ACTA ARITHMETICA
151.3 (2012)

Almost-primes represented by quadratic polynomials

by

Robert J. Lemke Oliver (Atlanta, GA)

1. Introduction. Let $G(x) = c_g x^g + c_{g-1}x^{g-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x]$ be an irreducible polynomial of degree g and discriminant D, and let $\rho(m) = \rho_G(m)$ denote the number of incongruent solutions to the congruence $G(n) \equiv 0 \pmod m$. Throughout, we assume that $c_g > 0$ and $\rho(p) \neq p$ for all primes p. The question of how often $G(x)$ represents primes is the content of a conjecture by Bouniakowsky [2] and, more generally, by Schinzel [13] and Bateman and Horn [1]:

Conjecture. Assuming the notation and hypotheses above, we have

$$\#\{1 \le n \le x : G(n) \text{ is prime}\} \sim \Gamma_G \cdot \frac{x}{\log x},$$

where

$$\Gamma_G := \frac{1}{g} \prod_{p \text{ prime}} \left(1 - \frac{\rho(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-1}.$$

The prime number theorem for primes in arithmetic progressions implies that this conjecture is true when $g = 1$. Very little is known if $g \ge 2$.

Remark. There have been fantastic recent results on the related problem for polynomials in two variables, such as $x^2 + y^4$ and $x^3 + 2y^3$, which Friedlander and Iwaniec [5] and Heath-Brown [6] have shown to represent primes infinitely often; in fact, they have obtained the asymptotic orders of the sets of such primes.

Here we consider how frequently $G(x)$ represents numbers that are "almost prime." To this end, let P_r denote the set of squarefree positive integers with at most r distinct prime factors. The best general result along the lines of the above conjecture asserts that a degree g polynomial $G(x)$ represents P_{g+1} infinitely often. For $g \le 7$, this is due to Kuhn [9], Wang [15],

2010 *Mathematics Subject Classification*: 11C08, 11N32, 11N36.
Key words and phrases: almost-primes, prime-representing polynomials, linear sieve, Hooley's method.

DOI: 10.4064/aa151-3-2

and Levin [11], and for general g this follows from work of Buhštab [3] and Richert [12]. In the special case of $G(x) = x^2 + 1$, a deep theorem of Iwaniec [8] states that $G(x)$ represents P_2 infinitely often. To prove this, Iwaniec obtained a new form of the error in the linear sieve, and he proved an equidistribution result about the roots of the quadratic congruence $x^2+1 \equiv 0 \pmod{m}$. By generalizing Iwaniec's result, we are able to obtain the following theorem.

THEOREM 1. *If $G(x) = c_2x^2 + c_1x + c_0 \in \mathbb{Z}[x]$ is irreducible, with $c_2 > 0$ and $\Gamma_G \neq 0$, then there are infinitely many positive integers n such that $G(n)$ is in P_2.*

REMARK. 1) If $G(x) = c_2x^2 + c_1x + c_0 \in \mathbb{Z}[x]$ is irreducible, with $c_2 > 0$ and $\Gamma_G = 0$, then, since $\rho_G(p) \leq 2$ for all primes p, we must have $\rho_G(2) = 2$. The polynomials $G_0(x) := G(2x)/2$ and $G_1(x) := G(2x + 1)/2$ are irreducible, have integer coefficients, and satisfy $\rho_{G_0}(2) = \rho_{G_1}(2) = 1$. Theorem 1 then shows that $G(n)$ is $2P_2$ infinitely often.

2) The author, in unpublished work, has obtained conditions on higher degree $G(x)$ which would allow one to conclude that $G(x)$ represents P_g infinitely often. Unfortunately, these conditions are rather technical, and there are no higher degree polynomials yet known to satisfy them.

To prove Theorem 1, we use the method employed by Iwaniec [8] to consider arbitrary quadratic polynomials. In Section 2, we transform the original problem into a sifting problem to which we can apply Iwaniec's linear sieve inequality. To obtain non-trivial cancellation in the resulting error terms and deduce Theorem 1, we need a result on the distribution of roots of $G(x)$ to various moduli, which we prove in Section 3. To prove this result for $G(x) = x^2 + 1$, Iwaniec made use of the fact that $\operatorname{disc}(x^2 + 1) = -4$ is negative, which allowed him to use the theory of positive definite quadratic forms. It is here, therefore, that most of the additional work in handling arbitary quadratic polynomials is necessary, to account for the fact that the discriminant may be positive and also that $G(x)$ may not be monic. This equidistribution problem also provides the obstruction for establishing the analogue of Theorem 1 for higher degree polynomials.

2. Proof of Theorem 1. We assume from now on that $G(x)$ is a fixed irreducible quadratic polynomial with positive leading coefficent such that $\rho(2) \neq 2$. We apply the method of Iwaniec [8] to obtain an estimate for

$$\#\{1 \leq n < x : G(n) \in P_2\}.$$

We will introduce a weighted sum in Section 2.1 which will change the problem into one of establishing estimates of sifting functions, which we

study by using the linear sieve in Section 2.2. In Section 2.3, we then use these estimates to complete the proof of Theorem 1.

2.1. A weighted sum. If we let

$$\mathcal{A} = \mathcal{A}_x := \{G(n) : 1 \le n < x\}, \tag{2.1}$$

we wish to estimate the sum

$$\sum_{a \in \mathcal{A} \cap P_2} 1.$$

To do so, we introduce a weight function $w(n)$ and instead sum $w(a)$. Let λ be a real number such that $2 \le \lambda < 3$, and assume x is sufficiently large so that $G(n) \le x^\lambda$ for all $n \le x$. If n is a positive integer, let p_n and $\omega(n)$ denote the smallest prime divisor of n and the number of distinct prime divisors of n, respectively. For a prime $p < x^{\lambda/2}$ such that $p \mid n$, let

$$\omega_p(n) := \begin{cases} 1 - \dfrac{\log p}{\lambda/2 \log x} & \text{if } p = p_n, \\ \dfrac{\log p_n}{\lambda/2 \log x} & \text{if } p > p_n \text{ and } p < x^{\lambda/4}, \\ 1 - \dfrac{\log p}{\lambda/2 \log x} & \text{if } p > p_n \text{ and } p \ge x^{\lambda/4}, \end{cases}$$

then let

$$w(n) := 1 - \frac{\lambda/2}{3-\lambda} \sum_{p \mid n,\, p < x^{\lambda/2}} \omega_p(n). \tag{2.2}$$

Remark. The weights $w(n)$ are the same weights that Iwaniec used, which are due to Richert (unpublished, see [8]). Laborde [10] developed weights which would yield a slightly better implied constant for the asymptotic $\#(\mathcal{A} \cap P_2) \gg x/\log x$, but since we have suppressed the constant, we choose to use Richert's weights to maintain continuity with Iwaniec.

We require a lemma due to Iwaniec [8, Lemma 1], which asserts that the weight function $w(n)$ detects P_2 for squarefree n.

