The least common multiple of a bivariate quadratic sequence

by

NOAM KIMMEL (Tel Aviv)

Contents

1. Introduction ................................................................. 1
2. Proof of the degenerate cases............................................ 6
3. Proof of the generic case.................................................. 9
4. Preliminary lemmas ....................................................... 13
5. Small multiples of large primes represented by \( F \) .................. 22
6. Further thoughts and conjectures ....................................... 33
References ................................................................. 36

1. Introduction

1.1. The prime number theorem. Consider the Chebyshev function

\[ \psi(N) = \sum_{n \leq N} A(n), \]

where \( A \) is the von Mangoldt function

\[ A(n) = \begin{cases} 
\log p, & n = p^k \text{ for } p \text{ prime and } k > 0, \\
0, & \text{otherwise}.
\end{cases} \]

The prime number theorem is equivalent to the assertion that \( \psi(N) \sim N \).

An alternative definition for \( \psi(N) \) can be given using the least common multiple of the first \( N \) integers:

\[ \psi(N) = \log(\text{LCM}\{1, \ldots, N\}). \]

Thus, we see that the PNT can be stated in the following way:

**Theorem 1.1 (PNT).**

\[ \log(\text{LCM}\{n\}_{n \leq N}) \sim N. \]
1.2. LCM of consecutive polynomial values. One can naturally wonder about generalizations of the PNT arising from the formulation given in Theorem 1.1. Let \( f \in \mathbb{Z}[t] \), and define
\[
\psi_f(N) = \log \left( \text{LCM}_{n \leq N} \{ f(n) \} \right).
\]
It is an interesting problem to understand the asymptotic behaviour of \( \psi_f(N) \) for various \( f \).

The case where \( f \) is a linear polynomial was resolved in \([1]\). This was later extended in \([8]\) to all polynomials \( f \) which are a product of linear terms. In both cases, it was shown that \( \psi_f(N) \sim c_f N \) for some constant \( c_f \). The main ingredient of both proofs is Dirichlet’s theorem on primes in arithmetic progressions.

In \([4]\), Cilleruelo considers the case where \( f \) is an irreducible polynomial of degree 2. In this case he shows that
\[
\psi_f(N) \sim N \log N.
\]
He further conjectures that if \( f \) is an irreducible polynomial of degree \( d > 2 \), then \( \psi_f(N) \sim (d - 1)N \log N \).

While the upper bound
\[
\psi_f(N) \leq (d - 1)N \log N
\]
follows implicitly from Cilleruelo’s work, proving the lower bound seems to be a difficult problem. In \([11]\) Maynard and Rudnick prove the lower bound
\[
\psi_f(N) \gtrsim \frac{1}{d} N \log N,
\]
which is of the correct order of magnitude. This was later improved by Sah \([13]\) to
\[
\psi_f(N) \gtrsim N \log N.
\]
However, while these bounds give the correct order of magnitude, no irreducible polynomial of degree \( d > 2 \) has been exhibited for which the conjecture holds. For further details regarding this problem see the survey \([2]\).

1.3. LCM of multivariate polynomial values. We consider another natural generalization of Theorem 1.1. Let \( F \in \mathbb{Z}[x, y] \), and denote
\[
\psi_F(N) = \log \left( \text{LCM}_{0 < F(x,y) \leq N} \{ F(x, y) \} \right).
\]
One can ask about the asymptotic behaviour of \( \psi_F(N) \). A similar problem was proposed by Shparlinski \([3]\).

For example, consider the case where \( F(x, y) = x^2 + y^2 \). It is a classical result of Fermat that a number \( n \) is of the form \( x^2 + y^2 \) if and only if \( n \) has
the form
\[ n = 2^a \prod_{p_i \equiv 3 \pmod{4}} p_i^{2b_i} \prod_{p_j \equiv 1 \pmod{4}} p_j^{c_j}. \]

From this we get
\[ \psi_F(N) = \left\lfloor \log_2 N \right\rfloor \log 2 + 2 \sum_{\substack{p^k \leq \sqrt{N} \\mod{3}}} \log p + \sum_{\substack{p^k \leq N \\mod{1}}} \log p. \]

Thus, from the prime number theorem in arithmetic progressions we get \( \psi_F(N) \sim \frac{1}{2} N \). Note that this result relies heavily on the multiplicative properties of the image of \( F \). If we were to consider \( F(x, y) = x^2 + y^2 + 1 \) instead, the method above would not work.

1.4. A random model. In order to better understand what to expect from \( \psi_F(N) \) for \( F(x, y) = x^2 + y^2 + 1 \), we can consider the following random model. Let \( F \in \mathbb{Z}[x, y] \), and denote
\[ \delta_F(N) = \frac{\# \{0 < n \leq N \mid n = F(x, y)\}}{N}. \]

It was shown in [5] that if we take a random set \( A \subset \{1, \ldots, N\} \) where each element is taken with probability \( \delta = \delta(N) \), then
\[ \psi(A) := \log \left( \text{LCM} \{a\} \right) \sim N \frac{\log(\delta^{-1})\delta}{1 - \delta} \]
almost surely as \( N \) tends to infinity (provided \( N \delta(N) \to \infty \)).

Therefore, if we were to model the image of \( F \) as a random subset of \( \{1, \ldots, N\} \) where each element is taken with probability \( \delta_F(N) \), then we would expect
\[ \psi_F(N) \sim N \frac{\log(\delta_F^{-1}(N))\delta_F(N)}{1 - \delta_F(N)}. \]

Assuming some local phenomena arising from small primes, we still expect that
\[ \psi_F(N) \asymp N \frac{\log(\delta_F^{-1}(N))\delta_F(N)}{1 - \delta_F(N)}. \hspace{1cm} (1.1) \]

We already know that this model does not predict the correct asymptotic for all \( F \). To see this, consider once more the example \( F(x, y) = x^2 + y^2 \). In this case \( \delta_F(N) \asymp \frac{1}{\sqrt{\log N}} \), so the random model (1.1) would predict \( \psi_F(N) \asymp \frac{N \log \log N}{\sqrt{\log N}} \). But we saw that in this case \( \psi_F(N) \sim \frac{1}{2} N \), which is significantly larger.

On the other hand, if we were to consider \( F(x, y) = x^2 + y^2 + 1 \) instead, then it turns out that \( \psi_F(N) \) has order of magnitude \( \frac{N \log \log N}{\sqrt{\log N}} \), which agrees
with the order of magnitude predicted by the random model (1.1). This will follow from our main result in Theorem 1.4.

The discrepancy between $\psi_F(N)$ for $F(x, y) = x^2 + y^2$ and the random model (1.1) can be attributed to the multiplicative structure of the image of $F$, which causes abnormally high correlations between primes and the image of $F$.

1.5. Main results. We give a complete description of the order of magnitude of $\psi_F(N)$ where $F(x, y) \in \mathbb{Z}[x, y]$ is a polynomial of degree 2, and when it agrees with the random model (1.1). Denote

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y]$$

and assume that $F$ represents arbitrarily large integers. We denote by

$$\Delta = b^2 - 4ac$$

the discriminant of the homogeneous part of $F$, which we refer to as the discriminant of $F$. We also denote by

$$D = af^2 + ce^2 - bfe + \Delta g$$

the Hessian determinant of the associated quadratic form

$$\overline{F}(x, y, z) = z^2 F(x/z, y/z).$$

We refer to $D$ as the large discriminant of $F$.

As before, we also set

$$\delta_F(N) = \frac{\# \{0 < n \leq N \mid n = F(x, y) \}}{N}.$$ 

Our main results are the following theorems:

**Theorem 1.2.** Let $F$ be as above, and assume that $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly dependent. Then

$$\delta_F(N) \sim \frac{1}{\sqrt{(a, c)N}}.$$ 

(1) If $F$ is irreducible then

$$\psi_F(N) \sim N \frac{\log(\delta_F^{-1}(N)) \delta_F(N)}{1 - \delta_F(N)} \sim \sqrt{N \log N}.$$ 

(2) If $F$ is reducible then

$$\psi_F(N) \sim c_F \sqrt{N}$$

for some explicit constant $c_F$.

**Remark.** The condition that $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly dependent means that $F$ is a function of essentially one variable (this will be made precise in the proof). In this case, the random model (1.1) predicts the correct results when
$F$ is irreducible, and even gives the correct constant, but fails in the reducible case.

**Theorem 1.3.** Let $F$ be as above, and assume that $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly independent.

1. If $\Delta$ is a perfect square, then $1 \ll \delta_F(N) \ll 1$ and $N \ll \psi_F(N) \ll N$.

2. If $\Delta$ is not a perfect square and $D = 0$ then

$$\frac{1}{\sqrt{\log N}} \ll \delta_F(N) \ll \frac{1}{\sqrt{\log N}} \quad \text{and} \quad N \ll \psi_F(N) \ll N.$$

**Remark.** The condition that $\Delta$ is a perfect square means that the homogeneous part of $F$ factors into linear terms over the rationals, and in this case the random model (1.1) predicts the correct order of magnitude. The condition that $D = 0$ means that $F$ is equivalent (over the rationals) to a (homogeneous) binary quadratic form. In this case the random model fails to give the correct order of magnitude for $\psi_F(N)$.

**Theorem 1.4.** Let $F$ be as above, and assume that $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly independent. Assume also that $\Delta$ is not a perfect square, and that $D \neq 0$. In this case

$$\frac{1}{\sqrt{\log N}} \ll \delta_F(N) \ll \frac{1}{\sqrt{\log N}},$$

$$\frac{N \log \log N}{\sqrt{\log N}} \ll \psi_F(N) \ll \frac{N \log \log N}{\sqrt{\log N}}.$$

**Remark.** In this case we have

$$\frac{N \log \log N}{\sqrt{\log N}} \asymp \frac{\log(\delta_F^{-1}(N))\delta_F(N)}{1 - \delta_F(N)},$$

which means that $\psi_F(N)$ has the same order of magnitude that we would expect from a random set according to (1.1).

However, precise asymptotics seem to be beyond our method. In Section 6 we give a conjecture for the asymptotics of $\psi_{x^2+y^2+1}(N)$, and present some numerical evidence.

We handle the degenerate cases (Theorems 1.2, 1.3) in Section 2. The bulk of the paper will be devoted to treating the generic case (Theorem 1.4). The main ingredients of the proof are the half-dimensional sieve, the Bombieri–Vinogradov theorem, and genus theory for quadratic forms.

**1.6. Notations and assumptions.** We say that a function $P(x, y) \in \mathbb{Z}[x, y]$ represents an integer $n$ if there exist $x_0, y_0 \in \mathbb{Z}$ such that $n = P(x_0, y_0)$. If there exist relatively prime $x_1, y_1 \in \mathbb{Z}$ such that $n = P(x_1, y_1)$ we say that $n$ is properly represented by $P$. 
Sums of the form $\sum_{n=1}^{F(x,y)\leq N} n$ are to be regarded as taken over positive integers $n \leq N$ which are represented by $F$, without counting the number of different representations of $n$ as $F(x,y)$.

Unless otherwise stated, we use $(\cdot, \cdot)$ to denote GCD, and $[\cdot, \cdot]$ to denote LCM. $F$ will denote the polynomial $ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x,y]$. We will denote by $G_F(x,y) = ax^2 + bxy + cy^2$ the homogeneous part of $F$; $\Delta = \Delta_F$ will denote the discriminant of $F$, and $D = D_F$ the large discriminant of $F$.

When relevant, we assume all implied constants coming from the $\ll$ and $O(\cdot)$ notations depend on $F$.

Throughout the paper, the letters $p, q$ will denote primes.

