RESIDUE-CLASS DISTRIBUTION OF ARITHMETIC FUNCTIONS TO VARYING MODULI

by

AKASH SINGHA ROY

(Under the Direction of Paul Pollack)

ABSTRACT

The distribution of values of arithmetic functions in residue classes is a problem of significant interest in elementary, analytic and combinatorial number theory. Much work has been done studying this problem for fixed moduli. In this thesis, we extend many of the results in the literature for large classes of additive and multiplicative functions, so as to allow the modulus to vary within a wide range. In fact, we find essentially best possible analogues of the Siegel-Walfisz theorem (from prime number theory) for the joint distribution of families of such functions.

Our primary tools are sieve methods and methods from the "anatomy of integers", which we often use to detect certain "mixing" phenomena in multiplicative groups. Additionally, we use several ideas and machinery from classical analytic number theory, character sums, linear algebra over rings, as well as tools from arithmetic and algebraic geometry.

INDEX WORDS: Equidistribution, uniform distribution, weak uniform distribution, weak equidistribution, joint distribution, arithmetic functions, residue class, additive functions, multiplicative functions, Siegel-Walfisz.

RESIDUE-CLASS DISTRIBUTION OF ARITHMETIC FUNCTIONS TO VARYING MODULI

by

AKASH SINGHA ROY

B.SC. HONOURS IN MATHEMATICS AND COMPUTER SCIENCE,

Chennai Mathematical Institute, India, 2021

A Dissertation Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

ATHENS, GEORGIA

2025

RESIDUE-CLASS DISTRIBUTION OF ARITHMETIC FUNCTIONS TO VARYING MODULI

by

AKASH SINGHA ROY

Major Professor: Paul Pollack

Committee: Neil Lyall
Akos Magyar
Giorgis Petridis

Electronic Version Approved:

Ron Walcott
Vice Provost for Graduate Education and Dean of the Graduate School
The University of Georgia
August 2025

To my mother

and

to the memory of my grandparents.

Acknowledgements

One section is not nearly enough space to adequately thank those without whom I would not be where I am today, however I will make an attempt. First and foremost, I would like to thank the Almighty for showing me the way and for protecting my family during some extremely difficult times. I am thankful to my biggest supporter, my mother, who despite living on the other side of the planet, has been an endless source of positivity and emotional support that helped me overcome several obstacles. I am grateful to my step-father for coming into our lives, and for being a strong pillar of support for my mother, especially when I had to leave home to pursue my studies.

From the academic side, I would first of all, like to thank my advisor Paul Pollack. I met Paul as a Counselor in the Ross/Asia Mathematics Program 2019: Our correspondence began on a bus ride from Nanjing to Zhenjiang during the program, and three years later, I would go on to become his PhD student here at UGA. I am truly indebted to him, not only for the numerous fruitful discussions and his immense wisdom (both in mathematics and outside), but also for his optimism, kindness and encouragement, and most importantly, for believing in me when I myself didn't.

My committee members, Neil Lyall, Akos Magyar and Giorgis Petridis, have all been extremely helpful, supportive and understanding during my journey. When I enrolled at UGA in Fall 2022, Neil was starting as Department Head in the Mathematics De-

partment, and I still remember how helpful he was when I was stuck with immigration processes. I feel truly privileged to have gotten the opportunity to take Ergodic Theory and Circle Methods with Akos, as well as Additive Combinatorics and Ramsey Theory with Giorgis: I have truly enjoyed and learnt a lot from all these classes, and they have made me really excited to expand my research into new directions. And of course, I would like to thank my committee members for reading through this manuscript and providing valuable feedback.

The number theory group at UGA has been tremendously supportive towards me. I am grateful to Pete for giving me the opportunity to speak at the Number Theory Seminar. I would also take this opportunity to thank Dino Lorenzini for teaching me Elliptic Curves and for some fruitful discussions related to my research, as well as to Jiuya Wang for teaching Arithmetic Statistics and for new exciting research projects. A special shout-out to Fai Chandee, Xiannan Li, Noah Lebowitz–Lockard and Nathan McNew: It has been amazing collaborating with all of you.

This section would be severely incomplete without mentioning the Ross Mathematics Program, which I had the privilege of attending for three successive years (2017, '18 and '19): It is here that I got to develop my passion for number theory as a subject to pursue research in, and it is through this program that I came to know my advisor as well. Special thanks go to Timothy All, Jim Fowler and Daniel Shapiro, as well as my Counselor Tristan Phillips, for making the program such a welcoming, friendly and memorable experience. And I certainly cannot forget some of the wonderful mentors, teachers (in mathematics and outside) and Professors that I have had the privilege of being taught by during my high school and undergraduate years: Ashani Dasgupta, Pallab Das, Pramit Das, Chirantan Chowdhury, Sujoy Chakraborty, Kashinath Adhya, Upendra Kulkarni, Purusottam Rath, Sinnou David, Sanoli Gun, Krishna Hanu-

manthu, Clare D'Cruz and K.V. Subrahmanyam.

I would also like to express my sincere appreciation to several other people in the department whose presence made UGA such a homely environment: David Gay for his compassionate mentorship as graduate coordinator and for nominating me for multiple grants and awards; Enka Lakuriqi, Jimmy Dillies and Tekin Karadag for their concern for my well-being and their support with all things related to teaching; Mike Usher and Jingzhi Tie for their accommodations in teaching assignments; Bill Graham and Laura Rider for helping me adjust as an incoming student; Lucy Barrera, Christy McDonald and Rinakia Jones for their help with all kinds of paperwork and (especially) for their patience when I panicked about these; my peer mentors Paco Adajar and Peter Woolfitt who went out of their way to make me feel welcome as an incoming student. And a shout-out to my friends and colleagues in UGA for all their help, the memorable conversations, and the mathematical, professional, administrative, philosophical, intellectual and non–intellectual, and occasionally outright unhinged discussions: Arghadeep Basu (from the statistics department), Paco Adajar, Peter Woolfitt, Swaroop Hegde, Josh Stucky, Steve Fan, Patrick Akande, Rishika Agrawal, Sreerupa Bhattacharjee, Michaela Coleman, Raemeon Cowan, Gary Dunkerley, Zack Garza, Matt Hamil, Jie Ji, Matt Just, Dustin Kasser, Gabe Loos, Andrew Lott, Han Lou, Krishnamohan Nandakumar, Nagendar (Reddy) Ponagandla, and Ye Tian. Special mention to Paco, not only for being an amazing office-mate, roommate, peer mentor and academic brother, but also for showing me the art of making puns that can have a mixed bag of extreme effects in listeners.

Last but not the least, I would like to thank William Banks, Régis de la Bretèche, Caroline Turnage–Butterbaugh, Karl Dilcher, Kevin Ford, Michael Filaseta, Larry Guth, Tsz Ho Chan, Jeffrey Lagarias, Robert Lemke-Oliver, Florian Luca, Yu-Ru

Liu, Amita Malik, Carl Pomerance, Yuta Suzuki, Lola Thompson, Enrique Trevino, Ognian Trifonov, Lee Troupe, Asif Zaman and Tamar Ziegler for their helpful advise as well as their interest in my work.

Contents

Acknowledgements v

List of Tables xiii

List of Figures xiv

1 Introduction **1**

1.1 Uniform distribution in residue classes 2

1.2 Equidistribution of additive functions in residue classes: Fixed moduli 5

1.3 Equidistribution of multiplicative functions in residue classes: Fixed moduli 9

1.3.1 The correct notion of "equidistribution" 9

1.3.2 Building up towards the general criterion: Weak equidistribution of the Euler totient 13

1.3.3 Narkiewicz's criteria for weak equidistribution and applications 18

1.4 Allowing the modulus to vary... 27

1.4.1 Equidistribution to varying moduli: Siegel–Walfisz for polynomially–defined additive functions 29

1.4.2 Equidistribution to varying moduli: Siegel–Walfisz for polynomially–defined multiplicative functions 32

1.5 Summary of later chapters 38

1.5.1 Notation and conventions 40

2 Weak equidistribution of a single function to a varying "rough" modulus: The mixing phenomenon 42

2.1 Main results of this chapter 43

2.2 A preparatory estimate: The frequency with which $(f(n), q) = 1$ . . . 48

2.3 Framework for the proof of Theorems 2.1.2 and 2.1.3 52

2.4 Linearly defined functions: Proof of Theorem 2.1.1 58

2.5 General polynomially defined functions: Proof of Theorem 2.1.2 . . . 62

2.6 Equidistribution along inputs with several prime factors exceeding q: Proof of Theorem 2.1.3 65

2.7 Concluding remarks and further questions 69

3 Joint distribution in residue classes of families of polynomially-defined additive functions 74

3.1 Main results 75

3.2 Preliminary Discussion: Delange's equidistribution criteria and consequences for polynomially-defined additive functions 80

3.3 Preparation for Theorems 3.1.1, 3.1.2 and 3.1.3: Obtaining the main term 85

3.4 Joint equidistribution without input restriction: Proof of Theorem 3.1.1 103

3.4.1 Optimality of range of q in Theorem 3.1.1 105

3.5 Complete uniformity for general moduli: Proof of Theorem 3.1.2 . . . 106

3.6 Complete uniformity in squarefree moduli: Proof of Theorem 3.1.3 . . 114

3.6.1 Optimality in the input restrictions in Theorem 3.1.3: 121

3.7 Necessity of the linear independence hypothesis: Proof of Theorem 3.1.4 124

4 Joint distribution in residue classes of families of polynomially-defined

multiplicative functions **128**

4.1 Main results 129

4.1.1 Multiplicative independence and the Invariant Factor Hypothesis 129

4.1.2 Set-up for the main results in this chapter 131

4.1.3 The Main Results 132

4.1.4 Necessity of the multiplicative independence and invariant factor hypotheses 135

4.1.5 Some more concrete applications of our main results 137

4.1.6 Summary of the main ideas 139

4.2 Technical preparation: The number of $n \leq x$ for which $\gcd(f(n), q) = 1$ 140

4.2.1 Proof of the lower bound. 141

4.2.2 Proof of the upper bound. 141

4.3 The main term in Theorems 4.1.1 to 4.1.3: Contribution of "convenient" n 146

4.4 Counting solutions to congruences: Proof of Proposition 4.3.4 155

4.4.1 Preparation for the proof of Proposition 4.3.4 155

4.4.2 Proof of Proposition 4.3.4 162

4.5 Proof of Theorem 4.4.5 for nontrivial tuples of characters not in $\mathcal{C}_k(Q_0)$ 173

4.6 Proof of Theorem 4.4.5 for tuples of characters in $\mathcal{C}_k(Q_0)$ 178

4.6.1 Analysis of the Dirichlet series. 179

4.6.2 Preparing for the contour shift: Auxiliary functions and intermediate bounds 185

4.6.3 Perron's formula and the contour shifts 191

4.7 Equidistribution to restricted moduli: Proof of Theorem 4.1.1 202

4.7.1 Optimality in the ranges of q in Theorem 4.1.1. 203

4.8 Restricted inputs to general moduli: Proof of Theorem 4.1.2 207

4.9 Final preparatory step for Theorem 4.1.3: Counting points on varieties 214
4.10 Restricted inputs to squarefree moduli: Proof of Theorem 4.1.3 220
4.10.1 Optimality of the conditions of Theorem 4.1.3 224
4.11 Necessity of the multiplicative independence and invariant factor hypotheses: Proofs of Theorems 4.1.4 and 4.1.5 226
4.11.1 Explicit Examples. 231
4.12 Concluding Remarks 233

5 Distribution of the aliquot sum function to varying prime moduli 236
5.1 Technical Preparation 237
5.2 Contribution of the convenient n 241
5.3 Bounding the contribution of inconvenient n 245
5.4 Concluding remarks 248

References 249

List of Tables

Table 1: Explicit numerical distributions of $\varphi(n)$ mod 5 ..... pg. 16

List of Figures

Figure 1: Case 1: $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$ and there is a Siegel zero β_e mod Q. pg. 195

Figure 2: Case 2: $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$ and there is no Siegel zero mod Q. pg. 195

Figure 3: Case 3: $(\alpha_k(Q), c_{\widehat{\chi}}) = (1,1)$ and there is a Siegel zero β_e mod Q. pg. 196

Chapter 1

Introduction

The distribution of values of arithmetic functions in residue classes has drawn a lot of attention in elementary, analytic and combinatorial number theory, with multiple authors such as Delange, Narkiewicz, Dence and Pomerance, Banks and Shparlinski, Śliwa, Rayner, Dobrowolski, Fomenko, and others studying such value distributions for *fixed* moduli. In this dissertation, we extend several of their works and study the distribution of arithmetic functions in residue classes to moduli that are allowed to *vary* within a wide range. This study is motivated by the celebrated Siegel–Walfisz theorem on the distribution of primes in progressions, and we obtain essentially best possible analogues of the Siegel–Walfisz theorem for large classes of additive and multiplicative functions.

In this introductory chapter, we recount some of the relevant past work done on this subject, motivate the problems studied here, and summarize the contents of this dissertation.

Section 1.1

Uniform distribution in residue classes

Let f be an integer valued arithmetic function and q be a positive integer. We say that f is uniformly distributed or equidistributed modulo q if

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

for each residue class a mod q. In shorthand, we will say that f is UD mod q. This notion was introduced by Niven in [53].

For instance, the function $f(n) = n$ is easily seen to be equidistributed modulo any $q \in \mathbb{N}$. A somewhat less trivial example is the function $f(n)$ that maps n to the n-th Fibonacci number, which is known to be equidistributed modulo q precisely when q is a power of 5 (see [52, 37]).

Using the additive characters mod q, we can decide whether an arithmetic function f is equidistributed mod q. In what follows, we use $e(t)$ to denote $e^{2\pi i t}$.

Lemma 1.1.1. *Consider any arithmetic function $f : \mathbb{N} \to \mathbb{Z}$ and a fixed positive integer q. Then f is UD mod q if and only if for every nonzero residue class r mod q, we have*

$$\sum_{n \le x} e\left(\frac{rf(n)}{q}\right) = o(x) \quad \text{as} \quad x \to \infty.$$

Proof. Assume that f is UD mod q. Then for any residue class a mod q, we have $\#\{n \le x : f(n) \equiv a \pmod q\} = (1 + o(1))x/q$ as $x \to \infty$. As such, for any residue

class $r \bmod q$, we have

$$\begin{aligned}\sum_{n\le x} e\left(\frac{rf(n)}{q}\right) &= \sum_{a \bmod q} e\left(\frac{ra}{q}\right) \sum_{\substack{n\le x \\ f(n)\equiv a \pmod q}} 1 \\ &= \left(\frac{1}{q}\sum_{a \bmod q} e\left(\frac{ra}{q}\right) + o(1)\right) x.\end{aligned}$$

as $x \to \infty$. Now if $r \not\equiv 0 \pmod q$, then $\sum_{a \bmod q} e(ra/q)$ vanishes, proving the forward implication.

For the reverse implication, we use the last observation to detect the condition $f(n) \equiv a \pmod q$. (In other words, we use the "orthogonality relations" of additive characters.) Indeed, using $\mathbb{1}_{\mathcal{P}}$ to denote the indicator function of a property $\mathcal{P}$, we see that for any residue class $a \bmod q$, we have

$$\begin{aligned}\#\{n \le x : f(n) \equiv a \pmod q\} &= \sum_{n\le x} \mathbb{1}_{f(n)-a\equiv 0 \pmod q} \\ &= \sum_{n\le x} \frac{1}{q} \sum_{r \bmod q} e\left(\frac{r(f(n)-a)}{q}\right).\end{aligned}$$

Interchanging sums and isolating the term $r \equiv 0 \pmod q$, we obtain

$$\#\{n \le x : f(n) \equiv a \pmod q\} = \frac{x}{q} + \frac{1}{q} \sum_{r\not\equiv 0 \pmod q} e\left(\frac{-ra}{q}\right) \sum_{n\le x} e\left(\frac{rf(n)}{q}\right).$$

The lemma now follows from the hypothesis that $\sum_{n\le x} e\left(rf(n)/q\right) = o(x)$ as $x \to \infty$, for each $r \not\equiv 0 \pmod q$. □

Remark 1.1.2. *Lemma 1.1.1 should be reminiscent of the classical "Weyl equidistribution criterion" that is used to test for "uniform distribution mod* 1*". Here we say that a sequence* $\{\alpha_n\}_{n=1}^{\infty}$ *of real numbers is* uniformly distributed mod 1 *if for any*

subinterval (a, b) *of* $[0, 1]$*, we have*

$$\lim_{x\to\infty} \frac{1}{x} \#\{n \le x : \{\alpha_n\} \in (a, b)\} \;=\; b - a,$$

where $\{\alpha\} \coloneqq \alpha - \lfloor\alpha\rfloor$ *denotes the fractional part of a real number* α*. This is* ***not*** *the same as the vacuous notion of "uniform distribution mod* q*" with* $q = 1$*. The notions of "uniform distribution mod* q*" (for a general* q*) and "uniform distribution mod* 1*" are not directly related to one another, however there are some connections. See [49, Chapter 1] for some remarks on these connections.*

Remark 1.1.3. *An interesting question to ask would be: Can we characterize those sets* $X \subset \mathbb{N}$ *for which there exists a function* $f : \mathbb{N} \to \mathbb{Z}$ *satisfying the following property:* f *is UD mod* $q \iff q \in X$*.*

A tautological necessary condition on X *is that it must be "divisor closed", i.e. for any* $q \in X$*, all the divisors of* q *must also lie in* X*. (This follows from the observation that any residue class mod* d *is a union of* q/d *many residue classes mod* q*.) This condition was also proven to be sufficient by A. Zame in [81].*

This notion of equidistribution generalizes naturally to a family $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ of arithmetic functions: We say that this family is jointly equidistributed (or jointly UD) modulo q if for any family of residue classes $a_1, \dots, a_K \bmod q$, we have

$$\#\{n \le x : \ \forall i \in [K], \quad f_i(n) \equiv a_i \pmod q\} \ \sim \ \frac{x}{q^K} \quad \text{as} \quad x \to \infty. \tag{1.1}$$

(Here and below, $[K]$ denotes the set $\{1, \dots, K\}$.) A straightforward extension of the argument given for Lemma 1.1.1 yields the following generalization of it.

Lemma 1.1.4. *The functions* $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ *are jointly UD modulo a fixed*

$q \in \mathbb{N}$ if and only if for every tuple of residue classes $(r_1, \dots, r_K) \not\equiv (0, \dots, 0)$ mod q we have

$$\sum_{n \leq x} e\left(\frac{r_1 f_1(n) + \cdots + r_K f_K(n)}{q}\right) = o(x) \quad as \quad x \to \infty.$$

Section 1.2

Equidistribution of additive functions in residue classes: Fixed moduli

The main topic in this thesis is to study the distribution of additive and multiplicative functions in residue classes. Here, we say that $f : \mathbb{N} \to \mathbb{Z}$ is additive if it satisfies $f(mn) = f(m) + f(n)$ for all pairs of **coprime** positive integers m and n. On the other hand, we say that $f : \mathbb{N} \to \mathbb{Z}$ is multiplicative if it satisfies $f(mn) = f(m)f(n)$ for all such m and n.

Some of the most well-known examples of additive functions are:

- The function $\omega(n) = \sum_{p|n} 1$ counting the distinct prime divisors of n.
- The function $\Omega(n) = \sum_{p^k \| n} k = \sum_{p|n} v_p(n)$ counting the prime divisors of n with appropriate multiplicity. Here $v_p(n)$ is the exponent (highest power) of p in the prime factorization of n.
- The function $\beta(n) = \sum_{p|n} p$ summing the distinct prime divisors of n.
- The "Alladi-Erdős" function $A(n) = \sum_{p^k \| n} pk = \sum_{p|n} p v_p(n)$ summing the prime divisors of n with appropriate multiplicity.

Each of these functions is interesting in its own right, and various aspects of these

functions have been studied in the literature. As for their distribution in residue classes, one of the earliest results in this direction is the following

Theorem 1.2.1. *$\omega(n)$ is UD mod q for any $q \in \mathbb{N}$. The same is true for $\Omega(n)$.*

This result is due to Pillai [56], generalizing work of von Mangoldt who showed this for $q = 2$. A similar result was also obtained by Sigmund Selberg in [70].

The Alladi–Erdős function also exhibits equidistribution modulo any positive integer q: This was proven with a very strong error term for $q = 2$ by Alladi and Erdős [3] themselves, and subsequently generalized to arbitrary q by Goldfeld [28].

Theorem 1.2.2. *$A(n)$ is UD mod q for any $q \in \mathbb{N}$. In fact, there exists an absolute constant $c > 0$ such that for $r \in \{0, 1\}$, we have*

$$\#\{n \leq x : A(n) \equiv r \pmod 2\} = \frac{x}{2} + O(x \exp(-c\sqrt{\log x}))$$

as $x \to \infty$. Moreover, for any fixed $q > 2$ and any residue class r mod q, we have as $x \to \infty$,

$$\#\{n \leq x : A(n) \equiv r \pmod q\} = \frac{x}{q} + O\left(\frac{x}{\sqrt{\log x}}\right). \tag{1.2}$$

In 1969, Delange [19] gave a criterion for a general additive function $f : \mathbb{N} \to \mathbb{Z}$ to be equidistributed modulo a fixed $q \in \mathbb{N}$, in terms of the divergence of the sums $S_d := \sum_{d \nmid f(p)} 1/p$ for certain divisors d of q. (See Theorem 1 and Remark 3.1.1 in [19].)

Theorem 1.2.3. *Let $f : \mathbb{N} \to \mathbb{Z}$ be an additive function and $q > 1$ a given integer. Consider the sums $S_d := \sum_{p:\ d \nmid f(p)} 1/p$. Then f is equidistributed mod q if and only if S_ℓ diverges for every odd prime ℓ dividing q, **and** one of the following hold:*

(i) *q is odd;*

(ii) *$2 \parallel q$, and either S_2 diverges or $f(2^r)$ is odd for all $r \geq 1$;*

(iii) *$4 \mid q$, S_4 diverges, and either S_2 diverges or $f(2^r)$ is odd for all $r \geq 1$.*

It is worth noting that Theorem 1.2.1 and the first assertion of Theorem 1.2.2 follow immediately from Theorem 1.2.3: Indeed, since $\omega(p) = \Omega(p) = 1$ for any prime p, we see that for any $d > 1$, the sum $\sum_{p:d\nmid\omega(p)} 1/p = \sum_{p:d\nmid\Omega(p)} 1/p = \sum_p 1/p$ diverges.

In order to establish Theorem 1.2.3, Delange's main idea (a theme that is highly recurrent while proving equidistribution results to fixed moduli) is to utilize the Weyl-type criterion Lemma 1.1.1, and recognize that since $f(n)$ is an additive function, the functions $e(rf(n)/q)$ are *multiplicative*, and as such the sums $\sum_{n\leq x} e(rf(n)/q)$ are amenable to the plethora of tools from the vast subject of "mean values of multiplicative functions". For Theorem 1.2.3, it suffices to use one of the oldest known results in this subject: A theorem of Wirsing [80] that gives a necessary and sufficient condition for the mean value of a multiplicative function $g : \mathbb{N} \to \mathbb{U}$ to vanish, in terms of the average behavior of g at the primes and the behavior of g at powers of 2. (Here $\mathbb{U} \coloneqq \{z \in C : |z| \leq 1\}$ is the unit disk in the complex plane, and by the "mean value" of g, we mean the quantity $\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} g(n)$.)

In his sequel [20] to the aforementioned paper, Delange characterizes when a given family $f_1, \ldots, f_M$ of integral-valued additive functions is jointly equidistributed to a given integer modulus q, by reducing the problem to the equidistribution of a single additive function. The following is the special case of Delange's result that will be relevant in this dissertation. (This corresponds to the assignment $q_i' \coloneqq 1$, $\delta \coloneqq q$ in the result stated in section 4 of [20].)

Theorem 1.2.4. *A given family $f_1, \ldots, f_M$ of integral-valued additive functions is*

jointly equidistributed modulo $q > 1$ if and only if for all integers $k_1, \dots, k_M$ satisfying $\gcd(k_1, \dots, k_M) = 1$,[1] *the additive function $k_1 f_1 + \cdots + k_M f_M$ is equidistributed mod q.*

We remark that the formulation above is equivalent to that in [20, Section 4], which is stated with the additional restriction that $k_1, \dots, k_M \in \{0, \dots, q-1\}$. Indeed, assume that $\sum_{i=1}^{M} \lambda_i f_i$ is equidistributed mod q for all $(\lambda_1, \dots, \lambda_M) \in \{0, 1 \cdots, q-1\}^M$ satisfying $\gcd(\lambda_1, \dots, \lambda_M) = 1$. We claim that $\sum_{i=1}^{M} k_i f_i$ is equidistributed mod q for all $(k_1, \dots, k_M) \in \mathbb{Z}^M$ satisfying $\gcd(k_1, \dots, k_M) = 1$. To see this, we consider any tuple $(k_1, \dots, k_M) \in \mathbb{Z}^M$ having $\gcd(k_1, \dots, k_M) = 1$, and let $k_1', \dots, k_M' \in \{0, 1, \dots, q-1\}$ be the unique integers satisfying $k_i' \equiv k_i \pmod{q}$. Then $d' := \gcd(k_1', \dots, k_M') \in \{1, \dots, q-1\}$ must be coprime to q, for otherwise, there is a prime ℓ dividing $\gcd(q, k_1', \dots, k_M')$ hence also dividing $\gcd(q, k_1, \dots, k_M) = 1$. Write $k_i' =: d' k_i''$ for some $k_1'', \dots, k_M'' \in \{0, 1, \dots, q-1\}$ having $\gcd(k_1'', \dots, k_M'') = 1$. Since d' is invertible mod q and the function $\sum_{i=1}^{M} k_i'' f_i$ is equidistributed mod q, it follows so is the function $\sum_{i=1}^{M} k_i f_i$, as $\sum_{i=1}^{M} k_i f_i \equiv \sum_{i=1}^{M} k_i' f_i \equiv d' \sum_{i=1}^{M} k_i'' f_i \pmod{q}$.

Analogous to the first step in the proof of Theorem 1.2.3, Lemma 1.1.4 becomes relevant in the proof of Theorem 1.2.4. As an application of Theorems 1.2.4 and 1.2.3, and of Dirichlet's theorem on primes in progressions, we have the following extension of (parts of) Theorems 1.2.1 and 1.2.2.

Corollary 1.2.5. *$\omega(n)$ and $A(n)$ are jointly UD modulo any fixed $q \in \mathbb{N}$. The same holds true for $\Omega(n)$ and $A(n)$.*

Remark 1.2.6. *One might ask the following variant of the question asked in Remark 1.1.3: For which sets $X \subset \mathbb{N}$ does there exist an additive function $f : \mathbb{N} \to \mathbb{Z}$ that*

[1] Whenever we speak of $\gcd(k_1, \dots, k_M)$, we assume implicitly that $(k_1, \dots, k_M) \neq (0, \dots, 0)$.

satisfies the following equivalence: f is UD mod $q \iff q \in X$. This question was answered by Narkiewicz in Theorem 4.6 of his monograph [49].

Section 1.3

Equidistribution of multiplicative functions in residue classes: Fixed moduli

We start by giving an account of the results known on the distribution of multiplicative functions to fixed moduli.

1.3.1. The correct notion of "equidistribution"

It turns out that for multiplicative functions, the notion of "equidistribution" defined in the previous section is not the correct one to work with. To see why that is, let's consider one of the most classical examples of a multiplicative function, the Euler totient $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$, which will make an appearance everywhere in this dissertation. It is a well-known result (for instance, implicit in work of Landau [38]) that for any fixed $q \in \mathbb{N}$, "almost all" positive integers n are divisible by a prime $p \equiv 1 \pmod{q}$. In other words, for any fixed q, we have

$$\#\{n \leq x : \exists\ p \equiv 1 \pmod{q} \text{ s.t. } p \mid n\} \sim x \qquad \text{as} \quad x \to \infty.$$

But if n is divisible by a prime $p \equiv 1 \pmod{q}$, this forces $q \mid (p-1) \mid \varphi(n)$. As such, for any fixed q, we obtain

$$\#\{n \leq x : \varphi(n) \equiv 0 \pmod{q}\} \sim x \qquad \text{as} \quad x \to \infty.$$

In particular, this means that $\varphi(n)$ is not equidistributed modulo *any* integer $q > 1$. Motivated by this, Narkiewicz in [45] introduces the notion of weak uniform distribution: Given an integer-valued arithmetic function f and a positive integer q, we say that f is weakly uniformly distributed (or weakly equidistributed or WUD) modulo q if there are infinitely many positive integers n for which $\gcd(f(n), q) = 1$, and if

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

for each coprime residue class a mod q. In other words, our sample space of relevant inputs is the set $\{n : \gcd(f(n), q) = 1\}$ and every coprime residue class mod q gets its fair share of the sample space. For example, f would be WUD mod 6 if $\{n : \gcd(f(n), 6) = 1\}$ is infinite and if the two coprime residue classes 1 mod 6 and 5 mod 6 each (asymptotically) receive 50% of the values $f(n)$ that are coprime to 6.

This definition extends naturally to families of arithmetic functions: We say that the functions $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ 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

$$\#\{n \le x : \forall i \in [K], \quad f_i(n) \equiv a_i \pmod q\} \sim \frac{1}{\varphi(q)^K}\#\{n \le x : \gcd(f_1(n) \cdots f_K(n), q) = 1\} \quad (1.3)$$

as $x \to \infty$, for all coprime residue classes $a_1, \dots, a_K$ mod q.

Just like we used the additive characters $e(r(\cdot)/q)$ to detect arbitrary residue classes mod q, we can use the multiplicative characters (or Dirichlet characters) to detect coprime residue classes mod q. Doing this gives us the following analogues of Lemmas 1.1.1 and 1.1.4, which could be thought of as our "Weyl–type" criteria for weak

equidistribution. In what follows, we use U_q to denote the unit group mod q and $\chi_{0,q}$ to denote the trivial (or principal) character mod q. We also follow the standard convention that $\chi(m) = 0$ for any Dirichlet character χ mod q and any integer m not coprime to q.

Lemma 1.3.1. *Consider arithmetic functions $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ and a fixed positive integer q such that there are infinitely many n for which $\gcd(f_1(n) \dots f_K(n), q) = 1$. Then $f_1, \dots, f_K$ are jointly WUD modulo q if and only if for all tuples of Dirichlet characters $(\chi_1, \dots, \chi_K) \neq (\chi_{0,q}, \dots, \chi_{0,q})$ mod q, we have*

$$\sum_{n \leq x} \chi_1(f_1(n)) \dots \chi_K(f_K(n)) \quad = \quad o\left(\sum_{n \leq x} \chi_{0,q}(f_1(n) \dots f_K(n))\right) \qquad as \quad x \to \infty. \tag{1.4}$$

In particular, consider $f : \mathbb{N} \to \mathbb{Z}$ and $q \in \mathbb{N}$ for which $\{n : \gcd(f(n), q) = 1\}$ is infinite. Then f is WUD mod q if and only if for any nontrivial character χ mod q,

$$\sum_{n \leq x} \chi(f(n)) = o\left(\sum_{n \leq x} \chi_{0,q}(f(n))\right) \quad as \quad x \to \infty. \tag{1.5}$$

Proof. The argument is analogous to that given for Lemma 1.1.1, by substituting the "additive orthogonality relations" by the "orthogonality relations for Dirichlet characters". Indeed for the forward implication, note that if $f_1, \dots, f_K$ are jointly WUD mod q, then for all tuples of Dirichlet characters $(\chi_1, \dots, \chi_K) \neq (\chi_{0,q}, \dots, \chi_{0,q})$ mod q, we have

$$\sum_{n \leq x} \chi_1(f_1(n)) \dots \chi_K(f_K(n)) \quad = \quad \sum_{a_1, \dots, a_K \in U_q} \chi_1(a_1) \dots \chi_K(a_K) \sum_{\substack{n \leq x \\ (\forall i) \ f_i(n) \equiv a_i \pmod q}} 1.$$

Using (1.3) and the definition of $\chi_{0,q}$, we obtain

$$\sum_{n\le x}\chi_1(f_1(n))\dots\chi_K(f_K(n)) = \left(\frac{1}{\varphi(q)^K}\sum_{a_1,\dots,a_K\in U_q}\left(\prod_{i=1}^K\chi_i(a_i)\right)+o(1)\right)\sum_{n\le x}\chi_{0,q}(f_1(n)\dots f_K(n)).$$

But since $(\chi_1,\dots,\chi_K)\neq(\chi_{0,q},\dots,\chi_{0,q}) \bmod q$, we must have $\sum_{a_i\in U_q}\chi_i(a_i)=0$ for some $i\in[K]$, which means that

$$\sum_{a_1,\dots,a_K\in U_q}\left(\prod_{i=1}^K\chi_i(a_i)\right)=\prod_{i=1}^K\left(\sum_{a_i\in U_q}\chi_i(a_i)\right)=0,$$

yielding the forward implication.

For the reverse implication, recall that for any coprime residue $a \bmod q$, we have $\mathbb{1}_{m\equiv a\,(\mathrm{mod}\ q)}=\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\overline{\chi}(a)\chi(m)$, with the sum being over all Dirichlet characters $\chi \bmod q$. This allows us to write for any $a_1,\dots,a_K\in U_q$,

$$\#\{n\le x:\forall i\in[K],\ f_i(n)\equiv a_i\ (\mathrm{mod}\ q)\}=\sum_{n\le x}\prod_{i=1}^K\left(\frac{1}{\varphi(q)}\sum_{\chi_i \bmod q}\overline{\chi}_i(a_i)\chi_i(f_i(n))\right).$$

Expanding the product and interchanging sums, we obtain

$$\#\{n\le x:\forall i\in[K],\ \ f_i(n)\equiv a_i\ (\mathrm{mod}\ q)\} = \frac{1}{\varphi(q)^K}\sum_{\chi_1,\dots,\chi_K \bmod q}\left(\prod_{i=1}^K\overline{\chi}_i(a_i)\right)\sum_{n\le x}\chi_1(f_1(n))\dots\chi_K(f_K(n)).$$

Finally, the contribution of the tuple $(\chi_1,\dots,\chi_K)=(\chi_{0,q},\dots,\chi_{0,q})$ to the above sum is exactly $\varphi(q)^{-K}\#\{n\le x:\gcd(f_1(n)\dots f_K(n),q)=1\}$, whereas by our hypothesis (1.4), the contribution of each tuple $(\chi_1,\dots,\chi_K)\neq(\chi_{0,q},\dots,\mathrm{s}\chi_{0,q}) \bmod q$ is

$o(\varphi(q)^{-K}\#\{n \leq x : \gcd(f_1(n)\dots f_K(n), q) = 1\})$. This yields the desired asymptotic (1.3). □

Remark 1.3.2. *As in Remarks 1.1.3 and 1.2.6, one can ask what conditions on a set $X \subset \mathbb{N}$ are necessary and sufficient for there to exist some function $f : \mathbb{N} \to \mathbb{Z}$ (or some multiplicative function $f : \mathbb{N} \to \mathbb{Z}$) satisfying the property:*

$$f \text{ is WUD mod } q \iff q \in X.$$

This time an obvious necessary condition on X is that if q lies in X, then so must any divisor d of q that has the same prime factors as q: This is because coprimality mod q is equivalent to coprimality mod d, and any reduced residue class mod d is a union of exactly $\varphi(q)/\varphi(d) = q/d$ many reduced residue classes mod q. However, whether this condition is sufficient or not remains an unsolved question (even for the existence of a general arithmetic function f). See [46] and [49] for more remarks on this problem.

1.3.2. Building up towards the general criterion: Weak equidistribution of the Euler totient

While Delange was able to exactly characterize the equidistribution of a general *additive* function modulo an integer, it seems a much more difficult (possibly intractable) problem to exactly characterize the weak equidistribution of a general *multiplicative* function. While results are known for very specific multiplicative functions, the most general results known in literature are able to capture large classes of interesting multiplicative functions (leaving out other classes of interesting multiplicative functions). Some of the most general criteria available in the literature are for multiplicative functions that can be controlled by polynomials at the first few powers of all primes; we will be calling them "polynomially–defined" multiplicative functions.

Precisely, we will say that a **multiplicative** function $f : \mathbb{N} \to \mathbb{Z}$ is polynomially–defined if there exists $V \in \mathbb{N} \cup \{\infty\}$ and polynomials $\{W_v\}_{v=1}^{V}$ with integer coefficients such that $f(p^v) = W_v(p)$ for all $v \in [V]$ and all primes p. In other words, the polynomial W_v controls the behavior of f at the v-th powers of all primes. Several well–known multiplicative functions fall within this class:

- The Euler totient function $f(n) = \varphi(n)$ for which $W_v(T) = T^v - T^{v-1}$.
- The sum of divisors function $f(n) = \sigma(n) = \sum_{d|n} d$ for which $W_v(T) = T^v + T^{v-1} + \cdots + T + 1$.
- More generally, the functions $\sigma_r(n) = \sum_{d|n} d^r$ for which $W_v(T) = T^{rv} + T^{r(v-1)} + \cdots + T^r + 1$. For odd r, these functions also occur as Fourier coefficients of Eisenstein series.
- The divisor function $d(n)$ that counts the number of positive divisors of n, for which $W_v(T) = v + 1$. More generally, the generalized divisor functions $d_r(n) = \sum_{n_1,\ldots,n_r \atop n_1 \ldots n_r = n} 1$, for which $W_v(T) = \binom{v+r-1}{v}$.

These are some natural examples of polynomially–defined multiplicative functions arising in number theory. One can also construct more artificial examples (as is done in applications), such as by fixing any (finite) $V \in \mathbb{N}$, and then defining $f : \mathbb{N} \to \mathbb{Z}$ to be any multiplicative function satisfying $f(p^v) = W_v(p)$ only for $v \in [V]$, with $\{W_v\}_{v=1}^{V}$ being any of the respective polynomials from the examples above, along with $f(p^{V+1}) = \lfloor p^{1/2} \rfloor$. All results below will show that the distribution of such functions in coprime residue classes is highly similar to that of the respective function from the list above.

In [45], Narkiewicz gives a general criterion to decide weak equidistribution of a

single polynomially–defined multiplicative function to a fixed modulus. Although this criterion requires a lot of technical set–up, its proof involves a similar underlying theme as Delange's criterion (Theorem 1.2.3). To highlight these ideas in a simple manner, we consider the consequence of Narkiewicz's criterion for the Euler totient (see [45, Corollary 2]).

Proposition 1.3.3. *$\varphi(n)$ is WUD mod q if and only if* $\gcd(q, 6) = 1$. *Moreover in this case, we have for any $a \in U_q$,*

$$\#\{n \leq x : \varphi(n) \equiv a \pmod{q}\} \sim C_q \frac{x}{(\log x)^{1-\alpha(q)}} \quad as \quad x \to \infty, \tag{1.6}$$

where $\alpha(q) = \prod_{\substack{\ell \mid q \\ \ell \text{ prime}}} \left(1 - \frac{1}{\ell - 1}\right)$ *and $C_q > 0$ is a constant depending only on q.*

Here the necessity of the condition $\gcd(q, 2) = 1$ is clear because otherwise the sample space $\{n : \gcd(\varphi(n), q) = 1\}$ becomes finite. The necessity of the condition $\gcd(q, 3) = 1$ is a little more subtle: Basically, the numbers $p - 1 = \varphi(p)$, for primes $p \neq 3$, either fail to be coprime to 3 or are "trapped" in the trivial subgroup of $(\mathbb{Z}/3\mathbb{Z})^\times$. This prevents $\varphi(n)$ from being weakly equidistributed modulo 3 (and hence also modulo multiples of 3).

The following table illustrates the weak equidistribution of $\varphi(n)$ mod 5. Here for $x \geq 1$ and $r \in \{1, 2, 3, 4\}$, we have defined

$$\rho_r(x) \coloneqq \frac{\#\{n \leq x : \varphi(n) \equiv r \pmod{5}\}}{\#\{n \leq x : \gcd(\varphi(n), 5) = 1\}}.$$

It is worth noting that in the table below, the convergence of each $\rho_r(x)$ to the expected value 0.25 is extremely slow, a point that is addressed by some ongoing work of the author (not part of this thesis), and will be briefly discussed in the

concluding remarks of Chapter 4 (section 4.12).

Table 1: Explicit numerical distributions of $\varphi(n)$ mod 5:

x	$\rho_1(x)$	$\rho_2(x)$	$\rho_3(x)$	$\rho_4(x)$
10^5	0.27165	0.28003	0.23993	0.20837
10^6	0.27157	0.27556	0.23979	0.21307
10^7	0.27073	0.27267	0.23999	0.21660
10^8	0.26998	0.27051	0.24032	0.21917
10^9	0.26924	0.26884	0.24063	0.22127

Outline of proof of Proposition 1.3.3:

As mentioned above, the skeletal idea behind the argument is similar to that in Delange's criterion: Use our "Weyl–type" criterion and estimate the relevant character sums using mean value estimates for multiplicative functions. Indeed by Lemma 1.3.1, $\varphi(n)$ is WUD mod q if any only if

$$\sum_{n\le x}\chi(\varphi(n)) = o\left(\sum_{n\le x}\chi_{0,q}(\varphi(n))\right) \qquad \text{as} \quad x\to\infty \tag{1.7}$$

for every nontrivial character χ mod q.

The sums $\sum_{n\le x}\chi(\varphi(n))$ are once again amenable to mean value results on multiplicative functions, but here this input comes from a Tauberian Theorem of Delange and Ikehara; see for instance [50, Appendix II, Theorem I]. (To apply this theorem, we need to rewrite the Dirichlet series $\sum_{n\ge1}\chi(\varphi(n))/n^s$ in a suitable form, which we do by utilizing its Euler product and invoking basic properties of Dirichlet L–functions.)

An application of this theorem shows that for *any* character χ mod q, we have $\sum_{n\le x}\chi(\varphi(n)) = c_\chi x/(\log x)^{1-\alpha(\chi)} + o(x/(\log x)^{1-\alpha(\chi)})$, where c_χ is a complex number and $\alpha(\chi) = \frac{1}{\varphi(q)}\sum_{b\in U_q}\chi(b-1)$. By the triangle inequality, we have $\mathrm{Re}(\alpha(\chi)) \le$

$|\alpha(\chi)| \leq \alpha(\chi_0)$, with equality precisely when $\chi(b-1) = 1$ for all b in the set $\{b \in U_q : b-1 \in U_q\}$. Thus condition (1.7) holds precisely when for every such nontrivial character χ mod q, we have $c_\chi = 0$. Now the constant c_χ involves an (absolutely convergent) Euler product, hence it vanishes precisely when one of the Euler factors vanishes; this Euler factor is of the form $1 + \sum_{v \geq 1} \chi(\varphi(p^v))/p^v$ for some prime p. The upshot is that φ is WUD mod q precisely when

For every $\chi \neq \chi_{0,q}$ mod q satisfying $\chi(b-1) = 1$ on the set

$$\{b \in U_q : b-1 \in U_q\}, \quad \text{we have } \sum_{j \geq 0} \frac{\chi(\varphi(p^j))}{p^j} = 0 \text{ for some prime } p. \quad (1.8)$$

A straightforward application of the triangle inequality now shows the equation $1 + \sum_{v \geq 1} \chi(\varphi(p^v))/p^v = 0$ is possible only if $p = 2$, and this in turn forces $\chi(2) = 3$, which is impossible. This shows that there *cannot* exist a nontrivial character χ mod q acting trivially on the set $\{b - 1 \in U_q : b \in U_q\}$. An elementary construction using the Chinese Remainder Theorem now shows that this is possible precisely when $\gcd(q, 6) = 1$.

Finally, the asymptotic (1.6) follows from the aforementioned Delange–Ikehara Tauberian Theorem. The exponent $\alpha(q)$ arises from the proportion of unit residues u mod q for which $u - 1$ is also a unit mod q. □

Remark 1.3.4.

- *All the arguments above until condition* (1.8) *go through with minor (mostly notational) modifications to prove Narkiewicz's general criterion, which we have stated as Theorem 1.3.6 below.*

- *By Proposition 1.3.3, $\varphi(n)$ is not weakly equidistributed mod* 3*. Dence and*

Pomerance [21] study the distribution of $\varphi(n)$ mod 3. They find that the residue class 1 mod 3 asymptotically receives about twice as many values of $\varphi(n)$ as compared to the residue class -1 mod 3.

Theorem 1.3.5. *For $r \in \{-1, 1\}$, we have as $x \to \infty$,*

$$\#\{n \leq x : \varphi(n) \equiv r \pmod 3\} \sim c_r x/\sqrt{\log x},$$

where $c_1 \approx 0.6109$ and $c_{-1} \approx 0.3284$.

1.3.3. Narkiewicz's criteria for weak equidistribution and applications

Consider now a general polynomially–defined multiplicative function $f : \mathbb{N} \to \mathbb{Z}$, so that there exist polynomials $\{W_v\}_{v=1}^{V}$ with integer coefficients satisfying $f(p^v) = W_v(p)$ for all primes p and for all $v \in [V]$. Fix a positive integer q. As for $\varphi(n)$, we use our criterion Lemma 1.3.1 to reduce the problem of characterizing the weak equidistiribution of $f(n)$ mod q to the problem of estimating the partial sums $\sum_{n\leq x} \chi(f(n))$.

Now the Dirichlet series $\sum_{n\geq 1} \chi(f(n))/n^s$ is absolutely convergent in the half-plane $\mathrm{Re}(s) > 1$, and possesses the Euler product $\prod_p(1 + \sum_{v\geq 1} \chi(f(p^v))/p^{vs})$. Defining $R_v(q) \coloneqq \{u \in U_q : W_v(u) \in U_q\}$ for each $v \in [V]$, note that if $R_v(q)$ were empty for some v, then $\chi(f(p^v)) = \chi(W_v(p))$ would be zero for all primes p not dividing q. Hence to gain some traction on the aforementioned Euler product, we should assume (the non–degeneracy condition) that $R_v(q)$ is nonempty for some $v \in [V]$. With k denoting the least such v, we say that q is k–admissible, and in this case,

$$\sum_{n\geq 1} \frac{\chi(f(n))}{n^s} = \prod_{p\nmid q}\left(1 + \sum_{v\geq k} \frac{\chi(f(p^v))}{p^{vs}}\right) \cdot \prod_{p|q}\left(1 + \sum_{v\geq 1} \frac{\chi(f(p^v))}{p^{vs}}\right)$$

Notice that each Euler factor in the infinite part of the Euler product starts at the

k-th power of primes: As such, the above Dirichlet series defines an analytic function on the half plane $\mathrm{Re}(s) > 1/k$ and its behavior is determined by the polynomial W_k. (In the discussion for $\varphi(n)$ in the previous subsection, we had $k = 1$, so $W_k(T)$ was just $T - 1$.)

Carrying out the arguments until (1.8) in the outline of the proof of Proposition 1.3.3 now shows that in order for f to be weakly equidistributed mod q, it is necessary and sufficient to have a condition of the form (1.8). This leads to the following general criterion for weak equidistribution due to Narkiewicz (see [45, Theorem I]).

Theorem 1.3.6. *Let $f : \mathbb{N} \to \mathbb{Z}$ be a polynomially–defined multiplicative function, with polynomials $\{W_v\}_{v=1}^{V} \subset \mathbb{Z}[T]$ satisfying $f(p^v) = W_v(p)$ for all $v \in [V]$ and all primes p. Fix $k \in [V]$ and a k-admissible $q \in \mathbb{N}$.*

Then f is WUD mod q if and only if for every nontrivial Dirichlet character χ mod q satisfying $\chi(W_k(b)) = 1$ on the set $\{b \in U_q : W_k(b) \in U_q\}$, there exists a prime p satisfying $\sum_{j\geq 0} \chi(f(p^j))\ p^{-j/k} = 0$. When this happens, there exists a constant $C_q > 0$ depending only on q such that for any $a \in U_q$, we have

$$\#\{n \leq x : f(n) \equiv a \pmod q\} \ \sim\ C_q \frac{x}{(\log x)^{1-\alpha(q)}} \quad as \quad x \to \infty,$$

where $\alpha(q) \coloneqq \frac{1}{\varphi(q)} \#\{u \in U_q : W_k(u) \in U_q\}$.

It remains a highly nontrivial problem to make this condition more explicit in the above generality, for instance by replacing the "existence of prime" condition by a simpler one, or by reducing the computation of the infinite sum $\sum_{j\geq 0} \chi(f(p^j))\ p^{-j/k}$ to a finite computation. Concrete examples of such explicit criteria are Proposition 1.3.3 and some of the results below. See Chapter VI of Narkiewicz's monograph [49] for an algortihmic solution to this problem in some cases.

Remark 1.3.7. *As we will see in Chapter 4, the hypothesis of k-admissibility means that we are working in a really sparse sample set of inputs; in fact $\#\{n \leq x : \gcd(f(n), q) = 1\} = o(x^{1/k})$ as $x \to \infty$. In general, sparse sets like this can often present difficulties while studying arithmetic questions about them, but Narkiewicz's work is able to deal with these difficulties for a fixed modulus.*

However, if $f : \mathbb{N} \to \mathbb{Z}$ is controlled by polynomials up to the V-th powers of primes, but if q is not k-admissible for any $k \in [V]$, then the sample space becomes too sparse to say anything worthwhile (at least without assuming further control on the behavior of f); see for instance [45, Theorem II].

A case of particular interest is when Narkiewicz's criterion holds vacuously, namely, when there are no nontrivial characters χ mod q satisfying $\chi(W_k(b)) = 1$ on the set $\{b \in U_q : W_k(b) \in U_q\}$, or equivalently, when the set $\{W_k(b) : bW_k(b) \in U_q\}$ generates U_q. When this happens, we will say that f is regularly WUD mod q (this terminology was introduced by Narkiewicz in [48]).

Corollary 1.3.8. *In the setting of Theorem 1.3.6, assume that the set $\{W_k(b) : bW_k(b) \in U_q\}$ generates U_q. Then f is WUD mod q.*

We will say that f is regular if for *any* $q \in \mathbb{N}$ for which f is WUD mod q, it must also hold that f is regularly WUD mod q. The outline given for Proposition 1.3.3 shows that $\varphi(n)$ is regular; in fact, this is how Narkiewicz originally deduced Proposition 1.3.3 from Theorem 1.3.6 in [45]. It turns out that the divisor function $d(n)$, the sum of divisors function $\sigma(n)$, as well as the "sum-of-divisor-powers" functions $\sigma_r(n)$ for $r > 2$, are all regular. Observing this for $d(n)$, Narkiewicz [45, Corollary 1] was able to show the following.

Corollary 1.3.9. *The divisor function $d(n)$ is WUD mod q if and only if one of the*

following hold:

(a) $q = 4$.

(b) $q = 2 \cdot 3^m$ *for some* $m \in \mathbb{N}$.

(c) $q = p^m$ *for some* $m \in \mathbb{N}$ *and* 2 *is a primitive root mod* q.

(d) $q = 2p^m$ *for some* $m \in \mathbb{N}$ *and* 3 *is a primitive root mod* q.

In any of these cases, we have for any $a \in U_q$,

$$\#\{n \leq x : d(n) \equiv a \pmod{q}\} \sim C_q x^{1/M} \quad as \quad x \to \infty,$$

where $C_q > 0$ *is a constant depending only on* q *and* $M = \min_{p|q} p - 1$.

Observing that the sum of divisors function $\sigma(n)$ is also regular, Śliwa (see [75]) was able to explicitly characterize those moduli q to which it is weakly equidistributed.

Proposition 1.3.10. *$\sigma(n)$ is WUD mod q iff $6 \nmid q$.*

It remains a highly nontrivial problem to give an explicit classification of all the moduli q to which $\sigma_r(n)$ is weakly equidistributed, for a general $r > 1$. Several authors have made partial contributions to this problem, which we summarize below. The starting point in all the following results is Narkiewicz's criterion Theorem 1.3.6.

1. In the aforementioned paper [75], Śliwa gave some necessary and sufficient conditions for σ_r to be WUD mod q when either $\gcd(\varphi(q), r) = 1$ or $\varphi(q) \mid r$.

2. Fomenko [24] showed that for any fixed $r \in \mathbb{N}$, σ_r is WUD modulo all odd primes $q \gg r^2$.

3. When r itself is an odd prime, Dobrowolski (see [49, Chapter V, Theorem 6.12]) gave some sufficient arithmetic conditions on q for σ_r to be WUD mod q.

4. In [48], Narkiewicz proved that for any $r \geq 3$, the function $\sigma_r(n)$ is regular. Under some natural conditions, he also gave an effective algorithm to classify all moduli to which a given polynomially–defined multiplicative function is regularly WUD. As an application of his algorithm, he showed that σ_3 is WUD mod q if and only if either $\gcd(q, 14) = 1$ or $\gcd(q, 6) = 2$.

5. Narkiewicz's algorithm was improved by Rayner in [64] and [65]. In [64], he showed that for any odd r, there are two finite effectively computable sets $K_1, K_2 \subset \mathbb{Z}$ such that σ_r is WUD mod q iff **either** q is odd and not divisible by an element of K_1, **or** q is even and not divisible by an element of K_2. He computed K_1, K_2 for odd $r \leq 50$. In [65], he extended this work to even $2 \leq r \leq 50$.

6. Narkiewicz and Rayner [51] characterized all q modulo which σ_2 is weakly equidistributed. They show that σ_2 is the only non-regular σ_r, and their characterization of such q is also more complicated than for the other σ_r.

As a consequence of our main theorems in Chapter 4, we can extend all the aforementioned results to varying moduli q satisfying optimal arithmetic restrictions.

In [47], Narkiewicz extended his criterion Theorem 1.3.6 to decide joint weak equidistribution for *families* of "polynomially defined" multiplicative functions to a fixed modulus q. The statement of the general criterion is a natural extension of Theorem 1.3.6, but to state it concisely, we develop the following notation which will also be relevant later in this dissertation.

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

- For any q and $v \in [V]$, define $R_v(q) \coloneqq \{u \in U_q : \prod_{i=1}^K W_{i,v}(u) \in U_q\}$.

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

- Define $\mathcal{Q}(k; f_1, \cdots, f_K)$ to be the set of all k-admissible integers q such that for every tuple $(\chi_1, \dots, \chi_K) \neq (\chi_0, \dots, \chi_0)$ of Dirichlet characters[2] mod q for which the product $\prod_{i=1}^K \chi_i \circ W_{i,k}$ acts trivially on the set $R_k(q)$ [3], there exists a prime p satisfying
$$\sum_{j \geq 0} \frac{\chi_1(f_1(p^j)) \cdots \chi_K(f_K(p^j))}{p^{j/k}} = 0. \tag{1.9}$$
(By the triangle inequality, it is easy to see that any such prime p must be at most 2^k.)

Narkiewicz's criterion [47, Theorem 1] in this setting is then stated as follows.

Theorem 1.3.11. *Fix a k-admissible integer q. The functions $f_1, \dots, f_K$ are jointly weakly equidistributed modulo q if and only if $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$.*

We thus have the following generalization of Corollary 1.3.8.

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

[3] i.e. $\prod_{i=1}^K \chi_i(W_{i,k}(u)) = 1$ for all $u \in R_k(q)$; note that $R_k(q)$ is precisely the support of the product $\prod_{i=1}^K \chi_i \circ W_{i,k}$ (i.e. the set of u where it is nonzero)

Corollary 1.3.12. *Assume that q is k-admissible and that the set*

$$\{(W_{1,k}(u),\dots,W_{K,k}(u)) \bmod q : u\prod_{i=1}^{K} W_{i,k}(u) \in U_q\} \subset U_q^K$$

generates the group U_q^K. Then $(f_1,\dots,f_K)$ are jointly WUD mod q.

When the condition in the above corollary holds, we will say that $(f_1,\dots,f_K)$ are regularly WUD modulo q. Likewise, we can define a family $(f_1,\dots,f_K)$ to be regular.

In [46], Narkiewicz gives an effective algorithm to determine, – for a given family of polynomials $(F_1,\dots,F_K)$ for which $\prod_{i=1}^K F_i$ is squarefree, – the collection of all moduli q for which the set $\{(F_1(u),\dots,F_K(u)) \bmod q : u\prod_{i=1}^K F_i(u) \in U_q\}$ generates the group U_q^K. His algorithm thus also determines effectively, for a given $k \in [V]$, the set of all k-admissible q for which $(f_1,\dots,f_K)$ are regularly WUD mod q (see [46, Theorem II]).

As part of the aforementioned algorithm, he shows that the problem of determining all moduli q for which $\{(F_1(u),\dots,F_K(u)) \bmod q : u\prod_{i=1}^K F_i(u) \in U_q\}$ does not generate U_q^K can be reduced to the finite computation of determining this set under the additional constraints that $v_2(q) \le 3$, that $v_\ell(q) \le 2$ for all odd primes ℓ, and that all prime divisors of q are at most $(1+\sum_{i=1}^K \deg F_i)^2$. For $K=1$ (i.e. a single polynomial), his algorithm doesn't need F_1 to be squarefree but only needs F_1 to not be a constant multiple of a proper power (i.e. square or higher power) of another polynomial.

Using this algorithm and his general criterion Theorem 1.3.11, Narkiewicz characterizes all fixed moduli q such the family (φ,σ) are jointly WUD mod q: It turns out that the necessary condition coming from Proposition 1.3.3 is also sufficient.

Corollary 1.3.13. *The family (φ, σ) is jointly WUD mod q iff* $\gcd(q, 6) = 1$.

Remark 1.3.14. *Note that all the results quoted from [46] and [47] have been stated in greater generality: Narkiewicz actually studies the joint equidistribution of a family of polynomially–defined multiplicative functions with respect to a family of fixed moduli $(q_1, \ldots, q_K)$, where this notion is defined in the natural manner. In particular, Corollary 1.3.13 is the special case of the more complicated [46, Theorem I] that classifies all moduli (q_1, q_2) such that (φ, σ) are jointly WUD modulo (q_1, q_2). Here, we have stuck to the case of a single modulus (i.e., the case when $q_1 = \cdots = q_K = q$) since this case will be most relevant in the rest of this thesis.*

The following consequence of the $k = 1$ case of Theorem 1.3.11 (see [47, Theorem 2]) will be relevant in the initial few chapters of this thesis.

Theorem 1.3.15. *In the notation preceding the statement of Theorem 1.3.11, assume the following:*

(i) None of the polynomials $\{W_{i,1} : 1 \leq i \leq K\}$ are a constant multiple of a proper power of another polynomial.

(ii) For all $i \neq j$, the product $W_{i,1}W_{j,1}$ is squarefree in $\mathbb{Z}[T]$.

Then there exists a constant $C > 0$ depending only on the polynomials $\{W_{1,1}, \ldots, W_{K,1}\}$ such that $(f_1, \ldots, f_K)$ are jointly WUD modulo any fixed $q \in \mathbb{N}$ supported on primes exceeding C. That is, any such q lies in $\mathcal{Q}(1; f_1, \ldots, f_K)$.

Remark 1.3.16. *The constant $C > 0$ above depends only on the degrees, leading coefficients, and the product of all distinct irreducible divisors of the $\{W_{i,1}\}_{i=1}^{K}$.*

In particular, for $K = k = 1$, we have the following simple sufficient condition, which

we restate in simpler notation.

Corollary 1.3.17. *Let $f : \mathbb{N} \to \mathbb{Z}$ be a multiplicative function for which there exists a nonconstant separable polynomial $F \in \mathbb{Z}[T]$ satisfying $f(p) = F(p)$ for all primes p.* [4] *Then there exists a constant $C(F) > 0$ depending only on F such that f is WUD modulo any $q \in \mathbb{N}$ supported on primes exceeding $C(F)$.*

The deduction of Theorem 1.3.15 from Theorem 1.3.11 is one of the main contents of [47]. One of the key ingredients in this deduction is the following result on the behavior of character tuples on polynomial images of the unit group, which will also be useful to us to prove the optimality of some of our main results in later chapters. (See [47, Lemma 5] for the original statement of the following result.)

Lemma 1.3.18.

(a) Consider $K \geq 2$, and nonconstant polynomials $F_1, \dots, F_K \in \mathbb{Z}[T]$ whose product is squarefree. Let $\ell > (1 + \sum_{i=1}^{K} \deg F_i)^2$ be a prime that neither divides the leading coefficient nor the discriminant of $F_1 \dots F_K$.

Then for any $m \geq 1$ and any tuple of Dirichlet characters $(\chi_1, \dots, \chi_K)$ mod ℓ^m, not all trivial, the product $\prod_{i=1}^{K} \chi_i(F_i(u))$ cannot be constant on the set $\{u \bmod \ell^m : \ell \nmid u \prod_{i=1}^{K} F_i(u)\}$.

(b) Consider a polynomial $F \in \mathbb{Z}[T]$ which is not a constant multiple of a proper power of another polynomial. Let $\ell > \max\{5, (1 + \deg F)^2\}$ be a prime that neither divides the leading coefficient of F nor the discriminant of the product of the distinct irreducible factors of F.

Then for any $m \geq 1$ and any nontrivial Dirichlet character χ mod ℓ^m, the

[4] Here by "separable", we mean that F has no roots of multiplicity greater than 1.

function $\chi(F(u))$ cannot be constant on the set $\{u \bmod \ell^m : \ell \nmid uF(u)\}$.

Here is yet another concrete application of Corollary 1.3.12 and Lemma 1.3.18.

Corollary 1.3.19. *The family $(\varphi, \sigma, \sigma_2)$ is jointly weakly equidistributed modulo any fixed integer q supported on primes exceeding* 23.

Section 1.4

Allowing the modulus to vary...

In all these results, the modulus q has been assumed to be fixed. A natural question of some interest is whether one can allow q to **vary** with our stopping point x. This question is motivated by the celebrated Siegel–Walfisz Theorem, according to which for any fixed $K_0 > 0$, the primes up to any x are weakly equidistributed uniformly to moduli $q \leq (\log x)^{K_0}$. We state the qualitative version of this theorem below, although this result is known with error terms of size $O(x \exp(-c\sqrt{\log x}))$; see for instance [44, Corollary 11.19].

Theorem 1.4.1. *Fix $K_0 > 0$. As $x \to \infty$, we have*

$$\#\{p \leq x : p \equiv a \pmod q\} \sim \frac{1}{\varphi(q)}\#\{p \leq x\} \sim \frac{1}{\varphi(q)} \cdot \frac{x}{\log x},$$

uniformly in moduli $q \leq (\log x)^{K_0}$ and in coprime residues a mod q.

A general problem in elementary and analytic number theory is to find analogues of the Siegel–Walfisz theorem in other contexts, and this problem has been ardently studied in various contexts, such as for smooth numbers and mean values of multiplicative functions. In our context, one may ask: Can we find analogues of the Siegel–Walfisz theorem for the value distributions of additive or multiplicative functions or (more

generally) for the joint distributions of families of such functions?

To formalize this, given a constant $K_0 > 0$, we shall say that the functions $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ are jointly equidistributed (or jointly UD) mod q, uniformly for $q \le (\log x)^{K_0}$, if

$$\#\{n \le x : \ \forall i \in [K], \quad f_i(n) \equiv a_i \pmod q\} \ \sim \ \frac{x}{q^K} \quad \text{as} \quad x \to \infty, \tag{1.10}$$

uniformly in moduli $q \le (\log x)^{K_0}$ and in residue classes $a_1, \dots, a_K \bmod q$. Explicitly, this means that for any $\epsilon > 0$, there exists $X(\epsilon, K_0) > 0$ depending only on ϵ and K_0 such that the ratio of the left hand side of (1.10) to the right hand side lies in $(1-\epsilon, 1+\epsilon)$ for all $x > X(\epsilon, K_0)$, all $q \le (\log x)^{K_0}$ and all residues $a_1, \dots, a_K \bmod q$.

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

Likewise, we shall say that the functions $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ 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 (1.3) holds as $x \to \infty$, uniformly in moduli $q \le (\log x)^{K_0}$ and in *coprime* residue classes $a_1, \dots, a_K \bmod q$. Explicitly, this means that for any $\epsilon > 0$, there exists $X(\epsilon, K_0) > 0$ such that the ratio of the left hand side of (1.3) to the right hand side lies in $(1-\epsilon, 1+\epsilon)$ for all $x > X(\epsilon, K_0)$, $q \le (\log x)^{K_0}$ and *coprime* residues $a_1, \dots, a_K \bmod q$.

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

1.4.1. Equidistribution to varying moduli: Siegel–Walfisz for polynomially–defined additive functions

The equidistribution of a single polynomially-defined additive function with uniformity in modulus seems to have been first studied for the Alladi-Erdős function $A(n) = \sum_{p^k \| n} k \cdot p$ in [60]. The special case of Lemma 3.3 in that paper with $y = x$ yields the equidistribution of $A(n)$ to moduli q varying up to (a little less than) the square root of $\log x$.

Proposition 1.4.2. *Fix $\delta > 0$. The function $A(n)$ is UD mod q, uniformly for $q \leq (\log x)^{1/2-\delta}$. In fact, we have*

$$\#\{n \leq x : A(n) \equiv a \pmod q\} = \frac{x}{q} + O\left(\frac{x}{(\log x)^{1/2-\delta}}\right)$$

uniformly in $q \leq \log x$ and in residues a mod q.

Note that Goldfeld's result (1.2) gives a sharper error term for fixed moduli q. The main idea in the proof of Proposition 1.4.2 is to estimate the character sums $\sum_{n \leq x} e(rA(n)/q)$ by invoking the following quantitatively precise version of the result of Halász [30] which states that a multiplicative function F taking values on the unit disk has mean value 0 unless F "pretends" to be[5] n^{it} for some t. The following version of the statement has been taken from [76, Corollary III.4.12], and its development is attributed to Halász, Montgomery and Tenenbaum.

Theorem 1.4.3. *Let F be a multiplicative function such that $|F(n)| \leq 1$ for all n. Uniformly in $x, T \geq 2$, we have*

$$\frac{1}{x}\sum_{n \leq x} F(n) \ll \frac{1}{T} \; + \; \exp\left(-\min_{|t| \leq T} \sum_{p \leq x} \frac{1 - \mathrm{Re}(F(p)p^{-it})}{p}\right).$$

[5] in the sense of Granville and Soundararajan [29]

In order to apply Theorem 1.4.3 to our sums $\sum_{n\leq x} e(rA(n)/q)$, we need to put a suitable lower bound on the sums $\sum_{p\leq x}(1-\mathrm{Re}(A(p)p^{-it}))/p$: We do this by essentially covering the range of summation with "multiplicatively narrow subintervals" wherein the quantity u^{it} is roughly constant, as u varies within the subinterval and as t varies within $[-\log x, \log x]$. This allows us to deduce Proposition 1.4.2.

Proposition 1.4.2 was improved in [61] to allow q to vary within the full "Siegel–Walfisz" range, but without a good quantitative error.

Proposition 1.4.4. *Fix $K_0 > 0$. Then $A(n)$ is UD mod q, uniformly for $q \leq (\log x)^{K_0}$.*

This result comes as a byproduct of a certain "mixing phenomenon" in the multiplicative group mod q that we will be using to establish some of the main results in this thesis. The said "mixing" idea was originally used in the paper of Pollack with the author [61] (which forms the contents of Chapter 2) in order to extend Corollary 1.3.17 to q varying within a wide range, thus taking the first few steps towards obtaining uniform analogues of Narkiewicz's general criterion Theorem 1.3.11.

One of the topics we will study in this thesis is the phenomenon of joint equidistribution for families of polynomially–defined additive functions: Here, we say that an additive function $g\colon \mathbb{N}\to\mathbb{Z}$ is polynomially-defined if there exists a nonconstant polynomial $G\in\mathbb{Z}[T]$ satisfying $g(p)=G(p)$ for all primes p; we will then say that g is defined by (the polynomial) G. For example, both the additive functions $\beta(n) \coloneqq \sum_{p|n} p$ and the Alladi-Erdős function $A(n)=\sum_{p^k\|n} kp$ are defined by the polynomial $G(T)=T$. (Note that our definition of a polynomially–defined multiplicative function was more general, but this should not create any confusion since we will always make it explicit whether we are considering an additive or multiplicative function.)

Our starting point to study this joint equidistribution is Delange's criteria Theorems 1.2.3 and 1.2.4, which we reformulate (in section 3.2) to more explicit results for *polynomially–defined* additive functions: Certainly if $(f_1, \dots, f_K)$ are jointly equidistributed mod $q \leq (\log x)^{K_0}$, then q has to satisfy the conditions of these two theorems.

For a single *arbitrary* polynomially–defined additive function $g : \mathbb{N} \to \mathbb{Z}$, Akande [1] shows that the arithmetic conditions in Theorem 1.2.3 are also sufficient for g to be weakly equidistributed modulo q varying uniformly up to small powers of $\log x$.

Theorem 1.4.5. *Fix $K_0 > 0$ and $\delta \in (0, 1]$. Let $g : \mathbb{N} \to \mathbb{Z}$ be an additive function defined by a polynomial $G \in \mathbb{Z}[T]$ of degree $D > 0$. Let $\mathcal{Q}(g)$ denote the set of all (fixed) moduli that satisfy Delange's criterion in Theorem 1.2.3. Then g is UD modulo $q \in \mathcal{Q}(g)$ varying uniformly up to $(\log x)^{\min\{K_0,(1-\delta)(1-1/D)^{-1}\}}$.*

Note that for $D = 1$, the range of uniformity is $(\log x)^{K_0}$, the full "Siegel–Walfisz range". For $D > 1$, he is also able to prove that the exponent of $\log x$ is essentially optimal. To show all of these, he suitably adapts the arguments in [61] (in particular, the aforementioned "mixing" idea) by means of certain exponential sum estimates, in order to show that the behavior of g modulo q can be related to that modulo a bounded divisor of q ("bounded" in size by a constant depending only on the fixed polynomial G).

In Chapter 3 (based on the manuscript [73]), we shall extend all of the aforementioned results for a general family of polynomially–defined additive functions $g_1, \dots, g_M : \mathbb{N} \to \mathbb{Z}$ that are defined by polynomials $G_1, \dots, G_M \in \mathbb{Z}[T]$. We will show that asssuming the linear independence of the derivatives of the G_i (a condition which we prove to be necessary), the family $(g_1, \dots, g_M)$ is equidistributed uniformly modulo q satisfying Delange's criteria (Theorem 1.2.4 and 1.2.3) that is allowed to vary up to

certain small powers of $\log x$; we can also prove these powers to be essentially optimal (except in the case $M = \deg(G_1) = 1$ addressed by Akande). Furthermore, we show that uniformity is restored in the complete Siegel–Walfisz range (up to arbitrary powers of $\log x$) provided we appropriately restrict our inputs, restrictions that we are also able to optimize in most cases.

To do all this, we need to refine some of the arguments used in the aforementioned results and also use some new ideas not present therein. For instance, we need to look at the Smith normal forms and invariant factors of certain matrices to bound certain character sums. Moreover, we need to bound the contributions of certain "bad" inputs n by carefully studying the prime decompositions of such n and using different kinds of "anatomical arguments"[6] in different cases.

