ACTA ARITHMETICA
124.4 (2006)

On the representation of almost primes by pairs of quadratic forms

by

Gihan Marasingha (Oxford)

1. INTRODUCTION

An integer is said to be an *almost prime of order* r, and is denoted P_r, if it is the product of at most r (not necessarily distinct) prime factors. Schinzel's celebrated hypothesis H may be reformulated in the language of almost primes as follows:

Hypothesis H. *Let* $F_1, \ldots, F_n$ *be irreducible polynomials over the integers such that the product* $F := F_1 \cdots F_n$ *has no fixed prime divisor* (*that is*, *there does not exist a prime* p *such that* $F(x) \equiv 0 \pmod{p}$ *for all* $x \in \mathbb{N}$). *Then there exist infinitely many* $x \in \mathbb{N}$ *such that* $F(x) = P_n$.

The only verified case is that of one linear polynomial. This is Dirichlet's theorem on arithmetic progressions. As far as quadratic polynomials are concerned, one of the best results is due to Iwaniec [9], who modified a weighted linear sieve of Richert to demonstrate that $x^2+1 = P_2$ for infinitely many x.

It has been known since the time of Dirichlet which binary quadratic forms represent primes; see the books by Buell [1] and Cox [2], for example. However the situation for pairs of forms appears to be completely open. In this paper, we investigate an approximation to Schinzel's hypothesis for the case $n = 2$. The result we achieve involves binary quadratic forms rather than polynomials, and we shall show that the product of the forms is P_5 for infinitely many values of the variables, as opposed to the P_2 result predicted by Schinzel's hypothesis. Our present theorem is an improvement on Diamond and Halberstam's P_7 result for quadratic polynomials, a special case of a result in [5]. To be precise, our main theorem is the following:

2000 *Mathematics Subject Classification*: Primary 11N36; Secondary 11N05.

This paper was written with the support of an EPSRC studentship, award number 00801473.

THEOREM 1.1. *Let* $q_i(x,y) := a_i x^2 + 2b_i xy + c_i y^2$ *for* $i = 1,2$ *be irreducible quadratic forms over the integers such that* $a_i \equiv 1 \pmod 4$. *Let* δ_i *be the discriminant of the form* q_i. *Let* $D := 6\,\mathrm{Res}(q_1,q_2)a_1a_2c_1c_2\delta_1\delta_2$, *where* $\mathrm{Res}(q_1,q_2)$ *is the resultant of the forms* q_1 *and* q_2. *If* $D \neq 0$ *and if there exists* $\mathbf{z} \in \mathbb{Z}^2$ *such that* $(q_i(\mathbf{z}); D) = 1$ *for* $i = 1,2$, *then there exist infinitely many pairs* $(x,y) \in \mathbb{Z}^2$ *such that*

$$q_1(x,y)q_2(x,y) = P_5.$$

Moreover, if $\mathcal{R}^{(0)}$ *is a convex subset of* $\mathbb{R}^2$ *with piecewise continuously differentiable boundary, then there exists a positive absolute constant* $\beta < 1$ *such that for all sufficiently large* X,

$$\#\{(x,y) \in X\mathcal{R}^{(0)} : q_1(x,y)q_2(x,y) = P_5\} \gg X^2 \prod_{p<X^\beta} \left(1 - \frac{\omega(p)}{p}\right),$$

where the implied constant depends at most on the forms q_1 *and* q_2, *and on the region* $\mathcal{R}^{(0)}$; *and where*

$$\omega(p) = 2 + \chi_1(p) + \chi_2(p) - (1 + \chi_1(p) + \chi_2(p))/p,$$

the characters χ_1 *and* χ_2 *defined by* $\chi_i(p) := \left(\frac{\delta_i}{p}\right)$.

Our principal external tool will be a multi-dimensional sieve of Diamond and Halberstam [5], a special case of which is presented as Theorem 3.1 in the present work. The most exacting aspect of our almost-primes problem is the derivation of an upper bound for the error term $\sum |R_d|$ which appears in Diamond and Halberstam's sieve. We devote Section 2 to the necessary groundwork. In doing so, we develop a "level of distribution" formula which is strongly related to the sum of the $|R_d|$. Similar formulæ have been applied by Heath-Brown [6], Daniel [3], and others in the investigation of asymptotic formulæ for the number of points of bounded height on given varieties.

We shall use the following standard notation: $d(n)$ is the number of positive divisors of n; $\phi(n)$ is the number of nonnegative integers less than and prime to n; $\mu(n)$ is the Möbius function; $\nu(n)$ is the number of distinct prime factors of n; and $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. We will use the symbol C to denote a positive numerical constant, though its value may vary in the course of a proof.

2. THE LEVEL OF DISTRIBUTION

In our application of Diamond and Halberstam's sieve, we shall encounter a sum over error terms $|R_d|$, which we will be able to relate to quantities of the form

$$\#(\Lambda^*_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) - \frac{\varrho^*(d_1,d_2)}{(d_1d_2D)^2}\,\mathrm{vol}(\mathcal{R}),$$

where $\Lambda^*_{\mathbf{d}}$ is a lattice-like object, and $(d_1d_2)^2/\varrho^*(d_1,d_2)$ plays a rôle similar to the determinant of the lattice. Naturally, we wish to derive a good upper bound for the error term involved. In the language of sieve theory, such a result is often referred to as a "level of distribution formula".

The sets $\Lambda_{\mathbf{d}}$ and $\Lambda^*_{\mathbf{d}}$ which we are concerned with are as follows:

$$\begin{aligned} \Lambda_{\mathbf{d}} &:= \{\mathbf{x} \in \mathbb{Z}^2 : d_i \mid q_i(\mathbf{x}) \ (i = 1,2)\}, \\ \Lambda^*_{\mathbf{d}} &:= \{\mathbf{x} \in \Lambda_{\mathbf{d}} : (\mathbf{x}; d_1d_2) = 1\}, \end{aligned} \tag{1}$$

where we use $(a;b)$ to denote the highest common factor of a and b.

A technicality arises due to problems for those $\mathbf{x}$ such that $(q_i(\mathbf{x}); D) > 1$, with D as in Theorem 1.1. This leads us to consider the set

$$\Psi := \{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv \mathbf{z} \ (\mathrm{mod}\, D)\}, \tag{2}$$

and hence the task of estimating $\#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi)$.

Define the multiplicative functions ϱ and ϱ^* by

$$\begin{aligned} \varrho(\mathbf{d}) &:= \#\{\mathbf{x} \in [0, d_1d_2)^2 : d_i \mid q_i(\mathbf{x}) \ (i = 1,2)\}, \\ \varrho^*(\mathbf{d}) &:= \#\{\mathbf{x} \in [0, d_1d_2)^2 : (\mathbf{x}; d_1d_2) = 1 \text{ and } d_i \mid q_i(\mathbf{x}) \ (i = 1,2)\}. \end{aligned} \tag{3}$$

One would expect to be able to estimate the size of the set $\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi$ by $\mathrm{vol}(\mathcal{R})\varrho(\mathbf{d})(d_1d_2D)^{-2}$, and indeed, we shall prove the following result:

THEOREM 2.1 (Level of distribution). *Let $q_i(x,y) := a_ix^2 + 2b_ixy + c_iy^2$ for $i = 1,2$ be a pair of irreducible quadratic forms in $\mathbb{Z}[X,Y]$, with $a_i, b_i, c_i \in \mathbb{Z}$, such that* $\mathrm{Res}(q_1,q_2) \neq 0$. *Defining $\Lambda_{\mathbf{d}}$ and Ψ as in* (1) *and* (2), *let*

$$T(M,\mathbf{Q}) := \sum_{\substack{d_i \le Q_i \\ (d_i;D)=1}} \sup_{\partial(\mathcal{R}) \le M} \left| \#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) - \frac{\mathrm{vol}(\mathcal{R})\varrho(d_1,d_2)}{(d_1d_2D)^2} \right|.$$

Then there exist absolute constants ν_1 and ν_2, both at least 1, *such that*

$$T(M,\mathbf{Q}) \ll Q_1Q_2(\log 2Q_1Q_2)^{\nu_1} + M\sqrt{Q_1Q_2}\,(\log 2Q_1Q_2)^{\nu_2}.$$

We approach this theorem by first examining the functions ϱ and ϱ^*, then developing upper bounds and formulæ relating the two functions. As in Daniel's work, we shall reformulate the "starred" problem in terms of lattices, and use a point-counting argument to generate the main term. The evaluation of the error term will be elementary but technical.

2.1. Transition from $\Lambda^*_{\mathbf{d}}$ to $\Lambda_{\mathbf{d}}$. We begin with the following bridging result which will be employed in Section 2.4 to express the unstarred sum in terms of the starred sum, leading to Theorem 2.1.

LEMMA 2.1 (Transition formula). *Let $D \in \mathbb{N}$ and suppose that $(d_1; D) = (d_2; D) = 1$. Then*

$$\#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) = \sum_{b \mid \psi(\mathbf{d})} \#(\Lambda_{\mathbf{c}}^* \cap \mathcal{R}/b \cap \Psi_b),$$

where $c_i := d_i/(d_i; b^2)$ for $i = 1, 2$, the multiplicative function ψ is defined by

$$\psi(p^\alpha, p^\beta) := p^{\lceil \max(\alpha,\beta)/2 \rceil},$$

and the lattice coset Ψ_b is defined by

$$\Psi_b := \{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv b^{-1}\mathbf{z} \ (\mathrm{mod}\, D)\},$$

where b^{-1} denotes the multiplicative inverse of b modulo D.

By definition, $\#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) = \#\{\mathbf{x} \in \mathcal{R} : d_i \mid q_i(\mathbf{x}),\ i = 1, 2,\ \mathbf{x} \in \Psi\}$. We partition this set according to $(\mathbf{x}; \psi(\mathbf{d}))$ to get

$$\sum_{b \mid \psi(\mathbf{d})} \#\{\mathbf{x} \in \mathcal{R} : q_i(\mathbf{x}) \equiv 0 \ (\mathrm{mod}\, d_i),\ (\mathbf{x}; \psi(\mathbf{d})) = b,\ \mathbf{x} \in \Psi\}.$$

Using the easily checked facts that $\psi(\mathbf{d})/b = \psi(\mathbf{c})$, and that $(\mathbf{y}; \psi(\mathbf{c})) = 1$ iff $(\mathbf{y}; c_1c_2) = 1$, we rewrite this as

$$\sum_{b \mid \psi(\mathbf{d})} \#\{\mathbf{y} \in \mathcal{R}/b : q_i(\mathbf{y}) \equiv 0 \ (\mathrm{mod}\, c_i),\ (\mathbf{y}; c_1c_2) = 1,\ \mathbf{y} \in \Psi_b\},$$

and hence the result.

2.2. Upper bounds for ϱ. It is crucial to understand the number of simultaneous zeros of our quadratic forms to given moduli. Two simplifications are useful to consider. First, we consider a "starred" function ϱ^* which counts the number of solutions which are coprime to the modulus. Second, we consider only one form at a time. The latter simplification is similar to a problem considered by Daniel [3].

To begin with, we note the fact that ϱ and ϱ^* are multiplicative functions, reducing the problem to evaluating the functions for prime power arguments.

2.2.1. *The one-form problem.* In the derivation of our upper bound for the two-form ϱ function, we will be able to reduce to the simpler one-form problem. It is possible to derive stronger results if we restrict to one form, including an elegant formula for $\varrho(p^\alpha)$, which will be utilised in Section 3.

Let q be an irreducible quadratic form in the variables x_1 and x_2. Define

$$\varrho^*(a) := \#\{\mathbf{x} \in [0, a)^2 : q(\mathbf{x}) \equiv 0 \ (\mathrm{mod}\, a),\ (\mathbf{x}; a) = 1\},$$
$$\varrho(a) := \#\{\mathbf{x} \in [0, a)^2 : q(\mathbf{x}) \equiv 0 \ (\mathrm{mod}\, a)\}.$$

LEMMA 2.2. *We have the upper bounds*

$$\varrho^*(p^\alpha) \ll \phi(p^\alpha), \qquad \varrho(p^\alpha) \ll \alpha p^\alpha$$

for all primes p and for all positive integers α. Moreover,

$$\varrho^*(p^\alpha) \le 2\phi(p^\alpha), \qquad \varrho(p) \le 2p$$

for all positive integers α and for all primes p which satisfy $(e_1e_2\delta; p) = 1$, where e_1 and e_2 are the coefficients of the monomials x_1^2 and x_2^2 respectively, and δ is the discriminant of q.

