Journal of Number Theory **93**, 108–182 (2002)
doi:10.1006/jnth.2001.2722, available online at http://www.idealibrary.com on IDEAL®

An Asymptotic Formula for the Number of Smooth Values of a Polynomial

Greg Martin

Department of Mathematics, The University of British Columbia, Room 121, 1984 Mathematics Road, Vancouver, British Columbia V6T 1Z2, Canada
E-mail: gerg@math.toronto.edu

Communicated by A. Hildebrand

Received October 4, 1999

1. INTRODUCTION

Integers without large prime factors, dubbed *smooth numbers*, are by now firmly established as a useful and versatile tool in number theory. More than being simply a property of numbers that is conceptually dual to primality, smoothness has played a major role in the proofs of many results, from multiplicative questions to Waring's problem to complexity analyses of factorization and primality-testing algorithms. In these last applications, what is needed is an understanding of the distribution of smooth numbers among the values taken by a polynomial, which is the subject of this paper. Specifically, we show a connection between the asymptotic number of prime values taken by a polynomial and the asymptotic number of smooth values so taken, showing another way in which these two properties are more than abstractly linked.

There are conjectures about the distribution of prime values of polynomials that by now have become standard. Dickson [4] first conjectured that any K linear polynomials with integer coefficients forming an "admissible" set infinitely often take prime values simultaneously, where $\{L_1, \ldots, L_K\}$ is admissible if for every prime p, there exists an integer n such that none of $L_1(n), \ldots, L_K(n)$ is a multiple of p; subsequently, Hardy and Littlewood [7] proposed an asymptotic formula for how often this occurs. Schinzel and Sierpiński's "Hypothesis H" [12] asserts that for an admissible set $\{F_1, \ldots, F_K\}$ of irreducible polynomials (integer-valued, naturally) of any degree, there are infinitely many integers n such that each of $F_1(n), \ldots, F_K(n)$ is prime; a quantitative version of this conjecture was first published by Bateman and Horn [2]. We must introduce some notation before we can describe the conjectured asymptotic formula, which we

0022-314X/02 $35.00

prefer to recast in terms of a single polynomial F rather than a set $\{F_1, ..., F_K\}$ of irreducible polynomials.

Let $F(t) = F_1(t)...F_K(t)$ be the product of K distinct irreducible polynomials with integer coefficients. We say that the polynomial F is *admissible* if the set $\{F_1, ..., F_K\}$ is admissible, that is, if for every prime p there exists an integer n such that $F(n)$ is not a multiple of p. Let $\pi(F; x)$ denote the number of positive integers n not exceeding x such that each $F_i(n)$ is a prime (positive or negative). When F is an admissible polynomial, the size of $\pi(F; x)$ is heuristically $C(F)\,\mathrm{li}(F; x)$, these two quantities being defined as

$$C(F) = \prod_p \left(1 - \frac{1}{p}\right)^{-K} \left(1 - \frac{\sigma(F; p)}{p}\right), \tag{1.1}$$

where $\sigma(F; n)$ denotes the number of solutions of $F(a) \equiv 0 \pmod{n}$, and

$$\mathrm{li}(F; x) = \int_{\substack{0 < t < x \\ \min\{|F_1(t)|, ..., |F_K(t)|\} \geq 2}} \frac{dt}{\log |F_1(t)| \dots \log |F_K(t)|}. \tag{1.2}$$

The second condition of integration is included only to avoid having to worry about the singularities of the integrand (though we could have instead defined $\mathrm{li}(F; x)$ using the Cauchy principal value, for example); we note that $\mathrm{li}(F; x)$ reduces to the familiar logarithmic integral $\mathrm{li}(x) = \int_2^x dt/\log t$ when $F(t) = t$. At this time, the only case where the conjecture has been established (even non-quantitatively) is when F is a linear polynomial, when the problem reduces to counting primes in a fixed arithmetic progression.

The prime number theorem $\pi(x) \sim \mathrm{li}(x)$ says that the "probability" of an integer of size X being prime is $1/\log X$; if we pretend that the primality of the various $F_i(n)$ are independent random events, then $\mathrm{li}(F; x)$ would be the expected number of positive integers $n \leq x$ for which all the $F_i(n)$ are prime. (Of course, for a fixed polynomial F, the quantity $\mathrm{li}(F; x)$ is itself asymptotic to $x/\log^K x$, as appears in [2]; but the specific expression (1.2) should be more accurate uniformly over polynomials F.) This first guess needs to be modified, however, to account for the fact that the values of F might be more or less likely to be divisible by a given small prime p than a "randomly chosen" integer of the same size; taking this factor into account is the role of the constant $C(F)$ (which is a convergent infinite product—see the discussion following Eq. (6.1) below).

We would like to have a similar understanding of the distribution of smooth values of a polynomial. Let us define

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

the number of y-smooth values of F on arguments up to x; this generalizes the standard counting function $\Psi(x, y)$ of y-smooth numbers up to x. Known upper bounds (see for instance [11]) and lower bounds (see [3]) for $\Psi(F; x, y)$ do indicate the order of magnitude of $\Psi(F; x, y)$ in certain ranges; however, in contrast to $\pi(F; x)$, there seems to be no consensus concerning the expected asymptotic formula for $\Psi(F; x, y)$.

We can form a probabilistic heuristic for the behavior of $\Psi(F; x, y)$ from the known asymptotic formula

$$\Psi(x, y) \sim x\rho\left(\frac{\log x}{\log y}\right), \tag{1.3}$$

where $\rho(u)$ is the Dickman rho-function, defined as the (unique) continuous solution of the differential-difference equation $u\rho'(u) = -\rho(u-1)$ for $u \geqslant 1$, satisfying the initial condition $\rho(u) = 1$ for $0 \leqslant u \leqslant 1$. (We record for later reference that $\rho(u) = 1 - \log u$ for $1 \leqslant u \leqslant 2$.) An interpretation of the asymptotic formula (1.3) is that a "randomly chosen" integer of size X has probability $\rho(u)$ of being $X^{1/u}$-smooth. Again pretending that the multiplicative properties of the various $F_i(n)$ are independent of one another, we are led to the probabilistic prediction that

$$\Psi(F; x, y) \sim x \prod_{i=1}^{K} \rho\left(\frac{\log F_i(x)}{\log y}\right),$$

or equivalently, if we let d_i denote the degree of F_i,

$$\Psi(F; x, x^{1/u}) \sim x\rho(d_1 u) \dots \rho(d_K u). \tag{1.4}$$

It might seem unclear whether this heuristic needs to include some sort of dependence on the local properties of F, analogous to the constant $C(F)$ defined above. The purpose of this paper is to demonstrate, assuming a suitable quantitative version of the conjectured asymptotic formula for prime values of polynomials, that the probabilistic prediction (1.4) is indeed the correct one.

Let us define

$$E(F; x) = \pi(F; x) - C(F)\,\mathrm{li}(F; x), \tag{1.5}$$

so that $E(F; x)$ is conjecturally the error term in the asymptotic formula for prime values of polynomials. Our results will depend upon the following hypothesis:

HYPOTHESIS UH. *Let $d \geqslant K \geqslant 1$ be integers and B any large positive constant. Then, with $C(F)$ as defined in Eq.* (1.1),

$$E(F; t) \ll_{d, B} \frac{C(F)\, t}{\log^{K+1} t} + 1 \tag{1.6}$$

uniformly for all integer-valued polynomials F, of degree d with precisely K distinct irreducible factors, whose coefficients are at most t^B in absolute value.

Hypothesis UH asserts that the quantitative version of Hypothesis H holds with a considerable range of Uniformity in the coefficients of the polynomial F. We immediately remark that we do not need the full strength of Hypothesis UH for our main theorem, but the precise requirement is much more complicated to state (see Eq. (2.11) and Proposition 2.9 below). We do comment, however, that in the case of linear polynomials ($d = K = 1$), Hypothesis UH is equivalent to a well-accepted conjecture on the distribution of primes in short segments of arithmetic progressions (see Appendix B). Thus the uniformity required by Hypothesis UH is not unrealistic.

Notice that if F is not admissible, then there exists a prime p such that $\sigma(p) = p$; therefore $C(F) = 0$ and hence $E(F; t) = \pi(F; t)$. On the other hand, every value of F is then divisible by p, and so the only possible prime values of F are $\pm p$. Since each of these values can be taken at most $\deg F = d$ times, we see that $\pi(F; t) \ll_d 1$ when F is not admissible. Consequently, Hypothesis UH automatically holds for non-admissible polynomials. We have chosen the form (1.6) for the hypothesized bound on $E(F; t)$ so that it can be applied without checking in advance whether the polynomial F is admissible.

We are now ready to state our main theorem.

THEOREM 1.1. *Assume Hypothesis* UH. *Let F be an integer-valued polynomial, let K be the number of distinct irreducible factors of F, and let $d_1, \ldots, d_K$ be the degrees of these factors. Let $d = \max\{d_1, \ldots, d_K\}$, and let k be the number of distinct irreducible factors of F whose degree equals d. Then for any real number $U < (d - 1/k)^{-1}$, the asymptotic formula*

$$\Psi(F; x, x^{1/u}) = x\rho(d_1 u) \ldots \rho(d_K u) + O_{F, U}\left(\frac{x}{\log x}\right) \tag{1.7}$$

holds uniformly for $x \geqslant 1$ and $0 < u \leqslant U$.

In particular, if F is an irreducible polynomial of degree d, then for any real number $U < 1/(d-1)$, the asymptotic formula

$$\Psi(F; x, x^{1/u}) = x\rho(du) + O_{F, U}\left(\frac{x}{\log x}\right)$$

holds with the stated uniformity. We note that in the case $d=K=1$, where $k=1$ and $F(t)=qt+a$ is a linear polynomial, Theorem 1.1 reduces to a well-known asymptotic formula for smooth numbers in a fixed arithmetic progression, since

$$\begin{aligned}\Psi(F; x, x^{1/u}) &= \Psi(qx+a, x^{1/u}; q, a) - \Psi(a, x^{1/u}; q, a)\\ &= \Psi(qx, x^{1/u}; q, a) + O(1)\\ &= \frac{qx\rho(u)}{q}\left(1+O_{q,a}\left(\frac{1}{\log x}\right)\right)\\ &= x\rho(u) + O_{F,U}\left(\frac{x}{\log x}\right)\end{aligned}$$

(see the survey article [8]; here $\Psi(x, y; q, a)$ denotes the number of y-smooth numbers up to x that are congruent to $a \pmod q$). This asymptotic formula is known unconditionally to hold for arbitrarily large values of U, which is consistent with the interpretation of the condition $U<(d-1/k)^{-1}=\infty$ in this case.

Theorem 1.1 shows, given what we believe to be true about prime values of polynomials, that the probabilistic prediction (1.4) of the asymptotic formula for $\Psi(F; x, y)$ is indeed valid for a suitable range of u. We remark that the formula (1.7) is trivially true for $u<1/d$, since in this range the smoothness parameter $x^{1/u}$ will asymptotically exceed the sizes of the factors $F_i(n)$ of $F(n)$, each of which is $\ll_F x^d$. Since $(d-1/k)^{-1}>1/d$, Theorem 1.1 applies to a nontrivial range of u; even though this range is limited, the theorem provides the first hard evidence that the probabilistic prediction is the correct one for general polynomials. The proof of Theorem 1.1 comprises the bulk of this paper and is outlined in Section 2.

If we let $\Phi(F; x, y)$ denote the number of primes q up to x for which $F(q)$ is y-smooth, then a similar probabilistic argument yields the prediction

$$\Phi(F; x, x^{1/u}) \sim \pi(F; x)\, \rho(d_1 u) \ldots \rho(d_K u), \tag{1.8}$$

and the methods used to establish Theorem 1.1 could be extended to prove an analogous result for $\Phi(F; x, x^{1/u})$. Instead of proceeding in this generality, we prefer to focus on a special case for which a stronger theorem can be established. Shifted primes $q+1$ without large prime factors played an important role in the recent proof by Alford *et al.* [1] that there are infinitely many Carmichael numbers; the counting function of these smooth shifted primes is precisely $\Phi(F; x, y)$ where $F(t)=t+1$. More generally, for any nonzero integer a we define

$$\Phi_a(x, y) = \#\{q \leqslant x,\ q \text{ prime} : p \mid q-a \Rightarrow p \leqslant y\},$$

the number of shifted primes $q-a$ with q not exceeding x that are y-smooth. We prove the following theorem:

THEOREM 1.2. *Assume Hypothesis* UH. *Let* $0<U<3$ *be a real number and* $a\neq 0$ *an integer. Then*

$$\Phi_a(x, x^{1/u}) = \pi(x)\,\rho(u) + O_{a,U}\left(\frac{\pi(x)}{\log x}\right) \tag{1.9}$$

uniformly for $x \geqslant 1+\max\{a, 0\}$ *and* $0<u\leqslant U$.

Our method (see Section 9) is capable in principle of establishing Theorem 1.2 for arbitrarily large values of U; however, the combinatorial complexity of the proof would increase each time U passed an integer. This is because there is no Buchstab-type identity for smooth shifted primes like the one commonly used to establish the asymptotic formula (1.3) for smooth numbers, so one must explicitly write an inclusion-exclusion formula to characterize the smooth numbers in question. The proof of Theorem 1.2 for the stated range of U is indicative of how the more general result would be established. The fact that the Dickman function $\rho(u)$ appears unaltered in Theorem 1.2 in the expanded range $0<u<3$, where the behavior of ρ is more complicated, gives further evidence that the probabilistic predictions (1.4) and (1.8) are correct in general, without any modifications resulting from the local properties of the polynomial F.

As with Theorem 1.1, the precise hypothesis that we require for establishing Theorem 1.2 is much less stringent than Hypothesis UH. We remark that we could show, using no new ideas but with a substantial amount of bookkeeping, that Theorem 1.2 holds uniformly for $a \ll x$ if we insert an additional factor of loglog x into the error term in the asymptotic formula (1.9). In particular, by taking $x=a=N$, such a strengthening would encompass the Goldbach-like problem of counting the number of representations of an integer N as $N=p+n$ where p is prime and n is $N^{1/u}$-smooth.

2. THE STRUCTURE OF THE PROOF OF THEOREM 1.1

The proof of Theorem 1.1 is quite long and, unfortunately, mired in technical details in many places. In the interest of making the overall structure of the proof more evident, we have broken the proof down into several propositions, precisely stated in this section, from which Theorem 1.1 will be deduced near the end of the section. These propositions will themselves be proved in the sections to come.

In descriptive terms, the proof of Theorem 1.1 proceeds according to the following outline:

1. We show that we may assume, without loss of generality, that the polynomial F satisfies several technical conditions on its factorization and on its local properties. This reduction is described in Proposition 2.1 below.

2. Using an inclusion-exclusion argument on the factors of F, we write $\Psi(F; x, y)$ as a combination (see Proposition 2.2) of terms of the form $M(f; x, y)$, defined in Eq. (2.1) below, where f runs through divisors of F.

3. We establish a "pseudo-asymptotic formula" (where the behavior of one of the primary terms $H(f; x, y)$, defined in Eq. (2.11) below, is unknown), given in Theorem 2.8, for the expressions $M(f; x, y)$. The proof of this theorem is itself broken into several steps:

(a) We convert $M(f; x, y)$ into a combination of terms of the form $\pi(f_i; x_i)$, where the f_i are drawn from a family of polynomials determined by f, as described in Proposition 2.3;

(b) We apply Brun's sieve method to establish in Proposition 2.4 an upper bound for the smaller terms of this form;

(c) By investigating the relationships among the local properties of the polynomials in this family, we evaluate a certain finite sum (see Proposition 2.5) involving constants of the type $C(f_i)$ defined in Eq. (1.1);

(d) We establish an asymptotic formula for a weighted mean value of the multiplicative function that arises in the previous step, which is the content of Proposition 2.6.

4. Next, we show that Hypothesis UH implies an upper bound for the term $H(f; x, y)$, as given in Proposition 2.9, and thus converts the pseudo-asymptotic formula from Theorem 2.8 into a true asymptotic formula for the $M(f; x, y)$.

5. Finally, since $\Psi(F; x, y)$ has been expressed as a combination of terms of the form $M(f; x, y)$ in Proposition 2.2, we can recast Theorem 2.8 into our final goal, an asymptotic formula for $\Psi(F; x, y)$.

The rest of this section will be devoted to making this outline rigorous and establishing Theorems 2.8 and 1.1 assuming the validity of the propositions to be stated. We begin by defining the technical conditions we would like to impose on the polynomial F. Other than the first two terms, we make no claims that the following terminology is (or should become) standard—we simply wish to use concise, reasonably provocative words rather than include long, awkward phrases at every turn.

- Recall that a polynomial is *squarefree* if it is not divisible by the square of any nonconstant polynomial.

- Recall also that a polynomial with integer coefficients is *primitive* if the greatest common divisor of its coefficients is 1. A polynomial is primitive if and only if each of its irreducible factors is primitive, and the factorization of a primitive polynomial over the rationals is the same as its factorization over the integers (both these statements are consequences of Gauss' Lemma).

- We say that a polynomial is *balanced* if it is the product of distinct irreducible polynomials all of the same degree, so that in particular, a balanced polynomial is squarefree.

- We say that an irreducible polynomial g is *effective* if $g(0) \geqslant 2$ and $g'(t) \geqslant 1$ for all $t \geqslant 0$, and we say that an arbitrary polynomial f is effective if all of its irreducible factors are effective. This certainly implies that $f(0) \geqslant 2$ and $f'(t) \geqslant 1$ for all $t \geqslant 0$, and hence $f(t) > t$ for all $t \geqslant 0$.

- In agreement with the use of the term in Section 1, we call a polynomial with integer coefficients *admissible* if it takes at least one nonzero value modulo every prime. In particular, any admissible polynomial is primitive.

- Finally, we say that a polynomial f with integer coefficients is *exclusive* if no two distinct irreducible factors of f have a common zero modulo any prime. A primitive polynomial f is exclusive if and only if the resultant $\operatorname{Res}(g, h)$ of g and h equals 1 for every pair g, h of distinct irreducible factors of f.

Now that this terminology is in place, we can state the proposition that allows us to place various restrictions on the polynomial F in Theorem 1.1.

PROPOSITION 2.1. *Suppose that Theorem* 1.1 *holds for any polynomial with integer coefficients that is balanced, effective, admissible, and exclusive. Then it holds for any integer-valued polynomial.*

This proposition is established in Section 3 by considering an arbitrary polynomial restricted to suitable arithmetic progressions.

Next we introduce the quantity $M(f; x, y)$ for which we shall establish a pseudo-asymptotic formula in Theorem 2.8. Given a primitive polynomial f, define

$$M(f; x, y) = \#\{1 \leqslant n \leqslant x : \text{ for each irreducible factor } g \text{ of } f, \text{ there exists a prime } p > y \text{ such that } p \mid g(n)\}. \quad (2.1)$$

The connection between smooth values of polynomials and these expressions $M(f; x, y)$ is given in the following proposition:

Proposition 2.2. *Let F be a primitive polynomial, and let $F_1, \ldots, F_K$ denote the distinct irreducible factors of F. Then for any real numbers $x \geqslant y \geqslant 1$,*

$$\Psi(F; x, y) = \lfloor x \rfloor + \sum_{1 \leqslant k \leqslant K} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant K} M(F_{i_1} \ldots F_{i_k}; x, y).$$

The statement of the next proposition requires a bit more notation. In fact, the following notation will be used in the statements of Propositions 2.3–2.7, Theorem 2.8, and Proposition 2.9:

• Let f be a polynomial with integer coefficients that is primitive and balanced. Let k denote the number of irreducible factors of f, let $f_1, \ldots, f_k$ denote these irreducible factors, and let d denote their common degree.

• Let u and U be real numbers in the range

$$1/d \leqslant u \leqslant U < \min\{(d - 1/k)^{-1}, 2/d\}. \tag{2.2}$$

• Given a real number $x \geqslant 1$, set $y = x^{1/u}$ and $\xi_i = f_i(x)$ for $1 \leqslant i \leqslant k$. Note that $\xi_i \asymp x^d$ as x goes to infinity (where $X \asymp Y$ means $Y \ll X \ll Y$), and that the upper bound (2.2) on U implies that $y \geqslant \sqrt{\xi_i}$ when x is sufficiently large in terms of f and U.

• As in Section 1, let $\pi(f; t)$ denote the number of integers $1 \leqslant n \leqslant t$ for which each $f_i(n)$ is prime.

• Given positive integers $h_1, \ldots, h_k$, define

$$\mathcal{R}(f; h_1, \ldots, h_k) = \{1 \leqslant b \leqslant h_1 \ldots h_k : h_i \mid f_i(b) \text{ for each } 1 \leqslant i \leqslant k\}. \tag{2.3}$$

For any element b of $\mathcal{R}(f; h_1, \ldots, h_k)$, define the polynomial $f_{h_1 \ldots h_k, b}$ by

$$f_{h_1 \ldots h_k, b}(t) = \frac{f(h_1 \ldots h_k t + b)}{h_1 \ldots h_k}. \tag{2.4}$$

We remark that $f_{h_1 \ldots h_k, b}$ actually has integer coefficients (see the remarks following Eq. (3.5) below).

When we prove Propositions 2.3–2.7 and 2.9 in later sections, we shall adhere to this notation as well. With the notation in place, we can describe the connection between the expressions $M(f; x, y)$ defined in Eq. (2.1) and prime values of polynomials.

Proposition 2.3. *Let f be a polynomial that is balanced, effective, primitive, and exclusive. Then when x is sufficiently large we have*

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \left(\pi\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k} \right) - \pi(f_{h_1 \ldots h_k, b}; \eta_{h_1, \ldots, h_k}) \right) \tag{2.5}$$

for certain quantities $\eta_{h_1, \ldots, h_k}$ that satisfy $\eta_{h_1, \ldots, h_k} \asymp (y \max\{h_1, \ldots, h_k\})^{1/d} \times (h_1 \ldots h_k)^{-1}$.

Together, Propositions 2.2 and 2.3 provide the link between smooth values of polynomials and prime values of polynomials. These propositions are combinatorial in nature, and their proofs are given in Section 4.

Of the two terms of the form $\pi(f; t)$ in each summand on the right-hand side of Eq. (2.5), the first term is the significant one. The following proposition provides a tidy bound for the contribution to the sum from the second terms (those containing the quantities $\eta_{h_1, \ldots, h_k}$).

Proposition 2.4. *Let f be a polynomial that is balanced, effective, and primitive. If the quantities $\eta_{h_1, \ldots, h_k}$ satisfy $\eta_{h_1, \ldots, h_k} \asymp (y \max\{h_1, \ldots, h_k\})^{1/d} \times (h_1 \ldots h_k)^{-1}$, then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \pi(f_{h_1 \ldots h_k, b}; \eta_{h_1, \ldots, h_k}) \ll_f \frac{x}{\log x}.$$

This proposition is established by an application of Brun's upper bound sieve method to each summand, as we show in Section 7. The only complication is keeping track of the dependence on $h_1, \ldots, h_k$, and b in the bounds obtained; the multiple sum over $h_1, \ldots, h_k$ that results is then bounded by a mean-value theorem for multiplicative functions (Proposition A.1 in Appendix A).

The next proposition is, in a sense, the most important step in the proof, as it relates a complicated expression involving the numbers of local roots of a family of polynomials to a value of an explicit multiplicative function. To state this proposition, we recall from Section 1 that $\sigma(f; n)$ denotes the number of solutions of $f(a) \equiv 0 \pmod{n}$, and we define two related multiplicative functions as

$$G(f; n) = \prod_{p \mid n} \left(1 - \frac{\sigma(f; p)}{p} \right)^{-1} \quad \text{and}$$

$$\sigma^*(f; n) = \prod_{p^\nu \parallel n} \left(\sigma(f; p^\nu) - \frac{\sigma(f; p^{\nu+1})}{p} \right). \tag{2.6}$$

If we assume that f is admissible, then $\sigma(f;p)<p$ for all primes p, and hence $G(f;p)$ is well-defined. We remark that both of these multiplicative functions are nonnegative (for σ^* this is not transparent—see Eq. (5.5) below) and that $\sigma^*(f;n)\leqslant\sigma(f;n)$.

