Friable values of binary forms

Comment. Math. Helv. 87 (2012), 639–667
DOI 10.4171/CMH/264

Commentarii Mathematici Helvetici

Friable values of binary forms

Antal Balog, Valentin Blomer, Cécile Dartyge and Gérald Tenenbaum

To the memory of our friend and colleague George Greaves

Abstract. Let $F \in \mathbb{Z}[X, Y]$ be an integral binary form of degree $g \geqslant 2$, and let

$$\Psi_F(x, y) := \operatorname{card}\{1 \leqslant a, b \leqslant x : P^+(F(a, b)) \leqslant y\}$$

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 $y = x^{1/\sqrt{e}+\varepsilon}$ if $g = 3$. Better results are obtained if F is reducible.

Mathematics Subject Classification (2010). 11E76, 11N25, 11N36, 11Y05.

Keywords. Friable integers, binary forms, sieves.

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 $P^+(\pm 1) = 1$, $P^-(1) = \infty$, $P^+(0) = 0$.[1] Given a real number $y > 1$, an integer n is called y-friable (or sometimes y-smooth) if $P^+(n) \leqslant y$. 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,

$$\Psi(x, x^\varepsilon) := \operatorname{card}\{1 \leqslant a \leqslant x : P^+(a) \leqslant x^\varepsilon\} \sim \varrho(1/\varepsilon)x$$

where ϱ 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.

[1] For the purpose of this paper, the value of $P^+(0)$ is irrelevant, since for a binary form F there are at most $\ll x$ pairs $(a, b) \in [1, x]^2$ such that $F(a, b) = 0$. The above definition is chosen to simplify the presentation.

In this article, we consider integral binary forms $F \in \mathbb{Z}[X, Y]$, and define

$$\Psi_F(x, y) := \operatorname{card}\{1 \leqslant a, b \leqslant x : P^+(F(a, b)) \leqslant y\}.$$

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

$$\Psi_F(x, y) \asymp x^2. \tag{1.1}$$

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 $\exp((\log x)^\varepsilon) \leqslant y \leqslant x$. 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 $t \geqslant 2$ and no repeated irreducible factor. Let g be the largest degree of an irreducible factor of F and let k (resp. ℓ) denote the number of distinct irreducible factors of F having degree g (resp. $g - 1$). Given any positive real number ε, the estimate*

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

holds for all large x provided $y \geqslant x^{\alpha_F + \varepsilon}$, where the exponent α_F is defined by

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

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 $\deg(F) = t \leqslant 3$, the level of distribution of the sequence $\{F(a, b)\}$ for $1 \leqslant a, b \leqslant x$, given by Proposition 2 below, exceeds $x^{t/2}$.

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

$$\alpha_F := \begin{cases} 1/\sqrt{\mathrm{e}} & \text{if } F \text{ is irreducible;} \\ 0 & \text{if } F \text{ is reducible.} \end{cases}$$

Then

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

provided $y \geqslant x^{\alpha_F + \varepsilon}$.

We have $1/\sqrt{\mathrm{e}} = 0.606\ldots$, so $x^{1/\sqrt{\mathrm{e}}} = (x^3)^{0.202\ldots}$. 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 $\Psi_F(x, x^\varepsilon) \gg x$ holds for any ε and any F: just consider the values $F(a, ca)$ for x^ε-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 $\{F(a, b) : 1 \leqslant a, b \leqslant x\}$ 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

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

We consider the approximation

$$A_d(x;F) = \frac{\gamma_F(d)}{d^2}x^2 + r_d(x), \tag{2.1}$$

where

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

is a multiplicative function and $r_d(x)$ is an error term. When $F(X,Y)$ is irreducible and not linear, Greaves [G1], [G2][2] 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)

$$\sum_{d \leq z} |r_d(x)| \ll_{\varepsilon,F} (z+x)z^{\varepsilon}. \tag{2.2}$$

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

$$\begin{aligned}\sum_{d \leq z} \sup_{|\partial\mathscr{R}| \leq M} \Bigg| \sum_{\substack{(a,b)\in\mathscr{R} \\ F(a,b)\equiv 0 \pmod d}} 1 - \frac{\gamma_F(d)\operatorname{vol}\mathscr{R}}{d^2} \Bigg| \\ \ll_{\varepsilon,F} M\sqrt{z}\{\log(2z)\}^{\nu_t} + z\{\log(2z)\}^{3t-1},\end{aligned} \tag{2.3}$$

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

Let us temporarily assume that F is irreducible and set

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

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

$$\gamma_F(p) = (p-1)\varrho_F(p) + 1, \quad \gamma_F(p^2) = p(p-1)\varrho_F(p^2) + p^2, \tag{2.4}$$

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

$$\gamma_F(p^\nu) \ll p^{1+[\nu/3]} \quad (\nu \geq 1). \tag{2.5}$$

[2] Note that these works employ a different normalization for the multiplicative function appearing in the main term of (2.1).

This follows by combining (7.2)–(7.4) of [Dan] 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,

$$\sum_{p\leqslant\xi}\frac{\gamma_F(p)\log p}{p^2}=\log\xi+O(1)\quad(\xi\geqslant 1). \tag{2.6}$$

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

$$\sum_{n\geqslant 1}\frac{\gamma_F(n)}{n^{s+1}}=\zeta_{\mathbb{K}}(s)\mathscr{G}(s) \tag{2.7}$$

where $\mathscr{G}$ is an Euler product, absolutely convergent in $\Re s>1-1/t$, $\mathbb{K}:=\mathbb{Q}(\vartheta)$ for some root ϑ of $F(X,1)$ and $\zeta_{\mathbb{K}}$ is the Dedekind zeta function of the field $\mathbb{K}$.

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

$$(H_\varepsilon)\qquad x\geqslant 3,\quad \exp\left\{(\log\log x)^{5/3+\varepsilon}\right\}\leqslant z\leqslant x.$$

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

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

For $x\geqslant z\geqslant 2$, 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

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

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

$$\mathscr{F}(s)=\zeta_{\mathbb{K}}(s)\mathscr{G}(s)$$

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

$$\sum_{\substack{n\leqslant x\\ P^-(n)>z}} f(n) = \big(x\omega(u)-z\big)\frac{\mathrm{e}^{\gamma}}{\zeta(1,z)} + O\Big(\frac{x\varrho(u)}{(\log z)^2}\big\{H(u)^{-c} + Z_\varepsilon^{-1}\big\}\Big).$$

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

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

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

$$\mathscr{F}(s;z) = \mathscr{F}(s)(s-1)(\log z)\hat{\varrho}\big((s-1)\log z\big)\Big\{1+O\Big(\frac{1}{L_\varepsilon(z)}\Big)\Big\} \tag{2.8}$$

whenever $z\geqslant 2$, $\Re s > 1-1/(\log z)^{2/5+\varepsilon}$, $|\Im s|\leqslant L_\varepsilon(z)$. 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 $\mathscr{F}(s)/\mathscr{F}(s;z)$, which satisfies the same asymptotic formula, given by (2.8), in the same range H_ε. This is proved, in particular, by appealing to the fact that $\zeta_{\mathbb{K}}(s)$ 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 4.4 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 $F_1,\dots,F_m$, and write $\boldsymbol{F} = (F_1,\dots,F_m)$. For all $\boldsymbol{d} = (d_1,\dots,d_m)\in\mathbb{N}^m$ and $x\geqslant 1$, we write

$$\boldsymbol{F}(a,b)\equiv 0 \pmod{\boldsymbol{d}}$$

to mean that $F_j(a,b)\equiv 0 \pmod{d_j}$ for $1\leqslant j\leqslant m$, and define

$$A(x;\boldsymbol{F},\boldsymbol{d}) := \operatorname{card}\{1\leqslant a,b\leqslant x : \boldsymbol{F}(a,b)\equiv 0 \pmod{\boldsymbol{d}}\}.$$

Our generalization is stated as follows.