Lemma 1 (Iwaniec). *If $n \le x^\lambda$ and $w(n) > 0$, then n has at most two distinct prime factors.*

By Lemma 1, for any $z \le x^{\lambda/4}$ we have

$$\#\{a \in \mathcal{A} : a \in P_2\} \ge \sum_{\substack{a \in \mathcal{A} \\ (a, P(z)) = 1 \\ a \text{ squarefree}}} w(a),$$

where $P(z) = \prod_{p<z} p$. If $z = x^\gamma$ for some $\gamma > 0$, there are few non-squarefree

$a \in \mathcal{A}$ such that $(a, P(z)) = 1$, as

$$\sum_{\substack{n<x \\ (G(n),P(z))=1 \\ G(n) \text{ not squarefree}}} 1 \ll x^{\lambda/2} z^{-1/2} + x^{2/3} (\log x)^{4/3},$$

which we obtain by Iwaniec's argument for $x^2 + 1$ and an application of the square sieve [4, Theorem 2.3.5]. Hence, we consider the sum

$$W(\mathcal{A}, z) = \sum_{\substack{a \in \mathcal{A} \\ (a,P(z))=1}} w(a), \tag{2.3}$$

with the goal of showing that $W(\mathcal{A}, z) \gg x/\log x$. For any positive integer q, let

$$\mathcal{A}_q := \{a \in \mathcal{A} : a \equiv 0 \pmod{q}\}.$$

Following Iwaniec, we can write $W(\mathcal{A}, z)$ in terms of the sifting functions

$$S(\mathcal{A}_q, u) := \#\{a \in \mathcal{A}_q : (a, P(u)) = 1\}, \tag{2.4}$$

namely

(2.5)

$$\begin{aligned} W(\mathcal{A}, z) = S(\mathcal{A}, z) + \frac{\lambda/2}{3-\lambda} \Bigg[& \sum_{z \le p < x^{\lambda/4}} \sum_{z \le p_1 < p} \frac{\log p/p_1}{\lambda/2 \log x} S(\mathcal{A}_{pp_1}, p_1) \\ & - \sum_{z \le p < x^{\lambda/4}} \left(\left(1 - 2\frac{\log p}{\lambda/2 \log x} \right) S(\mathcal{A}_p, p) + \frac{\log p}{\lambda/2 \log x} S(\mathcal{A}_p, z) \right) \\ & - \sum_{x^{\lambda/4} < p < x^{\lambda/2}} \left(1 - \frac{\log p}{\lambda/2 \log x} \right) S(\mathcal{A}_p, z) \Bigg]. \end{aligned}$$

2.2. The linear sieve. We have reduced the problem to that of obtaining a lower bound for the function $W(\mathcal{A}, z)$ defined by (2.3), and by (2.4) and (2.5) this reduces to the problem of obtaining good estimates for the sifting functions $S(\mathcal{A}_q, u)$. We recall the following linear sieve inequality [8, Lemma 2].

Lemma 2 (Iwaniec). *Let $q \ge 1$, $u \ge 2$, $M \ge 2$, and $N \ge 2$. For any $\eta > 0$ we have*

$$S(\mathcal{A}_q, u) \le V(u) x \frac{\rho(q)}{q} (F(s) + E) + 2^{\eta^{-7}} R(\mathcal{A}_q; M, N),$$

$$S(\mathcal{A}_q, u) \ge V(u) x \frac{\rho(q)}{q} (f(s) - E) - 2^{\eta^{-7}} R(\mathcal{A}_q; M, N),$$

where $s = \log MN/\log u$, $E \ll \eta s^2 + \eta^{-8}e^{-s}(\log MN)^{-1/3}$, *and*

$$V(u) = \prod_{p<u}\left(1 - \frac{\rho(p)}{p}\right).$$

The functions $F(s)$ *and* $f(s)$ *are the continuous solutions of the system of differential-difference equations*

$$\begin{aligned} sf(s) &= 0 && \text{if } 0 < s \le 2,\\ sF(s) &= 2e^C && \text{if } 0 < s \le 3,\\ (sf(s))' &= F(s-1) && \text{if } s > 2,\\ (sF(s))' &= f(s-1) && \text{if } s > 3, \end{aligned}$$

where C *is Euler's constant. The error term* $R(\mathcal{A}_q; M, N)$ *has the form*

$$R(\mathcal{A}_q; M, N) = \sum_{m<M,\, n<N,\, mn|P(u)} a_m b_n r(\mathcal{A}_q; mn), \tag{2.6}$$

where

$$r(\mathcal{A}_q; d) := |\mathcal{A}_{[q,d]}| - \frac{\rho([q,d])}{[q,d]}x,$$

and the coefficients a_m *and* b_n *are real numbers, bounded by* 1 *in absolute value, and supported on squarefree values of* m *and* n.

The functions $F(s)$ and $f(s)$ both tend to 1 monotonically as $s \to \infty$, $F(s)$ from above and $f(s)$ from below. Thus, we wish to choose M and N so that s is large, but we do so at the expense of increasing the size of the error term $R(\mathcal{A}_q; M, N)$. Consequently, we are mainly concerned with bounding $R(\mathcal{A}_q; M, N)$ for large values of M and N.

LEMMA 3. *With notation as in Lemma* 2, *for any* $\epsilon > 0$ *we have*

$$\sum_{m<x^{1-8\epsilon}} \left| \sum_{\substack{n<x^{\gamma_0-\gamma_1\epsilon}\\(n,m)=1}} b_n r(\mathcal{A}; mn)\right| \ll x^{1-\epsilon},$$

where $\gamma_0 := \frac{1-\alpha_0}{2(1+\beta_0)}$ *and* $\gamma_1 := \frac{4\alpha_0}{1+\beta_0}$, *where* α_0 *and* β_0 *are defined in Lemma* 4.

Before we prove Lemma 3, we state a result whose proof we postpone until Section 3 (see Lemma 8).

LEMMA 4. *Let* q *be a squarefree number,* d *an odd divisor of* q, μ *an integer prime to* d, *and* ω *a root of* $G(x)$ *modulo* d. *Furthermore, let* $M < M_1 < 2M$ *and* $0 \le \alpha < \beta < 1$. *Let* $P(M_1, M; q, d, \mu, \omega, \alpha, \beta)$ *denote the number of pairs of integers* m, Ω *such that* $M < m < M_1$, $(m, q) = 1$, $m \equiv \mu \pmod d$, $\alpha \le \Omega/mq < \beta$, $G(\Omega) \equiv 0 \pmod{mq}$, *and* $\Omega \equiv \omega \pmod d$.

Then there are constants $A(q) > 0$, $\alpha_0 < 1$ and β_0 such that, for every $\epsilon > 0$,

$$P(M_1, M; q, d, \mu, \omega, \alpha, \beta) = (\beta - \alpha)(M_1 - M)\rho\Big(\frac{q}{d}\Big)\frac{A(q)}{\phi(d)} + O(M^{\alpha_0+\epsilon}q^{\beta_0+\epsilon}).$$

Proof of Lemma 3. Let

$$B(x; m, N) := \sum_{n<N,\,(n,m)=1} b_n r(\mathcal{A}; mn).$$

Our initial task will be to bound $B(x; m, N)$ by using Lemma 4. By the Cauchy–Schwarz inequality, we get

$$\sum_{M<m<2M} |B(x; m, N)| \le M^{1/2}\Big(\sum_{M<m<2M} B(x; m, N)^2\Big)^{1/2}. \tag{2.7}$$

Since we have

$$B(x; m, N) = \sum_{\substack{0\le v<m\\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \sum_{\substack{n<N\\ (n,m)=1}} b_n\Big(\sum_{\substack{k<x\\ k\equiv v \,(\mathrm{mod}\, m)\\ G(k)\equiv 0 \,(\mathrm{mod}\, n)}} 1 - \frac{x}{m}\frac{\rho(n)}{n}\Big),$$

the Cauchy–Schwarz inequality implies that

$$\begin{aligned} B(x; m, N)^2 &\le \rho(m) \sum_{\substack{0\le v<m\\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \Big[\sum_{\substack{n<N\\ (n,m)=1}} b_n\Big(\sum_{\substack{k<x\\ k\equiv v \,(\mathrm{mod}\, m)\\ G(k)\equiv 0 \,(\mathrm{mod}\, n)}} 1 - \frac{x}{m}\frac{\rho(n)}{n}\Big)\Big]^2 \\ &\ll M^{\epsilon} \sum_{\substack{0\le v<m\\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \Big[\sum_{\substack{n<N\\ (n,m)=1}} b_n\Big(\sum_{\substack{k<x\\ k\equiv v \,(\mathrm{mod}\, m)\\ G(k)\equiv 0 \,(\mathrm{mod}\, n)}} 1 - \frac{x}{m}\frac{\rho(n)}{n}\Big)\Big]^2. \end{aligned}$$