1.4.2. Equidistribution to varying moduli: Siegel–Walfisz for polynomially–defined multiplicative functions

Much of this thesis began with the problem of trying to give best possible analogues of the Siegel–Walfisz theorem for general families of polynomially–defined multiplicative functions, extending Narkiewicz's criterion Theorem 1.3.11 to varying moduli q with optimal restrictions. It appears that the first result in the direction of this problem was obtained in joint work of Lebowitz-Lockard, Pollack and the author, who extended Proposition 1.3.3 on the weak equidistribution of the Euler totient to **prime** moduli varying within the full Siegel–Walfisz range (see [40, Theorem 1.1]):

Theorem 1.4.6. *Fix $K_0 > 0$. The Euler totient $\varphi(n)$ is weakly equidistributed modulo prime p lying in $[5, (\log x)^{K_0}]$. In fact,*

$$\#\{n \le x : \varphi(n) \equiv a \pmod p\} \sim \frac{1}{p-1} \cdot \frac{x}{(\log x)^{1/(p-1)}} \quad as \quad x \to \infty,$$

[6] in the sense of "anatomy of integers"

uniformly in prime moduli p satisfying $5 \leq p \leq (\log x)^{K_0}$ and in coprime residues a mod p.

The proof of this theorem combines two different methods, an analytic and an anatomical method. For small p (roughly smaller than $(\log\log x)^2$), we apply the analytic method of Landau–Selberg–Delange, more precisely, an explicit version of this enunciated by Chang and Martin [12] that allows for additional uniformity in certain important parameters. On the other hand, when p is a little larger than $\log\log x$, we apply a combinatorial and anatomical method of Banks–Harman–Shparlinski [7]: In a very crude summary, this involves splitting off the largest prime factor P of our inputs n, using multiple sieve–theoretic arguments to ensure that P is large and appears only once in n, and then writing n in the form mP, so that the congruence $\varphi(n) \equiv a \pmod{p}$ can be rewritten as a linear congruence in P, thus throwing P in a residue class mod p and allowing us to estimate the number of possible P via the Siegel–Walfisz theorem. Note that the analytic part of our argument uses crucially that nontrivial Jacobi sums over $\mathbb{F}_p$ are bounded by $\sqrt{p}$ in absolute value; the trivial bound of p would only allow the method to work for p up to about $\log\log x$, just shy of what is required for overlap with our second range. However, these methods are crucially limited to $\varphi(n)$ (and $\sigma(n)$) and to prime moduli.

Instead of directly trying to get complete uniform analogues of the most general criterion Theorem 1.3.11, let us first try to do this for Theorem 1.3.15 (which, recall, gives weak equidistribution of $f_1, \ldots, f_K$ to moduli supported on large primes, under some restrictions on the polynomials defining the f_i at the primes) or Corollary 1.3.17 (the special case of Theorem 1.3.15 for a single function). In [59], we were able to get a partial uniform analogue of Theorem 1.3.15, where we showed that a multiplicative function $f : \mathbb{N} \to \mathbb{Z}$ controlled by a nonconstant separable polynomial at the primes

is WUD modulo q varying up to a very small power of $\log x$ that is "almost prime", in the sense that the quantity $\delta(q) = \sum_{\substack{\ell \text{ prime} \\ \ell | q}} 1/\ell$ becomes negligible as $x \to \infty$. (See [59, Theorem 1.1] for the original statement of the following result.)

Theorem 1.4.7. *Let $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ be multiplicative functions for which there exist nonconstant polynomials $F_1, \dots, F_K \in \mathbb{Z}[T]$ with $F_1 \dots F_K$ separable, such that $f_i(p) = F_i(p)$ for all $i \in [K]$ and all primes p.*

Fix $\epsilon > 0$. Then (1.3) holds as $x \to \infty$, uniformly in $q \to \infty$ satisfying $q \leq (\log x)^{1/K - \epsilon}$ and $\delta(q) = o(1)$.

As an application, note that while Theorem 1.3.15 shows that the family $(n, \varphi(n), \sigma(n))$ is jointly WUD modulo all fixed sufficiently large primes, Theorem 1.4.7 shows that such equidistribution also holds uniformly modulo all primes $p \leq (\log x)^{1/3-\epsilon}$ exceeding a certain (fixed) threshold. (With the more explicit version of Theorem 1.3.15 in [47], one can show that this threshold is 17.)

The main idea in the proof of Theorem 1.4.7 is to extend the anatomical method used for Theorem 1.4.6, by splitting off the largest J prime factors of our inputs n, for some fixed judiciously-chosen J. In other words, we write $n = mP_J \dots P_1$ with $P(m) \leq P_J \leq \dots \leq P_1$. (Here $P(m)$ is the largest prime factor of m.) Most of the time, $P_J, \dots, P_1$ will appear to the first power only in n, so that $f_k(n) = f_k(m) f_k(P_J) \cdots f_k(P_1)$. Then given m, we use the Siegel–Walfisz theorem and character sum estimates to understand the number of choices for $P_1, \dots, P_J$ compatible with the congruence conditions on $f_k(n)$.

The highly stringent restriction $\delta(q) = o(1)$ is nothing but a facet of the above argument. In [61], Pollack and the author were able to remove this requirement and get the complete uniform analogue of Corollary 1.3.17. To do this, we observed a

certain "quantitative ergodicity" phenomenon in the multiplicative group mod q, by virtue of which for any fixed polynomial $F \in \mathbb{Z}[T]$ and any $q \in \mathbb{N}$ supported on primes large enough compared to F, the images of the elements of U_q under F demonstrate a certain "mixing" in U_q. (A related idea was used in a different problem by Kátai [34].)

With notation as in Corollary 1.3.17 and with moduli q satisfying the "roughness" condition therein, we showed that if F is linear then weak equidistribution holds up to arbitrary powers of $\log x$. (In particular, this extends Proposition 1.3.3 on the weak equidistribution of $\varphi(n)$ to the complete Siegel–Walfisz range.) In the general case, however, q can only be allowed to vary up to *small* powers of $\log x$, which we were able to optimize [61, Theorem 1.3]. Uniformity could be restored in the full Siegel-Walfisz range by suitably restricting the set of inputs n [61, Theorem 1.4]. See Chapter 2 for more details.

Now we come to the grand finale: The problem of giving best possible uniform analogues of Narkiewicz's general criterion Theorem 1.3.11. It turns out all the developments mentioned until this point are still really far from solving this problem in its complete generality. This is because several of the arguments in the last work above are limited to a single function (i.e. the case $K = 1$) and do not generalize to a family of functions, whereas the latest work for families mentioned so far (Theorem 1.4.7) requires hypotheses that are way too restrictive. Moreover, even in the special case of a single function, we have only restricted to the case when q is 1-admissible and supported on only large prime factors, and we have also been assuming that our defining polynomial is separable. In particular, these results do not give satisfactory uniform analogues of many of the results stated in subsection § 1.3.3, since the results in § 1.3.3 involve k-admissible moduli for arbitrary $k > 1$; here k is as in the set up

preceding the statement of Theorem 1.3.11.

In Chapter 4 (based on the latest manuscripts [71] and [72]), we remove all these limitations and solve the full general problem posed at the start of this subsection. We obtain essentially best possible uniform analogues of Narkiewicz's criterion Theorem 1.3.11 in its complete generality to a single varying modulus.

One of our main results is that in the setting of Theorem 1.3.11 and under two **provably unavoidable** technical hypotheses H_1 and H_2, the family $f_1, \dots, f_K$ is jointly WUD to a modulus $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ that is also allowed to vary within essentially optimal ranges. Roughly, this result looks like the following:

Theorem 1.4.8 (Theorem 4.1.1, summarized)**.** *Fix $K_0 > 0$. In the setting of Theorem 1.3.11 and under hypotheses H_1 and H_2, the family $(f_1, \dots, f_K)$ is jointly WUD, uniformly modulo $q \leq (\log x)^{c_q}$ lying in $\mathcal{Q}(k; f_1, \dots, f_K)$. Here $c_q \in (0, K_0]$ is a parameter depending (essentially) on q and on the polynomials $W_{1,k}, \dots, W_{K,k}$ (that define the f_i at the k-th powers of primes).*

Note that lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ is the necessary arithmetic restriction for $(f_1, \dots, f_K)$ to be jointly weakly equidistributed to a k-admissible modulus q. In Theorem 4.1.1, we give explicit expressions for c_q in an exhaustive list of cases. It is worth mentioning that c_q depends on the number of roots of the polynomial $W_1 \dots W_K$ modulo the primes divisors of q. The best possible lower bound on c_q that holds in general is $c_q \gg (\log\log(3q))^{-\sum_{i=1}^{K} \deg W_{i,k}}$, however c_q can be bounded below by a constant in several applications (for instance, if most prime divisors of q avoid certain residue classes). In fact, we either optimize c_q or we show that c_q is K_0 itself; in the latter case, we have uniformity in the full Siegel–Walfisz range.

In the former case, c_q turns out to be a small parameter, giving uniformity only up

to small powers of $\log x$ (which are essentially optimal). We show that uniformity can be restored up to arbitrary powers of $\log x$ by restricting to inputs n that have sufficiently many large prime divisors. More precisely, with $P_R(n)$ denoting the R-th largest prime factor of n counted with multiplicity (and defining $P_R(n) \coloneqq 1$ if n has fewer than R prime factors), we have

Theorem 1.4.9 (Theorems 4.1.2 and 4.1.3, summarized)**.** *Fix $K_0 > 0$. In the setting of Theorem 1.3.11, and under hypotheses H_1 and H_2, there exists a fixed integer R (depending only on k, K and $\sum_{i=1}^{K} \deg W_{i,k}$) such that*

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

uniformly in $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and in units $(a_i)_{i=1}^K$ mod q.

The original statements contain the exhaustive case-wise list of explicit values of R: Most of these values are exactly or almost optimal in their respective cases, thus ensuring equidistribution among as large a set of inputs as possible.

In [72], we obtain cleaner versions of the last two theorems when additional control is available *either* on the multiplicative functions f_i *or* on the anatomy of our inputs n. We also show that even if *one* of the two hypotheses H_1 or H_2 is violated, then uniformity would fail in the above theorems in some of the worst possible ways: Not only would uniformity fail modulo arbitrarily large $q \le (\log x)^{K_0}$, but also would be *unrecoverable* no matter how much we restrict our set of inputs n to those having many large prime factors. Thus, our results in [71, 72] are essentially best possible qualitative analogues of the Siegel-Walfisz theorem for families of polynomially-defined multiplicative functions. As consequences, we are able to give complete uniform ana-

logues of all the results of Narkiewicz, Śliwa, Dobrowolski, Fomenko, Rayner and others, that were stated in subsection § 1.3.3.

The arguments used to prove our general results comprise a wide variety of themes spanning several areas of mathematics. First of all, we need to refine our "mixing phenomenon" with more sophisticated anatomical arguments, supplemented by character sum machinery combined with linear algebra over residue rings. But this only takes us partway: To get the desired main terms, we crucially need arguments from both the classical and "pretentious" sides of analytic number theory. Note that the anatomical part of our arguments cannot be substituted by analytic arguments either, since the latter do not give us the full range of uniformity. Furthermore, to bound the contributions of certain "bad" inputs, we need to employ various sieve theoretic techniques and understand the rational points of certain affine varieties over finite fields using tools from arithmetic/algebraic geometry. The complete details of all the results, arguments, optimality and applications have been provided in Chapter 4.

Section 1.5

Summary of later chapters

The summary of most of the thesis has been given in the last two subsections. Chapters 2, 3 and 4 have been organized in the chronology of papers written: Chapter 2 describes the work in [61] leading to the complete uniform analogue of Corollary 1.3.17. In Chapter 3 (based on [73]), we digress to additive functions and give the complete uniform analogue of Delange's criterion for a family of polynomially–defined additive functions (as alluded to in subsection § 1.4.2). In Chapter 4 (based on [71] and [72]), we obtain the best possible uniform analogues of the Siegel–Walfisz theorem for a general family of polynomially–defined multiplicative functions.

In the last chapter of the thesis, we venture out of the additive and multiplicative realms. One of the most well-known examples of an arithmetic function that is neither additive nor multiplicative is the sum of proper divisors (or aliquot divisors) function $s(n) = \sigma(n) - n$. This function has been the subject of a variety of exciting results and elusive conjectures. In Chapter 5, we explore the distribution of $s(n)$ to varying prime moduli. Since $s(n) = 1$ for all prime n, the Prime Number Theorem shows that to get uniformity up to arbitrary powers of $\log x$, one needs to at least to restrict to composite inputs n. We show that this restriction is sufficient to have $s(n)$ be equidistributed to prime moduli p varying within the full Siegel–Walfisz range. This is based on work done in [40] (the same paper containing our oldest result Theorem 1.4.6), and it turns out that the methods of Chapters 2–4 can be adapted to simplify our arguments from that paper. (Chapter 5 contains this simplified argument and not the original argument in [40].)

Remark 1.5.1. *We conclude this chapter with the remark that the problem of investigating distribution in residue classes of an integer sequence can be thought of as investigating the trailing digits of the terms of that sequence. (This is especially apparent if q is a power of 10, and more generally if q is a power of some integer b and we work in "base b".) The dual question is that of studying leading digits, and in this regard, the "Benford phenomenon" is of significant interest. We say that a sequence of numbers follows "Benford's Law" if smaller digits are more likely to appear in the sequence and vice versa (defined in a precise way). This phenomenon was originally observed by Simon Newcomb, and since then has been studied for a variety of interesting sequences. In [60] and [43], we study this phenomenon for the sequence of "intermediate prime factors". In [11], Chandee, Li, Pollack and the author give a general criterion for a multiplicative function to satisfy the Benford phenomenon, and using this criterion we study the Benford behavior of several interesting multi-*

plicative functions, including but not limited to Hecke eigenvalues of newforms (such as Ramanujan's τ-function). We will not be elaborating on these works in this thesis.

1.5.1. Notation and conventions

- We do not consider the zero function as multiplicative, so if f is multiplicative, then $f(1) = 1$.

- By $P(n)$ and $P^-(n)$, we will mean the largest and least prime divisors of n, respectively. For most of the thesis, we will stick to the convention that $P(1) \coloneqq 1$ and $P^-(1) \coloneqq \infty$.

- We set $P_1(n) = P(n)$ and define, inductively, $P_k(n) = P_{k-1}(n/P(n))$. Thus, $P_k(n)$ is the kth largest prime factor of n counted with multiplicity, with $P_k(n) = 1$ if $\Omega(n) < k$.

- Given $z > 0$, we say that a positive integer n is z-smooth if $P(n) \leq z$, 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, let $R^\times$ denote the multiplicative group of units of R. Write $U_q \coloneqq (\mathbb{Z}/q\mathbb{Z})^\times$.

- We denote the number of primes dividing q counted with and without multiplicity by $\Omega(q)$ and $\omega(q)$ respectively.

- For a Dirichlet character χ mod q, we use $\mathfrak{f}(\chi)$ for 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 $\mathrm{ord}_\ell(H)$ to denote the highest power of ℓ dividing all the coefficients of H; for an integer $m \neq 0$, we may use $v_\ell(m)$ in place of $\mathrm{ord}_\ell(m)$.

- Let $\mathbb{M}_{A\times B}(\mathbb{Z})$ denote the ring of $A \times B$ matrices with integer entries, while $GL_{A\times B}(\mathbb{Z})$ refer 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 $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v\leq k}}$. Other dependence will be noted explicitly (for example, with parentheses or subscripts): Notably, we shall use $C(F_1, \ldots, F_K)$, $C'(F_1, \ldots, F_K)$ and so on, to denote constants depending on the fixed polynomials $F_1, \ldots, F_K$.

- We write $\log_k$ for the k-th iterate of the natural logarithm.

Other notation will be locally defined as required.

Chapter 2

Weak equidistribution of a single function to a varying "rough" modulus: The mixing phenomenon

In this chapter, we introduce the "mixing phenomenon" (briefly alluded to in subsections 1.4.1 and 1.4.2) in order to obtain complete uniform analogues of Corollary 1.3.17 that gave sufficient conditions for the weak equidistribution of a single polynomially–defined multiplicative function to a fixed modulus supported on large primes. (We restate the corollary as a proposition below.) Throughout this chapter, we will be considering a multiplicative function $f : \mathbb{N} \to \mathbb{Z}$ for which there exists a nonconstant separable polynomial $F \in \mathbb{Z}[T]$ satisfying $f(p) = F(p)$ for all primes p.

Proposition 2.0.1. *There exists a constant $C(F) > 0$ depending only on F such that f is WUD modulo any fixed $q \in \mathbb{N}$ supported on primes exceeding $C(F)$.*

This chapter is based on the joint paper [61] of Pollack and the author.

Section 2.1

Main results of this chapter

Our first theorem shows that one has uniformity in q up to an arbitrary (but fixed) power of $\log x$ when F is linear.

Theorem 2.1.1. *Let f be a fixed polynomially-defined function with $F(T) = RT + S$, where $R, S \in \mathbb{Z}$ with $R \neq 0$. Fix a real number $K_0 > 0$. Then $f(n)$ is WUD mod q, uniformly for $q \leq (\log x)^{K_0}$ coprime to $6R$.*

A concrete consequence of this result is that the Euler totient $\varphi(n)$ is weakly equidistributed to moduli q coprime to 6 that vary up to any fixed power of $\log x$: This optimally extends Proposition 1.3.3 to moduli q varying within the Siegel–Walfisz range. We are not sure what to conjecture for how far the range of uniformity can be extended. For $f(n) = \varphi(n)$, we cannot replace $(\log x)^{K_0}$ with $L(x)^{1+\delta}$ for any $\delta > 0$, where $L(x) = x^{\log\log\log x/\log\log x}$. This is a direct consequence of work of Pomerance [63] showing that for all large x, there is an integer $m \leq x$ having all prime factors at most $\log x$ and possessing at least $x/L(x)^{1+\delta/2}$ many φ-preimages $n \leq x$. (He proved this result conditional on a plausible conjecture about shifted primes with no large prime factors.)

When the defining polynomial F has degree larger than 1, our method applies but the results require some preparation to state. Let $F(T) \in \mathbb{Z}[T]$ be nonconstant. For each positive integer q, define

$$\nu(q) = \#\{a \bmod q : \gcd(a, q) = 1 \text{ and } F(a) \equiv 0 \pmod q\} \tag{2.1}$$

and let

$$\alpha(q) = \frac{1}{\varphi(q)} \#\{a \bmod q : \gcd(aF(a), q) = 1\}. \tag{2.2}$$

It is straightforward to check, using the Chinese Remainder Theorem, that

$$\alpha(q) = \prod_{\substack{\ell \mid q \\ \ell \text{ prime}}} \left(1 - \frac{\nu(\ell)}{\ell - 1}\right). \tag{2.3}$$

If F has degree D, then $\nu(\ell) \leq D$ whenever ℓ does not divide the leading coefficient of F. Thus, if q is coprime to that coefficient and every prime dividing q exceeds $D+1$, then $\alpha(q)$ is nonzero. Furthermore if $\alpha(q)$ is nonzero, then $\nu(\ell) \leq \min\{\ell - 2, D\}$ for all primes $\ell \mid q$. By Mertens' theorem and the bound $\omega(q) \leq \log(3q)$, this yields

$$\alpha(q) \gg_D \exp\left(-\sum_{\substack{\ell \mid q:\ \ell > D \\ \ell \text{ prime}}} \frac{\nu(\ell)}{\ell}\right) \geq \exp\left(-D \sum_{\substack{\ell \leq \omega(q) \\ \ell \text{ prime}}} \frac{1}{\ell}\right) \gg_D (\log\log(3q))^{-D}. \tag{2.4}$$

The lower bound (2.4) will prove important later.

Theorem 2.1.2. *Let f be a fixed, polynomially-defined multiplicative function. Fix $\delta \in (0, 1]$. There is a constant $C = C(F)$ such that the following holds. For each fixed K_0, the values $f(n)$ for $n \leq x$ are asymptotically weakly equidistributed mod q provided that $q \leq (\log x)^{K_0}$, that q is divisible only by primes exceeding C, and that either*

(i) q is squarefree with $\omega(q) \leq (1-\delta)\alpha(q) \log\log x / \log D$, or

(ii) $q \leq (\log x)^{\alpha(q)(1-\delta)(1-1/D)^{-1}}$.

Conditions (i) and (ii) in Theorem 2.1.2 reflect genuine obstructions to uniformity. To motivate (i), fix an integer $D \geq 2$, and let $F(T) = (T-2)(T-4)\cdots(T-2D)+2$. Note

that F is Eisenstein at 2, so F is irreducible over $\mathbb{Q}$ and thus without multiple roots. Let f be the completely multiplicative function with $f(p) = F(p)$ for all primes p, and let q be a squarefree product of primes exceeding $D+1$. Then $F(p) \equiv 2 \pmod q$ whenever $(p-2)\cdots(p-2D) \equiv 0 \pmod q$. This congruence puts p in one of $D^{\omega(q)}$ coprime residue classes mod q. Hence, we expect $\gg \frac{D^{\omega(q)}}{\varphi(q)}\frac{x}{\log x}$ primes $p \le x$ with $F(p) \equiv 2 \pmod q$, and we are assured this many primes (by Siegel–Walfisz) if q is bounded by a power of $\log x$. On the other hand, Proposition 2.2.1 below implies (under this same restriction on the size of q) that the number of $n \le x$ with $\gcd(f(n), q) = 1$ is $x/(\log x)^{1-(1+o(1))\alpha(q)}$. Thus, the residue class $2 \bmod q$ will be 'overrepresented' (vis-à-vis the expectation of weak uniform distribution) if $D^{\omega(q)} > (\log x)^{(1+\delta)\alpha(q)}$ for any fixed $\delta > 0$, or in other words, if $\omega(q) > (1+\delta)\alpha(q)\log_2 x/\log D$. It follows that (i) is essentially optimal.

For completeness, we construct arbitrarily large classes of moduli $q \le (\log x)^{O(1)}$ which satisfy the last inequality above (with F still being the polynomial constructed in the previous paragraph). Let $K_D > 0$ be a constant depending only on D. Letting $Y := K_D \log_2 x$ and $q := \prod_{\substack{\ell \text{ prime} \\ D+1<\ell\le Y}} \ell$, the prime number theorem shows that $q \le (\log x)^{2K_D}$ and that $\omega(q) \ge Y/2\log Y$. On the other hand, the decomposition (2.3) shows that $\alpha(q) \ll \exp\left(-\sum_{\substack{\ell \text{ prime} \\ D+1<\ell\le Y}} \nu(\ell)/\ell\right) \ll 1/\log Y$, where the implied constant depends only on D. (Here we have used the Prime Ideal Theorem.) Hence, by fixing K_D large enough in terms of D, we have constructed arbitrarily large classes of moduli $q \le (\log x)^{O(1)}$ which all satisfy $\omega(q) > (1+\delta)\alpha(q)\log_2 x/\log D$.

To motivate (ii), fix $D \ge 2$, and let f be the completely multiplicative function given by $f(p) = (p-1)^D + 1$ for all primes p. Let q be a Dth power, say $q = q_1^D$. Then $f(p) \equiv 1 \pmod q$ whenever $p \equiv 1 \pmod{q_1}$. Thus, if q is bounded by a

power of $\log x$, there will be $\gg x/\varphi(q_1)\log x$ primes $p \le x$ for which $f(p) \equiv 1 \pmod q$. On the other hand, if we assume all primes dividing q_1 exceed $D+1$, Proposition 2.2.1 implies that there are $x/(\log x)^{1-(1+o(1))\alpha(q)}$ integers $n \le x$ with $\gcd(f(n), q) = 1$. It follows that the residue class 1 mod q will be overrepresented if $q^{1-1/D} = q/q_1 > (\log x)^{(1+\delta)\alpha(q)}$. This means that for weak equidistribution we require q to be no more than $\approx (\log x)^{\alpha(q)(1-1/D)^{-1}}$. So (ii) is essentially best possible as well.

In both of the constructions described above, the obstruction to uniformity came from prime inputs p. Tweaking the construction slightly, we could easily produce obstructions to uniformity of the form rp, with r fixed (or even with r growing slowly with x). In our final theorem, we pinpoint the 'problem' here as one of having too few large prime factors. Specifically, we show that uniformity up to an arbitrary power of $\log x$ can be restored by considering only inputs with sufficiently many prime factors exceeding q. In fact, for squarefree moduli q, it suffices to restrict to inputs with composite q-rough part.

Theorem 2.1.3. *Let f be a fixed, polynomially-defined function. There is a constant $C(F)$ such that the following hold.*

(a) For each fixed $K_0 > 0$,

$$\begin{aligned}&\#\{n \le x : P_{D+2}(n) > q,\ f(n) \equiv a \pmod q\} \\ &\qquad \sim \frac{1}{\varphi(q)}\#\{n \le x : P_{D+2}(n) > q,\ \gcd(f(n), q) = 1\} \qquad \text{as } x \to \infty, \quad (2.5)\end{aligned}$$

uniformly for coprime residue classes $a \bmod q$ with $q \le (\log x)^{K_0}$ and q divisible only by primes exceeding $C(F)$.

(b) For each fixed $K_0 > 0$,

$$\#\{n \le x : P_2(n) > q,\ f(n) \equiv a \pmod q\} \sim \frac{1}{\varphi(q)} \#\{n \le x : P_2(n) > q,\ \gcd(f(n), q) = 1\} \quad \text{as } x \to \infty,$$

uniformly for coprime residue classes $a \bmod q$ with q squarefree, $q \le (\log x)^{K_0}$, and q divisible only by primes exceeding $C(F)$.

The methods used to prove the aforementioned theorems refines that used to obtain the earlier results Theorems 1.4.6 and 1.4.7. The essential new ingredient, which allows us to dispense with the primality or "almost primality" conditions in those theorems, is the exploitation of a certain ergodic (or mixing) phenomenon within the multiplicative group mod q. As one illustration: Let q be a positive integer coprime to 6. From the collection of units u mod q for which $u + 1$ is also a unit, choose uniformly at random $u_1, u_2, u_3, \ldots$, and construct the products $u_1, u_1u_2, u_1u_2u_3, \ldots$. Once J is large, each unit mod q is roughly equally likely to appear as $u_1 \cdots u_J$. This particular example plays a starring role in our approach to the weak equidistribution of Euler's φ-function.

When $f = \varphi$, Theorem 2.1.1 is in the spirit of the Siegel–Walfisz theorem, with primes replaced by values of $\varphi(n)$. For investigations of the corresponding 'Linnik's theorem', concerning the least n for which $\varphi(n)$ falls into a given progression, see [13, 25, 26, 27].

Finally, it is worth mentioning that although in the spirit of Narkiewicz's results, we stated Theorems 2.1.1, 2.1.2 and 2.1.3 for $F(T) \in \mathbb{Z}[T]$, our methods go through (with minor modifications) for integer-valued polynomials F, namely those satisfying $F(\mathbb{Z}) \subset \mathbb{Z}$. Writing any such polynomial in the form $G(T)/Q$ for some positive

integer Q and $G(T) \in \mathbb{Z}[T]$, we need only ensure in addition that the constant $C(F)$ appearing in the aforementioned theorems exceeds Q.

Section 2.2

A preparatory estimate: The frequency with which $(f(n), q) = 1$

The following proposition is contained in results of Scourfield [68]. Nevertheless, we give a complete treatment here because the results of [68] are much more precise than we will need. The weaker version below admits a simpler and shorter proof (although we make no claim to originality regarding the underlying ideas).

For readability, we sometimes abbreviate $\alpha(q)$ to α, suppressing dependence on q.

Proposition 2.2.1. *Fix a multiplicative function f with the property that $f(p) = F(p)$ for all primes p, where $F(T) \in \mathbb{Z}[T]$ is nonconstant. Fix $K_0 > 0$. If x is sufficiently large and $q \le (\log x)^{K_0}$ with $\alpha = \alpha(q) > 0$, then*

$$\#\{n \le x : (f(n), q) = 1\} = \frac{x}{(\log x)^{1-\alpha}} \exp(O((\log\log(3q))^{O(1)})). \tag{2.6}$$

We treat separately the implicit upper and lower bounds in Proposition 2.2.1.

Upper bound

The following mean value estimate is a simple consequence of [32, Theorem 01, p. 2] (and also of the more complicated Theorem 03 from that same chapter).

Lemma 2.2.2. *Let g be a multiplicative function with $0 \le g(n) \le 1$ for all n. For*

all $x \geq 3$,

$$\sum_{n \leq x} g(n) \ll \frac{x}{\log x} \exp\left(\sum_{p \leq x} \frac{g(p)}{p}\right).$$

Here the implied constant is absolute.

If we set $g(n) := \mathbb{1}_{\gcd(f(n),q)=1}$, then the left-hand side of (2.6) is precisely $\sum_{n \leq x} g(n)$. Note that the multiplicativity of f implies the multiplicativity of g. The following lemma, due independently to Norton [54, Lemma, p. 669] and Pomerance [62, Remark 1], allows us to estimate the sums of $g(p)/p$ appearing in Lemma 2.2.2.

Lemma 2.2.3. *Let q be a positive integer, and suppose x is a real number with $x \geq \max\{3, q\}$. For each coprime residue class $a \bmod q$,*

$$\sum_{\substack{p \leq x \\ p \equiv a \pmod q}} \frac{1}{p} = \frac{\log_2 x}{\varphi(q)} + \frac{1}{p_{q,a}} + O\left(\frac{\log(3q)}{\varphi(q)}\right),$$

where $p_{q,a}$ denotes the least prime congruent to a modulo q.

Lemma 2.2.4. *Let $F(T) \in \mathbb{Z}[T]$ be a fixed nonconstant polynomial. For each positive integer q and each real number $x \geq 3q$,*

$$\sum_{p \leq x} \frac{\mathbb{1}_{\gcd(F(p),q)=1}}{p} = \alpha \log_2 x + O((\log\log(3q))^{O(1)}),$$

where $\alpha = \alpha(q)$ is as defined in (2.2).

Proof. Using the Möbius function to detect the coprimality condition, we write

$$\sum_{\substack{p \leq x \\ \gcd(F(p),q)=1}} \frac{1}{p} = \sum_{\substack{3q < p \leq x \\ \gcd(F(p),q)=1}} \frac{1}{p} + O(\log_2(100q))$$

$$= \sum_{d|q} \mu(d) \sum_{\substack{3q<p\le x \\ d|F(p)}} \frac{1}{p} + O(\log_2(100q)). \tag{2.7}$$

If p is a prime with $p > 3q$, then $d \mid F(p)$ precisely when p belongs to one of $\nu(d)$ coprime residue classes modulo d. By Lemma 2.2.3 (with d replacing q),

$$\sum_{\substack{3q<p\le x \\ d|F(p)}} \frac{1}{p} = \frac{\nu(d)}{\varphi(d)} \log\log x + O\left(\frac{\nu(d)\log(3d)}{\varphi(d)} + \frac{\nu(d)\log_2(3q)}{\varphi(d)}\right).$$

Substituting this estimate into (2.7) yields a main term of $(\sum_{d|q} \frac{\mu(d)\nu(d)}{\varphi(d)}) \log_2 x = \alpha \log_2 x$, as desired. Turning to the errors,

$$\begin{aligned}
\sum_{\substack{d|q \\ d \text{ squarefree}}} \frac{\nu(d)\log(3d)}{\varphi(d)} &= \sum_{\substack{d|q \\ d \text{ squarefree}}} \frac{\nu(d)}{\varphi(d)} (\log 3 + \sum_{\ell|d} \log(\ell)) \\
&\le (\log 3) \sum_{\substack{d|q \\ d \text{ squarefree}}} \frac{\nu(d)}{\varphi(d)} + \sum_{\ell|q} \log \ell \cdot \frac{\nu(\ell)}{\ell - 1} \sum_{\substack{r|q/\ell \\ r \text{ squarefree}}} \frac{\nu(r)}{\varphi(r)} \\
&\ll \left(\sum_{\substack{d|q \\ d \text{ squarefree}}} \frac{\nu(d)}{\varphi(d)} \right) \left(1 + \sum_{\ell|q} \log \ell \cdot \frac{\nu(\ell)}{\ell - 1} \right).
\end{aligned}$$

Now $\sum_{d|q,\ d \text{ squarefree}} \frac{\nu(d)}{\varphi(d)} = \prod_{\ell|q}(1 + \nu(\ell)/(\ell - 1)) \ll (\log_2(3q))^D$ (keeping in mind that $\nu(\ell) \le D$ for all but $O(1)$ many primes ℓ). Furthermore,

$$\begin{aligned}
\sum_{\ell|q} \nu(\ell) \frac{\log \ell}{\ell - 1} \ll \sum_{\ell|q} \frac{\log \ell}{\ell} &\le \sum_{\ell \le \log(3q)} \frac{\log \ell}{\ell} + \sum_{\substack{\ell|q \\ \ell > \log(3q)}} \frac{\log \ell}{\ell} \\
&\ll \log_2(3q) + \frac{\log_2(3q)}{\log(3q)} \sum_{\substack{\ell|q \\ \ell > \log(3q)}} 1,
\end{aligned}$$

and this is

$$\ll \log_2(3q) + \frac{\log_2(3q)}{\log(3q)} \cdot \frac{\log q}{\log_2(3q)} \ll \log_2(3q).$$

Thus, $\sum_{d|q,\ d \text{ squarefree}} \frac{\nu(d)\log(3d)}{\varphi(d)} \ll (\log_2(3q))^{D+1}$. Finally,

$$\sum_{\substack{d|q \\ d \text{ squarefree}}} \frac{\nu(d)\log_2(3q)}{\varphi(d)} \ll \log_2(3q) \cdot \prod_{\ell|q} \left(1 + \frac{\nu(\ell)}{\ell - 1}\right) \ll (\log_2(3q))^{D+1}.$$

Collecting estimates, $\sum_{p \le x} \mathbb{1}_{\gcd(F(p),q)=1}/p = \alpha \log_2 x + O((\log_2(3q))^{D+1})$. □

The upper bound half of Proposition 2.2.1 follows (in slightly more precise form) immediately from Lemmas 2.2.2 and 2.2.4. In fact, we have shown the upper bound in the much wider range $q \le x/3$.

Lower bound

The following lemma is due to Barban [8, Lemma 3.5]; see also [67, Theorem 3.5, p. 61].

Lemma 2.2.5. *Let g be a multiplicative function with $0 \le g(n) \le 1$ for all n. For all $x \ge 3$,*

$$\sum_{\substack{n \le x \\ n \text{ squarefree}}} \frac{g(n)}{n} \gg \exp\left(\sum_{p \le x} \frac{g(p)}{p}\right).$$

Here the implied constant is absolute.

Proof of the lower bound in Proposition 2.2.1. Consider n of the form mP, where $m \le x^{1/3}$ is a squarefree product of primes p with $\gcd(f(p), q) = 1$ and $P \in (x^{1/2}, x/m]$ is a prime with $(f(P), q) = 1$. Each such n has $f(n) = f(m)f(P)$ coprime to q.

Given m as above, we count corresponding P. The prime P is restricted to one of the $\alpha(q)\varphi(q)$ residue classes a mod q with $\gcd(aF(a), q) = 1$. Hence, given $m \le x^{1/3}$ as

above, the Siegel–Walfisz theorem guarantees that there are

$$\gg (\alpha(q)\varphi(q)) \cdot \frac{1}{\varphi(q)} \frac{x}{m \log x} = \alpha(q) \frac{x}{m \log x}$$

values of P. Now sum on m; by Lemma 2.2.5,

$$\sum \frac{1}{m} = \sum_{\substack{m \le x^{1/3} \\ m \text{ squarefree}}} \frac{\mathbb{1}_{\gcd(f(m),q)=1}}{m} \gg \exp\left(\sum_{p \le x^{1/3}} \frac{\mathbb{1}_{\gcd(f(p),q)=1}}{p} \right).$$

The final sum on p is within $O(1)$ of the corresponding sum taken over all $p \le x$. The lower bound half of Proposition 2.2.1 now follows from Lemma 2.2.4, bearing in mind that $\alpha(q) \gg (\log\log(3q))^{-D}$. □

Section 2.3

Framework for the proof of Theorems 2.1.2 and 2.1.3

Define $J = J(x)$ by setting

$$J = \lfloor \log\log\log x \rfloor.$$

(For our purposes, any integer-valued function tending to infinity sufficiently slowly would suffice.) With δ from the statement of Theorem 2.1.2, we let $y = y(x)$ be defined by

$$y := \exp((\log x)^{\delta/2})$$

and we say that the positive integer n is convenient (with respect to a given large real number x) if (a) $n \le x$, (b) the J largest prime factors of n exceed y, and (c) none of these J primes are repeated in n. That is, n is convenient if n admits an expression

$n = mP_J \cdots P_1$, where $P_1, \dots, P_J$ are primes with

$$\max\{P(m), y\} < P_J < \cdots < P_1, \tag{2.8}$$

$$P_J \cdots P_1 \le x/m. \tag{2.9}$$

The framework developed in this section will go through in the proof of Theorem 2.1.3 (§2.6) by setting $\delta := 1$.

Now let f be a fixed multiplicative function with $f(p) = F(p)$ for all primes p, where $F(T) \in \mathbb{Z}[T]$ is nonconstant. Fix $K_0 > 0$, and suppose that $q \le (\log x)^{K_0}$. We set

$$N(q) = \#\{n \le x : \gcd(f(n), q) = 1\},$$

and we define $N_{\mathrm{con}}(q)$ and $N_{\mathrm{inc}}(q)$ analogously, incorporating the extra requirement that n be convenient or inconvenient, respectively.

We will repeatedly use the following standard estimate on the count of smooth numbers. The result below is a consequence of the Corollary on p. 15 of [10], but see [76, Theorem 5.13 and Corollary 5.19, Chapter III.5] for more concrete results.

Lemma 2.3.1. *Suppose $X \ge Y \ge 3$, and let $u := \frac{\log X}{\log Y}$. Whenever $u \to \infty$ and $X \ge Y \ge (\log X)^2$, we have*

$$\psi(X, Y) = X \exp(-(1 + o(1))u \log u).$$

Lemma 2.3.2. *$N(q) \sim N_{con}(q)$, as $x \to \infty$. Here the asymptotic holds uniformly in q with $q \le (\log x)^{K_0}$ and $\alpha(q) \ne 0$.*

Proof. We must show that $N_{\mathrm{inc}}(q) = o(N(q))$, as $x \to \infty$.

Suppose the integer $n \le x$ is counted by $N_{\mathrm{inc}}(q)$. We can assume that $P(n) > z := x^{1/\log_2 x}$. Indeed, by Lemma 2.3.1, the number of $n \le x$ with $P(n) \le z$ is at most $x/(\log x)^{(1+o(1))\log_3 x}$ and this is $o(N(q))$ by our 'rough-and-ready' estimate of Proposition 2.2.1. We can similarly assume that n has no repeated prime factors exceeding y, since the number of exceptions is $O(x/y)$, which is again $o(N(q))$.

Write $n = PAB$, where $P = P(n)$ and A is the largest divisor of n/P supported on primes exceeding y. Thus $P > z$ and $P(B) \le y < P^-(A)$. Observe that $AB = n/P \le x/z$. So if A and B are given, the number of possibilities for P is bounded by $\pi(x/AB) \ll x/AB\log z \ll x(\log\log x)/AB\log x$. We sum on A, B. As n has no repeated primes exceeding y but n is inconvenient, it must be that $\Omega(A) < J$. Thus, $\sum 1/A \le (1+\sum_{p\le x} 1/p)^J \le (2\log_2 x)^J \le \exp(O((\log_3 x)^2))$. Using that $(f(B), q) = 1$ (as $f(n) = f(B)f(AP)$) and that B is y-smooth,

$$\sum \frac{1}{B} \le \prod_{p\le y}\left(\sum_{j=0}^{\infty}\frac{\mathbb{1}_{(f(p^j),q)=1}}{p^j}\right) \ll \exp\left(\sum_{p\le y}\frac{\mathbb{1}_{(f(p),q)=1}}{p}\right),$$

and this is $\ll (\log x)^{\alpha\delta/2}\exp(O((\log_2 q)^{O(1)}))$ by Lemma 2.2.4. We conclude that these n make a contribution to $N_{\mathrm{inc}}(q)$ of size at most $\frac{x}{(\log x)^{1-\alpha\delta/2}}\exp(O((\log_3 x)^2 + (\log_2 q)^{O(1)}))$. Since $q \le (\log x)^{K_0}$ and $\alpha(q)$ obeys the lower bound (2.4), this contribution is also $o(N(q))$. □

Let $N(q,a)$ denote the number of $n \le x$ with $f(n) \equiv a \pmod q$, and define $N_{\mathrm{con}}(q,a)$ and $N_{\mathrm{inc}}(q,a)$ analogously. By Lemma 2.3.2, the weak equidistribution of f mod q will follow if $N(q,a) \sim \frac{1}{\varphi(q)}N_{\mathrm{con}}(q)$.

As a first step in this direction, we compare $N_{\text{con}}(q)$ and $N_{\text{con}}(q,a)$. Clearly,

$$N_{\text{con}}(q) = \sum_{\substack{m\le x\\ \gcd(f(m),q)=1}} \sideset{}{'}\sum_{P_1,\dots,P_J} 1,$$

where the $'$ on the sum indicates that $P_1,\dots,P_J$ run through primes satisfying (2.8), (2.9), and

$$\gcd(f(P_1)\cdots f(P_J),q)=1. \tag{2.10}$$

Similarly,

$$N_{\text{con}}(q,a) = \sum_{\substack{m\le x\\ \gcd(f(m),q)=1}} \sideset{}{''}\sum_{P_1,\dots,P_J} 1,$$

where the $''$ condition indicates that we enforce (2.8), (2.9) and (in place of (2.10))

$$f(m)f(P_1)f(P_2)\cdots f(P_J)\equiv a \pmod q. \tag{2.11}$$

Let

$$\mathcal{V}'_q = \{(v_1,\dots,v_J) \bmod q : \gcd(v_1\dots v_J,q)=1, \gcd(F(v_1)\cdots F(v_J),q)=1\}$$

and

$$\mathcal{V}''_{q,a,m} = \{(v_1,\dots,v_J) \bmod q : \gcd(v_1\dots v_J,q)=1, f(m)F(v_1)\cdots F(v_J)\equiv a \pmod q\}.$$

Then (2.10) amounts to restricting $(P_1,\dots,P_J)$, taken mod q, to belong to $\mathcal{V}'_q$, while (2.11) restricts this same tuple to $\mathcal{V}''_{q,a,m}$. By (2.2), $\#\mathcal{V}'_q = (\varphi(q)\alpha(q))^J$.

The conditions (2.9) and (2.10) are independent of the ordering of $P_1,\dots,P_J$. Thus,

letting $L_m = \max\{y, P(m)\}$,

$$\sum_{P_1,\dots,P_J}{}' 1 = \frac{1}{J!} \sum_{\mathbf{v}\in\mathcal{V}_q'} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} 1. \tag{2.12}$$

We proceed to remove the congruence conditions on the P_j from the inner sum. For each tuple $(v_1,\dots,v_J) \bmod q \in \mathcal{V}_q'$,

$$\sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} 1 = \sum_{\substack{P_2,\dots,P_J \text{ distinct} \\ P_2\cdots P_J \le x/mL_m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} \sum_{\substack{P_1 \ne P_2,\dots,P_J \\ L_m < P_1 \le x/mP_2\cdots P_J \\ P_1 \equiv v_1 \pmod q}} 1.$$

Since $L_m \ge y$ and $q \le (\log x)^{K_0} = (\log y)^{2K_0/\delta}$, the Siegel–Walfisz theorem implies that

$$\sum_{\substack{P_1 \ne P_2,\dots,P_J \\ L_m < P_1 \le x/mP_2\cdots P_J \\ P_1 \equiv v_1 \pmod q}} 1 = \frac{1}{\varphi(q)} \sum_{\substack{P_1 \ne P_2,\dots,P_J \\ L_m < P_1 \le x/mP_2\cdots P_J}} 1 + O\left(\frac{x}{mP_2\cdots P_J} \exp(-C_0\sqrt{\log y})\right),$$

for some positive constant $C_0 := C_0(K_0,\delta)$ depending only on K_0 and δ. Putting this back into the last display and bounding the O-terms crudely, we find that

$$\sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} 1 = \frac{1}{\varphi(q)} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m \\ (\forall j \ge 2)\ P_j \equiv v_j \pmod q}} 1 + O\left(\frac{x}{m}\exp\left(-\frac{1}{2}C_0(\log x)^{\delta/4}\right)\right).$$

Proceeding in the same way to remove the congruence conditions on $P_2,\dots,P_J$, we

arrive at the estimate

$$\sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J\le x/m \\ \text{each } P_j>L_m \\ \text{each } P_j\equiv v_j \pmod q}} 1 = \frac{1}{\varphi(q)^J} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J\le x/m \\ \text{each } P_j>L_m}} 1 + O\left(\frac{x}{m}\exp\left(-\frac{1}{4}C_0(\log x)^{\delta/4}\right)\right). \quad (2.13)$$

Inserting this estimate into (2.12) and keeping in mind that $\#\mathcal{V}_q' \le (\log x)^{K_0 J}$ (trivially), we conclude that

$$\begin{aligned} N_{\mathrm{con}}(q) &= \sum_{\substack{m\le x \\ \gcd(f(m),q)=1}} {\sum_{P_1,\dots,P_J}}' 1 \\ &= \sum_{\substack{m\le x \\ \gcd(f(m),q)=1}} \frac{\#\mathcal{V}_q'}{\varphi(q)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J\le x/m \\ \text{each } P_j>L_m}} 1\right) + O\left(x\exp\left(-\frac{1}{8}C_0(\log x)^{\delta/4}\right)\right). \end{aligned} \quad (2.14)$$

An entirely analogous argument yields the same estimate with $N_{\mathrm{con}}(q)$ replaced by $N_{\mathrm{con}}(q,a)$ and $\mathcal{V}_q'$ replaced by $\mathcal{V}_{q,a,m}''$. Comparing (2.14) with its $N_{\mathrm{con}}(q,a)$ analogue and rewriting

$$\frac{\#\mathcal{V}_{q,a,m}''}{\varphi(q)^J} = \frac{\#\mathcal{V}_{q,a,m}''}{\#\mathcal{V}_q'}\cdot\frac{\#\mathcal{V}_q'}{\varphi(q)^J},$$

we are motivated to introduce the following hypothesis.

Hypothesis A. $\frac{\#\mathcal{V}_{q,a,m}''}{\#\mathcal{V}_q'} \sim \frac{1}{\varphi(q)}$, *as* $x\to\infty$, *uniformly in* q *and* a *and uniformly in* $m\le x$ *with* $\gcd(f(m),q)=1$.

We will soon see how to verify Hypothesis A in the situations described in Theorems 2.1.1, 2.1.2, and 2.1.3. The phrase "uniformly in q and a" in Hypothesis A should be read as "uniformly in q and a subject to the restrictions of these theorem statements".

If Hypothesis A holds, we may deduce (keeping in mind Lemma 2.3.2, and that $x\exp(-\frac{1}{8}C_0(\log x)^{\delta/4}) = o(N(q)/\varphi(q))$)

$$\begin{aligned} N_{\mathrm{con}}(q,a) &= \sum_{\substack{m\le x\\ \gcd(f(m),q)=1}} \sideset{}{''}\sum_{P_1,\dots,P_J} 1 \\ &= (1+o(1))\frac{1}{\varphi(q)}N_{\mathrm{con}}(q) + o\left(\frac{N(q)}{\varphi(q)}\right) = (1+o(1))\frac{1}{\varphi(q)}N(q). \end{aligned}$$

Since $N(q,a) = N_{\mathrm{con}}(q,a) + N_{\mathrm{inc}}(q,a)$, weak uniform distribution mod q will follow if the contribution from $N_{\mathrm{inc}}(q,a)$ is shown to be negligible. We record this condition as our next Hypothesis.

Hypothesis B. *$N_{\mathrm{inc}}(q,a) = o(N(q)/\varphi(q))$, as $x\to\infty$, uniformly in q and a.*

Section 2.4

Linearly defined functions: Proof of Theorem 2.1.1

We proceed to verify Hypotheses A and B.

Verification of Hypothesis A. Let $m \le x$ with $\gcd(f(m),q) = 1$, and let $w \in \mathbb{Z}$ be a value of $af(m)^{-1}$ modulo q. We will estimate $\#\mathcal{V}''_{q,a,m}$ via the product formula $\#\mathcal{V}''_{q,a,m} = \prod_{\ell^e\|q} V''_{\ell^e}$, where

$$V''_{\ell^e} := \#\{(v_1,\dots,v_J) \bmod \ell^e : \gcd(v_1\dots v_J,\ell) = 1,\ \prod_{i=1}^{J}(Rv_i+S) \equiv w \pmod{\ell^e}\}.$$

By assumption, $(\ell, 6R) = 1$ for all $\ell \mid q$.

Suppose first that $\ell \mid S$. Then the condition $\gcd(v_1\dots v_J,\ell) = 1$ is implied by

$\prod_{i=1}^{J}(Rv_i+S)\equiv w \pmod{\ell^e}$. Noting that the map $v\mapsto Rv+S$ is a permutation of $\mathbb{Z}/\ell^e\mathbb{Z}$, we see that $V''_{\ell^e}=\varphi(\ell^e)^{J-1}$ and

$$\varphi(\ell^e)V''_{\ell^e}=\varphi(\ell^e)^J. \tag{2.15}$$

When $\ell\nmid S$, we must work somewhat harder. By inclusion-exclusion,

$$V''_{\ell^e}=\sum_{j=0}^{J}(-1)^j\binom{J}{j}V''_{\ell^e,j}, \tag{2.16}$$

where

$$V''_{\ell^e,j}=\#\{(v_1,\dots,v_J) \bmod \ell^e : \ell\mid v_1,v_2,\dots,v_j,\ \prod_{i=1}^{J}(Rv_i+S)\equiv w \pmod{\ell^e}\}.$$

If $0\le j<J$, then $V''_{\ell^e,j}=(\ell^{e-1})^j\varphi(\ell^e)^{J-j-1}$: Each of $v_1,\dots,v_j$ can be chosen arbitrarily from the ℓ^{e-1} classes divisible by ℓ, while $v_{j+1},\dots,v_{J-1}$ can be chosen arbitrarily subject to each of Rv_i+S (for $i=j+1,\dots,J-1$) being a unit mod ℓ^e; this then determines v_J. Similarly, $V''_{\ell^e,J}=O((\ell^{e-1})^{J-1})$. Referring back to (2.16),

$$\begin{aligned}\varphi(\ell^e)V''_{\ell^e}&=(\varphi(\ell^e)-\ell^{e-1})^J+O(\ell^e(\ell^{e-1})^{J-1})\\&=(\ell^e(1-2/\ell))^J\left(1+O(\ell(\ell-2)^{-J})\right).\end{aligned} \tag{2.17}$$

By (2.15) and (2.17), in either case for ℓ we have

$$\varphi(\ell^e)V''_{\ell^e}=\left(\varphi(\ell^e)\left(1-\frac{\nu(\ell)}{\ell-1}\right)\right)^J\cdot\left(1+O(\ell(\ell-2)^{-J})\right).$$

Multiplying over ℓ,

$$\varphi(q)\#\mathcal{V}''_{q,a,m} = (\varphi(q)\alpha(q))^J \prod_{\ell^e \| q} \left(1 + O(\ell(\ell-2)^{-J})\right) = \#\mathcal{V}'_q \prod_{\ell^e \| q} \left(1 + O(\ell(\ell-2)^{-J})\right).$$

So to verify Hypothesis A, it is enough to show that the final product is $1 + o(1)$. This follows if $\sum_{\ell^e \| q} \ell(\ell-2)^{-J} = o(1)$, which is straightforward to prove: Since q is coprime to 6, we have for all large x that

$$\sum_{\ell^e \| q} \ell(\ell-2)^{-J} < \sum_{\ell \geq 5} \ell(\ell-2)^{-J} \leq 3^{-J/2} \sum_{\ell \geq 5} \ell(\ell-2)^{-J/2} \leq 3^{-J/2} \sum_{\ell \geq 5} \ell(\ell-2)^{-3} \ll 3^{-J/2}.$$

□

Remark 2.4.1. *It is also possible to estimate V''_{ℓ^e} via character sums, which will be our primary tool for general $F(T) \in \mathbb{Z}[T]$. By orthogonality (as in* (2.18) *below), $\varphi(\ell^e)V''_{\ell^e} = \sum_{\chi \bmod \ell^e} \bar{\chi}(w) Z_\chi^J$, where*

$$\begin{aligned} Z_\chi :&= \sum_{v \bmod \ell^e} \chi_0(v)\chi(Rv+S) \\ &= \sum_{u \bmod \ell^e} \chi(u) - \sum_{\substack{u \bmod \ell^e \\ u \equiv S \bmod \ell}} \chi(u); \end{aligned}$$

here we have used that as v runs over coprime residues mod ℓ^e, the expression $Rv+S$ runs over all the residues mod ℓ^e except for those congruent to S mod ℓ. If $\ell \mid S$, it is then immediate that $Z_\chi = \mathbb{1}_{\chi=\chi_0}\varphi(\ell^e)$ (with χ_0 denoting the principal character mod ℓ^e), once again giving us $\varphi(\ell^e)V''_{\ell^e} = \varphi(\ell^e)^J$. On the other hand, if $\ell \nmid S$, then fixing a generator g mod ℓ^e and considering the unique $r \in \{0, 1, \ldots, \varphi(\ell^e) - 1\}$ satisfying $g^r \equiv S \pmod{\ell^e}$, we observe that the sets $\{u \bmod \ell^e : u \equiv S \bmod \ell\}$ and

$\{g^{r+(\ell-1)k} \bmod \ell^e : 0 \le k < \ell^{e-1}\}$ *are equal. Hence,*

$$\sum_{\substack{u \bmod \ell^e \\ u \equiv S \bmod \ell}} \chi(u) = \mathbb{1}_{\chi^{\ell-1}=\chi_0} \chi(S) \ell^{e-1}.$$

As such, $Z_\chi = \mathbb{1}_{\chi=\chi_0} \ell^{e-1}(\ell-2) + O(\mathbb{1}_{\chi^{\ell-1}=\chi_0,\ \chi\neq\chi_0} \ell^{e-1})$*, which again leads to (2.17) since there are* $\ell - 2$ *nontrivial characters* χ *mod* ℓ^e *satisfying* $\chi^{\ell-1} = \chi_0$*.*

Verification of Hypothesis B. We proceed as in the proof of Lemma 2.3.2. Let $n \le x$ be an inconvenient solution to $f(n) \equiv a \pmod q$. We can assume $P(n) > z = x^{1/\log_2 x}$, since the number of exceptional $n \le x$ is $o(N(q)/\varphi(q))$. Similarly, we can assume that n has no repeated prime factors exceeding $y = \exp((\log x)^{\delta/2})$. Write $n = PAB$, where $P := P(n)$ and A is the largest divisor of n/P supported on primes exceeding y. Then $z < P \le x/AB$ and $(RP+S)f(AB) \equiv a \pmod q$. Given A and B, this congruence is satisfied for P belonging to at most one coprime residue class mod q. So by the Brun–Titchmarsh inequality, given A and B there are $\ll x/\varphi(q)AB\log(z/q) \ll x\log_2 x/\varphi(q)AB\log x$ corresponding values of P. Note that we have saved a factor of $\varphi(q)$ here over the analogous estimate in Lemma 2.3.2. Summing on A, B, and making the same estimates as in the argument for Lemma 2.3.2, yields

$$N_{\mathrm{inc}}(q,a) \le \frac{x}{\varphi(q)(\log x)^{1-\alpha\delta/2}} \exp(O((\log_3 x)^2 + (\log_2 q)^{O(1)})),$$

and this is $o(N(q)/\varphi(q))$. □

Section 2.5

General polynomially defined functions: Proof of Theorem 2.1.2

To check Hypothesis A in the context of Theorem 2.1.2, we require the following character sum estimate, which follows from the Weil bounds when $e = 1$ and from work of Cochrane [14] (see also [15]) when $e > 1$. See [59, Proposition 2.6] for a detailed discussion.

Lemma 2.5.1. *Let $F_1(T), \dots, F_K(T) \in \mathbb{Z}[T]$ be nonconstant polynomials for which the product $F_1(T) \cdots F_K(T)$ has no multiple roots. Let ℓ be an odd prime not dividing the leading coefficient of any of the $F_k(T)$ and not dividing the discriminant of $F_1(T) \cdots F_K(T)$. Let e be a positive integer, and let $\chi_1, \dots, \chi_K$ be Dirichlet characters modulo ℓ^e, at least one of which is primitive. Then*

$$\left| \sum_{x \bmod \ell^e} \chi_1(F_1(x)) \cdots \chi_K(F_K(x)) \right| \leq (d-1)\ell^{e(1-1/d)},$$

where $d = \sum_{k=1}^{K} \deg F_k(T)$.

Let $\Delta(F)$ denote the discriminant of $F(T)$ if $F(0) = 0$ and the discriminant of $TF(T)$ if $F(0) \neq 0$. Throughout this section and the next, we assume that $C(F)$ is fixed so large that primes exceeding $C(F)$ are odd and divide neither the leading coefficient of F nor $\Delta(F)$. We also assume that $C(F) > (4D)^{2D+2}$ where $D = \deg F(T)$.

Verification of Hypothesis A. Suppose that $m \leq x$ has $\gcd(f(m), q) = 1$ and write w

for a value of $af(m)^{-1} \bmod q$. Then $\#\mathcal{V}''_{q,a,m} = \prod_{\ell^e \| q} V''_{\ell^e}$ and $\#\mathcal{V}'_q = \prod_{\ell^e \| q} V'_{\ell^e}$, where

$$V''_{\ell^e} := \#\{(v_1, \dots, v_J) \bmod \ell^e : \gcd(v_1 \dots v_J, \ell) = 1,\ \prod_{i=1}^{J} F(v_i) \equiv w \pmod{\ell^e}\}$$

and

$$V'_{\ell^e} := \#\{(v_1, \dots, v_J) \bmod \ell^e : \gcd(v_1 \dots v_J F(v_1) \cdots F(v_J), \ell) = 1\}.$$

With χ_0 denoting the principal Dirichlet character mod ℓ^e,

$$\varphi(\ell^e) V''_{\ell^e} = \sum_{\chi \bmod \ell^e} \bar{\chi}(w) \sum_{v_1,\dots,v_J \bmod \ell^e} \chi_0(v_1 \cdots v_J)\chi(F(v_1) \cdots F(v_J)) \tag{2.18}$$

$$= V'_{\ell^e} + \sum_{\substack{\chi \bmod \ell^e \\ \chi \neq \chi_0}} \bar{\chi}(w) Z_\chi^J, \tag{2.19}$$

where $Z_\chi := \sum_{v \bmod \ell^e} \chi_0(v)\chi(F(v))$. For each χ of conductor ℓ^{e_0} with $1 \le e_0 \le e$, Lemma 2.5.1 gives $|Z_\chi| = \ell^{e-e_0} |\sum_{x \bmod \ell^{e_0}} \chi_0(x)\chi(F(x))| \le D\ell^{(e-e_0)+e_0(1-1/(D+1))} = D\ell^{e-e_0/(D+1)}$. (If ℓ divides $F(0)$, then $\sum_{x \bmod \ell^{e_0}} \chi_0(x)\chi(F(x)) = \sum_{x \bmod \ell^{e_0}} \chi(F(x))$, and we apply Lemma 2.5.1 with $k = 1$ and $F_1(T) = F(T)$; otherwise we take $k = 2$, $F_1(T) = T$, and $F_2(T) = F(T)$.) As there are fewer than ℓ^{e_0} characters of conductor ℓ^{e_0},

$$\Big| \sum_{\substack{\chi \bmod \ell^e \\ \chi \neq \chi_0}} \bar{\chi}(w) Z_\chi^J \Big| \le \sum_{1 \le e_0 \le e} \ell^{e_0} (D\ell^{e-e_0/(D+1)})^J = D^J \ell^{eJ} \sum_{1 \le e_0 \le e} \ell^{e_0(1-J/(D+1))}.$$

Since $J \ge D+2$ once x is sufficiently large, each term in the sum $\sum_{1 \le e_0 \le e} \ell^{e_0(1-J/(D+1))}$ is smaller than half the previous, and $\sum_{1 \le e_0 \le e} \ell^{e_0(1-J/(D+1))} \le 2\ell^{1-J/(D+1)}$. Thus, $|\sum_{\substack{\chi \bmod \ell^e \\ \chi \neq \chi_0}} \bar{\chi}(w) Z_\chi^J| \le 2D^J \ell^{eJ} \ell^{1-J/(D+1)}$. Since $V'_{\ell^e} = (\varphi(\ell^e)\alpha(\ell^e))^J$, we conclude from (2.19) that

$$\varphi(\ell^e) V''_{\ell^e} = V'_{\ell^e}(1 + R_\ell), \tag{2.20}$$

where

$$|R_\ell| \le 2D^J \left(\frac{\ell^e}{\varphi(\ell^e)}\alpha(\ell^e)^{-1}\right)^J \ell^{1-J/(D+1)} \le 2(4D)^J \ell^{1-J/(D+1)}.$$

(We use here that $\ell^e/\varphi(\ell^e), \alpha(\ell^e)^{-1} \le 2$.) Multiplying over ℓ in (2.20), we see that Hypothesis A will follow if $(4D)^J \sum_{\ell|q} \ell^{1-J/(D+1)} = o(1)$. To check this last inequality, observe that when x is large,

$$\begin{aligned}(4D)^J \sum_{\ell|q} \ell^{1-J/(D+1)} &\le (4D)^J C(F)^{-J/(2D+2)} \sum_{\ell|q} \ell^{1-J/(2D+2)} \\ &\le (4D/C(F)^{1/(2D+2)})^J \sum_{\ell} \ell^{-2} < 2(4D/C(F)^{1/(2D+2)})^J;\end{aligned}$$

this last quantity tends to 0 since $C(F) > (4D)^{2D+2}$ and $J \to \infty$. □

Verification of Hypothesis B. We follow the arguments for the corresponding step in §2.4. Let $\xi(q)$ be the maximum number of roots v mod q of any congruence $F(v) \equiv a \pmod q$, where the maximum is over all residue classes a mod q. Then there are at most $\xi(q)$ possibilities for the residue class of P modulo q and our previous arguments yield

$$\begin{aligned}N_{\text{inc}}(q,a) &\le \xi(q)\frac{x}{\varphi(q)(\log x)^{1-\alpha\delta/2}} \exp(O((\log_3 x)^2 + (\log_2 q)^{O(1)})) \\ &< \xi(q)\frac{x}{\varphi(q)(\log x)^{1-2\alpha\delta/3}}.\end{aligned}$$

This last quantity is certainly $o(N(q)/\varphi(q))$ as long as $\xi(q) \ll (\log x)^{(1-\delta)\alpha}$ (say). By the choice of $C(F)$, we have $\xi(q) \le D^{\omega(q)}$ for squarefree q, verifying Hypothesis B for squarefree q having $\omega(q) \le (1-\delta)\alpha \log_2 x/\log D$. On the other hand, by a result of Konyagin (see Lemma 2.5.2 below), each congruence $F(v) \equiv a \pmod q$ has $O(q^{1-1/D})$ roots modulo q. Consequently, Hypothesis B also holds true for $q \le (\log x)^{\alpha(1-\delta)(1-1/D)^{-1}}$, completing the proof of Theorem 2.1.2. □

For completeness, we state the result of Konyagin (see [35, 36]) that we used above.

Lemma 2.5.2. *Fix a nonconstant polynomial* $W(T) = \sum_{j=0}^{D} a_j T^j \in \mathbb{Z}[T]$. *Then uniformly in integers* q *satisfying* $\gcd(q, a_0, \dots, a_D) = 1$, *we have* $\#\{u \in \mathbb{Z}/q\mathbb{Z} : W(u) \equiv 0 \pmod q\} \ll_D q^{1-1/D}$.

In the proof above, we have applied Lemma 2.5.2 with $W(T)$ being the fixed polynomial $F(T)$, and with the aforementioned gcd condition being satisfied automatically thanks to having $P^-(q) > C(F)$ in Theorem 2.1.2.

Section 2.6

Equidistribution along inputs with several prime factors exceeding q: Proof of Theorem 2.1.3

Proof of (a). Recall that for the purposes of Theorem 2.1.3, we take $\delta := 1$ and $y = \exp((\log x)^{1/2})$ in the framework developed in section 2.3. Lemma 2.3.2 still applies to show that $N(q) \sim N_{\mathrm{con}}(q)$ as $x \to \infty$, uniformly in $q \le (\log x)^{K_0}$ having $\alpha(q) \neq 0$. In particular, if $P_{D+2}(n) \le q$, then $P_J(n) < q \le y$ (once x is large); thus n is inconvenient, placing it in a set of size $o(N(q))$. It follows that the right-hand side of (2.5) is $\sim N(q)/\varphi(q)$, and our task is that of showing the same for the left-hand side. The proof of Hypothesis A in §2.5 gives $N_{\mathrm{con}}(q, a) \sim N(q)/\varphi(q)$. It remains only to show that there are $o(N(q)/\varphi(q))$ inconvenient n with $P_{D+2}(n) > q$ and $f(n) \equiv a \pmod q$.

As usual, we can assume $P(n) > z := x^{1/\log_2 x}$ and that n has no repeated prime factor exceeding $y = \exp(\sqrt{\log x})$. Since n is inconvenient, we must have $P_J(n) \le y$. We suppose first that one of the largest $D+2$ primes in n is repeated. Write $n = PSm$, where $P = P(n)$, S is the largest squarefull divisor of n/P; hence, $Sm \le x/z$

and $S > q^2$. Given S and m, there are fewer than $\pi(x/Sm) \ll x \log_2 x/Sm \log x$ possibilities for P. Summing on squarefull $S > q^2$ bounds the number of n, given m, as $\ll x \log_2 x/qm \log x$. To handle the sum on m, write $m = AB$, where A is the largest divisor of m composed of primes exceeding y. Then $\Omega(A) < J$, while B is y-smooth with $\gcd(f(B), q) = 1$. Bounding $\sum 1/A$ and $\sum 1/B$ as in the proof of Lemma 2.3.2, we deduce that $\sum 1/m \le (\log x)^{\frac{1}{2}\alpha} \exp((\log_3 x)^{O(1)})$. Putting it all together, we see that the number of n in this case is at most $\frac{x}{q(\log x)^{1-\frac{1}{2}\alpha}} \exp((\log_3 x)^{O(1)})$, which is $o(N(q)/\varphi(q))$.

We now suppose that each $P_i := P_i(n)$ appears to the first power in n, for $i = 1, 2, \dots, D+2$, and we write $n = P_1 \cdots P_{D+2} m$. Since $f(n) \equiv a \pmod q$, it must be that $\gcd(f(m), q) = 1$. Furthermore, letting w denote a value of $af(m)^{-1} \bmod q$,

$$(P_1, \dots, P_{D+2}) \bmod q \in \mathcal{V}_q(w),$$

where

$$\mathcal{V}_q(w) := \{(v_1, \dots, v_{D+2}) \bmod q : \gcd(v_1 \cdots v_{D+2}, q) = 1,\ F(v_1) \cdots F(v_{D+2}) \equiv w \pmod q\}.$$

Let us estimate the size of $\#\mathcal{V}_q(w)$. Put

$$V_{\ell^e} = \#\{(v_1, \dots, v_{D+2}) \bmod \ell^e : \gcd(v_1 \cdots v_{D+2}, \ell) = 1,\ F(v_1) \cdots F(v_{D+2}) \equiv w \pmod{\ell^e}\},$$

so that $\#\mathcal{V}_q(w) = \prod_{\ell^e \| q} V_{\ell^e}$. From the proof of (2.20), with J replaced by $D+2$,

$$\varphi(\ell^e) V_{\ell^e} = (\alpha(\ell^e)\varphi(\ell^e))^{D+2}(1 + R_\ell),$$

where $|R_\ell| \le 2(4D)^{D+2}\ell^{-1/(D+1)} \ll \ell^{-1/(D+1)}$. Multiplying on ℓ gives

$$\begin{aligned}\varphi(q)\#\mathcal{V}_q(w) &\ll \alpha(q)^{D+2}\varphi(q)^{D+2}\exp\Big(O\big(\sum_{\ell|q}\ell^{-1/(D+1)}\big)\Big)\\ &\ll \varphi(q)^{D+2}\exp(O((\log q)^{1-1/(D+1)})).\end{aligned} \tag{2.21}$$

Given $P_2,\dots,P_{D+2}$, m, and $\mathbf{v} = (v_1,\dots,v_{D+2}) \bmod q \in \mathcal{V}_q(w)$, the number of possibilities for P_1 is $\ll x\log_2 x/\varphi(q)mP_2\cdots P_{D+2}\log x$, by Brun–Titchmarsh. Summing on $P_2,\dots,P_{D+2}$, we see that the number of possibilities for n given $\mathbf{v}$ and m is $\ll x(\log_2 x)^{O(1)}/\varphi(q)^{D+2}m\log x$. (We use here that

$$\sum_{\substack{q<p\le x\\ p\equiv v \,(\mathrm{mod}\ q)}}\frac{1}{p} \ll \frac{\log_2 x}{\varphi(q)},$$

uniformly in the choice of v, which follows from Brun–Titchmarsh and partial summation; alternatively, one can apply Lemma 2.2.3.) We sum on $\mathbf{v} \in \mathcal{V}_q(w)$, using (2.21), and then sum on m, writing $m = AB$ and making the estimates as earlier in this proof. We find that the total number of n is at most

$$\frac{x}{\varphi(q)(\log x)^{1-\frac{1}{2}\alpha}}\exp(O((\log_2 x)^{1-1/(D+1)})),$$

which is $o(N(q)/\varphi(q))$. □

Proof of (b). We follow the proof of (a), replacing $D+2$ everywhere by 2. It suffices to show that

$$\varphi(\ell)V_\ell \le \varphi(\ell)^2(1+O(1/\sqrt{\ell})) \tag{2.22}$$

for each ℓ, for then $\varphi(q)\#\mathcal{V}_q(w) \ll \varphi(q)^2\exp(O((\log q)^{1/2}))$, which is a suitable analogue of (2.21).

Certainly V_ℓ is bounded by the count of $\mathbb{F}_\ell$-points on the affine curve $F(x)F(y) = w$.