The argument presented below closely follows the work of Daniel [3]. Define

$$\tau_1(a) := \#\{x \in [0,a) : q(x,1) \equiv 0 \ (\mathrm{mod}\, a)\},$$
$$\tau_2(a) := \#\{x \in [0,a) : q(1,x) \equiv 0 \ (\mathrm{mod}\, a)\}.$$

Note that $e_1e_2 \ne 0$, by irreducibility of the form q. Let p be a prime such that p does not divide e_1e_2. Suppose $\mathbf{x}$ is counted by $\varrho^*(p^\alpha)$ for $\alpha \ge 1$, that is, $q(x_1,x_2) \equiv 0 \ (\mathrm{mod}\, p^\alpha)$ and $(\mathbf{x}; p) = 1$.

We shall show p is coprime to both x_1 and x_2. Suppose, for contradiction, that $p \mid x_2$; then $e_1x_1^2 \equiv 0 \ (\mathrm{mod}\, p)$, but p does not divide e_1, hence $p \mid x_1$, a contradiction. We get a similar contradiction if we assume $p \mid x_1$. Hence the vectors $\mathbf{x}$ counted by $\varrho^*(p^\alpha)$ are precisely those for which $q(x_1,x_2) \equiv 0$ $(\mathrm{mod}\, p^\alpha)$ and x_1, x_2 are both coprime to p. From this, we may deduce that

$$\varrho^*(p^\alpha) = \tau_1(p^\alpha)\phi(p^\alpha) = \tau_2(p^\alpha)\phi(p^\alpha) \tag{4}$$

for $\alpha \ge 1$ if p does not divide e_1e_2. To derive the second identity, for example, note that

$$\begin{aligned}\varrho^*(p^\alpha) &= \#\{\mathbf{x} \in [0,p^\alpha)^2 : q(\mathbf{x}) \equiv 0 \ (\mathrm{mod}\, p^\alpha),\ (x_1;p) = (x_2;p) = 1\} \\ &= \#\{\mathbf{x} \in [0,p^\alpha)^2 : q(1, x_2x_1^{-1}) \equiv 0 \ (\mathrm{mod}\, p^\alpha),\ (x_1;p) = (x_2;p) = 1\} \\ &= \#\{\mathbf{y} \in [0,p^\alpha)^2 : q(1, y_2) \equiv 0 \ (\mathrm{mod}\, p^\alpha),\ (y_1;p) = (y_2;p) = 1\},\end{aligned}$$

where x_1^{-1} denotes the inverse of x_1 modulo p^α.

Even if $p \mid e_1e_2$, we know that p does not divide x_1 or p does not divide x_2, so $\varrho^*(p^\alpha) \le (\tau_1(p^\alpha) + \tau_2(p^\alpha))\phi(p^\alpha)$ for all p and $\alpha \ge 1$. We now apply the following theorem of Huxley [7]:

THEOREM 2.2. *If $g \in \mathbb{Z}[X]$ is a polynomial of degree $n \ge 2$ and nonzero discriminant δ, then for all prime powers p^e, $t(p^e) \le np^{m_p/2}$, where $p^{m_p} \parallel \delta$ and where*

$$t(a) := \#\{x \in [0,a) : g(x) \equiv 0 \ (\mathrm{mod}\, a)\}.$$

The polynomials $q(x,1)$ and $q(1,x)$ are irreducible, hence have no repeated root; so the theorem applies, giving $\tau_1(p^\alpha) + \tau_2(p^\alpha) \le 4\delta^{1/2} \ll 1$ uniformly for all p and $\alpha \ge 1$. Hence $\varrho^*(p^\alpha) \ll \phi(p^\alpha)$.

Huxley's theorem also applies for the special case where $(e_1e_2\delta; p) = 1$. As p is coprime to the discriminant, we have $\tau_1(p^\alpha) \le 2$ for all α, and an application of (4) gives $\varrho^*(p^\alpha) \le 2\phi(p^\alpha)$.

We can express ϱ in terms of ϱ^*, and we have

$$\varrho(p^\alpha) = p^{2(\alpha-\lceil\alpha/2\rceil)} + \sum_{0\le\beta<\lceil\alpha/2\rceil} p^{2\beta}\varrho^*(p^{\alpha-2\beta}). \tag{5}$$

To see this, we employ the more general result, equation (7), that

$$\varrho(\mathbf{d}) = \sum_{b\mid\psi(\mathbf{d})} \varrho^*(\mathbf{c})\left(\frac{(d_1;b^2)(d_2;b^2)}{b}\right)^2$$

for a two-form function $\varrho(\mathbf{d})$, where $\psi(p^\alpha,p^\beta) = p^{\lceil\max(\alpha,\beta)/2\rceil}$, and $c_i = d_i/(d_i;b^2)$. This immediately gives the desired result by reducing to the one-form function $\varrho(d) := \varrho(d,1)$. Formula (5) gives our bound for ϱ, and Lemma 2.2 is proved.

For certain applications, we shall need a more exact formula, which is provided by the following lemma:

Lemma 2.3. *Let $q(x_1,x_2)=ax_1^2+2bx_1x_2+cx_2^2$ be an irreducible quadratic form. Suppose that p does not divide $2ac\delta$. Then*

$$\varrho(p^\alpha) = \phi(p^\alpha)\left\{1+\left(\frac{\delta}{p}\right)\right\}\lceil\alpha/2\rceil + p^{2(\alpha-\lceil\alpha/2\rceil)},$$

where $\delta := b^2-ac$ is the discriminant of q.

By the argument of Lemma 2.2, we have $\varrho^*(p^\alpha) = \phi(p^\alpha)\tau_1(p^\alpha)$, where $\tau_1(p^\alpha)$ is the number of solutions of $q(x,1)\equiv 0 \pmod{p^\alpha}$. Now x is such a solution if and only if

$$(x+a^{-1}b)^2 \equiv a^{-1}(a^{-1}b^2-c) \pmod{p^\alpha},$$

where a^{-1} is the multiplicative inverse of a modulo p^α. By Hensel's lemma, we only need to count the number of solutions to this equation modulo p, so

$$\tau_1(p^\alpha) = \tau_1(p) = 1+\left(\frac{a^{-1}(a^{-1}b^2-c)}{p}\right) = 1+\left(\frac{\delta}{p}\right),$$

hence $\varrho^*(p^\alpha) = \phi(p^\alpha)\{1+\left(\frac{\delta}{p}\right)\}$. Applying equation (5) yields the result.

2.2.2. *The two-form problem.* We now consider the two-form variants of ϱ^* and ϱ, defined in (3).

2.2.3. *The function ϱ^**

Lemma 2.4. *For every prime p one has $\varrho^*(p^e,p^f) \ll p^{\max(e,f)}$, and if p is coprime to* $\mathrm{Res}(q_1,q_2)$, *then*

$$\varrho^*(p^e,p^f) = 0 \quad \textit{if } e>0 \textit{ and } f>0. \tag{6}$$

First, we shall show that $\varrho^*(p^e,p^f)\ll p^{\max(e,f)}$ for all p. We may assume that $\varrho^*(p^e,p^f)\neq 0$. Thus there exists $\mathbf{x}=(x_1,x_2)$ such that $(\mathbf{x};p)=1$, $q_1(\mathbf{x})\equiv 0 \pmod{p^e}$, and $q_2(\mathbf{x})\equiv 0 \pmod{p^f}$. Without loss of generality, assume p does not divide x_2.

Define $Q_i(Y):=q_i(Y,1)$, and $y\equiv x_1x_2^{-1} \pmod{p^{\max(e,f)}}$, where x_2^{-1} is the multiplicative inverse of x_2 modulo $p^{\max(e,f)}$. Now $0\equiv q_1(x_1,x_2)\equiv x_2^2Q_i(y) \pmod{p^e}$, and p does not divide x_2, hence $p^e\mid Q_1(y)$.

Similarly, $p^f\mid Q_2(y)$, whence $p^{\min(e,f)}\mid Q_1(y)$ and $p^{\min(e,f)}\mid Q_2(y)$. We deduce that $p^{\min(e,f)}\mid \operatorname{Res}(q_1,q_2)$. This restricts what $\min(e,f)$ can be. Precisely, define m_p by $p^{m_p}\parallel \operatorname{Res}(q_1,q_2)$; then $\min(e,f)\le m_p$. Note that for fixed q_1,q_2, we have $m_p=0$ for all but finitely many p. Now

$$\begin{aligned}\varrho^*(p^e,p^f)&\le \#\{\mathbf{x}\ (\operatorname{mod} p^{e+f}) : p^f\mid q_2(\mathbf{x}),\ (\mathbf{x};p)=1\}\\ &= p^{2e}\#\{\mathbf{x}\ (\operatorname{mod} p^{f}) : p^f\mid q_2(\mathbf{x}),\ (\mathbf{x};p)=1\},\end{aligned}$$

whence $\varrho^*(p^e,p^f)\ll p^{2e}p^f$, where we have used the one-form result, Lemma 2.2. A similar argument gives $\varrho^*(p^e,p^f)\ll p^{2f}p^e$, which combine to give

$$\varrho^*(p^e,p^f)\ll p^{2m_p}p^{\max(e,f)}.$$

Now $m_p=0$ for all but finitely many p, so $\varrho^*(p^e,p^f)\ll p^{\max(e,f)}$. Moreover, we extract from the proof that if $(p;\operatorname{Res}(q_1,q_2))=1$, and if $\min(e,f)>0$, then $\min(e,f)>m_p$, and hence $\varrho^*(p^e,p^f)=0$, which implies the result (6), and our lemma is proved.

2.2.4. *The function ϱ*

LEMMA 2.5. *For every prime p and for all nonnegative integers e and f, let $m:=\min(e,f)$, $M:=\max(e,f)$. Then $\varrho(p^e,p^f)\ll (M-m+1)p^{2m+M}$ and $\varrho(p,p)\ll p^2$. Moreover, for all but a finite set of primes p, one has $\varrho(p,1)\le 2p$ and $\varrho(1,p)\le 2p$.*

Assume $e=\min(e,f)$. Recall the definitions (1) of $\Lambda_{\mathbf{d}}$ and $\Lambda_{\mathbf{d}}^*$. We may write $\varrho(\mathbf{d})=\#(\Lambda_{\mathbf{d}}\cap(0,d_1d_2]^2)$ and $\varrho^*(\mathbf{d})=\#(\Lambda_{\mathbf{d}}^*\cap(0,d_1d_2]^2)$. Applying Lemma 2.1 and using the notation of Section 2.1, we have

$$\varrho(\mathbf{d})=\sum_{b\mid\psi(\mathbf{d})}\#(\Lambda_{\mathbf{c}}^*\cap(0,d_1d_2/b]^2)=\sum_{b\mid\psi(\mathbf{d})}\varrho^*(\mathbf{c})\biggl(\frac{(d_1;b^2)(d_2;b^2)}{b}\biggr)^2, \tag{7}$$

where $c_i=d_i/(d_i;b^2)$. In particular,

$$\varrho(p^e,p^f)=\sum_{0\le\beta\le\lceil f/2\rceil}\varrho^*\biggl(\frac{p^e}{(p^e;p^{2\beta})},\frac{p^f}{(p^f;p^{2\beta})}\biggr)\biggl(\frac{(p^e;p^{2\beta})(p^f;p^{2\beta})}{p^\beta}\biggr)^2. \tag{8}$$

Split the range of summation as $0 \le 2\beta \le e$, $e < 2\beta < f$, and $\beta = \lceil f/2 \rceil$. We have the following upper bound for $\varrho(p^e, p^f)$:

$$\sum_{0\le\beta\le e/2} \varrho^*(p^{e-2\beta}, p^{f-2\beta})p^{6\beta} + \sum_{e/2<\beta<f/2} \varrho^*(1, p^{f-2\beta})p^{2e+2\beta} + (p^{e+f-\lceil f/2\rceil})^2$$
$$\ll \sum_{0\le\beta\le e/2} p^{f+4\beta} + \sum_{e/2<\beta<f/2} p^{2e+f} + p^{2e+f} \ll (f-e)p^{2e+f} + p^{2e+f},$$

as required.

We can do a little better in special cases. If $e = 0$ or $f = 0$, then $\varrho(p^e, p^f)$ reduces to the one-form problem, so by Lemma 2.2 we have $\varrho(p, 1) \le 2p$, $\varrho(1, p) \le 2p$, for all but finitely many primes p. Also, by equation (8), we have

$$\varrho(p, p) = \varrho^*(p, p) + p^2 = O(p^2), \tag{9}$$

which completes proof of Lemma 2.5.

