Mathematische Zeitschrift (2021) 299:527–542
https://doi.org/10.1007/s00209-020-02674-7

Mathematische Zeitschrift

Common divisors of totients of polynomial sequences

J. Brüdern[1] · K. Soundararajan[2]

Received: 24 September 2019 / Accepted: 18 November 2020 / Published online: 6 February 2021

1 Introduction

This paper considers two related problems connected to sieving values of polynomials by primes lying in certain arithmetic progressions. The first problem was raised by Calegari [1], who asked in a blog post whether one can show that there are infinitely many n such that n^2+1 is not divisible by any prime $p \equiv 1 \bmod 2^m$ where m is some fixed large integer. One expects that the polynomial $(4n+2)^2+1 = 16n^2+16n+5$ takes prime values infinitely often, so that there should be infinitely many values of n with n^2+1 divisible by no prime $\equiv 1 \bmod 8$. In Theorem 4 we shall give a resolution of Calegari's question for irreducible quadratic polynomials.

The other problem, referenced in the title of the paper, was raised by Venkataramana [8,9]. Let $f \in \mathbb{Z}[x]$ be a primitive polynomial of degree k (that is, the coefficients of f have gcd equal to 1), and consider

$$\mathcal{G}(f) = \gcd\{\phi(f(n)) : n \in \mathbb{N}\}. \tag{1}$$

Venkataramana [8,9] asked whether $\mathcal{G}(f)$ is bounded by a number depending only on the degree k of the polynomial f. If this is the case, then we denote by $\mathcal{G}_k$ the lowest common multiple of $\mathcal{G}(f)$ as f varies over primitive polynomials of degree k. If Venkataramana's question has an affirmative answer for a particular degree k, then informally we shall say that $\mathcal{G}_k$ is finite.

Venkatarama handled the case of linear polynomials and found that $\mathcal{G}(f) \mid 4$ holds for all $f(n) = an+b$ with $(a,b)=1$. The polynomials n, $2n+1$ and $16n+5$ show that $\mathcal{G}(f)$ takes all three admissible values 1, 2 and 4. In particular, we have $\mathcal{G}_1 = 4$. Results of this type have been applied to the congruence subgroup problem, and as Venkataramana points out, in this context Serre [5] had obtained *inter alia* that $\mathcal{G}_1$ is a divisor of 8. If all values of the polynomial f are divisible by some prime $p \equiv 1 \bmod h$, then $\phi(f(n))$ will always have h as a divisor. Thus we see that Venkataramana's question is also related to sifting polynomial sequences by an arithmetic progression of primes.

✉ J. Brüdern
joerg.bruedern@mathematik.uni-goettingen.de

K. Soundararajan
ksound@stanford.edu

[1] Mathematisches Institut, Universität Göttingen, Bunsenstrasse 3–5, 37073 Göttingen, Germany

[2] Department of Mathematics, Stanford University, 450 Serra Mall, Bldg. 380, Stanford, CA 94305-2125, USA

In this paper we are concerned with bounding $\mathcal{G}(f)$ for polynomials of higher degree. In brief, we are able to establish the finiteness of $\mathcal{G}_2$, and we also give a bound for $\mathcal{G}(f)$ when the polynomial f splits completely into linear factors. The methods used in establishing that $\mathcal{G}_2$ is finite also resolve Calegari's question on sieving quadratic polynomials (see Theorem 4). Assuming the Schinzel conjectures on prime values taken by polynomials we are able to describe the factorisation of $\mathcal{G}(f)$ quite precisely, for all polynomials, and thereby establish the finiteness of $\mathcal{G}_k$. Examples will demonstrate that the conditional results are optimal in some cases. We now describe our results more precisely. Let us recall first Schinzel's hypothesis.

Schinzel's Hypothesis H Let $F_1, \dots, F_r$ be irreducible polynomials with integer coefficients, and positive leading coefficients. Suppose that the product $F_1 \cdots F_r$ is not divisible by any fixed prime. Then there are infinitely many natural numbers n such that $F_j(n)$ is prime for each $1 \le j \le r$.

Theorem 1 *Assume Schinzel's hypothesis. Let $f = f_1^{a_1} \cdots f_s^{a_s}$ be a primitive polynomial with integer coefficients, with the f_j being distinct irreducibles of degree k_j. Let r_j be the maximal integer such that K_{f_j} (a field obtained by adjoining a root of f_j to $\mathbb{Q}$) contains the r_j-th roots of unity. Then $\phi(r_j)|k_j$, and $\mathcal{G}(f)$ divides $\phi(k!)r_1^2 \cdots r_s^2$.*

In the case of a linear polynomial f the proof of Theorem 1 will call upon Schinzel's hypothesis only for linear polynomials, whence that case depends on Dirichlet's theorem, and we recover Venkataramana's result unconditionally.

Example 1 Suppose $f(n) = \prod_{j=1}^{k}(a_j n+b_j)$ is the product of k primitive linear polynomials. Here Theorem 1 gives $\mathcal{G}(f) \mid 4^k\phi(k!)$. When $k=2$, the polynomial $f(n) = (16n+5)(16n+13)$ has $\mathcal{G}(f) = 16$, matching the bound of Theorem 1. More generally, if we consider $f(n) = (n+1)\cdots(n+k)$, then $k!$ divides $f(n)$ for all n and so $\phi(k!)$ divides $\mathcal{G}(f)$. So the result in Theorem 1 is tight except perhaps for the power of 2 dividing $\mathcal{G}(f)$.

Since quadratic fields have 2, 4, or 6 roots of unity, if f is a primitive irreducible polynomial of degree 2 then by Theorem 1 the possible values of $\mathcal{G}(f)$ must be divisors of 36 or 16 (assuming Schinzel's hypothesis). We now give examples to show that this cannot be sharpened, thereby showing that Schinzel's hypothesis implies $\mathcal{G}_2 = 144$.

Example 2 Consider the polynomial $f(n) = 16n^2+1$, which takes values $\equiv 1 \bmod 16$. The prime divisors of $f(n)$ are congruent to $1 \bmod 4$. Hence, if $f(n)$ has at least two distinct prime factors p_1, p_2, say, then $16|(p_1-1)(p_2-1)$, and therefore, $16 \mid \phi(f(n))$. It remains to consider the case where $f(n)$ is a power of a prime p. Since $f(n) = (4n)^2+1$ can never be a perfect square for $n \ge 1$, we may restrict attention to $f(n) = p^\ell$ with ℓ odd. But then p must be $1 \bmod 16$, and once again 16 divides $\phi(f(n))$. This proves that $\mathcal{G}(f) = 16$, with the convention that the natural numbers start at 1. If the natural numbers start at 0, simply consider $f(n+1)$. More generally, by shifting a polynomial by a large integer, we may discard any finite set of undesired values in understanding $\mathcal{G}$. The reader may wish to construct irreducible quadratic polynomials where $\mathcal{G}(f)$ is a given proper divisor of 16.