Expanding the square on the right-hand side and reintroducing the sum over m, we get

$$\begin{aligned} \sum_{M<m<2M} B(x; m, N)^2 &\\ &\ll M^{\epsilon}(W(x; M, N) - 2xV(x; M, N) + x^2U(M, N)), \end{aligned} \tag{2.8}$$

where

$$\begin{aligned} W(x; M, N) &\\ &:= \sum_{M<m<2M} \sum_{\substack{0\le v<m\\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \sum_{\substack{n_1,n_2<N\\ (n_1n_2,m)=1}} b_{n_1}b_{n_2} \sum_{\substack{k_1,k_2<x\\ k_1\equiv k_2\equiv v \,(\mathrm{mod}\, m)\\ G(k_1)\equiv G(k_2)\equiv 0 \,(\mathrm{mod}\, n)}} 1, \end{aligned} \tag{2.9}$$

$$V(x;M,N) := \sum_{M<m<2M} \sum_{\substack{0\le v<m \\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \frac{1}{m} \sum_{\substack{n_1,n_2<N \\ (n_1n_2,m)=1}} b_{n_1}b_{n_2}\frac{\rho(n_2)}{n_2} \sum_{\substack{k<x \\ k\equiv v \,(\mathrm{mod}\, m) \\ G(k)\equiv 0 \,(\mathrm{mod}\, n_1)}} 1, \tag{2.10}$$

and

$$U(M,N) := \sum_{M<m<2M} \sum_{\substack{0\le v<m \\ G(v)\equiv 0 \,(\mathrm{mod}\, m)}} \frac{1}{m^2} \sum_{\substack{n_1,n_2<N \\ (n_1n_2,m)=1}} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}. \tag{2.11}$$

We will estimate $W(x;M,N)$, $V(x;M,N)$, and $U(M,N)$ separately with the goal of showing that their main terms cancel in the expression (2.8). Our main tools to this end are Lemma 4 and partial summation. We follow the method of Iwaniec [8, proof of Proposition 1] closely, with more effort being necessary only in the estimation of $W(x;M,N)$. Consequently, for $U(M,N)$ and $V(x;M,N)$ we state only the results, noting that they follow in the same fashion as the estimate of $W(x;M,N)$ we provide below. In particular, the required estimate for $U(M,N)$ is

$$U(M,N) = \frac{1}{2M} \sum_{n_1,n_2<N} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}A([n_1,n_2]) + O(M^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}), \tag{2.12}$$

and the required estimate for $V(x;M,N)$ is

$$V(x;M,N) = \frac{x}{2M} \sum_{n_1,n_2<N} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}A([n_1,n_2]) + O(x^{\epsilon} + xM^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}). \tag{2.13}$$

Following Iwaniec's method for $W(x;M,N)$ as far as we can, we obtain

$$W(x;M,N) = \sum_{n_1,n_2<N} b_{n_1}b_{n_2}T^*(n_1,n_2;x,M) + O(x^{1+\epsilon}),$$

where to define $T^*(n_1,n_2;x,M)$ we need to first define the integers c and d. For integers $l_1, l_2 < x/M$, let $0 \le c < [n_1,n_2]$ be the solution to

$$\begin{aligned} c &\equiv l_1 \left(\mathrm{mod}\ \frac{n_1}{(n_1,n_2)}\right), \\ c &\equiv l_2 \left(\mathrm{mod}\ \frac{n_2}{(n_1,n_2)}\right), \\ c &\equiv l_1 \ (\mathrm{mod}\ (n_1,n_2)), \end{aligned}$$

and let

$$d := \frac{(n_1, n_2)}{(n_1, n_2, l_1 - l_2)}.$$

With the above definitions, we have

$$T^*(n_1, n_2; x, M) := \sum_{\substack{l_1, l_2 < x/M \\ l_1 \equiv l_2 \,(\mathrm{mod}\,(2, n_1, n_2))}} \sum_{\substack{0 \le \mu < d \\ (\mu, d) = 1}} \sum_{\substack{0 \le v < d \\ G(\mu l_1 + v) \equiv 0 \,(\mathrm{mod}\, d) \\ G(\mu l_2 + v) \equiv 0 \,(\mathrm{mod}\, d)}} \sum_{\substack{M < m < M_1, (m, n_1 n_2) = 1 \\ m \equiv \mu \,(\mathrm{mod}\, d),\, cm \le \Omega < (c+1)m \\ \Omega \equiv \mu l_1 + v \,(\mathrm{mod}\, d) \\ G(\Omega) \equiv 0 \,(\mathrm{mod}\, m[n_1, n_2])}} 1, \tag{2.14}$$

where $M_1 = \min(2M, x/l_1, x/l_2)$. The innermost sum in (2.14) is precisely

$$P\left(M_1, M; [n_1, n_2], d, \mu, \mu l_1 + v, \frac{c}{[n_1, n_2]}, \frac{c+1}{[n_1, n_2]}\right),$$

so Lemma 4 implies that

$$T^*(n_1, n_2; x, M) = \frac{A([n_1, n_2])\rho([n_1, n_2])}{[n_1, n_2]} \sum_{\substack{l_1, l_2 < x/M \\ l_1 \equiv l_2 \,(\mathrm{mod}\,(2, n_1, n_2))}} \frac{M_1 - M}{\rho(d)\phi(d)} \sum_{\mu, v} 1 + O(x^2 M^{\alpha_0 - 2 + \epsilon} N^{2\beta_0 + \epsilon}). \tag{2.15}$$

The sum $\sum_{\mu,v} 1$ is counting the number of integers μ and v modulo d such that $(\mu, d) = 1$ and $G(\mu l_1 + v) \equiv G(\mu l_2 + v) \equiv 0 \pmod{d}$. This is the same as the number of choices of $\mu l_1 + v$ and $\mu l_2 + v$ such that $G(\mu l_1 + v) \equiv G(\mu l_2 + v) \equiv 0 \pmod{d}$ and their difference, $\mu(l_1 - l_2)$, is invertible modulo d. Since d is squarefree and the number of solutions is multiplicative in d, there are exactly $\rho(d)\psi(d)$ ways of doing this, where $\psi(d)$ is the multiplicative function defined by $\psi(p) := \rho(p) - 1$ for each prime p. Hence, the sum in (2.15) is equal to

$$\phi((n_1, n_2))^{-1} \sum_{\substack{l_1, l_2 < x/M \\ l_1 \equiv l_2 \,(\mathrm{mod}\,(2, n_1, n_2))}} \phi((n_1, n_2, l_1 - l_2)) \psi\left(\frac{(n_1, n_2)}{(n_1, n_2, l_1 - l_2)}\right)(M_1 - M).$$

Since $\rho(p) = 0$, 1, or 2, we must have $\psi(p) = 0, \pm 1$. We first note that if $\psi(p) = -1$ for some $p \mid [n_1, n_2]$, then $\rho(p) = 0$ and so $T^*(n_1, n_2; x, M)$ would then be 0. We therefore assume $\psi(p) \neq -1$ and evaluate $T^*(n_1, n_2; x, M)$.

Let $n \mid (n_1, n_2)$ be maximal such that $\psi(n) = 1$, and let $n_0 = (n_1, n_2)/n$. Since

$$\psi\left(\frac{(n_1, n_2)}{(n_1, n_2, l_1 - l_2)}\right) = \psi\left(\frac{n_0}{(n_0, l_1 - l_2)}\right),$$

it follows that $\psi((n_1,n_2)/(n_1,n_2,l_1-l_2))=0$ unless $n_0\,|\,(l_1-l_2)$. Hence, we consider

$$\frac{1}{\phi((n_1,n_2))}\sum_{\substack{l_1,l_2<x/M\\ l_1\equiv l_2\,(\mathrm{mod}\,n_0)}}\frac{\phi((n_1,n_2,l_1-l_2))}{\psi((n_1,n_2,l_1-l_2)/n_0)}(M_1-M),$$

which, by using the fact that $(n_1,n_2,l_1-l_2)=n_0(n,l_1-l_2)$, is given by

$$\frac{1}{\phi(n)}\sum_{\substack{l_1,l_2<x/M\\ l_1\equiv l_2\,(\mathrm{mod}\,n_0)}}\phi((n,l_1-l_2))(M_1-M).$$

