ALMOST-PRIMES REPRESENTED BY IRREDUCIBLE POLYNOMIALS

ROBERT J. LEMKE OLIVER

Abstract. Let $G(x)$ be an irreducible polynomial with integer coefficients. It is conjectured that the set $\{n \in \mathbb{N} : G(n) \text{ is prime}\}$ is infinite for most $G(x)$. If P_r denotes the set of squarefree positive integers with at most r prime factors, we consider the set $\{n \in \mathbb{N} : G(n) \in P_r\}$ with the goal of showing that it is infinite for a suitable choice of r. Considerable work has been done on this problem, with the most notable results being due to Iwaniec, Buhštab, and Richert. Here we show that if $\deg(G(x)) = 2$, then we may take $r = 2$. For those $G(x)$ with $\deg(G(x)) \geq 3$, we establish conditions on $G(x)$ which allow us to conclude that there is a suitable choice of $r \leq \deg(G(x))$.

1. Introduction

Let $G(x) = c_g x^g + c_{g-1}x^{g-1} + \ldots + c_1 x + c_0 \in \mathbb{Z}[x]$ 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 [14] and Bateman and Horn [1]:

Conjecture. Assuming the notation and hypotheses above, we have that

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

where

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

Dirichlet's Theorem on primes in arithmetic progressions implies that this conjecture is true when $g = 1$. Very little is known if $g \geq 2$.

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 represent primes infinitely often.

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 $G(x)$ represents P_{g+1} infinitely often. For $g \leq 7$, this is due to Kuhn [10], Wang [16], and Levin [12], and for general g this follows from work of Buhštab [3] and Richert [13]. In the special case of $G(x) = x^2 + 1$, a deep theorem of Iwaniec [9] 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. 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 that $\rho_G(2) = 2$. 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 $G(x)$ is twice P_2 infinitely often.

Theorem 1 follows from the next theorem, which concerns polynomials of general degree $g \geq 2$. To ease notation, we say that $G(x)$ is *good* if it satisfies the following five conditions:

(I) $c_g > 0$.

(II) $\Gamma_G \neq 0$.

(III) If we define the multiplicative function $\psi(m)$ by the Möbius inversion

$$\psi(m) := (\rho * \mu)(m) = \sum_{d|m} \rho(d)\mu\left(\frac{m}{d}\right),$$

then there is an $\alpha_1 < 1$ such that for any $0 < Y < X$ and $\mu, q \geq 1$ we have

$$\sum_{\substack{X<x<X+Y \\ x\equiv\mu(\text{mod } q)}} \psi(x) \ll_\epsilon Y^{\alpha_1+\epsilon}.$$

(IV) There are constants $\alpha_2 < 1$, $\alpha_3 < 1 - \alpha_2$, β_2, and β_3 such that if we let $0 < M < M_1 < 2M$ be real, q be a squarefree positive integer, d be an odd divisor of q, μ be an integer coprime to d, ω be a solution of the congruence $G(x) \equiv 0 \,(\text{mod } d)$, $h \neq 0$ be an integer, $\tau(h)$ be the number of divisors of h, $e(x) = e^{2\pi i x}$, and $\epsilon > 0$, then we have

$$\sum_{\substack{M<m<M_1, (m,q)=1, m\equiv\mu(\text{mod } d) \\ 0\leq\Omega<qm, G(\Omega)\equiv 0(\text{mod } mq), \Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{mq}\right) \ll \left(1 + hM^{\alpha_3+\epsilon}q^{\beta_3+\epsilon}\right) M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}\tau(h).$$

(V) If $z = x^\gamma$ for some $\gamma > 0$ and $P(z) = \prod_{p<z} p$, then

$$\#\{1 \leq n < x : (G(n), P(z)) = 1 \text{ and } G(n) \text{ is not squarefree}\} = o\left(\frac{x}{\log x}\right).$$

With this definition, we have the following theorem.

Theorem 2. If $G(x)$ is good, then there is an $r \leq g$ such that $G(x)$ is in P_r infinitely often.

Three Remarks:

1) As the proof of Theorem 2 will show, the least $r \leq g$ guaranteed by conditions (I) through (V) may be determined explicitly.

2) Condition (IV) in our definition of a good polynomial should be thought of as saying that we have a power savings in M over the trivial estimate $O_q(M)$. It is stated in the above form purely for convenience in the proof of Theorem 1.

3) Here we verify conditions (III), (IV), and (V) for quadratic polynomials. Hooley [8] has shown an equidistribution result similar to (IV) for the polynomial $G(x) = x^3+2$, conditional upon his Hypothesis R* on the size of short Kloosterman sums. In another paper, Hooley [7] also established results on the number of squarefree values of a cubic polynomial, which may possibly be adapted to prove (V).