2. Proof of the degenerate cases. In this section we prove Theorems 1.2 and 1.3.

2.1. The single variable case. We begin with a proof of Theorem 1.2. 

Proof of Theorem 1.2. Let $F$ be as in Theorem 1.2. Since $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly dependent, there exist $A, B, \alpha, \beta, \gamma$ with $(A, B) = 1$ such that

$$A \frac{\partial F}{\partial x} = B \frac{\partial F}{\partial y} = \alpha x + \beta y + \gamma.\$$

It follows that $\alpha A = \beta B$ and

$$F(x,y) = \frac{1}{2A\alpha} (\alpha x + \beta y + \gamma)^2 + C$$

for some constant $C$. Hence, there is some quadratic polynomial $f(t) \in \mathbb{Z}[t]$ such that

$$F(x,y) = f\left(\frac{\alpha}{(\alpha,\beta)} x + \frac{\beta}{(\alpha,\beta)} y\right),$$

with leading coefficient $(\alpha, \beta)^2/(2A\alpha)$.

Furthermore,

$$a = \frac{\alpha}{2A} = \frac{\alpha^2}{2A\alpha}, \quad c = \frac{\beta}{2B} = \frac{\beta^2}{2A\alpha}.$$

We then get

$$(a, c) = \left(\frac{\alpha^2}{2A\alpha}, \frac{\beta^2}{2A\alpha}\right) = \frac{(\alpha, \beta)^2}{2A\alpha},$$

which is the leading coefficient of $f$.

To summarize, the image of $F(x,y)$ is equal to the image of $f(t)$, a quadratic polynomial with leading coefficient $(a, c)$. From this we see that

$$\delta_F(N) \sim \frac{1}{\sqrt{(a,c)N}}.$$
If $F$ is reducible, then so is $f$. This means that $f$ is a product of linear terms. Thus, from [8] we get

$$\psi_F(N) = \log \left( \frac{\text{LCM}_{0<n\leq \sqrt{N/(c,a)}} \{f(n)\}}{\sqrt{N}} \right) \sim c_f \frac{\sqrt{N}}{\sqrt{(c,a)}}$$

for some explicit constant $c_f$.

Assume now that $F$ is irreducible. This means that $f$ is also irreducible. Thus, from [4] we get

$$\psi_F(N) = \log \left( \frac{\text{LCM}_{0<n\leq \sqrt{N/(c,a)}} \{f(n)\}}{\sqrt{N}} \right) \sim \frac{\sqrt{N} \log N}{2 \sqrt{(a,c)}}.$$  

2.2. The degenerate discriminants case. Before proving Theorem [1.3] we prove the following two lemmas.

**Lemma 2.1.** Let $F$ be as in Theorem [1.3] If the image of $F$ contains an arithmetic progression, then

$$N \ll \psi_F(N) \ll N.$$  

**Proof.** The upper bound $\psi_F(N) \ll N$ always holds since

$$\psi_F(N) \ll \log(\text{LCM}\{1, \ldots, N\}) \sim N.$$  

Assume now that $\text{Im}(F)$ contains an arithmetic progression $\{An + B\}_{n \in \mathbb{Z}}$, $A \neq 0$. Denote $G = (A, B)$, and $A' = A/G$, $B' = B/G$. Note that $(A', B') = 1$. In this case we have

$$\psi_F(N) \gg \log \left( \frac{\text{LCM}_{0<n\leq (N-B)/A} \{A'n + B'\}}{\sqrt{N}} \right)$$

$$\gg \sum_{0<n\leq (N-B)/A} \Lambda(A'n + B') \gg N,$$

where the last inequality follows from Dirichlet’s theorem on primes in arithmetic progressions.  

We shall say that a polynomial $P(x, y) \in \mathbb{Z}[x, y]$ belongs to the class $\mathcal{H}$ if for every integer $A \neq 0$, $P$ represents an integer prime to $A$.

**Lemma 2.2.** Let

$$F = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y].$$  

Assume that $F$ represents arbitrarily large integers, and that $\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}$ are linearly independent. There exists $H \in \mathcal{H}$ and a constant $C_F$ such that $H$ has linearly independent partial derivatives, represents arbitrarily large integers, and

$$\delta_H(N) \ll \delta_F(C_FN), \quad \psi_H(N) \ll \psi_F(C_FN).$$  

Furthermore, the small and large discriminants of $H$ satisfy

$$\Delta_H = C_F^{-2} \Delta_F, \quad D_H = C_F^{-2} D_F.$$
Proof. Denote 
\[ F(x, y) = ax^2 + bxy + cy^2 + ex + fy + g. \]
From [10, Lemma 2] we find that the condition that \( F \) be in the class \( \mathcal{H} \) is equivalent to the conditions
\[ (a, b, c, e, f, g) = 1, \quad a, c, b, g \not\equiv e, f, 0, 0 \pmod{2}. \]
Denote \( W = (a, b, c, e, f, g) \). We start by defining \( G = W^{-1}F \). Denote 
\[ G(x, y) = a'x^2 + b'xy + c'y^2 + e'x + f'y + g'. \]
It is easy to see that \( G \) still represents arbitrarily large integers, and 
\[ \psi_F(WN) \sim \psi_G(N), \quad \delta_F(WN) \sim \delta_G(N). \]
If \( G \in \mathcal{H} \), pick \( H = G \) and \( C_F = W \). Otherwise, \( G \) represents only even integers. We then define \( H(x, y) = \frac{1}{2}G(2x, 2y) \). From [10, Lemma 2] we see that \( H \) is in \( \mathcal{H} \). Furthermore, it can be easily verified that \( H \) has linearly independent partial derivatives, and represents arbitrarily large integers. It can also be seen that 
\[ \psi_H(N) \ll \psi_G(2N), \quad \delta_H(N) \ll \delta_G(2N). \]
Thus, the statement of the lemma holds with \( H \) and \( C_F = 2W \). The statement about the discriminants of \( H \) follows from computation. 

Proof of Theorem 1.3. Let \( F \) be as in Theorem 1.3 and assume that \( \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} \) are linearly independent.
We begin by considering the case in which \( \Delta \neq 0 \) is a perfect square. Without loss of generality, we can assume \( a \neq 0 \). In this case, the quadratic part of \( F \), which we denote
\[ G_F(x, y) = ax^2 + bxy + cy^2, \]
satisfies \( 4aG_F(x, y) = (2ax + r_1y)(2ax + r_2y) \) with \( r_1, r_2 = b \pm \sqrt{\Delta} \). Since \( \Delta \neq 0 \), at least one of the vectors \((2a, r_1), (2a, r_2) \in \mathbb{Z}^2 \), say \((2a, r_1)\), is not proportional to \((f, e) \in \mathbb{Z}^2 \). Then
\[ F(r_1t, -2at) = t \cdot (r_1e - 2af) + g. \]
It follows that the image of \( F \) contains an arithmetic progression. Thus, from Lemma 2.1 we get 
\[ N \ll \psi_F(N) \ll N. \]
Assume now that \( \Delta = 0 \). In this case the quadratic part of \( F \) is a square. Assuming once more that \( a \neq 0 \) we get
\[ 4aF(x, y) = (2ax + by)^2 + 2c(2ax + by) + 2(2af - eb)y + 4ag. \]
Since \( \frac{\partial F}{\partial x}, \frac{\partial F}{\partial y} \) are linearly independent, we must have \( 2af - eb \neq 0 \). It follows that
\[ F(bt, -2at) = t \cdot (2af - be) + g. \]
Thus, the image of $F$ contains an arithmetic progression, so from Lemma 2.1 we get

\[ N \ll \psi_F(N) \ll N. \]

Note that we showed that if $\Delta$ is a perfect square (zero or non-zero), the image of $F$ contains an arithmetic progression. Hence, in this case

\[ 1 \ll \delta_F(N) \ll 1. \]

Consider now the case where $\Delta$ is not a perfect square, and $D = 0$. Let $H \in \mathbb{Z}[x, y]$ be as in Lemma 2.2, and $C_F$ the constant from the lemma. Like $F$, the discriminant of $H$ is not a perfect square, and the large discriminant is 0. From [10, Proposition 3], we get

\[ \sum_{\substack{p \leq N \\ p \text{ prime}}} 1 \gg \frac{N}{\log N}. \]

It follows that $\psi_H(N) \gg N$. Since

\[ \psi_F(N) \gg \psi_H(C_F N) \gg N \]

we get $\psi_F(N) \gg N$ as required. Note that the upper bound $\psi_F(N) \ll N$ is always true as previously noted.

The bounds

\[ \frac{1}{\sqrt{\log N}} \ll \delta_F(N) \ll \frac{1}{\sqrt{\log N}} \]

are given in Lemmas 4.9 and 4.10.

3. Proof of the generic case. In this section we prove Theorem 1.4. That is, we show that for $F$ satisfying the assumption of Theorem 1.4,

\[ \frac{N \log \log N}{\sqrt{\log N}} \ll \psi_F(N) \ll \frac{N \log \log N}{\sqrt{\log N}}. \]

For the proof we will need estimations for the number of small multiples of large primes represented by $F$. These estimates will be stated in Lemmas 3.4, 3.6 and 3.7 which we will prove in Section 5. The claim that $\delta_F(N)$ has order of magnitude $\frac{1}{\sqrt{\log N}}$ is given in Lemmas 4.9 and 4.10.

Throughout the section we assume that

\[ F(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y] \]

satisfies the assumptions of Theorem 1.4. We denote by $\Delta = b^2 - 4ac$ the discriminant of $F$, and by $D = af^2 + ce^2 - bfe + \Delta g$ the large discriminant of $F$. 
3.1. The upper bound. In this section we prove the following:

**Proposition 3.1.**

\[ \psi_F(N) \ll \frac{N \log \log N}{\sqrt{\log N}}. \]

We begin by stating some preliminary lemmas, and then show how Proposition 3.1 follows.

**Lemma 3.2.** Denote

\[ \text{LCM}_{0 < F(x, y) \leq N} \{ F(x, y) \} = \prod_{p \leq N \atop p \text{ prime}} p^{\theta_p}. \]

Then

\[ \sum_{p \leq N \atop p \text{ prime} \atop \theta_p \geq 2} \left( \theta_p - 1 \right) \log p = \mathcal{O}(\sqrt{N}). \]

This lemma shows that the contribution to \( \psi_F(N) \) coming from multiplicities is negligible.

**Proof.** Indeed,

\[ \sum_{p \leq N \atop p \text{ prime} \atop \theta_p > 1} (\theta_p - 1) \log p \leq \sum_{m \geq 2} \sum_{p \leq N^{1/m} \atop p \text{ prime}} \log p \ll \sqrt{N}. \]

**Lemma 3.3.** With the notations from Lemma 3.2, and for \( s > 0 \),

\[ \sum_{p \leq N/\log^s N \atop p \text{ prime} \atop \theta_p \geq 1} \log p \ll \frac{N}{\log^s N}. \]

This lemma will be used to bound the contribution of small primes to the LCM.

**Proof.** We have

\[ \sum_{p \leq N/\log^s N \atop p \text{ prime} \atop \theta_p \geq 1} \log p \leq \sum_{p \leq N/\log^s N \atop p \text{ prime}} \log p \ll \frac{N}{\log^s N}. \]

**Lemma 3.4.** For \( k \leq \log^5 N \) denote

\[ S_k(N) = \sum_{kp = F(x, y) \leq N \atop p \text{ prime}} 1. \]
Then
\[ S_k(N) \ll \frac{N}{k \log^{3/2} N} \prod_{q | k} \left( 1 - \frac{1}{q} \right)^{-1}. \]

We postpone the proof of this lemma to Section 5.