We now have, letting $\xi:=\mu*\phi$,

$$\begin{aligned}\sum_{\substack{0<l_1<l_2\\ l_1\equiv l_2\,(\mathrm{mod}\,n_0)}}\phi((n,l_1-l_2))&=\sum_{\substack{0<l_1<l_2\\ l_1\equiv l_2\,(\mathrm{mod}\,n_0)}}\sum_{t|(n,l_1-l_2)}\xi(t)\\&=\frac{l_2}{n_0}\sum_{t|n}\frac{\xi(t)}{t}+O(\phi(n))\\&=\frac{l_2\phi(n)\rho(n)}{n_0n}+O(\phi(n)),\end{aligned}$$

where the last equality follows from the evaluation of $\sum_{t|n}\xi(t)/t$ on primes. We are thus led to consider

$$\sum_{l_2<x/M}l_2\biggl(\min\Bigl(2M,\frac{x}{l_2}\Bigr)-M\biggr)=\frac{x^2}{4M}+O(x).$$

Inserting these estimates into (2.15), we now see that

$$\begin{aligned}T^*(n_1,n_2;x,M)=\frac{x^2}{2M}&\biggl(A([n_1,n_2])\frac{\rho([n_1,n_2])}{n_1n_2}\rho(n)\biggr)\\&+O\biggl(xN^{\epsilon}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}+x^2M^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}\biggr).\end{aligned}$$

Hence, we have

$$\begin{aligned}W(x;M,N)=\frac{x^2}{2M}&\sum_{n_1,n_2<N}b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}\,\frac{\rho(n)}{\rho((n_1,n_2))}A([n_1,n_2])\\&+O(x^{1+\epsilon}+x^2M^{\alpha_0-2+\epsilon}N^{2+2\beta_0+\epsilon}).\end{aligned}$$

Since primes $p\,|\,n_0$ satisfy $\psi(p)=0$ and hence $\rho(p)=1$, it follows that $\rho((n_1,n_2))=\rho(n)$. This implies the required estimate

$$\begin{aligned}W(x;M,N)=\frac{x^2}{2M}&\sum_{n_1,n_2<N}b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}A([n_1,n_2])\\&+O(x^{1+\epsilon}+x^2M^{\alpha_0-2+\epsilon}N^{2+2\beta_0+\epsilon}).\end{aligned}\tag{2.16}$$

Inserting the estimates (2.12), (2.13), and (2.16) into (2.8), we see that the main terms cancel, and we obtain

$$\sum_{M<m<2M} B(x;m,N)^2 \ll (x + x^2 M^{\alpha_0-2} N^{2+2\beta_0}) x^{\epsilon} M^{\epsilon} N^{\epsilon}. \tag{2.17}$$

Returning to the statement of the lemma, let $N = x^{\gamma_0-\gamma_1\epsilon}$. With this choice of N, it suffices to show for any $M < x^{1-8\epsilon}$ that

$$\sum_{M<m<2M} |B(x;m,N)| \ll x^{1-3\epsilon/2}.$$

If $M < x^{1-\gamma_0-\epsilon}$, the trivial estimate

$$|B(x;m,N)| \le \rho(m) \sum_{n<N} \rho(n) \ll \rho(m) N$$

yields the desired result.

If $M > x^{1-\gamma_0-\epsilon}$, we use the estimate (2.17) in (2.7), and obtain

$$\sum_{M<m<2M} |B(x;m,N)| \ll ((Mx)^{1/2} + xM^{(\alpha_0-1)/2} N^{1+\beta_0}) x^{\epsilon} M^{\epsilon} N^{\epsilon} \ll x^{1-3\epsilon/2}$$

by our choice of $M < x^{1-8\epsilon}$ and $N = x^{\gamma_0-\gamma_1\epsilon}$. ∎

Armed with Lemma 3, we are now able to acquire the desired estimate for the sifting functions $S(\mathcal{A}_q, u)$.

LEMMA 5. *If $z < x^{\lambda/2r}$, then for any $\epsilon > 0$ and x sufficiently large, we have*

$$\sum_{\substack{q<x^{1-\epsilon} \\ (q,P(z_q))=1}} c_q S(\mathcal{A}_q, z_q)$$
$$< V(z) x \Bigg(\sum_{\substack{q<x^{1-\epsilon} \\ (q,P(z_q))=1}} c_q \frac{\rho(q)}{q} F\left(\frac{(1+\gamma_0)\log x - \log q}{\log z_q} \right) \frac{\log z}{\log z_q} + O_{\log z}(\epsilon) \Bigg),$$

with γ_0 as defined in Lemma 3, provided that for each q, $z \le z_q < x^{\lambda/2r}$ and $0 \le c_q \le 1$.

This lemma is essentially the same as Proposition 2 in [8], so we present it without proof. We obtain a lower bound for the sum in Lemma 5 by replacing F with f.

2.3. Proof of Theorem 1. With Lemma 5 at our disposal, we obtain a lower bound for the size of the set

$$\{1 \le n < x : G(n) \in P_2\}.$$

We wish to apply Lemmas 2 and 5 to equation (2.5) to obtain a lower bound for $W(\mathcal{A}, z)$. We may do this for each term in (2.5) but the short sum

$$\sum_{x^{1-\epsilon}\le p<x}\left(1-\frac{\log p}{\lambda/2\log x}\right)S(\mathcal{A}_p,z).$$

However, in this case, we make the estimate

$$S(\mathcal{A}_p,z)\ll\frac{x}{p\log(x/p)},$$

yielding the bound $O(\epsilon x/\log x)$. For notational convenience, set

$$\alpha:=1+\gamma_0\quad\text{and}\quad\gamma:=\frac{\log z}{\log x}.$$

By partial summation, we obtain

$$\begin{aligned}W(\mathcal{A},z)>V(z)x\Bigg(f\Big(\frac{\alpha}{\gamma}\Big)&+\Bigg[\int_{\gamma}^{1/2}\int_{\gamma}^{u}\frac{u-t}{1}\,\frac{\gamma}{t}f\Big(\frac{\alpha-u-t}{t}\Big)\frac{dt}{t}\,\frac{du}{u}\\&-\int_{\gamma}^{1/2}\Big((1-2u)\frac{\gamma}{u}F\Big(\frac{\alpha-u}{u}\Big)+uF\Big(\frac{\alpha-u}{\gamma}\Big)\Big)\frac{du}{u}\\&-\int_{1/2}^{1}(1-u)F\Big(\frac{\alpha-u}{\gamma}\Big)\frac{du}{u}\Bigg]-\epsilon\Bigg)\\&=:V(z)x(W-\epsilon),\end{aligned}$$

where we have let λ tend to 2, which is permitted by continuity. Since $\Gamma_G\neq 0$, we have $V(z)\asymp\log^{-1}x$ by Mertens' Theorem and we wish to show that $W>0$.

We observe that W decreases monotonically as α increases from 1, so we wish to find $\gamma<1/2$ such that $W|_{\alpha=1}>0$. However, we will not immediately substitute $\alpha=1$ into the above formula. Instead, we will choose $\gamma=\alpha/6$ and take the limit as α tends to 1 from the right. Using

$$sF(s)=2e^C\Bigg(1+\int_2^{s-1}\log(u-1)\,\frac{du}{u}\Bigg)$$

if $3\le s\le 5$, and

$$sf(s)=2e^C\Bigg(\log(s-1)+\int_3^{s-1}\int_2^{t-1}\log(u-1)\,\frac{du}{u}\,\frac{dt}{t}\Bigg)$$

if $4\le s\le 6$, we obtain

$$W = \frac{\alpha e^C}{3}\bigg(\log\Big(\frac{5}{6}\alpha\Big) - \frac{\alpha-1}{\alpha}\log(\alpha-1) - \int_2^4 \bigg[t\log\Big(\frac{6(t+1)}{5(t+2)}\Big) + (t+1)\log\Big(1-\frac{t}{5}\Big)\bigg]\frac{\log(t-1)}{t(t+1)}\,dt\bigg).$$

Upon taking the limit $\alpha \to 1^+$, we see that

$$W_1 = \frac{e^C}{3}\bigg(\log\Big(\frac{5}{6}\Big) - \int_2^4 \bigg[t\log\Big(\frac{6(t+1)}{5(t+2)}\Big) + (t+1)\log\Big(1-\frac{t}{5}\Big)\bigg]\frac{\log(t-1)}{t(t+1)}\,dt\bigg),$$

which a numerical computation reveals to be positive.