Proposition 2. *Let $\varepsilon > 0$ and $0\leqslant s\leqslant m$. Assume further that $F_1,\dots,F_s$ are linear forms and that $F_{s+1},\dots,F_m$ are forms of degree $\geqslant 2$. Then, uniformly for*

$D_1 \geqslant 1, \dots, D_m \geqslant 1$, $x \geqslant 1$, *we have*

$$\sum_{d_1 \leqslant D_1} \cdots \sum_{d_m \leqslant D_m} \mu^2(\Delta_m) \left| A(x; \boldsymbol{F}, \boldsymbol{d}) - x^2 \prod_{1 \leqslant j \leqslant m} \frac{\gamma_{F_j}(d_j)}{d_j^2} \right| \ll \big(x \breve{D}_s + \breve{D}_s^2 \hat{D}_s + D\big) D^{\varepsilon}, \tag{2.9}$$

with

$$\Delta_m := \prod_{1 \leqslant j \leqslant m} d_j, \quad \breve{D}_s := 1 + \sum_{1 \leqslant j \leqslant s} D_j, \quad \hat{D}_s := \prod_{s < j \leqslant m} D_j, \quad D := \prod_{1 \leqslant j \leqslant m} D_j.$$

When $\boldsymbol{F}$ has no linear factor, we have $s = 0$, and our definition of $\breve{D}_s$ ensures that $\breve{D}_s \neq 0$ 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 of Proposition 2. We detect congruences via exponential sums. We have

$$A(x; \boldsymbol{F}, \boldsymbol{d}) = \frac{1}{\Delta_m^2} \sum_{0 \leqslant g,h < \Delta_m} \sum_{\substack{0 \leqslant u,v < \Delta_m \\ \boldsymbol{F}(u,v) \equiv 0 \pmod{\boldsymbol{d}}}} \sum_{1 \leqslant a,b \leqslant x} \mathrm{e}\left(\frac{g(u-a) + h(v-b)}{\Delta_m}\right).$$

The main contribution arises from $g = h = 0$. Since $(d_i, d_j) = 1$ for all $i \neq j$, this yields a term $x^2 \prod_{1 \leqslant j \leqslant m} \{\gamma_{F_j}(d_j)/d_j^2\}$. To estimate the remaining terms, we consider separately those pairs (g, h) such that $g = 0$ or $h = 0$. Writing

$$S(\boldsymbol{d}; g, h) := \sum_{\substack{0 \leqslant u,v < \Delta_m \\ \boldsymbol{F}(u,v) \equiv 0 \pmod{\boldsymbol{d}}}} \mathrm{e}\left(\frac{gu + hv}{\Delta_m}\right),$$

we have

$$A(x; \boldsymbol{F}, \boldsymbol{d}) = x^2 \prod_{1 \leqslant j \leqslant m} \frac{\gamma_{F_j}(d_j)}{d_j^2} + R_1(\boldsymbol{d}) + R_2(\boldsymbol{d}), \tag{2.10}$$

with

$$\begin{aligned} R_1(\boldsymbol{d}) &:= \frac{x}{\Delta_m^2} \sum_{1 \leqslant h < \Delta_m} (S(\boldsymbol{d}; 0, h) + S(\boldsymbol{d}; h, 0)) \sum_{1 \leqslant a \leqslant x} \mathrm{e}\left(\frac{-ha}{\Delta_m}\right) \\ &\ll \frac{x}{\Delta_m} \sum_{1 \leqslant h < \Delta_m} \frac{|S(\boldsymbol{d}; 0, h) + S(\boldsymbol{d}; h, 0)|}{\min(h, \Delta_m - h)} \\ &\ll \frac{x}{\Delta_m} \sum_{1 \leqslant h \leqslant \Delta_m/2} \frac{|S(\boldsymbol{d}; 0, h)| + |S(\boldsymbol{d}; h, 0)|}{h}, \end{aligned}$$

$$R_2(\boldsymbol{d}) := \frac{1}{\Delta_m^2} \sum_{1\leqslant g,h<\Delta_m} S(\boldsymbol{d};g,h) \sum_{1\leqslant a,b\leqslant x} \mathrm{e}\left(\frac{-ga-hb}{\Delta_m}\right)$$
$$\ll \sum_{1\leqslant g,h\leqslant \Delta_m/2} \frac{|S(\boldsymbol{d};g,h)|+|S(\boldsymbol{d};-g,h)|}{gh}.$$

We proceed to bound the exponential sums $S(\boldsymbol{d},g,h)$. Put $\Delta'_m := \Delta_m/d_1$. Since $(d_1,\Delta'_m)=1$, the Chinese remainder theorem implies that each pair $\{u,v\}$ with $1\leqslant u,v\leqslant \Delta_m$ has a representation in the form $u=u_1\Delta'_m+u_2d_1, v=v_1\Delta'_m+v_2d_1$ with $0\leqslant u_1,v_1<d_1$ and $0\leqslant u_2,v_2<\Delta'_m$. Since the forms F_j are homogeneous, the congruence conditions become

$$F_j(u,v)\equiv 0 \pmod{d_j} \iff \begin{cases} F_j(u_2d_1,v_2d_1)\equiv 0 \pmod{d_j} & \text{if } j\neq 1,\\ F_1(u_1\Delta'_m,v_1\Delta'_m)\equiv 0 \pmod{d_1} & \text{if } j=1,\end{cases}$$
$$\iff \begin{cases} F_j(u_2,v_2)\equiv 0 \pmod{d_j} & \text{if } j\neq 1,\\ F_1(u_1,v_1)\equiv 0 \pmod{d_1} & \text{if } j=1.\end{cases}$$

Thus we obtain

$$S(\boldsymbol{d};g,h) = \sum_{\substack{0\leqslant u,v<d_1\\ F_1(u,v)\equiv 0 \pmod{d_1}}} \mathrm{e}\left(\frac{gu+hv}{d_1}\right) \sum_{\substack{0\leqslant u_2,v_2<\Delta'_m\\ F_j(u_2,v_2)\equiv 0 \pmod{\Delta'_m}}} \mathrm{e}\left(\frac{gu_2+hv_2}{d_2\cdots d_m}\right)$$
$$= \prod_{1\leqslant j\leqslant m} \sum_{\substack{0\leqslant u,v<d_j\\ F_j(u,v)\equiv 0 \pmod{d_j}}} \mathrm{e}\left(\frac{gu+hv}{d_j}\right) =: \prod_{1\leqslant j\leqslant m} S_j(d_j;g,h), \tag{2.11}$$

say. When $d_j=p$ is a prime and $\deg(F_j)\geqslant 2$, Greaves (see [G1] or [G2]) proved that

$$S_j(p;g,h) \ll \big(F_j(-h,g),p\big). \tag{2.12}$$

This inequality is also satisfied when $\deg(F_j)=1$, i.e. F_j is of type $F_j(X,Y)=\alpha_jX+\beta_jY$ with $(\alpha_j,\beta_j)=1$. Indeed, if $(\alpha_j,p)=1$, we have

$$S_j(p;g,h) = \sum_{\substack{0\leqslant u,v<p\\ u\equiv -\overline{\alpha_j}\beta_jv \pmod p}} \mathrm{e}\left(\frac{gu+hv}{p}\right),$$

where $\overline{\alpha}_j$ is defined modulo p by the equation $\alpha_j\overline{\alpha}_j\equiv 1 \pmod p$. Thus

$$S_j(p;g,h) = \sum_{0\leqslant v<p} \mathrm{e}\left(\frac{v(h-g\overline{\alpha}_j\beta_j)}{p}\right) = \begin{cases} p & \text{if } -\alpha_jh+\beta_jg\equiv 0 \pmod p,\\ 0 & \text{otherwise}\end{cases} \tag{2.13}$$

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

$$S_j(p;g,h) = \begin{cases} p & \text{if } p \mid g, \\ 0 & \text{otherwise.} \end{cases} \tag{2.14}$$

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

$$S_j(d_j;g,h) = \prod_{p \mid d_j} S_j(p;g,h) \ll C_j^{\omega(d_j)} \left(F_j(-h,g), d_j\right),$$

where $C_j > 0$ depends only of F_j. Thus, there exists $C = C(\boldsymbol{F}) > 0$ such that

$$S(\boldsymbol{d},g,h) \ll C^{\omega(\Delta_m)} \prod_{1 \leqslant j \leqslant m} \left(F_j(-h,g), d_j\right). \tag{2.15}$$

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

$$S_j(d_j;g,h) = \begin{cases} d_j & \text{if } F_j(-h,g) \equiv 0 \pmod{d_j}, \\ 0 & \text{otherwise.} \end{cases} \tag{2.16}$$

We are now in a position to estimate the contributions to (2.9) of the error terms $R_j(\boldsymbol{d})$ in (2.10). Let $0 < \varepsilon_1 < \varepsilon$. The case of $R_2(\boldsymbol{d})$ is typical. We observe that when $\deg F_j \geqslant 2$, 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 $F_i(-h,g) = 0$ for some $1 \leqslant i \leqslant s$ then $F_j(-h,g) \neq 0$ for all $1 \leqslant j \leqslant s$ such that $j \neq i$.