To prove Theorem 2, we generalize the method employed by Iwaniec [9] to consider polynomials of arbitrary degree $g > 1$. In doing so, we transform the original problem into one of estimation of the error in the linear sieve. To obtain non-trivial cancellation in the error terms in these estimates, we need a result on the distribution of roots of $G(x)$ to various moduli, which we establish in Section 2 (see Lemma 3). From these estimates, we are able to establish Theorem 2 in Section 3 by generalizing the method of Iwaniec. In Section 4, we show that any irreducible quadratic polynomial satisfies conditions (III), (IV), and (V), thereby establishing Theorem 1.

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.

Notation

Throughout this paper, the use of ϵ represents an arbitary positive real number which may change from one equation to the next. Whenever an ϵ appears in an asymptotic bound, the implied constant implicitly depends upon it. We will also adopt the convention that p always represents a prime number. This occurs most frequently in the indices of sums and products, which are then assumed to be taken only over primes. Lastly, as we are concerned with a fixed choice of $G(x)$, we consider the discriminant D to be a constant in our asymptotic statements.

2. An equidistribution result for the congruence $G(x) \equiv 0 \,(\mathrm{mod}\ m)$

In this section we assume that $G(x)$ satisfies the conditions (III) and (IV) (we do not require that (I), (II), or (V) hold). We will use these conditions to derive an equidistribution result for the roots of the congruence $G(x) \equiv 0 \pmod{m}$, but before we can do this, we need a result concerning the Dirichlet series $L(\psi, s) := \sum_{m=1}^{\infty} \frac{\psi(m)}{m^s}$, where $\psi = \rho * \mu$ and $\rho(m)$ is the number of incongruent solutions to $G(x) \equiv 0 \pmod{m}$.

Lemma 1. 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

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

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 real and tending to 1 from the right, we have that

$$\log\left(L_0(\psi, s)\right) \quad = \quad \sum_{p \nmid D} \log\left(1 + \frac{\psi(p)}{p^s}\right) \leq (1 + \delta) \sum_{p \nmid D} \frac{\psi(p)}{p^s}$$

and

$$\log\left(L_0(\psi,s)\right) \geq (1-\delta)\sum_{p\nmid D}\frac{\psi(p)}{p^s},$$

where $\delta > 0$ is some small number tending to 0 as s tends to 1. Since $\rho(p)$ depends only on the conjugacy class C of Frob_p in $\mathrm{Gal}(G)$ and $\psi(p) = \rho(p) - 1$, we have, letting $\mathrm{Gal}(G)^{\#}$ denote the set of conjugacy classes of $\mathrm{Gal}(G)$, that

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

where $\theta(s)$ is real-valued and continuous for $s \geq 1$. The last equality follows from the Chebotarev Density Theorem (for example, see Proposition 1.5 of [15]). Since $\rho(C)$ is the number of roots of $G(x)$ in $\mathbb{C}$ fixed by elements of C, 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 that

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

by Burnside's Lemma. Hence, we see that

$$\log\left(L_0(\psi,s)\right) \leq (1+\delta)\theta(s) \quad \text{and} \quad \log\left(L_0(\psi,s)\right) \geq (1-\delta)\theta(s).$$

Thus, $L_0(\psi,1)$ exists and is real. The fact that $L(\psi,1)$ is positive comes immediately from its Euler product and the definition of $\psi(m)$. □

We will also need a lemma of Iwaniec [9, Lemma 7] on the approximation of the characteristic function $\chi_I(t)$ of the interval $I := [\alpha,\beta)$ by Fourier series.

Lemma 2 (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

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

with Fourier coefficients A_h and B_h satisfying

$$|A_h|,|B_h| \leq \min\left(\frac{1}{|h|},\frac{\Delta^{-2}}{|h|^3}\right) =: C_h. \tag{2.1}$$

Armed with Lemmas 1 and 2, we now prove the main result of this section, which is a generalization of Iwaniec's Lemma 4 [9]. For a squarefree integer q we define

$$A(q) := \frac{\phi(q)}{q}\frac{L(\psi,1)}{L_q(\psi,1)}, \tag{2.2}$$

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

$$L_q(\psi,1) := \prod_{p|q}\left(1+\frac{\psi(p)}{p}+\ldots+\frac{\psi(p^{r_p})}{p^{r_p}}\right), \tag{2.3}$$

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.