We also recall the definition (1.2) of $\mathrm{li}(f;x)$, and for polynomials f that are effective and balanced we define the modified function

$$\mathrm{li}_{h_1,\ldots,h_k}(f;x)=\int_{\substack{0<t<x\\ \min\{f_1(t)/h_1,\ldots,f_k(t)/h_k\}\geqslant 2}}\frac{dt}{\log(f_1(t)/h_1)\ldots\log(f_k(t)/h_k)} \tag{2.7}$$

for any positive integers $h_1, \ldots, h_k$. We can now state the following proposition:

Proposition 2.5. *Let f be a polynomial that is balanced, effective, admissible, and exclusive, and let $h_1, \ldots, h_k$ be pairwise coprime positive integers. Then*

$$\begin{aligned}\sum_{b\in\mathscr{R}(f;h_1,\ldots,h_k)} C(f_{h_1\ldots h_k,b})\,\mathrm{li}\left(f_{h_1\ldots h_k,b};\frac{x-b}{h_1\ldots h_k}\right)\\ =\frac{C(f)\,G(f;h_1\ldots h_k)\,\sigma^*(f_1;h_1)\ldots\sigma^*(f_k;h_k)\,\mathrm{li}_{h_1,\ldots,h_k}(f;x)}{h_1\ldots h_k}\\ +O_f(G(f;h_1\ldots h_k)\,\sigma^*(f_1;h_1)\ldots\sigma^*(f_k;h_k))\end{aligned} \tag{2.8}$$

uniformly for $x\geqslant 1$.

As one might guess, the sum on the left-hand side of Eq. (2.8) arises from the first terms in the summands of Eq. (2.5). The $\mathrm{li}(\cdot)$ factor is quite benign, as it does not depend very much on b; the important part of the evaluation, as we shall see in Section 5, is to understand the relationship between the constants $C(f_{h_1\ldots h_k,b})$ and $C(f)$ itself.

We have two more propositions to state before coming to our proof of the pseudo-asymptotic formula for $M(f;x,y)$. In that proof, we shall need to sum the right-hand side of Eq. (2.8) over the possible values of the h_i. The first of these two propositions gives us an asymptotic formula for the resulting sum of the main term from (2.8), while the second proposition estimates the resulting error term.

Proposition 2.6. *Let f be a polynomial that is balanced, effective, admissible, and exclusive. Then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y}} \cdots \sum_{\substack{h_k \leqslant \xi_k/y \\ (h_i, h_j)=1\,(1 \leqslant i < j \leqslant k)}} \frac{G(f; h_1 \ldots h_k)\,\sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)\,\mathrm{li}_{h_1, \ldots, h_k}(f; x)}{h_1 \ldots h_k}$$

$$= C(f)^{-1}\, x \log^k(du) + O_{f,U}\left(\frac{x}{\log x}\right) \tag{2.9}$$

uniformly for $x \geqslant 1$ *and* $0 < u \leqslant U$.

Proposition 2.6 is definitely the longest part of the proof, taking all of Section 8 to complete and requiring the machinery of Appendix A, although the difficulties are technical rather than conceptual. Even ignoring the presence of the $\mathrm{li}_{h_1, \ldots, h_k}$ term in the sum on the left-hand side of Eq. (2.9), that sum is made more difficult to analyze because of the coprimality condition of summation—otherwise, the multiple sum would just be a k-fold product of sums of multiplicative functions of one variable. Proposition A.4 below provides a general asymptotic formula for multiple sums of multiplicative functions where the variables of summation are restricted in this way. Once we understand the behavior of that sum with the $\mathrm{li}_{h_1, \ldots, h_k}$ term omitted (see Lemma 8.1), we employ a lengthy partial summation argument to assess the effect of the $\mathrm{li}_{h_1, \ldots, h_k}$ term on the actual sum.

The second of these two propositions is much easier to establish than the first, due to the fact that we seek only an upper bound rather than an asymptotic formula. This means that the coprimality condition of summation can be omitted and a mean-value theorem for multiplicative functions (Proposition A.1) invoked in the proof, which can be found in Section 6.

Proposition 2.7. *Let f be a polynomial that is balanced and admissible. Then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y}} \cdots \sum_{\substack{h_k \leqslant \xi_k/y \\ (h_i, h_j)=1\,(1 \leqslant i < j \leqslant k)}} G(f; h_1 \ldots h_k)\,\sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k) \ll_{f,U} \frac{x}{\log x}$$

uniformly for $x \geqslant 1$ *and* $0 < u \leqslant U$.

Assuming the validity of Propositions 2.3–2.7, we can at last state and prove our main result concerning the expressions $M(f; x, y)$. We have repeated the definitions of the various symbols so as to have the statement of the theorem be self-contained.

Theorem 2.8. *Let f be a polynomial that is balanced, effective, admissible, and exclusive. Let k denote the number of irreducible factors of f, let*

$f_1, \ldots, f_k$ denote these irreducible factors, and let d denote their common degree. Let u and U be real numbers in the range (2.2). *Given a real number $x \geqslant 1$, set $y = x^{1/u}$ and $\xi_i = f_i(x)$ for $1 \leqslant i \leqslant k$. If $M(f; x, y)$ is defined as in Eq.* (2.1) *and $E(f; x)$ is defined as in Eq.* (1.5), *then we have*

$$M(f; x, y) = x \log^k(du) + H(f; x, y) + O_{f,U}\left(\frac{x}{\log x}\right) \tag{2.10}$$

uniformly for $x \geqslant 1$ and $0 < u \leqslant U$, where $H(f; x, y)$ is defined by

$$H(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} E\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right). \tag{2.11}$$

Of course, it is the unknown size of $H(f; x, y)$ that keeps Eq. (2.10) from being an unconditional asymptotic formula for $M(f; x, y)$, which would lead to an unconditional asymptotic formula for $\Psi(F; x, y)$ using Proposition 2.2; it is to control the size of $H(f; x, y)$ that Hypothesis UH will be used (see the proof of Proposition 2.9 below).

Proof. Proposition 2.3 tells us that

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \left(\pi\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right) - \pi(f_{h_1 \ldots h_k, b}; \eta_{h_1, \ldots, h_k})\right).$$

From the definition (1.5) of $E(f; x)$, we can write this as

$$\begin{aligned} M(f; x, y) = {} & \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}) \operatorname{li}\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right) \\ & + \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} E\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right) \\ & - \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \pi(f_{h_1 \ldots h_k, b}; \eta_{h_1, \ldots, h_k}). \end{aligned} \tag{2.12}$$

If we define

$$M_1(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}) \operatorname{li}\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right) \tag{2.13}$$

and use the definition (2.11) of $H(f; x, y)$, Eq. (2.12) becomes

$$M(f; x, y) = M_1(f; x, y) + H(f; x, y) + O_{f,U}\left(\frac{x}{\log x}\right),$$

where we have used Proposition 2.4 to estimate the final sum in (2.12). It therefore suffices to show that

$$M_1(f; x, y) = x \log^k(du) + O_{f,U}\left(\frac{x}{\log x}\right). \tag{2.14}$$

The inner sum in the definition (2.13) can be evaluated by Proposition 2.5, yielding

$$M_1(f; x, y) = C(f) \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \dots h_k)\, \sigma^*(f_1; h_1) \dots \sigma^*(f_k; h_k)\, \mathrm{li}_{h_1, \dots, h_k}(f; x)}{h_1 \dots h_k}$$
$$+ O\Bigg(\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} G(f; h_1 \dots h_k)\, \sigma^*(f_1; h_1) \dots \sigma^*(f_k; h_k) \Bigg).$$

Using the asymptotic formula given by Proposition 2.6 for the main term in this last expression and the estimate in Proposition 2.7 to bound the error term, we see that

$$M_1(f; x, y) = C(f)\left(C(f)^{-1}\, x \log^k(du) + O_{f,U}\left(\frac{x}{\log x}\right)\right) + O_{f,U}\left(\frac{x}{\log x}\right)$$
$$= x \log^k(du) + O_{f,U}\left(\frac{x}{\log x}\right),$$

which establishes Eq. (2.14) and hence the theorem. ∎

As we mentioned before, Hypothesis UH implies an upper bound for the expression $H(f; x, y)$ defined in Eq. (2.11). The following proposition, proved in Section 6 using again the mean-value theorem for multiplicative functions (Proposition A.1), provides the needed estimate.

PROPOSITION 2.9. *Assume Hypothesis* UH. *Let f be a polynomial with integer coefficients that is balanced, effective, and admissible. Then* $H(f; x, y) \ll_{f,U} x/\log x$.

If we assume for now the validity of Theorem 2.8 and Propositions 2.1, 2.2, and 2.9, we have all the tools we need to establish our main theorem.

Proof of Theorem 1.1. As mentioned after the statement of Theorem 1.1, the theorem is already known unconditionally in the case $d=K=1$, and so we may assume that $dK \geqslant 2$. First suppose that the polynomial F has integer coefficients and is balanced, effective, admissible, and exclusive; in this case the statement of Theorem 1.1 reduces to

$$\Psi(F; x, y) = x\rho(du)^K + O_{F,U}\left(\frac{x}{\log x}\right). \tag{2.15}$$

Now Proposition 2.2 tells us that

$$\Psi(F; x, y) = \lfloor x \rfloor + \sum_{1 \leqslant k \leqslant K} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant K} M(F_{i_1} \dots F_{i_k}; x, y). \tag{2.16}$$

We note that any divisor of a polynomial that is balanced, effective, admissible, and exclusive will itself have those four properties. Therefore, setting f to equal any of these polynomials $F_{i_1} \dots F_{i_k}$ (so that the convention that k denotes the number of irreducible factors of f is consistent with the use of k in Eq. (2.16)), we see from Theorem 2.8 that

$$M(f; x, y) = x \log^k(du) + H(f; x, y) + O_{f,U}\left(\frac{x}{\log x}\right). \tag{2.17}$$

But from Proposition 2.9, under Hypothesis UH we have $H(f; x, y) \ll_{f,U} x/\log x$, and therefore $H(f; x, y)$ can be absorbed into the error term in the asymptotic formula (2.17). With this formula, Eq. (2.16) becomes

$$\Psi(F; x, y) = \lfloor x \rfloor + \sum_{1 \leqslant k \leqslant K} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant K} \left(x \log^k(du) + O_{F,U}\left(\frac{x}{\log x}\right)\right).$$

For any $1 \leqslant k \leqslant K$ there are $\binom{K}{k}$ ways to choose the k indices $i_1, \dots, i_k$, and so this becomes

$$\begin{aligned}\Psi(F; x, y) &= x + \sum_{1 \leqslant k \leqslant K} (-1)^k \binom{K}{k} x \log^k(du) + O_{F,U}\left(\frac{x}{\log x}\right) \\ &= x(1 - \log du)^K + O_{F,U}\left(\frac{x}{\log x}\right)\end{aligned}$$

by the binomial theorem. But $1 \leqslant du \leqslant 2$ when u is in the range (2.2), and so $\rho(du) = 1 - \log du$ as remarked earlier. Therefore this last equation is equivalent to Eq. (2.15), which establishes Theorem 1.1 for polynomials with integer coefficients that are balanced, effective, admissible, and exclusive. But then by Proposition 2.1, Theorem 1.1 holds for all integer-valued polynomials. ∎

This completes the proof of Theorem 1.1 modulo the proofs of Propositions 2.1 through 2.7 and 2.9, which will be given in the next seven sections. As remarked in the introduction, Theorem 1.2 will be addressed in Section 9, while Appendix A contains mean-value results for multiplicative functions, and Appendix B is devoted to showing that Hypothesis UH in the case of linear polynomials is equivalent to a certain statement concerning the number of primes in short segments of arithmetic progressions.

3. TECHNICAL CONDITIONS ON THE POLYNOMIAL F

Our goal for this section is to establish Proposition 2.1. The idea is to relate the number of smooth values of a given integer-valued polynomial F to the number of smooth values of certain polynomials having the properties in the statement of the proposition. The tricky properties are admissibility and exclusiveness; the other properties are addressed by the following elementary lemma.

Lemma 3.1. *Let $F(t)$ be a nonconstant integer-valued polynomial, let d be the largest of the degrees of the irreducible factors of F, and let k be the number of distinct irreducible factors of F of degree d. Let α be a real number exceeding $d-1$. There exists an effective polynomial $F_1(t)$ with integer coefficients that is the product of k distinct irreducible polynomials of degree d, such that*

$$\Psi(F_1; x, y) = \Psi(F; x, y) + O_{F,\alpha}(1) \tag{3.1}$$

uniformly for $x \geqslant 1$ and $y \geqslant x^{\alpha}$.

Proof. We remark that it suffices to show that Eq. (3.1) holds when x is sufficiently large, by adjusting the constant implicit in the O-notation if necessary. Recall that the *content* of a polynomial F is the greatest common divisor of all of its coefficients (so that a polynomial is primitive precisely when its content equals 1). Since $F(t)$ is integer-valued, the coefficients of F are all rational, so we can choose a positive integer m such that $mF(t)$ has integer coefficients. Write

$$mF(t) = \pm c_0 G_1(t)^{\mu_1} \dots G_k(t)^{\mu_k} H_1(t)^{\nu_1} \dots H_l(t)^{\nu_l}, \tag{3.2}$$

where c_0 is the content of $mF(t)$, the μ_i and v_i are positive integers, and the G_i and H_i are distinct primitive, irreducible polynomials with positive leading coefficients satisfying $\deg G_i = d$ for $1 \leqslant i \leqslant k$ and $\deg H_i \leqslant d-1$ for $1 \leqslant i \leqslant l$.

Set $F_0(t) = G_1(t) \ldots G_k(t)$, so that F_0 is a balanced polynomial with integer coefficients. If $n \leqslant x$ is an integer such that $F(n) \neq 0$, then it is clear from Eq. (3.2) that the largest prime factor p of $F_0(n)$ is the same as the largest prime factor of $F(n)$ provided that p exceeds all prime divisors of $mc_0 H_1(n) \ldots H_l(n)$. In particular, as long as

$$y > \max\{m, c_0, |H_1(n)|, \ldots, |H_l(n)|\}, \tag{3.3}$$

then $F_0(n)$ is y-smooth precisely when $F(n)$ is y-smooth. But $y \geqslant x^\alpha$ and each $H_i(x) \ll_F x^{d-1}$, so we see that the inequality (3.3) always holds when x is sufficiently large (in terms of F and α), since $\alpha > d-1$. Therefore

$$\Psi(F_0; x, y) = \Psi(F; x, y) + O_{F,\alpha}(1), \tag{3.4}$$

the error arising from values of n for which $F(n) = 0$, of which there can be at most $\deg F$.

Now we choose a positive real number $t_0 = t_0(F)$ such that for each $1 \leqslant i \leqslant k$, we have $G_i(t_0) \geqslant 2$ and $G_i'(t) \geqslant 1$ for all $t \geqslant t_0$. If we set $F_1(t) = F_0(t + t_0)$, then F_1 is again a balanced polynomial with integer coefficients, and moreover F_1 is effective by our choice of t_0. Finally, we see that

$$\Psi(F_1; x, y) = \Psi(F_0; x + t_0, y) - \Psi(F_0; t_0, y) = \Psi(F_0; x, y) + O_F(1).$$

This together with Eq. (3.4) establishes the lemma. ∎

To address the properties of admissibility and exclusiveness, we consider the restriction of a polynomial F to an arithmetic progression. If Q is a positive integer and a is any integer, we can use the Taylor expansion of F at a to see that

$$F(Qt + a) = F(a) + QF'(a)\, t + Q^2 \frac{F''(a)}{2} t^2 + \cdots + Q^D \frac{F^{(D)}(a)}{D!} t^D, \tag{3.5}$$

where $D = \deg F$; note that each of the expressions $F^{(j)}(a)/j!$ is an integer. If a is chosen so that Q divides $F(a)$, we see that every coefficient on the right-hand side of (3.5) is divisible by Q, whence $F(Qt + a)/Q$ is a polynomial with integer coefficients.

Even if $f(a)$ is not a multiple of Q, the coefficients of $F(Qt + a)$ might all be divisible by some common factor which we would like to remove. If we divide all of the coefficients of a polynomial F by $\operatorname{cont} F$, we call the resulting polynomial the *primitivization* of F. The following lemma shows that if we consider a polynomial restricted to an arithmetic progression to a suitable modulus, then its primitivization has the desired properties of admissibility and exclusivity.

LEMMA 3.2. *Let F_1 be a squarefree polynomial with integer coefficients, and let D denote the degree of F_1 and Δ the discriminant of F_1. Let Q be a positive integer satisfying:*

- *for all primes $p \leqslant D$, we have $\operatorname{ord}_p(Q) > \operatorname{ord}_p(\Delta)$;*
- *for every pair G_1, H_1 of distinct nonconstant irreducible factors of F_1, and for all primes p dividing their resultant $\operatorname{Res}(G_1, H_1)$, we have $\operatorname{ord}_p(Q) > \operatorname{ord}_p(\operatorname{Res}(G_1, H_1))$.*

Let a be any positive integer, let F_2 denote the polynomial $F_2(t) = F_1(Qt + a)$, and let F_3 denote the primitivization of F_2. Then F_3 is admissible and exclusive.

We remark that it is always possible to find an integer Q satisfying the hypotheses of the lemma when F_1 is squarefree, since this implies that $\Delta \neq 0$ and $\operatorname{Res}(G_1, H_1) \neq 0$ for any two distinct nonconstant irreducible factors G_1 and H_1 of F_1. In fact, the smallest such Q is

$$Q = Q(F_1) = \prod_{p \leqslant D} p^{\operatorname{ord}_p(\Delta)+1} \prod_{\substack{G_1 \neq H_1 \text{ irreducible} \\ G_1 H_1 \mid F_1}} \left(\prod_{p \mid \operatorname{Res}(G_1, H_1)} p^{\operatorname{ord}_p(\operatorname{Res}(G_1, H_1))+1} \right). \tag{3.6}$$

Proof. We shall strive first for admissibility and then for exclusiveness (as if we were climbing the social ladder). If p is a prime greater than D, then the primitivization F_3 of F_2 is not the zero polynomial (mod p), since any primitive polynomial has at least one nonzero coefficient modulo every prime; and in fact F_3 has degree at most D. Therefore F_3 has at most D zeros (mod p), and so takes at least one nonzero value (mod p).

If p is a prime not exceeding D, then from the identity (3.5) applied to F_1, we see that the content of F_2 is

$$\operatorname{cont}(F_2) = \gcd\left\{ F_1(a), QF_1'(a), Q^2 \frac{F_1''(a)}{2}, \cdots, Q^D \frac{F_1^{(D)}(a)}{D!} \right\}.$$

Thus for any prime p,

$$\operatorname{ord}_p(\operatorname{cont}(F_2)) = \min\left\{ \operatorname{ord}_p(F_1(a)), \operatorname{ord}_p(Q) + \operatorname{ord}_p(F_1'(a)), \right.$$

$$\left. 2\operatorname{ord}_p(Q) + \operatorname{ord}_p\left(\frac{F_1''(a)}{2}\right), \cdots, D\operatorname{ord}_p(Q) + \operatorname{ord}_p\left(\frac{F_1^{(D)}(a)}{D!}\right) \right\}, \tag{3.7}$$

where all of the terms of the form $\mathrm{ord}_p(\cdot)$ are nonnegative since the quantities involved are all integers. By general properties of the discriminant of a polynomial, we know that if p^ν divides both $F_1(a)$ and $F_1'(a)$, then p^ν divides Δ. Put another way,

$$\min\{\mathrm{ord}_p(F_1(a)), \mathrm{ord}_p(F_1'(a))\} \leqslant \mathrm{ord}_p(\Delta) < \mathrm{ord}_p(Q),$$

where the last inequality is one of our hypotheses on Q. In particular, one of the first two terms on the right-hand side of Eq. (3.7) is less than $2\,\mathrm{ord}_p(Q)$, and hence Eq. (3.7) can be simplified to

$$\mathrm{ord}_p(\mathrm{cont}(F_2)) = \min\{\mathrm{ord}_p(F_1(a)), \mathrm{ord}_p(Q) + \mathrm{ord}_p(F_1'(a))\}. \tag{3.8}$$

If $\mathrm{ord}_p(F_1(a)) \leqslant \mathrm{ord}_p(Q) + \mathrm{ord}_p(F_1'(a))$, then $\mathrm{cont}(F_2) = bp^{\mathrm{ord}_p(F_1(a))}$ for some integer b that is not divisible by p, and so

$$F_3(0) = \frac{F_2(0)}{bp^{\mathrm{ord}_p(F_1(a))}} \equiv b^{-1} \frac{F_1(a)}{p^{\mathrm{ord}_p(F_1(a))}} \not\equiv 0 \pmod p.$$

On the other hand, if $\mathrm{ord}_p(F_1(a)) > \mathrm{ord}_p(Q) + \mathrm{ord}_p(F_1'(a))$, then $\mathrm{cont}(F_2) = bp^{\mathrm{ord}_p(Q)+\mathrm{ord}_p(F_1'(a))}$ for some integer b that is not divisible by p, and so

$$F_3(1) = \frac{F_2(1)}{bp^{\mathrm{ord}_p(Q)+\mathrm{ord}_p(F_1'(a))}} \equiv b^{-1} \frac{QF_1'(a)}{p^{\mathrm{ord}_p(QF_1'(a))}} \not\equiv 0 \pmod p.$$

In either case we see that F_3 takes a nonzero value (mod p), and so F_3 is admissible.

To show that F_3 is exclusive we want to show, given two distinct irreducible factors G_3 and H_3 of F_3, that G_3 and H_3 have no common zeros modulo any prime. Note that any irreducible factor G_3 of F_3 is the primitivization of an irreducible factor G_2 of F_2, by Gauss' lemma on the contents of polynomials with integer coefficients; and any irreducible factor G_2 of F_2 has the form $G_2(t) = G_1(Qt+a)$ for some irreducible factor G_1 of F_1. Similarly, there is an irreducible factor H_1 of F_1 such that H_3 is the primitivization of $H_2(t) = H_1(Qt+a)$. If p is a prime not dividing $\mathrm{Res}(G_1, H_1)$, then G_1 and H_1 have no common zeros (mod p) by general properties of the resultant of two polynomials, whence the same is clearly true for G_2 and H_2 and thus for G_3 and H_3; so it suffices to consider the case where p divides $\mathrm{Res}(G_1, H_1)$.

Again, by general properties of the resultant of two polynomials, we know that if p^ν divides both $G_1(a)$ and $H_1(a)$, then p^ν divides $\mathrm{Res}(G_1, H_1)$. Put another way,

$$\min\{\mathrm{ord}_p(G_1(a)), \mathrm{ord}_p(H_1(a))\} \leqslant \mathrm{ord}_p(\mathrm{Res}(G_1, H_1)).$$

By exchanging the Gs and Hs if necessary, we can assume without loss of generality that

$$\operatorname{ord}_p(G_1(a)) \leqslant \operatorname{ord}_p(\operatorname{Res}(G_1, H_1)) < \operatorname{ord}_p(Q), \tag{3.9}$$

where the last inequality is another of our hypotheses on Q. From the equation analogous to (3.7) for G_2, we see that the inequality (3.9) implies that $\operatorname{ord}_p(\operatorname{cont}(G_2)) = \operatorname{ord}_p(G_1(a))$. Therefore $\operatorname{cont}(G_2) = bp^{\operatorname{ord}_p(G_1(a))}$ for some integer b that is not divisible by p, and so

$$G_3(n) = \frac{G_2(n)}{bp^{\operatorname{ord}_p(G_1(a))}} \equiv b^{-1} \frac{G_1(a)}{p^{\operatorname{ord}_p(G_1(a))}} \not\equiv 0 \pmod p$$

independent of n, so that G_3 has no zeros (mod p) whatsoever. Hence certainly G_3 and H_3 have no common zeros (mod p), which shows that F_3 is exclusive. ∎

With these two lemmas in hand we can now establish Proposition 2.1, which we restate here for the reader's convenience.