We can now prove the upper bound for \( \psi_F(N) \).

**Proof of Proposition 3.1.** From Lemmas 3.2 and 3.3 we get
\begin{align*}
\psi_F(N) &= \sum_{p \text{ prime}} \log p + \mathcal{O} \left( \frac{N}{\sqrt{\log N}} \right).
\end{align*}

With the notation of Lemma 3.4 we get
\begin{align*}
\sum_{p \text{ prime}} \log p &\ll \log N \sum_{k \leq \sqrt{\log N}} S_k(N).
\end{align*}

From Lemma 3.4 we then get
\begin{align*}
\sum_{p \text{ prime}} \log p &\ll \log N \frac{N}{\log^{3/2} N} \sum_{k \leq \sqrt{\log N}} \frac{1}{k} \prod_{q | k} \left( 1 - \frac{1}{q} \right)^{-1} \ll \frac{N \log \log N}{\sqrt{\log N}}.
\end{align*}

Consequently, from (3.1)–(3.2) we get
\[ \psi_F(N) \ll \frac{N \log \log N}{\sqrt{\log N}}. \]

**3.2. The lower bound.** We now look at the lower bound.

**Proposition 3.5.** We have
\[ \psi_F(N) \gg \frac{N \log \log N}{\sqrt{\log N}}. \]

We begin by stating some relevant lemmas.

**Lemma 3.6.** For \( k \leq \log^5 N \) denote
\[ S_k(N) = \sum_{kp = F(x,y) \leq N} 1. \]
There exists a constant $c_F$ depending only on $F$ such that if $k$ is prime to $c_F$ then
\[
S_k(N) \gg \frac{N}{k \log^{3/2} N} \prod_{\substack{q \mid k \\ (\frac{q}{k}) = -1}} \left( 1 - \frac{1}{q} \right)^{-1}
\]

**Lemma 3.7.** Let $k_2 < k_1 \leq \log^5 N$, and denote
\[
S_{k_1,k_2}(N) = \sum_{p \text{ prime}} 1.
\]

Then
\[
S_{k_1,k_2}(N) \ll \frac{N}{k_1 \log^2 N} \prod_{\substack{q \mid k_1 k_2 (k_1 - k_2) \\ q > 3}} \left( 1 - \frac{3}{q} \right)^{-1}.
\]

We postpone the proofs of Lemmas 3.6 and 3.7 to Section 5.

**Proof of Proposition 3.5**. By ignoring small primes, we have
\[
\psi_F(N) \geq \sum_{p \text{ prime}} \log p \sim \log N \sum_{p \text{ prime}} 1.
\]

An iteration of the inclusion-exclusion principle then gives
\[
\frac{1}{\log N} \psi_F(N) \gg \sum_{k \leq \log^{1/2 - \epsilon} N} S_k(N) - \sum_{k_1 \leq \log^{1/2 - \epsilon} N} \sum_{k_2 < k_1} S_{k_1,k_2}(N),
\]

where $c_F$ is the constant from Lemma 3.6.

For the first sum we use Lemma 3.6 to get
\[
\sum_{k \leq \log^{1/2 - \epsilon} N} S_k(N) \gg \frac{N}{\log^{3/2} N} \sum_{k \leq \log^{1/2 - \epsilon} N} \frac{1}{k} \gg \frac{N \log \log N}{\log^{3/2} N}.
\]

For the second double sum we use Lemma 3.7 and noting that
\[
\prod_{\substack{q \mid k_1 k_2 (k_1 - k_2) \\ q > 3}} \left( 1 - \frac{3}{q} \right)^{-1} \ll (\log \log N)^3.
\]
we get

\[
\sum_{k_1 \leq \log^{1/2-\epsilon} N} \sum_{k_2 < k_1} S_{k_1,k_2}(N) = \ll \sum_{k_1 \leq \log^{1/2-\epsilon} N} \frac{1}{k_1} \sum_{k_2 < k_1} \frac{N(\log \log N)^3}{\log^2 N} \ll \frac{N(\log \log N)^3}{\log^{3/2+\epsilon} N}.
\]

From (3.3)–(3.5) we get

\[\psi_F(N) \gg \frac{N \log \log N}{\sqrt{\log N}}\]
as required.

4. Preliminary lemmas. In this section we prove some lemmas which will be used in the following section.

4.1. Lemmas from sieve theory

**Theorem 4.1 (Bombieri–Vinogradov theorem).**

\[
\sum_{Q \leq \sqrt{N}/\log^{35} N} \max_{a, (a,Q) = 1} \left| \pi(N, Q; a) - \frac{\text{Li}(N)}{\phi(Q)} \right| \ll \frac{N}{\log^{30} N}.
\]

**Proof.** Follows from [7, Theorem 1].

**Theorem 4.2 (Main theorem of the $\beta$-sieve).** Let $\kappa \geq 0$ be a real number (referred to as the sieve dimension). Let $\mathcal{P}$ be a set of primes. Let $\mathcal{A} = (a_n)$ be a finite sequence of non-negative numbers. Denote $\mathcal{A}_\lambda$ the subsequence of $\mathcal{A}$ consisting of those $a_n$ with $\lambda \mid n$. Denote also $|\mathcal{A}_\lambda| = \sum_{\lambda \mid n} a_n$.

Let $X > 0$ be a real number, and let $g(\lambda)$ be a multiplicative function satisfying $0 \leq g(p) < 1$. Denote

\[|\mathcal{A}| = g(\lambda)X + r_\lambda.
\]

Assume that there exists $L \geq 1$ such that for all $2 \leq w < z$ we have

\[\prod_{\substack{w \leq p < z \\ p \in \mathcal{P}}} (1 - g(p))^{-1} \leq \left( \frac{\log z}{\log w} \right)^{\kappa} \left( 1 + \frac{L}{\log w} \right).
\]

Let $2 < z \leq D$, and denote $s = \log D/\log z$. Denote $P(z) = \prod_{p < z, p \in \mathcal{P}} p$ and $S(\mathcal{A}, z) = \sum_{(n, P(z)) = 1} a_n$. Then

\[
S(\mathcal{A}, z) \leq X \prod_{\substack{p < z \\ p \in \mathcal{P}}} (1 - g(p)) \left\{ C_\kappa(s) + O\left( \frac{1}{\log^{1/6} D} \right) \right\} + \sum_{\lambda \mid P(z), \lambda \leq D} |r_\lambda|.
\]
\begin{align}
|A_\lambda^\Omega| &= \sum_{\forall p \mid \lambda : n \mod p \in \Omega_p} a_n.
\end{align}

Let $X > 0$ be a real number, and denote

\begin{align}
|A_\lambda^\Omega| &= X g(\lambda) + r_\lambda.
\end{align}

Let $2 < z \leq D$, and denote $s = \log D / \log z$ and $P(z) = \prod_{p < z, p \in \mathcal{P}} p$. Further denote

\begin{align}
S(\mathcal{A}, z, \Omega) &= \sum_{\forall p \mid P(z) : n \mod p \notin \Omega_p} a_n.
\end{align}

Then

\begin{align}
S(\mathcal{A}, z, \Omega) &\leq X \prod_{p < z, p \in \mathcal{P}} (1 - g(p)) \left\{ C_\kappa(s) + \mathcal{O}\left( \frac{1}{\log^{1/6} D} \right) \right\} + \sum_{\lambda \mid P(z) \atop \lambda \leq D} |r_\lambda|,
\end{align}

\begin{align}
S(\mathcal{A}, z, \Omega) &\geq X \prod_{p < z, p \in \mathcal{P}} (1 - g(p)) \left\{ c_\kappa(s) + \mathcal{O}\left( \frac{1}{\log^{1/6} D} \right) \right\} - \sum_{\lambda \mid P(z) \atop \lambda \leq D} |r_\lambda|,
\end{align}

where the functions $C_\kappa, c_\kappa$ satisfy

\begin{align}
C_\kappa(s) &= 1 + O(e^{-s}), 
\quad c_\kappa(s) = 1 + O(e^{-s}).
\end{align}

If $\kappa = 1/2$ then $s^{1/2}C(s) = 2\sqrt{e^\gamma / \pi}$ for $0 \leq s \leq 2$, and

\begin{align}
s^{1/2}C(s) &= \sqrt{e^\gamma} \int_1^s \frac{dt}{\pi (t(t - 1))^{1/2}}
\end{align}

for $1 \leq s \leq 3$.

The constants in the $\mathcal{O}$ notations depend only on $\kappa, L$.

\textbf{Proof.} The bounds (4.2), (4.3) are given in [6, Theorem 11.13]. The claim in (4.4) is given in [6, (11.68)]. The expressions for $C_{1/2}, c_{1/2}$ are given in [6, Chapter 14].

We are going to use Theorem 4.2 with $\kappa = 1/2$ and $\kappa = 2$. When applied with $\kappa = 2$, we will also need a slight variation of Theorem 4.2 which allows us to sift by non-zero residue classes.

\textbf{Theorem 4.3.} Let $\mathcal{P}$ be a set of primes. Let $\mathcal{A} = (a_n)$ be a finite sequence of non-negative numbers. For each $p \in \mathcal{P}$ let $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$ be a set of residue classes modulo $p$. Let $g$ be a multiplicative function with $0 \leq g(p) < 1$. Let $\kappa \geq 0$ be some number, and assume $g$ satisfies (4.1) with $\kappa$ and some $L \geq 1$. Denote by $A_{\Omega}^\lambda$ the subsequence of $\mathcal{A}$ consisting of those $n$’s for which $n \mod p$ is in $\Omega_p$ for all $p | \lambda$, and denote

\begin{align}
S(\mathcal{A}, z) &= \prod_{\forall p \mid P(z)} (1 - g(p)) \left\{ C_\kappa(s) + \mathcal{O}\left( \frac{1}{\log^{1/6} D} \right) \right\} + \sum_{\lambda \mid P(z) \atop \lambda \leq D} |r_\lambda|.
\end{align}

\begin{align}
S(\mathcal{A}, z) &\geq X \prod_{p < z, p \in \mathcal{P}} (1 - g(p)) \left\{ c_\kappa(s) + \mathcal{O}\left( \frac{1}{\log^{1/6} D} \right) \right\} - \sum_{\lambda \mid P(z) \atop \lambda \leq D} |r_\lambda|,
\end{align}

where $S(\mathcal{A}, z)$ is the average of $\mathcal{A}$ over all residue classes modulo $P(z)$.
where the functions $C_\kappa, c_\kappa$ satisfy

$$C_\kappa(s) = 1 + O(e^{-s}), \quad c_\kappa(s) = 1 + O(e^{-s}).$$

The constants in the $O$ notations depend only on $\kappa, L$.

**Proof.** Define the function

$$f(n) = \prod_{\substack{p \in P \ni p \leq z \mod p \in \Omega_p}} p.$$ 

We now define the sequence $B = (b_m)$ by

$$b_m = \sum_{f(n) = m} a_n.$$ 

With these notations, $|A^\Omega_\lambda| = |B^\lambda|$ and $S(A, z, \Omega) = S(B, z)$. Applying Theorem 4.2 to the sequence $B$ gives the required result. 

**Remark.** We will at times apply Theorems 4.2 and 4.3 with a finite set $M \subset \mathbb{N}$ in place of the sequence $A$, in which case the sequence $A$ is to be understood as the indicator series of $M$: $a_n = \mathbb{1}_M(n)$.