The polynomial $F(x)F(y) - w$ is absolutely irreducible over $\mathbb{F}_\ell$. Indeed, suppose that $F(x)F(y) - w = U(x,y)V(x,y)$ for some $U(x,y), V(x,y) \in \overline{\mathbb{F}}_\ell[x,y]$. Then for each root $\theta \in \overline{\mathbb{F}}_\ell$ of F, we find that $-w = U(\theta,y)V(\theta,y)$, and so in particular $U(\theta,y)$ is constant. Thus, if we write

$$U(x,y) = \sum_{k \geq 0} a_k(x) y^k,$$

with each $a_k(x) \in \overline{\mathbb{F}}_\ell[x]$, then $a_k(\theta) = 0$ for each $k > 0$. Since F has no multiple roots over $\overline{\mathbb{F}}_\ell$, each such $a_k(x)$ is forced to be a multiple of $F(x)$, hence $U(x,y) \equiv a_0(x) \pmod{F(x)}$. A symmetric argument shows that $V(x,y) \equiv b_0(y) \pmod{F(y)}$ for some $b_0(y) \in \overline{\mathbb{F}}_\ell[y]$, so that $V(x,\theta) = b_0(\theta)$. Consequently, for any root $\theta \in \overline{\mathbb{F}}_\ell$ of F,

$$-w \equiv F(x)F(\theta) - w \equiv U(x,\theta)V(x,\theta) \equiv a_0(x)b_0(\theta) \pmod{F(x)},$$

which shows that $U(x,y) \equiv a_0(x) \equiv c \pmod{F(x)}$ for some constant $c \in \overline{\mathbb{F}}_\ell$. But this forces $c = U(\theta,\theta)$, showing that $F(x)$ divides $U(x,y) - U(\theta,\theta)$. By symmetry, so does $F(y)$, and we obtain $U(x,y) = U(\theta,\theta) + F(x)F(y)Q(x,y)$ for some $Q(x,y) \in \overline{\mathbb{F}}_\ell[x,y]$. Degree considerations now imply that for $U(x,y)$ to divide $F(x)F(y) - w$, either $Q(x,y)$ is a nonzero constant, in which case $V(x,y)$ is constant, or $Q(x,y) = 0$, in which case $U(x,y)$ is constant.

Now we apply the following version of the Hasse–Weil bound [41, Corollary 2(b)].

Proposition 2.6.1. *If V is an absolutely irreducible affine plane curve, then $\#V(\mathbb{F}_\ell) \leq \ell + O(\sqrt{\ell})$, where the implied constant depends only on the degree of V.*

This gives that the number of $\mathbb{F}_\ell$-points on $F(x)F(y) = w$ is at most $\ell + 1 + \frac{1}{2}(2D-1)(2D-2)\lfloor 2\sqrt{\ell}\rfloor$, which is $\varphi(\ell)(1 + O(1/\sqrt{\ell}))$, yielding (2.22). □

Section 2.7

Concluding remarks and further questions

Elementary methods often enjoy a robustness surpassing their analytic counterparts, and our (quasi)elementary approach to weak uniform distribution is no exception. Not only does our method yield a range of uniformity in q wider than that (seemingly) accessible to more 'obvious' attacks via mean value theorems for multiplicative functions, but the method applies to functions that do not fit conveniently into the 'multiplicative managerie'. We illustrate with the following theorem; note that the distribution in residue classes of the function $A^*(n)$ below does not seem easily approached via mean value theorems.

Theorem 2.7.1. *Fix $K_0 \geq 1$. The sum of prime divisors function $A(n) := \sum_{j=1}^{\Omega(n)} P_j(n)$, as well as the alternating sum of prime divisors function $A^*(n) := \sum_{j=1}^{\Omega(n)} (-1)^{j-1} P_j(n)$, is asymptotically uniformly distributed to all moduli $q \leq (\log x)^{K_0}$. In other words, as $x \to \infty$,*

$$\sum_{\substack{n \leq x \\ A(n) \equiv a \,(\mathrm{mod}\ q)}} 1 \ \sim \ \sum_{\substack{n \leq x \\ A^*(n) \equiv a \,(\mathrm{mod}\ q)}} 1 \ \sim \ \frac{x}{q}, \tag{2.23}$$

uniformly in moduli $q \leq (\log x)^{K_0}$ and residue classes $a \bmod q$.

Remark 2.7.2. *The uniform distribution of $A(n)$ mod q for each fixed q is a consequence of the theorem of Delange quoted in the introduction, with more precise results appearing in work of Goldfeld [28]. For varying q, the problem seems to have been first considered in [60]; there Halász's mean value theorem is used to show uniform*

distribution of $A(n)$ mod q for $q \le (\log x)^{\frac{1}{2}-\delta}$ (for any fixed $\delta > 0$), a significantly narrower range than that allowed by Theorem 2.7.1.

Proof of Theorem 2.7.1. With $y := \exp(\sqrt{\log x})$, arguments analogous to (but simpler than) those in the proof of Lemma 2.3.2 show that the number of inconvenient $n \le x$ is $o(x)$, while arguments analogous to (but simpler than) those in the verification of Hypothesis B of §2.4 show that the number of inconvenient $n \le x$ having $A(n) \equiv a \pmod q$ or $A^*(n) \equiv a \pmod q$ is $o(x/q)$. Hence, it suffices to show that

$$N(q,a) \sim N^*(q,a) \quad \sim \frac{1}{q} \sum_{\text{convenient } n \le x} 1, \tag{2.24}$$

where $N(q,a)$ (respectively, $N^*(q,a)$) denotes the number of convenient $n \le x$ having $A(n) \equiv a \pmod q$ (resp., $A^*(n) \equiv a \pmod q$).

Proceeding as in §2.3, we define, for an arbitrary residue class w mod q,

$$\mathcal{V}_q(w) := \{(v_1, \dots, v_J) \bmod q : \gcd(v_1 \dots v_J, q) = 1,\ \sum_{j=1}^{J} v_j \equiv w \pmod q\}$$

and

$$\mathcal{V}_q^*(w) := \{(v_1, \dots, v_J) \bmod q : \gcd(v_1 \dots v_J, q) = 1,\ \sum_{j=1}^{J} (-1)^{j-1} v_j \equiv w \pmod q\},$$

and we write

$$N(q,a) = \sum_{m \le x} \frac{1}{J!} \sum_{\mathbf{v} \in \mathcal{V}_{q,a,m}} \sum_{\substack{P_1, \dots, P_J \text{ distinct} \\ P_1 \cdots P_J \le x/m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} 1,$$

$$N^*(q,a) = \sum_{m\le x} \frac{1}{J!} \sum_{\mathbf{v}\in\mathcal{V}^*_{q,a,m}} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m \\ \text{each } P_j \equiv v_j \pmod q}} 1,$$

where $\mathcal{V}_{q,a,m} := \mathcal{V}_q(a - A(m))$ and $\mathcal{V}^*_{q,a,m} := \mathcal{V}^*_q(a - (-1)^J A^*(m))$.

By J applications of Siegel-Walfisz, we now obtain

$$N(q,a) := \sum_{m\le x} \frac{\#\mathcal{V}_{q,a,m}}{\varphi(q)^J} \left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m}} 1 \right) + O\left(x \exp\left(-\frac{1}{8} C_0 (\log x)^{1/4} \right) \right) \tag{2.25}$$

$$N^*(q,a) := \sum_{m\le x} \frac{\#\mathcal{V}^*_{q,a,m}}{\varphi(q)^J} \left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J \text{ distinct} \\ P_1\cdots P_J \le x/m \\ \text{each } P_j > L_m}} 1 \right) + O\left(x \exp\left(-\frac{1}{8} C_0 (\log x)^{1/4} \right) \right), \tag{2.26}$$

for some constant $C_0 > 0$ depending only on K_0. As an analogue of our Hypothesis A, we claim that as $x \to \infty$,

$$\#\mathcal{V}_{q,a,m} \sim (\mathbb{1}_{2\nmid q} + 2\cdot \mathbb{1}_{2|q,\, J\equiv a - A(m) \pmod 2}) \frac{\varphi(q)^J}{q}, \tag{2.27}$$

$$\#\mathcal{V}^*_{q,a,m} \sim (\mathbb{1}_{2\nmid q} + 2\cdot \mathbb{1}_{2|q,\, J\equiv a - (-1)^J A^*(m) \pmod 2}) \frac{\varphi(q)^J}{q}, \tag{2.28}$$

uniformly in $m \le x$ and in $q \le (\log x)^{K_0}$. (If $\mathbb{1}_{2\nmid q} + 2\cdot \mathbb{1}_{2|q,\, J\equiv a - A(m) \pmod 2} = 0$, the asymptotic (2.27) should be interpreted as the claim $\mathcal{V}_{q,a,m}$ is empty, and similarly for (2.28).) To this end, it suffices to show that

$$\#\mathcal{V}^*_q(w) = \#\mathcal{V}_q(w) \sim (\mathbb{1}_{2\nmid q} + 2\cdot \mathbb{1}_{2|q,\, J\equiv w \pmod 2}) \frac{\varphi(q)^J}{q}, \tag{2.29}$$

uniformly in $q \le (\log x)^{K_0}$ and in residue classes w mod q. The equality in (2.29)

follows immediately from the one-to-one correspondence

$$(v_1, \cdots, v_J) \leftrightarrow (v_1, -v_2, \cdots, (-1)^{J-1} v_J)$$

between $\mathcal{V}_q(w)$ and $\mathcal{V}_q^*(w)$. To see the asymptotic, we write $\#\mathcal{V}_q(w) = \prod_{\ell^e \| q} V_{\ell^e}$, where for each prime power $\ell^e \parallel q$,

$$\begin{aligned} V_{\ell^e} :&= \#\{(v_1, \ldots, v_J) \bmod \ell^e : \gcd(v_1 \ldots v_J, \ell) = 1,\ \sum_{j=1}^{J} v_j \equiv w \pmod{\ell^e}\} \\ &= \frac{\varphi(\ell^e)^J}{\ell^e} + \frac{1}{\ell^e} \sum_{0<r<\ell^e} \exp\left(-\frac{2\pi i r w}{\ell^e}\right) S_\ell(r)^J, \end{aligned}$$

with $S_\ell(r) := \sum_{v \bmod \ell^e,\ (v,\ell)=1} \exp(2\pi i r v/\ell^e)$ (a Ramanujan sum). This sum can be exactly evaluated with the following identity (see [44, Theorem 4.1, p. 110]):

$$S_\ell(r) = \sum_{\substack{v \bmod \ell^e \\ (v,\ell)=1}} \exp\left(\frac{2\pi i r v}{\ell^e}\right) = \mathbb{1}_{\ell^{e-1} \| r}(-\ell^{e-1}) \text{ for all } r \in \{1, \cdots, \ell^e - 1\}. \quad (2.30)$$

We deduce that as $x \to \infty$,

$$\#\mathcal{V}_q(w) = (\mathbb{1}_{2 \nmid q} + 2 \cdot \mathbb{1}_{2|q,\, J \equiv w \,(\mathrm{mod}\ 2)}) \frac{\varphi(q)^J}{q} \prod_{\substack{\ell | q \\ \ell > 2}} \left(1 + O\left(\frac{1}{(\ell-1)^{J-1}}\right)\right),$$

leading to (2.29), since $\sum_{\ell|q,\, \ell>2} 1/(\ell-1)^{J-1} = o(1)$ as $J \to \infty$.

Plugging (2.27) and (2.28) into (2.25) and (2.26) respectively, and carrying out our initial reductions in reverse order completes the proof of (2.24), and hence also that of (2.23), for odd $q \le (\log x)^{K_0}$. On the other hand, when q is even we obtain

$$N(q,a) = \frac{2}{q} \sum_{\substack{n \le x \\ A(n) \equiv a \,(\mathrm{mod}\ 2)}} 1 + o\left(\frac{x}{q}\right), \quad N^*(q,a) = \frac{2}{q} \sum_{\substack{n \le x \\ A^*(n) \equiv a \,(\mathrm{mod}\ 2)}} 1 + o\left(\frac{x}{q}\right);$$

here, it has been noted that $a - A(m) \equiv J \pmod 2$ is equivalent to $A(mP_1 \cdots P_J) \equiv a \pmod 2$, and likewise for A^* in place of A. Since $A(n)$ is known to be equidistributed mod 2 (as discussed in the remarks preceding the theorem), and $A^*(n) \equiv A(n) \pmod 2$, the theorem follows. □

We close on a more speculative note. The mixing exploited in this chapter can be interpreted as a quantitative ergodicity phenomenon for random walks on multiplicative groups. However, our proofs go through character sum estimates; one might say that no actual Markov chains were harmed in the production of our arguments. It would be interesting to investigate the extent to which the (rather substantially developed) theory of Markov chain mixing could be brought directly to bear on these kinds of uniform and weak uniform distribution questions. This has the potential to open up applications in situations where character sum technology is unavailable.

Chapter 3

Joint distribution in residue classes of families of polynomially-defined additive functions

We extend the results in subsection § 1.4.1 to a family of polynomially–defined additive functions, thus also partially extending Delange's Theorems 1.2.4 and 1.2.3 from fixed to varying moduli. In this chapter, $g_1, \dots, g_M : \mathbb{N} \to \mathbb{Z}$ will be additive functions for which there exist nonconstant polynomials $G_1, \dots, G_M \in \mathbb{Z}[T]$ satisfying $g_i(p) = G_i(p)$ for all primes p and all $i \in [M]$. This chapter is based on the paper [73] of the author.

Section 3.1

Main results

In the first main result of this chapter, we shall extend Theorem 1.4.5 to families of additive functions. To this end, let g_i and G_i be as above, and let $\mathcal{Q}_{(g_1,\dots,g_M)}$ denote the set of moduli q such that $g_1,\dots,g_M$ are jointly equidistributed mod q. For technical reasons to be elaborated on later (see Theorem 3.1.4), we will assume in our main results (Theorems 3.1.1, 3.1.2 and 3.1.3) that the derivatives of G_i are linearly independent over $\mathbb{Q}$. This amounts to assuming that no nontrivial $\mathbb{Z}$-linear combination of the G_i reduces to a constant in $\mathbb{Z}[T]$, or in other words, that the polynomials $\{G_i(T) - G_i(0) : 1 \le i \le M\} \subset \mathbb{Q}[T]$ are $\mathbb{Q}$-linearly independent. (For $M = 1$, this simply amounts to G_1 being nonconstant.) In particular, this hypothesis forces the maximum of the degrees of the G_i to be no less than M.

Our first main result shows that $g_1,\dots,g_M$ are jointly equidistributed to moduli q lying in $\mathcal{Q}_{(g_1,\dots,g_M)}$ varying uniformly up to a small power of $\log x$. In what follows, we denote by D and $D_{\min}$ the maximum and the minimum of the degrees of $G_1,\dots,G_M$ respectively,[1] so that by the above discussion, $D \ge M$.

Theorem 3.1.1. *Fix $K \ge 1$, $\delta \in (0,1]$ and an integer $M \ge 1$. Let $g_1,\dots,g_M$ be additive functions defined by the polynomials $G_1,\dots,G_M$ such that the polynomials $\{G_i'\}_{1\le i\le M} \subset \mathbb{Z}[T]$ are $\mathbb{Q}$-linearly independent. Then $g_1,\dots,g_M$ are jointly equidistributed modulo q, uniformly for $q \le (\log x)^K$ lying in $\mathcal{Q}_{(g_1,\dots,g_M)}$, under any of the following additional conditions.*

(i) $M = 1$, and either q is squarefree or G_1 is linear.

[1] The asymmetry in notation is due to the much greater frequency of the appearance of D in our results, as compared to $D_{\min}$.

(ii) $M \geq 2$, $q \leq (\log x)^{(1-\delta)/(M-1)}$, *and either* q *is squarefree or at least one of* $G_1, \dots, G_M$ *is linear.*

(iii) $q \leq (\log x)^{(1-\delta)(M-1/D_{\min})^{-1}}$.

Subpart (i) and the special case $M = 1$ of subpart (iii) are contained in Theorem 1.4.5 from [1], but we have included them here in order to give a self-contained and unified treatment. These assertions will of course be automatically established by our method as well. However, our method is significantly different from that used in [1] as there are several additional ideas required to generalize these special cases to our theorem above.

In subsection § 3.4.1, we shall show that the ranges of q in the subparts of the above theorem are all essentially optimal. In the constructions described there, the obstructions to uniformity will come from the prime inputs p, analogous to what we observed in Chapter 2. Our next two results point out that the inputs n with too few 'large' prime factors present the key obstructions to uniformity. In other words, uniformity in q up to an arbitrary power of $\log x$ can be restored by restricting the set of n to those with sufficiently many prime divisors (counted with multiplicty) exceeding q.

Theorem 3.1.2. *Fix* $K, M \geq 1$ *and let* $g_1, \dots, g_M$ *be additive functions defined by the polynomials* $G_1, \dots, G_M$, *such that* $\{G_i'\}_{1 \leq i \leq M} \subset \mathbb{Z}[T]$ *are* $\mathbb{Q}$*-linearly independent. Assume that* $D = \max_{1 \leq i \leq M} \deg G_i \geq 2$. *We have*

$$\#\{n \leq x : P_{MD+1}(n) > q, \quad (\forall i)\ g_i(n) \equiv b_i \pmod q\}$$
$$\sim \frac{1}{q^M} \#\{n \leq x : P_{MD+1}(n) > q\} \sim \frac{x}{q^M} \quad \text{as } x \to \infty,$$

uniformly in moduli $q \leq (\log x)^K$ *lying in* $\mathcal{Q}_{(g_1,\dots,g_M)}$*, and in residue classes* $b_1, \dots, b_M$ *mod* q*.*

Here we omit the possibility $D = 1$, as in this case, the fact that $D \geq M$ forces $M = 1$, putting us in the setting of Theorem 3.1.1(i), where we already have complete uniformity in q in the Siegel–Walfisz range. For squarefree moduli q, it turns out that a much weaker restriction on the inputs suffices: we need only assume that n has at least twice as many prime factors (counted with multiplicity) exceeding q as the number M of additive functions considered.

Theorem 3.1.3. *Fix* $K \geq 1$*,* $M \geq 2$ *and let* $g_1, \dots, g_M$ *be additive functions defined by the polynomials* $G_1, \dots, G_M$*, such that* $\{G_i'\}_{1 \leq i \leq M} \subset \mathbb{Z}[T]$ *are* $\mathbb{Q}$*-linearly independent. We have*

$$\#\{n \leq x : P_{2M}(n) > q, \quad (\forall i)\ g_i(n) \equiv b_i \pmod q\}$$
$$\sim \frac{1}{q^M} \#\{n \leq x : P_{2M}(n) > q\} \sim \frac{x}{q^M} \qquad \text{as } x \to \infty,$$

uniformly in squarefree $q \leq (\log x)^K$ *lying in* $\mathcal{Q}_{(g_1,\dots,g_M)}$*, and in residues* $b_1, \dots, b_M$ *mod* q*.*

Here, we omit the case $M = 1$ as complete uniformity in squarefree $q \leq (\log x)^K$ has already been attained in Theorem 3.1.1(i). In subsection § 3.6.1, we will show that the restriction $P_{2M}(n) > q$ is nearly optimal in the sense that it cannot be weakened to $P_{2M-3}(n) > q$ for any $M \geq 2$, and that for $M = 2$, it cannot be weakened to $P_{2M-2}(n) > q$ either.

We now illustrate the necessity of our recurring linear independence hypothesis. It turns out that if the polynomials $\{G_i'\}_{i=1}^M$ are not assumed to be $\mathbb{Q}$-linearly inde-

pendent, then the M congruences $g_i(n) \equiv b_i \pmod{q}$ might degenerate to (at most) $M-1$ congruences for sufficiently many inputs n. As such, it is not possible to restore uniformity in moduli $q \leq (\log x)^K$ no matter how many prime factors of our inputs n we assume to be larger than q. Specifically, for any large integer R, we can always construct integers $b_1, \dots, b_M$ which are overrepresented by the $g_1, \dots, g_M$ among the set of inputs $n \leq x$ having $P_R(n) > q$. We show this precisely below.

Theorem 3.1.4. *Fix $K \geq 1, M \geq 2$ and polynomials $G_1, \dots, G_{M-1} \in \mathbb{Z}[T]$ such that $\{G_i'\}_{i=1}^{M-1} \subset \mathbb{Z}[T]$ are $\mathbb{Q}$-linearly independent. Consider nonzero integers $\{a_i\}_{i=1}^{M-1}$ and a polynomial $G_M \in \mathbb{Z}[T]$ satisfying $G_M' = \sum_{i=1}^{M-1} a_i G_i'$ and $G_M(0) \neq \sum_{i=1}^{M-1} a_i G_i(0)$. Let $g_1, \dots, g_M$ be additive functions defined by the polynomials $G_1, \dots, G_M$. There exists a computable constant $C_{\boldsymbol{G}} > 0$ depending only on the system $\widehat{G} := (G_1, \dots, G_M)$ that satisfies the following properties:*

For any integer $Q > 1$ with $P^-(Q) > C_{\boldsymbol{G}}$, the functions $g_1, \dots, g_M$ are jointly equidistributed mod Q. However, for any fixed $R > C_{\boldsymbol{G}}$ and any integers $\{b_i\}_{i=1}^{M-1}$, there exists an integer b_M such that

$$\#\{n \leq x : P_R(n) > q, \quad (\forall i)\ g_i(n) \equiv b_i \pmod{q}\} \gg \frac{x(\log_2 x)^{R-1}}{q^{M-1}\log x} \quad \text{as } x \to \infty,$$

uniformly in moduli $q \leq (\log x)^K$ having $P^-(q) > C_{\boldsymbol{G}}$.

Thus, the above theorem shows that without the $\mathbb{Q}$-linear independence of the $\{G_i'\}_{i=1}^{M}$, uniformity could fail to *all* moduli $q \in (\log x, (\log x)^{K_0}]$ having sufficiently large prime factors, despite $g_1, \dots, g_M$ being jointly equidistributed to any fixed modulus having sufficiently large prime factors. We expect that with appropriate modifications of our methods, it might be possible to obtain analogues of Theorems 3.1.1, 3.1.2 and

3.1.3 (with more limited ranges of unformity in q) when $\{G_i'\}_{i=1}^M$ are not $\mathbb{Q}$-linearly independent: from our arguments below, it seems reasonable to expect that the corresponding ranges of q and restrictions on the inputs n should then depend on the rank of the matrix of coefficients of the polynomials $\{G_i'\}_{i=1}^M$.

We conclude this introductory section with the remark that although for the sake of simplicity of statements, we have been assuming that our additive functions $\{g_i\}_{i=1}^M$ and polynomials $\{G_i\}_{i=1}^M$ are both fixed, our proofs of Theorems 3.1.1, 3.1.2, 3.1.3 and 3.1.4 will reveal that these results are also uniform in the additive functions $\{g_i\}_{i=1}^M$ as long as they are defined by the fixed polynomials $\{G_i\}_{i=1}^M$.

Additional notation and conventions in this chapter:

Given polynomials $G_1, \dots, G_M \in \mathbb{Z}[T]$, we shall (in this chapter) use D and $D_{\min}$ to denote the maximum and the minimum of the degrees of the G_i, respectively. As usual, 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 $G_1, \dots, G_M$. Other dependence will be noted explicitly (for example, with parentheses or subscripts); notably, we shall use $C(\mathbf{G})$ or $C_{\mathbf{G}}$ to denote constants depending only on the vector $\widehat{G} := (G_1, \dots, G_M)$ of defining polynomials.

For a positive integer n, we define $\Omega^*_{>q}(n) := \sum_{\substack{p^k \| n \\ p>q,\ k>1}} k$ to be the number of prime divisors of n (counted with multiplicity) that exceed q and appear to an exponent greater than 1 in the prime factorization of n.

Section 3.2

Preliminary Discussion: Delange's equidistribution criteria and consequences for polynomially-defined additive functions

We start by stating the following explicit consequences of Delange's criteria Theorems 1.2.3 and 1.2.4 in our setting of polynomially-defined additive functions, which is how they shall be useful to us. In what follows, for a given polynomial $G \in \mathbb{Z}[T]$, we set

$$\alpha_G(q) \coloneqq \frac{1}{\varphi(q)} \#(G^{-1}(U_q) \cap U_q) = \frac{1}{\varphi(q)} \#\{v \in U_q : G(v) \in U_q\}$$

denote the proportion of unit residues v mod q whose image under the polynomial G is also a unit mod q. By the Chinese Remainder Theorem, $\alpha_G(q) = \prod_{\ell | q} \alpha_G(\ell)$.

Lemma 3.2.1. *Let $g\colon \mathbb{N} \to \mathbb{Z}$ be an additive function defined by a nonconstant polynomial $G \in \mathbb{Z}[T]$. We can describe the set*

$$\mathcal{Q}_g = \{q \in \mathbb{N} : g \text{ is equidistributed mod } q\}$$

as follows:

(i) If $2 \mid g(2^r)$ for some $r \geq 1$, then $\mathcal{Q}_g = \{q : \alpha_G(q) \neq 0\}$.

(ii) If $2 \nmid g(2^r)$ for all $r \geq 1$ and if $4 \mid (G(1), G(3))$, then

$$\mathcal{Q}_g = \{q : 2 \nmid q,\ \alpha_G(q) \neq 0\} \cup \{q : 2 \parallel q,\ \alpha_G(q/2) \neq 0\}.$$

(iii) If $2 \nmid g(2^r)$ *for all* $r \geq 1$ *and if* $4 \nmid (G(1), G(3))$*, then* $\mathcal{Q}_g = \left\{q : \alpha_G\left(\frac{q}{2^{v_2(q)}}\right) \neq 0\right\}$.

Proof. In what follows, let $q' \coloneqq q/2^{v_2(q)}$ denote the largest odd divisor of q. An application of the Siegel–Walfisz Theorem with partial summation shows that for any divisor $d > 1$ of q and any $X > e^q$, we have

$$S_d(X) \coloneqq \sum_{\substack{p \leq X \\ d \mid g(p)}} \frac{1}{p} = \sum_{\substack{p \leq X \\ d \mid G(p)}} \frac{1}{p}$$
$$= \sum_{\substack{r \in U_d \\ d \mid G(r)}} \sum_{\substack{p \leq X \\ p \equiv r \bmod d}} \frac{1}{p} + O_q(1) = \beta_G(d) \log_2 X + O_q(1),$$

where $\beta_G(d) \coloneqq \frac{1}{\varphi(d)} \#\{r \in U_d : d \nmid G(r)\}$. Letting $X \to \infty$, we deduce that the sum $S_d = \sum_{p:\ d \mid g(p)} 1/p$ diverges if and only if $\beta_G(d) \neq 0$. But since $\beta_G(\ell) = \alpha_G(\ell)$ for any prime ℓ, Theorem 1.2.3 shows that if $q \in \mathcal{Q}_g$, then $\alpha_G(\ell) \neq 0$ for all odd primes ℓ dividing q, so that $\alpha_G(q') \neq 0$. On the other hand, if $\alpha_G(q) \neq 0$ for some q, then $\beta_G(\ell) = \alpha_G(\ell) \neq 0$ for all primes dividing q, so that S_ℓ diverges for all such primes, and Theorem 1.2.3 leads to $q \in \mathcal{Q}_g$ (since $S_4 \geq S_2$). In summary, we have so far shown that $\{q : \alpha_G(q) \neq 0\} \subset \mathcal{Q}_g \subset \{q : \alpha_G(q') \neq 0\}$, which in particular means that $\{q : 2 \nmid q,\ q \in \mathcal{Q}_g\} = \{q : 2 \nmid q,\ \alpha_G(q) \neq 0\}$.

Now consider an even integer $q \in \mathcal{Q}_g$, so that it satisfies the necessary condition $\alpha_G(q') \neq 0$.

(i) If $2 \mid g(2^r)$ for some $r \geq 1$, then by Theorem 1.2.3, the sum S_2 must diverge. By the above discussion, this means that $\alpha_G(2) = \beta_G(2)$ must be nonzero, leading to $\alpha_G(q) \neq 0$. Hence, in this case $\mathcal{Q}_g = \{q : \alpha_G(q) \neq 0\}$.

(ii) Suppose $2 \nmid g(2^r)$ for all $r \geq 1$ and $4 \mid (G(1), G(3))$. Then $\alpha_G(2) = 0$, so that by Theorem 1.2.3(ii) and the discussion in the previous paragraph, we have

$\{q : 2 \parallel q,\ q \in \mathcal{Q}_g\} = \{q : 2 \parallel q,\ \alpha_G(q/2) \neq 0\}$. Moreover, no positive integer divisible by 4 can lie in $\mathcal{Q}_g$: this follows by Theorem 1.2.3(iii), since the condition $4 \mid (G(1), G(3))$ implies that $\beta_G(4) = 0$, and that S_4 converges. Hence, in this case $\mathcal{Q}_g$ is as in the statement of the lemma.

(iii) Finally if $2 \nmid g(2^r)$ for all $r \geq 1$ and if $4 \nmid (G(1), G(3))$, then S_4 diverges, and Theorem 1.2.3 along with the inclusions obtained in the previous paragraph show that q lies in $\mathcal{Q}_g$ if and only if $\alpha_G(q') \neq 0$.

This completes the proof of the lemma. □

The following observation paves the way for a simple application of Theorem 1.2.4 in the setting of polynomially-defined additive functions.

Lemma 3.2.2. *Let $M \geq 2$ and $g_1, \ldots, g_M : \mathbb{N} \to \mathbb{Z}$ be additive functions defined by the nonconstant polynomials $G_1, \ldots, G_M \in \mathbb{Z}[T]$, and let ℓ be a prime. If $\alpha_{k_1G_1+\cdots+k_MG_M}(\ell) \neq 0$ for all integer tuples $(k_1, \ldots, k_M)$ satisfying $\gcd(k_1, \ldots, k_M) = 1$, then the polynomials $G_1, \ldots, G_M$ must be $\mathbb{F}_\ell$-linearly independent. Further, if $\ell > D + 1$, then this condition is also sufficient.*

Proof. To establish the first assertion, we assume by way of contradiction that there exist $\mu_1, \ldots, \mu_M \in \{0, 1, \ldots, \ell - 1\}$ not all zero, such that $\sum_{r=1}^{M} \mu_r G_r(T)$ vanishes identically in $\mathbb{F}_\ell[T]$. We will construct integers $k_1, \ldots, k_M$ satisfying $\gcd(k_1, \ldots, k_M) = 1$ and $\alpha_{k_1G_1+\cdots+k_MG_M}(\ell) = 0$. To that end, consider some $i \in [M]$ for which $\mu_i \not\equiv 0 \pmod{\ell}$ and let $k_r \coloneqq \mu_r$ for all $r \in [M] \setminus \{i\}$.

Now choose any $j \in [M] \setminus \{i\}$. By the Chinese Remainder Theorem, there exists an integer k_i such that $k_i \equiv \mu_i \pmod{\ell}$ and $\gcd(k_i, k_j) = 1$. With this choice of integers $(k_1, \ldots, k_M)$, we see that $\gcd(k_1, \cdots, k_M) = 1$ and that the polyno-

mial $\sum_{r=1}^{M} k_r G_r(T) \equiv \sum_{r=1}^{M} \mu_r G_r(T) \pmod{\ell}$ is identically zero in $\mathbb{F}_\ell[T]$, so that $\alpha_{k_1G_1+\cdots+k_MG_M}(\ell) = 0$. This proves the first assertion of the lemma.

To show the second assertion, we consider any prime $\ell > D+1$. Suppose there did exist a tuple of integers $(k_1, \ldots, k_M)$ satisfying $\gcd(k_1, \ldots, k_M) = 1$ and $\alpha_{k_1G_1+\cdots+k_MG_M}(\ell) = 0$. Then on the one hand, $(k_1, \ldots, k_M) \not\equiv (0, \ldots, 0) \pmod{\ell}$. On the other hand, the polynomial $\sum_{r=1}^{M} k_r G_r(T)$ (considered as an element of $\mathbb{F}_\ell[T]$) has degree at most D but has at least $\#U_\ell = \varphi(\ell) = \ell - 1 > D$ roots in $\mathbb{F}_\ell$. As such, $\sum_{r=1}^{M} k_r G_r(T)$ vanishes identically in $\mathbb{F}_\ell[T]$ yielding a nontrivial $\mathbb{F}_\ell$-linear dependence relation between the $\{G_r\}_{r=1}^{M}$. □

We remark that the matrix of coefficients alluded to towards the end of section 3.1 will play a pivotal role in our arguments. To set things up, we write $G_i'(T) =: \sum_{r=0}^{D-1} a_{i,r} T^r$ for some integers $\{a_{i,r} : 1 \leq i \leq M, 0 \leq r \leq D-1\}$, so that $a_{i,D-1} \neq 0$ for some i (since $D = \max_{1 \leq i \leq M} \deg G_i$). Note that since $G_i \in \mathbb{Z}[T]$, we have $(r+1) \mid a_{i,r}$ for all $i \in [M]$ and $0 \leq r \leq D-1$. By the matrix of coefficients or coefficient matrix of the polynomials $\{G_i'\}_{1 \leq i \leq M}$, we shall mean the $D \times M$ integer matrix

$$A_0 \coloneqq \begin{pmatrix} a_{1,0} & \cdots & a_{M,0} \\ \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots \\ a_{1,D-1} & \cdots & a_{M,D-1} \end{pmatrix} \tag{3.1}$$

whose i-th column lists the coefficients of the polynomial G_i' in ascending order of the degree of T. It is important to note that if the polynomials $\{G_i'\}_{i=1}^{M}$ are $\mathbb{Q}$-linearly independent, then the columns of the matrix A_0 form $\mathbb{Q}$-linearly independent vectors, so that A_0 has full rank. As such, the Smith normal form S_0 of A_0 only has nonzero entries on its main diagonal. In other words, A_0 has exactly M invariant factors

$\beta_1, \dots, \beta_M \in \mathbb{Z}\backslash\{0\}$, which must also satisfy $\beta_i \mid \beta_{i+1}$ for all $1 \le i < M$. Furthermore, since S_0 is obtained from A_0 by a change of basis over $\mathbb{Z}$, it follows that the primes ℓ for which the columns of A_0 (or equivalently, the polynomials $\{G_i'\}_{i=1}^M$) are $\mathbb{F}_\ell$-linearly dependent are precisely those which divide at least one of the β_i (or equivalently, those which divide β_M). As a consequence, letting $C_0(\mathbf{G})$ be any constant exceeding $\max\{D+1, |\beta_M|\}$ (so that $C_0(\mathbf{G})$ depends only on the vector $\widehat{G} := (G_1, \dots, G_M)$), we see that:

$$\text{The polynomials } \{G_i'\}_{i=1}^M \text{ are } \mathbb{F}_\ell\text{-linearly independent for all primes } \ell > C_0(\mathbf{G}). \tag{3.2}$$

Our arguments leading to (3.2) show that under the weaker hypothesis that the $\{G_i\}_{i=1}^M$ are $\mathbb{Q}$-linearly independent, there exists a constant $C_1(\widehat{G}) > D+1$ such that $\{G_i\}_{i=1}^M$ are $\mathbb{F}_\ell$-linearly independent for all $\ell > C_1(\widehat{G})$. Note that if $\{G_i'\}_{i=1}^M$ are $\mathbb{Q}$ (respectively, $\mathbb{F}_\ell$)-linearly independent, then so are $\{G_i\}_{i=1}^M$. Hence, if $\{G_i'\}_{i=1}^M$ are $\mathbb{Q}$-linearly independent, then with $C_0(\mathbf{G})$ as in (3.2), the $\{G_i\}_{i=1}^M$ are also $\mathbb{F}_\ell$-linearly independent for any prime $\ell > C_0(\mathbf{G})$. Combining these observations with Theorem 1.2.4 and Lemmas 3.2.1 and 3.2.2, we obtain the following useful consequence.

Corollary 3.2.3. *Let $g_1, \dots, g_M : \mathbb{N} \to \mathbb{Z}$ be additive functions defined by the nonconstant polynomials $G_1, \dots, G_M \in \mathbb{Z}[T]$. Then for any $q > 1$ with $P^-(q) > D+1$, the functions $g_1, \dots, g_M$ are jointly equidistributed mod q if and only if the polynomials $\{G_i\}_{i=1}^M$ are $\mathbb{F}_\ell$-linearly independent for every prime $\ell \mid q$. In particular,*

(i) If the polynomials $\{G_i\}_{i=1}^M$ are $\mathbb{Q}$-linearly independent (so that $C_1(\widehat{G})$ exists), then any q having $P^-(q) > C_1(\widehat{G})$ lies in $\mathcal{Q}_{(g_1,\dots,g_M)}$.

(ii) If the polynomials $\{G_i'\}_{i=1}^M$ are $\mathbb{Q}$-linearly independent (so that $C_0(\widehat{G})$ exists), then any q having $P^-(q) > C_0(\boldsymbol{G})$ lies in $\mathcal{Q}_{(g_1,\dots,g_M)}$.

Section 3.3

Preparation for Theorems 3.1.1, 3.1.2 and 3.1.3: Obtaining the main term

Analogous to Chapter 2, we start by defining $J := J(x) := \lfloor \log_3 x \rfloor$. Let $\delta \in (0, 1]$ be as in the statement of Theorem 1.1; the development in this section will also go through in Theorems 3.1.2 and 3.1.3 with (say) $\delta := 1$.

We define $y := \exp\left((\log x)^{\delta/2}\right)$, and call a positive integer $n \leq x$ convenenient if the J largest prime divisors of n exceed y and exactly divide n, that is, if

$$\max\{P_{J+1}(n), y\} < P_J(n) < \cdots < P_1(n).$$

Any convenient n can thus be uniquely written in the form $mP_J \cdots P_1$, with

$$L_m := \max\{y, P(m)\} < P_J < \cdots < P_1. \tag{3.3}$$

We will show that the convenient n give the most dominant contribution to the counts considered in Theorems 3.1.1, 3.1.2 and 3.1.3.

Proposition 3.3.1. *Fix $K, M \geq 1$ and let $g_1, \ldots, g_M$ be additive functions defined by the nonconstant polynomials $G_1, \ldots, G_M \in \mathbb{Z}[T]$, such that $\{G_i'\}_{1 \leq i \leq M} \subset \mathbb{Q}[T]$ are $\mathbb{Q}$-linearly independent. Let $D = \max_{1 \leq i \leq M} \deg G_i$. We have*

$$\#\{n \leq x : n \text{ convenient}, \ (\forall i) \ g_i(n) \equiv b_i \pmod q\} \sim \frac{x}{q^M}, \qquad \text{as } x \to \infty,$$

uniformly in moduli $q \leq (\log x)^K$ lying in $\mathcal{Q}_{(g_1,\ldots,g_M)}$, and in residues b_i mod q.

Proof. Writing each convenient n uniquely in the form $mP_J \cdots P_1$, where $m, P_J, \dots, P_1$ satisfy (3.3), we find that $g_i(n) = g_i(m) + \sum_{j=1}^{J} G_i(P_j)$. The conditions $g_i(n) \equiv b_i \pmod q$ $(1 \le i \le M)$ can then be rewritten as $(P_1, \dots, P_J) \bmod q \in \mathcal{V}'_{q,m} := \mathcal{V}_{J,M}\left(q; (b_i - g_i(m))_{i=1}^M\right)$, where

$$\mathcal{V}_{J,M}\left(q; (w_i)_{i=1}^M\right) := \left\{(v_1, \dots, v_J) \in (U_q)^J : \ (\forall i) \ \sum_{j=1}^{J} G_i(v_j) \equiv w_i \pmod q\right\}.$$

(Note that this set can be defined for any set of polynomials $\{G_i\}_{i=1}^M$ regardless of whether or not they come from a set of additive functions.) As a consequence,

$$\begin{aligned}\sum_{\substack{n \le x \text{ convenient} \\ (\forall i) \ g_i(n) \equiv b_i \pmod q}} 1 &= \sum_{m \le x} \sum_{(v_1,\dots,v_J) \in \mathcal{V}'_{q,m}} \sum_{\substack{P_1,\dots,P_J \\ P_1 \cdots P_J \le x/m \\ L_m < P_J < \cdots < P_1 \\ (\forall j) \ P_j \equiv v_j \pmod q}} 1 \\ &= \sum_{m \le x} \sum_{(v_1,\dots,v_J) \in \mathcal{V}'_{q,m}} \frac{1}{J!} \sum_{\substack{P_1,\dots,P_J > L_m \\ P_1 \cdots P_J \le x/m \\ P_1,\dots,P_J \text{ distinct} \\ (\forall j) \ P_j \equiv v_j \pmod q}} 1,\end{aligned} \tag{3.4}$$

where in the last equality above, we have noted that the conditions $P_1 \cdots P_J \le x/m$ and $(P_1, \dots, P_J) \bmod q \in \mathcal{V}'_{q,m}$ are both independent of the ordering of $P_1, \dots, P_J$.

We now estimate the innermost sum on $P_1, \dots, P_J$ by removing the congruence conditions on the P_j. For each tuple $(v_1, \dots, v_J) \bmod q \in \mathcal{V}'_{q,m}$, we see that

$$\sum_{\substack{P_1,\dots,P_J > L_m \\ P_1 \cdots P_J \le x/m \\ P_1,\dots,P_J \text{ distinct} \\ (\forall j) \ P_j \equiv v_j \pmod q}} 1 = \sum_{\substack{P_2,\dots,P_J > L_m \\ P_2 \cdots P_J \le x/mL_m \\ P_2,\dots,P_J \text{ distinct} \\ (\forall j) \ P_j \equiv v_j \pmod q}} \sum_{\substack{P_1 \ne P_2,\dots,P_J \\ L_m < P_1 \le x/mP_2 \cdots P_J \\ P_1 \equiv v_1 \pmod q}} 1.$$

Since $L_m \ge y$ and $q \le (\log x)^K = (\log y)^{2K/\delta}$, the Siegel–Walfisz theorem yields

$$\sum_{\substack{P_1\neq P_2,\dots,P_J\\ L_m<P_1\le x/mP_2\cdots P_J\\ P_1\equiv v_1 \pmod q}} 1 \;=\; \frac{1}{\varphi(q)} \sum_{\substack{P_1\neq P_2,\dots,P_J\\ L_m<P_1\le x/mP_2\cdots P_J}} 1 + O\left(\frac{x}{mP_2\cdots P_J}\exp(-C_0\sqrt{\log y})\right),$$

for some positive constant $C_0 := C_0(K,\delta)$ depending only on K and δ. Putting this back into the last display, we find that

$$\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \pmod q}} 1 \;=\; \frac{1}{\varphi(q)} \sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}\\ (\forall j\ge 2)\ P_j\equiv v_j \pmod q}} 1 \;+\; O\left(\frac{x}{m}\exp\left(-\frac{1}{2}C_0(\log x)^{\delta/4}\right)\right),$$

where we have put the bound

$$\sum_{P_2,\dots,P_J\le x}\frac{1}{P_2\cdots P_J} \le \left(\sum_{p\le x}\frac{1}{p}\right)^{J-1} \le (2\log_2 x)^{J-1} \le \exp(O((\log_3 x)^2)).$$

Proceeding in the same way to successively remove the congruence conditions on $P_2,\dots,P_J$, we deduce that

$$\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \pmod q}} 1 \;=\; \frac{1}{\varphi(q)^J} \sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1 \;+\; O\left(\frac{x}{m}\exp\left(-\frac{1}{4}C_0(\log x)^{\delta/4}\right)\right). \quad (3.5)$$

Inserting this into (3.4) and noting that $\#\mathcal{V}'_{q,m} \le \varphi(q)^J \le (\log x)^{KJ}$, we obtain

$$\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ g_i(n)\equiv b_i \pmod q}} 1 = \sum_{m\le x}\frac{\#\mathcal{V}'_{q,m}}{\varphi(q)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) + O\left(x\exp\left(-\frac{C_0}{8}(\log x)^{\delta/4}\right)\right). \quad (3.6)$$

The following proposition, which we shall establish momentarily, will provide the

desired estimate on the cardinalities of the sets $\mathcal{V}'_{q,m}$. For future convenience and independent interest, we state it in slightly greater generality than necessary in our immediate application.

Proposition 3.3.2. *Let $G_1, \dots, G_M \in \mathbb{Z}[T]$ be nonconstant polynomials, such that $\{G'_i\}_{1\le i\le M} \subset \mathbb{Z}[T]$ are $\mathbb{Q}$-linearly independent. Let $D = \max_{1\le i\le M} \deg G_i$ and $C := C(\boldsymbol{G})$ be a constant exceeding $\max\{C_0(\boldsymbol{G}), (2D)^{2D+4}\}$, where $C_0(\boldsymbol{G})$ is the constant in (3.2). We have*

$$\frac{\#\mathcal{V}_{N,M}\left(q;(w_i)_{i=1}^M\right)}{\varphi(q)^N} = \left(\frac{Q_0}{q}\right)^M \left\{\frac{\#\mathcal{V}_{N,M}\left(Q_0;(w_i)_{i=1}^M\right)}{\varphi(Q_0)^N} + O\left(\frac{1}{C^N}\right)\right\} \prod_{\substack{\ell\mid q\\ \ell>C}} \left(1+O\left(\frac{(2D)^N}{\ell^{N/D-M}}\right)\right),$$

uniformly in $N \ge MD+1$, in all positive integers $q>1$, and in residue classes $w_1, \dots, w_M$ mod q, where Q_0 is a divisor of q of size $O(1)$ supported on primes at most C.

To estimate the count $\#\mathcal{V}'_{q,m}$ in (3.6), we apply the above proposition with $N := J$ which goes to infinity with x and hence exceeds $MD+1$ for all sufficiently large x. For the same reason, we find that as $x \to \infty$,

$$\sum_{\substack{\ell\mid q\\ \ell>C}} \frac{(2D)^N}{\ell^{N/D-M}} \le (2D)^J \sum_{\substack{\ell\mid q\\ \ell>C}} \frac{1}{\ell^{J/(D+2)}} \le \frac{(2D)^J}{C^{J/(2D+4)}} \sum_{\ell\ge 2} \frac{1}{\ell^2} \le \left(\frac{2D}{C^{1/(2D+4)}}\right)^J = o(1).$$

As such, an application of the above proposition yields

$$\frac{\#\mathcal{V}_{J,M}\left(q;(w_i)_{i=1}^M\right)}{\varphi(q)^J} \;=\; (1+o(1))\left(\frac{Q_0}{q}\right)^M\left\{\frac{\#\mathcal{V}_{J,M}\left(Q_0;(w_i)_{i=1}^M\right)}{\varphi(Q_0)^J}+O\left(\frac{1}{C^J}\right)\right\},$$

uniformly in q and $(w_1,\dots,w_M)$ mod q, where $Q_0 \mid q$ and $Q_0 = O(1)$. In particular, this same estimate holds for $\mathcal{V}'_{q,m} = \mathcal{V}_{J,M}\left(q;(b_i-g_i(m))_{i=1}^M\right)$, and we obtain from (3.6),

$$\begin{aligned}
&\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ g_i(n)\equiv b_i \pmod q}} 1\\
&= (1+o(1))\left(\frac{Q_0}{q}\right)^M \sum_{m\le x}\left\{\frac{\#\mathcal{V}'_{Q_0,m}}{\varphi(Q_0)^J}+O(C^{-J})\right\}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right)\\
&\qquad\qquad + \;O\left(x\exp\left(-\frac{1}{8}C_0(\log x)^{\delta/4}\right)\right)\\
&= (1+o(1))\left(\frac{Q_0}{q}\right)^M \sum_{m\le x}\frac{\#\mathcal{V}'_{Q_0,m}}{\varphi(Q_0)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right)+o\left(\frac{x}{q^M}\right)
\end{aligned}$$

where we have recalled that

$$\sum_{m\le x}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right)\le\sum_{m\le x}\left(\sum_{\substack{P_1,\dots,P_J\\ P_1\cdots P_J\le x/m\\ L_m<P_J<\cdots<P_1}} 1\right)\le x.$$

But now, applying the estimate (3.6) with Q_0 playing the role of q, we find that

$$\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ g_i(n)\equiv b_i \pmod q}} 1 \;=\; (1+o(1))\left(\frac{Q_0}{q}\right)^M \sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ g_i(n)\equiv b_i \pmod{Q_0}}} 1 \;+\; o\left(\frac{x}{q^M}\right).$$

Before proceeding further, we state the following bound on the number of positive integers without many large prime factors. The following is a variant of [59, Lemma

2.3] which follows from the same arguments.

Lemma 3.3.3. *Uniformly in $x \geq y \geq 10$ and $R \geq 2$, we have*

$$\#\{n \leq x : P_R(n) \leq y\} \ \ll \ x\frac{\log y}{\log x}(2\log\log x)^{R-1}.$$

Recall that any inconvenient $n \leq x$ either has $P_J(n) \leq y$ or has a repeated prime factor exceeding y. The number of $n \leq x$ satisfying the latter condition is no more than $\sum_{p>y}\sum_{n\leq x:\ p^2|n} 1 \leq x\sum_{p>y} 1/p^2 \ll x/y = o(x)$. Moreover, by Lemma 3.3.3, the number of $n \leq x$ having $P_J(n) \leq y$ is $\ll x(\log_2 x)^{J-1}/(\log x)^{1-\delta}$ which is also $o(x)$. This yields

$$\sum_{\substack{n\leq x \text{ convenient}\\ (\forall i)\ g_i(n)\equiv b_i \pmod q}} 1 \ = \ (1+o(1))\left(\frac{Q_0}{q}\right)^M \sum_{\substack{n\leq x\\ (\forall i)\ g_i(n)\equiv b_i \pmod{Q_0}}} 1 \ + \ o\left(\frac{x}{q^M}\right).$$

Finally, since q lies in $\mathcal{Q}_{(g_1,\dots,g_M)}$, so does its divisor Q_0, and as $Q_0 = O(1)$, the sum occurring on the right hand side above is $(1+o(1))x/Q_0^M$. This completes the proof of Proposition 3.3.1, up to that of Proposition 3.3.2. □

Before beginning the proof of Proposition 3.3.2, we state some (relevant special cases of) known bounds on mixed exponential sums, which will provide some key technical inputs in our arguments. First, we have the renowned bound of Weil [78] coming from his work on the Riemann Hypothesis for curves over a finite field (see also Schmidt [66, chapter II, Corollary 2F]). In what follows, we set $e(t) \coloneqq \exp(2\pi i t)$. For a positive integer Q, we use $\chi_{0,Q}$ to denote the trivial (or principal) character mod Q. For a prime ℓ, $\chi_{0,\ell}$ is also the principal character modulo any power of ℓ.

Proposition 3.3.4. *Let $F \in \mathbb{Z}[T]$ be a polynomial of degree $D_0 \geq 1$, and let $\ell > D_0$*

be a prime such that F doesn't reduce to a constant modulo ℓ. Then we have

$$\left| \sum_{v \bmod \ell} \chi_{0,\ell}(v) e(F(v)/\ell) \right| \leq D_0 \ell^{1/2}.$$

We will also need analogues of the above bound for prime powers, which have been obtained by Cochrane and Zheng [17, equation (1.13), Theorems 1.1 and 8.1]. (See [14] for more general results.) In what follows, for a nonconstant polynomial $F \in \mathbb{Z}[T]$ and a prime ℓ, we define $t_\ell(F) \coloneqq \mathrm{ord}_\ell(F')$, that is $t_\ell(F)$ is the highest power of ℓ dividing the coefficients of the polynomial F'. Let $\mathcal{A}_{F,\ell}$ denote the set of nonzero roots in $\mathbb{F}_\ell$ of the polynomial $\ell^{-t_\ell(F)}F'$ (considered as a nonzero element of $\mathbb{F}_\ell[T]$). We use $M_\ell(F)$ to denote the maximum of the multiplicities of the zeros of $\ell^{-t_\ell(F)}F'$ in $\mathbb{F}_\ell$, with $M_\ell(F) \coloneqq \infty$ if there is no such zero.

Proposition 3.3.5. *Let $F \in \mathbb{Z}[T]$ be a polynomial of degree $D_0 \geq 1$, and let ℓ^e be a prime power such that F doesn't reduce to a constant modulo ℓ. Let $t \coloneqq t_\ell(F)$ and $M \coloneqq M_\ell(F)$.*

(i) If $\ell > 2$ and $e \geq t + 2$, then

$$\left| \sum_{v \bmod \ell^e} \chi_{0,\ell}(v) e(F(v)/\ell^e) \right| \leq D_0 \cdot \ell^{t/(M+1)} \cdot \ell^{e(1-1/(M+1))}.$$

(ii) For $\ell = 2$ and $e \geq t + 3$, we have

$$\left| \sum_{v \bmod 2^e} \chi_{0,2}(v) e(F(v)/2^e) \right| \leq 2D_0 \cdot 2^{t/(M+1)} \cdot 2^{e(1-1/(M+1))}.$$

Proof of Proposition 3.3.2. We start by showing that

$$\#\mathcal{V}_{N,M}\left(\ell^e;(w_i)_{i=1}^M\right)=\frac{\varphi(\ell^e)^N}{\ell^{eM}}\left(1+O\left(\frac{(2D)^N}{\ell^{N/D-M}}\right)\right) \tag{3.7}$$

uniformly for all primes $\ell > C = C(\mathbf{G})$, positive integers $e \geq 1$ and $N \geq MD+1$, and $w_i \in \mathbb{Z}/\ell^e\mathbb{Z}$. Indeed, by the orthogonality of additive characters, we can write

$$\begin{aligned}
&\#\mathcal{V}_{N,M}\left(\ell^e;(w_i)_{i=1}^M\right)\\
&=\#\left\{(v_1,\dots,v_N)\in(U_{\ell^e})^N:\ (\forall i)\ \sum_{j=1}^N G_i(v_j)\equiv w_i\ (\mathrm{mod}\ \ell^e)\right\}\\
&=\sum_{(v_1,\dots,v_N)\in(U_{\ell^e})^N}\prod_{i=1}^M\left(\frac{1}{\ell^e}\sum_{r_i\bmod\ell^e}e\left(-\frac{r_iw_i}{\ell^e}\right)\ e\left(\frac{r_i}{\ell^e}\sum_{j=1}^N G_i(v_j)\right)\right)\\
&=\frac{\varphi(\ell^e)^N}{\ell^{eM}}\left\{1+\frac{1}{\varphi(\ell^e)^N}\sum_{(r_1,\dots,r_M)\not\equiv(0,\dots,0)\bmod\ell^e}e\left(-\frac{1}{\ell^e}\sum_{i=1}^M r_iw_i\right)\left(Z_{\ell^e;\,r_1,\dots,r_M}\right)^N\right\},
\end{aligned} \tag{3.8}$$

where $Z_{\ell^e;\,r_1,\dots,r_M}\coloneqq\sum_{v\bmod\ell^e}\chi_{0,\ell}(v)e\left(\frac{1}{\ell^e}\sum_{i=1}^M r_iG_i(v)\right)$ and $\chi_{0,\ell}$ denotes the trivial character mod ℓ^e (which is also the trivial character mod ℓ).

Now in the case $D=1$, we must have $M=1$, so that we may write $G_1(T)=:AT+B$ for some integers $A\neq 0$ and B. For each nonzero residue r mod ℓ^e, we have $r=:\ell^{e-e_0}r'$ for some $e_0\in\{1,\cdots,e\}$ and some coprime residue r' mod ℓ^{e_0}. Hence, $|Z_{\ell^e;\,r}|=\ell^{e-e_0}\left|\sum_{\substack{v\bmod\ell^{e_0}\\ \gcd(v,\ell^{e_0})=1}}e(r'Av/\ell^{e_0})\right|$. The last sum being a Ramanujan sum is nonzero precisely when $\ell^{e_0-1}|r'A$ by equation (2.30). But this forces $e_0=1$ because $\ell\nmid A$ (by definition of $C_0(\mathbf{G})=C_0(\{G_1\})$) and $\ell\nmid r'$ (by definition of r'.) If $e_0=1$, then $|Z_{\ell^e;\,r}|\leq\ell^{e-1}$, and since there are at most ℓ many residues r mod ℓ^e which are

divisible by ℓ^{e-1}, we find from (3.8) that

$$\begin{aligned}\#\mathcal{V}_{N,M}\left(\ell^e;(w_i)_{i=1}^M\right) &= \frac{\varphi(\ell^e)^N}{\ell^e}\left\{1+O\left(\frac{1}{\varphi(\ell^e)^N}\cdot\ell\cdot(\ell^{e-1})^N\right)\right\}\\ &= \frac{\varphi(\ell^e)^N}{\ell^e}\left\{1+O\left(\frac{2^N}{\ell^{N-1}}\right)\right\}\end{aligned}$$

uniformly in $N\geq 1$. This establishes the bound (3.7) in the case $D=1$, so in order to complete the proof of (3.7), we may assume that $D\geq 2$.

Now for a given tuple $(r_1,\dots,r_M)\not\equiv(0,\dots,0) \bmod \ell^e$, we must have

$$\gcd(\ell^e,r_1,\dots,r_M)=\ell^{e-e_0}$$

for some $1\leq e_0\leq e$. Hence, we can write $r_i\coloneqq \ell^{e-e_0}r_i'$ for some $(r_1',\dots,r_M') \bmod \ell^{e_0}$ satisfying $(r_1',\dots,r_M')\not\equiv(0,\dots,0) \bmod \ell$, which shows that

$$\begin{aligned}|Z_{\ell^e;r_1,\dots,r_M}| &= \ell^{e-e_0}\left|\sum_{v \bmod \ell^{e_0}}\chi_{0,\ell}(v)e\left(\frac{1}{\ell^{e_0}}\sum_{i=1}^M r_i'G_i(v)\right)\right|\\ &= \ell^{e-e_0}\left|\sum_{v \bmod \ell^{e_0}}\chi_{0,\ell}(v)e\left(\frac{F(v)}{\ell^{e_0}}\right)\right|,\end{aligned}$$

where $F(T)\coloneqq\sum_{i=1}^M r_i'(G_i(T)-G_i(0))$. Now we observe that since $\ell>C(\mathbf{G})>C_0(\mathbf{G})$, the polynomials $\{G_i'\}_{i=1}^M$ are $\mathbb{F}_\ell$-linearly independent, hence so are the polynomials $\{G_i-G_i(0)\}_{i=1}^M$. This prevents the polynomial F from reducing to a constant mod ℓ (for if it did, then this constant would be zero). Consequently, if $e_0=1$, then Proposition 3.3.4 yields $|Z_{\ell^e;r_1,\dots,r_M}|\leq \ell^{e-e_0}\cdot D\ell^{1/2}=D\ell^{e-1/2}$. On the other hand, if $e_0\geq 2$, then from Proposition 3.3.5(i), we obtain $|Z_{\ell^e;r_1,\dots,r_M}|\leq \ell^{e-e_0}\cdot D\ell^{e_0(1-1/D)}=D\ell^{e-e_0/D}$; here we have noted that $\ell>C>2$, $t_\ell(F)=\operatorname{ord}_\ell(F')=\operatorname{ord}_\ell\big(\sum_{i=1}^M r_i'G_i'\big)=0\leq e_0-2$ and that $M_\ell(F)\leq\deg(F')\leq D-1$. For each $1\leq e_0\leq e$, there are

at most $\ell^{e_0 M}$ many possible tuples $(r_1', \dots, r_M')$ mod ℓ^{e_0}, hence at most $\ell^{e_0 M}$ tuples $(r_1, \dots, r_M)$ mod ℓ^e satisfying $\gcd(\ell^e, r_1, \dots, r_M) = \ell^{e-e_0}$. We deduce that

$$\begin{aligned}
&\sum_{(r_1,\dots,r_M)\not\equiv(0,\dots,0) \bmod \ell^e} |Z_{\ell^e; r_1,\dots,r_M}|^N \\
&\qquad \le \ell^M \left(D\ell^{e-1/2}\right)^N + \sum_{2\le e_0\le e} \ell^{e_0 M} \left(D\ell^{e-e_0/D}\right)^N \\
&\qquad \le \sum_{1\le e_0\le e} \ell^{e_0 M} \left(D\ell^{e-e_0/D}\right)^N \\
&\qquad \le \frac{D^N \ell^{eN}}{\ell^{N/D-M}} \sum_{r\ge 0} \frac{1}{\left(\ell^{N/D-M}\right)^r} \ll \frac{D^N \ell^{eN}}{\ell^{N/D-M}},
\end{aligned}$$

where the last bound uses the fact that $N/D - M \ge 1/D$, so that the last sum occurring in the above display is no more than $\sum_{r\ge 0} 2^{-r/D} \ll 1$. (It is while passing from the first line to the second in the above display where we use the assumption that $D \ge 2$.) Inserting the bound obtained above into (3.8) and noting that $\ell/(\ell-1) \le 2$ completes the proof of estimate (3.7).

Given an arbitrary positive integer q, let $\widetilde{q} := \prod_{\substack{\ell^e \| q \\ \ell \le C}} \ell^e$ denote the largest divisor of q supported on primes not exceeding the constant C (the "C-smooth part" of q). We can again invoke the orthogonality of additive characters to write, for any tuple of residues $(w_1, \dots, w_M)$ mod $\widetilde{q}$,

$$\begin{aligned}
&\#\mathcal{V}_{N,M}\left(\widetilde{q}; (w_i)_{i=1}^M\right) \\
&\quad = \#\left\{(v_1,\dots,v_N) \in (U_{\widetilde{q}})^N : \ (\forall i) \ \sum_{j=1}^N G_i(v_j) \equiv w_i \pmod{\widetilde{q}}\right\} \\
&\quad = \frac{1}{\widetilde{q}^M} \sum_{r_1,\dots,r_M \bmod \widetilde{q}} e\left(-\frac{1}{\widetilde{q}} \sum_{i=1}^M r_i w_i\right) \left(Z_{\widetilde{q}; r_1,\dots,r_M}\right)^N,
\end{aligned} \tag{3.9}$$

where $Z_{\widetilde{q};r_1,\dots,r_M} \coloneqq \sum_{v \bmod \widetilde{q}} \chi_{0,\widetilde{q}}(v) e\left(\frac{1}{\widetilde{q}}\sum_{i=1}^{M} r_i G_i(v)\right)$ and $\chi_{0,\widetilde{q}}$ denotes the trivial character mod $\widetilde{q}$.

Now with $\beta_1,\dots,\beta_M$ being the invariant factors of the matrix A_0 defined in (3.1) (listed in ascending order), we fix $R \coloneqq R(\widehat{G}) \in \mathbb{N}_{\geq 2}$ to be any integer constant such that

$$R > CD(4D|\beta_M|)^C.$$

Let $Q_1 \coloneqq \prod_{\ell^e \| \widetilde{q}:\ e>R} \ell^{e-R}$ and

$$Q_0 \coloneqq \widetilde{q}/Q_1 = \prod_{\ell^e \| \widetilde{q}} \ell^{\min\{e,R\}} = \prod_{\ell^e \| q:\ \ell \leq C} \ell^{\min\{e,R\}},$$

so that $Q_0 \mid q$ and $Q_0 \leq \prod_{\ell \leq C} \ell^R \ll 1$. We write $\#\mathcal{V}_{N,M}\left(\widetilde{q};(w_i)_{i=1}^M\right) =: S' + S''$, where S' counts the contribution of all tuples $(r_1,\dots,r_M)$ mod $\widetilde{q}$ where all the components r_i are divisible by Q_1, that is,

$$S' \coloneqq \frac{1}{\widetilde{q}^M} \sum_{\substack{r_1,\dots,r_M \bmod \widetilde{q} \\ (r_1,\dots,r_M) \equiv (0,\dots,0) \bmod Q_1}} e\left(-\frac{1}{\widetilde{q}}\sum_{i=1}^{M} r_i w_i\right) \left(Z_{\widetilde{q};r_1,\dots,r_M}\right)^N.$$

Any tuple $(r_1,\dots,r_M)$ mod $\widetilde{q}$ counted in S' is thus of the form $(Q_1 s_1,\dots,Q_1 s_M)$ for some tuple $(s_1,\dots,s_M)$ mod Q_0 that is uniquely determined by $(r_1,\dots,r_M)$. We find

that

$$\begin{aligned} Z_{\widetilde{q};\, r_1,\dots,r_M} &= \sum_{v \bmod \widetilde{q}} \chi_{0,\widetilde{q}}(v) e\left(\frac{1}{Q_0}\sum_{i=1}^{M} s_i G_i(v)\right) \\ &= \sum_{u \bmod Q_0} \chi_{0,Q_0}(u) e\left(\frac{1}{Q_0}\sum_{i=1}^{M} s_i G_i(u)\right) \sum_{\substack{v \in U_{\widetilde{q}} \\ v \equiv u \bmod Q_0}} 1 \\ &= \frac{\varphi(\widetilde{q})}{\varphi(Q_0)}\, Z_{Q_0;\, s_1,\dots,s_M} \end{aligned}$$

where the last equality above follows from a simple counting argument. Consequently,

$$S' = \frac{1}{\widetilde{q}^M}\left(\frac{\varphi(\widetilde{q})}{\varphi(Q_0)}\right)^N \sum_{s_1,\dots,s_M \bmod Q_0} e\left(-\frac{1}{Q_0}\sum_{i=1}^{M} s_i w_i\right) \left(Z_{Q_0;\, s_1,\dots,s_M}\right)^N.$$

An application of the orthogonality identity (3.9) with Q_0 playing the role of $\widetilde{q}$ yields

$$S' = \left(\frac{Q_0}{\widetilde{q}}\right)^M \left(\frac{\varphi(\widetilde{q})}{\varphi(Q_0)}\right)^N \#\mathcal{V}_{N,M}\left(Q_0; (w_i)_{i=1}^M\right). \tag{3.10}$$

Now we consider the sum

$$S'' = \frac{1}{\widetilde{q}^M} \sum_{\substack{r_1,\dots,r_M \bmod \widetilde{q} \\ (r_1,\dots,r_M) \not\equiv (0,\dots,0) \bmod Q_1}} e\left(-\frac{1}{\widetilde{q}}\sum_{i=1}^{M} r_i w_i\right) \left(Z_{\widetilde{q};\, r_1,\dots,r_M}\right)^N.$$

Consider any tuple $(r_1,\dots,r_M) \bmod \widetilde{q}$ occurring in S''. By the definition of Q_1, there exists a prime power $\ell^e \parallel \widetilde{q}$ for which $e > R$ but $v_\ell(\gcd(r_1,\dots,r_M)) < e - R$. Letting $Q' \coloneqq \widetilde{q}/\gcd(\widetilde{q}, r_1,\dots,r_M)$ and $r_i' \coloneqq r_i/\gcd(\widetilde{q}, r_1,\dots,r_M)$ (for $1 \le i \le M$), we therefore deduce that for any such aforementioned prime ℓ, we have $v_\ell(Q') > R$, so that Q' is not $(R+1)$-free. Moreover, $r_1',\dots,r_M'$ are uniquely determined mod Q' and satisfy $\gcd(Q', r_1',\dots,r_M') = 1$. Now for each i, we can write $r_i'/Q' = \sum_{\ell^{e_\ell} \parallel Q'} r_{i,\ell}'/\ell^{e_\ell}$

mod 1, where the sum is over the prime powers ℓ^{e_ℓ} exactly dividing Q'; [2] here, for each $\ell^{e_\ell} \parallel Q'$, $r'_{i,\ell}$ is uniquely determined mod ℓ^{e_ℓ} by the relation $r'_{i,\ell}\prod_{\substack{p^{e_p}\parallel Q'\\ p\neq\ell}} p^{e_p} \equiv r'_i \pmod{\ell^{e_\ell}}$. Since $\gcd(Q', r'_1, \dots, r'_M) = 1$, it follows that $\ell \nmid \gcd(r'_{1,\ell}, \dots, r'_{M,\ell})$ for each prime $\ell \mid Q'$. By the Chinese Remainder Theorem, we can factor

$$\begin{aligned} Z_{\widetilde{q};\, r_1,\dots,r_M} &= \frac{\varphi(\widetilde{q})}{\varphi(Q')} \sum_{v \bmod Q'} \chi_{0,Q'}(v) e\left(\frac{1}{Q'}\sum_{i=1}^{M} r'_i G_i(v)\right) \\ &= \frac{\varphi(\widetilde{q})}{\varphi(Q')} \prod_{\ell^{e_\ell}\parallel Q'} Z_{\ell^{e_\ell};\, r'_{1,\ell},\dots,r'_{M,\ell}}. \end{aligned} \tag{3.11}$$

Write $G'_i(T) =: \sum_{j=0}^{D-1} a_{i,j} T^j$ as in the discussion preceding (3.1). We claim that for any prime $\ell \mid Q'$,

$$\begin{aligned} t_\ell \coloneqq t_\ell(r'_{1,\ell}, \dots, r'_{M,\ell}) &\coloneqq \operatorname{ord}_\ell\left(\sum_{i=1}^{M} r'_{i,\ell} G'_i\right) \\ &= v_\ell\left(\gcd_{0\le j\le D-1} \sum_{i=1}^{M} a_{i,j} r'_{i,\ell}\right) \le v_\ell(\beta_M), \end{aligned} \tag{3.12}$$

where (recall) $\beta_1, \dots, \beta_M$ are the invariant factors of the matrix A_0 in (3.1). The third equality simply follows from the fact that

$$\sum_{i=1}^{M} r'_{i,\ell} G'_i(T) = \sum_{j=0}^{D-1}\left(\sum_{i=1}^{M} a_{i,j} r'_{i,\ell}\right) T^j.$$

To show the inequality in (3.12), it suffices to show that ℓ^{t_ℓ} must divide β_M. To do the latter, we recall that, by the theory of modules over a principal ideal domain, that there exist a $D \times D$ integer matrix P_0 and an $M \times M$ integer matrix R_0 such that $\det P_0, \det R_0 \in \{\pm 1\}$ and $P_0 A_0 R_0$ is the Smith normal form S_0 of A_0. As such, $P_0 A_0 = S_0 R_0^{-1}$ where the matrix R_0^{-1} has integer entries $(k_{i,j})_{1\le i,j\le M}$. Now

[2] We are just applying Bezout's identity; equivalently, this may be thought of as partial fraction decomposition over the integers.

ℓ^{t_ℓ} divides all the numbers $\{\sum_{i=1}^{M} a_{i,j} r'_{i,\ell} : 0 \leq j \leq D-1\}$, which are precisely the entries of the matrix $A_0 \begin{pmatrix} r'_{1,\ell} & \dots & r'_{M,\ell} \end{pmatrix}^{\intercal}$ (here $\begin{pmatrix} r'_{1,\ell} & \dots & r'_{M,\ell} \end{pmatrix}^{\intercal}$ denotes the column vector listing the $r'_{i,\ell}$). As such, ℓ^{t_ℓ} also divides the entries of the matrix $P_0 A_0 \begin{pmatrix} r'_{1,\ell} & \dots & r'_{M,\ell} \end{pmatrix}^{\intercal}$, and hence also those of the matrix

$$S_0 R_0^{-1} \begin{pmatrix} r'_{1,\ell} \\ \dots \\ r'_{M,\ell} \end{pmatrix}_{M\times 1} = \begin{pmatrix} \beta_1(k_{1,1} r'_{1,\ell} + \dots + k_{1,M} r'_{M,\ell}) \\ \dots \\ \beta_M(k_{M,1} r'_{1,\ell} + \dots + k_{M,M} r'_{M,\ell}) \\ 0 \\ \dots \\ 0 \end{pmatrix}_{D\times 1}. \tag{3.13}$$

But now if ℓ divides all of the numbers $k_{1,1} r'_{1,\ell} + \dots + k_{1,M} r'_{M,\ell}, \dots\dots, k_{M,1} r'_{1,\ell} + \dots + k_{M,M} r'_{M,\ell}$, then

$$R_0^{-1} \begin{pmatrix} r'_{1,\ell} \\ \dots \\ \dots \\ r'_{M,\ell} \end{pmatrix}_{M\times 1} = \begin{pmatrix} k_{1,1} r'_{1,\ell} + \dots + k_{1,M} r'_{M,\ell} \\ \dots \\ \dots \\ k_{M,1} r'_{1,\ell} + \dots + k_{M,M} r'_{M,\ell} \end{pmatrix}_{M\times 1} \equiv \begin{pmatrix} 0 \\ \dots \\ \dots \\ 0 \end{pmatrix}_{M\times 1} \pmod{\ell}.$$

This forces ℓ to divide $\gcd(r'_{1,\ell}, \dots, r'_{M,\ell})$, which is impossible since $\ell \mid Q'$ (see the line preceding (3.11)). Since ℓ^{t_ℓ} divides the entries of the rightmost matrix in (3.13), it follows that ℓ^{t_ℓ} must divide at least one of the invariant factors β_i, and hence must also divide β_M. This establishes our claim (3.12).