Example 3 Start with $f_0(n) = n^2+n+1$, and consider $f(n) = f_0(72n)$. The values of f are all $\equiv 1 \bmod 72$, and any prime factor of $f(n)$ must be $\equiv 1 \bmod 6$. Thus if $f(n)$ is divisible by two distinct primes then $\phi(f(n))$ will be a multiple of 36. If $f(n)$ is prime, then $\phi(f(n))$ will be a multiple of 72. It remains to consider the case $f(n) = p^\ell$ for $\ell \ge 2$. If $3 \nmid \ell$ and $4 \nmid \ell$ then $p^\ell \equiv 1 \bmod 72$ implies that $p \equiv 1 \bmod 36$, and once again 36 divides

$\phi(f(n))$. The last remaining possibilities entail that $f(n)$ is either a cube or a fourth power. Since these correspond to integer points on two curves of positive genus, there are only finitely many such n (which we could certainly determine in this example). By translating the polynomial f if necessary, we can avoid these finitely many examples, and arrive at a quadratic polynomial $\widetilde{f}$ with $36|\mathcal{G}(\widetilde{f})$. Similar examples can be constructed starting with other cyclotomic polynomials; for instance starting with $n^4+n^3+n^2+n+1$ we can find a quartic polynomial f with $25|\mathcal{G}(f)$.

In the above examples, we were led to consider when a polynomial with integer coefficients and degree at least 2 takes pure power values. We note, in passing, the work of Schinzel and Tijdeman [6] which ensures that if the polynomial has at least three simple zeros then there are only finitely many such pure power values.

Suppose now that f splits completely into linear factors. Then, as noted above, our conditional Theorem 1 tells us that $\mathcal{G}(f)$ is a divisor of $4^k\phi(k!)$. In this situation, we can give an unconditional bound for the possible values of $\mathcal{G}(f)$.

Theorem 2 *Suppose f is a primitive polynomial of degree k splitting completely into linear factors. Then $\mathcal{G}(f)$ is not divisible by any prime larger than $2k+1$. Moreover, for every prime ℓ not exceeding $2k+1$ there exists a constant $C(k,\ell)$ such that the power of ℓ dividing $\mathcal{G}(f)$ is at most $C(k,\ell)$.*

We are also able to show unconditionally that $\mathcal{G}_2$ is finite. In view of the preceding theorem, it is enough to consider primitive irreducible quadratic polynomials.

Theorem 3 *There is a number G with the property that for all primitive and irreducible quadratic polynomials f with positive leading coefficient one has $\mathcal{G}(f)\le G$.*

The proofs of the unconditional results depend on the fundamental lemma in sieve theory, and the switching principle. When discussing irreducible quadratic polynomials we will have to rely also on quantitative estimates concerning the equidistribution of the roots of quadratic polynomials, a subject initiated by Hooley [4]. We require bounds for averages of Weyl sums associated with these roots, twisted with an additive character. The works of Hooley [4], Duke et al. [2] and Toth [7] enable us to handle such sums. While the important works of Duke et al. [2] and Toth [7] permit very uniform such results, we only need a modest level of distribution which would already be accessible from Hooley's work.

As mentioned earlier, the techniques developed for proving Theorem 3 also allow us to provide an affirmative answer to a question of Calegari [1].

Theorem 4 *Let f be an irreducible quadratic polynomial with no fixed prime factor. There exist absolute constants δ and h_0 with the following property. If $h>h_0$ then there are infinitely many n such that $f(n)$ is divisible by no prime below n^{δ}, and by no prime $p\equiv 1 \bmod h$.*

2 Preliminary reductions

We begin with a simple lemma discussing what happens when a primitive polynomial is restricted to the integers in an arithmetic progression.

Lemma 1 *Let $f\in\mathbb{Z}[x]$ be a primitive polynomial, and let $a \bmod q$ be an arithmetic progression. The greatest common divisor of the coefficients of the polynomial $F(x)=f(a+qx)$ is composed only of primes dividing q, and must also be a divisor of $f(a)$. In particular, if $(f(a),q)=1$ then F is a primitive polynomial.*

Proof Let p be a prime with $p \nmid q$. When reduced mod p, the polynomials f and F both have the same degree. Since f is primitive, it is non-zero mod p, and therefore so is F. Thus the gcd of the coefficients of F is composed only of primes dividing q. It is clear that this gcd must divide $F(0) = f(a)$, and so the lemma holds. □

Although the coefficients of f have no common factor, it may still be that the values $f(n)$ for $n \in \mathbb{N}$ have a common factor. Our first lemma allows us to get rid of this common factor, and restrict attentions to polynomials for which the values have no non-trivial common factor.

Lemma 2 *Let $f \in \mathbb{Z}[x]$ be a primitive polynomial, and let d denote the greatest common factor of $f(n)$ for all $n \in \mathbb{N}$. Then d is a divisor of $k!$. Moreover, with $D = d\prod_{p \le k} p$ we may find a number $a \in \mathbb{Z}$ such that $F(x) = f(a + Dx)/d$ is a primitive polynomial with integer coefficients and with $F(n)$ being coprime to $k!$ for all n. In particular, the values $F(n)$ have no common factor. Finally, $\mathcal{G}(f)$ is a divisor of $\phi(d)\mathcal{G}(F)$.*

Proof Write the polynomial f in the basis of binomial coefficients: $f(x) = b_0\binom{x}{0} + b_1\binom{x}{1} + \ldots + b_k\binom{x}{k}$ with $b_i \in \mathbb{Z}$. By considering the values $x = 0, 1, \ldots, k$ we see that the greatest common factor of all the $f(n)$ (which we denote by d) is the greatest common factor of these coefficients $b_0, \ldots, b_k$. Since the denominators appearing in the binomial coefficients all divide $k!$, note that $d/(d, k!)$ divides every coefficient of f. Since f is primitive, we conclude that the common factor d must be a divisor of $k!$.

Suppose $p \le k$ and $p^\alpha \| d$. Then there must exist a residue class $a_p \bmod p^{\alpha+1}$ with $p^\alpha \| f(n)$ for all $n \equiv a_p \bmod p^{\alpha+1}$. Thus by the chinese remainder theorem we may find a progression $a + Dn$ with $F(x) = f(a + Dx)/d$ being a polynomial with integer coefficients and with $k!$ being coprime to all values of F. By Lemma 1, the polynomial F is primitive, and since $k!$ is coprime to the values $F(n)$, we know further that the values of F have no common prime factor. This establishes our second assertion fully. The third assertion that $\mathcal{G}(f)$ divides $\phi(d)\mathcal{G}(F)$ follows at once. □

Lemma 3 *Let $f \in \mathbb{Z}[x]$ be irreducible, and let K_f be a field obtained by adjoining some root of f to $\mathbb{Q}$. Given a natural number m, the following two conditions are equivalent:*

(i) *K_f contains the m-th roots of unity.*
(ii) *All but finitely many of the primes p that divide the values of f satisfy $p \equiv 1 \bmod m$.*

Proof If a large prime p divides a value of f, then there must be an ideal of norm p in K_f. If K_f contains the m-th roots of unity, then an ideal of norm p in K_f must lie above a prime of norm p in $\mathbb{Q}(e^{2\pi i/m})$. Since the primes that split completely in $\mathbb{Q}(e^{2\pi i/m})$ are $\equiv 1 \bmod m$, we conclude that (i) implies (ii).

