 x] \times [c_3 x, c_4 x] : P^+(r \tilde{F}(r, s)) \leq y \}$$

for suitable constants $c_1 < c_2, c_3 < c_4$, and by changing the sign of the middle term of $\tilde{F}$ if necessary, we can assume that $c_1, \ldots, c_4 > 0$. Let $f$ be a smooth nonnegative function supported on $I := [c_3 x, c_4 x]$ such that $\sup_I |f^{(j)}(t)| \ll j x^{-j}$ for all $j \in \mathbb{N}$ and $\int_I f(t) \, dt = c_0 x$ for some $c_0 > 0$. Let $0 < \varepsilon < 1/10$ and put $D := x^{2-\varepsilon/2}$, $y := x^\varepsilon$, $z := x^\varepsilon/100$. Then we can bound the previous display from below by

$$\gg \sum_{x^{-\varepsilon/20} D \leq d \leq D} \sum_{c_1 x \leq r \leq c_2 x} \sum_{P^+(r) \leq z} f(s),$$

where $d \equiv 1 \mod d$, $P^+(d) \leq y$. 

(5.1)
since there is only a bounded number of ways to write \(F(r, s) = dd'\) with \(d\) as required in the summation condition, and all pairs \((r, s)\) of this form yield a \(y\)-friable value of \(F(r, s)\). We transform the innermost sum by splitting \(s\) into residue classes modulo \(d\) and applying Poisson summation. In this way we obtain

\[
\sum_{F(r, s) \equiv 0 \ (\text{mod} \ d)} f(s) = \sum_{s \ (\text{mod} \ d)} \frac{1}{d} \sum_{h \in \mathbb{Z}} e\left(\frac{hs}{d}\right) \hat{f}\left(\frac{h}{d}\right)
\]

where

\[
(5.2) \quad \hat{f}(z) := \int_{-\infty}^{\infty} f(t)e(-zt) \, dt \ll \frac{x}{(1 + |z|x)^A}
\]

for any \(A \geq 0\) (after \([A] + 1\) partial integrations), and \(\hat{f}(0) = c_0x\). Let

\[
(5.3) \quad \gamma_h,r(d) := \sum_{s \ (\text{mod} \ d)} e\left(\frac{hs}{d}\right).
\]

The term \(h = 0\) will contribute the main term

\[
(5.4) \quad M := c_0x \sum_{D/x^{1/20} \leq d \leq D} \frac{1}{d} \sum_{\substack{c_1x \leq r \leq c_2x \\ \tau \in \mathbb{Z} \ \text{even}}} \gamma_0,r(d)
\]

to \((5.1)\), while we treat the remaining part,

\[
E := \sum_{h \neq 0} \sum_{D/x^{1/20} \leq d \leq D} \frac{1}{d} \sum_{\substack{c_1x \leq r \leq c_2x \\ \tau \in \mathbb{Z} \ \text{even}}} \gamma_h,r(d) \hat{f}\left(\frac{h}{d}\right),
\]

as an error term. First we observe that by choosing \(A\) large enough in \((5.2)\), we can truncate the \(h\)-sum at \(H := Dx^{(c/6) - 1} = x^{1-c/3}\) with a negligible error, say \(\ll 1/x\). Next we open the Fourier transform and perform the change of variables \(\tau := ht/H\), obtaining

\[
(5.5) \quad E \ll \sum_{D/x^{1/20} \leq d \leq D} \frac{1}{d} \int_{-\infty}^{\infty} \left| \sum_{\tau \in \mathbb{Z}} H_f \frac{H}{h} \hat{f}\left(\frac{H}{h}\right) \sum_{\substack{c_1x \leq r \leq c_2x \\ \tau \in \mathbb{Z} \ \text{even}}} \gamma_h,r(d) \, d\tau + O\left(\frac{1}{x}\right)
\]

To estimate the inner sum, we use the following large sieve inequality which is a slight generalization of [FI, Lemma 3].