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

$$R_2(\boldsymbol{d}) = T_0(\boldsymbol{d}) + \sum_{1 \leqslant j \leqslant s} T_j(\boldsymbol{d}) \tag{2.17}$$

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

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

$$\begin{aligned}\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}&\mu(\Delta_m)^2T_0(\boldsymbol{d})\\ &\ll\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}\Delta_m^{\varepsilon_1}\sum_{\substack{1\leqslant g,h\leqslant\Delta_m/2\\ F(-h,g)\neq 0}}\frac{1}{gh}\prod_{1\leqslant j\leqslant m}|(F_j(-h,g),d_j)|\\ &\ll D^{\varepsilon_1}\sum_{\substack{1\leqslant g,h\leqslant D/2\\ F(-h,g)\neq 0}}\frac{1}{gh}\prod_{1\leqslant j\leqslant m}\sum_{d_j\leqslant D_j}\big|\big(F_j(-h,g),d_j\big)\big|.\end{aligned}$$

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

$$\sum_{d\leqslant D}(N,d)=\sum_{d\leqslant D}\sum_{t\mid(N,d)}\varphi(t)\leqslant\sum_{t\mid N,\,t\leqslant D}\varphi(t)D/t\leqslant D\tau(N),\tag{2.18}$$

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

$$\begin{aligned}\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}&\mu(\Delta_m)^2T_0(\boldsymbol{d})\\ &\ll D^{1+\varepsilon_1}\sum_{\substack{1\leqslant g,h\leqslant D/2\\ F(-h,g)\neq 0}}\frac{1}{gh}\prod_{1\leqslant j\leqslant m}\tau\big(|F_j(-h,g)|\big)\ll D^{1+\varepsilon}.\end{aligned}\tag{2.19}$$

Next, we estimate the contributions to (2.9) of the quantities $T_j(\boldsymbol{d})$ for $1\leqslant j\leqslant s$. 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 $\Delta_s:=\prod_{1\leqslant i\leqslant s}d_i$. By (2.16) we have

$$\begin{aligned}\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}&\mu(\Delta_m)^2T_j(\boldsymbol{d})\\ &\ll\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}\Delta_m^{\varepsilon_1}\sum_{\substack{1\leqslant g\leqslant\Delta_m/2,\,\alpha_j\mid g\\ d_i\mid F_i(-g\beta_j/\alpha_j,g)\,(j\neq i\leqslant s)}}\frac{\Delta_s}{g^2}\prod_{s<r\leqslant m}|(F_r(-h,g),d_r)|.\end{aligned}$$

Let $\varepsilon_2\in]\varepsilon_1,\varepsilon[$, where ε is given in Proposition 2 and ε_1 was defined after (2.16). First, we use (2.18) to estimate the d_j-partial sums for $s<j\leqslant m$ much in the same way as we did for the terms $T_0(\boldsymbol{d})$. We obtain

$$\begin{aligned}\sum_{d_1\leqslant D_1}\cdots\sum_{d_m\leqslant D_m}&\mu(\Delta_m)^2T_j(\boldsymbol{d})\\ &\ll\widehat{D}_sD^{\varepsilon_2}\sum_{d_1\leqslant D_1}\cdots\sum_{d_s\leqslant D_s}\mu^s(\Delta_m)\sum_{\substack{1\leqslant g\leqslant\Delta_s\widehat{D}_s,\,\alpha_j\mid g\\ d_i\mid F_i(-g\beta_j/\alpha_j,g)\,(j\neq i\leqslant s)}}\frac{\Delta_s}{g^2}.\end{aligned}$$

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

$$\frac{g}{\alpha_j} \equiv 0 \left(\mathrm{mod}\ \frac{d_i}{(d_i, \alpha_j\beta_i - \alpha_i\beta_j)}\right).$$

Since the d_i are mutually coprime we have

$$\operatorname*{lcm}_{j\neq i\leqslant s}\left\{\frac{d_i}{(d_i, \alpha_j\beta_i - \alpha_i\beta_j)}\right\} = \frac{\Delta_s}{Kd_j}$$

where $K = K(\boldsymbol{d})$ satisfies

$$K \mid \prod_{\substack{1\leqslant i\leqslant s\\ i\neq j}} (\alpha_j\beta_i - \alpha_i\beta_j)$$

and is therefore bounded uniformly with respect to $\boldsymbol{d}$. Thus there exists $K_0(\boldsymbol{d}) \in \mathbb{N}$, $K_0(\boldsymbol{d}) \ll 1$, such that, whenever g satisfies the conditions $d_i \mid F_i(-g\beta_j/\alpha_j, g)$ for $1 \leqslant i \leqslant s, i \neq j$, then $\Delta_s/\{K_0(\boldsymbol{d})d_j\} \mid g$. Writing $g = \Delta_s g'/\{K_0(\boldsymbol{d})d_j\}$, we infer that

$$\begin{aligned}\sum_{d_1\leqslant D_1} \cdots \sum_{d_m\leqslant D_m} &\mu(\Delta_m)^2 T_j(\boldsymbol{d})\\ &\ll \hat{D}_s D^{\varepsilon_2} \sum_{d_1\leqslant D_1} \cdots \sum_{d_s\leqslant D_s} \mu(\Delta_s)^2 \sum_{1\leqslant \Delta_s g'/\{K_0(\boldsymbol{d})d_j\}\leqslant \Delta_s \hat{D}_s} \frac{d_j^2}{\Delta_s g'^2}\\ &\ll D_j^2 \hat{D}_s D^{\varepsilon}.\end{aligned} \tag{2.20}$$

The contribution to (2.9) of the terms $R_1(\boldsymbol{d})$ 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 $1 \leqslant j \leqslant m$. With computations parallel to those employed to estimate the contribution to (2.9) of the terms $T_0(\boldsymbol{d})$, we obtain

$$\sum_{d_1\leqslant D_1} \cdots \sum_{d_m\leqslant D_m} \mu(\Delta_m)^2 |R_1(\boldsymbol{d})| \ll xD^{\varepsilon}.$$

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

$$R_1(\boldsymbol{d}) \ll \frac{xd_1C^{\omega(\Delta_m)}}{\Delta_m} \sum_{1\leqslant h\leqslant \Delta_m/2} \frac{1}{h} \prod_{2\leqslant j\leqslant m} \big|(F_j(-h, 0), d_j)\big|.$$

Arguing as for the estimation of the terms $T_j(\boldsymbol{d})$ $(j \neq 0)$, we obtain

$$\sum_{d_1\leqslant D_1} \cdots \sum_{d_m\leqslant D_m} \mu(\Delta_m)^2 |R_1(\boldsymbol{d})| \ll D^{\varepsilon} D_1 x.$$

Similarly, if $F_1(X,Y) = X, F_2(X,Y) = Y$, we have

$$\sum_{d_1 \leqslant D_1} \cdots \sum_{d_m \leqslant D_m} \mu(\Delta_m)^2 |R_1(\boldsymbol{d})| \ll D^{\varepsilon}(D_1 + D_2)x,$$

and so in any case

$$\sum_{d_1 \leqslant D_1} \cdots \sum_{d_m \leqslant D_m} \mu(\Delta_m)^2 |R_1(\boldsymbol{d})| \ll D^{\varepsilon} \breve{D}_s x. \tag{2.21}$$

Combining (2.19), (2.20) (summed over $1 \leqslant j \leqslant s$) 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

$$P^+(G(a,b)) \ll x^{\alpha_F} = o(y)$$

for all $1 \leqslant a, b \leqslant x$. Thus, irreducible factors of F having small degree may be discarded. Let m be the integer defined by

$$m := \begin{cases} k & \text{if } k \geqslant 2, \\ \ell + 1 & \text{if } k = 1. \end{cases}$$

Then m is the number of distinct irreducible factors of F having degree $\geqslant \alpha_F$. If $m = k$, we write the factorization of F in the form:

$$F(X,Y) = G(X,Y) \prod_{1 \leqslant j \leqslant k} F_j(X,Y)^{\beta_j},$$

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. $k = 1$, $\ell \geqslant 1, m = \ell + 1$), then we write the factorization of F as

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

where $F_1, \ldots, F_\ell$ 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 m-dimensional vectors $\boldsymbol{w} = (w_1, \dots, w_m)$ and $\boldsymbol{z} = (z_1, \dots, z_m)$, the quantity $H_F(x; \boldsymbol{w}, \boldsymbol{z})$ is defined as the number of integer pairs $(a, b) \in [1, x]^2$ such that, for all $j \in [1, k]$, the number $F_j(a, b)$ has at least one divisor d_j with $w_j < d_j \leqslant z_j$.