3. An equidistribution result for the congruence $G(x) \equiv 0 \pmod m$. Here we prove Lemma 4, an equidistribution result for the roots of the congruence $G(x) \equiv 0 \pmod m$, where $G(x)$ is any irreducible quadratic polynomial. The proof of Theorem 1 is complete once this lemma is proved. Before we can do this, however, we need a result concerning the Dirichlet series $L(\psi, s) := \sum_{m=1}^{\infty} \psi(m)/m^s$, where $\psi = \rho * \mu$ and $\rho(m)$ is the number of incongruent solutions to $G(x) \equiv 0 \pmod m$.

LEMMA 6. *The series $L(\psi, s)$ converges to a positive real number at $s = 1$.*

Proof. If D is the discriminant of $G(x)$, then, by Hensel's Lemma, we can express the Euler product for $L(\psi, s)$ as

$$L(\psi, s) = \lambda_D(s)\prod_{p\nmid D}\Big(1 + \frac{\psi(p)}{p^s}\Big) =: \lambda_D(s)L_0(\psi, s),$$

where $\lambda_D(s)$ is the product arising from primes $p \mid D$. Since it is a finite product, it will have no bearing on the convergence of $L(\psi, 1)$. Thus, we are only concerned with the convergence of $L_0(\psi, 1)$. Assuming that s is tending to 1 in the half-plane $\Re(s) > 1$, we have

$$\log(L_0(\psi, s)) = \sum_{p\nmid D}\log\Big(1 + \frac{\psi(p)}{p^s}\Big) = \sum_{p\nmid D}\frac{\psi(p)}{p^s} + O\bigg(\sum_{p\nmid D}\frac{1}{p^{2\Re(s)-\epsilon}}\bigg) = \sum_{p\nmid D}\frac{\psi(p)}{p^s} + O(1).$$

Since $\rho(p)$ can be interpreted Galois-theoretically and depends only on the conjugacy class C of Frob_p in $\mathrm{Gal}(G)$, we have, letting $\mathrm{Gal}(G)^{\#}$ denote the

set of conjugacy classes of $\mathrm{Gal}(G)$ and recalling that $\psi(p) = \rho(p) - 1$,

$$\sum_{p\nmid D} \frac{\psi(p)}{p^s} = \sum_{C\in \mathrm{Gal}(G)^{\#}} (\rho(C)-1) \sum_{\mathrm{Frob}_p \in C} p^{-s}$$
$$= \sum_{C\in \mathrm{Gal}(G)^{\#}} (\rho(C)-1) \frac{\#C}{\#\mathrm{Gal}(G)} \log\left(\frac{1}{s-1}\right) + \theta(s),$$

where $\theta(s)$ is holomorphic for $\Re(s) \geq 1$. The last equality follows from the Chebotarev Density Theorem (for example, see Proposition 1.5 of [14]). The value of $\rho(C)$ is the number of roots of $G(x)$ in $\mathbb{C}$ fixed by elements of C, so letting $\mathrm{Fix}(C)$ (resp. $\mathrm{Fix}(\sigma)$, for $\sigma \in \mathrm{Gal}(G)$) be the number of fixed points of an element of C (resp. the number of fixed points of σ), we have

$$\sum_{C\in \mathrm{Gal}(G)^{\#}} \#C \cdot (\rho(C)-1) = \sum_{C\in \mathrm{Gal}(G)^{\#}} \#C \cdot \mathrm{Fix}(C) - \#\mathrm{Gal}(G)$$
$$= \sum_{\sigma\in \mathrm{Gal}(G)} \mathrm{Fix}(\sigma) - \#\mathrm{Gal}(G) = 0,$$

by Burnside's Lemma. Hence, we see that $\log(L_0(\psi, s)) = O(1)$ as s tends to 1. Thus, the infinite product converges and $L_0(\psi, 1)$ exists, whence $L(\psi, 1)$ does as well. The fact that $L(\psi, 1)$ is positive and real comes immediately from its Euler product and the definition of $\psi(m)$. ∎

We will also need a lemma of Iwaniec [8, Lemma 7] on the approximation of the characteristic function $\chi_I(t)$ of the interval $I := [\alpha, \beta) \subseteq [0, 1)$ by Fourier series.

Lemma 7 (Iwaniec). *Let $2\Delta < \beta - \alpha < 1 - 2\Delta$. There exist two functions $A(t)$ and $B(t)$ such that*

$$|\chi_I(t) - A(t)| = B(t)$$

and

$$A(t) = \beta - \alpha + \sum_{h\neq 0} A_h e(ht), \qquad B(t) = \Delta + \sum_{h\neq 0} B_h e(ht),$$

with Fourier coefficients A_h and B_h satisfying

$$|A_h|, |B_h| \leq \min\left(\frac{1}{|h|}, \frac{\Delta^{-2}}{|h|^3}\right) =: C_h. \tag{3.1}$$

Armed with Lemmas 6 and 7, we now prove the main result of this section, which is a generalization of Iwaniec's Lemma 4 of [8], and is the precise statement of our Lemma 4. For a squarefree integer q we define

$$A(q) := \frac{\phi(q)}{q} \frac{L(\psi, 1)}{L_q(\psi, 1)}, \tag{3.2}$$

where $\phi(n)$ is Euler's totient function,

$$L_q(\psi,1) := \prod_{p|q}\left(1+\frac{\psi(p)}{p}+\cdots+\frac{\psi(p^{r_p})}{p^{r_p}}\right), \tag{3.3}$$

and r_p is the smallest integer such that $\psi(p^k)=0$ for all $k>r_p$. We note that r_p exists as a consequence of Hensel's Lemma because $G(x)$ is irreducible.

LEMMA 8. *Let q be a squarefree number, d an odd divisor of q, μ an integer prime to d, and ω a root of $G(x)$ modulo d. Furthermore, let $M<M_1<2M$ and $0\le\alpha<\beta<1$. Let $P(M_1,M;q,d,\mu,\omega,\alpha,\beta)$ denote the number of pairs of integers m,Ω such that $M<m<M_1$, $(m,q)=1$, $m\equiv\mu \pmod d$, $\alpha\le\Omega/mq<\beta$, $G(\Omega)\equiv 0 \pmod{mq}$, and $\Omega\equiv\omega \pmod d$. Then there are constants $\alpha_0<1$ and β_0 such that, for every $\epsilon>0$,*

$$P(M_1,M;q,d,\mu,\omega,\alpha,\beta)=(\beta-\alpha)(M_1-M)\rho\left(\frac{q}{d}\right)\frac{A(q)}{\phi(d)}+O(M^{\alpha_0+\epsilon}q^{\beta_0+\epsilon}).$$

Proof. By Lemma 7, we have

$$\begin{aligned} &P(M_1,M;q,d,\mu,\omega,\alpha,\beta)\\ &=(\beta-\alpha)\sum_{\substack{M<m<M_1,\,(m,q)=1,\,m\equiv\mu \pmod d\\ 0\le\Omega<mq,\,G(\Omega)\equiv 0 \pmod{mq},\,\Omega\equiv\omega \pmod d}} 1\\ &\quad+O\left(\rho(q)\Delta M+\sum_{h\neq 0}C_h\left|\sum_{\substack{M<m<M_1,\,(m,q)=1,\,m\equiv\mu \pmod d\\ 0\le\Omega<mq,\,G(\Omega)\equiv 0 \pmod{mq},\,\Omega\equiv\omega \pmod d}} e\left(\frac{h\Omega}{mq}\right)\right|\right). \end{aligned} \tag{3.4}$$