### 4.2. Technical lemmas

**Lemma 4.4.** Let $A \neq 0$ be an integer. If an integer $\Delta \equiv 0, 1 \pmod{4}$ is different from a perfect square then there exists a constant $c = c(\Delta)$ which does not depend on $A$ such that for all $x > 2$,

$$\sum_{m \leq x \atop q | m \Rightarrow (\frac{\Delta}{q}) = 1 \atop (m, A) = 1} m^{-1} \log^{-2}(3 + \frac{x}{m}) \prod_{q | m} \left(1 - \frac{1}{q}\right)^{-2} \leq c \log^{-3/2} x \prod_{q | A \atop (\frac{\Delta}{q}) = 1} \left(1 - \frac{1}{q}\right).$$

**Proof.** Throughout the proof, the constants $c_i$ will depend on $\Delta$. We have

$$\sum_{m \leq x \atop q | m \Rightarrow (\frac{\Delta}{q}) = 1 \atop (m, A) = 1} \frac{1}{m} \prod_{q | m} \left(1 - \frac{1}{q}\right)^{-2} \leq \prod_{q \leq x \atop (\frac{\Delta}{q}) = 1 \atop (q, A) = 1} \left(1 + \frac{1}{q} + \frac{2}{q(q - 1)} + \frac{1}{q(q - 1)^2}\right)$$

$$\leq c_1 \log^{1/2} x \prod_{q | A \atop (\frac{\Delta}{q}) = 1} \left(1 - \frac{1}{q}\right).$$

Denote $a(m) = \log^{-2}(3 + x/m)$. Then for $1 \leq m \leq x$,

$$a'(m) \leq 2m^{-1} \log^{-3} \left(3 + \frac{x}{m}\right).$$
By partial summation we now get
\[
\sum_{m \leq x} m^{-1} \log^{-2} \left( 3 + \frac{x}{m} \right) \prod_{q|m} \left( 1 - \frac{1}{q} \right)^{-2} \leq c_2 \prod_{q|A} \left( 1 - \frac{1}{q} \right) \left( \frac{x}{m} \log \frac{3}{1 - \frac{1}{q}} \right) \leq c_3 \log^{3/2} x \prod_{q|A} \left( 1 - \frac{1}{q} \right). \]

**Lemma 4.5.** Let \( \Delta \neq 0 \) be some integer. Then for \( X \geq 1 \),

\[
\sum_{(r_1, \Delta) = 1} \sum_{(r_2, \Delta) = 1} \sum_{q|d_1 \Rightarrow q|\Delta} \sum_{q|d_2 \Rightarrow q|\Delta} \frac{1}{[r_1^2 d_1, r_2^2 d_2]} \leq c(\Delta) \frac{\log^2 X + 1}{\sqrt{X}}.
\]

**Proof.** Throughout the proof, the constants \( c_i \) will depend on \( \Delta \). We denote
\[
\tau(n) = \sum_{[a,b]=n} 1 = \sum_{d|n^2} 1.
\]

For \( s > 0 \) we have
\[
\sum_{k=0}^{\infty} \frac{\tau(p^k)}{p^{sk}} = \sum_{k=0}^{\infty} (2k + 1) p^{-sk} = \frac{1 + p^{-s}}{(1 - p^{-s})^2}.
\]

It is also known that
\[
\sum_{n \leq N} \tau(n) \asymp N \log^2 N.
\]

By changing the order of summation, enumerating over \( l_r = [r_1, r_2] \) and \( l_d = [d_1, d_2] \), we find that the LHS of (4.5), which we will denote \( \Sigma \), satisfies
\[
\Sigma = \sum_{(r_1, \Delta) = 1} \sum_{q|d_1 \Rightarrow q|\Delta} \frac{\tau(l_r) \tau(l_d)}{l_r^2 l_d}.
\]

We separate the last sum into two sums as follows:
\[
\Sigma \leq \sum_{l_d \leq X} \sum_{q|d_1 \Rightarrow q|\Delta} \frac{\tau(l_r) \tau(l_d)}{l_r^2 l_d} + \sum_{l_d \geq X} \sum_{q|d_1 \Rightarrow q|\Delta} \frac{\tau(l_r) \tau(l_d)}{l_r^2 l_d} = \Sigma_1 + \Sigma_2.
\]
We begin by estimating $\Sigma_1$. From (4.7) and partial summation we have

$$\sum_{l_r(X/l_d)^{1/2} \geq (l_r, \Delta) = 1} \frac{\tau(l_r)}{l_r^2} \leq c_1 \frac{\log^2 X}{\sqrt{X}} \sqrt{l_d}.$$

Hence,

$$\Sigma_1 \leq \sum_{l_d < X \atop q|l_d \Rightarrow q|\Delta} \frac{\tau(l_d)}{l_d} \sum_{l_r \geq (X/l_d)^{1/2} \atop (l_r, \Delta) = 1} \frac{\tau(l_r)}{l_r^2} \leq c_2 \frac{\log^2 X}{\sqrt{X}} \sum_{l_d \atop q|l_d \Rightarrow q|\Delta} \frac{\tau(l_d)}{\sqrt{l_d}} \leq c_2 \frac{\log^2 X}{\sqrt{X}} \prod_{q|\Delta} \frac{1 + q^{-1/2}}{(1 - q^{-1/2})^2},$$

where for the last equality we have used (4.6). It follows that

$$\Sigma_1 \leq c_3 \frac{\log^2 X}{\sqrt{X}}.$$  \hspace{1cm} (4.9)

As for $\Sigma_2$, we find that for $\delta > 0$,

$$\Sigma_2 \leq c_4 \sum_{l_r} \frac{\tau(l_r)}{l_r^2} \sum_{l_d > X \atop q|l_d \Rightarrow q|\Delta} \frac{\tau(l_d)}{l_d} \leq c_5 \sum_{l_d \atop q|l_d \Rightarrow q|\Delta} \frac{\tau(l_d)}{l_d} \left( \frac{l_d}{X} \right)^{\delta}$$

$$= c_5 \frac{\log^2 X}{\sqrt{X}} \prod_{q|\Delta} \frac{1 + q^{-1/2}}{(1 - q^{-1/2})^2} \leq c_6 (\delta) \frac{\log^2 X}{X^{\delta}},$$

where we have once more used (4.6). Choosing $\delta = 1/2$ we get

$$\Sigma_2 \ll X^{-1/2}.$$ \hspace{1cm} (4.10)

Thus, from (4.7), (4.9), (4.10) we get

$$\Sigma \leq c \frac{\log^2 X + 1}{\sqrt{X}},$$

as required.  \hspace{1cm} $\blacksquare$

**Lemma 4.6.** Let $\Delta \neq 0$ be some integer. Then for $X > 0$,

$$\sum_{(r_1, \Delta) = 1 \atop (r_2, \Delta) = 1} \sum_{d_1 \atop q|d_1 \Rightarrow q|\Delta} \sum_{d_2 \atop q|d_2 \Rightarrow q|\Delta} \sum_{[r_1^2 d_1, r_2^2 d_2] \leq X} 1 \leq c(\Delta) \sqrt{X} \log^2 X.$$ \hspace{1cm} (4.11)

**Proof.** We use the notations from Lemma 4.5. Denoting the LHS of (4.11) by $\Sigma$, we get

$$\Sigma \leq \sum_{l_d \leq X \atop q|l_d \Rightarrow q|\Delta} \tau(l_d) \sum_{l_r \leq \sqrt{X/l_d}} \tau(l_r).$$
From (4.7) we then get

$$\Sigma \leq \sqrt{X} \log^2 X \sum_{q \mid q_1 \Rightarrow q_2 \mid \Delta} \frac{\tau(l_d)}{\sqrt{l_d}} = \sqrt{X} \log^2 X \prod_{q \mid \Delta} \frac{1 + q^{-1/2}}{(1 - q^{-1/2})^2},$$

where the last equality follows from (4.6).

**Lemma 4.7.** Let $\Delta \neq 0$ be some integer. Then

$$\Sigma \ll Y \prod_{p \nmid \Delta} \left( 1 + \left( \frac{1 + p^{-2}}{(1 - p^{-2})^2} - 1 \right) \left( 1 - \frac{3}{p} \right)^{-1} \right) \prod_{p \mid \Delta} \frac{1 + p^{-1}}{(1 - p^{-1})^2}$$

where the last equality follows from (4.6).

**Proof.** Denote the LHS of (4.12) by $\Sigma$. Using the notations from Lemma 4.5 we can rewrite $\Sigma$ as

$$\Sigma = \sum_{(l_r, \Delta) = 1} \sum_{q \mid l_r \Rightarrow q_2 \mid \Delta} \frac{\tau(l_r) \tau(l_d)}{l_r^2 l_d^2} \prod_{q \mid q_1 r_2, q > 3} \left( 1 - \frac{3}{q} \right)^{-1}.$$

We can write this last sum as an Euler product. Using (4.6) we get

$$\Sigma \ll \prod_{p \nmid 6 \Delta} \left( 1 + \left( \frac{1 + p^{-2}}{(1 - p^{-2})^2} - 1 \right) \left( 1 - \frac{3}{p} \right)^{-1} \right) \prod_{p \mid \Delta} \frac{1 + p^{-1}}{(1 - p^{-1})^2}$$

$$\leq \frac{c(\Delta)}{\prod_{p \mid \Delta} \left( 1 + \frac{O(1)}{p^2} \right)} \ll 1.$$

**4.3. Lemmas for quadratic polynomials.** We now state an important lemma from [10] regarding representability by a quadratic polynomial $F(x, y)$ in $\mathbb{Z}[x, y]$. This lemma will help us reduce the problem of representability by $F$ to that of representability by a homogeneous quadratic form.

Let

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y].$$

Denote by $\Delta_F$ the discriminant of $F$, and by $D_F$ the large discriminant of $F$. Denote also

$$\alpha = bf - 2ce, \quad \beta = be - 2af.$$

Assume further that $F$ is in the class $\mathcal{H}$, that $F$ represents arbitrarily large integers, that the partial derivatives of $F$ are linearly independent, and that $\Delta_F$ is not a perfect square.

We will further assume that $F$ satisfies

$$\tag{4.13} (a, b, c) \mid (e, f), \quad (ac, \Delta) = (a, b, c)^2, \quad (g, \Delta) = 1, \quad (\alpha, \beta) \mid \Delta.$$

Before stating the lemma, we introduce some notations. We define $W = (a, b, c, e, f)$ (which is equal to $(a, b, c)$ due to (4.13)), and $P(x, y) = \frac{ax^2 + bxy + cy^2 + ex + fy + g}{2}$. In the next lemma we write $P(x, y)$ with respect to $W = (a, b, c, e, f)$.
$W^{-1}(F-g)$, which we denote

$$P(x, y) = a_Px^2 + b_Pxy + c_Py^2 + e_px + f_py.$$  

We denote by $\Delta_P = W^{-2}\Delta_F$ the discriminant of $P$. We also set

$$\alpha_P = W^{-2}\alpha, \quad \beta_P = W^{-2}\beta, \quad G_P(x, y) = a_Px^2 + b_Pxy + c_py^2.$$  

From the equations

$$2a_P\alpha_P + b_P\beta_P = \Delta_pe_P, \quad 2c_P\beta_P + b_P\alpha_P = \Delta_pf_P,$$

we have $(2\alpha_P, \Delta_P) = (2\beta_P, \Delta_P)$. Hence, one of $(\alpha_P, \Delta_P), (\beta_P, \Delta_P)$ must divide the other, say $(\beta_P, \Delta_P) | (\alpha_P, \Delta_P)$. Set

$$\alpha_1 = \frac{\alpha_P}{(\beta_P, \Delta_P)}, \quad \beta_1 = \frac{\beta_P}{(\beta_P, \Delta_P)}, \quad \Delta_1 = \frac{\Delta_P}{(\beta_P, \Delta_P)}$$

and

$$\varphi(x, y) = G_P\left(\frac{3 + (-1)^{(\alpha_1, \Delta_1)}}{2}x, y\right).$$

With these notations we have:

**Lemma 4.8** ([10, Corollary 2]). Let $F$ be as above. Let $A \in \mathbb{Z}\setminus\{0\}$. There exists an integer $Q$ prime to $A$ (which is explicitly given in [10]) such that the following holds. If $n$ is an integer such that $n \equiv g \pmod{W}$,

$$4a_P\frac{n-g}{W} + e_P^2$$

is a quadratic residue modulo $(2\beta_P, \Delta_P)$, and

$$4a_P\frac{n-g}{W} + G_P(\alpha_1, \beta_1) = Q^2\varphi(x, y)$$

has a solution $x, y$ such that $(x, y, \Delta_1) = 1$, then $n$ is represented by $F$.