That (ii) implies (i) follows upon applying the Chebotarev density theorem to the extension $K_f(e^{2\pi i/m})$ of K_f, obtained by adjoining (if necessary) the m-th roots of unity to K_f. The assumption (ii) means that if there is a prime of norm p in K_f then $p \equiv 1 \pmod m$, but then the Frobenius at any such prime in K_f acts trivially on the m-th roots of unity. Thus for almost all primes of degree 1 in K_f the Frobenius action on $K_f(e^{2\pi i/m})$ is the identity, implying that the degree $[K_f(e^{2\pi i/m}), K_f]$ must be 1. □

Lemma 4 *Assume Schinzel's Hypothesis. Let $f \in \mathbb{Z}[x]$ be a primitive irreducible polynomial of degree k, and suppose that $k!$ is coprime to the values of f. Let ℓ be a prime, and suppose that K_f contains the ℓ^α-th roots of unity, but not the $\ell^{\alpha+1}$-th roots. Then the largest power of ℓ that divides $\mathcal{G}(f)$ is at most 2α.*

Proof By Lemma 2 we know that f has no common prime factor, so that we may find a natural number a such that $\ell \nmid f(a)$ and $f(a) \neq 1$. Let $\beta \geq 0$ be the largest power of ℓ dividing $f(a)-1$. Consider the irreducible polynomial $F(x) = f(a+\ell^{\beta+1}x)$, which by Lemma 1 is primitive, and by Lemma 2 has no common prime factor. By Schinzel's hypothesis, we may find arbitrarily large n with $F(n)$ prime. Then $\phi(F(n)) = F(n) - 1 \equiv f(a) - 1 \bmod \ell^{\beta+1}$, so that the largest power of ℓ dividing $\mathcal{G}(F)$ is at most β. Since $\mathcal{G}(f)$ divides $\mathcal{G}(F)$, this establishes the lemma provided $\beta \leq 2\alpha$.

Suppose now that $\beta \geq 2\alpha+1 \geq \alpha+1$. By Lemma 3 we know that all but finitely many of the primes dividing $F(n)$ are $1 \bmod \ell^{\alpha}$ and also that there are infinitely many primes dividing $F(n)$ that are $\not\equiv 1 \bmod \ell^{\alpha+1}$. Let q be such a prime, and select q to be large enough so that q does not divide the discriminant of F. Since q does not divide the discriminant of F, we may pick a natural number a such that $q|F(a)$, but $q^2 \nmid F(a)$. Now consider the irreducible polynomial $F_2(x) = F(a+qx)/q$, which by Lemma 1 is primitive, and by Lemma 2 has no common prime factor (since the values of f are coprime to $k!$). By Schinzel's hypothesis $F_2(n)$ takes prime values infinitely often. Let p be one such prime value. Since the values of F are $1 \bmod \ell^{\alpha+1}$ (by our assumption that $\beta \geq 2\alpha+1$) and $q \not\equiv 1 \bmod \ell^{\alpha+1}$ we know that p also is not $1 \bmod \ell^{\alpha+1}$. Therefore the largest power of ℓ dividing $\mathcal{G}(f)$ is at most the power of ℓ dividing $(p-1)(q-1)$, which is 2α. This completes our proof. □

Corollary 1 *Assume Schinzel's Hypothesis. Let f be a primitive irreducible polynomial of degree k, and such that $k!$ is coprime to all the values $f(n)$. Let r be the maximal integer such that K_f contains the r-th roots of unity. Then $\phi(r)$ divides k, and $\mathcal{G}(f)$ divides r^2.*

Now we want to proceed to the general case of a polynomial of degree k, not necessarily irreducible. We begin with a simple observation.

Lemma 5 *If f and g are two coprime polynomials in $\mathbb{Z}[x]$ then for all large primes q at most one of $f(n)$ or $g(n)$ can be divisible by q.*

Proof By the Euclidean algorithm we may find polynomials u and v with integer coefficients and a non-zero integer c such that $f(x)u(x) + g(x)v(x) = c$. Thus if $q \nmid c$, then q can divide at most one of $f(n)$ or $g(n)$. □

Now we are ready for the general form of Lemma 4; indeed the argument follows closely our earlier argument, but we have kept the special case of Lemma 4 for the sake of clarity.

Lemma 6 *Assume Schinzel's Hypothesis. Let $f \in \mathbb{Z}[x]$ be a primitive polynomial of degree k and such that $k!$ is coprime to all the values $f(n)$. Suppose f factors as $f_1^{a_1} \cdots f_s^{a_s}$ where the $f_j \in \mathbb{Z}[x]$ are pairwise coprime irreducible polynomials and $a_j \geq 1$. Let ℓ be a prime, and suppose ℓ^{α_j} is the largest power of ℓ such that K_{f_j} contains the ℓ^{α_j}-th roots of unity. Then the largest power of ℓ dividing $\mathcal{G}(f)$ is at most $2(\alpha_1 + \ldots + \alpha_s)$.*

Proof Since the polynomials f_j are all primitive, we may find a natural number a such that $\ell \nmid f_j(a)$ for all j, and with $f_j(a) \neq 1$ for all j. Then $\ell^{\beta} \,\|\, \prod_j (f_j(a) - 1)$ for some non-negative integer β. Below we shall restrict ourselves to the progression $n \equiv a \bmod \ell^{\beta+1}$. On the progression $a \bmod \ell^{\beta+1}$ we must have $\ell^{\beta_j} \,\|\, (f_j(a + n\ell^{\beta+1}) - 1)$ for all n, where β_j is a non-negative integer. We now define inductively further residue classes $a_j \bmod q_j$ as follows.

Suppose a_j and q_j have been defined for $j < J$, and we now seek to define a_J and q_J. If $\beta_J \leq \alpha_J$ then take $a_J = q_J = 1$. Suppose now that $\beta_J \geq \alpha_J + 1$. By Lemma 3 there are infinitely many primes q with $q \not\equiv 1 \bmod \ell^{\beta_J+1}$ and q dividing some value of $f_J(n)$. Take

q_J to be one such prime, and choose it to be larger than q_j for all $j < J$, and also to be larger than the discriminant of f_J and the resolvents of f_j and f_J (for all $j \neq J$) so that by Lemma 5 if $q_J | f_J(n)$ then it can divide no other $f_j(n)$. With this choice of q_J, take a_J such that $q_J \| f_J(a_J)$.

Now consider $n \equiv a \bmod \ell^{\beta+1}$ and $n \equiv a_j \bmod q_j$ for all $j \leq s$. Call this progression $A + nQ$ say, with $Q = \ell^{\beta+1} q_1 \cdots q_s$, and put $F_j(n) = f_j(A+nQ)/q_j$. At the prime ℓ, note that $\ell \nmid f_j(a)$; at the prime q_j (ignore if $q_j = 1$) we have $q_j \| f_j(a_j)$ and so $q_j \nmid F_j(n)$; and if $r \neq j$ then the prime q_r (again ignore if $q_r = 1$) cannot divide $F_j(n)$ since q_r divides $f_r(n)$. Thus by Lemma 1 the polynomials F_j are primitive. Since their values are coprime to $k!$ we further have by Lemma 2 that $F_1 \cdots F_s$ is a primitive polynomial with no common prime factor.