Lemma 3. 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 $M<m<M_1$, $(m,q)=1$, $m\equiv\mu\,(\text{mod } d)$, $\alpha\le\frac{\Omega}{mq}<\beta$, $G(\Omega)\equiv 0\,(\text{mod } mq)$, and $\Omega\equiv\omega\,(\text{mod } d)$. Then there are constants $\alpha_0<1$ and β_0 such that, for every $\epsilon>0$,

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

Proof. By Lemma 2, we have that

$$\begin{aligned} P(M_1,M;q,d,\mu,\omega,\alpha,\beta) = (\beta-\alpha) &\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod } d)\\ 0\le\Omega<mq,G(\Omega)\equiv0(\text{mod } mq),\Omega\equiv\omega(\text{mod } d))}} 1 \\ &+O\left(\rho(q)\Delta M+\sum_{h\neq0}C_h\left|\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod } d)\\ 0\le\Omega<mq,G(\Omega)\equiv0(\text{mod } mq),\Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{mq}\right)\right|\right). \end{aligned} \tag{2.4}$$

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

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

Hence, by (III), we have that

$$\begin{aligned}\rho\left(\frac{q}{d}\right)\sum_{\substack{M<m<M_1\\(m,q)=1\\m\equiv\mu(\text{mod }d)}}\rho(m) &= \rho\left(\frac{q}{d}\right)\sum_{a\leq T,(a,q)=1}\psi(a)\left(\phi\left(\frac{q}{d}\right)\frac{M_1-M}{aq}+O\left(\phi\left(\frac{q}{d}\right)\right)\right)\\ &\quad+O\left(\rho(q)\phi(q)M^{\frac{1+\alpha_1}{2}+\epsilon}\right)\\ &=\rho\left(\frac{q}{d}\right)\phi\left(\frac{q}{d}\right)\frac{M_1-M}{q}\sum_{\substack{a\leq T\\(a,q)=1}}\frac{\psi(a)}{a}+O\left(\rho(q)\phi(q)T^{1+\epsilon}\right)+O\left(\rho(q)\phi(q)M^{\frac{1+\alpha_1}{2}+\epsilon}\right)\\ &=\rho\left(\frac{q}{d}\right)\phi\left(\frac{q}{d}\right)\frac{M_1-M}{q}\frac{L(\psi,1)}{L_q(\psi,1)}+O\left(\rho(q)\phi(q)\left(M\frac{\phi(q)}{q}T^{\alpha_1-1+\epsilon}+T^{1+\epsilon}+M^{\frac{1+\alpha_1}{2}+\epsilon}\right)\right).\end{aligned}$$

By choosing $T=M^{\frac{1}{2-\alpha_1}}$, we see that the error above is $O\left(M^{\frac{1+\alpha_1}{2}+\epsilon}q^{1+\epsilon}\right)$.

We now estimate the error term in (2.4), which is

$$O\left(\rho(q)\Delta M+\sum_{h\neq 0}C_h\left|\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod }d)\\0\leq\Omega<mq,G(\Omega)\equiv0(\text{mod }mq),\Omega\equiv\omega(\text{mod }d)}}e\left(\frac{h\Omega}{mq}\right)\right|\right).$$

By (IV), we may bound the above sum by

$$\begin{aligned}\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod }d)\\0\leq\Omega<mq,G(\Omega)\equiv0(\text{mod }mq),\Omega\equiv\omega(\text{mod }d)}}e\left(\frac{h\Omega}{mq}\right) &\ll M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}\sum_{h\neq0}C_h\left(1+hM^{\alpha_3+\epsilon}q^{\beta_3+\epsilon}\right)\tau(h)\\ &\ll M^{\alpha_2+\epsilon}q^{\beta_2+\epsilon}\left(1+\frac{M^{\alpha_3+\epsilon}q^{\beta_3+\epsilon}}{\Delta}\right)(\log\Delta)^2,\end{aligned}$$

where the last equality has come from (2.1).

If $\alpha_3<0$, we take $\Delta=M^{\alpha_3}q^{\beta_3}$, yielding that the error in equation (2.4) is

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

in which case we may take $\alpha_0=\max\left(\frac{1+\alpha_1}{2},\alpha_2,1+\alpha_3\right)$ and $\beta_0=\max\left(1,\beta_2,\beta_3\right)$. If $\alpha_3\geq0$, we take $\Delta=M^{\frac{\alpha_2+\alpha_3-1}{2}}q^{\beta_3}$, yielding that the error in equation (2.4) is

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

and we may take $\alpha_0=\max\left(\frac{1+\alpha_1}{2},\frac{1+\alpha_2+\alpha_3}{2}\right)$ and $\beta_0=\max\left(1,\beta_2,\beta_3\right)$.

□

3. Proof of Theorem 2

We now generalize the method of Iwaniec [9] to obtain an estimate for

$$\#\{1\leq n<x:G(n)\in P_r\},$$

where $r\leq g$ is a positive integer. We will introduce a weighted sum in Section 3.1 which will change the problem into one of establishing estimates of sifting functions, which we study by using the linear sieve in Section 3.2. In Section 3.3, we then use these estimates to complete the proof of Theorem 2. Throughout Section 3 we assume that $G(x)$ satisfies the conditions (I), (III), (IV), and (V). Only in Section 3.3 will we assume condition (II).