2.3. Level of distribution—starred version. In the calculation of our sum, we need to evaluate $\#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi)$. Here, Ψ is defined to be the lattice coset $\{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv \mathbf{z} \pmod{D}\}$ for chosen $\mathbf{z}$ and D which depend only on the forms in question. We will see that it is only necessary to consider those $\mathbf{d}$ for which $(d_1; D) = (d_2; D) = 1$.

The level of distribution formula gives us the error term involved in estimating $\#(\Lambda_{\mathbf{d}} \cap \mathcal{R} \cap \Psi)$ by $\mathrm{vol}(\mathcal{R})\varrho(\mathbf{d})/(d_1 d_2 D)^2$, as we average over $\mathbf{d}$ and $\mathcal{R}$.

As mentioned in the background section, it is simpler to deal first with a "starred" level of distribution formula. This is one in which we impose coprimality conditions. We have

Lemma 2.6. *Define*

$$T^*(M, \mathbf{Q}) := \sum_{\substack{d_i \le Q_i \\ (d_i; D)=1}} \sup_{\mathcal{R}:\, \partial R \le M} \left| \#(\Lambda^*_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) - \frac{\varrho^*(d_1, d_2)}{(d_1 d_2 D)^2} \mathrm{vol}(\mathcal{R}) \right|.$$

If $q_i(x, y) = a_i x^2 + 2b_i xy + c_i y^2$ *(for* $i = 1, 2$*) are a pair of irreducible quadratic forms in* $\mathbb{Z}[X, Y]$ *such that* $a_i, b_i, c_i \in \mathbb{Z}$ *and such that* $\mathrm{Res}(q_1, q_2) \ne 0$, *then*

$$T^*(M, \mathbf{Q}) \ll M\sqrt{Q_1 Q_2}\,(\log 2Q_1 Q_2)^{2^2 5^5} + Q_1 Q_2 (\log 2Q_1 Q_2)^6$$

uniformly for $M > 0$ *and* $Q_1, Q_2 \ge 1$.

2.3.1. *The quantities* $\Lambda^*_{\mathbf{d}}$. Assume that $\mathbf{d} = (d_1, d_2)$ is fixed and define $a := d_1 d_2$. Let $\mathcal{U}(a)$ be the set of equivalence classes of $\mathbf{x} \in \mathbb{Z}^2$ under multiplication with $(x_1; x_2; a) = 1$. That is, if $(\mathbf{x}; a) = (\mathbf{y}; a) = 1$, then we define a relation by

$$\mathbf{x} \sim \mathbf{y} \quad \text{iff} \quad (\exists \lambda \in \mathbb{Z})(\mathbf{x} \equiv \lambda \mathbf{y} \pmod{a}).$$

Our motivation for this definition is that we wish to partition $\Lambda^*_{\mathbf{d}}$ into equivalence classes. It is easily checked that $\sim$ is an equivalence relation, and that $(\lambda; a) = 1$. Moreover, suppose $\mathbf{y} \in \mathcal{A}$ for some $\mathcal{A} \in \mathcal{U}(a)$, then if $(\lambda; a) = 1$, we have $\lambda\mathbf{y} \in \mathcal{A}$. In fact, for a fixed $\mathbf{y} \in \mathcal{A}$,

$$\mathcal{A} = \{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv \lambda \mathbf{y} \text{ for some } \lambda \text{ with } (\lambda; a) = 1\}.$$

Bringing forms into play, one may verify that if $\mathbf{y} \in \Lambda^*_{\mathbf{d}}$, then $\lambda\mathbf{y} \in \Lambda^*_{\mathbf{d}}$, given $(\lambda; a) = 1$. So for a given $\mathcal{A} \in \mathcal{U}(a)$, either $\mathcal{A} \subset \Lambda^*_{\mathbf{d}}$ or $\mathcal{A} \cap \Lambda^*_{\mathbf{d}} = \emptyset$. This suggests the definition $\mathcal{U}'(\mathbf{d}) := \{\mathcal{A} \in \mathcal{U}(d_1 d_2) : \mathcal{A} \subset \Lambda^*_{\mathbf{d}}\}$. Hence we may partition $\Lambda^*_{\mathbf{d}}$ into disjoint sets as follows:

$$\Lambda^*_{\mathbf{d}} = \bigcup_{\mathcal{A} \in \mathcal{U}'(\mathbf{d})} \mathcal{A}.$$

For a given $\mathcal{A}$, fix $\mathbf{y} \in \mathcal{A}$. Then for any $\mathbf{x} \in \mathcal{A}$, we have $\mathbf{x} \equiv \lambda\mathbf{y} \pmod{a}$ for $(\lambda; a) = 1$. The vector $\mathbf{x}$ is uniquely determined modulo a by λ, so there are exactly $\phi(a)$ choices for $\mathbf{x}$ modulo a. Stated another way, $\#(\mathcal{A} \cap [0, a)^2) = \phi(a)$. Hence,

$$\varrho^*(d_1, d_2) = \#\mathcal{U}'(\mathbf{d})\phi(d_1 d_2). \tag{10}$$

Return to our summand:

$$\begin{aligned}
&\left|\#(\Lambda^*_{\mathbf{d}} \cap \mathcal{R} \cap \Psi) - \frac{\varrho^*(d_1, d_2)}{(d_1 d_2 D)^2} \operatorname{vol}(\mathcal{R})\right| \qquad (11)\\
&\quad = \left|\Big(\sum_{\mathcal{A} \in \mathcal{U}'(\mathbf{d})} \#(\mathcal{A} \cap \mathcal{R} \cap \Psi)\Big) - \frac{\varrho^*(d_1, d_2)}{(d_1 d_2 D)^2} \operatorname{vol}(\mathcal{R})\right| \\
&\quad = \left|\sum_{\mathcal{A} \in \mathcal{U}'(\mathbf{d})} \left\{\#(\mathcal{A} \cap \mathcal{R} \cap \Psi) - \frac{\varrho^*(d_1, d_2)}{\#\mathcal{U}'(\mathbf{d})(d_1 d_2 D)^2} \operatorname{vol}(\mathcal{R})\right\}\right| \\
&\quad \le \sum_{\mathcal{A} \in \mathcal{U}'(\mathbf{d})} \left|\#(\mathcal{A} \cap \mathcal{R} \cap \Psi) - \frac{\phi(d_1 d_2)}{(d_1 d_2 D)^2} \operatorname{vol}(\mathcal{R})\right|,
\end{aligned}$$

where we have used equation (10) in the last line.

2.3.2. *Estimating* $\#(\mathcal{A} \cap \mathcal{R} \cap \Psi)$. The next task is to calculate the quantity $\#(\mathcal{A} \cap \mathcal{R} \cap \Psi)$. Our line of attack will be to introduce lattices $G(\mathcal{A})$ generated by the sets $\mathcal{A}$. Applying techniques from the geometry of numbers, we will express the error in terms of a "minimal basis" of $G(\mathcal{A})$.

Choose $\mathcal{A} \in \mathcal{U}(a)$ and define $G(\mathcal{A})$ by

$$G(\mathcal{A}) := \{\mathbf{x} \in \mathbb{Z}^2 : (\exists \lambda \in \mathbb{Z})(\exists \mathbf{y} \in \mathcal{A})(\mathbf{x} \equiv \lambda \mathbf{y} \pmod{a})\}.$$

Fix $\mathbf{y}_0 \in \mathcal{A}$. Then we may rewrite $G(\mathcal{A})$ as

$$G(\mathcal{A}) = \{\mathbf{x} \in \mathbb{Z}^2 : (\exists \lambda \in \mathbb{Z})(\mathbf{x} \equiv \lambda \mathbf{y}_0 \pmod{a})\}$$

and it becomes clear that $G(\mathcal{A})$ is the sublattice of $\mathbb{Z}^2$ generated by the vectors of $\mathcal{A}$. We can see that $\mathcal{A} = \{\mathbf{x} \in G(\mathcal{A}) : (\mathbf{x}; a) = 1\}$, so

$$\begin{aligned}\#(\mathcal{A} \cap \mathcal{R} \cap \Psi) &= \sum_{\mathbf{x} \in G(\mathcal{A}) \cap \mathcal{R} \cap \Psi} \sum_{b \mid (\mathbf{x}; a)} \mu(b) \\ &= \sum_{b \mid a} \mu(b) \cdot \#\{\mathbf{x} \in \mathcal{R}/b : b\mathbf{x} \in G(\mathcal{A}) \cap \Psi\}.\end{aligned}$$

The appearance of $b\mathbf{x} \in G(\mathcal{A})$ in our equation for $\#(\mathcal{A} \cap \mathcal{R} \cap \Psi)$ suggests that we should work modulo a/b, and motivates the following definition: given $c \mid a$, and given $\mathcal{A} \in \mathcal{U}(a)$, we define $\mathcal{A} \pmod{c}$ to be the unique element of $\mathcal{U}(c)$ such that $\mathcal{A} \subset \mathcal{A} \pmod{c}$. If $b \mid a$, then $b\mathbf{x} \in G(\mathcal{A})$ iff $\mathbf{x} \in G(\mathcal{A} \pmod{a/b})$.

Moreover, $b\mathbf{x} \in \Psi$ iff $\mathbf{x} \equiv b^{-1}\mathbf{z} \pmod{D}$. The inverse exists as $b \mid a = d_1 d_2$, and we have assumed that each d_i is coprime to D. Define $\Psi' := \{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv b^{-1}\mathbf{z} \pmod{D}\}$. Then

$$\#(\mathcal{A} \cap \mathcal{R} \cap \Psi) = \sum_{b \mid a} \mu(b) \cdot \#(\mathcal{R}/b \cap G(\mathcal{A} \pmod{a/b}) \cap \Psi'). \tag{12}$$

Define $\mathcal{R}_1 := \mathcal{R}/b$, $a_1 := a/b$, $\mathcal{A}_1 = \mathcal{A} \pmod{a_1}$. Then, bearing in mind that $\det(G(\mathcal{A}_1)) = a_1$, an application of Lemma 2.1 in [3] allows us to deduce:

Lemma 2.7. *There exist vectors* $\mathbf{v}^{(1)}, \mathbf{v}^{(2)} \in G(\mathcal{A}_1)$ *with the following properties*:

1. *the pair* $(\mathbf{v}^{(1)}, \mathbf{v}^{(2)})$ *is a basis of* $G(\mathcal{A}_1)$,
2. $|\mathbf{v}^{(1)}| = \min\{|\mathbf{v}| : \mathbf{v} \in G(\mathcal{A}_1) \setminus \{\mathbf{0}\}\}$, *and*
3. $a_1 \le |\mathbf{v}^{(1)}|\,|\mathbf{v}^{(2)}| \le 2a_1/\sqrt{3}$.

Let $\theta : \mathbb{R}^2 \to \mathbb{R}^2$ be the automorphism which maps the canonical basis of $\mathbb{R}^2$ to $(\mathbf{v}^{(1)}, \mathbf{v}^{(2)})$. Then θ has matrix

$$\begin{pmatrix} v_1^{(1)} & v_1^{(2)} \\ v_2^{(1)} & v_2^{(2)} \end{pmatrix},$$

and $|\det \theta| = [\mathbb{Z}^2 : G(\mathcal{A}_1)] = a_1$.

We shall now derive a simple condition for $\mathbf{x} \in G(\mathcal{A}_1) \cap \Psi'$. First note that although $b^{-1}\mathbf{z}$ may not be a member of $G(\mathcal{A}_1)$, we may find a representative $\mathbf{z}'$ of $b^{-1}\mathbf{z}$ modulo D which is in $G(\mathcal{A}_1)$, as D is coprime to a_1. Write $\mathbf{x} = \theta\mathbf{a}$, $\mathbf{z}' = \theta\mathbf{b}$. As $(D; a_1) = 1$, we may invert θ modulo D and deduce that $\mathbf{x} \equiv \mathbf{z}'$

$(\bmod D)$ iff $\mathbf{a} \equiv \mathbf{b} \pmod{D}$. Hence $\mathbf{x} \in \mathcal{R}_1 \cap G(\mathcal{A}_1) \cap \Psi'$ iff $\mathbf{a} \in \theta^{-1}(\mathcal{R}_1) \cap \mathbb{Z}^2$ and $\mathbf{a} \equiv \mathbf{b} \pmod{D}$.