PROPOSITION 2.1. *Suppose that Theorem* 1.1 *holds for any polynomial with integer coefficients that is balanced, effective, admissible, and exclusive. Then it holds for any integer-valued polynomial.*

Proof. Let F be an integer-valued polynomial, let K be the number of distinct irreducible factors of F, and let $d_1, \ldots, d_K$ be the degrees of these factors. Let $d = \max\{d_1, \ldots, d_K\}$, and let k be the number of distinct irreducible factors of F whose degree equals d. Let u and U be real numbers satisfying $1/d \leqslant u \leqslant U < (d - 1/k)^{-1}$; let $x \geqslant 1$ be a real number and set $y = x^{1/u}$. We are trying to show that the asymptotic formula (1.7) holds. If $d_j \leqslant d - 1$ then $d_j u < (d-1)(d-1/k)^{-1} \leqslant 1$, in which case $\rho(d_j u) = 1$. Thus we are trying to prove that

$$\Psi(F; x, x^{1/u}) = x\rho(du)^k + O\left(\frac{x}{\log x}\right) \tag{3.10}$$

holds uniformly for $x \geqslant 1$ and $0 < u \leqslant U$, where here and throughout this proof, all constants implicit in O-notation may depend on F and U. Notice that $y \geqslant x^{\alpha}$ where $\alpha = 1/U > d - 1/k \geqslant d - 1$. Therefore, by Lemma 3.1 we can find an effective polynomial $F_1(t)$ with integer coefficients that is the product of k distinct irreducible polynomials of degree d, such that

$$\Psi(F_1; x, y) = \Psi(F; x, y) + O(1). \tag{3.11}$$

Let $Q = Q(F_1)$ be the integer given by Eq. (3.6), so that Q satisfies the hypotheses of Lemma 3.2. For each fixed integer $0 \leqslant a < Q$, define the polynomial $F_2(a; t) = F_1(Qt+a)$, and let $F_3(a; t)$ be the primitivization of $F_2(a; t)$. Each of these polynomials $F_3(a; t)$ has integer coefficients, and is balanced and effective because F_1 is. Moreover, by Lemma 3.2 each $F_3(a; t)$ is admissible and exclusive as well. By the hypothesis of the proposition to be proved, we know that Theorem 1.1 holds for each $F_3(a; t)$. Therefore (assuming Hypothesis UH) we have

$$\Psi(F_3(a; t); x, x^{1/u}) = x\rho(du)^k + O\left(\frac{x}{\log x}\right), \tag{3.12}$$

since each $F_3(a; t)$, like F_1, is the product of k distinct irreducible polynomials of degree d.

On the other hand, every integer $1 \leqslant n \leqslant x$ is congruent (mod Q) to some integer $0 \leqslant a < Q$, and so every value $F_1(n)$ for $1 \leqslant n \leqslant x$ corresponds to a value $F_2(a; m)$ for some $0 \leqslant m < (x-a)/Q$. Furthermore, the corresponding value $F_3(a; m)$ simply equals $F_2(a; m)/\mathrm{cont}(F_2)$, a difference which does not affect whether the value is $x^{1/u}$-smooth as soon as x exceeds $\mathrm{cont}(F_2)^U$. Therefore, when x is sufficiently large in terms of F, we have

$$\begin{aligned}\Psi(F_1; x, x^{1/u}) &= \sum_{0 \leqslant a < Q} \Psi\left(F_3(a; t); \frac{x-a}{Q}, x^{1/u}\right) \\ &= \sum_{0 \leqslant a < Q} \Psi\left(F_3(a; t); \frac{x-a}{Q}, \left(\frac{x-a}{Q}\right)^{1/u_a}\right),\end{aligned} \tag{3.13}$$

where

$$u_a = \frac{u \log((x-a)/Q)}{\log x} = u + O\left(\frac{1}{\log x}\right).$$

The function $\rho(u)$ satisfies $-1 < \rho'(u) < 0$ for all $u > 1$, and so $\rho(du_a) = \rho(du) + O(1/\log x)$. Using the asymptotic formula (3.12) in Eq. (3.13), we conclude that

$$\begin{aligned}\Psi(F_1; x, x^{1/u}) &= \sum_{0 \leqslant a < Q} \left(\frac{x-a}{Q} \rho(du_a)^k + O\left(\frac{x}{\log x}\right)\right) \\ &= \sum_{0 \leqslant a < Q} \left(\frac{x-a}{Q} \left(\rho(du) + O\left(\frac{1}{\log x}\right)\right)^k\right) + O\left(\frac{x}{\log x}\right) \\ &= x\rho(du)^k + O\left(\frac{x}{\log x}\right).\end{aligned}$$

Together with Eq. (3.11), this shows that the asymptotic formula (3.10) holds for the original polynomial F, which establishes the proposition. ∎

4. TWO COMBINATORIAL PROPOSITIONS

In this section we establish the combinatorial Propositions 2.2 and 2.3, which link the counting function of smooth values of a polynomial to the counting functions of prime values of a related family of polynomials, via the expressions $M(f; x, y)$ defined in Eq. (2.1). The first of these two propositions exhibits $\Psi(F; x, y)$ as a combination of terms of the form $M(f; x, y)$.

PROPOSITION 2.2. *Let F be a primitive polynomial, and let $F_1, \ldots, F_K$ denote the distinct irreducible factors of F. Then for any real numbers $x \geqslant y \geqslant 1$,*

$$\Psi(F; x, y) = \lfloor x \rfloor + \sum_{1 \leqslant k \leqslant K} (-1)^k \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant K} M(F_{i_1} \ldots F_{i_k}; x, y).$$

Proof. This is simply inclusion–exclusion on the factors of F that, for a given argument n, have large prime divisors. For any integer n define

$$X_i(n) = \begin{cases} 1, & \text{if there exists a prime } p > y \text{ dividing } F_i(n), \\ 0, & \text{otherwise (i.e., if } F_i(n) \text{ is } y\text{-smooth).} \end{cases} \tag{4.1}$$

Then for any nonempty subset S of $\{1, \ldots, K\}$, the definition (2.1) of $M(f; x, y)$ for $f = \prod_{i \in S} F_i$ is equivalent to

$$M\left(\left(\prod_{i \in S} F_i\right); x, y\right) = \sum_{n \leqslant x} \left(\prod_{i \in S} X_i(n)\right).$$

But the definition (4.1) also implies that

$$\prod_{i=1}^{K} (1 - X_i(n)) = \begin{cases} 1, & \text{if } F(n) \text{ is } y\text{-smooth,} \\ 0, & \text{otherwise,} \end{cases}$$

since $F(n)$ is y-smooth if and only if each $F_i(n)$ is y-smooth. We therefore find that

$$\Psi(F; x, y) = \sum_{n \leqslant x} \prod_{i=1}^{K} (1 - X_i(n)) = \lfloor x \rfloor + \sum_{n \leqslant x} \sum_{\substack{S \subset \{1, \ldots, K\} \\ S \neq \varnothing}} \prod_{i \in S} (-X_i(n))$$

$$= \lfloor x \rfloor + \sum_{1 \leqslant k \leqslant K} (-1)^k \sum_{\substack{S \subset \{1, \ldots, K\} \\ |S| = k}} M\left(\left(\prod_{i \in S} F_i\right); x, y\right),$$

which is equivalent to the statement of the proposition. ∎

The second of these two propositions exhibits $M(f; x, y)$ as a combination of terms of the form $\pi(f_{h_1\dots h_k, b}, \cdot)$. All of the notation introduced in Section 2 will be assumed for the remainder of this section. We also need to define, for any positive integers $h_1, \dots, h_k$ and any element b of $\mathscr{R}(f; h_1, \dots, h_k)$, the polynomial

$$f^{(i)}_{h_1, \dots, h_k; b}(t) = \frac{f_i(h_1 \dots h_k t + b)}{h_i} \tag{4.2}$$

for each $1 \leqslant i \leqslant k$. The fact that h_i divides each $f_i(b)$ implies, by the Taylor expansion (3.5) applied to f_i, that each $f^{(i)}_{h_1, \dots, h_k; b}$ has integer coefficients. Because of this, the polynomial $f_{h_1\dots h_k, b}$ has the natural factorization $f_{h_1\dots h_k, b} = f^{(1)}_{h_1, \dots, h_k; b} \cdots f^{(k)}_{h_1, \dots, h_k; b}$ into irreducible polynomials.

Proposition 2.3. *Let f be a polynomial that is balanced, effective, primitive, and exclusive. Then when x is sufficiently large we have*

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \dots, h_k)} \left(\pi\left(f_{h_1\dots h_k, b}; \frac{x-b}{h_1 \dots h_k} \right) - \pi(f_{h_1\dots h_k, b}; \eta_{h_1, \dots, h_k}) \right) \tag{4.3}$$

for certain quantities $\eta_{h_1, \dots, h_k}$ that satisfy $\eta_{h_1, \dots, h_k} \asymp (y \max\{h_1, \dots, h_k\})^{1/d} \times (h_1 \dots h_k)^{-1}$.

Proof. We recall the definition (2.1) of $M(f; x, y)$:

$$M(f; x, y) = \#\{1 \leqslant n \leqslant x : \text{for each irreducible factor } g \text{ of } f, \text{ there exists a prime } p > y \text{ such that } p \mid g(n)\}.$$

Since $y \geqslant \sqrt{\xi_i}$ for each i when x is sufficiently large, there is a unique k-tuple $(p_1, \dots, p_k)$ of primes for each argument n that is counted by $M(f; x, y)$. If we write the values $f_i(n)$ as $p_i h_i$ for suitable integers h_i, we see that

$$\begin{aligned} M(f; x, y) &= \#\{(n, p_1, \dots, p_k, h_1, \dots, h_k) : 1 \leqslant n \leqslant x, \\ &\qquad \text{each } p_i > y, \text{ each } f_i(n) = p_i h_i\} \\ &= \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} \#\{1 \leqslant n \leqslant x : \\ &\qquad \text{each } h_i \mid f_i(n), \text{ each } f_i(n)/h_i \text{ is a prime exceeding } y\}. \end{aligned}$$

Because f is exclusive, no prime can divide two different values $f_i(n)$ at the same argument n; therefore, we may insert the condition of summation $(h_i, h_j) = 1$ $(1 \leqslant i < j \leqslant k)$ without changing the sum. Furthermore, if h_i divides $f_i(n)$ for each i, then n is congruent to some element b of $\mathscr{R}(f; h_1, \ldots, h_k)$ by its definition (2.3), and conversely. Therefore

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} \#\{1 \leqslant n \leqslant x, n \equiv b \pmod{h_1 \ldots h_k} : \text{each } f_i(n)/h_i \text{ is a prime exceeding } y\}.$$

Making the change of variables $n = h_1 \ldots h_k m + b$, we see that

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} \#\left\{0 \leqslant m \leqslant \frac{x-b}{h_1 \ldots h_k} : \text{each } f_i(h_1 \ldots h_k m + b)/h_i \text{ is a prime exceeding } y\right\}$$

$$= \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} \#\left\{0 \leqslant m \leqslant \frac{x-b}{h_1 \ldots h_k} : \text{each } f^{(i)}_{h_1, \ldots, h_k; b}(m) \text{ is a prime exceeding } y\right\}$$

by the definition (4.2) of the $f^{(i)}_{h_1, \ldots, h_k; b}$. The polynomial f is effective and hence strictly increasing for $t \geqslant 0$, so if we define $\eta_{h_1, \ldots, h_k}$ to be the smallest real number η such that $f^{(i)}_{h_1, \ldots, h_k; b}(\eta) \geqslant y$ for each i, then we see that

$$M(f; x, y) = \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} \left(\pi\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right) - \pi(f_{h_1 \ldots h_k, b}; \eta_{h_1, \ldots, h_k})\right).$$

As for the size of $\eta_{h_1, \ldots, h_k}$, we see from the definition (4.2) of $f^{(i)}_{h_1, \ldots, h_k; b}$ that

$$(f^{(i)}_{h_1, \ldots, h_k; b})^{-1}(y) = \frac{f_i^{-1}(h_i y) - b}{h_1 \ldots h_k} \asymp \frac{(h_i y)^{1/d}}{h_1 \ldots h_k}$$

since each f_i has degree d, and so $\eta_{h_1, \ldots, h_k} \asymp (y \max\{h_1 \ldots h_k\})^{1/d} (h_1 \ldots h_k)^{-1}$. This establishes the proposition. ∎

5. ROOTS OF POLYNOMIALS MODULO INTEGERS

The object of this section is to establish Proposition 2.5. The tools we shall need are relationships between the number of local roots of polynomials of the form $f_{h_1 \dots h_k, b}$, defined in Eq. (2.4), and the number of local roots of the polynomial f itself. For the first part of this section, we make no particular assumption on the polynomial f except that it has integer coefficients. For any positive integer h we define

$$\mathscr{R}(f; h) = \{1 \leqslant b \leqslant h : h \mid f(b)\}, \tag{5.1}$$

analogous to the definition (2.3) of $\mathscr{R}(f; h_1, \dots, h_k)$. For any integer b that is congruent (mod h) to some element of $\mathscr{R}(f; h)$, we define the polynomial $f_{h,b}$ by $f_{h,b}(t) = f(ht+b)/h$, consistent with the notation $f_{h_1 \dots h_k, b}$ defined in Eq. (2.4).

We recall that $\sigma(f; h)$ denotes the number of solutions of $f(b) \equiv 0 \pmod{h}$, or simply the cardinality of $\mathscr{R}(f; h)$. Clearly σ is a nonnegative, integer-valued function satisfying $\sigma(f; h) \leqslant h$ for all positive integers h. Also, if m and n are relatively prime positive integers, then by the Chinese remainder theorem there is a bijection between roots of $f \pmod{mn}$ and pairs of roots of $f \pmod{m}$ and $\pmod{n}$; this implies that $\sigma(f; h)$ is a multiplicative function of h.

The following four lemmas exhibit simple relationships between values of $\sigma(f_{h,b})$ and values of $\sigma(f)$.

Lemma 5.1. *Let f be a polynomial with integer coefficients, let h be a positive integer, and let b be an element of $\mathscr{R}(f; h)$. If a prime p does not divide h, then $\sigma(f_{h,b}; p) = \sigma(f; p)$.*

Proof. By definition,

$$\begin{aligned} \sigma(f_{h,b}; p) &= \#\{a \pmod{p} : f_{h,b}(a) \equiv 0 \pmod{p}\} \\ &= \#\left\{a \pmod{p} : \frac{f(ha+b)}{h} \equiv 0 \pmod{p}\right\}. \end{aligned} \tag{5.2}$$

Since p does not divide h, we may multiply both sides of the latter congruence by h. Then making the bijective change of variables $a' \equiv ha + b \pmod{p}$, we see that

$$\sigma(f_{h,b}; p) = \#\{a' \pmod{p} : f(a') \equiv 0 \pmod{p}\} = \sigma(f; p),$$

as claimed. ∎

LEMMA 5.2. *Let f be a polynomial with integer coefficients, let h be a positive integer, and let b and b' be integers with $f(b) \equiv f(b') \equiv 0 \pmod{h}$. If $b \equiv b' \pmod{h}$ then $\sigma(f_{h,b}; p) = \sigma(f_{h,b'}; p)$.*

Proof. Write $b = b' + hq$ for some integer q. Making the bijective change of variables $a' \equiv a + q \pmod{p}$ in the latter congruence in Eq. (5.2), we see that

$$\sigma(f_{h,b}; p) = \#\left\{a' \pmod{p} : \frac{f(ha'+b')}{h} \equiv 0 \pmod{p}\right\} = \sigma(f_{h,b'}; p),$$

as claimed. ∎

LEMMA 5.3. *Let f be a polynomial with integer coefficients, let h be a positive integer, and let b be an element of $\mathscr{R}(f; h)$. If a prime power p^ν exactly divides h, then $\sigma(f_{h,b}; p) = \sigma(f_{p^\nu,b}; p)$.*

Proof. Write $h = p^\nu h'$ for some integer h'. Since p does not divide h', we may multiply both sides of the latter congruence in Eq. (5.2) by h'. Then making the bijective change of variables $a' \equiv h'a \pmod{p}$, we see that

$$\sigma(f_{h,b}; p) = \#\left\{a' \pmod{p} : \frac{f(p^\nu a'+b)}{p^\nu} \equiv 0 \pmod{p}\right\} = \sigma(f_{p^\nu,b}; p),$$

as claimed. ∎

LEMMA 5.4. *Let f be a polynomial with integer coefficients and let h and n be positive integers. Then $\sum_{b \in \mathscr{R}(f;h)} \sigma(f_{h,b}; n) = \sigma(f; nh)$.*

Proof. By definition,

$$\begin{aligned}\sigma(f_{h,b}; n) &= \#\{a \pmod{n} : f_{h,b}(a) \equiv 0 \pmod{n}\}\\ &= \#\{a \pmod{n} : f(ha+b)/h \equiv 0 \pmod{n}\}\\ &= \#\{a \pmod{n} : f(ha+b) \equiv 0 \pmod{nh}\} \qquad (5.3)\\ &= \#\{c \pmod{nh},\ c \equiv b \pmod{h} : f(c) \equiv 0 \pmod{nh}\}\\ &= \#\{c \in \mathscr{R}(f; nh) : c \equiv b \pmod{h}\}.\end{aligned}$$

Now every root of $f \pmod{nh}$ is certainly a root of $f \pmod{h}$, and so it follows that every $c \in \mathscr{R}(f; nh)$ is congruent to some $b \in \mathscr{R}(f; h)$. Therefore

$$\begin{aligned}\sigma(f; nh) = \#\{c \in \mathscr{R}(f; nh)\} &= \sum_{b \in \mathscr{R}(f;h)} \#\{c \in \mathscr{R}(f; nh) : c \equiv b \pmod{h}\}\\ &= \sum_{b \in \mathscr{R}(f;h)} \sigma(f_{h,b}; n)\end{aligned}$$

from the last line of Eq. (5.3), which establishes the lemma. ∎

We remark that the last line in Eq. (5.3) shows that the quantity $\sigma(f_{h,b}; n)$ can be interpreted as the number of "lifts" of the root b of f (mod h) to roots of f (mod nh). Also, since the inequality $\sigma(f; n) \leqslant n$ is trivial for any polynomial f, we see from Lemma 5.4 that

$$\sigma(f; nh) = \sum_{b \in \mathscr{R}(f;h)} \sigma(f_{h,b}; n) \leqslant \sum_{b \in \mathscr{R}(f;h)} n = n\sigma(f; h). \tag{5.4}$$

Next we recall the definition (2.6) of the multiplicative function $\sigma^*(f; n)$,

$$\sigma^*(f; n) = \prod_{p^\nu \parallel n} \left(\sigma(f; p^\nu) - \frac{\sigma(f; p^{\nu+1})}{p} \right),$$

and establish some of its properties. First, we may put $h = p^\nu$ and $n = p$ in Eq. (5.4) to see that

$$\sigma^*(f; p^\nu) = \sigma(f; p^\nu) - \frac{\sigma(f; p^{\nu+1})}{p} \geqslant \sigma(f; p^\nu) - \frac{p\sigma(f; p^\nu)}{p} = 0. \tag{5.5}$$

This shows that σ^* is always nonnegative. Next we give an alternate characterization (and in fact the reason for existence) of the quantity $\sigma^*(f; h)$. The following lemma provides the key fact needed for the proof of Proposition 2.5.

LEMMA 5.5. *For any polynomial f with integer coefficients and any positive integer h,*

$$\sum_{b \in \mathscr{R}(f;h)} \prod_{p \mid h} \left(1 - \frac{\sigma(f_{h;b}; p)}{p} \right) = \sigma^*(f; h).$$

Proof. Factor $h = p_1^{\nu_1} \dots p_l^{\nu_l}$ into powers of distinct primes. We first note that by Lemma 5.3,

$$\begin{aligned} \sum_{b \in \mathscr{R}(f;h)} \prod_{p \mid h} \left(1 - \frac{\sigma(f_{h;b}; p)}{p} \right) &= \sum_{b \in \mathscr{R}(f;h)} \prod_{p^\nu \parallel h} \left(1 - \frac{\sigma(f_{p^\nu,b}; p)}{p} \right) \\ &= \sum_{b \in \mathscr{R}(f;h)} \prod_{i=1}^{l} \left(1 - \frac{\sigma(f_{p_i^{\nu_i},b}; p_i)}{p_i} \right). \end{aligned}$$

For every l-tuple $(b_1, \dots, b_l)$ such that each $b_i \in \mathscr{R}(f; p_i^{\nu_i})$, the Chinese Remainder Theorem gives us a $b \in \mathscr{R}(f; h)$ such that $b \equiv b_i \pmod{p_i^{\nu_i}}$ for each $1 \leqslant i \leqslant l$, and this correspondence is bijective. Therefore

$$\sum_{b \in \mathscr{R}(f;h)} \prod_{i=1}^{l} \left(1 - \frac{\sigma(f_{p_i^{\nu_i},b}; p_i)}{p_i} \right) = \sum_{\substack{(b_1, \dots, b_l) \\ b_i \in \mathscr{R}(f; p_i^{\nu_i})}} \prod_{i=1}^{l} \left(1 - \frac{\sigma(f_{p_i^{\nu_i},b_i}; p_i)}{p_i} \right),$$

since $\sigma(f_{p_i^{\nu_i},b};p_i)$ only depends on $b \pmod{p_i^{\nu_i}}$ by Lemma 5.2. This last sum now factors:

$$\begin{aligned}
&\sum_{\substack{(b_1,\ldots,b_l)\\ b_i\in\mathscr{R}(f;p_i^{\nu_i})}}\prod_{i=1}^{l}\left(1-\frac{\sigma(f_{p_i^{\nu_i},b_i};p_i)}{p_i}\right)\\
&\quad=\prod_{i=1}^{l}\sum_{b_i\in\mathscr{R}(f;p_i^{\nu_i})}\left(1-\frac{\sigma(f_{p_i^{\nu_i},b_i};p_i)}{p_i}\right)\\
&\quad=\prod_{i=1}^{l}\left(\sum_{b_i\in\mathscr{R}(f;p_i^{\nu_i})}1-\frac{1}{p_i}\sum_{b_i\in\mathscr{R}(f;p_i^{\nu_i})}\sigma(f_{p_i^{\nu_i},b_i};p_i)\right)\\
&\quad=\prod_{i=1}^{l}\left(\sigma(f;p_i^{\nu_i})-\frac{\sigma(f;p_i^{\nu_i+1})}{p_i}\right)
\end{aligned}\tag{5.6}$$

by the definition of σ and by Lemma 5.4 with $h=p_i^{\nu_i}$ and $n=p_i$. Since the last expression of Eq. (5.6) is just $\prod_{i=1}^{l}\sigma^*(f;p_i^{\nu_i})=\sigma^*(f;h)$, the lemma is established. ▌

For the remainder of this section, we specialize to the case where f is a primitive, balanced polynomial with integer coefficients, and we let k denote the number of distinct irreducible factors of f. We also recall the definitions (1.2), (2.3), and (2.7) of $\mathrm{li}(F;x)$, $\mathscr{R}(f;h_1,\ldots,h_k)$, and $\mathrm{li}_{h_1,\ldots,h_k}(f;x)$, respectively.

