arXiv:math/9807102v1 [math.NT] 20 Jul 1998

LOWER BOUNDS FOR THE NUMBER OF SMOOTH VALUES OF A POLYNOMIAL

GREG MARTIN

Abstract. We investigate the problem of showing that the values of a given polynomial are smooth (i.e., have no large prime factors) a positive proportion of the time. Although some results exist that bound the number of smooth values of a polynomial from above, a corresponding lower bound of the correct order of magnitude has hitherto been established only in a few special cases. The purpose of this paper is to provide such a lower bound for an arbitrary polynomial. Various generalizations to subsets of the set of values taken by a polynomial are also obtained.

1. Introduction

Our knowledge of the multiplicative properties of the values taken by a polynomial with integer coefficients (or, more generally, an integer-valued polynomial) is quite limited. For instance, it is conjectured that if $h(t)$ is a polynomial that is not identically zero modulo any prime, then the irreducible factors of h will simultaneously take prime values for infinitely many values of n; in fact, there is a conjectured asymptotic formula (see Bateman–Horn [3]) for the number of positive integers $n \le x$ for which this occurs. Dirichlet's theorem on primes in arithmetic progressions verifies this conjecture when h is a linear polynomial, but when h has degree at least 2, these conjectures are still unresolved; it is unknown, for instance, whether there are infinitely many primes of the form n^2+1, or whether there are infinitely many primes p such that $p+2$ is also prime (the twin primes conjecture).

Another multiplicative property of integers is *smoothness*: an integer is y-smooth if none of its prime factors exceed y. Since an integer n is prime if and only if all of its prime factors exceed $n^{1/2}$, smoothness is in some sense the complementary property to being prime. If we define $\Psi(x,y)$ to be the number of y-smooth positive integers not exceeding x, then it is well-known that $\Psi(x, x^{1/u})$ is asymptotic to $\rho(u)x$ for fixed u or for u growing not too quickly with x, where ρ is the solution of a particular differential-difference equation. In particular, for a fixed real number $0<\alpha<1$, the x^α-smooth integers comprise a positive proportion of the integers up to x.

When h is a polynomial of degree 1, we again have an asymptotic formula for the number of integers $n \le x$ for which $h(n)$ is $x^{1/u}$-smooth, which for fixed u and h was first established in the work of Buchstab [4] on smooth numbers in arithmetic progressions (later work has provided results having some uniformity in the coefficients of the linear polynomial; see Hildebrand–Tenenbaum [12, Section 6] for a discussion of such results). Our qualitative understanding of the smooth values of a fixed polynomial h of degree $g \ge 2$ is somewhat better than that of its prime values. Schinzel shows [20, Theorem 13] that

$$\textit{there are infinitely many integers } n \textit{ for which } h(n) \textit{ is } n^{g-1-\delta(g)}\textit{-smooth,} \tag{1}$$

1991 *Mathematics Subject Classification.* 11N32.

where $\delta(g)$ is a certain real number which satisfies $0 < \delta(g) < 1$ and $\delta(g) = 2/g + O(g^{-2})$ for large g; this is a nontrivial result because $h(n)$ has order of magnitude n^g. He also shows [20, Theorem 15] that if h has the special form $h(t) = At^g + B$ for some nonzero integers A, B, and $g \ge 2$, then for any positive real number α there are infinitely many integers n for which $h(n)$ is n^α-smooth. The same conclusion also holds, by work of Balog and Wooley [2] (extending a result of Eggleton and Selfridge [6]), when $h(t) = \prod_{1\le i\le g}(A_i t + B_i)$ is the product of linear polynomials with integer coefficients.

Unfortunately, the proofs of these results do not give very strong estimates for how many smooth values are taken by h. If we define the counting function of the y-smooth values of h,

$$\Psi(h; x, y) = \#\{1 \le n \le x : p \mid h(n) \Rightarrow p \le y\}$$

(where p generically denotes a prime), then presumably, for any fixed polynomial h and positive real number α, we should have $\Psi(h; x, x^\alpha) \sim c(h, \alpha)x$ for some positive constant $c(h, \alpha)$. However, the arguments of Schinzel and Balog–Wooley imply only lower bounds of the form $\Psi(h; x, y) \gg x^\beta$ for rather small values of β.

When h is a linear polynomial, Buchstab's work referred to above gives the asymptotic formula $\Psi(h; x, x^\alpha) \sim \rho(\alpha^{-1})x$, directly extending the formula for $\Psi(x, x^{1/u})$ mentioned earlier. There are a few results of Hmyrova [13, 14] and Timofeev [23] that give upper bounds for $\Psi(h; x, x^\alpha)$ for polynomials of arbitrary degree; however, there has been very little progress towards establishing a lower bound of the presumed order of magnitude,

$$\Psi(h, x, x^\alpha) \gg_{h,\alpha} x, \tag{2}$$

for polynomials of degree at least 2. It is known that the lower bound (2) holds for any $\alpha > 0$ when h has the form $h(t) = At(Bt + C)$, where A, B, and C are integers with $AB > 0$, by work of Balog and Ruzsa [1] (generalizing a result of Hildebrand [10]). It also holds for $\alpha > e^{-1/(g-1)}$ when $h(t) = (t + 1)(t + 2)\dots(t + g)$ for some $g \ge 2$, by work of Hildebrand [11]. The only result along these lines for irreducible polynomials is due to Dartyge [5], who shows that (2) holds for $\alpha > 149/179$ when $h(t) = t^2 + 1$.

We are able to establish a lower bound of the form (2) for an arbitrary polynomial, as indicated in the following theorem.

Theorem 1. *Let $h(t)$ be an integer-valued polynomial (not identically zero), and let g be the largest of the degrees of the irreducible factors of h. Let k be the number of distinct irreducible factors of h of degree g, and let δ be any positive real number less than $(2k+1)^{-1}$. Then when x is sufficiently large, we have*

$$\Psi(h; x, x^{g-\delta}) \gg_{h,\delta} x. \tag{3}$$

In particular, if h is irreducible, then the lower bound (3) holds for any $0 < \delta < 1/3$.

By the definition of g, the values $h(n)$ with $n \le x$ are trivially $O_h(x^g)$-smooth; Theorem 1 asserts that a positive proportion of the values $h(n)$ with $n \le x$ are $x^{g-\delta}$-smooth. One feature of this result is that the amount x^δ that we are able to save from the trivial smoothness parameter does not depend on the polynomial h, but only on the degrees of its irreducible factors.

Our methods can be extended to show the abundance of smooth values $h(n)$ with n restricted to various sets. Our goal is to obtain a lower bound of the correct order of magnitude for the number of y-smooth values $h(n)$, for some non-trivial value of y; it turns

out that we can do this with n restricted in a wide variety of ways. For the purposes of illustration, we state the following theorems.

Theorem 2. *Let $h(t)$, g, k, and δ be as in Theorem 1. For real numbers $x \geq L \geq 2$, define*

$$\Psi(h; x, L, y) = \Psi(h; x, y) - \Psi(h; x - L, y).$$

Then when x is sufficiently large, we have

$$\Psi(h; x, L, x^g L^{-\delta}) \gg_{h,\delta} L. \tag{4}$$

In particular, if h is irreducible, then the lower bound (4) holds for any $0 < \delta < 1/3$.

Thus a positive proportion of the values taken a polynomial on a short interval of length L are nontrivially smooth by a fractional power of L.

Theorem 3. *Let $h(t)$, g, and k be as in Theorem 1. Let $\mathcal{A}$ be any set of integers whose density η exists and is positive, and let δ be any positive real number less than $\eta/(2k+\eta)$. Define*

$$\Psi_{\mathcal{A}}(h; x, y) = \#\{1 \leq n \leq x,\, n \in \mathcal{A} : p \mid h(n) \Rightarrow p \leq y\}.$$

Then when x is sufficiently large, we have

$$\Psi_{\mathcal{A}}(h; x, x^{g-\delta}) \gg_{h,\eta,\delta} x.$$

For example, if h is an irreducible polynomial of degree g, then a positive proportion of the values that h takes on squarefree integers are $x^{g-\delta}$-smooth for any $\delta < 3/(\pi^2+3) = 0.2331\ldots$. A suitably modified theorem can be established for sets of integers whose densities do not exist, one consequence of which is the following: if $\mathcal{A}$ is a set of integers such that there is never an abundance of values $h(a)$, $a \in \mathcal{A}$, that are nontrivially smooth by a power of x (i.e., if $\lim_{x\to\infty} \Psi_{\mathcal{A}}(h; x, x^{g-\varepsilon})/x = 0$ for every $\varepsilon > 0$), then $\mathcal{A}$ must have density 0.

It is worth noting that the proofs of Theorems 1–3 can be extended to the case where h is a polynomial in more than one variable. In fact, one can obtain stronger results, in terms of the admissible ranges of the smoothness parameter, by a more sophisticated treatment of the error terms arising in the application of the sieve in Section 5. For instance, the lower bound (3) holds for δ as large as $1/2 + o(1)$ as the number of variables increases, at least under some hypothesis controlling the singularities of the polynomial. We do not discuss the details herein.

The values that a polynomial takes on prime arguments form a natural arithmetic set, and the question of whether such a set contains infinitely many prime numbers is an important motivating problem of sieve theory. For example, when $h(t) = t+2$, this question is precisely the twin primes conjecture. Analogously, we can ask whether such a set contains many smooth numbers; the following theorem demonstrates that it does.

Theorem 4. *Let $h(t)$, g, and k be as in Theorem 1, and let δ be a positive real number less than $(4k+2)^{-1}$. Define*

$$\Phi(h; x, y) = \#\{1 \leq q \leq x,\, q \text{ prime} : p \mid h(q) \Rightarrow p \leq y\}.$$

Then when x is sufficiently large, we have

$$\Phi(h; x, x^{g-\delta}) \gg_{h,\delta} x/\log x. \tag{5}$$

In particular, if h is irreducible, then the lower bound (5) holds for any $0 < \delta < 1/6$.