We note at the outset that if $k \geqslant 2$, then there exists a constant K, depending only on F, such that

$$\Psi_F(x, y) \geqslant H_F(x; \boldsymbol{w}, \boldsymbol{z}) \tag{3.1}$$

whenever

$$Kx^g/y < w_j \leqslant z_j \leqslant y \quad (1 \leqslant j \leqslant k). \tag{3.2}$$

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

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

$$Kx^{g-1}/y < w_j \leqslant z_j \leqslant y \quad (1 \leqslant j \leqslant \ell), \quad Kx^g/y < w_m \leqslant z_m \leqslant y. \tag{3.3}$$

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

$$H_F(x; \boldsymbol{w}, \boldsymbol{z}) \gg x^2 \tag{3.4}$$

for

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

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

Let us first assume $\deg(F) \geqslant 4$. When $k \geqslant 2$, conditions (3.2) are fulfilled for $y = x^{\alpha_F + \varepsilon}$ with α_F as in Theorem 1, if δ is sufficiently small in terms of ε and k. The required lower bound hence follows from (3.1). When $k = 1, g \geqslant 3$, we arrive at the same conclusion by noting that (3.3) holds for small enough δ. In the case $k = 1$, $g = 2$, we have $\ell \geqslant 2$. Therefore $m \geqslant 3$, and so the first set of conditions in (3.3) holds for small enough δ. However, the inequality $z_m \leqslant y$ is not necessarily satisfied and we adapt the definition of $H_F(x; \boldsymbol{w}, \boldsymbol{z})$ 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 $\deg(F) \geqslant 4$), and prove (3.4) in this case. Let $\boldsymbol{w}, \boldsymbol{z}$ be as above. We observe that

$$B_F(a,b) := \prod_{1\leqslant j\leqslant m} \sum_{\substack{p_j \mid F_j(a,b)\\ w_j < p_j \leqslant z_j}} 1 \leqslant \left(\frac{\max_{1\leqslant j\leqslant m} \log(Kx^g)}{\log w_j}\right)^m \ll \left(\frac{m^2 g}{1-\delta(1+m^2)}\right)^m \tag{3.5}$$

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

$$H_F(x;\boldsymbol{w},\boldsymbol{z}) \gg \sum_{1\leqslant a,b\leqslant x} B_F(a,b) = \sum_{w_1 < p_1 \leqslant z_1} \cdots \sum_{w_m < p_m \leqslant z_m} \sum_{\substack{1\leqslant a,b\leqslant x\\ p_j \mid F_j(a,b)\ (1\leqslant j\leqslant m)}} 1. \tag{3.6}$$

Our choice of $\boldsymbol{z}$ guarantees that $z_1 \cdots z_m < x^{2-\eta}$ for sufficiently small $\eta > 0$. Moreover, the primes $p_1, \dots, p_m$ in (3.6) are distinct since $]w_j, z_j] \cap]w_h, z_h] = \varnothing$ if $j \neq h$. By Proposition 2 it follows that

$$H_F(x;\boldsymbol{w},\boldsymbol{z}) \gg x^2 \prod_{1\leqslant j\leqslant m} \sum_{w_j < p_j \leqslant z_j} \frac{\gamma_{F_j}(p_j)}{p_j^2} + O\big(x^{2-\eta/2}\big). \tag{3.7}$$

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

$$\sum_{w_j < p_j \leqslant z_j} \frac{\gamma_{F_j}(p_j)}{p_j^2} = \log\left(\frac{\log z_j}{\log w_j}\right) + O\left(\frac{1}{\log w_j}\right). \tag{3.8}$$

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 $\deg(F) \geqslant 4$), we replace the weights $B_F(a,b)$ by

$$B_F^*(a,b) := \Bigg(\sum_{\substack{s_m < p_m \leqslant t_m\\ u_m < q_m \leqslant v_m\\ p_m q_m \mid F_m(a,b)}} 1\Bigg) \prod_{1\leqslant j\leqslant \ell} \sum_{\substack{p_j \mid F_j(a,b)\\ w_j < p_j \leqslant z_j}} 1, \tag{3.9}$$

where p_j, q_m denote primes and

$$t_m = u_m := x^{\frac{1}{2}-\delta+(1-\delta)/(2m)}, \quad s_m := t_m x^{-\delta}, \quad v_m := u_m x^{\delta}.$$

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 other steps are as in the previous case. We have

$$\Psi_F(x,y) \gg \sum_{1\leqslant a,b\leqslant x} B_F^*(a,b) \gg \sum_{w_1 < p_1 \leqslant z_1} \cdots \sum_{\substack{s_m < p_m \leqslant t_m\\ u_m < q_m \leqslant v_m}} \sum_{\substack{1\leqslant a,b\leqslant x\\ p_j \mid F_j(a,b)\ (1\leqslant j\leqslant \ell)\\ p_m q_m \mid F_m(a,b)}} 1.$$

Applying Proposition 2 and using the fact that γ_{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 $\deg(F) \geqslant 4$.

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

$$B_F(a,b) := \sum_{\substack{p_1 p_2 | F(a,b) \\ x^{1-\delta} < p_1 \leqslant x \\ x^{1-2\delta} < p_2 \leqslant x^{1-\delta}}} 1.$$

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

$$B_F(a,b) := \sum_{p_1 | F_1(a,b)} 1 \sum_{p_2 q_2 | F_2(a,b)} 1,$$

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

$$x^{(1/3)-\delta} < p_1 \leqslant x^{1/3}, \quad x^{(2/3)-\delta} < p_2 \leqslant x^{2/3}, \quad x^{(2/3)-2\delta} < q_2 \leqslant x^{(2/3)-\delta}.$$

When $F = F_1 F_2 F_3$ is a product of three linear factors we select

$$B_F(a,b) := \prod_{1 \leqslant j \leqslant 3} \sum_{p_j q_j | F_j(a,b)} 1,$$

subject to the conditions $x^{(1/3)-(j-1/2)\delta} < p_j \leqslant x^{(1/3)-(j-1)\delta}$ and $x^{(1/3)-j\delta} < q_j \leqslant x^{(1/3)-(j-1/2)\delta}$.

(b) F is a quadratic form. When F is irreducible we take

$$B_F(a,b) := \sum_{\substack{x^{2-2\delta} < d \leqslant x^{2-\delta} \\ P^+(d) < y,\, P^-(d) > x^\eta \\ d | F(a,b)}} 1 \ll 2^{2/\eta},$$

where δ and η are sufficiently small parameters and x is sufficiently large. The lower bound

$$\sum_{\substack{x^{2-2\delta} < d \leqslant x^{2-\delta} \\ P^+(d) < y,\, P^-(d) > x^\eta \\ d | F(a,b)}} \frac{\gamma_F(d)}{d^2} \gg 1$$

is then derived from the inequality

$$\sum_{\substack{x^{2-2\delta}<d\leqslant x^{2-\delta}\\ P^+(d)<y,\, P^-(d)>x^\eta\\ d\mid F(a,b)}} \frac{\gamma_F(d)}{d^2} \geqslant \prod_{1\leqslant j\leqslant J} \sum_{x^{j\eta}<p_j\leqslant x^{(j+1)\eta}} \frac{\gamma_F(p_j)}{p_j^2},$$

where J is chosen in such a way that

$$2-2\delta < \tfrac{1}{2}J(J+1)\eta, \quad \tfrac{1}{2}J(J+3)\eta < 2-\delta.$$

This is indeed possible provided δ and η/δ 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. $F = F_1F_2$ 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

$$\gamma_F(p) < p^2 \tag{4.1}$$

for all p. Let $\mathscr{S}_0$ be the set of primes dividing the discriminant[3] or the leading coefficients of F, and let $\mathscr{S}$ denote the union of $\mathscr{S}_0$ and the set of those primes satisfying $\varrho_F(p) = 0$. Then $\mathscr{S}_0$ is a finite set depending only on F, and by Hensel's lemma we have

$$\varrho_F(p^2) \neq p\varrho_F(p) \tag{4.2}$$

for all $p \notin \mathscr{S}$. For this and the following sections we use the notation

$$\mathscr{P}_z := \prod_{p\leqslant z} p, \quad \mathscr{P}_z^* := \prod_{\substack{p\leqslant z\\ p\notin\mathscr{S}}} p, \quad \mathscr{P}_z^0 := \prod_{\substack{p\leqslant z\\ p\notin\mathscr{S}_0}} p$$

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 $P^+(uvw) \leqslant y$, $(uw, \mathscr{P}_z) = 1$, $2 \leqslant z \leqslant y \leqslant x$. We choose

$$z = x^\eta,$$

[3] The discriminant of F is in fact the discriminant of the polynomial $F(X,1)$.

a small power of x. Then any $F(a,b)$ has at most a bounded number of such factorizations. We are free to impose further conditions on v to make computations more comfortable. For example, we can provide $(uw,v)=1$ by requiring $P^+(v)\leqslant z$, and ease the application of multiplicativity by asking that v is square-free. For the application of the sieve, we shall also need to exclude a few bad primes from v, hence we require $v \mid \mathscr{P}_z^*$. In other words, u and w are free of prime factors below z or above y, while v is composed of some primes below z but not in $\mathscr{S}$. We will use three different levels of small parameters and put

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

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

$$\operatorname{card}\{1\leqslant a,b\leqslant x : P^+(F(a,b))\leqslant y\} \gg S := \sum_{\substack{1\leqslant a,b\leqslant x\\ |F(a,b)|=uvw\\ U/x^{\varepsilon}<u\leqslant U,\, V/x^{\delta}<v\leqslant V\\ P^+(uw)\leqslant y\\ (uw,\mathscr{P}_z)=1,\, v|\mathscr{P}_z^*}} 1.$$