We will now show that for any prime power $\ell^{e_\ell} \parallel Q'$ for which $e_\ell > R$, we have

$$\begin{aligned} |Z_{\ell^{e_\ell}; r'_{1,\ell},\dots,r'_{M,\ell}}| &= \left| \sum_{v \bmod \ell^{e_\ell}} \chi_{0,\ell}(v) e\left(\frac{1}{\ell^{e_\ell}} \sum_{i=1}^{M} r'_{i,\ell} G_i(v)\right)\right| \\ &\le 2D|\beta_M|\ell^{e_\ell(1-1/D)}. \end{aligned} \tag{3.14}$$

To show this, we note that since $G_i'(T) = \sum_{j=0}^{D-1} a_{i,j}T^j$, we have $G_i(T) - G_i(0) = \sum_{j=0}^{D-1} \frac{a_{i,j}}{j+1}T^{j+1}$ (recall that $(j+1) \mid a_{i,j}$), so that with

$$c_\ell \coloneqq \operatorname{ord}_\ell\left(\sum_{i=1}^{M} r'_{i,\ell}(G_i(T) - G_i(0))\right) = v_\ell\left(\gcd_{0\le j\le D-1} \frac{\sum_{i=1}^{M} a_{i,j} r'_{i,\ell}}{j+1}\right), \tag{3.15}$$

we have

$$\begin{aligned} |Z_{\ell^{e_\ell}; r'_{1,\ell},\dots,r'_{M,\ell}}| &= \left| \sum_{v \bmod \ell^{e_\ell}} \chi_{0,\ell}(v) e\left(\frac{1}{\ell^{e_\ell - c_\ell}} \sum_{j=0}^{D-1} \left(\ell^{-c_\ell} \frac{\sum_{i=1}^{M} a_{i,j} r'_{i,\ell}}{j+1}\right) v^{j+1}\right)\right| \\ &= \ell^{c_\ell} \left| \sum_{v \bmod \ell^{e_\ell - c_\ell}} \chi_{0,\ell}(v) e\left(\frac{\widetilde{F}(v)}{\ell^{e_\ell - c_\ell}}\right)\right|, \end{aligned}$$

where $\widetilde{F}(T) \coloneqq \sum_{j=0}^{D-1} \left(\ell^{-c_\ell} \frac{\sum_{i=1}^{M} a_{i,j} r'_{i,\ell}}{j+1}\right) T^{j+1} \in \mathbb{Z}[T]$. By (3.15) and (3.12), we see that $\widetilde{F}$ cannot reduce to a constant mod ℓ and that $c_\ell \le t_\ell \le v_\ell(\beta_M)$. Furthermore, (3.12) also shows that

$$\begin{aligned} \operatorname{ord}_\ell(\widetilde{F}') &= \operatorname{ord}_\ell\left(\sum_{j=0}^{D-1}\left(\sum_{i=1}^{M} a_{i,j} r'_{i,\ell}\right) T^j\right) - c_\ell = t_\ell - c_\ell \\ &\le v_\ell(\beta_M) - c_\ell \le R - 3 - c_\ell < (e_\ell - c_\ell) - 3. \end{aligned}$$

(Here we use $e_\ell > R > |\beta_M| + 3$.) Consequently, some subpart of Proposition 3.3.5

applies, yielding

$$\begin{aligned}|Z_{\ell^{e_\ell};r'_{1,\ell},\dots,r'_{M,\ell}}| &\le \ell^{c_\ell}\cdot 2D\ell^{\mathrm{ord}_\ell(\widetilde{F}')}\cdot \ell^{(e_\ell-c_\ell)(1-1/(M_\ell(\widetilde{F})+1))}\\ &\le \ell^{c_\ell}\cdot 2D\ell^{v_\ell(\beta_M)-c_\ell}\cdot \ell^{e_\ell(1-1/D)} \le 2D|\beta_M|\ell^{e_\ell(1-1/D)}.\end{aligned}$$

Here, $M_\ell(\widetilde{F})$ is the largest multiplicity of a zero in $\mathbb{F}_\ell$ of the polynomial $\ell^{-\mathrm{ord}_\ell(\widetilde{F}')}\widetilde{F}'$, and we have used that this multiplicity is no more than $\deg(\widetilde{F}') \le D-1$. This establishes (3.14).

Applying the bound (3.14) to each prime power $\ell^{e_\ell} \parallel Q'$ for which $e_\ell > R$, and applying the trivial bound $|Z_{\ell^{e_\ell};r'_{1,\ell},\dots,r'_{M,\ell}}| \le \varphi(\ell^{e_\ell})$ for all the other prime powers $\ell^{e_\ell} \parallel Q'$, the factorization (3.11) yields

$$\begin{aligned}|Z_{\widetilde{q};r_1,\dots,r_M}| &\le \frac{\varphi(\widetilde{q})}{\varphi(Q')}\left(\prod_{\substack{\ell^{e_\ell}\parallel Q'\\ e_\ell\le R}}\varphi(\ell^{e_\ell})\right)\cdot\left(\prod_{\substack{\ell^{e_\ell}\parallel Q'\\ e_\ell> R}}2D|\beta_M|\ell^{e_\ell(1-1/D)}\right)\\ &\le (2D|\beta_M|)^{\omega(Q')}\cdot\varphi(\widetilde{q})\cdot\prod_{\substack{\ell^{e_\ell}\parallel Q'\\ e_\ell> R}}\left(\frac{\ell^{e_\ell(1-1/D)}}{\varphi(\ell^{e_\ell})}\right)\\ &\le (4D|\beta_M|)^{C}\cdot\frac{\varphi(\widetilde{q})}{A^{1/D}}.\end{aligned}$$

Here A denotes the $(R+1)$-full part of Q' and in the last bound above, we have noted that $\omega(Q') \le \omega(\widetilde{q}) \le \sum_{\ell\le C}1 \le C$. Since Q' is not $(R+1)$-free, we have $A > 1$.

Applying this bound for each of the sums $Z_{\widetilde{q};\, r_1,\dots,r_M}$ occurring in S'', we obtain

$$|S''| \le \frac{(4D|\beta_M|)^{CN}\varphi(\widetilde{q})^N}{\widetilde{q}^M} \sum_{\substack{A|\widetilde{q}:\ A>1\\ A \text{ is } (R+1)\text{-full}}} \frac{1}{A^{N/D}} \cdot \sum_{\substack{Q',r'_1,\dots,r'_M\\ Q'|\widetilde{q}:\,(R+1)\text{-full part of } Q' \text{ is } A\\ r'_1,\dots,r'_M \bmod Q'\\ \gcd(r'_1,\dots,r'_M,Q')=1}} \sum_{\substack{r_1,\dots,r_M \bmod \widetilde{q}\\ Q'=\widetilde{q}/\gcd(\widetilde{q},r_1,\dots,r_M)\\ (\forall i)\ r'_i=r_i/\gcd(\widetilde{q},r_1,\dots,r_M)}} 1.$$

Since any choice of $Q' \mid \widetilde{q}$ and residues $r'_1,\dots,r'_M \bmod Q'$ uniquely determines $r_1,\dots,r_M \bmod \widetilde{q}$ by the relations $r_i = r'_i\widetilde{q}/Q'$, we see that

$$\begin{aligned}|S''| &\le \frac{(4D|\beta_M|)^{CN}\varphi(\widetilde{q})^N}{\widetilde{q}^M} \sum_{\substack{A|\widetilde{q}:\ A>1\\ A \text{ is } (R+1)\text{-full}}} \frac{1}{A^{N/D}} \cdot \sum_{\substack{Q'|\widetilde{q}\\ (R+1)\text{-full part of } Q' \text{ is } A}} \sum_{\substack{r'_1,\dots,r'_M \bmod Q'\\ \gcd(r'_1,\dots,r'_M,Q')=1}} 1\\ &\le \frac{(4D|\beta_M|)^{CN}\varphi(\widetilde{q})^N}{\widetilde{q}^M} \sum_{\substack{A|\widetilde{q}:\ A>1\\ A \text{ is } (R+1)\text{-full}}} \frac{1}{A^{N/D}} \sum_{\substack{Q'|\widetilde{q}\\ (R+1)\text{-full part of } Q' \text{ is } A}} (Q')^M.\end{aligned}$$

Now any divisor Q' of $\widetilde{q}$ with $(R+1)$-full part equal to A must be of the form Ad for some $(R+1)$-free divisor d of $\widetilde{q}$, and $d \le \prod_{\ell|\widetilde{q}} \ell^R \le \prod_{\ell\le C} \ell^R \le C^{CR} \ll 1$. Consequently the innermost sum in the last expression above is at most $A^M \sum_{d \text{ is } (R+1)\text{-free}}^{d|\widetilde{q}} d^M \ll A^M$, leading to

$$|S''| \ll \frac{(4D|\beta_M|)^{CN}\varphi(\widetilde{q})^N}{\widetilde{q}^M} \sum_{\substack{A|\widetilde{q}:\ A>1\\ A \text{ is } (R+1)\text{-full}}} \frac{1}{A^{N/D-M}}, \tag{3.16}$$

Since $N \ge MD+1$, we have $N/D - M \ge 1/D$, so that for all primes ℓ, we have

$$\sum_{v\ge R+1} \frac{1}{\ell^{v(N/D-M)}} \le \frac{1}{\ell^{(R+1)(N/D-M)}} \sum_{v\ge 0} \frac{1}{\ell^{v/D}}$$

$$\leq \frac{1}{\ell^{(R+1)(N/D-M)}} \cdot \frac{2^{1/D}}{2^{1/D}-1} \leq \frac{2D \cdot 2^{1/D}}{2^{(R+1)/D}} \leq \frac{2D^2}{R} \leq \frac{1}{2}.$$

(Here, we have noted that $2^{1/D} - 1 = \exp(\log 2/D) - 1 \geq \log 2/D > 1/2D$ and that $2^{R/D} \geq R/D \geq 4D$.) This means that for all primes $\ell \leq C$, we have

$$\log\left(1 + \sum_{v \geq R+1} \frac{1}{\ell^{v(N/D-M)}}\right) \ll \sum_{v \geq R+1} \frac{1}{\ell^{v(N/D-M)}} \ll \frac{1}{\ell^{(R+1)(N/D-M)}} \ll \frac{1}{\ell^{RN/D}} \leq \frac{1}{2^{RN/D}},$$

and since $\widetilde{q}$ is C-smooth, this leads to

$$\sum_{\substack{A \mid \widetilde{q}:\ A>1 \\ A \text{ is } (R+1)\text{-full}}} \frac{1}{A^{N/D-M}} \leq \prod_{\ell \mid \widetilde{q}} \left(1 + \sum_{v \geq R+1} \frac{1}{\ell^{v(N/D-M)}}\right) - 1 = \exp\left(O\left(\frac{1}{2^{RN/D}}\right)\right) - 1 \ll \frac{1}{2^{RN/D}}.$$

Inserting this into (3.16), we obtain

$$|S''| \ll \left(\frac{(4D|\beta_M|)^C}{2^{R/D}}\right)^N \frac{\varphi(\widetilde{q})^N}{\widetilde{q}^M} \leq C^{-N} \frac{\varphi(\widetilde{q})^N}{\widetilde{q}^M},$$

noting in the last step that $(4D|\beta_M|)^C/2^{R/D} \leq D(4D|\beta_M|)^C/R \leq C^{-1}$, by the definition of R. From (3.10), we now obtain

$$\begin{aligned} \#\mathcal{V}_{N,M}\left(\widetilde{q}; (w_i)_{i=1}^M\right) &= S' + S'' \\ &= \left(\frac{Q_0}{\widetilde{q}}\right)^M \varphi(\widetilde{q})^N \left\{ \frac{\#\mathcal{V}_{N,M}\left(Q_0; (w_i)_{i=1}^M\right)}{\varphi(Q_0)^N} + O\left(C^{-N}\right) \right\}. \end{aligned}$$

Finally, writing

$$\#\mathcal{V}_{N,M}\left(q;(w_i)_{i=1}^M\right)=\#\mathcal{V}_{N,M}\left(\widetilde{q};(w_i)_{i=1}^M\right)\prod_{\ell^e\|q:\ \ell>C}\#\mathcal{V}_{N,M}\left(\ell^e;(w_i)_{i=1}^M\right),$$

and invoking the estimate above for $\#\mathcal{V}_{N,M}\left(\widetilde{q};(w_i)_{i=1}^M\right)$ in conjunction with (3.7) for all the powers $\ell^e \| q$ of primes $\ell > C$, we obtain the estimate claimed in Proposition 3.3.2. □

Section 3.4

Joint equidistribution without input restriction: Proof of Theorem 3.1.1

By Proposition 3.3.1, it remains to show that the count of inconvenient $n \le x$ for which all the $g_i(n) \equiv b_i \pmod q$ is $o(x/q^M)$ as $x \to \infty$ in the prescribed ranges of q. Setting $z := x^{1/\log_2 x}$, we first remove from these $n \le x$, the ones that either have $P(n) \le z$ or have a repeated prime factor exceeding y. By Lemma 2.3.1, the number of $n \le x$ having $P(n) \le z$ is $O\left(x/(\log x)^{(1+o(1))\log_3 x}\right)$, and as seen before, the number of $n \le x$ having a repeated prime factor exceeding y is $O(x/y)$. Both of these bounds being $o(x/q^M)$, it suffices to consider the contribution Σ_0 of those inconvenient $n \le x$ which have $P(n) > z$ and do not possess any repeated prime factor exceeding y.

By the definition of "inconvenient", any n counted in Σ_0 must also have $P_J(n) \le y$, and hence can be written in the form $n = mP$, where $P := P(n) > z$, $P_J(m) \le y$ and $\gcd(m, P) = 1$. As such, $g_i(n) = g_i(m) + G_i(P)$, and the congruence $g_i(n) \equiv b_i \pmod q$ shows that $P \bmod q$ lies in the set $\mathcal{V}_{1,M}\left(q;(b_i - g_i(m))_{i=1}^M\right)$. Setting

$$\xi_{\mathbf{G}}(q) := \max\{\#\mathcal{V}_{1,M}\left(q;(w_i)_{i=1}^M\right) : w_1,\dots,w_M \bmod q\},$$

the Brun-Titchmarsh theorem shows that for a given m, the number of possibilities for P is no more than

$$\sum_{\substack{z<P\le x/m\\ P \bmod q\ \in \mathcal{V}_{1,M}\left(q;(b_i-g_i(m))_{i=1}^M\right)}} 1 \ \ll\ \xi_{\mathbf{G}}(q)\frac{x/m}{\varphi(q)\log(z/q)} \ll\ \frac{\xi_{\mathbf{G}}(q)}{\varphi(q)}\ \frac{x\log_2 x}{m\log x}. \tag{3.17}$$

To estimate the sum of $1/m$ over $m \le x$ having $P_J(m) \le y$, we write each such m in the form BA where $P(B) \le y < P^-(A)$ and $\Omega(A) \le J$. As such, the sum of the reciprocals of the possible A is at most

$$\sum_{\substack{A\le x\\ \Omega(A)\le J}} \frac{1}{A} \le \left(1+\sum_{p\le x}\frac{1}{p}\right)^J \le (2\log_2 x)^J \le \exp\left(O((\log_3 x)^2)\right),$$

while the sum of the reciprocals of the possible B is no more than

$$\begin{aligned}\sum_{B:\ P(B)\le y}\frac{1}{B} &\le \prod_{p\le y}\left(1+\frac{1}{p}+O\left(\frac{1}{p^2}\right)\right)\\ &\le \exp\left(\sum_{p\le y}\frac{1}{p}+O(1)\right) \ll \log y.\end{aligned}$$

Collecting estimates, we obtain

$$\sum_{\substack{m\le x\\ P_J(m)\le y}}\frac{1}{m} \ll (\log x)^{\delta/2}\exp\left(O((\log_3 x)^2)\right), \tag{3.18}$$

which from the bound (3.17) reveals that

$$\Sigma_0 \ll \frac{\xi_{\mathbf{G}}(q)}{\varphi(q)}\frac{x\log_2 x}{(\log x)^{1-\delta/2}}\exp\left(O((\log_3 x)^2)\right) \ll \frac{\xi_{\mathbf{G}}(q)}{q}\frac{x}{(\log x)^{1-2\delta/3}}. \tag{3.19}$$

We now proceed to show the assertions in the three subparts of the theorem.

Proof of (i), (ii). If at least one of $G_1, \dots, G_M$ is linear, then $\xi_{\mathbf{G}}(q) \ll 1$ and we obtain $\Sigma_0 \ll x/q(\log x)^{1-2\delta/3}$. This is $o(x/q^M)$ as soon as $q^{M-1} \leq (\log x)^{1-\delta}$. This condition is tautological if $M = 1$, and for $M \geq 2$ it is equivalent to $q \leq (\log x)^{(1-\delta)/(M-1)}$.

If q is squarefree, then with $D_1 = \deg G_1$, we see that $\#\mathcal{V}_{1,M}\left(q; (w_i)_{i=1}^M\right) \leq \#\mathcal{V}_{1,1}\left(q; w_1\right)$ $= \prod_{\ell | q} \#\mathcal{V}_{1,1}\left(\ell; w_1\right) \ll (D_1)^{\omega(q)} \leq (\log x)^{\delta/100}$. (Here we have noted that for any sufficiently large ℓ, the polynomial $G_1(T) - w_1$ cannot vanish identically mod ℓ, and hence has at most D_1 roots mod ℓ.) As such, from (3.19), it follows that $\Sigma_0 \ll x/q(\log x)^{1-3\delta/4}$. This is automatically $o(x/q^M)$ if $M = 1$, while for $M \geq 2$, we need only assume that $q \leq (\log x)^{(1-\delta)/(M-1)}$.

Proof of (iii). Finally, assume (by relabelling if necessary) that $\deg G_1 = D_{\min}$. By Lemma 2.5.2, we have $\#\mathcal{V}_{1,M}\left(q; (w_i)_{i=1}^M\right) \leq \#\mathcal{V}_{1,1}\left(q; w_1\right) \ll q^{1-1/D_{\min}}$. (To be precise, we apply Lemma 2.5.2 to the polynomial congruence $(G_1(T) - w_1)/d \equiv 0 \pmod{q/d}$, where d is the greatest common divisor of q and the coefficients of the polynomial $G_1(T) - w_1$. Note that each solution mod q/d lifts to a solution mod q in $\leq d \ll 1$ ways.) Consequently, we obtain $\Sigma_0 \ll x/q^{1/D_{\min}}(\log x)^{1-2\delta/3}$. This is $o(x/q^M)$ as soon as $q^{M-1/D_{\min}} \leq (\log x)^{1-\delta}$, completing the proof of the theorem.

3.4.1. Optimality of range of q in Theorem 3.1.1

We will now construct polynomials $G_1, \dots, G_M$ which will show that the various restrictions on the range of q in Theorem 3.1.1 are all essentially optimal. To that end, let $G \in \mathbb{Z}[T]$ be any monic polynomial having a nonzero integer root a. Let $G_i(T) \coloneqq G(T)^i$, so that the polynomials $\{G_i'\}_{i=1}^M$ having distinct degrees are automatically $\mathbb{Q}$-linearly independent. Letting $C_0(\mathbf{G})$ be the constant coming from (3.2), Corollary 3.2.3 shows that any integer q having $P^-(q) > C_0(\mathbf{G})$ lies in $\mathcal{Q}_{(g_1,\dots,g_M)}$. Moreover, any prime p satisfying $p \equiv a \pmod q$ also satisfies $G(p) \equiv 0 \pmod q$, hence also $g_i(p) = G_i(p) = G(p)^i \equiv 0 \pmod q$ for all i. As such, for all $q \leq (\log x)^K$ having

$P^-(q) > \max\{|a|, C_0(\mathbf{G})\}$, the Siegel–Walfisz Theorem yields

$$\sum_{\substack{n\le x\\ (\forall i)\ g_i(n)\equiv 0 \,(\mathrm{mod}\ q)}} 1 \ge \sum_{\substack{p\le x\\ p\equiv a \,(\mathrm{mod}\ q)}} 1 \gg \frac{x}{\varphi(q)\log x} \gg \frac{x}{q\log x}.$$

For any $M \ge 2$, this last expression grows strictly faster than x/q^M as soon as q^{M-1} grows faster than $\log x$, for instance if $q > (\log x)^{(1+\delta)/(M-1)}$. This construction shows that the range of q in Theorem 3.1.1(ii) is essentially optimal.

Now consider any $M \ge 1$, $D \ge 1$, and let $G(T) \coloneqq (T-1)^d$. Then with $G_i(T) = G(T)^i$, we see that $D_{\min} = d$. For moduli q of the form q_1^d (for some $q_1 > 1$), any prime $p \equiv 1 \pmod{q_1}$ satisfies $G(p) = (p-1)^d \equiv 0 \pmod{q}$. Hence, if $q_1 \le (\log x)^K$ has $P^-(q_1) > C_0(\mathbf{G})$, then $q = q_1^d \le (\log x)^{Kd}$ also has $P^-(q) > C_0(\mathbf{G})$, and we find that on the one hand $q \in \mathcal{Q}_{(g_1,\dots,g_M)}$, while on the other,

$$\sum_{\substack{n\le x\\ (\forall i)\ g_i(n)\equiv 0 \,(\mathrm{mod}\ q)}} 1 \ge \sum_{\substack{p\le x\\ p\equiv 1 \,(\mathrm{mod}\ q_1)}} 1 \gg \frac{x}{\varphi(q_1)\log x} \gg \frac{x}{q^{1/d}\log x}.$$

This last expression grows strictly faster than x/q^M as soon as $q^{M-1/d}$ grows faster than $\log x$, for instance if $q > (\log x)^{(1+\delta)(M-1/d)^{-1}}$. Since $d = D_{\min}$, this example shows that the range of q in Theorem 3.1.1(iii) is essentially optimal as well.

Section 3.5

Complete uniformity for general moduli: Proof of Theorem 3.1.2

In section 3.3, we had defined $J = \lfloor \log_3 x \rfloor$ and for the purposes of this theorem, we took $\delta \coloneqq 1$, so that $y = \exp((\log x)^{1/2})$. If x is sufficiently large then any convenient

n has $P_{MD+1}(n) \geq P_J(n) \geq y > q$. Moreover, by Lemma 3.3.3, the number of $n \leq x$ having $P_{MD+1}(n) \leq q$ is $o(x)$. By Proposition 3.3.1, it remains to show that there are $o(x/q^M)$ many inconvenient $n \leq x$ having $P_{MD+1}(n) > q$ and satisfying $g_i(n) \equiv b_i \pmod{q}$ for all i.

Now by the arguments in the beginning of the previous section, the number of $n \leq x$ which either have $P(n) \leq z = x^{1/\log_2 x}$ or have a repeated prime factor exceeding y is $o(x/q^M)$. As such, in order to complete the proof of the theorem, it suffices to show that

$$\sum_{\substack{n\leq x:\ P_{MD+1}(n)>q \\ P_J(n)\leq y;\ P(n)>z \\ p>y \Longrightarrow p^2\nmid n \\ (\forall i)\ g_i(n)\equiv b_i \pmod{q}}} 1 \quad \ll \quad \frac{x}{q^M(\log x)^{1/3}} \tag{3.20}$$

uniformly in $q \leq (\log x)^K$ and in residues $(b_1, \ldots, b_M) \bmod q$.

Assume first that $M \geq 2$. To show (3.20) write the count on the left hand side as

$$\Sigma_0 + \Sigma_1 + \Sigma_2 + \Sigma,$$

where

- Σ_0 counts those n which are exactly divisible by at least $MD+1$ many distinct primes exceeding q,
- For $r \in \{1, 2\}$, Σ_r counts the n that are exactly divisible by at least $(M-r)D+1$ but at most $(M-r+1)D$ many distinct primes exceeding q, and
- Σ counts the remaining n, namely, those that are exactly divisible by at most $(M-2)D$ many distinct primes exceeding q.

We proceed to show that the expression on the right hand side of (3.20) bounds

each of Σ_0, Σ_1, Σ_2 and Σ. To do this, we shall bound the cardinalities of the sets $\mathcal{V}_{N,M}\left(q;(w_i)_{i=1}^{M}\right)$ that arise by discarding some of the congruences defining the set. The following consequence of Proposition 3.3.2 will be useful: for any fixed $r \in \{0,1,\dots,M-1\}$, we have

$$\#\mathcal{V}_{(M-r)D+1,M-r}\left(q;(w_i)_{i=1}^{M-r}\right) \ll \frac{\varphi(q)^{(M-r)D+1}}{q^{M-r}} \exp\left(O\left((\log q)^{1-1/D}\right)\right) \tag{3.21}$$

uniformly in moduli $q>1$ and in residue classes $(w_1,\dots,w_M) \bmod q$. Here, we have noted that $\{G_i'\}_{i=1}^{M-r}$ are $\mathbb{Q}$-linearly independent, as well as the facts that $\max_{1\le i\le M-r}\deg G_i \le D$, and that

$$\prod_{\ell\mid q}\left(1+O\left(\frac{1}{\ell^{1/D}}\right)\right) \le \exp\left(O\left(\sum_{\ell\le\omega(q)}\frac{1}{\ell^{1/D}}\right)\right) \ll \exp\left(O\left((\log q)^{1-1/D}\right)\right),$$

with the last sum on ℓ being bounded by partial summation and Chebyshev's estimates.

Bounding Σ_0: Any n counted in Σ_0 is exactly divisible by at least $M(D+1)+1$ many prime factors exceeding q and has $P(n)>z$, $P_J(n)\le y$. Hence, n can be written in the form $mP_1\cdots P_{M(D+1)+1}$, where $P_1 \coloneqq P(n) > z$, $q < P_{M(D+1)+1} < \cdots < P_1$, $P_J(m)\le y$ and $\gcd(m, P_1\cdots P_{M(D+1)+1})=1$. As such, $g_i(n)=g_i(m)+\sum_{1\le j\le M(D+1)+1}G_i(P_j)$ and the congruences $g_i(n)\equiv b_i \pmod q$ force $(P_1,\dots,P_{M(D+1)+1})$ mod q to lie in the set $V_m \coloneqq \mathcal{V}_{M(D+1)+1,M}\left(q;(b_i-g_i(m))_{i=1}^{M}\right)$.

Given m and $\widehat{v} \coloneqq (v_1,\dots,v_{M(D+1)+1}) \in V_m$, we count the number of possible $P_1,\dots,P_{M(D+1)+1}$ satisfying $(P_1,\dots,P_{M(D+1)+1}) \equiv \widehat{v} \bmod q$. For a given choice of $P_2,\dots,P_{M(D+1)+1}$, the number of possible P_1 is, by the Brun-Titchmarsh inequality,

no more than

$$\sum_{\substack{z<P_1\le x/mP_2\cdots P_{M(D+1)+1}\\ P_1\equiv v_1 \pmod q}} 1 \ll \frac{x/mP_2\cdots P_{M(D+1)+1}}{\varphi(q)\log(z/q)} \ll \frac{x\log_2 x}{\varphi(q)mP_2\cdots P_{M(D+1)+1}\log x}.$$

For each $j \in \{2,\dots,M(D+1)+1\}$, the sum on P_j is, by Brun-Titchmarsh and partial summation, no more than

$$\sum_{\substack{q<p\le x\\ p\equiv v_j \pmod q}} \frac{1}{p} \ll \frac{\log_2 x}{\varphi(q)}.$$

Hence, given m and $\widehat{v}=(v_1,\dots,v_{M(D+1)+1})\in V_m$, the number of possible $P_1,\dots,P_{M(D+1)+1}$ satisfying $(P_1,\dots,P_{M(D+1)+1})\equiv \widehat{v} \bmod q$ is

$$\ll \frac{x(\log_2 x)^{O(1)}}{\varphi(q)^{M(D+1)+1}m\log x},$$

leading to

$$\Sigma_0 \ll \frac{x(\log_2 x)^{O(1)}}{\log x}\sum_{\substack{m\le x\\ P_J(m)\le y}}\frac{1}{m}\cdot\frac{\#V_m}{\varphi(q)^{M(D+1)+1}}.$$

Using (3.21) to bound $V_m = \mathcal{V}_{M(D+1)+1,M}\left(q;(b_i-g_i(m))_{i=1}^M\right)$, followed by (3.18) to bound the resulting sum on m, we deduce that

$$\Sigma_0 \ll \frac{x(\log_2 x)^{O(1)}}{q^M\log x}\exp\left(O\left((\log q)^{1-1/D}\right)\right)\sum_{\substack{m\le x\\ P_J(m)\le y}}\frac{1}{m} \ll \frac{x}{q^M(\log x)^{1/3}},$$

yielding the desired bound for Σ_0. It is to be noted that this bound on Σ_0 holds true for any $M\ge 1$.

Bounding Σ_1*:* Recall that $\Omega^*_{>q}(n) := \sum_{\substack{p^k \| n \\ p>q,\ k>1}} k$ counts (with multiplicity) the number of prime factors of n exceeding q that appear to an exponent larger than 1 in the prime factorization of n; as such, the squarefull part of n (i.e., the largest squarefull divisor of n) exceeds $q^{\Omega^*_{>q}(n)}$.

Now, any n counted in Σ_1 is exactly divisible by least $(M-1)D+1$ but at most MD many distinct primes exceeding q. Since $P_{M(D+1)+1}(n) > q$, it follows that $\Omega^*_{>q}(n) \geq 2$, so that the squarefull part of n exceeds q^2. As such, n can be written in the form $mSP_{(M-1)D+1} \cdots P_1$, where $m, S, P_{(M-1)D+1}, \ldots, P_1$ are pairwise coprime, $P_1 := P(n) > z$, $q < P_{(M-1)D+1} < \cdots < P_1$, $P_J(m) \leq y$, and $S > q^2$ is squarefull. Since

$$g_i(n) = g_i(mS) + \sum_{1 \leq j \leq (M-1)D+1} G_i(P_j),$$

the congruence conditions $g_i(n) \equiv b_i \pmod q$, considered for $1 \leq i \leq M-1$, force $(P_1, \ldots, P_{(M-1)D+1}) \equiv \widehat{v} \bmod q$ for some

$$\widehat{v} := (v_1, \ldots, v_{(M-1)D+1}) \in \mathcal{V}_{(M-1)D+1, M-1}\left(q; (b_i - g_i(mS))_{i=1}^{M-1}\right).$$

Given m, S and $\widehat{v}$, the argument given for bounding Σ_0 above shows that the number of possible $P_1, \ldots, P_{(M-1)D+1}$ satisfying $(P_1, \ldots, P_{(M-1)D+1}) \equiv \widehat{v} \bmod q$ is

$$\ll \frac{x(\log_2 x)^{O(1)}}{\varphi(q)^{(M-1)D+1} mS \log x}.$$

This yields

$$\Sigma_1 \ll \frac{x(\log_2 x)^{O(1)}}{\log x} \sum_{\substack{m \leq x \\ P_J(m) \leq y}} \frac{1}{m}.$$

$$\sum_{S>q^2 \text{ squarefull}} \frac{1}{S} \cdot \frac{\#\mathcal{V}_{(M-1)D+1,M-1}\left(q;(b_i-g_i(mS))_{i=1}^{M-1}\right)}{\varphi(q)^{(M-1)D+1}},$$

so that by (3.21),

$$\Sigma_1 \ll \frac{x(\log_2 x)^{O(1)}}{q^{M-1}\log x}\exp\left(O\left((\log q)^{1-1/D}\right)\right)\sum_{\substack{m\le x\\ P_J(m)\le y}}\frac{1}{m}\sum_{S>q^2 \text{ squarefull}}\frac{1}{S}.$$

Using (3.18) along with the bound $\sum_{S>q^2 \text{ squarefull}} 1/S \ll 1/q$, we obtain

$$\Sigma_1 \ll \frac{x(\log_2 x)^{O(1)}}{q^M(\log x)^{1/2}}\exp\left(O\left((\log q)^{1-1/D}+(\log_3 x)^2\right)\right) \ll \frac{x}{q^M(\log x)^{1/3}},$$

showing the desired bound for Σ_1.

Bounding Σ_2: Any n counted in Σ_2 is exactly divisible by least $(M-2)D+1$ but at most $(M-1)D$ many distinct primes exceeding q. Since $P_{M(D+1)+1}(n) > q$, it follows that $\Omega^*_{>q}(n) \ge MD+1-(M-1)D = D+1$. Now assume that $D \ge 3$, so that $\Omega^*_{>q}(n) \ge 4$, and the squarefull part of n exceeds q^4. In this case, any n counted in Σ_2 can be written in the form $mSP_{(M-2)D+1}\cdots P_1$, where $m, S, P_{(M-2)D+1}, \dots, P_1$ are pairwise coprime, $P_1 \coloneqq P(n) > z$, $q < P_{(M-2)D+1} < \cdots < P_1$, $P_J(m) \le y$, and $S > q^4$ is squarefull. Since $g_i(n) = g_i(mS) + \sum_{1\le j\le (M-2)D+1} G_i(P_j)$, the congruence conditions $g_i(n) \equiv b_i \pmod q$, considered for $1 \le i \le M-2$, force $(P_1,\dots,P_{(M-2)D+1}) \equiv \widehat{v} \bmod q$ for some

$$\widehat{v} \coloneqq (v_1,\dots,v_{(M-2)D+1}) \in \mathcal{V}_{(M-2)D+1,M-2}\left(q;(b_i-g_i(mS))_{i=1}^{M-2}\right).$$

Replicating the argument given for Σ_1 shows that

$$\begin{aligned}\Sigma_2 &\ll \frac{x(\log_2 x)^{O(1)}}{\log x} \sum_{\substack{m\le x\\ P_J(m)\le y}} \frac{1}{m}\cdot \\ &\qquad \sum_{S>q^4 \text{ squarefull}} \frac{1}{S}\cdot \frac{\#\mathcal{V}_{(M-2)D+1,M-2}\left(q;(b_i-g_i(mS))_{i=1}^{M-2}\right)}{\varphi(q)^{(M-2)D+1}} \\ &\ll \frac{x(\log_2 x)^{O(1)}}{q^{M-2}\log x}\exp\left(O\left((\log q)^{1-1/D}\right)\right) \sum_{\substack{m\le x\\ P_J(m)\le y}} \frac{1}{m} \sum_{S>q^4 \text{ squarefull}} \frac{1}{S} \\ &\ll \frac{x(\log_2 x)^{O(1)}}{q^M(\log x)^{1/2}}\exp\left(O\left((\log q)^{1-1/D}+(\log_3 x)^2\right)\right) \\ &\ll \frac{x}{q^M(\log x)^{1/3}}.\end{aligned}$$

showing the desired bound for Σ_2 in the case $D \ge 3$.

Now assume that $D = 2$, so that $2 \le M \le D = 2$ forces $M = 2$. Any n counted in Σ_2 has $P_5(n) > q$ but at most $(M-1)D = 2$ of these exactly divide n. Hence, n is either divisible by the cube of a prime exceeding q or is (exactly) divisible by the squares of two distinct primes exceeding q. Any n of the first kind can be written in the form mp^sP for some primes p, P satisfying $P = P(n) > z$ and $q < p < P$, and some positive integers s, m satisfying $s \ge 3$, $P_J(m) \le y$. Given m, p and s, the number of possible $P \in (z, x/mp^s]$ is $O(x/mp^s \log z)$. Summing this over all $s \ge 3$, all $p > q$, and then over all possible m, and invoking (3.18) in conjunction with the fact that $\sum_{p>q} 1/p^3 \ll 1/q^2$, we find that the total contribution of all n of the first kind is $\ll x/q^2(\log x)^{1/3}$ which is absorbed in the desired expression.

On the other hand, if n is divisible by the squares of two distinct primes exceeding q, then it is of the form $mp_1^{s_1}p_2^{s_2}P$ for some primes P, p_1, p_2 satisfying $P = P(n) > z$ and $q < p_2 < p_1 < P$, and for some positive integers m, s_1, s_2 satisfying $s_1 \ge 2$, $s_2 \ge 2$

and $P_J(m) \le y$. Given m, p_1, p_2, s_1, s_2, the number of possible $P \in (z, x/mp_1^{s_1}p_2^{s_2}]$ is $O(x/mp_1^{s_1}p_2^{s_2}\log z)$. Summing this over all possible s_i, p_i, and m via (3.18) and the fact that $\sum_{p>q} 1/p^2 \ll 1/q$, we deduce that the total contribution of all n that are divisible by the squares of two primes is $\ll x/q^2(\log x)^{1/3}$. This establishes the desired bound on the sum Σ_2 in the remaining case $D = 2$.

Bounding Σ*:* Any n counted in Σ has $P_{M(D+1)+1}(n) > q$, but no more than $(M-2)D$ of these exactly divide n. Since $D = \max_{1\le i\le M} \deg G_i \ge M$, it follows that any such n has $\Omega^*_{>q}(n) \ge M(D+1)+1-(M-2)D = 2D+1 \ge 2M+1$, so that the squarefull part of n exceeds q^{2M+1}. Consequently, any n counted in Σ can be written in the form mSP, where $P := P(n) > z$, $S > q^{2M+1}$ is squarefull and $P_J(m) \le y$. Given m and S, the number of possible $P \in (z, x/mS]$ is $O(x/mS\log z)$. Summing this over all squarefull $S > q^{2M+1}$ and then over all m by means of (3.18), we find that

$$\Sigma \ll \frac{x\log_2 x}{\log x} \sum_{\substack{m\le x\\ P_J(m)\le y}} \frac{1}{m} \sum_{\substack{S>q^{2M+1}\\ S \text{ squarefull}}} \frac{1}{S} \ll \frac{x}{q^{M+1/2}(\log x)^{1/3}},$$

yielding the desired bound for Σ, and completing the proof of the estimate (3.20), for $M \ge 2$.

The case $M = 1$ is much simpler: we need only split the count in the left hand side of (3.20) as $\Sigma_0 + \Sigma$ where Σ_0 counts those n that have no repeated prime factor exceeding q. As such, any n counted in Σ_0 is exactly divisible by at least $D+1$ primes exceeding q, whereupon the exact same arguments given for the "Σ_0" defined in the case $M \ge 2$ show that $\Sigma_0 \ll x/q(\log x)^{1/3}$. On the other hand, any n counted in Σ has a repeated prime factor exceeding q, and thus is of the form mSP, with $P := P(n) > z$, $S > q^2$ squarefull and $P_J(m) \le y$. Proceeding as for the "Σ" considered in the case $M \ge 2$, we obtain $\Sigma \ll x/q(\log x)^{1/3}$. This shows the estimate (3.20) in the remaining case

$M = 1$, completing the proof of theorem. □

Section 3.6

Complete uniformity in squarefree moduli: Proof of Theorem 3.1.3

Arguing as in the beginning of the previous section, in order to complete the proof of the theorem, it suffices to show the following analogue of (3.20)

$$\sum_{\substack{n\leq x:\ P_{2M}(n)>q\\ P_J(n)\leq y;\ P(n)>z\\ p>y\implies p^2\nmid n\\ (\forall i)\ g_i(n)\equiv b_i\ (\mathrm{mod}\ q)}} 1 \ \ll\ \frac{x}{q^M(\log x)^{1/3}} \tag{3.22}$$

uniformly in squarefree $q \leq (\log x)^K$ and in residues $(b_1, \dots, b_M)$ mod q.

The following analogue of (3.21) will be useful for this purpose: for each $r \in \{0, 1, \dots, M-1\}$, we have

$$\#\mathcal{V}_{2(M-r),M-r}\left(q; (w_i)_{i=1}^{M-r}\right) \leq \lambda^{\omega(q)}\frac{\varphi(q)^{2(M-r)}}{q^{M-r}} \tag{3.23}$$

uniformly for squarefree $q > 1$ and in residue classes $(w_1, \dots, w_{M-r})$ mod q, for some constant $\lambda := \lambda(\widehat{G}) > 1$. It suffices to show this bound for $r = 0$ for then it may be applied with $M - r$ playing the role of M (recalling that $\{G_i'\}_{i=1}^{M-r}$ are $\mathbb{Q}$-linearly independent for any such r).

As in Proposition 3.3.2, we let $C := C(\mathbf{G})$ be a constant exceeding $\max\{C_0(\mathbf{G}), (2D)^{2D+4}\}$, with $C_0(\mathbf{G})$ defined in (3.2). Then for all $\ell \leq C(\mathbf{G})$, we have trivially

$$\#\mathcal{V}_{2M,M}\left(\ell; (w_i)_{i=1}^{M}\right) \leq \varphi(\ell)^{2M} \leq \lambda_1\frac{\varphi(\ell)^{2M}}{\ell^M} \tag{3.24}$$

by fixing $\lambda_1 \coloneqq \lambda_1(\widehat{G}) > C(\mathbf{G})^M$.

Now consider a prime $\ell > C(\mathbf{G})$. By orthogonality we can write, as in (3.8),

$$\#\mathcal{V}_{2M,M}\left(\ell;(w_i)_{i=1}^M\right) = \frac{\varphi(\ell)^{2M}}{\ell^M}\Bigg\{1+ \frac{1}{\varphi(\ell)^{2M}}\sum_{(r_1,\dots,r_M)\not\equiv(0,\dots,0) \bmod \ell} e\left(-\frac{1}{\ell}\sum_{i=1}^M r_i w_i\right)\left(Z_{\ell;\,r_1,\dots,r_M}\right)^{2M}\Bigg\},$$

where $Z_{\ell;\,r_1,\dots,r_M} \coloneqq \sum_{v \bmod \ell} \chi_{0,\ell}(v) e\left(\frac{1}{\ell}\sum_{i=1}^M r_i G_i(v)\right)$. Since $\ell > C(\mathbf{G}) > C_0(\mathbf{G})$, the polynomials $\{G_i'\}_{i=1}^M$ must be $\mathbb{F}_\ell$-linearly independent, so that for each $(r_1,\dots,r_M) \not\equiv (0,\dots,0) \bmod \ell$, the polynomial $\sum_{i=1}^M r_i G_i(T)$ does not reduce to a constant mod ℓ. As such, the Weil bound (Proposition 3.3.4) yields $|Z_{\ell;\,r_1,\dots,r_M}| \le D\ell^{1/2}$, leading to

$$\#\mathcal{V}_{2M,M}\left(\ell;(w_i)_{i=1}^M\right) = \frac{\varphi(\ell)^{2M}}{\ell^M}\left\{1+O\left(\ell^M\frac{(D\ell^{1/2})^{2M}}{\varphi(\ell)^{2M}}\right)\right\} \le \lambda_2\frac{\varphi(\ell)^{2M}}{\ell^M}, \tag{3.25}$$

for some constant $\lambda_2 \coloneqq \lambda_2(\widehat{G}) > C(\mathbf{G})^M$. Finally, we choose $\lambda \coloneqq \max\{\lambda_1,\lambda_2\}$ and write, for any squarefree $q > 1$,

$$\#\mathcal{V}_{2M,M}\left(q;(w_i)_{i=1}^M\right) = \prod_{\ell\mid q:\ \ell\le C}\#\mathcal{V}_{2M,M}\left(\ell;(w_i)_{i=1}^M\right)\cdot\prod_{\ell\mid q:\ \ell> C}\#\mathcal{V}_{2M,M}\left(\ell;(w_i)_{i=1}^M\right).$$

Combining (3.24) for all the prime divisors $\ell \le C$ with (3.25) for all the prime divisors $\ell > C$, we obtain the desired bound (3.23) for $r = 0$. As argued before, this also implies (3.23) for any $r \in \{0,1,\dots,M-1\}$.

Coming to the proof of (3.22), we write the count on the left hand side as

$$\Sigma_1 + \Sigma_2 + \cdots + \Sigma_M + \Sigma,$$

where

- Σ_1 counts those n which are exactly divisible by at least $2M$ many distinct primes exceeding q,
- For each $r \in \{1, \dots, M-1\}$, Σ_{r+1} counts the n that are exactly divisible by either $2M-2r$ many or by $2M-2r+1$ many distinct primes exceeding q, and
- Σ counts the remaining n, namely, those that are exactly divisible by at most one prime exceeding q.

Bounding Σ_1: Any n counted in Σ_1 can be written in the form $mP_{2M}\cdots P_1$, where $P_1 \coloneqq P(n) > z$, $q < P_{2M} < \cdots < P_1$, $P_J(m) \le y$ and where $\gcd(m, P_{2M}\cdots P_1) = 1$. As such, the congruences $g_i(n) \equiv b_i \pmod q$ force $(P_1, \dots, P_{2M}) \equiv \widehat{v} \bmod q$ for some

$$\widehat{v} \coloneqq (v_1, \dots, v_{2M}) \in \mathcal{V}_{2M,M}\left(q; (b_i - g_i(m))_{i=1}^M\right).$$

Given m and $\widehat{v}$, the arguments in the previous section show that the number of possible $P_1, \dots, P_{2M}$ satisfying $(P_1, \dots, P_{2M}) \equiv \widehat{v} \bmod q$ is

$$\ll \frac{x(\log_2 x)^{O(1)}}{\varphi(q)^{2M} m \log x}.$$

Consequently,

$$\Sigma_1 \ll \frac{x(\log_2 x)^{O(1)}}{\log x} \sum_{\substack{m \le x \\ P_J(m) \le y}} \frac{1}{m} \cdot \frac{\#\mathcal{V}_{2M,M}\left(q; (b_i - g_i(m))_{i=1}^M\right)}{\varphi(q)^{2M}}.$$

Using (3.23) to bound the cardinality $\#\mathcal{V}_{2M,M}\left(q; (b_i - g_i(m))_{i=1}^M\right)$ in conjunction with

(3.18) to bound the resulting sum on m, we obtain

$$\Sigma_1 \ll \lambda^{\omega(q)} \frac{x(\log_2 x)^{O(1)}}{q^M (\log x)^{1/2}} \exp\left(O\left((\log_3 x)^2\right)\right) \ll \frac{x}{q^M (\log x)^{1/3}},$$

showing the desired bound for Σ_1.

Bounding $\Sigma_2, \dots, \Sigma_M$: We start by making the following general observation:

Let E be a set of primes and for a positive integer N, let $\Omega_E^*(N) \coloneqq \sum_{\substack{p^k \| n \\ p \in E,\ k>1}} k$ denote the number of prime divisors of N (counted with multiplicity) lying in the set E and appearing to an exponent greater than 1 in the prime factorization of N. Then for any $t \geq 2$, any positive integer N having $\Omega_E^*(N) \geq t$ is divisible by $p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ for some distinct primes $p_1, \dots, p_s \in E$, and integers $\alpha_1, \dots, \alpha_s \geq 2$ summing to t or $t+1$. More precisely, there exist positive integers s, m, $\alpha_1, \dots, \alpha_s, \beta_1, \dots, \beta_s$ and distinct primes $p_1, \dots, p_s \in E$ such that $\alpha_1, \dots, \alpha_s \geq 2$, $\sum_{i=1}^s \alpha_i \in \{t, t+1\}$, $\gcd(m, p_1 \cdots p_s) = 1$, $N = m p_1^{\beta_1} \cdots p_s^{\beta_s}$ and $\beta_i \geq \alpha_i$ for all $i \in [s]$.

This is seen by a simple induction on t, the case $t = 2$ being clear with the tuple $(\alpha_1, \dots, \alpha_s)$ being the singleton (2) and the case $t = 3$ being clear with $(\alpha_1, \dots, \alpha_s) \in \{(3), (2,2)\}$. Consider any $T \geq 4$, assume that the result holds for all $t < T$, and let N be a positive integer with $\Omega_E^*(N) \geq T$. Let p_1 be the largest prime divisor of N lying in the set E and satisfying $p_1^2 \mid n$, and let $\beta_1 \coloneqq v_{p_1}(N) \geq 2$. If $\beta_1 \geq T-1$, then we are done with $(\alpha_1, \dots, \alpha_s)$ being (T) or $(T-1, 2)$, so suppose $\beta_1 \leq T-2$. Then the positive integer $N' \coloneqq N/p_1^{\beta_1}$ is not divisible by p_1, and has $\Omega_E^*(N') \geq T - \beta_1 \geq T - (T-2) = 2$. As such, by the inductive hypothesis applied to N' and $t \coloneqq T - \beta_1$, there exist $s, m, \alpha_2, \dots, \alpha_s, \beta_2, \dots, \beta_s$ and distinct primes $p_2, \dots, p_s \in E$ satisfying $\alpha_2, \dots, \alpha_s \geq 2$, $\sum_{i=2}^s \alpha_i \in \{T - \beta_1, T - \beta_1 + 1\}$, $\gcd(m, p_2 \cdots p_s) = 1$, $N' = m p_2^{\beta_2} \cdots p_s^{\beta_s}$ and $\beta_i \geq \alpha_i$ for all $i \in \{2, \dots, s\}$. Since $p_1 \nmid N'$, we see that the primes $p_1, \dots, p_s \in E$ must all

be distinct and that $\gcd(m, p_1 \cdots p_s) = 1$. Consequently, with $\alpha_1 \coloneqq \beta_1 \geq 2$, we have $N = p_1^{\beta_1} N' = m p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ with $\sum_{i=1}^{s} \alpha_i \in \{T, T+1\}$ and with $\beta_i \geq \alpha_i$ for all $i \in [s]$. This completes the induction step, establishing the claimed observation.

With this observation in hand, we note that for each $r \in \{1, \dots, M-1\}$, any n counted in the sum Σ_{r+1} is of the form $m p_1^{\beta} \cdots p_s^{\beta_s} P_{2M-2r} \cdots P_1$ where all of the following hold:

(i) $P_1 \coloneqq P(n) > z$;

(ii) $q < P_{2M-2r} < \cdots < P_1$;

(iii) $p_1, \dots, p_s > q$;

(iv) $\beta_1 \geq \alpha_1, \dots, \beta_s \geq \alpha_s$ for some positive integers $\alpha_1, \dots, \alpha_s$ at least 2 summing to either $\max\{2, 2r-1\}$ or to $2r$;

(v) $P_J(m) \leq y$;

(vi) $m, p_1, \dots, p_s$, $P_{2M-2r}, \dots, P_1$ are all pairwise coprime.

Indeed, any n counted in Σ_{r+1} is exactly divisible by at least $2M - 2r$ but at most $2M - 2r + 1$ many primes (counted with multiplicity) exceeding q. Hence in the case $r = 1$ we have $\Omega^*_{>q}(n) \geq 2$ while for $r \in \{2, \dots, M-1\}$, we have $\Omega^*_{>q}(n) \geq 2M - (2M - 2r + 1) \geq 2r - 1$, so altogether $\Omega^*_{>q}(n) \geq \max\{2, 2r-1\}$. Let $P_1, P_2, \dots, P_{2M-2r}$ be primes exceeding q that exactly divide n, and satisfy $P_1 \coloneqq P(n) > z$ and $P_{2M-2r} < \cdots < P_2 < P_1$. Then with $n' \coloneqq n/P_1 \cdots P_{2M-2r}$, we still have $\Omega^*_{>q}(n') = \Omega^*_{>q}(n) \geq \max\{2, 2r-1\}$ and $\gcd(n', P_1 \cdots P_{2M-2r}) = 1$. Invoking the above observation for $N \coloneqq n'$, $t \coloneqq \max\{2, 2r-1\}$ and E the set of primes exceeding q, we find that $n' = m p_1^{\beta} \cdots p_s^{\beta_s}$ for some $s \geq 1$, primes $p_1, \dots, p_s > q$ and positive integers $m, \beta_1, \dots, \beta_s$ such that $m, p_1, \dots, p_s$ are pairwise coprime, and $\beta_1 \geq \alpha_1, \dots, \beta_s \geq$

α_s for some positive integers $\alpha_1, \dots, \alpha_s$ at least 2 summing to either $\max\{2, 2r-1\}$ or $2r$. (Here, we have recalled that in the case $t = 2$, the tuple $(\alpha_1, \dots, \alpha_s) = (2)$ was sufficient.) Altogether, we find that $n = n'P_1 \cdots P_{2M-2r} = mp_1^{\beta} \cdots p_s^{\beta_s} P_1 \cdots P_{2M-2r}$, with $m, p_1, \dots, p_s, \beta_1, \dots, \beta_s, P_1, \dots, P_{2M-2r}$ satisfying the conditions (i)-(vi).

Consequently, $g_i(n) = g_i(mp_1^{\beta_1} \cdots p_s^{\beta_s}) + \sum_{j=1}^{2M-2r} G_i(P_j)$, and the conditions $g_i(n) \equiv b_i \pmod q$ for $i \in [M-r]$ force $(P_1, \dots, P_{2M-2r}) \equiv \widehat{v} \bmod q$ for some element $\widehat{v} \coloneqq (v_1, \dots, v_{2M-2r})$ of the set

$$\mathcal{V}_{2M-2r,M-r}\left(q; (b_i - g_i(mp_1^{\beta} \cdots p_s^{\beta_s}))_{i=1}^{M-r}\right).$$

Given $m, s, \alpha_1, \dots, \alpha_s,\ p_1, \dots, p_s,\ \beta_1, \dots, \beta_s$ and $\widehat{v}$, the arguments in the previous section show that the number of possible $P_1, \dots, P_{2M-2r}$ satisfying $(P_1, \dots, P_{2M-2r}) \equiv \widehat{v} \bmod q$ is

$$\ll \frac{x(\log_2 x)^{O(1)}}{\varphi(q)^{2M-2r} m p_1^{\beta_1} \cdots p_s^{\beta_s} \log x}.$$

Using (3.23) to bound $\#\mathcal{V}_{2M-2r,M-r}\left(q; (b_i - g_i(mp_1^{\beta} \cdots p_s^{\beta_s}))_{i=1}^{M-r}\right)$, we find that

$$\Sigma_{r+1} \ll \lambda^{\omega(q)} \frac{x(\log_2 x)^{O(1)}}{q^{M-r} \log x} \sum_{\substack{m \le x \\ P_J(m) \le y}} \frac{1}{m} \sum_{\substack{s \ge 1;\ \alpha_1, \dots, \alpha_s \ge 2 \\ \alpha_1 + \cdots + \alpha_s \in \{2r-1, 2r\}}} \sum_{\substack{p_1, \dots, p_s > q \\ \beta_1 \ge \alpha_1, \dots, \beta_s \ge \alpha_s}} \frac{1}{p_1^{\beta_1} \cdots p_s^{\beta_s}}.$$

Now, the sum on $p_1, \dots, p_s, \beta_1, \dots, \beta_s$ is no more than

$$\prod_{i=1}^{s} \left(\sum_{p_i > q} \sum_{\beta_i \ge \alpha_i} \frac{1}{p_i^{\beta_i}} \right) \ll \prod_{i=1}^{s} \left(\sum_{p_i > q} \frac{1}{p_i^{\alpha_i}} \right) \ll \frac{1}{q^{\alpha_1 + \cdots + \alpha_s - s}}.$$

In addition since $s \ge 1$ and $\sum_{i=1}^{s} \alpha_i \ge 2r-1$ and each $\alpha_i \ge 2$, we find that $\sum_{i=1}^{s} \alpha_i - s \ge r$: indeed, from the bound $\sum_{i=1}^{s} \alpha_i - s \ge 2s - s = s \ge 1$, it remains to only see that for $r \ge 2$, we have $\sum_{i=1}^{s} \alpha_i - s \ge \max\{s, 2r-1-s\} \ge r$. Collecting estimates,

we obtain

$$\Sigma_{r+1} \ll \lambda^{\omega(q)} \frac{x(\log_2 x)^{O(1)}}{q^M \log x} \sum_{\substack{m \le x \\ P_J(m) \le y}} \frac{1}{m} \sum_{\substack{s \ge 1;\ \alpha_1,\dots,\alpha_s \ge 2 \\ \alpha_1+\cdots+\alpha_s \in \{2r-1, 2r\}}} 1.$$

But since there are $O(1)$ many possible $s \ge 1$ and tuples $(\alpha_1, \dots, \alpha_s)$ of positive integers summing to $2r-1$ or to $2r$, this automatically leads to

$$\Sigma_{r+1} \ll \lambda^{\omega(q)} \frac{x(\log_2 x)^{O(1)}}{q^M \log x} \sum_{\substack{m \le x \\ P_J(m) \le y}} \frac{1}{m}.$$

As a consequence, (3.18) yields

$$\Sigma_{r+1} \ll \frac{\lambda^{\omega(q)} x}{q^M (\log x)^{1/2}} \exp\left(O\left((\log_3 x)^2\right)\right) \ll \frac{x}{q^M (\log x)^{1/3}},$$

yielding the desired bound for all of $\Sigma_2, \dots, \Sigma_M$.

Bounding Σ: Any n counted in Σ has $2M$ many prime factors (counted with multiplicity) exceeding q, out of which at most one of them can exactly divide n. Hence $\Omega^*_{>q}(n) \ge 2M-1$, and by the same argument as given above, any n counted in Σ can be expressed in the form $mp_1^{\beta_1} \cdots p_s^{\beta_s} P$, where $P \coloneqq P(n) > z$, $p_1, \dots, p_s > q$ are primes, $P_J(m) \le y$, and $\beta_1 \ge \alpha_1, \dots, \beta_s \ge \alpha_s$ for some positive integers $\alpha_1, \dots, \alpha_s$ at least 2 summing to either $2M-1$ or $2M$. Given $m, s, \alpha_1, \dots, \alpha_s, p_1, \dots, p_s, \beta_1, \dots, \beta_s$, the number of possible P is $\ll x/mp_1^{\beta_1} \cdots p_s^{\beta_s} \log z$. As above, we have $\sum_{i=1}^s \alpha_i - s \ge \max\{s, 2M-1-s\} \ge M$, so that the sum over $s, \alpha_1, \dots, \alpha_s, p_1, \dots, p_s, \beta_1, \dots, \beta_s$ is $O(q^{-M})$. Finally, using (3.18) to bound the sum on m, we obtain $\Sigma \ll x/q^M (\log x)^{1/3}$.

This completes the proof of (3.22), and hence that of Theorem 3.1.3. □

3.6.1. Optimality in the input restrictions in Theorem 3.1.3:

For any $M \geq 2$, we construct additive functions $g_1, \dots, g_M$ showing that the restriction $P_{2M}(n) > q$ cannot be weakened to $P_{2M-3}(n) > q$ in our range of q. For $M = 2$, the condition $P_{2M-3}(n) > q$ translates to $P(n) > q$; by Lemma 2.3.1, this latter condition may be ignored up to a negligible error, so the first counterexample in subsection § 3.4.1 suffices.

Now assume that $M \geq 3$; consider additive functions $g_1, \dots, g_M : \mathbb{N} \to \mathbb{Z}$ defined by the polynomials $G_i(T) \coloneqq (T-1)^i$, and satisfying the conditions $g_i(p^2) \coloneqq 0$ for all primes p and all $i \in [M]$. As observed in subsection § 3.4.1, the polynomials $\{G_i'\}_{i=1}^M$ are $\mathbb{Q}$-linearly independent, and with $C_0(\mathbf{G})$ as in (3.2), we have $q \in \mathcal{Q}_{(g_1,\dots,g_M)}$ for all moduli q having $P^-(q) > C_0(\mathbf{G})$.

We see that $G_i(p) \equiv 0 \pmod q$ for all i and for all primes $p \equiv 1 \pmod q$. Consequently, if $p_1, \dots, p_{M-2}, P$ are primes satisfying $q < p_{M-2} < \cdots < p_1 < x^{1/(4M-8)} < x^{1/3} < P \leq x/(p_1 \cdots p_{M-2})^2$ and $P \equiv 1 \pmod q$, then the positive integer $n \coloneqq (p_1 \cdots p_{M-2})^2 P$ is less than or equal to x, has $P_{2M-3}(n) > q$ and satisfies the conditions $g_i(n) = G_i(P) + \sum_{j=1}^{M-2} g_i(p_j^2) \equiv 0 \pmod q$ for all $i \in \{1, \dots, M\}$. By the Siegel–Walfisz Theorem, we find that

$$\begin{aligned}
\sum_{\substack{n \leq x:\ P_{2M-3}(n) > q \\ (\forall i)\ g_i(n) \equiv 0 \pmod q}} 1 \ &\geq \sum_{q < p_{M-2} < \cdots < p_1 < x^{1/(4M-8)}} \ \sum_{\substack{x^{1/3} < P \leq x/(p_1 \cdots p_{M-2})^2 \\ P \equiv 1 \pmod q}} 1 \\
&\gg \sum_{q < p_{M-2} < \cdots < p_1 < x^{1/(4M-8)}} \left(\frac{x}{\varphi(q)(p_1 \cdots p_{M-2})^2 \log x} + O(x^{1/3}) \right) \\
&\gg \frac{x}{q \log x} \sum_{\substack{p_1, \dots, p_{M-2} \text{ distinct} \\ q < p_1, \dots, p_{M-2} < x^{1/(4M-8)}}} \frac{1}{(p_1 \cdots p_{M-2})^2}
\end{aligned}$$

Ignoring the distinctness condition in the sum above incurs a total error

$$\ll \frac{x}{q\log x}\sum_{p_1,p_2,\dots,p_{M-3}>q}\frac{1}{p_1^4p_2^2\cdots p_{M-3}^2}$$
$$\ll \frac{x}{q\log x}\left(\sum_{p>q}\frac{1}{p^4}\right)\left(\sum_{p>q}\frac{1}{p^2}\right)^{M-4} \ll \frac{x}{q^M\log x}.$$

On the other hand,

$$\sum_{p_1,\dots,p_{M-2}\in(q,x^{1/(4M-8)})}\frac{1}{(p_1\cdots p_{M-2})^2} = \left(\sum_{q<p<x^{1/(4M-8)}}\frac{1}{p^2}\right)^{M-2}$$
$$\gg \frac{1}{(q\log q)^{M-2}}.$$

Collecting estimates, we obtain for all sufficiently large q,

$$\sum_{\substack{n\le x:\ P_{2M-3}(n)>q\\ (\forall i)\ g_i(n)\equiv 0\,(\mathrm{mod}\ q)}} 1 \gg \frac{x}{q^{M-1}\log x(\log q)^{M-2}} + O\left(\frac{x}{q^M\log x}\right)$$
$$\gg \frac{x}{q^{M-1}\log x(\log_2 x)^{M-2}},$$

which grows strictly faster than x/q^M as soon as $q > \log x\cdot(\log_2 x)^{M-1}$ (say). We conclude that the condition $P_{2M}(n) > q$ cannot be replaced by $P_{2M-3}(n) > q$ for *any* $M \ge 2$.

One might wonder whether one of the conditions $P_{2M-1}(n) > q$ or $P_{2M-2}(n) > q$ could possibly suffice to restore uniformity in squarefree $q \le (\log x)^K$. In this direction, we now construct an example showing that the condition $P_{2M-2}(n) > q$ is also insufficient for $M = 2$. Indeed, let consider additive functions g_1, g_2 defined by the polynomials $G_1(T) \coloneqq T$ and $G_2(T) \coloneqq T^3$, so that $\{G_1', G_2'\}$ are clearly $\mathbb{Q}$-linearly independent.

With $C_0(\mathbf{G})$ as usual, we have $q \in \mathcal{Q}_{(g_1,g_2)}$ for all q having $P^-(q) > C_0(\mathbf{G})$.

However, if n is of the form P_1P_2 for distinct primes P_1, P_2 satisfying $P_1, P_2 > y := \exp((\log x)^{1/2})$ and $P_2 \equiv -P_1 \pmod q$, then $P_2(n) > y > q$, while $G_i(P_1)+G_i(P_2) \equiv 0 \pmod q$ for $i \in \{1,2\}$, so that $g_1(n) \equiv g_2(n) \equiv 0 \pmod q$. As such, for $2 < q \le (\log x)^K$, a simpler version of the arguments leading to (3.5) yields

$$\begin{aligned}\sum_{\substack{n\le x:\ P_2(n)>q\\ (\forall i)\ g_i(n)\equiv 0 \,(\mathrm{mod}\ q)}} 1 \ &\ge \sum_{v\in U_q}\frac{1}{2!}\sum_{\substack{P_1,P_2>y\\ P_1\ne P_2,\ P_1P_2\le x\\ P_1\equiv v,\ P_2\equiv -v \,(\mathrm{mod}\ q)}} 1\\ &\gg \frac{1}{\varphi(q)}\sum_{P_1,P_2>y:\ P_1P_2\le x} 1 + O(x\exp(-C'(\log x)^{1/4}))\\ &\gg \frac{x\log_2 x}{q\log x},\end{aligned} \tag{3.26}$$

where $C' := C'(K) > 0$ is a constant, and the last bound above is a simple consequence of Chebyshev's and Mertens' estimates. In particular, this shows that the tuple $(0,0)$ mod q is overrepresented by (g_1, g_2) once $q > \log x/(\log_2 x)^{1/2}$, showing failure of uniformity in squarefree q after a very small threshold, under the restriction $P_{2M-2}(n) > q$ for $M = 2$.

It is to be noted that our arguments above go through for any two polynomials $G_i(T) := A_iT^{k_i} + B_i$ ($i \in \{1,2\}$), for any two *distinct odd* positive integers k_i, and any integers $A_i \ne 0$ and B_i. Indeed, the distinctness of k_1 and k_2 ensures that G_1' and G_2' are $\mathbb{Q}$-linearly independent, while their parity ensures that any two primes P_1, P_2 satisfying $P_2 \equiv -P_1 \pmod q$ also satisfy $G_i(P_1) + G_i(P_2) \equiv 2B_i \pmod q$ for both $i \in \{1,2\}$. As such, the above arguments show that there are $\gg x\log_2 x/q\log x$ many $n \le x$ satisfying $g_i(n) \equiv 2B_i \pmod q$ for $i \in \{1,2\}$. This gives an infinite family of counterexamples showing that the condition $P_{2M-2}(n) > q$ is not sufficient to restore

uniformity in squarefree $q \leq (\log x)^K$ in the case $M = 2$.

In conclusion, this means that our restriction $P_{2M}(n) > q$ in Theorem 3.1.3 is at most "one step away" from optimal, in the sense that it might still be possible to weaken it to $P_{2M-1}(n) > q$.

Section 3.7

Necessity of the linear independence hypothesis: Proof of Theorem 3.1.4

Recall that the $\mathbb{Q}$-linear independence of $\{G_i'\}_{i=1}^{M-1}$ is equivalent to that of $\{G_i - G_i(0)\}_{i=1}^{M-1}$; likewise, the condition $G_M' = \sum_{i=1}^{M-1} a_i G_i'$ is exactly equivalent to the condition $G_M(T) - G_M(0) = \sum_{i=1}^{M-1} a_i(G_i(T) - G_i(0))$ in the ring $\mathbb{Q}[T]$. We claim that the polynomials $\{G_i\}_{i=1}^{M}$ are $\mathbb{Q}$-linearly independent. Indeed, suppose there exist integers $\beta_1, \ldots, \beta_M$ for which $\sum_{i=1}^{M} \beta_i G_i(T) = 0$ in $\mathbb{Q}[T]$. Since $G_M(T) = G_M(0) + \sum_{i=1}^{M-1} a_i(G_i(T) - G_i(0))$, we find that

$$\sum_{i=1}^{M-1} (\beta_i + \beta_M a_i) G_i(T) = \beta_M \left(\sum_{i=1}^{M-1} a_i G_i(0) - G_M(0) \right), \tag{3.27}$$

so that $\sum_{i=1}^{M-1} (\beta_i + \beta_M a_i)(G_i(T) - G_i(0)) = 0$. Since $\{G_i(T) - G_i(0)\}_{i=1}^{M-1}$ are $\mathbb{Q}$-linearly independent, the last relation forces $\beta_i = -\beta_M a_i$ for all $i \in \{1, \ldots, M-1\}$, which by (3.27) leads to

$$\beta_M \left(\sum_{i=1}^{M-1} a_i G_i(0) - G_M(0) \right) = 0.$$

Now if $\beta_M \neq 0$, then the above relation forces $\sum_{i=1}^{M-1} a_i G_i(0) = G_M(0)$ contrary to hypothesis. Hence, we must have $\beta_M = 0$, forcing $\beta_i = -\beta_M a_i = 0$ for all

$i \in \{1, \dots, M-1\}$. This shows that $\{G_i\}_{i=1}^M$ are indeed $\mathbb{Q}$ linearly independent.

As such by Corollary 3.2.3(i) and the discussion preceding it, there exists a constant $C_1(\widehat{G}) > 0$ such that $\{G_i\}_{i=1}^M$ are $\mathbb{F}_\ell$-linearly independent for all $\ell > C_1(\widehat{G})$, and so $Q \in \mathcal{Q}_{(g_1,\dots,g_M)}$ for all moduli $Q > 1$ having $P^-(Q) > C_1(\widehat{G})$. In addition, since $\{G_i'\}_{i=1}^{M-1}$ are $\mathbb{Q}$-linearly independent, there exists (by (3.2)) a constant $C_0(G_1, \dots, G_{M-1}) > 0$ such that $\{G_i'\}_{i=1}^{M-1}$ are $\mathbb{F}_\ell$-linearly independent for any $\ell > C_0(G_1, \dots, G_{M-1})$.