LEMMA 5.6. *Let f be a polynomial that is effective, primitive, and balanced. For any positive integers $h_1,\ldots,h_k$ and any $b\in\mathscr{R}(f;h_1,\ldots,h_k)$, we have*

$$\mathrm{li}\left(f_{h_1\ldots h_k,b};\frac{x-b}{h_1\ldots h_k}\right)=\frac{\mathrm{li}_{h_1,\ldots,h_k}(f;x)}{h_1\ldots h_k}+O_f(1)$$

uniformly for $x\geqslant 1$.

Proof. From the definition (1.2) of $\mathrm{li}(F,x)$, we see that

$$\begin{aligned}
&\mathrm{li}\left(f_{h_1\ldots h_k,b};\frac{x-b}{h_1\ldots h_k}\right)\\
&\quad=\int_{\substack{0<t\leqslant(x-b)/h_1\ldots h_k\\ \min\{f^{(1)}_{h_1,\ldots,h_k;b}(t),\ldots,f^{(k)}_{h_1,\ldots,h_k;b}(t)\}\geqslant 2}}\frac{dt}{\log f^{(1)}_{h_1,\ldots,h_k;b}(t)\ldots\log f^{(k)}_{h_1,\ldots,h_k;b}(t)}\\
&\quad=\frac{1}{h_1\ldots h_k}\int_{\substack{b<v\leqslant x\\ \min\{f_1(v)/h_1,\ldots,f_k(v)/h_k\}\geqslant 2}}\frac{dv}{\log(f_1(v)/h_1)\ldots\log(f_k(v)/h_k)}
\end{aligned}$$

by the change of variables $v = h_1 \dots h_k t + b$. We may change the lower limit of integration from b to 0, incurring an error that is $\leqslant b(\log 2)^{-k} \ll_f b \leqslant h_1 \dots h_k$. Therefore

$$\mathrm{li}\left(f_{h_1 \dots h_k, b}; \frac{x-b}{h_1 \dots h_k}\right) = \frac{\mathrm{li}_{h_1, \dots, h_k}(f; x)}{h_1 \dots h_k} + O_f(1)$$

as claimed. ▮

We have one more lemma to establish before we can prove Proposition 2.5, and for this lemma we must define one more piece of notation. To avoid double subscripts such as $(f_i)_{h,b}$, we define the polynomial $f^{(i)}_{h,b}$ by $f^{(i)}_{h,b}(t) = f_i(ht+b)/h$, which as before has integer coefficients if h divides $f_i(b)$; this is to be distinguished from the polynomial $f^{(i)}_{h_1, \dots, h_k; b}$, which still corresponds to its definition (4.2).

LEMMA 5.7. *Let f be a polynomial with integer coefficients that is primitive, balanced, and exclusive; let $h_1, \dots, h_k$ be pairwise coprime positive integers and let b be an element of $\mathcal{R}(f; h_1, \dots, h_k)$. If a prime p divides h_i for some $1 \leqslant i \leqslant k$, then $\sigma(f_{h_1 \dots h_k, b}; p) = \sigma(f^{(i)}_{h_i, b}; p)$.*

Proof. By the definition of σ, and using the remark following Eq. (4.2) to factor the polynomial $f_{h_1 \dots h_k, b}$, we have

$$\begin{aligned} \sigma(f_{h_1 \dots h_k, b}; p) &= \#\{a \ (\mathrm{mod}\ p) : f_{h_1 \dots h_k, b}(a) \equiv 0 \ (\mathrm{mod}\ p)\} \\ &= \#\{a \ (\mathrm{mod}\ p) : f^{(1)}_{h_1, \dots, h_k; b}(a) \dots f^{(k)}_{h_1, \dots, h_k; b}(a) \equiv 0 \ (\mathrm{mod}\ p)\} \\ &= \#\left\{a \ (\mathrm{mod}\ p) : \prod_{j=1}^{k} \frac{f_j(h_1 \dots h_k a + b)}{h_j} \equiv 0 \ (\mathrm{mod}\ p)\right\}. \end{aligned} \tag{5.7}$$

Since the h_j are pairwise coprime, p does not divide any of the h_j other than h_i. Also, since b is a root of $f_i \ (\mathrm{mod}\ p)$ and f is exclusive, b cannot be a root of any other $f_j \ (\mathrm{mod}\ p)$. Therefore, since $h_i \equiv 0 \ (\mathrm{mod}\ p)$, we see that $f_j(h_1 \dots h_k a + b) \equiv f_j(b) \not\equiv 0 \ (\mathrm{mod}\ p)$ for all $j \neq i$.

We may therefore divide the congruence in Eq. (5.7) by $f_j(h_1 \dots h_k a + b)/h_j$ for each $j \neq i$ and make the change of variables $a' = h_1 \dots h_{i-1} h_{i+1} \dots h_k a$ to obtain

$$\begin{aligned} \sigma(f_{h_1 \dots h_k, b}; p) &= \#\left\{a' \ (\mathrm{mod}\ p) : \frac{f_i(h_i a' + b)}{h_i} \equiv 0 \ (\mathrm{mod}\ p)\right\} \\ &= \#\{a' \ (\mathrm{mod}\ p) : f^{(i)}_{h_i, b}(a') \equiv 0 \ (\mathrm{mod}\ p)\} = \sigma(f^{(i)}_{h_i, b}; p), \end{aligned}$$

which establishes the lemma. ▮

Armed with these several lemmas, we are now ready to establish:

PROPOSITION 2.5. *Let f be a polynomial that is balanced, effective, admissible, and exclusive, and let $h_1, \ldots, h_k$ be pairwise coprime positive integers. Then*

$$\sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}) \operatorname{li}\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right)$$
$$= \frac{C(f)\, G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k) \operatorname{li}_{h_1, \ldots, h_k}(f; x)}{h_1 \ldots h_k}$$
$$+ O_f(G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)) \tag{5.8}$$

uniformly for $x \geqslant 1$.

Proof. By Lemma 5.6 we can write

$$\sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}) \operatorname{li}\left(f_{h_1 \ldots h_k, b}; \frac{x-b}{h_1 \ldots h_k}\right)$$
$$= \left(\frac{\operatorname{li}_{h_1, \ldots, h_k}(f; x)}{h_1 \ldots h_k} + O_f(1)\right) \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}).$$

Thus to establish the lemma, it suffices to show that

$$\sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b}) = C(f)\, G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k). \tag{5.9}$$

If p is a prime that does not divide $h_1 \ldots h_k$, then we know that $\sigma(f_{h_1, \ldots, h_k; b}; p) = \sigma(f; p)$ by Lemma 5.1. Thus

$$\sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b})$$
$$= \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\sigma(f_{h_1 \ldots h_k, b}; p)}{p}\right)$$
$$= \prod_p \left(1 - \frac{1}{p}\right)^{-k} \left(1 - \frac{\sigma(f; p)}{p}\right) \prod_{p \mid h_1 \ldots h_k} \left(1 - \frac{\sigma(f; p)}{p}\right)^{-1}$$
$$\times \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \prod_{p \mid h_1 \ldots h_k} \left(1 - \frac{\sigma(f_{h_1 \ldots h_k, b}; p)}{p}\right)$$
$$= C(f)\, G(f; h_1 \ldots h_k) \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \prod_{i=1}^{k} \prod_{p \mid h_i} \left(1 - \frac{\sigma(f^{(i)}_{h_i, b}; p)}{p}\right),$$

where we have used Lemma 5.7 to change $\sigma(f_{h_1\dots h_k,b})$ to the $\sigma(f^{(i)}_{h_i,b})$ in the last equality. All that remains to establish Eq. (5.9), and hence the proposition, is to show that

$$\sum_{b\in\mathscr{R}(f;h_1,\dots,h_k)} \prod_{i=1}^{k} \prod_{p\mid h_i} \left(1-\frac{\sigma(f^{(i)}_{h_i,b};p)}{p}\right) = \sigma^*(f_1;h_1)\dots\sigma^*(f_k;h_k). \tag{5.10}$$

For every k-tuple $(b_1, \dots, b_k)$ such that each $b_i \in \mathscr{R}(f_i; h_i)$, the Chinese remainder theorem gives us a $b \in \mathscr{R}(f; h_1, \dots, h_k)$ such that $b \equiv b_i \pmod{h_i}$ for each $1 \leqslant i \leqslant k$, and this correspondence is bijective. Therefore

$$\sum_{b\in\mathscr{R}(f;h_1,\dots,h_k)} \prod_{i=1}^{k} \prod_{p\mid h_i} \left(1-\frac{\sigma(f^{(i)}_{h_i,b};p)}{p}\right) = \sum_{\substack{(b_1,\dots,b_k)\\ b_i\in\mathscr{R}(f_i;h_i)}} \prod_{i=1}^{k} \prod_{p\mid h_i} \left(1-\frac{\sigma(f^{(i)}_{h_i,b_i};p)}{p}\right),$$

since for a given prime p the quantity $\sigma(f^{(i)}_{h_i,b};p)$ depends only on $b \pmod{h_i}$ by Lemma 5.2. This last sum now factors as

$$\begin{aligned}\sum_{\substack{(b_1,\dots,b_k)\\ b_i\in\mathscr{R}(f_i;h_i)}} \prod_{i=1}^{k} \prod_{p\mid h_i} \left(1-\frac{\sigma(f^{(i)}_{h_i,b_i};p)}{p}\right) &= \prod_{i=1}^{k} \sum_{b_i\in\mathscr{R}(f_i;h_i)} \prod_{p\mid h_i} \left(1-\frac{\sigma(f^{(i)}_{h_i,b_i};p)}{p}\right) \\ &= \prod_{i=1}^{k} \sigma^*(f_i;h_i)\end{aligned}$$

by Lemma 5.5. This establishes Eq. (5.10) and hence the proposition. ∎

6. MULTIPLICATIVE FUNCTIONS OF ONE VARIABLE

Two propositions from Section 2 are established in this section. Proposition 2.7 is rather easy, as it follows from crude upper bounds for the multiplicative functions $G(f;n)$ and $\sigma(f;n)$ defined in Eq. (2.6). Proposition 2.9, on the other hand, requires an accurate knowledge of the order of magnitude of the summatory function of $G(f;n)\,\sigma(f;n)$. For this we use a mean-value result (see Proposition A.3 in Appendix A) for a general sum $\sum_{n\leqslant x} g(n)$ of a multiplicative function g. To apply such a mean-value result, some conditions on the values of the multiplicative function in question must be verified; the next three lemmas provide simple estimates of this type for the multiplicative functions $\sigma(f;n)$, $G(f;n)$, and $\sigma^*(f;n)$. In these three lemmas, all constants implicit in the $\ll$ and O-notations may depend on the polynomial f.

LEMMA 6.1. *If f is a squarefree polynomial with integer coefficients, then $\sigma(f;p^\nu) \ll 1$ uniformly for all prime powers p^ν.*

Proof. Let Δ be the discriminant of f, which is nonzero since f is squarefree, and write $\Delta = \prod_p p^{\theta(p)}$ where all but finitely many of the $\theta(p)$ are zero. Huxley [9] gives a bound for σ that implies

$$\sigma(f; p^\nu) \leqslant (\deg f)\, p^{\theta(p)/2}$$

for any squarefree polynomial f and any prime power p^ν (this estimate is improved by Stewart [13], though it will suffice for our purposes as stated). In particular we see that $\sigma(f; p^\nu) \leqslant (\deg f)\, \Delta^{1/2}$ for all prime powers p^ν, which establishes the lemma. ∎

LEMMA 6.2. *If f is a polynomial with integer coefficients that is squarefree and admissible, then $G(f; p^\nu) = 1 + O(1/p)$ and $\sigma^*(f; p^\nu) = \sigma(f; p^\nu) + O(1/p)$ uniformly for all prime powers p^ν.*

Proof. From general facts about polynomials over finite fields, for a given prime p either $\sigma(f; p) = p$ or $\sigma(f; p) \leqslant \deg f$. However, the fact that f is admissible means $\sigma(f; p) < p$, and so $\sigma(f; p) \leqslant \deg f$ for all primes p. This implies that for all primes $p \geqslant 2 \deg f$,

$$G(f; p^\nu) - 1 = \left(1 - \frac{\sigma(f; p)}{p}\right)^{-1} - 1 = \frac{\sigma(f; p)}{p - \sigma(f; p)} \leqslant \frac{\deg f}{p/2} \ll \frac{1}{p}.$$

This shows that $G(f; p^\nu) = 1 + O(1/p)$ for all prime powers p (by adjusting the implicit constant if necessary). Similarly,

$$\sigma(f; p^\nu) - \sigma^*(f; p^\nu) = \frac{\sigma(f; p^{\nu+1})}{p} \ll \frac{1}{p}$$

by Lemma 6.1, showing that $\sigma^*(f; p^\nu) = \sigma(f; p^\nu) + O(1/p)$. ∎

LEMMA 6.3. *If f is a polynomial with integer coefficients that is squarefree and admissible, then for any $\varepsilon > 0$, we have $\sigma(f; n) \ll_\varepsilon n^\varepsilon$ and $G(f; n) \ll_\varepsilon n^\varepsilon$.*

Proof. It is well known that the number $\omega(n)$ of distinct prime divisors of n satisfies $\omega(n) \ll \log n / \log \log n$, which implies that $A^{\omega(n)} \ll_{A,\varepsilon} n^\varepsilon$ for any positive constants A and ε. Therefore, any multiplicative function $g(n)$ satisfying $|g(p^\nu)| \leqslant A$ for all prime powers p^ν automatically satisfies $g(n) \ll_{A,\varepsilon} n^\varepsilon$. By Lemmas 6.1 and 6.2, respectively, both σ and G have this property for some constant A depending on the polynomial f, and so the lemma is established. ∎

The crude upper bounds given in Lemma 6.3 are enough to establish Proposition 2.7. For this proposition, as well as for Proposition 2.9 which is proved at the end of this section, we recall from Section 2 the definitions of the parameters d, k, u, U, ξ_i, and y.

PROPOSITION 2.7. *Let f be a polynomial that is balanced and admissible. Then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} G(f; h_1 \dots h_k)\, \sigma^*(f_1; h_1) \dots \sigma^*(f_k; h_k) \ll_{f,U} \frac{x}{\log x}$$

uniformly for $x \geqslant 1$ and $0 < u \leqslant U$.

Proof. If we include in the sum those (nonnegative) terms for which the h_i are not necessarily pairwise coprime, and use the trivial inequality $\sigma^*(f; n) \leqslant \sigma(f; n)$, we see that

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} G(f; h_1 \dots h_k)\, \sigma^*(f_1; h_1) \dots \sigma^*(f_k; h_k)$$
$$\leqslant \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} G(f; h_1 \dots h_k)\, \sigma(f_1; h_1) \dots \sigma(f_k; h_k).$$

Given $\varepsilon > 0$, we see from Lemma 6.3 that

$$\sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} G(f; h_1 \dots h_k)\, \sigma(f_1; h_1) \dots \sigma(f_k; h_k)$$
$$\ll_{f,\varepsilon} \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} (h_1 \dots h_k)^{2\varepsilon} \ll_{f,\varepsilon} \left(\frac{\xi_1 \dots \xi_k}{y^k}\right)^{1+2\varepsilon} \leqslant (x^{k(d-1/U)})^{1+2\varepsilon}.$$

Since $k(d-1/U) < 1$ by the upper bound (2.2) on U, we can choose ε so small (depending on f and U) that the right-hand side is $\ll_{f,U} x/\log x$, which establishes the proposition. ∎

When applying Proposition A.3 to a particular multiplicative function, it is of course necessary to verify the hypothesis (A.26) for that function. When the function in question is $\sigma(f; n)$ for some polynomial f, the relevant asymptotic formula is well-known. If f is a polynomial with integer coefficients with k distinct irreducible factors, then the values taken by σ on primes are k on average; more precisely, Nagel [10] showed that the asymptotic formula

$$\sum_{p \leqslant w} \frac{\sigma(f; p) \log p}{p} = k \log w + O_f(1) \tag{6.1}$$

holds for all $w \geqslant 2$. For the purposes of establishing Proposition 2.9 (and, in the next section, Proposition 2.4), we need to verify this hypothesis for the slightly different function $G(f;n)\,\sigma(f;n)$, while for Proposition 2.6, the appropriate function is $G(f;n)\,\sigma^*(f;n)$. These verifications are the subject of the following lemma.

LEMMA 6.4. *Let f be a squarefree polynomial with integer coefficients, and let f_i denote any one of the irreducible factors of f. Then*

$$\sum_{p\leqslant w}\frac{G(f;p)\,\sigma(f_i;p)\log p}{p}=\log w+O_f(1),$$

and the same is true if σ is replaced by σ^*.

Proof. The constants implicit in the $\ll$ and O-notations in this proof may depend on the polynomial f and thus on f_i as well. By Lemma 6.2 we know that

$$G(f;p)\,\sigma(f_i;p)=\sigma(f_i;p)(1+O(1/p))=\sigma(f_i;p)+O(1/p)$$

using Lemma 6.1, and so

$$\begin{aligned}\sum_{p\leqslant w}\frac{G(f;p)\,\sigma(f_i;p)\log p}{p}&=\sum_{p\leqslant w}\frac{\sigma(f_i;p)\log p}{p}+O\left(\sum_p\frac{\log p}{p^2}\right)\\&=\log w+O(1)\end{aligned}$$

by the asymptotic formula (6.1) and the fact that the last sum is convergent.

Again by Lemmas 6.1 and 6.2, we see that $G(f;p)\,\sigma^*(f_i;p)=\sigma(f_i;p)+O(1/p)$, and so

$$\begin{aligned}\sum_{p\leqslant w}\frac{G(f;p)\,\sigma^*(f_i;p)\log p}{p}&=\sum_{p\leqslant w}\frac{\sigma(f_i;p)\log p}{p}+O\left(\sum_p\frac{\log p}{p^2}\right)\\&=\log w+O(1)\end{aligned}$$

as before. This establishes the lemma. ∎

We may now establish an upper bound of the correct order of magnitude for the summatory functions that will arise in the proofs of Proposition 2.9 and (in the next section) Proposition 2.4.

LEMMA 6.5. *Let f be a polynomial with integer coefficients that is squarefree and admissible, and let f_i be any one of the irreducible factors of f. Then*

$$\sum_{n\leqslant x}\frac{G(f;n)\,\sigma(f_i;n)}{n}\ll_f\log x\qquad\text{and}\qquad\sum_{n\leqslant x}\frac{G(f;n)\,\sigma(f_i;n)}{n^{1-\beta}}\ll_{f,\beta}x^\beta$$

for any $\beta>0$.

Proof. We want to apply Proposition A.3 to establish the first claim of the lemma. The function $G(f;n)\,\sigma(f_i;n)$ is nonnegative and multiplicative, and by Lemma 6.3 we know that $G(f;n)\,\sigma(f_i;n) \ll_f n^{1/4}$, say. Furthermore, Lemma 6.4 verifies the condition (A.26) with $\kappa = 1$. Therefore we may apply Proposition A.3(a) to see that

$$\sum_{n\leqslant x} \frac{G(f;n)\,\sigma(f_i;n)}{n} = c(G(f;n)\,\sigma(f_i;n)) \log x + O_f(1).$$

This establishes the first claim of the lemma; the second claim follows easily from the first by a simple partial summation argument. ▮

We are now ready to establish Proposition 2.9, showing that Hypothesis UH implies an upper bound for the expression $H(f;x,y)$, which is a sum of error terms of the type $E(f_i;x_i)$. Again we recall the definitions of d, k, u, U, ξ_i, and y.

PROPOSITION 2.9. *Assume Hypothesis UH. Let f be a polynomial with integer coefficients that is balanced, effective, and admissible. Then $H(f;x,y) \ll_{f,U} x/\log x$.*

Proof. All constants implicit in the $\ll$ and O-notations in this proof may depend on the polynomial f and the parameter U. We recall the definition (2.11) of $H(f;x,y)$:

$$H(f;x,y) = \sum_{\substack{h_1\leqslant \xi_1/y \\ (h_i,h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k\leqslant \xi_k/y} \sum_{b\in\mathcal{R}(f;h_1,\ldots,h_k)} E\left(f_{h_1\ldots h_k,b}; \frac{x-b}{h_1\ldots h_k}\right). \tag{6.2}$$

Notice that

$$h_1\ldots h_k \leqslant \xi_1\ldots\xi_k/y^k \ll x^{kd}(x^{1/u})^{-d} \leqslant x^{k(d-1/U)}$$

for $u\leqslant U$; in particular, when U satisfies the bound (2.2), the exponent $k(d-1/U)$ is strictly less than 1. Consequently the coefficients of the polynomial $f_{h_1\ldots h_k,b}$ are certainly $\ll (h_1\ldots h_k)^{d-1} \ll x^d$ in size, while we have the lower bound

$$\frac{x-b}{h_1\ldots h_k} \gg x^{1-k(d-1/U)}. \tag{6.3}$$

We may therefore apply Hypothesis UH with $B = d/(1-k(d-1/U)) > 0$ to the error terms $E(f_{h_1\ldots h_k,b};(x-b)/h_1\ldots h_k)$ in Eq. (6.2); this yields

$$H(f;x,y) \ll \sum_{\substack{h_1\leqslant \xi_1/y \\ (h_i,h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k\leqslant \xi_k/y} \sum_{b\in\mathcal{R}(f;h_1,\ldots,h_k)} \left(\frac{C(f_{h_1\ldots h_k,b})(x-b)/h_1\ldots h_k}{(\log((x-b)/h_1\ldots h_k))^{k+1}} + 1\right)$$

using Hypothesis UH. We see from the lower bound (6.3) that the logarithmic term in the denominator can be replaced by $\log x$, yielding

$$H(f; x, y) \ll \frac{x}{\log^{k+1} x} \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{1}{h_1 \ldots h_k} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} C(f_{h_1 \ldots h_k, b})$$
$$+ \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, \ldots, h_k)} 1;$$

and by Eq. (5.9) and the definition of $\mathscr{R}(f; h_1, \ldots, h_k)$, this is the same as

$$H(f; x, y) \ll \frac{C(f)\, x}{\log^{k+1} x} \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)}{h_1 \ldots h_k}$$
$$+ \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sigma(f_1; h_1) \ldots \sigma(f_k; h_k).$$

Since the h_i are pairwise coprime, we may factor the multiplicative function $G(f; h_1 \ldots h_k)$ into $G(f; h_1) \ldots G(f; h_k)$ in the first sum on the right-hand side of this last equation. By then deleting the restrictions $(h_i, h_j)=1$ from the conditions of summation in both sums, and noting that $1 \leqslant G(f; h_i)$ and $\sigma^*(f_i, h_i) \leqslant \sigma(f_i; h_i)$, we see that

$$\begin{aligned} H(f; x, y) &\ll \frac{x}{\log^{k+1} x} \prod_{i=1}^{k} \sum_{h_i \leqslant \xi_i/y} \frac{G(f; h_i)\, \sigma(f_i; h_i)}{h_i} \\ &\quad + \prod_{i=1}^{k} \sum_{h_i \leqslant \xi_i/y} G(f; h_i)\, \sigma(f_i; h_i) \\ &\ll \frac{x}{\log^{k+1} x} \prod_{i=1}^{k} \log \frac{\xi_i}{y} + \prod_{i=1}^{k} \frac{\xi_i}{y} \end{aligned} \tag{6.4}$$

by Lemma 6.5 (applied with $\beta=1$ in the second sum). Clearly each $\log \xi/y \ll \log x$, while

$$\prod_{i=1}^{k} \frac{\xi_i}{y} \ll x^{k(d-1/u)} \ll \frac{x}{\log x},$$

again since $k(d-1/u)<1$ by the upper bound (2.2) on U. Therefore the estimate (6.4) becomes $H(f; x, y) \ll x/\log x$, which establishes the proposition. ∎

7. PRIME VALUES OF POLYNOMIALS

In this section we establish Proposition 2.4, by using Brun's upper bound sieve method to estimate the numbers of prime values of the polynomials $f_{h_1 \dots h_k, b}$. To apply Brun's sieve, we must verify some conditions on the number $\sigma(f_{h,b}; p)$ of local roots of the polynomials $f_{h,b}$; this is the subject of the following two lemmas.