3.1. **A weighted sum.** If we let

$$\mathcal{A} := \{G(n) : 1 \le n < x\}, \tag{3.1}$$

we wish to estimate the sum

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

To do so, we introduce a weight function $w(n)$ and instead sum $w(a)$. Let λ be a real number such that $g \le \lambda < g + 1$, 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 $p < x^{\lambda/r}$ such that $p|n$, let

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

then let

$$w(n) := 1 - \frac{\lambda/r}{g+1-\lambda} \sum_{p|n, p<x^{\lambda/r}} \omega_p(n). \tag{3.2}$$

Remark. The weights $w(n)$ are essentially the same weights that Iwaniec used, which are due to Richert (unpublished, see [9]). Laborde [11] developed weights which would yield a slightly sharper estimate for $\#\mathcal{A} \cap P_r$, resulting in an improved value of r for high degree g. The need for conditions (III), (IV), and (V) remains unchanged, however, so we make this choice of $w(n)$ for simplicity.

Lemma 4. If $n \le x^\lambda$ and $w(n) > 0$, then n has at most r distinct prime factors.

Proof. If $p_n < q < x^{\lambda/2r}$ are primes dividing n, then we have

$$w(n) \;\le\; 1 - \frac{\lambda/r}{g+1-\lambda}\left(1 - \frac{\log p_n}{\lambda/r \log x} + \frac{\log p_n}{\lambda/r \log x}\right) = \frac{g+1-\frac{r+1}{r}\lambda}{g+1-\lambda} \le 0.$$

Hence, n has at most one prime factor less than $x^{\lambda/2r}$. Thus, we have that

$$w(n) \;=\; 1 - \frac{\lambda/r}{g+1-\lambda} \sum_{p|n} \left(1 - \frac{\log p}{\lambda/r \log x}\right) \le \frac{g+1-\frac{\lambda}{r}\omega(n)}{g+1-\lambda},$$

whence $\omega(n) \le r$. □

By Lemma 4, for any $z \le x^{\lambda/2r}$ we have that

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

where $P(z) = \prod_{p<z} p$. Condition (V) guarantees that there are few non-squarefree $a \in \mathcal{A}$ such that $(a, P(z)) = 1$. Hence, we consider the sum

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

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

$$\mathcal{A}_q := \{a \in \mathcal{A} : a \equiv 0 \,(\mathrm{mod}\ q)\}.$$

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

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

namely that

$$\begin{aligned} W(\mathcal{A}, z) &= S(\mathcal{A}, z) + \frac{\lambda/r}{g+1-\lambda}\Bigg[\sum_{z\le p<x^{\lambda/2r}} \sum_{z\le p_1<p} \frac{\log p/p_1}{\lambda/r\log x} S(\mathcal{A}_{pp_1}, p_1) \\ &\quad - \sum_{z\le p<x^{\lambda/2r}} \left(\left(1 - 2\frac{\log p}{\lambda/r\log x}\right) S(\mathcal{A}_p, p) + \frac{\log p}{\lambda/r\log x} S(\mathcal{A}_p, z)\right) \\ &\quad - \sum_{x^{\lambda/2r}<p<x^{\lambda/r}} \left(1 - \frac{\log p}{\lambda/r\log x}\right) S(\mathcal{A}_p, z)\Bigg]. \end{aligned} \tag{3.3}$$

3.2. **The linear sieve.** By means of (3.3), we have transformed the problem of estimating how often $G(x)$ represents P_r into an estimation of the sifting functions $S(\mathcal{A}_q, u)$. We recall the following linear sieve inequality [9, Lemma 2].

Lemma 5 (Iwaniec)**.** *Let $q \ge 1$, $u \ge 2$, $M \ge 2$, and $N \ge 2$. For any $\eta > 0$ we have*

$$\begin{aligned} S(\mathcal{A}_q, u) &\le V(u)x(F(s) + E) + 2^{\eta^{-7}} R(\mathcal{A}_q; M, N), \\ S(\mathcal{A}_q, u) &\ge V(u)x(f(s) - E) - 2^{\eta^{-7}} R(\mathcal{A}_q; M, N), \end{aligned}$$

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

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

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

$$R(\mathcal{A}_q; M, N) = \sum_{m<M, n<N, mn|P(u)} a_m b_n r(\mathcal{A}_q; mn), \tag{3.4}$$

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 6. With notation as in Lemma 5, 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 $\gamma_1 := \frac{4\alpha_0}{1+\beta_0}$.

