JOINT DISTRIBUTION IN RESIDUE CLASSES OF FAMILIES OF POLYNOMIALLY-DEFINED MULTIPLICATIVE FUNCTIONS II

AKASH SINGHA ROY

Abstract. We study the distribution of families of multiplicative functions among the coprime residue classes to moduli varying uniformly in a wide range, extending a criterion of Narkiewicz and obtaining essentially best possible analogues of the Siegel–Walfisz Theorem for large classes of multiplicative functions. We also uncover some surprising phenomena on when equidistribution fails. This paper is a sequel to a previous paper with the same title, and we obtain some useful variants of some of the main results therein. Our results are completely uniform in the modulus, optimal in various parameters and hypothesis, and also have applications for most interesting (integer–valued) multiplicative functions, such as Euler's totient $\varphi(n)$, the sum of divisors functions $\sigma(n)$, coefficients of Eisensetein series etc., and to the joint distribution of collections/families of such functions. One of the primary themes behind our arguments is the quantitative detection of a certain mixing (or ergodicity) phenomenon in multiplicative groups via methods belonging to the 'anatomy of integers', but we also use several tools from arithmetic and algebraic geometry, character sums, and linear algebra over rings; these methods may be potentially useful in various other problems as well.

1. Introduction

We say that an integer-valued arithmetic function g is uniformly distributed (or equidistributed) modulo q if $\#\{n \le x : g(n) \equiv b \pmod q\} \sim x/q$ as $x \to \infty$, for each residue class b mod q. However, for multiplicative functions, this is not the correct notion of uniform distribution to consider; for example, it can be shown that the Euler totient function $\varphi(n)$ is almost always divisible by any fixed integer q, and hence is not equidistributed modulo any $q > 1$. Motivated by this, Narkiewicz in [27] introduces the notion of weak uniform distribution: He defines an arithmetic function $f : \mathbb{N} \to \mathbb{Z}$ to be weakly uniformly distributed (or weakly equidistributed or WUD) modulo an integer q if there are infinitely many positive integers n for which $\gcd(f(n), q) = 1$, and if

$$\#\{n \le x : f(n) \equiv a \pmod q\} \sim \frac{1}{\varphi(q)} \#\{n \le x : \gcd(f(n), q) = 1\}, \quad \text{as } x \to \infty,$$

for each coprime residue class a mod q. Extending this to families of arithmetic functions, we say that the integer-valued arithmetic functions $f_1, \dots, f_K$ are jointly weakly equidistributed (or jointly WUD) modulo q if there are infinitely many n for which $\gcd(f_1(n) \cdots f_K(n), q) = 1$, and if for all coprime residue classes $a_1, \dots, a_K$ mod q, we have

2020 *Mathematics Subject Classification.* Primary 11A25; Secondary 11N36, 11N37, 11N64, 11N69.

Key words and phrases. multiplicative function, uniform distribution, equidistribution, weak uniform distribution, joint distribution.

(1.1)

$$\#\{n \le x : \forall i \in [K],\ f_i(n) \equiv a_i \pmod q\} \sim \frac{1}{\varphi(q)^K}\#\{n \le x : \gcd(f_1(n)\cdots f_K(n), q) = 1\}$$

as $x \to \infty$. (Here and below, $[K]$ denotes the set $\{1, \dots, K\}$.)

The phenomenon of weak equidistribution to fixed moduli has been deeply studied for a single as well as for collections of multiplicative functions by several authors, prominent among them being Narkiewicz [27, 28, 29, 30, 31], Rayner [32, 40, 41], Śliwa [49], Dobrowolski [31, Theorem 6.12], Fomenko [15], Dence and Pomerance [12]. For example, while Narkiewicz [27] shows that $\varphi(n)$ is weakly equidistributed precisely modulo those q that are *coprime to* 6, Śliwa [49] shows that the sum of divisors function $\sigma(n) = \sum_{d \mid n} d$ is WUD mod q exactly when q is *not a multiple of* 6. Śliwa's result was generalized to the functions $\sigma_r(n) := \sum_{d \mid n} d^r$ (some of which are Fourier coefficients of the Eisenstein series), by Narkiewicz and Rayner [30, 31, 32, 40, 41]. In [29], Narkiewicz gives a general criterion for deciding weak equidistribution in collections of "polynomially-defined" multiplicative functions, namely those that can be controlled by the values of polynomials at the first few powers of all primes; we shall state this criterion in the next section. (See [27, Theorem 1] for his earlier criterion for a single multiplicative function.)

In all these results, the modulus q is fixed, so a natural and interesting extension of this question is whether weak equidistribution continues to hold as q varies uniformly in a suitable range depending on the stopping point x of inputs. A prototype of this result is the Siegel–Walfisz Theorem for primes in arithmetic progressions, but we seek an analogue of this theorem with primes replaced by values of multiplicative functions. To formalize this, given a constant $K_0 > 0$, we shall say that integer-valued arithmetic functions $f_1, \dots, f_K$ are jointly weakly equidistributed (or jointly WUD) mod q, uniformly for $q \le (\log x)^{K_0}$, if:

(i) For every such q, $\prod_{i=1}^K f_i(n)$ is coprime to q for infinitely many n, and

(ii) The relation (1.1) holds as $x \to \infty$, uniformly in moduli $q \le (\log x)^{K_0}$ and in coprime residue classes $a_1, \dots, a_K$ mod q. Explicitly, this means that for any $\epsilon > 0$, there exists $X(\epsilon) > 0$ such that the ratio of the left hand side of (1.1) to the right hand side lies in $(1 - \epsilon, 1 + \epsilon)$ for all $x > X(\epsilon)$, $q \le (\log x)^{K_0}$ and coprime residues $a_1, \dots, a_K$ mod q.

If $K = 1$ and $f_1 = f$, we shall simply say that f is weakly equidistributed (or WUD) mod q, uniformly for $q \le (\log x)^{K_0}$.

The question of weak equidistribution to varying moduli seems to have been first studied in [23], [36] and [38], which made some partial progress towards obtaining a uniform analogue of Narkiewicz's aforementioned criterion for a single "polynomially-defined" multiplicative function. But many of these arguments could not be generalized to families of multiplicative functions (and as such, could not be used to give uniform analogues of Narkiewicz's general criterion in [29]). Moreover, even for a single function, they were still far from being satisfactory uniform analogues of Narkiewicz's single-function criterion (in [27]), since it needed several additional hypotheses. In fact, the work in [23], [36] and [38] could not even be applied to give satisfactory weak equidistribution results for the functions $\sigma_r(n)$ to varying moduli.

However in recent work [48], we have been able to give complete uniform extensions of Narkiewicz's general criterion in [29] for families of multiplicative functions to a single varying modulus q. Our results are optimal in both the range of uniformity and the arithmetic restrictions on q, as well as in various other parameters. For instance, we were able to show that under two technical conditions (which we will prove to be unavoidable in this manuscript), a given family of polynomially-defined multiplicative functions is jointly WUD *exactly* to those moduli q that satisfy Narkiewicz's criterion, and also vary uniformly up to small powers of $\log x$, where these powers are all essentially optimal as well. Applications of our theorems also extended the results of Narkiewicz, Rayner, Dobrowolski, Fomenko and others.

In [48], we also showed that weak equidistribution is restored in the full "Siegel-Walfisz range" $q \le (\log x)^{K_0}$ provided we restrict attention to inputs n having sufficiently many large prime factors counted with multiplicity. A smaller threshold becomes sufficient (thus ensuring equidistribution among larger sample spaces of inputs) whenever q is squarefree. Such constraints were governed by a certain quantitative ergodicity (or mixing) phenomena in the multiplicative group mod q coming from values of polynomials in the unit group, however to detect this mixing, we required methods from the "anatomy of integers", along with character sum bounds, "pure analytic" ideas coming from a modification of the Landau–Selberg–Delange method as well as tools belonging to the realms of arithmetic and algebraic geometry.

In this manuscript, we continue the investigations in [48]. Modifying the methods therein, we study the equidistribution of families of "polynomially-defined" multiplicative functions among those inputs n whose factorizations are reasonably well-behaved. We obtain cleaner versions of the input restrictions in [48] alluded to above. We also investigate when those input restrictions can be weakened if some reasonable additional control is available on the behavior of the given multiplicative functions at some higher prime powers. Finally, we demonstrate the necessity of the two technical hypotheses assumed in the main results in [48].

2. The setting and the main results

We say that an arithmetic function f is polynomially-defined if there exists $V \ge 1$ and polynomials $\{W_v\}_{1 \le v \le V}$ with integer coefficients satisfying $f(p^v) = W_v(p)$ for all primes p and all $v \in [V]$. The following set-up will be assumed in the entire manuscript: Fix $K, V \ge 1$.

- Consider multiplicative functions $f_1, \ldots, f_K \colon \mathbb{N} \to \mathbb{Z}$ and polynomials $\{W_{i,v}\}_{\substack{1 \le i \le K \\ 1 \le v \le V}} \subset \mathbb{Z}[T]$ satisfying $f_i(p^v) = W_{i,v}(p)$ for any prime p, any $i \in [K]$ and $v \in [V]$.

- Consider the multiplicative function $f := \prod_{i=1}^K f_i$ and the polynomials $\{W_v\}_{1 \le v \le V} \subset \mathbb{Z}[T]$ given by $W_v := \prod_{i=1}^K W_{i,v}$, so that $f(p^v) = W_v(p)$ for all primes p and all $v \in [V]$.

- For any q and $v \in [V]$, define $R_v(q) := \{u \in U_q : \prod_{i=1}^K W_{i,v}(u) \in U_q\} = \{u \in U_q : W_v(u) \in U_q\}$; here $U_q := (\mathbb{Z}/q\mathbb{Z})^\times$ denotes the multiplicative group mod q, so that saying "$r \in U_q$" for an integer r is synonymous with saying that "$\gcd(r, q) = 1$".

- Fix $k \in [V]$ and assume that $\{W_{i,k}\}_{1 \le i \le K}$ are all nonconstant. We say that a positive integer q is k-admissible (with respect to the family $(W_{i,v})_{\substack{1 \le i \le K \\ 1 \le v \le V}}$) if the set $R_k(q)$ is nonempty but the sets $R_v(q)$ are empty for all $v < k$.

- For each $v \in [V]$, let $\alpha_v := \alpha_v(q) := \frac{1}{\varphi(q)} \# R_v(q)$, $D_v := \deg W_v = \sum_{i=1}^K \deg W_{i,v}$, $D := D_k = \sum_{i=1}^K \deg W_{i,k}$, and $D_{\min} := \min_{1 \le i \le K} \deg W_{i,k}$. Note that if q is k-admissible, then $\alpha_v = 0$ for $1 \le v < k$, while $\alpha_k \gg_{W_k} (\log\log(3q))^{-D}$ by the Chinese Remainder Theorem and a standard argument using Mertens' Theorem.
- We define $\mathcal{Q}(k; f_1, \cdots, f_K)$ to be the set of all k-admissible integers q such that for every tuple $(\chi_1, \ldots, \chi_K) \neq (\chi_0, \ldots, \chi_0)$ of Dirichlet characters[1] mod q for which the product $\prod_{i=1}^K \chi_i \circ W_{i,k}$ is trivial on $R_k(q)$ [2], there exists a prime p satisfying

$$\sum_{j \ge 0} \frac{\chi_1(f_1(p^j)) \cdots \chi_K(f_K(p^j))}{p^{j/k}} = 0. \tag{2.1}$$

Narkiewicz's criterion [29, Theorem 1] in this setting is then stated as follows.

Theorem N. *Fix a k-admissible integer q. The functions $f_1, \ldots, f_K$ are jointly weakly equidistributed modulo q if and only if $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$.*

In [48], we extended Theorem N to obtain results that are completely uniform in the modulus q varying up to a fixed but arbitrary power of $\log x$. Our results needed to impose two additional hypotheses that we will in this manuscript prove to be necessary. To describe these hypothesis, we need to define a few terms. First, we say that the polynomials $\{F_i\}_{1 \le i \le K} \subset \mathbb{Z}[T]$ are multiplicatively independent (over $\mathbb{Z}$) if there is no tuple of integers $(c_i)_{i=1}^K \neq 0$ for which $\prod_{i=1}^K F_i^{c_i}$ is identically constant in $\mathbb{Q}(T)$.

Given nonconstant polynomials $\{F_i\}_{i=1}^K \subset \mathbb{Z}[T]$, we factor $F_i =: r_i \prod_{j=1}^M G_j^{\mu_{ij}}$ where $r_i \in \mathbb{Z}$, $\{G_j\}_{j=1}^M \subset \mathbb{Z}[T]$ are pairwise coprime primitive[3] irreducible polynomials and μ_{ij} are nonnegative integers, such that each G_j appears with a positive exponent μ_{ij} in some F_i. Letting $\omega(F_1 \cdots F_K) := M$, we define the exponent matrix of $(F_i)_{i=1}^K$ to be the $M \times K$ matrix

$$E_0 := E_0(F_1, \ldots, F_K) := \begin{pmatrix} \mu_{11} & \cdots & \mu_{K1} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ \mu_{1M} & \cdots & \mu_{KM} \end{pmatrix} \in \mathbb{M}_{M \times K}(\mathbb{Z}).$$

Now E_0 has a Smith Normal Form: An $M \times K$ diagonal matrix $\operatorname{diag}(\beta_1, \ldots, \beta_r, 0, \ldots, 0)$, where $r := \min\{M, K\}$ and $\beta_1, \ldots, \beta_r \in \mathbb{Z}$ are the "invariant factors" of E_0, so that $\beta_j \mid \beta_{j+1}$ for each j (for the moment, we allow the possibility that $\beta_j = 0$ for some j and accept the convention that $0 \mid 0$). Set $\beta(F_1, \ldots, F_K)$ to denote the "last" invariant factor β_r of E_0.

Invariant Factor Hypothesis: Given $B_0 > 0$, we shall say that a positive integer q satisfies $IFH(F_1, \ldots, F_K; B_0)$ if $\gcd(\ell - 1, \beta(F_1, \ldots, F_K)) = 1$ for any prime $\ell \mid q$ satisfying $\ell > B_0$.

In a wide variety of applications, $\prod_{i=1}^K F_i$ is separable over $\mathbb{Q}$, so that $\beta(F_1, \ldots, F_K) = 1$, making this hypothesis vacuous (i.e., any q satisfies $IFH(F_1, \ldots, F_K; B_0)$ for any $B_0 > 0$). In [48], we assumed throughout that the polynomials $\{W_{i,k}\}_{1 \le i \le K}$ are multiplicatively independent and

[1] Here χ_0 or $\chi_{0,q}$ denotes, as usual, the trivial or principal character mod q.

[2] i.e., $\prod_{i=1}^K \chi_i(W_{i,k}(u)) = 1$ for all $u \in R_k(q)$

[3] i.e., the greatest common divisor of their coefficients is 1

that q satisfies $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$; Theorems 2.4 and 2.5 below will demonstrate their necessity. Note that the multiplicative independence condition guarantees that $\omega(\prod_{i=1}^K W_{i,k}) \geq K$ and that $\beta(W_{1,k}, \dots, W_{K,k}) \neq 0$, as the computation of the Smith normal form is a base-change over $\mathbb{Z}$.

Our first main result in [48] shows that a given family $f_1, \dots, f_K$ is jointly WUD modulo any $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ satisfying $IFH(W_{1,k}, \dots, W_{K,k};\ B_0)$, that is allowed to vary up to small powers of $\log x$: These powers are different in different cases, but they are all essentially optimal, in the sense that weak equidistribution fails if the power is reduced slightly. A special case of our results is that the Euler totient $\varphi(n)$ and the sum of divisors $\sigma(n)$ are jointly WUD uniformly modulo $q \leq (\log x)^{(1-\epsilon)\alpha(q)}$ coprime to 6, where $\alpha(q) := \prod_{\ell | q}(\ell - 3)/(\ell - 1)$ and $\epsilon > 0$ is fixed but arbitrary; here the exponent is optimal and the arithmetic restriction is necessary (the latter by [28, Theorem 1]).

We also showed ([48, subsec 8.1]) that obstructions to uniformity came from those inputs n which have too few large prime factors. As such, complete uniformity in q up to a fixed but arbitrary power of $\log x$ can be restored by restricting the set of inputs n to those divisible by a sufficient number of primes exceeding q (see [48, Theorems 2.2, 2.3]); here and below, all prime factors are counted with multiplicity unless stated otherwise. This reason for this restriction is that it gives rise to multivariate polynomial congruences involving a large number of variables, thus ensuring that these congruences maximally "cut down" the ambient space of tuples (via power–saving amplification in certain character sums). As such, the values taken by these multivariate polynomials that are coprime to q become jointly equidistributed in the unit group mod q.

To state the precise result, we let $P_1(n) := P(n)$ denote the largest prime divisor of n (let $P(1) := 1$), and inductively define $P_k(n) := P_{k-1}(n/P(n))$. Thus, $P_k(n)$ is the k-th largest prime factor of n (counted with multiplicity), with $P_k(n) = 1$ if $\Omega(n) < k$.