This last sum counts all five-tuples (a,b,u,v,w) satisfying the long list of conditions. The condition $P^+(w)\leqslant y$ 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 $P^+(u)\leqslant y$ as we only need a lower bound. In other words

$$\begin{aligned} S \geqslant & \sum_{\substack{Ux^{-\varepsilon}<u\leqslant U\\ P^+(u)\leqslant y\\ (u,\mathscr{P}_z)=1}} \sum_{\substack{Vx^{-\delta}<v\leqslant V\\ v|\mathscr{P}_z^*}} \sum_{\substack{1\leqslant a,b\leqslant x\\ F(a,b)\equiv 0 \pmod{uv}\\ (F(a,b)/(uv),\mathscr{P}_z)=1}} 1 \\ & - \sum_{\substack{w\\ P^+(w)>y\\ (w,\mathscr{P}_z)=1}} \sum_{\substack{Vx^{-\delta}<v\leqslant V\\ v|\mathscr{P}_z^*}} \sum_{\substack{1\leqslant a,b\leqslant x\\ F(a,b)\equiv 0 \pmod{vw}\\ (F(a,b)/(vw),\mathscr{P}_z)=1\\ U/x^{\varepsilon}<|F(a,b)|/(vw)\leqslant U}} 1. \end{aligned} \tag{4.3}$$

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

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

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

$$\begin{aligned} &\ll \sum_{w\leqslant W_0} \sum_{\substack{v\leqslant V\\ (v,w)=1}} \sum_{\substack{|F(a,b)|\leqslant vwU\\ F(a,b)\equiv 0 \pmod{vw}}} 1 \\ &\ll \sum_{w\leqslant W_0} \sum_{v\leqslant V} \frac{\gamma_F(v)\gamma_F(w)(vwU)^{2/3}}{v^2w^2} + O(x^{\eta}(VW_0 + (UVW_0)^{1/3}(VW_0)^{1/2})) \\ &\ll (UVW_0)^{2/3} + x^{\eta}\{VW_0 + U^{1/3}(VW_0)^{5/6}\}. \end{aligned}$$

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

$$\begin{aligned} W = U :=& x^{1+\varepsilon+4\delta},\ U_0 := U/x^{\varepsilon}, \\ V :=& x^{1-\varepsilon-6\delta},\ V_0 := V/x^{\delta}, \\ W_0 :=& x^{1+\delta} = W/x^{\varepsilon+3\delta}. \end{aligned} \tag{4.4}$$

With these bounds we can drop the uncomfortable conditions on the size of $|F(a,b)|$ in the second term in (4.3). Next the conditions $(w, \mathscr{P}_z) = 1$ in the first term and $(u, \mathscr{P}_z) = 1$ in the second term can be controlled with a fundamental lemma type sieve. For a general formulation of a sieve method, see [HR]. There are sieving weights $\lambda_d^{\pm}$, supported on $d \leqslant D = x^{\delta}$, $d \mid \mathscr{P}_z$ such that $\sum_{d\mid n} \lambda_d^{\pm} \gtrless$ the characteristic function of $(n, \mathscr{P}_z) = 1$. Using these weights in the appropriate place we arrive at

$$\begin{aligned} S \geqslant & \sum_{\substack{U_0<u\leqslant U\\ P^+(u)\leqslant y\\ (u,\mathscr{P}_z)=1}} \sum_{\substack{V_0<v\leqslant V\\ v\mid\mathscr{P}_z^*}} \sum_{\substack{d\leqslant D\\ d\mid\mathscr{P}_z}} \lambda_d^- \sum_{\substack{1\leqslant a,b\leqslant x\\ F(a,b)\equiv 0 \pmod{uvd}}} 1 \\ & - \sum_{\substack{W_0<w\leqslant W\\ P^+(w)>y\\ (w,\mathscr{P}_z)=1}} \sum_{\substack{V_0<v\leqslant V\\ v\mid\mathscr{P}_z^*}} \sum_{\substack{d\leqslant D\\ d\mid\mathscr{P}_z}} \lambda_d^+ \sum_{\substack{1\leqslant a,b\leqslant x\\ F(a,b)\equiv 0 \pmod{vwd}}} 1 + O(x^{2-\eta}). \end{aligned}$$

At this stage, we derive from (2.2) the following relation

$$\begin{aligned} S \geqslant & \sum_{\substack{U_0<u\leqslant U\\ P^+(u)\leqslant y\\ (u,\mathscr{P}_z)=1}} \sum_{\substack{V_0<v\leqslant V\\ v\mid\mathscr{P}_z^*}} \sum_{\substack{d\leqslant D\\ d\mid\mathscr{P}_z}} \frac{\lambda_d^-\gamma_F(uvd)x^2}{(uvd)^2} \\ & - \sum_{\substack{W_0<w\leqslant W\\ P^+(w)>y\\ (w,\mathscr{P}_z)=1}} \sum_{\substack{V_0<v\leqslant V\\ v\mid\mathscr{P}_z^*}} \sum_{\substack{d\leqslant D\\ d\mid\mathscr{P}_z}} \frac{\lambda_d^+\gamma_F(vwd)x^2}{(vwd)^2} + O(x^{2-\eta}). \end{aligned} \tag{4.5}$$

We plainly have $(uw, vd) = 1$. Hence we have to compute

$$T^{\pm} := \sum_{\substack{V_0<v\leqslant V\\ v\mid\mathscr{P}_z^*}} \sum_{\substack{d\leqslant D\\ d\mid\mathscr{P}_z}} \frac{\lambda_d^{\pm}\gamma_F(vd)}{(vd)^2},$$

and (4.5) becomes

$$S \geqslant x^2T^- \sum_{\substack{U_0<u\leqslant U\\ P^+(u)\leqslant y\\ (u,\mathscr{P}_z)=1}} \frac{\gamma_F(u)}{u^2} - x^2T^+ \sum_{\substack{W_0<w\leqslant W\\ P^+(w)>y\\ (w,\mathscr{P}_z)=1}} \frac{\gamma_F(w)}{w^2} + O(x^{2-\eta}). \tag{4.6}$$

Remark. Although a big chunk of computation is still ahead, we have at this point a flash of the final result. Suppose that $y = x^{\vartheta}$. Since $z = x^{\eta} = D^{\varepsilon}$, we expect that, for suitable constants $c > 0$, $\kappa(\varepsilon)$, we have

$$T^- \sim T^+ \sim \frac{c}{\log z} \sum_{\substack{V_0 < v \leqslant V \\ v \mid \mathscr{P}_z^*}} \frac{\gamma_F(v)}{v^2} \sim \kappa(\varepsilon) > 0.$$

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

$$\sum_{v \mid \mathscr{P}_z^*} \frac{\gamma_F(v)}{v^2} \asymp \log z.$$

Bearing in mind that $\gamma_F(q)/q$ is 1 on average, we similarly expect that, with a suitable constant $b > 0$, we have

$$\sum_{\substack{U_0 < u \leqslant U \\ P^+(u) \leqslant y \\ (u, \mathscr{P}_z) = 1}} \frac{\gamma_F(u)}{u^2} \sim b\Big(1 - \log\Big(\frac{\log U}{\log y}\Big)\Big)\frac{\log(U/U_0)}{\log z} \sim \frac{b}{\varepsilon^2}\Big(1 - \log\frac{1}{\vartheta}\Big),$$

and, much in the same way,

$$\sum_{\substack{W_0 < w \leqslant W \\ P^+(w) > y \\ (w, \mathscr{P}_z) = 1}} \frac{\gamma_F(w)}{w^2} \sim b \log\Big(\frac{\log W}{\log y}\Big)\frac{\log(W/W_0)}{\log z} \sim \frac{b}{\varepsilon^2}\log\frac{1}{\vartheta}.$$

Finally these expectations lead to

$$S \geqslant \Big\{1 - 2\log\frac{1}{\vartheta} + o(1)\Big\}\frac{b\kappa(\varepsilon)x^2}{\varepsilon^2}.$$

This exceeds a positive constant times x^2 precisely when $\vartheta > 1/\sqrt{\mathrm{e}}$.

4.2. Estimation of the main term. We return to (4.6). For any fixed $v \mid \mathscr{P}_z^*$ we note that $\gamma_F(v) \neq 0$ by (2.4) and (4.2), and we define

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

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 $v \mid \mathscr{P}_z^*$, as it is not true for $\varrho_F(p) = 0,\ p \mid v$, 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 μ_p for the p-adic valuation of m, we have

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

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

$$\begin{aligned} T^\pm &= \sum_{\substack{V_0 < v \leqslant V \\ v \mid \mathscr{P}_z^*}} \frac{\gamma_F(v)}{v^2} \sum_{\substack{d \leqslant D \\ d \mid \mathscr{P}_z}} \frac{\lambda_d^\pm g_v(d)}{d} \\ &= \sum_{\substack{V_0 < v \leqslant V \\ v \mid \mathscr{P}_z^*}} \frac{\gamma_F(v)}{v^2} \Big\{1 + O\big(\mathrm{e}^{-(\log D)/\log z}\big)\Big\} \prod_{p \leqslant z} \Big(1 - \frac{g_v(p)}{p}\Big) \\ &= \Big\{1 + O\big(\mathrm{e}^{-1/\varepsilon}\big)\Big\} \prod_{p \leqslant z} \Big(1 - \frac{\gamma_F(p)}{p^2}\Big) \sum_{\substack{V_0 < v \leqslant V \\ v \mid \mathscr{P}_z^*}} \frac{\gamma_F^*(v)}{v^2}, \end{aligned}$$

where, for shorter reference we have written

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

This is still a multiplicative function. Note that by (2.4) we have $\gamma_F^*(p) = 0$ if $\varrho_F(p) = 0$, 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 $\mathscr{S}_0$, that is

$$T^\pm = \Big\{1 + O\big(\mathrm{e}^{-1/\varepsilon}\big)\Big\} \prod_{p \leqslant z} \Big(1 - \frac{\gamma_F(p)}{p^2}\Big) \sum_{\substack{V_0 < v \leqslant V \\ v \mid \mathscr{P}_z^0}} \frac{\gamma_F^*(v)}{v^2}.$$

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

$$\{1 + o(1)\}\mathrm{e}^{-\gamma} \int_{(1-\varepsilon-7\delta)/\varepsilon^3}^{(1-\varepsilon-6\delta)/\varepsilon^3} \varrho(t)\,\mathrm{d}t \prod_{p \mid \mathscr{P}_z^0} \Big(1 + \frac{\gamma_F^*(p)}{p^2}\Big) = \{\kappa_0(\varepsilon) + o(1)\}\log z,$$

say.