**Proposition 3.** Let \(F(X, Y) = \alpha X^2 + \beta XY + \gamma Y^2 \in \mathbb{Z}[X, Y]\) be an arbitrary (positive definite or indefinite, not necessarily primitive) quadratic form whose discriminant \(\Delta = \beta^2 - 4\alpha\gamma\) is not a perfect square. Define \(\gamma_h,r(d)\) as in \((5.3)\) with \(F\) replaced by \(F\). For any sequence \(\xi_h,r\) of complex numbers, positive real numbers \(D, H, R\), and any \(\delta > 0\), we have

\[
\sum_{d \leq D} \left| \sum_{h \leq H} \sum_{r \leq R} \xi_h,r \gamma_h,r(d) \right| \ll \delta, \quad D^{1/2}(D + HR)^{1/2} \left(\sum_{h,r} |\xi_h,r|^2\right)^{1/2} (DHR)^{\delta}.
\]
We postpone the proof of this estimate to the next section and proceed with bounding the error term (5.5). This is
\[ x^{5/20} HD^{1/2}(Hx)^{1/2} \int_{-\varepsilon x}^{\varepsilon x} \left( \frac{R(x)}{H \tau} \right)^{1/2} d\tau \delta(DHR)^{\delta} \ll \frac{x^{x/20} x^{40} H R^{1/2} x^{3/2}}{D^{1/2}} = x^{2-\varepsilon/200} \]
on choosing \( \delta = \varepsilon/240 \). This is plainly acceptable.

Let us now turn to the main term \( M \) defined in (5.4). We first observe that our summation conditions imply \( (r, d) = 1 \), so that \( \gamma_0(r) =: g(d) \) is independent of \( r \). It therefore remains to show that
\[ \sum_{\substack{D/x^{1/20} \leq d \leq D \\ (d, \Delta) = 1}} g(d) \geq c(\varepsilon) \geq 0 \]
for some constant \( c(\varepsilon) \). For a prime \( p \nmid 2n\Delta \) we have \( g(p) = 1 + (\Delta|p) \in \{0, 2\} \) which depends only on \( p \) modulo \( \Delta \). Let \( \sum_p \) denote a sum over primes satisfying \( g(p) = 2 \). For such primes, we have \( g(p^r) \geq 2 \) for all integers \( r \geq 1 \). Let
\[ \varepsilon > 0, \quad \varepsilon_0 := \frac{\varepsilon}{40} \left( \frac{40 - 11\varepsilon}{10.5\varepsilon} \right) < \frac{\varepsilon}{40}, \quad \mathcal{F} := [x^{\varepsilon_0}, x^{\varepsilon/40}], \quad k := \left[ \frac{80}{\varepsilon} - 20 \right] \in \mathbb{N}. \]
Note that \( x^{\varepsilon_0/40} \leq x^{2-\varepsilon/2} = D \) and \( x^{k\varepsilon_0} \geq x^{2-11\varepsilon/20} = D x^{-\varepsilon/20} \). Thus the left hand side of (5.6) can be bounded below by
\[ \left( \sum_{p \in \mathcal{F}} \frac{1}{p} \right)^k \geq c(\varepsilon). \]
This completes the proof of the Theorem.

5.3. A large sieve inequality. We prove Proposition 3. The basic device is a well-spacing property of the fractions \( \nu/d \) (mod 1), where \( d \sim D \) and \( \nu \) runs through the solutions of \( F(\nu, 1) \equiv 0 \) (mod \( d \)); we follow closely the argument of [FI], where the case \( F(r, s) = r^2 + s^2 \) is treated. The underlying idea goes back to Hooley [Ho], see also [To]. In the sequel, all implicit and explicit constants depend at most upon \( F \), and the word “bounded” is understood as “bounded only in terms of \( F \”).