Theorem 2.1. [48, Theorems 2.2, 2.3] *Uniformly in coprime residues $a_1, \dots, a_K$ modulo $q \leq (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfying $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$, we have*

$$\begin{aligned} (2.2)\quad & \#\{n \leq x : P_R(n) > q,\ (\forall i)\ f_i(n) \equiv a_i \pmod q\} \\ & \sim \frac{1}{\varphi(q)^K}\#\{n \leq x : \gcd(f(n), q) = 1\} \sim \frac{1}{\varphi(q)^K}\#\{n \leq x : P_R(n) > q, \gcd(f(n), q) = 1\} \end{aligned}$$

as $x \to \infty$, where

$$\begin{cases} R = k(KD+1), & \text{if } k < D \\ R \text{ is the least integer exceeding } k\left(1 + (k+1)\left(K - 1/D\right)\right), & \text{if } k \geq D. \end{cases}$$

If q is also squarefree, then in (2.2), the following (usually) smaller values of R suffice:

$$R := \begin{cases} 2, & \text{if } K = k = 1 \text{ and } W_{1,1} \text{ is not squarefull.} \\ k(Kk + K - k) + 1, & \text{if } k > 1 \text{ and at least one of } \{W_{i,k}\}_{1 \leq i \leq K} \text{ is not squarefull.} \\ k(Kk + K - k + 1) + 1, & \text{in general.} \end{cases}$$

Here we write a polynomial $F \in \mathbb{Z}[T]$ as $F = r \prod_{j=1}^{M} H_j^{\nu_j}$ for some $\nu_j \in \mathbb{N}$ and pairwise coprime primitive irreducibles $H_j \in \mathbb{Z}[T]$, and we say that F is "squarefull" (in $\mathbb{Z}[T]$) if $(\prod_{j=1}^{M} H_j)^2 \mid F$. This is equivalent to saying that every root of F in $\mathbb{C}$ has multiplicity at least 2. In [48], we also showed that most of the values of R above are either exactly or nearly optimal.

As a byproduct of our arguments in [48], we gave an explicit description of the anatomy of our relevant inputs n (see Lemma 3.2 below): We showed that all the relevant inputs n, namely those for which $f(n) = \prod_{i=1}^{K} f_i(n)$ is coprime to q, are "almost" k-full, in the sense that n is of the form Bm for some integer B having size bounded by a constant and some integer m which is divisible by the k-th powers of all its prime factors. Furthermore, the dominant contribution in all our asymptotics comes from those inputs n which are exactly divisible by the k-th powers of several large primes. These observations make the anatomy of the "k-th power part" of n a natural object to consider, where we define the k-th power part of n to be the largest positive integer n_k such that n_k^k is a unitary divisor of n; in other words, no prime divisor of the integer n/n_k^k appears to an exponent divisible by k. (If $k = 1$, then simply $n_1 := n$.) A natural question that arises is whether the restrictions in Theorem 2.1 can be weakened if some control is available on the n_k, for instance if some of the large primes dividing n appear in n_k (or equivalently, if they appear to a k-th power in n). It turns out that is indeed the case.

Theorem 2.2. *Assume $D > 1$. Uniformly in coprime residues $a_1, \ldots, a_K$ modulo $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfying $IFH(W_{1,k}, \ldots, W_{K,k}; B_0)$, we have*

$$(2.3) \quad \#\{n \le x : P_R(n_k) > q,\ (\forall i)\ f_i(n) \equiv a_i \pmod q\}$$
$$\sim \frac{1}{\varphi(q)^K} \#\{n \le x : \gcd(f(n), q) = 1\} \sim \frac{1}{\varphi(q)^K} \#\{n \le x : P_R(n_k) > q, \gcd(f(n), q) = 1\}$$

as $x \to \infty$, where

$$R = \begin{cases} KD + 1, & \text{in general,} \\ 2K + 1, & \text{if } q \text{ is squarefree,} \\ 2, & \text{if } q \text{ is squarefree, } K = 1 \text{ and } W_{1,k} \text{ is not squarefull.} \end{cases}$$

Here, we assume that $D > 1$ since in the case $D = 1$ (namely, when $K = 1$ and $W_{1,k}$ is linear), [48, Theorem 2.1(i)] already gives complete uniformity in all $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$, *without* any restrictions on the inputs n. The implied constants in the above theorem depend only on B_0 and on the polynomials $\{W_{i,v}\}_{\substack{1 \le i \le K \\ 1 \le v \le k}}$, and are in particular independent of V and of the polynomials $\{W_{i,v}\}_{\substack{1 \le i \le K \\ k < v \le V}}$. In the special case $k = 1$, the formulas above coincide with the relevant consequences of [48, Theorems 2.2, 2.3]. Even in the special case $k = K = 1$, this theorem improves over [38, Theorem 1.4(a)].

It is worthwhile to strive for the optimality of R since doing so ensures weak equidistribution among the largest possible set of inputs n. The value $R = KD + 1$ above is optimal for the sum of divisors function $\sigma(n)$ to even moduli q: Indeed the resulting restriction is "$P_3(n_2) > q$" and this cannot be replaced by the weaker restriction "$P_2(n_2) > q$" since by the discussion in [47, subsec 6.1], we can construct infinitely many even moduli q and residues $w \in U_q$ such that the total number of inputs n of the form $(P_1P_2)^2$ (for $P_1, P_2 > q$) that satisfy $\sigma(n) \equiv w \pmod q$ grows much faster than the expected proportion $\frac{1}{\varphi(q)}\#\{n \le x : \gcd(\sigma(n), q) = 1\}$. Likewise, by the discussion in [47, subsec 7.1], the restriction "$P_2(n_2) > q$" coming from the value $R = 2$ for $\sigma(n)$ to squarefree moduli, is also optimal. Moreover, in § 4.1, we will construct more general classes of examples showing that it not possible to reduce the "$2K + 1$" to "$2K - 1$" for *any* $K \ge 2$. In these examples, $\{W_{i,k}\}_{i=1}^K$ will be pairwise coprime irreducibles, making $\prod_{i=1}^K W_{i,k}$ separable over $\mathbb{Q}$.

Our constructions demonstrating the aforementioned optimality or near-optimality of the values of R will come from multiplicative functions f_i for which the polynomials $\{W_{i,k}\}_{1\le i\le K}$ are nonconstant (in fact multiplicatively independent), but for which the polynomials $\{W_{i,2k}\}_{1\le i\le K}$ are constant. In practice however, the $W_{i,v}$ are often nonconstant for many more values of v (beyond a fixed threshold k); in fact, for many well-known arithmetic functions f (such as the Euler totient and sums of divisor-powers $\sigma_r(n) := \sum_{d\mid n} d^r$), the values $f(p^v)$ are controlled by nonconstant polynomials $W_v \in \mathbb{Z}[T]$ for *all* $v \ge 1$. Hence, it is natural to ask whether the restriction on inputs n in Theorems 2.1 and 2.2 can be weakened when such additional control on the f_i is available, or in other words, if V (the number of powers of primes at which we are assuming the f_i to be controlled by nonconstant polynomials $W_{i,v}$) can be taken to be sufficiently large. It turns out that we can almost always do this for squarefree q and in several cases in general.

Theorem 2.3. *Assume that the polynomials $\{W_{i,v}\}_{1\le i\le K} \subset \mathbb{Z}[T]$ are multiplicatively independent for each v satisfying $k \le v \le V$. Let $D_0 := \max_{k\le v\le V} D_v = \max_{k\le v\le V} \sum_{i=1}^K \deg W_{i,v}$.*

(a) *If <u>either</u> $V > k(K + 1 - 1/D_{\min}) - 1$ and $R := \max\{k(KD + 1), (Kk - 1)D_0 + 2\}$, <u>or</u>*

(b) *If q is squarefree, $V \ge Kk$, and $R := k(2K + 1)$,*

then the relations (2.2) hold, uniformly in coprime residues $a_1, \dots, a_K$ modulo $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfying $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$.

The implied constants in this theorem could depend on the full set of polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le V}}$. Notice that for any $K > 2$, the result under (b) unconditionally improves over the assertions for squarefree q in Theorems 2.1 and 2.2 in terms of weakening the restriction on inputs n. On the other hand, the result under condition (a) improves over the corresponding assertions in Theorem 2.2 whenever k or D is large enough compared to D_0.

We now explain the necessity of the two key additional hypotheses that we have been assuming in our main results in [48] and so far, namely the multiplicative independence of $\{W_{i,k}\}_{1\le i\le K} \subset \mathbb{Z}[T]$ and the invariant factor hypothesis. It turns out that without the former condition, the K congruences $f_i(n) \equiv a_i \pmod q$ (for $1 \le i \le K$) may degenerate to fewer congruences for sufficiently many inputs n, making weak equidistribution fail uniformly to *all* sufficiently large $q \le (\log x)^{K_0}$. In this situation, weak equidistribution *cannot* be restored *no matter* how much we restrict the set of inputs n to those having sufficiently many large prime factors. We make this explicit in the next result.

Theorem 2.4. *Fix $R \geq 1$, $K > 1$ and assume that $\{W_{i,k}\}_{1 \leq i \leq K-1} \subset \mathbb{Z}[T]$ are multiplicatively independent, with $\sum_{i=1}^{K-1} \deg W_{i,k} > 1$. Suppose $W_{K,k} = \prod_{i=1}^{K-1} W_{i,k}^{\lambda_i}$ for some nonnegative integers $(\lambda_i)_{i=1}^{K-1} \neq (0, \dots, 0)$. There exists a constant $C \coloneqq C(W_{1,k}, \dots, W_{K-1,k}) > 0$ such that*

$$\#\{n \leq x : P_{Rk}(n) > q, \ (\forall i \in [K]) \ f_i(n) \equiv a_i \pmod q\} \geq$$
$$\#\{n \leq x : P_R(n_k) > q, \ (\forall i \in [K]) \ f_i(n) \equiv a_i \pmod q\} \gg \frac{1}{\varphi(q)^{K-1}} \cdot \frac{x^{1/k} (\log\log x)^{R-2}}{\log x}$$

as $x \to \infty$, uniformly in k-admissible $q \leq (\log x)^{K_0}$ supported on primes $\ell > C$ satisfying $\gcd(\ell - 1, \beta(W_{1,k}, \dots, W_{K-1,k})) = 1$, and in $a_i \in U_q$ with $a_K \equiv \prod_{i=1}^{K-1} a_i^{\lambda_i} \pmod q$.

The compatibility of the relations in $\{W_{i,k}\}_{1 \leq i \leq K}$ and $(a_i)_{i=1}^K$ suggests why the K congruences degenerate to $K-1$ congruences. Note that the above lower bound will in fact come from the n which are supported on primes much larger than q. A similar lower bound holds for $K = 1$ when $W_k = W_{1,k}$ is constant (see the remark preceding subsection § 7.1). Using the above theorem, we shall construct (in § 7.1) explicit examples of polynomials $\{W_{i,k}\}_{1 \leq i \leq K-1}$ and moduli $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ where the above lower bound grows strictly faster than the expected proportion of $n \leq x$ having $\gcd(f(n), q) = 1$. This would demonstrate an overrepresentation of the coprime residues $(a_i \bmod q)_{i=1}^K$ by the multiplicative functions $f_1, \dots, f_K$, coming from inputs n that have at least Rk many prime factors exceeding q, showing the necessity of our hypothesis on the multiplicative independence of $\{W_{i,k}\}_{1 \leq i \leq K}$.

Turning to the invariant factor hypothesis, we show that the failure of this condition incurs an additional factor over the expected proportion of $n \leq x$ satisfying $\gcd(f(n), q) = 1$. For certain choices of q and $\{W_{i,k}\}_{1 \leq i \leq K}$, this factor can be made too large, once again leading to an overrepresentation of the tuple $(a_i \bmod q)_{i=1}^K$ by the multiplicative functions $f_1, \dots, f_K$. In what follows, $P^-(q)$ denotes the smallest prime dividing q.

Theorem 2.5. *Fix $R \geq 1$ and assume that $\{W_{i,k}\}_{1 \leq i \leq K} \subset \mathbb{Z}[T]$ are nonconstant, monic and multiplicatively independent, so that $\beta = \beta(W_{1,k}, \dots, W_{K,k}) \in \mathbb{Z} \setminus \{0\}$. There exists a constant $C \coloneqq C(W_{1,k}, \dots, W_{K,k}) > 0$ such that*

$$\#\{n \leq x : P_{Rk}(n) > q, \ (\forall i \in [K]) \ f_i(n) \equiv a_i \pmod q\} \geq \tag{2.4}$$
$$\#\{n \leq x : P_R(n_k) > q, \ (\forall i \in [K]) \ f_i(n) \equiv a_i \pmod q\} \gg \frac{2^{\#\{\ell | q: \ \gcd(\ell-1, \beta) \neq 1\}}}{\varphi(q)^K} \cdot \frac{x^{1/k} (\log\log x)^{R-2}}{\log x}$$

as $x \to \infty$, uniformly in k-admissible $q \leq (\log x)^{K_0}$ having $P^-(q) > C$, and in coprime residues $(a_i)_{i=1}^K$ mod q which are all congruent to 1 modulo the largest squarefree divisor of q.

Here, the restriction on the residues a_i is imposed in order to have a positive contribution of certain character sums modulo the prime divisors of q. In subsection § 7.1, we shall construct explicit examples of $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ and $\{W_{i,k}\}_{1 \leq i \leq K}$ for which the expression in the above lower bound is much larger than the expected proportion of $n \leq x$ having $\gcd(f(n), q) = 1$.

We give some concrete applications of our main results to arithmetic functions of common interest. For instance, Śliwa [49] shows that $\sigma(n)$ is WUD modulo q precisely when q is either odd or is even but not divisible by 3. By [48, Theorem 2.1], $\sigma(n)$ is WUD modulo all odd $q \le (\log x)^{K_0}$ but among the latter q, it is only WUD among those that vary up to small powers of $\log x$ (without any restrictions on the inputs n). However by Theorem 2.2, uniformity is restored in the full "Siegel–Walfisz" range $q \le (\log x)^{K_0}$ provided we restrict to n with $P_3(n_2) > q$, or for squarefree $q \le (\log x)^{K_0}$, we restrict to n with $P_2(n_2) > q$. As discussed after the statement of Theorem 2.2, both these restrictions are optimal.

For another example, we mentioned before that $\varphi(n)$ and $\sigma(n)$ are jointly WUD modulo $q \le (\log x)^{(1-\epsilon)\alpha(q)}$ coprime to 6, and that these two restrictions on q are necessary and essentially optimal. By Theorem 2.2, complete uniformity is restored to all moduli $q \le (\log x)^{K_0}$ coprime to 6 by restricting to inputs n with $P_5(n) > q$.

We can give more applications of our main results to study the weak equidistribution of the Fourier coefficients of Eisenstein series. More generally, we can study the functions $\sigma_r(n) := \sum_{d|n} d^r$ (for $r > 1$). It is easy to see that the polynomial $\sum_{0\le j\le v} T^{rj} = \frac{T^{r(v+1)}-1}{T^r-1}$ is separable. For $r = 3$, Narkiewicz [30] shows that the only two possible k for which some q can be k-admissible are $k = 1, 2$, and moreover, $\mathcal{Q}(1; \sigma_3) = \{q : \gcd(q, 14) = 1\}$ while $\mathcal{Q}(2; \sigma_3) = \{q : \gcd(q, 6) = 2\}$. Combining this with Theorems 2.2 and 2.3, we see that σ_3 is WUD modulo all $q \le (\log x)^{K_0}$ in $\mathcal{Q}(1; \sigma_3)$, provided we either restrict to inputs n with $P_4(n) > q$ or (for squarefree q) to n's with $P_2(n) > q$. In addition, σ_3 is WUD modulo all $q \le (\log x)^{K_0}$ in $\mathcal{Q}(2; \sigma_3)$, provided we either restrict to inputs n with $P_{14}(n) > q$ or (for squarefree q) to n's with either $P_2(n_2) > q$ or $P_6(n) > q$.

For a general r, Theorems 2.2 and 2.3 show that σ_r is WUD modulo $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k, \sigma_r)$ if we restrict to inputs n with $P_{kr+1}(n_k) > q$ or (for squarefree q) to n's having either $P_2(n_k) > q$ or $P_{3k}(n) > q$. An explicit characterization of the moduli $q \le (\log x)^{K_0}$ to which a given σ_r is weakly equidistributed thus reduces to an understanding of the possible k and of the set $\mathcal{Q}(k; \sigma_r)$ for a given (fixed) r; both of these are problems of fixed moduli that (as mentioned in the introduction) have been studied in great depth in [49], [15], [32], [30], [31], [40] and [41]. In fact, Rayner [40, 41] has explicitly characterized the sets $\mathcal{Q}(k; \sigma_r)$ for all odd $r \le 200$ and all even $r \le 50$; partial results are also known for general $r \ge 4$.

We conclude this section with the remark that although for the sake of simplicity of statements, we have been assuming that our multiplicative functions $\{f_i\}_{i=1}^K$ and polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le V}}$ are both fixed, our proofs will reveal that these results are also uniform in the $\{f_i\}_{i=1}^K$ as long as they are defined by the fixed polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le V}}$.