LEMMA 7.1. *Let f be a squarefree polynomial with integer coefficients, let h be a positive integer, and let b be an element of $\mathcal{R}(f; h)$. Then $\sigma(f_{h,b}; p) \ll_f 1$ uniformly for all primes p (where the implicit constant does not depend on h or b).*

Proof. If p does not divide h, then $\sigma(f_{h,b}; p) = \sigma(f; p)$ by Lemma 5.1. On the other hand, if p^ν exactly divides h, then $\sigma(f_{h,b}; p) = \sigma(f_{p^\nu,b}; p)$ by Lemma 5.3; moreover, Lemma 5.4 applied with $h = p^\nu$ and $n = p$ certainly implies that $\sigma(f_{p^\nu,b}; p) \leqslant \sigma(f; p^{\nu+1})$. In either case, we have $\sigma(f_{h,b}; p) \leqslant \sigma(f; p^\alpha)$ for some positive integer α, and Lemma 6.1 tells us that $\sigma(f; p^\alpha) \ll_f 1$. This establishes the lemma. ∎

LEMMA 7.2. *Let f be a squarefree polynomial with integer coefficients, let h be a positive integer, and let b be an element of $\mathcal{R}(f; h)$ such that the polynomial $f_{h,b}$ is admissible. Then*

$$\left(1 - \frac{\sigma(f_{h,b}; d)}{d}\right)^{-1} \ll_f 1 \tag{7.1}$$

uniformly for all positive integers d (where the implicit constant does not depend on h or b).

Proof. If p^ν is any prime power, then putting $h = p$ and $n = p^{\nu-1}$ in the inequality (5.4), we see that $\sigma(f_{h,b}; p^\nu) \leqslant p^{\nu-1}\sigma(f_{h,b}; p)$. This implies that

$$\frac{\sigma(f_{h,b}; d)}{d} = \prod_{p^\nu \| d} \frac{\sigma(f_{h,b}; p^\nu)}{p^\nu} \leqslant \prod_{p \mid d} \frac{\sigma(f_{h,b}; p)}{p}.$$

Since each $\sigma(f_{h,b}; p)/p \leqslant 1$, it follows that for any prime p dividing d, we have $\sigma(f_{h,b}; d)/d \leqslant \sigma(f_{h,b}; p)/p$ and hence

$$\left(1 - \frac{\sigma(f_{h,b}; d)}{d}\right)^{-1} \leqslant \left(1 - \frac{\sigma(f_{h,b}; p)}{p}\right)^{-1}.$$

Therefore to establish the lemma, it suffices to establish the upper bound (7.1) for primes. But $p - \sigma(f_{h,b}; p)$ is a nonnegative integer, and it cannot be 0 since we are assuming that $f_{h,b}$ is admissible. Therefore $p-\sigma(f_{h,b}; p) \geqslant 1$, so we can write

$$\left(1-\frac{\sigma(f_{h,b}; p)}{p}\right)^{-1} = 1+\frac{\sigma(f_{h,b}; p)}{p-\sigma(f_{h,b}; p)} \leqslant 1+\sigma(f_{h,b}; p) \ll_f 1$$

by Lemma 7.1. This establishes the lemma. ∎

In the next lemma, we apply Brun's sieve to obtain the desired upper bound for the number of prime values of the polynomials $f_{h_1 \ldots h_k, b}$, with the dependence on the parameters $h_1, \ldots, h_k$ and b made explicit.

LEMMA 7.3. *Let f be a polynomial with integer coefficients that is squarefree, effective, and primitive, and let k denote the number of distinct irreducible factors of f. For any positive integers $h_1, \ldots, h_k$ and any $b \in \mathcal{R}(f; h_1, \ldots, h_k)$, we have*

$$\pi(f_{h_1 \ldots h_k, b}; t) \ll_f \frac{t}{\log^k t} G(f; h_1 \ldots h_k) \tag{7.2}$$

(where the implicit constant does not depend on $h_1, \ldots, h_k$, or b).

Proof. If the polynomial $f_{h_1 \ldots h_k, b}$ is not admissible then $\pi(f_{h_1 \ldots h_k, b}; t) \ll_f 1$ (see the remarks following the statement of Hypothesis UH). Clearly $G(f; h_1, \ldots, h_k) \geqslant 1$ from its definition, and so the upper bound (7.2) holds easily in this case. Thus for the remainder of the proof, we may assume that $f_{h_1 \ldots h_k, b}$ is in fact admissible.

We first bound $\pi(f_{h_1 \ldots h_k, b}; t)$ by noting that

$$\begin{aligned} \pi(f_{h_1 \ldots h_k, b}; t) &= \#\{n \leqslant t : \text{ each } f^{(i)}_{h_1, \ldots, h_k; b}(n) \text{ is prime}\} \\ &= \#\{n \leqslant t : \text{ for each } i,\ p \mid f^{(i)}_{h_1, \ldots, h_k; b}(n) \Rightarrow p > (f^{(i)}_{h_1, \ldots, h_k; b}(n))^{1/2}\} \\ &\leqslant \#\{n \leqslant t : p \mid f_{h_1 \ldots h_k, b}(n) \Rightarrow p > t^{1/3}\} + O(t^{2/3}), \end{aligned} \tag{7.3}$$

since $f^{(i)}_{h_1, \ldots, h_k; b}(n) > n$ for each i. This casts the problem of estimating $\pi(f_{h_1 \ldots h_k, b}; t)$ in terms of a sieving problem.

The version of Brun's sieve that we now employ can be found in Halberstam and Richert [6, Theorem 2.2]. Given a set $\mathcal{A}$ of integers, assume that a real number X and a multiplicative function $\omega(d)$ can be chosen such that

$$\#\{a \in \mathcal{A} : d \mid a\} = \frac{\omega(d)}{d} X + R_d, \qquad \text{where} \quad |R_d| \leqslant \omega(d). \tag{7.4}$$

Assume that ω satisfies the two conditions

$$0 \leqslant \omega(p) \ll 1 \qquad \text{and} \qquad \left(1-\frac{\omega(d)}{d}\right)^{-1} \ll 1. \tag{7.5}$$

Then we have the upper bound

$$\#\{a \in \mathscr{A} : p \mid a \Rightarrow p > z\} \ll X \prod_{p \leqslant z} \left(1-\frac{\omega(p)}{p}\right) \tag{7.6}$$

uniformly for $2 \leqslant z \leqslant X$, where the implicit constant depends only on the implicit constants in the conditions (7.5) on ω.

For our application, we take $\mathscr{A} = \{f_{h_1 \dots h_k, b}(n) : 1 \leqslant n \leqslant t\}$ and $z = t^{1/3}$; with these choices, the left-hand side of the bound (7.6) is exactly $\#\{1 \leqslant n \leqslant t : p \mid f_{h_1 \dots h_k, b}(n) \Rightarrow p > t^{1/3}\}$. We also set $X = t$ and $\omega(d) = \sigma(f_{h_1 \dots h_k, b}; d)$. Of course the condition (7.4) is satisfied, since the polynomial $f_{h_1 \dots h_k, b}$ has $\sigma(f_{h_1 \dots h_k, b}; d)$ zeros (mod d) in every block of d consecutive integers. On the other hand, since we are assuming that $f_{h_1 \dots h_k, b}$ is admissible, Lemmas 7.1 and 7.2 show that the conditions (7.5) are satisfied. The bound (7.6) thus implies that

$$\begin{aligned}\#\{1 \leqslant n \leqslant t : p \mid f_{h_1 \dots h_k, b}(n) \Rightarrow p > t^{1/3}\} &\ll_f t \prod_{p \leqslant t^{1/3}} \left(1-\frac{\sigma(f_{h_1 \dots h_k, b}; p)}{p}\right) \\ &\ll_f \frac{t}{\log^k t} \prod_{p \leqslant t^{1/3}} \left(1-\frac{1}{p}\right)^{-k} \left(1-\frac{\sigma(f; p)}{p}\right) \\ &\quad \times \prod_{\substack{p \leqslant t^{1/3} \\ p \mid h_1 \dots h_k}} \left(1-\frac{\sigma(f; p)}{p}\right)^{-1} \left(1-\frac{\sigma(f_{h_1 \dots h_k, b}; p)}{p}\right) \end{aligned} \tag{7.7}$$

using Lemma 5.1. The first product converges to $C(f)$ as t tends to infinity, while the factors $1-\sigma(f_{h_1 \dots h_k, b}; p)/p$ in the second product can be deleted for the purpose of finding an upper bound. Therefore

$$\begin{aligned}\#\{n \leqslant t &: p \mid f_{h_1 \dots h_k, b}(n) \Rightarrow p > t^{1/3}\} \\ &\ll_f \frac{t}{\log^k t} (C(f)+o(1)) \prod_{\substack{p \leqslant t^{1/3} \\ p \mid h_1 \dots h_k}} \left(1-\frac{\sigma(f; p)}{p}\right)^{-1} \\ &\ll_f \frac{t}{\log^k t} G(f; h_1 \dots h_k).\end{aligned}$$

In light of the inequality (7.3), this establishes the lemma. ∎

The last lemma we give before proceeding to the proof of Proposition 2.4 is an elementary lemma concerning the behavior of the quantity $\eta_{h_1, \dots, h_k}$.

LEMMA 7.4. *Let $h_1, ..., h_k$ be positive integers satisfying $h_i \leqslant \xi_i / y$. Suppose the quantity $\eta_{h_1, ..., h_k}$ satisfies $\eta_{h_1, ..., h_k} \asymp (y \max\{h_1, ..., h_k\})^{1/d} (h_1 \dots h_k)^{-1}$. Then*

$$\eta_{h_1, ..., h_k} \leqslant y^{1/d}(h_1^{1/d} + \cdots + h_k^{1/d})(h_1 \dots h_k)^{-1} \tag{7.8}$$

and $\log \eta_{h_1, ..., h_k} \gg_{k, d, U} \log x$ *uniformly for* $x \geqslant 1$.

Proof. The inequality (7.8) is easy to see by noting that

$$(\max\{h_1, ..., h_k\})^{1/d} = \max\{h_1^{1/d}, ..., h_1^{1/d}\} \leqslant h_1^{1/d} + \cdots + h_1^{1/d}.$$

As for the second assertion, the hypothesis $h_i \leqslant \xi_i / y$ implies that

$$\eta_{h_1, ..., h_k} \gg \frac{(y \max\{h_1, ..., h_k\})^{1/d}}{h_1 \dots h_k} \geqslant y^{1/d}(\max\{h_1, ..., h_k\})^{1/d-k}$$
$$\geqslant y^k(\max\{\xi_1, ..., \xi_k\})^{1/d-k} \gg x^{k/u} x^{1-dk}.$$

Since the exponent $k/u + 1 - dk$ of x is positive by the upper bound (2.2) on u, this establishes the lemma. ∎

We now have the tools we need to prove:

PROPOSITION 2.4. *Let f be a polynomial that is balanced, effective, and primitive. If the quantities $\eta_{h_1, ..., h_k}$ satisfy $\eta_{h_1, ..., h_k} \asymp (y \max\{h_1, ..., h_k\})^{1/d}$ $(h_1 \dots h_k)^{-1}$, then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1 \, (1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathscr{R}(f; h_1, ..., h_k)} \pi(f_{h_1 \dots h_k, b}; \eta_{h_1, ..., h_k}) \ll_f \frac{x}{\log x}.$$

Proof. All of the constants implicit in the $\ll$-notation in this proof may depend on the polynomial f. We use the bound given by Lemma 7.3 on each term in the inner sum, yielding

$$\sum_{b \in \mathscr{R}(f; h_1, ..., h_k)} \pi(f_{h_1 \dots h_k, b}; \eta_{h_1, ..., h_k}) \ll \frac{\eta_{h_1, ..., h_k}}{\log^k \eta_{h_1, ..., h_k}} G(f; h_1 \dots h_k) \sum_{b \in \mathscr{R}(f; h_1, ..., h_k)} 1. \tag{7.9}$$

By the second assertion of Lemma 7.4, we may replace the denominator $\log^k \eta_{h_1, ..., h_k}$ by $\log^k x$. In addition, since the h_i are pairwise coprime we may factor the term $G(f; h_1 \dots h_k) = G(f; h_1) \dots G(f; h_k)$; and the final sum in

Eq. (7.9) is precisely $\sigma(f_1; h_1)\ldots\sigma(f_k; h_k)$ by the definition of $\mathcal{R}(f; h_1, \ldots, h_k)$. Therefore

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \pi(f_{h_1\ldots h_k, b}; \eta_{h_1, \ldots, h_k})$$
$$\ll \frac{1}{\log^k x} \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} \eta_{h_1, \ldots, h_k} G(f; h_1)\,\sigma(f_1; h_1)\ldots G(f; h_k)\,\sigma(f_k; h_k),$$

where we have deleted the condition $(h_i, h_j) = 1$.

By the first assertion of Lemma 7.4, this estimate becomes

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \pi(f_{h_1\ldots h_k, b}; \eta_{h_1, \ldots, h_k})$$
$$\ll \frac{y^{1/d}}{\log^k x} \sum_{i=1}^{k} \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{h_i^{1/d} G(f; h_1)\,\sigma(f_1; h_1)\ldots G(f; h_k)\,\sigma(f_k; h_k)}{h_1 \ldots h_k}. \tag{7.10}$$

For the term with $i = 1$, for instance, we may use the second claim of Lemma 6.5 with $\beta = 1/d$ to bound the sum over h_1, and the first claim of Lemma 6.5 to bound the remaining sums over $h_2, \ldots, h_k$, giving

$$\sum_{h_1 \leqslant \xi_1/y} \frac{G(f; h_1)\,\sigma(f_1; h_1)}{h_1^{1-1/d}} \prod_{i=2}^{k} \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_i)\,\sigma(f_i; h_i)}{h_i}$$
$$\ll \left(\frac{\xi_1}{y}\right)^{1/d} \prod_{i=2}^{k} \log \frac{\xi_i}{y} \ll \frac{x \log^{k-1} x}{y^{1/d}}$$

since $\log(\xi_i/y) \ll \log x$. The other terms are similar, and we see from the estimate (7.10) that

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \sum_{b \in \mathcal{R}(f; h_1, \ldots, h_k)} \pi(f_{h_1\ldots h_k, b}; \eta_{h_1, \ldots, h_k}) \ll \frac{x}{\log x},$$

which establishes the proposition. ∎

8. PARTIAL SUMMATION

The proof of Proposition 2.6 will occupy all of this section. Our first goal is to understand an unweighted version of the sum on the left-hand side of Eq. (2.9), where the $\mathrm{li}_{h_1, \ldots, h_k}(f; x)$ terms have been omitted. Proposition A.4

of Appendix A is precisely the tool we need to evaluate asymptotically a multivariable sum of multiplicative functions of this form. The beauty of the outcome is that the local factors conspire to make the constant in the asymptotic formula exactly equal to $C(f)^{-1}$.

LEMMA 8.1. *Let f be a polynomial with integer coefficients that is squarefree, admissible, and exclusive, and let $f_1, \ldots, f_k$ be the distinct irreducible factors of f. For all real numbers $1 \leqslant t_1, \ldots, t_k \leqslant x$, we have*

$$\sum_{\substack{h_1 \leqslant t_1 \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant t_k} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)}{h_1 \ldots h_k}$$
$$= C(f)^{-1} \left(\prod_{i=1}^{k} \log t_i \right) + O_f(\log^{k-1} x).$$

Proof. All of the constants implicit in the O-notation in this proof may depend on the polynomial f (and thus on k and its irreducible factors f_i as well). For each $1 \leqslant i \leqslant k$, the function $G(f; n)\, \sigma^*(f_i; n)$ is a nonnegative multiplicative function satisfying $G(f; n)\, \sigma^*(f_i; n) \leqslant G(f; n)\, \sigma(f_i; n) \ll n^{\varepsilon}$ by Lemma 6.3 (note that each factor f_i of the admissible polynomial f is itself admissible). Moreover, by Lemma 6.4 the asymptotic formula (A.29) holds for each $G(f; n)\, \sigma^*(f_i; n)$ with $\kappa_i = 1$. We may therefore conclude from Proposition A.4 that

$$\sum_{\substack{h_1 \leqslant t_1 \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant t_k} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)}{h_1 \ldots h_k}$$
$$= c(G(f; n)\, \sigma^*(f_1; n), \ldots, G(f; n)\, \sigma^*(f_k; n)) \prod_{i=1}^{k} (\log t_i + O(1)).$$

We have $\prod_{i=1}^{k} (\log t_i + O(1)) = \prod_{i=1}^{k} \log t_i + O(\log^{k-1} x)$ since each $t_i \leqslant x$, and so to establish the lemma it suffices to show that

$$c(G(f; n)\, \sigma^*(f_1; n), \ldots, G(f; n)\, \sigma^*(f_k; n)) = C(f)^{-1}. \tag{8.1}$$

Since each $\kappa_i = 1$, we see from the definition (A.31) that

$$c(G(f; n)\, \sigma^*(f_1; n), \ldots, G(f; n)\, \sigma^*(f_k; n))$$
$$= \Gamma(2)^{-k} \prod_p \left(1 - \frac{1}{p}\right)^k$$
$$\times \left(1 + \sum_{\nu=1}^{\infty} \frac{G(f; p^\nu)\, \sigma^*(f_1; p^\nu) + \cdots + G(f; p^\nu)\, \sigma^*(f_k; p^\nu)}{p^\nu}\right). \tag{8.2}$$

Rewriting

$$\sum_{\nu=1}^{\infty} \frac{G(f;p^\nu)\,\sigma^*(f_1;p^\nu)+\cdots+G(f;p^\nu)\,\sigma^*(f_k;p^\nu)}{p^\nu} = \left(1-\frac{\sigma(f;p)}{p}\right)^{-1} \sum_{i=1}^{k} \left(\sum_{\nu=1}^{\infty} \frac{\sigma^*(f_i;p^\nu)}{p^\nu}\right)$$

by the definition of G, we note that the inner sum on the right-hand side is a telescoping series by the definition of σ^*:

$$\sum_{\nu=1}^{\infty} \frac{\sigma^*(f_i;p^\nu)}{p^\nu} = \sum_{\nu=1}^{\infty} \left(\frac{\sigma(f_i;p^\nu)}{p^\nu} - \frac{\sigma(f_i;p^{\nu+1})}{p^{\nu+1}}\right) = \frac{\sigma(f_i;p)}{p}.$$

Thus Eq. (8.2) becomes

$$c(G(f;n)\,\sigma^*(f_1;n), ..., G(f;n)\,\sigma^*(f_k;n)) = \prod_p \left(1-\frac{1}{p}\right)^k \left(1+\left(1-\frac{\sigma(f;p)}{p}\right)^{-1} \sum_{i=1}^{k} \frac{\sigma(f_i;p)}{p}\right).$$

Since f is an exclusive polynomial, for any prime p the number of roots of $f \pmod p$ is equal to the sum of the numbers of roots of each $f_i \pmod p$; in other words, $\sum_{i=1}^{k} \sigma(f_i;p) = \sigma(f;p)$. Therefore

$$\begin{aligned} c(G(f;n)\,\sigma^*(f_1;n), ..., G(f;n)\,\sigma^*(f_k;n)) &= \prod_p \left(1-\frac{1}{p}\right)^k \left(1+\left(1-\frac{\sigma(f;p)}{p}\right)^{-1} \cdot \frac{\sigma(f;p)}{p}\right) \\ &= \prod_p \left(1-\frac{1}{p}\right)^k \left(1-\frac{\sigma(f;p)}{p}\right)^{-1} = C(f)^{-1}, \end{aligned}$$

which establishes Eq. (8.1) and hence the lemma. ▮

Next we use partial summation to convert the asymptotic formula in Lemma 8.1 to the asymptotic formula asserted in Proposition 2.6, completing the proof of that proposition. The partial summation argument is not deep but is quite messy, both because the function $\mathrm{li}_{h_1, ..., h_k}(f;x)$ defined in Eq. (2.7) is somewhat complicated, and because the k-fold sum in the statement of Proposition 2.6 requires an inductive argument with partial summation being employed in each variable. Addressing the former of these difficulties, the following lemma gives the asymptotics of the function $\mathrm{li}_{h_1, ..., h_k}(f;x)$. We recall the definitions of the parameters d, k, u, U, ξ_i, and y for use in this section, and we allow all constants implicit in the $\ll$

and O-notations in this section to depend on the polynomial f (and thus on d, k, and the ξ_i as well) and on U.

LEMMA 8.2. *For any effective polynomial f and any positive integers $h_1, ..., h_k$ satisfying $h_i \leqslant \xi_i/y$, we have*

$$\mathrm{li}_{h_1,\ldots,h_k}(f;x) = \frac{x}{\prod_{i=1}^k (\log \xi_i/h_i)} + O\left(\frac{x}{(\log x)^{k+1}}\right) \tag{8.3}$$

uniformly for $x \geqslant 1$.

Proof. By adjusting the constant implicit in the O-notation if necessary, it suffices to establish the asymptotic formula (8.3) when x is sufficiently large (in terms of f and U). Notice that $f_i(x/(\log x)^{k+1}) > x/(\log x)^{k+1}$ for each $1 \leqslant i \leqslant k$, from the fact that f is effective. Notice also that each $\xi_i/y \ll x^{d-1/U}$, where the exponent $d-1/U$ is strictly less than $1/k \leqslant 1$. Therefore for each $1 \leqslant i \leqslant k$, the expression $f_i(x/(\log x)^{k+1})/(\xi_i/y)$ tends to infinity with x. We assume that x is so large that

$$\min_{1 \leqslant i \leqslant k} \left\{ \frac{f_i(x/(\log x)^{k+1})}{\xi_i/y} \right\} \geqslant 2. \tag{8.4}$$

By the monotonicity of the f_i and the hypothesis bounding the h_i, this certainly implies that

$$\min_{1 \leqslant i \leqslant k} \{f_i(t)/h_i\} \geqslant 2 \tag{8.5}$$

for any $t \geqslant x/(\log x)^{k+1}$.

We define $v(t) = 1/\prod_{i=1}^k \log(f_i(t)/h_i)$, the integrand in the definition (2.7) of $\mathrm{li}_{h_1,\ldots,h_k}(f;x)$. Splitting that integral at the point $x/(\log x)^{k+1}$ yields

$$\mathrm{li}_{h_1,\ldots,h_k}(f;x) = \int_{\substack{0<t\leqslant x/(\log x)^{k+1} \\ \min\{f_1(t)/h_1,\ldots,f_k(t)/h_k\}\geqslant 2}} v(t)\,dt + \int_{\substack{x/(\log x)^{k+1}<t\leqslant x \\ \min\{f_1(t)/h_1,\ldots,f_k(t)/h_k\}\geqslant 2}} v(t)\,dt.$$

We estimate the first integral trivially by noting that $v(t) \leqslant (\log 2)^{-k} \ll 1$ when t lies in the range of integration. In the second integral, the condition $\min\{f_1(t)/h_1, \ldots, f_k(t)/h_k\} \geqslant 2$ holds since we are considering only values of x that are so large that the inequality (8.5) is satisfied. Therefore

$$\mathrm{li}_{h_1,\ldots,h_k}(f;x) = \int_{x/(\log x)^{k+1}}^{x} v(t)\,dt + O\left(\frac{x}{(\log x)^{k+1}}\right).$$

and thus to establish the lemma it suffices to show that

$$\int_{x/(\log x)^{k+1}}^{x} v(t)\,dt = xv(x) + O\left(\frac{x}{(\log x)^{k+1}}\right). \tag{8.6}$$

We accomplish this by integrating by parts:

$$\begin{aligned}\int_{x/(\log x)^{k+1}}^{x} v(t)\,dt \\ &= tv(t)\big|_{x/(\log x)^{k+1}}^{x} - \int_{x/(\log x)^{k+1}}^{x} tv'(t)\,dt \\ &= xv(x) + O\left(\frac{xv(x/(\log x)^{k+1})}{(\log x)^{k+1}} + x\max\{tv'(t) : x/(\log x)^{k+1} \leqslant t \leqslant x\}\right).\end{aligned} \tag{8.7}$$

For any $t \geqslant x/(\log x)^{k+1}$, we note that

$$\log\frac{f_i(t)}{h_i} \geqslant \log\left(\frac{x/(\log x)^{k+1}}{\xi_i/y}\right) \gg \log x \tag{8.8}$$

for each $1 \leqslant i \leqslant k$ (see the remarks preceding Eq. (8.4)), and so we have $v(t) \ll (\log x)^{-k}$ for t in this range. Also, by logarithmic differentiation we see that

$$\begin{aligned}v'(t) &= v(t)\left(\sum_{i=1}^{k} \frac{-f_i'(t)}{f_i(t)\log(f_i(t)/h_i)}\right) \ll \frac{1}{\log^k x}\sum_{i=1}^{k}\frac{f_i'(t)}{f_i(t)\log x} \\ &\ll \frac{1}{t(\log x)^{k+1}}\end{aligned}$$

from the estimate (8.8) and the fact that $f_i'(t)/f_i(t) \ll 1/t$ for any polynomial f_i. Given these estimates for $v(t)$ and $v'(t)$, we see that Eq. (8.7) implies Eq. (8.6) and hence the lemma. ∎

The next lemma encapsulates the k-fold partial summation argument mentioned prior to the statement of Lemma 8.2.