Write $\mathbf{a} = \mathbf{b} + D\mathbf{c}$. The above condition is equivalent to

$$\mathbf{c} \in \mathbb{Z}^2 \cap \left\{ \frac{1}{D} \left(\theta^{-1}(\mathcal{R}_1) - \mathbf{b}\right) \right\}.$$

We are now in a position to estimate the number of lattice points on $\frac{1}{D}(\theta^{-1}(\mathcal{R}_1) - \mathbf{b})$. The error term in approximating the number of lattice points enclosed by a curve C by its area $\mathrm{vol}(C)$ is given by $O(\partial(C) + 1)$. The reader is referred to Lemma 2.1.1 in [8] for further details. An application of this result gives

$$\#(\mathcal{R}_1 \cap G(\mathcal{A}_1) \cap \Psi') = \frac{1}{D^2} \mathrm{vol}(\theta^{-1}(\mathcal{R}_1)) + O(\partial(\theta^{-1}(\mathcal{R}_1)) + 1) \tag{13}$$

and

$$\mathrm{vol}(\theta^{-1}(\mathcal{R}_1)) = \frac{1}{a_1} \mathrm{vol}(\mathcal{R}_1) = \frac{b}{a} \frac{1}{b^2} \mathrm{vol}(\mathcal{R}) = \frac{1}{ab} \mathrm{vol}(\mathcal{R}). \tag{14}$$

Note that

$$\theta^{-1} = \frac{1}{a_1} \begin{pmatrix} v_2^{(2)} & -v_1^{(2)} \\ -v_2^{(1)} & v_1^{(1)} \end{pmatrix},$$

hence

$$|\theta^{-1}| := \max_{\mathbf{u} \in \mathbb{R}^2 \setminus \mathbf{0}} \frac{|\theta^{-1}(\mathbf{u})|}{|\mathbf{u}|} \ll \frac{1}{a_1} \max(|\mathbf{v}^{(1)}|, |\mathbf{v}^{(2)}|) \ll \frac{|\mathbf{v}^{(2)}|}{a_1} \ll \frac{1}{|\mathbf{v}^{(1)}|},$$

by Lemma 2.7.

Also, $\partial(\theta^{-1}(\mathcal{R}_1)) \ll |\theta^{-1}| \partial(\mathcal{R}_1)$ and $\partial(\mathcal{R}_1) = \partial(\mathcal{R})/b$, so

$$\partial(\theta^{-1}(\mathcal{R}_1)) \ll \frac{\partial(\mathcal{R})}{b|\mathbf{v}^{(1)}|} \ll \frac{M}{b|\mathbf{v}^{(1)}|}.$$

Substituting this and equation (14) into (13) gives

$$\#(\mathcal{R}_1 \cap G(\mathcal{A}_1) \cap \Psi') = \frac{\mathrm{vol}(\mathcal{R})}{abD^2} + O\left(\frac{M}{b|\mathbf{v}^{(1)}|} + 1 \right). \tag{15}$$

In what follows, we shall write $\mathbf{v}(\mathcal{A}_1)$ for $\mathbf{v}^{(1)}$ in order to specify the equivalence class.

We know $\mathbf{v}(\mathcal{A}_1) \equiv \lambda \mathbf{y} \pmod{a/b}$ for some $\lambda \in \mathbb{Z}$ and some $\mathbf{y} \in \mathcal{A}$. Then $b\mathbf{v}(\mathcal{A}_1) \equiv (\lambda b)\mathbf{y} \pmod{a}$, so $b\mathbf{v}(\mathcal{A}_1) \in G(\mathcal{A})$, hence $b|\mathbf{v}(\mathcal{A}_1)| \geq |\mathbf{v}(\mathcal{A})|$. Insert this into equation (15):

$$\#(\mathcal{R}/b \cap G(\mathcal{A} \pmod{a/b}) \cap \Psi') = \frac{\mathrm{vol}(\mathcal{R})}{abD^2} + O\left(\frac{M}{|\mathbf{v}(\mathcal{A})|} + 1 \right).$$

Then substituting this into equation (12) gives

$$\begin{aligned}(16)\qquad \#(\mathcal{A}\cap\mathcal{R}\cap\Psi) &= \sum_{b\mid a}\mu(b)\biggl(\frac{\operatorname{vol}(\mathcal{R})}{abD^2}+O\biggl(\frac{M}{|\mathbf{v}(\mathcal{A})|}+1\biggr)\biggr)\\ &= \frac{\phi(a)}{a^2D^2}\operatorname{vol}(\mathcal{R})+O\biggl(d(a)\biggl(\frac{M}{|\mathbf{v}(\mathcal{A})|}+1\biggr)\biggr).\end{aligned}$$

Finally, substituting this into equation (11), we have

$$\begin{aligned}(17)\qquad & T^*(M,\mathbf{Q})\\ &\le \sum_{\substack{d_i\le Q_i\\(d_i;D)=1}}\ \sum_{\mathcal{A}\in\mathcal{U}'(\mathbf{d})}\ \sup_{\mathcal{R}:\,\partial\mathcal{R}\le M}\biggl|\#(\mathcal{A}\cap\mathcal{R}\cap\Psi)-\frac{\operatorname{vol}(\mathcal{R})\phi(d_1d_2)}{(d_1d_2D)^2}\biggr|\\ &\ll \sum_{\substack{d_i\le Q_i\\(d_i;D)=1}}\ \sum_{\mathcal{A}\in\mathcal{U}'(\mathbf{d})} d(d_1d_2)\biggl(\frac{M}{|\mathbf{v}(\mathcal{A})|}+1\biggr)\\ &\ll M\sum_{d_i\le Q_i} d(d_1d_2)\sum_{\mathcal{A}\in\mathcal{U}'(\mathbf{d})}\frac{1}{|\mathbf{v}(\mathcal{A})|}+\sum_{d_i\le Q_i} d(d_1d_2)\#\mathcal{U}'(\mathbf{d})\\ &= MT_1^*(\mathbf{Q})+T_2^*(\mathbf{Q}),\qquad \text{say.}\end{aligned}$$

2.3.3. *Evaluating $T_1^*(\mathbf{Q})$.* It is our aim in this section to prove:

LEMMA 2.8. *The quantity*

$$T_1^*(\mathbf{Q}) := \sum_{d_i\le Q_i} d(d_1d_2)\sum_{\mathcal{A}\in\mathcal{U}'(\mathbf{d})}\frac{1}{|\mathbf{v}(\mathcal{A})|}$$

satisfies the upper bound:

$$T_1^*(\mathbf{Q}) \ll \sqrt{Q_1Q_2}\,(\log 2Q_1Q_2)^{2^25^5}.$$

For $\mathcal{A}\in\mathcal{U}'(\mathbf{d})$, we have $|\mathbf{v}(\mathcal{A})|\ll\sqrt{d_1d_2}$, by Lemma 2.7, and there exist $\mathbf{y}\in\mathcal{A}$, $\lambda\in\mathbb{Z}$ such that $\mathbf{v}(\mathcal{A})\equiv\lambda\mathbf{y}\pmod{d_1d_2}$. Therefore, for $i=1,2$, $q_i(\mathbf{v}(\mathcal{A}))\equiv\lambda^2q_i(\mathbf{y})\equiv 0\pmod{d_i}$, so $d_i\mid q_i(\mathbf{v}(\mathcal{A}))$. Consequently,

$$T_1^*(\mathbf{Q}) \le \sum_{0<|\mathbf{v}|\ll\sqrt{Q_1Q_2}}\frac{1}{|\mathbf{v}|}\sum_{\substack{d_i\le Q_i\\ d_i\mid q_i(\mathbf{v})}} d(d_1d_2)\#\mathcal{U}'(\mathbf{d}).$$

As one would expect, we shall proceed by tackling the innermost quantity first. To begin with, we shall replace $d(d_1d_2)\#\mathcal{U}'(\mathbf{d})$ with a simpler multiplicative function. The first step is the proof that $\#\mathcal{U}'(\mathbf{d})\ll 2^{\nu(d_1d_2)}$. Write $d_1=\prod p^e$ and $d_2=\prod p^f$, and apply equation (10):

$$\#\mathcal{U}'(\mathbf{d}) = \frac{\varrho^*(\mathbf{d})}{\phi(d_1d_2)} = \prod_p\frac{\varrho^*(p^e,p^f)}{\phi(p^{e+f})},$$

by multiplicativity of ϱ^*.

For the rest of this section, define $P := \mathrm{Res}(q_1, q_2)$. By Lemma 2.4, if $(p; P) = 1$ and if $\min(e, f) > 0$, then $\varrho^*(p^e, p^f) = 0$. Thus $\#\mathcal{U}'(\mathbf{d}) = 0$ unless for all p satisfying $(p; P) = 1$ we have $\min(e, f) = 0$, in which case, we may write

$$\begin{aligned}\#\mathcal{U}'(\mathbf{d}) &\le \prod_{p\colon (p;P)=1} \frac{\varrho^*(p^e,1)}{\phi(p^e)} \prod_{p\colon (p;P)=1} \frac{\varrho^*(1,p^f)}{\phi(p^f)} \prod_{p\colon p\mid P} C\,\frac{p^{\max(e,f)}}{\phi(p^{e+f})} \\ &\ll \prod_{p\colon (p;P)=1} \frac{\varrho^*(p^e,1)}{\phi(p^e)} \prod_{p\colon (p;P)=1} \frac{\varrho^*(1,p^f)}{\phi(p^f)}.\end{aligned}$$

Now define $\varrho_1^*(b) := \varrho^*(b, 1)$ and $\varrho_2^*(b) := \varrho^*(1, b)$.

By an application of Lemma 2.2, there exist integers P_1 and P_2, depending only on the forms q_1 and q_2, such that $\varrho_i^*(p^\alpha) \le 2\phi(p^\alpha)$ if $(p; P_i) = 1$, and $\varrho_i^*(p^\alpha) \ll p^\alpha$ for all p^α.

Hence,

$$\begin{aligned}\#\mathcal{U}'(\mathbf{d}) &\ll \prod_{p\colon (p;PP_1)=1} \frac{\varrho_1^*(p^e)}{\phi(p^e)} \prod_{p\colon (p;PP_2)=1} \frac{\varrho_2^*(p^f)}{\phi(p^f)} \prod_{p\colon p\mid P_1} C\,\frac{\varrho_1^*(p^e)}{\phi(p^e)} \prod_{p\colon p\mid P_2} C\,\frac{\varrho_2^*(p^f)}{\phi(p^f)} \\ &\le \prod_{p\colon (p;PP_1)=1} 2 \prod_{p\colon (p;PP_2)=1} 2 \prod_{p\colon p\mid P_1} C \prod_{p\colon p\mid P_2} C \ll 2^{\nu(d_1 d_2)},\end{aligned}$$

as required, bearing in mind that each factor of 2 comes from a prime which divides either d_1 or d_2, but not both.

Observing that $2^{\nu(d_1d_2)} \le d(d_1d_2)$, and using the submultiplicativity property of d, we deduce that

$$d(d_1d_2)\#\mathcal{U}'(\mathbf{d}) \ll d(d_1)^2 d(d_2)^2,$$

whence

$$T_1^*(\mathbf{Q}) \ll \sum_{0<|\mathbf{v}|\le\sqrt{Q_1Q_2}} \frac{1}{|\mathbf{v}|} \sum_{d_i\mid q_i(\mathbf{v})} d(d_1)^2 d(d_2)^2.$$

Defining the function h by $h(n) := \sum_{a\mid n} d(a)^2$, we have

$$T_1^*(\mathbf{Q}) \ll \sum_{0<|\mathbf{v}|\le\sqrt{Q_1Q_2}} \frac{1}{|\mathbf{v}|}\, h(q_1(\mathbf{v}))h(q_2(\mathbf{v})). \tag{18}$$

2.3.4. *The function h.* Our approach to the evaluation of this sum will be to decompose it into dyadic intervals. Unfortunately, the arguments of the function h are $q_1(\mathbf{v})$ and $q_2(\mathbf{v})$, which are, in order of magnitude, the square of our summation variable $|\mathbf{v}|$. To facilitate the decomposition, we shall employ Lemma 2.10 below, which guarantees the existence of a divisor m_i of $q_i(\mathbf{v})$ of the correct order of magnitude, such that we can replace

$h(q_i(\mathbf{v}))$ with $h(m_i)^5$. To verify the conditions of Lemma 2.10, we shall need the following preliminary lemma:

LEMMA 2.9. *The function h is multiplicative. Moreover, h is submultiplicative in the sense that $h(m_1m_2) \le h(m_1)h(m_2)$ for all m_1, m_2. Furthermore, $h(p) \ll 1$ uniformly in p.*

Multiplicativity is trivial. To prove submultiplicativity, it suffices to show that $h(p^{e+f}) \le h(p^e)h(p^f)$. Now

$$h(p^e) = \sum_{i=1}^{e+1} i^2 = (e+1)(e+2)(2e+3)/6,$$

giving

$$\begin{aligned} &h(p^e)h(p^f) - h(p^{e+f}) \\ &\quad = ef(61 + 81f + 81e + 26e^2 + 18e^2f + 81ef + 4e^2f^2 + 18ef^2 + 26f^2); \end{aligned}$$

this is clearly nonnegative, demonstrating submultiplicativity. We also have $h(p) = 5 \ll 1$ uniformly for all p, completing the proof of Lemma 2.9.