Proof. 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 the equidistribution results from Section 2. By the Cauchy-Schwarz inequality, we get

$$\sum_{M<m<2M} |B(x; m, N)| \leq M^{\frac{1}{2}} \left(\sum_{M<m<2M} B(x; m, N)^2 \right)^{\frac{1}{2}}. \tag{3.5}$$

Since we have that

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

the Cauchy-Schwarz inequality implies that

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

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

$$\sum_{M<m<2M} B(x; m, N)^2 \ll M^\epsilon \left(W(x; M, N) - 2xV(x; M, N) + x^2 U(M, N) \right), \tag{3.6}$$

where

$$W(x;M,N) \;:=\; \sum_{M<m<2M} \sum_{\substack{0\le v<m\\ G(v)\equiv 0(\mathrm{mod}\ m)}} \sum_{\substack{n_1,n_2<N\\ (n_1n_2,m)=1}} b_{n_1}b_{n_2} \sum_{\substack{k_1,k_2<x\\ k_1\equiv k_2\equiv v(\mathrm{mod}\ m)\\ G(k_1)\equiv G(k_2)\equiv 0(\mathrm{mod}\ n)}} 1, \tag{3.7}$$

$$V(x;M,N) \;:=\; \sum_{M<m<2M} \sum_{\substack{0\le v<m\\ G(v)\equiv 0(\mathrm{mod}\ m)}} \sum_{\substack{n_1,n_2<N\\ (n_1n_2,m)=1}} b_{n_1}b_{n_2}\frac{\rho(n_2)}{n_2} \sum_{\substack{k<x\\ k\equiv v(\mathrm{mod}\ m)\\ G(k)\equiv 0(\mathrm{mod}\ n_1)}} 1, \tag{3.8}$$

and

$$U(M,N) := \sum_{M<m<2M} \sum_{\substack{0\le v<m\\ G(v)\equiv 0(\mathrm{mod}\ m)}} \frac{1}{m^2} \sum_{\substack{n_1,n_2<N\\ (n_1n_2,m)=1}} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}. \tag{3.9}$$

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 (3.6). Our main tools to this end are Lemma 3 and partial summation. We follow the method of Iwaniec [9, Proof of Proposition 1] closely, with more effort being necessary only in the estimation of $W(x;M,N)$. Consequently, we state only the results for $U(M,N)$ and $V(x;M,N)$, 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

$$U(M,N) = \frac{1}{2M}\sum_{n_1,n_2<N} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}A([n_1,n_2]) + O\left(M^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}\right), \tag{3.10}$$

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

$$V(x;M,N) = \frac{x}{2M}\sum_{n_1,n_2<N} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1n_2}A([n_1,n_2]) + O\left(x^{\epsilon} + xM^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}\right). \tag{3.11}$$

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

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

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

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

and let

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

With the above definitions, we have

$$T^*(n_1,n_2;x,M) := \sum_{\substack{l_1,l_2<\frac{x}{M}\\ l_1\equiv l_2 (\mathrm{mod}\ (2,n_1,n_2))}} \sum_{\substack{0\le\mu<d\\ (\mu,d)=1}} \sum_{\substack{0\le v<d\\ G(\mu l_1+v)\equiv 0 (\mathrm{mod}\ d)\\ G(\mu l_2+v)\equiv 0 (\mathrm{mod}\ d)}} \sum_{\substack{M<m<M_1,(m,n_1n_2)=1\\ m\equiv\mu (\mathrm{mod}\ d), cm\le\Omega<(c+1)m\\ \Omega\equiv\mu l_1+v (\mathrm{mod}\ d), G(\Omega)\equiv 0 (\mathrm{mod}\ m[n_1,n_2])}} 1, \tag{3.12}$$

where $M_1=\min\left(2M,\frac{x}{l_1},\frac{x}{l_2}\right)$. The innermost sum in (3.12) 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 3 implies that

$$\begin{aligned} T^*(n_1,n_2;x,M) &= \frac{A([n_1,n_2])\rho([n_1,n_2])}{[n_1,n_2]} \sum_{\substack{l_1,l_2<\frac{x}{M}\\ l_1\equiv l_2 (\mathrm{mod}\ (2,n_1,n_2))}} \frac{M_1-M}{\rho(d)\phi(d)}\sum_{\mu,v}1 \\ &\quad +O\left(x^2M^{\alpha_0-2+\epsilon}N^{2\beta_0+\epsilon}\right). \end{aligned} \tag{3.13}$$

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 μl_1+v and μl_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. Hence, the sum in (3.13) is equal to

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

Let $n\mid(n_1,n_2)$ be maximal such that $\psi(n)\neq 0$, and let $n_0=\frac{(n_1,n_2)}{n}$. Since we have

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

it follows that $\psi\left(\frac{(n_1,n_2)}{(n_1,n_2,l_1-l_2)}\right)=0$ unless $n_0\mid(l_1-l_2)$. Hence, we consider