Lemma 8.3. *For each integer $0 \leqslant l \leqslant k$, the asymptotic formula*

$$\begin{aligned}\sum_{\substack{n_1 \leqslant t_1 \\ (n_i, n_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{n_k \leqslant t_k} \frac{G(f; n_1 \dots n_k)\,\sigma^*(f_1; n_1)\dots\sigma^*(f_k; n_k)}{n_1 \dots n_k \cdot (\log \xi_1/n_1)\dots(\log \xi_l/n_l)} \\ = C(f)^{-1}\left(\prod_{i=1}^{l}\log\left(\frac{\log \xi_i}{\log \xi_i/t_i}\right)\right)\left(\prod_{i=l+1}^{k}\log t_i\right) + O((\log x)^{k-l-1})\end{aligned}$$

holds for all real numbers $t_1, \dots, t_k$ satisfying $1 \leqslant t_i \leqslant \xi_i/y$.

Proof. Set

$$W_l(t_1, \ldots, t_k) = \sum_{\substack{n_1 \leqslant t_1 \\ (n_i, n_j)=1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{n_k \leqslant t_k} \frac{G(f; n_1 \ldots n_k)\, \sigma_1^*(n_1) \ldots \sigma_k^*(n_k)}{n_1 \ldots n_k \cdot (\log \xi_1/n_1) \ldots (\log \xi_l/n_l)}.$$

The key to the proof is to notice that W_l can be expressed in terms of W_{l-1} by partial summation,

$$\begin{aligned} W_l(t_1, \ldots, t_k) &= \int_{t=1^-}^{t_l} \frac{dW_{l-1}(t_1, \ldots, t_{l-1}, t, t_{l+1}, \ldots, t_k)}{\log \xi_l/t} \\ &= \frac{W_{l-1}(t_1, \ldots, t_k)}{\log \xi_l/t_l} - \int_1^{t_l} \frac{W_{l-1}(t_1, \ldots, t_{l-1}, t, t_{l+1}, \ldots, t_k)\, dt}{t(\log \xi_l/t)^2} \end{aligned} \tag{8.9}$$

upon integration by parts.

We proceed by induction on l; the base case $l = 0$ follows immediately from Lemma 8.1, since $\xi_i/y \leqslant x$ for x sufficiently large. For the inductive step, suppose that the lemma holds for the case $l-1$, so that we know the asymptotic formula for W_{l-1}; we can then insert this asymptotic formula into Eq. (8.9) to obtain

$$\begin{aligned} W_l(t_1, \ldots, t_k) = &\left\{ C(f)^{-1} \left(\prod_{i=1}^{l-1} \log\left(\frac{\log \xi_i}{\log \xi_i/t_i} \right) \right) \left(\prod_{i=l}^{k} \log t_i \right) + O((\log x)^{k-l}) \right\} \\ &\times \frac{1}{\log \xi_l/t_l} \\ &- \int_1^{t_l} \left\{ C(f)^{-1} \left(\prod_{i=1}^{l-1} \log\left(\frac{\log \xi_i}{\log \xi_i/t_i} \right) \right) \right. \\ &\left. \times \log t \left(\prod_{i=l+1}^{k} \log t_i \right) + O((\log x)^{k-l}) \right\} \frac{dt}{t(\log \xi_l/t)^2} \\ = &\, C(f)^{-1} \left(\prod_{i=1}^{l-1} \log\left(\frac{\log \xi_i}{\log \xi_i/t_i} \right) \right) \left(\prod_{i=l+1}^{k} \log t_i \right) \\ &\times \left\{ \frac{\log t_l}{\log \xi_l/t_l} - \int_1^{t_l} \frac{\log t\, dt}{t(\log \xi_l/t)^2} \right\} \\ &+ O\left(\frac{(\log x)^{k-l}}{\log \xi_l/t_l} + \int_1^{t_l} \frac{(\log x)^{k-l}\, dt}{t(\log \xi_l/t)^2} \right). \end{aligned} \tag{8.10}$$

Since $\log \xi_l/t \geqslant \log y \gg \log x$ for all $1 \leqslant t \leqslant t_l$, this error term is $\ll (\log x)^{k-l-1}$. Moreover, making the change of variables $t \mapsto \log t$ yields

$$\int_1^{t_l} \frac{\log t\, dt}{t(\log \xi_l/t)^2} = \int_0^{\log t_l} \frac{t\, dt}{(\log \xi_l - t)^2} = \left(\log(\log \xi_l - t) + \frac{\log \xi_l}{\log \xi_l - t}\right)\Bigg|_0^{\log t_l}$$

$$= \left(\log(\log \xi_l/t_l) + \frac{\log \xi_l}{\log \xi_l/t_l}\right) - (\log(\log \xi_l) + 1)$$

$$= \frac{\log t_l}{\log \xi_l/t_l} - \log\left(\frac{\log \xi_l}{\log \xi_l/t_l}\right).$$

Therefore Eq. (8.10) becomes

$$W_l(t_1, ..., t_k) = C(f)^{-1}\left(\prod_{i=1}^{l-1} \log\left(\frac{\log \xi_i}{\log \xi_i/t_i}\right)\right)\left(\prod_{i=l+1}^{k} \log t_i\right)$$
$$\times \log\left(\frac{\log \xi_l}{\log \xi_l/t_l}\right) + O((\log x)^{k-l-1}),$$

which is the desired asymptotic formula for the case l. This establishes the lemma. ∎

We are now ready to establish:

Proposition 2.6. *Let f be a polynomial that is balanced, effective, admissible, and exclusive. Then*

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)\, \mathrm{li}_{h_1, ..., h_k}(f; x)}{h_1 \ldots h_k}$$
$$= C(f)^{-1}\, x \log^k(du) + O_{f,U}\left(\frac{x}{\log x}\right) \tag{8.11}$$

uniformly for $x \geqslant 1$ and $0 < u \leqslant U$.

Proof. By Lemma 8.2,

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)\, \mathrm{li}_{h_1, ..., h_k}(f; x)}{h_1 \ldots h_k}$$
$$= x \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)}{h_1 \ldots h_k \cdot (\log \xi_1/h_1) \ldots (\log \xi_k/h_k)}$$
$$+ O\left(\frac{x}{(\log x)^{k+1}} \sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i, h_j) = 1\,(1 \leqslant i < j \leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f; h_1 \ldots h_k)\, \sigma^*(f_1; h_1) \ldots \sigma^*(f_k; h_k)}{h_1 \ldots h_k}\right).$$

The main term can be evaluated by Lemma 8.3 with $l=k$, while the error term is

$$\leqslant \frac{x}{(\log x)^{k+1}} \sum_{h_1 \leqslant \xi_1/y} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f;h_1)\,\sigma(f_1;h_1)\ldots G(f;h_k)\,\sigma(f_k;h_k)}{h_1\ldots h_k}$$

$$\ll \frac{x}{(\log x)^{k+1}} \log\frac{\xi_1}{y}\cdots\log\frac{\xi_k}{y} \ll \frac{x}{\log x}$$

by k applications of Lemma 6.5. We obtain

$$\sum_{\substack{h_1 \leqslant \xi_1/y \\ (h_i,h_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{h_k \leqslant \xi_k/y} \frac{G(f;h_1\ldots h_k)\,\sigma^*(f_1;h_1)\ldots\sigma^*(f_k;h_k)\,\mathrm{li}_{h_1,\ldots,h_k}(f;x)}{h_1\ldots h_k}$$
$$= x\left(C(f)^{-1}\log\left(\frac{\log\xi_1}{\log y}\right)\cdots\log\left(\frac{\log\xi_k}{\log y}\right)+O((\log x)^{-1})\right)+O\left(\frac{x}{\log x}\right). \tag{8.12}$$

Since $\log\xi_i=\log f_i(x)=d\log x+O(1)$ for each $1\leqslant i\leqslant k$, we see that $\log\xi_i/\log y=du+O(1/\log x)$, whence the right-hand side of Eq. (8.12) becomes $C(f)^{-1}\,x\log^k(du)+O(x/\log x)$. This establishes the proposition. ∎

9. SMOOTH SHIFTED PRIMES

The purpose of this section is to establish Theorem 1.2. The proof of this theorem has a structure similar to that of Theorem 1.1, though of course it is much simpler to describe since we are dealing with a very concrete situation. First the number of smooth shifted primes $q+a$ is related combinatorially to the numbers of prime values of certain polynomials $f_{h,a}$ defined in Lemma 9.2 below; then the conjectured asymptotic formulas for the corresponding expressions $\pi(f_{h,a},\cdot)$ are used and the resulting sums analyzed as in the proof of Theorem 1.1. Where appropriate, therefore, we omit some of the details of the following proofs and refer the reader to the relevant arguments in earlier sections.

To begin with, we need to understand the behavior of the Dickman function $\rho(u)$ in the expanded range $u\leqslant 3$, which is the subject of the first lemma.

LEMMA 9.1. *We have*

$$1-\log u+\sum_{t^{1/u}<p\leqslant t^{1/2}} p^{-1}\log\left(\frac{\log t/p}{\log p}\right)=\rho(u)+O\left(\frac{1}{\log t}\right) \tag{9.1}$$

uniformly for $1\leqslant u\leqslant 3$ *and* $t>1$ *(where the sum in Eq.* (9.1) *is empty if* $u\leqslant 2$*).*

Proof. We could use partial summation to asymptotically evaluate the sum in Eq. (9.1) in terms of elementary functions and the dilogarithm function, and then verify that the resulting expression satisfies the differential-difference equation characterizing the function ρ. However, if we take it as known that

$$\Psi(t,t^{1/u})=t\rho(u)+O\left(\frac{t}{\log t}\right) \tag{9.2}$$

uniformly for $1\leqslant u\leqslant 3$ and $t>1$, then we can use the following simpler argument. For u in this range we can write

$$\begin{aligned}\Psi(t,t^{1/u})&=\#\{n\leqslant t\}-\sum_{t^{1/u}<p\leqslant t}\#\{n\leqslant t: p\mid n\}+\sum_{\substack{t^{1/u}<p_1<p_2\\ p_1p_2\leqslant t}}\#\{n\leqslant t: p_1p_2\mid t\}\\ &=t+O(1)-\sum_{t^{1/u}<p\leqslant t}\left(\frac{t}{p}+O(1)\right)\\ &\quad+\sum_{t^{1/u}<p_1\leqslant t^{1/2}}\ \sum_{p_1<p_2\leqslant t/p_1}\left(\frac{t}{p_1p_2}+O(1)\right)\end{aligned}$$

(where the final sum on each line is empty if $u\leqslant 2$). Using Mertens' formula this becomes

$$\begin{aligned}\Psi(t,t^{1/u})&=t-t\left(\log\left(\frac{\log t}{\log t^{1/u}}\right)+O\left(\frac{1}{\log t^{1/u}}\right)\right)+O(\pi(t))\\ &\quad+\sum_{t^{1/u}<p_1\leqslant t^{1/2}}\left(\frac{t}{p_1}\left(\log\left(\frac{\log t/p_1}{\log p_1}\right)+O\left(\frac{1}{\log p_1}\right)\right)+O(\pi(t/p_1))\right)\\ &=t\left(1-\log u+\sum_{t^{1/u}<p\leqslant t^{1/2}}p^{-1}\log\left(\frac{\log t/p}{\log p}\right)\right)+O\left(\frac{t}{\log t}\right).\end{aligned}$$

Comparing this to the known asymptotic formula (9.2) establishes the lemma. ∎

Next we must establish a result analogous to Proposition 2.6, giving an asymptotic formula for a weighted sum of a certain multiplicative function.

In the current situation, the sum in question is a simpler one-dimensional sum; also, the relevant constants $C(f_{h,a})$ can be evaluated explicitly, obviating the need for a result analogous to Proposition 2.5. The following lemma provides an asymptotic formula for the unweighted version of the appropriate sum.

LEMMA 9.2. *Let a be a nonzero integer and let* $f(t)=t(t-a)$, *so that* $f_{h,a}(t)=(ht+a)\,t$ *for any integer h. Then*

$$\sum_{h\leqslant t}\frac{C(f_{h,a})}{h}=\log t+O_a(1)$$

uniformly for $t\geqslant 1$.

Proof. Define the multiplicative function

$$g(n)=\prod_{\substack{p\mid n\\ p>2}}\frac{p-1}{p-2}.$$

For the particular polynomial $f_{h,a}$, it is an easy exercise to compute from the definition (1.1) of $C(f_{h,a})$ that

$$C(f_{h,a})=\begin{cases}0, & \text{if } 2\nmid ha \text{ or } (h,a)>1,\\ 2C_2\,g(ha), & \text{if } 2\mid ha \text{ and } (h,a)=1,\end{cases}$$

where C_2 is the twin primes constant

$$C_2=\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right).$$

If we assume that a is even, this gives

$$\sum_{h\leqslant t}\frac{C(f_{h,a})}{h}=2C_2\,g(a)\sum_{\substack{h\leqslant t\\ (h,a)=1}}\frac{g(h)}{h}. \tag{9.3}$$

Note that $g(n)\leqslant 2^{\omega(n)}\ll_\varepsilon n^\varepsilon$ for any positive ε (see the proof of Lemma 6.3), and that

$$\sum_{p\leqslant w}\frac{g(p)\log p}{p}=\frac{\log 2}{2}+\sum_{2<p\leqslant w}\frac{\log p}{p}\left(1+\frac{1}{p-2}\right)=\log w+O(1), \tag{9.4}$$

since the sum $\sum_{p>2} (\log p)/p(p-2)$ converges. We can thus apply Proposition A.3(b) with $\kappa=1$ to see that

$$\sum_{\substack{h\leqslant t\\(h,a)=1}} \frac{g(h)}{h} = c_a(g)\log t + O(\delta(a)),$$

where $c_a(g)$ is as defined in Eq. (A.28). In light of Eq. (9.3), therefore, to establish the lemma (for even a) it suffices to show that $2C_2\,g(a)\,c_a(g)=1$. But by the definition (A.28),

$$\begin{aligned} c_a(g) &= \prod_{p\mid a}\left(1-\frac{1}{p}\right)\prod_{p\nmid a}\left(1-\frac{1}{p}\right)\left(1+\frac{g_a(p)}{p}+\frac{g_a(p^2)}{p^2}+\cdots\right)\\ &= \prod_{p\mid a}\left(1-\frac{1}{p}\right)\prod_{p\nmid a}\frac{(p-1)^2}{p(p-2)}\\ &= \frac{1}{2}\prod_{\substack{p\mid a\\p>2}}\left(\frac{p-1}{p}\right)\cdot C_2^{-1}\prod_{\substack{p\mid a\\p>2}}\frac{p(p-2)}{(p-1)^2} = \frac{1}{2C_2\,g(a)}, \end{aligned}$$

as desired. This establishes the lemma when a is even, and the same argument slightly modified holds when a is odd. ∎

Next we analyze the weighted version of the sum in Lemma 9.2, analogous to (but again simpler than) the proof of Lemma 8.3 in Section 8.

LEMMA 9.3. *Let a be a nonzero integer and let $f(t)=t(t-a)$. Given real numbers $x\geqslant 1$ and $2\leqslant u\leqslant 3$, let $y=x^{1/u}$ and $\xi=x-a$. Then*

$$\sum_{h\leqslant \xi/y} C(f_{h,a})\,\mathrm{li}\left(f_{h,a};\frac{\xi}{h}\right) = \frac{x\log u}{\log x} + O\left(\frac{x}{\log^2 x}\right)$$

and

$$\begin{aligned} &\sum_{y<p\leqslant \xi^{1/2}}\ \sum_{p<h\leqslant \xi/p^2} C(f_{ph,a})\,\mathrm{li}\left(f_{ph,a};\frac{\xi}{ph}\right)\\ &\qquad = \frac{x}{\log x}\sum_{y<p\leqslant \xi^{1/2}} p^{-1}\log\left(\frac{\log \xi/p}{\log p}\right) + O\left(\frac{x}{\log^2 x}\right) \end{aligned}$$

uniformly for $x\geqslant 1+\max\{a,0\}$.

Proof. Using the same techniques as in the proofs of Lemmas 5.6 and 8.2, we can see that

$$\mathrm{li}\left(f_{h,a};\frac{\xi}{h}\right) = \frac{x}{h\log x\log(\xi/h)} + O\left(\frac{x}{h\log^3 x}\right),$$

and so

$$\sum_{h\leqslant \xi/y} C(f_{h,a})\,\mathrm{li}\left(f_{h,a};\frac{\xi}{h}\right)$$
$$=\frac{x}{\log x}\sum_{\substack{h\leqslant \xi/y\\(h,a)=1}}\frac{C(f_{h,a})}{h\log(\xi/h)}+O\left(\frac{x}{\log^3 x}\sum_{h\leqslant \xi/y}\frac{C(f_{h,a})}{h}\right).$$

The sum in the error term is $\ll \log \xi/y$ by Lemma 9.2, whence the error term is $\ll x/\log^2 x$ in its entirety. Using partial summation (see the proof of Lemma 8.3), we can show that Lemma 9.2 implies

$$\sum_{h\leqslant \xi/y}\frac{C(f_{h,a})}{h\log(\xi/h)}=\log\left(\frac{\log \xi}{\log y}\right)+O\left(\frac{1}{\log x}\right)=\log u+O\left(\frac{1}{\log x}\right).$$

This establishes the first claim of the lemma.

Similarly,

$$\sum_{y<p\leqslant \xi^{1/2}}\ \sum_{p<h\leqslant \xi/p^2} C(f_{ph,a})\,\mathrm{li}\left(f_{ph,a};\frac{\xi}{ph}\right)$$
$$=\frac{x}{\log x}\sum_{y<p\leqslant \xi^{1/2}}\frac{1}{p}\sum_{p<h\leqslant \xi/p^2}\frac{C(f_{ph,a})}{h\log(\xi/ph)}$$
$$+O\left(\frac{x}{\log^3 x}\sum_{y<p\leqslant \xi^{1/2}}\frac{1}{p}\sum_{p<h\leqslant \xi/p^2}\frac{C(f_{ph,a})}{h}\right).$$

Again the error term can be shown to be $\ll x/\log^2 x$, while the inner sum in the main term can be evaluated by a similar partial summation argument:

$$\sum_{h\leqslant \xi/p^2}\frac{C(f_{ph,a})}{h\log(\xi/ph)}=\log\left(\frac{\log x/p}{\log p}\right)+O\left(\frac{1}{\log x}\right).$$

This establishes the second part of the lemma. ∎

We are now prepared to establish Theorem 1.2.

Proof of Theorem 1.2. Let a be a nonzero integer and define $f(t)=t(t-a)$, so that $f_{h,a}(t)=(ht+a)\,t$. All constants implicit in the $\ll$ and O-notations in this proof may depend on the nonzero integer a and thus on the polynomial f as well. Let $x\geqslant 1+\max\{a,0\}$ be a real number, let u and U be real numbers satisfying $1\leqslant u\leqslant U<3$ (since the theorem is trivially true for $u<1$), and define $\xi=x-a$ and $y=x^{1/u}$. Reserving the letters p and q to denote primes always, we have

$$\begin{aligned}\Phi_a(x, y) &= \#\{q \leqslant x : q-a \text{ is } y\text{-smooth}\} \\ &= \pi(x) - \sum_{y<p\leqslant \xi} \#\{q \leqslant x : p \mid (q-a)\} + \sum_{\substack{y<p_1<p_2 \\ p_1p_2 \leqslant \xi}} \#\{q \leqslant x : p_1 p_2 \mid (q-a)\},\end{aligned}$$

where this last sum (and similar ones to follow) is empty if $y^2 > \xi$, which holds for x sufficiently large if and only if $u < 2$. If we make the substitutions $q = ph + a$ in the first sum and $q = p_1 p_2 h + a$ in the second, and transform the resulting expressions in a manner similar to the proof of Proposition 2.3, the end result is

$$\begin{aligned}\Phi_a(x, y) &= \pi(x) - \sum_{h \leqslant \xi/y} \#\{y < p \leqslant \xi/h : p,\ hp+a \text{ are both prime}\} \\ &\quad + \sum_{y<p_1\leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p_1^2} \#\{p_1 < p_2 \leqslant \xi/p_1 h : p_2,\ p_1 p_2 h + a \text{ are both prime}\} \\ &= \pi(x) - \sum_{h \leqslant \xi/y} \left(\pi\left(f_{h,a}; \frac{\xi}{h}\right) - \pi(f_{h,a}; y)\right) \\ &\quad + \sum_{y<p\leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p^2} \left(\pi\left(f_{ph,a}; \frac{\xi}{ph}\right) - \pi(f_{ph,a}; p)\right).\end{aligned} \tag{9.5}$$

Now by Lemma 7.3,

$$\sum_{h \leqslant \xi/y} \pi(f_{h,a}; y) \ll \frac{y}{\log^2 y} \sum_{h \leqslant \xi/y} G(f; h).$$

Since $G(f; p) = 1 + O(1/p)$ by Lemma 6.2, we can apply the estimate (A.6) following from Proposition A.1, with $\beta = 1$, to see that

$$\sum_{h \leqslant \xi/y} \pi(f_{h,a}; y) \ll \frac{y}{\log^2 y} \cdot \frac{\xi}{y} \ll \frac{x}{\log^2 x}.$$

Similarly,

$$\begin{aligned}\sum_{y<p\leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p^2} \pi(f_{ph,a}; p) &\ll \sum_{y<p\leqslant \xi^{1/2}} \frac{p}{\log^2 p} \sum_{h \leqslant \xi/p^2} G(f; ph) \\ &\ll \log \xi^{1/2} \sum_{y<p\leqslant \xi^{1/2}} \frac{pG(f; p)}{\log^3 p} \sum_{h \leqslant \xi/p^2} G(f; h) \\ &\ll \xi \log x \sum_{y<p\leqslant \xi^{1/2}} \frac{1}{p \log^3 p}\end{aligned}$$

since $G(f; p) \ll 1$. The resulting expression is $\ll \xi \log x/\log^3 y \ll x/\log^2 x$. Therefore from Eq. (9.5),

$$\Phi_a(x, y) = \frac{x}{\log x} - \sum_{h \leqslant \xi/y} \pi\left(f_{h,a}; \frac{\xi}{h}\right) + \sum_{y < p \leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p^2} \pi\left(f_{ph,a}; \frac{\xi}{ph}\right) + O\left(\frac{x}{\log^2 x}\right)$$

since $\pi(x) = x/\log x + O(x/\log^2 x)$ by the prime number theorem.