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

$$\begin{aligned} S &\geqslant \{1 + O(\mathrm{e}^{-1/\varepsilon})\} x^2 \kappa(\varepsilon) \Bigg(\sum_{\substack{U_0 < u \leqslant U \\ P^+(u) \leqslant y \\ (u, \mathscr{P}_z) = 1}} \frac{\gamma_F(u)}{u^2} - \sum_{\substack{W_0 < w \leqslant W \\ P^+(w) > y \\ (w, \mathscr{P}_z) = 1}} \frac{\gamma_F(w)}{w^2} \Bigg) + O(x^{2-\eta}) \\ &\geqslant \{1 + O(\mathrm{e}^{-1/\varepsilon})\} x^2 \kappa(\varepsilon) \Bigg(\sum_{\substack{U_0 < u \leqslant U \\ (u, \mathscr{P}_z) = 1}} \frac{\gamma_F(u)}{u^2} - 2 \sum_{\substack{W_0 < w \leqslant W \\ P^+(w) > y \\ (w, \mathscr{P}_z) = 1}} \frac{\gamma_F(w)}{w^2} \Bigg) + O(x^{2-\eta}), \end{aligned} \tag{4.8}$$

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 $D = x^\delta$, $z = x^\eta = D^\varepsilon$. From Proposition 1, we obtain

$$\sum_{\substack{n \leqslant \xi \\ (n, \mathscr{P}_z) = 1}} \frac{\gamma_F(n)}{n} = \{1 + O(\mathrm{e}^{-1/\varepsilon})\} \frac{\xi}{\log z},$$

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

$$\sum_{\substack{n \leqslant \xi \\ (n, \mathscr{P}_z) = 1}} \frac{\gamma_F(n)}{n} \ll \frac{\xi}{\log z} + 1$$

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

$$\sum_{\substack{U_0 < u \leqslant U \\ (u, \mathscr{P}_z) = 1}} \frac{\gamma_F(u)}{u^2} = \{1 + O(\mathrm{e}^{-1/\varepsilon})\} \frac{\log(U/U_0)}{\log z},$$

and

$$\begin{aligned} \sum_{\substack{W_0 < w \leqslant W \\ P^+(w) > y \\ (w, \mathscr{P}_z) = 1}} \frac{\gamma_F(w)}{w^2} &= \sum_{y < p \leqslant W} \frac{\gamma_F(p)}{p^2} \sum_{\substack{W_0/p < w \leqslant W/p \\ (w, \mathscr{P}_z) = 1}} \frac{\gamma_F(w)}{w^2} \\ &= \sum_{y < p \leqslant W} \frac{\gamma_F(p)}{p^2} \{1 + O(\mathrm{e}^{-1/\varepsilon})\} \frac{\log(W/W_0)}{\log z} \\ &= \{1 + O(\varepsilon)\} \log\left(\frac{\log W}{\log y}\right) \frac{\log(W/W_0)}{\log z}. \end{aligned}$$

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

$$\begin{aligned} S &\geqslant \{1 + O(\mathrm{e}^{-1/\varepsilon})\} x^2 \kappa(\varepsilon) \left(\frac{\log(U/U_0)}{\log z} - 2\log\left(\frac{\log W}{\log y}\right) \frac{\log(W/W_0)}{\log z} \right) \\ &\qquad + O(x^{2-\eta}) \\ &= \{1 + O(\mathrm{e}^{-1/\varepsilon})\} \left\{ \varepsilon - 2(\varepsilon + 3\delta) \log\left(\frac{1+\varepsilon+4\delta}{\vartheta}\right) \right\} \frac{\kappa(\varepsilon)}{\varepsilon^3} x^2 + O(x^{2-\eta}) \\ &\geqslant \left\{ 1 - 2\log\frac{1}{\vartheta} + O(\varepsilon) \right\} \frac{\kappa(\varepsilon)}{\varepsilon^2} x^2 + O(x^{2-\eta}). \end{aligned}$$

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

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

say F_1 and F_2, are linearly independent over $\mathbb{Q}$. Let $A = \left(\begin{smallmatrix} \alpha_1 & \beta_1 \\ \alpha_2 & \beta_2 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Q})$, and set $\Delta := \det A \neq 0$. If we write $r = F_1(a,b)$, $s = F_2(a,b)$, then $\left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right) = A \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$, and therefore

$$F_3(a,b) = \alpha_3' r + \beta_3' s, \quad \text{where} \quad (\alpha_3',\, \beta_3') := (\alpha_3,\, \beta_3) A^{-1} \in \left(\frac{1}{\Delta}\mathbb{Z}\right)^2.$$

Thus

$$S := \mathrm{card}\{(r,s) : \Delta \mid r, \Delta \mid s, A^{-1} \left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right) \in [1,x]^2, P^+(rs(\alpha_3' r + \beta_3' s)) \leqslant y\}$$

is a lower bound for the number of $1 \leqslant a, b \leqslant x$ 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

$$\mathscr{A} := \{\alpha_3' r : r \in [c_1 x, c_2 x], \Delta \mid r, P^+(r) \leqslant y\}$$

and

$$\mathscr{B} := \{\beta_3' s : s \in [c_3 x, c_4 x], \Delta \mid s, P^+(s) \leqslant y\}.$$

Then $|\mathscr{A}| \cdot |\mathscr{B}| \gg x^2$ and $\mathscr{A}, \mathscr{B} \subseteq [-c_5 x, c_5 x]$ 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 $\mathscr{A}, \mathscr{B} \subseteq \mathbb{Z}$, not only for $\mathscr{A}, \mathscr{B} \subseteq \mathbb{N}$), we obtain

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

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

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

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 α_1 and β_1 are 0, we can assume that $\alpha_1 \neq 0$. Let $A = \left(\begin{smallmatrix} \alpha_1 & \beta_1 \\ 0 & 1 \end{smallmatrix}\right)$, and change variables $\left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right) := A \left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right)$. Then

$$\alpha_1^2 F_2(a,b) = \alpha r^2 + \beta rs + \gamma s^2 =: \widetilde{F}(r,s)$$

where $\alpha = \alpha_2 \neq 0, \beta = \alpha_1\beta_2 - 2\beta_1\alpha_2, \gamma = \beta_1^2\alpha_2 - \beta_1\beta_2\alpha_1 + \gamma_2\alpha_1^2$, and the discriminant of $\widetilde{F}$ is $\widetilde{\Delta} := \alpha_1^2\Delta$. By the same argument as above,

$$\operatorname{card}\left\{(r,s) : r \equiv \beta_1 s \pmod{\alpha_1},\ A^{-1}\left(\begin{smallmatrix} r \\ s \end{smallmatrix}\right) \in [1,x]^2,\ P^+(r\,\widetilde{F}(r,s)) \leqslant y\right\}$$

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

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

for suitable constants $c_1 < c_2, c_3 < c_4$, and by changing the sign of the middle term of $\widetilde{F}$ if necessary, we can assume that $c_1, \dots, c_4 > 0$. 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 $\int_I f(t)\,\mathrm{d}t = c_0 x$ 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

$$\gg \sum_{\substack{x^{-\varepsilon/20} D \leqslant d \leqslant D \\ (d, \mathscr{P}_z) = 1 \\ P^+(d) \leqslant y}} \sum_{\substack{c_1 x \leqslant r \leqslant c_2 x \\ P^+(r) \leqslant z}} \sum_{\widetilde{F}(r,s) \equiv 0 \pmod{d}} f(s), \tag{5.1}$$

since there is only a bounded number of ways to write $\widetilde{F}(r,s) = dd'$ with d as required in the summation condition, and all pairs (r,s) of this form yield a y-friable

value of $\widetilde{F}(r,s)$. We transform the innermost sum by splitting s into residue classes modulo d and applying Poisson summation. In this way we obtain

$$\sum_{\widetilde{F}(r,s)\equiv 0 \pmod d} f(s) = \sum_{\substack{s \pmod d \\ \widetilde{F}(r,s)\equiv 0 \pmod d}} \frac{1}{d} \sum_{h\in\mathbb{Z}} \mathrm{e}\Big(\frac{hs}{d}\Big) \hat{f}\Big(\frac{h}{d}\Big)$$

where

$$\hat{f}(z) := \int_{-\infty}^{\infty} f(t)\mathrm{e}(-zt)\,\mathrm{d}t \ll \frac{x}{(1+|z|x)^A} \tag{5.2}$$

for any $A \geqslant 0$ (after $[A]+1$ partial integrations), and $\hat{f}(0) = c_0 x$. Let

$$\gamma_{h,r}(d) := \sum_{\substack{s \pmod d \\ d \mid \widetilde{F}(r,s)}} \mathrm{e}\Big(\frac{hs}{d}\Big). \tag{5.3}$$