Thus we may apply Schinzel's hypothesis to the polynomials F_j and find arbitrarily large n with all $F_j(n)$ being prime. What is the power of ℓ dividing $\phi(\prod_j f_j(A+nQ)^{a_j})$? By construction this is the power of ℓ dividing $\prod_j \phi(q_j)(F_j(n)-1)$.

If $q_j = 1$ then $\beta_j \leq \alpha_j$ and $\ell^{\beta_j} \| (F_j(n)-1)$, so that the power of ℓ dividing $\phi(q_j)(F_j(n)-1)$ is at most α_j. If $q_j > 1$ then $\beta_j \geq \alpha_j + 1$ and both q_j and $F_j(n) = f_j(A+nQ)/q_j$ are primes that are not $1 \bmod \ell^{\alpha_j+1}$ (because $f_j(A+nQ) \equiv 1 \bmod \ell^{\alpha_j+1}$ here), and therefore $\phi(q_j)(F_j(n)-1)$ is divisible at most by $\ell^{2\alpha_j}$.

We conclude that the power of ℓ dividing $\phi(\prod_j f_j(A+nQ)^{a_j})$ is at most $2(\alpha_1 + \ldots + \alpha_s)$, which completes our proof. □

3 Proof of Theorem 1

With the results from Sect. 2 in hand, we can finish the proof of Theorem 1 in a few sentences. Given a primitive polynomial $f = f_1^{a_1} \cdots f_s^{a_s}$, by passing to a progression (as in Lemma 2) we may find a polynomial $F = F_1^{a_1} \cdots F_s^{a_s}$ with $F(n)$ coprime to $k!$ and with $\mathcal{G}(f)$ being a divisor of $\phi(k!)\mathcal{G}(F)$. Further, the fields obtained by adjoining a root of f_j to $\mathbb{Q}$ are the same as the fields obtained by adjoining a root of F_j to $\mathbb{Q}$. Thus, appealing to Lemma 6, we find that $\mathcal{G}(F)$ is a divisor of $r_1^2 \cdots r_s^2$. This completes our proof.

4 Polynomials that split completely: Proof of Theorem 2

We turn to the proof of Theorem 2. If f is primitive and splits completely into linear factors, then

$$f(n) = \prod_{j=1}^{s} (c_j n + d_j)^{a_j}$$

with the c_j non-zero, $(c_j, d_j) = 1$ for all j, and the rationals d_j/c_j distinct. We may suppose that f has positive leading coefficient, and then we can arrange matters such that the c_j are all positive. We require the "square-free kernel" of f, given by

$$g(n) = \prod_{j=1}^{s} (c_j n + d_j).$$

Further we suppose that f is not divisible by primes at most $2k+1$, with k the degree of f. Lemma 2 allows us to do this for the primes $p \leq k$, and for each prime $k+1 \leq p \leq 2k+1$

we may find a residue class a_p mod p such that $c_j a_p + d_j \not\equiv 0 \bmod p$ for all j and then restrict n to the progression a_p mod p.

First let us show that no prime $\ell > 2k + 1$ divides $\mathcal{G}(f)$. By passing to a progression mod ℓ we may suppose that $\ell \nmid f(n)$ for all n. Now ℓ can divide $\phi(f(n))$ if and only if $f(n)$ is divisible by some prime $p \equiv 1 \bmod \ell$. Consider the sifting problem of finding n such that for all primes $p \equiv 1 \bmod \ell$ one has $c_j n \not\equiv -d_j \bmod p$ for all j. This is a sieve of dimension $s/(\ell - 1) < 1/2$, and the sequence to be sifted, with $n \le x$, has level of distribution $x^{1-\epsilon}$, for any $\epsilon > 0$. Sieve theory in dimension below half therefore shows that there are (many) values of n with the desired property (see, for example, [3, Theorem 11.21]).

Now consider a prime $\ell \le 2k + 1$, where we wish to show that the power of ℓ dividing $\mathcal{G}(f)$ is bounded. Let A be a large natural number. Let z be a large parameter, which is considered large in comparison to all the other parameters c_j, d_j, A. Let $P(z)$ denote the product of all primes below z. We seek a lower bound for

$$S(x, z) = \sum_{\substack{n \le x \\ (g(n), P(z))=1}} \left(1 - \sum_{\substack{z<p\le x \\ p\equiv 1 \bmod \ell^A}} \sum_{\substack{j \\ p|c_j n+d_j}} 1 \right). \tag{2}$$

The quantity summed in $S(x, z)$ equals 1 when n is such that $g(n)$ is divisible by no prime below z and by no prime $\equiv 1 \bmod \ell^A$, and is non-positive for other n. Thus a lower bound for $S(x, z)$ with x being a fixed power of z and A a fixed natural number, would produce n for which $g(n)$ has a bounded number of prime factors none of which are 1 mod ℓ^A, which will give our desired conclusion.

We begin our investigation of $S(x, z)$ by estimating the first (positive) term in the definition (2). Let $\varrho(p)$ denote the number of incongruent solutions to $g(n) \equiv 0 \mod p$. For large primes p we then have $\varrho(p) = s$, and hence the product

$$\mathfrak{S} = \prod_p \left(1 - \frac{\varrho(p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-s} \tag{3}$$

converges to a non-zero number. We may now apply the fundamental lemma of sieve theory in dimension s. This tells us that there is a positive real number C such that for all $x \ge z^{9s}$, one has

$$\sum_{\substack{n \le x \\ (g(n), P(z))=1}} 1 \ge C\mathfrak{S}\frac{x}{(\log z)^s},$$

see for example [3, Theorem 11.22]. Note here that $\mathfrak{S}$ depends on g but C does not.

Now we turn to the contribution of the negative terms in the sum defining S. By reasons of symmetry it is enough to think of the case $p|c_1 n + d_1$, say.

Consider first the terms with $z < p \le x/z^{9s}$. In this case, we apply an upper bound sieve, for example again [3, Theorem 11.22]. Then, with $\mathfrak{S}$ as above, we find that contribution is bounded above by

$$C'\mathfrak{S} \sum_{\substack{z<p\le x/z^{9s} \\ p\equiv 1 \bmod \ell^A}} \frac{x}{p(\log z)^s}$$

where again C' is a suitable positive constant that does not depend on g. We choose $x = z^{30s}$. Then, since z is large, the above does not exceed

$$\leq 2C'\mathfrak{S}\frac{x}{(\log z)^s}\frac{1}{\ell^A}\log\frac{\log x/z^{9s}}{\log z} = 2C'\mathfrak{S}\frac{x}{(\log z)^s}\frac{\log(21s)}{\ell^A}.$$

Now consider the contribution of larger values of p. Here we employ the switching principle: write $c_1n + d_1 = rp$, and then sum over r instead. We must have $r \ll z^{9s}$ with r composed only of prime factors above z, and moreover we must have n in a particular residue class mod $r\ell^A$ (since $r|(c_1n+d_1)$ and we must have $(c_1n+d_1)/r \equiv 1 \bmod \ell^A$). Once more we apply the upper bound sieve, replacing the condition that $(c_1n + d_1)/r$ being prime by just the weaker restriction that it is coprime to $P(z)$. Thus the desired contribution is

$$\leq C'\mathfrak{S}\sum_{\substack{r\ll z^{9s}\\ (r,P(z))=1}}\frac{x}{(r\ell^A)(\log z)^s} \leq C''\mathfrak{S}\frac{x}{(\log z)^s}\frac{\log(10s)}{\ell^A}$$

where now C'' is a suitable constant with $C'' \geq C'$.