Let us fix a positive integer \( d \). Completing the square, we find a one-to-one correspondence between the two sets\footnote{For the second set, we have identified (non-canonically) the pairs \( (\nu, k) \in [0, d] \times \mathbb{Z} \) such that \((2\nu + \beta)^2 - 4\alpha dk = \Delta \) with the pairs \( (\nu, k) \in (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z} \) satisfying this equation.}
\[ \{ \nu \ (\text{mod } d) : F(\nu, 1) \equiv 0 \ (\text{mod } d) \} \text{ and } \{(\nu, k) \in (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z} : (2\nu + \beta)^2 - 4\alpha dk = \Delta \}, \]
and the latter set can be identified with the set of (not necessarily primitive) integral quadratic forms
\[ aX^2 + bXY + dY^2 : b^2 - 4ad = \Delta, a \equiv 0 \ (\text{mod } \alpha), b \ (\text{mod } 2d\alpha), b \equiv \beta \ (\text{mod } 2\alpha), \]
via
\[ a = \alpha k \text{ and } b = 2\alpha \nu + \beta. \]
The group \( SL_2(\mathbb{Z}) \) acts on the set of all integral binary quadratic forms \( \mathcal{F}(\Delta) \) of discriminant \( \Delta \): if \( \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \) and \( Q(X, Y) = aX^2 + bXY + cY^2 \in \mathcal{F}(\Delta) \), then \( Q^\sigma(X, Y) = Q((X, Y) \cdot \sigma) = a^\sigma X^2 + b^\sigma XY + c^\sigma Y^2 \) with
\[ a^\sigma = Q(r, s), b^\sigma = 2art + bru + bst + 2cru, c^\sigma = Q(t, u). \]
It is known that \( SL_2(\mathbb{Z}) \setminus \mathcal{F}(\Delta) = \{ Q_1, \ldots, Q_h \} \) is finite. For each representative \( Q_j = a_jX^2 + b_jXY + c_jY^2 \), say, let \( \mathcal{F}_j(d) \) be the set of matrices \( \sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \) such that \( Q_j^\sigma \) contributes
to (5.7). Clearly we must have \( Q_j(t, u) = d \). The set \( \mathcal{O}(Q_j) := \{ \sigma \in SL_2(\mathbb{Z}) : Q_j^\sigma = Q_j \} \) of automorphisms of \( Q_j \) acts on \( \mathcal{S}_j(d) \), and matrices in the same \( \mathcal{O}(Q_j) \)-orbit contribute the same quadratic form to (5.7). Thus we see that by (5.8) a typical fraction \( \nu/d \) is of the form

\[
(5.9) \quad \frac{\nu}{d} = \frac{b_j^2 - \beta}{2\alpha} = \frac{2a_jrt + bj(ru + st) + 2cj_0s - \beta}{2aQ_j(t, u)}, \quad \text{with } 1 \leq j \leq h,
\]

where \( \tilde{r} = r \). We claim that for each \( \sigma = (t^\ast u^\ast) \in \mathcal{S}_j(d) \) there is a representative modulo \( \mathcal{O}(Q_j) \) such that \( t, u \ll \sqrt{d} \). Indeed, if \( \Delta < 0 \), then \( (\tilde{t} \tilde{u}) \in \mathcal{S}_j(d) \) implies \( (2a_jt + bj_u)^2 - \Delta u^2 = 4a_jd \), and the claim is obvious. If \( \Delta > 0 \), we can assume that \( Q_j \) is a primitive form (otherwise divide by \( \text{gcd} \) of the coefficients). Then it is known [La] that \( \mathcal{O}(Q_j) \) is generated by \( \bar{t} = (-1, -1) \) and \( \sigma_0 := \left( \frac{(t-bj)/2}{a^n}, \frac{-c_j/2}{(j+bj)/2} \right) \) corresponding to the fundamental solution of Pell’s equation \( \xi^2 - \Delta \eta^2 = 4 \). For a point \( P := (x_0, y_0) \in \mathbb{R}^2 \) on the hyperbola \( Q_j(x, y) = d \), the segment \( [P, P \cdot \sigma_0] \) is a fundamental domain for the action of \( \mathcal{O}(Q_j) \) on the pairs \( (t, u) \) with \( (\tilde{t} \tilde{u}) \in \mathcal{S}_j(d) \), and hence we can assume that \( (t, u) \) is on that segment. Choosing \( P \) such that \( x_0, y_0 \ll \sqrt{d} \), we obtain the claim also in the indefinite case.

If \( |t| > |u| \), we can write (5.9) as (using \( ru - st = 1 \))

\[
(5.10) \quad \frac{\nu}{d} = \frac{r}{\alpha} - \frac{bt + 2cj_u + \beta t}{2\alpha Q_j(t, u)} = \frac{r}{\alpha} + O\left(\frac{1}{d}\right)
\]

where \( r \equiv \tilde{u} \pmod{|t|} \), and we can assume \( r \ll |t| \ll \sqrt{d} \). Analogously, if \( |u| > |t| \), we obtain the expression

\[
\frac{\nu}{d} = \frac{s}{\alpha u} - \frac{aj t + 2bj_u + \beta t}{2\alpha Q_j(t, u)} = \frac{s}{\alpha u} + O\left(\frac{1}{d}\right)
\]