We now show how this lemma gives a lower bound on $\delta_F(N)$.

**Lemma 4.9.** Let

$$F(x, y) = ax^2 + bxy + cy^2 + ex + fy + g \in \mathbb{Z}[x, y].$$

Assume that $F$ represents arbitrarily large integers, that the partial derivatives of $F$ are linearly independent, and that $\Delta_F$ is not a perfect square. Then

$$\delta_F(N) \gg \frac{1}{\sqrt{\log N}}.$$  

**Proof.** From Lemma 2.2 we see that it is enough to prove the statement for $F$ in $\mathcal{H}$. We can further assume that $F$ satisfies (4.13). This follows from [10, Lemma 3] which states that there is an affine change of variables

$$F'(x, y) = F(a_1x + a_2y + a_3, b_1x + b_2y + b_3)$$

such that $F'$ is still in $\mathcal{H}$ and satisfies (4.13). Once more, since $\psi_F(N) \ll \psi_F(N)$, we can simply assume that $F$ satisfies (4.13).
Let \( Q \) be as in Lemma 4.8 for \( A = \Delta D \). From [10, Lemma 6], there exists an integer \( R \) prime to \( A \) such that if \( n \) is properly represented by the genus of \( \varphi \), then \( R^2 n \) is represented by \( \varphi \) with a representation \( R^2 n = \varphi(x_0, y_0) \) which satisfies \((x_0, y_0) \mid R\). We use the notations from Lemma 4.8. Denote \( \Delta = 3 - (-1)^{\Delta P D F} QR \).

Since \((\alpha_1, \beta_1) = 1\), the number \( G_P(\alpha_1, \beta_1) \) is properly represented by \( \varphi \). Let \( d \) be the greatest divisor of \( G_P(\alpha_1, \beta_1) \) whose prime factors all divide \( \Delta \). Let \( L \) be defined by the congruence

\[
C^2 L \equiv \frac{G_P(\alpha_1, \beta_1)}{d} \pmod{\Delta}, \quad 0 < L < |\Delta|.
\]

Denote also

\[
T = C^2 W \frac{|d\Delta|}{\Delta^2}, \quad l = W \frac{C^2 d L - G_P(\alpha_1, \beta_1)}{\Delta^2} + g.
\]

From the proof of [10, Lemma 13] we then deduce that for \( n \equiv l \pmod{T} \) the number

\[
4 a_P \frac{n - g}{W} + e_P^2
\]

is a quadratic residue modulo \((2\beta_P, \Delta_P)\), and \( n \equiv g \pmod{W} \). Thus, from Lemma 4.8 we see that in order for an integer \( n \equiv l \pmod{T} \) to be represented by \( F \), it is enough that \( \Delta^2 (n - g)/W + G(\alpha_1, \beta_1) \) be of the form \( Q^2 \varphi(x_0, y_0) \) with \( x_0, y_0 \) satisfying \((x_0, y_0, \Delta_1) = 1\). We can denote

\[
\frac{\Delta^2 (n - g)}{W} + G(\alpha_1, \beta_1) = C^2 dm
\]

with \( m \equiv L \pmod{\Delta} \). From our choice of \( R \), if \( C^2 dm/(QR)^2 \) is properly represented by the genus of \( \varphi \), then \( C^2 dm \) is of the form \( Q^2 \varphi(x_0, y_0) \) with \( x_0, y_0 \) satisfying \((x_0, y_0) \mid R\). Since \((R, \Delta_1) = 1\), we also have \((x_0, y_0, \Delta_1) = 1\). From [10 Lemma 7], the condition \( q \mid m \Rightarrow (\frac{\Delta}{q}) = 1 \) is sufficient for \( C^2 dm/(QR)^2 \) to be properly represented by the genus of \( \varphi \).

Thus,

\[
\sum_{0 < n \leq N} 1 \gg \sum_{n \equiv P(x,y)} \sum_{m \leq N} \sum_{m \equiv L \pmod{\Delta}} \sum_{q \mid m} \sum_{(\frac{\Delta}{q}) = 1} 1.
\]

The last sum can be bounded from below using a \( \frac{1}{2} \)-dimensional sieve. We start with the set \( M = \{m \leq N \mid m \equiv L \pmod{\Delta} \} \). For \( \lambda \) prime to \( \Delta \) with all prime factors \( q \) of \( \lambda \) satisfying \((\frac{\Delta}{q}) = 1 \) we denote \( M_\lambda = \{m \in M \mid \lambda \mid m\} \). Then \(|M_\lambda| = \frac{N}{\lambda |\Delta|} + O(1)\).
Since each \( m \in \mathcal{M} \) satisfies \( \left( \frac{\Delta \varphi}{m} \right) = 1 \), it has to be divisible by an even number of primes \( q \) for which \( \left( \frac{\Delta \varphi}{q} \right) = -1 \). It follows that it is enough to sieve out primes up to \( \sqrt{N} \).

Thus, applying Theorem 4.2 with \( D = N \log^{-2} N \) and some \( 1 < s < 2 \) we get

\[
\sum_{\substack{m \leq N \\ m \equiv L \pmod{\Delta \varphi} \\ q|m \Rightarrow \left( \frac{\Delta \varphi}{q} \right) = 1}} 1 \]

\[
\gg N \prod_{p \leq D^{1/s} \atop \left( \frac{\Delta \varphi}{p} \right) = -1} \left( 1 - \frac{1}{p} \right) \left\{ c_{1/2}(s) + O(\log^{-1/6} D) \right\} + O \left( \frac{N}{\log^{2} N} \right)
\]

\[
= \frac{N}{\sqrt{\log N}}.
\]

Consequently,

\[
\delta_F(N) \gg \frac{1}{N} \sum_{\substack{m \leq N \\ m \equiv L \pmod{\Delta \varphi} \\ q|m \Rightarrow \left( \frac{\Delta \varphi}{q} \right) = 1}} 1 \gg \frac{1}{\sqrt{\log N}}. \tag{4.14}
\]

**Lemma 4.10.** Let \( F \) be as in Lemma 4.9. Then

\[
\delta_F(N) \ll \frac{1}{\sqrt{\log N}}.
\]

**Proof.** Denote \( G(x, y) = ax^2 + bxy + cy^2 \). One can check that

\[
\Delta_F^2 F(x, y) = G(\Delta_F x + \alpha, \Delta_F y + \beta) + D_F \Delta_F.
\]

Denote \( G'(x, y) = (a, b, c)^{-1} G(x, y) \). It follows that \( \delta_F(N) \ll \delta_{G'}(N) \). From genus theory for quadratic forms, it is known that if \( n = G'(x, y) \) then \( n \) must be of the form \( n = r^2 dm \) where \( q \mid d \Rightarrow q \mid \Delta_{G'} \), and \( q \mid m \Rightarrow \left( \frac{\Delta_{G'}}{q} \right) = 1 \).

Thus, we have

\[
\sum_{n \leq N \atop n = F(x, y)} 1 \ll \sum_{r} \sum_{d \leq N/r^2} \sum_{m \leq N/r^2 d \atop q|m \Rightarrow \left( \frac{\Delta_{G'}}{q} \right) = 1} 1.
\]

Once more, we can bound the last sum using the \( \frac{1}{2} \)-dimensional sieve. For \( X > 0 \), let \( \mathcal{M} = \{ m \mid m \leq X \} \), and \( \mathcal{M}_\lambda = \{ m \in \mathcal{M} \mid \lambda \mid m \} \). Let

\[
\mathcal{P} = \left\{ p \mid \left( \frac{\Delta_{G'}}{p} \right) = -1 \right\}.
\]
Applying Theorem 4.2 with $D = X/\log^2 X$ and some $s \geq 1$ we get
\[
\sum_{m \leq X, q|m \Rightarrow \frac{A^{G'}}{q}=1} 1 \ll X \prod_{p \leq D^{1/s}} \left(1 - \frac{1}{p}\right) \{C_{1/2}(s) + O((\log^{-1/6} D))\} + O\left(\frac{X}{\log^2 X}\right)
\]
\[
\ll \frac{X}{\sqrt{\log(X+3)}}.
\]
Plugging this into (4.14) we get
\[
\sum_{n \leq N} 1 \ll \sum_{n=F(x,y)} \sum_{d|n} \frac{N}{r^2d\sqrt{\log\left(\frac{N}{r^2d} + 3\right)}} \ll \frac{N}{\sqrt{\log N}}.
\]
It follows that $\delta_F(N) \ll 1/\sqrt{\log N}$. 

5. Small multiples of large primes represented by $F$. In this section we prove Lemmas 3.4, 3.6 and 3.7. These lemmas all have to do with estimating the number of small multiples of large primes which are represented by $F$. Throughout the section, we let $F$ be as in Theorem 1.4, and we use the same notations.

We further denote
\[
\alpha = bf - 2ce, \quad \beta = be - 2af,
\]
and let $G_F(x, y) = ax^2 + bxy + cy^2$ be the quadratic part of $F$.

5.1. An upper bound for $S_k(N)$

Proof of Lemma 3.4. By computation, one can see that
\[
\Delta^2 F(x, y) = G_F(\Delta x + \alpha, \Delta y + \beta) + \Delta D.
\]
Hence,
\[
(5.1) \quad S_k(N) = \sum_{p \text{ prime}} 1 \ll \sum_{p \text{ prime}} 1 \ll \sum_{p \text{ prime}} 1.
\]
We denote $C = (a, b, c)$, $B = -\Delta D$, $A = \Delta^2 k$. Set also $\varphi = C^{-1} G_F$, the primitive quadratic form associated to $G_F$. Note that $\Delta \varphi = C^{-2} \Delta$, which means that $\left(\frac{\Delta x}{q}\right) = \left(\frac{\Delta}{q}\right)$ for all primes $q$ not dividing $C$. 

Throughout the proof, the implied constants in the $\ll$ notation will depend on $F$, but not on $k$. This means that they can depend on $B, C, \Delta$, but not on $A$.

With these notations we see from (5.1) that
\begin{equation}
S_k(N) \ll \sum_{\substack{p \text{ prime} \leq N/A \atop Ap + B = C\varphi(x,y)}} 1.
\end{equation}

This sum was considered by Iwaniec [10, Theorem 3]. We follow the proof of the upper bound given there, with a slight modification so that the bound remains uniform for $A \leq \log^5 N$.