This is sufficient to satisfy the conditions of the following lemma, which is to be found in [3] as Lemma 2.2:

LEMMA 2.10. *Let h be some positive submultiplicative arithmetical function such that $h(p) \ll 1$ uniformly in p. Let $\eta \ge 1$. Then for every natural number n, there exists a positive integer m satisfying $m \mid n$, $m \le n^{1/\eta}$, and*

$$h(n) \ll_\eta h(m)^{1+\lfloor \eta \rfloor}.$$

We apply Lemma 2.10 to equation (18), with $\eta = 4$, to obtain

$$T_1^*(\mathbf{Q}) \ll \sum_{\substack{j \ge 0 \\ P=2^j \ll \sqrt{Q_1Q_2}}} \frac{1}{P} \sum_{P \le |\mathbf{v}| \le 2P} \sum_{\substack{m_i | q_i(\mathbf{v}) \\ m_i \ll P^{1/2} \\ i=1,2}} h(m_1)^5 h(m_2)^5,$$

where we have split the range for $|\mathbf{v}|$ into dyadic intervals, and used the fact that $q_i(\mathbf{v}) \ll |\mathbf{v}|^2$ to deduce that $m_i \le |q_i(\mathbf{v})|^{1/4}$ implies $m_i \ll P^{1/2}$. We have

$$T_1^*(\mathbf{Q}) \ll \sum_{\substack{j \ge 0 \\ P=2^j \ll \sqrt{Q_1Q_2}}} \frac{1}{P} \sum_{m_1, m_2 \ll P^{1/2}} h(m_1)^5 h(m_2)^5 \sum_{\substack{|\mathbf{v}| \le 2P \\ q_i(\mathbf{v}) \equiv 0 \, (\mathrm{mod}\, m_i) \\ i=1,2}} 1.$$

The innermost sum is of order $\varrho(m_1, m_2)\{P^2/(m_1m_2)^2 + P/(m_1m_2)\}$, where the second term accounts for the error at the boundary. We have arranged that $m_1m_2 \ll P$, whence the second term is subsumed by the first, and hence the innermost sum is of order $\varrho(m_1,m_2)P^2/(m_1m_2)^2$, so

$$T_1^*(\mathbf{Q}) \ll \sum_{\substack{j\ge 0\\ P=2^j\ll\sqrt{Q_1Q_2}}} P \sum_{m_1,m_2\ll P^{1/2}} \frac{h(m_1)^5h(m_2)^5\varrho(m_1,m_2)}{m_1^2m_2^2}$$
$$\ll \sqrt{Q_1Q_2} \sum_{m_1,m_2\ll (Q_1Q_2)^{1/4}} \frac{h(m_1)^5h(m_2)^5\varrho(m_1,m_2)}{m_1^2m_2^2}.$$

At this point, we marshal together the facts we have uncovered concerning the function ϱ. We know that ϱ is multiplicative and we have the results of Lemma 2.5, including $\varrho(p,p) \ll p^2$. Furthermore we have $\varrho(p^e,p^f) \ll (M-m+1)p^{2m+M}$, where $m=\min(e,f)$ and $M=\max(e,f)$, and, by the one-form problem, $\varrho(p^e,1), \varrho(1,p^e) \ll ep^e$. Moreover, there exists a natural number P such that if $(p;P)=1$ then $\varrho(p,1)\le 2p$ and $\varrho(1,p)\le 2p$.

Note that for a doubly multiplicative function g, one has

$$\sum_{m_1,m_2\le Q} g(m_1,m_2) \le \prod_{p\le Q}\sum_{e,f=0}^{\infty} g(p^e,p^f).$$

Applying this to the above expression for T_1^*, we deduce

$$T_1^*(\mathbf{Q}) \ll \sqrt{Q_1Q_2} \prod_{p\ll (Q_1Q_2)^{1/4}} \sum_{e,f=0}^{\infty} \frac{h(p^e)^5h(p^f)^5\varrho(p^e,p^f)}{p^{2e+2f}}.$$

Let $g(p^e,p^f)$ denote the summand. In order to be able to apply our upper bound for ϱ, we split the sum as follows:

$$\sum_{f=0}^{\infty}\sum_{e=0}^{\infty} g(p^e,p^f) = \sum_{f=0}^{\infty}\sum_{e=0}^{f} g(p^e,p^f) + \sum_{e=1}^{\infty}\sum_{f=0}^{e-1} g(p^e,p^f) =: S_1+S_2.$$

Let p be a good prime, in the sense that $(p;P)=1$. Then, bearing in mind that $\varrho(p,p)\ll p^2$, we have

$$S_1 \le 1+\frac{2\cdot 5^5}{p}+\frac{C}{p^2}+C\sum_{f=2}^{\infty}\sum_{e=0}^{f}\frac{f^{16}e^{15}}{p^f}.$$

Call the double sum S'. Then

$$p^2S' \ll \sum_{f=2}^{\infty}\frac{f^{32}}{p^{f-2}} \le \sum_{f=2}^{\infty}\frac{f^{32}}{2^{f-2}},$$

and this is convergent by the ratio test, so $S'=O(1/p^2)$, and hence $S_1\le$

$1 + 2 \cdot 5^5/p + C'/p^2$. Similarly, $S_2 \le 2 \cdot 5^5/p + C/p^2$. So

$$S_1 + S_2 \le 1 + \frac{2^2 5^5}{p} + \frac{C}{p^2},$$

given that p is any good prime.

The analysis above shows that $S_1 + S_2 < \infty$ even for the finitely many bad primes p such that $p \,|\, P$.

Thus

$$T_1^*(\mathbf{Q}) \ll \sqrt{Q_1 Q_2} \prod_{p \ll (Q_1 Q_2)^{1/4}} \left(1 + \frac{2^2 5^5}{p} + \frac{C}{p^2}\right),$$

and an application of Mertens' theorem leads to our upper bound

$$T_1^*(\mathbf{Q}) \ll \sqrt{Q_1 Q_2}\, (\log 2Q_1 Q_2)^{2^2 5^5}.$$

To be precise, we have used the following:

Lemma 2.11. *Let $Q > 1$ and $C > 0$ be real numbers. Let k be a natural number and define*

$$S' = \prod_{p \le Q} \left(1 + \frac{k}{p} + \frac{C}{p^2}\right).$$

Then

$$S' \ll_{k,C} (\log Q)^k.$$

Observe

$$S' = \prod_{p \le Q} \left(1 - \frac{1}{p}\right)^{-k} \prod_{p \le Q} \left(1 - \frac{1}{p}\right)^{k} \left(1 + \frac{k}{p} + \frac{C}{p^2}\right).$$

Define a function $f : [0,1] \to \mathbb{R}$ by $f(x) = (1-x)^k (1 + kx + Cx^2)$. Then $f(x) = (1 - kx + \cdots \pm x^k)(1 + kx + Cx^2)$, so there exist constants c_i depending on k such that

$$\begin{aligned} f(x) &= 1 + c_2 x^2 + \cdots + c_{k+2} x^{k+2} \le 1 + |c_2| x^2 + \cdots + |c_{k+2}| x^{k+2} \\ &\le 1 + \{|c_2| + \cdots + |c_{k+2}|\} x^2 \le 1 + Lx^2 \le (1 + x^2)^L, \end{aligned}$$

where L depends only on k and C.

Recall Mertens' theorem, which states

$$\prod_{p \le z} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log z} + O\left(\frac{1}{(\log z)^2}\right).$$

This gives us

$$S' \le \prod_{p \le Q} \left(1 - \frac{1}{p}\right)^{-k} \prod_{p \le Q} \left(1 + \frac{1}{p^2}\right)^{L} \ll (\log Q)^k \prod_{p \le Q} \left(1 + \frac{1}{p^2}\right)^{L}.$$

Now

$$\prod_{p\le Q}\left(1+\frac{1}{p^2}\right)=\sum_{p\mid n\,\Rightarrow\, p\le Q}\frac{1}{n^2}\le\sum_{n=1}^{\infty}\frac{1}{n^2}=:C'$$

so $S'\ll(\log Q)^k(C')^L\ll_{k,C}(\log Q)^k$, as required.

2.3.5. *Evaluating $T_2^*(\mathbf{Q})$.* We shall prove

LEMMA 2.12. *The quantity T_2^* satisfies the upper bound*

$$T_2^*(\mathbf{Q})\ll Q_1Q_2\log(2Q_1Q_2)^6.$$

Recall

$$T_2^*(\mathbf{Q}):=\sum_{\substack{d_i\le Q_i\\ i=1,2}}d(d_1d_2)\#\mathcal{U}'(\mathbf{d}).$$

In our analysis of the sum $T_1^*(\mathbf{Q})$, we demonstrated that $\#\mathcal{U}'(\mathbf{d})\ll 2^{\nu(d_1d_2)}$. We see that $2^{\nu(a)}\le d(a)$ for any a and that the d function satisfies $d(ab)\le d(a)d(b)$ for any a and b. Thus,

$$\begin{aligned}T_2^*(\mathbf{Q})&\le\Big(\sum_{d_1\le Q_1}d(d_1)^2\Big)\Big(\sum_{d_2\le Q_2}d(d_2)^2\Big)\ll Q_1Q_2(\log Q_1)^3(\log Q_2)^3\\&\ll Q_1Q_2(\log 2Q_1Q_2)^6.\end{aligned}$$

In the last line, we use the AM-GM inequality to deduce

$$(\log A_1)^n(\log A_2)^n\ll(\log A_1A_2)^{2n}\tag{19}$$

This proves Lemma 2.12.

Combining this with Lemma 2.8 gives us our starred level of distribution formula, Lemma 2.6.

2.4. Level of distribution—unstarred version. Recall our convention that the symbol c_i represents $d_i/(d_i;b^2)$. We apply Lemma 2.1 and equation (7) to give the following expression for $T(M,\mathbf{Q})$:

$$\sum_{\substack{d_i\le Q_i\\(d_i;D)=1}}\sup_{\substack{\mathcal{R}:\\ \partial(\mathcal{R})\le M}}\Bigg|\sum_{b\mid\psi(d_1,d_2)}\bigg\{\#(\Lambda_{\mathbf{c}}^*\cap\mathcal{R}/b\cap\Psi_b)-\frac{\varrho^*(\mathbf{c})}{(c_1c_2D)^2}\operatorname{vol}(\mathcal{R}/b)\bigg\}\Bigg|$$

$$\le\sum_{\substack{c_i\le Q_i\\(c_i;D)=1}}\sum_{\substack{b\le Q_1Q_2\\(b_i;D)=1}}\delta(\mathbf{Q},\mathbf{c},b)\sup_{\substack{\mathcal{R}:\\ \partial(\mathcal{R})\le M}}\bigg|\#(\Lambda_{\mathbf{c}}^*\cap\mathcal{R}/b\cap\Psi_b)-\frac{\varrho^*(\mathbf{c})}{(c_1c_2D)^2}\operatorname{vol}(\mathcal{R}/b)\bigg|,$$

where $\delta(\mathbf{Q},\mathbf{c},b)=\#\{(d_1,d_2):d_i\le Q_i,\ c_i=d_i/(d_i;b^2),\ b\mid\psi(d_1,d_2)\}$.

We shall derive an upper bound for δ. The approach used is to fix a prime p and to consider quantities β, α_i, and γ_i for $i=1,2$ such that $p^{\alpha_i}\parallel d_i$,

$p^{\gamma_i} \parallel c_i$, and $p^\beta \parallel b$. We take the quantities β and γ_i to be fixed: our task is to count the number of possibilities for α_i. For a fixed prime p, it may be verified that there are at most 8β possibilities, whence $\delta(\mathbf{Q}, \mathbf{c}, b) \leq \prod_{p^\beta \| b} 8\beta =: g(b)$. By induction on β, we find that $8\beta \leq \binom{\beta+7}{7}$, thus employing the fact that $d_8(b) = \prod_{p^\beta \| b} \binom{\beta+7}{7}$, we have $g(b) \leq d_8(b)$. Consequently,

$$\sum_{b \leq B} \delta(\mathbf{Q}, \mathbf{c}, b) \leq \sum_{b \leq B} g(b) \leq \sum_{b \leq B} d_8(B) \ll B(\log B)^7,$$

where the last step uses $\sum_{b \leq B} d_k(b) \ll B(\log B)^{k-1}$, which follows from (12.1.4) in [10].