Notation and conventions: We do not consider the zero function as multiplicative (thus, if f is multiplicative, then $f(1) = 1$). Given $z > 0$, we say that a positive integer n is z-smooth if $P(n) \le z$, and z-rough if $P^-(n) > z$; by the z-smooth part (resp. z-rough part) of n, we shall mean the largest z-smooth (resp. z-rough) positive integer dividing n. For a ring R, we shall use $R^\times$ to denote the multiplicative group of units of R. We denote the number of primes dividing q counted with and without multiplicity by $\Omega(q)$ and $\omega(q)$ respectively, and we write $U_q := (\mathbb{Z}/q\mathbb{Z})^\times$. For a Dirichlet character χ mod q, we use $\mathfrak{f}(\chi)$ to denote the conductor of χ. When there is no danger of confusion, we shall write $(a_1, \ldots, a_k)$ in place of $\gcd(a_1, \ldots, a_k)$. Throughout, the letters p and ℓ are reserved for primes. For nonzero $H \in \mathbb{Z}[T]$, we use $\operatorname{ord}_\ell(H)$ to denote the highest power of ℓ dividing all the coefficients of H; for an integer $m \ne 0$, we shall sometimes use $v_\ell(m)$ in place of $\operatorname{ord}_\ell(m)$. We use $\mathbb{M}_{A\times B}(\mathbb{Z})$ to refer to the ring of $A \times B$

matrices with integer entries, while $GL_{A\times B}(\mathbb{Z})$ refers to the group of units of $\mathbb{M}_{A\times B}(\mathbb{Z})$, i.e. the matrices with determinant ±1. Implied constants in $\ll$ and O-notation, as well as implicit constants in qualifiers like "sufficiently large", may always depend on any parameters declared as "fixed"; in particular, they will always depend on the polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le k}}$. Other dependence will be noted explicitly (for example, with parentheses or subscripts); notably, we shall use $C(F_1,\dots,F_K)$, $C'(F_1,\dots,F_K)$ and so on, to denote constants depending on the fixed polynomials $F_1,\dots,F_K$. We write $\log_k$ for the k-th iterate of the natural logarithm.

3. Preparatory Results

In this section, we collect some of the results established in [48] that will also be useful to prove the main results in this manuscript. Continuing with the set-up listed in the beginning of the previous section, we start by giving a general estimate for the count of how often the function $f(n)=\prod_{i=1}^K f_i(n)$ is coprime to q.

Proposition 3.1. [48, Proposition 3.1] *For all sufficiently large x, we have*

$$\sum_{\substack{n\le x\\ (f(n),q)=1}} 1 \;=\; \sum_{\substack{n\le x\\ \text{each } (f_i(n),q)=1}} 1 = \frac{x^{1/k}}{(\log x)^{1-\alpha_k}}\exp(O((\log_2(3q))^{O(1)})), \tag{3.1}$$

uniformly in k-admissible $q\le(\log x)^{K_0}$.

The following lemma describes the anatomy of all our relevant inputs n, namely those for which $\gcd(f(n),q)=1$.

Lemma 3.2. [48, Lemma 3.3] *If q is k-admissible, then the k-free part of any positive integer n satisfying $\gcd(f(n),q)=1$ is bounded. More precisely, it is of size $O(1)$, where the implied constant depends only on the polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le k}}$.*

As part of the argument for Proposition 3.1, we needed the following technical estimates. These were useful everywhere in [48] and will continue to be useful to us throughout in this manuscript. In the rest of the paper, we let $z=x^{1/\log_2 x}$ and $y=\exp(\sqrt{\log x})$.

Lemma 3.3. [48, eqns (3.3), (4.3), (4.5)] *In the above setting, we have the following bounds:*

$$\sum_{\substack{n\le x:\ P(n)\le z\\ (f(n),q)=1}} 1 \ll \frac{x^{1/k}}{(\log x)^{(1/k+o(1))\log_3 x}}, \qquad \sum_{\substack{n\le x:\ (f(n),q)=1\\ \exists\ p>y:\ p^{k+1}\mid n}} 1 \ll \left(\frac{x}{y}\right)^{1/k}, \tag{3.2}$$

$$\sum_{\substack{m\le x\\ P_{Jk}(m)\le y,\ (f(m),q)=1\\ p>y \implies p^{k+1}\nmid m}} \frac{1}{m^{1/k}} \ll (\log x)^{\alpha_k/2}\exp\left(O((\log_3 x)^2+(\log_2(3q))^{O(1)})\right), \tag{3.3}$$

The following proposition estimates the number of solution tuples to certain polynomial congruences involving the $\{W_{i,k}\}_{1\le i\le K}$, and was crucially required in [48].

Proposition 3.4. [48, Proposition 4.4] *Assume that $\{W_{i,k}\}_{1\le i\le K}$ are multiplicatively independent. There exists a constant $C_0 := C_0(W_{1,k}, \ldots, W_{K,k}; B_0) > (8D)^{2D+2}$ depending only on $\{W_{i,k}\}_{1\le i\le K}$ and B_0, such that for $\underline{\text{any}}$ constant $C > C_0$, the following estimates hold uniformly in coprime residues $(w_i)_{i=1}^K$ to moduli q satisfying $\alpha_k(q) \ne 0$ and $IFH(W_{1,k}, \ldots, W_{K,k}; B_0)$: We have*

$$\begin{aligned}(3.4)\quad &\frac{\#\mathcal{V}_{N,K}^{(k)}\left(q; (w_i)_{i=1}^K\right)}{\varphi(q)^N} \\ &= \frac{\alpha_k(q)^N}{\alpha_k(Q_0)^N}\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K \left\{\frac{\#\mathcal{V}_{N,K}^{(k)}\left(Q_0; (w_i)_{i=1}^K\right)}{\varphi(Q_0)^N} + O\left(\frac{1}{C^N}\right)\right\} \prod_{\substack{\ell\mid q\\ \ell>C_0}}\left(1 + O\left(\frac{(4D)^N}{\ell^{N/D-K}}\right)\right),\end{aligned}$$

uniformly for $N \ge KD + 1$, where Q_0 is a C_0-smooth divisor of q of size $O_C(1)$. Moreover

$$(3.5)\qquad \frac{\#\mathcal{V}_{N,K}^{(k)}\left(q; (w_i)_{i=1}^K\right)}{\varphi(q)^N} \le \frac{\left(\prod_{\ell^e\| q} e\right)^{\mathbb{1}_{N=KD}}}{q^{N/D}}\ \exp\left(O(\omega(q))\right), \quad \textit{for each } 1 \le N \le KD.$$

We will also require the following variants of the above proposition for squarefree and prime moduli, which are Corollary 5.4 and Proposition 10.1 in [48], respectively.

Lemma 3.5. *Assume that $\{W_{i,k}\}_{1\le i\le K}$ are multiplicatively independent. Then*

$$(3.6)\qquad \frac{\#\mathcal{V}_{N,K}^{(k)}\left(q; (w_i)_{i=1}^K\right)}{\varphi(q)^N} \ll \begin{cases}\varphi(q)^{-K}\exp\left(O(\sqrt{\log q})\right), & \textit{for each fixed } N \ge 2K+1\\ q^{-N/2}\exp\left(O(\omega(q))\right), & \textit{for each fixed } N \le 2K,\end{cases}$$

uniformly in $w_i \in U_q$ modulo squarefree q satisfying $\alpha_k(q) \ne 0$ and $IFH(W_{1,k}, \ldots, W_{K,k}; B_0)$.

Lemma 3.6. *Let $F \in \mathbb{Z}[T]$ be a fixed nonconstant polynomial which is not squarefull. Define $\mathcal{V}_{2,1}(\ell; w) := \{(v_1, v_2) \in U_\ell^2 : F(v_1)F(v_2) \equiv w \pmod{\ell}\}$. Then $\#\mathcal{V}_{2,1}(\ell; w) \le \varphi(\ell)\left(1 + O\left(\ell^{-1/2}\right)\right)$, uniformly for primes ℓ and coprime residues w mod ℓ.*

Some of the most crucial ingredients for Proposition 3.4 and Lemma 3.5 are certain bounds on sums of Dirichlet characters to prime power moduli. The first of these is a version of the Weil bounds [51, Corollary 2.3] (see also [9], [52] and [42]) and deals with the case of prime moduli.

Proposition 3.7. *Let ℓ be a prime, χ a Dirichlet character mod ℓ, and $F \in \mathbb{Z}[T]$ a nonconstant polynomial which is not congruent mod ℓ to a polynomial of the form $c \cdot G(T)^{\mathrm{ord}(\chi)}$ for some $c \in \mathbb{F}_\ell$ and $G \in \mathbb{F}_\ell[T]$, where $\mathrm{ord}(\chi)$ denotes the order of the character χ. Then*

$$\left|\sum_{u \bmod \ell} \chi(F(u))\right| \le (d-1)\sqrt{\ell},$$

where d is the degree of the largest squarefree divisor of F.

The second bound is due to Cochrane [6, Theorems 1.2 and 7.1, eqn. (1.15)] and deals with moduli that are higher powers of primes. To state this, we need the following set-up: For a polynomial $H \in \mathbb{Z}[T]$, we denote by H' or $H'(T)$ the formal derivative of H. Given a prime ℓ, the ℓ-critical polynomial associated to H is the polynomial $\mathcal{C}_H := \ell^{-\mathrm{ord}_\ell(H')} H' \in \mathbb{Z}[T]$; this can be considered as a nonzero element of the ring $\mathbb{F}_\ell[T]$. If H does not vanish identically in $\mathbb{F}_\ell[T]$ (i.e., if $\mathrm{ord}_\ell(H) = 0$), then by the ℓ-critical points of H, we shall mean the set $\mathcal{A}(H;\ell) \subset \mathbb{F}_\ell$ of zeros of the polynomial $\mathcal{C}_H$ which are not zeros of H (both polynomials considered mod ℓ). For any $\theta \in \mathbb{F}_\ell$, we use $\mu_\theta(H)$ to denote the multiplicity of θ as a zero of H.

Proposition 3.8. *Let ℓ be a prime, $g \in \mathbb{Z}[T]$ a nonconstant polynomial, and $t := \mathrm{ord}_\ell(g')$. Consider an integer $e \geq t+2$ and a primitive character χ mod ℓ^e. Let $M := \max_{\theta \in \mathcal{A}(g;\ell)} \mu_\theta(\mathcal{C}_g)$ be the maximum multiplicity of an ℓ-critical point.*

(i) *For odd ℓ, we have $|\sum_{u \bmod \ell^e} \chi(g(u))| \leq \left(\sum_{\theta \in \mathcal{A}(g;\ell)} \mu_\theta(\mathcal{C}_g)\right) \ell^{t/(M+1)}\ \ell^{e(1-1/(M+1))}$.*

(ii) *For $\ell = 2$ and $e \geq t+3$, we have $|\sum_{u \bmod 2^e} \chi(g(u))| \leq (12.5) 2^{t/(M+1)}\ 2^{e(1-1/(M+1))}$. In fact, the sum is zero if g has no 2-critical points.*

We will require both these bounds in our arguments for Theorems 2.2 and 2.3. However, to make use of them, we need to better understand the main condition in Proposition 3.7 as well as the quantities "t" and "M" that arise in Proposition 3.8.

Proposition 3.9. [48, Proposition 5.3] *Let $\{F_i\}_{i=1}^K \subset \mathbb{Z}[T]$ be nonconstant and multiplicatively independent. There exists a constant $C_1 := C_1(F_1, \dots, F_K) \in \mathbb{N}$ such that all of the following hold:*

(a) *For any prime ℓ, there are $O(1)$ many tuples $(A_1, \dots, A_K) \in [\ell-1]^K$ for which $F_1^{A_1} \cdots F_K^{A_K}$ is of the form $c \cdot G^{\ell-1}$ in $\mathbb{F}_\ell[T]$ for some $c \in \mathbb{F}_\ell$ and $G \in \mathbb{F}_\ell[T]$; here, the implied constant depends at most on $\{F_i\}_{i=1}^K$. In fact, if $\ell > C_1$ and $\gcd(\ell - 1, \beta(F_1, \dots, F_K)) = 1$, then the only such tuple is $(A_1, \dots, A_K) = (\ell-1, \dots, \ell-1)$.*

(b) *For any prime ℓ and any $(A_1, \dots, A_K) \in \mathbb{N}^K$ satisfying $\ell \nmid \gcd(A_1, \dots, A_K)$, we have in the two cases below,*

$$\tau(\ell) := \mathrm{ord}_\ell\left((T^{\varphi(\ell^r)} F_1(T)^{A_1} \cdots F_K(T)^{A_K})'\right) = \mathrm{ord}_\ell(\widetilde{F}(T)) \begin{cases} = 0, & \text{if } \ell > C_1, r \geq 2 \\ \leq C_1, & \text{if } \ell \leq C_1, \mathrm{ord}_\ell\left(\prod_{i=1}^K F_i\right) = 0, r \geq C_1 + 2, \end{cases} \tag{3.7}$$

where $\widetilde{F}(T) := \sum_{i=1}^K A_i F_i'(T) \prod_{\substack{1 \leq j \leq K \\ j \neq i}} F_j(T)$. In either of the two cases above, any root $\theta \in \mathbb{F}_\ell$ of the polynomial $\mathcal{C}_\ell(T) := \ell^{-\tau(\ell)} (T^{\varphi(\ell^r)} F_1(T)^{A_1} \cdots F_K(T)^{A_K})'$ which is not a root of $T \prod_{i=1}^K F_i(T)$, must be a root of the polynomial $\ell^{-\tau(\ell)} \widetilde{F}(T)$ of the same multiplicity.[4]

Finally, we have the following asymptotic which plays an integral part in the proofs of Theorems 2.2 and 2.3. It states that the dominant contribution in all our asymptotics comes from those inputs n which are exactly divisible by the k-th powers of *several very large* primes. To state this result explicitly, we start by setting $J := \lfloor \log_3 x \rfloor$ and recalling that $y := \exp(\sqrt{\log x})$. We

[4] Once again, the last three polynomials are being considered as nonzero elements of $\mathbb{F}_\ell[T]$.

define $n \le x$ to be convenient if it can be uniquely written in the form $n = m(P_J \cdots P_1)^k$ for $m \le x$ and primes $P_1, \dots, P_J$ satisfying

$$L_m := \max\{y, P(m)\} < P_J < \cdots < P_1. \tag{3.8}$$

In other words, n is convenient iff the largest J *distinct* prime divisors of n exceed y and each appear to exactly the k-th power in n. Note that any n having $P_{Jk}(n) \le y$ must be inconvenient; on the other hand, if n is inconvenient and satisfies $\gcd(f(n), q) = 1$ then either $P_{Jk}(n) \le y$ or n is divisible by the $(k+1)$-th power of a prime exceeding y.

Theorem 3.10. *Fix $K_0, B_0 > 0$ and assume that $\{W_{i,k}\}_{1 \le i \le K} \subset \mathbb{Z}[T]$ are nonconstant and multiplicatively independent. As $x \to \infty$, we have*

$$\sum_{\substack{n \le x \text{ convenient} \\ (\forall i)\ f_i(n) \equiv a_i \pmod q}} 1 \sim \frac{1}{\varphi(q)^K} \sum_{\substack{n \le x \\ (f(n), q) = 1}} 1,$$

uniformly in coprime residues $a_1, \dots, a_K$ to moduli $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfying $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$.

4. Restricted inputs to general moduli: Proof of Theorem 2.2

We first show the equality of the second and third quantities in (2.3). This follows from the estimate below: Fix $T \in \mathbb{N}_{>1}$. Then as $x \to \infty$ and uniformly in k-admissible $q \le (\log x)^{K_0}$,

$$\sum_{\substack{n \le x:\ P_T(n_k) \le q \\ \gcd(f(n), q) = 1}} 1 = o\Bigg(\sum_{\substack{n \le x \\ \gcd(f(n), q) = 1}} 1 \Bigg). \tag{4.1}$$

To show this, we write any n counted in the left side uniquely in the form $n = BN^kA$, where B is k-free, A is $(k+1)$-full and the exponent of any prime in A is not a multiple of k. Then $n_k = N$, and B, N, A are pairwise coprime, so that $f(n) = f(B)f(N^k)f(A)$, and

$$\sum_{\substack{n \le x:\ P_T(n_k) \le q \\ \gcd(f(n), q) = 1}} 1 \le \sum_{\substack{B \le x \\ B \text{ is } k\text{-free} \\ (f(B), q) = 1}} \sum_{\substack{N, A:\ N^k A \le x/B \\ P_T(N) \le q;\ A \text{ is } (k+1)\text{-full} \\ \gcd(f(N^k)f(A), q) = 1}} 1. \tag{4.2}$$

If $A > x^{1/2}$, then $N \le (x/AB)^{1/k} \le x^{1/2k}$. Since A is $(k+1)$-full, the contribution of the tuples (B, N, A) with $A > x^{1/2}$ is $\ll \sum_{B \ll 1} \sum_{N \le x^{1/2k}} (x/BN^k)^{1/(k+1)} \ll x^{1/k - 1/2k(k+1)}$, which by Proposition 3.1, is negligible compared to the right hand expression in (4.1). On the other hand, if $A \le x^{1/2}$, then given B and A, [36, Lemma 2.3] shows there are $\ll x^{1/k}(\log_2 x)^T / B^{1/k} A^{1/k} \log x$ many $N \le (x/AB)^{1/k}$ having $P_T(N) \le q$. The sum over A is $\le \prod_p (1 + \sum_{v \ge k+1} p^{-v/k}) \ll 1$ and by Lemma 3.2, we have $B = O(1)$. As such, the total contribution of all tuples (B, N, A) with $A \le x^{1/2}$ is $O(x^{1/k}(\log_2 x)^T / \log x)$. By (3.1), this is also negligible compared to the right hand side of (4.1). This proves (4.1), establishing the asymptotic equality of the second and third expressions in (2.3). It thus remains to show the first equality in (2.3) to complete the proof of Theorem 2.2.

We may assume q to be sufficiently large, otherwise the theorem follows directly from Theorem N and (4.1). Parts of the arguments below are modified from [48], but we give the complete argument for the sake of completeness. Any convenient n is automatically counted in the left hand side of (2.3) since it has $P_J(n_k) > y$. By Theorem 3.10, it suffices to show that the contributions of the inconvenient n to the left hand side of (2.3) is negligible compared to $\varphi(q)^{-K}\#\{n \le x : (f(n), q) = 1\}$. In fact, by the two bounds in (3.2), it remains to show that

$$\sum\nolimits^*_{n:\ P_R(n_k)>q} 1 \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}, \tag{4.3}$$

with the respective values of R. Here and in the rest of the manuscript, any sum of the form $\sum_n^*$ denotes a sum over positive integers $n \le x$ that are not z-smooth, not divisible by the $(k+1)$-th power of a prime exceeding y, have $P_{Jk}(n) \le y$ and satisfy $f_i(n) \equiv a_i \pmod q$ for all $i \in [K]$. Other conditions imposed on this sum are additional to these.