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

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

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

Both $\psi(m)$ and $\phi(m)$ are multiplicative functions, so we can define a multiplicative function $\xi(m)$ such that $\frac{\phi}{\psi} = 1 * \xi$. Then we have that

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

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

$$\sum_{l_2<\frac{x}{M}} l_2\left(\min\left(2M, \frac{x}{l_2}\right) - M\right) = \frac{x^2}{4M} + O(x).$$

Inserting these estimates into (3.13), we now see that

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

Hence, we have

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

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

$$\begin{aligned}W(x; M, N) &= \frac{x^2}{2M}\sum_{n_1,n_2<N} b_{n_1}b_{n_2}\frac{\rho(n_1)\rho(n_2)}{n_1 n_2}A([n_1, n_2])\\ &\quad + O\left(x^{1+\epsilon} + x^2 M^{\alpha_0-2+\epsilon}N^{2+2\beta_0+\epsilon}\right).\end{aligned} \tag{3.14}$$

Inserting the estimates (3.10), (3.11), and (3.14) into (3.6), we see that the main terms cancel, and we obtain that

$$\sum_{M<m<2M} B(x; m, N)^2 \ll \left(x + x^2 M^{\alpha_0-2}N^{2+2\beta_0}\right)x^{\epsilon}M^{\epsilon}N^{\epsilon}. \tag{3.15}$$

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 (3.15) in equation (3.5), and obtain

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

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

Armed with Lemma 6, we are now able to acquire the desired estimate for the sifting functions $S(\mathcal{A}_q, u)$.

Lemma 7. If $z < x^{\lambda/2r}$, then for any $\epsilon > 0$ and x sufficiently large, we have

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

with γ_0 as defined in Lemma 6, 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 [9], so we present it without proof. We obtain a lower bound for the sum in Lemma 7 by replacing F with f.

3.3. **Proof of Theorem 2.** With Lemma 7 at our disposal, we obtain a lower bound for the size of the set

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

for each $\frac{g}{1+\gamma_0} < r \le g$. The reason for the lower bound on r is made clear below.

We wish to apply Lemma 5 and Lemma 7 to equation (3.3) to obtain a lower bound for $W(\mathcal{A}, z)$. We may do this for each term in (3.3) but the short sum

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

However, in this case, we make the estimate

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

yielding the bound $O\left(\frac{\epsilon x}{\log x}\right)$. For notational convenience, set

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

By partial summation, we obtain

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

The functions $F(s)$ and $f(s)$ are only defined for $s > 0$, but the condition that $r > \frac{g}{\alpha}$ guarantees that we evaluate them only at positive values. Since $V(z) \asymp \log^{-1} x$ by Mertens' Theorem and (II), we wish to show that $W > 0$ for some r in the range $\frac{g}{\alpha} < r \leq g$.

By continuity, we may take $\lambda = g$. Furthermore, treating α and γ as constants, W depends only on the ratio $s := \frac{g}{r}$, and, in fact, decreases monotonically as s increases from 1. Similarly, W also decreases monotonically as α increases from 1. We therefore wish to find $\gamma < \frac{1}{2}$ such that $W|_{s=1,\alpha=1} > 0$. However, we will not immediately substitute $\alpha = 1$ into the above formula. Instead, we will choose $\gamma = \frac{\alpha}{6}$ and take the limit as α tends to 1 from the right. Using that

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

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

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

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

$$\begin{aligned} W|_{s=1} \;&=\; \frac{\alpha e^C}{3}\left(\log\left(\frac{5}{6}\alpha\right) - \frac{\alpha-1}{\alpha}\log(\alpha-1)\right. \\ &\qquad \left. - \int_2^4 \left[t\log\left(\frac{6(t+1)}{5(t+2)}\right) + (t+1)\log\left(1-\frac{t}{5}\right)\right]\frac{\log(t-1)}{t(t+1)}dt\right). \end{aligned}$$

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

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

which a numerical computation reveals to be positive.

4. Proof of Theorem 1

In this section we show that the criteria (III), (IV), and (V) are satisfied for any irreducible quadratic $G(x) = c_2x^2 + c_1x + c_0$, thereby establishing Theorem 1. We begin by considering (V). By Iwaniec's argument for $G(x) = x^2 + 1$ [9] coupled with an application of the square sieve [4, Theorem 2.3.5], we get that

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

Since λ can be taken to be $2 + \epsilon$ for any $\epsilon > 0$, this is $o\left(\frac{x}{\log x}\right)$ when $z = x^\gamma$ for any $\gamma > 0$. This confirms (V).