From the proof of [10, Theorem 3] we get
\begin{equation}
\sum_{\substack{p \leq N/A \atop Ap + B = C\varphi(x,y)}} 1 \leq \sum_{q \mid d \Rightarrow q \mid \Delta} \sum_{r = 1}^{\tau(Cr^2d)} \sum_{\substack{m \leq N + B \atop (A, B)^2 = 1}} \sum_{\substack{x \leq \frac{N(A, B, Cr^2d)}{ACr^2dm} \atop |a_i x + b_i| \text{ primes for } i = 1, 2}} 1
\end{equation}

where
\begin{align*}
a_1 &= \frac{Cr^2dm}{(A, B, Cr^2d)}, \quad b_1 = l_m, \quad a_2 = \frac{A}{(A, B)}, \quad b_2 = \frac{(Al_m + B)(A, B, Cr^2d)}{(A, B)Cr^2dm},
\end{align*}
and $l_m$ is a solution to the congruence
\begin{equation*}
\frac{A}{(A, B)}l_m + \frac{B}{(A, B)} \equiv 0 \left( \mod \frac{Cr^2dm}{(A, B, Cr^2d)} \right).
\end{equation*}

Denote
\begin{equation*}
\Sigma(r, d, m) = \sum_{|a_i x + b_i| \text{ primes for } i = 1, 2} 1.
\end{equation*}

We deduce from [10, Lemma 9] that
\begin{equation}
\Sigma(r, d, m) \ll \frac{N}{Adr^2m} \log^{-2} \left( \frac{N}{Adr^2m} + 3 \right) \prod_{q \mid rm} \left( 1 - \frac{1}{q} \right)^{-2} \prod_{q \mid A} \left( 1 - \frac{1}{q} \right)^{-1}.
\end{equation}
By (5.4), Lemma 4.4, and using partial summation we get

$$
\sum_{m \leq N + B} \Sigma(r, d, m) \ll \frac{N}{A d^2 r^2} \prod_{q | r} \left(1 - \frac{1}{q}\right)^{-2} \prod_{q | A} \left(1 - \frac{1}{q}\right)^{-1}
$$

$$\times \sum_{m \leq N + B} \frac{1}{m} \log^{-2} \left(\frac{N}{A d r^2 m} + 3\right)
$$

$$\ll \frac{N}{A d r^2 \log^{3/2} N} \prod_{q | r} \left(1 - \frac{1}{q}\right)^{-2} \prod_{q | A} \left(1 - \frac{1}{q}\right)^{-1}.
$$

Plugging this into (5.3) we get

(5.5) $$
\sum_{p \leq N / A} 1
$$

$$\ll \sum_{d} \sum_{r} \frac{N}{A d r^2 \log^{3/2} N} \prod_{q | r} \left(1 - \frac{1}{q}\right)^{-2} \prod_{q | A} \left(1 - \frac{1}{q}\right)^{-1}
$$

$$= \frac{N}{A \log^{3/2} N} \prod_{q | A} \left(1 - \frac{1}{q}\right)^{-1} \sum_{r} \left(\frac{1}{r^2} \prod_{q | r} \left(1 - \frac{1}{q}\right)^{-2}\right) \sum_{d} \frac{1}{d}.
$$

Noting that

$$\sum_{r} \frac{1}{r^2} \prod_{q | r} \left(1 - \frac{1}{q}\right)^{-2}, \quad \sum_{d} \frac{1}{d} = \prod_{q | \Delta} \left(1 - \frac{1}{q}\right)^{-1}
$$

are finite, and also noting that $$A = \Delta^2 k$$, we see from (5.5) that

$$\sum_{p \leq N / A} 1 \ll \frac{N}{k \log^{3/2} N} \prod_{q | k} \left(1 - \frac{1}{q}\right)^{-1}.
$$

From (5.2) we then get the required bound

$$S_k(N) \ll \frac{N}{k \log^{3/2} N} \prod_{q | k} \left(1 - \frac{1}{q}\right)^{-1}.$$

5.2. A lower bound for $S_k(N)$. We now prove Lemma 3.6. In [10] Lemma 13 Iwaniec proved a lower bound for $S_1(N)$. We follow the proof given there, with slight modifications so that we can prove lower bounds for all $S_k(N)$ with $k \leq \log^5 N$.

We can assume that our function $F$ is in the class $\mathcal{H}$. This is true due to Lemma 2.2 on replacing $F$ by the function $H$ given in the lemma if necessary.

We can further assume that $F$ satisfies

\[(5.6) \quad (a, b, c) | (e, f), \quad (ac, \Delta) = (a, b, c)^2, \quad (g, \Delta) = 1, \quad (\alpha, \beta) | \Delta.\]

This follows from [10, Lemma 3] which states that there is an affine change of variables

$$F'(x, y) = F(a_1 x + a_2 y + a_3, b_1 x + b_2 y + b_3)$$

such that $F'$ is still in $\mathcal{H}$ and satisfies (5.6). Once more, since $\psi_{F'}(N) \ll \psi_{F}(N)$, we can simply assume that $F$ satisfies (5.6).

Proof of Lemma 3.6. We use the notations of Lemma 4.8. Let $Q$ be as in Lemma 4.8 for $A = \Delta D$. From [10, Lemma 6], there exists an integer $R$ prime to $A$ such that if $n$ is properly represented by the genus of $\varphi$, then $R^2n$ is represented by $\varphi$ with a representation $R^2 n = \varphi(x_0, y_0)$ which satisfies $(x_0, y_0) | R$.

Denote

$$C = 3 + \frac{(-1)^{\Delta_D} D}{2} QR,$$

and $\Delta_\varphi$ the discriminant of $\varphi$. Let $d$ be the largest divisor of $G_P(\alpha_1, \beta_1)$ whose prime factors all divide $\Delta_\varphi$. Let $L$ be defined by the congruence

$$C^2 L \equiv \frac{G_P(\alpha_1, \beta_1)}{d} (\mod \Delta_\varphi), \quad 0 < L < |\Delta_\varphi|.$$

Finally, let

$$T = C^2 W \frac{|\Delta_\varphi|}{\Delta_1^2}, \quad l = W \frac{C^2 d L - G_P(\alpha_1, \beta_1)}{\Delta_1^2} + g.$$

From the proof of [10] Lemma 13 we then find that for $n \equiv l (\mod T)$, the number

$$4a_P \frac{n - g}{W} + e^2_P$$

is a quadratic residue modulo $(2\beta_P, \Delta_P)$, and $n \equiv g (\mod W)$.

We choose $c_F = T\Delta D$, that is, we assume that $(k, T) = 1$ and also $(k, \Delta D) = 1$. Denote

$$\mathcal{M} = \left\{ m \left| \frac{\Delta_1^{kp - g}}{W} + G_P(\alpha_1, \beta_1) = C^2 dm, \ kp \equiv l (\mod T), \ kp \leq N \right. \right\}.$$
It follows from Lemma 4.8 and from our choice of \( R \) that for \( m \in \mathcal{M} \), if \( C^2dm/R^2 \) is properly represented by the genus of \( \varphi \), then \( kp \) is represented by \( F \). Thus, we have reduced the problem of representability by \( F \) to that of proper representability by the genus of \( \varphi \).

Genus theory for quadratic forms gives simple criteria for when a number is properly represented by the genus of \( \varphi \). Such a result is given in [10, Lemma 5], which implies that for \( C^2dm/R^2 \) to be properly represented by the genus of \( \varphi \), it suffices that all prime divisors \( q \) of \( m \) satisfy \( \left( \frac{\Delta_{\varphi}}{q} \right) = 1 \).

It can be verified that for \( m \in \mathcal{M} \),
\[
(m, \Delta_P DW^{-2}) = 1, \quad (m, k) = 1.
\]
Thus, denoting
\[
Q = \left\{ q \mid \left( \frac{\Delta_{\varphi}}{q} \right) = 1, (q, k\Delta_P D/W^2) = 1 \right\},
\]
we get
\[
S_k(N) \gg \sum_{\substack{m \in \mathcal{M} \\ q|m \Rightarrow q \in Q}} 1.
\]

In order to estimate this sum, we will use the \( \frac{1}{2} \)-dimensional sieve. For \( \lambda \) such that \( (\lambda, k\Delta_P D/W^2) = 1 \) denote
\[
\mathcal{M}_\lambda = \{ m \in \mathcal{M} \mid \lambda \mid m \}
\]
\[
= \left\{ m \mid \Delta_1^2kp - gW + G_P(\alpha_1, \beta_1) = C^2dm, kp \equiv l_\lambda \pmod{\lambda T}, kp \leq N \right\},
\]
where
\[
l_\lambda = W \frac{C^2dL_\lambda - G_P(\alpha_1, \beta_1)}{\Delta_1^2} + g, \quad L_\lambda \equiv \begin{cases} L \pmod{\Delta_{\varphi}}, \\ 0 \pmod{\lambda}. \end{cases}
\]
We can then see that \( |\mathcal{M}_\lambda| = \pi(N/k, \lambda T, l_\lambda) + O(1) \). Denote
\[
\mathcal{P} = \left\{ q \mid \left( \frac{\Delta_{\varphi}}{q} \right) = -1, (q, k\Delta_P D/W^2) = 1 \right\}.
\]
All \( m \in \mathcal{M} \) satisfy \( m \equiv L \pmod{\Delta_{\varphi}} \). From [10, Lemma 4] we know that \( \left( \frac{\Delta_{\varphi}}{L} \right) = 1 \). It follows that each \( m \in \mathcal{M} \) satisfies \( \left( \frac{\Delta_{\varphi}}{m} \right) = 1 \), and so must be divisible by an even number of primes from \( \mathcal{P} \).

Denote by \( \mathcal{S}(\mathcal{A}, z) \) the size of the sifted set
\[
\mathcal{A} \setminus \bigcup_{\substack{p \in \mathcal{P} \\ p<z}} \mathcal{A}_p.
\]
Since each \( m \in \mathcal{M} \) is divisible by an even number of primes from \( \mathcal{P} \), we find
that for $1 \leq s < 2$,

$$(5.8) \sum_{m \in M} 1 \geq S(M, N^{1/(2s)}) - \sum_{p_1, p_2 \in \mathcal{P}} S(M_{p_1 p_2}, N^{1/(2s)}).$$

The term $S(M, N^{1/(2s)})$ can be evaluated using the $\frac{1}{2}$-dimensional sieve. We apply Theorem 4.2 where we set $\kappa = 1/2$, $D = \sqrt{N} / \log^{40} N$, $z = D^{1/s} \sim N^{1/(2s)}$, $X = \text{Li}(N/k) / \phi(T)$ and $g(p) = \phi(T) / \phi(pT)$ for $p \in \mathcal{P}$ and $g(p) = 0$ for primes $p$ not in $\mathcal{P}$. We then get

$$(5.9) S(M, N^{1/(2s)}) \geq \frac{N}{k \log N} \prod_{p < z} \left(1 - \frac{1}{q} \right)^{-1} \{ c_{1/2}(s) + O(\log^{-1/12} N) \} + \mathcal{R}(D),$$

where

$$\mathcal{R}(D) = \sum_{q | \lambda \Rightarrow q \in \mathcal{P}} \left| \pi\left( \frac{N}{k}, \lambda T, \frac{l_\lambda}{k} \right) - \frac{\text{Li}(N/k)}{\phi(\lambda T)} \right|. $$

Using the **Bombieri–Vinogradov theorem** and since $k \leq \log^5 N$, we get $\mathcal{R}(D) \ll N \log^{-30} N$, which is going to be negligible. Since we regard $F$ as a constant, we see from (5.9) that

$$(5.10) S(M, N^{1/(2s)}) \geq \frac{N}{k \log^{3/2} N} \prod_{q | k} \left(1 - \frac{1}{q} \right)^{-1} \{ c_{1/2}(s) + O\left( \frac{1}{\log^{1/12} N} \right) \}. $$