Define $\omega_\|(n) := \#\{p > q : p^k \parallel n\} = \#\{n \le x : p \parallel n_k\}$ and $\omega_k(n) := \#\{p > q : p^2 \mid n_k\}$. We first show that the contribution of all n with $\omega_k(n) \ge K$ to the sum in (4.3) is absorbed in the right hand side, irrespective of the value of R. This would follow once we show that

$$\sum_{\substack{n\le x:\, (f(n),q)=1\\ \omega_k(n)\ge K,\, P_{Jk}(n)\le y,\, P(n)>z\\ p>y \implies p^{k+1}\nmid n}} 1 \ll \frac{x^{1/k}}{q^K(\log x)^{1-2\alpha_k/3}}. \tag{4.4}$$

Indeed, any n counted above has $P(n) > z > y$ and is also not divisible by the $(k+1)$-th power of any prime exceeding y. Thus n is of the form $m(p_K \dots p_1)^{2k}P^k$ where $P = P(n) > z$, $p_1, \dots, p_K > y$, and where the integer m satisfies $P_{Jk}(m) \le y$ and $(f(m), q) = 1$ and is not divisible by the $(k+1)$-th power of any prime exceeding y. Given m and $p_1, \dots, p_K$, the number of possible P satisfying $z < P \le x^{1/k}/m^{1/k}(p_1 \dots p_K)^2$ is $\ll x^{1/k}/m^{1/k}(p_1 \dots p_K)^2 \log z$ by Chebyshev's estimates. Since $\sum_{p>q} 1/p^2 \ll 1/q$, it follows by (3.3) that the left hand side of (4.4) is $\ll x^{1/k}/q^K(\log x)^{1-2\alpha_k/3}$, where we have recalled that $\alpha_k \gg 1/\log_2(3q) \gg 1/\log_3 x$. As such, to complete the proof of Theorem 2.2, it remains to show that the contribution of all n with $\omega_k(n) \le K-1$ to the sum in (4.3) is absorbed in the right hand side of (4.3).

The case $R = KD+1$: We start by showing that

$$\sum\nolimits^*_{n:\ \omega_\|(n)\ge KD+1} 1, \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}. \tag{4.5}$$

Indeed, any n counted in the above sum can be written as $m(P_{KD+1}\cdots P_1)^k$, where $P_{Jk}(m) \le y$, $(f(m), q) = 1$, where m is not divisible by the $(k+1)$-th power of any prime exceeding y, where $P_1, \dots, P_{KD+1} > q$ are primes satisfying $P_1 := P(n) > z$ and $q < P_{KD+1} < \cdots < P_1$, and where $m, P_1, \dots, P_{KD+1}$ are all pairwise coprime. Thus $f_i(n) = f_i(m)\prod_{j=1}^{KD+1} f_i(P_j^k) = f_i(m)\prod_{j=1}^{KD+1} W_{i,k}(P_j)$, whereupon the conditions $f_i(n) \equiv a_i \pmod q$ translate to $(P_1, \dots, P_{KD+1}) \bmod q \in \mathcal{V}^{(k)}_{KD+1,K}\big(q; (a_i f_i(m)^{-1})_{i=1}^K\big)$. Now, given m, a tuple $(v_1, \dots, v_{KD+1}) \in \mathcal{V}^{(k)}_{KD+1,K}\big(q; (a_i f_i(m)^{-1})_{i=1}^K\big)$, and primes $P_2, \dots, P_{KD+1}$ satisfying $P_j \equiv v_j \pmod q$ for all $j \ge 2$, the number of primes P_1 in $(q,\ x^{1/k}/m^{1/k}P_2\cdots P_{KD+1}]$ satisfying $P_1 \equiv v_1 \pmod q$ is $\ll x^{1/k}\log_2 x/m^{1/k}P_2\cdots P_{KD+1}\varphi(q)\log x$, by the Brun-Titchmarsh theorem. Summing this over all possible $P_2, \dots, P_{KD+1}$ and noting that $\sum_{\substack{q<p\le x\\ p\equiv v \pmod q}} 1/p \ll \log_2 x/\varphi(q)$ uniformly in

$v \in U_q$ (by Brun–Titchmarsh and partial summation), we find that the number of possible $(P_1, \dots, P_{KD+1})$ satisfying $P_j \equiv v_j \pmod q$ for each $j \in [KD+1]$ is no more than

$$\sum_{\substack{q<P_{KD+1}<\cdots<P_2\le x\\ (\forall j)\ P_j\equiv v_j \pmod q}} \ \sum_{\substack{z<P_1\le x^{1/k}\big/ m^{1/k}P_2\cdots P_{KD+1}\\ P_1\equiv v_1 \pmod q}} 1 \ll \frac{1}{\varphi(q)^{KD+1}}\cdot\frac{x^{1/k}(\log_2 x)^{O(1)}}{m^{1/k}\log x}. \tag{4.6}$$

uniformly in $v_j \in U_q$. Define $V'_{r,K} := \max\left\{\#\mathcal{V}_{r,K}^{(k)}\big(q;(w_i)_{i=1}^K\big) : w_1,\dots,w_K \in U_q\right\}$. Summing (4.6) over all $(v_1,\dots,v_{KD+1}) \in \mathcal{V}_{KD+1,K}^{(k)}\big(q;(a_if_i(m)^{-1})_{i=1}^K\big)$ and then over all m via (3.3), we obtain

$$\sideset{}{^*}\sum_{n:\ \omega_\parallel(n)\ge KD+1} 1 \ll \frac{V'_{KD+1,K}}{\varphi(q)^{KD+1}}\cdot\frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}}\cdot\exp\left(O\big((\log_3 x)^2+(\log_2(3q))^{O(1)}\big)\right). \tag{4.7}$$

Now applying (3.4) with $N := KD+1$, we see that $V'_{KD+1,K}/\varphi(q)^{KD+1} \ll \varphi(q)^{-K}\prod_{\ell\mid q}(1+O(\ell^{-1/D})) \ll \varphi(q)^{-K}\exp\big(O((\log q)^{1-1/D})\big)$. This proves (4.5).

Next, we show that

$$\sideset{}{^*}\sum_{\substack{n:\ \omega_\parallel(n)=KD\\ \omega_k(n)\ge 1}} 1 \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}. \tag{4.8}$$

Indeed any n counted in this sum is of the form $mp^{ck}(P_{KD}\cdots P_1)^k$ for some $m, c \ge 2$ and distinct primes $p, P_1, \dots, P_{KD}$ exceeding q, which satisfy the conditions $P_1 = P(n) > z$, $P_{KD} < \cdots < P_1$, $P_{Jk}(m) \le y$ and $f_i(n) = f_i(mp^{ck})\prod_{j=1}^{KD} W_{i,k}(P_j)$. As such, $(P_1,\dots,P_{KD}) \bmod q \in \mathcal{V}_{KD,K}^{(k)}\big(q;(a_if_i(mp^{ck})^{-1})_{i=1}^K\big)$. Given m, p, c and $(v_1,\dots,v_{KD}) \in \mathcal{V}_{KD,K}^{(k)}\big(q;(a_if_i(mp^{ck})^{-1})_{i=1}^K\big)$, the arguments leading to (4.6) show that the number of possible $(P_1,\dots,P_{KD})$ satisfying $(P_j)_{i=1}^{KD} \equiv (v_j)_{i=1}^{KD} \pmod q$ is $\ll x^{1/k}(\log_2 x)^{O(1)}\big/\varphi(q)^{KD}m^{1/k}p^c\log x$. Summing this successively over all $(v_1,\dots,v_{KD})$, $c \ge 2$, $p > q$ and all possible m using (3.3) and the fact that $\sum_{p>q} 1/p^2 \ll 1/q$, we deduce that the left hand side of (4.8) is $\ll \frac{V'_{KD,K}}{\varphi(q)^{KD}}\cdot\frac{x^{1/k}}{q(\log x)^{1-2\alpha_k/3}}$. Since by (3.5), we have $V'_{KD,K}\big/\varphi(q)^{KD} \ll q^{-K}(\prod_{\ell^e\parallel q} e)\exp(O(\omega(q))) \ll q^{-K+1}$, we obtain (4.8).

Any n with $P_{KD+1}(n_k) > q$ and $\omega_k(n) = 0$ contributing to (4.3) must have $\omega_\parallel(n) \ge KD+1$, and hence is counted in (4.5). Moreover, any n contributing to (4.3) having $P_{KD+1}(n_k) > q$ and $\omega_\parallel(n) = KD$ must also have $\omega_k(n) \ge 1$ and is thus counted in (4.8). Thus by (4.4), (4.5) and (4.8), it remains to show that for each $r \in [KD-1]$ and $s \in [K-1]$, the contribution $\widetilde{\Sigma}_{r,s}$ of all n with $\omega_\parallel(n) = r$ and $\omega_k(n) = s$ to the left hand side of (4.3) is absorbed in the right.

Any n counted in $\widetilde{\Sigma}_{r,s}$ has n_k of the form $m'p_1^{c_1}\cdots p_s^{c_s}P_1\cdots P_r$ for some distinct primes $p_1,\dots,p_s$, $P_1,\dots,P_r$ and integers $m', c_1,\dots,c_s$, which satisfy conditions (i)–(v): **(i)** $P(m') \le q$; **(ii)** $P_1 := P(n_k) = P(n) > z$, $q < P_r < \cdots < P_1$; **(iii)** $p_1,\dots,p_s > q$; **(iv)** $c_1,\dots,c_s \ge 2$ and $c_1+\cdots+c_s \ge KD+1-r$; **(v)** m', $p_1,\dots,p_s,P_1,\dots,P_r$ are all pairwise coprime. Hence, n is of the form $mp_1^{c_1k}\cdots p_s^{c_sk}P_1^k\cdots P_r^k$, where $p_1,\dots,p_s,P_1,\dots,P_r$ are as above, and: **(vi)** $P_{Jk}(m) \le y$; **(vii)** $f_i(n) = f_i(mp_1^{c_1k}\cdots p_s^{c_sk})\prod_{j=1}^r W_{i,k}(P_j)$ for each $i \in [K]$.

Now since $r \le KD-1$ and $c_1 + \cdots + c_s \ge KD+1-r$, the integers $\tau_j := \min\{c_j, KD+1-r\}$ ($j \in [s]$) satisfy $\tau_1, \ldots, \tau_s \in [2, KD+1-r]$ and $\tau_1 + \cdots + \tau_s \ge KD+1-r$. Consequently

$$\widetilde{\Sigma}_{r,s} \le \sum_{\substack{\tau_1,\ldots,\tau_s \in [2,KD+1-r] \\ \tau_1+\cdots+\tau_s \ge KD+1-r}} \widetilde{\mathcal{N}}_{r,s}(\tau_1, \ldots, \tau_s), \tag{4.9}$$

where $\widetilde{\mathcal{N}}_{r,s}(\tau_1, \ldots, \tau_s)$ denotes the number of n which can be written in the form $mp_1^{c_1k} \cdots p_s^{c_sk} P_1^k \cdots P_r^k$ with $m, p_1, \ldots, p_s, c_1, \ldots, c_s, P_1, \ldots, P_r$ satisfying the conditions (ii), (iii), (vi), (vii) above, and with $c_1 \ge \tau_1, \ldots, c_s \ge \tau_s$. We show that for each $\tau_1, \ldots, \tau_s$ counted above,

$$\widetilde{\mathcal{N}}_{r,s}(\tau_1, \ldots, \tau_s) \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}. \tag{4.10}$$

The argument is analogous to that given for (4.8), so we only sketch it. We write any n counted in $\widetilde{\Sigma}_{r,s}$ in the form $mp_1^{c_1k} \cdots p_s^{c_sk} P_1^k \cdots P_r^k$, with $m, p_1, \ldots, p_s, c_1, \ldots, c_s, P_1, \ldots, P_r$ satisfying the conditions (ii), (iii), (vi), (vii) above, and with $c_1 \ge \tau_1, \ldots, c_s \ge \tau_s$, so that $(P_1, \ldots, P_r)$ mod $q \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1k} \cdots p_s^{c_sk})^{-1})_{i=1}^K\big)$. Replicating the arguments leading to the bound (4.6), we find that, given $m, p_1, \ldots, p_s, c_1, \ldots, c_s$ and $(v_1, \ldots, v_r) \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1k} \cdots p_s^{c_sk})^{-1})_{i=1}^K\big)$, the number of possible $P_1, \ldots, P_r$ satisfying the congruences $P_j \equiv v_j \pmod q$ for each $j \in [r]$, is $\ll x^{1/k}(\log_2 x)^{O(1)} / \varphi(q)^r m^{1/k} p_1^{c_1} \cdots p_s^{c_s} \log x$. Summing this over all v_j, m, p_j and c_j via the bounds (3.3) and $\sum_{p_j > q:\, c_j \ge \tau_j} p_j^{-c_j} \ll q^{-\tau_j+1}$, we obtain

$$\widetilde{\mathcal{N}}_{r,s}(\tau_1, \ldots, \tau_s) \ll \frac{1}{q^{\tau_1+\cdots+\tau_s-s}} \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}} \exp\left(O\big((\log_3 x)^2 + (\log_2(3q))^{O(1)}\big)\right). \tag{4.11}$$

Now applying (3.5) and using the fact that $\tau_1 + \cdots + \tau_s \ge \max\{2s, KD+1-r\}$, we find that $V'_{r,K}/\varphi(q)^r q^{\tau_1+\cdots+\tau_s-s} \ll \exp\big(O(\omega(q))\big)/q^{\max\{s, KD+1-r-s\}+r/D} \ll \varphi(q)^{-K}$, since from $D \ge 2$, it is easily seen that $\max\{s, KD+1-r-s\} + r/D > K$. This proves (4.10), so that (4.9) yields $\widetilde{\Sigma}_{r,s} \ll x^{1/k}/\varphi(q)^K (\log x)^{1-2\alpha_k/3}$ for all $r \in [KD-1]$ and $s \in [K-1]$. This establishes Theorem 2.2 in the case $R = KD+1$.

The case $R = 2$: In the rest of the argument, we may assume that q is sufficiently large and squarefree. We first show the bound (4.3) for $R = 2$, which is the case when $K = 1$ and $W_{1.k}$ is not squarefull. First consider the contribution of all n with $\omega_k(n) \ge 1$: Any such n is of the form $mp^{ck}P^k$ where $P > z$, $p > q$, $c \ge 2$, $P_{Jk}(m) \le y$, $(f(m), q) = 1$ and m is not divisible by the $(k+1)$-th power of a prime exceeding y. Given m, p, c, the number of $P \in (z, x^{1/k}/m^{1/k}p^c)$ is $\ll x^{1/k} \log_2 x / m^{1/k} p^c \log x$. Summing this over all $p > q$, $c \ge 2$ and all possible m via (3.3), we find that the contribution of all n with $\omega_k(n) \ge 1$ to (4.3) is $\ll x^{1/k}/q(\log x)^{1-2\alpha_k/3}$, as desired.

On the other hand, any n with $P_2(n_k) > q$ and $\omega_k(n) = 0$ must have $\omega_{\|}(n) \ge 2$, and can thus be written in the form $m(P_2P_1)^k$, where $P_1 > z$, $q < P_2 < P_1$, $P_{Jk}(m) \le y$, $(f(m), q) = 1$ and m is not divisible by the $(k+1)$-th power of a prime exceeding y. Combining the arguments leading to (4.7) along with Lemma 3.6, we see that the contribution of such n is

$$\ll \frac{V'_{2,1}}{\varphi(q)^2} \cdot \frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}} \exp\left(O\big((\log_3 x)^2 + (\log_2(3q))^{O(1)}\big)\right) \ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}. \tag{4.12}$$

The conclusions in the last two paragraphs establish Theorem 2.2 in the third case $R = 2$.