Thus a positive proportion of the values a polynomial takes on primes are nontrivially smooth by a power of x. The aforementioned work of Hmyrova contains upper bounds for $\Phi(h;x,y)$ as well as for $\Psi(h;x,y)$, but it was hitherto unknown for nonlinear polynomials h whether $\Phi(h;x,x^{g-\delta})$ even tended to infinity with x for any fixed positive δ. For linear polynomials, Theorem 4 is weaker in terms of the admissible range of δ than existing theorems; for example, Friedlander [7] shows that the lower bound (5) holds for any δ less than $1-1/(2\sqrt{e}) = 0.6967\ldots$ when $h(t)=t+a$ for some nonzero integer a.

Finally, we establish by elementary means a theorem that in some sense interpolates between Theorem 1 and Schinzel's result (1):

Theorem 5. *Let $h(t)$, g, and k be as in Theorem 1. Then when x is sufficiently large, we have $\Psi(h;x,x^{g-1/k}) \gg_h x\log^{-k}x$. In particular, if h is irreducible, then $\Psi(h;x,x^{g-1}) \gg_h x\log^{-1}x$.*

Theorem 5 has a weaker smoothness parameter than (1) but provides a stronger quantitative lower bound, while it has a stronger smoothness parameter than Theorem 1 but a weaker lower bound.

Section 2 of this paper contains the outline of the approach to establishing Theorems 1–3, as well as definitions of much of the notation used throughout the paper. Section 3 examines the multiplicative functions that arise in the course of implementing this plan, while Section 4 addresses the asymptotics of sums of multiplicative functions. Section 5 deals with the sieve-related work and culminates in a proof of Proposition 6 below. Section 6 provides an outline of the modifications to this proof necessary to establish Theorem 4, and Section 7 contains a proof of Theorem 5.

Throughout this paper, we use the usual notation (m,n) and $[m,n]$ for the greatest common divisor and least common multiple, respectively, of m and n; $\mu(n)$ for the Möbius function; $\phi(n)$ for the Euler totient function; $d(n)$ for the number of divisors of n; $\Lambda(n)$ for the von Mangoldt function; and $\omega(n)$ for the number of distinct prime factors of n. We also use the notation $m \mid n$ to mean that m divides n, and $p^r \mid\mid n$ to mean that the prime power p^r exactly divides n, i.e., p^r divides n but p^{r+1} does not. The constants implicit in the O- and $\ll$ symbols in this paper may depend where appropriate on the polynomial under investigation (h, when it denotes a polynomial, or f) and on quantities defined only in terms of that polynomial (e.g., g, k, t_0, and Δ), and also on δ and ε; the same dependencies are allowed when the phrase "sufficiently large" is used.

The author would like to express his appreciation to Michael Bennett, John Friedlander, Hugh Montgomery, Pieter Moree, Carl Pomerance, and especially Trevor Wooley for helpful discussions regarding existing results in this area and preliminary versions of this work. The author would also like to thank Henryk Iwaniec for providing access to some of his unpublished work and Jon Sorenson for providing translations of several of the Russian papers cited herein. The author was supported by a National Science Foundation Graduate Research Fellowship and by National Science Foundation grant DMS 9304580.

2. Outline of the Approach and Notation

Theorems 1–3 will follow from the more quantitative Proposition 6 below. It is convenient to define, for any integer-valued polynomial h, the quantities $C(h;x,y)$ and $C(h;x,L,y)$, the

complements of the quantities $\Psi(h;x,y)$ and $\Psi(h;x,L,y)$:

$$C(h;x,y) = x - \Psi(h;x,y),$$
$$C(h;x,L,y) = L - \Psi(h;x,L,y).$$

Proposition 6. *Let $f(t)$ be an irreducible integer-valued polynomial that is not identically zero modulo any prime. Let $x \geq L \geq 2$ and $0 < \delta < 1/2$ be real numbers, and set $\xi = \max_{n\leq x} |f(n)|$. Then*

$$C(f;x,L,\xi L^{-\delta}) \leq L\Big(\frac{2\delta}{1-\delta} + O(\log^{-1/3} L)\Big).$$

Let us see why Proposition 6 implies Theorem 2 for a general polynomial $h(t)$. First we let m be the largest integer such that h is identically zero (mod m); i.e., m is the greatest common divisor of the values $h(n)$ for $n \in \mathbf{Z}$. If we set $h_1(t) = h(t)/m$, then h_1 is still integer-valued, and furthermore h_1 is not identically zero modulo any prime by the definition of m. Also, as long as y is greater than m, the value $h(n)$ is y-smooth precisely when $h_1(n)$ is y-smooth. Thus it suffices to consider h_1.

Let g be the largest degree of any irreducible factor of h_1 (equivalently, of h), and write

$$h_1(t) = f_1(t)^{r_1} \cdots f_k(t)^{r_k} h_2(t),$$

where the f_i are distinct irreducible polynomials of degree g with integer coefficients and every irreducible factor of h_2 has degree at most $g-1$. Let $\xi_i = \max_{n\leq x} |f_i(n)|$ and $\xi = \max_i \xi_i$, and note that ξ has order of magnitude x^g. The values $h_2(n)$ when $n \leq x$ are always $O(x^{g-1})$-smooth; in particular, given any $0 < \delta < 1$, they are $\xi L^{-\delta}$-smooth for x sufficiently large, since $L \leq x$. Thus $h_1(n)$ fails to be $\xi L^{-\delta}$-smooth precisely when at least one of the $f_i(n)$ is not $\xi L^{-\delta}$-smooth, which implies that

$$C(h_1;x,L,\xi L^{-\delta}) \leq \sum_{i=1}^{k} C(f_i;x,L,\xi L^{-\delta}) \leq \sum_{i=1}^{k} C(f_i;x,L,\xi_i L^{-\delta}). \tag{6}$$

Since h_1 is not identically zero modulo any prime, the same is true of each f_i. This allows us to apply Proposition 6 to each term in the latter sum in the inequality (6), which becomes

$$C(h_1;x,L,\xi L^{-\delta}) \leq kL\Big(\frac{2\delta}{1-\delta} + O(\log^{-1/3} L)\Big). \tag{7}$$

Therefore $\Psi(h_1;x,L,\xi L^{-\delta}) = L - C(h_1;x,L,\xi L^{-\delta}) \gg L$ whenever $\delta < (1+2k)^{-1}$, which is the assertion of Theorem 2, aside from the minor difference between ξ and x^g which can be accommodated by a very small change in δ.

Theorem 3 follows from the inequality (7), with $L = x$, whenever δ is small enough that $2\delta k/(1-\delta)$ is less than the density η of $\mathcal{A}$, which is equivalent to the condition that $\delta < \eta/(2k+\eta)$. Theorem 1 certainly follows from Proposition 6 as well, since it is the special case of Theorem 2 with $L = x$, or a special case of Theorem 3 with $\eta = 1$.

It is worth remarking that when $g = 1$, Proposition 6 is a result about smooth integers in short intervals or short arithmetic progressions. For the purposes of illustration, we take $h(t)$ to be simply t, and put $L = x^\beta$ for some $0 < \beta < 1$ and $\delta = (1-\alpha)/\beta$ for some $1 - \beta/2 < \alpha < 1$, so that $0 < \delta < 1/2$ and $\xi L^{-\delta} = x^\alpha$. Proposition 6 then gives us

$$\Psi(x,x^\alpha) - \Psi(x - x^\beta, x^\alpha) \geq \Big(\frac{\beta - 3(1-\alpha)}{\beta - (1-\alpha)} + o(1)\Big)x^\beta, \tag{8}$$

which is nontrivial in the range $\alpha+\beta/3>1$. Existing results give nontrivial lower bounds for $\Psi(x,x^\alpha)-\Psi(x-x^\beta,x^\alpha)$ for larger ranges of α and β (see for instance Friedlander–Lagarias [8, Theorem 2.4]), so the lower bound (8) is not qualitatively new, although the constant on the right-hand side seems to be an improvement over existing results for certain values of α and β. Although Proposition 6 also gives an explicit lower bound for the number of smooth integers in a short interval from a fixed arithmetic progression, the methods in [8] and similar papers can surely be applied to this situation as well.

One can show that the values of f are often free of small prime factors by using a lower bound sieve to sieve out those values that are multiples of small primes; however, this approach has no chance of showing that the values of f are often smooth if the degree of f is at least 2. One would have to sieve by $\gg x^g$ primes, necessitating a sum of $\gg x^g$ error terms. The most optimistic hope would be that the individual error terms were uniformly bounded and that we could obtain square-root cancellation in the sum of the error terms, and even this would result in an error whose magnitude would be $\gg x^{g/2}$, which would swamp the main term. Instead, we will establish Proposition 6 by bounding from above the number of values of f that are divisible by a prime greater than $\xi L^{-\delta}$; broadly speaking, we will accomplish this by grouping these values by their cofactors, the remainders when the large prime divisors are removed from the values (equation (39) below contains an example of this grouping), and using an upper bound sieve.

3. Multiplicative Functions Associated to a Polynomial

Let f be an irreducible integer-valued polynomial that is not identically zero modulo any prime, as in the statement of Proposition 6. We define $\sigma(h)$ to be the number of solutions of $f(x)\equiv 0 \pmod h$. It is easily seen, by the Chinese remainder theorem and the assumption that f is not identically zero modulo any prime, that σ is a multiplicative function satisfying $0\le\sigma(h)<h$. We also have a bound on $\sigma(h)$ in terms of the degree g and the discriminant Δ of f. Write $\Delta=\prod_p p^{\nu(p)}$, where all but finitely many of the $\nu(p)$ are zero (the discriminant Δ itself is nonzero because f is irreducible). Huxley [15] gives a bound for σ that implies

$$\sigma(p^r)\le g p^{\nu(p)/2} \tag{9}$$

for any prime power p^r (this estimate is improved by Stewart [21], though it will suffice for our purposes as stated). From the bound (9) it follows that $\sigma(h)\le g^{\omega(h)}\Delta^{1/2}\ll g^{\omega(h)}\ll h^\varepsilon$ for any $\varepsilon>0$, since the implicit constants may depend on f and ε.