We set $C_{\mathbf{G}}$ to be any constant exceeding

$$\max\{C_1(\widehat{G}), 4M(32D)^{2D+4}, C_0(G_1, \dots, G_{M-1})\},$$

and henceforth consider moduli q having $P^-(q) > C_{\mathbf{G}}$, so that $q \in \mathcal{Q}_{(g_1,\dots,g_M)}$. Given any $R > C_{\mathbf{G}}$ and integers $\{b_i\}_{i=1}^{M-1}$, set $b_M := G_M(0)R + \sum_{i=1}^{M-1} a_i(b_i - G_i(0)R)$. Then the relations $\sum_{j=1}^R G_i(v_j) \equiv b_i \pmod q$ for $i \in \{1, \dots, M-1\}$ also imply that $\sum_{j=1}^R G_M(v_j) \equiv b_M \pmod q$. As such, for any R distinct primes $P_1, \dots, P_R$, with $(P_1, \dots, P_R) \bmod q$ lying in the set

$$\begin{aligned} V &:= \mathcal{V}_{R,M-1}\left(q; (b_i)_{i=1}^{M-1}\right) \\ &= \left\{ (v_j)_{j=1}^R \in (U_q)^R : (\forall i \in [M-1]) \ \sum_{j=1}^R G_i(v_j) \equiv b_i \pmod q \right\}, \end{aligned}$$

we have $g_i(P_1 \cdots P_R) \equiv b_i \pmod q$ for *all* $i \in [M]$. Letting $y := \exp((\log x)^{1/2})$, a simpler version of the arguments leading to (3.5) yields, for $q \le (\log x)^K$,

$$\sum_{\substack{n \le x:\ P_R(n) > q \\ (\forall i)\ g_i(n) \equiv b_i \pmod q}} 1 \ \ge \sum_{(v_1,\dots,v_R) \in V} \frac{1}{R!} \sum_{\substack{P_1,\dots,P_R > y \\ P_1 \cdots P_R \le x \\ P_1,\dots,P_R \text{ distinct} \\ (\forall j)\ P_j \equiv v_j \pmod q}} 1$$

$$\gg \frac{\#V}{\varphi(q)^R} \sum_{\substack{P_1,\dots,P_R>y \\ P_1\cdots P_R\le x \\ P_1,\dots,P_R \text{ distinct}}} 1 + O(x\exp(-C'(\log x)^{\delta/4}))$$

$$\gg \frac{\#V}{\varphi(q)^R} \sum_{\substack{P_1,\dots,P_R>y \\ P_1\cdots P_R\le x}} 1 + O(x\exp(-C'(\log x)^{\delta/4}))$$

for some constant $C' \coloneqq C'(K) > 0$. A direct induction on R (involving Chebyshev's estimate) shows that the last sum above is

$$\sum_{\substack{n\le x:\ P^-(n)>y \\ \Omega(n)=R}} 1 \ \gg\ \frac{x(\log_2 x)^{R-1}}{\log x},$$

leading to

$$\sum_{\substack{n\le x:\ P_R(n)>q \\ (\forall i)\ g_i(n)\equiv b_i \pmod q}} 1 \ \gg\ \frac{\#V}{\varphi(q)^R}\cdot\frac{x(\log_2 x)^{R-1}}{\log x} + O(x\exp(-C'(\log x)^{\delta/4})).$$

As such, to complete the proof of the theorem, it remains to show that

$$\#V = \#\mathcal{V}_{R,M-1}\left(q;(b_i)_{i=1}^{M-1}\right) \gg \frac{\varphi(q)^R}{q^{M-1}}. \tag{3.28}$$

To show this, we argue as in the proof of the estimate (3.7): for each prime power $\ell^e \parallel q$, we write

$$\#\mathcal{V}_{R,M-1}\left(\ell^e;(b_i)_{i=1}^{M-1}\right) = \frac{\varphi(\ell^e)^R}{\ell^{e(M-1)}}\Bigg\{1 + \frac{1}{\varphi(\ell^e)^R}\sum_{(r_1,\dots,r_{M-1})\not\equiv(0,\dots,0) \bmod \ell^e} e\left(-\frac{1}{\ell^e}\sum_{i=1}^{M-1} r_i b_i\right)\left(Z_{\ell^e;r_1,\dots,r_{M-1}}\right)^R\Bigg\},$$

where

$$Z_{\ell^e;r_1,\dots,r_{M-1}} \coloneqq \sum_{v \bmod \ell^e} \chi_{0,\ell}(v) e\left(\frac{1}{\ell^e}\sum_{i=1}^{M-1} r_i G_i(v)\right)$$

for each $(r_1,\dots,r_{M-1}) \not\equiv (0,\dots,0) \bmod \ell^e$. For any such $(r_1,\dots,r_{M-1})$, we have $\gcd(\ell^e, r_1,\dots,r_{M-1}) = \ell^{e-e_0}$ for some $1 \le e_0 \le e$ and $|Z_{\ell^e;r_1,\dots,r_{M-1}}| \le D\ell^{e-e_0/D}$ (here it is important that since $\ell > C_{\widehat{G}}$, the polynomials $\{G_i'\}_{i=1}^{M-1}$ are $\mathbb{F}_\ell$-linearly independent). We obtain

$$\begin{aligned}\frac{1}{\varphi(\ell^e)^R} &\sum_{(r_1,\dots,r_{M-1})\not\equiv(0,\dots,0) \bmod \ell^e} |Z_{\ell^e;r_1,\dots,r_{M-1}}|^R \\ &\le \frac{D^R \ell^{eR}}{\varphi(\ell^e)^R} \sum_{e_0\ge 1} \left(\ell^{M-1-R/D}\right)^{e_0} \le \frac{2(2D)^R}{\ell^{R/D-M+1}}.\end{aligned}$$

Since $R/D - M \ge R/(D+2)$ and $\ell^{1/(2D+4)} > (C_{\mathbf{G}})^{1/(2D+4)} > 32D$, this leads to

$$\begin{aligned}\frac{1}{\varphi(\ell^e)^R} &\sum_{(r_1,\dots,r_{M-1})\not\equiv(0,\dots,0) \bmod \ell^e} |Z_{\ell^e;r_1,\dots,r_{M-1}}|^R \le \frac{2(2D)^R}{\ell^{R/(D+2)}} \\ &\le \frac{2(2D)^R}{(32D)^R} \cdot \frac{1}{\ell^{R/(2D+4)}} \le \frac{1}{8^R \ell^{R/(2D+4)}} \le \frac{1}{8\ell^2}.\end{aligned}$$

Hence, for each prime power $\ell^e \parallel q$,

$$\#\mathcal{V}_{R,M-1}\left(\ell^e; (b_i)_{i=1}^{M-1}\right) \ge \frac{\varphi(\ell^e)^R}{\ell^{e(M-1)}}\left(1 - \frac{1}{8\ell^2}\right), \tag{3.29}$$

and since $\prod_{\ell\mid q}\left(1-\frac{1}{8\ell^2}\right) \ge 1 - \frac{1}{8}\sum_{\ell\ge 2}\frac{1}{\ell^2} \ge \frac{7}{8}$, we obtain by multiplying all the bounds (3.29),

$$\#V = \prod_{\ell^e\parallel q} \#\mathcal{V}_{R,M-1}\left(\ell^e; (b_i)_{i=1}^{M-1}\right) \ge \frac{7}{8}\cdot\frac{\varphi(q)^R}{q^{M-1}}.$$

This shows (3.28), completing the proof of Theorem 3.1.4, and demonstrating the necessity of the linear independence hypothesis in the generality of our setting. □

Chapter 4

Joint distribution in residue classes of families of polynomially-defined multiplicative functions

We return to the general setting of Theorem 1.3.11, with $f_1, \dots, f_K : \mathbb{N} \to \mathbb{Z}$ being a family of multiplicative functions for which there exist 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 all $i \in [K]$, $v \in [V]$ and all primes p. In Chapter 2, we gave a uniform analogue of Corollary 1.3.17 on the weak equidistribution of a single polynomially–defined multiplicative function to a varying 1-admissible modulus supported on large primes. However, most of the arguments in that chapter are completely limited to the case of a single multiplicative function (i.e. $K = 1$) and do not generalize to families. Even for a single function, they are still far from being complete varying-modulus analogues of Theorem 1.3.6 because they crucially need q to be 1-admissible (i.e. $k = 1$) and have only large prime factors, and also crucially need the only defining polynomial $W_{1,1}$ to be separable.

In this chapter, we remove all these limitations, and obtain best possible analogues of Theorem 1.3.11 to varying moduli. Our results are thus also best possible analogues of the Siegel–Walfisz theorem for families of polynomially–defined multiplicative functions. These results are thus also new for a single multiplicative function as they give complete uniform analogues of Narkiewicz's single function criterion Theorem 1.3.6. Special cases of our main results thus also give uniform analogues (with optimal arithmetic restrictions) of the works of Narkiewicz, Śliwa, Rayner, Dobrowolski, Fomenko and others mentioned in the discussion following Proposition 1.3.10.

In the last paragraph of subsection § 1.4.2, we already gave a glimpse of some of the ideas used in our arguments. A more detailed summary of the arguments is given towards the end of the next section.

This chapter is based on the papers [71] and [72] of the author.

Section 4.1

Main results

4.1.1. Multiplicative independence and the Invariant Factor Hypothesis

For concrete and provably unavoidable reasons (see Theorems 4.1.4 and 4.1.5 below), we are going to need two additional hypotheses (which we had been calling "H_1" and "H_2" before the statement of Theorem 1.4.8). We first define the relevant notation and terminology.

1. We say that the polynomials $\{F_i\}_{1\leq i\leq K} \subset \mathbb{Z}[T]$ are multiplicatively independent (over $\mathbb{Z}$) if there is no tuple of integers $(c_1, \ldots, c_K) \neq (0, \ldots, 0)$ for which the product $\prod_{i=1}^{K} F_i^{c_i}$ is identically constant in $\mathbb{Q}(T)$. This hypothesis is very easy to satisfy, for

example it is satisfied by $\{F_i\}_{1\le i\le K}\subset\mathbb{Z}[T]$ if $\prod_{i=1}^{K}F_i$ is separable. It is also satisfied if each F_i has an irreducible factor that is not present in the other F_j (for $j\neq i$).

2. Assume that $\{F_i\}_{i=1}^{K}\subset\mathbb{Z}[T]$ are multiplicatively independent. Factor $F_i = r_i\prod_{j=1}^{M}G_j^{\mu_{ij}}$ with $r_i\in\mathbb{Z}$, $\{G_j\}_{j=1}^{M}\subset\mathbb{Z}[T]$ being pairwise coprime primitive[1] irreducibles and with $\mu_{ij}\ge 0$ being integers, such that each G_j appears with a positive exponent μ_{ij} in some F_i. Let $\omega(F_1\cdots F_K)\coloneqq M$ and define the exponent matrix of $(F_i)_{i=1}^{K}$ to be the $M\times K$ matrix

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

so that E_0 has a positive entry in each row. Since $\{F_i\}_{i=1}^{K}\subset\mathbb{Z}[T]$ are multiplicatively independent, the columns of E_0 are $\mathbb{Q}$-linearly independent and $\omega(F_1\cdots F_K)=M\ge K$.

3. Continuing from above, E_0 has a Smith Normal Form given by the $M\times K$ diagonal matrix $\mathrm{diag}(\beta_1,\dots,\beta_K)$, where $\beta_1,\dots,\beta_K\in\mathbb{Z}$ are the invariant factors of E_0 satisfying $\beta_1\mid\cdots\mid\beta_K$; since the columns of E_0 are $\mathbb{Q}$-linearly independent, it follows that β_i are all nonzero. (Here we fixed some ordering of the G_j to define E_0 but the invariant factors are independent of this ordering.) We shall use $\beta(F_1,\dots,F_K)$ to denote the last invariant factor β_K. We define the

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

[1] We say that a polynomial in $\mathbb{Z}[T]$ is primitive when the greatest common divisor of its coefficients is 1.

prime $\ell \mid q$ such that $\ell > B_0$.

Example: Often in applications, $\prod_{i=1}^{K} F_i$ is separable over $\mathbb{Q}$ (or more generally, the exponent matrix $E_0(F_1, \dots, F_K)$ is equivalent to the diagonal matrix $\mathrm{diag}(1, \dots, 1)$); when this happens, $\beta(F_1, \dots, F_K) = 1$, so *any* integer satisfies $IFH(F_1, \dots, F_K; B_0)$ for any $B_0 > 0$.

4.1.2. Set-up for the main results in this chapter

Most of the set-up for the main results has already been done before Theorem 1.3.11, however owing to the necessity of some additional notation, we state the *complete* set-up below for the convenience of the reader:

- Consider multiplicative functions $f_1, \dots, f_K \colon \mathbb{N} \to \mathbb{Z}$ 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 $v \in [V]$.

- Let $f \coloneqq \prod_{i=1}^{K} f_i$ and $W_v \coloneqq \prod_{i=1}^{K} W_{i,v}$, so $f(p^v) = W_v(p)$ for all primes p and all v.

- For each $v \in [V]$, define $D_v \coloneqq \deg W_v = \sum_{i=1}^{K} \deg W_{i,v}$. Also let $D \coloneqq D_k$, and $D_{\min} \coloneqq \min_{1 \le i \le K} \deg W_{i,k}$.

- For any q and $v \in [V]$, define $R_v(q) = \{u \in U_q : W_v(u) \in U_q\}$ and $\alpha_v(q) \coloneqq \frac{1}{\varphi(q)} \# R_v(q)$.

- Fix $k \in [V]$, and say that q is k-admissible if $R_k(q) = \emptyset$ but $R_v(q) \neq \emptyset$ for all $v < k$.

  Note that if q is k-admissible, then $\alpha_v(q) = 0$ for $v < k$, while $\alpha_k(q) \gg_{W_k} (\log\log(3q))^{-D}$ by the Chinese Remainder Theorem and a standard argument using Mertens' Theorem.

- Assume that $\{W_{i,k}\}_{1\le i\le K}$ are multiplicatively independent.
- Define $\mathcal{Q}(k; f_1, \cdots, f_K)$ exactly as before the statement of Theorem 1.3.11.

4.1.3. The Main Results

In Theorems 4.1.1 to 4.1.3 below, we fix $K_0, B_0 > 0$. Our implied constants depend only on K_0, B_0 and 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 $\{W_{i,v}\}_{\substack{1\le i\le K\\ k<v\le V}}$.

Theorem 4.1.1. *Fix $\epsilon \in (0,1)$. The functions $f_1, \ldots, f_K$ are jointly weakly equidistributed, uniformly to all moduli $q \le (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfying $IFH(W_{1,k}, \ldots, W_{K,k};\, B_0)$, provided any one of the following holds.*

(i) *Either $K = 1$ and $W_{1,k} = W_k$ is linear, or if $K \ge 2$, $q \le (\log x)^{(1-\epsilon)\alpha_k(q)/(K-1)}$ and at least one of $\{W_{i,k}\}_{1\le i\le K}$ is linear (i.e., $D_{\min} = 1$).*

(ii) *q is squarefree and $q^{K-1} D_{\min}^{\omega(q)} \le (\log x)^{(1-\epsilon)\alpha_k(q)}$.*

(iii) *$D_{\min} > 1$ and $q \le (\log x)^{(1-\epsilon)\alpha_k(q)(K-1/D_{\min})^{-1}}$.*

A concrete application: Corollary 1.3.13 (special case of [46, Theorem 1]) shows that $\varphi(n)$ and $\sigma(n)$ are jointly WUD modulo a fixed integer q precisely when q is coprime to 6; in fact, $\mathcal{Q}(1; \varphi, \sigma) = \{q : (q,6) = 1\}$. Theorem 4.1.1 shows that (φ, σ) are jointly WUD uniformly modulo $q \le (\log x)^{(1-\epsilon)\alpha(q)}$ coprime to 6, where $\alpha(q) \coloneqq \alpha_1(q) = \prod_{\ell \mid q}(\ell - 3)/(\ell - 1)$ and $\epsilon > 0$ is fixed but arbitrary.

Optimality of the conditions in Theorem 4.1.1: Note that except in the very first case when $K = 1$ and $W_k = W_{1,k}$ is linear (which is also when we already have the best possible analogue of the Siegel-Walfisz theorem), Theorem 4.1.1 gives uniformity only up to *small* powers of $\log x$. In subsection § 4.7.1, we will construct general

counterexamples showing that for *any* K, k, D and $D_{\min}$, the ranges of q in (i)–(iii) above are all essentially optimal, except perhaps in the very first case. We will also show that for any $K \geq 2$, the range of q in (i) is essentially optimal, even if q is squarefree and $\{W_{i,k}\}_{1\leq i\leq K}$ are *all* linear, for *any* choice of (pairwise coprime) linear functions! In particular, this means that the aforementioned range $(\log x)^{(1-\epsilon)\alpha(q)}$ is basically optimal for the joint weak equidistribution of (φ, σ), even if we restrict to squarefree q. Thus, this special case of Theorem 4.1.1(i) is the optimal uniform analogue of Narkiewicz's result in [46] for a single varying modulus.

Restoring uniformity in the Siegel–Walfisz range:

Our constructions in § 4.7.1 will reveal that obstructions to uniformity in q come from inputs n of the form P^k for primes P. Modifying those constructions, we can produce more obstructions of the form mP^k with m fixed or growing slowly with x. It turns out that once again, uniformity is restored in the full Siegel–Walfisz range if we restrict attention to those n that are divisible by sufficiently many primes exceeding q. Since $D = 1$ forces $K = 1$ and $W_k = W_{1,k}$ to be linear (a case in which Theorem 4.1.1(i) already gives complete uniformity in $q \leq (\log x)^{K_0}$), we assume in Theorems 4.1.2 and 4.1.3 below that $D \geq 2$.

Theorem 4.1.2. *The following hold as $x \to \infty$, uniformly in coprime residues $a_1, \dots, a_K$ to moduli $q \leq (\log x)^{K_0}$ that lie in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and satisfy hypothesis $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$.*

$$\begin{aligned}\#\{n \leq x : P_R(n) > q,\ \ (\forall i)\ f_i(n) \equiv a_i \pmod q\}& \\ \sim \frac{1}{\varphi(q)^K}\#\{n \leq x : \gcd(f(n), q) = 1\}& \\ \sim \frac{1}{\varphi(q)^K}\#\{n \leq x : P_R(n) > q, \gcd(f(n), q) = 1\}.& \qquad (4.1)\end{aligned}$$

Here

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

Even in the special case $k = K = 1$, this theorem improves over Theorem 2.1.3(a). The value of R is optimal for $K = 1$ and $f_1(n) = \sigma(n)$ modulo even q; see the discussion on applications in subsection § 4.1.5. For squarefree q, it suffices to have much weaker restrictions on n (that are often optimal in greater generality) to restore uniformity in the Siegel–Walfisz range.

Theorem 4.1.3. *The formulae* (4.1) *hold as* $x \to \infty$*, uniformly in coprime residues* $a_1, \dots, a_K$ *to* squarefree *moduli* $q \leq (\log x)^{K_0}$ *lying in* $\mathcal{Q}(k; f_1, \cdots, f_K)$ *and satisfying* $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$*, with*

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

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 $(\prod_{j=1}^{M} H_j)^2 \mid F$. Note that this is equivalent to saying that $\prod_{\substack{\theta \in \mathbb{C} \\ F(\theta)=0}} (T-\theta)^2 \mid F(T)$ in $\mathbb{C}[T]$, i.e., that every root of F in $\mathbb{C}$ has multiplicity at least 2.

It is worthwhile to try optimizing R above since doing so ensures weak equidistribution

among the largest possible set of inputs n. In subsection § 4.10.1, we show that the first two values of R in Theorem 4.1.3 are exactly optimal, in the sense that for any K and k, reducing the "2" to "1" or the "$k(Kk+K-k)+1$" to "$k(Kk+K-k)$" destroys uniformity in $q \leq (\log x)^{K_0}$: We also construct infinitely many general counterexamples showing this. In these examples, $\{W_{i,k}\}_{i=1}^{K}$ are pairwise coprime irreducibles, making $\prod_{i=1}^{K} W_{i,k}$ separable over $\mathbb{Q}$ (so that IFH is satisfied trivially).

4.1.4. Necessity of the multiplicative independence and invariant factor hypotheses

We now explain the necessity of these two hypotheses that we have been assuming in our results so far. It turns out that even if one of them is violated, then uniformity would fail in the above theorems in some of the worst possible ways: Not only would uniformity fail modulo arbitrarily large $q \leq (\log x)^{K_0}$, but also would be *unrecoverable* no matter how much we restrict our set of inputs n to those having many large prime factors!

For instance, without the multiplicative independence condition, the K congruences $f_i(n) \equiv a_i \pmod q$ (for $1 \leq i \leq K$) may degenerate to fewer congruences for sufficiently many inputs n. This would lead to failure of weak equidistribution uniformly to *all* sufficiently large q, *no matter how much* we restrict the inputs n to those having many large prime factors.

Theorem 4.1.4. *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 $C := C(W_{1,k},\dots,W_{K-1,k}) > 0$ such that*

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

as $x \to \infty$*, uniformly in* k*-admissible* $q \le (\log x)^{K_0}$ *supported on primes* $\ell > C$ *satisfying* $\gcd(\ell - 1, \beta(W_{1,k}, \ldots, W_{K-1,k})) = 1$*, and uniformly 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 $\{W_{i,k}\}_{1\le i\le K}$ 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 § 4.11.1). Using the above theorem, we shall construct (in § 4.11.1) explicit examples of polynomials $\{W_{i,k}\}_{1\le i\le K-1}$ 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 $n \le x$ 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 $f_1, \ldots, f_K$, 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 $\{W_{i,k}\}_{1\le i\le K}$.

Turning to the invariant factor hypothesis, we will show that the failure of this condition incurs an additional factor over the expected main term. For certain choices of q and $\{W_{i,k}\}_{1\le i\le K}$, 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 $f_1, \ldots, f_K$.

Theorem 4.1.5. *Fix* $R \ge 1$ *and assume that* $\{W_{i,k}\}_{1\le i\le K} \subset \mathbb{Z}[T]$ *are nonconstant, monic and multiplicatively independent, so that* $\beta = \beta(W_{1,k}, \ldots, W_{K,k}) \in \mathbb{Z} \setminus \{0\}$. *There exists a constant* $C := C(W_{1,k}, \ldots, W_{K,k}) > 0$ *such that*

$$\#\{n \le x : P_{Rk}(n) > q,\ (\forall i \in [K])\ f_i(n) \equiv a_i \pmod q\} \gg \frac{2^{\#\{\ell | q:\ \gcd(\ell-1,\beta)\neq 1\}}}{\varphi(q)^K} \cdot \frac{x^{1/k}(\log\log x)^{R-2}}{\log x} \quad (4.2)$$

as $x \to \infty$, uniformly in k-admissible $q \le (\log x)^{K_0}$ having $P^-(q) > C$, and uniformly 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 § 4.11.1, we shall construct explicit examples of $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ and $\{W_{i,k}\}_{1\le i\le K}$ for which the expression in the above lower bound is much larger than the expected proportion of $n \le x$ having $\gcd(f(n), q) = 1$. We shall establish Theorems 4.1.4 and 4.1.5 in section 4.11.

4.1.5. Some more concrete applications of our main results

We give several applications of our main results to arithmetic functions of common interest. In fact, as applications of Theorems 4.1.1 to 4.1.3 we can extend the results of Narkiewicz, Rayner, Śliwa, Dobrowolski and Fomenko (alluded to in the introduction) to varying moduli, – without imposing any unnecessary arithmetic restrictions on the moduli. For instance, recall Śliwa's result Proposition 1.3.10 that $\sigma(n)$ is weakly equidistributed precisely to fixed moduli that are not multiples of 6; in fact, his work shows that $\mathcal{Q}(1;\sigma) = \{q : \gcd(q,2) = 1\}$ and $\mathcal{Q}(2;\sigma) = \{q : \gcd(q,6) = 2\}$. Calling the members of the set $\mathcal{Q}(2;\sigma)$ *"special"*, our main results extend Śliwa's work as follows:

- By Theorem 4.1.1(i), $\sigma(n)$ is WUD uniformly to all odd moduli $q \le (\log x)^{K_0}$.

- Theorem 4.1.1(iii) shows that $\sigma(n)$ is WUD uniformly modulo all *special* $q \leq (\log x)^{(2-\delta)\widetilde{\alpha}(q)}$, where $\widetilde{\alpha}(q) := \alpha_2(q) = \prod_{\substack{\ell \mid q \\ \ell \equiv 1 \pmod 3}} (1 - 2/(\ell - 1))$.

- By Theorem 4.1.1(ii), $\sigma(n)$ is WUD uniformly modulo all squarefree *special* $q \leq (\log x)^{K_0}$ satisfying $2^{\omega(q)} \leq (\log x)^{(1-\epsilon)\widetilde{\alpha}(q)}$. By the example constructed in [71, subsection 7.1], these restrictions are optimal.

- By Theorem 4.1.2 (resp. 4.1.3), $\sigma(n)$ is WUD uniformly modulo *all special* (resp. modulo squarefree *special*) $q \leq (\log x)^{K_0}$ by restricting to inputs n with $P_6(n) > q$ (resp. $P_4(n) > q$). [2] By the examples constructed in [71], both of these restrictions are optimal as well.

We can give more applications of our main results to explicitly study the weak equidistribution of the functions $\sigma_r(n) := \sum_{d \mid n} d^r$ (for $r > 1$). An easy check shows that the polynomial $\sum_{0 \leq j \leq v} T^{rj} = \frac{T^{r(v+1)}-1}{T^r-1}$ shares no roots with its derivative, hence is separable. Calling the $q \in \mathcal{Q}(k; \sigma_r)$ as "k-special", Theorem 4.1.1 thus shows that σ_r is WUD uniformly modulo all k-special $q \leq (\log x)^{(1-\epsilon)\alpha_k(q)(1-1/kr)^{-1}}$, and modulo all squarefree k-special $q \leq (\log x)^{K_0}$ having $\omega(q) \leq (1-\epsilon)\alpha_k(q) \log\log x / \log(kr)$. Further, by Theorems 4.1.2 and 4.1.3, weak equidistribution is restored modulo all k-special (resp. modulo squarefree k-special) $q \leq (\log x)^{K_0}$ by restricting to n with $P_{k(kr+1)}(n) > q$ (resp. $P_{k+1}(n) > q$).

An explicit characterization of the moduli $q \leq (\log x)^{K_0}$ to which a given σ_r is weakly equidistributed thus reduces to an understanding of the possible k (for which $\mathcal{Q}(k; \sigma_r) \neq \emptyset$) 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 discussion following Proposition 1.3.10) have been studied in great depth in [75], [24], [51], [48], [49], [64] and [65].

[2] Here we have noted that the condition $P_3(n) > q$ forces $P_4(n) > q$ since for $\sigma(n)$ to be coprime to the even number q, it is necessary for n to be of the form m^2 or $2m^2$.

Other applications: we saw using Theorem 4.1.1 that $\varphi(n)$ and $\sigma(n)$ are jointly WUD modulo $q \leq (\log x)^{(1-\epsilon)\alpha(q)}$ coprime to 6, and that these two restrictions on q are necessary and essentially optimal. By Theorem 4.1.2, complete uniformity is restored to all moduli $q \leq (\log x)^{K_0}$ coprime to 6 by restricting to inputs n with $P_5(n) > q$. These results also imply that the function $\varphi(n)\sigma(n)$ is WUD uniformly modulo $q \leq (\log x)^{(1-\epsilon)\alpha(q)}$ coprime to 6; moreover, $\varphi(n)\sigma(n)$ is WUD uniformly modulo all $q \leq (\log x)^{K_0}$ coprime to 6 if we restrict to n with $P_5(n) > q$. Likewise, we can get interesting consequences of Theorems 4.1.1 to 4.1.3 for the families (φ, σ_3), $(\varphi, \sigma, \sigma_2)$, $(\varphi, \sigma, \sigma_2, \sigma_3)$ etc., as well as to exotic families like $(\varphi\sigma, \sigma_4)$, $(\varphi\sigma, \sigma\sigma_2), (\sigma, \sigma_2^2, \sigma_3^3, \sigma_4^4)$, $(\sigma\sigma_3, \sigma_2^2)$ and so on.

In general, Theorems 4.1.1 to 4.1.3 can be used to obtain more explicit analogues of the Siegel-Walfisz theorem for a family $(f_1, \ldots, f_K)$ of polynomially-defined multiplicative functions by means of an explicit understanding of the sets $\mathcal{Q}(k; f_1, \cdots, f_K)$. This is a "fixed modulus problem" that, – as mentioned in subsection § 1.4.2, – has been studied by multiple authors.

4.1.6. Summary of the main ideas

The arguments used to establish Theorems 4.1.1 to 4.1.3 comprise several themes.

(1) By studying the anatomy (prime factorizations) of our inputs n much more carefully, we refine the "mixing" phenomenon in Chapter 2.

(2) We invoke Halász's theorem and carefully estimate certain "pretentious distances" by adapting a technique used to bound exponential sums.

(3) We judiciously modify the Landau-Selberg-Delange method to obtain sharp upper bounds on the mean values of certain multiplicative functions involving characters mod q, **uniformly** for $q \leq (\log x)^{K_0}$ (applying known mean value results directly is

not enough to get the desired uniformity). To make these modifications, we adapt some ideas of Scourfield [69].

(4) Character sum machinery and linear algebra over rings come into play throughout the chapter. In fact, we invoke various extensions of the Weil bounds, and carefully study the Smith normal forms and invariant factors of several matrices, to bound certain character sums.

(5) We reformulate certain counting problems in terms of counting rational points of affine varieties over finite fields, which can be approached with arithmetic an geometric and algebro-geometric machinery, such as the Lang–Weil bound and properties of regular sequences.

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 $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v\leq V}}$ 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 $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v\leq V}}$.

In the conclusion of this chapter, we mention some new interesting questions arising from the results and methods used in this work.

Section 4.2

Technical preparation: The number of $n \leq x$ for which $\gcd(f(n), q) = 1$

In this section, we shall provide a rough estimate on the count of $n \leq x$ for which $f(n) = \prod_{i=1}^K f_i(n)$ is coprime to the modulus q, uniformly in $q \leq (\log x)^{K_0}$. We will

show the following estimate, which generalizes Proposition 2.2.1. In the rest of the chapter, we abbreviate $\alpha_v(q)$ to α_v for each $v \in [V]$.

Proposition 4.2.1. *For all sufficiently large x and uniformly in k-admissible $q \le (\log x)^{K_0}$, we have*

$$\sum_{\substack{n \le x \\ (f(n),q)=1}} 1 \;=\; \sum_{\text{each } \substack{n \le x \\ (f_i(n),q)=1}} 1 = \frac{x^{1/k}}{(\log x)^{1-\alpha_k}} \exp(O((\log_2(3q))^{O(1)})). \tag{4.3}$$

4.2.1. Proof of the lower bound.

Any $m \le x^{1/k}$ satisfying $\gcd(f(m^k), q) = 1$ is certainly counted in the left hand side of (4.3). To estimate the number of such m, we apply Proposition 2.2.1, with $f(n^k)$ and $x^{1/k}$ playing the roles of "$f(n)$" and "x" in the quoted proposition. This shows that the sum in (4.3) is bounded below by the right hand side.

4.2.2. Proof of the upper bound.

We start by giving an upper bound on the count of r-full smooth numbers; here we consider any $n \in \mathbb{N}$ to be 1-full (and we consider 1 as being r-full for any $r \ge 1$). The case $r = 1$ of the following result is Lemma 2.3.1.

Lemma 4.2.2. *Fix $r \in \mathbb{N}$. We have as $X, Z \to \infty$,*

$$\#\{n \le X : P(n) \le Z,\ n \text{ is } r\text{-full}\} \ll X^{1/r} (\log Z) \exp\left(-\frac{U}{r} \log U + O(U \log_2(3U))\right),$$

uniformly for $(\log X)^{\max\{3,2r\}} \le Z \le X^{1/2}$, where $U := \log X / \log Z$.

Proof of Lemma 4.2.2. The proof is an application of Rankin's trick. We start by

letting $\eta \le \min\{1/3, 1/2r\}$ be a positive parameter to be chosen later, and observe that

$$\sum_{\substack{n \le X:\ P(n) \le Z \\ n \text{ is } r\text{-full}}} 1 \le \sum_{\substack{n \text{ is } r\text{-full} \\ P(n) \le Z}} \left(\frac{X}{n}\right)^{(1-\eta)/r} \ll X^{(1-\eta)/r} \exp\left(\sum_{p \le Z} \frac{1}{p^{1-\eta}}\right), \tag{4.4}$$

where we have used the Euler product and noted that $\sum_p \sum_{v \ge r+1} p^{-v(1-\eta)/r} \ll \sum_p p^{-(1-\eta)(1+1/r)} \ll_r 1$ since $(1-\eta)(1+1/r) \ge (1+1/r)(1-\min\{1/3, 1/2r\}) > 1$.

Now set $\eta := \frac{\log U}{\log Z} \le \min\left\{\frac{1}{3}, \frac{1}{2r}\right\}$. We write $\sum_{p \le Z} 1/p^{1-\eta} = \log_2 Z + \sum_{p \le Z} (\exp(\eta \log p) - 1)/p + O(1)$. Since $\eta \log p \le \log 2 \ll 1$ for all $p \le 2^{1/\eta}$, we find that the contribution of $p \le 2^{1/\eta}$ to the last sum above is

$$\sum_{p \le 2^{1/\eta}} (\exp(\eta \log p) - 1)/p \ll \eta \sum_{p \le 2^{1/\eta}} \log p/p \ll 1,$$

while the contribution of $p \in (2^{1/\eta}, Z]$ is at most

$$(\exp(\eta \log Z) - 1) \sum_{2^{1/\eta} < p \le Z} 1/p \ \ \le\ \ U(\log_2 U + O(1)).$$

Collecting estimates, we obtain $\sum_{p \le Z} 1/p^{1-\eta} = \log_2 Z + O(U \log_2(3U))$, which from (4.4) completes the proof of the lemma. □

The following important observation will be useful throughout the chapter.

Lemma 4.2.3. *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 $\{W_{i,v}\}_{\substack{1 \le i \le K \\ 1 \le v \le k}}$.*

Proof. Let $S_v := \{\ell \text{ prime } : \alpha_v(\ell) = 0\}$. (Recall α_v and W_v from § 4.1.2.) Note the

following:

Observation 1. For each $1 \leq v < k$, the set S_v consists only of primes of size $O(1)$, with the implied constant depending only on the polynomials $W_{1,v}, \dots, W_{K,v}$:

This is because for any prime ℓ, we have $\alpha_v(\ell) = \frac{1}{\varphi(\ell)} \#\{u \in U_\ell : W_v(u) \in U_\ell\} \geq 1 - D_v/(\ell - 1)$. Thus, $\alpha_v(\ell) > 0$ for all $\ell > 1 + D_v = 1 + \sum_{i=1}^{K} \deg W_{i,v}$.

Observation 2. For any positive integer n satisfying $\gcd(f(n), q) = 1$, the k-free part of n must only be divisible by primes from $\bigcup_{1 \leq v < k} S_v$:

Assume by way of contradiction, that there exists some n satisfying $\gcd(f(n), q) = 1$ and some prime $p \notin \bigcup_{1 \leq v < k} S_v$ satisfying $p^r \parallel n$ for some $r < k$. Then $W_r(p) = f(p^r)$ divides $f(n)$. Since q is k-admissible and $r < k$, we must have $\alpha_r(q) = 0$. But since $\alpha_r(q) = \prod_{\ell \mid q} \alpha_r(\ell)$ by the Chinese Remainder Theorem, it follows that there must be some prime $\ell_0 \mid q$ for which $\alpha_r(\ell_0) = 0$. By definition of α_r, this means that for any unit $u \in U_{\ell_0}$, we must have $\ell_0 \mid W_r(u)$. In particular, since the prime p above does not lie in S_r while ℓ_0 does, it follows that $p \neq \ell_0$, so that $\ell_0 \mid W_r(p) \mid f(n)$, contradicting the requirement that $\gcd(f(n), q) = 1$.

Lemma 4.2.3 follows immediately Observations 1 and 2. □

Coming to the proof of the upper bound implied in (4.3), we define $y \coloneqq \exp(\sqrt{\log x})$ and start by removing those n which are divisible by the $(k+1)$-th power of a prime exceeding y. Writing any such n as AB for some k-free B and k-full A, Lemma 4.2.3

shows that $B \ll 1$ so that the contribution of such n to (4.3) is

$$\sum_{\substack{n\le x:\ (f(n),q)=1\\ \exists\ p>y:\ p^{k+1}|n}} 1 \ll \sum_{\substack{A\le x\\ A \text{ is } k\text{-full}\\ \exists\ p>y:\ p^{k+1}|n}} 1$$

$$\le \sum_{p>y} \sum_{\substack{v\ge k+1\\ p^v\le x}} \sum_{\substack{m\le x/p^v\\ m \text{ is } k\text{-full}}} 1 \ll \sum_{p>y} \sum_{v\ge k+1} \left(\frac{x}{p^v}\right)^{1/k} \ll \left(\frac{x}{y}\right)^{1/k}, \quad (4.5)$$

where we have used the fact that the number of k-full integers up to X is $O(X^{1/k})$ (see [23]). The last expression above is negligible in comparison to the right hand side of (4.3). Hence, it remains to bound the number of n satisfying $(f(n), q) = 1$ that are not divisible by the $(k+1)$-th power of any prime exceeding y.

We write any such n in the form BMN, where N is y-rough, BM is y-smooth, B is k-free, M is k-full, and B, M, N are pairwise coprime. By Lemma 4.2.3, we see that $B = O(1)$ and that N is k-full. But also since n is not divisible by the $(k+1)$-th power of any prime exceeding y, we must have $N = A^k$ for some squarefree y-rough integer A. Consequently,

$$\sum_{\substack{n\le x:\ (f(n),q)=1\\ p>y \implies p^{k+1}\nmid n}} 1 \quad \le \sum_{\substack{B\le x\\ (f(B),q)=1\\ B \text{ is } k\text{-free}}} \sum_{\substack{M\le x/B:\ M \text{ is } k\text{-full}\\ P(M)\le y,\ (f(M),q)=1}} \sum_{\substack{A\le (x/BM)^{1/k}\\ P^-(A)>y:\ (f(A^k),q)=1\\ A \text{ squarefree}}} 1. \quad (4.6)$$

We now write the right hand side of the above inequality as $\Sigma_1 + \Sigma_2$, where Σ_1 and Σ_2 count the contribution of (B, M, A) with $M \le x^{1/2}$ and $M > x^{1/2}$, respectively.

Bounding Σ_2: Any A counted in Σ_2 satisfies $A \le (x/BM)^{1/k} \le x^{1/2k}/B^{1/k}$, so that

$$\Sigma_2 \le \sum_{\substack{B\le x\\ (f(B),q)=1\\ B \text{ is } k\text{-free}}} \sum_{\substack{A\le x^{1/2k}/B^{1/k}\\ P^-(A)>y:\ (f(A^k),q)=1\\ A \text{ squarefree}}} \sum_{\substack{M\le x/BA^k:\ P(M)\le y\\ M \text{ is } k\text{-full},\ (f(M),q)=1}} 1.$$

To bound the innermost sum, we invoke Lemma 4.2.2; here $U = \frac{\log(x/BA^k)}{\log y} \ge \frac{1}{2}\sqrt{\log x}$. This yields

$$\Sigma_2 \ll \sum_{\substack{B \le x \\ (f(B),q)=1 \\ B \text{ is } k\text{-free}}} \sum_{\substack{A \le x^{1/2k}/B^{1/k} \\ P^-(A) > y:\ (f(A^k),q)=1 \\ A \text{ squarefree}}} \frac{x^{1/k}}{B^{1/k}A} \exp\left(-\frac{1}{6k}\sqrt{\log x} \cdot \log_2 x\right).$$

Recalling that $B = O(1)$ and bounding the sum on A trivially by $2\log x$, we deduce that $\Sigma_2 \ll x^{1/k} \exp\left(-\sqrt{\log x}\right)$, which is negligible compared to the right hand side of (4.3).

Bounding Σ_1: To bound the (innermost) sum on A in Σ_1, we invoke Lemma 2.2.2 on the multiplicative function $g(A) \coloneqq \mu(A)^2 \mathbb{1}_{P^-(A)>y} \mathbb{1}_{(f(A^k),q)=1}$, with μ denoting the Möbius function. Since $M \le x^{1/2}$ and $B \ll 1$, this gives

$$\Sigma_1 \ll \frac{x^{1/k}}{\log x} \exp\left(\sum_{y<p\le x} \frac{\mathbb{1}_{(W_k(p),q)=1}}{p}\right) \sum_{\substack{M \le x^{1/2}:\ M \text{ is } k\text{-full} \\ P(M) \le y,\ (f(M),q)=1}} \frac{1}{M^{1/k}}.$$

But since the sum on M above is no more than

$$\begin{aligned} \sum_{\substack{M \text{ is } k\text{-full} \\ P(M)\le y,\ (f(M),q)=1}} \frac{1}{M^{1/k}} &\le \prod_{p \le y} \left(1 + \frac{\mathbb{1}_{(f(p^k),q)=1}}{p} + O\left(\frac{1}{p^{1+1/k}}\right)\right) \\ &\ll \exp\left(\sum_{p\le y} \frac{\mathbb{1}_{(W_k(p),q)=1}}{p}\right), \end{aligned} \tag{4.7}$$

it follows by an estimation of $\sum_{p\le y} \mathbb{1}_{(W_k(p),q)=1}/p$ via Lemma 2.2.4, that Σ_1 is absorbed in the right hand side of (4.3). This establishes Proposition 4.2.1.

Section 4.3

The main term in Theorems 4.1.1 to 4.1.3: Contribution of "convenient" n

We start by defining

$$J \coloneqq \lfloor \log_3 x \rfloor \text{ and } y \coloneqq \exp((\log x)^{\epsilon/2}),$$

where ϵ is as in the statement of Theorem 4.1.1 and $\epsilon \coloneqq 1$ for Theorems 4.1.2 and 4.1.3. We call $n \leq x$ convenient if the largest J *distinct* prime divisors of n exceed y and each appear to exactly the k-th power in n. [3] In other words, n is convenient iff it can be uniquely written in the form $n = m(P_J \cdots P_1)^k$ for $m \leq x$ and primes $P_1, \ldots, P_J$ satisfying

$$L_m \coloneqq \max\{y, P(m)\} < P_J < \cdots < P_1. \tag{4.8}$$

Note that any n having $P_{Jk}(n) \leq y$ must be inconvenient; on the other hand, if n is inconvenient and satisfies $\gcd(f(n), q) = 1$ then either $P_{Jk}(n) \leq y$ or n is divisible by the $(k+1)$-th power of a prime exceeding y. These observations will be helpful in the rest of the chapter.

We start by showing that there are a negligible number of inconvenient $n \leq x$ satisfying $\gcd(f(n), q) = 1$.

[3] This is the more general version of the "convenient n" defined in section 2.3 where we were working in the case $k = 1$.

Proposition 4.3.1. *We have as $x \to \infty$,*

$$\sum_{\substack{n\le x:\ (f(n),q)=1\\ n\ inconvenient}} 1 \;=\; o\Bigg(\sum_{\substack{n\le x\\ (f(n),q)=1}} 1\Bigg), \tag{4.9}$$

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

Proof. By (4.5) and (4.3), the contribution of the n's that are divisible by the $(k+1)$-th power of a prime exceeding y is negligible. Letting $z := x^{1/\log_2 x}$, we show that the contribution of z-smooth n to the left side of (4.9) is also negligible compared to the right. Indeed, writing any such n in the form AB for some k-free B and k-full A, we have $P(A) \le z$ whereas (by Lemma 4.2.3) $B = O(1)$. Hence the contribution of z-smooth n is, by Lemma 4.2.2,

$$\sum_{\substack{n\le x:\ P(n)\le z\\ (f(n),q)=1}} 1 \;\ll \sum_{\substack{A\le x:\ P(A)\le z\\ A \text{ is } k\text{-full}}} 1 \;\ll x^{1/k}\exp\left(-\left(\frac{1}{k}+o(1)\right)\log_2 x\log_3 x\right), \tag{4.10}$$

which is indeed negligible compared to the right hand side of (4.9).

It remains to consider the contribution of those n which are neither z-smooth nor divisible by the $(k+1)$-th power of a prime exceeding y. Since n is inconvenient, we must have $P_{Jk}(n) \le y$ (see the discussion just preceding the statement of this proposition). Hence, n can be written in the form mP^k where $P := P(n) > z$ and $m = n/P^k$, so that $P_{Jk}(m) \le y$, $\gcd(m,P) = 1$ and $f(n) = f(m)f(P^k)$. Given m, there are at most $\sum_{z<P\le (x/m)^{1/k}} 1 \ll x^{1/k}/m^{1/k}\log z$ many possibilities for P.

Consequently,

$$\sum_{\substack{n\le x \text{ inconvenient}\\ P(n)>z,\ (f(n),q)=1\\ p>y\Longrightarrow p^{k+1}\nmid n}} 1 \le \sum_{\substack{n\le x:\ P_{Jk}(n)\le y\\ P(n)>z,\ (f(n),q)=1\\ p>y\Longrightarrow p^{k+1}\nmid n}} 1$$
$$\ll \frac{x^{1/k}\log_2 x}{\log x} \sum_{\substack{m\le x\\ P_{Jk}(m)\le y,\ (f(m),q)=1\\ p>y\Longrightarrow p^{k+1}\nmid m}} \frac{1}{m^{1/k}}. \tag{4.11}$$

As in the argument preceding (4.6), we write any m occurring in the above sum (uniquely) in the form BMA^k, where B is k-free, M is k-full, A is squarefree, $P(BM)\le y < P^-(A)$, and $\Omega(A)\le J$ (since $P_{Jk}(n)\le y$). Since $B=O(1)$, we deduce that

$$\sum_{\substack{m\le x\\ P_{Jk}(m)\le y,\ (f(m),q)=1\\ p>y\Longrightarrow p^{k+1}\nmid m}} \frac{1}{m^{1/k}} \ll \sum_{\substack{M\ k\text{-full}\\ P(M)\le y,\ (f(M),q)=1}} \frac{1}{M^{1/k}} \sum_{\substack{A\le x\\ \Omega(A)\le J}} \frac{1}{A}.$$

The sum on A is no more than

$$(1+\sum_{p\le x} 1/p)^J \le (2\log_2 x)^J \le \exp(O((\log_3 x)^2)),$$

while the sum on M is $\ll \exp(\alpha_k \log_2 y + O((\log_2(3q))^{O(1)}))$ by (4.7) and Lemma 2.2.4. Altogether,

$$\sum_{\substack{m\le x\\ P_{Jk}(m)\le y,\ (f(m),q)=1\\ p>y\Longrightarrow p^{k+1}\nmid m}} \frac{1}{m^{1/k}} \ll (\log x)^{\alpha_k\epsilon/2} \exp\big(O((\log_3 x)^2 + (\log_2(3q))^{O(1)})\big). \tag{4.12}$$

Inserting this into (4.11) and comparing with (4.3) completes the proof. □

It turns out that the convenient n give the dominant contributions in our asymptotics, in the sense that it is these n that give the desired main term.

Theorem 4.3.2. *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 $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$.

We shall prove this theorem in the next few sections. In this section and the next, we take the first step by showing a weaker version of this result, where we reduce the congruences $f_i(n) \equiv a_i$ from modulus q to a bounded divisor of q.

Proposition 4.3.3. *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. There exists a constant $\lambda := \lambda(W_{1,k}, \dots, W_{K,k}; B_0) > 0$ depending only on $\{W_{i,k}\}_{1\le i\le K} \subset \mathbb{Z}[T]$ and B_0, such that as $x \to \infty$, we have*

$$\begin{aligned}\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 \\ = \left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K \sum_{\substack{n\le x:\ (f(n),q)=1\\ (\forall i)\ f_i(n)\equiv a_i \pmod{Q_0}}} 1 \ + \ o\left(\frac{1}{\varphi(q)^K} \sum_{\substack{n\le x\\ (f(n),q)=1}} 1\right), \quad (4.13)\end{aligned}$$

uniformly in coprime residues $a_1, \dots, a_K$ to k-admissible moduli $q \le (\log x)^{K_0}$ satisfying $IFH(W_{1,k}, \dots, W_{K,k}; B_0)$. Here Q_0 is some divisor of q satisfying $Q_0 \le \lambda$.

Proof. For any $N \geq 1$ and $(w_i)_{i=1}^K \in U_q^K$, we define

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

We write each convenient n uniquely in the form $m(P_J\cdots P_1)^k$, where $m, P_J, \dots, P_1$ satisfy (4.8). Then $f_i(n) = f_i(m)\prod_{j=1}^J W_{i,k}(P_j)$, so that the conditions $f_i(n)\equiv a_i \pmod q$ amount to $\gcd(f(m),q)=1$ and

$$(P_1,\dots,P_J) \bmod q \in \mathcal{V}'_{q,m} \coloneqq \mathcal{V}_{J,K}^{(k)}\left(q;(a_i f_i(m)^{-1})_{i=1}^K\right).$$

Noting that the conditions $P_1\cdots P_J \leq (x/m)^{1/k}$ and $(P_1,\dots,P_J) \bmod q \in \mathcal{V}'_{q,m}$ are both independent of the ordering of $P_1,\dots,P_J$, we obtain

$$\sum_{\substack{n\leq x \text{ convenient}\\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 = \sum_{\substack{m\leq x\\ (f(m),q)=1}} \sum_{(v_1,\dots,v_J)\in\mathcal{V}'_{q,m}} \frac{1}{J!} \sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\leq (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \pmod q}} 1. \tag{4.14}$$

Proceeding exactly as in the argument for (2.13), we remove the congruence conditions on $P_1,\dots,P_J$ by successive applications of the Siegel–Walfisz Theorem. We get

$$\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\leq (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \pmod q}} 1 = \frac{1}{\varphi(q)^J} \sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\leq (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}}} 1 + O\left(\frac{x^{1/k}}{m^{1/k}}\exp\left(-K_1(\log x)^{\epsilon/4}\right)\right)$$

for some constant $K_1 \coloneqq K_1(K_0) > 0$.

Collecting estimates and noting that $\#\mathcal{V}'_{q,m} \leq \varphi(q)^J \leq (\log x)^{K_0 J}$, we obtain

$$\sum_{\substack{n\leq x \text{ convenient} \\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 = \sum_{\substack{m\leq x \\ (f(m),q)=1}} \frac{\#\mathcal{V}'_{q,m}}{\varphi(q)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m \\ P_1\cdots P_J\leq (x/m)^{1/k} \\ P_1,\dots,P_J \text{ distinct}}} 1\right) + O\left(x^{1/k}\exp\left(-\frac{K_1}{2}(\log x)^{\epsilon/4}\right)\right). \quad (4.15)$$

Here in the last step we have crudely bounded the sum $\sum_{\substack{m\leq x \\ (f(m),q)=1}} m^{-1/k}$ by writing each m as AB for some k-full A and k-free B satisfying $\gcd(A,B)=1$, and recalling that $B = O(1)$ while $\sum 1/A \leq \prod_{p\leq x}\left(1+1/p+O\left(1/p^{1+1/k}\right)\right)$. The following proposition estimates $\#\mathcal{V}'_{q,m}$. Note that it actually involves *only* B_0 and the polynomials $\{W_{i,k}\}_{1\leq i\leq K}$, nothing else.

Proposition 4.3.4. *Assume that $\{W_{i,k}\}_{1\leq i\leq K}$ are multiplicatively independent. Define the quantities $D = \sum_{i=1}^K \deg W_{i,k}$ and $\alpha_k(q) = \frac{1}{\varphi(q)}\#\{u\in U_q : \prod_{i=1}^K W_{i,k}(u)\in U_q\}$ as before.*

There exists a constant $C_0 := C_0(W_{1,k},\dots,W_{K,k};B_0) > (8D)^{2D+2}$ depending only on $\{W_{i,k}\}_{1\leq i\leq K}$ and B_0, such that for <u>any</u> constant $C > C_0$, the following two estimates hold uniformly in coprime residues $(w_i)_{i=1}^K$ to moduli q satisfying $\alpha_k(q)\neq 0$ and $IFH(W_{1,k},\dots,W_{K,k};B_0)$:

$$\frac{\#\mathcal{V}^{(k)}_{N,K}\left(q;(w_i)_{i=1}^K\right)}{\varphi(q)^N} = \frac{\alpha_k(q)^N}{\alpha_k(Q_0)^N}\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K\left\{\frac{\#\mathcal{V}^{(k)}_{N,K}\left(Q_0;(w_i)_{i=1}^K\right)}{\varphi(Q_0)^N}+O\left(\frac{1}{C^N}\right)\right\} \prod_{\substack{\ell\mid q \\ \ell>C_0}}\left(1+O\left(\frac{(4D)^N}{\ell^{N/D-K}}\right)\right), \quad (4.16)$$

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

Moreover

$$\frac{\#\mathcal{V}_{N,K}^{(k)}\left(q;(w_i)_{i=1}^K\right)}{\varphi(q)^N} \le \frac{\left(\prod_{\ell^e\|q} e\right)^{\mathbb{1}_{N=KD}}}{q^{N/D}}\ \exp\left(O(\omega(q))\right), \quad \textit{for each } 1\le N\le KD. \tag{4.17}$$

Applying (4.16) with $N := J = \lfloor \log_3 x\rfloor \ge KD+1$, and with C fixed to be a constant exceeding $2C_0^{C_0}$, we see that

$$\frac{\#\mathcal{V}'_{q,m}}{\varphi(q)^J} = (1+o(1))\frac{\alpha_k(q)^J}{\alpha_k(Q_0)^J}\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K\left\{\frac{\#\mathcal{V}'_{Q_0,m}}{\varphi(Q_0)^J}+O\left(\frac{1}{C^J}\right)\right\},$$

where $\mathcal{V}'_{Q_0,m} := \mathcal{V}_{J,K}^{(k)}\big(Q_0;(a_if_i(m)^{-1})_{i=1}^K\big)$ and we have noted that

$$\sum_{\substack{\ell\mid q\\ \ell>C_0}} (4D)^J/\ell^{J/D-K} \le \left(4D/C_0^{1/(2D+2)}\right)^J = o(1).$$

We insert this into (4.15), and observe that since $\alpha_k(q)\neq 0$, since $Q_0\mid q$ and since Q_0 is C_0-smooth, we have

$$\alpha_k(Q_0)C \ge C\prod_{\ell\le C_0}\left(1-\frac{\ell-2}{\ell-1}\right) \ge \frac{C}{C_0^{C_0}} \ge 2.$$

Thus

$$\begin{aligned}\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ f_i(n)\equiv a_i \,(\mathrm{mod}\ q)}} 1 &= (1+o(1))\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K\frac{\alpha_k(q)^J}{\alpha_k(Q_0)^J}\sum_{\substack{m\le x\\ (f(m),q)=1}}\frac{\#\mathcal{V}'_{Q_0,m}}{\varphi(Q_0)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}}} 1\right)\\ &\quad + o\left(\frac{1}{\varphi(q)^K}\sum_{\substack{n\le x\\ (f(n),q)=1}} 1\right),\end{aligned} \tag{4.18}$$

where we have noted that

$$\sum_{\substack{n\le x \text{ convenient}\\ \gcd(f(n),q)=1}} 1 = \alpha_k(q)^J \sum_{\substack{m\le x\\ (f(m),q)=1}} \left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}}} 1\right) + O\left(x^{1/k}\exp\left(-\frac{K_1}{2}(\log x)^{\epsilon/4}\right)\right). \quad (4.19)$$

Here (4.19) can be proven by replicating the arguments leading to (4.15) and observing that

$$\#\{(v_1,\dots,v_J)\in U_q^J:\ \prod_{j=1}^J W_k(v_j)\in U_q\} = (\alpha_k(q)\varphi(q))^J.$$

Now for each $(w_i)_{i=1}^K \in U_q^K$, we define $\mathcal{U}_{J,K}\big(q,Q_0;(w_i)_{i=1}^K\big)$ to be the set of tuples $(v_1,\dots,v_J)\in U_q^J$ satisfying $\prod_{j=1}^J W_{i,k}(v_j)\in U_q$ and $\prod_{j=1}^J W_{i,k}(v_j)\equiv w_i \pmod{Q_0}$ for each $i\in[K]$. Observe that any convenient n satisfying $\gcd(f(n),q)=1$ and $f_i(n)\equiv a_i \pmod{Q_0}$ for all $i\in[K]$, can be uniquely written in the form $n=m(P_J\cdots P_1)^k$, where $P_J,\dots,P_1$ are primes satisfying (4.8), and where $\gcd(f(m),q)=1$ and $(P_1,\dots,P_J) \bmod q \in \mathcal{U}_m := \mathcal{U}_{J,K}\big(q,Q_0;\ (a_i f_i(m)^{-1})_{i=1}^K\big)$. As such, by the arguments leading to (4.15), we obtain

$$\sum_{\substack{n\le x \text{ convenient}\\ \gcd(f(n),q)=1\\ (\forall i)\ f_i(n)\equiv a_i \pmod{Q_0}}} 1 = \sum_{\substack{m\le x\\ (f(m),q)=1}} \frac{\#\mathcal{U}_m}{\varphi(q)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}}} 1\right) + o\left(\frac{1}{\varphi(q)^K}\sum_{\substack{n\le x\\ (f(n),q)=1}} 1\right). \quad (4.20)$$

A simple counting argument shows the following general observation: Let $F\in\mathbb{Z}[T]$ be nonconstant, and let d,d' be positive integers such that $d'\mid d$ and $\alpha_F(d) := \frac{1}{\varphi(d)}\#\{u\in U_d : F(u)\in U_d\}$ is nonzero (hence so is $\alpha_F(d')$). Then for any $u\in U_{d'}$ for

which $F(u) \in U_{d'}$, we have

$$\#\{U \in U_d : \ U \equiv u \pmod{d'}, \ F(U) \in U_d\} = \frac{\alpha_F(d)\varphi(d)}{\alpha_F(d')\varphi(d')}. \tag{4.21}$$

Using this general observation for $F \coloneqq W_k = \prod_{i=1}^{K} W_{i,k}$ (so that $\alpha_F = \alpha_k$), we obtain

$$\#\mathcal{U}_{J,K}\big(q, Q_0; (w_i)_{i=1}^K\big) = \left(\frac{\alpha_k(q)\varphi(q)}{\alpha_k(Q_0)\varphi(Q_0)}\right)^J \#\mathcal{V}_{J,K}^{(k)}\big(Q_0, (w_i)_{i=1}^K\big)$$

for all $(w_i)_{i=1}^K \in U_q^K$. Applying this with $w_i \coloneqq a_i f_i(m)^{-1}$ and recalling that $\mathcal{V}'_{Q_0,m}$ $= \mathcal{V}_{J,K}^{(k)}\big(Q_0; (a_i f_i(m)^{-1})_{i=1}^K\big)$, we get from (4.20),

$$\begin{aligned}\sum_{\substack{n\le x \text{ convenient}\\ \gcd(f(n),q)=1\\ (\forall i)\ f_i(n)\equiv a_i \pmod{Q_0}}} 1 \ &= \frac{\alpha_k(q)^J}{\alpha_k(Q_0)^J} \sum_{\substack{m\le x\\ (f(m),q)=1}} \frac{\mathcal{V}'_{Q_0,m}}{\varphi(Q_0)^J}\left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J > L_m\\ P_1\cdots P_J \le (x/m)^{1/k}\\ P_1,\dots,P_J \text{ distinct}}} 1\right)\\ &\qquad + \ o\left(\frac{1}{\varphi(q)^K} \sum_{\substack{n\le x\\ (f(n),q)=1}} 1\right).\end{aligned}$$

Comparing this with (4.18), we obtain

$$\begin{aligned}\sum_{\substack{n\le x \text{ convenient}\\ (\forall i)\ f_i(n)\equiv a_i \pmod{q}}} 1 \ &= (1+o(1))\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K \sum_{\substack{n\le x \text{ convenient}\\ \gcd(f(n),q)=1\\ (\forall i)\ f_i(n)\equiv a_i \pmod{Q_0}}} 1\\ &\qquad + \quad o\left(\frac{1}{\varphi(q)^K} \sum_{\substack{n\le x\\ (f(n),q)=1}} 1\right).\end{aligned}$$

Finally, an application of Proposition 4.3.1 allows us to remove the condition of n being convenient from the main term on the right hand side above. This completes the proof of Proposition 4.3.3, up to the proof of Proposition 4.3.4, which we take up in the next section. □

Section 4.4

Counting solutions to congruences: Proof of Proposition 4.3.4

4.4.1. Preparation for the proof of Proposition 4.3.4

We temporarily abandon all the previous set-up just for this subsection. We shall make use of two character sum bounds, which we state in the next two propositions.

Proposition 4.4.1. *Let ℓ be a prime, χ a Dirichlet character mod ℓ. Let $F \in \mathbb{Z}[T]$ be 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*

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

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

This is a version of the Weil bounds and is a special case of [77, Corollary 2.3] (see also [18], [79] and [66] for older results). We will also need an analogue of the above result for character sums to higher prime power moduli, and this input is provided by the following consequences of Theorems 1.2 and 7.1 and eqn. (1.15) in work of Cochrane [14] (see [16] for related results).

In what follows, for a polynomial $H \in \mathbb{Z}[T]$, we denote by H' or $H'(T)$ the formal derivative of H. Let ℓ be a prime such that $\mathrm{ord}_\ell(H) = 0$, so that H is not identically zero in $\mathbb{F}_\ell[T]$ (see § 1.5.1 for definition of ord_ℓ). By the ℓ-critical polynomial associated to H we shall mean the polynomial $\mathcal{C}_H := \ell^{-\mathrm{ord}_\ell(H')} H'$, which has integer coefficients and can be considered as a nonzero element of the ring $\mathbb{F}_\ell[T]$. 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). Finally, for any $\theta \in \mathbb{F}_\ell$, we use $\mu_\theta(H)$ to denote the multiplicity of θ as a zero of H.

Proposition 4.4.2. *Let ℓ be a prime, $g \in \mathbb{Z}[T]$ a nonconstant polynomial, and $t \coloneqq \mathrm{ord}_\ell(g')$. Consider an integer $e \geq t+2$ and a primitive character χ mod ℓ^e. Let $M \coloneqq \max_{\theta \in \mathcal{A}(g;\ell)} \mu_\theta(\mathcal{C}_g)$ be the maximum multiplicity of an ℓ-critical point of g.*

(i) For odd ℓ, we have

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

(ii) For $\ell = 2$ and $e \geq t+3$, we have

$$\left| \sum_{u \bmod 2^e} \chi(g(u)) \right| \leq (12.5) 2^{t/(M+1)} \ 2^{e(1-1/(M+1))}.$$

In fact, the sum is zero if g has no 2-critical points.

In order to make use of the aforementioned bounds, we will need to understand the quantities that appear when we apply them. The following observations enable us to do this.

Proposition 4.4.3. *Let $\{F_i\}_{i=1}^K \subset \mathbb{Z}[T]$ be nonconstant and multiplicatively independent. There exists a constant $C_1 \coloneqq C_1(F_1, \ldots, F_K) \in \mathbb{N}$ such that all of the following hold:*

(a) *For any prime ℓ, there are $O(1)$ many tuples $(A_1, \ldots, A_K) \in [\ell-1]^K$ 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,*

$$\tau(\ell) \coloneqq \mathrm{ord}_\ell\left((T^{\varphi(\ell^r)}F_1(T)^{A_1}\cdots F_K(T)^{A_K})'\right) = \mathrm{ord}_\ell(\widetilde{F}(T)) \begin{cases} = 0, & \text{if } \ell > C_1, r \geq 2 \\ \leq C_1, & \text{if } \ell \leq C_1, \mathrm{ord}_\ell\left(\prod_{i=1}^K F_i\right) = 0, r \geq C_1+2, \end{cases} \tag{4.22}$$

where $\widetilde{F}(T) \coloneqq \sum_{i=1}^K A_i F_i'(T)\prod_{\substack{1\leq j\leq K\\ j\neq i}} F_j(T)$. *In either of the two cases above, any root* $\theta \in \mathbb{F}_\ell$ *of the polynomial*

$$\mathcal{C}_\ell(T) \coloneqq \ell^{-\tau(\ell)}(T^{\varphi(\ell^r)}F_1(T)^{A_1}\cdots F_K(T)^{A_K})'$$

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]

Proof. We start by writing $F_i =: r_i\prod_{j=1}^M G_j^{\mu_{ij}}$ as in subsection § 4.1.1, so that $r_i \in \mathbb{Z}$ and $G_1,\dots,G_M \in \mathbb{Z}[T]$ are irreducible, primitive and pairwise coprime, and $M = \omega(F_1\cdots F_K)$. Recall that $M \geq K$ and that the exponent matrix $E_0(F_1,\dots,F_K)$ has $\mathbb{Q}$-linearly independent columns, making $\beta(F_1,\dots,F_K)$ a nonzero integer. Further, since G_j are pairwise coprime irreducibles, the resultants $\mathrm{Res}(G_j, G_{j'})$ and discriminants $\mathrm{disc}(G_j)$ are nonzero integers for all $j \neq j' \in [M]$. Note that for any prime

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

ℓ not dividing the leading coefficient of any G_j and not dividing

$$\prod_{1\le j\le M} \mathrm{disc}(G_j)\cdot \prod_{1\le j\ne j'\le M} \mathrm{Res}(G_j, G_{j'}),$$

the product $\prod_{j=1}^{M} G_j$ is separable in $\mathbb{F}_\ell[T]$.

Also since $(F_1^{c_1}\cdots F_K^{c_K})' = \left(\prod_{i=1}^{K} F_i^{c_i-1}\right)\sum_{i=1}^{K} c_i F_i' \prod_{\substack{1\le j\le K\\ j\ne i}} F_j$, the multiplicative independence of the polynomials $\{F_i\}_{i=1}^{K}$ forces the polynomials $\left\{F_i' \prod_{\substack{1\le j\le K\\ j\ne i}} F_j\right\}_{i=1}^{K} \subset \mathbb{Z}[T]$ to be $\mathbb{Q}$-linearly independent. Writing $D \coloneqq \deg(F_1\cdots F_K)$ and writing each $F_i'(T)\prod_{\substack{1\le j\le K\\ j\ne i}} F_j(T) = \sum_{j=0}^{D-1} c_{i,j}T^j$ for some $\{c_{i,j}\}_{0\le j\le D-1}\subset\mathbb{Z}$, we thus deduce that the columns of the matrix

$$M_1 \coloneqq M_1(F_1,\dots,F_K) \coloneqq \begin{pmatrix} c_{1,0} & \cdots & c_{K,0}\\ \cdots & \cdots & \cdots\\ \cdots & \cdots & \cdots\\ c_{1,D-1} & \cdots & c_{K,D-1}\end{pmatrix} \in \mathbb{M}_{D\times K}(\mathbb{Z}) \tag{4.23}$$

must be $\mathbb{Q}$-linearly independent. Consequently, $D\ge K$ and the last diagonal entry $\widetilde{\beta}\in\mathbb{Z}\setminus\{0\}$ of the Smith Normal form of M_1 is also the largest invariant factor of M_1 (in size).

Fix $C_1 \coloneqq C_1(F_1,\dots,F_K)$ to be any positive integer exceeding all of the following:

- $\max\left\{2,\ \ |\widetilde{\beta}|,\ \ \prod_{j=1}^{M}|\mathrm{disc}(G_j)|\cdot\prod_{1\le j\ne j'\le M}|\mathrm{Res}(G_j,G_{j'})|\right\}$
  (recall that these are all nonzero),
- the sizes of the leading coefficients of $F_1,\dots,F_K,G_1,\dots,G_M$.

We claim that any such C_1 satisfies the properties in the statement of the proposition.

Proof of (a). We may assume that $\ell > C_1$. Let $\beta \coloneqq \beta(F_1, \dots, F_K)$, as defined in § 4.1.1. By the discussion at the start of the proof, the conditions defining C_1 force $G_1, \dots, G_M$ to be pairwise coprime in $\mathbb{F}_\ell[T]$. Let $(A_1, \dots, A_K) \neq (0, \dots, 0)$ be any tuple of nonnegative integers 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 $G \in \mathbb{F}_\ell[T]$. We claim that $A_1, \dots, A_K$ must all be divisible by $(\ell-1)/d_1$ where $d_1 \coloneqq \gcd(\ell-1, \beta)$. This will be enough to complete the proof of (a), since there are no more than $d_1^K \leq |\beta|^K \ll 1$ many tuples $(A_1, \dots, A_K) \in [\ell-1]^K$ with each A_i divisible by $(\ell-1)/d_1$.

To establish the above claim, we may assume without loss of generality that G is monic, and note that $c \in \mathbb{F}_\ell^\times$ since $\mathrm{ord}_\ell(F_1 \cdots F_K) = 0$ by definition of C_1. Write each G_j as $\lambda_j H_j$ in the ring $\mathbb{F}_\ell[T]$, for some $\lambda_j \in \mathbb{F}_\ell^\times$ and nonconstant monic $H_j \in \mathbb{F}_\ell[T]$ (which can be done since ℓ doesn't divide the leading coefficient of any G_j). Then $F_i = r_i \prod_{j=1}^M G_j^{\mu_{ij}} = \rho_i \prod_{j=1}^M H_j^{\mu_{ij}}$ for some $\rho_i \in \mathbb{F}_\ell^\times$. Since $c \cdot G^{\ell-1} = \prod_{i=1}^K F_i^{A_i} = \left(\prod_{i=1}^K \rho_i^{A_i}\right) \cdot \prod_{1 \leq j \leq M} H_j^{\sum_{i=1}^K \mu_{ij} A_i}$ in $\mathbb{F}_\ell[T]$, and $G, H_1, \dots, H_M$ are all monic, we find that $G^{\ell-1} = \prod_{1 \leq j \leq M} H_j^{\sum_{i=1}^K \mu_{ij} A_i}$. But now since $\prod_{1 \leq j \leq M} G_j$ is separable in $\mathbb{F}_\ell[T]$, so is $\prod_{1 \leq j \leq M} H_j$, and we deduce that $\sum_{i=1}^K \mu_{ij} A_i \equiv 0 \pmod{\ell-1}$ for each $j \in [M]$. This can be rewritten as the matrix congruence $(0 \cdots \cdots 0)^\top \equiv E_0 (A_1 \cdots A_K)^\top \pmod{\ell-1}$; each side of this congruence is an $M \times 1$ matrix, $Y^\top$ denotes the transpose of a matrix Y and E_0 is the exponent matrix defined in § 4.1.1.

Now since $M \geq K$ and E_0 has full rank, there exist $P_0 \in GL_{M \times M}(\mathbb{Z})$ and $R_0 \in GL_{K \times K}(\mathbb{Z})$ for which $P_0 E_0 R_0$ is the Smith Normal Form $\mathrm{diag}(\beta_1, \dots, \beta_K)$ of E_0, with $\beta_1, \dots, \beta_K \in \mathbb{Z} \setminus \{0\}$ being the invariant factors of E_0. Thus $\beta_i \mid \beta_{i+1}$ for all $1 \leq i < K$ and $\beta = \beta(F_1, \dots, F_K) = \beta_K$. This means that $P_0 E_0 = \mathrm{diag}(\beta_1, \dots, \beta_K) R_0^{-1}$ and

writing $(q_{ij})_{1\le i,j\le K} \coloneqq R_0^{-1}$, we find that

$$\begin{pmatrix} 0 \\ \cdots \\ \cdots \\ 0 \end{pmatrix}_{M\times 1} \equiv P_0 E_0 \begin{pmatrix} A_1 \\ \cdots \\ A_K \end{pmatrix}_{K\times 1} \equiv \begin{pmatrix} \beta_1(q_{11}A_1 + \cdots + q_{1K}A_K) \\ \cdots \\ \beta_K(q_{K1}A_1 + \cdots + q_{KK}A_K) \\ 0 \\ \cdots \\ 0 \end{pmatrix}_{M\times 1} \pmod{\ell-1}.$$

Hence for each $i \in [K]$, $\beta_i(q_{i1}A_1 + \cdots + q_{iK}A_K) \equiv 0 \pmod{\ell-1}$, so that $(\ell-1)/\gcd(\ell-1,\beta_i)$ divides $q_{i1}A_1 + \cdots + q_{iK}A_K$. But since $\beta_i \mid \beta_K$, it follows that $(\ell-1)/\gcd(\ell-1,\beta_K) = (\ell-1)/d_1$ also divides $q_{i1}A_1 + \cdots + q_{iK}A_K$ for each $i \in [K]$. We obtain

$$\begin{pmatrix} 0 \\ \cdots \\ 0 \end{pmatrix}_{K\times 1} \equiv \begin{pmatrix} q_{11}A_1 + \cdots + q_{1K}A_K \\ \cdots \\ q_{K1}A_1 + \cdots + q_{KK}A_K \end{pmatrix}_{K\times 1} \equiv R_0^{-1} \begin{pmatrix} A_1 \\ \cdots \\ A_K \end{pmatrix}_{K\times 1} \left(\mathrm{mod}\ \frac{\ell-1}{d_1}\right), \tag{4.24}$$

establishing the desired claim that $(A_1,\dots,A_K) \equiv (0,\dots,0) \left(\mathrm{mod}\ \frac{\ell-1}{d_1}\right)$.