The case $R = 2K+1$: We start by observing the following two bounds, which can be shown by replicating the arguments given for (4.5) and (4.8), and replacing the use of Proposition 3.4 by Lemma 3.5:

$$\sideset{}{^*}\sum_{n:\ \omega_{\parallel}(n) \ge 2K+1} 1,\ \sideset{}{^*}\sum_{\substack{n:\ \omega_{\parallel}(n)=2K \\ \omega_k(n)\ge 1}} 1 \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}. \tag{4.13}$$

Any n with $P_{2K+1}(n_k) > q$ and $\omega_k(n) = 0$ (resp. $\omega_{\parallel}(n) = 2K$) must also have $\omega_{\parallel}(n) \ge 2K+1$ (resp. $\omega_k(n) \ge 1$). As such, by (4.4) and (4.13), in order to complete the proof of Theorem 2.2 for $R = 2K+1$, it suffices to show that for any $r \in [2K-1]$ and $s \in [K-1]$, the contribution $\widetilde{\Sigma}_{r,s}$ of all n with $\omega_{\parallel}(n) = r$ and $\omega_k(n) = s$ to the left hand side of (4.3) satisfies

$$\widetilde{\Sigma}_{r,s} \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}. \tag{4.14}$$

Now any n counted in $\widetilde{\Sigma}_{r,s}$ has n_k of the form $m' p_1^{c_1} \cdots p_s^{c_s} P_1 \cdots P_r$ for some distinct primes $p_1, \dots, p_s$, $P_1, \dots, P_r$ and integers $m', c_1, \dots, c_s$, which satisfy conditions (i)–(v) in the argument given for the case "$R = KD+1$", but with instances of "$KD+1$" replaced by "$2K+1$", so that in particular, $c_1 + \cdots + c_s \ge 2K+1-r$. Hence again n is of the form $m p_1^{c_1 k} \cdots p_s^{c_s k} P_1^k \cdots P_r^k$, where $p_1, \dots, p_s, P_1, \dots, P_r$ are as above, $P_{Jk}(m) \le y$, $(f(m), q) = 1$ and $f_i(n) = f_i(m p_1^{c_1 k} \cdots p_s^{c_s k}) \prod_{j=1}^r W_{i,k}(P_j)$ for each $i \in [K]$. Defining $\tau_j := \min\{c_j, 2K+1-r\}$ for all $j \in [s]$, we see that $\tau_j \ge 2$ (since $r \le 2K-1$) and that $\tau_1 + \cdots + \tau_s \ge 2K+1-r$. Thus

$$\widetilde{\Sigma}_{r,s} \le \sum_{\substack{\tau_1, \dots, \tau_s \in [2, 2K+1-r] \\ \tau_1 + \cdots + \tau_s \ge 2K+1-r}} \widetilde{\mathcal{N}}_{r,s}(\tau_1, \dots, \tau_s), \tag{4.15}$$

where again $\widetilde{\mathcal{N}}_{r,s}(\tau_1, \dots, \tau_s)$ denotes the number of n counted in (4.3) expressible in the form $m p_1^{c_1 k} \cdots p_s^{c_s k} P_1^k \cdots P_r^k$ with $m, p_1, \dots, p_s, c_1, \dots, c_s, P_1, \dots, P_r$ being pairwise coprime and satisfying $P_1 > z$; $q < P_r < \cdots < P_1$; $p_1, \dots, p_s > q$; $P_{Jk}(m) \le y$; $(f(m), q) = 1$; $f_i(n) = f_i(m p_1^{c_1 k} \cdots p_s^{c_s k}) \prod_{j=1}^r W_{i,k}(P_j)$ and $c_j \ge \tau_j$ for all $j \in [s]$. The bound (4.11) thus continues to hold, and invoking Lemma 3.5 along with the fact that $\tau_1 + \cdots + \tau_s - s + r/2 \ge \max\{s + r/2,\ 2K+1-(s+r/2)\} > K$, we get $\widetilde{\mathcal{N}}_{r,s}(\tau_1, \dots, \tau_s) \ll x^{1/k} / \varphi(q)^K (\log x)^{1-2\alpha_k/3}$, for each $\tau_1, \dots, \tau_s$ in (4.15). This yields (4.14), concluding the proof of Theorem 2.2. □

4.1. **Optimality in the conditions.** As discussed after the statement of Theorem 2.2, the values $R = KD+1$ and $R = 2$ are optimal for the sum of divisors function $\sigma(n)$ to even moduli and squarefree even moduli respectively. We will now show that for *any* $K, k \ge 1$, the value $R = 2K+1$ is nearly optimal in the sense that it cannot be reduced to $2K-1$. To this end, we fix an arbitrary $k \in \mathbb{N}$ and $d > 1$, and define $W_{i,k}(T) := \prod_{j=1}^d (T - 2j) + 2(2i-1)$, so that $\prod_{i=1}^K W_{i,k}$ is separable (over $\mathbb{Q}$). As shown at the start of [48, subsec 8.1], there exists a constant $\widetilde{C} := \widetilde{C}(W_{1,k}, \dots, W_{K,k})$ such that for *any* multiplicative functions $(f_1, \dots, f_K)$ satisfying $f_i(p^k) = W_{i,k}(p)$ for all primes p and all $i \in [K]$, any $\widetilde{C}$-rough k-admissible integer lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$; in other words, $(f_1, \dots, f_K)$ are jointly WUD modulo any fixed $\widetilde{C}$-rough k-admissible integer.

Let $\widetilde{C}_0 > \max\{4KD, \widetilde{C}\}$ be any constant (depending only on $\{W_{i,k}\}_{1\le i\le K}$) exceeding the size of the (nonzero) discriminant of $\prod_{i=1}^K W_{i,k}$. Fix a prime $\ell_0 > \widetilde{C}_0$ and nonconstant polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v<k}} \subset \mathbb{Z}[T]$ such that all the coefficients of all these polynomials are divisible by the prime ℓ_0. Consider any multiplicative functions $f_1, \dots, f_K \colon \mathbb{N} \to \mathbb{Z}$ satisfying $f_i(p^v) := W_{i,v}(p)$ and $f_i(p^{2k}) := 1$ for all primes p, all $i \in [K]$ and $v \in [k]$.

Now let q be any squarefree integer of the form $\prod_{\ell_0\le\ell\le Y} \ell$, where $Y = K_1 \log_2 x$ for some constant $K_1 > 0$ to be determined later. Then $q \le (\log x)^{O(1)}$ and since $P^-(q) = \ell_0$, it follows that for any $v < k$, the product $\prod_{i=1}^K W_{i,v}$ can never take values coprime to q. On the other hand, since $P^-(q) > 4Kd$, the residue $2 \in U_q$ satisfies $\prod_{i=1}^K W_{i,k}(2) = \prod_{i=1}^K (2(2i-1)) \in U_q$. Hence, q is k-admissible and hence also lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$ (by definitions of ℓ_0 and $\widetilde{C}_0$). We also note that for any prime $\ell \mid q$, the residues $1, \dots, d$ are all distinct modulo ℓ (since $\ell > d$). As such, by the Chinese Remainder Theorem, the congruence $\prod_{j=1}^d (v - 2j) \equiv 0 \pmod q$ has exactly $d^{\omega(q)}$ distinct solutions $v \in U_q$.

Consider any $n \le x$ of the form $(p_1 \cdots p_{K-1})^{2k} P^k$ with $P, p_1, \dots, p_{K-1}$ being primes satisfying $P := P(n) > x^{1/3k}$, $q < p_{K-1} < \cdots < p_1 < x^{1/4Kk}$ and $\prod_{1\le j\le d}(P - 2j) \equiv 0 \pmod q$. Then $n_k = (p_1 \cdots p_{K-1})^2 P$, $P_{2K-1}(n_k) = p_{K-1} > q$ and $f_i(n) = W_{i,k}(P) \equiv 2(2i-1) \pmod q$ for each $i \in [K]$. Since the congruence $\prod_{j=1}^d (v-2j) \equiv 0 \pmod q$ has exactly $d^{\omega(q)}$ distinct solutions $v \in U_q$, it follows by the Siegel-Walfisz Theorem that, given $p_1, \dots, p_{K-1}$, the number of possible P is $\gg d^{\omega(q)} x^{1/k} / \varphi(q)(p_1 \cdots p_{K-1})^2 \log x$, where we have noted that $(p_1 \cdots p_{K-1})^2 \le x^{2(K-1)/4Kk} \le x^{1/2k}$. We find that

$$\sum_{\substack{n\le x:\, P_{2K-1}(n_k)>q\\ (\forall i) f_i(n)\equiv 2(2i-1) \ (\mathrm{mod}\ q)}} 1 \gg \frac{d^{\omega(q)} x^{1/k}}{\varphi(q)\log x}\left(\sum_{q<p_1,\dots,p_{K-1}\le x^{1/4Kk}} \frac{1}{(p_1 \dots p_{K-1})^2} - \sum_{\substack{p_1,\dots,p_{K-1}>q\\ \exists i\ne j:\, p_i=p_j}} \frac{1}{(p_1 \dots p_{K-1})^2}\right),$$

where we have divided by $k! \ll 1$ to replace the ordering condition on $p_1, \dots, p_{K-1}$ by a distinctness condition. Here the second sum is empty for $K < 3$. Now the first sum above is equal to $\prod_{1\le j\le K-1}\left(\sum_{q<p_j\le x^{1/4Kk}} p_j^{-2}\right) \gg 1/(q\log q)^{K-1}$, whereas the second sum is $\ll (\sum_{p>q} p^{-4})(\sum_{p>q} p^{-2})^{K-3} \ll q^{-K}$. Altogether, we find that

$$\sum_{\substack{n\le x:\, P_{2K-1}(n_k)>q\\ (\forall i) f_i(n)\equiv 2(2i-1) \ (\mathrm{mod}\ q)}} 1 \gg \frac{d^{\omega(q)}}{\varphi(q)^K} \cdot \frac{x^{1/k}}{(\log_2 x)^K \log x}.$$

By (3.1) and the fact that $\alpha_k \gg 1/\log_2(3q)$, we see that the right hand side above grows strictly faster than the expected proportion $\frac{1}{\varphi(q)}\#\{n \le x : (f(n), q) = 1\}$ if $d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$ for some $\epsilon > 0$. But by the Chinese Remainder Theorem and the Prime Ideal Theorem, we see that

$$\alpha_k = \prod_{\ell_0\le\ell\le Y}\left(1 - \frac{1}{\ell-1}\#\{u \in U_q : \prod_{i=1}^K W_{i,k}(u) \equiv 0 \pmod \ell\}\right) < \frac{\kappa}{\log Y}$$

for some constant $\kappa = \kappa(W_{1,k}, \dots, W_{K,k}; \ell_0) > 0$. Since $\omega(q) = \#\{\ell : \ell_0 \le \ell \le Y\} > Y/2\log Y$, it follows that the desired bound $d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$ holds if $Y > 2\kappa(1+\epsilon)\log_2 x/\log d$, which can be guaranteed by choosing the constant $K_1 > 2\kappa(1+\epsilon)/\log d$. Thus, with this choice of q, we see that the coprime residues $(2(2i-1))_{i=1}^K$ are overrepresented by the multiplicative functions $f_1, \dots, f_K$ if we only restrict to inputs n having $P_{2K-1}(n_k) > q$. The condition $P_{2K+1}(n_k) > q$ in Theorem 2.2 thus cannot be weakened to $P_{2K-1}(n_k) > q$.

5. Counting solution tuples to general multivariate polynomial congruences: Final preparatory step for Theorem 2.3

In order to complete the proof of Theorem 2.3, we will need to generalize (3.5). The following notation and conventions will be relevant only in the rest of the section.

Let $\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}} \subset \mathbb{Z}[T]$ be a fixed collection of nonconstant polynomials such that for each $r \in [L]$, the polynomials $\{G_{i,r}\}_{1\le i\le K} \subset \mathbb{Z}[T]$ are multiplicatively independent. Define $D_0 := \max_{1\le r\le L} \sum_{i=1}^K \deg G_{i,r}$. Let $N \ge 1$ and $\{F_{i,j}\}_{\substack{1\le i\le K\\ 1\le j\le N}} \subset \mathbb{Z}[T]$ be a family of polynomials such that for each $j \in [N]$, the vector $(F_{i,j})_{i=1}^K$ coincides with one of the vectors $(G_{i,j'})_{i=1}^K$ for some $j' \in [L]$ (possibly depending on j). In this case we define, for any integer q,

$$\widetilde{\alpha}_j(q) := \frac{1}{\varphi(q)}\#\{u \in U_q : \prod_{i=1}^K F_{i,j}(u) \in U_q\} = \frac{1}{\varphi(q)}\#\{u \in U_q : \prod_{i=1}^K G_{i,j'}(u) \in U_q\},$$

and let $\alpha_N^*(q) := \prod_{j=1}^N \widetilde{\alpha}_j(q)$. For any $(w_i)_{i=1}^K \in U_q^K$, define

$$\widetilde{\mathcal{V}}_{N,K}\left(q; (w_i)_{i=1}^K\right) := \left\{(v_1, \dots, v_N) \in U_q^N :\ (\forall i \in [K])\ \prod_{j=1}^N F_{i,j}(v_j) \equiv w_i \pmod q\right\}.$$

Fix $B_0 > 0$. In the result below, the implied constants may depend only on B_0 and on the fixed collection of polynomials $\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}$ (besides other parameters declared explicitly).

Proposition 5.1. *There exists a constant $C_0 := C_0\left(\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}; B_0\right) > (8D_0)^{2D_0+2}$ depending only on $\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}$ and B_0, such that the following hold for any **fixed** $N \ge 1$.*

(a) *Uniformly in q and in coprime residues $w_1, \dots, w_K$ mod q, we have*

$$\frac{\#\widetilde{\mathcal{V}}_{N,K}\left(q; (w_i)_{i=1}^K\right)}{\varphi(q)^N} \le \frac{\left(\prod_{\ell^e \| q} e\right)^{\mathbb{1}_{N=KD_0}}}{q^{\min\{K, N/D_0\}}} \exp\left(O(\omega(q))\right). \tag{5.1}$$

(b) *Uniformly in **squarefree** q and in coprime residues $w_1, \dots, w_K$ mod q, we have*

$$\frac{\#\widetilde{\mathcal{V}}_{N,K}\left(q; (w_i)_{i=1}^K\right)}{\varphi(q)^N} \ll \frac{1}{q^{\min\{K, N/2\}}} \exp\left(O(\omega(q) + \mathbb{1}_{N\ge 2K+1}\sqrt{\log q})\right). \tag{5.2}$$

Proof. The argument is analogous to that given for (3.5) in [48], however we need to be careful of the fact that we no longer have any invariant factor hypotheses. In what follows, q is an arbitrary positive integer (unless stated otherwise). We may assume that $\alpha_N^*(q) \ne 0$, for both (a) and (b) are tautological otherwise (since the left hand side becomes zero). In particular, this means that $\text{ord}_\ell(\prod_{i=1}^K \prod_{j=1}^N F_{i,j}) = 0$ for each prime $\ell \mid q$. Fix $C_0 :=$

$C_0\left(\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}; B_0\right)$ to be any constant exceeding B_0, $(32D_0)^{2D_0+2}$, the sizes of the leading and constant coefficients of $\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}$, as well as the constants $C_1(G_{1,r},\dots,G_{K,r})$ coming from applications of Proposition 3.9 to each of the families $\{G_{i,r}\}_{1\le i\le K}$ of multiplicatively independent polynomials. We will show that any such choice of C_0 suffices.

Proof of (a). We consider the case $D_0 > 1$; the case $D_0 = 1$ can be dealt with by a simpler version of this argument (also we don't need the case $D_0 = 1$ in the proof of Theorem 2.3). For an arbitrary positive integer Q and coprime residues $w_1,\dots,w_K$ mod Q, we apply the orthogonality of Dirichlet characters to detect the congruences defining $\widetilde{\mathcal{V}}_{N,K}\left(Q;(w_i)_{i=1}^K\right)$. This yields

(5.3)
$$\#\widetilde{\mathcal{V}}_{N,K}\left(Q;(w_i)_{i=1}^K\right) = \frac{1}{\varphi(Q)^K}\sum_{\chi_1,\dots,\chi_K \bmod Q}\overline{\chi}_1(w_1)\cdots\overline{\chi}_K(w_K)\prod_{j=1}^N Z_{Q;\,\chi_1,\dots,\chi_K}(F_{1,j},\dots,F_{K,j}),$$

where $Z_{Q;\,\chi_1,\dots,\chi_K}(F_{1,j},\dots,F_{K,j}) := \sum_{v \bmod Q}\chi_{0,Q}(v)\prod_{i=1}^K\chi_i(F_{i,j}(v))$ and $\chi_{0,Q}$ denotes (as usual) the trivial character mod Q.

We will first show that for each fixed $N \ge 1$, there is a constant K' depending at most on N and $\{G_{i,r}\}_{\substack{1\le i\le K\\ 1\le r\le L}}$ such that

$$\frac{\#\widetilde{\mathcal{V}}_{N,K}(\ell^e;(w_i)_{i=1}^K)}{\varphi(\ell^e)^N} \le K'\ \frac{e^{\mathbb{1}_{N=KD_0}}}{(\ell^e)^{\min\{K,N/D_0\}}}. \tag{5.4}$$

uniform in residues $w_1,\dots,w_K \in U_{\ell^e}$ for primes $\ell > C_0$. To this end, we start by applying (5.3) with $Q := \ell^e$ to get

$$\begin{aligned}&\frac{\#\widetilde{\mathcal{V}}_{N,K}(\ell^e;(w_i)_{i=1}^K)}{\varphi(\ell^e)^N}\\ &\qquad\le \frac{1}{\varphi(\ell^e)^K}\left\{1+\frac{1}{\varphi(\ell^e)^N}\sum_{(\chi_1,\dots,\chi_K)\ne(\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e}\ \prod_{j=1}^N\left|Z_{\ell^e;\,\chi_1,\dots,\chi_K}(F_{1,j},\dots,F_{K,j})\right|\right\}.\end{aligned} \tag{5.5}$$

Consider any tuple $(\chi_1,\dots,\chi_K) \ne (\chi_{0,\ell},\dots,\chi_{0,\ell})$ mod ℓ^e and any $j \in [N]$. Let $\ell^{e_0} := \operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)] \in \{\ell,\dots,\ell^e\}$. Using $\chi_1,\dots,\chi_K$ to also denote the characters mod ℓ^{e_0} inducing $\chi_1,\dots,\chi_K$ respectively, we get

$$Z_{\ell^e;\,\chi_1,\dots,\chi_K}(F_{1,j},\dots,F_{K,j}) = \ell^{e-e_0}\ Z_{\ell^{e_0};\,\chi_1,\dots,\chi_K}(F_{1,j},\dots,F_{K,j}) \tag{5.6}$$

Letting γ denote a generator of the group $U_{\ell^{e_0}}$ for each $\ell > C_0 > 2$, we see that the character group mod ℓ^{e_0} is generated by the character ψ_{e_0} defined by $\psi_{e_0}(\gamma) := \exp(2\pi i/\varphi(\ell^{e_0}))$. As such, there exists a tuple $(A_1,\dots,A_K) \in [\varphi(\ell^{e_0})]$ satisfying $\chi_i = \psi_{e_0}^{A_i}$ for each i, and

$$(A_1,\dots,A_K) \not\equiv \begin{cases}(0,\dots,0) \pmod{\ell}, & \text{if } e_0 > 1,\\ (0,\dots,0) \pmod{\ell-1}, & \text{if } e_0 = 1,\end{cases} \tag{5.7}$$

since at least one of $\chi_1, \dots, \chi_K$ is primitive mod ℓ^{e_0}. This gives

$$Z_{\ell^{e_0};\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j}) = \sum_{v \bmod \ell^{e_0}} \psi_{e_0}\left(v^{\varphi(\ell^{e_0})} \prod_{i=1}^{K} F_{i,j}(v)^{A_i}\right). \tag{5.8}$$

We now consider two possibilities, namely when $e_0 = 1$ or $e_0 \geq 2$.