It is well-known that $\sigma(p)$ is equal to 1 on average, since f is irreducible; in fact, Nagel [18] showed that, for any polynomial $H(t)$ with integer coefficients and with $\sigma(H;p)$ roots $\pmod p$ for each prime p, the asymptotic formula

$$\sum_{p<w}\frac{\sigma(H;p)\log p}{p}=\kappa(H)\log w+O_H(1) \tag{10}$$

holds for all $w\ge 2$, where $\kappa(H)$ is the number of irreducible factors of H. This readily implies that

$$\prod_{w_1\le p<w_2}\Big(1-\frac{\sigma(p)}{p}\Big)^{-1}=\Big(\frac{\log w_2}{\log w_1}\Big)\Big(1+O\Big(\frac{1}{\log w_1}\Big)\Big) \tag{11}$$

for all $2 \le w_1 \le w_2$, or equivalently (by Mertens' formula)

$$\prod_{p<w}\Big(1-\frac{\sigma(p)}{p}\Big)^{-1} = e^{\gamma}\log w\Big(1+O\Big(\frac{1}{\log w}\Big)\Big)\prod_{p}\Big(1-\frac{\sigma(p)}{p}\Big)^{-1}\Big(1-\frac{1}{p}\Big) \tag{12}$$

for all $w \ge 2$, where γ is Euler's constant.

We also define a multiplicative function $\sigma^*(h)$ by stipulating that on prime powers p^r, we have

$$\sigma^*(p^r) = \sigma(p^r) - \frac{\sigma(p^{r+1})}{p}. \tag{13}$$

We remark that $\sigma(p^{r+1})$ counts the number of roots of $f \pmod{p^{r+1}}$, each of which corresponds to a root of $f \pmod{p^r}$ simply by reducing $\pmod{p^r}$. Moreover, this correspondence is at most p-to-1, i.e., $\sigma(p^{r+1}) \le p\sigma(p^r)$. Consequently, σ^* is a nonnegative function. Since $\sigma^*(p^r)$ obviously does not exceed $\sigma(p^r)$ for any prime power p^r, we have that $0 \le \sigma^*(h) \le \sigma(h)$ for any h.

We also note that $\sigma^*(h) = 0$ if and only if there is a prime p dividing h such that $\sigma(ph) = p\sigma(h)$, by the multiplicativity of σ and σ^*. This is equivalent to saying that there is a prime p such that every integer that is a root of $f \pmod{h}$ is also a root of $f \pmod{ph}$; such a prime must necessarily divide h, by the multiplicativity of σ and the assumption that f is not identically zero modulo any prime.

Expressions of the form $\sigma(nh)/\sigma(h)$ will arise later in connection with σ^*, and we will need to know that such expressions are multiplicative in the variable n. This is a general property of multiplicative functions which we establish in the following lemma.

Lemma 7. *If $g(n)$ is a multiplicative function, then for any fixed number h satisfying $g(h) \ne 0$, the function $g(nh)/g(h)$ is also a multiplicative function of n.*

Proof: It is easily seen that a multiplicative function g satisfies $g(m)g(n) = g([m,n])g((m,n))$ for any numbers m and n, by writing all four arguments as products of prime powers. This implies that if n_1 and n_2 are relatively prime, we have

$$\frac{g(n_1h)}{g(h)}\frac{g(n_2h)}{g(h)} = \frac{g([n_1h,n_2h])g((n_1h,n_2h))}{g(h)^2} = \frac{g(n_1n_2h)g(h)}{g(h)^2} = \frac{g(n_1n_2h)}{g(h)},$$

which establishes the lemma. □

We will also need the following upper bound when we apply the sieve in Section 5.

Lemma 8. *For any positive integer h such that $\sigma^*(h) > 0$, and for any real numbers $2 \le w_1 \le w_2$, we have*

$$\prod_{w_1<p\le w_2}\Big(1-\frac{\sigma(ph)}{p\sigma(h)}\Big)^{-1} \le \Big(\frac{\log w_2}{\log w_1}\Big)\Big(1+O\Big(\frac{1}{\log w_1}\Big)\Big),$$

where the implicit constant does not depend on h.

Proof: We recall that $\sigma^*(h) \le \sigma(h)$, so that the assumption that $\sigma^*(h)$ is positive implies that $\sigma(h)$ is also positive. If a prime p does not divide h, then $\sigma(ph) = \sigma(p)\sigma(h)$ by the multiplicativity of σ. If p divides h but does not divide the discriminant Δ of f, then

every root b of $f \pmod h$ must satisfy $f'(b) \not\equiv 0 \pmod p$. In this case, every root b of $f \pmod h$ corresponds to exactly one root of $f \pmod{ph}$ by Hensel's Lemma, and in particular, $\sigma(ph) = \sigma(h)$ in this case. Therefore we can write

$$\prod_{w_1<p\le w_2}\Big(1-\frac{\sigma(ph)}{p\sigma(h)}\Big)^{-1} = \prod_{w_1<p\le w_2}\Big(1-\frac{\sigma(p)}{p}\Big)^{-1}\prod_{\substack{w_1<p\le w_2\\ p\mid h,\, p\nmid\Delta}}\Big(1-\frac{\sigma(p)}{p}\Big)\Big(1-\frac{1}{p}\Big)^{-1}$$
$$\times\prod_{\substack{w_1<p\le w_2\\ p\mid h,\, p\mid\Delta}}\Big(1-\frac{\sigma(p)}{p}\Big)\Big(1-\frac{\sigma(ph)}{p\sigma(h)}\Big)^{-1}. \quad (14)$$

Equation (11) gives an asymptotic formula for the first product in this equation. Each term in the second product is at most 1, since the fact that $\sigma(h) > 0$ certainly implies that f has at least one root $\pmod p$ for every prime p dividing h, so that $\sigma(p) \ge 1$ for the primes in the second product of equation (14). Finally, the third product can be bounded above by

$$\prod_{\substack{w_1<p\le w_2\\ p^r\|h,\, p\mid\Delta}}\Big(1-\frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big)^{-1}$$

by the fact that σ is nonnegative and multiplicative. Furthermore, since $\sigma^*(h) > 0$ is equivalent to the condition that $\sigma(p^{r+1}) < p\sigma(p^r)$ for every prime power p^r exactly dividing h, this product can in turn be bounded by

$$\prod_{\substack{p>w_1\\ p\mid\Delta}}\max_{\substack{r\ge0\\ \sigma(p^{r+1})<p\sigma(p^r)}}\Big(1-\frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big)^{-1} \le \prod_{\substack{p>w_1\\ p\mid\Delta}}\max_{r\ge0} p\sigma(p^r) \le \prod_{\substack{p>w_1\\ p\mid\Delta}} gp^{1+\nu(p)/2}$$

by the upper bound (9).

Equation (14) now becomes

$$\prod_{w_1<p\le w_2}\Big(1-\frac{\sigma(ph)}{p\sigma(h)}\Big) \le \Big(\frac{\log w_2}{\log w_1}\Big)\Big(1+O\Big(\frac{1}{\log w_1}\Big)\Big)\prod_{\substack{p>w_1\\ p\mid\Delta}} gp^{1+\nu(p)/2}.$$

This last product is bounded above independently of h, and it has the value 1 as soon as w_1 exceeds Δ. Therefore its contribution can be absorbed into the implicit constant in the error term. This establishes the lemma. □

4. Sums of Multiplicative Functions

Our primary goal for this section is to establish an asymptotic formula for a summatory function $M_g(x)$ associated with a multiplicative function $g(n)$, defined by

$$M_g(x) = \sum_{n\le x}\frac{g(n)}{n}.$$

We are interested in an asymptotic formula for $M_g(x)$ when $g(p)$ is constant on average over primes, as is usually the case for the multiplicative functions that arise in sieve problems. Specifically, we impose the condition that there is a constant $\kappa = \kappa(g)$ such that

$$\sum_{p\le x}\frac{g(p)\log p}{p} = \kappa\log x + O_g(1) \quad (15)$$

for all $x \geq 2$.

Although the ideas used in establishing the following proposition have been part of the "folklore" for some time, the literature does not seem to contain a result in precisely this form. Wirsing's pioneering work [24], for instance, requires g to be a nonnegative function and implies an asymptotic formula for $M_g(x)$ without a quantitative error term; while Halberstam and Richert [9, Lemma 5.4] give an analogous result with a quantitative error term, but one that requires g to be supported on squarefree integers in addition to being nonnegative. Both results are slightly too restrictive for our purposes as stated.

Consequently we provide a self-contained proof of an asymptotic formula for $M_g(x)$ with a quantitative error term, for multiplicative functions g that are not necessarily supported on squarefree integers. The proof below, which is based on unpublished work of Iwaniec (used with his kind permission) that stems from ideas of Wirsing and Chebyshev, has the advantage that g is freed from the requirement of being nonnegative. We state the result in a more general form than is required for our present purposes, with a mind towards other applications and because the proof is exactly the same in the more general setting.

Proposition 9. *Suppose that $g(n)$ is a complex-valued multiplicative function such that the asymptotic formula* (15) *holds for some complex number $\kappa = \xi + i\eta$ satisfying $\eta^2 < 2\xi + 1$ (so that $\xi > -1/2$ in particular). Suppose also that*

$$\sum_p \frac{|g(p)| \log p}{p} \sum_{r=1}^{\infty} \frac{|g(p^r)|}{p^r} + \sum_p \sum_{r=2}^{\infty} \frac{|g(p^r)| \log p^r}{p^r} < \infty, \tag{16}$$

and that there exists a nonnegative real number $\beta = \beta(g) < \xi + 1$ such that

$$\prod_{p \leq x} \Big(1 + \frac{|g(p)|}{p}\Big) \ll_g \log^{\beta} x \tag{17}$$

for all $x \geq 2$. Then the asymptotic formula

$$M_g(x) = c(g) \log^{\kappa} x + O_g((\log x)^{\beta - 1}) \tag{18}$$

holds for all $x \geq 2$, where $\log^{\kappa} x$ denotes the principal branch of t^{κ}, and $c(g)$ is defined by the convergent product

$$c(g) = \Gamma(\kappa + 1)^{-1} \prod_p \Big(1 - \frac{1}{p}\Big)^{\kappa} \Big(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\Big). \tag{19}$$

We remark that the condition (17) cannot hold with any $\beta < |\kappa|$ if g satisfies the asymptotic formula (15). The necessity that β be less than $\xi + 1$, so that the formula (18) is truly an asymptotic formula, requires us to consider only those κ for which $|\kappa| < \xi + 1$; this is the source of the condition $\eta^2 < 2\xi + 1$ on κ.