Combining the two upper bounds with the lower bound, we infer that (recall $x = z^{30s}$)

$$S(z^{30s}, z) \geq \mathfrak{S}\frac{x}{(\log z)^s}\left(C - C''\frac{3s\log(21s)}{\ell^A}\right),$$

We choose A so large that

$$S(z^{30s}, z) \geq \frac{1}{2}C\mathfrak{S}\frac{x}{(\log z)^s}.$$

Thus we have produced many $n \leq z^{30s}$ for which $g(n)$ has no prime factor below z, and no prime factor $\equiv 1 \bmod \ell^A$. Since $g(n) \ll x^s = z^{30s^2}$, it follows that $g(n)$ has at most $31s^2$ prime factors, and none of these prime factors can be $1 \bmod \ell^A$. Thus the power of ℓ dividing $\phi(g(n))$ (which is also the power of ℓ dividing $\phi(f(n))$) is at most $31s^2(A-1)$, so that the exponent of ℓ dividing $\mathcal{G}(f)$ may be bounded in terms of A and k, as claimed.

5 Irreducible quadratic polynomials

Now familiar arguments show that Theorem 3 follows from Theorem 4. Thus it remains to establish the latter, and this is our main task in this section. The basic strategy is similar to that applied in the previous section.

Let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ be a primitive irreducible quadratic polynomial with positive leading coefficient and no fixed prime divisor. Whenever the natural number h is large and the real number δ is small enough, we need to show that there are infintely many n with $f(n)$ coprime to the primes below n^δ, and to all the primes in the progression $1 \bmod h$.

Let $D = b^2 - 4ac$ denote the discriminant of f, and put $H = 2a|D|h$. We fix a progression $\nu \bmod H$ such that $(f(\nu), H) = 1$, and assume that $1 \leq \nu \leq H$. Let x be large, and put $z = x^\delta$ for a suitably small $\delta > 0$; we shall assume that $\delta \leq 1/100$. Put $P^\dagger = \prod_{p\leq z, p\nmid H} p$.

We wish to bound from below

$$S = \sum_{\substack{x \le n \le 2x \\ n \equiv \nu \bmod H \\ (f(n), P^{\dagger})=1}} \left(1 - \sum_{\substack{p \equiv 1 \bmod h \\ z \le p \le f(2x) \\ p | f(n)}} 1 \right). \tag{4}$$

The quantity summed in S equals 1 when n is such that $f(n)$ has no prime factor below $z = x^{\delta}$ and no prime factor $\equiv 1 \bmod h$, and is non-positive for other n. Thus a lower bound for S will guarantee the existence of such n, as needed for Theorem 4. Sieve methods will allow us to obtain such a lower bound provided δ is small enough, and h is large enough.

To aid the reader, we comment on the sizes of the various parameters. The quantity δ is an absolute constant, which must be chosen small in order to make a lower bound sieve work. The parameter h must be chosen large in terms of δ in order for the negative terms in (4) to be smaller than the positive contribution; in our argument we want $h \ge C3^{1/\delta}$ for a positive constant C, but with more effort one only needs $h \ge C/\delta^2$. The parameter x (and therefore $z = x^{\delta}$) is taken to be sufficiently large in terms of h, δ, and the coefficients of the polynomial f.

We start with the positive term in S. An application of the fundamental lemma from sieve theory, for example in the form of [3, Thm. 6.12], shows that

$$\sum_{\substack{n \le x \\ n \equiv \nu \bmod H \\ (f(n), P^{\dagger})=1}} 1 \ge \frac{1}{2} \frac{x}{H} \prod_{\substack{p \le z \\ p \nmid H}} \left(1 - \frac{\varrho(p)}{p} \right),$$

where, for a general modulus r we denote by $\varrho(r)$ the number of solutions to the congruence $f(x) \equiv 0 \bmod r$. Note that $\varrho(r)$ is a multiplicative function, and for a prime $p \nmid H$ (and so in particular $p \nmid 2aD$), it is easy to verify that $\varrho(p^v) = 1 + (\frac{D}{p})$ for all $v \ge 1$ (where $(\frac{D}{\cdot})$ denotes the Kronecker–Legendre symbol, which is a Dirichlet character mod $|D|$). On average $\varrho(p) = 1$, and so for large z we have

$$\prod_{\substack{p \le z \\ p \nmid H}} \left(1 - \frac{\varrho(p)}{p} \right) \sim \frac{e^{-\gamma}}{\log z} \frac{H}{\phi(H)} \prod_{\substack{p \le z \\ p \nmid H}} \left(1 - \frac{\varrho(p)}{p} \right) \left(1 - \frac{1}{p} \right)^{-1}.$$

Thus, with $\mathfrak{S} = \prod_{p \nmid H} (1 - \varrho(p)/p)(1 - 1/p)^{-1} > 0$ the positive term in S exceeds

$$\frac{x}{4\phi(H)} \frac{\mathfrak{S}}{\log z}.$$

It remains to estimate the contributions from negative terms to (4), which we split into three parts depending on the size of p. Divide the primes $z \le p \le f(2x)$ into the three ranges $z \le p \le x/z^9$, $x/z^9 \le p \le xz^9$ and $xz^9 < p \le f(2x)$. Corresponding to these ranges, define

$$S_1 = \sum_{\substack{x \le n \le 2x \\ n \equiv \nu \bmod H \\ (f(n), P^{\dagger})=1}} \sum_{\substack{p \equiv 1 \bmod h \\ z \le p \le xz^{-9} \\ p | f(n)}} 1,$$

similarly define S_2 and S_3. Thus

$$S \geq \frac{1}{4}\frac{\mathfrak{S}}{\log z}\frac{x}{\phi(H)} - S_1 - S_2 - S_3. \tag{5}$$

The range $z \leq p \leq x/z^9$ can be handled by a simple sieve argument (as in the previous section), while the third range $xz^9 \leq p \leq f(2x)$ can be handled similarly after a “switching argument” writing $f(n) = pr$ (so that r is small). The middle range $x/z^9 \leq p \leq xz^9$ is the most difficult part of the argument, and involves the work of Hooley and others on Weyl sums attached to roots of quadratic congruences.