Case 1*:* Suppose $e_0 = 1$. For each $j \in [N]$, consider $j' \in [L]$ satisfying $(G_{i,j'})_{i=1}^K = (F_{i,j})_{i=1}^K$. By Proposition 3.9(a), we see there are $O_L(1)$ many possible tuples $(\chi_1, \dots, \chi_K)$ of characters mod ℓ^e having $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell$, for which $T^{\varphi(\ell)} \prod_{i=1}^K F_{i,j}(T)^{A_i} = T^{\varphi(\ell)} \prod_{i=1}^K G_{i,j'}(T)^{A_i}$ is of the form $c \cdot G(T)^{\ell-1}$ in $\mathbb{F}_\ell[T]$ for some $j \in [N]$ (here A_i are as above). For all the remaining tuples $(\chi_1, \dots, \chi_K)$ with $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell$, we may invoke Proposition 3.7 to obtain, **for all** $j \in [N]$,

$$|Z_{\ell;\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j})| = \left| \sum_{v \bmod \ell} \psi_1\left(v^{\varphi(\ell)} \prod_{i=1}^{K} F_{i,j}(v)^{A_i}\right) \right| \leq \left(\sum_{i=1}^{K} \deg F_{i,j}\right) \ell^{1/2} \leq D_0 \ell^{1/2}.$$

By (5.6), we deduce that for all but $O_L(1)$ many tuples $(\chi_1, \dots, \chi_K)$ of characters mod ℓ^e satisfying $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell$, we have

$$|Z_{\ell^e;\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j})| \leq D_0 \ell^{e-1/2} \quad \text{for every } j \in [N], \tag{5.9}$$

Case 2: Now assume that $e_0 \geq 2$. Consider an arbitrary $j \in [N]$ and let $(G_{i,j'})_{i=1}^K = (F_{i,j})_{i=1}^K$ for some $j' \in [L]$. Since $\ell > C_0 > C_1(G_{1,j'}, \dots, G_{K,j'})$ and $e_0 \geq 2$, Proposition 3.9(b) and (5.7) show that $\tau(\ell) := \mathrm{ord}_\ell\left((T^{\varphi(\ell^{e_0})} \prod_{i=1}^K F_{i,j}(T)^{A_i})'\right) = 0$. Consequently, (5.8) and Proposition 3.8(i) yield $|Z_{\ell^{e_0};\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j})| \leq \left(\sum_{\theta \in \mathcal{A}_\ell} \mu_\theta(\mathcal{C}_\ell)\right) \ell^{e_0(1-1/(M_\ell+1))}$, where $\mathcal{A}_\ell \subset \mathbb{F}_\ell$ denotes the set of ℓ-critical points of the polynomial $T^{\varphi(\ell^{e_0})} \prod_{i=1}^K F_{i,j}(T)^{A_i}$, $\mathcal{C}_\ell(T) := (T^{\varphi(\ell^{e_0})} \prod_{i=1}^K F_{i,j}(T)^{A_i})'$ and $M_\ell := \max_{\theta \in \mathcal{A}_\ell} \mu_\theta(\mathcal{C}_\ell)$. Moreover, by the last assertion in Propositon 3.9, any $\theta \in \mathcal{A}_\ell$ is a root of the polynomial $\widetilde{F}(T) := \sum_{i=1}^K A_i F'_{i,j}(T) \prod_{\substack{1 \leq r \leq K \\ r \neq i}} F_{r,j}(T)$ (a nonzero element of $\mathbb{F}_\ell[T]$), and $\mu_\theta(\mathcal{C}_\ell) = \mu_\theta(\widetilde{F})$. As such, $M_\ell \leq \sum_{\theta \in \mathcal{A}_\ell} \mu_\theta(\mathcal{C}_\ell) \leq D_0 - 1$, yielding $|Z_{\ell^{e_0};\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j})| \leq (D_0 - 1)\ell^{e_0(1-1/D_0)}$. Thus, by (5.6),

$$|Z_{\ell^e;\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j})| \leq (D_0 - 1)\ell^{e-e_0/D_0} \text{ if } \ell^{e_0} := \mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] \in \{\ell^2, \dots, \ell^e\}. \tag{5.10}$$

For any $e_0 \in \{1, \dots, e\}$ there are at most $\ell^{e_0 K}$ tuples $(\chi_1, \dots, \chi_K)$ of characters mod ℓ^e having $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell^{e_0}$. Bounds (5.9) and (5.10) show that for each fixed $N \geq 1$,

$$\sum_{(\chi_1,\dots,\chi_K) \neq (\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e} \left| \prod_{j=1}^{N} Z_{\ell^e;\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j}) \right| \ll \varphi(\ell^e)^N + D_0^N \ell^{eN} \sum_{1 \leq e_0 \leq e} \ell^{e_0(K-N/D_0)}, \tag{5.11}$$

where we have used $D_0 > 1$ to see that $K - N/2 \leq K - N/D_0$. If $N \geq KD_0 + 1$, then from $\ell^{N-K/D_0} \leq \ell^{-1/D_0} \leq C_0^{-1/D_0} \leq 1/2$, we see that

$$\frac{1}{\varphi(\ell^e)^N} \sum_{(\chi_1,\dots,\chi_K) \neq (\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e} \left| \prod_{j=1}^{N} Z_{\ell^e;\ \chi_1,\dots,\chi_K}(F_{1,j}, \dots, F_{K,j}) \right| \ll 1.$$

On the other hand if $N \in \{1, \ldots, KD_0\}$, the expression in (5.11) leads to

$$\frac{1}{\varphi(\ell^e)^N} \sum_{(\chi_1,\ldots,\chi_K) \neq (\chi_{0,\ell},\ldots,\chi_{0,\ell}) \bmod \ell^e} \left| \prod_{j=1}^{N} Z_{\ell^e;\ \chi_1,\ldots,\chi_K}(F_{1,j}, \ldots, F_{K,j}) \right| \ll e^{\mathbb{1}_{N=KD_0}} \ell^{e(K-N/D_0)}.$$

Inserting the last two bounds displays into (5.5) yields (5.4).

Now for an arbitrary q, we let $\widetilde{q} \coloneqq \prod_{\substack{\ell^e \| q \\ \ell \leq C_0}} \ell^e$ denote the C_0-smooth part of q. By (5.3),

$$\#\widetilde{\mathcal{V}}_{N,K}\left(\widetilde{q}; (w_i)_{i=1}^K\right) = \frac{1}{\varphi(\widetilde{q})^K} \sum_{\chi_1,\ldots,\chi_K \bmod \widetilde{q}} \overline{\chi}_1(w_1) \cdots \overline{\chi}_K(w_K) \prod_{j=1}^{N} Z_{\widetilde{q};\ \chi_1,\ldots,\chi_K}(F_{1,j}, \ldots, F_{K,j}). \tag{5.12}$$

Fix κ to be any integer constant exceeding $(30D_0C_0^{C_0})^{2C_0}$, and let $Q_0 \coloneqq \prod_{\ell^e \| \widetilde{q}} \ell^{\min\{e,\kappa\}} = \prod_{\ell \leq C_0} \ell^{\min\{v_\ell(q),\kappa\}}$ denote the largest $(\kappa+1)$-free divisor of $\widetilde{q}$. Write the expression on the right hand side of (5.12) as $\mathcal{S}' + \mathcal{S}''$, where $\mathcal{S}'$ denotes the contribution of those tuples $(\chi_1, \ldots, \chi_K)$ mod $\widetilde{q}$ for which $\mathrm{lcm}[\mathfrak{f}(\chi_1), \ldots, \mathfrak{f}(\chi_K)]$ is $(\kappa+1)$-free, or equivalently, those $(\chi_1, \ldots, \chi_K)$ for which $\mathrm{lcm}[\mathfrak{f}(\chi_1), \ldots, \mathfrak{f}(\chi_K)]$ divides Q_0.

By arguments entirely analogous to those leading to equations (5.18) and (5.19) in [48], we can show that for any fixed $N \geq 1$, we have

$$\frac{\mathcal{S}'}{\varphi(\widetilde{q})^N} = \left(\frac{\varphi(Q_0)}{\varphi(\widetilde{q})}\right)^K \frac{\#\widetilde{\mathcal{V}}_{N,K}\left(Q_0; (w_i)_{i=1}^K\right)}{\varphi(Q_0)^N} \ll \frac{1}{\varphi(\widetilde{q})^K} \ll \frac{1}{\widetilde{q}^K} \quad \text{and} \quad \frac{|\mathcal{S}''|}{\varphi(\widetilde{q})^N} \ll \frac{\left(\prod_{\ell^e \| \widetilde{q}} e\right)^{\mathbb{1}_{N=KD_0}}}{\widetilde{q}^{\min\{K,N/D_0\}}}.$$

Combining these, we obtain for any fixed $N \geq 1$,

$$\frac{\#\widetilde{\mathcal{V}}_{N,K}\left(\widetilde{q}; (w_i)_{i=1}^K\right)}{\varphi(\widetilde{q})^N} \ll \frac{\left(\prod_{\ell^e \| \widetilde{q}} e\right)^{\mathbb{1}_{N=KD_0}}}{\widetilde{q}^{\min\{K,N/D_0\}}}. \tag{5.13}$$

Finally, multiplying resp. (5.13) with the relations (5.4) over all $\ell^e \parallel q$ with $\ell > C_0$ completes the proof of subpart (a).

Proof of (b). This follows by a much simpler version of the above arguments. Indeed applying (5.5) with $e \coloneqq 1$ and (5.9), we obtain for all primes $\ell > C_0$ dividing q, $\#\widetilde{\mathcal{V}}_{N,K}(\ell, (w_i)_{i=1}^K)/\varphi(\ell)^N \ll \ell^{-\min\{K,N/2\}}(1 + O(\mathbb{1}_{N \geq 2K+1}\ell^{-1/2}))$. Multiplying this over all such primes and noting that $\prod_{\ell | q}(1 + O(\ell^{-1/2})) \ll \exp(O(\sqrt{\log q}))$ and $\prod_{\ell | q:\, \ell \leq C_0} \ell \ll 1$, we obtain the desired bound. □

Remark. Taking $K = L = N = 1$ and $G_{1,1} = H \in \mathbb{Z}[T]$ with $\deg H = d \geq 1$ in (5.1), we get

$$\frac{1}{\varphi(q)} \#\{v \in U_q : H(v) \equiv w \pmod{q}\} \ll \frac{(\prod_{\ell^e \| q} e)^{\mathbb{1}_{d=1}}}{q^{1/d}} \cdot \exp\left(O(\omega(q))\right) \ll_\delta \frac{1}{q^{1/d-\delta}} \tag{5.14}$$

for any fixed $\delta > 0$. This is only slightly weaker than the results of Konyagin in [19, 20].

6. Restricted inputs with higher polynomial control: Proof of Theorem 2.3

By the same initial reductions as in the proof of Theorem 2.2, it suffices to show that

$$\sum\nolimits^{*}_{n:\ P_R(n)>q} 1 \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}, \tag{6.1}$$

with the respective values of R in the two subparts. The subsequent calculations will hold for either value of R until stated explicitly. Note that (for the first time in our proofs), we will allow our implied constants to depend on V, and on the full set of polynomials $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le V}}$.

We will first show that in either of the two subparts of the theorem, the contribution to the left hand side of (6.1) from the n's which are divisible by the $(V+1)$-th power of a prime exceeding q can be absorbed in the right hand side. Any such n can be written in the form mp^cP^k, where $P := P(n) > z$, $p \in (q, P)$ is prime, $c \ge V+1$, $P_{Jk}(m) \le y$ and $P \bmod q \in \mathcal{V}_{1,K}^{(k)}\big(q; (a_i f_i(mp^c)^{-1})\big)$. Proceeding as in the proof of (4.8), we see that the contribution of such n is $\ll \frac{V'_{1,K}}{\varphi(q)q^{(V+1)/k-1}} \cdot \frac{x^{1/k}}{(\log x)^{1-2\alpha_k/3}}$. For general q, an application of (5.14) (with H being a polynomial among $\{W_{i,k}\}_{1\le i\le K}$ having least degree) shows that the expression above is $\ll x^{1/k}/q^K(\log x)^{1-2\alpha_k/3}$, since $(V+1)/k - 1 + 1/D_{\min} > K$ by the hypothesis of Theorem 2.3(a). On the other hand, if q is squarefree, then from $V'_{1,K} \ll D_{\min}^{\omega(q)}$ and $V \ge Kk$, it follows that the contribution of such n is once again $\ll x^{1/k}/q^K(\log x)^{1-2\alpha_k/3}$.

To prove (6.1), it thus only remains to consider the contribution of the n's for which $v_p(n) \le V$ for any prime $p > q$. We recall that $\omega_{\parallel}(n) = \#\{p > q : p^k \parallel n\}$ and define $\omega^*(n) = \#\{p > q : p^{k+1} | n\}$. By replicating the arguments leading to (4.4) (see [48, eq (9.3)]), we can show that

$$\sum_{\substack{n\le x:\ (f(n),q)=1\\ \omega^*(n)\ge Kk,\ P_{Jk}(n)\le y,\ P(n)>z\\ p>y \implies p^{k+1}\nmid n}} 1 \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}. \tag{6.2}$$

We thus only need to consider the contribution of those n which have $v_p(n) \le V$ for any prime $p > q$ as well as $\omega^*(n) \in [Kk-1]$ and $\omega_{\parallel}(n) \in [KD]$ (resp. $\omega_{\parallel}(n) \in [2K]$ if q is squarefree). This is because the contribution of the n having $\omega_{\parallel}(n) \ge KD+1$ (resp. $\omega_{\parallel}(n) \ge 2K+1$) has already been bounded in (4.5) (resp. (4.13)), while the contribution of the n having $\omega^*(n) \ge Kk$ has already been bounded in (6.2), and finally since any n for which $\omega^*(n) = 0$ must anyway have $\omega_{\parallel}(n) \ge KD+1$ (resp. $\omega_{\parallel}(n) \ge 2K+1$) as $R \ge k(KD+1)$ (resp. $R \ge k(2K+1)$). It thus remains to show that for a given $r \in [KD]$ (resp. $r \in [2K]$) and $s \in [Kk-1]$, we have

$$\widetilde{\mathcal{M}}_{r,s} \ll \frac{x^{1/k}(\log_2 x)^{O(1)}}{q^K \log x}, \tag{6.3}$$

where $\widetilde{\mathcal{M}}_{r,s}$ denotes the contribution to the left hand side of (6.1) from all the n having $\omega_{\parallel}(n) = r$, $\omega^*(n) = s$, and $k \le v_p(n) \le V$ for all $p > q$ dividing n. For given r and s,

$$\widetilde{\mathcal{M}}_{r,s} \le \sum_{\substack{c_1,\dots,c_s\in[k+1,V]\\ c_1+\cdots+c_s\ge R-kr}} \widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s), \tag{6.4}$$

with $\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s)$ denoting the count of n in $\widetilde{\mathcal{M}}_{r,s}$ which can be written in the form $mp_1^{c_1}\cdots p_s^{c_s}P_1^k\cdots P_r^k$, with $p_1,\dots,p_s,P_1,\dots,P_r$ being distinct primes exceeding q, $P(m)\le q$, $P_1 = P(n) > z$, $P_r < \cdots < P_1$, *and* $f_i(n) = f_i(m)\prod_{l=1}^s W_{i,c_l}(p_l)\cdot\prod_{j=1}^r W_{i,k}(P_j)$. With $\mathcal{V}_{r+s,K}(q;\ (c_j)_{j=1}^s;\ (w_i)_{i=1}^K)$ being the set of tuples $(u_1,\dots,u_s,v_1,\dots,v_r)\in U_q^{s+r}$ satisfying the congruences $\prod_{l=1}^s W_{i,c_l}(u_l)\cdot\prod_{j=1}^r W_{i,k}(v_j)\equiv w_i \pmod q$ for each $i\in[K]$, the conditions $f_i(n)\equiv a_i \pmod q$ amount to $(p_1,\dots,p_s,\ P_1,\dots,P_r) \bmod q\ \in\ \mathcal{V}_{r+s,K}\big(q;\ (c_j)_{j=1}^s;\ (a_if_i(m)^{-1})_{i=1}^K\big)$.