We now write this as

$$\Phi_a(x, y) = \frac{x}{\log x} - \sum_{h \leqslant \xi/y} C(f_{h,a}) \operatorname{li}\left(f_{h,a}; \frac{\xi}{h}\right) + \sum_{y < p \leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p^2} C(f_{ph,a}) \operatorname{li}\left(f_{ph,a}; \frac{\xi}{ph}\right) + H(x, y) + O\left(\frac{x}{\log^2 x}\right),$$

where

$$H(x, y) = -\sum_{h \leqslant \xi/y} E\left(f_{h,a}; \frac{\xi}{h}\right) + \sum_{y < p \leqslant \xi^{1/2}} \sum_{h \leqslant \xi/p^2} E\left(f_{ph,a}; \frac{\xi}{ph}\right). \tag{9.6}$$

We see from Lemma 9.3 that this is the same as

$$\begin{aligned}\Phi_a(x, y) &= \frac{x}{\log x}\left(1 - \log u + \sum_{y < p \leqslant \xi^{1/2}} p^{-1} \log\left(\frac{\log x/p}{\log p}\right)\right) + H(x, y) + O\left(\frac{x}{\log^2 x}\right) \\ &= \pi(x)\, \rho(u) + H(x, y) + O\left(\frac{\pi(x)}{\log x}\right) \qquad (9.7)\end{aligned}$$

by Lemma 9.1 and the prime number theorem. Moreover, assuming Hypothesis UH we can show by the method of the proof of Proposition 2.9 that $H(x, y) \ll \pi(x)/\log x$. This establishes Theorem 1.2. ▌

APPENDIX A

Sums of Multiplicative Functions

In this appendix we establish asymptotic formulæ for summatory functions associated with multiplicative functions $g(n)$, typified by the complete one-dimensional sum

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

We shall also consider the modified sum $M_g(x, q)$, where the sum is taken over only those integers coprime to q, as well as multidimensional analogues, where the several variables of summation are restricted to be coprime to one another. We are interested in such asymptotic formulæ when each multiplicative function g is constant on average over primes, as is usually the case for multiplicative functions that arise in sieve problems, for example. Specifically, we impose the condition on g that there is a constant $\kappa = \kappa(g)$ such that

$$\sum_{p \leqslant w} \frac{g(p) \log p}{p} = \kappa \log w + O_g(1) \tag{A.1}$$

for all $w \geqslant 2$.

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 [14], 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 [6, 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 A.1. *Suppose that $g(n)$ is a complex-valued multiplicative function such that the asymptotic formula* (A.1) *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*

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

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

$$\prod_{p \leqslant x} \left(1 + \frac{|g(p)|}{p}\right) \ll_g \log^\beta x \tag{A.3}$$

for all $x \geqslant 2$. *Then the asymptotic formula*

$$M_g(x) = c(g) \log^\kappa x + O_g((\log x)^{\beta-1}) \tag{A.4}$$

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

$$c(g) = \Gamma(\kappa+1)^{-1} \prod_p \left(1 - \frac{1}{p}\right)^\kappa \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\right). \tag{A.5}$$

The conditions (A.2) and (A.3) are usually very easily verified in practice. We remark that the condition (A.3) cannot hold with any $\beta < |\kappa|$ if g satisfies the asymptotic formula (A.1). The necessity that β be less than $\xi + 1$, so that the formula (A.4) 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. We also remark that from Eq. (A.4), it follows easily by partial summation that

$$\sum_{n<x} g(n) \ll_g x \log^{\beta-1} x \tag{A.6}$$

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

$$\begin{aligned}
\sum_{n \leqslant x} \frac{g(n) \log n}{n} &= \sum_{n \leqslant x} \frac{g(n)}{n} \sum_{p^r \| n} \log p^r \\
&= \sum_{r=1}^{\infty} \sum_{p \leqslant x^{1/r}} \frac{g(p^r) \log p^r}{p^r} \sum_{\substack{m \leqslant x/p^r \\ p \nmid m}} \frac{g(m)}{m} \\
&= \sum_{p \leqslant x} \frac{g(p) \log p}{p} \sum_{m \leqslant x/p} \frac{g(m)}{m} - \sum_{p \leqslant x} \frac{g(p) \log p}{p} \sum_{\substack{m \leqslant x/p \\ p \mid m}} \frac{g(m)}{m} \\
&\quad + \sum_{r=2}^{\infty} \sum_{p \leqslant x^{1/r}} \frac{g(p^r) \log p^r}{p^r} \sum_{\substack{m \leqslant x/p^r \\ p \nmid m}} \frac{g(m)}{m} \\
&= \Sigma_1 - \Sigma_2 + \Sigma_3,
\end{aligned} \tag{A.7}$$

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

$$\Delta(x) = \sum_{p \leqslant x} \frac{g(p) \log p}{p} - \kappa \log x, \tag{A.8}$$

then Σ_1 becomes

$$\Sigma_1 = \sum_{m \leqslant x} \frac{g(m)}{m} \sum_{p \leqslant x/m} \frac{g(p) \log p}{p} = \kappa \sum_{m \leqslant x} \frac{g(m)}{m} \log \frac{x}{m} + \sum_{m \leqslant x} \frac{g(m)}{m} \Delta\left(\frac{x}{m}\right). \tag{A.9}$$

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

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

by partial summation, we can rewrite Eq. (A.7) using Eq. (A.9) as

$$M_g(x) \log x - (\kappa+1) \int_2^x M_g(t)\, t^{-1} dt = E_g(x), \tag{A.10}$$

where we have defined

$$E_g(x) = (\kappa+1) \log 2 + \sum_{m \leqslant x} \frac{g(m)}{m} \Delta\left(\frac{x}{m}\right) - \Sigma_2 + \Sigma_3. \tag{A.11}$$

We integrate both sides of Eq. (A.10) against $x^{-1}(\log x)^{-\kappa-2}$, obtaining

$$\int_2^x M_g(u)\, u^{-1}(\log u)^{-\kappa-1}\, du - (\kappa+1) \int_2^x u^{-1}(\log u)^{-\kappa-2} \int_2^u M_g(t)\, t^{-1}\, dt\, du$$
$$= \int_2^x E_g(u)\, u^{-1}(\log u)^{-\kappa-2}\, du. \tag{A.12}$$

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; Eq. (A.12) 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 Eq. (A.10), divide by $\log x$, and rearrange terms to get

$$M_g(x) = (\kappa+1) \log^\kappa x \int_2^x E_g(u)\, u^{-1}(\log u)^{-\kappa-2}\, du + E_g(x) \log^{-1} x. \tag{A.13}$$

An upper bound for $E_g(x)$ is now needed. Since $\Delta(x)$ is bounded from its definition (A.8) and the asymptotic formula (A.1), we have

$$\sum_{m \leqslant x} \frac{g(m)}{m} \Delta\left(\frac{x}{m}\right) \ll \sum_{m \leqslant x} \frac{|g(m)|}{m}. \tag{A.14}$$

We also have

$$\sum_{m \leqslant x} \frac{|g(m)|}{m} \leqslant \prod_{p \leqslant x} \left(1 + \sum_{r=1}^{\infty} \frac{|g(p^r)|}{p^r}\right) \leqslant \prod_{p \leqslant x} \left(1 + \frac{|g(p)|}{p}\right) \prod_{p \leqslant x} \left(1 + \sum_{r=2}^{\infty} \frac{|g(p^r)|}{p^r}\right). \tag{A.15}$$

Because the sum $\sum_p \sum_{r=2}^{\infty} |g(p^r)|/p^r$ converges by the hypothesis (A.2), the last product in Eq. (A.15) is bounded as x tends to infinity. Therefore the hypothesis (A.3) implies that

$$\sum_{m \leqslant x} \frac{|g(m)|}{m} \ll \log^{\beta} x. \tag{A.16}$$

The terms Σ_2 and Σ_3 can be estimated by

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

and

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

and so both Σ_2 and Σ_3 are $\ll \log^{\beta} x$ by the estimate (A.16) and the hypothesis (A.2). Therefore, by the definition (A.11) of $E_g(x)$, we see that

$$E_g(x) \ll \log^{\beta} x. \tag{A.17}$$

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

$$\int_x^{\infty} E_g(u)\, u^{-1} (\log u)^{-\kappa-2}\, du \ll \int_x^{\infty} u^{-1} (\log u)^{\beta-\xi-2}\, du \ll (\log x)^{\beta-\xi-1}, \tag{A.18}$$

and so Eq. (A.13) and the bound (A.17) give us the asymptotic formula

$$M_g(x) = c(g) \log^\kappa x + O((\log x)^{\beta-1}) \tag{A.19}$$

for $x \geqslant 2$, where

$$c(g) = (\kappa+1) \int_2^\infty E_g(u)\, u^{-1} (\log u)^{-\kappa-2}\, du. \tag{A.20}$$

To complete the proof of the proposition, we need to show that $c(g)$ can be written in the form given by (A.5); we accomplish this indirectly, using the asymptotic formula (A.19). 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 (A.16) and partial summation, we see that $\zeta_g(s)$ converges absolutely for $s > 1$ (we shall only need to consider real values of s), and thus has an Euler product representation

$$\zeta_g(s) = \prod_p \left(1 + \frac{g(p)}{p^s} + \frac{g(p^2)}{p^{2s}} + \cdots\right) \tag{A.21}$$

for $s > 1$.

We can also use partial summation to write

$$\zeta_g(s+1) = s \int_1^\infty M_g(t)\, t^{-s-1}\, dt \tag{A.22}$$

for $s > 0$. Since $M_g(x) = 1$ for $1 \leqslant x < 2$, 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 (A.19), Eq. (A.22) becomes

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

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

$$\begin{aligned} s^\kappa \zeta_g(s+1) &= c(g) \int_0^\infty u^\kappa e^{-u}\,du \\ &\quad + O\left(\int_0^{s\log 2} (s^\xi + u^\xi)\, e^{-u}\,du + s^{\xi-\beta+1} \int_{s\log 2}^\infty u^{\beta-1} e^{-u}\,du \right) \\ &= c(g)\,\Gamma(\kappa+1) + O(s^{\xi-\beta+1} \log s^{-1}) \end{aligned} \tag{A.23}$$

as $s\to 0^+$, where the exponent $\xi-\beta+1$ is positive and at most 1 (since $\beta \geqslant |\kappa| \geqslant \xi$). Because the Riemann ζ-function satisfies $s\zeta(s+1)=1+O(s)$ as $s\to 0^+$, Eq. (A.23) implies

$$\zeta(s+1)^{-\kappa} \zeta_g(s+1) = c(g)\,\Gamma(\kappa+1) + O(s^{\xi-\beta+1}\log s^{-1}). \tag{A.24}$$

On the other hand, from Eq. (A.21) we certainly have the Euler product representation

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

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

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

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

Consequently, taking the limit of both sides of equation (A.24) as $s\to 0^+$ gives us

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

(where we have just shown that the product on the left-hand side converges), which is equivalent to (A.5). This establishes the proposition. ∎

From Proposition A.1 we can quickly derive a similar asymptotic formula for the restricted sum

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

Proposition A.2. *Suppose that $g(n)$ satisfies the hypotheses of Proposition* A.1. *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 $x \geqslant 2$ and all nonzero integers q, where

$$c_q(g) = \Gamma(\kappa+1)^{-1} \left(\frac{\phi(q)}{q}\right)^\kappa \prod_{p \nmid q} \left(1 - \frac{1}{p}\right)^\kappa \left(1 + \frac{g(p)}{p} + \frac{g(p^2)}{p^2} + \cdots\right) \tag{A.25}$$

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

Proof. We would like to apply Proposition A.1 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 $|g_q(n)| \leqslant |g(n)|$, and so the estimates (A.2) and (A.3) for g_q follow from the same estimates for g. We also have

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

from the assumption that g satisfies equation (A.1). Therefore g_q satisfies Eq. (A.1) 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 A.1, the only modification necessary is to include a factor of $\delta(q)$ on the right-hand sides of the estimates (A.14), (A.17), and (A.18) and in the error term in Eq. (A.19). Therefore, the application of Proposition A.1 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

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

the proposition is established. ▌

For convenience, we state below a particular case of Propositions A.1 and A.2, where the hypotheses have been somewhat simplified.

Proposition A.3. *Let $g(n)$ be a nonnegative multiplicative function satisfying $g(n) \ll n^{\alpha}$ for some constant $\alpha < 1/2$. Suppose that there is a real number κ (necessarily nonnegative) such that*

$$\sum_{p \leqslant w} \frac{g(p) \log p}{p} = \kappa \log w + O_g(1) \tag{A.26}$$

for all $w \geqslant 2$. Then:

(a) *the asymptotic formula*

$$\sum_{n \leqslant x} \frac{g(n)}{n} = c(g) \log^{\kappa} x + O_g(\log^{\kappa-1} x) \tag{A.27}$$

holds for all $x \geqslant 2$, where $c(g)$ is defined by the convergent product (A.5)*;*

(b) *the asymptotic formula*

$$\sum_{\substack{n \leqslant x \\ (n,q)=1}} \frac{g(n)}{n} = c_q(g) \log^{\kappa} x + O_g(\delta(q) \log^{\kappa-1} x)$$

holds uniformly for all $x \geqslant 2$ and all positive integers q, where

$$c_q(g) = c(g) \prod_{p \mid q} \left(1+\frac{g(p)}{p}+\frac{g(p^2)}{p^2}+\cdots\right)^{-1}$$

and

$$\delta(q) = 1 + \sum_{p \mid q} \frac{g(p) \log p}{p}. \tag{A.28}$$

Proof. We have

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

since $2-2\alpha>1$. Hence the condition (A.2) is satisfied. Also, since g is a nonnegative function, we have

$$\prod_{p\leqslant x}\left(1+\frac{|g(p)|}{p}\right)\leqslant \prod_{p\leqslant x}\exp\left(\frac{|g(p)|}{p}\right)=\exp\left(\sum_{p\leqslant x}\frac{g(p)}{p}\right)$$
$$=\exp(\kappa\log x+O_g(1))\ll_g \log^\kappa x$$

by the asymptotic formula (A.1), which shows that the condition (A.3) is also satisfied with $\beta=\kappa$. Therefore the two parts of this proposition are just special cases of Propositions A.1 and A.2, respectively. The form given in Eq. (A.28) for $c_q(g)$ is equivalent to the form given in Eq. (A.25), since the assumption that g is nonnegative implies that the sum $(1+g(p)/p+g(p^2)/p^2+\cdots)$ is nonzero. ∎

Finally, the following proposition analyzes the behavior of a general sum of several multiplicative functions, where the variables of summation are not permitted to have common factors.

PROPOSITION A.4. *Let k be a positive integer, and let $g_1(n)$, ..., $g_k(n)$ be nonnegative multiplicative functions. Suppose that there exists a real number $\alpha<1/2$ such that, for each $1\leqslant i\leqslant k$, the estimate $g_i(n)\ll n^\alpha$ holds for all positive integers n. Suppose further that κ_1, ..., κ_k are real numbers such that, for each $1\leqslant i\leqslant k$,*

$$\sum_{p\leqslant w}\frac{g_i(p)\log p}{p}=\kappa_i\log w+O_{g_i}(1) \tag{A.29}$$

for all $w\geqslant 2$. Then the asymptotic formula

$$\sum_{n_1\leqslant x_1}\cdots\sum_{\substack{n_k\leqslant x_k\\(n_i,n_j)=1\,(1\leqslant i<j\leqslant k)}}\frac{g_1(n_1)\ldots g_k(n_k)}{n_1\ldots n_k}$$
$$=c(g_1,\ldots,g_k)\prod_{i=1}^{k}(\log^{\kappa_i}x_i+O_{g_1,\ldots,g_k}((\log x_i)^{\kappa_i-1})) \tag{A.30}$$

holds for all $x_1, ..., x_k \geqslant 1$, *where* $c(g_1, ..., g_k)$ *is defined by the convergent product*

$$c(g_1, ..., g_k) = (\Gamma(\kappa_1+1)\cdots\Gamma(\kappa_k+1))^{-1}$$
$$\times \prod_p \left(1-\frac{1}{p}\right)^{\kappa_1+\cdots+\kappa_k} \left(1+\frac{g_1(p)+\cdots+g_k(p)}{p}+\frac{g_1(p^2)+\cdots+g_k(p^2)}{p^2}+\cdots\right). \tag{A.31}$$

Proof. All of the constants implicit in the O- and $\ll$ symbols in this proof may depend on the multiplicative functions g_i, and thus on k, α, and the κ_i as well. Define

$$S_k = S_k(g_1, ..., g_k; x_1, ..., x_k) = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)...g_k(n_k)}{n_1...n_k}.$$

We establish the desired asymptotic formula (A.30) for S_k by induction on k. The base case $k=1$ of the induction is exactly the statement of Proposition A.3(a). Supposing now that we know that the asymptotic formula (A.30) holds for sums of the form S_k, we wish to show that it holds for S_{k+1}.

We rewrite S_{k+1} as

$$S_{k+1} = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)...g_k(n_k)}{n_1...n_k} \sum_{\substack{m \leqslant x_{k+1} \\ (m, n_1...n_k)=1}} \frac{g_{k+1}(m)}{m}, \tag{A.32}$$

and we can use Proposition A.3(b) to obtain an asymptotic formula for this inner sum. For any index i, let $\gamma_i(n)$ be the multiplicative function defined on prime powers by

$$\gamma_i(p^\nu) = 1+\frac{g_i(p)}{p}+\frac{g_i(p^2)}{p^2}+\cdots$$

(independent of ν), which satisfies

$$\gamma_i(p) = 1+O\left(\frac{p^\alpha}{p}+\frac{p^{2\alpha}}{p^2}+\cdots\right) = 1+O(p^{-1+\alpha}) \tag{A.33}$$

by the hypothesized estimate on the size of g_i, and set

$$\delta(n) = 1+\sum_{p\mid n} \frac{g_{k+1}(p)\log p}{p}.$$

Then by Proposition A.3(b), Eq. (A.32) becomes

$$\begin{aligned} S_{k+1} = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \biggl\{ &\frac{g_1(n_1)\dots g_k(n_k)}{n_1\dots n_k} \\ &\times (c(g_{k+1})\, \gamma_{k+1}(n_1\dots n_k)^{-1} (\log x_{k+1})^{\kappa_{k+1}} \\ &+ O(\delta(n_1\dots n_k)(\log x_{k+1})^{\kappa_{k+1}-1})) \biggr\} \\ = c(g_{k+1})(\log x_{k+1})^{\kappa_{k+1}}\, T_k + O((\log x_{k+1})^{\kappa_{k+1}-1}\, U_k), \end{aligned} \tag{A.34}$$

where $c(g_{k+1})$ is defined in Eq. (A.5), and where we have defined

$$T_k = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\, \gamma_{k+1}(n_1)^{-1} \dots g_k(n_k)\, \gamma_{k+1}(n_k)^{-1}}{n_1\dots n_k}$$

(using the multiplicativity of γ_{k+1} and the fact that the n_i are pairwise coprime) and

$$U_k = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)\, \delta(n_1\dots n_k)}{n_1\dots n_k}.$$

First we obtain an asymptotic formula for T_k. The sum T_k is precisely of the form S_k with each g_i replaced by $g_i \gamma_{k+1}^{-1}$. By Eq. (A.33), for each $1 \leqslant i \leqslant k$ the multiplicative function $g_i \gamma_{k+1}^{-1}$ satisfies

$$\begin{aligned} \sum_{p \leqslant x} \frac{g_i(p)\, \gamma_{k+1}(p)^{-1} \log p}{p} &= \sum_{p \leqslant x} \frac{g_i(p) \log p}{p} (1 + O(p^{-1+\alpha})) \\ &= \sum_{p \leqslant x} \frac{g_i(p) \log p}{p} + O\biggl(\sum_{p \leqslant x} p^{-2+2\alpha} \log p \biggr) \\ &= \kappa_i \log x + O(1) \end{aligned}$$

since $\alpha < 1/2$. We may therefore invoke the induction hypothesis to show that the asymptotic formula

$$\begin{aligned} T_k &= \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1\leqslant i<j\leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\, \gamma_{k+1}(n_1)^{-1} \dots g_k(n_k)\, \gamma_{k+1}(n_k)^{-1}}{n_1\dots n_k} \\ &= c(g_1 \gamma_{k+1}^{-1}, \dots, g_k \gamma_{k+1}^{-1}) \prod_{i=1}^{k} (\log^{\kappa_i} x_i + O((\log x_i)^{\kappa_i - 1})) \end{aligned} \tag{A.35}$$

holds for T_k.

Next we obtain an estimate for U_k. By the definition of $\delta(n)$ we have

$$\begin{aligned} U_k &= \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)}{n_1 \dots n_k} \left(1 + \sum_{p \mid n_1 \dots n_k} \frac{g_{k+1}(p) \log p}{p}\right) \\ &= \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)}{n_1 \dots n_k} \\ &\quad + \sum_{p \leqslant x_1 \dots x_k} \frac{g_{k+1}(p) \log p}{p} \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k) \\ p \mid n_1 \dots n_k}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)}{n_1 \dots n_k} \\ &= S_k + \sum_{p \leqslant x_1 \dots x_k} \frac{g_{k+1}(p) \log p}{p} \sum_{i=1}^{k} V_i(p), \end{aligned} \tag{A.36}$$

where we have defined

$$V_i(p) = \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k) \\ p \mid n_i}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)}{n_1 \dots n_k}.$$

We can rewrite $V_k(p)$, for example, as

$$\begin{aligned} V_k(p) &= \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k-1)}} \cdots \sum_{n_{k-1} \leqslant x_{k-1}} \frac{g_1(n_1)\dots g_{k-1}(n_{k-1})}{n_1 \dots n_{k-1}} \sum_{\substack{n_k \leqslant x_k \\ (n_k, n_1 \dots n_{k-1})=1 \\ p \mid n_k}} \frac{g_k(n_k)}{n_k} \\ &= \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k-1)}} \cdots \sum_{n_{k-1} \leqslant x_{k-1}} \frac{g_1(n_1)\dots g_{k-1}(n_{k-1})}{n_1 \dots n_{k-1}} \left(\sum_{\nu=1}^{\infty} \frac{g_k(p^\nu)}{p^\nu} \sum_{\substack{m \leqslant x_k/p^\nu \\ (m, pn_1 \dots n_{k-1})=1}} \frac{g_k(m)}{m} \right). \end{aligned}$$

In this innermost sum of nonnegative terms, we can delete the restriction that n_k be coprime to p and extend the range of summation from $m \leqslant x_k/p^\nu$ to $m \leqslant x_k$; this yields (after renaming m to n_k) the upper bound

$$V_k(p) \leqslant \sum_{\substack{n_1 \leqslant x_1 \\ (n_i, n_j)=1\,(1 \leqslant i<j \leqslant k)}} \cdots \sum_{n_k \leqslant x_k} \frac{g_1(n_1)\dots g_k(n_k)}{n_1 \dots n_k} \sum_{\nu=1}^{\infty} \frac{g_k(p^\nu)}{p^\nu} = (\gamma_k(p)-1)\, S_k.$$

The same analysis shows that $(\gamma_i(p)-1)\, S_k$ is an upper bound for $V_i(p)$ for each $1 \leqslant i \leqslant k$.

With this upper bound, Eq. (A.36) becomes

$$U_k \leqslant S_k \left(1 + \sum_{i=1}^{k} \sum_{p \leqslant x_1 \dots x_k} \frac{g_{k+1}(p)(\gamma_i(p)-1) \log p}{p}\right).$$

By the induction hypothesis for S_k, we see that $S_k \ll (\log^{\kappa_1} x_1 \dots \log^{\kappa_k} x_k)$. Furthermore, both $g_{k+1}(p)/p$ and each $\gamma_i(p)-1$ are $\ll p^{-1+\alpha}$ (the latter by Eq. (A.33)). Therefore

$$U_k \ll (\log^{\kappa_1} x_1 \dots \log^{\kappa_k} x_k)\left(1+\sum_p p^{2\alpha-2}\log p\right) \ll \log^{\kappa_1} x_1 \dots \log^{\kappa_k} x_k$$

since $\alpha < 1/2$.