We now turn our attention to (III). If $(m, D) = 1$, then $\psi(m) = \left(\frac{D}{m}\right)\mu(m)^2$. Hence,

$$\begin{aligned} \sum_{\substack{X<m<X+Y \\ m\equiv\mu \pmod q}} \psi(m) \;&=\; \sum_{t|D}\psi(t) \sum_{\substack{\frac{X}{t}<m<\frac{X+Y}{t} \\ tm\equiv\mu \pmod q \\ (m,D)=1}} \left(\frac{D}{m}\right)\mu(m)^2 \\ &\ll\; Y^\epsilon \sum_{t|D} |\psi(t)|t^{-\epsilon} \ll Y^\epsilon, \end{aligned}$$

since $\sum_{t|D} |\psi(t)|t^{-\epsilon}$ depends only on D and ϵ. Thus, we may take $\alpha_1 = 0$ in (III).

Lastly, we must show that $G(x)$ satisfies (IV), which regards estimation of

$$\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod } d)\\ 0\le\Omega<qm,G(\Omega)\equiv 0(\text{mod } mq),\Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{mq}\right).$$

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

$$\sum_{\substack{M<m<M_1,(m,q)=1,m\equiv\mu(\text{mod } d)\\ 0\le\Omega<qm,G(\Omega)\equiv 0(\text{mod } mq),\Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{mq}\right) = \sum_{l|\frac{q}{d}} \mu(l) \sum_{\substack{qM<E<qM_1,E\equiv\mu q(\text{mod } dq),E\equiv 0(\text{mod } lq)\\ 0\le\Omega<E,G(\Omega)\equiv 0(\text{mod } E),\Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{E}\right).$$

We will estimate the inner sum by using the theory of quadratic forms. If c_2 and E are relatively prime, there is a bijection between roots $G(\Omega) \equiv 0\,(\text{mod } E)$ 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, we first take out the part of E not relatively prime to c_2, getting

$$\begin{aligned}\sum_{\substack{qM<E<qM_1,E\equiv\mu q(\text{mod } dq)\\ E\equiv 0(\text{mod } lq),0\le\Omega<E\\ G(\Omega)\equiv 0(\text{mod } E),\Omega\equiv\omega(\text{mod } d)}} e\left(\frac{h\Omega}{E}\right) &= \sideset{}{^*}\sum_{\substack{f\le T\\ (f,c_1)=1}} \sum_{\substack{0\le u<fc_2\\ (u,c_2)=1}} \sum_{\substack{0\le v<f\\ G(v)\equiv 0(\text{mod } f)\\ v\equiv\omega(\text{mod } (d,f))}} e\left(\frac{hv\bar{u}}{f}\right) \sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega\bar{f}}{E}\right)\\ &\quad +O\left((qM)^{1+\epsilon}T^{-1+\epsilon}\right),\end{aligned}$$

where the star on the first summation indicates that f is composed only of primes dividing c_2, $\bar{u}$ 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 $\frac{qM}{f} < E < \frac{qM_1}{f}$, $fE \equiv 0\,(\text{mod } lq)$, $fE \equiv \mu q\,(\text{mod } dq)$, $E \equiv u\,(\text{mod } fc_2)$, $0 \le \Omega < E$, $\Omega \equiv \omega \left(\text{mod } \frac{d}{(d,f)}\right)$, and $G(\Omega) \equiv 0\,(\text{mod } E)$.

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

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

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 $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma^0(fc_2)$ such that

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

where

$$\Gamma^0(fc_2) = \left\{\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbb{Z}) : \beta \equiv 0\,(\text{mod } fc_2)\right\}.$$

Then we have that

$$E = a\alpha^2 + (2b + c_1)\alpha\gamma + c\gamma^2 =: E_{\alpha,\gamma}, \tag{4.1}$$

and

$$y = 2a\alpha\beta + (2b + c_1)(\alpha\delta + \beta\gamma) + 2c\gamma\delta. \tag{4.2}$$

Hence, we see that

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

from which it follows that

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

Thus, we have that

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

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

$$\sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega\bar{f}}{E}\right) = \sideset{}{'}\sum_{Q=[a,2b+c_1,c]} \sideset{}{^*}\sum_{\alpha,\gamma} e\left(\theta_{\alpha,\gamma}\right), \tag{4.3}$$

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 $\frac{qM}{f} < a\alpha^2 + (2b + c_1)\alpha\gamma + c\gamma^2 < \frac{qM_1}{f}$, restricted to one representation of the form (4.1) and (4.2), and satisfying

$$\begin{aligned} &fE_{\alpha,\gamma} \equiv 0 \,(\mathrm{mod}\; lq)\,, \\ &fE_{\alpha,\gamma} \equiv \mu q \,(\mathrm{mod}\; dq)\,, \\ &E_{\alpha,\gamma} \equiv u \,(\mathrm{mod}\; fc_2)\,, \text{ and} \\ &\left(\tfrac{1-\bar{u}E_{\alpha,\gamma}}{c_2}\right)(c\gamma + b\alpha) - \alpha\omega \equiv 0 \left(\mathrm{mod}\; \tfrac{d}{(d,f)}\right). \end{aligned} \tag{4.4}$$