Note that we are summing over $c_i \leq Q_i$, $b \leq Q_1 Q_2$, but we may restrict the range of summation by observing a relationship which holds when $\delta(\mathbf{Q}, \mathbf{c}, b) \neq 0$. Suppose that $\delta(\mathbf{Q}, \mathbf{c}, b) \neq 0$; then there exist d_1, d_2 such that $b \,|\, \psi(d_1, d_2)$ and $c_i = d_i/(d_i; b^2)$. It is easily verified that $b \,|\, \psi(d_1, d_2)$ implies $b \,|\, d_1 d_2$, and hence $b \,|\, (d_1; b^2)(d_2; b^2)$. This may be rewritten as $c_1 c_2 b \,|\, d_1 d_2$, from which it follows that $c_1 c_2 b \leq Q_1 Q_2$.

For the sake of simplicity, we shall replace the expression

$$\left| \#(\Lambda_{\mathbf{c}}^* \cap \mathcal{R}/b \cap \Psi_b) - \frac{\varrho^*(\mathbf{c})}{(c_1 c_2 D)^2} \operatorname{vol}(\mathcal{R}/b) \right|$$

with $L(\mathbf{c}, b, \mathcal{R})$. Then our sum $T(M, \mathbf{Q})$ is estimated by

$$\begin{aligned} T(M, \mathbf{Q}) &\ll \sum_{\substack{c_1, c_2: \\ (c_i; D) = 1 \\ c_i \leq Q_i}} \sum_{\substack{b: \\ (b; D) = 1 \\ c_1 c_2 b \leq Q_1 Q_2}} \delta(\mathbf{Q}, \mathbf{c}, b) \sup_{\substack{\mathcal{R}: \\ \partial(\mathcal{R}) \leq M}} L(\mathbf{c}, b, \mathcal{R}) \\ &\leq \sum_{\substack{j_i: \\ C_i = 2^{j_i} \leq Q_i}} \sum_{\substack{C_i \leq c_i \leq 2C_i \\ (c_i; D) = 1}} \sum_{\substack{b: \\ (b; D) = 1 \\ b \leq \frac{Q_1 Q_2}{c_1 c_2}}} d_8(b) \sup_{\substack{\mathcal{R}: \\ \partial(\mathcal{R}) \leq M}} L(\mathbf{c}, b, \mathcal{R}). \end{aligned}$$

If we further split the range for b into dyadic intervals, then

$$T(M, \mathbf{Q}) \ll \sum_{\substack{j_i: \\ C_i = 2^{j_i} \leq Q_i}} \sum_{\substack{C_i \leq c_i \leq 2C_i \\ (c_i; D) = 1}} \sum_{\substack{k: \\ B = 2^k \leq \frac{Q_1 Q_2}{c_1 c_2}}} \sum_{\substack{b: \\ (b; D) = 1 \\ B \leq b \leq 2B}} d_8(b) \sup_{\partial(\mathcal{R}) \leq M} L(\mathbf{c}, b, \mathcal{R}).$$

Our aim is to use the estimate for $\sum_b d_8(b)$, but we need to handle sensitively the factor of $\sup L(\mathbf{c}, b, \mathcal{R})$. For each choice of B, define $b(B)$ by requiring $B \leq b(B) \leq 2B$, $(b(B); D) = 1$ and requiring that for all b with $B \leq b \leq 2B$ and $(b; D) = 1$, one has

$$\sup_{\partial(\mathcal{R}) \leq M} L(\mathbf{c}, b, \mathcal{R}) \leq \sup_{\partial(\mathcal{R}) \leq M} L(\mathbf{c}, b(B), \mathcal{R}).$$

Let S denote the set of integers B such that there are no b in the range $B \le b \le 2B$ with $(b;D)=1$. We have the upper bound

$$T(M,\mathbf{Q}) \ll \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} \sum_{\substack{C_i\le c_i\le 2C_i\\ (c_i;D)=1}} \sum_{\substack{k:\\ B=2^k\le \frac{Q_1Q_2}{c_1c_2}\\ B\notin S}} B(\log 2B)^7 \sup_{\partial(\mathcal{R})\le M} L(\mathbf{c}, b(B), \mathcal{R})$$

$$\le \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} \sum_{\substack{k:\\ B=2^k\le \frac{Q_1Q_2}{C_1C_2}\\ B\notin S}} B(\log 2B)^7 \sum_{\substack{C_i\le c_i\le 2C_i\\ (c_i;D)=1}} \sup_{\partial(\mathcal{R})\le M} L(\mathbf{c}, b(B), \mathcal{R}).$$

Writing $\mathcal{R}' := \mathcal{R}/b(B)$, we may now apply our starred level of distribution formula (Lemma 2.6) to the inner sum, which is bounded from above by

$$\sum_{\substack{C_i\le c_i\le 2C_i\\ (c_i;D)=1}} \sup_{\partial(\mathcal{R}')\le M/B} \left| \#(\Lambda^*_{\mathbf{c}} \cap \mathcal{R}' \cap \Psi_{b(B)}) - \frac{\varrho^*(\mathbf{c})}{(c_1c_2D)^2}\operatorname{vol}(\mathcal{R}')\right|$$

$$\ll \frac{M}{B}\sqrt{C_1C_2}\,(\log 8C_1C_2)^{2^25^5} + C_1C_2(\log 8C_1C_2)^6,$$

so

$$T(M,\mathbf{Q}) \ll M \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} \sqrt{C_1C_2}\,(\log 8C_1C_2)^{2^25^5} \sum_{k\le \log_2 \frac{Q_1Q_2}{C_1C_2}} (\log 2^{k+1})^7$$

$$+ \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} C_1C_2(\log 8C_1C_2)^6 \sum_{k\le \log_2 \frac{Q_1Q_2}{C_1C_2}} 2^k(\log 2^{k+1})^7.$$

Estimating the sums over k by the appropriate integrals, we arrive at

$$T(M,\mathbf{Q}) \ll M \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} \sqrt{C_1C_2}\,(\log 8C_1C_2)^{2^25^5}(\log 2Q_1Q_2)^8$$

$$+ \sum_{\substack{j_i:\\ C_i=2^{j_i}\le Q_i}} C_1C_2(\log 8C_1C_2)^6\,\frac{Q_1Q_2}{C_1C_2}\,(\log Q_1Q_2)^7$$

$$\ll M(\log 2Q_1Q_2)^8 \sum_{j_i\le \log_2 Q_i} 2^{(j_1+j_2)/2}(\log 2^{j_1+j_2+3})^{2^25^5}$$

$$+ Q_1Q_2(\log 2Q_1Q_2)^7 \sum_{j_i\le \log_2 Q_i} (\log 2^{j_1+j_2+3})^6.$$

Once more we estimate the sums via integrals to get

$$T(M,\mathbf{Q}) \ll M(\log 2Q_1Q_2)^8\sqrt{Q_1Q_2}\,(\log 2Q_1)^{2^25^5}(\log 2Q_2)^{2^25^5}$$
$$+ Q_1Q_2(\log 2Q_1Q_2)^7(\log 2Q_1)^7(\log 2Q_2)^7.$$

Finally, we bring the result into the desired form by applying the AM-GM inequality as in equation (19). This proves the level of distribution formula.

3. PAIRS OF FORMS WITH ALMOST PRIME VALUES

In the next section, we set the scene by introducing the terminology of sieves, before going on to the derivation of Theorem 1.1 in Section 3.2.

3.1. The terminology of sieves. Sieve methods aim at finding the primes in a multiset (essentially a sequence) of natural numbers $\mathfrak{A}$. Typically, one defines a sifting set $\mathfrak{P}$ of primes, then one tries to discover the value of the sifting function

$$S(\mathfrak{A}, \mathfrak{P}, z) := |\{a : a \in \mathfrak{A}, \text{if } p \in \mathfrak{P} \text{ and } p \,|\, a, \text{then } p \geq z\}|.$$

This is useful in giving bounds for the number of primes in $\mathfrak{A}$.

In our case, we are examining almost-primes, so we will want a lower bound for $|\{P_5 : P_5 \in \mathfrak{A}\}|$, where our multiset $\mathfrak{A}$ will be

$$\mathfrak{A} := \{q_1(x,y)q_2(x,y) : (x,y) \in \mathbb{Z}^2 \cap X\mathcal{R}^{(0)} \cap \Psi\},$$

and, taking $D = 6\,\mathrm{Res}(q_1, q_2)a_1a_2c_1c_2\delta_1\delta_2$, as in the statement of Theorem 1.1, we define $\Psi := \{\mathbf{x} \in \mathbb{Z}^2 : \mathbf{x} \equiv \mathbf{z} \pmod D\}$, where $\mathbf{z}$ is chosen such that $(q_1(\mathbf{z}); D) = (q_2(\mathbf{z}); D) = 1$. For the sifting set $\mathfrak{P}$, we shall take all primes which do not divide D.

In the evaluation of the sifting function, it is necessary to consider a number of auxiliary quantities, including $\mathfrak{A}_d := \{a : a \in \mathfrak{A},\ a \equiv 0 \pmod d\}$. We will need to use an approximation Y for the number of elements in the set $\mathfrak{A}$. In the case under consideration, it is natural to take $Y = X^2 \,\mathrm{vol}(\mathcal{R}^{(0)})/D^2$.

We shall choose the function $\omega(p)$ such that

$$Y\,\frac{\omega(p)}{p} = \begin{cases} |\mathfrak{A}_p| \text{ approximately} & \text{for } p \in \mathfrak{P}, \\ 0 & \text{for } p \in \overline{\mathfrak{P}}, \end{cases}$$

where $\overline{\mathfrak{P}}$ is the complement of $\mathfrak{P}$ in the set of all primes. We extend the definition of ω by multiplicativity to all squarefree numbers.

The quantity R_d is, in some sense, the error in approximating $|\mathfrak{A}_d|$ by $Y\omega(d)/d$, that is, we define

$$R_d := |\mathfrak{A}_d| - \frac{\omega(d)}{d}\,Y \quad \text{ if } \mu(d) \neq 0.$$

3.2. Proof of the main result. Our main tool will be the following weighted sieve of Diamond and Halberstam [5]:

THEOREM 3.1. *With the notation of Section* 3.1, *suppose there exist real constants* $\kappa > 1$, $A_1, A_2 \geq 2$, *and* $A_3 \geq 1$ *such that*

$$\text{(A)} \qquad 0 \leq \omega(p) < p,$$

(B) $$\prod_{z_1 \le p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \le \left(\frac{\log z}{\log z_1}\right)^{\kappa} \left(1 + \frac{A_1}{\log z_1}\right), \qquad 2 \le z_1 < z,$$

(C) $$\sum_{\substack{d < Y^{\alpha}/(\log Y)^{A_3} \\ (d;\overline{\mathfrak{P}})=1}} \mu^2(d) 4^{\nu(d)} |R_d| \le A_2 \frac{Y}{\log^{\kappa+1} Y},$$

for some α with $0 < \alpha \le 1$; that

(D) $$(a;\overline{\mathfrak{P}}) = 1 \quad \textit{for all } a \in \mathfrak{A};$$

and that

(E) $$|a| \le Y^{\alpha\mu} \quad \textit{for some } \mu, \textit{ and for all } a \in \mathfrak{A}.$$

Then there exists a real constant $\beta_\kappa > 2$ such that for any real numbers u and v satisfying

$$\alpha^{-1} < u < v, \qquad \beta_\kappa < \alpha v,$$

we have

$$|\{P_r : P_r \in \mathfrak{A}\}| \gg Y \prod_{p < Y^{1/v}} \left(1 - \frac{\omega(p)}{p}\right)$$

whenever

(20) $$r > \alpha\mu u - 1 + \frac{\kappa}{f_\kappa(\alpha v)} \int_1^{v/u} F_\kappa(\alpha v - s)\left(1 - \frac{u}{v}\right)\frac{ds}{s},$$

where f_k and F_k are solutions to a system of delay differential equations specified in [5]*. Let $I(\kappa, \alpha, \mu)$ denote the minimum value of the lower bound on the right of* (20) *as u and v vary, subject to the above constraints. As tabulated in* [5], $I(2,1,2) < 5$.

An examination of Diamond and Halberstam's paper shows that I is a continuous function of α and μ, so for our purposes, it will be sufficient to demonstrate that Theorem 3.1 applies for $\kappa = 2$, and for any $\alpha < 1$, and $\mu > 2$.

3.2.1. *Condition* (A). We shall now verify the conditions required for the application of Theorem 3.1, critically employing the level of distribution formula in the estimation of the error-sum (C). To begin, we need to formulate an appropriate definition for the quantity $\omega(p)$.