The sum S_1 may be upper bounded as in the previous section. In the current context an upper bound sieve produces

$$S_1 \ll \frac{\mathfrak{S}}{\phi(H)} \sum_{\substack{p\equiv 1 \bmod h \\ z\leq p\leq xz^{-9}}} \frac{x}{p\log z} \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}\frac{\log((1/\delta)-9)}{\phi(h)},$$

so that when h is large enough compared to $1/\delta$ we may conclude that

$$S_1 \leq \frac{1}{20}\frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}.$$

The sum S_3 also accepts treatment following the pattern laid out in the preceding section. If $p|f(n)$ and $p > xz^9$, we put $f(n) = pr$ so that $r \leq f(2x)/p \ll xz^{-9}$ with $r \equiv f(\nu) \bmod h$. Given such a small value of r, the problem then amounts to requiring $f(n)$ to be a multiple of r (which means that n lies in one of $\varrho(r)$ residue classes mod r), and also lying in the residue class $\nu \bmod H$. We separate the case $r = 1$ (which can only occur if $f(\nu) \equiv 1 \bmod h$); the other terms satisfy $r > z$ since r must be coprime to all primes below z. If $r = 1$, then $f(n)$ must be prime and by the upper bound sieve

$$\sum_{\substack{x\leq n\leq 2x \\ f(n)\text{ prime} \\ n\equiv\nu \bmod H}} 1 \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log x}.$$

For the terms $z < r \ll xz^{-9}$, the upper bound sieve gives

$$\sum_{\substack{x\leq n\leq 2x \\ r|f(n) \\ n\equiv\nu \bmod H \\ (f(n),P^\dagger)=1}} 1 \ll \frac{\mathfrak{S}}{\phi(H)}\frac{\rho(r)}{r}\frac{x}{\log z}.$$

Therefore

$$S_3 \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log x} + \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}\sum_{\substack{z<r\ll xz^{-9} \\ r\equiv f(\nu) \bmod h \\ (r,P^\dagger H)=1}} \frac{\varrho(r)}{r}.$$

Since $r \ll xz^{-9}$ and all prime factors of r are larger than $z = x^\delta$, it follows that r has at most $1/\delta$ prime factors and so $\rho(r) \leq 2^{1/\delta}$. It follows that

$$S_3 \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log x} + \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}\sum_{\substack{z<r\ll xz^{-9} \\ r\equiv f(\nu) \bmod h \\ (r,P^\dagger H)=1}} \frac{2^{1/\delta}}{r} \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log x} + \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}\frac{2^{1/\delta}}{\delta\phi(h)}.$$

By choosing δ sufficiently small, and h sufficiently large in terms of δ (for example, making $h \geq C3^{1/\delta}$ for some constant C) we conclude that

$$S_3 \leq \frac{1}{20} \frac{\mathfrak{S}}{\phi(H)} \frac{x}{\log z}.$$

Finally we turn to the sum S_2. As before, we write $n = pr$ with $p \equiv 1 \bmod h$ and $xz^{-9} \leq p \leq xz^9$ so that the complementary variable r satisfies $r \equiv f(\nu) \bmod h$ and $x/z^9 \ll r \ll xz^9$. We sum over r instead of p and exchange the order of summation to see that

$$S_2 \ll \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r, HP^\dagger)=1}} \sum_{\substack{x \leq n \leq 2x \\ n \equiv \nu \bmod H \\ r | f(n) \\ (f(n), P^\dagger)=1}} 1. \tag{6}$$

Anticipating an application of Poisson summation, it is convenient to smooth the sum over n above. For concreteness, let $\Phi : \mathbb{R} \to \mathbb{R}$ be the smooth function defined by $\Phi(0) = 1$ and for $t \neq 0$ by

$$\Phi(t) = \left(\frac{\sin t}{t}\right)^2.$$

Since Φ is always non-negative, and $\Phi(t) \gg 1$ for $1 \leq t \leq 2$, we may bound S_2 by $\ll S_2'$ where

$$S_2' = \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r, H)=1}} \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \nu \bmod H \\ r | f(n) \\ (f(n), P^\dagger)=1}} \Phi\left(\frac{n}{x}\right). \tag{7}$$

We treat the sieving condition $(f(n), P^\dagger) = 1$ by Selberg's upper bound sieve. Put $\theta_1 = 1$ and let θ_d be real numbers with $\theta_d = 0$ unless $d \leq z$ is square-free with $d | P^\dagger$. Write

$$\lambda_d = \sum_{[d_1, d_2]=d} \theta_{d_1} \theta_{d_2}, \tag{8}$$

so that λ_d is non-zero only for d that are square-free divisors of $P^\dagger$ with $d \leq z^2$. With this notation

$$S_2' \leq \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r, H)=1}} \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \nu \bmod H \\ r | f(n)}} \Phi\left(\frac{n}{x}\right) \left(\sum_{d | (P^\dagger, f(n))} \theta_d \right)^2 = \sum_{d | P^\dagger} \lambda_d T(d), \tag{9}$$

where

$$T(d) = \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r, H)=1}} \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \nu \bmod H \\ [r, d] \| f(n)}} \Phi\left(\frac{n}{x}\right). \tag{10}$$

Lemma 7 *With notations as above, uniformly for $d \leq z^2$ with $d | P^\dagger$ we have*

$$T(d) = \frac{x}{H} \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r, H)=1}} \frac{\varrho([d, r])}{[d, r]} + O(x^{63/64} z^{15}).$$

Here the implied constant in the error term may depend upon the polynomial f, and on h and H.

We postpone the proof of this lemma to the next section, and proceed to complete the estimation of S_2.

The next lemma provides an asymptotic formula for the sum over r appearing in Lemma 7.

Lemma 8 *Let D_0 be the fundamental discriminant corresponding to D, so that D/D_0 is a perfect square. If $d \le z^2$ is a divisor of $P^\dagger$ then*

$$\sum_{\substack{xz^{-10}\le r\le xz^{10}\\ r\equiv f(v) \bmod h\\ (r,H)=1}} \frac{\varrho([d,r])}{[d,r]} = (20\log z)\frac{g(d)}{d}\frac{\phi(H)}{H}\prod_{p\nmid H}\left(1+\frac{(\frac{D}{p})}{p}\right)\frac{1}{\phi(h)}\,(1+\delta(D_0|h)) + O(x^{-\frac{1}{8}}z^{10}),$$

where $\delta(D_0|h)$ equals 1 if D_0 divides h, and equals 0 otherwise, and g is a multiplicative function given by

$$g(d) = \varrho(d)\prod_{p|d}\frac{(2p-1)}{(p+1)}.$$

The implied constant in the error term may depend on the polynomial f, and on h and H.

Lemma 8 will be proved in the final section of this paper. Here we continue with the estimation of S_2'. Using Lemmas 7 and 8 in (9) we obtain

$$S_2' \le \sum_{\substack{d|P^\dagger\\ d\le z^2}}\lambda_d T(d) = T(1)\sum_{\substack{d|P^\dagger\\ d\le z^2}}\lambda_d\frac{g(d)}{d} + O\left(x^{\frac{63}{64}}z^{15}\sum_{d\le z^2}|\lambda_d|\right).$$

We follow the familiar procedure of Selberg's sieve to minimize the main term above, which is a quadratic form in the θ_d, subject to the linear constraint $\theta_1 = 1$. As is well known, the optimal θ_d satisfy $|\theta_d| \le 1$ (see [3, (7.9)]) so that $\lambda_d \ll d^\epsilon$ and the error term above may be bounded as $O(x^{99/100})$ provided δ is small enough. As for the main term, note that $g(p) = 0$ if $(\frac{D}{p}) = -1$ and $g(p) = 4 + O(1/p)$ if $(\frac{D}{p}) = 1$, so that the problem corresponds to a sieve of dimension 2. Carrying out the Selberg sieve in this context (see Theorem 7.1 and Proposition 7.3 of [3]) we conclude that (recall x is taken to be sufficiently large when compared to h, $1/\delta$, or the coefficients of f)

$$S_2' \ll T(1)\prod_{\substack{p\le z\\ p\nmid H}}\left(1-\frac{g(p)}{p}\right).$$

After a small calculation, it follows that

$$S_2 \ll S_2' \ll \frac{\mathfrak{S}}{\phi(H)}\frac{x}{\phi(h)\log z}.$$

If h is large enough, we may conclude that

$$S_2 \le \frac{1}{20}\frac{\mathfrak{S}}{\phi(H)}\frac{x}{\log z}.$$

Theorem 4 is now available: we take $\delta > 0$ small and h suitably large in terms of $1/\delta$, so that the estimates of S_1, S_2 and S_3 hold. Then for all sufficiently large z (here large may depend on f) one has

$$S_1 + S_2 + S_3 \leq \frac{3}{20} \frac{\mathfrak{S}}{\phi(H)} \frac{x}{\log z},$$

and we conclude from (5) that $S \gg \mathfrak{S} x (\phi(H) \log z)^{-1}$, as desired.