for (5.9) where \( s \equiv \tilde{t} \pmod{|u|} \), and we can assume \( s \ll |u| \ll \sqrt{d} \). We partition now the (multi-)set

\[
\{ \frac{\nu}{d} \pmod{1} : F(\nu, 1) \equiv 0 \pmod{d}, D \leq d \leq 2D \}
\]

into \( 2h \) classes \( C_i, 1 \leq i \leq 2h \), according to the representative \( Q_j, 1 \leq j \leq h \), in (5.9) and according to \( |t| > |u| \) or \( |u| > |t| \), and we consider one of these classes \( C_i \) with, say, \( |t| > |u| \). If \( (\tilde{t} \tilde{u}) \in SL_2(\mathbb{Z}) \) is any matrix, there are at most two choices for \( (\tilde{t} \tilde{u}) \) with \( |t| > |u| \). Hence we can partition \( C_i \) into a bounded number of subclasses \( C_{i,k}, k \leq 1 \), such that the fractions \( \nu/d \in C_{i,k} \) correspond to matrices \( (\tilde{t} \tilde{u}) \) with different values of \( r/(\alpha t) \pmod{1} \). We can consider one such subclass and order the fractions \( \nu/d \in C_{i,k} \), viewed as elements of \([0, 1]\), in ascending order:

\[
\frac{\nu_1}{d_1} \leq \frac{\nu_2}{d_2} \leq \ldots
\]

Since

\[
(5.11) \quad 0 \neq \left| \frac{r_1}{\alpha t_1} - \frac{r_2}{\alpha t_2} \right| \geq \frac{1}{\alpha t_1 t_2} \gg \frac{1}{D},
\]

for two matrices \( (\tilde{t}_1 \tilde{u}_1) \), \( (\tilde{t}_2 \tilde{u}_2) \) corresponding to two members in \( C_{i,k} \), there is a constant \( L \in \mathbb{N} \) large enough in terms of the implicit constants in (5.10) and (5.11) such that

\[
\left\| \frac{\nu_{L+\ell}}{d_{L+\ell}} - \frac{\nu_{\ell}}{d_{\ell}} \right\| \gg \frac{1}{D}
\]

for all \( \ell \in \mathbb{N} \). Once again we partition \( C_{i,k} \) into a bounded number of subclasses such that any two fractions \( \nu/d, \nu'/d' \) in a given subclass satisfy

\[
\left\| \frac{\nu}{d} - \frac{\nu'}{d'} \right\| \gg \frac{1}{D}.
\]

---

5 Here we note that \( u = 0 \) can only happen when \( t = 1 \), and we interpret \( \tilde{0} := 0 \pmod{1} \).
Applying the classical large sieve inequality (see e.g. [S]) for each subclass separately we conclude
\[
\sum_{D \leq d \leq 2D} \sum_{F(\nu) \equiv 0 (d)} |\sum_{n \leq N} \varrho_n e \left( \frac{\nu n}{d} \right)|^2 \ll (D + N) \sum_{n \leq N} |\varrho_n|^2
\]
for any sequence \( \varrho_n \). Now we are exactly in the situation of [FI, Lemma 2], and we conclude verbatim as in [FI, pp. 252-254] the proposition.

References


[Gr] A. Granville, Smooth numbers: Computational number theory and beyond, MSRI workshop, Proceedings, 56 pp., to appear

[Mo] P. Moree, On the number of \( y \)-smooth natural numbers \( \leq x \) representable as a sum of two integer squares, manuscripta math. 80 (1993), 199-211
[TW2] G. Tenenbaum, J. Wu, Moyennes de certaines fonctions multiplicatives sur les entiers friables, 3, Compositio Math. 144 no. 2 (2008), 339-376

Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest H-1364, Hungary
E-mail address: balog@renyi.hu

Mathematisches Institut, Bunsenstr. 3-5, 37073 Göttingen, Germany
E-mail address: blomer@uni-math.gwdg.de

Institut Élie Cartan, Université Henri Poincaré Nancy 1, BP 239, 54506 Vandœuvre Cedex, France
E-mail address: cecile.dartyte@iecn.u-nancy.fr

Institut Élie Cartan, Université Henri Poincaré Nancy 1, BP 239, 54506 Vandœuvre Cedex, France
E-mail address: gerald.tenenbaum@iecn.u-nancy.fr