Recall that for $p \in \mathfrak{P}$, we would like $Y\omega(p)/p$ to be roughly $|\mathfrak{A}_p|$, so we need an estimate for $|\mathfrak{A}_p|$. Writing $\Omega = X\mathcal{R}^{(0)} \cap \Psi$, we have

$$\begin{aligned} |\mathfrak{A}_p| &= \#\{(a,b) \in \Omega : p \mid q_1(a,b)q_2(a,b)\} \\ &= \#\{(a,b) \in \Omega : p \mid q_1(a,b)\} + \#\{(a,b) \in \Omega : p \mid q_2(a,b)\} \\ &\quad - \#\{(a,b) \in \Omega : p \mid q_1(a,b),\, p \mid q_2(a,b)\} \\ &= \#(\Lambda_{(p,1)} \cap \Omega) + \#(\Lambda_{(1,p)} \cap \Omega) - \#(\Lambda_{(p,p)} \cap \Omega). \end{aligned}$$

Now, we have the approximation

$$\#(\varLambda_{\mathbf{d}} \cap \mathcal{R} \cap \varPsi) \approx \frac{\varrho(d_1, d_2)}{(d_1 d_2 D)^2} \operatorname{vol}(\mathcal{R}),$$

whence

$$|\mathfrak{A}_p| \approx \frac{X^2 \operatorname{vol}(\mathcal{R}^{(0)})}{p^2 D^2} \{\varrho(p,1) + \varrho(1,p)\} - \frac{X^2 \operatorname{vol}(\mathcal{R}^{(0)})}{p^4 D^2} \varrho(p,p).$$

This leads us to define

$$\omega(p) = \begin{cases} p^{-1}(\varrho(p,1) + \varrho(1,p)) - p^{-3}\varrho(p,p), & p \in \mathfrak{P}, \\ 0, & p \in \overline{\mathfrak{P}}. \end{cases}$$

With this definition, we may quickly verify condition (A). First, we must check that $0 \le \omega(p)$. We may assume that $p \in \mathfrak{P}$, and by equation (9), we have $\varrho(p,p) = \varrho^*(p,p) + p^2$. As $(p; D) = 1$, Lemma 2.4 provides us with $\varrho^*(p,p) = 0$, so

$$\omega(p) = (\varrho(p,1) + \varrho(1,p) - 1)p^{-1},$$

but, from the definition, $\varrho(p,1) \ge 1$, so $\omega(p) \ge 0$.

On the other hand, by Lemma 2.3, we have

$$\varrho(p,1) = 1 + (p-1)\left(1 + \left(\frac{\delta_1}{p}\right)\right), \qquad \varrho(1,p) = 1 + (p-1)\left(1 + \left(\frac{\delta_2}{p}\right)\right),$$

so, writing $\chi_i(p) := \left(\frac{\delta_i}{p}\right)$,

$$\omega(p) = 2 + \chi_1(p) + \chi_2(p) - (1 + \chi_1(p) + \chi_2(p))/p,$$

whence $\omega(p) \le 4 < p$, as we have assumed $p \ge 5$. Incidentally, this inequality explains the factor of 6 in our choice of D.

3.2.2. *Condition* (B). This condition expresses the κ-dimensionality of the sieve problem. One should think of the quantity $\omega(p)/p$ as being the probability that an element of $\mathfrak{A}$ is divisible by p, and that κ is the "average" value of $\omega(p)$, in some sense. In many sieve problems, one finds that $\kappa = 1$, a linear sieve. However, in our problem, we will demonstrate that $\kappa = 2$, as one would expect from the above definition of $\omega(p)$.

We must prove

$$\prod_{z_1 \le p < z} \left(1 - \frac{\omega(p)}{p}\right)^{-1} \le \left(\frac{\log z}{\log z_1}\right)^{\kappa} \left(1 + \frac{A_1}{\log z_1}\right), \qquad 2 \le z_1 < z.$$

Without loss of generality, we may assume that $z_1 \ge 5$, as $\omega(p) = 0$ if $p = 2$ or 3. So upon taking logs, we must demonstrate

$$\sum_{z_1 \le p < z} \sum_{i=1}^{\infty} \frac{\omega(p)^i}{ip^i} \le \kappa \log\log z - \kappa \log\log z_1 + \log(1 + A_1/\log z_1)$$

for $z_1 \geq 5$. Now for any $B_1 > 0$ there exists a constant A_1 such that $B_1 x \leq \log(1+A_1 x)$ whenever $0 \leq x \leq 1$, so we may replace $\log(1+A_1/\log z_1)$ in the above equation by $B_1/\log z_1$.

We expect the sum $\sum_{z_1 \leq p < z} \omega(p)/p$ to contribute the main term, and begin by considering the error term, bearing in mind that $\omega(p) \leq 4$ for all primes p. We have

$$\sum_{i=2}^{\infty} \sum_{z_1 \leq p < z} \frac{\omega(p)^i}{ip^i} \leq \sum_{i=2}^{\infty} \sum_{n \geq z_1} \frac{4^i}{in^i} \leq \sum_{i=2}^{\infty} \frac{4^i}{i} \Big(\int_{x=z_1}^{\infty} \frac{1}{x^i}\, dx + \frac{1}{z_1} \Big)$$
$$\ll 1/z_1 \ll 1/\log z_1,$$

as required.

The main term is $\sum_{z_1 \leq p < z} \omega(p)/p$, which expands to

$$\sum_{z_1 \leq p < z} \frac{2}{p} + \sum_{z_1 \leq p < z} \frac{\chi_1(p)}{p} + \sum_{z_1 \leq p < z} \frac{\chi_2(p)}{p} - \sum_{z_1 \leq p < z} \frac{1+\chi_1(p)+\chi_2(p)}{p^2}$$
$$= 2\log\log z - 2\log\log z_1 + \sum_{z_1 \leq p < z} \frac{\chi_1(p)}{p} + \sum_{z_1 \leq p < z} \frac{\chi_2(p)}{p} + O(1/z_1).$$

In estimating the sums involving characters, we use a result of Mertens', to be found in Chapter 7 of [4], that for any nonprincipal character χ, one has $\sum_p p^{-1}\chi(p)\log p = O(1)$. So

$$\sum_{z_1 \leq p \leq z} \frac{\chi(p)}{p} = \sum_{z_1 \leq p \leq z} \frac{\chi(p)\log p}{p} \frac{1}{\log p} \leq \sum_{z_1 \leq p \leq z} \frac{\chi(p)\log p}{p} \frac{1}{\log z_1} \ll \frac{1}{\log z_1}.$$

This completes our verification of condition (B). We see that κ, the dimension of the sieve, has the value $\kappa = 2$.

3.2.3. *Condition* (C). Condition (C) is concerned with the quantity

$$|R_d| := \Big| |\mathfrak{A}_d| - \frac{\omega(d)}{d} Y \Big|$$

for squarefree d. Essentially, we shall sum $|R_d|$ as d varies in some range. In this problem, the range of summation is referred to as the level of distribution, and it is our aim to ensure that the level of distribution is as large as possible, whilst requiring that the sum be bounded above by $Y/(\log Y)^3$.

We would like to bring our work to bear on the level of distribution formula, and thus to relate $|\mathfrak{A}_d|$ to quantities of the form $\#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi)$. Our goal is fulfilled by the following formula:

LEMMA 3.1.

$$|\mathfrak{A}_d| = \sum_{\substack{c_1, c_2 \mid d \\ d \mid c_1 c_2}} \mu\Big(\frac{c_1 c_2}{d}\Big) \#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi).$$

For the duration of this proof, let us write Ω for $\mathbb{Z}^2 \cap X\mathcal{R}^{(0)} \cap \Psi$; then

$$\begin{aligned}
|\mathfrak{A}_d| &= \sum_{d_1 d_2 = d} \#\{\mathbf{x} \in \Omega : (q_1(\mathbf{x}); d) = d_1 \text{ and } d_2 \mid q_2(\mathbf{x})\} \\
&= \sum_{d_1 d_2 = d} \sum_{\substack{\mathbf{x} \in \Omega \\ d_i | q_i(\mathbf{x}) \\ (q_1(\mathbf{x})/d_1; d_2) = 1}} 1 = \sum_{d_1 d_2 = d} \sum_{\substack{\mathbf{x} \in \Omega \\ d_i | q_i(\mathbf{x})}} \sum_{\substack{e | q_1(\mathbf{x})/d_1 \\ e | d_2}} \mu(e) \\
&= \sum_{d_1 d_2 = d} \sum_{e | d_2} \mu(e) \sum_{\substack{\mathbf{x} \in \Omega \\ d_1 e | q_1(\mathbf{x}) \\ d_2 | q_2(\mathbf{x})}} 1 = \sum_{\substack{e, d_1 : \\ e d_1 | d}} \mu(e) \sum_{\substack{\mathbf{x} \in \Omega \\ e d_1 | q_1(\mathbf{x}) \\ d/d_1 | q_2(\mathbf{x})}} 1.
\end{aligned}$$

Write $c_1 = ed_1$ and $c_2 = d/d_1$. Then

$$|\mathfrak{A}_d| = \sum_{\substack{d | c_1 c_2 \\ c_1, c_2 | d}} \mu\left(\frac{c_1 c_2}{d}\right) \sum_{\substack{\mathbf{x} \in \Omega \\ c_1 | q_1(\mathbf{x}) \\ c_2 | q_2(\mathbf{x})}} 1,$$

and hence the result.

Naturally, it would be advantageous to express $\omega(d)/d$ in a similar form. Indeed, we may write

$$\frac{\omega(d)}{d} = \prod_{p | d} \frac{\omega(p)}{p} = \sum_{\substack{c_1, c_2 | d \\ d | c_1 c_2}} \mu\left(\frac{c_1 c_2}{d}\right) \frac{\varrho(c_1, c_2)}{(c_1 c_2)^2},$$

whence

$$\begin{aligned}
|R_d| &= \left| \sum_{\substack{c_1, c_2 | d \\ d | c_1 c_2}} \mu\left(\frac{c_1 c_2}{d}\right) \left\{ \#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi) - Y \frac{\varrho(c_1, c_2)}{(c_1 c_2)^2} \right\} \right| \\
&\leq \sum_{\substack{c_1, c_2 | d \\ d | c_1 c_2}} \left| \#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi) - Y \frac{\varrho(c_1, c_2)}{(c_1 c_2)^2} \right|.
\end{aligned}$$

Our ultimate aim is to derive a level of distribution of the form Y^α, for any positive $\alpha < 1$.

We consider the sum

$$E := \sum_{\substack{d < Y^\alpha \\ (d; \overline{\mathfrak{P}}) = 1}} \mu^2(d) 4^{\nu(d)} \sum_{\substack{c_1, c_2 | d \\ d | c_1 c_2}} \left| \#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi) - Y \frac{\varrho(c_1, c_2)}{(c_1 c_2)^2} \right|,$$

and we desire an upper bound for E. Let us introduce another variable, k, which specifies the highest common factor of c_1 and c_2. Define

$$U := \{d \in \mathbb{Z} : (d;\overline{\mathfrak{P}}) = 1,\ \mu^2(d) = 1\},$$
$$T_k := \{(c_1, c_2) \in U^2 : (c_1; c_2) = k\}.$$

This leads to the expression

$$E = \sum_{\substack{d<Y^\alpha \\ d\in U}} \mu^2(d)4^{\nu(d)} \sum_{\substack{k<Y^\alpha \\ k\in U}} \sum_{\substack{(c_1,c_2)\in T_k \\ c_1,c_2 \mid d \\ d\mid c_1c_2 \\ c_1c_2\le kY^\alpha}} |\ldots|,$$

where $|\ldots| := |\#(\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi) - Y\varrho(c_1, c_2)/(c_1c_2)^2|$. Note that $[c_1, c_2] = c_1c_2/k$, so the condition $c_1, c_2 \mid d$ implies that $c_1c_2/k \mid d$, and hence that $c_1c_2 \le dk$. This is the origin of the "extra" condition $c_1c_2 \le kY^\alpha$ in the inner sum.