By the Chinese Remainder Theorem, the sum in the main term above is given by

$$\begin{aligned} \rho\left(\frac{q}{d}\right)\sum_{\substack{M<m<M_1\\(m,q)=1\\m\equiv\mu \pmod d}}\rho(m)&=\rho\left(\frac{q}{d}\right)\sum_{\substack{a\le T\\(a,q)=1}}\psi(a)\sum_{\substack{M/a<b<M_1/a,(b,q/d)=1\\b\equiv\mu\bar{a} \pmod d}}1\\ &\quad+\rho\left(\frac{q}{d}\right)\sum_{\substack{b<2M^{1/2}\\(b,q)=1}}\sum_{\substack{\max(M/b,T)<a<M_1/b\\a\equiv\mu\bar{b} \pmod d,\,(a,q/d)=1}}\psi(a). \end{aligned}$$

If $(a,D)=1$, then $\psi(a)=\left(\frac{D}{a}\right)\mu(a)^2$. Hence,

$$\begin{aligned} &\rho\left(\frac{q}{d}\right)\sum_{\substack{M<m<M_1\\(m,q)=1\\m\equiv\mu \pmod d}}\rho(m)\\ &\qquad=\rho\left(\frac{q}{d}\right)\sum_{a\le T,\,(a,q)=1}\psi(a)\left(\phi\left(\frac{q}{d}\right)\frac{M_1-M}{aq}+O\left(\phi\left(\frac{q}{d}\right)\right)\right)\\ &\qquad\quad+O(\rho(q)\phi(q)M^{1/2+\epsilon}) \end{aligned}$$

$$= \rho\left(\frac{q}{d}\right)\phi\left(\frac{q}{d}\right)\frac{M_1 - M}{q}\sum_{\substack{a\le T\\(a,q)=1}}\frac{\psi(a)}{a} + O(\rho(q)\phi(q)T^{1+\epsilon}) + O(\rho(q)\phi(q)M^{1/2+\epsilon})$$

$$= \rho\left(\frac{q}{d}\right)\phi\left(\frac{q}{d}\right)\frac{M_1 - M}{q}\frac{L(\psi,1)}{L_q(\psi,1)} + O\left(\rho(q)\phi(q)\left(M\frac{\phi(q)}{q}T^{-1+\epsilon} + T^{1+\epsilon} + M^{1/2+\epsilon}\right)\right).$$

By choosing $T = M^{1/2}$, we see that the error above is $O(M^{1/2+\epsilon}q^{1+\epsilon})$.

We now estimate the error term in (3.4), which is

$$O\left(\rho(q)\Delta M + \sum_{h\neq 0} C_h \left| \sum_{\substack{M<m<M_1,\,(m,q)=1,\,m\equiv\mu \pmod d\\ 0\le\Omega<mq,\,G(\Omega)\equiv 0 \pmod{mq},\,\Omega\equiv\omega \pmod d}} e\left(\frac{h\Omega}{mq}\right)\right|\right).$$

We will bound the above sum by an estimate of the form

$$\begin{aligned}(3.5)\qquad \sum_{\substack{M<m<M_1,\,(m,q)=1,\,m\equiv\mu \pmod d\\ 0\le\Omega<mq,\,G(\Omega)\equiv 0 \pmod{mq},\,\Omega\equiv\omega \pmod d}} e\left(\frac{h\Omega}{mq}\right) &\ll M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}\sum_{h\neq 0} C_h(1 + hM^{\alpha_3+\epsilon}q^{\beta_3+\epsilon})\tau(h)\\ &\ll M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}\left(1 + \frac{M^{\alpha_3+\epsilon}q^{\beta_3+\epsilon}}{\Delta}\right)(\log\Delta)^2,\end{aligned}$$

where $\alpha_2 < 1$, $\alpha_3 < 1 - \alpha_2$, and β_2 and β_3 are real numbers, and the last equality has come from (3.1).

If $\alpha_3 < 0$, we take $\Delta = M^{\alpha_3}q^{\beta_3}$, to deduce that the error in equation (3.4) is

$$O(M^{1+\alpha_3+\epsilon}q^{\beta_3+\epsilon} + M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}),$$

in which case we may take $\alpha_0 = \max(1/2, \alpha_2, 1+\alpha_3)$ and $\beta_0 = \max(1, \beta_2, \beta_3)$. If $\alpha_3 \ge 0$, we take $\Delta = M^{(\alpha_2+\alpha_3-1)/2}q^{\beta_3}$ to find that the error in (3.4) is

$$O(M^{(1+\alpha_2+\alpha_3)/2+\epsilon}q^{\beta_3+\epsilon} + M^{(1+\alpha_2+\alpha_3)/2+\epsilon}q^{\beta_2+\epsilon}),$$

and we may take $\alpha_0 = \max(1/2, (1 + \alpha_2 + \alpha_3)/2)$ and $\beta_0 = \max(1, \beta_2, \beta_3)$. Thus, it only remains to establish (3.5).

We begin by removing the condition that $(m, q) = 1$ by Möbius inversion:

$$\begin{aligned}&\sum_{\substack{M<m<M_1,\,(m,q)=1,m\equiv\mu \pmod d\\ 0\le\Omega<qm,\,G(\Omega)\equiv 0 \pmod{mq},\,\Omega\equiv\omega \pmod d}} e\left(\frac{h\Omega}{mq}\right)\\ &\qquad = \sum_{l\mid q/d}\mu(l)\sum_{\substack{qM<E<qM_1,\,E\equiv\mu q \pmod{dq},\,E\equiv 0 \pmod{lq}\\ 0\le\Omega<E,\,G(\Omega)\equiv 0 \pmod E,\,\Omega\equiv\omega \pmod d}} e\left(\frac{h\Omega}{E}\right).\end{aligned}$$

We will estimate the inner sum by using the theory of quadratic forms, a method originally due to Hooley [7]. If c_2 and E are relatively prime, there is a bijection between roots of $G(\Omega) \equiv 0 \pmod{E}$ and quadratic forms $[E, y, z]$ of discriminant D, given explicitly by $\Omega = \frac{y-c_1}{2}\overline{c_2}$, where $0 \le \overline{c_2} < E$ is the inverse of c_2 modulo E. To apply this correspondence, therefore, we first take out the part of E not relatively prime to c_2, getting

$$\sum_{\substack{qM<E<qM_1, E\equiv\mu q \,(\mathrm{mod}\, dq)\\ E\equiv 0 \,(\mathrm{mod}\, lq),\, 0\le\Omega<E\\ G(\Omega)\equiv 0 \,(\mathrm{mod}\, E),\, \Omega\equiv\omega \,(\mathrm{mod}\, d)}} e\left(\frac{h\Omega}{E}\right)$$

$$= \sum_{\substack{f\le T\\ (f,c_1)=1}}^{*} \sum_{\substack{0\le u<fc_2\\ (u,c_2)=1}} \sum_{\substack{0\le v<f\\ G(v)\equiv 0 \,(\mathrm{mod}\, f)\\ v\equiv\omega \,(\mathrm{mod}\, (d,f))}} e\left(\frac{hv\bar{u}}{f}\right) \sum_{E,\Omega}^{*} e\left(\frac{h\Omega\bar{f}}{E}\right) + O((qM)^{1+\epsilon}T^{-1+\epsilon}),$$

where the star on the first summation indicates that f is composed only of primes dividing c_2, and furthermore, $\bar{u}$ is the inverse of u modulo fc_2, $\bar{f}$ is the inverse of f modulo E, T is a parameter to be specified later, and the star on the innermost summation indicates that E and Ω satisfy $qM/f < E < qM_1/f$, $fE \equiv 0 \pmod{lq}$, $fE \equiv \mu q \pmod{dq}$, $E \equiv u \pmod{fc_2}$, $0 \le \Omega < E$, $\Omega \equiv \omega \pmod{d/(d,f)}$, and $G(\Omega) \equiv 0 \pmod{E}$.