The term $h = 0$ will contribute the main term

$$M := c_0 x \sum_{\substack{D/x^{\varepsilon/20} \leqslant d \leqslant D \\ (d,\mathscr{P}_z)=1 \\ P^+(d)\leqslant y}} \frac{1}{d} \sum_{\substack{c_1 x \leqslant r \leqslant c_2 x \\ P^+(r)\leqslant z}} \gamma_{0,r}(d) \tag{5.4}$$

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

$$E := \sum_{h\neq 0} \sum_{\substack{x^{-\varepsilon/20} D \leqslant d \leqslant D \\ (d,\mathscr{P}_z)=1 \\ P^+(d)\leqslant y}} \frac{1}{d} \sum_{\substack{c_1 x \leqslant r \leqslant c_2 x \\ P^+(r)\leqslant z}} \gamma_{h,r}(d) \hat{f}\Big(\frac{h}{d}\Big),$$

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

$$\begin{aligned} E &\leqslant \sum_{D/x^{\varepsilon/20}\leqslant d\leqslant D} \frac{1}{d} \int_{-\infty}^{\infty} \Big| \sum_{0<|h|\leqslant H} \frac{H}{h} f\Big(\frac{H\tau}{h}\Big) \sum_{\substack{c_1 x \leqslant r \leqslant c_2 x \\ P^+(r)\leqslant z}} \gamma_{h,r}(d) \Big| \,\mathrm{d}\tau + O\Big(\frac{1}{x}\Big) \\ &= \sum_{D/x^{\varepsilon/20}\leqslant d\leqslant D} \frac{1}{d} \int_{-c_4 x}^{c_4 x} \Big| \sum_{\substack{H|\tau|/(c_4 x) < |h| \leqslant H|\tau|/(c_3 x) \\ \tau h > 0}} \frac{H}{h} f\Big(\frac{H\tau}{h}\Big) \\ &\qquad\qquad \sum_{\substack{c_1 x \leqslant r \leqslant c_2 x \\ P^+(r)\leqslant z}} \gamma_{h,r}(d) \Big| \,\mathrm{d}\tau + O\Big(\frac{1}{x}\Big). \end{aligned} \tag{5.5}$$

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

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 $\breve{F}$ replaced by F. For any sequence $\xi_{h,r}$ of complex numbers, positive real numbers D, H, R, and any $\delta > 0$, we have*

$$\sum_{d\leqslant D}\Big|\sum_{h\leqslant H}\sum_{r\leqslant R}\xi_{h,r}\gamma_{h,r}(d)\Big| \ll_{\delta,F} D^{1/2}(D+HR)^{1/2}\Big(\sum_{h,r}|\xi_{h,r}|^2\Big)^{1/2}(DHR)^{\delta}.$$

We postpone the proof of this estimate to the next section and proceed with bounding the error term (5.5). This is

$$\ll \frac{x^{\varepsilon/20}}{D}HD^{1/2}(Hx)^{1/2}\int_{-c_4x}^{c_4x}\Big(\frac{Rx}{H\tau}\Big)^{1/2}\,\mathrm{d}\tau(DHR)^{\delta} \ll \frac{x^{\varepsilon/20}x^{4\delta}HR^{1/2}x^{3/2}}{D^{1/2}} = x^{2-\varepsilon/60}$$

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 $\gamma_{0,r}(d) =: g(d)$ is independent of r. It therefore remains to show that

$$\sum_{\substack{D/x^{\varepsilon/20}\leqslant d\leqslant D\\(d,\mathscr{P}_z)=1\\P^+(d)\leqslant y}}\frac{g(d)}{d} \geqslant c(\varepsilon) > 0 \tag{5.6}$$

for some constant $c(\varepsilon)$. For a prime $p \nmid 2\alpha\widetilde{\Delta}$ we have $g(p) = 1 + (\widetilde{\Delta}|p) \in \{0,2\}$ which depends only on p modulo $\widetilde{\Delta}$. Let $\sum_p^*$ denote a sum over primes satisfying $g(p) = 2$. For such primes, we have $g(p^\nu) \geqslant 2$ for all integers $\nu \geqslant 1$. Let

$$\frac{\varepsilon}{80} < \varepsilon_0 := \frac{\varepsilon}{40}\Big(\frac{40-11\varepsilon}{40-10.5\varepsilon}\Big) < \frac{\varepsilon}{40},\quad \mathscr{I} := [x^{\varepsilon_0}, x^{\varepsilon/40}],\quad k := \Big[\frac{80}{\varepsilon} - 20\Big] \in \mathbb{N}.$$

Note that $x^{k\varepsilon/40} \leqslant x^{2-\varepsilon/2} = D$ and $x^{k\varepsilon_0} \geqslant x^{2-11\varepsilon/20} = Dx^{-\varepsilon/20}$. Thus the left hand side of (5.6) can be bounded below by

$$\Big(\sum_{p\in\mathscr{I}}{}^*\frac{1}{p}\Big)^k \geqslant c(\varepsilon).$$

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 $\nu/d \pmod 1$, where $d \sim D$ and ν runs through the solutions of $F(\nu, 1) \equiv 0 \pmod d$; 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[4]

$$\{\nu \pmod d : F(\nu, 1) \equiv 0 \pmod d\}$$

and

$$\{(\nu, k) \in (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z} : (2\alpha\nu + \beta)^2 - 4\alpha d k = \Delta\},$$

and the latter set can be identified with the set of (not necessarily primitive) integral quadratic forms

$$\begin{aligned}\{aX^2 + bXY + dY^2 : b^2 - 4ad = \Delta,\ a \equiv 0 \pmod\alpha,\\ b \pmod{2\alpha d},\ b \equiv \beta \pmod{2\alpha}\},\end{aligned} \tag{5.7}$$

via

$$a = \alpha k \quad \text{and} \quad b = 2\alpha\nu + \beta. \tag{5.8}$$

The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of all integral binary quadratic forms $\mathcal{F}(\Delta)$ of discriminant Δ: if $\sigma = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ 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

$$a^\sigma = Q(r,s), \quad b^\sigma = 2art + bru + bst + 2csu, \quad c^\sigma = Q(t,u).$$

It is known that $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{F}(\Delta) = \{Q_1, \dots, Q_h\}$ is finite. For each representative $Q_j = a_j X^2 + b_j XY + c_j Y^2$, say, let $\mathscr{S}_j(d)$ be the set of matrices $\sigma = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that Q_j^σ contributes to (5.7). Clearly we must have $Q_j(t,u) = d$. The set $\mathcal{O}(Q_j) := \{\sigma \in \mathrm{SL}_2(\mathbb{Z}) : Q_j^\sigma = Q_j\}$ of automorphisms of Q_j acts on $\mathscr{S}_j(d)$, 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 ν/d is of the form

$$\frac{\nu}{d} = \frac{b_j^\sigma - \beta}{2\alpha d} = \frac{2a_j rt + b_j(ru + st) + 2c_j su - \beta}{2\alpha Q_j(t,u)}, \tag{5.9}$$

with $1 \leqslant j \leqslant h$, $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \in \mathscr{S}_j(d)$. We claim that for each $\sigma = \left(\begin{smallmatrix} * & * \\ t & u \end{smallmatrix}\right) \in \mathscr{S}_j(d)$ there is a representative modulo $\mathcal{O}(Q_j)$ such that $t, u \ll \sqrt{d}$. Indeed, if $\Delta < 0$, then

[4] For the second set, we have identified (non-canonically) the pairs $(\nu, k) \in [0, d[\times\mathbb{Z}$ such that

$$(2\alpha\nu + \beta)^2 - 4\alpha d k = \Delta$$

with the pairs $(\nu, k) \in (\mathbb{Z}/d\mathbb{Z}) \times \mathbb{Z}$ satisfying this equation.