Proof of (b). We start by noting that

$$\begin{aligned}(T^{\varphi(\ell^r)}F_1(T)^{A_1}\cdots F_K(T)^{A_K})' \\ = \varphi(\ell^r)T^{\varphi(\ell^r)-1}\prod_{i=1}^{K}F_i(T)^{A_i} + T^{\varphi(\ell^r)}\left(\prod_{i=1}^{K}F_i(T)^{A_i-1}\right)\widetilde{F}(T),\end{aligned} \tag{4.25}$$

where $\widetilde{F}(T)$ is as in the statement of the proposition. We claim that $\mathrm{ord}_\ell(\widetilde{F}) \le \mathbb{1}_{\ell\le C_1}C_1$ for all primes ℓ satisfying $\mathrm{ord}_\ell(F_1\cdots F_K) = 0$ and for all nonnegative integers

$A_1, \ldots, A_K$ satisfying $(A_1, \ldots, A_K) \not\equiv (0, \ldots, 0) \bmod \ell$. To show this, we proceed as in the proof of (a), but working with the matrix M_1 defined in (4.23) in place of the exponent matrix E_0. Observe that $\widetilde{F}(T) = \sum_{j=0}^{D-1} \left(\sum_{i=1}^{K} c_{i,j} A_i \right) T^j$, hence if $\kappa(\ell) \coloneqq \mathrm{ord}_\ell(\widetilde{F})$, then $\ell^{\kappa(\ell)}$ divides all the entries of the matrix $M_1 (A_1 \cdots A_K)^\top$. Since M_1 has full rank and $D = \sum_{i=1}^{K} \deg F_i \geq K$ many rows, and since $(A_1, \ldots, A_K) \not\equiv (0, \ldots, 0) \bmod \ell$, an argument entirely analogous to the one leading to (4.24) shows that $\ell^{\kappa(\ell)}$ divides the last invariant factor $\widetilde{\beta}$ of M_1. Hence $\mathrm{ord}_\ell(\widetilde{F}) = \kappa(\ell) \leq v_\ell(\widetilde{\beta})$ and our claim follows as $|\widetilde{\beta}| < C_1$.

As a consequence, we find that $\mathrm{ord}_\ell \left(T^{\varphi(\ell^r)} \left(\prod_{i=1}^{K} F_i(T)^{A_i - 1} \right) \widetilde{F}(T) \right) = \mathrm{ord}_\ell(\widetilde{F}) \leq \mathbb{1}_{\ell \leq C_1} C_1$ for all primes $\ell \leq C_1$ satisfying $\mathrm{ord}_\ell(F_1 \cdots F_K) = 0$, and also for all primes $\ell > C_1$ (for which the condition $\mathrm{ord}_\ell(F_1 \cdots F_K) = 0$ is automatic by definition of C_1). But now since $\mathrm{ord}_\ell(\varphi(\ell^r)) \geq 1$ for $r \geq 2$ and $\mathrm{ord}_\ell(\varphi(\ell^r)) \geq C_1 + 1$ for $r \geq C_1 + 2$, (4.25) shows that $\tau(\ell) = \mathrm{ord}_\ell \left(T^{\varphi(\ell^r)} \left(\prod_{i=1}^{K} F_i(T)^{A_i - 1} \right) \widetilde{F}(T) \right)$, establishing subpart (b) of the proposition.

Finally, since in both the cases of (4.22), we have $\tau(\ell) < r - 1$, the identity (4.25) reveals that

$$\begin{aligned} \mathcal{C}_\ell(T) &\equiv \ell^{-\tau(\ell)} \left(T^{\varphi(\ell^r)} \prod_{i=1}^{K} F_i(T)^{A_i} \right)' \\ &\equiv T^{\varphi(\ell^r)} \left(\prod_{i=1}^{K} F_i(T)^{A_i - 1} \right) \left(\ell^{-\tau(\ell)} \widetilde{F}(T) \right) \text{ in the ring } \mathbb{F}_\ell[T]. \end{aligned}$$

As such, any root of the polynomial $\theta \in \mathbb{F}_\ell$ of $\mathcal{C}_\ell(T)$ (considered as a nonzero element of $\mathbb{F}_\ell[T]$) which is not a root of $T \prod_{i=1}^{K} F_i(T)$, must be a root of $\ell^{-\tau(\ell)} \widetilde{F}(T)$, and θ must have the same multiplicity in $\mathcal{C}_\ell(T)$ and $\ell^{-\tau(\ell)} \widetilde{F}(T)$. This completes the proof of Proposition 4.4.3. $\square$

4.4.2. Proof of Proposition 4.3.4

We return to the set-up in Proposition 4.3.4. Since $\alpha_k(q) \neq 0$, we have

$$\mathrm{ord}_\ell(\prod_{i=1}^{K} W_{i,k}) = 0$$

for each prime $\ell \mid q$. Fix $C_0 \coloneqq C_0\left(\{W_{i,k}\}_{1\leq i\leq K}; B_0\right)$ to be any constant exceeding B_0, $(32D)^{2D+2}$, the sizes of the leading and constant coefficients of $\{W_{i,k}\}_{1\leq i\leq K}$, as well as the constant $C_1(W_{1,k},\dots,W_{K,k})$ coming from an application of Proposition 4.4.3 to the family $\{W_{i,k}\}_{1\leq i\leq K}$ of multiplicatively independent polynomials. We will show that any such choice of C_0 suffices.

We first consider the case $D > 1$; the case $D = 1$ will be dealt with towards the end of the argument. For an arbitrary positive integer Q and coprime residues $w_1,\dots,w_K \bmod Q$, an application of the orthogonality of Dirichlet characters yields

$$\#\mathcal{V}_{N,K}^{(k)}\left(Q;(w_i)_{i=1}^K\right) = \frac{1}{\varphi(Q)^K}\sum_{\chi_1,\dots,\chi_K \bmod Q} \overline{\chi}_1(w_1)\cdots\overline{\chi}_K(w_K)(Z_{Q;\chi_1,\dots,\chi_K})^N, \quad (4.26)$$

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

Dealing with the large primes dividing q: We first show that there exists a constant $K' = K'(\{W_{i,k}\}_{1\leq i\leq K})$ such that uniformly in primes $\ell > C_0$ dividing q, we have

$$\frac{\#\mathcal{V}_{N,K}^{(k)}\left(\ell^e;(w_i)_{i=1}^K\right)}{\varphi(\ell^e)^N}$$

$$\begin{cases} = \dfrac{\alpha_k(\ell)^N}{\varphi(\ell^e)^K}\left(1+O\left(\dfrac{(4D)^N}{\ell^{N/D-K}}\right)\right), \text{ uniformly in } N \geq KD+1 \\ \\ \leq K' \ e^{\mathbb{1}_{N=KD}}\ell^{-eN/D}, \text{ for each } 1 \leq N \leq KD. \end{cases} \tag{4.27}$$

To show these, we start by applying (4.26) to get

$$\frac{\#\mathcal{V}_{N,K}^{(k)}(\ell^e;(w_i)_{i=1}^K)}{\varphi(\ell^e)^N} = \frac{\alpha_k(\ell)^N}{\varphi(\ell^e)^K}\Bigg\{1 + \frac{1}{(\alpha_k(\ell)\varphi(\ell^e))^N}\sum_{(\chi_1,\dots,\chi_K)\neq(\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e}\left(\prod_{i=1}^K \overline{\chi}_i(w_i)\right)(Z_{\ell^e;\,\chi_1,\dots,\chi_K})^N\Bigg\}, \tag{4.28}$$

where we have recalled that $\alpha_k(\ell) \neq 0$ since $\alpha_k(q) \neq 0$. For any tuple $(\chi_1,\dots,\chi_K) \neq (\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e$, let $\ell^{e_0} \coloneqq \operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)] \in \{\ell,\dots,\ell^e\}$. Using $\chi_1,\dots,\chi_K$ to also denote the characters mod ℓ^{e_0} inducing $\chi_1,\dots,\chi_K$ respectively, we see that $Z_{\ell^e;\,\chi_1,\dots,\chi_K} = \ell^{e-e_0}\ Z_{\ell^{e_0};\,\chi_1,\dots,\chi_K}$. Moreover $U_{\ell^{e_0}}$ is cyclic since $\ell > C_0 > 2$. Letting γ denote a generator of $U_{\ell^{e_0}}$, we see that the character group mod ℓ^{e_0} is generated by the character ψ_{e_0} given by $\psi_{e_0}(\gamma) \coloneqq \exp(2\pi i/\varphi(\ell^{e_0}))$. Hence, 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 since at least one of $\chi_1,\dots,\chi_K$ is primitive mod ℓ^{e_0}, we also have

$$(A_1,\dots,A_K) \not\equiv \begin{cases} (0,\dots,0) \pmod{\ell}, & \text{if } e_0 > 1, \\ (0,\dots,0) \pmod{\ell-1}, & \text{if } e_0 = 1. \end{cases} \tag{4.29}$$

We can now write

$$\begin{aligned} Z_{\ell^e;\,\chi_1,\dots,\chi_K} &= \ell^{e-e_0}\ Z_{\ell^{e_0};\,\chi_1,\dots,\chi_K} \\ &= \ell^{e-e_0}\sum_{v \bmod \ell^{e_0}} \psi_{e_0}\left(v^{\varphi(\ell^{e_0})}\prod_{i=1}^K W_{i,k}(v)^{A_i}\right). \end{aligned} \tag{4.30}$$

Case 1: If $e_0 = 1$, then since $\ell > C_0 > B_0$, we have

$$\gcd(\ell - 1, \beta(W_{1,k}, \dots, W_{K,k})) = 1.$$

Further, since $\ell > C_0 > C_1(W_{1,k}, \dots, W_{K,k})$, we see by (4.29) and Proposition 4.4.3(a) that $\prod_{i=1}^{K} W_{i,k}^{A_i}$ cannot be of the form $c \cdot G^{\ell-1}$ in $\mathbb{F}_\ell[T]$. As such, (4.30) and Proposition 4.4.1 show that

$$|Z_{\ell^e;\ \chi_1,\dots,\chi_K}| \le D\ell^{e-1/2} \quad \text{for any tuple } (\chi_1, \dots, \chi_K) \bmod \ell^e \text{ having } e_0 = 1. \tag{4.31}$$

Case 2: If $e_0 \ge 2$, then since $\operatorname{ord}_\ell(\prod_{i=1}^{K} W_{i,k}) = 0$ and $\ell > C_0 > C_1(W_{1,k}, \dots, W_{K,k})$, Proposition 4.4.3 and (4.29) show that

$$\tau(\ell) \coloneqq \operatorname{ord}_\ell((T^{\varphi(\ell^{e_0})} \prod_{i=1}^{K} W_{i,k}(T)^{A_i})') = 0 \le e_0 - 2.$$

Thus (4.30) and Proposition 4.4.2(i) yield

$$|Z_{\ell^e;\ \chi_1,\dots,\chi_K}| \le \left(\sum_{\theta \in \mathcal{A}_\ell} \mu_\theta(\mathcal{C}_\ell) \right) \ell^{e - e_0/(M_\ell+1)},$$

where $\mathcal{A}_\ell \subset \mathbb{F}_\ell$ denotes the set of ℓ-critical points of $T^{\varphi(\ell^{e_0})} \prod_{i=1}^{K} W_{i,k}(T)^{A_i}$, namely the roots of $\mathcal{C}_\ell(T) = (T^{\varphi(\ell^{e_0})} \prod_{i=1}^{K} W_{i,k}(T)^{A_i})'$ in $\mathbb{F}_\ell$ that are not roots of $T^{\varphi(\ell^{e_0})} \prod_{i=1}^{K} W_{i,k}(T)^{A_i}$. But by the last assertion in Proposition 4.4.3, we see that

$$M_\ell \le \sum_{\theta \in \mathcal{A}_\ell} \mu_\theta(\mathcal{C}_\ell) \le \deg(\sum_{i=1}^{K} A_i W_{i,k}' \prod_{\substack{1 \le j \le K \\ j \ne i}} W_{j,k}) \le D - 1.$$

This yields

$$|Z_{\ell^e;\,\chi_1,\ldots,\chi_K}| \le D\ell^{e-e_0/D} \quad \text{for any tuple } (\chi_1,\ldots,\chi_K) \bmod \ell^e \ \text{ having } e_0 > 1. \tag{4.32}$$

Combining the conclusions of Cases 1 and 2, and using the fact that there are at most $\ell^{e_0 K}$ many tuples $(\chi_1,\ldots,\chi_K)$ of characters mod ℓ^e having $\mathrm{lcm}[\mathfrak{f}(\chi_1),\ldots,\mathfrak{f}(\chi_K)] = \ell^{e_0}$, we get

$$\frac{1}{(\alpha_k(\ell)\varphi(\ell^e))^N} \sum_{(\chi_1,\ldots,\chi_K)\neq(\chi_{0,\ell},\ldots,\chi_{0,\ell}) \bmod \ell^e} |Z_{\ell^e;\chi_1,\ldots,\chi_K}|^N \ \le\ (4D)^N \sum_{1\le e_0\le e} \ell^{e_0(K-N/D)}, \tag{4.33}$$

where in the last inequality above, we have used the facts that $D \ge 2$ and $\alpha_k(\ell) \ge 1 - D/(\ell-1) \ge 1 - D/(C_0-1) \ge 1/2$. Now if $N \ge KD+1$, then $\ell^{K-N/D} \le C_0^{-1/D} \le 1/2$, so that the last sum in (4.33) is at most $2(4D)^N \ell^{K-N/D}$. On the other hand, if $N \le KD$, then the same sum is $\ll e^{\mathbb{1}_{N=KD}} \ell^{e(K-N/D)}$. Inserting these two bounds into (4.33) and (4.28) gives (4.27).

Dealing with the small primes dividing q: Now for an arbitrary q, we let $\widetilde{q} := \prod_{\substack{\ell^e \| q \\ \ell \le C_0}} \ell^e$ denote the C_0-smooth part of q. By (4.26),

$$\#\mathcal{V}_{N,K}^{(k)}\left(\widetilde{q};(w_i)_{i=1}^K\right) = \frac{1}{\varphi(\widetilde{q})^K} \sum_{\chi_1,\ldots,\chi_K \bmod \widetilde{q}} \overline{\chi}_1(w_1)\cdots\overline{\chi}_K(w_K)(Z_{\widetilde{q};\chi_1,\ldots,\chi_K})^N. \tag{4.34}$$

Given a constant $C > C_0$, we fix κ to be any **integer** constant exceeding $C \cdot (30DC_0^{C_0})^{2C_0}$. Let $Q_0 := \prod_{\ell^e \| \widetilde{q}} \ell^{\min\{e,\kappa\}} = \prod_{\ell \le C_0} \ell^{\min\{v_\ell(q),\kappa\}}$ denote the largest $(\kappa+1)$-free divisor of $\widetilde{q}$. Write the expression on the right hand side of (4.34) as $\mathcal{S}' + \mathcal{S}''$,

where

$$\mathcal{S}' \coloneqq \frac{1}{\varphi(\widetilde{q})^K} \sum_{\substack{\chi_1,\dots,\chi_K \bmod \widetilde{q} \\ \operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)] \text{ is } (\kappa+1)\text{-free}}} \overline{\chi}_1(w_1)\cdots\overline{\chi}_K(w_K)(Z_{\widetilde{q};\,\chi_1,\dots,\chi_K})^N$$

denotes the contribution of those tuples $(\chi_1,\dots,\chi_K)$ mod $\widetilde{q}$ for which $\operatorname{lcm}[\mathfrak{f}(\chi_1),\ \dots,\ \mathfrak{f}(\chi_K)]$ is $(\kappa+1)$-free, or equivalently, those $(\chi_1,\dots,\chi_K)$ for which $\operatorname{lcm}[\mathfrak{f}(\chi_1),\ \dots,\ \mathfrak{f}(\chi_K)]$ divides Q_0.

For each tuple $(\chi_1,\dots,\chi_K)$ counted in $\mathcal{S}'$, there exists a unique tuple $(\psi_1,\dots,\psi_K)$ of characters mod Q_0 inducing $(\chi_1,\dots,\chi_K)$ mod $\widetilde{q}$, respectively. Noting that $\alpha_k(\widetilde{q}) = \alpha_k(Q_0)$, a straightforward calculation using (4.21) shows that

$$\begin{aligned} Z_{\widetilde{q};\,\chi_1,\dots,\chi_K} &= \sum_{u \bmod Q_0} \chi_{0,Q_0}(u) \prod_{i=1}^{K} \psi_i(W_{i,k}(u)) \sum_{\substack{v \bmod \widetilde{q} \\ v\equiv u \bmod Q_0 \\ \gcd(v\prod_{i=1}^K W_{i,k}(v),\widetilde{q})=1}} 1 \\ &= \frac{\varphi(\widetilde{q})}{\varphi(Q_0)}\, Z_{Q_0;\ \psi_1,\dots,\psi_K} \end{aligned}$$

Using this and invoking (4.26) with $Q \coloneqq Q_0$, we obtain

$$\begin{aligned} \frac{\mathcal{S}'}{\varphi(\widetilde{q})^N} &= \frac{\varphi(\widetilde{q})^{-K}}{\varphi(Q_0)^N} \sum_{\psi_1,\dots,\psi_K \bmod Q_0} \left(\prod_{i=1}^{K} \overline{\psi}_i(w_i)\right) (Z_{Q_0;\,\psi_1,\dots,\psi_K})^N \\ &= \left(\frac{\varphi(Q_0)}{\varphi(\widetilde{q})}\right)^K \frac{\#\mathcal{V}_{N,K}^{(k)}\left(Q_0;(w_i)_{i=1}^K\right)}{\varphi(Q_0)^N} \end{aligned} \tag{4.35}$$

We now deal with the remaining sum $\mathcal{S}''$ which is the contribution of those $(\chi_1,\dots,\chi_K)$ mod $\widetilde{q}$ for which $\operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)]$ is not $(\kappa+1)$-free. For each such $(\chi_1,\dots,\chi_K)$, we factor $\chi_i =: \prod_{\ell^e \| \widetilde{q}} \chi_{i,\ell}$, where $\chi_{i,\ell}$ is a character mod ℓ^e. Defining e_ℓ to be $v_\ell\left(\operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)]\right)$, we observe that since $\mathfrak{f}(\chi_i) = \prod_{\ell^e \| q} \mathfrak{f}(\chi_{i,\ell})$ and each $\mathfrak{f}(\chi_{i,\ell})$ is a power of ℓ, we must have $\operatorname{lcm}[\mathfrak{f}(\chi_{1,\ell}),\ \dots,\ \mathfrak{f}(\chi_{K,\ell})] = \ell^{e_\ell}$. For each $\ell^e \parallel \widetilde{q}$, let

$(\chi_{1,\ell},\dots,\chi_{K,\ell})$ also denote the characters mod ℓ^{e_ℓ} inducing $(\chi_{1,\ell},\dots,\chi_{K,\ell})$ mod ℓ^e respectively. Then at least one of $\chi_{1,\ell},\dots,\chi_{K,\ell}$ must be primitive mod ℓ^{e_ℓ}. The factorization $Z_{\widetilde{q};\,\chi_1,\dots,\chi_K} = \prod_{\ell^e \| \widetilde{q}} Z_{\ell^e;\,\chi_{1,\ell},\dots,\chi_{K,\ell}}$ now yields

$$|Z_{\widetilde{q};\,\chi_1,\dots,\chi_K}| \le \left(\prod_{\substack{\ell^e \| \widetilde{q} \\ e_\ell \le \kappa}} \varphi(\ell^e) \right) \prod_{\substack{\ell^e \| \widetilde{q} \\ e_\ell \ge \kappa+1}} \left(\ell^{e-e_\ell} |Z_{\ell^{e_\ell};\,\chi_{1,\ell},\dots,\chi_{K,\ell}}| \right). \tag{4.36}$$

We claim that for all prime powers $\ell^e \parallel \widetilde{q}$ with $e_\ell \ge \kappa+1$, we have

$$|Z_{\ell^{e_\ell};\,\chi_{1,\ell},\dots,\chi_{K,\ell}}| \le (DC_0^{C_0})\ \ell^{e_\ell(1-1/D)}. \tag{4.37}$$

For odd ℓ, this follows essentially by the same argument as that given to bound $Z_{\ell^e;\,\chi_1,\dots,\chi_K}$ in "Case 2" before: The only difference is that this time we use *both* the assertions in (4.22) since $e_\ell \ge \kappa+1 > (30DC_0)^{2C_0}+1 > C_0+2$. Now assume that $\ell = 2$, i.e. $e_2 = v_2(\mathrm{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_K)]) \ge \kappa+1 \ge 31$. We shall use Proposition 4.4.2(ii).

To do this, we observe that the characters ψ, η mod 2^{e_2} defined by

$$\psi(5) \coloneqq \exp(2\pi i/2^{e_2-2}),\ \psi(-1) \coloneqq 1 \quad \text{and} \quad \eta(5) \coloneqq 1, \eta(-1) \coloneqq -1$$

generate the character group mod 2^{e_2}. Hence for each $i \in [K]$, there exist $r_i \in [2^{e_2-2}]$ and $s_i \in [2]$ satisfying $\chi_{i,2} = \psi^{r_i}\eta^{s_i}$; also $2 \nmid \gcd(r_1,\dots,r_K)$ as $e_2 \ge 4$ and at least one of $\chi_{1,2},\dots,\chi_{K,2}$ is primitive mod 2^{e_2}. Thus $Z_{2^{e_2}} = \sum_{v \bmod 2^{e_2}} \psi\left(g(v)\right)\ \eta\left(v^2 \prod_{i=1}^K W_{i,k}(v)^{s_i}\right)$, where $g(T) \coloneqq \prod_{i=1}^K W_{i,k}(T)^{r_i}$ and we have abbreviated $Z_{2^{e_2};\,\chi_{1,2},\dots,\chi_{K,2}}$ to $Z_{2^{e_2}}$. Since η is induced by the nontrivial character mod 4, writing $v \coloneqq 4u+\lambda$ and $h_\lambda(T) \coloneqq$

$g(4T+\lambda)$ gives

$$\begin{aligned} Z_{2^{e_2}} &= \sum_{\lambda=\pm 1} \eta\left(\prod_{i=1}^{K} W_{i,k}(\lambda)^{s_i}\right) \sum_{u \bmod 2^{e_2-2}} \psi\left(h_\lambda(u)\right) \\ &= \frac{1}{4}\sum_{\lambda=\pm 1} \eta\left(\prod_{i=1}^{K} W_{i,k}(\lambda)^{s_i}\right) \sum_{u \bmod 2^{e_2}} \psi\left(h_\lambda(u)\right) \end{aligned} \tag{4.38}$$

If $\eta\left(\prod_{i=1}^{K} W_{i,k}(\lambda)^{s_i}\right) \neq 0$, then $\prod_{i=1}^{K} W_{i,k}(\lambda)^{s_i} \equiv 1 \pmod 2$, so

$$\operatorname{ord}_2\left(\prod_{i=1}^{K} W_{i,k}(4T+\lambda)^{r_i-1}\right) = 0.$$

As such, with $\widetilde{G} \coloneqq \sum_{i=1}^{K} r_i W_{i,k}' \prod_{j\neq i} W_{j,k}$, we see that

$$\tau_\lambda(2) \coloneqq \operatorname{ord}_2(h_\lambda'(T)) = 2 + \operatorname{ord}_2(\widetilde{G}(4T+\lambda)) \leq 2 + \operatorname{ord}_2(\widetilde{G}) + 2\deg(\widetilde{G}) \leq C_0 + 2D; \tag{4.39}$$

here we have used (4.22) and the fact that $\operatorname{ord}_2(F(4T+\lambda)) \leq \operatorname{ord}_2(F) + 2\deg(F)$ for any nonconstant polynomial F. [5]

Two consequences of (4.39) are that $2^{-(\tau_\lambda(2)-2)}\widetilde{G}(4T+\lambda) \in \mathbb{Z}[T]$ and that $\tau_\lambda(2) \leq \kappa - 3 \leq e_2 - 3$. Thus Proposition 4.4.2(ii) applies, yielding

$$\left|\sum_{u \bmod 2^{e_2}} \psi\left(h_\lambda(u)\right)\right| \leq (12.5)\cdot 2^{C_0+2D}\cdot 2^{e_2(1-1/(M_\lambda+1))},$$

where M_λ is the maximum multiplicity of a 2-critical point of h_λ.

Since $\prod_{i=1}^{K} W_{i,k}(4T+\lambda)^{r_i-1} \equiv 1 \pmod 2$, it follows that any such critical point $\theta \in \mathbb{F}_2$ is a root of the polynomial $2^{-(\tau_\lambda(2)-2)}\widetilde{G}(4T+\lambda)$, giving $M_\lambda \leq \deg \widetilde{G}(4T+\lambda) \leq D-1$,

[5] This can be seen by writing the coefficients of $F(4T+\lambda)$ in terms of those of F, and using a simple divisibility argument.

so that

$$\left| \sum_{u \bmod 2^{e_2}} \psi\left(h_\lambda(u)\right) \right| \leq (12.5) \cdot 2^{C_0+2D} \cdot 2^{e_2(1-1/D)} \leq D C_0^{C_0} \cdot 2^{e_2(1-1/D)}.$$

Inserting this into (4.38) completes the proof of (4.37) in the remaining case $\ell = 2$.

Combining (4.36) with (4.37), we find that for each $(\chi_1, \dots, \chi_K)$ counted in $\mathcal{S}''$, we have

$$|Z_{\widetilde{q};\chi_1,\dots,\chi_K}| \leq (2D_0 C_0^{C_0})^{C_0} \varphi(\widetilde{q}) A^{-1/D_0},$$

where $A := \prod_{\ell^e \| \widetilde{q}:\ e_\ell \geq \kappa+1} \ell^{e_\ell}$ denotes the $(\kappa+1)$-full part of $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)]$, i.e, the largest $(\kappa+1)$-full divisor of $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)]$. Now for a divisor d of $\widetilde{q}$, there are at most d^K many tuples $(\chi_1, \dots, \chi_K)$ of characters mod $\widetilde{q}$ for which $\mathrm{lcm}[\mathfrak{f}(\chi_1), \dots, \mathfrak{f}(\chi_K)] = d$. Hence, summing this last bound over all possible $(\chi_1, \dots, \chi_K)$ occurring in the sum $\mathcal{S}''$, we obtain

$$\begin{aligned} |\mathcal{S}''| &\leq \frac{1}{\varphi(\widetilde{q})^K} \sum_{\substack{A \mid \widetilde{q}:\ A>1 \\ A \text{ is } (\kappa+1)\text{-full}}} \sum_{\substack{d \mid \widetilde{q} \\ (\kappa+1)\text{-full part} \\ \text{of } d \text{ is } A}} d^K \cdot \frac{(2D_0 C_0^{C_0})^{C_0 N} \varphi(\widetilde{q})^N}{A^{N/D}} \\ &\ll \frac{\varphi(\widetilde{q})^N}{\varphi(\widetilde{q})^K} \cdot (2D_0 C_0^{C_0})^{C_0 N} \sum_{\substack{A \mid \widetilde{q}:\ A>1 \\ A \text{ is } (\kappa+1)\text{-full}}} \frac{1}{A^{N/D-K}}. \end{aligned}$$

In the last step above, we have noted that for any d dividing $\widetilde{q}$ whose $(\kappa+1)$-full part is A, we have $d \ll A$. Continuing,

$$\frac{|\mathcal{S}''|}{\varphi(\widetilde{q})^N} \ll \frac{(2D_0 C_0^{C_0})^{C_0 N}}{\varphi(\widetilde{q})^K} \left\{ \prod_{\ell^e \| \widetilde{q}} \left(1 + \sum_{\kappa+1 \leq \nu \leq e} \frac{1}{\ell^{\nu(N/D-K)}} \right) - 1 \right\}. \tag{4.40}$$

Now if $N \geq KD+1$, then since $\kappa > C \cdot (30 D C_0^{C_0})^{2C_0} \geq D(D+3)$, we see that the sum on ν above is at most $2^{-\kappa(N/D-K)} \left(1 - 2^{-1/D}\right)^{-1} \leq \frac{2^{D+2}}{2^{\kappa/D}} \leq \frac{1}{2}$. Hence $\log(1 +$

$\sum_{\kappa+1\le\nu\le e}\ell^{-\nu(N/D-K)}) \ll 2^{-\kappa(N/D-K)} \ll 2^{-\kappa N/D}$. In addition, since $P(\widetilde{q}) \le C_0$, equation (4.40) gives

$$\begin{aligned}\frac{|\mathcal{S}''|}{\varphi(\widetilde{q})^N} &\ll \frac{(2D_0C_0^{C_0})^{C_0N}}{\varphi(\widetilde{q})^K}\left\{\exp\left(O\left(\frac{1}{2^{\kappa N/D}}\right)\right)-1\right\}\\ &\ll \frac{1}{\varphi(\widetilde{q})^K}\cdot\left(\frac{(2D_0C_0^{C_0})^{C_0}}{2^{\kappa/D}}\right)^N \ll \frac{C^{-N}}{\varphi(\widetilde{q})^K},\end{aligned} \tag{4.41}$$

where in the last step, we have recalled that $\kappa/D > D^{-1}\cdot C\cdot(30DC_0^{C_0})^{2C_0} > C\cdot(2C_1)^{C_0}$. Combining (4.41) with (4.35), we deduce that

$$\frac{\#\mathcal{V}_{N,K}^{(k)}\left(\widetilde{q};(w_i)_{i=1}^K\right)}{\varphi(\widetilde{q})^N} = \frac{\mathcal{S}'+\mathcal{S}''}{\varphi(\widetilde{q})^N} \tag{4.42}$$

$$= \left(\frac{\varphi(Q_0)}{\varphi(\widetilde{q})}\right)^K\left\{\frac{\#\mathcal{V}_{N,K}^{(k)}\left(Q_0;(w_i)_{i=1}^K\right)}{\varphi(Q_0)^N}+O\left(\frac{1}{C^N}\right)\right\}, \tag{4.43}$$

uniformly for $N \ge KD+1$ and in coprime residues $w_1,\dots,w_K$ to any modulus q.

On the other hand, for each $N \in [KD]$, we have $1+\sum_{\kappa+1\le\nu\le e}\ell^{-\nu(N/D-K)} \ll e^{\mathbb{1}_{N=KD}}\ \ell^{e(K-N/D)}$, which from (4.40), yields $|\mathcal{S}''|/\varphi(\widetilde{q})^N \ll \left(\prod_{\ell^e\|\widetilde{q}}\ e\right)^{\mathbb{1}_{N=KD}}\Big/\widetilde{q}^{N/D}$. Combining this with the trivial bound $|\mathcal{S}'|/\varphi(\widetilde{q})^N \ll \varphi(\widetilde{q})^{-K} \ll \widetilde{q}^{-K} \ll \widetilde{q}^{-N/D}$ coming from (4.35), we find that for each $N \in [KD]$, we have

$$\frac{\#\mathcal{V}_{N,K}^{(k)}\left(\widetilde{q};(w_i)_{i=1}^K\right)}{\varphi(\widetilde{q})^N} \ll \frac{\left(\prod_{\ell^e\|\widetilde{q}}\ e\right)^{\mathbb{1}_{N=KD}}}{\widetilde{q}^{N/D}}, \quad \text{uniformly in } q \text{ and } (w_i)_{i=1}^K \in U_q^K. \tag{4.44}$$

Proposition 4.3.4 now follows in the case $D > 1$ by combining (4.27) with (4.42) (for $N > KD$) or (4.44) (for $N \le KD$), and then noting that $\prod_{\ell|q:\ \ell>C_0}\alpha_k(\ell) = \alpha_k(q)/\alpha_k(Q_0)$.

Now assume that $D = 1$, so that $K = 1$ and $W_{1,k}(T) \coloneqq RT+S$ for some integers R and S with $R \ne 0$. We first make the following general observation, which is

immediate from Proposition 4.4.2: For any primitive character $\chi \bmod \ell^b$, the sum $Z_{\ell^b;\chi} \coloneqq \sum_{v \bmod \ell^b} \chi_{0,\ell}(v)\chi(Rv+S) = \sum_{v \bmod \ell^b} \chi(v^{\varphi(\ell^b)}(Rv+S))$ is zero for any odd prime ℓ and any integer $b \geq v_\ell(R)+2$, as well as for $\ell = 2$ and any $b \geq v_2(R)+3$. Indeed in both these cases, the polynomial $F(T) = T^{\varphi(\ell^b)}(RT+S)$ has no ℓ-critical point, since $\mathrm{ord}_\ell(F') = v_\ell(R)$ which forces $\ell^{-\mathrm{ord}_\ell(F')}F'(T) = (\ell^{-v_\ell(R)}R)T^{\varphi(\ell^b)}$ in $\mathbb{F}_\ell[T]$.

By this observation, it follows that uniformly in $N \geq 1$ and in $\ell^e \parallel q$ with $\ell > C_0$ $(> |R|)$, we have

$$\frac{\#\mathcal{V}_{N,1}^{(k)}(\ell^e;w)}{\varphi(\ell^e)^N} = \frac{\alpha_k(\ell)^N}{\varphi(\ell^e)}\left(1 + O\left(\left(\frac{2}{\ell-1}\right)^{N-1}\right)\right). \tag{4.45}$$

Indeed, we simply invoke (4.28) and note that if $\mathfrak{f}(\chi) = \ell^{e_0}$ for some $e_0 \geq 2 = v_\ell(R)+2$, then $Z_{\ell^e;\chi} = 0$ as seen above. On the other hand, if $\mathfrak{f}(\chi) = \ell$ (and there are $\ell-2$ many such characters mod ℓ^e), then

$$|Z_{\ell^e;\chi}| = \ell^{e-1}\left|\sum_{v \bmod \ell} \chi(Rv+S) - \chi(S)\right| = \ell^{e-1}\left|\sum_{u \bmod \ell} \chi(u) - \chi(S)\right| \leq \ell^{e-1}.$$

Letting $\widetilde{q} \coloneqq \prod_{\substack{\ell^e \parallel q \\ \ell \leq C_0}} \ell^e$ as before, we fix an integer $\kappa > C_0+3$, and write $\#\mathcal{V}_{N,1}^{(k)}(\widetilde{q};w) = \varphi(\widetilde{q})^{-1}\sum_{\chi \bmod \widetilde{q}} \overline{\chi}(w)(Z_{\widetilde{q};\chi})^N = \mathcal{S}' + \mathcal{S}''$, where $\mathcal{S}'$ again denotes the contribution of those $\chi \bmod \widetilde{q}$ for which $\mathfrak{f}(\chi)$ is $(\kappa+1)$-free. Then (4.35) continues to hold, and $\mathcal{S}'' = 0$ by the general observation above. This yields

$$\frac{\#\mathcal{V}_{N,1}^{(k)}(\widetilde{q};w)}{\varphi(\widetilde{q})^N} = \frac{\varphi(Q_0)}{\varphi(\widetilde{q})} \cdot \frac{\#\mathcal{V}_{N,1}^{(k)}(Q_0;w)}{\varphi(Q_0)^N},$$

which combined with (4.45), proves Proposition 4.3.4 in the final case $D = 1$. □

With Proposition 4.3.4 established, the proof of Proposition 4.3.3 is now complete.

We will eventually also need the following variant of Proposition 4.3.4, which follows from an argument that is a much simpler version of that given for (4.27).

Corollary 4.4.4. *Assume that $\{W_{i,k}\}_{1\le i\le K}$ are multiplicatively independent. Then*

$$\frac{\#\mathcal{V}_{N,K}^{(k)}\left(q;(w_i)_{i=1}^K\right)}{\varphi(q)^N} \ll \begin{cases} \varphi(q)^{-K}\exp\Big(O(\sqrt{\log q})\Big), & \text{for each fixed } N\ge 2K+1 \\ q^{-N/2}\exp\big(O(\omega(q))\big), & \text{for each fixed } N\le 2K, \end{cases} \tag{4.46}$$

uniformly in coprime residues $w_1,\dots,w_K$ modulo squarefree q satisfying $\alpha_k(q)\neq 0$ and hypothesis $IFH(W_{1,k},\dots,W_{K,k};B_0)$.

Towards Theorem 4.3.2

To deduce Theorem 4.3.2 from Proposition 4.3.3, we apply the orthogonality of Dirichlet characters to see that the main term in the right hand side of (4.13) is equal to

$$\begin{aligned}\left(\frac{\varphi(Q_0)}{\varphi(q)}\right)^K \sum_{\substack{n\le x:\ (f(n),q)=1\\ (\forall i)\ f_i(n)\equiv a_i \pmod{Q_0}}} 1 &= \frac{1}{\varphi(q)^K}\sum_{\substack{n\le x\\ (f(n),q)=1}} 1 \\ &+ \frac{1}{\varphi(q)^K}\sum_{(\chi_1,\dots,\chi_K)\neq(\chi_{0,Q_0},\dots,\chi_{0,Q_0}) \bmod Q_0}\left(\prod_{i=1}^K \overline{\chi}_i(a_i)\right) \\ &\qquad\cdot\sum_{n\le x}\mathbb{1}_{(f(n),q)=1}\prod_{i=1}^K\chi_i(f_i(n)).\end{aligned}$$

Henceforth, let $Q := \prod_{\ell\mid q}\ell$ denote the radical of q. To obtain Theorem 4.3.2, it remains to prove that each $\sum_{n\le x}\mathbb{1}_{(f(n),q)=1}\prod_{i=1}^K\chi_i(f_i(n)) = o\Big(\sum_{\substack{n\le x\\(f(n),q)=1}}1\Big)$. For $Q\ll 1$, this follows by applying Theorem 1.3.11 to the divisor $Q^*:=\operatorname{lcm}[Q,Q_0]\ll 1$ of q. (Note that as q lies in $\mathcal{Q}(k;f_1,\cdots,f_K)$, so does Q^*, since q and Q^* have the same

prime factors.) So we may assume that Q is sufficiently large. Theorem 4.3.2 would follow once we show the result below. Here λ and Q_0 are as in Proposition 4.3.3.

Theorem 4.4.5. *There exists a constant $\delta_0 := \delta_0(\lambda) > 0$ such that, uniformly in moduli $q \leq (\log x)^{K_0}$ lying in $\mathcal{Q}(k; f_1, \cdots, f_K)$ and having sufficiently large radical, we have*

$$\sum_{n \leq x} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),q)=1} \ll \frac{x^{1/k}}{(\log x)^{1-(1-\delta_0)\alpha_k(Q)}}$$

for all tuples of characters $(\chi_1, \ldots, \chi_K) \neq (\chi_{0,Q_0}, \ldots, \chi_{0,Q_0}) \bmod Q_0$.

Let $\mathcal{C}_k(Q_0)$ denote the set of tuples of characters $(\psi_1, \ldots, \psi_K) \bmod Q_0$, not all trivial, such that $\prod_{i=1}^{K} \psi_i(W_{i,k}(u))$ is constant on its support, which is precisely the set $R_k(Q_0) = \{u \in U_{Q_0} : W_k(u) \in U_{Q_0}\}$. To prove Theorem 4.4.5, we separately consider the two cases when a tuple of characters mod Q_0 lies in $\mathcal{C}_k(Q_0)$ or not.

Section 4.5

Proof of Theorem 4.4.5 for nontrivial tuples of characters not in $\mathcal{C}_k(Q_0)$

For any integer $d \geq 1$ and any nontrivial tuple $(\psi_1, \ldots, \psi_K)$ of characters mod d not lying in $\mathcal{C}_k(d)$, we have

$$\left| \sum_{u \bmod d} \chi_{0,d}(u) \psi_1(W_{1,k}(u)) \cdots \psi_K(W_{K,k}(u)) \right| < \alpha_k(d)\varphi(d).$$

With λ as in Proposition 4.3.3, we define the constant $\delta_1 := \delta_1(W_{1,k}, \ldots, W_{K,k}; B_0) \in (0, 1)$ to be

$$\max_{\substack{d\le\lambda\\ \alpha_k(d)\neq 0}} \max_{\substack{(\psi_1,\dots,\psi_K)\neq(\chi_{0,d},\dots,\chi_{0,d}) \bmod d\\ (\psi_1,\dots,\psi_K)\ \notin\ \mathcal{C}_k(d)}} \frac{1}{\alpha_k(d)\varphi(d)}\left|\sum_{u \bmod d} \chi_{0,d}(u)\psi_1(W_{1,k}(u))\cdots\psi_K(W_{K,k}(u))\right|.$$

Then since $Q_0 \le \lambda$, we have for any nontrivial tuple $(\chi_1,\dots,\chi_K) \notin \mathcal{C}_k(Q_0)$,

$$\left|\sum_{u \bmod Q_0} \chi_{0,Q_0}(u)\chi_1(W_{1,k}(u))\cdots\chi_K(W_{K,k}(u))\right| \le \delta_1\alpha_k(Q_0)\varphi(Q_0). \tag{4.47}$$

We set $\delta := (1-\delta_1)/2$ and $Y := \exp((\log x)^{\delta/3})$. To establish Theorem 4.4.5 for all $(\chi_1,\dots,\chi_K) \notin \mathcal{C}_k(Q_0)$, it suffices to show that

$$\sum_{\substack{n\le x\\ p>Y \implies p^{k+1}\nmid n}} \chi_1(f_1(n))\cdots\chi_K(f_K(n))\ \mathbb{1}_{(f(n),q)=1} \ll \frac{x^{1/k}}{(\log x)^{1-(\delta_1+\delta)\alpha_k}}. \tag{4.48}$$

This is because by the arguments before (4.5), the contribution of the n's not counted above is negligible. Writing any n counted in (4.48) uniquely as BMA^k (as done before (4.6)), we see that the sum in (4.48) equals

$$\sum_{\substack{B\le x\\ P(B)\le Y\\ B \text{ is } k\text{-free}}} \mathbb{1}_{(f(B),q)=1}\left(\prod_{i=1}^{K}\chi_i(f_i(B))\right) \sum_{\substack{M\le x/B\\ M \text{ is } k\text{-full}\\ P(M)\le Y}} \mathbb{1}_{(f(M),q)=1}\left(\prod_{i=1}^{K}\chi_i(f_i(M))\right)$$
$$\sum_{A\le (x/BM)^{1/k}} \mathbb{1}_{P^-(A)>Y}\ \mathbb{1}_{(f(A^k),q)=1}\ \mu(A)^2\prod_{i=1}^{K}\chi_i(f_i(A^k)) \tag{4.49}$$

Moreover, the arguments leading to the bound for Σ_2 towards the end of section 4.2 show that the tuples (B,M,A) having $M > x^{1/2}$ give negligible contribution to the above sum. To prove (4.48), it thus only remains to bound the contribution of tuples (B,M,A) with $M \le x^{1/2}$ to the triple sum in (4.49). To deal with such tuples, we

will establish the following general upper bound uniformly for $X \geq \exp((\log Y)^2)$:

$$\sum_{A \leq X} \mathbb{1}_{P^-(A)>Y}\ \mathbb{1}_{(f(A^k),q)=1}\ \mu(A)^2 \prod_{i=1}^{K} \chi_i(f_i(A^k)) \ll \frac{X}{(\log X)^{1-\alpha_k(\delta_1+\delta/2)}}. \tag{4.50}$$

We apply a quantitative version of Halász's Theorem [76, Corollary III.4.12] on the multiplicative function

$$F(A) \coloneqq \mathbb{1}_{P^-(A)>Y}\ \mathbb{1}_{(f(A^k),q)=1}\ \mu(A)^2 \prod_{i=1}^{K} \chi_i(f_i(A^k)),$$

taking $T \coloneqq \log X$. This requires us to put, for each $t \in [-T, T]$, a lower bound on the sum below (which is the square of a certain "pretentious distance"):

$$\begin{aligned}
&\mathcal{D}(X;t) \\
&\coloneqq \sum_{p \leq X} \frac{1}{p} \left(1 - \operatorname{Re}\left(\mathbb{1}_{p>Y}\ \mathbb{1}_{(f(p^k),q)=1}\ \mu(p)^2\ p^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(f_i(p^k))\right)\right) \\
&= (1-\alpha_k)\log_2 X + \alpha_k \log_2 Y \qquad (4.51) \\
&\quad + \sum_{\substack{Y < p \leq X \\ (W_k(p),q)=1}} \frac{1}{p} \left(1 - \operatorname{Re}\left(p^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(p))\right)\right) + O\big((\log_2(3q))^{O(1)}\big);
\end{aligned}$$

here to get the second line from the first, we use Lemma 2.2.4.

To get a lower bound on $\mathcal{D}(X;t)$, we proceed analogously to the proof of [60, Lemma 3.3]. The key idea is to split the range of the last sum above into blocks of small multiplicative width, so that the complex number $p^{-\mathrm{i}t}$ is essentially constant for all p lying in a given block. More precisely, we cover the interval $(Y, X]$ with finitely many disjoint intervals $\mathcal{I} \coloneqq \big(\eta, \eta(1 + 1/\log^2 X)\big]$ for certain choices of $\eta \in (Y, X]$, choosing the smallest η to be Y and allowing the rightmost endpoint of such an interval to jut

out slightly past X but no more than $X(1 + 1/\log^2 X)$. Then the last sum in (4.51) equals

$$\sum_{\mathcal{I}} \sum_{\substack{p \in \mathcal{I} \\ (W_k(p),q)=1}} \frac{1}{p} \left(1 - \mathrm{Re}\left(p^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(p))\right)\right) + O\left(\frac{1}{\log^3 X}\right) \tag{4.52}$$

Consider any $\mathcal{I}$ occurring in the sum above. For each $p \in \mathcal{I}$, we have

$$|p^{-\mathrm{i}t} - \eta^{-\mathrm{i}t}| \leq \left| \int_{t \log \eta}^{t \log p} \exp(-i\varrho)\, d\varrho \right| \leq |t \log p - t \log \eta| \leq \frac{|t|}{\log^2 X} \leq \frac{1}{\log X}.$$

This shows that uniformly in $\mathcal{I}$, the inner sum in (4.52) is equal to

$$\begin{aligned} \sum_{\substack{p \in \mathcal{I} \\ (W_k(p),q)=1}} & \frac{1}{p} \left(1 - \mathrm{Re}\left(p^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(p))\right)\right) \\ &= \sum_{\substack{u \in U_q \\ (W_k(u),q)=1}} \left(1 - \mathrm{Re}\left(\eta^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(u))\right)\right) \sum_{\substack{p \in \mathcal{I} \\ p \equiv u \pmod q}} \frac{1}{p} \\ &\qquad + O\left(\frac{1}{\log X} \sum_{p \in \mathcal{I}} \frac{1}{p}\right) \end{aligned} \tag{4.53}$$

Note that $p = (1 + o(1))\eta$ for all $p \in \mathcal{I}$. (Here and in what follows, the asymptotic notation refers to the behavior as $x \to \infty$, and is uniform in the choice of $\mathcal{I}$.) For parameters Z, W depending on X, we write $Z \gtrsim W$ to mean $Z \geq (1 + o(1))W$. By the Siegel Walfisz Theorem,

$$\sum_{\substack{p \in \mathcal{I} \\ p \equiv u \pmod q}} \frac{1}{p} \gtrsim \frac{1}{\eta} \sum_{\substack{p \in \mathcal{I} \\ p \equiv u \pmod q}} 1 \gtrsim \frac{1}{\varphi(q)} \cdot \frac{1}{\eta} \sum_{p \in \mathcal{I}} 1 \gtrsim \frac{1}{\varphi(q)} \sum_{p \in \mathcal{I}} \frac{1}{p}.$$

Hence the whole main term on the right hand side of (4.53) is

$$\gtrsim \frac{1}{\varphi(q)} \sum_{p\in\mathcal{I}} \frac{1}{p} \sum_{\substack{u\in U_q \\ (W_k(u),q)=1}} \left(1 - \mathrm{Re}\left(\eta^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(u))\right)\right) \tag{4.54}$$

$$\gtrsim (\alpha_k - \alpha_k\delta_1) \left(\sum_{p\in\mathcal{I}} \frac{1}{p}\right), \tag{4.55}$$

where in the last step above, we have used (4.21) and (4.47) to see that

$$\frac{1}{\varphi(q)} \left| \sum_{\substack{u\in U_q \\ (W_k(u),q)=1}} \prod_{i=1}^{K} \chi_i(W_{i,k}(u)) \right| = \frac{\alpha_k(q)}{\alpha_k(Q_0)\varphi(Q_0)} \left| \sum_{r \bmod Q_0} \chi_{0,Q_0}(r) \prod_{i=1}^{K} \chi_i(W_{i,k}(r)) \right| \leq \alpha_k\delta_1.$$

Inserting the bound obtained in (4.54) into (4.53), we find that each inner sum in (4.52) is

$$\sum_{\substack{p\in\mathcal{I} \\ (W_k(p),q)=1}} \frac{1}{p} \left(1 - \mathrm{Re}\left(p^{-\mathrm{i}t} \prod_{i=1}^{K} \chi_i(W_{i,k}(p))\right)\right) \gtrsim \alpha_k(1-\delta_1) \sum_{p\in\mathcal{I}} \frac{1}{p} + O\left(\frac{1}{\log X} \sum_{p\in\mathcal{I}} \frac{1}{p}\right).$$

The O-term above when summed over all $\mathcal{I}$ is $\ll (\log X)^{-1} \sum_{p\leq 2X} p^{-1} \ll \log_2 X/\log X$. Thus, the whole main term in (4.52) is at least

$$\alpha_k \left(1 - \delta_1 - \frac{\delta}{2}\right) (\log_2 X - \log_2 Y).$$

Using this fact along with (4.51) yields

$$\mathcal{D}(X;t) \geq \left(1 - \alpha_k \left(\delta_1 + \frac{\delta}{2}\right)\right) \log_2 X + \alpha_k \left(\delta_1 + \frac{\delta}{2}\right) \log_2 Y + O\big((\log_2(3q))^{O(1)}\big),$$

uniformly for $t \in [-T, T]$. As such, [76, Corollary III.4.12] establishes the claimed bound (4.50).

Now for each $M \leq x^{1/2}$, we have $(x/BM)^{1/k} \gg x^{1/2k}$. Applying (4.50) to each of the innermost sums in (4.49), we see that the total contribution of all tuples (B, M, A) with $M \leq x^{1/2}$ to the triple sum in (4.49) is

$$\ll \sum_{B \ll 1} \sum_{\substack{M \leq x^{1/2}:\ M \text{ is } k\text{-full} \\ P(M) \leq Y,\ (f(M), q)=1}} \frac{(x/BM)^{1/k}}{(\log x)^{1-\alpha_k(\delta_1+\delta/2)}} \ll \frac{x^{1/k}}{(\log x)^{1-\alpha_k(\delta_1+\delta)}};$$

here we have bounded the sum on M using (4.7) (with "Y" playing the role of "y") and Lemma 2.2.4. This proves (4.48), and hence also Theorem 4.4.5 for all nontrivial tuples of characters $(\chi_1, \dots, \chi_K)$ mod Q_0 not in $\mathcal{C}_k(Q_0)$. □

Section 4.6

Proof of Theorem 4.4.5 for tuples of characters in $\mathcal{C}_k(Q_0)$

It suffices to consider the case when x is an integer, and we will do so in the rest of the section. Our argument consists of suitably modifying the Landau–Selberg–Delange method for mean values of multiplicative functions (see for instance [76, Chapter II.5]), and to study the behavior of a product of L-functions raised to complex powers by accounting for the presence of Siegel zeros modulo q. This is partly inspired from work of Scourfield [69] and will also need some results from her paper. We will denote complex numbers in the standard notation $s = \sigma + it$.[6]

[6]The parameters σ and σ_k (to be defined later) in this section have nothing to do with the divisor functions $\sigma_r(n) = \sum_{d|n} d^r$ mentioned in the introduction. We are not working with the divisor functions in this section.

Recall that $Q = \prod_{\ell|q} \ell$; since q is k-admissible, so is Q. Consider any $\widehat{\chi} \coloneqq (\chi_1, \dots, \chi_K) \in \mathcal{C}_k(Q_0)$, so that the product $\prod_{i=1}^K \chi_i(W_{i,k}(u))$ is constant on $R_k(Q_0)$; let $c_{\widehat{\chi}}$ denote this constant value. Consider the Dirichlet series

$$F_\chi(s) \coloneqq \sum_{n\geq 1} \frac{\mathbb{1}_{(f(n),q)=1}}{n^s} \prod_{i=1}^K \chi_i(f_i(n)) = \sum_{n\geq 1} \frac{\mathbb{1}_{(f(n),Q)=1}}{n^s} \prod_{i=1}^K \chi_i(f_i(n))$$

which is absolutely convergent in the half-plane $\sigma > 1$.

In the rest of this section, we fix μ_0 satisfying $\max\{0.7, k/(k+1)\} < \mu_0 < 1$.

4.6.1. Analysis of the Dirichlet series.

We start by giving a meromorphic continuation of $F_\chi(s)$ to a larger region. To do this, set $\mathcal{L}_Q(t) \coloneqq \log(Q(|tk|+1))$ and recall that there exists an absolute constant $c_1 > 0$ such that the product $\prod_{\psi \bmod Q} L(s,\psi)$ has at most one zero β_e (counted with multiplicity) in the region $\sigma > 1 - c_1/\log(Q(|t|+1))$, which is necessarily real and simple; β_e is called the "Siegel zero". If β_e exists, then it is a root of $L(s,\psi_e)$ for some real character $\psi_e \bmod Q$, which we will be referring to as the "exceptional character". By reducing the constant c_1 if necessary, we may assume that $c_1 < 1 - \mu_0$, and that the conductor of ψ_e (which is squarefree) is large enough that it is not $(D+2)$-smooth.

Let $\mathcal{D}_k(c_0)$ denote the region

$$\left\{\sigma + it : \sigma > \frac{1}{k}\left(1 - \frac{c_1}{\mathcal{L}_Q(t)}\right)\right\}.$$

Then $\prod_{\psi \bmod Q} L(sk,\psi)$ has at most one zero and exactly one pole in the region $\mathcal{D}_k(c_0)$, namely β_e/k and $1/k$, respectively.

Branch cuts and complex logarithms: In the rest of the section, we assume that

the complex plane has been cut along the line $\sigma \le 1/k$ if $\alpha_k(Q)$ and $c_{\widehat{\chi}}$ are not both 1, whereas if $\alpha_k(Q) = c_{\widehat{\chi}} = 1$, then the complex plane is cut along the line $\sigma \le \beta_e/k$. (If $\alpha_k(Q) = c_{\widehat{\chi}} = 1$ and if there is also no Siegel zero mod q, then there is no cut.)

Lemma 4.6.1. *The Dirichlet series $F_\chi(s)$ is absolutely convergent on the half-plane $\sigma > \frac{1}{k}$, where it satisfies*

$$F_\chi(s) = F_1(sk)^{c_{\widehat{\chi}}}\ g(sk)^{c_{\widehat{\chi}}}\ G_{\chi,1}(s)\ G_{\chi,2}(s) \tag{4.56}$$

with

$$F_1(sk) = \left(\prod_{Q_1 | Q} \prod_{\substack{\psi \bmod Q_1 \\ \psi \text{ primitive}}} L(sk, \psi)^{\gamma(\psi)} \right)^{\alpha_k(Q)}$$

$$g(sk) = \left(\prod_{Q_1 | Q} \prod_{\substack{\psi \bmod Q_1 \\ \psi \text{ primitive}}} \prod_{\ell \mid \frac{Q}{Q_1}} \left(1 - \frac{\psi(\ell)}{\ell^{ks}}\right)^{\gamma(\psi)} \right)^{\alpha_k(Q)},$$

$$\gamma(\psi) = \frac{1}{\alpha_k(Q)\varphi(Q)} \sum_{\substack{v \in U_Q \\ W_k(v) \in U_Q}} \overline{\chi}(v).$$

Here, the functions $F_1(sk)$, $g(sk)$, $G_{\chi,1}(s)$ and $G_{\chi,2}(s)$ satisfy the following properties:

(i) $F_1(sk)$ is holomorphic and nonvanishing in the region $\mathcal{D}_k(c_0) - (-\infty, 1/k]$. [7] *In fact, if $\alpha_k(Q) = c_{\widehat{\chi}} = 1$ and if β_e exists (resp. doesn't exist), then the same is true in the bigger region $\mathcal{D}_k(c_0) - (-\infty, \beta_e/k]$ (resp. $\mathcal{D}_k(c_0)$).*

(ii) $g(sk)$ and $G_{\chi,1}(s)$ are holomorphic and nonvanishing in the half-plane $\sigma > \mu_0/k$,

[7] This region is obtained by omitting the ray $(-\infty, 1/k]$ from the region $\mathcal{D}_k(c_0)$.

and we have, uniformly for all s in this region,

$$\max\left\{\left|\frac{g'(sk)}{g(sk)}\right|, \left|\frac{G'_{\chi,1}(s)}{G_{\chi,1}(s)}\right|\right\} \ll \max\{1, (\log Q)^{1-\sigma k}\} \ \log\log Q. \tag{4.57}$$

(iii) $G_{\chi,2}(s)$ is holomorphic in the half-plane $\sigma > \mu_0/k$, wherein

$$|G_{\chi,2}(s)|, |G'_{\chi,2}(s)| \ll 1.$$

Before proving this lemma, we state some results from [69] (or immediate consequences thereof) that will be useful to us in the sequel.

Lemma 4.6.2.

(i) [69, Lemma 3(i)(a)] We have $\sum_{\ell|m} \ell^{-\sigma} \log \ell \ll \max\{1, (\log m)^{1-\sigma}\} \log\log m$, uniformly in positive integers $m \geq 3$ and in complex numbers s having $\sigma > 0.7$.

(ii) [69, Lemma 7] For all $y > 1$ and $0 < \lambda \leq 1$, we have $\int_y^\infty \ e^{-u}u^{\lambda-1}\mathrm{du} \leq y^{\lambda-1}e^{-y}$.

(iii) [69, Lemma 9(ii)] With $g(s)$ coming from the statement of Lemma 4.6.1, we have $|g'(s)/g(s)| \ll \max\{1, (\log Q)^{1-\sigma}\} \log\log Q$, uniformly for s having $\sigma > 0.7$.

(iv) [69, Lemma 15(i)] With $F_1(s)$ coming from the statement of Lemma 4.6.1,

$$\left|\frac{F_1'(s)}{F_1(s)} + \frac{\alpha_k(Q)}{s-1} - \frac{\alpha_k(Q)\gamma(\psi_e)}{s-\beta_e}\right| \ \ll \ \log(Q(|t|+1)),$$

uniformly in complex numbers s satisfying $\sigma \geq 1 - c_1/2\log(Q(|t|+1))$.

Here, subpart (ii) is a standard bound on the tail of the integral defining a Gamma function, and follows by integrating by parts. Subpart (iv) is a direct consequence of [69, Lemma 15(i)] with the parameter "ξ" there defined to be $\log(Q(|t|+1))$.

Proof of Lemma 4.6.1. **Absolute convergence of $F_\chi(s)$ on the region $\sigma > 1/k$:** To see this, we start by noting that $F_\chi(s)$ is tautologically absolutely convergent on $\sigma > 1$, and in this half plane, we have the Euler product

$$F_\chi(s) = \prod_p \left(1 + \sum_{v\geq 1} \frac{\mathbb{1}_{(f(p^v),Q)=1}}{p^{vs}} \prod_{i=1}^{K} \chi_i(f_i(p^v))\right). \tag{4.58}$$

In the rest of the proof, we **fix** $B_k > 2^{k/\mu_0}$ such that B_k exceeds any k-free integer n satisfying $\gcd(f(n), q) = 1$; recall that by Lemma 4.2.3, B_k can be chosen to depend only on $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v\leq k}}$. Then the contribution of primes $p \leq B_k$ to the aforementioned Euler product is a finite product, each factor of which is absolutely convergent in the region $\sigma > 0$. On the other hand, by Lemma 4.2.3 and the facts that Q is k-admissible and $(\chi_1, \dots, \chi_K) \in \mathcal{C}_k(Q_0)$, the total contribution of all primes $p > B_k$ to the above Euler product (4.58) is

$$\prod_{p>B_k} \left(1 + \frac{c_{\widehat{\chi}}\mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}} + O\left(\frac{1}{p^{(k+1)\sigma}}\right)\right), \tag{4.59}$$

which is absolutely convergent in the region $\sigma > 1/k$. (This is because the series $\sum_p c_{\widehat{\chi}}\mathbb{1}_{(W_k(p),Q)=1}/p^{ks}$ is absolutely convergent for $\sigma > 1/k$.) This shows that $F_\chi(s)$ is absolutely convergent on the region $\sigma > 1/k$.

The product decomposition (4.56)**:** Thus (4.58) holds in the region $\sigma > 1/k$, and in this same region, we may write

$$\begin{aligned} F_\chi(s) = &\left(\prod_{\substack{b\in U_Q\\ W_k(b)\in U_Q}} \prod_{p\equiv b \,(\mathrm{mod}\ Q)} \left(1 - \frac{1}{p^{ks}}\right)^{-c_{\widehat{\chi}}}\right) \cdot \left(\prod_{\substack{p\mid Q\\ W_k(p)\in U_Q}} \left(1 - \frac{1}{p^{ks}}\right)^{-c_{\widehat{\chi}}}\right) \\ &\cdot \prod_p \left(1 + \sum_{v\geq 1} \frac{\mathbb{1}_{(f(p^v),Q)=1}}{p^{vs}} \prod_{i=1}^{K} \chi_i(f_i(p^v))\right) \left(1 - \frac{\mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}}\right)^{c_{\widehat{\chi}}} \end{aligned} \tag{4.60}$$

Now for $\sigma > 1/k$, the orthogonality of Dirichlet characters mod Q and the fact that $\log L(sk,\psi) = \sum_{p,v} \psi(p^v)/p^{vsk}$ show that the logarithm of the first double product in (4.60) is equal to

$$\begin{aligned}
&c_{\widehat{\chi}} \sum_{\substack{b\in U_Q\\ W_k(b)\in U_Q}} \sum_{\substack{p,v\ge 1\\ p\equiv b \pmod Q}} \frac{1}{vp^{vks}} \\
&= c_{\widehat{\chi}} \sum_{\substack{b\in U_Q\\ W_k(b)\in U_Q}} \left\{ \frac{1}{\varphi(Q)} \sum_{\psi \bmod Q} \overline{\psi}(b) \sum_p \frac{\psi(p)}{p^{ks}} + \sum_{\substack{p,v\ge 2\\ p\equiv b \pmod Q}} \frac{1}{vp^{vks}} \right\} \\
&= \alpha_k(Q) c_{\widehat{\chi}} \sum_{\psi \bmod Q} \gamma(\psi) \log L(sk,\psi) \\
&\qquad + c_{\widehat{\chi}} \sum_{\substack{b\in U_Q\\ W_k(b)\in U_Q}} \sum_{v\ge 2} \left(\sum_{p\equiv b \pmod Q} \frac{1}{vp^{vks}} - \sum_{p:\ p^v\equiv b \pmod q} \frac{1}{vp^{vks}} \right).
\end{aligned}$$

We insert this into (4.60), noting that $L(sk,\psi) = L(sk,\psi^*) \prod_{\ell \mid \frac{Q}{Q_1}} (1 - \psi^*(\ell)/\ell^{sk})$ and that $\gamma(\psi) = \gamma(\psi^*)$ if the primitive character ψ^* mod Q_1 induces ψ mod Q. This yields (4.56), with

$$G_{\chi,2}(s) := \prod_{p\le B_k} \left(1 + \sum_{v\ge 1} \frac{\mathbb{1}_{(f(p^v),Q)=1}}{p^{vs}} \prod_{i=1}^K \chi_i(f_i(p^v)) \right) \left(1 - \frac{\mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}} \right)^{c_{\widehat{\chi}}}$$

and

$$\begin{aligned}
G_{\chi,1}(s) := \prod_{p> B_k} &\left(1 + \sum_{v\ge 1} \frac{\mathbb{1}_{(f(p^v),Q)=1}}{p^{vs}} \prod_{i=1}^K \chi_i(f_i(p^v)) \right) \left(1 - \frac{\mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}} \right)^{c_{\widehat{\chi}}} \\
&\cdot \exp\left(c_{\widehat{\chi}} \sum_{\substack{b\in U_Q\\ W_k(b)\in U_Q}} \sum_{v\ge 2} \left(\sum_{p\equiv b \pmod Q} \frac{1}{vp^{vks}} - \sum_{p:\ p^v\equiv b \pmod q} \frac{1}{vp^{vks}} \right) \right) \\
&\cdot \prod_{\substack{p\mid Q\\ W_k(p)\in U_Q}} \left(1 - \frac{1}{p^{ks}} \right)^{-c_{\widehat{\chi}}}, \quad (4.61)
\end{aligned}$$

where B_k was as defined after (4.58).

Proving statements (i)–(iii) of the lemma: To see (i), recall that $\prod_{\psi \bmod Q} L(sk,\psi)$ has is holomorphic and nonvanishing in the region $\mathcal{D}_k(c_0) - (-\infty, 1/k]$. In fact, if $\alpha_k(Q) = c_{\widehat{\chi}} = 1$, then

$$F_1(sk) = L(sk,\chi_0) \cdot \left(\prod_{\substack{Q_1 | Q \\ Q_1 > 1}} \prod_{\substack{\psi \bmod Q_1 \\ \psi \text{ primitive}}} L(sk,\psi)^{\gamma(\psi)} \right)^{\alpha_k(Q)},$$

which shows the other assertions of (i). Also (iii) is immediate by a direct calculation using the definition of $G_{\chi,2}(s)$.

We thus focus on (ii). By the very definition of $g(sk)$, we see that it is holomorphic and nonvanishing in the half-plane $\sigma > 0$. Also the bound on $|g'(sk)/g(sk)|$ in (4.57) is an immediate consequence of Lemma 4.6.2(iii).

To show the assertions for $G_{\chi,1}(s)$, we recall that by the arguments preceding (4.59) the first product (over primes $p > B_k$) in (4.61) is equal to

$$\prod_{p > B_k} \left(1 + \frac{c_{\widehat{\chi}} \mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}} + O\left(\frac{1}{p^{(k+1)\sigma}}\right)\right) \left(1 - \frac{\mathbb{1}_{(W_k(p),Q)=1}}{p^{ks}}\right)^{c_{\widehat{\chi}}} = \prod_{p > B_k} \left(1 + O\left(\frac{1}{p^{(k+1)\sigma}}\right)\right),$$

which is absolutely convergent and defines a holomorphic function in the half plane $\sigma > \mu_0/k$. (Here is it important that $\mu_0/k > 1/(k+1)$.) Likewise the exponential factor in (4.61) defines a holomorphic function in the same half plane, hence so does $G_{\chi,1}(s)$. To see that $G_{\chi,1}(s)$ is also nonvanishing in this region, we need only see that the condition $p > B_k > 2^{k/\mu_0}$ guarantees that each of the factors $1 + \sum_{v \geq 1} \frac{\mathbb{1}_{(f(p^v),Q)=1}}{p^{vs}} \prod_{i=1}^{K} \chi_i(f_i(p^v))$ in (4.61) has size at least $1 - \sum_{v \geq k} p^{-v\sigma} > 1 -$

$2p^{-k\sigma} > 1 - 2B_k^{-\mu_0} > 0$. Finally, a straightforward computation using (4.61) shows that for $\sigma > \mu_0/k$, we have

$$\frac{G'_{\chi,1}(s)}{G_{\chi,1}(s)} = -c_{\widehat{\chi}} k \sum_{\substack{p|Q \\ W_k(p)\in U_Q}} \frac{\log p}{p^{ks}} + O(1) \ll \sum_{p|Q} \frac{\log p}{p^{k\sigma}},$$

completing the proof of (4.57) via Lemma 4.6.2(i). □

4.6.2. Preparing for the contour shift: Auxiliary functions and intermediate bounds

Our objective is to relate the sum in Theorem 4.4.5 to the Dirichlet series $F_\chi(s)$ by an effective version of Perron's formula, and shift the contour to the left of the line $\sigma = 1/k$. As such, we will need the following proposition in order to estimate the resulting integrals.

To set up, we choose $\epsilon_1 \coloneqq \epsilon_1(\lambda)$ to be a constant (depending only on λ) satisfying $0 < \epsilon_1 < 1 - \cos(2\pi/d)$ for any positive integer $d \leq \lambda$. Consider the functions

$$\begin{aligned}
\widetilde{F}_\chi(s) &\coloneqq F_1(sk)^{c_{\widehat{\chi}}}\, g(sk)^{c_{\widehat{\chi}}}\, G_{\chi,1}(s) \\
\widetilde{H}_\chi(s) &\coloneqq \widetilde{F}_\chi(s) \left(s - \frac{1}{k}\right)^{\alpha_k(Q)c_{\widehat{\chi}}} \left(s - \frac{\beta_e}{k}\right)^{-\alpha_k(Q)c_{\widehat{\chi}}\gamma(\psi_e)}, \\
H_\chi(s) &\coloneqq \frac{\widetilde{F}_\chi(s)}{s} \left(s - \frac{1}{k}\right)^{\alpha_k(Q)c_{\widehat{\chi}}},
\end{aligned}$$

where here and in what follows, any term or factor involving β_e is to be understood as omitted if the Siegel zero doesn't exist. By Lemma 4.6.1(i) and (ii), we see that:

1. $\widetilde{F}_\chi(s)$ is holomorphic and nonvanishing on $\mathcal{D}_k(c_0) - (-\infty, 1/k]$. If $\alpha_k(Q) = c_{\widehat{\chi}} = 1$ and if β_e exists (resp. doesn't exist), then the same is true on $\mathcal{D}_k(c_0) - (-\infty, \beta_e/k]$

(resp. $\mathcal{D}_k(c_0)$).

2. $H_\chi(s)$ analytically continues into and is nonvanishing on $\mathcal{D}_k(c_0) - (-\infty, \beta_e/k]$.

3. $\widetilde{H}_\chi(s)$ analytically continues into and is nonvanishing on $\mathcal{D}_k(c_0)$.

(Recall our branch cut conventions elucidated at the start of the section.)

In what follows, we set $T \coloneqq \exp(\sqrt{\log x})$.

Proposition 4.6.3. *We have the following bounds:*

(i) $|H_\chi(1/k)| \ll (\log x)^{\alpha_k(Q)\epsilon_1/5}$.

(ii) $|\widetilde{H}_\chi(s)| \ll (\log x)^{\alpha_k(Q)\epsilon_1/4}$ *uniformly for real* s *satisfying*

$$\frac{1}{k}\left(1 - \frac{c_1}{4\log Q}\right) \leq s \leq \frac{1}{k}.$$

(iii) $|F_\chi(s)| \ll (\log x)^{(1/2+\epsilon_1)\alpha_k(Q)}$ *uniformly for complex numbers* $s = \sigma + it$ *satisfying* $\sigma \geq \frac{1}{k}\left(1 - \frac{c_1}{2\mathcal{L}_Q(t)}\right)$, $|t| \leq T$ *and* $|s - \theta/k| \gg 1/\mathcal{L}_Q(t)$ *for* $\theta \in \{1, \beta_e\}$.