6 An auxiliary estimate: Proof of Lemma 7

In the definition of $T(d)$, we group terms according to (r, d) which we denote by u. Thus

$$T(d) = \sum_{u|d} \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r,d)=u \\ (r,H)=1}} \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \nu \bmod H \\ r(d/u) | f(n)}} \Phi\left(\frac{n}{x}\right). \tag{11}$$

We now focus on the inner sum over n above. Temporarily, we put $f_\nu(n) = f(\nu + nH)$ so that the inner sum over n in (11) may be written as

$$\sum_{\substack{n \in \mathbb{Z} \\ r(d/u) | f_\nu(n)}} \Phi\left(\frac{\nu + nH}{x}\right) = \sum_{\substack{1 \leq \xi \leq r(d/u) \\ f_\nu(\xi) \equiv 0 \bmod rd/u}} \sum_{\substack{n \in \mathbb{Z} \\ n \equiv \xi \bmod rd/u}} \Phi\left(\frac{\nu + nH}{x}\right). \tag{12}$$

Here we parametrize the inner sum by $n = \xi + r(d/u)m$ and apply the Poisson summation formula to the sum over m. The Fourier transform of Φ is

$$\widehat{\Phi}(t) = \int_{-\infty}^{\infty} \Phi(\alpha) e(-\alpha t)\, \mathrm{d}\alpha = \max(0, 1 - |t|),$$

and we find that

$$\sum_{\substack{n \in \mathbb{Z} \\ n \equiv \xi \bmod rd/u}} \Phi\left(\frac{\nu + nH}{x}\right) = \frac{x}{Hr(d/u)} \sum_{m \in \mathbb{Z}} e\left(\frac{m(\nu + H\xi)}{Hr(d/u)}\right) \widehat{\Phi}\left(\frac{xm}{Hr(d/u)}\right).$$

Inserting this into (12) brings in the sum

$$\varrho_m^{(\nu)}(q) = \sum_{\substack{\xi = 1 \\ f_\nu(\xi) \equiv 0 \bmod q}}^{q} e\left(\frac{m\xi}{q}\right),$$

which has been studied by Hooley [4], Duke, Friedlander and Iwaniec [2] and Toth [7], and we find that

$$T(d) = \frac{x}{H} \sum_{u|d} \frac{u}{d} \sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ r \equiv f(\nu) \bmod h \\ (r,d)=u \\ (r,H)=1}} \frac{1}{r} \sum_{m \in \mathbb{Z}} e\left(\frac{m\nu}{Hr(d/u)}\right) \varrho_m^{(\nu)}(rd/u) \widehat{\Phi}\left(\frac{xm}{Hr(d/u)}\right). \tag{13}$$

Consider first the term $m = 0$ in (13). Note that $(r, H) = 1$ so that $(r, h) = 1$, and since $d | P^\dagger$ we also have $(d, h) = 1$. It follows that $\varrho_0^\nu(rd/u) = \varrho(rd/u) = \varrho([d, r])$, and so the contribution of the $m = 0$ term matches the main term of Lemma 7.

This leaves us with the terms where $m \neq 0$. Since $\widehat{\Phi}(t) = 0$ for $|t| \geq 1$, only terms with $x|m| < Hr(d/u)$ make a non-zero contribution. For such values of m, note that $|m\nu/(Hrd/u)| \leq |\nu|/x \leq H/x$ so that $e(m\nu/(hrd/u)) = 1 + O(H/x)$. Using the trivial estimate $\varrho_m^{(\nu)}(q) \ll q^{\epsilon}$ when considering the contribution arising from the $O(k/x)$, we readily find that the terms with $m \neq 0$ yield

$$\frac{x}{H}\sum_{u|d}\frac{u}{d}\sum_{m\neq 0}\sum_{\substack{xz^{-10}\leq r\leq xz^{10}\\ r\equiv f(\nu) \bmod h\\ (r,d)=u\\ (r,H)=1}}\frac{\varrho_m^{(\nu)}(rd/u)}{r}\widehat{\Phi}\left(\frac{xm}{Hr(d/u)}\right) + O(z^{15}). \tag{14}$$

To bound the sum over r above, we invoke the work of Toth [7] (see also the closely related Proposition 1 in [2]). His formula (16) with $L = 8$, provides the estimate

$$\sum_{R<r\leq 2R}\varrho_m^{(\nu)}(Ar)e\left(\frac{jr}{h}\right) \ll R^{63/64}A^{1/32}.$$

Here the implied constant may depend upon the coefficients of f, h, and ν, but is independent of m in the range where $|m|$ is less than a small power of R. By Möbius inversion we can also impose a coprimality condition on r above, thus obtaining

$$\sum_{\substack{R<r\leq 2R\\ (r,B)=1}}\varrho_m^{(\nu)}(Ar)e\left(\frac{jr}{h}\right) \ll R^{63/64}(AB)^{1/32}.$$

Using the orthogonality of additive characters, we may further restrict r to any given progression mod h:

$$\sum_{\substack{R<r\leq 2R\\ (r,B)=1\\ r\equiv c \bmod h}}\varrho_m^{(\nu)}(Ar) = \frac{1}{h}\sum_{j \bmod h} e\left(-\frac{jc}{h}\right)\sum_{\substack{R<r\leq 2R\\ (r,B)=1}}\varrho_m^{(\nu)}(Ar)e\left(\frac{jr}{h}\right) \ll R^{63/64}(AB)^{1/32}.$$

Using this estimate and partial summation it is easy to see that the quantity in (14) is

$$\ll \frac{x}{H}\sum_{u|d}\frac{u}{d}\sum_{|m|\leq Hz^{12}}(xz^{-10})^{-1/64}(dH)^{1/32} + z^{15} \ll x^{63/64}z^{15},$$

where the implied constant may depend on f and H (and so we have dropped the term $H^{1/32}$). This completes our proof.

7 Quadratic congruences on average: Proof of Lemma 8

If $(\frac{D}{p}) = -1$ for any prime $p|d$, then $\varrho(p) = 0$ and so $\varrho([d, r]) = 0$ for all r. In this case the lemma holds trivially, and henceforth we assume that $(\frac{D}{p}) = 1$ for all primes $p|d$.