Using this estimate for U_k and the asymptotic formula (A.35) for T_k, we see that Eq. (A.34) becomes

$$\begin{aligned} S_k &= c(g_{k+1})\Big\{(\log x_{k+1})^{\kappa_{k+1}} c(g_1\gamma_{k+1}^{-1}, \dots, g_k\gamma_{k+1}^{-1}) \\ &\quad \times \prod_{i=1}^{k} (\log^{\kappa_i} x_i + O((\log x_i)^{\kappa_i - 1}))\Big\} \\ &\quad + O((\log x_{k+1})^{\kappa_{k+1}-1} \log^{\kappa_1} x_1 \dots \log^{\kappa_k} x_k) \\ &= c(g_{k+1})\, c(g_1\gamma_{k+1}^{-1}, \dots, g_k\gamma_{k+1}^{-1}) \prod_{i=1}^{k+1} (\log^{\kappa_i} x_i + O((\log x_i)^{\kappa_i - 1})). \end{aligned} \tag{A.37}$$

This would establish the lemma if only we had $c(g_1, \dots, g_{k+1})$ in place of the product $c(g_{k+1})\, c(g_1\gamma_{k+1}^{-1}, \dots, g_k\gamma_{k+1}^{-1})$. However, the Γ-factors of these two expressions are certainly equal by inspection. For each prime p, moreover, the power of $(1-1/p)$ in the infinite products of the two expressions equals $\kappa_1 + \cdots + \kappa_{k+1}$ in both cases, and we also have

$$\begin{aligned} &\gamma_{k+1}(p) \times \left(1 + \frac{g_1(p)\,\gamma_{k+1}(p)^{-1} + \cdots + g_k(p)\,\gamma_{k+1}(p)^{-1}}{p} \right. \\ &\qquad \left. + \frac{g_1(p^2)\,\gamma_{k+1}(p^2)^{-1} + \cdots + g_k(p^2)\,\gamma_{k+1}(p^2)^{-1}}{p^2} + \cdots \right) \\ &\quad = \gamma_{k+1}(p) + \frac{g_1(p) + \cdots + g_k(p)}{p} + \frac{g_1(p^2) + \cdots + g_k(p^2)}{p^2} + \cdots \\ &\quad = 1 + \frac{g_1(p) + \cdots + g_{k+1}(p)}{p} + \frac{g_1(p^2) + \cdots + g_{k+1}(p^2)}{p^2} + \cdots. \end{aligned}$$

Therefore the local factors in the infinite products of $c(g_{k+1}) \times c(g_1\gamma_{k+1}^{-1}, \dots, g_k\gamma_{k+1}^{-1})$ and $c(g_1, \dots, g_{k+1})$ are also equal, and so the asymptotic formula (A.37) is equivalent to the statement of the lemma. ∎

APPENDIX B

Prime Values of Linear Polynomials

In this appendix, we show that in the case of linear polynomials, Hypothesis UH is equivalent to a well-believed statement about the number of primes in short segments of arithmetic progressions, which for purposes of reference we shall call Hypothesis AP:

HYPOTHESIS AP. *Given real numbers $0 < \varepsilon < 1$ and $C > 1$, the asymptotic formula*

$$\pi(x; q, a) - \pi(x-y; q, a) = \frac{y}{\phi(q) \log x} + O\left(\frac{y}{\phi(q) \log^2 x}\right) \tag{B.1}$$

holds uniformly for all real numbers x and y satisfying $1 \leqslant y \leqslant x \leqslant y^C$ and all coprime integers $1 \leqslant a \leqslant q \leqslant y^{1-\varepsilon}$.

Of course, it is equivalent to ask only that the asymptotic formula (B.1) hold when x and y are sufficiently large, by adjusting the constant implicit in the O-notation if necessary. The conditions $x \leqslant y^C$ and $q \leqslant y^{1-\varepsilon}$ mean that the primes being counted are only polynomially large as a function of the number of terms y/q in the segment of the arithmetic progression. This restriction is not made merely for simplicity: Friedlander and Granville [5], expanding on the ground-breaking ideas of Maier, showed that even in the case $y = x$, the asymptotic formula (B.1) can fail when the size of q is $x/\log^D x$ for arbitrarily large D. Certainly one can construct by elementary methods, for any given y, an integer x so that the interval $[x-y, x]$ contains no primes whatsoever, so that (B.1) cannot hold without some restriction on x.

As remarked in Section 1, Hypothesis UH holds automatically for non-admissible polynomials. Note that a linear polynomial $qt+b$ (where by multiplying by -1 if necessary, we may assume that q is positive) is admissible if and only if $(b, q) = 1$, in which case $C(qt+b)$ is easily seen to equal $q/\phi(q)$. So for linear polynomials, Hypothesis UH can be stated as follows:

HYPOTHESIS UH1. *Given a constant $B > 0$, we have*

$$\pi(qt+b; T) = \frac{q}{\phi(q)} \operatorname{li}(qt+b; T) + O\left(\frac{q}{\phi(q)} \frac{T}{\log^2 T}\right) \tag{B.2}$$

uniformly for all real numbers $T \geqslant 1$ and all coprime integers q and b satisfying $1 \leqslant q \leqslant T^B$ and $|b| \leqslant T^B$.

Again it is clearly equivalent to ask that the asymptotic formula (B.2) hold for sufficiently large integer values of T. Before demonstrating the equivalence between Hypothesis UH1 and Hypothesis AP, we remark that $\mathrm{li}(F;T)$ can be expressed in terms of the ordinary logarithmic integral $\mathrm{li}(x)$ when $F(t)=qt+b$ is a linear polynomial. Assuming that q and b are positive, we can make the change of variables $v=qt+b$ in the integral in the definition (1.2) of $\mathrm{li}(F;T)$ to see that

$$\mathrm{li}(F;T)=\int_{\substack{0<t<T\\ qt+b\geqslant 2}}\frac{dt}{\log(qt+b)}=\frac{1}{q}\int_{\max\{b,2\}<v<qT+b}\frac{dv}{\log v}$$
$$=\frac{\mathrm{li}(qT+b)-\mathrm{li}(b)}{q}+O(1). \tag{B.3}$$

In fact, this formula holds without the assumption that q and b are positive, if we make the conventions that $\mathrm{li}(x)=-\mathrm{li}(|x|)$ if $x\leqslant -2$ and $\mathrm{li}(x)=0$ if $|x|\leqslant 2$.

We also need a lemma on the behavior of the logarithmic integral $\mathrm{li}(x)$.

LEMMA B.1. *We have*

$$\mathrm{li}(x)-\mathrm{li}(x-y)=\frac{y}{\log x}+O\left(\frac{y}{\log^2 x}\right)$$

uniformly for $2\leqslant y\leqslant x-2$.

Proof. It is easily seen by integration by parts that

$$\mathrm{li}(x)=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right). \tag{B.4}$$

First we consider the case where $x-x/\log x\leqslant y\leqslant x-2$. In this case, we have

$$\mathrm{li}(x-y)\leqslant \mathrm{li}\left(\frac{x}{\log x}\right)\ll\frac{x}{\log^2 x}$$

by Eq. (B.4). Also by (B.4),

$$\mathrm{li}(x)=\frac{x}{\log x}+O\left(\frac{x}{\log^2 x}\right)=\frac{y}{\log x}+O\left(\frac{x-y}{\log x}+\frac{x}{\log^2 x}\right).$$

But since $x-y\leqslant x/\log x$ we have $x\ll y$, and so we see that the error term is $\ll y/\log^2 x$, which establishes the lemma in this case.

In the remaining case, where $2 \leqslant y \leqslant x - x/\log x$, we note that

$$\operatorname{li}(x) - \operatorname{li}(x-y) = \int_{x-y}^{x} \frac{dt}{\log t} = \frac{x}{\log x} - \frac{x-y}{\log(x-y)} + O\left(\int_{x-y}^{x} \frac{dt}{\log^2 t}\right)$$

by integration by parts. The integral in the error term is over an interval of length y, and the integrand never exceeds $(\log(x-y))^{-2} \ll (\log x)^{-2}$, and so the error term is $\ll y/\log^2 x$. As for the main term, the fact that $y \leqslant x - x/\log x$ implies that $(1 - y/x)^{-1} \leqslant \log x$, and so we can write

$$\begin{aligned}
\frac{x}{\log x} - \frac{x-y}{\log(x-y)} &= \frac{x}{\log x} - \frac{x-y}{\log x + \log(1-y/x)} \\
&= \frac{x}{\log x} - \frac{x-y}{\log x}\left(1 + O\left(\frac{\log(1-y/x)^{-1}}{\log x}\right)\right) \\
&= \frac{y}{\log x} + O\left(\frac{y}{\log^2 x} A\left(1 - \frac{y}{x}\right)\right),
\end{aligned}$$

where we have defined the function $A(t) = t \log t^{-1}/(1-t)$. One can check that this function A is bounded on the interval (0, 1), and so this error term is simply $O(y/\log^2 x)$, which establishes the lemma. ∎

As a consequence of Lemma B.1, we see that the asymptotic formula (B.1) in Hypothesis AP can be restated as

$$\pi(x; q, a) - \pi(x-y; q, a) = \frac{\operatorname{li}(x) - \operatorname{li}(x-y)}{\phi(q)} + O\left(\frac{y}{\phi(q) \log^2 x}\right). \tag{B.5}$$

On the other hand, as a consequence of Eq. (B.3), the asymptotic formula (B.2) in Hypothesis UH1 can be restated as

$$\pi(qt+b; T) = \frac{\operatorname{li}(qT+b) - \operatorname{li}(b)}{\phi(q)} + O\left(\frac{q}{\phi(q)} \frac{T}{\log^2 T}\right). \tag{B.6}$$

We are now able to show that Hypothesis UH1 and Hypothesis AP are equivalent statements.

Proof that Hypothesis UH1 *implies Hypothesis* AP. Let $0 < \varepsilon < 1$ and $C > 1$ be real numbers, let x and y be sufficiently large real numbers satisfying $y \leqslant x \leqslant y^C$, and let a and q be coprime integers satisfying $1 \leqslant a \leqslant q \leqslant y^{1-\varepsilon}$. We want to show that the asymptotic formula (B.5) holds for $\pi(x; q, a) - \pi(x-y; q, a)$.

Suppose first that x and y are integer multiples of q. Then

$$\begin{aligned}\pi(x;q,a)-\pi(x-y;q,a) &= \#\{x-y<p\leqslant x : p\equiv a \pmod q\}\\ &= \#\{0<m\leqslant y/q : qm+(x-y)+a \text{ is prime}\}\\ &= \pi(qt+b;T)+O(1), \qquad\qquad \text{(B.7)}\end{aligned}$$

where we have defined $b=x-y+a$ and $T=y/q$. For these values of b and T we have

$$1\leqslant \max\{b,q\}=\max\{x-y+a,q\}\leqslant x+q\leqslant y^C+y^{1-\varepsilon}.$$

If we choose $B>C/\varepsilon$, then this implies for y sufficiently large

$$1\leqslant \max\{b,q\}<(y^{\varepsilon})^B\leqslant\left(\frac{y}{q}\right)^B=T^B.$$

Therefore, we may apply Hypothesis UH1 with this choice of B to the expression $\pi(qt+b,T)$. Using the equivalent formulation (B.6) of Hypothesis UH1, Eq. (B.7) becomes

$$\begin{aligned}&\pi(x;q,a)-\pi(x-y;q,a)\\ &\quad=\frac{\mathrm{li}(qT+b)-\mathrm{li}(b)}{\phi(q)}+O\left(\frac{q}{\phi(q)}\frac{T}{\log^2 T}\right)+O(1)\\ &\quad=\frac{\mathrm{li}(x+a)-\mathrm{li}(x-y+a)}{\phi(q)}+O\left(\frac{q}{\phi(q)}\frac{y/q}{\log^2(y/q)}\right)\\ &\quad=\frac{\mathrm{li}(x)-\mathrm{li}(x-y)}{\phi(q)}+O\left(\frac{a}{\phi(q)}\right)+O\left(\frac{y}{\phi(q)\log^2(y/q)}\right).\end{aligned}$$

Using the assumptions on the sizes of x, y, q, and a, the error terms can be replaced by $O(y/(\phi(q)\log^2 x))$, and so we have derived the desired asymptotic formula (B.5).

This shows that Hypothesis UH1 implies Hypothesis AP in the case where x and y are integer multiples of q. However, if we let x' and y' be the integer multiples of q closest to x and y, respectively, then $\pi(x';q,a)=\pi(x;q,a)+O(1)$ and similarly for $\pi(x'-y';q,a)$. Therefore Hypothesis UH1 implies Hypothesis AP for any values of x and y in the appropriate range.

Proof that Hypothesis AP *implies Hypothesis* UH1. Let B be a positive real number, let T be a sufficiently large real number, and let q and b be coprime integers satisfying $1\leqslant q\leqslant T^B$ and $|b|\leqslant T^B$. We want to show that the asymptotic formula (B.6) holds for $\pi(qt+b;T)$.

Suppose first that b is positive. If we let a denote the smallest positive integer congruent to $b \pmod q$, then

$$\begin{aligned}\pi(qt+b; T) &= \#\{1 \leqslant m \leqslant T : qm+b \text{ is prime}\} \\ &= \#\{b < n \leqslant qT+b : n \text{ is prime}, \ n \equiv a \pmod q\} \\ &= \pi(x; q, a) - \pi(x-y; q, a),\end{aligned} \tag{B.8}$$

where we have defined $x = qT+b$ and $y = qT$. Clearly we have $1 \leqslant a \leqslant q$ and $1 \leqslant y \leqslant x$. Moreover, if we choose $C > B+1$, then

$$x = qT + b \leqslant T^{B+1} + T^B < T^C \leqslant (qT)^C = y^C$$

when T is sufficiently large; and if we also let $\varepsilon = (B+1)^{-1}$, then

$$q = q^{1-\varepsilon} q^{\varepsilon} \leqslant q^{1-\varepsilon} (T^B)^{\varepsilon} = (qT)^{1-\varepsilon} \leqslant y^{1-\varepsilon}. \tag{B.9}$$

Therefore we can apply Hypothesis AP with these values of C and ε to the difference $\pi(x; q, a) - \pi(x-y; q, a)$. Using the equivalent formulation (B.5) of Hypothesis AP, Eq. (B.8) becomes

$$\begin{aligned}\pi(qt+b; T) &= \frac{\operatorname{li}(x) - \operatorname{li}(x-y)}{\phi(q)} + O\left(\frac{y}{\phi(q) \log^2 x}\right) \\ &= \frac{\operatorname{li}(qT+b) - \operatorname{li}(b)}{\phi(q)} + O\left(\frac{qT}{\phi(q) \log^2 T}\right)\end{aligned}$$

(since $\log x \geqslant \log T$), which is the desired asymptotic formula (B.6).

This shows that Hypothesis AP implies Hypothesis UH1 in the case where b is positive. Notice that $\pi(qt+b; T)$ counts the number of primes in the set $\{q+b, 2q+b, ..., qT-q+b, qT+b\}$; on the other hand, $\pi(qt-(qT+b); T)$ counts the number of primes in the set $\{-(qT-q+b), ..., -(q+b), -b\}$, which differs from the aforementioned set only by the negative signs on each element and a difference of one element at each end. Consequently, $\pi(qt+b; T) = \pi(qt-(qT+b); T) + O(1)$, and so if b is so negative that $qT+b$ is also negative, we can replace b by $-(qT+b)$ and reduce to the case already considered.

Finally, consider the case where b is negative but $qT+b$ is positive. Replacing b by $qT+b$ as in the previous paragraph if necessary, we may assume that $qT+b \geqslant |b|$. In this case the analogous equation to (B.8) is

$$\begin{aligned}\pi(qt+b; T) &= \#\{1 \leqslant m \leqslant T : qm+b \text{ is prime}\} \\ &= \#\{1 \leqslant n \leqslant qT+b : n \text{ is prime}, \ n \equiv a \pmod q\} \\ &\quad + \#\{b < n \leqslant -1 : |n| \text{ is prime}, \ n \equiv a \pmod q\} \\ &= \pi(x_1; q, a) + \pi(x_2; q, q-a),\end{aligned} \tag{B.10}$$

with a defined (as above) to be the smallest positive integer congruent to $b \pmod q$, and where we have defined $x_1 = qT + b = qT - |b|$ and $x_2 = |b|$. Notice that

$$qT + b \geqslant |b| \quad \Rightarrow \quad qT/2 \geqslant |b| \quad \Rightarrow \quad x_1 = qT - |b| \geqslant qT/2.$$

Notice also that $q \leqslant (qT)^{1-\varepsilon}$ was shown in Eq. (B.9) (where $\varepsilon = (B+1)^{-1}$ as before). If we choose a real number ε' satisfying $0 < \varepsilon' < \min\{(B+1)^{-1}, (2B)^{-1}, 1/3\}$, we see that

$$q \leqslant (qT)^{1-\varepsilon} < (2x_1)^{1-\varepsilon} < x_1^{1-\varepsilon'}$$

since T is sufficiently large. Consequently we may apply Hypothesis AP to $\pi(x_1; q, a)$ with $x = y = x_1$; the equivalent formulation (B.5) gives us

$$\pi(x_1; q, a) = \frac{\mathrm{li}(x_1)}{\phi(q)} + O\left(\frac{x_1}{\phi(q)\log^2 x_1}\right). \tag{B.11}$$

The idea is now to apply a similar argument to the other term $\pi(x_2; q, q-a)$ in Eq. (B.10) when x_2 is reasonably large, and to bound this expression trivially when x_2 is rather small.

In this vein, assume first that

$$x_2 > \sqrt{T} \qquad \text{and} \qquad x_2^{1-\varepsilon'} \geqslant q. \tag{B.12}$$

In this case, we can apply Eq. (B.5) to $\pi(x_2; q, q-a)$ with $x = y = x_2$, resulting in

$$\pi(x_2; q, q-a) = \frac{\mathrm{li}(x_2)}{\phi(q)} + O\left(\frac{x_2}{\phi(q)\log^2 x_2}\right).$$

This, together with Eq. (B.11), means that Eq. (B.10) becomes

$$\begin{aligned}
\pi(qt+b; T) &= \frac{\mathrm{li}(x_1)}{\phi(q)} + O\left(\frac{x_1}{\phi(q)\log^2 x_1}\right) + \frac{\mathrm{li}(x_2)}{\phi(q)} + O\left(\frac{x_2}{\phi(q)\log^2 x_2}\right) \\
&= \frac{\mathrm{li}(qT-|b|) + \mathrm{li}(|b|)}{\phi(q)} + O\left(\frac{qT-|b|}{\phi(q)\log^2 x_1} + \frac{|b|}{\phi(q)\log^2 x_1}\right) \\
&= \frac{\mathrm{li}(qT+b) - \mathrm{li}(b)}{\phi(q)} + O\left(\frac{q}{\phi(q)}\frac{T}{\log^2 T}\right)
\end{aligned}$$

(since $\log x_1 \geqslant \log x_2 \geqslant \log \sqrt{T}$), using the convention about $\mathrm{li}(b)$ mentioned after Eq. (B.3).

On the other hand, assume that one of the two conditions (B.12) fails for x_2. If $x_2 \leqslant \sqrt{T}$ then certainly $\pi(x_2; q, q-a) \leqslant \sqrt{T}$. Also, if $x_2^{1-\varepsilon'} < q$ then

$$\pi(x_2; q, q-a) \leqslant 1 + \frac{x_2}{q} \ll x_2^{\varepsilon'} = |b|^{\varepsilon'} \leqslant (T^B)^{\varepsilon'} < \sqrt{T}$$

as well. Using this and the asymptotic formula (B.11), Eq. (B.10) now becomes

$$\begin{aligned} \pi(qt+b; T) &= \frac{\operatorname{li}(x_1)}{\phi(q)} + O\left(\frac{x_1}{\phi(q)\log^2 x_1}\right) + O(\sqrt{T}) \\ &= \frac{\operatorname{li}(qT-|b|)}{\phi(q)} + O\left(\frac{qT-|b|}{\phi(q)\log^2 x_1} + \sqrt{T}\right) \\ &= \frac{\operatorname{li}(qT+b)}{\phi(q)} + O\left(\frac{q}{\phi(q)}\frac{T}{\log^2 T}\right), \end{aligned} \tag{B.13}$$

since $\log x_1 \gg \log T$.

Now

$$\frac{-\operatorname{li}(b)}{\phi(q)} = \frac{\operatorname{li}(|b|)}{\phi(q)} \leqslant \frac{x_2}{q/\log\log q} \leqslant \frac{\max\{\sqrt{T}, q^{(1-\varepsilon')^{-1}}\}}{q/\log\log q}$$

since x_2 fails at least one of the conditions (B.12). Because $(1-\varepsilon')^{-1} < 3\varepsilon'/2$ by the restriction $\varepsilon' < 1/3$, we have

$$\frac{-\operatorname{li}(b)}{\phi(q)} \ll \max\{\sqrt{T}, q^{3\varepsilon'/2}\} \leqslant \max\{\sqrt{T}, (T^B)^{3/4B}\} \leqslant T^{3/4} \ll \frac{q}{\phi(q)}\frac{T}{\log^2 T}$$

since $\varepsilon' < (2B)^{-1}$. Therefore the term $-\operatorname{li}(b)/\phi(q)$ may be inserted into the last line of Eq. (B.13), which establishes the asymptotic formula (B.6) in this last case.

ACKNOWLEDGMENTS

The author acknowledges the support of National Science Foundation Grant DMS 9304580 and Natural Sciences and Engineering Research Council Grant A5123. The author also thanks the anonymous referee, whose thorough reading of the manuscript greatly reduced the number of typographical errors herein.

REFERENCES

1. W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math. (2)* **139**, No. 3 (1994), 703–722.

2. P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.
3. C. Dartyge, G. Martin, and G. Tenenbaum, Polynomial values free of large prime factors, *Periodica Math. Hungarica* **43**, No. 1–2 (2001), 111–119.
4. L. E. Dickson, A new extension of Dirichlet's theorem on prime numbers, *Messenger Math.* **33** (1903), 155–161.
5. J. Friedlander and A. Granville, Limitations to the equi-distribution of primes, I, *Ann. of Math. (2)* **129**, No. 2 (1989), 363–382.
6. H. Halberstam and H.-E. Richert, "Sieve Methods," Academic Press, London, 1974.
7. G. H. Hardy and J. E. Littlewood, Some problems of "partitio numerorum." III. On the expression of a number as a sum of primes, *Acta Math.* **44** (1923), 1–70.
8. A. Hildebrand and G. Tenenbaum, Integers without large prime factors, *J. Théor. Nombres Bordeaux* **5**, No. 2 (1993), 411–484.
9. M. N. Huxley, A note on polynomial congruences, *in* "Recent Progress in Analytic Number Theory," Vol. 1, pp. 193–196, Academic Press, London/New York, 1981.
10. T. Nagel, Généralisation d'un théorème de Tchebycheff, *J. Math. Pures Appl. (8)* **4** (1921), 343–356.
11. M. Nair and G. Tenenbaum, Short sums of certain arithmetic functions, *Acta Math.* **180**, No. 1 (1998), 119–144.
12. A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; erratum, **5** (1958), 259.
13. C. L. Stewart, On the number of solutions of polynomial congruences and Thue equations, *J. Amer. Math. Soc.* **4**, No. 4 (1991), 793–835.
14. E. Wirsing, Das asymptotische Verhalten von Summen über multiplikative Funktionen, *Math. Ann.* **143** (1961), 75–102.