(iv) Uniformly in real $s \leq 1/k$ *satisfying* $s \geq \frac{1}{k}\left(\frac{2}{3} + \frac{\beta_e}{3}\right)$ *(if the Siegel zero exists) or* $s \geq \frac{1}{k}\left(1 - \frac{c_1}{4\log Q}\right)$ *(otherwise), we have*

$$\left|H_\chi\left(\frac{1}{k}\right)G_{\chi,2}\left(\frac{1}{k}\right) - H_\chi(s)G_{\chi,2}(s)\right| \ll (\log x)^{(1/20+\alpha_k(Q)/5)\epsilon_1}\left(\frac{1}{k} - s\right).$$

Proof. We start with the following

General observation: We have $|\widetilde{H}_\chi(s)| \asymp |\widetilde{H}_\chi(w)|$ uniformly in complex numbers s and w satisfying $\mathrm{Im}(s) = \mathrm{Im}(w) =: t$, and $|s - w| \ll \mathcal{L}_Q(t)^{-1}$ and $\mathrm{Re}(w) \geq \mathrm{Re}(s) \geq \frac{1}{k}\left(1 - \frac{c_1}{2\mathcal{L}_Q(t)}\right)$.

Indeed by the definitions of $\widetilde{H}_\chi(s)$ and $\widetilde{F}_\chi(s)$, we have

$$\begin{aligned}&\left|\frac{\widetilde{H}'_\chi(z)}{\widetilde{H}_\chi(z)}\right| \\ &= \left|c_{\widehat{\chi}}k\left(\frac{F_1'(kz)}{F_1(kz)}+\frac{\alpha_k(Q)}{kz-1}-\frac{\alpha_k(Q)\gamma(\psi_e)}{kz-\beta_e}\right)+c_{\widehat{\chi}}k\frac{g'(kz)}{g(kz)}+\frac{G'_{\chi,1}(z)}{G_{\chi,1}(z)}\right| \ll \mathcal{L}_Q(t) \quad (4.62)\end{aligned}$$

uniformly for complex numbers $z=u+it$ satisfying $u \geq \frac{1}{k}\left(1-\frac{c_1}{2\mathcal{L}_Q(t)}\right)$. In the last bound above, we have used (4.57) and Lemma 4.6.2(iv). The general observation now follows by writing

$$\log\left(\frac{\widetilde{H}_\chi(w)}{\widetilde{H}_\chi(s)}\right)=\int_{\mathrm{Re}(s)}^{\mathrm{Re}(w)} \frac{\widetilde{H}'_\chi(u+it)}{\widetilde{H}_\chi(u+it)}\,\mathrm{d}u.$$

(i) Let $b_k(t) \coloneqq \frac{1}{k}\left(1+\frac{c_3}{\mathcal{L}_Q(t)}\right)$ for some absolute constant $c_3>0$. By the above observation and the definitions of $\widetilde{F}_\chi(s)$, $\widetilde{H}_\chi(s)$ and $H_\chi(s)$, we see that

$$\begin{aligned}\left|H_\chi\left(\frac{1}{k}\right)\right| &\ll \left|\widetilde{H}_\chi\left(\frac{1}{k}\right)\right|(1-\beta_e)^{-\alpha_k(Q)} \ll |\widetilde{H}_\chi(b_k(0))|\,(1-\beta_e)^{-\alpha_k(Q)} \\ &\ll |\widetilde{F}_\chi(b_k(0))|\,(\log Q)(1-\beta_e)^{-2\alpha_k(Q)} \\ &\ll |F_1(kb_k(0))g(kb_k(0))|^{\mathrm{Re}(c_{\widehat{\chi}})}\,(\log Q)^2(1-\beta_e)^{-2\alpha_k(Q)}. \quad (4.63)\end{aligned}$$

Here in the last bound, we have noted that $|G_{\chi,1}(b_k(0))| \ll \log_2 Q$, as is evident from the fact that $\prod_{\substack{p|Q\\ W_k(p)\in U_Q}}(1-p^{-kb_k(0)})^{-1} \ll \exp(\sum_{p|Q}1/p) \ll \exp(\sum_{p\leq\omega(Q)}1/p) \ll \log\omega(Q) \ll \log_2 Q$.

Now proceeding exactly as in the proof of (4.56), we see that for all s with $\sigma>1/k$, we have

$$\sum_{n\geq 1}\frac{\mathbb{1}_{(f(n^k),Q)=1}}{n^{ks}}=F_1(ks)\;g(ks)\;\widetilde{G}(s), \quad (4.64)$$

where

$$\widetilde{G}(s) = \prod_{p} \left(1 + \sum_{v\geq 2} \frac{1}{p^{vks}} (\mathbb{1}_{(f(p^{kv}),Q)=1} - \mathbb{1}_{(W_k(p),Q)=1}\ \mathbb{1}_{(f(p^{k(v-1)}),Q)=1})\right)$$
$$\cdot \exp\left(\sum_{\substack{b\in U_Q \\ W_k(b)\in U_Q}} \sum_{v\geq 2} \left(\sum_{p\equiv b \,(\mathrm{mod}\ Q)} \frac{1}{vp^{vks}} - \sum_{p:\ p^v\equiv b \,(\mathrm{mod}\ Q)} \frac{1}{vp^{vks}}\right)\right)$$
$$\cdot \prod_{\substack{p|Q \\ W_k(p)\in U_Q}} \left(1-\frac{1}{p^{ks}}\right)^{-1}.$$

Uniformly for s with $\sigma \geq 1/k$, we observe that the infinite product above has size at least $1 - \sum_{p,v\geq 2} 1/p^v \gg 1$ and at most $\exp(\sum_{p,v\geq 2} 1/p^v) \ll 1$. Likewise, the exponential factor has size $\asymp 1$ in the same region. Moreover, for $\sigma \geq 1/k$, the product over $p \mid Q$ is $\asymp |\exp(\sum_{p|Q:\ (W_k(p),Q)=1}\ p^{-ks})|$, which is $\gg 1$ and $\ll \exp(\sum_{p|Q}\ p^{-1}) \ll \log_2 Q$. Putting these observations together, we find that

$$1 \ll \widetilde{G}(s) \ll \log_2 Q, \quad \text{uniformly in complex numbers } s \text{ having } \sigma \geq 1/k. \tag{4.65}$$

Applying this lower bound on $\widetilde{G}(b_k(0))$, the equality (4.64) yields

$$|F_1(kb_k(0))\ g(kb_k(0))| \ll \sum_{n\geq 1} \frac{\mathbb{1}_{(f(n^k),Q)=1}}{n^{kb_k(0)}} \leq \zeta(kb_k(0))$$
$$= \frac{1}{kb_k(0)-1} + O(1) \ll \log Q,$$

so that from (4.63), we obtain $|H_\chi(1/k)| \ll (\log Q)^3(1-\beta_e)^{-2\alpha_k(Q)}$. Subpart (i) now follows as $Q \leq (\log x)^{K_0}$ and as $1-\beta_e \gg_{\epsilon_1} Q^{-\epsilon_1/20K_0} \gg_{\epsilon_1} (\log x)^{-\epsilon_1/20}$ by Siegel's Theorem.

(ii) By the general observation at the start of the proof, we have $|\widetilde{H}_\chi(s)| \ll |\widetilde{H}_\chi(1/k)| \ll$

$|H_\chi(1/k)|(1-\beta_e)^{-\alpha_k(Q)} \ll |H_\chi(1/k)|(\log x)^{\alpha_k(Q)\epsilon_1/20}$. The result now follows from (i).

(iii) By the same general observation, we have $|\widetilde{H}_\chi(s)| \ll |\widetilde{H}_\chi(b_k(t)+it)|$, and since $|s-\theta/k| \gg 1/\mathcal{L}_Q(t)$, we have $b_k(t)+it-\theta/k \asymp s-\theta/k$ for $\theta \in \{1,\beta_e\}$. Thus $|\widetilde{F}_\chi(s)| \ll |\widetilde{F}_\chi(b_k(t)+it)|$. (Recall that $\widetilde{H}_\chi(s) \coloneqq \widetilde{F}_\chi(s)\left(s-\frac{1}{k}\right)^{\alpha_k(Q)c_{\widehat{\chi}}}\left(s-\frac{\beta_e}{k}\right)^{-\alpha_k(Q)c_{\widehat{\chi}}\gamma(\psi_e)}$.) Using (4.61) and replicating the arguments that led to (4.65), we also obtain

$$(\log_2 Q)^{-1} \ll G_{\chi,1}(s) \ll \log_2 Q,$$
$$\text{uniformly in complex numbers } s \text{ having } \sigma \geq 1/k. \quad (4.66)$$

Thus uniformly for s as in subpart (iii) of the proposition, we have

$$|\widetilde{F}_\chi(s)| \ \ll \ |\widetilde{F}_\chi(b_k(t)+it)| \ \ll \ (\log_2 Q)\cdot |F_1(k(b_k(t)+it))g(k(b_k(t)+it))|^{\mathrm{Re}(c_{\widehat{\chi}})}.$$

(Recall that $\widetilde{F}_\chi(s) = F_1(sk)^{c_{\widehat{\chi}}}\ g(sk)^{c_{\widehat{\chi}}}\ G_{\chi,1}(s)$.) Next by (4.64) and (4.65), we get

$$|\widetilde{F}_\chi(s)| \ll (\log_2 Q)\left|\sum_{n\geq 1}\frac{\mathbb{1}_{(f(n^k),Q)=1}}{n^{k(b_k(t)+it)}}\right|^{\mathrm{Re}(c_{\widehat{\chi}})} \ll (\log_2 Q)\left(\sum_{n\geq 1}\frac{\mathbb{1}_{(f(n^k),Q)=1}}{n^{kb_k(t)}}\right)^{\mathrm{Re}(c_{\widehat{\chi}})}.$$

By (4.64), (4.65) and (4.66), we get

$$|\widetilde{F}_\chi(s)| \ll (\log_2 Q)^2|F_1(kb_k(t))g(kb_k(t))|^{\mathrm{Re}(c_{\widehat{\chi}})} \ll (\log_2 Q)^3|\widetilde{F}_\chi(b_k(t))|.$$

By definitions of $b_k(t)$ and $\widetilde{H}_\chi(b_k(t))$, the last bound gives

$$|\widetilde{F}_\chi(s)| \ll (\log_3 x)^3|\widetilde{H}_\chi(b_k(t))|\mathcal{L}_Q(t)^{\alpha_k(Q)}(1-\beta_e)^{-\alpha_k(Q)}.$$

Finally, recall that $|t| \leq T = \exp(\sqrt{\log x})$, that $1-\beta_e \gg_{\epsilon_1} (\log x)^{-\epsilon_1/20}$, and that $|\widetilde{H}_\chi(b_k(t))| \ll |\widetilde{H}_\chi(1/k)| \ll (\log x)^{\alpha_k(Q)\epsilon_1/4}$ (by subpart (ii) the general observation at

the start of the proof). This yields $|\widetilde{F}_\chi(s)| \ll (\log x)^{\alpha_k(Q)(1/2+\epsilon_1)}$. Lemma 4.6.1(iii) now proves the assertion.

(iv) It suffices to show that uniformly for s satisfying the same conditions as in this subpart,

$$|H_\chi(s)| + |H'_\chi(s)| \ll (\log x)^{\alpha_k(Q)\epsilon_1/5}\left(\log Q + \frac{1}{1-\beta_e}\right). \tag{4.67}$$

(Here as usual, the second term on the right is omitted if there is no Siegel zero, otherwise it dominates.) Indeed once we establish (4.67), then from the bound $1-\beta_e \gg_{\epsilon_1} (\log x)^{-\epsilon_1/20}$, it follows that $|H_\chi(s)|+|H'_\chi(s)| \ll (\log x)^{(1/20+\alpha_k(Q)/5)\epsilon_1}$, which combined with Lemma 4.6.1(iii) and the observation $|H_\chi(1/k)G_{\chi,2}(1/k) - H_\chi(s)G_{\chi,2}(s)| = \left|\int_s^{1/k}(H_\chi(u)G_{\chi,2}(u))'\,\mathrm{d}u\right|$ completes the proof of the subpart.

To show (4.67), we recall that $H_\chi(s)$ is non-vanishing for s as in the subpart. Further (4.62) applies with $z = s$ for all s considered in this subpart, yielding

$$\begin{aligned}\left|\frac{H'_\chi(s)}{H_\chi(s)}\right| &= \left|\frac{\widetilde{H}'_\chi(s)}{\widetilde{H}_\chi(s)} - \frac{1}{s} + \frac{\alpha_k(Q)c_{\widetilde{\chi}}\gamma(\psi_e)}{s-\beta_e/k}\right| \\ &\ll \mathcal{L}_Q(0) + 1 + \frac{1}{1-\beta_e} \ll \log Q + \frac{1}{1-\beta_e}.\end{aligned}$$

As a consequence,

$$\begin{aligned}\left|\log\frac{H_\chi(1/k)}{H_\chi(s)}\right| &= \left|\int_s^{1/k}\frac{H'_\chi(u)}{H_\chi(u)}\,\mathrm{d}u\right| \\ &\ll \left(\frac{1}{k}-s\right)\left(\log Q + \frac{1}{1-\beta_e}\right) \ll 1,\end{aligned}$$

showing that $|H_\chi(s)| \asymp |H_\chi(1/k)|$ uniformly for all s in the statement. Collecting

these bounds, we obtain for all such s,

$$\begin{aligned}|H_\chi(s)| + |H'_\chi(s)| &\ll \left|H_\chi\left(\frac{1}{k}\right)\right| + \left|\frac{H'_\chi(s)}{H_\chi(s)}\right| \cdot \left|\frac{H_\chi(s)}{H_\chi(1/k)}\right| \cdot \left|H_\chi\left(\frac{1}{k}\right)\right| \\ &\ll \left|H_\chi\left(\frac{1}{k}\right)\right| \left(\log Q + \frac{1}{1-\beta_e}\right),\end{aligned}$$

so that the desired bound (4.67) now follows from subpart (i). This concludes the proof. □

4.6.3. Perron's formula and the contour shifts

We first show that there is some X sufficiently close to x for which the error term arising from an effective Perron's formula is small.

Lemma 4.6.4. *Let $h \coloneqq x/\log^2 x$. There exists a positive integer $X \in (x, x+h]$ satisfying*

$$\sum_{\substack{3X/4<n<5X/4 \\ n\neq X}} \frac{\mathbb{1}_{(f(n),Q)=1}}{|\log(X/n)|} \ll X^{1/k} \log X.$$

Proof. This would follow once we show that

$$\sum_{x<X\leq x+h} \sum_{\substack{3X/4<n<5X/4 \\ n\neq X}} \frac{\mathbb{1}_{(f(n),Q)=1}}{|\log(X/n)|} \ll x^{1/k} h \log x, \tag{4.68}$$

with the outer sum being over integers $X \in (x, x+h]$. (Recall that $x \in \mathbb{Z}^+$ in this entire section.) To show this, we write the sum on the left hand side as $S_1 + S_2$, where S_1 denotes the contribution of the case $3X/4 < n \leq X-1$. Writing any n contributing to S_1 as $X - v$ for some integer $v \in [1, X/4)$, we see that $|\log(X/n)| = -\log(1 - v/X) \gg v/X \gg v/x$. Recalling that $n = Bm$ for some k-free B of size

$O(1)$ and some k-full m, we thus have

$$S_1 \leq \sum_{3x/4<n<x+h} \sum_{\substack{x<X\leq x+h \\ n+1\leq X<4n/3}} \frac{\mathbb{1}_{(f(n),Q)=1}}{|\log(X/n)|} \ll x \sum_{B\ll 1} \sum_{\substack{\frac{3x}{4B}<m<\frac{x+h}{B} \\ m \text{ is } k\text{-full}}} \sum_{\substack{1\leq v<\frac{x+h}{4} \\ x<v+Bm\leq x+h}} \frac{1}{v}$$
$$\ll x \sum_{1\leq v\leq \frac{x+h}{4}} \frac{1}{v} \sum_{B\ll 1} \sum_{\substack{\frac{x-v}{B}<m\leq\frac{x-v+h}{B} \\ m \text{ is } k\text{-full}}} 1 \ll x\log x \left(x^{1/k}\frac{h}{x} + x^{1/(k+1)}\right) \ll x^{1/k} h \log x,$$

where we have bounded the last inner sum on m using the Erdős-Szekeres estimate on the count of k-full integers (see [23]). This shows that the sum S_1 is bounded by the right hand expression in (4.68). Similarly so is the sum S_2, proving (4.68). □

To complete the proof of Theorem 4.4.5, it suffices to establish the bound therein for the "X" found in Lemma 4.6.4 in place of "x", for once we do so, we may simply note that

$$\Big|\sum_{x<n\leq X} \chi_1(f_1(n))\cdots\chi_K(f_K(n))\mathbb{1}_{(f(n),q)=1}\Big|$$
$$\leq \sum_{x<n\leq X} \mathbb{1}_{(f(n),Q)=1} \leq \sum_{B\ll 1} \sum_{\substack{\frac{x}{B}<m\leq\frac{X}{B} \\ m \text{ is } k\text{-full}}} 1 \ll \frac{x^{1/k}}{\log^2 x}.$$

To show the bound in Theorem 4.4.5 for X, we start by applying an effective version of Perron's formula [76, Theorem II.2.3]. To bound the resulting error, we use Lemma 4.6.4 and note that

$$X^{\frac{1}{k}\left(1+\frac{1}{\log X}\right)} \left(\sum_{n\leq 3X/4} + \sum_{n\geq 5X/4}\right) \frac{\mathbb{1}_{(f(n),Q)=1}}{T|\log(X/n)| n^{\frac{1}{k}\left(1+\frac{1}{\log X}\right)}}$$
$$\ll \frac{X^{1/k}}{T} \sum_{B\ll 1} \sum_{\substack{m\geq 1 \\ m \text{ is } k\text{-full}}} \frac{1}{m^{\frac{1}{k}\left(1+\frac{1}{\log X}\right)}}$$
$$\ll \frac{X^{1/k}}{T} \prod_p \left(1 + \frac{1}{p^{1+1/\log X}} + O\left(\frac{1}{p^{1+1/k}}\right)\right)$$

$$\ll \frac{X^{1/k}}{T}\exp\left(\sum_p \frac{1}{p^{1+1/\log X}}\right) \ll \frac{X^{1/k}\log X}{T},$$

with the last bound above being a consequence of Mertens' Theorem along with the fact that

$$\begin{aligned}\sum_{p>X}\frac{1}{p^{1+1/\log X}} &\leq \sum_{j\geq 0}\sum_{X^{2^j}<p\leq X^{2^{j+1}}}\frac{1}{p^{1+1/\log X}}\\ &\leq \sum_{j\geq 0}\exp(-2^j)\sum_{X^{2^j}<p\leq X^{2^{j+1}}}\frac{1}{p} \ll 1.\end{aligned}$$

(Recall that $T=\exp(\sqrt{\log x})\geq \exp\left(\frac{1}{2}\sqrt{\log X}\right)$.) As such, [76, Theorem II.2.3] yields

$$\begin{aligned}&\sum_{n\leq X}\chi_1(f_1(n))\cdots\chi_K(f_K(n))\mathbb{1}_{(f(n),Q)=1}\\ &\qquad = \frac{1}{2\pi i}\int_{\frac{1}{k}\left(1+\frac{1}{\log X}\right)-iT}^{\frac{1}{k}\left(1+\frac{1}{\log X}\right)+iT}\frac{F_\chi(s)X^s}{s}\,\mathrm{d}s + O\left(\frac{X^{1/k}\log X}{T}\right). \quad (4.69)\end{aligned}$$

Our arguments will be divided into three possibilities:

Case 1: When $(\alpha_k(Q), c_{\widehat{\chi}})\neq(1,1)$ and there is a Siegel zero β_e mod Q.

Case 2: When $(\alpha_k(Q), c_{\widehat{\chi}})\neq(1,1)$ and there is no Siegel zero mod Q.

Case 3: When $(\alpha_k(Q), c_{\widehat{\chi}})=(1,1)$.

In Case 1, we will be assuming henceforth that $\beta_e > 1-\frac{5c_1}{24\log Q}$; otherwise decreasing c_1 reduces to Case 2. Let $\beta^* := \frac{2}{3}+\frac{\beta_e}{3}$ and $\sigma_k(t) := \frac{1}{k}\left(1-\frac{c_1}{4\mathcal{L}_Q(t)}\right)$, so that $\frac{\beta_e}{k}>\sigma_k(0)$. Let $\delta,\delta_1\in(0,\beta_e/10k)$ satisfy $\sigma_k(0)<\frac{\beta_e}{k}-2\delta_1<\frac{\beta_e}{k}+2\delta_1<\frac{\beta^*}{k}<\frac{1}{k}-2\delta$. Consider the contours

- Γ_2, the horizontal segment traversed from $\frac{1}{k}\left(1+\frac{1}{\log X}\right)+iT$ to $\sigma_k(T)+iT$.
- Γ_3, the part of the curve $\sigma_k(t)+it$ traversed from $t=T$ to $t=0$.

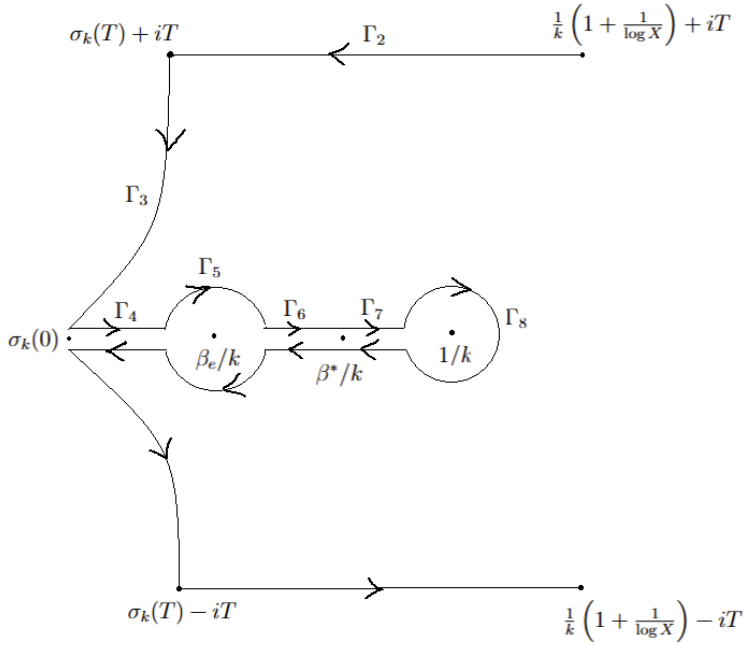
- $\Gamma_4 \coloneqq \Gamma_4(\delta_1)$, the segment traversed from $\sigma_k(0)$ to $\beta_e/k - \delta_1$ **above** the branch cut.
- $\Gamma_5 \coloneqq \Gamma_5(\delta_1)$, the semicircle of radius δ_1 centered at β_e/k, lying in the upper half plane and traversed clockwise.
- $\Gamma_6 \coloneqq \Gamma_6(\delta_1)$, the segment traversed from $\beta_e/k + \delta_1$ to β^*/k **above** the branch cut.
- $\Gamma_7 \coloneqq \Gamma_7(\delta)$, the segment traversed from β^*/k to $1/k - \delta$ **above** the branch cut.
- $\Gamma_8 \coloneqq \Gamma_8(\delta)$, the circle of radius δ centered at $1/k$, traversed clockwise from the point $1/k - \delta$ above the branch cut to its reflection below the branch cut.
- $\Gamma_4^* \coloneqq \Gamma_4^*(\delta)$, the segment traversed from $\sigma_k(0)$ to $1/k - \delta$ **above** the branch cut.
- $\Gamma_5^* \coloneqq \Gamma_5^*(\delta_1)$, the circle of radius δ_1 centered at β_e/k, traversed clockwise from the point $\beta_e/k - \delta_1$ above the branch cut to its reflection below the branch cut.

Here $\Gamma_5^*(\delta_1)$ is relevant only when our branch cut is along $\sigma \leq \beta_e/k$ (i.e., when $\alpha_k(Q) = c_{\widehat{\chi}} = 1$ and β_e exists), while the rest of the contours are defined irrespective of the branch cut. We define the contour Γ_1 by

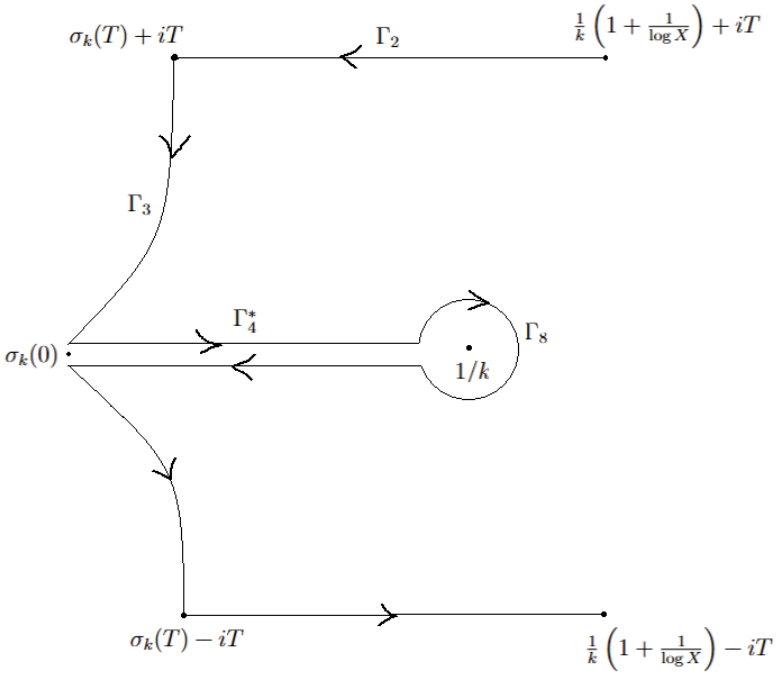
$$\Gamma_1 \coloneqq \begin{cases} \sum_{j=2}^{8} \Gamma_j + \sum_{j=2}^{7} \overline{\Gamma}_j, & \text{under Case 1} \\ \Gamma_2 + \Gamma_3 + \Gamma_4^* + \Gamma_8 + \overline{\Gamma}_4^* + \overline{\Gamma}_3 + \overline{\Gamma}_2, & \text{under Case 2} \\ \sum_{j=2}^{4} \Gamma_j + \Gamma_5^* + \sum_{j=2}^{4} \overline{\Gamma}_j, & \text{under Case 3.} \end{cases}$$

Here $\overline{\Gamma}_j$ (resp. $\overline{\Gamma}_4^*$) is the contour obtained by reflecting Γ_j (resp. Γ_4^*) about the real axis.

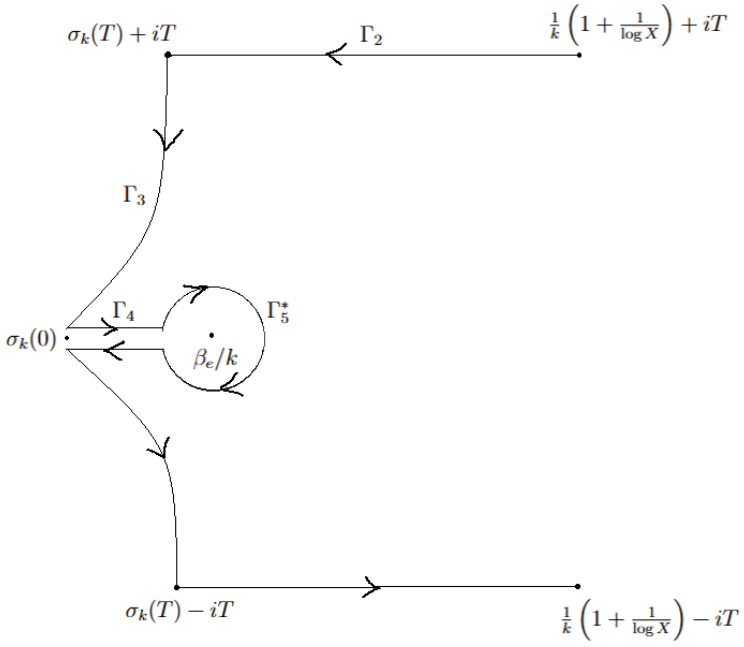
Case 1: $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$ and there is a Siegel zero β_e mod Q.



Case 2: $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$ and there is no Siegel zero mod Q.



Case 3: $(\alpha_k(Q), c_{\widetilde{\chi}}) = (1,1)$ and there is a Siegel zero β_e mod Q.



In Case 3, if β_e doesn't exist, then there is no branch cut and Γ_4, $\overline{\Gamma}_4$ and Γ_5^* are excluded from Γ_1. In all three cases, the integrand in (4.69) is analytic in the region enclosed by Γ_1 and the segment joining $\frac{1}{k}\left(1 + \frac{1}{\log X}\right) - iT$ and $\frac{1}{k}\left(1 + \frac{1}{\log X}\right) + iT$. (Note that if $c_{\widetilde{\chi}} = 1$, the definitions of $\mathcal{Q}(k; f_1, \cdots, f_K)$ and $G_{\chi,1}$, $G_{\chi,2}$ in Lemma 4.6.1 give $G_{\chi,2}(1/k) = 0$, canceling the simple pole of $F_1(sk)$ at $s = 1/k$. In particular, this happens in Case 3.) So

$$\sum_{n \le X} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),Q)=1}$$
$$= -\frac{1}{2\pi i} \int_{\Gamma_1} \frac{F_\chi(s) X^s}{s} \, \mathrm{d}s + O\left(\frac{X^{1/k} \log X}{T}\right). \quad (4.70)$$

We now proceed to estimate the integrals occurring on the right hand side above. In the following proposition, any result about an integral is valid whenever the cor-

responding contour is a part of Γ_1: so for instance, the assertion on Γ_8 (resp. Γ_5^*) holds under Cases 1 or 2 (resp. Case 3), those on Γ_5 and Γ_6 hold under Case 1, and the bound involving Γ_4 holds under Cases 1 and 3. Let I_j (resp. $\overline{I_j}$, I_j^*) denote the corresponding integral along Γ_j (resp. along $\overline{\Gamma}_j$, Γ_j^*).

Proposition 4.6.5. *We have the following bounds:*

(i) $|I_2| + |\overline{I_2}| + |I_3| + |\overline{I_3}| \ll X^{1/k} \exp(-\kappa_0 \sqrt{\log X})$ *for some positive constant* $\kappa_0 := \kappa_0(c_1, k)$ *depending only on* c_1 *and* k.

(ii) $\max\{|I_4 + \overline{I_4}|, |I_6 + \overline{I_6}|\} \ll X^{1/k} \exp(-\sqrt{\log X})$ *uniformly in* δ, δ_1 *as above.*

(iii) $\lim_{\delta_1 \to 0+} |I_5| = \lim_{\delta_1 \to 0+} |\overline{I_5}| = \lim_{\delta_1 \to 0+} |I_5^*| = \lim_{\delta \to 0+} |I_8| = 0$.

Proof. To show subpart (i), we use the fact that since $\beta_e > 1 - 5c_1/24 \log Q$, any s lying on Γ_2, Γ_3 or their conjugates satisfies the requirements of Proposition 4.6.3(iii). As such, (i) follows immediately from Proposition 4.6.3(iii) and the fact that $|s| \gg |t| + 1$ for all s.

For subpart (ii), we note that for all $s \in \Gamma_4$, we have

$$(s - 1/k)^{-\alpha_k(Q) c_{\widehat{\chi}}} = (1/k - s)^{-\alpha_k(Q) c_{\widehat{\chi}}} \; e^{-i\pi \alpha_k(Q) c_{\widehat{\chi}}}$$

and

$$(s - \beta_e/k)^{\alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)} = (\beta_e/k - s)^{\alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)} \; e^{i\pi \alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)}.$$

(This is clear if the branch cut is along $\sigma \leq 1/k$, and also if the branch cut is along $\sigma \leq \beta_e/k$ which is when $(\alpha_k(Q), c_{\widehat{\chi}}) = (1, 1)$.) Likewise, for all $s \in \overline{\Gamma_4}$, we have $(s - 1/k)^{-\alpha_k(Q) c_{\widehat{\chi}}} = (1/k - s)^{-\alpha_k(Q) c_{\widehat{\chi}}} \; e^{i\pi \alpha_k(Q) c_{\widehat{\chi}}}$ and $(s - \beta_e/k)^{\alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)} = (\beta_e/k - s)^{\alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)} \; e^{-i\pi \alpha_k(Q) c_{\widehat{\chi}} \gamma(\psi_e)}$. Since $e^{\pm i\pi \alpha_k(Q) c_{\widehat{\chi}} (\gamma(\psi_e) - 1)} \ll 1$, the definitions of

$\widetilde{F}_\chi(s)$ and $\widetilde{H}_\chi(s)$ show that

$$|I_4+\overline{I_4}| \ll \left|\int_{\sigma_k(0)}^{\beta_e/k-\delta_1} \frac{\widetilde{H}_\chi(s)G_{\chi,2}(s)X^s}{s}\left(\frac{1}{k}-s\right)^{-\alpha_k(Q)c_{\widehat{\chi}}}\left(\frac{\beta_e}{k}-s\right)^{\alpha_k(Q)c_{\widehat{\chi}}\gamma(\psi_e)}\,\mathrm{d}s\right|.$$

But now by Lemma 4.6.1(iii) and Proposition 4.6.3(ii), we see that

$$\begin{aligned}|I_4+\overline{I_4}| &\ll X^{\beta_e/k}(\log X)^{\alpha_k(Q)\epsilon_1/4}(1-\beta_e)^{-\alpha_k(Q)}\cdot\int_{\sigma_k(0)}^{\beta_e/k-\delta_1}\left(\frac{\beta_e}{k}-s\right)^{\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}}\gamma(\psi_e))}\mathrm{d}s\\ &\ll X^{\beta_e/k}(\log X)^{3\alpha_k(Q)\epsilon_1/10}\cdot\left(\frac{\beta_e}{k}-\sigma_k(0)\right)^{1+\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}}\gamma(\psi_e))}\\ &\ll X^{1/k}\exp(-\sqrt{\log X}).\end{aligned}$$

Here we have recalled that $\beta_e \le 1-c(\epsilon_1)/Q^{\epsilon_1/20K_0} \le 1-c(\epsilon_1)/(\log X)^{\epsilon_1/20}$ for some constant $c(\epsilon_1)>0$, and (as argued before Lemma 4.6.1) that $Q_e \coloneqq \mathfrak{f}(\psi_e)$ has a prime factor $\ell_e > D+2$, which upon factoring $\psi_e = \prod_{\ell|Q}\psi_{e,\ell}$ with $\psi_{e,\ell}$ being a character mod ℓ, led to

$$\alpha_k(Q)|\gamma(\psi_e)| \le \alpha_k(Q)\prod_{\ell|Q_e}\left|\frac{\sum_{v:\ vW_k(v)\in U_\ell}\overline{\psi}_{e,\ell}(v)}{\alpha_k(\ell)(\ell-1)}\right| \tag{4.71}$$

$$\le \frac{1}{\ell_e-1}\left|\sum_{\substack{v \bmod \ell_e\\ W_k(v)\equiv 0 \,(\mathrm{mod}\ \ell_e)}}\overline{\psi}_{e,\ell}(v)\right| \le \frac{D}{D+1}. \tag{4.72}$$

This shows the desired bound on I_4 in (ii), and the assertion for I_6 is entirely analogous.

Coming to subpart (iii), we parametrize the points of Γ_5 by $s=\beta_e/k+\delta_1 e^{i\theta}$ where $\pi \ge \theta \ge 0$. Since $\widetilde{M} \coloneqq \sup_{|s-\frac{\beta_e}{k}|\le\frac{1}{2}\left(\frac{\beta_e}{k}-\sigma_k(0)\right)}|\widetilde{H}_\chi(s)|$ is finite, we have for all

sufficiently small $\delta_1 > 0$,

$$|I_5| \ll \widetilde{M} \int_0^\pi X^{\beta_e/k+\delta_1} \left(\frac{1-\beta_e}{k} - \delta_1\right)^{-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})} \delta_1^{1+\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}}\gamma(\psi_e))}\, \mathrm{d}\theta$$
$$\ll \frac{\widetilde{M} X^{\beta_e/k+\delta_1} \delta_1^{1/(D+1)}}{\left(\frac{1-\beta_e}{k} - \delta_1\right)^{\alpha_k(Q)}},$$

where we have again seen that $1 + \alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}}\gamma(\psi_e)) \geq 1/(D+1)$ by (4.71). The last expression shows that $\lim_{\delta_1 \to 0+} |I_5| = 0$, and the assertions on $|\overline{I_5}|$ and $|I_5^*|$ are proved similarly. The same argument also shows that

$$|I_8| \ll M^* X^{1/k+\delta} \delta^{1-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})} \left(\frac{1-\beta_e}{k} - \delta\right)^{-\alpha_k(Q)}$$

for all sufficiently small $\delta > 0$, where $M^* = \sup_{|s-\frac{1}{k}| \leq \frac{1-\beta^*}{k}} |\widetilde{H}_\chi(s)|$. This yields $\lim_{\delta \to 0+} |I_8| = 0$, because $\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}}) < 1$ whenever $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$. □

Now in case 3, we let $\delta_1 \downarrow 0$ in (4.70) and invoke the relevant assertions of Proposition 4.6.5 to obtain $\sum_{n \leq X} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),Q)=1} \ll X^{1/k} \exp(-\kappa_1 \sqrt{\log X})$ for some constant $\kappa_1 > 0$. Hence to complete the proof of Theorem 4.4.5, it suffices to assume that $(\alpha_k(Q), c_{\widehat{\chi}}) \neq (1,1)$. In case 1, we obtain, by letting $\delta \downarrow 0$ and $\delta_1 \downarrow 0$ in (4.70),

$$\sum_{n \leq X} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),Q)=1}$$
$$= -\lim_{\delta \to 0+} \frac{I_7 + \overline{I_7}}{2\pi i} + O(X^{1/k} \exp(-\kappa_1 \sqrt{\log X})). \quad (4.73)$$

By an argument analogous to that given for Proposition 4.6.5(ii), it is easy to see that the above limit exists. Furthermore, writing $(s-1/k)^{-\alpha_k(Q)c_{\widehat{\chi}}} = (1/k-s)^{-\alpha_k(Q)c_{\widehat{\chi}}}\, e^{\pm i\pi\alpha_k(Q)c_{\widehat{\chi}}}$

as before, we see that the limit in (4.73) is equal to

$$\frac{\sin(\pi\alpha_k(Q)c_{\widehat{\chi}})}{\pi}\int_{\beta^*/k}^{1/k} H_\chi(s)G_{\chi,2}(s)X^s\left(\frac{1}{k}-s\right)^{-\alpha_k(Q)c_{\widehat{\chi}}}\mathrm{d}s,$$

We write the above integral as $H_\chi(1/k)G_{\chi,2}(1/k)I_1 - I_2$, where

$$I_1 \coloneqq \int_{\beta^*/k}^{1/k} X^s(1/k-s)^{-\alpha_k(Q)c_{\widehat{\chi}}}\,\mathrm{d}s.$$

Letting $s = 1/k - u/\log X$, and using $\beta^* = 2/3 + \beta_e/3 \le 1 - c(\epsilon_1)/3(\log X)^{\epsilon_1/20}$ along with Lemma 4.6.2(ii) we get

$$I_1 = \frac{X^{1/k}}{(\log X)^{1-\alpha_k(Q)c_{\widehat{\chi}}}}\left\{\Gamma(1-\alpha_k(Q)c_{\widehat{\chi}}) + O(\exp(-\sqrt{\log X}))\right\}.$$

Now using Proposition 4.6.3(iv) and making the same change of variable, we find that

$$\begin{aligned} I_2 &\ll (\log X)^{\left(\frac{1}{20}+\frac{\alpha_k(Q)}{5}\right)\epsilon_1}\int_{\beta^*/k}^{1/k} X^s\left(\frac{1}{k}-s\right)^{1-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})}\mathrm{d}s \\ &\ll \frac{X^{1/k}}{(\log X)^{2-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})-(1/20+\alpha_k(Q)/5)\epsilon_1}} \end{aligned} \tag{4.74}$$

as $\Gamma(2-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})) \ll 1$. Collecting estimates, we obtain from (4.73),

$$\begin{aligned} &\sum_{n\le X}\mathbb{1}_{(f(n),Q)=1}\prod_{i=1}^{K}\chi_1(f_1(n)) \\ &\qquad = \frac{H_\chi(1/k)G_{\chi,2}\,(1/k)}{\Gamma(\alpha_k(Q)c_{\widehat{\chi}})}\cdot\frac{X^{1/k}}{(\log X)^{1-\alpha_k(Q)c_{\widehat{\chi}}}}\Big(1+O(\exp(-\sqrt{\log X}))\Big) \\ &\qquad\qquad + O\left(\frac{X^{1/k}}{(\log X)^{2-\alpha_k(Q)\mathrm{Re}(c_{\widehat{\chi}})-(1/20+\alpha_k(Q)/5)\epsilon_1}}\right), \end{aligned} \tag{4.75}$$

by the reflection formula for the Gamma function and as $\Gamma(z) \gg 1$ for all z with $|z| \le 2$.

If $c_{\widehat{\chi}} \neq 1$, then $\mathrm{Re}(c_{\widehat{\chi}}) \leq \cos(2\pi/\varphi(Q_0)) < 1 - \epsilon_1$. Lemma 4.6.1(iii) and Proposition 4.6.3(i) yield

$$\begin{aligned}\sum_{n\leq X} \mathbb{1}_{(f(n),Q)=1} \prod_{i=1}^{K} \chi_1(f_1(n)) &\ll \frac{X^{1/k}}{(\log X)^{1-\alpha_k(Q)(\mathrm{Re}(c_{\widehat{\chi}})+\epsilon_1/5)}} \\ &\ll \frac{X^{1/k}}{(\log X)^{1-\alpha_k(Q)(1-\delta_0)}},\end{aligned}$$

with $\delta_0 \coloneqq \delta_0(\lambda) \coloneqq \min\{3\epsilon_1/4, 1-\epsilon_1/2\}$. On the other hand, if $c_{\widehat{\chi}} = 1$, then since $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$, we must have $G_{\chi,2}(1/k) = 0$ (as observed before (4.70)). Hence, (4.75) yields

$$\begin{aligned}\sum_{n\leq X} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),Q)=1} &\ll \frac{X^{1/k}}{(\log X)^{2-\alpha_k(Q)-(1/20+\alpha_k(Q)/5)\epsilon_1}} \\ &\ll \frac{X^{1/k}}{(\log X)^{1-\alpha_k(Q)(1-\delta_0)}},\end{aligned}$$

completing the proof of Theorem 4.4.5 in case 1.

Finally in case 2, (4.70) and Proposition 4.6.5 lead to the following analogue of (4.73):

$$\begin{aligned}&\sum_{n\leq X} \chi_1(f_1(n)) \cdots \chi_K(f_K(n)) \mathbb{1}_{(f(n),Q)=1} \\ &\qquad = -\lim_{\delta\to 0+} \frac{I_4^* + \overline{I_4^*}}{2\pi i} + O(X^{1/k} \exp(-\kappa_0 \sqrt{\log X})). \quad (4.76)\end{aligned}$$

An argument entirely analogous to the one given above leads to the sharper variant of (4.75) with the $\exp(-\sqrt{\log X})$ replaced by $\exp\left(-\frac{c_1 \log X}{8kK_0 \log_2 X}\right)$, completing the proof of Theorem 4.4.5.

This finally concludes the proof of Theorem 4.3.2. In order to establish Theorems 4.1.1 to 4.1.3, we thus need to appropriately bound the contributions of inconvenient

n's considered in the respective theorems. We take this up in the next several sections.

Section 4.7

Equidistribution to restricted moduli: Proof of Theorem 4.1.1

By Theorem 4.3.2, it remains to show that

$$\sum_{\substack{n\le x \text{ inconvenient}\\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 \;=\; o\bigg(\frac{1}{\varphi(q)^K}\sum_{\substack{n\le x\\ (f(n),q)=1}} 1\bigg) \quad \text{as} \quad x\to\infty, \tag{4.77}$$

uniformly in coprime residues $(a_i)_{i=1}^K$ to k-admissible moduli $q \le (\log x)^{K_0}$, under any one of the conditions (i)-(iii) of Theorem 4.1.1.

To show this, we set $z := x^{1/\log_2 x}$ and recall that, by (4.10), (4.5) and (4.3), the n's that are either z-smooth or divisible by the $(k+1)$-th power of a prime exceeding y give negligible contribution to the left hand side of (4.77) in comparison to the right hand side. The remaining n can be written in the form mP^k, where $P := P(n) > z$, $P_{Jk}(m) \le y$, m is not divisible by the $(k+1)$-th power of a prime exceeding y, and $\gcd(m,P)=1$, so that $f_i(n) = f_i(m)W_{i,k}(P)$. Given m, the number of possible P is, by the Brun-Titchmarsh inequality,

$$\ll \frac{V''_{1,q}}{\varphi(q)}\cdot\frac{(x/m)^{1/k}}{\log(z/q)} \ll \frac{V''_{1,q}}{\varphi(q)}\cdot\frac{x^{1/k}\log_2 x}{m^{1/k}\log x},$$

where $V''_{1,q} := \max\Big\{\#\mathcal{V}^{(k)}_{1,K}\big(q;(w_i)_{i=1}^K\big) :\ (w_i)_{i=1}^K \in U_q^K\Big\}$. Summing this over possible m, we get

$$\sum_{\substack{n\leq x \text{ inconvenient}\\ P(n)>z;\ p>y \Longrightarrow p^{k+1}\nmid n\\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 \ \ll\ \frac{V''_{1,q}}{\varphi(q)}\cdot\frac{x^{1/k}}{(\log x)^{1-\alpha_k\epsilon/2}}\exp\left(O((\log_3 x)^2+(\log_2(3q))^{O(1)})\right)$$

via (4.12). By Proposition 4.2.1, the quantity on the right hand side above is negligible compared to the right hand side of (4.77) whenever $q^{K-1}V''_{1,q}\ll(\log x)^{(1-2\epsilon/3)\alpha_k}$. But this does hold under any one of conditions (i)-(iii) in the statement of Theorem 4.1.1, because:

(i) $V''_{1,q}\ll 1$ if at least of one of $\{W_{i,k}\}_{1\leq i\leq K}$ is linear.

(ii) $V''_{1,q}\ll D_{\min}^{\omega(q)}$ if q is squarefree, since $\#\mathcal{V}_{1,K}^{(k)}(\ell;(w_i)_{i=1}^K)\leq D_{\min}$ for all $\ell\gg 1$.

(iii) $V''_{1,q}\ll q^{1-1/D_{\min}}$ by Lemma 2.5.2.

This establishes (4.77), completing the proof of Theorem 4.1.1. □

4.7.1. Optimality in the ranges of q in Theorem 4.1.1.

In all our examples below, $\{W_{i,k}\}_{i=1}^K\subset\mathbb{Z}[T]$ will be nonconstant with $\prod_{i=1}^K W_{i,k}$ separable over $\mathbb{Q}$. Then $\beta(W_{1,k},\dots,W_{K,k})=1$, guaranteeing that any integer satisfies $IFH(W_{1,k},\dots,W_{K,k};1)$. We claim that 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 q 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 q. Indeed, viewing a character of U_q^K as a tuple of characters mod q,[8] the condition (1.9) becomes vacuously true whenever $\mathcal{T}_k(q):=\{(W_{1,k}(u),\cdots,W_{K,k}(u))\in U_q^K\ :\ u\in U_q\}$ generates the group U_q^K. Now under the canonical isomorphism

[8]Here U_q^K is the direct product of U_q taken K times.

$U_q^K \to \prod_{\ell^e \| q} U_{\ell^e}^K$, the set $\mathcal{T}_k(q)$ maps to $\prod_{\ell^e \| q} \mathcal{T}_k(\ell^e)$. Thus by [49, Lemma 5.13], [9] if $\mathcal{T}_k(q)$ does not generate U_q^K, then there is some $\ell^e \parallel q$ and some tuple of characters $(\psi_1, \cdots, \psi_K) \neq (\chi_{0,\ell}, \ldots, \chi_{0,\ell}) \bmod \ell^e$ for which $\prod_{i=1}^K \psi_i(W_{i,k}(u))$ is constant on the set $R_k(\ell^e)$. Our claim now follows from Lemma 1.3.18.

Fix any $k \in \mathbb{N}$. Let $\widetilde{C}_0 > \max\{\widetilde{C}, 4KD\}$ be any constant depending only on the polynomials $\{W_{i,k}\}_{1 \le i \le K}$, which also exceeds the size of the leading coefficient and (nonzero) discriminant of $\prod_{i=1}^K W_{i,k}$. Then by Theorem 1.3.11, $f_1, \ldots, f_K$ are jointly weakly equidistributed modulo any (fixed) $\widetilde{C}_0$-rough k-admissible integer. Fix a prime $\ell_0 > \widetilde{C}_0$, and consider any nonconstant polynomials $\{W_{i,v}\}_{\substack{1 \le i \le K \\ 1 \le v \le k-1}} \subset \mathbb{Z}[T]$ all of whose coefficients are divisible by ℓ_0, so that $\alpha_v(\ell_0) = 0$ for each $v < k$. Our moduli q will have $P^-(q) = \ell_0$, so that $\alpha_v(q) = 0$ for all $v < k$. In each example below, we will show that $\alpha_k(q) \neq 0$, so that q is k-admissible and lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$ by definition of $\widetilde{C}_0$. The constant K_0 (in the assumption $q \le (\log x)^{K_0}$) is taken large enough in terms of $\{W_{i,k}\}_{i=1}^K$.

Optimality under condition (i). We show that for any $K \ge 2$, the range of q in Theorem 4.1.1(i) is optimal, – even if *all* of $W_{1,k}, \ldots, W_{K,k}$ are assumed to be linear, for *any* choice of (pairwise coprime) linear functions. Indeed, consider $W_{i,k}(T) \coloneqq c_i T + b_i \in \mathbb{Z}[T]$ for nonzero integers c_i and integers b_i satisfying $b_i/c_i \neq b_j/c_j$ for all $i \neq j$. Then $\prod_{i=1}^K W_{i,k}$ is clearly separable in $\mathbb{Q}[T]$. Choose a nonzero integer b such that $\prod_{i=1}^K (c_i b + b_i) \neq 0$. Let $\widetilde{C}_0 > \max\{|b|, |c_i b + b_i| : 1 \le i \le K\}$ be any constant satisfying the aforementioned requirements, so that any q with $P^-(q) = \ell_0 > \widetilde{C}_0$ is coprime to b and to $\prod_{i=1}^K W_{i,k}(b) = \prod_{i=1}^K (c_i b + b_i)$. Thus $\alpha_k(q) \neq 0$ and $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$. Now any prime $P \le x^{1/k}$ satisfying $P \equiv b \pmod q$ also satisfies

[9] This is a fact from finite group theory which states that if $A_1, \ldots, A_m$ are finite abelian groups, and if R_j is a nonempty subset of A_j for each $j \in [m]$, then $\prod_{j=1}^m R_j$ does not generate $\prod_{j=1}^m A_j$ if and only if there exist characters ψ_j of A_j, not all trivial, such that each ψ_j takes a constant value c_j on R_j, with $c_1 \ldots c_m = 1$.

$f_i(P^k) = W_{i,k}(P) \equiv c_i b + b_i \pmod q$ for all $i \in [K]$. The Siegel–Walfisz Theorem thus shows that there are $\gg x^{1/k}/\varphi(q)\log x$ many $n \le x$ satisfying $f_i(n) \equiv c_i b + b_i \pmod q$ for all $i \in [K]$. By Proposition 4.2.1, this last expression grows strictly faster than $\varphi(q)^{-K}\#\{n \le x : (f(n), q) = 1\}$ as soon as $q \ge (\log x)^{(1+\epsilon)\alpha_k/(K-1)}$ for any fixed $\epsilon \in (0,1)$, showing that the range of q in Theorem 4.1.1 under condition (i) is essentially optimal. Note that with $Y \in [2(1+\epsilon)\log_2 x/(K-1), (K_0/2)\log_2 x]$, the squarefree integer $q := \prod_{\ell_0 \le \ell \le Y} \ell$ satisfies all desired conditions; in particular $(\log x)^{(1+\epsilon)/(K-1)} \le q \le (\log x)^{K_0}$ and $P^-(q) = \ell_0$.

Optimality under condition (ii). To show that the range of squarefree q in Theorem 4.1.1(ii) is optimal, we define $W_{i,k}(T) := \prod_{1\le j\le d}(T-2j) + 2(2i-1) \in \mathbb{Z}[T]$ for some fixed $d > 1$. Eisenstein's criterion at the prime 2 shows that each $W_{i,k}$ is irreducible in $\mathbb{Q}[T]$, and the distinct $W_{i,k}$'s differ by a constant, making $\prod_{i=1}^K W_{i,k}$ separable over $\mathbb{Q}$. Now $2 \in U_q$, and $W_{i,k}(2) = 2(2i-1) \le 2(2K-1) < 4KD < \widetilde{C}_0 < P^-(q)$ for each $i \in [K]$. Thus, $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$ and $(2(2i-1))_{i=1}^K \in U_q^K$. Further, any prime P satisfying $\prod_{1\le j\le d}(P-2j) \equiv 0 \pmod q$ also satisfies $f_i(P^k) = W_{i,k}(P) \equiv 2(2i-1) \pmod q$ for each i. Since $2d = 2\deg W_{i,k} < 4KD < P^-(q)$, we see that $2, 4, \ldots, 2d$ are all distinct coprime residues modulo each prime dividing q, whereupon it follows that the congruence $\prod_{1\le j\le d}(v-2j) \equiv 0 \pmod q$ has exactly $d^{\omega(q)}$ distinct solutions $v \in U_q$ for squarefree q. Hence, there are $\gg \frac{d^{\omega(q)}}{\varphi(q)} \cdot \frac{x^{1/k}}{\log x}$ many primes $P \le x^{1/k}$ satisfying $f_i(P^k) \equiv 2(2i-1) \pmod q$ for all i, so there are also at least as many $n \le x$ for which all $f_i(n) \equiv 2(2i-1) \pmod q$. The last expression grows strictly faster than $\varphi(q)^{-K}\#\{n \le x : (f(n), q) = 1\}$ as soon as $q^{K-1}D_{\min}^{\omega(q)} = q^{K-1}d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$ for any fixed $\epsilon > 0$, showing that the range of q in Theorem 4.1.1(ii) is essentially optimal.

Note that it is possible to construct squarefree $q \le (\log x)^{K_0}$ satisfying the much

stronger requirement that $d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$ (and $P^-(q) = \ell_0$). Indeed, let $q \coloneqq \prod_{\ell_0 \le \ell \le Y} \ell$ for some $Y \le (K_0/2)\log_2 x$. Then $\omega(q) = \sum_{\ell_0 \le \ell \le Y} 1 \ge Y/2\log Y$. On the other hand, by the Chinese Remainder Theorem and the Prime Ideal Theorem, $\alpha_k(q) \le \kappa'/\log Y$ for some constant $\kappa' \coloneqq \kappa'(W_{1,k}, \dots, W_{K,k}; \ell_0)$. So we need only choose any

$$Y \in (4\kappa' \log_2 x/\log d, (K_0/2)\log_2 x)$$

in order to have $q \le (\log x)^{K_0}$ and $d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$.

For future reference, we observe that any n of the form P^k with P a prime exceeding q satisfies $P_k(n) > q$. Hence in the above setting, we have shown the stronger lower bound

$$\sum_{\substack{n \le x:\ P_k(n) > q \\ (\forall i)\ f_i(n) \equiv 2(2i-1) \pmod q}} 1 \ \ge \sum_{\substack{q < P \le x^{1/k} \\ \prod_{1 \le j \le d}(P-2j) \equiv 0 \pmod q}} 1 \ \gg \ \frac{d^{\omega(q)}}{\varphi(q)} \cdot \frac{x^{1/k}}{\log x}. \tag{4.78}$$

Optimality under condition (iii). Fix $d > 1$ and define $W_{i,k}(T) \coloneqq (T-1)^d + i \in \mathbb{Z}[T]$, so that $\prod_{i=1}^K W_{i,k}(T+1) = \prod_{i=1}^K (T^d + i)$ is clearly separable in $\mathbb{Q}[T]$, hence so is $\prod_{i=1}^K W_{i,k}(T)$. Let $q \coloneqq Q^d$ for some $Q \le (\log x)^{K_0/d}$ satisfying $P^-(Q) = \ell_0$. Then $1 \in R_k(q)$, showing that $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$. Moreover, $i \in U_q$ for each $i \in [K]$, and any prime $P \equiv 1 \pmod Q$ satisfies $f_i(P^k) = W_{i,k}(P) = (P-1)^d + i \equiv i \pmod q$. Consequently, there are $\gg x^{1/k}/q^{1/d}\log x$ many $n \le x$ satisfying $f_i(n) \equiv i \pmod q$ for all i, and this last expression grows strictly faster than $\varphi(q)^{-K}\#\{n \le x : (f(n), q) = 1\}$ as soon as $q^{K-1/D_{\min}} = q^{K-1/d} \ge (\log x)^{(1+\epsilon)\alpha_k}$ for some fixed $\epsilon \in (0,1)$. This establishes that the range of q in condition (iii) of Theorem 4.1.1 is optimal, and concrete examples of moduli q satisfying the conditions imposed so far, are those of the form Q^d, with Q lying in $[(\log x)^{(1+\epsilon)(K-1/d)^{-1}/d}, (\log x)^{K_0/d}]$ and having least prime factor ℓ_0.

Section 4.8

Restricted inputs to general moduli: Proof of Theorem 4.1.2

Fix $T \in \mathbb{N}_{>1}$. By Proposition 4.3.1 and the fact that $P_{Jk}(n) \leq P_T(n)$, it is immediate that

$$\sum_{\substack{n \leq x:\ P_T(n) \leq q \\ \gcd(f(n),q)=1}} 1 \quad = o\Bigg(\sum_{\substack{n \leq x \\ \gcd(f(n),q)=1}} 1 \Bigg). \tag{4.79}$$

In Theorems 4.1.2 and 4.1.3, we may assume q to be sufficiently large, for otherwise these results follow directly from Theorem 1.3.11 and (4.79). The latter formula also shows the equality of the second and third expressions in (4.1), so it remains to show the first equality in either. Recall that for this theorem, we have $\epsilon \coloneqq 1$ and $y = \exp(\sqrt{\log x})$ in the framework developed in section 4.3. Now any convenient n has $P_{Jk}(n) > y$ and hence is counted in the left hand side of (4.1). By Theorem 4.3.2, it suffices to show that the contributions of the inconvenient n to the left hand sides of (4.1) are negligible compared to $\varphi(q)^{-K}\#\{n \leq x : (f(n), q) = 1\}$. In fact, by (4.10) and (4.5), it remains to show (4.80) below to establish Theorem 4.1.2:

$$\sum\nolimits^{*}_{n:\ P_R(n)>q} 1 \quad \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}. \tag{4.80}$$

Here and in the rest of the chapter, any sum of the form $\sum_n^*$ denotes a sum over positive integers $n \leq x$ that are not z-smooth, not divisible by the $(k+1)$-th power of a prime exceeding y, have $P_{Jk}(n) \leq y$ 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.

Defining $\omega_{\|}(n) \coloneqq \#\{p > q : p^k \parallel n\}$ and $\omega^*(n) \coloneqq \#\{p > q : p^{k+1} \mid n\}$, we first show

the following three bounds:

$$\sum\nolimits^*_{n:\ \omega_{\|}(n)\geq KD+1} 1,\quad \sum\nolimits^*_{\substack{n:\ \omega_{\|}(n)=KD\\ \omega^*(n)\geq 1}} 1,\quad \sum_{\substack{n\leq x:\ (f(n),q)=1\\ \omega^*(n)\geq Kk,\ P_{Jk}(n)\leq y,\ P(n)>z\\ p>y\implies p^{k+1}\nmid n}} 1 \ll \frac{x^{1/k}}{\varphi(q)^K(\log x)^{1-2\alpha_k/3}}. \quad (4.81)$$

Any n counted in the first sum is of the form $m(P_{KD+1}\cdots P_1)^k$, where $P_{Jk}(m)\leq y$, where $P_1,\dots,P_{KD+1}$ are primes exceeding q satisfying $P_1 \coloneqq P(n) > z$ and $q < P_{KD+1} < \cdots < P_1$, and where $f_i(n) = f_i(m)\prod_{j=1}^{KD+1} f_i(P_j^k) = f_i(m)\prod_{j=1}^{KD+1} W_{i,k}(P_j)$. The conditions $f_i(n)\equiv a_i \pmod q$ can be rewritten as

$$(P_1,\dots,P_{KD+1}) \bmod q \ \in\ \mathcal{V}^{(k)}_{KD+1,K}\big(q;(a_if_i(m)^{-1})_{i=1}^K\big).$$

Given m, $(v_1,\dots,v_{KD+1})\in\mathcal{V}^{(k)}_{KD+1,K}\big(q;(a_if_i(m)^{-1})_{i=1}^K\big)$, and $P_2,\dots,P_{KD+1}$, the number of P_1 in $(q,\, x^{1/k}\big/m^{1/k}P_2\cdots P_{KD+1}]$ satisfying $P_1\equiv v_1 \pmod q$ is

$$\ll x^{1/k}\log_2 x\big/m^{1/k}P_2\cdots P_{KD+1}\varphi(q)\log x,$$

by Brun-Titchmarsh. We sum this over all possible $P_2,\dots,P_{KD+1}$, making use of the bound $\sum_{\substack{q<p\leq x\\ p\equiv v \pmod q}} 1/p \ll \log_2 x\big/\varphi(q)$ uniformly in $v\in U_q$ (which can be seen by Brun–Titchmarsh and partial summation). We deduce 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

$$\sum_{\substack{q<P_{KD+1}<\cdots<P_2\leq x\\ (\forall j)\ P_j\equiv v_j \pmod q}}\ \sum_{\substack{z<P_1\leq x^{1/k}\big/m^{1/k}P_2\cdots P_{KD+1}\\ P_1\equiv v_1 \pmod q}} 1 \ \ll\ \frac{1}{\varphi(q)^{KD+1}}\cdot\frac{x^{1/k}(\log_2 x)^{O(1)}}{m^{1/k}\log x}. \quad (4.82)$$

Define $V'_{r,K} \coloneqq \max\Big\{\#\mathcal{V}^{(k)}_{r,K}\big(q;(w_i)_{i=1}^K\big) : w_1,\dots,w_K\in U_q\Big\}$. Summing (4.82) over all

$(v_1, \dots, v_{KD+1}) \in \mathcal{V}^{(k)}_{KD+1,K}\big(q; (a_i f_i(m)^{-1})_{i=1}^K\big)$ and then over all m via (4.12) shows that

$$\sum\nolimits^*_{n:\ \omega_\parallel(n)\ge KD+1} 1 \tag{4.83}$$

$$\ll \frac{V'_{KD+1,K}}{\varphi(q)^{KD+1}} \cdot \frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}} \cdot \exp\big(O\big((\log_3 x)^2 + (\log_2(3q))^{O(1)}\big)\big)\,. \tag{4.84}$$

Applying (4.16) with $N \coloneqq KD+1$, we get

$$\begin{aligned} V'_{KD+1,K}/\varphi(q)^{KD+1} &\ll \varphi(q)^{-K} \prod_{\ell\mid q}(1+O(\ell^{-1/D})) \\ &\ll \varphi(q)^{-K} \exp\big(O((\log q)^{1-1/D})\big). \end{aligned}$$

This yields the first bound in (4.81).

Next, any n counted in the second sum in (4.81) can be written as $mp^c(P_{KD}\cdots P_1)^k$ for some m, c and distinct primes $p, P_1, \dots, P_{KD}$ exceeding q, which satisfy the conditions $P_1 = P(n) > z$, $q < P_{KD} < \cdots < P_1$, $P_{Jk}(m) \le y$, $c \ge k+1$ and $f_i(n) = f_i(m)f_i(p^c)\prod_{j=1}^{KD} W_{i,k}(P_j)$, so that $(P_1, \dots, P_{KD}) \bmod q \in \mathcal{V}^{(k)}_{KD,K}\big(q; (a_i f_i(mp^c)^{-1})_{i=1}^K\big)$. Given m, p, c and $(v_1, \dots, v_{KD}) \in \mathcal{V}^{(k)}_{KD,K}\big(q; (a_i f_i(mp^c)^{-1})_{i=1}^K\big)$, the arguments leading to (4.82) 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 $\ll x^{1/k}(\log_2 x)^{O(1)} \Big/ \varphi(q)^{KD} m^{1/k} p^{c/k} \log x$. Summing this successively over all $(v_1, \dots, v_{KD})$, $c \ge k+1$, $p > q$ and all possible m, shows that the second of the three sums in (4.81) is

$$\ll \frac{V'_{KD,K}}{q^{1/k}\varphi(q)^{KD}} \cdot \frac{x^{1/k}}{(\log x)^{1-2\alpha_k/3}}.$$

(Here we have noted that $\sum_{p>q,\ c\ge k+1} p^{-c/k} \ll \sum_{p>q} p^{-1-1/k} \ll q^{-1/k}$.) By (4.17), we have $V'_{KD,K} \Big/ q^{1/k}\varphi(q)^{KD} \ll 1/q^K$, proving the second inequality in (4.81).

Lastly, any n counted in the third sum in (4.81) still has $P(n) > z$ and $P(n)^k \parallel q$, and thus can be written in the form $mp_1^{c_1} \cdots p_{Kk}^{c_{Kk}} P^k$ for some distinct primes $p_1, \dots, p_{Kk}, P$ exceeding q and some integers $m, c_1, \dots, c_{Kk}$, which satisfy $P = P(n) > z$, $P_{Jk}(m) \leq y$, $c_j \geq k+1$ for all $j \in [Kk]$, and $\gcd(f(m), q) = 1$. Given $m, p_1, \dots, p_{Kk}, c_1, \dots, c_{Kk}$, the number of possible $P > z$ satisfying $P^k \leq x/mp_1^{c_1} \cdots p_{Kk}^{c_{Kk}}$ is

$$\ll x^{1/k} \big/ (mp_1^{c_1} \cdots p_{Kk}^{c_{Kk}})^{1/k} \log z.$$

Summing this over all $c_1, \dots, c_{Kk} \geq k+1$, and then over all $p_1, \dots, p_{Kk}, m$, shows the third bound in (4.81).

In the rest of the argument, R as in the statement of the theorem is the least integer exceeding

$$\max\left\{k(KD+1)-1, k\left(1+(k+1)\left(K-\frac{1}{D}\right)\right)\right\} = \begin{cases} k(KD+1)-1, & \text{if } k < D \\ k\left(1+(k+1)\left(K-1/D\right)\right) & \text{if } k \geq D. \end{cases}$$

Since q is sufficiently large, the q-rough part of any n satisfying $\gcd(f(n), q) = 1$ is k-full (by Lemma 4.2.3). As such, any n with $\omega^*(n) = 0$ counted in (4.80) must have $\omega_{\parallel}(n) \geq \lfloor R/k \rfloor \geq KD+1$, and hence is counted in the first sum in (4.81). Moreover, any n with $\omega_{\parallel}(n) = KD$ counted in (4.80) must also have $\omega^*(n) \geq R - k\omega_{\parallel}(n) \geq k(KD+1) - kKD \geq 1$, and hence is counted in the second sum in (4.81). By (4.81), it thus remains to show that the contribution of n having $\omega_{\parallel}(n) \in [KD-1]$ and $\omega^*(n) \in [Kk-1]$ to the left hand side of (4.80) is absorbed in the right hand side. This would follow once we show that for any fixed $r \in [KD-1]$ and $s \in [Kk-1]$, the contribution $\Sigma_{r,s}$ of all n with $\omega_{\parallel}(n) = r$ and $\omega^*(n) = s$ to the left hand side of

(4.80) is absorbed in the right hand side.

Now any n counted in $\Sigma_{r,s}$ is of the form $mp_1^{c_1}\cdots p_s^{c_s}P_1^k\cdots P_r^k$ for some distinct primes $p_1,\dots,p_s$, $P_1,\dots,P_r$ and integers $m,c_1,\dots,c_s$, which satisfy the following conditions:

(i) $P(m)\le q$;

(ii) $P_1 \coloneqq P(n) > z$; $q < P_r < \cdots < P_1$;

(iii) $p_1,\dots,p_s > q$;

(iv) $c_1,\dots,c_s \ge k+1$ and $c_1+\cdots+c_s \ge R-kr$;

(v) m, $p_1,\dots,p_s,P_1,\dots,P_r$ are all pairwise coprime, so that

$$f_i(n) = f_i(m)f(p_1^{c_1})\cdots f(p_s^{c_s})\prod_{j=1}^{r} W_{i,k}(P_j)$$

for each $i\in[K]$.

Here, property (i) holds because the q-rough part of any n satisfying $\gcd(f(n),q)=1$ is k-full, whereas $\omega_{\|}(n)=r$, $\omega^*(n)=s$.