We now swap the order of summation:

$$E \le \sum_{\substack{k<Y^\alpha \\ k\in U}} \sum_{\substack{(c_1,c_2)\in T_k \\ c_1c_2\le kY^\alpha}} |\ldots| \sum_{d\mid c_1c_2} \mu^2(d)4^{\nu(d)}.$$

Consider the inner sum. We have $\sum_{d\mid m} \mu^2(d)4^{\nu(d)} = 5^{\nu(m)} \ll_\varepsilon m^\varepsilon$ for any positive ε. Applied to our problem, the inner sum is bounded from above by Y^ε, leading to

$$E \ll_\varepsilon Y^\varepsilon \sum_{\substack{k<Y^\alpha \\ k\in U}} \sum_{\substack{(c_1,c_2)\in T_k \\ c_1c_2\le kY^\alpha}} |\ldots|.$$

We will make use of the divisibility properties of c_1 and c_2 to examine the inner sum, which will be denoted by $E(k)$. Write $c_i = kg_i$. Then $(g_1; g_2) = 1$. We claim that the map $\mathbf{x} \to \mathbf{x}/k$ is a bijection from $\Lambda_{\mathbf{c}} \cap X\mathcal{R}^{(0)} \cap \Psi$ to $\Lambda_{\mathbf{g}} \cap k^{-1}X\mathcal{R}^{(0)} \cap \Psi_k$. Clearly it is sufficient to prove that the given map is a bijection from $\Lambda_{\mathbf{c}}$ to $\Lambda_{\mathbf{g}}$. If $\mathbf{x} \in \Lambda_{\mathbf{c}}$ then $kg_i \mid q_i(\mathbf{x})$ for $i = 1, 2$. Hence $q_i(\mathbf{x}) \equiv 0 \pmod{k}$ for $i = 1, 2$; but k is squarefree and coprime to the resultant of q_1 and q_2, so, by an application of the Chinese Remainder Theorem, we must have $\mathbf{x} \equiv 0 \pmod{k}$. Write $\mathbf{x} = k\mathbf{y}$ for some $\mathbf{y} \in \mathbb{Z}^2$. Another direct application of the fact that $\mathbf{x} \in \Lambda_{\mathbf{c}}$ gives $g_i \mid k^2q_i(\mathbf{y})$ for $i = 1, 2$. Now, as c_i is squarefree for $i = 1, 2$, we have $(k; g_i) = 1$ for $i = 1, 2$, so we may deduce from $g_i \mid k^2q_i(\mathbf{y})$ that $g_i \mid q_i(\mathbf{y})$ for $i = 1, 2$, and hence that $\mathbf{y} \in \Lambda_{\mathbf{c}}$. It is trivial to demonstrate that if $\mathbf{y} \in \Lambda_{\mathbf{g}}$, then $k\mathbf{y} \in \Lambda_{\mathbf{c}}$, completing the proof of bijectivity.

To deal with the ϱ term, note that

$$\frac{\varrho(c_1, c_2)}{(c_1c_2)^2} = \frac{\varrho(kg_1, kg_2)}{(k^2g_1g_2)^2} = \frac{\varrho(k, k)}{k^4}\,\frac{\varrho(g_1, g_2)}{(g_1g_2)^2},$$

where we use multiplicativity of ϱ and the coprimality of k and g_1g_2 in the last line. Recall that the only solution of $q_i(\mathbf{x}) \equiv 0 \pmod{k}$ is the trivial solution $\mathbf{x} \equiv 0 \pmod{k}$. This allows us to deduce that the quantity $\varrho(k,k)$ is equal to k^2. In summary, we have

$$\frac{\varrho(c_1,c_2)}{(c_1c_2)^2} = \frac{\varrho(g_1,g_2)}{(kg_1g_2)^2}.$$

Employing these relations, we have the following upper bound for the inner sum:

$$E(k) \leq \sum_{\substack{(g_1,g_2)\in T_1:\\ kg_1g_2<Y^\alpha}} \left| \#(\Lambda_{\mathbf{g}} \cap k^{-1}X\mathcal{R}^{(0)} \cap \Psi_k) - Y\,\frac{\varrho(g_1,g_2)}{(kg_1g_2)^2} \right|.$$

In order to be able to apply the level of distribution formula, we split the summation into dyadic intervals. Given g_1 and g_2 such that $kg_1g_2 < Y^\alpha$, there exist unique integers n and m such that $2^{n-1} \leq g_1 < 2^n$ and $2^{m-1} \leq g_2 < 2^m$. Hence $k2^{n-1}2^{m-1} \leq kg_1g_2 < Y^\alpha$. We arrive at the estimate

$$E(k) \leq \sum_{\substack{n,m:\\ k2^{n+m}<4Y^\alpha}} \sum_{\substack{(g_1,g_2)\in T_1:\\ g_1<2^n\\ g_2<2^m}} \left| \#(\Lambda_{\mathbf{g}} \cap k^{-1}X\mathcal{R}^{(0)} \cap \Psi_k) - Y\,\frac{\varrho(g_1,g_2)}{(kg_1g_2)^2} \right|.$$

The inner sum is amenable to the level of distribution formula, and we see that $E(k)$ is bounded above by a quantity of order

$$\sum_{\substack{n,m:\\ k2^{n+m}<4Y^\alpha}} 2^{n+m}(\log 2^{n+m+1})^{\nu_1} + \frac{Y^{1/2}}{k}\,(2^{n+m})^{1/2}(\log 2^{n+m+1})^{\nu_2}.$$

To calculate this, we introduce the quantity $Q := \log_2(Y^\alpha/k)$. Then

$$\begin{aligned} E(k) &\ll \sum_{0\leq n<Q}\,\sum_{0\leq m<Q-n} 2^{n+m}(n+m+1)^{\nu_1} + \frac{Y^{1/2}}{k}\,(2^{n+m})^{1/2}(n+m+1)^{\nu_2} \\ &\ll \sum_{0\leq n<Q} 2^n(n+1)^{\nu_1} \sum_{0\leq m<Q-n} 2^m(m+1)^{\nu_1} \\ &\quad + \frac{Y^{1/2}}{k} \sum_{0\leq n<Q} 2^{n/2}(n+1)^{\nu_2} \sum_{0\leq m<Q-n} 2^{m/2}(m+1)^{\nu_2}. \end{aligned}$$

Now if $\beta > 0$, $\theta \geq 1$, and $N \geq 1$, then

$$\sum_{0\leq t<N} 2^{t\beta}(t+1)^\theta \ll_\beta N^\theta 2^{N\beta}.$$

Applying this result to our estimate for $E(k)$, we arrive at

$$E(k) \ll 2^Q \sum_{0\le n<Q} (n+1)^{\nu_1}(Q-n)^{\nu_1} + \frac{(2^QY)^{1/2}}{k} \sum_{0\le n<Q} (n+1)^{\nu_2}(Q-n)^{\nu_2}$$
$$\ll 2^Q Q^{2\nu_1+1} + \frac{(2^QY)^{1/2}}{k} Q^{2\nu_2+1}.$$

Recalling the definition of Q, we have the upper bound

$$E(k) \ll \frac{Y^\alpha}{k} (\log Y)^{\nu'} + \frac{Y^{(\alpha+1)/2}}{k^{3/2}} (\log Y)^{\nu'}$$

for some absolute constant ν'.

Finally, we sum $E(k)$ over k:

$$E \ll_\varepsilon Y^\varepsilon Y^\alpha (\log Y)^{\nu'+1} + Y^\varepsilon Y^{(\alpha+1)/2} (\log Y)^{\nu'} \ll_\varepsilon Y^{\max(\alpha+\varepsilon,\alpha/2+1/2+\varepsilon)}.$$

If we choose $\varepsilon = \min((1-\alpha)/5, \alpha - 1/2)$, then $E \ll_\alpha Y/(\log Y)^3$ and condition (C) is satisfied for any $\alpha < 1$.

3.2.4. *Conditions* (D) *and* (E). For $a \in \mathfrak{A}$, one has $a = q_1(\mathbf{x})q_2(\mathbf{x})$ with $\mathbf{x} \in \Psi$. The set Ψ was chosen so that $(q_1(\mathbf{x}); D) = (q_2(\mathbf{x}); D) = 1$ for all $\mathbf{x} \in \Psi$, so $(a; D) = 1$, whence $(a; \overline{\mathfrak{P}}) = 1$, satisfying condition (D).

In the consideration of condition (E), we observe that for all $a \in \mathfrak{A}$, one has $|a| \ll X^4 \ll Y^2$. That is, there exists a constant C (depending only on the choice of forms q_1 and q_2) such that $|a| \le CY^2$ for all $a \in \mathfrak{A}$. Define θ by $C = Y^\theta$. In order to satisfy condition (E), we need $|a| \le Y^{\mu\alpha}$, and it is sufficient to chose $\alpha < 1$ and μ such that $\mu \ge (2+\theta)/\alpha$.

A more careful analysis is required if we wish to make use of Diamond and Halberstam's explicit result that $I(2,1,2) > 5$. By continuity of I, there exists $\eta > 0$ such that $I(2,\alpha,\mu) > 5$, provided that $|\alpha-1|, |\mu-2| < \eta$. Set $\mu = (2+\theta)/\alpha$. For $\alpha < 1$, the above condition translates into $\alpha > (2+\theta)/(2+\eta)$ and $\alpha > 1-\eta$. We can choose such a value of α provided that $\theta < \eta$. Now $\theta = \log C/\log Y$, so the condition will be satisfied for all sufficiently large Y.

3.2.5. *Application of Theorem 3.1.* Having verified the conditions of Theorem 3.1, we find that for sufficiently large X, there exists a constant $v > 2$ such that

$$|\{P_5 : P_5 \in \mathfrak{A}\}| \gg X^2 \prod_{p<X^{2/v}} \left(1 - \frac{\omega(p)}{p}\right),$$

and this is sufficient for the proof of Theorem 1.1.

Before we conclude, let us consider the condition in Theorem 1.1 that there exists $\mathbf{z}$ such that $(q_i(\mathbf{z}); D) = 1$ for $i = 1,2$. The condition is not always satisfied, as the following pair of forms demonstrate:

$$q_1(x,y) = 3x^2 + 2xy + y^2, \quad q_2(x,y) = 2x^2 - 4xy + 3y^2.$$

Here, at least one of $q_1(x,y)$ and $q_2(x,y)$ is divisible by 3 for every choice of x and y, and 3 divides D.

On the other hand, we expect that the condition will be satisfied for most pairs of forms and we exhibit the following infinite class of forms for which the condition holds:

$$q_1(x,y) = x^2 + 2b_1xy + c_1y^2, \quad q_2(x,y) = x^2 + 2b_2xy + c_2y^2.$$

Take $\mathbf{z} = (1,0)$; then $q_i(\mathbf{z}) = 1$, satisfying the condition as long as the resultant $\mathrm{Res}(q_1, q_2)$ is nonzero.

3.3. Conclusion. Our investigations into pairs of binary quadratic forms depended crucially on deriving an appropriate level of distribution formula and then applying the weighted sieve of Diamond and Halberstam. This technique is not limited to pairs of forms and could be extended to the consideration of arbitrarily many binary quadratic forms. The level of distribution formula would give rise to parameters κ, α, and μ, and the main computational problem would be the calculation of the number r in Theorem 3.1.

Acknowledgements. I'd like to thank Roger Heath-Brown for his unstinting guidance and supervision throughout this research. Thanks, too, to Glyn Harman and Tim Browning for their many helpful suggestions. A final debt of gratitude is owed to Trevor Wooley, who originally posed this problem.

References

[1] D. A. Buell, *Binary Quadratic Forms. Classical Theory and Modern Computations*, Springer, New York, 1989.

[2] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*, Wiley, New York, 1989.

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

[4] H. Davenport, *Multiplicative Number Theory*, 2nd ed., Grad. Texts in Math. 74, Springer, New York, 1980.

[5] H. Diamond and H. Halberstam, *Some applications of sieves of dimension exceeding* 1, in: Sieve Methods, Exponential Sums, and Their Applications in Number Theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser. 237, Cambridge Univ. Press, Cambridge, 1997, 101–107.

[6] D. R. Heath-Brown, *Linear relations amongst sums of two squares*, in: Number Theory and Algebraic Geometry, London Math. Soc. Lecture Note Ser. 303, Cambridge Univ. Press, Cambridge, 2003, 133–176.

[7] M. N. Huxley, *A note on polynomial congruences*, in: Recent Progress in Analytic Number Theory, Vol. 1 (Durham, 1979), H. Halberstam and C. Hooley (eds.), Academic Press, London, 1981, 193–196.

[8] M. N. Huxley, *Area, Lattice Points, and Exponential Sums*, London Math. Soc. Monogr. (N.S.) 13, Oxford Univ. Press, Oxford, 1996.
[9] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. 47 (1978), 171–188.
[10] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, 2nd ed., Oxford Univ. Press, Oxford, 1986.

Mathematical Institute
24–29 St Giles'
Oxford, OX1 3LB, UK
E-mail: marasing@maths.ox.ac.uk

Received on 6.3.2006
and in revised form on 12.5.2006 (5148)