The conditions (16) and (17) are usually very easily verified in practice. For example, the condition (16) automatically holds if there is a constant $\alpha < 1/2$ such that $g(n) \ll n^{\alpha}$; and if g is in fact a nonnegative function (so that, in particular, κ is nonnegative), then the condition (17), with $\beta = \kappa$, follows from the asymptotic formula (15). We also remark that from equation (18), it follows easily by partial summation that

$$\sum_{n < x} g(n) \ll_g x \log^{\beta - 1} x \tag{20}$$

under the hypotheses of the proposition.

Proof: All of the constants implicit in the O- and $\ll$ symbols in this proof may depend on the multiplicative function g, and thus on κ and β as well. We begin by examining an analogue of $M_g(x)$ weighted by a logarithmic factor. We have

$$\begin{aligned}\sum_{n\le x}\frac{g(n)\log n}{n} &= \sum_{n\le x}\frac{g(n)}{n}\sum_{p^r\|n}\log p^r \\ &= \sum_{r=1}^{\infty}\sum_{p\le x^{1/r}}\frac{g(p^r)\log p^r}{p^r}\sum_{\substack{m\le x/p^r\\ p\nmid m}}\frac{g(m)}{m} \\ &= \sum_{p\le x}\frac{g(p)\log p}{p}\sum_{m\le x/p}\frac{g(m)}{m} - \sum_{p\le x}\frac{g(p)\log p}{p}\sum_{\substack{m\le x/p\\ p\mid m}}\frac{g(m)}{m} \qquad (21)\\ &\qquad + \sum_{r=2}^{\infty}\sum_{p\le x^{1/r}}\frac{g(p^r)\log p^r}{p^r}\sum_{\substack{m\le x/p^r\\ p\nmid m}}\frac{g(m)}{m} \\ &= \Sigma_1 - \Sigma_2 + \Sigma_3,\end{aligned}$$

say. If we define the function $\delta(x)$ by

$$\delta(x) = \sum_{p\le x}\frac{g(p)\log p}{p} - \kappa\log x, \qquad (22)$$

then Σ_1 becomes

$$\Sigma_1 = \sum_{m\le x}\frac{g(m)}{m}\sum_{p\le x/m}\frac{g(p)\log p}{p} = \kappa\sum_{m\le x}\frac{g(m)}{m}\log\frac{x}{m} + \sum_{m\le x}\frac{g(m)}{m}\delta\Big(\frac{x}{m}\Big). \qquad (23)$$

Since $M_g(x) = 1$ for $1 \le x < 2$ and

$$M_g(x)\log x - \sum_{m\le x}\frac{g(m)\log m}{m} = \sum_{m\le x}\frac{g(m)}{m}\log\frac{x}{m} = \int_1^x M_g(t)\frac{dt}{t}$$

by partial summation, we can rewrite equation (21) using equation (23) as

$$M_g(x)\log x - (\kappa+1)\int_2^x M_g(t)t^{-1}dt = E_g(x), \qquad (24)$$

where we have defined

$$E_g(x) = (\kappa+1)\log 2 + \sum_{m\le x}\frac{g(m)}{m}\delta\Big(\frac{x}{m}\Big) - \Sigma_2 + \Sigma_3. \qquad (25)$$

We integrate both sides of equation (24) against $x^{-1}(\log x)^{-\kappa-2}$, obtaining

$$\int_2^x M_g(u)u^{-1}(\log u)^{-\kappa-1}du - (\kappa+1)\int_2^x u^{-1}(\log u)^{-\kappa-2}\int_2^u M_g(t)t^{-1}dt\,du = \int_2^x E_g(u)u^{-1}(\log u)^{-\kappa-2}du. \qquad (26)$$

Some cancellation can be obtained on the left-hand side by switching the order of integration in the double integral and evaluating the new inner integral; equation (26) becomes simply

$$(\log x)^{-\kappa-1}\int_2^x M_g(u)u^{-1}du = \int_2^x E_g(u)u^{-1}(\log u)^{-\kappa-2}du.$$

We can substitute this into equation (24), divide by $\log x$, and rearrange terms to get

$$M_g(x) = (\kappa+1)\log^\kappa x \int_2^x E_g(u)u^{-1}(\log u)^{-\kappa-2}du + E_g(x)\log^{-1} x. \tag{27}$$

An upper bound for $E_g(x)$ is now needed. Since $\delta(x)$ is bounded from its definition (22) and the asymptotic formula (15), we have

$$\sum_{m\le x} \frac{g(m)}{m}\delta\Big(\frac{x}{m}\Big) \ll \sum_{m\le x}\frac{|g(m)|}{m}. \tag{28}$$

We also have

$$\sum_{m\le x}\frac{|g(m)|}{m} \le \prod_{p\le x}\left(1+\sum_{r=1}^\infty \frac{|g(p^r)|}{p^r}\right) \le \prod_{p\le x}\Big(1+\frac{|g(p)|}{p}\Big)\prod_{p\le x}\left(1+\sum_{r=2}^\infty\frac{|g(p^r)|}{p^r}\right). \tag{29}$$

Because the sum $\sum_p\sum_{r=2}^\infty |g(p^r)|/p^r$ converges by the hypothesis (16), the last product in equation (29) is bounded as x tends to infinity. Therefore the hypothesis (17) implies that

$$\sum_{m\le x}\frac{|g(m)|}{m} \ll \log^\beta x. \tag{30}$$

The terms Σ_2 and Σ_3 can be estimated by

$$\Sigma_2 = \sum_{p\le x}\frac{g(p)\log p}{p}\sum_{r=1}^\infty\frac{g(p^r)}{p^r}\sum_{\substack{l\le x/p^{r+1}\\ p\nmid l}}\frac{g(l)}{l} \ll \sum_{p\le x}\frac{|g(p)|\log p}{p}\sum_{r=1}^\infty\frac{|g(p^r)|}{p^r}\sum_{l\le x}\frac{|g(l)|}{l}$$

and

$$\Sigma_3 \ll \sum_{p\le x}\sum_{r=2}^\infty\frac{|g(p^r)|\log p^r}{p^r}\sum_{m\le x}\frac{|g(m)|}{m},$$

and so both Σ_2 and Σ_3 are $\ll \log^\beta x$ by the estimate (30) and the hypothesis (16). Therefore, by the definition (25) of $E_g(x)$, we see that

$$E_g(x) \ll \log^\beta x. \tag{31}$$

In particular, since $\beta < \xi+1$, we have

$$\int_x^\infty E_g(u)u^{-1}(\log u)^{-\kappa-2}du \ll \int_x^\infty u^{-1}(\log u)^{\beta-\xi-2}du \ll (\log x)^{\beta-\xi-1}, \tag{32}$$

and so equation (27) and the bound (31) give us the asymptotic formula

$$M_g(x) = c(g)\log^\kappa x + O((\log x)^{\beta-1}) \tag{33}$$

for $x\ge 2$, where

$$c(g) = (\kappa+1)\int_2^\infty E_g(u)u^{-1}(\log u)^{-\kappa-2}du. \tag{34}$$

To complete the proof of the proposition, we need to show that $c(g)$ can be written in the form given by (19); we accomplish this indirectly, using the asymptotic formula (33). Consider the zeta-function $\zeta_g(s)$ formed from g, defined by

$$\zeta_g(s) = \sum_{n=1}^\infty \frac{g(n)}{n^s}.$$

From the estimate (30) and partial summation, we see that $\zeta_g(s)$ converges absolutely for $s > 1$ (we will only need to consider real values of s), and thus has an Euler product representation

$$\zeta_g(s) = \prod_p \Big(1 + \frac{g(p)}{p^s} + \frac{g(p^2)}{p^{2s}} + \cdots\Big) \tag{35}$$

for $s > 1$.

We can also use partial summation to write

$$\zeta_g(s+1) = s\int_1^\infty M_g(t)t^{-s-1}dt \tag{36}$$

for $s > 0$. Since $M_g(x) = 1$ for $1 \le x < 2$, it is certainly true that

$$M_g(x) = c(g)\log^\kappa x + O(1 + \log^\xi x)$$

in that range; using this together with the asymptotic formula (33), equation (36) becomes

$$\begin{aligned}\zeta_g(s+1) = s\int_1^\infty c(g)\log^\kappa t\cdot t^{-s-1}dt \\ + O\bigg(s\int_1^2 (1+\log^\xi t)t^{-s-1}dt + s\int_2^\infty (\log t)^{\beta-1}t^{-s-1}dt\bigg),\end{aligned}$$

valid uniformly for $s > 0$. Making the change of variables $t = e^{u/s}$ in all three integrals and multiplying through by s^κ yields

$$\begin{aligned}s^\kappa\zeta_g(s+1) &= c(g)\int_0^\infty u^\kappa e^{-u}du + O\bigg(\int_0^{s\log 2}(s^\xi + u^\xi)e^{-u}du + s^{\xi-\beta+1}\int_{s\log 2}^\infty u^{\beta-1}e^{-u}du\bigg) \\ &= c(g)\Gamma(\kappa+1) + O(s^{\xi-\beta+1}\log s^{-1})\end{aligned} \tag{37}$$

as $s \to 0^+$, where the exponent $\xi - \beta + 1$ is positive and at most 1 (since $\beta \ge |\kappa| \ge \xi$). Because the Riemann ζ-function satisfies $s\zeta(s+1) = 1 + O(s)$ as $s \to 0^+$, equation (37) implies

$$\zeta(s+1)^{-\kappa}\zeta_g(s+1) = c(g)\Gamma(\kappa+1) + O(s^{\xi-\beta+1}\log s^{-1}). \tag{38}$$

On the other hand, from equation (35) we certainly have the Euler product representation

$$\zeta(s+1)^{-\kappa}\zeta_g(s+1) = \prod_p \Big(1 - \frac{1}{p^{s+1}}\Big)^\kappa\Big(1 + \frac{g(p)}{p^{s+1}} + \frac{g(p^2)}{p^{2(s+1)}} + \cdots\Big)$$

for $s > 0$, and one can show that in fact this Euler product converges uniformly for $s \ge 0$. The important contribution comes from the sum $\sum_p (g(p) - \kappa)/p^{s+1}$, and we see from the hypothesis (15) and partial summation that

$$\sum_{p>x}\frac{g(p)-\kappa}{p^{s+1}} \ll \frac{1}{x^s\log x}$$

uniformly for $s \ge 0$ and $x \ge 2$. The remaining contributions can be controlled using the hypothesis (16).