Given m and $(u_1,\dots,u_s,v_1,\dots,v_r)\in\mathcal{V}_{r+s,K}\big(q;\ (c_j)_{j=1}^s;\ (a_if_i(m)^{-1})_{i=1}^K\big)$, we bound the number of possible $(p_1,\dots,p_s,P_1,\dots,P_r)$ satisfying $(p_1,\dots,p_s,P_1,\dots,P_r)\equiv(u_1,\dots,u_s,v_1,\dots,v_r) \bmod q$. First, given $(p_1,\dots,p_s)$, the number of possible $(P_1,\dots,P_r)$ is, by the arguments leading to (4.6), $\ll x^{1/k}(\log_2 x)^{O(1)}\big/\varphi(q)^r p_1^{c_1/k}\cdots p_s^{c_s/k}m^{1/k}\log x$. We sum this over possible $p_1,\dots,p_s>q$, making use of the observation that for fixed $\varepsilon_1>0$, we have $\sum_{\substack{n>q\\ n\equiv u \pmod q}} 1/n^{1+\theta} \ll_{\varepsilon_1} 1/q^{1+\theta}$, uniformly in residue classes $u \bmod q$, and uniformly in $\theta>\varepsilon_1$. We find that the number of possible $(p_1,\dots,p_s,P_1,\dots,P_r)$ is $\ll x^{1/k}(\log_2 x)^{O(1)}\big/\varphi(q)^r q^{(c_1+\dots+c_s)/k}m^{1/k}\log x$. Finally we sum the above expression over all possible $(u_1,\dots,u_s,v_1,\dots,v_r)$ and then over all m satisfying $P(m)\le q$ and $(f(m),q)=1$. By Lemma 3.2, any such m is of the form BM for some k-free $B=O(1)$ and some k-full q-smooth M. Since the sum of $1/M^{1/k}$ is $\ll\prod_{p\le q}(1+\sum_{v\ge k}1/p^{v/k}))\ll\exp(\sum_{p\le q}1/p)\ll\log q$, we obtain

$$\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s)\ll\frac{1}{q^{(c_1+\dots+c_s)/k-s}}\cdot\frac{V'_{r+s,K}(q;\ (c_j)_{j=1}^s)}{\varphi(q)^{r+s}}\cdot\frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x},\tag{6.5}$$

where $V'_{r+s,K}(q;\ (c_j)_{j=1}^s) \coloneqq \max\big\{\#\mathcal{V}_{r+s,K}(q;\ (c_j)_{j=1}^s;\ (w_i)_{i=1}^K) : (w_i)_{i=1}^K\in U_q^K\big\}$.

Completing the proof of Theorem 2.3(a). We specialize to $R\coloneqq\max\{k(KD+1),(Kk-1)D_0+2\}$, and apply Proposition 5.1(a) with $(G_{i,r})_{\substack{1\le i\le K\\ 1\le r\le L}}$ being the system $(W_{i,v})_{\substack{1\le i\le K\\ k\le v\le V}}$, so that $G_{i,r}\coloneqq W_{i,k+r-1}$ and $\sum_{i=1}^K\deg G_{i,r}=D_{k+r-1}$. We also set $N\coloneqq r+s$, and define $\{F_{i,j}\}_{\substack{1\le i\le K\\ 1\le j\le N}}$ by setting (for all $i\in[K]$) $F_{i,j}\coloneqq W_{i,c_j}$ for $j\in[s]$ and $F_{i,j}\coloneqq W_{i,k}$ for $s+1\le j\le s+r$, so that $\widetilde{\mathcal{V}}_{N,K}\left(q;(w_i)_{i=1}^K\right)=\mathcal{V}_{r+s,K}(q;\ (c_j)_{j=1}^s;\ (w_i)_{i=1}^K)$.

If $r+s\ge KD_0+1$, then (5.1) (applied to $N\coloneqq r+s\in[KD_0+1,KD+Kk-1]$ [5]) yields $V'_{r+s,K}(q;\ (c_j)_{j=1}^s)/\varphi(q)^{r+s}\ll q^{-K}\exp\big(O(\omega(q))\big)$. Inserting this into (6.5) and using that $(c_1+\dots+c_s)/k-s\ge s/k\ge 1/k$, we obtain $\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s)\ll x^{1/k}(\log_2 x)^{O(1)}/q^K\log x$. On the other hand, if $r+s\le KD_0$, then (5.1) and (6.5) lead to

$$\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s)\ \ll\ \frac{\big(\prod_{\ell^e\| q}e\big)\exp\big(O(\omega(q))\big)}{q^{\max\{s/k+(r+s)/D_0,\ R/k-(1-1/D_0)(r+s)\}}}\cdot\frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x},$$

where we have recalled that $(c_1+\dots+c_s)/k-s\ge\max\{s/k,R/k-r-s\}$. Since $R>(Kk-1)D_0+1$, it is easy to check that the exponent of q above exceeds K. This proves that $\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s)\ll x^{1/k}(\log_2 x)^{O(1)}/q^K\log x$ for any tuple $(c_1,\dots,c_s)$ counted in the sum (6.4), and since there are $O(1)$ many such tuples, we obtain the desired bound (6.3).

[5] Here we are of course assuming that such r and s exist in the first place, which amounts to having $KD_0+1\le KD+Kk-1$

Completing the proof of Theorem 2.3(b). This time we use Proposition 5.1(b). If $r+s \ge 2K+1$, then (5.2) yields $V'_{r+s,K}(q;\ (c_j)_{j=1}^{s}) \ll q^{-K}\exp\big(O(\omega(q))\big)$. Inserting this into (6.5) and again using $(c_1+\cdots+c_s)/k - s \ge s/k \ge 1/k$ shows that $\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s) \ll x^{1/k}(\log_2 x)^{O(1)}/q^K\log x$ in this case. On the other hand, if $r+s \le 2K$, then (5.2) yields

$$\widetilde{\mathcal{M}}_{r,s}(c_1,\dots,c_s) \ \ll\ \frac{\exp\big(O(\omega(q))\big)}{q^{\max\{s/k+(r+s)/2,\ R/k-(r+s)/2\}}}\cdot\frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x},$$

and it is easy to see that the exponent of q above always exceeds K. □

This finally establishes Theorems 2.2 and 2.3. As such, we shall no longer continue with the set-up for these results. In the next section, we shall prove Theorems 2.4 and 2.5, and thus shall only be assuming the hypotheses mentioned explicitly in their respective statements.

7. Necessity of the multiplicative independence and invariant factor hypotheses: Proofs of Theorems 2.4 and 2.5

The first inequality in both theorems being tautological, we focus on the second. We first give a lower bound that will be useful in both the theorems. Until we specialize to each theorem, we will not assume anything about $\{W_{i,k}\}_{1\le i\le K} \in \mathbb{Z}[T]$ beyond that they are nonconstant, and our estimates will be uniform in all $q \le (\log x)^{K_0}$ and $(a_i)_{i=1}^{K} \in U_q^K$.

Let $y := \exp(\sqrt{\log x})$ and given any fixed $R \ge 1$, we let $V'_q := \mathcal{V}^{(k)}_{R,K}\big(q;(a_i)_{i=1}^{K}\big) = \{(v_1,\dots,v_R) \in U_q^R : (\forall i \in [K])\ \prod_{j=1}^{R} W_{i,k}(v_j) \equiv a_i \pmod q\}$. Consider any $N \le x$ of the form $N = (P_1\cdots P_R)^k$, where $P_1,\dots,P_R$ are primes satisfying $y < P_R < \cdots < P_1$, and $(P_1,\dots,P_R) \bmod q \in V'_q$. Then $P_R(N_k) > y > q$ and $f_i(N) = \prod_{j=1}^{R} W_{i,k}(P_j) \equiv a_i \pmod q$. Replacing the ordering condition on $P_1,\dots,P_R$ by the condition that they are distinct, we get

$$\sum_{\substack{n\le x:\ P_R(n_k)>q\\ (\forall i)\ f_i(n)\equiv a_i \ (\mathrm{mod}\ q)}} 1 \ =\ \sum_{(v_1,\dots,v_R)\in V'_q} \frac{1}{R!} \sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \ (\mathrm{mod}\ q)}} 1.$$

Proceeding exactly as in [38] to remove the congruence conditions on $P_1,\dots,P_R$ by successive applications of the Siegel–Walfisz Theorem, we see that

$$\sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \ (\mathrm{mod}\ q)}} 1 \ =\ \frac{1}{\varphi(q)^R} \sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}}} 1 \ +\ O\left(x^{1/k}\exp\left(-K_1(\log x)^{1/4}\right)\right) \tag{7.1}$$

for some constant $K_1 > 0$. Collecting estimates and using the fact that $\#V'_q \le \varphi(q)^R \le (\log x)^{K_0 R}$, we see that there is a constant $K_2 > 0$ such that

$$\sum_{\substack{n\le x:\ P_R(n_k)>q\\ (\forall i)\ f_i(n)\equiv a_i \ (\mathrm{mod}\ q)}} 1 \ \ge\ \frac{V'_q}{\varphi(q)^R}\cdot\frac{1}{R!} \sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}}} 1 \ -\ x^{1/k}\exp(-K_2(\log x)^{1/4}).$$

The sum in the main term is exactly the count of squarefree y-rough integers $m \le x^{1/k}$ having $\Omega(m) = R$. Ignoring this squarefreeness condition incurs a negligible error of $\sum_{p>y} \sum_{\substack{m \le x^{1/k} \\ p^2 \mid m}} 1 \ll x^{1/k}/y$. We thus find that the main term in the above display equals $\#\{m \le x^{1/k} : P^-(m) > y,\ \Omega(m) = R\}$, which is $\gg x^{1/k}(\log_2 x)^{R-1}/\log x$ by a straightforward induction on R (via Chebyshev's estimates). As a consequence,

$$\sum_{\substack{n \le x:\ P_R(n_k) > q \\ (\forall i)\ f_i(n) \equiv a_i \pmod q}} 1 \ \gg\ \frac{V_q'}{\varphi(q)^R} \cdot \frac{x^{1/k}(\log_2 x)^{R-1}}{\log x} \ -\ x^{1/k} \exp(-K_1(\log x)^{1/4}). \tag{7.2}$$

Completing the proof of Theorem 2.4. We now restrict to the $\{W_{i,k}\}_{1 \le i \le K}$ and $(a_i)_{i=1}^K$ considered in Theorem 2.4, so $K \ge 2$, $\{W_{i,k}\}_{1 \le i \le K-1} \subset \mathbb{Z}[T]$ are multiplicatively independent, $W_{K,k} = \prod_{i=1}^{K-1} W_{i,k}^{\lambda_i}$ for some tuple $(\lambda_i)_{i=1}^{K-1} \ne (0, \dots, 0)$ of nonnegative integers, and $(a_i)_{i=1}^K \in U_q^K$ satisfy $a_K \equiv \prod_{i=1}^{K-1} a_i^{\lambda_i} \pmod q$. The key observation is that relations assumed between the $\{W_{i,k}\}_{1 \le i \le K}$ and $(a_i)_{i=1}^K$ guarantee that $V_q' = \mathcal{V}_{R,K}^{(k)}\big(q; (a_i)_{i=1}^K\big) = \mathcal{V}_{R,K-1}^{(k)}\big(q; (a_i)_{i=1}^{K-1}\big)$, with the set $\mathcal{V}_{R,K-1}^{(k)}\big(q; (a_i)_{i=1}^{K-1}\big)$ defined by the congruences $\prod_{j=1}^R W_{i,k}(v_j) \equiv a_i \pmod q$, $i \in [K-1]$.

Define $D_1 := \sum_{i=1}^{K-1} \deg W_{i,k} > 1$ and let "C" in the statement of the theorem be any constant $C^* := C^*(W_{1,k}, \cdots, W_{K-1,k})$ exceeding $(32D_1)^{2D_1+2}$, the sizes of the leading and constant coefficients of $\{W_{i,k}\}_{i=1}^K$, and the constant $C_1^* := C_1(W_{1,k}, \dots, W_{K-1,k})$ coming from an application of Proposition 3.9 to the family $\{W_{i,k}\}_{i=1}^{K-1}$ of nonconstant multiplicatively independent polynomials. To show the lower bound in Theorem 2.4, we may assume that $R > 4KD_1(D_1+1)$. We shall carry out some of the arguments of Proposition 5.1; note that $\alpha_k(q) = \frac{1}{\varphi(q)} \#\{u \in U_q : \prod_{i=1}^{K-1} W_{i,k}(u) \in U_q\} \ne 0$. For each prime $\ell \mid q$, we have $\gcd(\ell - 1, \beta(W_{1,k}, \cdots, W_{K-1,k})) = 1$ and $\ell > C^* > C_1^*$. Thus the hypothesis $IFH(W_{1,k}, \dots, W_{K-1,k}; 1)$ holds true, and so do the corresponding analogues of the inequalities (5.9) and (5.10); in fact by the second assertion in Proposition 3.9(a), the analogue of (5.9) holds true for all tuples of characters $(\chi_1, \dots, \chi_{K-1}) \ne (\chi_{0,\ell}, \dots, \chi_{0,\ell}) \bmod \ell^e$ having $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_{K-1})] = \ell$. We find that

$$\begin{aligned} \frac{1}{\big(\alpha_k(\ell)\varphi(\ell^e)\big)^R} \sum_{(\chi_1, \dots, \chi_{K-1}) \ne (\chi_{0,\ell}, \dots, \chi_{0,\ell}) \bmod \ell^e} \big|Z_{\ell^e;\ \chi_1, \dots, \chi_{K-1}}(W_{1,k}, \dots, W_{K-1,k})\big|^R \\ \le \frac{D_1^R \ell^{eR}}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{1 \le e_0 \le e} \ell^{e_0(K - R/D_1)} \ \le\ \frac{2(4D_1)^R}{\ell^{R/D_1 - K}}, \end{aligned} \tag{7.3}$$

where as usual $Z_{\ell^e;\ \chi_1, \dots, \chi_{K-1}}(W_{1,k}, \dots, W_{K-1,k}) = \sum_{u \bmod \ell^e} \chi_{0,\ell}(u) \prod_{i=1}^{K-1} \chi_i(W_{i,k}(u))$. Now since $R \ge 4KD_1(D_1+1)$ and $\ell > C^* > (32D_1)^{2D_1+2}$, we see that $\ell^{R/D_1 - K} \ge \ell^{R/(D_1+1)} \ge \ell^{R/(2D_1+2)} \cdot (C^*)^{R/(2D_1+2)} \ge \ell^2 (32D_1)^R$, showing that the right hand expression in (7.3) is at most $1/4\ell^2$. Invoking the corresponding analogue of (5.3), we see for each prime power $\ell^e \parallel q$ that $\#\mathcal{V}_{R,K-1}^{(k)}(\ell^e; (a_i)_{i=1}^{K-1})/\varphi(\ell^e)^R \ \ge\ (\alpha_k(\ell)^R/\varphi(\ell^e)^{K-1}) \cdot (1 - 1/2\ell^2)$. But since $\prod_{\ell \mid q}(1 - 1/2\ell^2) \ge 1 - \frac{1}{2}\sum_{\ell \ge 2} 1/\ell^2 \ge 1/2$, we obtain $V_q'/\varphi(q)^R = \mathcal{V}_{R,K-1}^{(k)}\big(q; (a_i)_{i=1}^{K-1}\big)/\varphi(q)^R \ge \alpha_k(q)^R/2\varphi(q)^{K-1}$, which holds true uniformly in q having $P^-(q) > C^*$. Inserting this bound into (7.2) and recalling that $\alpha_k(q) \gg 1/(\log_2(3q))^D$, we are done. □

Completing the proof of Theorem 2.5. Again, it suffices to consider the case $R > 18KD(D+1)$ to prove (2.4). We start by choosing "C" in the statement of the theorem to be a constant $C_2 := C_2(W_{1,k}, \dots, W_{K,k})$ exceeding $(32D)^{6D+6}$, the sizes of the leading and constant coefficients of $\{W_{i,k}\}_{i=1}^K$, and the constant $C_1(W_{1,k}, \dots, W_{K,k})$ obtained by applying Proposition 3.9 to the family $\{W_{i,k}\}_{1 \le i \le K}$ of multiplicatively independent polynomials. The analogue of (5.10) continues to hold for each $\ell \mid q$, and thus

$$\begin{aligned}(7.4)\quad & \frac{1}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{\substack{(\chi_1,\dots,\chi_K) \bmod \ell^e \\ \operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)] \in \{\ell^2,\dots,\ell^e\}}} |Z_{\ell^e;\, \chi_1,\dots,\chi_K}(W_{1,k}, \dots, W_{K,k})|^R \\ & \le \frac{D^R \ell^{eR}}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{2 \le e_0 \le e} \ell^{e_0(K-R/D)} \le \frac{2(4D)^R}{\ell^{R/D-K}} \le \frac{1}{4\ell^2},\end{aligned}$$

where in the last inequality, we have recalled that $R > 4KD(D+1)$ and $\ell > C_2 \ge (32D)^{6D+6}$.