$\left(\begin{smallmatrix} * & * \\ t & u \end{smallmatrix}\right) \in \mathscr{S}_j(d)$ implies $(2a_jt + b_ju)^2 - \Delta u^2 = 4a_jd$, and the claim is obvious. If $\Delta > 0$, we can assume that Q_j is a primitive form (otherwise divide everything by the gcd of the coefficients). Then it is known [La] that $\mathcal{O}(Q_j)$ is generated by $-I = \left(\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right)$ and $\sigma_0 := \left(\begin{smallmatrix} (\xi - b_j\eta)/2 & -c_j\eta \\ a_j\eta & (\xi + b_j\eta)/2 \end{smallmatrix}\right)$ 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 $\left(\begin{smallmatrix} * & * \\ t & u \end{smallmatrix}\right) \in \mathscr{S}_j(d)$, 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 $ru - st = 1$)

$$\frac{\nu}{d} = \frac{r}{\alpha t} - \frac{b_jt + 2c_ju + \beta t}{2\alpha t Q_j(t, u)} = \frac{r}{\alpha t} + O\left(\frac{1}{d}\right) \tag{5.10}$$

where[5] $r \equiv \bar{u} \pmod{|t|}$, and we can assume $r \ll |t| \ll \sqrt{d}$. Analogously, if $|u| > |t|$, we obtain the expression

$$\frac{\nu}{d} = \frac{s}{\alpha u} - \frac{a_jt + 2b_ju + \beta t}{2\alpha u Q_j(t, u)} = \frac{s}{\alpha u} + O\left(\frac{1}{d}\right)$$

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

$$\left\{\frac{\nu}{d} \pmod 1 : F(\nu, 1) \equiv 0 \pmod d, D \leqslant d \leqslant 2D\right\}$$

into $2h$ classes $\mathcal{C}_i$, $1 \leqslant i \leqslant 2h$, according to the representative Q_j, $1 \leqslant j \leqslant h$, in (5.9) and according to $|t| > |u|$ or $|u| > |t|$, and we consider one of these classes $\mathcal{C}_i$ with, say, $|t| > |u|$. If $\left(\begin{smallmatrix} r & * \\ t & * \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ is any matrix, there are at most two choices for $\left(\begin{smallmatrix} s \\ u \end{smallmatrix}\right)$ with $|t| > |u|$. Hence we can partition $\mathcal{C}_i$ into a bounded number of subclasses $\mathcal{C}_{i,k}$, $k \ll 1$, such that the fractions $\nu/d \in \mathcal{C}_{i,k}$ correspond to matrices $\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ with different values of $r/(\alpha t) \pmod 1$. We consider one such subclass and order the fractions $\nu/d \in \mathcal{C}_{i,k}$, viewed as elements of $[0, 1[$, in ascending order:

$$\frac{\nu_1}{d_1} \leqslant \frac{\nu_2}{d_2} \leqslant \cdots.$$

Since

$$0 \neq \left|\frac{r_1}{\alpha t_1} - \frac{r_2}{\alpha t_2}\right| \geqslant \frac{1}{\alpha t_1 t_2} \gg \frac{1}{D}, \tag{5.11}$$

for two matrices $\left(\begin{smallmatrix} r_1 & * \\ t_1 & * \end{smallmatrix}\right), \left(\begin{smallmatrix} r_2 & * \\ t_2 & * \end{smallmatrix}\right)$ corresponding to two members in $\mathcal{C}_{i,k}$, there is a constant $L \in \mathbb{N}$ large enough in terms of the implicit constants in (5.10) and (5.11) such that

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

[5] Here we note that $u = 0$ can only happen when $t = 1$, and we interpret $\bar{0} := 0 \pmod 1$.

for all $\ell \in \mathbb{N}$. Once again we partition $\mathcal{C}_{i,k}$ into a bounded number of subclasses such that any two fractions $v/d, v'/d'$ in a given subclass satisfy

$$\left\| \frac{v}{d} - \frac{v'}{d'} \right\| \gg \frac{1}{D}.$$

Applying the classical large sieve inequality (see e.g. [S]) for each subclass separately we conclude

$$\sum_{D \leqslant d \leqslant 2D} \sum_{F(v,1) \equiv 0 \,(d)} \left| \sum_{n \leqslant N} \varrho_n \mathrm{e}\left(\frac{vn}{d}\right) \right|^2 \ll (D+N) \sum_{n \leqslant N} |\varrho_n|^2$$

for any sequence ϱ_n. Now we are exactly in the situation of Lemma 2 in [FI], and verbatim as in [FI], pp. 252–254, we derive the proposition.

References

[BW] A. Balog and T. Wooley, Sums of two squares in short intervals. *Canad. J. Math.* **52** (2000), 673–694 Zbl 0961.11030 MR 1767398

[Br] R. de la Bretèche, Sommes sans grand facteur premier. *Acta Arith.* **88** (1999), 1–14. Zbl 0935.11031 MR 1698349

[CP] R. Crandall and C. Pomerance, *Prime numbers, a computational perspective.* Springer-Verlag, New York 2001. Zbl 0995.11072 MR 1821158

[Dan] S. Daniel, On the divisor-sum problem for binary forms. *J. Reine Angew. Math.* **507** (1999), 107–129. Zbl 0913.11041 MR 1670278

[Dar] C. Dartyge, Propriétés multiplicatives des valeurs de certains polynômes en deux variables. *Acta Arith.* **58** (1996), 37–74. Zbl 0869.11070 MR 1425000

[DMT] C. Dartyge, G. Martin and G. Tenenbaum, Polynomial values free of large prime factors. *Acta. Math. Hung.* **43** (2001), 111–119. Zbl 0980.11041 MR 1830570

[FI] E. Fouvry and H. Iwaniec, Gaussian primes. *Acta Arith.* **79** (1997), 249–287. Zbl 0881.11070 MR 1438827

[Gr] A. Granville, Smooth numbers: Computational number theory and beyond. In *Algorithmic number theory: lattices, number fields, curves and cryptography*. Math. Sci. Res. Inst. Publ. 44, Cambridge University Press, Cambridge 2008, 267–323. Zbl 1230.11157 MR 2467549

[G1] G. Greaves, On the divisor-sum problem for binary cubic forms. *Acta Arith.* **17** (1970), 1–28. Zbl 0198.37903 MR 0263761

[G2] G. Greaves, Large prime factors of binary forms. *J. Number Theory* **3** (1971), 35–59. Zbl 0214.30301 MR 0271026

[HR] H. Halberstam and H. E. Richert, *Sieve methods*. London Math. Soc. Monogr. 4, Academic Press, London 1974. Zbl 0298.10026 MR 0424730

[HTW] G. Hanrot, G. Tenenbaum and J. Wu, Moyennes de certaines fonctions multiplicatives sur les entiers friables, 2. *Proc. Lond. Math. Soc.* **96** (2008), 107–135. Zbl 1195.11129 MR 2392317

[Ho] C. Hooley, On the greatest prime factor of a quadratic polynomial. *Acta Math.* **117** (1967), 281–299. Zbl 0146.05704 MR 0204383

[La] E. Landau, *Elementary number theory*. Chelsea, New York 1958. Zbl 0079.06201 MR 0092794

[Mo] P. Moree, On the number of y-smooth natural numbers $\leqslant x$ representable as a sum of two integer squares. Manuscripta Math. **80** (1993), 199–211 Zbl 0791.11046 MR 1233481

[S] A. Selberg, Lectures on sieves. *Collected papers*, Vol. II, Springer-Verlag, Berlin 1991. Zbl 0729.11001 MR 1295844

[T1] G. Tenenbaum, Sur une question d'Erdős et Schinzel. In *A tribute to Paul Erdős*, Cambridge University Press, Cambridge 1990, 405–443. Zbl 0713.11069 MR 1117034

[T2] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*. Cambridge Stud. Adv. Math. 46, Cambridge University Press, Cambridge 1995. Zbl 0831.11001 MR 1342300

[TW1] G. Tenenbaum and J. Wu, Moyennes de certaines fonctions multiplicatives sur les entiers friables. *J. Reine Angew. Math.* **564** (2003), 119–166 Zbl 1195.11132 MR 2021037

[TW2] G. Tenenbaum and J. Wu, Moyennes de certaines fonctions multiplicatives sur les entiers friables, 3. *Compositio Math.* **144** (2008), no. 2, 339–376. Zbl 1168.11043 MR 2406116

[To] A. Tóth, Roots of quadratic congruences. *Internat. Math. Res. Notices* **2000** (2000), no. 14, 719–739. Zbl 1134.11339 MR 1776618

Received September 8, 2009

Antal Balog, Alfréd Rényi Institute of Mathematics, Hungarian Academy of Sciences, POB 127, Budapest 1364, Hungary

E-mail: balog@renyi.hu

Valentin Blomer, Mathematisches Institut, Universität Göttingen, Bunsenstr. 3–5, 37073 Göttingen, Germany

E-mail: blomer@uni-math.gwdg.de

Cécile Dartyge, Institut Élie Cartan, Université Henri Poincaré Nancy 1, BP 239, 54506 Vandœuvre Cedex, France

E-mail: cecile.dartyge@iecn.u-nancy.fr

Gérald Tenenbaum, Institut Élie Cartan, Université Henri Poincaré Nancy 1, BP 239, 54506 Vandœuvre Cedex, France

E-mail: gerald.tenenbaum@iecn.u-nancy.fr