Consequently, taking the limit of both sides of equation (38) as $s \to 0^+$ gives us

$$\prod_p \Big(1 - \frac{1}{p}\Big)^\kappa\Big(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\Big) = c(g)\Gamma(\kappa+1)$$

(where we have just shown that the product on the left-hand side converges), which is equivalent to (19). This establishes the proposition. □

The following proposition gives a similar asymptotic formula for the restricted sum

$$M_g(x,q) = \sum_{\substack{n\le x\\(n,q)=1}} \frac{g(n)}{n}.$$

Although we will not need such a formula in this paper, results of this type have widespread applicability, and so we include it also with a mind towards other applications.

Proposition 10. *Suppose that $g(n)$ satisfies the hypotheses of Proposition 9. Then the asymptotic formula*

$$M_g(x,q) = c_q(g)\log^\kappa x + O_g(\delta(q)(\log x)^{\beta-1})$$

holds uniformly for all $x \ge 2$ and all nonzero integers q, where

$$c_q(g) = \Gamma(\kappa+1)^{-1}\Big(\frac{\phi(q)}{q}\Big)^\kappa \prod_{p\nmid q}\Big(1-\frac{1}{p}\Big)^\kappa\Big(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\cdots\Big)$$

and $\delta(q) = 1 + \sum_{p|q}|g(p)|\,(\log p)/p$.

We remark that we can also write

$$c_q(g) = c(q)\prod_{p|q}\Big(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\cdots\Big)^{-1},$$

as long as no term $(1+g(p)/p+g(p^2)/p^2+\cdots)$ sums to zero.

Proof: We would like to apply Proposition 9 to the multiplicative function $g_q(n)$ defined by

$$g_q(n) = \begin{cases} g(n), & \text{if } (n,q)=1,\\ 0, & \text{if } (n,q)>1.\end{cases}$$

Certainly $|g_q(n)| \le |g(n)|$, and so the estimates (16) and (17) for g_q follow from the same estimates for g. We also have

$$\begin{aligned}\sum_{p\le x}\frac{g_q(p)\log p}{p} = \sum_{\substack{p\le x\\p\nmid q}}\frac{g(p)\log p}{p} &= \sum_{p\le x}\frac{g(p)\log p}{p} - \sum_{\substack{p\le x\\p|q}}\frac{g(p)\log p}{p}\\ &= \kappa\log x + O_g(1) + O\Big(\sum_{p|q}\frac{|g(p)|\log p}{p}\Big)\end{aligned}$$

from the assumption that g satisfies equation (15). Therefore g_q satisfies equation (15) as well, with the error term being $\ll_g \delta(q)$ uniformly in x.

If we keep this dependence on q explicit throughout the proof of Proposition 9, the only modification necessary is to include a factor of $\delta(q)$ on the right-hand sides of the estimates (28), (31), and (32) and in the error term in equation (33). Therefore, the application of Proposition 9 to g_q yields

$$M_g(x,q) = M_{g_q}(x) = c(g_q)\log^\kappa x + O_g(\delta(q)(\log x)^{\beta-1}),$$

where the implicit constant is independent of q. Because

$$\begin{aligned} c(g_q) &= \Gamma(\kappa+1)^{-1}\prod_p \Big(1-\frac{1}{p}\Big)^{\kappa}\Big(1+\frac{g_q(p)}{p}+\frac{g_q(p^2)}{p^2}+\cdots\Big) \\ &= \Gamma(\kappa+1)^{-1}\prod_{p\mid q} \Big(1-\frac{1}{p}\Big)^{\kappa}\prod_{p\nmid q} \Big(1-\frac{1}{p}\Big)^{\kappa}\Big(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\cdots\Big) = c_q(g), \end{aligned}$$

the proposition is established. □

5. Application of the Upper Bound Sieve

In this section we reformulate Proposition 6 in a way that makes it amenable to treatment by sieve techniques. As in the statement of Proposition 6, we let $x \ge L \ge 2$ and $0 < \delta < 1/2$ be real numbers. We can multiply f by -1 if necessary to make the leading coefficient positive without affecting the smoothness of the values; and we can replace $f(t)$ by $f(t+t_0)$ for any fixed t_0 depending on f, since this only changes $C(f;x,L,\xi L^{-\delta})$ by $O(1)$. Thus we may assume without loss of generality that $f(n)$ is positive when n is positive.

Put $\xi = \max_{x-L<n\le x} f(n)$, and notice that $L^\delta < \xi^{1/2} < \xi L^{-\delta}$ when x is sufficiently large, since $\xi \gg x^g \ge x$ and $\delta < 1/2$. Letting p denote only primes, we have

$$\begin{aligned} C(f;x,L,\xi L^{-\delta}) &= \#\{x-L<n\le x : \exists p > \xi L^{-\delta} \text{ such that } p \mid f(n)\} \\ &= \#\{(n,p,h) : x-L<n\le x,\ p>\xi L^{-\delta},\ f(n)=ph\} \\ &= \sum_{h\ge 1} \#\{(n,p) : x-L<n\le x,\ p>\xi L^{-\delta},\ f(n)=ph\}. \end{aligned} \tag{39}$$

(The integer h plays the role of the cofactor mentioned at the end of Section 2.)

It is clear that h must not exceed L^δ if it is to contribute to this sum. Moreover, we claim that only those h for which $\sigma^*(h) > 0$ contribute to the sum. If $\sigma^*(h) = 0$, then by the remarks following the definition (13) of σ^*, there is a prime q dividing h such that whenever $f(n)$ is divisible by h, it is also the case that $f(n)/h$ is divisible by q. But $q \le h < L^\delta < \xi L^{-\delta}$, and so there are no pairs (n,p) satisfying the description on the last line of equation (39). We may therefore write

$$C(f;x,L,\xi L^{-\delta}) = \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \#\{(n,p) : x-L<n\le x,\ p>\xi L^{-\delta},\ f(n)=ph\}. \tag{40}$$

We remark that the purpose of insisting on this addition condition is to facilitate the passage from equation (51) to equation (52) in the proof of Lemma 11 below. If we retained those terms for which $\sigma^*(h) = 0$, a formal use of an upper bound sieve and a mean value theorem for multiplicative functions would result in infinite products containing local factors equaling zero and infinity (respectively). However, these factors would formally cancel at the end of the proof of Lemma 11 along with the rest of the local factors, and so we see that the restriction is technical rather than substantive.

To estimate the right-hand side of equation (40) using an upper bound sieve, we replace occurrences of the prime p by any integer m whose prime factors are large. We define

$$S(z) = \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \#\{(n,m) : x-L<n\le x,\ f(n)=mh,\ p\mid m \Rightarrow p>z\} \tag{41}$$

and notice that the right-hand side of equation (40) is precisely $S(\xi L^{-\delta})$. It is clear that $S(z)$ is a decreasing function of z, and therefore *to establish Proposition 6 and thus Theorems 1–3, it suffices to show that*

$$S(z) \le L\Big(\frac{2\delta}{1-\delta} + O(\log^{-1/3} L)\Big) \tag{42}$$

for some value of z in the range $2 \le z \le \xi L^{-\delta}$.

As is standard in sieve problems, to understand $S(z)$ we need to understand the corresponding sums over multiples of a given integer, and so we define

$$S_d = \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \#\{(n,m) : x-L<n\le x,\ f(n)=mh,\ d\mid m\}. \tag{43}$$

We see that

$$\begin{aligned} S_d &= \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \#\{x-L<n\le x : dh \mid f(n)\} \\ &= \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \Big(\frac{L\sigma(dh)}{dh} + O(\sigma(dh))\Big) = \frac{L}{d}\sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(dh)}{h} + O\Big(\sum_{1\le h<L^\delta}\sigma(dh)\Big), \end{aligned} \tag{44}$$

since every block of dh consecutive integers contains precisely $\sigma(dh)$ roots of $f \pmod{dh}$. We remark that we could evaluate the sums over h asymptotically at this time by Proposition 9, but as those familiar with sieve methods will recognize, it is crucial to keep the error term in the formula for S_d as small as possible before the sieve is applied. The use of Proposition 9 would permit only a relative error of $\log^{-1} L$ in this formula, which would never allow us to sieve by a set of primes up to a power of L.