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

Returning to (4.3), 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

$$\sideset{}{^*}\sum_{E,\Omega} e\left(\frac{h\Omega\bar{f}}{E}\right) = \sideset{}{'}\sum_{Q=[a,2b+c_1,c]} \frac{1}{|\Gamma_Q|} \sideset{}{^*}\sum_{\alpha,\gamma} e\left(\theta_{\alpha,\gamma}\right), \tag{4.5}$$

where the summation over α and γ is no longer restricted to one representation of (4.1) and (4.2) 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

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

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

$$\left|\sum_{|\gamma|<|\alpha|}{}^{*} e\left(\theta_{\alpha,\gamma}\right)\right| \ll c_G \sum_{\alpha} \sup_{\lambda,\Lambda} \left|\sum_{\gamma\equiv\lambda(\mathrm{mod}\ \Lambda)}{}^{*} e\left(\frac{h\left(\left(\overline{fc_2}fc_2-1\right)c\bar{u}\gamma - \overline{fc_2}fc_2\bar{\gamma}\right)}{fc_2\alpha} + h\phi_{\alpha,\gamma}\right)\right|. \tag{4.6}$$

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

$$\phi_{\alpha,\gamma} - \phi_{\alpha,\gamma+1} \ll \frac{\max(|a|,|b|,|c|)}{|\alpha|qM}. \tag{4.7}$$

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

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

Now, by using Lemma 8 and (4.7) with partial summation in (4.6), we get that

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

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

If $G(x)$ is monic, then $\max(|a|,|b|,|c|) \ll |D|^{\frac{1}{2}} = O(1)$ by the theory of reduced forms for $SL_2(\mathbb{Z})(=\Gamma^0(1))$. Since the number of reduced forms is finite and depends only on the discriminant, we then have that

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

The same estimate holds for $\sum_{m,\Omega} e\left(\frac{h\Omega}{mq}\right)$, establishing condition (IV).

If $G(x)$ is not monic, by considering the coset representatives of $\Gamma^0(fc_2)$ in $SL_2(\mathbb{Z})$, which can be taken modulo fc_2, we obtain $\max(|a|,|b|,|c|) = O(f^2)$, from which it follows that

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

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 $SL_2(\mathbb{Z})$, we see that

$$H_D(fc_2) \leq H_D(1)[SL_2(\mathbb{Z}) : \Gamma^0(fc_2)] \ll f^{1+\epsilon}.$$

Hence, we have that

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

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

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

We now consider the indefinite case (i.e. when $D > 0$). To deduce (IV) from the sum in (4.3), 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 $\tau := u + v\sqrt{\frac{D}{4}}$ is minimal with $\tau > 1$. If $\tau^m = u_m + v_m\sqrt{\frac{D}{4}}$, 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 (4.1) and (4.2) satisfying $\alpha > 0$ and

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

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

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

from which we derive that

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

if $G(x)$ is monic, and

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

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

References

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

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

[3] A. A. Buhštab. Combinatorial strengthening of the sieve of Eratosthenes method. *Uspehi Mat. Nauk*, 22(3 (135)):199–226, 1967.

[4] A. C. Cojocaru and M. R. Murty. *An introduction to sieve methods and their applications*, volume 66 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 2006.

[5] J. Friedlander and H. Iwaniec. The polynomial $X^2 + Y^4$ captures its primes. *Ann. of Math. (2)*, 148(3):945–1040, 1998.

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

[7] C. Hooley. On the square-free values of cubic polynomials. *J. Reine Angew. Math.*, 229:147–154, 1968.

[8] C. Hooley. On the greatest prime factor of a cubic polynomial. *J. Reine Angew. Math.*, 303/304:21–50, 1978.

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

[10] P. Kuhn. Über die primteiler eines polynoms. proceedings of the International Congress of Mathematicians, Amsterdam. 2:35–37, 1954.

[11] M. Laborde. Buchstab's sifting weights. *Mathematika*, 26(2):250–257 (1980), 1979.

[12] B. V. Levin. A one-dimensional sieve. *Acta Arith.*, 10:387–397, 1964/1965.

[13] H.-E. Richert. Selberg's sieve with weights. *Mathematika*, 16:1–22, 1969.

[14] A. Schinzel and W. Sierpiński. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith. 4 (1958), 185–208; erratum*, 5:259, 1958.

[15] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques. *Enseignement Math. (2)*, 22(3-4):227–260, 1976.

[16] Y. Wang. On sieve methods and some of their applications. *Sci. Sinica*, 11:1607–1624, 1962.

Department of Mathematics, University of Wisconsin, Madison, Wisconsin 53706
E-mail address: lemkeoli@math.wisc.edu