If $(\chi_1, \dots, \chi_K)$ is a tuple of characters mod ℓ^e having $\operatorname{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell$, then with ψ_ℓ being a generator of the character group mod ℓ, we have $\chi_i = \psi_\ell^{A_i}$ for some unique $(A_1, \dots, A_K) \in [\ell-1]^K$ satisfying $(A_1, \dots, A_K) \not\equiv (0, \dots, 0) \pmod{\ell-1}$. Recall from the arguments leading to (5.9) that if $\prod_{i=1}^K W_{i,k}^{A_i}$ is *not* of the form $c \cdot G^{\ell-1}$ in $\mathbb{F}_\ell[T]$, then $|Z_{\ell^e;\, \chi_1,\dots,\chi_K}(W_{1,k}, \dots, W_{K,k})| \le D\ell^{e-1/2}$. On the other hand, if $\prod_{i=1}^K W_{i,k}^{A_i}$ *is* of that form (with G monic, say), then since each $W_{i,k}$ is monic, we must have $\prod_{i=1}^K W_{i,k}^{A_i} = G^{\ell-1}$. Since $G(v)$ is a unit mod ℓ iff $\prod_{i=1}^K W_{i,k}(v)$ is, it follows that $Z_{\ell^e;\, \chi_1,\dots,\chi_K}(W_{1,k}, \dots, W_{K,k}) = \ell^{e-1} \sum_{v \bmod \ell} \psi_\ell\left((vG(v))^{\ell-1}\right) = \alpha_k(\ell)\varphi(\ell^e)$. Combining these observations with (7.4) and using that $\prod_{i=1}^K \overline{\chi}_i(a_i) = 1$ for any characters $(\chi_1, \dots, \chi_K)$ mod ℓ^e with $\operatorname{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = \ell$ (as $a_i \equiv 1 \bmod \ell$), we get

$$(7.5)\qquad \frac{\#\mathcal{V}_{R,K}^{(k)}\left(\ell^e; (a_i)_{i=1}^K\right)}{\varphi(\ell^e)^R} \ge \frac{\alpha_k(\ell)^R}{\varphi(\ell^e)^K}\left(1 + \mathcal{B}_\ell - \frac{1}{2\ell^2}\right),$$

where $\mathcal{B}_\ell$ denotes the number of tuples $(A_1, \dots, A_K) \in [\ell-1]^K \setminus \{(0, \dots, 0)\}$ for which $\prod_{i=1}^K W_{i,k}^{A_i}$ is a perfect $(\ell-1)$-th power in $\mathbb{F}_\ell[T]$.

Now recalling the definition of the constant $C_1 = C_1(W_{1,k}, \dots, W_{K,k})$ from the proof of Proposition 3.9, we know that for any $\ell > C_1$, the pairwise coprime irreducible factors of the product $\prod_{i=1}^K W_{i,k}$ in $\mathbb{Z}[T]$ continue to be separable and pairwise coprime in the ring $\mathbb{F}_\ell[T]$. By the arguments given in the proof of Proposition 3.9(a) (see [48]), $\prod_{i=1}^K W_{i,k}^{A_i}$ is a perfect $(\ell-1)$-th power in $\mathbb{F}_\ell[T]$ precisely when $E_0(A_1 \cdots A_K)^\top \equiv (0 \cdots\cdots 0)^\top \pmod{\ell-1}$, where $E_0 = E_0(W_{1,k}, \dots, W_{K,k})$ is the exponent matrix. Thus, $\mathcal{B}_\ell$ is exactly the number of nonzero vectors $X \in (\mathbb{Z}/(\ell-1)\mathbb{Z})^K$ satisfying the matrix equality $E_0X = 0$ over the ring $\mathbb{Z}/(\ell-1)\mathbb{Z}$.

Recall that E_0 has $\mathbb{Q}$-linearly independent columns and non-zero last invariant factor $\beta = \beta(W_{1,k}, \dots, W_{K,k}) \in \mathbb{Z}$. By [34, Theorem 6.4.17], the matrix equation $E_0X = 0$ has a nontrivial solution in the ring $\mathbb{Z}/(\ell-1)\mathbb{Z}$ precisely when some nonzero element of $\mathbb{Z}/(\ell-1)\mathbb{Z}$ annihilates all the $K \times K$ minors of the matrix E_0. But if $\gcd(\ell-1, \beta) \ne 1$, then the canonical image of $d := (\ell-1)/\gcd(\ell-1, \beta)$ in $\mathbb{Z}/(\ell-1)\mathbb{Z}$ clearly does this, since $d\beta \equiv 0$

$\pmod{\ell-1}$ and since β divides the gcd of the $K \times K$ minors of E_0 (in $\mathbb{Z}$). We thus obtain $\mathcal{B}_\ell \geq 1$ for each prime prime $\ell \mid q$ satisfying $\gcd(\ell-1,\beta) \neq 1$, which from (7.5) yields $V_q'/\varphi(q)^R \geq \ 2^{\#\{\ell|q:\ (\ell-1,\beta)\neq 1\}}\alpha_k(q)^R/2\varphi(q)^K$. Inserting this into (7.2) establishes (2.4). □

Remark: If $K = 1$ and $W_{1,k}$ is a constant c, then the k-admissibility of q forces $\gcd(q,c) = 1$, which by (7.2) gives $\#\{n \leq x : P_R(n_k) > q, f(n) \equiv c^R \pmod q\} \gg x^{1/k}(\log_2 x)^{R-1}/\log x$.

7.1. **Explicit Examples.** We now construct examples where the lower bounds in Theorems 2.4 and 2.5 grow strictly faster than the expected quantity $\varphi(q)^{-K}\#\{n \leq x : (f(n), q) = 1\}$.

Failure of joint weak equidistribution upon violation of multiplicative independence hypothesis (example for Theorem 2.4). By Proposition 3.1, it is clear that the lower bound in Theorem 2.4 grows strictly faster once q grows fast enough compared to $\log x$. For a concrete example, we start with any $\{W_{i,k}\}_{1\leq i\leq K-1} \subset \mathbb{Z}[T]$ for which $\beta^* = \beta(W_{1,k}, \ldots, W_{K-1,k})$ is odd (for instance, $W_{i,k} \coloneqq H_i^{b_i}$ for some pairwise coprime irreducibles $H_1, \ldots, H_{K-1} \in \mathbb{Z}[T]$ and odd integers $b_i > 1$ satisfying $b_i \mid b_{i+1}$ for each $i < K-1$). Fix nonnegative integers $(\lambda_i)_{i=1}^{K-1} \neq (0, \ldots, 0)$ and nonzero integers $(a_i)_{i=1}^{K}$ satisfying $a_K = \prod_{i-1}^{K-1} a_i^{\lambda_i}$ (in $\mathbb{Z}$), and let $W_{K,k} = \prod_{i=1}^{K-1} W_{i,k}^{\lambda_i}$. Consider a constant $\widetilde{C} > \max\{C^*, \prod_{i=1}^{K} |a_i|\}$, such that any $\widetilde{C}$-rough k-admissible integer lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$. Here C^* as in the proof of Theorem 2.4, so that $\widetilde{C} > D_1 + 1 = \sum_{i=1}^{K-1} \deg W_{i,k} + 1$. Let ℓ_0 be the least prime exceeding $\widetilde{C}$ and satisfying $\ell_0 \equiv -1 \bmod \beta^*$. [6] Let $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v\leq k-1}} \subset \mathbb{Z}[T]$ be nonconstant polynomials with all coefficients divisible by ℓ_0, and let $q \coloneqq \prod_{\substack{\ell_0\leq \ell\leq Y\\ \ell\equiv -1 \pmod{\beta^*}}} \ell$, with Y any parameter lying in $(4|\beta^*|\log_2 x, (K_0/2)\log_2 x)$. Since $\alpha_k(\ell) \geq 1 - D_1/(\ell-1) > 0$ for $\ell > \widetilde{C}$, we see that $q \leq (\log x)^{K_0}$ is k-admissible and hence lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$. As β^* is odd and $\ell \equiv -1 \pmod{\beta^*}$ for all $\ell \mid q$, we have $\gcd(\ell-1, \beta^*) = 1$ for all such ℓ. Further, $q = \exp\left(\sum_{\substack{\ell_0\leq \ell\leq Y\\ \ell\equiv -1 \pmod{\beta^*}}} \log \ell\right) \geq \exp\left(Y/2|\beta^*|\right) \ \geq\ \log^2 x$, so the lower bound in Theorem 2.4 grows strictly faster than $\varphi(q)^{-K}\#\{n \leq x : (f(n), q) = 1\}$.

Failure of joint weak equidistribution upon violation of Invariant Factor Hypothesis (example for Theorem 2.5). Define $W_{i,k}(T) \coloneqq T - i$ for each $i \in [K-1]$ and $W_{K,k}(T) \coloneqq (T-K)^d$, for some fixed $d \in \{2, \ldots, K\}$. Then $\{W_{i,k}\}_{1\leq i\leq K}$ are nonconstant, monic and pairwise coprime (hence multiplicatively independent); also $E_0(W_{1,k}, \ldots, W_{K,k}) = \operatorname{diag}(1, \ldots, 1, d)$ so $\beta \coloneqq \beta(W_{1,k}, \ldots, W_{K,k}) = d$. Note that $\alpha_k(\ell) = 1 - K/(\ell-1) > 0$ for any prime $\ell > K+1$. Let $C_3 \coloneqq C_3(W_{1,k}, \ldots, W_{K,k})$ be a constant exceeding the constant C_2 in the proof of Theorem 2.5, such that any k-admissible C_3-rough integer lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$; note that $C_3 > D + 1 \geq K + 2$. Let ℓ_0 be the least prime exceeding C_3 and satisfying $\ell_0 \equiv 1 \pmod d$, let $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v<k}} \subset \mathbb{Z}[T]$ be nonconstant polynomials all of whose coefficients are divisible by ℓ_0, and let $q \coloneqq \prod_{\substack{\ell_0\leq \ell\leq Y\\ \ell\equiv 1 \pmod d}} \ell$, with $Y \leq (K_0/2)\log_2 x$ a parameter to be chosen later.

Then $q \leq (\log x)^{K_0}$, $P^-(q) > C_3$ and $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$. By Theorem 2.5 and Proposition 3.1, it follows that the residues $a_i \equiv 1 \pmod q$ are overrepresented if $\#\{\ell \mid q :\ (\ell-1, \beta) \neq 1\} \geq 4\alpha_k \log_2 x$. But $\#\{\ell \mid q :\ (\ell-1,\beta) \neq 1\} = \sum_{\substack{\ell_0\leq \ell\leq Y\\ \ell\equiv 1 \pmod d}} 1 \geq Y/2\varphi(d)\log Y$, whereas

[6] Our arguments go through with the residue $-1 \bmod \beta^*$ replaced by any $c^* \in U_{\beta^*}$ for which $c^* - 1 \in U_{\beta^*}$.

(since $K \geq \varphi(d)$), we have $\alpha_k \leq K_3/\log Y$ for some constant $K_3 > 0$ depending at most on C_3, K and d. So we only need Y to satisfy $8K_3\varphi(d)\log_2 x < Y < (K_0/2)\log_2 x$.

Therefore, our multiplicative independence and invariant factor hypotheses are both necessary for achieving uniformity in $q \leq (\log x)^{K_0}$ in Theorems 2.1 to 2.3, and neither of them can be bypassed by restricting to inputs n with sufficiently many large prime factors.

Acknowledgements

This work was done in partial fulfillment of my PhD at the University of Georgia. As such, I would like to thank my advisor, Prof. Paul Pollack, for the past joint research and fruitful discussions that have led me to think about this question, as well as for his continued support and encouragement. I would also like to thank the Department of Mathematics at UGA for their support and hospitality.

Data Availability The manuscript has no associated data.

Declarations

Conflict of Interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

References

[1] A. Akande, *Uniform distribution of polynomially-defined additive functions to varying moduli*, submitted.
[2] K. Alladi, *The distribution of $\nu(n)$ in the sieve of Eratosthenes*, Quart. J. Math. Oxford Ser. (2) **33** (1982), no. 130, 129–148.
[3] K. Alladi and P. Erdös, *On an additive arithmetic function*, Pacific J. Math. **71** (1977), no. 2, 275–294.
[4] M.F. Atiyah, and L.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, 1969.
[5] W. Bruns, and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1998.
[6] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith. **101** (2002), 131–149.
[7] T. Cochrane, C.L. Liu, and Z.Y. Zheng, *Upper bounds on character sums with rational function entries*, Acta Math. Sin. (Engl. Ser.) **19**(2003), 327–338.
[8] T. Cochrane and Z. Zheng., *Pure and mixed exponential sums.*, Acta Arith. **91** (1999), 249–278.
[9] H. Davenport, *On character sums in finite fields*, Acta Math. **71** (1939), 99–121.
[10] H. Delange, *On integral-valued additive functions*, J. Number Theory **1** (1969), 419–430.
[11] ———, *On integral-valued additive functions, II*, J. Number Theory **6** (1974), 161–170.
[12] T. Dence and C. Pomerance, *Euler's function in residue classes*, Ramanujan J. **2**(1998), 7–20.
[13] Z. Dvir, J. Kollár, and S. Lovett, *Variety Evasive Sets*, Comput. Complexity **23** (2014), 509–529, ISSN 1016-3328.
[14] P. Erdös and G. Szekeres, *Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisces Problem*, Acta Univ. Szeged, vol. **7** (1934-1935), pp. 95–102.
[15] O.M. Fomenko, *The distribution of values of multiplicative functions with respect to a prime modulus*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI), **93**, 1980, pp. 218-224. (Russian)
[16] D. Goldfeld, *On an additive prime divisor function of Alladi and Erdős*, Analytic number theory, modular forms and q-hypergeometric series, Springer Proc. Math. Stat., vol. 221, Springer, Cham, 2017, pp. 297–309.
[17] G. Halász, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hungar., **19** (1968), 365–403
[18] R.R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.

[19] S. Konyagin, *Letter to the editors: "The number of solutions of congruences of the nth degree with one unknown"*, Mat. Sb. (N.S.) **110(152)** (1979), 158.

[20] ———, *The number of solutions of congruences of the nth degree with one unknown*, Mat. Sb. (N.S.) **109(151)** (1979), 171–187, 327.

[21] E. Landau, *Lösung des Lehmer'schen Problems*, American J. Math. **31** (1909), 86–102.

[22] S. Lang, and A. Weil. *Number of Points of Varieties in Finite Fields.*, American J. Math. **76**, no. 4 (1954), 819–827.

[23] N. Lebowitz-Lockard, P. Pollack, and A. Singha Roy, *Distribution mod p of Euler's totient and the sum of proper divisors*, Michigan Math. J., to appear.

[24] D.B. Leep and C.C. Yeomans, *The number of points on a singular curve over a finite field*, Arch. Math. (Basel) **63** (1994), 420–426.

[25] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 2006.

[26] H.L. Montgomery and R.C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[27] W. Narkiewicz, *On distribution of values of multiplicative functions in residue classes*, Acta Arith. **12** (1967), 269–279.

[28] ———, *Euler's function and the sum of divisors*, J. reine angew. Math. **323** (1981), 200–212.

[29] ———, *On a kind of uniform distribution for systems of multiplicative functions*, Litovsk. Mat. Sb. **22** (1982), 127–137.

[30] ———, *Distribution of coefficients of Eisenstein series in residue classes*, Acta Arith. **43** (1983), 83–92.

[31] ———, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Mathematics, vol. 1087, Springer-Verlag, Berlin, 1984.

[32] W. Narkiewicz and F. Rayner, *Distribution of Values of $\sigma_2(n)$ in Residue Classes*, Monatsh. Math. **94** (1982), 133–141.

[33] K.K. Norton, *On the number of restricted prime factors of an integer. I*, Illinois J. Math. **20** (1976), 681–705.

[34] S.E. Payne, *A Second Semester of Linear Algebra*, University of Colorado Denver, 2009.

[35] S.S. Pillai, *Generalisation of a theorem of Mangoldt*, Proc. Indian Acad. Sci., Sect. A **11** (1940), 13–20.

[36] P. Pollack and A. Singha Roy, *Joint distribution in residue classes of polynomial-like multiplicative functions*, Acta Arith. **202** (2022), 89–104.

[37] ———, *Benford behavior and distribution in residue classes of large prime factors*, Canad. Math. Bull., **66** (2023), no. 2, 626–642.

[38] ———, *Distribution in coprime residue classes of polynomially-defined multiplicative functions*, Math. Z. **303** (2023), no. 4, Paper No. 93, 20. MR 4565094.

[39] C. Pomerance, *On the distribution of amicable numbers*, J. Reine Angew. Math. **293(294)** (1977), 217–222.

[40] F. Rayner, *Weak Uniform Distribution for Divisor Functions. I*, Math. Comp. **50** (1988), 335–342.

[41] ———, *Weak Uniform Distribution for Divisor Functions. II*, Math. Comp. **51** (1988), 331–337.

[42] W.M. Schmidt, *Equations over finite fields*, Lecture Notes in Mathematics, vol. 536, Springer-Verlag Berlin Heidelberg 1976.

[43] W. Schwarz and J. Spilker, *Arithmetical functions*, London Mathematical Society Lecture Note Series, vol. 184, Cambridge University Press, Cambridge, 1994, An introduction to elementary and analytic properties of arithmetic functions and to some of their almost-periodic properties.

[44] E.J. Scourfield, *Uniform estimates for certain multiplicative properties*, Monatsh. Math. **97** (1984), 233–247.

[45] ———, *A uniform coprimality result for some arithmetic functions*, J. Number Theory **20** (1985), 315–353

[46] A. Singha Roy, *Joint distribution in residue classes of families of polynomially-defined additive functions*, submitted.

[47] ———, *Mean values of multiplicative functions and applications to the distribution of the sum of divisors*, submitted.

[48] ———, *Joint distribution in reisude classes of families of polynomially-defined multiplicative functions I*, submitted.

[49] J. Śliwa, *On distribution of values of $\sigma(n)$ in residue classes*, Colloq. Math. **27** (1973), 283-291, 332.

[50] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, third ed., Graduate Studies in Mathematics, vol. 163, American Mathematical Society, Providence, RI, 2015.

[51] D. Wan, *Generators and irreducible polynomials over finite fields*, Math. Comp. **66** (1997), no. 219, 1195–1212.

[52] A. Weil, *Sur les courbes algébriques et les variétes qui s'en déduisent*, Actual. Sci. Industr. **1041** (1948).

Department of Mathematics, University of Georgia, Athens, GA 30602

Email address: akash01s.roy@gmail.com