We now describe the upper bound linear sieve introduced by Rosser and developed by Iwaniec [16, 17]. For a real number $w \ge 2$, let $P(w) = \prod_{p<w} p$. Let $D > 1$ be a real number, and define a sequence $\{\lambda_d\}$ of real numbers that are supported on the squarefree numbers not exceeding D as follows: let $\lambda_1 = 1$, and if $d = p_1 \cdots p_r$ with $p_1 > \cdots > p_r$, define

$$\lambda_d = \begin{cases} (-1)^r, & \text{if } p_1\cdots p_{2i}p_{2i+1}^3 < D \text{ for all } 0 \le i < r/2, \\ 0, & \text{otherwise.} \end{cases}$$

The sequence $\{\lambda_d\}$ is in fact an upper bound sieve, that is, it satisfies

$$\sum_{d\mid n}\lambda_d \ge \sum_{d\mid n}\mu(d) = \begin{cases} 1, & \text{if } n=1, \\ 0, & \text{if } n>1, \end{cases} \tag{45}$$

where the latter equality is the characteristic property of the Möbius function. In addition, Iwaniec [16, Lemma 3] shows that, uniformly for all multiplicative functions M satisfying $0 \le M(p) < p$ for all primes p and

$$\prod_{w_1\le p<w_2}\Big(1-\frac{M(p)}{p}\Big)^{-1} \le \Big(\frac{\log w_2}{\log w_1}\Big)\Big(1+O\Big(\frac{1}{\log w_1}\Big)\Big) \tag{46}$$

for all $2 \le w_1 \le w_2$, we have

$$\sum_{d|P(z)} \lambda_d \frac{M(d)}{d} \le \prod_{p<z} \Big(1 - \frac{M(p)}{p}\Big)(F(s) + O(\log^{-1/3} D)), \tag{47}$$

for all $2 \le z \le D$, where $s = \log D/\log z$. Here $F(u)$ is the traditional upper-bound function of the linear sieve: it is the continuous solution for $u > 0$ of the system of differential-difference equations

$$\begin{aligned} F(u) = \frac{2e^\gamma}{u} \quad \text{and} \quad f(u) = 0 \qquad (0 < u \le 2), \\ (uF(u))' = f(u-1) \quad \text{and} \quad (uf(u))' = F(u-1) \qquad (2 < u). \end{aligned} \tag{48}$$

One can see that $F(u)$ and $f(u)$ are both nonnegative functions and hence that $uF(u)$ is nondecreasing. (Of course, the companion function $f(u)$ to $F(u)$ is not the same as the polynomial f whose values we are investigating; we will not need to refer to this companion function again, so no confusion should arise.)

With this notation in place, we can provide an upper bound for an expression that will arise in the main term of our sieve estimate for $S(z)$.

Lemma 11. *Let $L \ge 2$ and $0 < \delta < 1/2$ be real numbers. For any real numbers z and D satisfying $L^\delta \le z \le D \le \exp(\log^3 L)$, we have*

$$\sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1 \le h < L^\delta \\ \sigma^*(h) > 0}} \frac{\sigma(dh)}{h} \le \Big(\frac{2\delta \log L}{\log D}\Big)\Big(\frac{sF(s)}{2e^\gamma} + O(s \log^{-1/3} D)\Big), \tag{49}$$

where $s = \log D/\log z$.

We remark that the right-hand side of the inequality (49) has no local factors depending on the polynomial f. This should not be surprising, as the upper bound sieve λ_d is meant to mimic the behavior of $\mu(d)$, so that the sum on the left-hand side of (49) should behave like $\sum_d \sum_h \mu(d)\sigma(dh)/dh$. But for any multiplicative function M, we formally have

$$\sum_d \sum_h \mu(d) M(dh) = \sum_n M(n) \sum_{d|n} \mu(d) = M(1) = 1.$$

We also remark that we have collected the terms in the upper bound (49) in such a way as to highlight the quantity $sF(s)/2e^\gamma$. Since $sF(s)$ is a nondecreasing function, as noted after equation (48), we should take s to be as small as possible (subject to $z \le D$) when applying the asymptotic inequality (49). Thus we set $D = z$, whence $s = 1$ and $sF(s)/2e^\gamma = 1$ as well, again by (48). We obtain

$$\sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1 \le h < L^\delta \\ \sigma^*(h) > 0}} \frac{\sigma(dh)}{h} \le \Big(\frac{2\delta \log L}{\log z}\Big)(1 + O(\log^{-1/3} z)) \tag{50}$$

for any $L \ge 2$ and $z \ge L^\delta$.

Proof: We begin by recalling that $\sigma^*(h) \le \sigma(h)$, and so $\sigma(h)$ is positive whenever $\sigma^*(h)$ is positive. With this observation, we may write

$$\sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(dh)}{h} = \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(h)}{h} \sum_{d|P(z)} \lambda_d \frac{\sigma(dh)}{d\sigma(h)}. \tag{51}$$

By Lemma 7, the function $M(d) = \sigma(dh)/\sigma(h)$ is a multiplicative function of d, and so we would like to apply the upper bound (47) to the inner sums on the right-hand side of equation (51). The inequality (46) is satisfied uniformly in h by Lemma 8, and so it remains only to verify that $M(p) < p$ for every prime p. But if this were not the case, then we would have a prime p for which $\sigma(ph) = p\sigma(h)$. By the comments following the definition (13) of σ^*, this would then imply that $\sigma^*(h) = 0$, and these values of h are excluded from the sum in equation (51).

We are therefore allowed to apply the upper bound (47), and the resulting error term will be uniform in h as well. Equation (51) thus becomes

$$\begin{aligned}\sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(dh)}{h} &\le \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(h)}{h} \prod_{p<z} \Big(1 - \frac{\sigma(ph)}{p\sigma(h)}\Big)(F(s) + O(\log^{-1/3} D)) \\ &= (F(s) + O(\log^{-1/3} D)) \prod_{p<z} \Big(1 - \frac{\sigma(p)}{p}\Big) \\ &\quad \times \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(h)}{h} \prod_{\substack{p<z \\ p^r||h}} \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1}\Big(1 - \frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big)\end{aligned} \tag{52}$$

by the multiplicativity of σ. Equation (12) immediately gives the asymptotic formula

$$\prod_{p<z} \Big(1 - \frac{\sigma(p)}{p}\Big) = \frac{1}{e^\gamma \log z}\Big(1 + O\Big(\frac{1}{\log z}\Big)\Big) \prod_p \Big(1 - \frac{\sigma(p)}{p}\Big)\Big(1 - \frac{1}{p}\Big)^{-1} \tag{53}$$

for the first product in the last expression of inequality (52).

If we define a multiplicative function $G(h)$ by $G(h) = \prod_{p|h}(1 - \sigma(p)/p)^{-1}$ and use the assumption that $z \ge L^\delta$, then the sum over h in the last line of inequality (52) becomes

$$\begin{aligned}\sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(h)}{h} \prod_{\substack{p<z \\ p^r||h}} \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1}\Big(1 - \frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big) &= \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{1}{h} G(h) \prod_{p^r||h} \sigma(p^r)\Big(1 - \frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big) \\ &= \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{G(h)\sigma^*(h)}{h}\end{aligned} \tag{54}$$

by the definition (13) of σ^*. Clearly the restriction $\sigma^*(h) > 0$ is now superfluous and can be removed.

We would like to evaluate this last sum using Proposition 9. Notice that when p is a prime exceeding g and not dividing the discriminant Δ of f, then by the definitions of G and σ^* we have

$$G(p)\sigma^*(p) = \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1}\Big(\sigma(p) - \frac{\sigma(p^2)}{p}\Big) = \sigma(p) + O(p^{-1}),$$

since both $\sigma(p)$ and $\sigma(p^2)$ are bounded by g by the inequality (9). This implies that

$$\sum_{p<x} \frac{G(p)\sigma^*(p)\log p}{p} = O(1) + \sum_{\substack{g<p<x \\ p\nmid\Delta}} \Big(\frac{\sigma(p)\log p}{p} + O\Big(\frac{\log p}{p^2}\Big)\Big) = \log x + O(1)$$

by equation (10), verifying the major hypothesis (15) of Proposition 9 with $\kappa = 1$. Also, the remarks following the statement of Proposition 9 imply that the other hypotheses (16) and (17) are satisfied as well, the latter with $\beta = 1$.

Consequently, we may apply Proposition 9 to obtain

$$\sum_{1\le h\le L^\delta} \frac{G(h)\sigma^*(h)}{h} = \log L^\delta \prod_p \Big(1 + \frac{G(p)\sigma^*(p)}{p} + \frac{G(p^2)\sigma^*(p^2)}{p^2} + \cdots\Big)\Big(1 - \frac{1}{p}\Big) + O(1). \tag{55}$$

However, each term in this product contains the telescoping series

$$\begin{aligned}\frac{G(p)\sigma^*(p)}{p} + \frac{G(p^2)\sigma^*(p^2)}{p^2} + \cdots &= \Big(\frac{\sigma^*(p)}{p} + \frac{\sigma^*(p^2)}{p^2} + \cdots\Big)G(p) \\ &= \Big(\frac{\sigma(p)}{p} - \frac{\sigma(p^2)}{p^2} + \frac{\sigma(p^2)}{p^2} - \frac{\sigma(p^3)}{p^3} + \cdots\Big)\Big(1 - \frac{\sigma(p)}{p}\Big)^{-1} \\ &= \frac{\sigma(p)}{p}\Big(1 - \frac{\sigma(p)}{p}\Big)^{-1} = \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1} - 1,\end{aligned}$$

and thus in light of equation (55), equation (54) becomes

$$\begin{aligned}\sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(h)}{h} \prod_{\substack{p<z \\ p^r\|h}} \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1}\Big(1 - \frac{\sigma(p^{r+1})}{p\sigma(p^r)}\Big) &= \sum_{1\le h\le L^\delta} \frac{G(h)\sigma^*(h)}{h} \\ &= \log L^\delta\Big(1 + O\Big(\frac{1}{\log L}\Big)\Big) \prod_p \Big(1 - \frac{\sigma(p)}{p}\Big)^{-1}\Big(1 - \frac{1}{p}\Big). \end{aligned} \tag{56}$$

We are now able to establish the lemma. When we insert the expressions (53) and (56) into the upper bound (52), the infinite products in (53) and (56) cancel each other completely, leaving the upper bound

$$\sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1\le h<L^\delta \\ \sigma^*(h)>0}} \frac{\sigma(dh)}{h} \le (F(s) + O(\log^{-1/3} D)) \frac{\log L^\delta}{e^\gamma \log z}\Big(1 + O\Big(\frac{1}{\log z}\Big)\Big)\Big(1 + O\Big(\frac{1}{\log L}\Big)\Big).$$

On rearranging the various terms, writing $1/\log z$ as $s/\log D$, and using the hypothesis that $z \le D \le \exp(\log^3 L)$ to simplify the error terms, we obtain precisely the statement (49) of the lemma. □

We are now ready to establish Proposition 6, using the reformulation (42). Let z be a parameter to be specified later subject to $L^\delta \le z \le \xi L^{-\delta}$. We can write the definition (41)

of $S(z)$ as

$$\begin{aligned} S(z) &= \sum_{\substack{1\le h<L^\delta\\ \sigma^*(h)>0}} \sum_{\substack{m\\ p|m\Rightarrow p>z}} \#\{x-L<n\le x : f(n)=mh\} \\ &= \sum_{\substack{1\le h<L^\delta\\ \sigma^*(h)>0}} \sum_{m} \#\{x-L<n\le x : f(n)=mh\} \sum_{d|(m,P(z))} \mu(d), \end{aligned}$$

using the characteristic property of the Möbius function. Then, by the upper bound sieve property (45), we have

$$\begin{aligned} S(z) &\le \sum_{\substack{1\le h<L^\delta\\ \sigma^*(h)>0}} \sum_{m} \#\{x-L<n\le x : f(n)=mh\} \sum_{d|(m,P(z))} \lambda_d \\ &= \sum_{d|P(z)} \lambda_d \sum_{\substack{1\le h<L^\delta\\ \sigma^*(h)>0}} \#\{(n,m) : x-L<n\le x,\ f(n)=mh,\ d\mid m\} = \sum_{d|P(z)} \lambda_d S_d \end{aligned}$$

from the definition (43) of the S_d.