We are now able to use the bijection between roots of quadratic congruences and quadratic forms. From the explicit construction described above, we have

$$\sum_{E,\Omega}^{*} e\left(\frac{h\Omega\bar{f}}{E}\right) = \sum_{[E,y,z]}^{*} e\left(\frac{h\overline{fc_2}(y-c_1)}{2E}\right) = \sum_{[E,y,z]}^{*} e\left(\frac{h(y-c_1)}{2fc_2E} - \frac{h\bar{u}(y-c_1)}{2fc_2}\right),$$

where we have transferred the congruence conditions on Ω to conditions on y. Now, suppose the form $[E, y, z]$ is equivalent to $[a, 2b+c_1, c]$ under the action of $\Gamma^0(fc_2)$. In other words, there is an $\left(\begin{smallmatrix}\alpha & \beta\\ \gamma & \delta\end{smallmatrix}\right) \in \Gamma^0(fc_2)$ such that

$$\begin{pmatrix}\alpha & \gamma\\ \beta & \delta\end{pmatrix}\begin{pmatrix}a & (2b+c_1)/2\\ (2b+c_1)/2 & c\end{pmatrix}\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} = \begin{pmatrix}E & y/2\\ y/2 & z\end{pmatrix},$$

where

$$\Gamma^0(fc_2) = \left\{\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \beta \equiv 0 \pmod{fc_2}\right\}.$$

Then

$$E = a\alpha^2 + (2b+c_1)\alpha\gamma + c\gamma^2 =: E_{\alpha,\gamma}, \tag{3.6}$$

$$y = 2a\alpha\beta + (2b+c_1)(\alpha\delta+\beta\gamma) + 2c\gamma\delta. \tag{3.7}$$

Hence,

$$\frac{y-c_1}{2} = a\alpha\beta + c\gamma\delta + b(\alpha\delta+\beta\gamma) + c_1\beta\gamma,$$

from which it follows that

$$\alpha\frac{y-c_1}{2} = \beta E_{\alpha,\gamma} + c\gamma + b\alpha.$$

Thus,

$$\begin{aligned}\frac{h(y-c_1)}{2fc_2E} - \frac{h\bar{u}(y-c_1)}{2fc_2} &= \frac{h\beta}{fc_2\alpha} + \frac{h(c\gamma+b\alpha)}{fc_2\alpha E_{\alpha,\gamma}} - \frac{h\bar{u}(\beta E_{\alpha,\gamma}+c\gamma+b\alpha)}{fc_2\alpha}\\ &\equiv \frac{h((\overline{fc_2}fc_2-1)c\bar{u}\gamma - \overline{fc_2}fc_2\bar{\gamma})}{fc_2\alpha} + \frac{h(c\gamma+b\alpha)}{fc_2\alpha E_{\alpha,\gamma}} - \frac{hb\bar{u}}{fc_2} \pmod 1\\ &=: \frac{h((\overline{fc_2}fc_2-1)c\bar{u}\gamma - \overline{fc_2}fc_2\bar{\gamma})}{fc_2\alpha} + h\phi_{\alpha,\gamma},\end{aligned}$$

where $\bar{\gamma}$ and $\overline{fc_2}$ are the inverses modulo α of γ and fc_2, respectively. To simplify notation, we write $\theta_{\alpha,\gamma}$ for the quantity on the right-hand side above. We note that we may obtain a similar expression for $\theta_{\alpha,\gamma}$ with γ in the denominator. With this notation, we have

$$\sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega\bar{f}}{E}\right) = \sum_{Q=[a,2b+c_1,c]}{}' \sideset{}{^*}\sum_{\alpha,\gamma} e(\theta_{\alpha,\gamma}), \tag{3.8}$$

where the outer sum runs over a set of representatives of quadratic forms $Q=[a,2b+c_1,c]$ of discriminant D under the action of $\Gamma^0(fc_2)$, and the inner sum runs over coprime integers α and γ such that $qM/f < a\alpha^2 + (2b+c_1)\alpha\gamma + c\gamma^2 < qM_1/f$, restricted to one representation of the form (3.6) and (3.7), and satisfying

$$\begin{aligned}&fE_{\alpha,\gamma} \equiv 0 \pmod{lq},\\ &fE_{\alpha,\gamma} \equiv \mu q \pmod{dq},\\ &E_{\alpha,\gamma} \equiv u \pmod{fc_2},\\ &\left(\frac{1-\bar{u}E_{\alpha,\gamma}}{c_2}\right)(c\gamma+b\alpha) - \alpha\omega \equiv 0 \left(\mathrm{mod}\ \frac{d}{(d,f)}\right).\end{aligned} \tag{3.9}$$

If either α or γ is fixed, then the number of simultaneous solutions to these congruences, c_G, is bounded by $(q,c)\tau(q)(fc_2)^{1/2}$. Since $c=O(1)$ if $G(x)$ is monic, we see that c_G is $O(q^\epsilon)$ if $G(x)$ is monic and $O(q^{1+\epsilon}f^{1/2})$ otherwise.

Returning to (3.8), we now break into two cases, depending on the sign of D. If D is negative, then the forms $[a,2b+c_1,c]$ are positive definite, and we may write

$$\sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega\bar{f}}{E}\right) = \sum_{Q=[a,2b+c_1,c]}{}' \frac{1}{|\Gamma_Q|}\sideset{}{^*}\sum_{\alpha,\gamma} e(\theta_{\alpha,\gamma}), \tag{3.10}$$

where the summation over α and γ is no longer restricted to one representation of (3.6) and (3.7) and Γ_Q is the isotropy subgroup of Q in $\Gamma^0(fc_2)$. We consider this case completely before handling the indefinite case, $D > 0$.

Since the number of reduced forms is finite, we are primarily concerned with estimating

$$\sum_{\alpha,\gamma}^{*} e(\theta_{\alpha,\gamma}) = \sum_{|\gamma|<|\alpha|}^{*} e(\theta_{\alpha,\gamma}) + \sum_{|\alpha|<|\gamma|}^{*} e(\theta_{\alpha,\gamma}).$$

These two sums can be handled in the same way, so we will only provide details for the first. In this case, we have

$$\begin{aligned}(3.11)\qquad &\Big|\sum_{|\gamma|<|\alpha|}^{*} e(\theta_{\alpha,\gamma})\Big| \\ &\ll c_G \sum_{\alpha} \sup_{\lambda,\Lambda} \Big|\sum_{\gamma\equiv\lambda \,(\mathrm{mod}\, \Lambda)}^{*} e\bigg(\frac{h((\overline{fc_2}fc_2-1)c\bar{u}\gamma - \overline{fc_2}fc_2\bar{\gamma})}{fc_2\alpha} + h\phi_{\alpha,\gamma}\bigg)\Big|.\end{aligned}$$

We will use partial summation to handle this inner sum. To do so, we note that

$$(3.12)\qquad \phi_{\alpha,\gamma} - \phi_{\alpha,\gamma+1} \ll \frac{\max(|a|,|b|,|c|)}{|\alpha| qM}.$$

We will also need the following estimate for incomplete Kloosterman sums, which can be derived from Weil's bound via the method of completion.

LEMMA 9. *If u, v, and s are integers and if $0 < r_2 - r_1 < 2s$, then, for any integers λ and Λ, we have*

$$\sum_{\substack{r_1<r<r_2,\,(r,s)=1\\ r\equiv\lambda \,(\mathrm{mod}\, \Lambda)}} e\bigg(\frac{ur+v\bar{r}}{s}\bigg) \ll s^{1/2+\epsilon}(u,v,s)^{1/2}.$$

Now, by using Lemma 9 and (3.12) with partial summation in (3.11), we deduce that

$$\begin{aligned}\Big|\sum_{|\gamma|<|\alpha|}^{*} e(\theta_{\alpha,\gamma})\Big| &\ll c_G q^{1/4+\epsilon} M^{1/4+\epsilon} f^{1/4}\bigg(1 + \frac{h\max(|a|,|b|,|c|)}{qM}\bigg)\sum_{\alpha}(\alpha,h)^{1/2} \\ &\ll c_G q^{3/4+\epsilon} M^{3/4+\epsilon} f^{-1/4+\epsilon}\bigg(1 + \frac{h\max(|a|,|b|,|c|)}{qM}\bigg)\tau(h).\end{aligned}$$

We obtain the same estimate for $\sum^{*}_{|\alpha|<|\gamma|}$.