We further note that $c_{1/2}(s)$ behaves like $\sqrt{e^7/\pi} (s - 1)^{1/2}$ near $s = 1$. As for the term

$$\sum_{p_1, p_2 \in \mathcal{P}} S(M_{p_1 p_2}, N^{1/(2s)}),$$

we have

$$(5.11) \sum_{N^{1/(2s)} \leq p_1 \leq p_2} S(M_{p_1 p_2}, N^{1/(2s)}) \leq \sum_{m \leq M} \sum_{q | m \Rightarrow q \in \mathcal{Q}} \sum_{N^{1/(2s)} \leq p_1 \leq \sqrt{M}} \sum_{kp \leq N} 1 \Delta_2^2(kp-g) + WG_{\alpha_1, \beta_1} = WC^2 dp_1 p_2 m \quad p_1, p_2 \text{ prime} $$

$$= \sum_{m} \sum_{p_1} \Sigma(m, p_1),$$
where
\[ M = \frac{\Delta_1^2(N - g) + WG_P(\alpha_1, \beta_1)}{WC^2d}. \]

The inner sum \( \Sigma \) can be written as
\[ \Sigma(m, p_1) = \sum_{x \leq N/(kp_1mT) \atop p_1mT(x + (k^{-1}l_{p_1}(\mod p_1m))) \text{ prime}} 1. \]

Hence, from [10, Lemma 9] we get
\[ \Sigma(m, p_1) \ll \frac{N}{kp_1mT \log^2(N/(kp_1mT))} \prod_{q|m} \left( 1 - \frac{1}{q} \right)^{-1} \prod_{q|k} \left( 1 - \frac{1}{q} \right)^{-1}. \]

Thus, from (5.11) we get
\[ (5.12) \sum_{N^{1/(2s)} \leq p_1 \leq p_2 \atop p_1, p_2 \in \mathcal{P}} S(\mathcal{M}_{p_1p_2}, N^{1/(2s)}) \leq \frac{N}{k \log^2 N} \prod_{q|k} \left( 1 - \frac{1}{q} \right)^{-1} \sum_{m \leq N^{1-1/s} \atop q|m} \frac{1}{m} \prod_{q|m} \left( 1 - \frac{1}{q} \right)^{-1} \sum_{N^{1/2s} < p < N^{1/s} \atop p \in \mathcal{P}} \frac{1}{p} \]
\[ = \frac{N}{k \log^2 N} \prod_{q|k} \left( 1 - \frac{1}{q} \right)^{-1} \times \Sigma_m \times \Sigma_p. \]

For \( \Sigma_m \) we have
\[ \Sigma_m \ll \prod_{q \leq N^{1-1/s} \atop (q,k)=1, (\frac{k}{q})=1} \left( 1 + \frac{1}{q-1} \right) \ll \sqrt{1 - \frac{1}{s} \log^{1/2} N} \prod_{q|k} \left( 1 - \frac{1}{q} \right), \]
while for \( \Sigma_p \) we have \( \Sigma_p \ll \log s. \)

Plugging these results into (5.12) we get
\[ (5.13) \sum_{N^{1/(2s)} \leq p_1 \leq p_2 \atop p_1, p_2 \in \mathcal{P}} S(\mathcal{M}_{p_1p_2}, N^{1/(2s)}) \ll C(s) \frac{N}{k \log^{3/2} N} \prod_{q|k} \left( 1 - \frac{1}{q} \right)^{-1}, \]
where \( C(s) = \log s \cdot \sqrt{(s-1)/s} \) behaves like \( (s - 1)^{3/2} \) near \( s = 1. \).
Consequently, from (5.7), (5.8), (5.10) and (5.13) we get

$$S_k(N) \geq (K_1c_{1/2}(s) - K_2C(s)) \frac{N}{k \log^{3/2} N} \prod_{q|k \atop (\frac{\Delta}{q}) = -1} \left(1 - \frac{1}{q}\right)^{-1}$$

for some positive constants $K_1, K_2$ which depend on $F$. From the behaviour of $c_{1/2}(s), C(s)$ near $s = 1$, we find that for $s$ sufficiently close to 1, $K_1c_{1/2}(s) > K_2C(s)$. Thus

$$S_k(N) \gg \frac{N}{k \log^{3/2} N} \prod_{q|k \atop (\frac{\Delta}{q}) = -1} \left(1 - \frac{1}{q}\right)^{-1}$$

as required.

5.3. An upper bound for $S_{k_1,k_2}(N)$

Proof of Lemma 3.7. Let $k_1 < k_2 \leq \log^5 N$. Using the identity

$$\Delta^2 F(x, y) = G(\Delta x + \alpha, \Delta y + \beta) + \Delta D$$

we get

$$S_{k_1,k_2}(N) \ll \sum_{\Delta^2 k_1 p = G(x_1, y_1) + \Delta D} \sum_{\Delta^2 k_2 p = G(x_2, y_2) + \Delta D} 1$$

From genus theory for quadratic forms (e.g. [10, Lemma 5]), we know that if $n$ is properly represented by the genus of $G$, then every prime divisor $q$ of $n$ which is prime to $\Delta$ must satisfy $(\frac{\Delta}{q}) = 1$. Thus,

$$S_{k_1,k_2}(N) \ll \sum_{r_1, r_2 \in \mathbb{N}} \sum_{d_1, d_2} \sum_{m_1, m_2} 1$$

For $m_1, m_2$ square free

$$= \sum_{r_1, r_2, d_1, d_2} \Sigma_{m_1, m_2, p}.$$

We now wish to give an upper bound for the last sum. For this, we split the sum into several cases. We fix some small $\epsilon > 0$.

Case 1. We first consider the case where $[r_1^2 d_1, r_2^2 d_2] \leq N^\epsilon$. In this case we give an upper bound for $\Sigma_{m_1, m_2, p}$ using a 2-dimensional sieve. Note that for some choices of $r_1, r_2, d_1, d_2$ we will have $\Sigma_{m_1, m_2, p} = 0$. In this case $\Sigma_{m_1, m_2, p}$ will satisfy the upper bound trivially. Hence, in the argument that follows we assume that there are no local obstructions to the equations

$$\Delta^2 k_i p - \Delta D = r_i^2 d_i m_i, \quad i = 1, 2.$$
In order for the equation $\Delta^2 k_1 p - \Delta D = r_1^2 d_1 m_1$ to have a solution, we must have $\Delta(\Delta k_1, D) \mid r_1^2 d_1 m_1$. We then have

$$\frac{\Delta k_1}{(\Delta k_1, D)} p - \frac{D}{(\Delta k_1, D)} = \frac{r_1^2 d_1}{\Delta(\Delta k_1, D, r_1^2 d_1)} m_1',$$

where

$$m_1' = \frac{(\Delta k_1, D, r_1^2 d_1)}{(\Delta k_1, D)} m_1.$$

Denote

$$T_1 = \frac{r_1^2 d_1}{\Delta(\Delta k_1, D, r_1^2 d_1)} \quad \text{and} \quad l_1 = \frac{D}{(\Delta k_1, D)} \left( \frac{\Delta k_1}{(\Delta k_1, D)} \right)^{-1} \pmod{T_1}.$$

It follows that we must have

$$p \equiv l_1 \pmod{T_1}.$$

We can similarly define $T_2, l_2$ and deduce that in order for

$$\Delta^2 k_2 p - \Delta D = r_2^2 d_2 m_2$$

to have a solution, we must have $p \equiv l_2 \pmod{T_2}$. There exists $l$ which satisfies

$$l \equiv l_1 \pmod{T_1}, \quad l \equiv l_2 \pmod{T_2},$$

for otherwise we would have a local obstruction.

Let

$$\mathcal{A} = \{n \leq N/k_1 \mid n \equiv l \pmod{[T_1, T_2]} \}.$$

We would now like to sift $\mathcal{A}$ for primes $p$ which also satisfy (5.15). To this end, we define for each prime $q$ a set $\Omega_q$ of residue classes modulo $q$ that $n \in \mathcal{A}$ should avoid. For simplicity, we choose not to sift by primes dividing $6\Delta D k_1 k_2 (k_1 - k_2) r_1 r_2$. Denote the set of those primes by $Q$.

For $q$ such that $\left( \frac{\Delta}{q} \right) = -1$ and $q \not\in Q$ we define

$$\Omega_q = \left\{ 0, \frac{D}{(\Delta k_1, D)} \left( \frac{\Delta k_1}{(\Delta k_1, D)} \right)^{-1} \pmod{q}, \quad \frac{D}{(\Delta k_2, D)} \left( \frac{\Delta k_2}{(\Delta k_2, D)} \right)^{-1} \pmod{q} \right\}.$$

For other $q \not\in Q$, we define $\Omega_q = \{0\}$. For $q \in Q$ we define $\Omega_q = \emptyset$. Set also

$$g(q) = \frac{|\Omega_q|}{q} = \begin{cases} 1/q, & (\frac{\Delta}{q}) = 1 \text{ and } q \not\in Q, \\ 3/q, & (\frac{\Delta}{q}) = -1 \text{ and } q \not\in Q, \\ 0, & q \in Q, \end{cases}$$
We will now use the fact that for \( z < N \),
\[
\Sigma_{m_1,m_2,p} \ll S(A, z, \Omega) + O(z),
\]
and we will apply Theorem 4.3 in order to get an upper bound for \( S(A, z, \Omega) \).

In Theorem 4.3 we set \( X = (N/k_1)/[T_1, T_2] \) and \( g \) as above (where we extend \( g \) to be multiplicative). With these choices, we see that \( r_\lambda = |A_\lambda^Q| - Xg(\lambda) \) satisfies \( |r_\lambda| \leq g(\lambda)\lambda \) for square-free \( \lambda \)'s. From the definition of \( g \), we find that this implies the bound \( |r_\lambda| \leq d_3(\lambda) \) on square-free \( \lambda \)'s (where \( d_3 \) is the 3-fold divisor function). It follows that
\[
X_\lambda < D_\lambda \quad \text{for square-free } \lambda \'s.
\]

Therefore, in Theorem 4.3 we will set \( D = N^{1-\epsilon} \log^{-100} N \), which will make the error term \( \sum_{\lambda < D, \lambda \mid p(z)} |r_\lambda| \) negligible. Note that from the definition of \( T_1, T_2 \) we have \( T_i \mid r_i^2d_i \). It follows that \( [T_1, T_2] \ll [r_1^2d_1, r_2^2d_2] \), which implies
\[
\frac{N}{[T_1, T_2]} \gg \frac{N}{[r_1^2d_1, r_2^2d_2]} \gg N^{1-\epsilon}.
\]

We now apply Theorem 4.3 with \( \kappa = 2 \) and \( z = D^{1/s} \). We choose \( s \) suitably large such that \( C_2(s) > 0 \). We then get
\[
\Sigma_{m_1,m_2,p} \ll S(A, z, \Omega) + O(z)
\]
\[
\ll \frac{N/k_1}{[r_1^2d_1, r_2^2d_2] \log^2 N} \prod_{q \in \mathbb{Q}} \left( 1 - \frac{3}{q} \right)^{-1} + O(N^{1-\epsilon} \log^{-98} N)
\]
\[
\ll \frac{N/k_1}{[r_1^2d_1, r_2^2d_2] \log^2 N} \prod_{q \mid k_1k_2(k_1-k_2)} \left( 1 - \frac{3}{q} \right)^{-1} \prod_{q \mid r_1r_2} \left( 1 - \frac{3}{q} \right)^{-1}.
\]

Denote
\[
C(k_1, k_2) = \prod_{q \mid k_1k_2(k_1-k_2)} \left( 1 - \frac{3}{q} \right)^{-1}.
\]