Using the expression (44) for the S_d, we see that

$$S(z) \le L \sum_{d|P(z)} \frac{\lambda_d}{d} \sum_{\substack{1\le h<L^\delta\\ \sigma^*(h)>0}} \frac{\sigma(dh)}{h} + O\Big(\sum_{d|P(z)} \lambda_d \sum_{1\le h<L^\delta} \sigma(dh) \Big). \tag{57}$$

The first sum can be bounded above using the inequality (50). Moreover, the λ_d have absolute value at most 1 and are supported on integers less than D, which we have set equal to z in order to apply (50); thus the sum in the error term is

$$\ll \sum_{1\le d<z} \sum_{1\le h<L^\delta} \sigma(dh) \le \sum_{m<zL^\delta} d(m)\sigma(m).$$

Since $\sigma(p)$ satisfies the asymptotic formula (15) with $\kappa=1$, it follows that $d(p)\sigma(p)$ satisfies (15) with $\kappa=2$. The other hypotheses of Proposition 9 are again easily verified with $\beta=2$, and thus we may apply the upper bound (20) to obtain

$$\sum_{m<zL^\delta} d(m)\sigma(m) \ll zL^\delta \log zL^\delta.$$

The inequality (57) now becomes

$$S(z) \le L\Big(\frac{2\delta\log L}{\log z}\Big)(1+O(\log^{-1/3} z)) + O(zL^\delta \log zL^\delta). \tag{58}$$

We want to make the main term of this upper bound small, and so we want to choose z as large as possible (without making the error term dominant) subject to the condition $L^\delta \le z \le \xi L^{-\delta}$. We set $z = L^{1-\delta}\log^{-2} L$, a valid choice for sufficiently large L since $\delta<1/2$. This gives

$$S(z) \le L\Big(\frac{2\delta}{1-\delta} + O\Big(\frac{\log\log L}{\log L}\Big)\Big)(1+O(\log^{-1/3} L)) + O(L\log^{-1} L), \tag{59}$$

which is enough to establish Proposition 6 and therefore Theorems 1–3.

6. Smooth Values on Prime Arguments

In this section we outline the changes to the above method needed to establish Theorem 4. The ultimate object of study will now be

$$\Psi_\Lambda(f;x,y) = \sum_{\substack{1\le n\le x\\ p\mid f(n)\Rightarrow p\le y}} \Lambda(n);$$

if we can show that $\Psi_\Lambda(f;x,y) \gg x$, then it is easy to deduce that $\Phi(f;x,y) \gg x/\log x$ by a simple partial summation argument. We will use a subscripted Λ on the notation of the preceding sections to denote the appropriately modified quantities, e.g.,

$$C_\Lambda(f;x,y) = x - \Psi_\Lambda(f;x,y).$$

Theorem 4 is a consequence of the following proposition, which is analogous to the special case of Proposition 6 where $L = x$:

Proposition 12. *Let $f(t)$ be an irreducible integer-valued polynomial that is not identically zero modulo any prime. Let $x \ge 2$ be a real number and set $\xi = \max_{n\le x}|f(n)|$, and let δ and ε be positive real numbers such that $\delta+\varepsilon < 1/4$. Then*

$$C_\Lambda(f;x,\xi x^{-\delta}) \le x\Big(\frac{2\delta}{1/2-\delta-\varepsilon} + O(\log^{-1/3} x)\Big). \tag{60}$$

The multiplicative functions that arise in this context are $\sigma_\Lambda(h)$, the number of roots b of $f \pmod h$ such that $(b,h)=1$, and $\sigma^*_\Lambda(h)$, the multiplicative function satisfying $\sigma^*_\Lambda(p^r) = \sigma_\Lambda(p^r) - \sigma_\Lambda(p^{r+1})/p$ for every prime power p^r. For example, we have

$$\sigma_\Lambda(p) = \begin{cases} \sigma(p)-1, & \text{if } p \mid f(0),\\ \sigma(p), & \text{if } p \nmid f(0). \end{cases} \tag{61}$$

The outline of the proof of Proposition 12 is as follows. We define

$$S_\Lambda(z) = \sum_{\substack{1\le h<x^\delta\\ \sigma^*_\Lambda(h)>0}} \sum_{\substack{n\le x\\ (n,h)=1\\ h\mid f(n)\\ p\mid f(n)/h\Rightarrow p>z}} \Lambda(n),$$

a version of the definition (41) of $S(z)$ where each term is weighted by $\Lambda(n)$. Then, as in Section 5, we have $S_\Lambda(\xi x^{-\delta}) = C_\Lambda(f;x,\xi x^{-\delta}) + O(x^{\delta+\varepsilon})$, the error coming from the few terms counted by $C_\Lambda(f;x,\xi x^{-\delta})$ that are excluded from $S_\Lambda(\xi x^{-\delta})$ by the additional condition $(n,h)=1$ in the second sum. Since $S_\Lambda(z)$ is again a decreasing function of z, it suffices to show that $S_\Lambda(z)$ is bounded above by the right-hand side of equation (60) for some $2 \le z \le \xi x^{-\delta}$.

The error term in our asymptotic formula for

$$(S_\Lambda)_d = \sum_{\substack{1\le h<x^\delta\\ \sigma^*_\Lambda(h)>0}} \sum_{\substack{n\le x\\ (n,h)=1\\ dh\mid f(n)}} \Lambda(n) = \sum_{\substack{1\le h<x^\delta\\ \sigma^*_\Lambda(h)>0}} \sum_{\substack{b \pmod{dh}\\ (b,h)=1\\ dh\mid f(b)}} \sum_{\substack{n\le x\\ n\equiv b \pmod{dh}}} \Lambda(n)$$

will now come from errors in counting the number of primes in arithmetic progressions rather than the number of integers. If we define

$$E(t,q) = \max_{(a,q)=1} \left| \frac{t}{\phi(q)} - \sum_{\substack{1\le n\le t \\ n\equiv a \pmod q}} \Lambda(n) \right|,$$

then we have

$$(S_\Lambda)_d = \sum_{\substack{1\le h<x^\delta \\ \sigma_\Lambda^*(h)>0}} \sum_{\substack{b \pmod{dh} \\ (b,h)=1 \\ dh|f(b)}} \Big(\frac{x}{\phi(dh)} + O(E(x,dh))\Big). \tag{62}$$

Now if d is squarefree, then we can write $h' = h(d,h)$ and $d' = d/(d,h)$, so that $h'd' = hd$ and $(h',d') = 1$. Then the integers b such that $(b,h) = 1$ and $f(b) \equiv 0 \pmod{dh}$ are exactly those integers such that $(b,h') = 1$ and $f(b) \equiv 0 \pmod{h'}$ and $\pmod{d'}$. The number of such integers b with $1 \le b \le h'd'$ is $\sigma_\Lambda(h')\sigma(d')$, and so the number of terms in the inner sum of equation (62), while clearly at most $\sigma(dh)$, is precisely

$$\sigma_\Lambda(h')\sigma(d') = \sigma_\Lambda(h(d,h))\sigma\Big(\frac{d}{(d,h)}\Big) = \frac{\sigma_\Lambda(h(d,h))\sigma(d)}{\sigma((d,h))}.$$

Therefore we can derive the asymptotic formula

$$(S_\Lambda)_d = x \sum_{\substack{1\le h<x^\delta \\ \sigma_\Lambda^*(h)>0}} \frac{\sigma_\Lambda(h(d,h))\sigma(d)}{\sigma((d,h))\phi(dh)} + O\Big(\sum_{1\le h<x^\delta} \sigma(dh)E(x,dh)\Big)$$

for any squarefree d, analogous to equation (44). Since the λ_d are supported on squarefree integers, this leads to the upper bound

$$S_\Lambda(z) \le x \sum_{d|P(z)} \lambda_d \sum_{\substack{1\le h<x^\delta \\ \sigma_\Lambda^*(h)>0}} \frac{\sigma_\Lambda(h(d,h))\sigma(d)}{\sigma((d,h))\phi(dh)} + O\Big(\sum_{d|P(z)} \lambda_d \sum_{1\le h<x^\delta} \sigma(dh)E(x,dh)\Big),$$

analogous to the inequality (57).

The double sum in the main term of this inequality is similar to the expression treated in Lemma 11. Although the inner function of d and h is more complicated in this case, no major changes are needed to the method of proof of Lemma 11, and we can derive the following analogous upper bound:

Lemma 13. *Let $x \ge 2$ and $0 < \delta < 1/4$ be real numbers. For any real numbers z and D satisfying $x^\delta \le z \le D \le \exp(\log^3 z)$, we have*

$$\sum_{d|P(z)} \lambda_d \sum_{\substack{1\le h<x^\delta \\ \sigma_\Lambda^*(h)>0}} \frac{\sigma_\Lambda(h(d,h))\sigma(d)}{\sigma((d,h))\phi(dh)} \le \Big(\frac{2\delta\log x}{\log D}\Big)\Big(\frac{sF(s)}{2e^\gamma} + O(s\log^{-1/3} D)\Big),$$

where $s = \log D/\log z$.