If $G(x)$ is monic, then $\max(|a|,|b|,|c|) \ll |D|^{1/2} = O(1)$ by the theory of reduced forms for $\mathrm{SL}_2(\mathbb{Z})$ $(= \Gamma^0(1))$. Since the number of reduced forms is finite and depends only on the discriminant, we then have

$$\sum_{E,\Omega}^{*} e\bigg(\frac{h\Omega}{E}\bigg) = O\bigg(q^{3/4+\epsilon} M^{3/4+\epsilon}\bigg(1 + \frac{h}{qM}\bigg)\tau(h)\bigg).$$

The same estimate holds for $\sum_{m,\Omega} e\big(\frac{h\Omega}{mq}\big)$, establishing (3.5).

If $G(x)$ is not monic, by considering the coset representatives of $\Gamma^0(fc_2)$ in $\mathrm{SL}_2(\mathbb{Z})$, which can be taken modulo fc_2, we obtain $\max(|a|,|b|,|c|) = O(f^2)$, from which it follows that

$$\sum_{E,\Omega}^{*} e\left(\frac{h\Omega}{E}\right) \ll q^{7/4+\epsilon}M^{3/4+\epsilon}f^{1/4+\epsilon}H_D(fc_2)\left(1+\frac{hf^2}{qM}\right)\tau(h),$$

where $H_D(fc_2)$ denotes the number of reduced forms of discriminant D with respect to the action of $\Gamma^0(fc_2)$. By again considering the coset representatives of $\Gamma^0(fc_2)$ in $\mathrm{SL}_2(\mathbb{Z})$, we see that

$$H_D(fc_2) \le H_D(1)[\mathrm{SL}_2(\mathbb{Z}) : \Gamma^0(fc_2)] \ll f^{1+\epsilon}.$$

Hence,

$$\begin{aligned}\sum_{m,\Omega} e\left(\frac{h\Omega}{mq}\right) &\ll (qM)^{1+\epsilon}T^{-1+\epsilon} + q^{7/4+\epsilon}M^{3/4+\epsilon}\tau(h)\\ &\quad\times \sum_{f\le T}^{*}\sum_{(u,fc_2)=1}\rho(f)H_D(fc_2)f^{1/4+\epsilon}\left(1+\frac{hf^2}{qM}\right)\\ &\ll (qM)^{1+\epsilon}T^{-1+\epsilon} + q^{7/4+\epsilon}M^{3/4+\epsilon}T^{9/4+\epsilon}\tau(h)\left(1+\frac{hT^2}{qM}\right)\sum_{f\le T}^{*}1\\ &\ll (qM)^{1+\epsilon}T^{-1+\epsilon} + q^{7/4+\epsilon}M^{3/4+\epsilon}T^{9/4+\epsilon}\tau(h)\left(1+\frac{hT^2}{qM}\right),\end{aligned}$$

where, on the last line, we have used the fact that there are $O(T^\epsilon)$ values of $f \le T$ whose prime divisors all divide c_2. Upon choosing $T = q^{-3/13}M^{1/13}$, we see that (3.5) holds, with

$$\sum_{m,\Omega} e\left(\frac{h\Omega}{mq}\right) \ll q^{16/13+\epsilon}M^{12/13+\epsilon}(1+hq^{-19/13}M^{-11/13})\tau(h).$$

We now consider the indefinite case (i.e. when $D > 0$). To deduce (3.5) from the sum in (3.8), we apply the theory of Pell-type equations. If $D \equiv 0 \pmod 4$, let

$$u^2 - \frac{D}{4}v^2 = 1$$

be chosen such that $\tau := u + v\sqrt{D/4}$ is minimal with $\tau > 1$. If $\tau^m = u_m + v_m\sqrt{D/4}$, let $k = k_{fc_2}$ be the smallest positive integer such that $v_k \equiv 0 \pmod{fc_2}$. If $D \equiv 1 \pmod 4$, let

$$u^2 + uv - \frac{D-1}{4}v^2 = 1$$

be chosen such that $\tau := u + v\left(\frac{1+\sqrt{D}}{2}\right)$ is minimal with $\tau > 1$. If $\tau^m = u_m + v_m\left(\frac{1+\sqrt{D}}{2}\right)$, we again let k be the smallest positive integer such that $v_k \equiv 0 \pmod{fc_2}$.

With this notation, since we may take $a > 0$, there is a unique representative of (3.6) and (3.7) satisfying $\alpha > 0$ and

$$-\frac{2a(\tau^k-1)}{b+(\tau^k+1)\sqrt{D}}\alpha < \gamma \le \frac{2a(\tau^k-1)}{(\tau^k+1)\sqrt{D}-b}\alpha.$$

We apply the same techniques as in the positive definite case and find that

$$\sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega}{E}\right) \ll c_G q^{3/4+\epsilon} M^{3/4+\epsilon} f^{9/4+\epsilon} H_D(fc_2)\left(1+\frac{hf^2}{qM}\right)\tau(h),$$

from which we derive that

$$\sum_{m,\Omega} e\left(\frac{h\Omega}{mq}\right) \ll q^{3/4+\epsilon} M^{3/4+\epsilon}\left(1+\frac{h}{qM}\right)\tau(h)$$

if $G(x)$ is monic, and

$$\sum_{m,\Omega} e\left(\frac{h\Omega}{mq}\right) \ll q^{8/7+\epsilon} M^{20/21+\epsilon}(1+hq^{-9/7}M^{-18/21})\tau(h)$$

if $G(x)$ is not monic. This establishes (3.5). ∎

Acknowledgements. The author would like to thank Ken Ono for bringing this problem to his attention and for providing many helpful comments along the way. He would also like to thank Henryk Iwaniec, Evan Dummit, Amanda Folsom, Marie Jameson, and Riad Masri for their comments on earlier versions of this paper.

References

[1] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. 16 (1962), 363–367.

[2] V. Bouniakowsky, *Nouveaux théorèmes relatifs à la distinction des nombres premiers et à la décomposition des entiers en facteurs*, Sci. Math. Phys. 6 (1857), 305–329.

[3] A. A. Buhštab [A. A. Bukhshtab], *Combinatorial strengthening of the sieve of Eratosthenes method*, Uspekhi Mat. Nauk 22 (1967), no. 3, 199–226 (in Russian).

[4] A. C. Cojocaru and M. R. Murty, *An Introduction to Sieve Methods and Their Applications*, London Math. Soc. Student Texts 66, Cambridge Univ. Press, Cambridge, 2006.

[5] J. Friedlander and H. Iwaniec, *The polynomial X^2+Y^4 captures its primes*, Ann. of Math. (2) 148 (1998), 945–1040.

[6] D. R. Heath-Brown, *Primes represented by x^3+2y^3*, Acta Math. 186 (2001), 1–84.

[7] C. Hooley, *On the greatest prime factor of a quadratic polynomial*, ibid. 117 (1967), 281–299.

[8] H. Iwaniec, *Almost-primes represented by quadratic polynomials*, Invent. Math. 47 (2) (1978), 171–188.

[9] P. Kuhn, *Über die Primteiler eines Polynoms*, in: Proc. Int. Congress of Mathematicians, Amsterdam, 1954, Noordhoff, Groningen, and North-Holland, Amsterdam, Vol. 2, 1954, 35–37.
[10] M. Laborde, *Buchstab's sifting weights*, Mathematika 26 (1979), 250–257.
[11] B. V. Levin, *A one-dimensional sieve*, Acta Arith. 10 (1964/1965), 387–397 (in Russian).
[12] H.-E. Richert, *Selberg's sieve with weights*, Mathematika 16 (1969), 1–22.
[13] A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), 185–208; erratum, ibid. 5 (1959), 259.
[14] J.-P. Serre, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. (2) 22 (1976), 227–260.
[15] Y. Wang, *On sieve methods and some of their applications*, Sci. Sinica 11 (1962), 1607–1624.

Robert J. Lemke Oliver
Department of Mathematics and Computer Science
Emory University
400 Dowman Drive
Atlanta, GA 30322, U.S.A.
E-mail: rlemkeo@emory.edu

Received on 30.8.2010 (6474)