So in the case \( [r_1^2d_1, r_2^2d_2] \leq N^\epsilon \) we find that
\[
(5.16) \quad \Sigma_{m_1,m_2,p} \ll \frac{NC(k_1, k_2)}{k_1[r_1^2d_1, r_2^2d_2] \log^2 N} \prod_{q \mid r_1r_2} \left( 1 - \frac{3}{q} \right)^{-1}.
\]

**Case 2.** For \( N^\epsilon < [r_1^2d_1, r_2^2d_2] < N^{2-\epsilon} \) we use the trivial bound
\[
\Sigma_{m_1,m_2,p} \leq |A| \leq \frac{N}{k_1[T_1, T_2]} + 1.
\]
From the definition of $T_1, T_2$ we see that $[T_1, T_2] \gg [r_1^2 d_1, r_2^2 d_2]$ (with implied constants depending on $\Delta, D$), and so

$$\Sigma_{m_1, m_2, p} \leq |A| \ll \frac{N}{k_1 [r_1^2 d_1, r_2^2 d_2]} + 1 \ll \frac{N}{[r_1^2 d_1, r_2^2 d_2]} + 1.$$  

CASE 3. We now consider the case $[r_1^2 d_1, r_2^2 d_2] \geq N^{2-\epsilon}$. In this case, instead of bounding $\Sigma_{m_1, m_2, p}$ individually, we will give a bound for

$$\sum_{r_1, r_2 \in \mathbb{N}} \sum_{d_1, d_2} \Sigma_{m_1, m_2, p}.$$

Since $[r_1^2 d_1, r_2^2 d_2] \geq N^{2-\epsilon}$ we must have

$$\max(r_1^2 d_1, r_2^2 d_2) \geq N^{1-\epsilon/2}.$$

Assume without loss of generality that $r_1^2 d_1 \geq N^{1-\epsilon/2}$. It follows that $m_1 \leq N^{\epsilon/2}$ (since otherwise $r_1^2 d_1 m_1 > N$, which is impossible). For each such $m_1$ we want to count the number of $r_1, r_2, d_1, d_2, m_2, p$ which are involved in (5.18). Note that each valid choice of $m_1, r_1, d_1$ determines $p, m_2, d_2, r_2$ uniquely. Hence,

$$\sum_{r_1, r_2 \in \mathbb{N}} \sum_{d_1, d_2} \Sigma_{m_1, m_2, p}$$

$$\ll \sum_{m_1 \leq N^{\epsilon/2}} \sum_{r_1 \leq \sqrt{N}} \sum_{d_1 \leq N} \sum_{q|d_1} 1$$

$$\ll N^{\epsilon/2} \sqrt{N} \prod_{q|\Delta} \log_q N \ll N^{(1+\epsilon)/2} \log \omega(\Delta) N,$$

where $\omega(\Delta)$ is the number of distinct prime divisors of $\Delta$. In particular,

$$\sum_{r_1, r_2 \in \mathbb{N}} \sum_{d_1, d_2} \Sigma_{m_1, m_2, p} \ll N^{1-\delta}$$

for some $\delta > 0$.

We now split (5.14) into three sums according to the cases considered above. We get
Plugging these bounds into (5.21) we get

\[ S_{k_1,k_2}(N) \ll \sum_{r_1,r_2} \sum_{d_1,d_2} \Sigma_{m_1,m_2,p} \]

Applying the bounds (5.16), (5.17), we get

\[ S_{k_1,k_2}(N) \ll N C(k_1,k_2) \left( \sum_{r_1,r_2} \sum_{d_1,d_2} \frac{\Pi_{q|r_1r_2,q>3 \left( \frac{1}{3} \right)^{-1}}}{[r_1^2d_1,r_2^2d_2]} \right) + N \left( \sum_{r_1,r_2} \sum_{d_1,d_2} \frac{1}{[r_1^2d_1,r_2^2d_2]} \right) + \left( \sum_{r_1,r_2} \sum_{d_1,d_2} \Sigma_{m_1,m_2,p} \right) \]

\[ = N C(k_1,k_2) \Sigma_1 + N \Sigma_2 + \Sigma_3 + \Sigma_4. \]

From Lemma 4.7 we get \( \Sigma_1 \ll 1 \). Lemma 4.5 yields \( \Sigma_2 \ll \frac{\log^2 N}{N^{\epsilon/2}} \). From Lemma 4.6 we get \( \Sigma_3 \ll N^{1-\epsilon/2} \log^2 N \). Lastly, (5.20) implies \( \Sigma_4 \ll N^{1-\delta} \). Plugging these bounds into (5.21) we get

\[ S_{k_1,k_2}(N) \ll \frac{N C(k_1,k_2)}{k_1 \log^2 N} \]
as required.

6. Further thoughts and conjectures

6.1. The asymptotics of \( \psi_F \). We proved that, under the conditions of Theorem 1.4, the order of magnitude of \( \psi_F(N) \) is \( \frac{N \log \log N}{\sqrt{\log N}} \). However, proving precise asymptotics

\[ \psi_F(N) \sim c_F \frac{N \log \log N}{\sqrt{\log N}} \]
is beyond our methods.
In [12] Motohashi put forward a conjecture regarding the asymptotics for the number of primes up to $N$ which are of the form $x^2 + y^2 + 1$. This conjecture was corrected by Iwaniec [9] as follows:

**Conjecture 6.1.**

$$C_1 := \lim_{N \to \infty} \frac{\# \{ p \leq N \mid p = x^2 + y^2 + 1 \}}{N \log^{3/2} N}$$

$$= \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} \left( 1 - \frac{1}{p^2} \right)^{-1/2} \left( 1 - \frac{1}{p(p-1)} \right) \approx 0.610534 \ldots$$

We present some numerics to corroborate this conjecture. For this, we compare the ratio

$$R(N) = \sum_{\substack{p \leq N \\ p=x^2+y^2+1}} \log p / \sum_{\substack{n \leq N \\ n=x^2+y^2+1}} 1$$

with $C_1/L \approx 0.79889 \ldots$, where

$$L = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} \left( 1 - \frac{1}{p^2} \right)^{-1/2} \approx 0.76422 \ldots$$

is the Landau–Ramanujan constant. Figure 6.1 shows that there is an error of approximately 2.7% for $N = 10^{10}$.

![Fig. 6.1. Plot of $R(N)$, the ratio of the prime counting function $\sum_{p=x^2+y^2+1 \leq N} \log p$ to the number of integers $n \leq N$ of the form $n = x^2 + y^2 + 1$](image)

Following the same heuristics, we conjecture that

$$C_k := \lim_{N \to \infty} \frac{\# \{ p \leq N/k \mid kp = x^2 + y^2 + 1 \}}{N \log^{3/2} N}$$
exists and satisfies

\[ C_k = \begin{cases} \frac{C_1(k,2)}{k} \prod_{p \mid k, p \equiv 3 \pmod{4}} \frac{p^2 - 1}{p^2 - p - 1}, & 4 \mid k, \\ 0, & 4 \nmid k. \end{cases} \]

With these assumptions, we can give a conjecture for the constant arising in the asymptotics of \( \psi_{x^2+y^2+1}(N) \):

**Conjecture 6.2.** For \( F = x^2 + y^2 + 1 \),

\[ \psi_F(N) \sim c_F \frac{N \log \log N}{\sqrt{\log N}} \]

with

\[ c_F = \lim_{N \to \infty} \frac{1}{\log N} \sum_{k \leq N} C_k \]

\[ = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} (1 - \frac{1}{p^2})^{-1/2} \left( 1 - \frac{1}{p(p-1)} \right) \left( 1 + \frac{1}{p^2 - p - 1} \right) \]

\[ = \frac{1}{\sqrt{2}} \prod_{p \equiv 3 \pmod{4}} (1 - \frac{1}{p^2})^{-1/2} = L \approx 0.76422 \ldots . \]

**6.2. LCM for \( x, y \) in a box.** We have chosen to consider

\[ \psi_F(N) = \log \left( \frac{\text{LCM}_{0 < F(x,y) \leq N} \{F(x,y)\}}{\text{LCM}_{|x|,|y| \leq \sqrt{N}} \{F(x,y)\}} \right) \]

as a generalization of the LCM problem in the single variable case. Another possible generalization is given by

\[ L_F(N) = \log \left( \frac{\text{LCM}_{|x|,|y| \leq \sqrt{N}} \{F(x,y)\}}{\text{LCM}_{|x|,|y| \leq \sqrt{N}} \{F(x,y)\}} \right). \]

In the case of Theorem 1.4, \( L_F(N) \) has the same order of magnitude as \( \psi_F(N) \). We do not give a detailed proof of this statement, but only highlight the main idea for the equivalence.

Lemma 4.8 allows us to reduce the problem of computing \( \psi_F(N) \) for a general polynomial \( F(x,y) \) to computing \( \psi_F(N) \) for \( F \) a shifted quadratic form \( \varphi(x,y) + C \). So it is enough to show that \( \Theta(L_F(N)) = \Theta(\psi_F(N)) \) for the case \( F(x,y) = \varphi(x,y) + C \).

If \( \varphi \) is positive definite, then the equivalence is obvious. In the indefinite case, it follows from reduction theory for quadratic forms that if \( n \) is represented by \( \varphi \) then it is possible to find a representation \( n = \varphi(x,y) \) with \( |x|,|y| \ll \sqrt{n} \). From this, one can once more show that \( \Theta(L_F(N)) = \Theta(\psi_F(N)) \).
Acknowledgements. This research was supported by the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program (Grant agreement No. 786758).

References

[1] P. Bateman, J. Kalb, and A. Stenger, A limit involving least common multiples: 10797, Amer. Math. Monthly 109 (2002), 393–394.
[2] D. Bazzanella and C. Sanna, Least common multiple of polynomial sequences, Rend. Sem. Mat. Univ. Politec. Torino 78 (2020), 21–25.
[3] P. Candela, J. Rué, and O. Serra, Memorial to Javier Cilleruelo: a problem list, Integers 18 (2018), art. A28, 9 pp.
[4] J. Cilleruelo, The least common multiple of a quadratic sequence, Compos. Math. 147 (2011), 1129–1150.
[5] J. Cilleruelo, J. Rué, P. Šarka, and A. Zumalacárregui, The least common multiple of random sets of positive integers, J. Number Theory 144 (2014), 92–104.
[6] J. B. Friedlander and H. Iwaniec, Opera de cribro, Colloq. Publ. 57, Amer. Math. Soc., 2010.
[7] A. Granville, An alternative to Vaughan’s identity, [arXiv:2001.07777] (2020).
[8] S. Hong, G. Qian, and Q. Tan, The least common multiple of a sequence of products of linear polynomials, Acta Math. Hungar. 135 (2012), 160–167.
[9] H. Iwaniec, Primes of the type $\phi(x, y) + A$ where $\phi$ is a quadratic form, Acta Arith. 21 (1972), 203–234.
[10] H. Iwaniec, Primes represented by quadratic polynomials in two variables, Acta Arith. 24 (1974), 435–459.
[11] J. Maynard and Z. Rudnick, A lower bound on the LCM of polynomial sequences, Riv. Mat. Univ. Parma 12 (2021), 143–150.
[12] Y. Motohashi, On the distribution of prime numbers which are of the form $x^2 + y^2 + 1$, Acta Arith. 16 (1970), 351–364.
[13] A. Sah, An improved bound on the least common multiple of polynomial sequences, J. Théor. Nombres Bordeaux 32 (2020), 891–899.

Noam Kimmel
School of Mathematical Sciences
Faculty of Exact Sciences
Tel Aviv University
6997801 Tel Aviv, Israel
E-mail: noamkimmel@mail.tau.ac.il