Setting $D = z$ allows us to derive an upper bound for $S_\Lambda(z)$, analogous to equation (58), of the form

$$S_\Lambda(z) \le x\Big(\frac{2\delta\log x}{\log z}\Big)(1 + O(\log^{-1/3} z)) + O\Big(\sum_{1\le m<zx^\delta} d(m)\sigma(m)E(x,m)\Big). \tag{63}$$

Since both $d(m) \ll m^{\varepsilon/2}$ and $\sigma(m) \ll m^{\varepsilon/2}$ for any $\varepsilon > 0$, the latter by the observation following equation (9), we deduce that

$$\sum_{1\le m<zx^\delta} d(m)\sigma(m)E(x,m) \ll (zx^\delta)^\varepsilon \sum_{1\le m<zx^\delta} E(x,m).$$

If we choose $z = x^{1/2-\delta-\varepsilon}$ for some $\varepsilon < 1/4-\delta$ (so that $z > x^{1/4} > x^\delta$), then we may use the Bombieri–Vinogradov theorem to conclude that this last sum is $\ll x^{1-\varepsilon}$ and thus that the latter error term in the upper bound (63) is $\ll x^{1-\varepsilon/2}$. With this choice of z, the upper bound (63) then becomes

$$S_\Lambda(z) \le x\Big(\frac{2\delta}{1/2-\delta-\varepsilon} + O(\log^{-1/3} x)\Big),$$

which establishes Proposition 12 and therefore Theorem 4.

One can also demonstrate that a polynomial takes an abundance of smooth values on prime arguments in short intervals, by employing short-interval versions of the Bombieri–Vinogradov theorem. We state the following theorem without proof, except to remark that (64) below uses the work of Perelli, Pintz, and Salerno [19] and that (65) below uses the work of Timofeev [22].

Theorem 14. *Let $h(t)$, g, and k be as in Theorem 1. Let $x \ge 2$ and $0 < \theta < 1$ be real numbers and set $L = x^\theta$. Define*

$$\Phi(h; x, L, y) = \Phi(h; x, y) - \Phi(h; x-L, y).$$

Then when x is sufficiently large, the lower bound

$$\Phi(h; x, L, x^g L^{-\delta}) \gg_\theta L/\log x$$

holds for

$$0 < \delta < \frac{\theta - 1/2}{(2k+1)\theta} \quad \text{if } \theta > 3/5 \tag{64}$$

and for

$$0 < \delta < \frac{\theta - 11/20}{(2k+1)\theta} \quad \text{if } \theta > 7/12. \tag{65}$$

Under the assumption of the generalized Riemann hypothesis, the inequality $\theta > 3/5$ in (64) may be improved to $\theta > 1/2$.

It is also clear that Proposition 12 implies a smoothness result on the values a polynomial takes on a set of primes of positive density, analogous to Theorem 3.

7. An Elementary Lower Bound

In this final section we establish Theorem 5. By the same reasoning as before, it suffices to consider the case $h(t) = f_1(t)\cdots f_k(t)$ where the f_i are distinct irreducible polynomials of degree g that are not identically zero modulo any prime. Given a real number x, let $\mathcal{P}_i$ be the set of primes $p \in [\frac12 x^{1/k}, x^{1/k}]$ such that f_i has a root (mod p), and consider the set

$$\mathcal{P} = \{(p_1,\dots,p_k) \in \mathcal{P}_1 \times\cdots\times \mathcal{P}_k : p_i \ne p_j \ (i \ne j)\}$$

of k-tuples of distinct primes. Each element of $\mathcal{P}$ gives rise to a positive integer $n \le x$ such that $h(n)$ is $O(x^{g-1/k})$-smooth as follows. Choose residue classes n_i (mod p_i) such that

$f_i(n_i) \equiv 0 \pmod{p_i}$. Since the p_i are distinct, we can find a positive integer $n \le p_1 \cdots p_k$ with $n \equiv n_i \pmod{p_i}$ by the Chinese remainder theorem. Clearly each $f_i(n) \equiv 0 \pmod{p_i}$, and so we can write

$$h(n) = f_1(n) \cdots f_k(n) = (p_1 d_1) \cdots (p_k d_k)$$

for some integers d_i. We have $n \le p_1 \cdots p_k \le x$, and each $d_i = f_i(n)/p_i$ is thus $\ll n^g/p_i \ll x^{g-1/k}$. Therefore, $h(n)$ is $O(x^{g-1/k})$-smooth.

To determine the number of distinct values of n arising in this manner, and hence a lower bound for $\Psi(h; x, O(x^{g-1/k}))$, we need a lower bound for the cardinality of $\mathcal{P}$ and an upper bound for the number of different elements of $\mathcal{P}$ that could give rise to a particular value of n. If we write $\sigma_i(h)$ for the the number of roots of $f_i \pmod{h}$, we have $\sigma_i(p) \le g$ for any prime p, and thus

$$\begin{aligned} \#\mathcal{P}_i = \sum_{\substack{x^{1/k}/2 \le p \le x^{1/k} \\ \sigma_i(p) \ge 1}} 1 &\ge \sum_{x^{1/k}/2 \le p \le x^{1/k}} \frac{\sigma_i(p)}{g} \Big(\frac{\log p}{p} \frac{\frac{1}{2} x^{1/k}}{\log \frac{1}{2} x^{1/k}} \Big) \\ &= \frac{x^{1/k}}{2g \log \frac{1}{2} x^{1/k}} \sum_{x^{1/k}/2 \le p \le x^{1/k}} \frac{\sigma_i(p) \log p}{p} \gg \frac{x^{1/k}}{\log x} \end{aligned}$$

by the asymptotic formula (10). Therefore the cardinality of $\mathcal{P}_1 \times \cdots \times \mathcal{P}_k$ is $\gg x \log^{-k} x$; and since there are at most $x^{1-1/k}$ k-tuples in $\mathcal{P}_1 \times \cdots \times \mathcal{P}_k$ whose coordinates are not distinct, we see that $\#\mathcal{P} \gg x \log^{-k} x$.

On the other hand, if an element $(p_1, \ldots, p_k)$ of $\mathcal{P}$ gives rise to a particular n, then certainly each p_i must divide $f_i(n)$. However, each possible p_i is $\gg x^{1/k}$, while each $f_i(n)$ is $\ll x^g$; therefore there are at most gk candidates for each p_i when x is sufficiently large, and hence $(gk)^k \ll 1$ possible elements of $\mathcal{P}$ that give rise to n. From this we conclude that $\Psi(h; x, O(x^{g-1/k})) \gg x \log^{-k} x$, which establishes Theorem 5, aside from having $O(x^{g-1/k})$ as the smoothness parameter instead of $x^{g-1/k}$, which we can fix by replacing x by cx for a suitably small positive constant c.

This technique can also demonstrate an abundance of smooth values of polynomials of more than one variable, and in fact the range of smoothness can be enhanced somewhat by making use of existing results on small solutions of congruences for these polynomials.

References

[1] A. Balog and I. Z. Ruzsa, *On an additive property of stable sets*, Sieve Methods, Exponential Sums and Their Applications in Number Theory (Cardiff, 1995), Cambridge Univ. Press, New York, 1997, pp. 55–63.

[2] A. Balog and T. D. Wooley, *On strings of consecutive integers with no large prime factors*, J. Austral. Math. Soc. Ser. A (to appear).

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

[4] A. A. Buchstab, *On those numbers in an arithmetic progression all prime factors of which are small in magnitude*, Dokl. Akad. Nauk SSSR **67** (1949), 5–8.

[5] C. Dartyge, *Entiers de la forme $n^2 + 1$ sans grand facteur premier*, Acta Math. Hungar. **72** (1996), 1–34.

[6] R. B. Eggleton and J. L. Selfridge, *Consecutive integers with no large prime factors*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 1, 1–11.

[7] J. B. Friedlander, *Shifted primes without large prime factors*, Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 393–401.

[8] J. B. Friedlander and J. C. Lagarias, *On the distribution in short intervals of integers having no large prime factor*, J. Number Theory **25** (1987), no. 3, 249–273.

[9] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press, London, 1974.

[10] A. Hildebrand, *On a conjecture of Balog*, Proc. Amer. Math. Soc. **95** (1985), no. 4, 517–523.

[11] ———, *On integer sets containing strings of consecutive integers*, Mathematika **36** (1989), no. 1, 60–70.

[12] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théor. Nombres Bordeaux **5** (1993), 411–484.

[13] N. A. Hmyrova, *On polynomials with small prime divisors*, Dokl. Akad. Nauk SSSR **155** (1964), 1268–1271.

[14] ———, *On polynomials with small prime divisors II*, Izv. Akad. Nauk SSSR Ser. Mat. **30** (1966), 1367–1372.

[15] M. N. Huxley, *A note on polynomial congruences*, Recent Progress in Analytic Number Theory, vol. 1 (Durham, 1979), Academic Press, London–New York, 1981, pp. 193–196.

[16] H. Iwaniec, *A new form of the error term in the linear sieve*, Acta Arith. **37** (1980), 307–320.

[17] ———, *Rosser's sieve*, Acta Arith. **36** (1980), 171–202.

[18] T. Nagel, *Généralisation d'un théorème de Tchebycheff*, J. Math. Pures Appl. (8) **4** (1921), 343–356.

[19] A. Perelli, J. Pintz, and S. Salerno, *Bombieri's theorem in short intervals*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **11** (1984), no. 4, 529–539.

[20] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. **13** (1967/1968), 177–236.

[21] C. L. Stewart, *On the number of solutions of polynomial congruences and Thue equations*, J. Amer. Math. Soc. **4** (1991), no. 4, 793–835.

[22] N. M. Timofeev, *Distribution of arithmetic functions in short intervals in the mean with respect to progressions*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 2, 341–362, 447.

[23] ———, *Polynomials with small prime divisors*, Taškent. Gos. Univ. Naučn. Trudy (1977), no. 548 Voprosy Mat., 87–91, 145.

[24] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. **143** (1961), 75–102.

Department of Mathematics, University of Toronto, Canada M5S 3G3
E-mail address: gerg@math.toronto.edu