Let $d \leq z^2$ be a square-free divisor of $P^{\dagger}$ and let χ be a Dirichlet character mod h. Define

$$F(s; d, \chi) = \sum_{\substack{r=1\\ (r,H)=1}}^{\infty}\frac{\varrho([d, r])\chi(r)}{[d, r]r^s}.$$

Note that $\varrho(q)$ is a multiplicative function of q, and for a prime $p \nmid H$ it is easy to see that $\varrho(p^\ell) = 1 + (\frac{D}{p})$ for all $\ell \geq 1$. Therefore the series defining $F(s; d, \chi)$ converges absolutely in the region $\mathrm{Re}(s) > 0$. Further, a small calculation with Euler products establishes that

$$F(s; d, \chi) = \frac{\varrho(d)}{d} \frac{L(s+1, \chi) L(s+1, \chi(\frac{D}{\cdot}))}{L(2s+2, \chi^2(\frac{D}{\cdot})^2)} F_1(s; \chi) F_2(s; d, \chi), \tag{15}$$

where

$$F_1(s; \chi) = \prod_{p|H} \left(1 - \frac{\chi(p)}{p^{s+1}}\right)^{-1} \left(1 + \frac{\chi(p)(\frac{D}{p})}{p^{s+1}}\right), \tag{16}$$

and

$$F_2(s; d, \chi) = \prod_{p|d} \left(1 + \frac{\chi(p)}{p^s} - \frac{\chi(p)}{p^{s+1}}\right) \left(1 + \frac{\chi(p)(\frac{D}{p})}{p^{s+1}}\right)^{-1}. \tag{17}$$

These expressions furnish a meromorphic continuation of $F(s; d, \chi)$ to the region $\mathrm{Re}(s) > -1/2$, with simple poles at $s = 0$ only in the cases when χ is the principal character mod h, or when $\chi(\frac{D}{\cdot})$ is principal (which can only happen if the fundamental discriminant dividing D is also a divisor of h). Further, using the convexity bound for the Dirichlet L-functions appearing above, in the region $\mathrm{Re}(s) \geq -\frac{1}{4}$ (and away from the potential pole at $s = 0$) we have

$$|F(s; d, \chi)| \ll \frac{\varrho(d)}{d^{\frac{1}{4}}} (1 + |s|)^{\frac{1}{4}}. \tag{18}$$

With these facts in hand, we can proceed with a standard argument in analytic number theory, using a quantitative form of Perron's formula and shifting contours. We begin with Perron's formula

$$\sum_{\substack{xz^{-10} \leq r \leq xz^{10} \\ (r,H)=1}} \frac{\varrho([d, r])}{[d, r]} \chi(r) = \frac{1}{2\pi i} \int_{\mathrm{Re}(s)=1/\log x} F(s; d, \chi) \frac{(xz^{10})^s - (xz^{-10})^s}{s} ds.$$

After truncating the integral at $\mathrm{Im}(s) = \sqrt{x}$, and shifting contours to the line $\mathrm{Re}(s) = -\frac{1}{4}$ and using (18), we obtain that the above equals

$$(20 \log z) \operatorname*{Res}_{s=0} F(s; d, \chi) + O(\varrho(d) x^{-\frac{1}{8}} z^{10}). \tag{19}$$

It remains to calculate the residue of $F(s; d, \chi)$ in cases where a pole occurs (namely, when χ is principal, or when $\chi(\frac{D}{\cdot})$ is principal). When χ is the principal character mod h, a small calculation gives

$$\operatorname*{Res}_{s=0} F(s; d, \chi) = \frac{\varrho(d)}{d} \prod_{p|d} \left(\frac{(2p-1)}{(p+1)}\right) \frac{\phi(H)}{H} \prod_{p \nmid H} \left(1 + \frac{(\frac{D}{p})}{p}\right). \tag{20}$$

When $\chi(\frac{D}{\cdot})$ is the principal character (which is only possible if D_0, the fundamental discriminant corresponding to D, divides h) then a similar calculation shows that the residue of $L(s; d, \chi)$ is exactly the same as the right side above.

We now assemble the observations made above to complete the proof of the lemma. Using the orthogonality of characters mod h we have

$$\sum_{\substack{xz^{-10}\le r\le xz^{10}\\ (r,H)=1\\ r\equiv f(\nu) \bmod h}} \frac{\varrho([d,r])}{[d,r]} = \frac{1}{\phi(h)} \sum_{\chi \bmod h} \overline{\chi}(f(\nu)) \sum_{\substack{xz^{-10}\le r\le xz^{10}\\ (r,H)=1}} \frac{\varrho([d,r])}{[d,r]}\chi(r).$$

From (19) and (20) the above equals

$$(20\log z)\frac{g(d)}{d}\frac{\phi(H)}{H}\prod_{p\nmid H}\left(1+\frac{(\frac{D}{p})}{p}\right)\frac{1}{\phi(h)}\left(1+\delta(D_0|h)\left(\frac{D}{f(\nu)}\right)\right)+O(x^{-\frac{1}{8}}z^{10}).$$

Lastly, note that since $f(\nu)$ is coprime to D, and $4af(\nu) = (2a\nu+b)^2 - D$, one has $(\frac{D}{f(\nu)}) = 1$. The lemma follows.

Acknowledgements We thank the referee for suggestions that led to an improved presentation of our results. The first author is partially supported by grant BR 3048/2 provided by Deutsche Forschungsgemeinschaft. The second author is partially supported by a grant from the National Science Foundation and a Simons Investigator award from the Simons Foundation. This paper was begun while the second author was a Gauss Visiting Professor at Göttingen, supported by the Akademie der Wissenschaften zu Göttingen, and completed while he was a Senior Fellow at the Institute for Theoretical Studies, ETH Zürich. He thanks both institutions for their warm and generous hospitality.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

1. F. Calegari, Prime divisors of polynomials. Blog post available at https://galoisrepresentations.wordpress.com/2016/05/29/prime-divisors-of-polynomials/. Accessed 24 Sept 2019
2. Duke, W., Friedlander, J.B., Iwaniec, H.: Equidistribution of roots of a quadratic congruence to prime moduli. Ann. Math. (2) **141**(2), 423–441 (1995)
3. Friedlander, J., Iwaniec, H.: Opera de cribro. In: American Mathematical Society Colloquium Publications, vol. 57, pp. xx+527. American Mathematical Society, Providence (2010)
4. Hooley, C.: On the number of divisors of a quadratic polynomial. Acta Math. **110**, 97–114 (1963)
5. Serre, J.-P.: Le probleme de groupes de congruence pour SL_2. Ann. Math. **92**, 489–527 (1970)
6. Schinzel, A., Tijdeman, R.: On the equation $y^m = P(x)$. Acta Arith. **31**(2), 199–204 (1976)
7. Tóth, Á.: Roots of quadratic congruences. Int. Math. Res. Not. **14**, 719–739 (2000)
8. Venkataramana, T.N.: On the GCD of an infinite number of integers. In: Number Theory, pp. 155–161, Ramanujan Math. Soc. Lect. Notes Ser., 1. Ramanujan Math. Soc., Mysore (2005)
9. Venkataramana, T.N.: g.c.d. and Euler's totient function. Question on MathOverflow: https://mathoverflow.net/questions/113830/g-c-d-and-eulers-totient-function. Accessed 24 Sept 2019