With $\tau_i \coloneqq \min\{c_i, R-kr\}$, it is easy to see that the integers $\tau_1,\dots,\tau_s\in[k+1,R-kr]$ satisfy $\tau_1\le c_1,\dots,\tau_s\le c_s$ and $\tau_1+\cdots+\tau_s\ge R-kr$. (Here it is important that $R\ge k(KD+1)$, $r\le KD-1$ and $c_1+\cdots+c_s\ge R-kr$.) Turning this around, we find that

$$\Sigma_{r,s} \le \sum_{\substack{\tau_1,\dots,\tau_s\in[k+1,R-kr]\\ \tau_1+\cdots+\tau_s\ge R-kr}} \mathcal{N}_{r,s}(\tau_1,\dots,\tau_s), \tag{4.85}$$

where $\mathcal{N}_{r,s}(\tau_1,\dots,\tau_s)$ denotes the contribution of all n counted in (4.80) which can be written in the form $mp_1^{c_1}\cdots p_s^{c_s}P_1^k\cdots P_r^k$ for some distinct primes $p_1,\dots,p_s,P_1,\cdots,P_r$ and integers $m,c_1,\dots,c_s$ satisfying the conditions (i)-(v) above, along with

the condition $c_1 \geq \tau_1, \dots, c_s \geq \tau_s$. We will show that for each tuple $(\tau_1, \dots, \tau_s)$ occurring in (4.85), we have

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ \ll \ \frac{x^{1/k}(\log_2 x)^{O(1)}}{q^K \log x}. \tag{4.86}$$

Consider an arbitrary such tuple $(\tau_1, \dots, \tau_s)$, and write n in the form $mp_1^{c_1} \cdots p_s^{c_s} P_1^k \cdots P_r^k$ as above. The conditions $f_i(n) \equiv a_i \pmod q$ lead to

$$(P_1, \dots, P_r) \bmod q \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1} \cdots p_s^{c_s})^{-1})_{i=1}^K\big).$$

Given $m, p_1, \dots, p_s, c_1, \dots, c_s$ and

$$(v_1, \dots, v_r) \in \mathcal{V}_{r,K}^{(k)}\big(q; (a_i f_i(mp_1^{c_1} \cdots p_s^{c_s})^{-1})_{i=1}^K\big),$$

the arguments leading to (4.82) show that the number of possible $P_1, \dots, P_r$ satisfying $P_j \equiv v_j \bmod q$ for each $j \in [r]$, is

$$\ll x^{1/k}(\log_2 x)^{O(1)} \Big/ \varphi(q)^r m^{1/k} p_1^{c_1/k} \cdots p_s^{c_s/k} \log x.$$

With $V'_{r,K} = \max_{(w_i)_i \in U_q^K} \#\mathcal{V}_{r,K}^{(k)}\big(q; (w_i)_{i=1}^K\big)$ as before, the bounds $\sum_{p_i > q:\ c_i \geq \tau_i} p_i^{-c_i/k} \ll q^{-(\tau_i/k - 1)}$ yield

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{1}{q^{(\tau_1 + \dots + \tau_s)/k - s}} \, \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \sum_{\substack{m \leq x:\ P(m) \leq q \\ \gcd(f(m), q) = 1}} \frac{1}{m^{1/k}}. \tag{4.87}$$

Proceeding as in the argument for (4.12), we write any m in the above sum as BM

where B is k-free and M is k-full, so that $B = O(1)$ and $P(M) \leq q$. We find that

$$\sum_{\substack{m \leq x:\ P(m) \leq q \\ \gcd(f(m),q)=1}} \frac{1}{m^{1/k}} \ll \sum_{\substack{M \leq x:\ P(M) \leq q \\ M \text{ is } k\text{-full}}} \frac{1}{M^{1/k}} \leq \prod_{p \leq q} \left(1 + \frac{1}{p} + O\left(\frac{1}{p^{1+1/k}}\right)\right)$$
$$\ll \exp\left(\sum_{p \leq q} \frac{1}{p}\right) \ll \log q. \tag{4.88}$$

Inserting this into (4.87), we obtain

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{1}{q^{(\tau_1+\dots+\tau_s)/k-s}} \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}. \tag{4.89}$$

Now since $1 \leq r \leq KD - 1$, an application of (4.17) with $N := r$ now yields

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{\exp\big(O(\omega(q))\big)}{q^{(\tau_1+\dots+\tau_s)/k-s+r/D}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \tag{4.90}$$
$$\ll \frac{\exp\big(O(\omega(q))\big)}{q^{\max\{s/k, R/k-r-s\}+r/D}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}, \tag{4.91}$$

where in the last equality we have recalled that $\tau_1, \dots, \tau_s \geq k+1$ and $\tau_1 + \dots + \tau_s \geq R - kr$.

We claim that $\max\{s/k, R/k - r - s\} + r/D > K$. This is tautological if $s/k + r/D > K$, so suppose $s/k + r/D \leq K$. Then $r \leq D(K - s/k) \leq DK - D/k$, and $s \leq k(K - r/D)$ so that $R/k - r - s + r/D \geq R/k - Kk + ((k+1)/D - 1)r$.

Now if $k < D$, then $(k+1)/D - 1 \leq 0$, so for all $1 \leq r \leq DK - D/k$, we have $R/k - Kk + ((k+1)/D - 1)r \geq R/k - Kk + ((k+1)/D - 1)(DK - D/k)$ and this exceeds K since $R \geq k(KD+1)$. If on the other hand, we had $k \geq D$, then $k+1 > D$ and the minimum value of $R/k - Kk + ((k+1)/D - 1)r$ is attained at $r = 1$, giving us $R/k - Kk + ((k+1)/D - 1)r \geq R/k - Kk + ((k+1)/D - 1)$ which also exceeds

K since $R > k\big(1 + (1+k)(K - 1/D)\big)$. This shows our claim, so that (4.90) leads to (4.86). Summing (4.86) over the $O(1)$ many possible tuples $(\tau_1, \dots, \tau_s)$ occurring in the right hand side of (4.85) yields $\Sigma_{r,s} \ll x^{1/k}(\log_2 x)^{O(1)}/q^K \log x$, which (as argued before) establishes Theorem 4.1.2.

Section 4.9

Final preparatory step for Theorem 4.1.3: Counting points on varieties

To establish Theorem 4.1.3, we will need the following partial improvements of Corollary 4.4.4. In this section, we again deviate from the general notation set up for Theorems 4.1.1 to 4.1.3, so the notation set up in this section will be relevant in this section only.

Proposition 4.9.1. *Let $F \in \mathbb{Z}[T]$ be a fixed nonconstant polynomial which is not squarefull.*

- ***(a)*** *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.*
- ***(b)*** *Let $G \in \mathbb{Z}[T]$ be any fixed polynomial such that $\{F, G\} \subset \mathbb{Z}[T]$ are multiplicatively independent. Let $\mathcal{V}_{3,2}(\ell; u, w)$ be the set of $(v_1, v_2, v_3) \in U_\ell^3$ satisfying the two congruences $F(v_1)F(v_2)F(v_3) \equiv u \pmod{\ell}$ and $G(v_1)G(v_2)G(v_3) \equiv w \pmod{\ell}$. Then $\#\mathcal{V}_{3,2}(\ell; u, w) \ll_{F,G} \varphi(\ell)$, uniformly in primes ℓ and coprime residues u, w mod ℓ.*

Our starting idea will be to look at $\mathcal{V}_{2,1}(\ell; w)$ and $\mathcal{V}_{3,2}(\ell; u, w)$ as subsets of the sets of $\mathbb{F}_\ell$-rational points of certain varieties over the algebraic closure $\overline{\mathbb{F}}_\ell$ of $\mathbb{F}_\ell$.

Proposition 4.9.2. *Let V be a variety defined over $\mathbb{F}_\ell$ and $V(\mathbb{F}_\ell) \coloneqq V \cap \mathbb{F}_\ell$.*

(a) *If V is an absolutely irreducible affine plane curve, then $\#V(\mathbb{F}_\ell) \leq \ell + O(\sqrt{\ell})$, where the implied constant depends only on the degree of V.*

(b) *Let d be the positive integer such that $V \subset (\overline{\mathbb{F}}_\ell)^d$. We have $\#V(\mathbb{F}_\ell) \ll \ell^{\dim V}$, where $\dim V$ is the dimension of V as a variety, and the implied constant depends at most on d and on the number and degrees of the polynomials defining V.*

Subpart(a) is just Proposition 2.6.1 restated for convenience, while subpart (b) is a weaker version of [22, Claim 7.2] but in fact goes back to work of Lang and Weil [39, Lemma 1]. To make use of the aforementioned results, we will be needing the following observations.

Lemma 4.9.3. *Let $F, G \in \mathbb{Z}[T]$ be fixed multiplicatively independent polynomials such that F is not squarefull. There exist constants $\kappa_0(F)$ and $\kappa_1(F, G)$ such that:*

(a) *For any $N \geq 2$, $\ell > \kappa_0(F)$ and $w \in \mathbb{F}_\ell^\times$, the polynomial $\prod_{i=1}^N F(X_i) - w$ is absolutely irreducible over $\mathbb{F}_\ell$, that is, it is irreducible in the ring $\overline{\mathbb{F}}_\ell[X_1, \ldots, X_N]$.*

(b) *For any $\ell > \kappa_1(F, G)$ and $u, w \in \mathbb{F}_\ell^\times$, the polynomial $F(X)F(Y)F(Z) - u$ is irreducible and doesn't divide the polynomial $G(X)G(Y)G(Z) - w$ in the ring $\overline{\mathbb{F}}_\ell[X, Y, Z]$.*

Proof. Write $F \coloneqq r\prod_{j=1}^M G_j^{b_j}$ for some $r \in \mathbb{Z}$, $b_j \in \mathbb{N}$, and pairwise coprime irreducibles $G_j \in \mathbb{Z}[T]$, so that by the nonsquarefullness of F in $\mathbb{Z}[T]$, we have $b_j = 1$ for some $j \in [M]$. By the observations at the start of the proof of Proposition 4.4.3, there exists a constant $\kappa_0(F)$ such that for any prime $\ell > \kappa_0(F)$, ℓ doesn't divide the leading

coefficient of F and $\prod_{j=1}^{M} G_j$ is separable in $\mathbb{F}_\ell[T]$. This forces $\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (T-\theta)^2 \nmid F(T)$ in $\overline{\mathbb{F}}_\ell[T]$.

Proof of (a). We will show that for any $\ell > \kappa_0(F)$ and $U, V \in \overline{\mathbb{F}}_\ell[X_1, \dots, X_N]$ satisfying

$$\prod_{i=1}^{N} F(X_i) - w = U(X_1, \dots, X_N)V(X_1, \dots, X_N), \tag{4.92}$$

one of U or V must be constant. First note that for any root $\theta \in \overline{\mathbb{F}}_\ell$ of F, we have $-w = U(X_1, \dots, X_{N-1}, \theta)V(X_1, \dots, X_{N-1}, \theta)$, forcing $U(X_1, \dots, X_{N-1}, \theta)$ and $V(X_1, \dots, X_{N-1}, \theta)$ to be constant in the ring $\overline{\mathbb{F}}_\ell[X_1, \dots, X_N]$. Writing

$$U(X_1, \dots, X_N) = \sum_{\substack{i_1,\dots,i_{N-1}\geq 0 \\ i_1\leq R_1,\dots,i_{N-1}\leq R_{N-1}}} u_{i_1,\dots,i_{N-1}}(X_N)\ X_1^{i_1}\cdots X_{N-1}^{i_{N-1}},$$

and

$$V(X_1, \dots, X_N) = \sum_{\substack{j_1,\dots,j_{N-1}\geq 0 \\ j_1\leq T_1,\dots,j_{N-1}\leq T_{N-1}}} v_{j_1,\dots,j_{N-1}}(X_N)\ X_1^{j_1}\cdots X_{N-1}^{j_{N-1}}$$

(where $u_{i_1,\dots,i_{N-1}}, v_{j_1,\dots,j_{N-1}} \in \overline{\mathbb{F}}_\ell[X_N]$, and neither $u_{R_1,\dots,R_{N-1}}$ nor $v_{T_1,\dots,T_{N-1}}$ is identically zero), we thus find that $u_{i_1,\dots,i_{N-1}}(\theta) = v_{j_1,\dots,j_{N-1}}(\theta) = 0$ for any $(i_1, \dots, i_{N-1}) \neq (0, \dots, 0)$, $(j_1, \dots, j_{N-1}) \neq (0, \dots, 0)$, and any θ as above. Thus, if the tuples $(R_1, \dots, R_{N-1})$ and $(T_1, \dots, T_{N-1})$ are both nonzero, then $\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (X_N - \theta)$ divides $u_{R_1,\dots,R_{N-1}}(X_N)$ and $v_{T_1,\dots,T_{N-1}}(X_N)$ in $\overline{\mathbb{F}}_\ell[X_N]$. But then, if $\alpha \in \mathbb{Z}$ is the leading coefficient of F, then comparing the monomials (in $X_1, \dots, X_{N-1}$) with maximal total degree in (4.92), we find that $\alpha^{N-1}F(X_N) = u_{R_1,\dots,R_{N-1}}(X_N)\ v_{T_1,\dots,T_{N-1}}(X_N) \equiv 0 \pmod{\prod_{\substack{\theta\in\overline{\mathbb{F}}_\ell \\ F(\theta)=0}} (X_N - \theta)^2}$, which is impossible by the observations in the first paragraph of the proof. This forces one of $(R_1, \dots, R_{N-1})$ or $(T_1, \dots, T_{N-1})$ to be $(0, \dots, 0)$, say the latter. Then $V(X_1, \dots, X_N) = v_{0,\dots,0}(X_N)$ and since $N \geq 2$, plug-

ging $X_1 \coloneqq \theta$ for some root $\theta \in \overline{\mathbb{F}}_\ell$ of F into (4.92) yields

$$-w = U(\theta, X_2, \dots, X_N) v_{0,\dots,0}(X_N),$$

forcing V to be identically constant.

Proof of (b). We claim that for all primes $\ell \gg_{F,G} 1$, if the rational function $F^a G^b$ is constant in the ring $\overline{\mathbb{F}}_\ell(T)$ for some integers a, b, then $a \equiv b \equiv 0 \pmod{\ell}$.[10] The argument for this is a simple variant of that given for the inequality "$\mathrm{ord}_\ell(\widetilde{F}) \leq \mathbb{1}_{\ell \leq C_1} C_1$" in the proof of Proposition 4.4.3(b), so we only sketch it. Since $\{F, G\} \subset \mathbb{Z}[T]$ are multiplicatively independent, the polynomials $\{F'G, FG'\} \subset \mathbb{Z}[T]$ are $\mathbb{Q}$-linearly independent, hence so are the columns of the matrix M_1 listing the coefficients of $F'G$ and FG' in two columns. Hence we can find invertible matrices P_1 and Q_1 (where Q_1 is a 2×2 matrix) such that $P_1 M_1 Q_1 = \mathrm{diag}(\beta_1, \beta_2)$ for some $\beta_1, \beta_2 \in \mathbb{Z} \setminus \{0\}$ satisfying $\beta_1 \mid \beta_2$. Let $\ell > |\beta_2|$ be any prime not dividing the leading coefficients of F, G, $F'G$ or FG'. If $F^a G^b$ is identically constant in $\mathbb{F}_\ell[T]$, then $aF'G + bFG' \equiv 0$ in $\mathbb{F}_\ell[T]$, so $M_1 (a\ b)^\top \equiv 0 \pmod{\ell}$. Hereafter, familiar calculations yield $(a\ b)^\top \equiv 0 \pmod{\ell}$.

Collecting our observations, we have shown that there exists a constant $\kappa_1(F, G)$ such that for all primes $\ell > \kappa_1(F, G)$, the following three properties hold:

(i) $\ell > \kappa_0(F)$, so that $\prod_{\substack{\theta \in \overline{\mathbb{F}}_\ell \\ F(\theta) = 0}} (T - \theta)^2 \nmid F(T)$ in $\overline{\mathbb{F}}_\ell[T]$;

(ii) ℓ doesn't divide the leading coefficient of F or G; and,

(iii) For any $a, b \in \mathbb{Z}$ for which $F^a G^b$ is identically constant in $\overline{\mathbb{F}}_\ell(T)$, we have $\ell \mid a$ and $\ell \mid b$.

[10] It is not difficult to see that this also forces $a = b = 0$, but we won't need that.

We will now show that any such constant $\kappa_1(F,G)$ satisfies the property in subpart (b) of the lemma. By subpart (a), $F(X)F(Y)F(Z)-u$ is already irreducible in $\overline{\mathbb{F}}_\ell[X,Y,Z]$ for any $u \in \mathbb{F}_\ell^\times$. Assume by way of contradiction that for some $\ell > \kappa_1(F,G)$ and $u, w \in \mathbb{F}_\ell^\times$, we have

$$G(X)G(Y)G(Z)-w = H_0(X,Y,Z)\,(F(X)F(Y)F(Z)-u) \text{ for some } H_0 \in \overline{\mathbb{F}}_\ell[X,Y,Z]. \tag{4.93}$$

Write $H_0(X,Y,Z) =: \sum_{\substack{0\le i_1\le r_1\\ 0\le i_2\le r_2}} h_{i_1,i_2}(X)Y^{i_1}Z^{i_2}$ for some $h_{i_1,i_2} \in \overline{\mathbb{F}}_\ell[X]$ with h_{r_1,r_2} not identically zero. If $(r_1,r_2) = (0,0)$, then substituting a root of F and G in place of Y and Z respectively, we see that H_0 must be a constant $\lambda_0 \in \overline{\mathbb{F}}_\ell\backslash\{0\}$ satisfying $w = \lambda_0 u$. Thus $G(X)G(Y)G(Z) = \lambda_0 F(X)F(Y)F(Z)$. Now substituting some $\eta \in \overline{\mathbb{F}}_\ell$ which is not a root of FG in place of both Y and Z leads to $F(X)G(X)^{-1} = \lambda_0^{-1}F(\eta)^{-2}G(\eta)^2$, a nonzero constant. But since $(1,-1) \not\equiv (0,0) \pmod{\ell}$, this violates condition (iii) in the definition of $\kappa_1(F,G)$. Hence $(r_1,r_2) \neq (0,0)$.

Let $\alpha, \beta \in \mathbb{Z}$ denote the leading coefficients of F and G respectively. Comparing the monomials in Y and Z of maximal total degree in (4.93) yields $\beta^2 G(X) = \alpha^2 F(X) h_{r_1,r_2}(X)$ in $\overline{\mathbb{F}}_\ell[X]$, so that (since either side of this identity is nonzero), we get $F \mid G$ in $\overline{\mathbb{F}}_\ell[X]$. Write $G = F^m H$ for some $m \geq 1$ and $H \in \overline{\mathbb{F}}_\ell[X]$ such that $F \nmid H$ in $\overline{\mathbb{F}}_\ell[X]$. An easy finite induction shows that with

$$G_t(X,Y,Z) \coloneqq F(X)^{m-t}F(Y)^{m-t}F(Z)^{m-t}H(X)H(Y)H(Z) - u^{-t}w$$

and

$$\widehat{F}(X,Y,Z) \coloneqq F(X)F(Y)F(Z) - u,$$

we have $\widehat{F} \mid G_t$ for each $t \in \{0,1,\ldots,m\}$. Indeed, the case $t = 0$ is just (4.93), and if $\widehat{F} \mid G_t$ for some $t \leq m-1$, then writing $G_t = Q_t\widehat{F}$ shows that $F(X)F(Y)F(Z)$

$\mid (Q_t(X,Y,Z) - u^{-(t+1)}w)$. With Q_{t+1} defined by

$$Q_t(X,Y,Z) - u^{-(t+1)}w = F(X)F(Y)F(Z)Q_{t+1}(X,Y,Z),$$

we obtain $G_{t+1} = Q_{t+1}\widehat{F}$ completing the induction.

Applying this last observation with $t \coloneqq m$ shows that $\widehat{F}(X,Y,Z)$ divides the polynomial $H(X)H(Y)H(Z) - u^{-m}w$ in $\overline{\mathbb{F}}_\ell[X,Y,Z]$. We claim that this forces H to be constant. Indeed if not, then letting $\gamma \in \overline{\mathbb{F}}_\ell \setminus \{0\}$ be the leading coefficient of H, [11] writing $H(X)H(Y)H(Z) - u^{-m}w = (F(X)F(Y)F(Z) - u) \sum_{\substack{0 \le i_1 \le b_1 \\ 0 \le i_2 \le b_2}} g_{i_1,i_2}(X)Y^{i_1}Z^{i_2}$ for some $g_{i_1,i_2} \in \overline{\mathbb{F}}_\ell[X]$ with $g_{b_1,b_2} \neq 0$, and comparing the monomials in Y and Z of maximal degree, we obtain $\gamma^2 H(X) = \alpha^2 F(X) g_{b_1,b_2}(X)$. This leads to $F \mid H$, contrary to hypothesis. Hence H must be constant, so the identity $F^{-m}G = H$ in $\overline{\mathbb{F}}_\ell(X)$ violates condition (iii) in the definition of $\kappa_1(F,G)$, as $(-m,1) \not\equiv (0,0) \pmod{\ell}$. This shows that $\widehat{F}$ cannot divide $G(X)G(Y)G(Z) - w$, completing the proof. □

Given a commutative ring R and an R-module M, we say that $x \in R$ is an M-regular element if x is not a zero-divisor on M, that is, if $xz = 0$ for some $z \in M$ implies $z = 0$. A sequence $x_1, \ldots, x_n$ of elements of R is said to be M-regular if x_1 is an M-regular element, each x_i is an $M/(x_1, \ldots, x_{i-1})M$-regular element, *and* $M/(x_1, \ldots, x_n)M \neq 0$. It is well-known (see [9, Proposition 1.2.14]) that for any proper ideal I in a Noetherian ring R, the height of I is at least the length of the longest R-regular sequence contained in I.

Proof of Proposition 4.9.1. With $\kappa_0(F)$ and $\kappa_1(F,G)$ as in Lemma 4.9.3, the affine plane curve $\{(X,Y) \in \overline{\mathbb{F}}_\ell^2 : \ F(X)F(Y) - w = 0\}$ is absolutely irreducible for any $\ell > \kappa_0(F)$, so that Proposition 4.9.2(a) yields Proposition 4.9.1(a). For (b), it suffices to

[11] Here $\gamma \neq 0$ in $\overline{\mathbb{F}}_\ell$ because ℓ doesn't divide the leading coefficient of $G = F^m H$.

show that for any prime $\ell > \kappa_1(F,G)$, the variety $V_\ell \subset \overline{\mathbb{F}}_\ell^3$ defined by the polynomials $\widehat{F}(X,Y,Z) \coloneqq F(X)F(Y)F(Z) - u$ and $\widehat{G}(X,Y,Z) \coloneqq G(X)G(Y)G(Z) - w$ has $\ll_{F,G}$ ℓ many $\mathbb{F}_\ell$-rational points. Consider the ideal $I(V_\ell)$ of the ring $R \coloneqq \overline{\mathbb{F}}_\ell[X,Y,Z]$ consisting of all polynomials vanishing at all the points of V_ℓ, so that $(\widehat{F},\widehat{G}) \subset I(V_\ell)$. If $I(V_\ell) = R$, then $V_\ell = \emptyset$, so suppose $I(V_\ell) \subsetneq R$. Lemma 4.9.3(b) shows that the sequence $\widehat{G}, \widehat{F} \in I(V_\ell)$ is R-regular, so by [9, Proposition 1.2.14], $I(V_\ell)$ has height at least 2. By [4, Chapter 11, Exercise 7], the Krull-dimension of R is 3. Hence the Krull-dimension of $R/I(V_\ell)$ is at most $3 - 2 = 1$ (by, say, [42, p. 31]). Thus $\dim(V_\ell) \leq 1$, and Proposition 4.9.2 completes the proof. □

Section 4.10

Restricted inputs to squarefree moduli: Proof of Theorem 4.1.3

Returning to the notation set up in the introduction, we start with the same initial reductions as in section 4.8. As such, in order to establish the theorem, it suffices to show that

$$\sum\nolimits^{*}_{n:\ P_R(n)>q} 1 \ \ll \frac{x^{1/k}}{\varphi(q)^K (\log x)^{1-2\alpha_k/3}}, \tag{4.94}$$

with the respective values of R defined in the statement. Here we again have $\epsilon = 1$ and $y = \exp(\sqrt{\log x})$ in the framework developed in section 4.3. We retain the notation $\omega_{\|}(n) = \#\{p > q : p^k \,\|\, n\}$ and $\omega^*(n) = \#\{p > q : p^{k+1} \mid n\}$ from section 4.8.

The case $K = 1$, $W_{1,k}$ not squarefull.

In this case, (4.94) would follow once we show that

$$\sum\nolimits^{*}_{n:\ P_{k+1}(n)>q} 1 \ \ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}, \tag{4.95}$$

Indeed, any n counted in (4.95) which is divisible by the $(k+1)$-th power of a prime exceeding q can be written in the form mp^cP^k for some positive integers m, c and primes p, P, satisfying $P = P(n) > z$, $q < p < P$, $c \geq k+1$, $P_{Jk}(m) \leq y$ and $f(n) = f(m)f(p^c)W_k(P)$. Recalling that $\#\{u \in U_q : W_k(u) \equiv b \pmod q\} \ll D^{\omega(q)}$ uniformly in $b \in \mathbb{Z}$, the argument given for the second bound in (4.81) shows that the contribution of such n is $\ll \frac{D^{\omega(q)}}{q^{1/k}\varphi(q)} \cdot \frac{x^{1/k}}{(\log x)^{1-2\alpha_k/3}} \ \ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}$. On the other hand, for any n counted in (4.95) which is not divisible by the $(k+1)$-th power of any prime exceeding q, the condition $P_{k+1}(n) > q$ forces $\omega_{\|}(n) \geq 2$ (again since q is sufficiently large and the q-rough part of n is k-full). Thus $n = m(P_2P_1)^k$, for some m and primes P_1, P_2 satisfying $P_1 \coloneqq P(n) > z$, $q < P_2 < P_1$, $P_{Jk}(m) \leq y$ and $f(n) = f(m)W_k(P_1)W_k(P_2)$. The arguments before (4.83) show that the contribution of such n is $\ll \frac{V'_{2,1}}{\varphi(q)^2} \cdot \frac{x^{1/k}}{(\log x)^{1-\alpha_k/2}} \exp((\log_3 x)^{O(1)})$, which is $\ll \frac{x^{1/k}}{\varphi(q)(\log x)^{1-2\alpha_k/3}}$ by Proposition 4.9.1(a).

The remaining cases

To complete the proof of Theorem 4.1.3, it thus remains to show that we may take:
(i) $R = k(Kk+K-k)+1$ if $K, k \geq 2$ and at least one of $\{W_{i,k}\}_{1\leq i\leq K}$ is not squarefull.
(ii) $R = k(Kk + K - k + 1) + 1$, in general.
We shall call (i) as "Subcase 1" and (ii) as "Subcase 2", and we shall denote $R = k(Kk + K - k + \mathbb{1}) + 1$ to mean the respective value of R in the respective subcase.

We have the following analogues of the first two bounds in (4.81), which can be shown

by replicating arguments and replacing the use of Proposition 4.3.4 by Corollary 4.4.4.

$$\sum\nolimits^{*}_{n:\ \omega_{\|}(n)\geq 2K+1} 1, \quad \sum\nolimits^{*}_{\substack{n:\ \omega_{\|}(n)=2K \\ \omega^{*}(n)\geq 1}} 1 \quad \ll \quad \frac{x^{1/k}}{\varphi(q)^{K}(\log x)^{1-2\alpha_k/3}}, \tag{4.96}$$

If $\omega^*(n) = 0$, then $k\omega_{\|}(n) \geq R \geq k(Kk + K - k + \mathbb{1}) + 1$, so that $\omega_{\|}(n) \geq Kk + K - k + \mathbb{1} + 1 \geq 2K + 1$; hence, any n with $\omega^*(n) = 0$ counted in (4.94) is automatically counted in the first sum in (4.96). Likewise, the condition $\omega_{\|}(n) = 2K$ forces $\sum_{p>q:\ p^{k+1}|n} v_p(n) \geq R - k\omega_{\|}(n) \geq k((K-1)(k-1) - 1 + \mathbb{1}) + 1 \geq 1$, so that $\omega^*(n) \geq 1$; as such, any n with $\omega_{\|}(n) = 2K$ contributing to (4.94) is counted in the second sum in (4.96). Furthermore, by the third bound in (4.81), the contribution of all n having $\omega^*(n) \geq Kk$ to the left hand side of (4.94) is absorbed in the right hand side. It thus suffices to show that for any $r \in [2K-1]$ and $s \in [Kk-1]$, the contribution $\Sigma_{r,s}$ of all n with $\omega_{\|}(n) = r$ and $\omega^*(n) = s$ to the left hand side of (4.94) is absorbed in the right hand side.

Recall that any n counted in $\Sigma_{r,s}$ is of the form $mp_1^{c_1}\cdots p_s^{c_s}P_1^k\cdots P_r^k$ for some distinct primes $p_1, \dots, p_s,\ P_1, \dots, P_r$ and integers $m, c_1, \dots, c_s$, which satisfy the conditions (i)–(v) in the proof of Theorem 4.1.2, but with the current values of R. Once again, the integers $\tau_1, \dots, \tau_s$ defined by $\tau_j := \min\{c_j, R - kr\}$ satisfy $\tau_j \in [k+1, R-kr]$, $\tau_j \leq c_j$ and $\tau_1 + \cdots + \tau_s \geq R - kr$. (Here $R - kr \geq k + 1$ follows from $r \leq 2K - 1$ and $R = k(Kk + K - k + \mathbb{1}) + 1$.) Thus,

$$\Sigma_{r,s} \leq \sum_{\substack{\tau_1,\dots,\tau_s\in[k+1,R-kr] \\ \tau_1+\cdots+\tau_s\geq R-kr}} \mathcal{N}_{r,s}(\tau_1, \dots, \tau_s), \tag{4.97}$$

where $\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s)$ denotes the contribution of all n counted in the left hand side of (4.94) which can be written in the form $mp_1^{c_1}\cdots p_s^{c_s}\ P_1^k\cdots P_r^k$ for some distinct primes $p_1, \dots, p_s, P_1, \cdots, P_r$ and integers $m, c_1, \dots, c_s$ satisfying $c_1 \geq \tau_1, \dots, c_s \geq \tau_s$

and the conditions (i)–(v) in the proof of Theorem 4.1.2 (but with the current values of R). We will show that for each tuple $(\tau_1, \dots, \tau_s)$ occurring in (4.97), we have

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{x^{1/k}(\log_2 x)^{O(1)}}{q^K \log x} \exp\big(O(\sqrt{\log q})\big). \tag{4.98}$$

Now the bound (4.89) continues to hold, so we have

$$\mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) \ll \frac{1}{q^{(\tau_1+\dots+\tau_s)/k-s}} \frac{V'_{r,K}}{\varphi(q)^r} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \tag{4.99}$$

with the current values of $r, s, \tau_1, \dots, \tau_s$ and with $V'_{r,K}$ defined as before. By (4.46),

$$\begin{aligned} \mathcal{N}_{r,s}(\tau_1, \dots, \tau_s) &\ll \frac{\exp\big(O(\omega(q))\big)}{q^{(\tau_1+\dots+\tau_s)/k-s+r/2}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x} \\ &\ll \frac{\exp\big(O(\omega(q))\big)}{q^{\max\{s/k+r/2,\ R/k-r/2-s\}}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}. \end{aligned} \tag{4.100}$$

Now $\max\{s/k + r/2, R/k - r/2 - s\} > K$ whenever one of the following holds:

(a) In Subcase 1, we have *either* $k \geq 3$, $r \geq 3$, *or* $k = 2$, $r \geq 4$.

(b) In Subcase 2, we have $r \geq 2$.

Indeed, if $s/k + r/2 \leq K$, then $s \leq k(K - r/2)$, so that $R/k - r/2 - s \geq K + (k - 1)(r/2 - 1) - 1 + \mathbb{1} + 1/k$. This last quantity strictly exceeds K precisely under (a) or (b) above, establishing (4.98) under one of these two conditions. It thus only remains to tackle:

(i) the possibility that $r = 1$ in both Subcases 1 and 2, and

(ii) the possibilities $r = 2$ and $k = 2, r = 3$ in Subcase 1.

The possibility $r = 1$ is easily handled (in both subcases) by inserting into (4.99) the trivial bound $V'_{r,K} = V'_{1,K} \ll D_{\min}^{\omega(q)}$. Now assume we are in Subcase 1 and either $r = 2$ or $k = 2, r = 3$. Suppose wlog that $W_{1,k}$ is not squarefull. If $r = 2$, then Proposition 4.9.1(a) yields $\#\mathcal{V}_{2,K}^{(k)}(q; (w_i)_{i=1}^K)/\varphi(q)^2 \leq \#\mathcal{V}_{2,1}(q; w_1)/\varphi(q)^2 \ll$

$\varphi(q)^{-1}\exp(O(\sqrt{\log q}))$, uniformly for $(w_i)_{i=1}^K \in U_q^K$. Inserting this bound into (4.99), we deduce that $\mathcal{N}_{2,s}(\tau_1,\dots,\tau_s) \ll q^{-\max\{s/k+1,R/k-1-s\}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}\exp\big(O(\sqrt{\log q})\big)$. Since $\max\{s/k+1, R/k-1-s\} \geq K$, this shows (4.98) in Subcase 1 when $r=2$.

For $k=2, r=3$, the multiplicative independence of $\{W_{1,k}, W_{2,k}\}$ allows us to use Proposition 4.9.1(b) to get $\#\mathcal{V}_{3,K}^{(k)}(q;(w_i)_{i=1}^K)/\varphi(q)^3 \ll \exp\big(O(\omega(q))\big)/\varphi(q)^2$ uniformly for $(w_i)_{i=1}^K$. By (4.99),

$$\mathcal{N}_{3,s}(\tau_1,\dots,\tau_s) \ll q^{-\max\{s/2+2,\ R/2-1-s\}} \cdot \frac{x^{1/k}(\log_2 x)^{O(1)}}{\log x}\exp\big(O(\omega(q))\big),$$

and it is easily checked that $\max\{s/2+2,\ R/2-1-s\} > K$. This shows (4.98) in Subcase 1 when $k=2, r=3$, completing the proof of Theorem 4.1.3.

4.10.1. Optimality of the conditions of Theorem 4.1.3

We will now show that the first two values of R given in Theorem 4.1.3 are optimal. We retain the setting in subsection § 4.7.1 we had used to show optimality in Theorem 4.1.1(ii). To recall: fix an arbitrary $k \in \mathbb{N}$ and $d > 1$, and define $W_{i,k}(T) \coloneqq \prod_{j=1}^d (T-2j)+2(2i-1)$, so that $\prod_{i=1}^K W_{i,k}$ is separable (over $\mathbb{Q}$). Let $\widetilde{C}_0 > 4KD$ be any constant (depending only on $\{W_{i,k}\}_{1\leq i\leq K}$) exceeding the size of the (nonzero) discriminant of $\prod_{i=1}^K W_{i,k}$, and such that any $\widetilde{C}_0$-rough k-admissible integer lies in $\mathcal{Q}(k; f_1,\cdots,f_K)$. Fix a prime $\ell_0 > C_0$ and nonconstant polynomials $\{W_{i,v}\}_{\substack{1\leq i\leq K\\ 1\leq v<k}} \subset \mathbb{Z}[T]$ with all coefficients divisible by ℓ_0. Let $q \leq (\log x)^{K_0}$ be any squarefree integer having $P^-(q) = \ell_0$, so that as before $q \in \mathcal{Q}(k; f_1,\cdots,f_K)$. Recall also that $(2(2i-1))_{i=1}^K \in U_q^K$, that any prime P satisfying $\prod_{j=1}^d (P-2j) \equiv 0 \pmod q$ also satisfies $f_i(P^k) \equiv 2(2i-1) \pmod q$, and that the congruence $\prod_{j=1}^d (v-2j) \equiv 0 \pmod q$ has exactly $d^{\omega(q)}$ distinct solutions $v \in U_q$.

The first value $R=2$ in Theorem 4.1.3 is optimal since the condition $P_2(n) > q$

cannot be replaced by the condition $P(n) > q$, as shown in (4.78). We now show that the condition "$R = k(Kk + K - k) + 1$" in Theorem 4.1.3 cannot be weakened to "$R = k(Kk + K - k)$" for **any** K, k. To this end, let $f_1, \dots, f_K \colon \mathbb{N} \to \mathbb{Z}$ be any multiplicative functions such that $f_i(p^v) \coloneqq W_{i,v}(p)$ and $f_i(p^{k+1}) \coloneqq 1$ for all primes p, all $i \in [K]$ and $v \in [k]$. Consider n of the form $(p_1 \cdots p_{k(K-1)})^{k+1} P^k \le x$ where $P, p_1, \dots, p_{k(K-1)}$ are primes satisfying the conditions $P \coloneqq P(n) > x^{1/3k}$, $q < p_{k(K-1)} < \cdots < p_1 < x^{1/4Kk^2}$, and $\prod_{1 \le j \le d}(P - 2j) \equiv 0 \pmod q$. Then $P_{k(Kk+K-k)}(n) = p_{k(K-1)} > q$ and $f_i(n) = f_i(P^k) \prod_{j=1}^{k(K-1)} f_i(p_j^{k+1}) \equiv 2(2i-1) \pmod q$ for each $i \in [K]$. Given $p_1, \dots, p_{k(K-1)}$, the number of primes P satisfying $x^{1/3k} < P \le x^{1/k} \big/ (p_1 \cdots p_{k(K-1)})^{1+1/k}$ is $\gg d^{\omega(q)} x^{1/k} \big/ \varphi(q) (p_1 \cdots p_{k(K-1)})^{1+1/k} \log x$ by Siegel–Walfisz; here we have noted that $(p_1 \cdots p_{k(K-1)})^{1+1/k} \le x^{(K-1)(k+1)/4Kk^2} \le x^{1/2k}$. Dividing by $k!$ allows us to replace the condition $p_{k(K-1)} < \cdots < p_1$ by a distinctness condition, giving us

$$\sum_{\substack{n \le x \colon P_{k(Kk+K-k)}(n) > q \\ (\forall i) f_i(n) \equiv 2(2i-1) \pmod q}} 1 \gg \frac{d^{\omega(q)} x^{1/k}}{\varphi(q) \log x} (\mathcal{T}_1 - \mathcal{T}_2), \tag{4.101}$$

where $\mathcal{T}_1$ denotes the sum ignoring the distinctness condition on the $p_1, \dots, p_{k(K-1)}$, and $\mathcal{T}_2$ denotes the sum over all the tuples $(p_1, \dots, p_{k(K-1)})$ for which $p_i = p_j$ for some $i \ne j \in [k(K-1)]$. Now note that

$$\mathcal{T}_1 = \prod_{1 \le j \le k(K-1)} \left(\sum_{q < p_j \le x^{1/4Kk^2}} p_j^{-(1+1/k)} \right) \gg 1/q^{K-1} (\log q)^{k(K-1)}$$

while

$$\mathcal{T}_2 \ll \left(\sum_{p > q} p^{-(2+2/k)} \right) \left(\sum_{p > q} p^{-(1+1/k)} \right)^{k(K-1)-2} \ll 1/q^K.$$

Consequently, the expression on the right hand side of (4.101) is

$$\gg d^{\omega(q)}x^{1/k}/\varphi(q)^K(\log_2 x)^{k(K-1)+1}\log x,$$

which by Proposition 4.2.1, grows strictly faster than $\varphi(q)^{-K}\#\{n \le x : \gcd(f(n), q) = 1\}$ as soon as $d^{\omega(q)} > (\log x)^{(1+\epsilon)\alpha_k}$. We have already constructed such q in subsection § 4.7.1. Hence, the condition $P_{k(Kk+K-k)+1}(n) > q$ in Theorem 4.1.3 is optimal for any values of K and k.

As a remark, note that this example also shows that if $k = 1$, then for any K, the condition "$P_{2K+1}(n) > q$" coming from the third value of R in Theorem 4.1.3 is "almost optimal" in the sense that it cannot be replaced by "$P_{2K-1}(n) > q$".

Section 4.11

Necessity of the multiplicative independence and invariant factor hypotheses: Proofs of Theorems 4.1.4 and 4.1.5

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 $V_q' := \mathcal{V}_{R,K}^{(k)}\big(q; (a_i)_{i=1}^K\big) = \{(v_1, \dots, v_R) \in U_q^R : (\forall i \in [K])\ \prod_{j=1}^R W_{i,k}(v_j) \equiv a_i \pmod q\}$. 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 $P_{Rk}(N) > y > q$ 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

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

Proceeding exactly as in the argument for (2.13), we obtain

$$\sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}\\ (\forall j)\ P_j\equiv v_j \pmod q}} 1 \;=\; \frac{1}{\varphi(q)^R} \sum_{\substack{P_1,\dots,P_R>y\\ P_1\cdots P_R\le x^{1/k}\\ P_1,\dots,P_R \text{ distinct}}} 1 \;+\; O\left(x^{1/k}\exp\left(-K_1(\log x)^{1/4}\right)\right) \quad (4.102)$$

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

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

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,

$$\sum_{\substack{n\le x:\ P_{Rk}(n)>q\\ (\forall i)\ f_i(n)\equiv a_i \pmod q}} 1 \;\gg\; \frac{V_q'}{\varphi(q)^R}\cdot\frac{x^{1/k}(\log_2 x)^{R-1}}{\log x} \;-\; x^{1/k}\exp(-K_1(\log x)^{1/4}). \quad (4.103)$$

Completing the proof of Theorem 4.1.4

We now restrict to the $\{W_{i,k}\}_{1\le i\le K}$ and $(a_i)_{i=1}^K$ considered in Theorem 4.1.4, 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 $\prod_{j=1}^R W_{i,k}(v_j) \equiv a_i \pmod q$, only for $i \in [K-1]$.

Define $D_1 \coloneqq \sum_{i=1}^{K-1} \deg W_{i,k} > 1$ and let "C" in the statement of the theorem be any constant $C^* \coloneqq C^*(W_{1,k},\cdots,W_{K-1,k})$ exceeding $(32D_1)^{2D_1+2}$, the sizes of the leading and constant coefficients of $\{W_{i,k}\}_{i=1}^K$, and the constant $C_1^* \coloneqq C_1(W_{1,k},\dots,W_{K-1,k})$ coming from an application of Proposition 4.4.3 to the family $\{W_{i,k}\}_{i=1}^{K-1}$ of nonconstant multiplicatively independent polynomials. To show the lower bound in Theorem 4.1.4, we may assume that $R > 4KD_1(D_1+1)$. We shall carry out some of the arguments of Proposition 4.3.4.

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 (4.31) and (4.32); in fact by the second assertion in Proposition 4.4.3(a), the analogue of (4.31) 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 $\operatorname{lcm}[\mathfrak{f}(\chi_1),\dots,\mathfrak{f}(\chi_{K-1})] = \ell$. We find that

$$\frac{1}{\big(\alpha_k(\ell)\varphi(\ell^e)\big)^R} \sum_{(\chi_1,\dots,\chi_{K-1})\ne(\chi_{0,\ell},\dots,\chi_{0,\ell}) \bmod \ell^e} \big|Z_{\ell^e;\ \chi_1,\dots,\chi_{K-1}}(W_{1,k},\dots,W_{K-1,k})\big|^R$$

$$\leq \frac{D_1^R \ell^{eR}}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{1 \leq e_0 \leq e} \ell^{e_0(K-R/D_1)} \ \leq \ \frac{2(4D_1)^R}{\ell^{R/D_1-K}}, \quad (4.104)$$

where as usual $Z_{\ell^e;\ \chi_1,\ldots,\chi_{K-1}}(W_{1,k},\ldots,W_{K-1,k}) = \sum_{u \bmod \ell^e} \chi_{0,\ell}(u) \prod_{i=1}^{K-1} \chi_i(W_{i,k}(u))$. Now since $R \geq 4KD_1(D_1+1)$ and $\ell > C^* > (32D_1)^{2D_1+2}$, we see that $\ell^{R/D_1-K} \geq \ell^{R/(D_1+1)} \geq \ell^{R/(2D_1+2)} \cdot (C^*)^{R/(2D_1+2)} \geq \ell^2(32D_1)^R$, showing that the right hand expression in (4.104) is at most $1/4\ell^2$. Invoking the corresponding analogue of (4.26), we see for each prime power $\ell^e \parallel q$ that

$$\frac{\#\mathcal{V}^{(k)}_{R,K-1}(\ell^e;(a_i)_{i=1}^{K-1})}{\varphi(\ell^e)^R} \ \geq \ \frac{\alpha_k(\ell)^R}{\varphi(\ell^e)^{K-1}} \cdot \left(1 - \frac{1}{2\ell^2}\right).$$

But since $\prod_{\ell \mid q}(1-1/2\ell^2) \geq 1 - \frac{1}{2}\sum_{\ell \geq 2} 1/\ell^2 \geq 1/2$, we obtain

$$\frac{V_q'}{\varphi(q)^R} = \frac{\mathcal{V}^{(k)}_{R,K-1}\big(q;(a_i)_{i=1}^{K-1}\big)}{\varphi(q)^R} \geq \frac{\alpha_k(q)^R}{2\varphi(q)^{K-1}},$$

which holds true uniformly in q having $P^-(q) > C^*$. Inserting this bound into (4.103) and recalling that $\alpha_k(q) \gg 1/(\log_2(3q))^D$ completes the proof of Theorem 4.1.4. □

Completing the proof of Theorem 4.1.5

Again, it suffices to consider the case $R > 18KD(D+1)$ to prove (4.2). We start by choosing "C" in the statement of the theorem to be a constant $C_2 := C_2(W_{1,k},\ldots,W_{K,k})$ exceeding $(32D)^{6D+6}$, the sizes of the leading and constant coefficients of $\{W_{i,k}\}_{i=1}^K$, and the constant $C_1(W_{1,k},\ldots,W_{K,k})$ obtained by applying Proposition 4.4.3 to the family $\{W_{i,k}\}_{1 \leq i \leq K}$ of multiplicatively independent polynomials. The analogue of (4.32) continues to hold for each $\ell \mid q$, and thus

$$\frac{1}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{\substack{(\chi_1,\ldots,\chi_K) \bmod \ell^e \\ \mathrm{lcm}[\mathfrak{f}(\chi_1),\ldots,\mathfrak{f}(\chi_K)] \in \{\ell^2,\ldots,\ell^e\}}} |Z_{\ell^e;\ \chi_1,\ldots,\chi_K}(W_{1,k},\ldots,W_{K,k})|^R$$

$$\leq \frac{D^R \ell^{eR}}{(\alpha_k(\ell)\varphi(\ell^e))^R} \sum_{2 \leq e_0 \leq e} \ell^{e_0(K-R/D)} \ \leq \ \frac{2(4D)^R}{\ell^{R/D-K}} \ \leq \ \frac{1}{4\ell^2}, \quad (4.105)$$

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

If $(\chi_1, \ldots, \chi_K)$ is a tuple of characters mod ℓ^e having $\mathrm{lcm}[\mathfrak{f}(\chi_1), \ldots, \mathfrak{f}(\chi_K)] = \ell$, then with ψ_ℓ being a generator of the character group mod ℓ, we have $\chi_i = \psi_\ell^{A_i}$ for some unique $(A_1, \ldots, A_K) \in [\ell-1]^K$ satisfying $(A_1, \ldots, A_K) \not\equiv (0, \ldots, 0) \pmod{\ell-1}$. Recall from the arguments leading to (4.31) 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 $|Z_{\ell^e;\ \chi_1,\ldots,\chi_K}(W_{1,k}, \ldots, W_{K,k})| \leq D\ell^{e-1/2}$. 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 $Z_{\ell^e;\ \chi_1,\ldots,\chi_K}(W_{1,k}, \ldots, W_{K,k}) = \ell^{e-1} \sum_{v \bmod \ell} \psi_\ell\big((vG(v))^{\ell-1}\big) = \alpha_k(\ell)\varphi(\ell^e)$. Combining these observations with (4.105) and using that $\prod_{i=1}^K \overline{\chi}_i(a_i) = 1$ for any characters $(\chi_1, \ldots, \chi_K)$ mod ℓ^e with $\mathrm{lcm}[\mathfrak{f}(\chi_1), \ldots, \mathfrak{f}(\chi_K)] = \ell$ (as $a_i \equiv 1 \bmod \ell$), we get

$$\frac{\#\mathcal{V}_{R,K}^{(k)}\big(\ell^e; (a_i)_{i=1}^K\big)}{\varphi(\ell^e)^R} \ \geq \ \frac{\alpha_k(\ell)^R}{\varphi(\ell^e)^K}\left(1 + \mathcal{B}_\ell - \frac{1}{2\ell^2}\right), \quad (4.106)$$

where $\mathcal{B}_\ell$ denotes the number of tuples $(A_1, \ldots, A_K) \in [\ell-1]^K \setminus \{(0, \ldots, 0)\}$ 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 $C_1 = C_1(W_{1,k}, \ldots, W_{K,k})$ from the proof of Proposition 4.4.3, 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 4.4.3(a), $\prod_{i=1}^K W_{i,k}^{A_i}$ is a perfect $(\ell-1)$-th power in $\mathbb{F}_\ell[T]$ precisely when $E_0(A_1 \cdots A_K)^\top \equiv (0 \cdot \cdots \cdot 0)^\top \pmod{\ell-1}$, where $E_0 = E_0(W_{1,k}, \ldots, W_{K,k})$ 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 [55, 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 $\gcd(\ell-1, \beta) \neq 1$, 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 (4.106) yields $V_q'/\varphi(q)^R \geq 2^{\#\{\ell \mid q:\ (\ell-1,\beta)\neq 1\}}\alpha_k(q)^R/2\varphi(q)^K$. Inserting this into (4.103) establishes (4.2). □

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 (4.103) gives

$$\#\{n \leq x : P_{Rk}(n) > q, f(n) \equiv c^R \pmod{q}\} \gg x^{1/k}(\log_2 x)^{R-1}/\log x.$$

4.11.1. Explicit Examples.

We now construct examples where the lower bounds in Theorems 4.1.4 and 4.1.5 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 4.1.4)

By Proposition 4.2.1, it is clear that the lower bound in Theorem 4.1.4 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 $\beta^* = \beta(W_{1,k}, \dots, W_{K-1,k})$ is odd (for instance, $W_{i,k} := H_i^{b_i}$ for some pairwise coprime irreducibles $H_1, \dots, H_{K-1} \in \mathbb{Z}[T]$ and odd integers $b_i > 1$ satisfying $b_i \mid b_{i+1}$ for each $i < K-1$). Fix nonnegative integers

$(\lambda_i)_{i=1}^{K-1} \neq (0,\dots,0)$ 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 4.1.4, 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 $\ell_0 \equiv -1 \bmod \beta^*$. [12] Let $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v\le k-1}} \subset \mathbb{Z}[T]$ be nonconstant polynomials with all coefficients divisible by ℓ_0, and let $q := \prod_{\substack{\ell_0\le \ell\le Y\\ \ell\equiv -1 \,(\mathrm{mod}\ \beta^*)}} \ell$, with Y any parameter lying in $(4|\beta^*| \log_2 x, (K_0/2)\log_2 x)$. Since $\alpha_k(\ell) \ge 1 - D_1/(\ell-1) > 0$ for $\ell > \widetilde{C}$, we see that $q \le (\log x)^{K_0}$ 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, $q = \exp\Big(\sum_{\substack{\ell_0\le \ell\le Y\\ \ell\equiv -1 \,(\mathrm{mod}\ \beta^*)}} \log \ell\Big) \ge \exp(Y/2|\beta^*|) \ge \log^2 x$, so the lower bound in Theorem 4.1.4 grows strictly faster than $\varphi(q)^{-K}\#\{n \le x : (f(n), q) = 1\}$.

Failure of joint weak equidistribution upon violation of Invariant Factor Hypothesis (example for Theorem 4.1.5)

Define $W_{i,k}(T) := T - i$ for each $i \in [K-1]$ and $W_{K,k}(T) := (T-K)^d$, for some fixed $d \in \{2,\dots,K\}$. Then $\{W_{i,k}\}_{1\le i\le K}$ are nonconstant, monic and pairwise coprime (hence multiplicatively independent); also $E_0(W_{1,k},\dots,W_{K,k}) = \mathrm{diag}(1,\dots,1,d)$ so $\beta := \beta(W_{1,k},\dots,W_{K,k}) = d$. Note that $\alpha_k(\ell) = 1 - K/(\ell-1) > 0$ for any prime $\ell > K+1$. Let $C_3 := C_3(W_{1,k},\dots,W_{K,k})$ be a constant exceeding the constant C_2 in the proof of Theorem 4.1.5, such that any k-admissible C_3-rough integer lies in $\mathcal{Q}(k; f_1, \cdots, f_K)$; note that $C_3 > D + 1 \ge K + 2$. Let ℓ_0 be the least prime exceeding C_3 and satisfying $\ell_0 \equiv 1 \pmod{d}$, let $\{W_{i,v}\}_{\substack{1\le i\le K\\ 1\le v<k}} \subset \mathbb{Z}[T]$ be nonconstant polynomials all of whose coefficients are divisible by ℓ_0, and let $q := \prod_{\substack{\ell_0\le \ell\le Y\\ \ell\equiv 1 \,(\mathrm{mod}\ d)}} \ell$, with $Y \le (K_0/2)\log_2 x$ a parameter to be chosen later.

Then $q \le (\log x)^{K_0}$, $P^-(q) > C_3$ and $q \in \mathcal{Q}(k; f_1, \cdots, f_K)$. By Theorem 4.1.5 and

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

Proposition 4.2.1, 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 (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 4.1.1, 4.1.2 and 4.1.3, and neither of them can be bypassed by restricting to inputs n with sufficiently many large prime factors.

Section 4.12

Concluding Remarks

It is interesting to note that despite the extensive amount of 'multiplicative machinery' known in analytic number theory, there does not seem to be any estimate in the literature, a direct application of which can replace our arguments in section 4.6. For instance, Halász's Theorem only yields an upper bound on the character sums that is not precise enough, while a direct application of (known forms of) the Landau-Selberg-Delange method, – one of the most precise estimates on mean values of multiplicative functions known in literature, – seems to give an extremely small range of uniformity in q.

Theorem 4.1.3 suggests a few directions of improvement. First, as mentioned at the end of the previous section, we are still "one step away" from optimality in the case $K \geq 2$, $k = 1$: Theorem 4.1.3 shows that "$P_{2K+1}(n) > q$" is sufficient while the discussion in subsection § 4.10.1 shows that "$P_{2K-1}(n) > q$" is not, so the question is

whether the optimal value is "$2K$" or "$2K+1$". If it is the former, then we will need a sharper bound on $V'_{2K,K}$ than what comes from our methods in section 4.10. One can also ask whether it is possible to weaken the nonsquarefullness conditions in the statement of Theorem 4.1.3.

Recall also that the ranges of q in Theorem 4.1.1 are genuinely optimal in all the cases *except* in the very first one (namely when $K = 1$ and $W_k = W_{1,k}$ is linear): This includes the case of a *single* multiplicative function $f(n)$ controlled by a *single* linear polynomial at the primes, the most interesting concrete example of which is $\varphi(n)$ or $\sigma(n)$ itself! In these cases, we can prove that q cannot be allowed to grow much faster than $L(x) = x^{\log\log\log x/\log\log x}$ (see the end of the introduction in [40]), but owing to our heavy reliance on the Siegel-Walfisz theorem, the previous arguments do not extend past the range $q \leq (\log x)^{K_0}$. It would be interesting to obtain the best possible range of q in this remaining case; it seems that being able to do this may require significantly new ideas or an entirely different approach.

This chapter has obtained some of the best possible analogues of the *Siegel-Walfisz* theorem for families of polynomially-defined multiplicative functions. One of the next steps would be to study analogues of the *Bombieri-Vinogradov* theorem for such families. We might also ask for extensions of the results of this chapter to study the distribution of Fourier coefficients of modular forms (particularly Ramanujan's tau function $\tau(n)$) to varying moduli.

In the manuscript [72], we strengthen some of the results in this chapter under some additional finer control on the behavior of the given multiplicative functions at some higher prime powers.

Finally, in an upcoming manuscript [74] of the author, we extend the general Landau–

Selberg–Delange method (as formulated in [76, chapter II.5], for instance) from the case when the Dirichlet series in the picture is controlled by a complex power of the Riemann zeta to the case when it is controlled by a product of L-functions mod q raised to complex powers, where q varies in a wide range. As one of several applications of this result, we hope to give quantitative versions of Theorems 4.1.1 to 4.1.3. This would also enable us to understand the second-order behavior in these distributions as well as the rate of convergence to equidistribution. In particular, we should be able to explain the slow convergence to equidistribution observed in the table on $\varphi(n)$ mod 5 following the statement of Proposition 1.3.3. It is also very likely that the convergence to equidistribution is monotonic in general, even as q varies uniformly in the "Siegel–Walfisz" range; we should also be able to establish this.

Chapter 5

Distribution of the aliquot sum function to varying prime moduli

Let $s(n) = \sigma(n) - n$ denote the sum-of-proper-divisors (or sum-of-aliquot-divisors) function. In this chapter, we determine asymptotic formulas for the number of $n \leq x$ for which $s(n)$ lands in a given residue class modulo p, uniformly for primes p below any fixed power of $\log x$. This chapter is partly based on the manuscript [40], however, we have been able to simplify the arguments using ideas from Chapters 2–4.

For fixed modulus q, one has that $q \mid \sigma(n)$ for all n except those belonging to a set of density 0. This was observed already by Alaoglu and Erdős in 1944 [2, p. 882]. (See also the proof of Lemma 5 in [58], and Theorem 2 in [62].) Since $s(n) = \sigma(n) - n \equiv -n \pmod{q}$ whenever $q \mid \sigma(n)$, we immediately deduce that $s(n)$ is equidistributed mod q for each fixed modulus q.

We will show that $s(n)$ remains equidistributed for larger prime moduli p, but some care about the formulation is required. Since $s(q) = 1$ for every prime q, there are at

least $(1+o(1))x/\log x$ values of $n \le x$ with $s(n) \equiv 1 \pmod{p}$, no matter the value of p. This dashes any hope of equidistribution if p is appreciably larger than $\log x$. We work around this issue by considering $s(n)$ only for composite n.

Theorem 5.0.1. *Fix $K_0 > 0$. As $x \to \infty$, the number of composite $n \le x$ with $s(n) \equiv a \pmod{p}$ is $(1+o(1))x/p$, for every residue class a mod p with $p \le (\log x)^{K_0}$.*

Additional notation and conventions in this chapter:

We reserve the letters p, P for primes. In addition to employing the Landau–Bachmann–Vinogradov notation from asymptotic analysis, we write $A \gtrsim B$ (resp., $A \lesssim B$) to mean that $A \ge (1+o(1))B$ (resp., $A \le (1+o(1))B$).

Section 5.1

Technical Preparation

As shown in the introduction, $s(n)$ is equidistributed modulo each fixed prime p, hence to show Theorem 5.0.1, we may assume that $p \to \infty$ such that $p \le (\log x)^{K_0}$.

The following result is a special case of the fundamental lemma of sieve theory, as formulated in [31, Theorem 7.2, p. 209].

Lemma 5.1.1. *Let $X \ge Z \ge 3$. Suppose that the interval $I = (u, v]$ has length $v - u = X$. Let $\mathcal{Q}$ be a set of primes not exceeding Z. For each $q \in \mathcal{Q}$, choose a residue class $a_q \bmod q$. The number of integers $n \in I$ not congruent to $a_q \bmod q$ for any $q \in \mathcal{Q}$ is*

$$X \left(\prod_{q \in \mathcal{Q}} \left(1 - \frac{1}{q}\right) \right) \left(1 + O\left(\exp\left(-\frac{1}{2}\frac{\log X}{\log Z}\right)\right)\right).$$

We will need the following result on the count of $n \le x$ for which $\gcd(\sigma(n), p) = 1$, which refines Proposition 2.2.1 for the function $\sigma(n)$ to prime moduli. This follows as a direct consequence of [69, Theorem A] or [40, Lemma 5.1]; alternatively, a more elementary argument for this can be given by following the proof of the latter.

Lemma 5.1.2. *Fix $A > 0$. As $x, p \to \infty$ with $\frac{\log x}{\log p} \to \infty$, we have*

$$\sum_{\substack{n \le x \\ p \nmid \sigma(n)}} 1 \sim \frac{x}{p(\log x)^{1/(p-1)}}.$$

In what follows, given $J \in \mathbb{N}$ and units $R, S \bmod p$, we define

$$\mathcal{U}_J(p; R, S) = \{(v_1, \dots, v_J) \in U_p^J : \prod_{j=1}^{J}(v_j + 1) \equiv R, \ \prod_{j=1}^{J} v_j \equiv S \pmod p\}.$$

Moreover, given residues $a, r, s \bmod p$, we define

$$\mathcal{V}_J(p, a; R, S) = \{(v_1, \dots, v_J) \in U_p^J : \ r\prod_{j=1}^{J}(v_j + 1) \ - \ s\prod_{j=1}^{J} v_j \equiv a \pmod p\}.$$

We also define $\alpha(p) \coloneqq 1 - 1/(p-1)$. The following estimates on the sizes of $\mathcal{U}_J(p; R, S)$ and $\mathcal{V}_J(p, a; R, S)$ will be useful throughout our arguments.

Lemma 5.1.3. *As $x, p, J \to \infty$, we have*

$$\#\mathcal{U}_J(p; R, S) = (1 + o(1))\frac{(\alpha(p)\varphi(p))^J}{\varphi(p)^2}$$

uniformly in $R, S \in U_p$.

Proof. The argument is a much simpler version of that given for Proposition 4.3.4,

so we only outline it. By (4.26), we have

$$\#\mathcal{U}_J(p;R,S)=\frac{1}{\varphi(p)^2}\sum_{\chi,\psi \bmod p}\overline{\chi}(R)\overline{\psi}(S)\left(\sum_{v \bmod p}\chi(v+1)\psi(v)\right)^J.$$

For $(\chi,\psi)=(\chi_0,\chi_0) \bmod p$ (where χ_0 is again the trivial character mod p), we see that $\sum_{v \bmod p}\chi(v+1)\psi(v)=\#\{v\in U_p : v+1\in U_p\}=p-2=\alpha(p)\varphi(p)$. For the other $O(p^2)$ many possibilities of (χ,ψ), the sum $\sum_{v \bmod p}\chi(v+1)\psi(v)$ being a Jacobi sum has absolute value at most $p^{1/2}$. This shows that

$$\#\mathcal{U}_J(p;R,S)=\frac{(\alpha(p)\varphi(p))^J}{\varphi(p)^2}\left\{1+O\left(\frac{p^{J/2+2}}{(\alpha(p)\varphi(p))^J}\right)\right\},$$

and since $p,J\to\infty$, the O-term above is at most $\frac{p^{J/2+2}}{(p-2)^J}\le\frac{2^J}{p^{J/2-2}}=o(1)$. □

Lemma 5.1.4. *As $x,p,J\to\infty$, we have the following estimates, uniformly in residue classes a,r,s mod p.*

$$\#\mathcal{V}_J(p,a;R,S)=\begin{cases}(1+o(1))\cdot(\alpha(p)\varphi(p))^J/\varphi(p), & \text{if } a\in U_p, r\in U_p, s\equiv 0 \pmod p\\ \varphi(p)^{J-1}, & \text{if } a\in U_p, r\equiv 0 \pmod p, s\in U_p\\ (1+o(1))\cdot\varphi(p)^{J-1}, & \text{if } a\in U_p, r\in U_p, s\in U_p\\ (1+o(1))\cdot(\alpha(p)\varphi(p))^J/\varphi(p), & \text{if } a\equiv 0 \pmod p, r\in U_p, s\in U_p.\end{cases} \tag{5.1}$$

Proof. In the first case, we have $\mathcal{V}_J(p,a;R,S)=\{(v_1,\dots,v_J)\in U_p^J : r\prod_{j=1}^J(v_j+1)\equiv a \pmod p\}$, with $a,r\in U_p$, so its count is $(1+o(1))(\alpha(p)\varphi(p))^J/\varphi(p)$ by the arguments given for the verification of hypothesis A in section 2.4. In the second case, we see that $\mathcal{V}_J(p,a;R,S)=\{(v_1,\dots,v_J)\in U_p^J : \prod_{j=1}^J v_j\equiv -as^{-1} \pmod p\}$; since $as^{-1}\in U_p$, any of the $\varphi(p)^{J-1}$ many arbitrary assignments of $v_1,\dots,v_{J-1}$ throws v_J

in a unique coprime residue class mod p.

Now we come to the third case, namely when $a, r, s \in U_p$. We start by setting $R \equiv r\prod_{j=1}^{J}(v_j+1)$ and $S \equiv s\prod_{j=1}^{J} v_j \bmod p$, so that $R - S \equiv a \pmod p$. Note that $S \in U_p$, so that (separating the cases when R is or is not divsible by p, we may write)

$$\#\mathcal{V}_J(p,a;R,S) = \sum_{\substack{R,S\in U_p \\ R-S\equiv a \,(\mathrm{mod}\ p)}} \#\mathcal{U}_J(p;Rr^{-1},Ss^{-1}) + \#\{(v_1,\dots,v_J)\in U_p^J :\ p \mid \prod_{j=1}^{J}(v_j+1),\ \prod_{j=1}^{J} v_j \equiv -as^{-1} \pmod p\}. \quad (5.2)$$

By Lemma 5.1.3, the sum above is $(1+o(1))(\alpha(p)\varphi(p))^J/\varphi(p)$. To count the last cardinality in (5.2), note that omitting the divisibility condition would give a total of $\varphi(p)^{J-1}$ many tuples $(v_1,\dots,v_J)$ (as argued in the second case of (5.1)). On the other hand, by Lemma 5.1.3, the number of $(v_1,\dots,v_J) \in U_p^J$ satisfying $p \nmid \prod_{j=1}^{J}(v_j+1)$ and $\prod_{j=1}^{J} v_j \equiv -as^{-1} \pmod p$ is equal to $\sum_{b\in U_p} \#\mathcal{U}_J(p;b,-as^{-1}) = (1+o(1))(\alpha(p)\varphi(p))^J/\varphi(p)$. Putting all of this together into (5.2) shows that

$$\#\mathcal{V}_J(p,a;R,S) = (1+o(1))\cdot\frac{(\alpha(p)\varphi(p))^J}{\varphi(p)} \ +\ \varphi(p)^{J-1} \ -\ (1+o(1))\cdot\frac{(\alpha(p)\varphi(p))^J}{\varphi(p)}$$

which is $\varphi(p)^{J-1}(1+o(\alpha(p)^J))$, and hence also $\varphi(p)^{J-1}(1+o(1))$ as desired.

Finally, we come to the last case, namely when $a \equiv 0 \pmod p$ and $r, s \in U_p$. Setting $R \equiv r\prod_{j=1}^{J}(v_j+1) \equiv s\prod_{j=1}^{J} v_j \pmod p$, we see that this time, we must have $R \in U_p$, which allows us to write

$$\#\mathcal{V}_J(p,a;R,S) = \#\mathcal{V}_J(p,0;r,s) = \sum_{R\in U_p} \#\mathcal{U}_J(p;Rr^{-1},Rs^{-1}).$$

Invoking Lemma 5.1.3 on each $\mathcal{U}_J(p;Rr^{-1},Rs^{-1})$ thus completes the proof. □

In the spirit of the arguments in previous chapters, we set

$$J := \lfloor \log_3 x \rfloor \quad \text{and} \quad y := \exp((\log x)^{1/4}),$$

and we define n to be convenient if the J largest prime factors of n exceed y and none of them are repeated in n. Thus any convenient n can be uniquely written in the form $mP_J \dots P_1$, where $L_m := \max\{y, P(m)\} < P_J < \cdots < P_1$. Note that any convenient n is automatically composite. As such, we will say that n is inconvenient if it is **composite** and not convenient.

We then have the following analogue of Lemma 2.3.2 and Proposition 4.3.1.

Lemma 5.1.5. *Fix $K_0 > 0$. Uniformly in $p, x \to \infty$ satisfying $p \le (\log x)^{K_0}$, the number of inconvenient $n \le x$ is $o(x)$, and the number of inconvenient $n \le x$ divisible by p is $o(x/p)$.*

The proofs of both the assertions are much simpler versions of that of Lemma 2.3.2 so we omit the details. (The only additional observation for the second assertion is that if we write $n = BAP$ with $P(B) \le y < P^-(A)$ and with $P > z$ as in the proof of Lemma 2.3.2, then we must have $p \mid B$, so that $\sum 1/B \le p^{-1} \sum_{m:P(m)\le y} 1/m \ll (\log y)/p$.)

Section 5.2

Contribution of the convenient n

Once again, we show that the convenient n give the main term.

Proposition 5.2.1. *Fix $K_0 > 0$. We have*

$$\#\{n \le x \text{ convenient } : s(n) \equiv a \pmod p\} \sim \frac{x}{p} \quad \text{as } x, p \to \infty,$$

uniformly in $p \le (\log x)^{K_0}$ and in residues a mod p.

Proof. The exact same arguments as given for (3.6) or (4.15) show that

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv a \pmod p}} 1 = \sum_{m\le x} \frac{\#\mathcal{V}(m)}{\varphi(p)^J}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) + O\left(x\exp\left(-C_1(\log x)^{1/16}\right)\right) \tag{5.3}$$

where $\mathcal{V}(m) \coloneqq \mathcal{V}_J(p,a;\sigma(m),m)$. for some constant C_1 depending on K_0.

First consider any $a \in U_p$. Note that for $\mathcal{V}(m)$ to be nonempty, we must have $p \nmid m$ or $p \nmid \sigma(m)$. As such, the first three cases of (5.1) show that the count of convenient $n \le x$ satisfying $s(n) \equiv a \pmod p$ is

$$\begin{aligned}(1+o(1))\frac{\alpha(p)^J}{\varphi(p)} &\sum_{\substack{m\le x\\ p\nmid\sigma(m),\ p\mid m}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right)\\ &+ \frac{1}{\varphi(p)}\sum_{\substack{m\le x\\ p\mid\sigma(m),\ p\mid m}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) + \frac{1+o(1)}{\varphi(p)}\sum_{\substack{m\le x\\ p\nmid m\sigma(m)}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right).\end{aligned} \tag{5.4}$$

The first double sum (over $m \le x$ satisfying $p \nmid \sigma(m)$ and $p \mid m$) is at most

$$\sum_{\substack{m\le x\\ p\mid m}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) \le \sum_{\substack{m\le x\\ p\mid m}}\sum_{\substack{L_m<P_J<\cdots<P_1\\ P_1\cdots P_J\le x/m}} 1 \le \sum_{\substack{n\le x\\ p\mid n}} 1 \ll \frac{x}{p}. \tag{5.5}$$

Thus, collecting the main terms in the second and third double sums in (5.4) shows

that the expression in (5.4) is

$$\frac{1}{\varphi(p)}\sum_{\substack{m\le x\\ p\nmid m}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}}1\right) \;+\; o\left(\frac{1}{\varphi(p)}\sum_{\substack{m\le x\\ p\nmid m\sigma(m)}}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}}1\right)\right) \;+\; o\left(\frac{x}{p}\right).$$

By (5.5), removing the $p\nmid m$ condition in the main term above incurs a negligible error. Moreover, proceeding as in (5.5) shows that the double sum in the o-term above is at most x. This shows that

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv a \pmod p}} 1 \;=\; \frac{1}{\varphi(p)}\sum_{m\le x}\left(\frac{1}{J!}\sum_{\substack{P_1,\dots,P_J>L_m\\ P_1\cdots P_J\le x/m\\ P_1,\dots,P_J \text{ distinct}}}1\right) \;+\; o\left(\frac{x}{p}\right).$$

Reversing the splitting of convenient n and invoking the first assertion of Lemma 5.1.5 shows that the double sum in the right hand side above is $\sim x$, completing the proof of the proposition for $a \in U_p$.

Finally, consider the case $a \equiv 0 \pmod p$. We start by writing

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv 0 \pmod p}} 1 \;=\; \sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv 0 \pmod p\\ p\nmid n\sigma(n)}} 1 \;+\; \sum_{\substack{n\le x \text{ convenient}\\ p\mid n,\ p\mid\sigma(n)}} 1. \tag{5.6}$$

By the second assertion of Lemma 5.1.5, ignoring the convenient condition in the second sum on the right hand side above incurs an error of $o(x/p)$. Since the number of $n \le x$ divisible by p^2 is $o(x/p)$, we thus obtain

$$\sum_{\substack{n\le x \text{ convenient}\\ p\mid n,\ p\mid\sigma(n)}} 1 \;=\; \sum_{\substack{n\le x\\ p\| n,\ p\mid\sigma(n)}} 1 + o\left(\frac{x}{p}\right) \;=\; \sum_{\substack{m\le x/p\\ p\nmid m,\ p\mid\sigma(m)}} 1 + o\left(\frac{x}{p}\right) \;=\; \sum_{\substack{m\le x/p\\ p\mid\sigma(m)}} 1 + o\left(\frac{x}{p}\right);$$

in the second equality above, we have noted that if $p \parallel n$, then n can be uniquely written as mp for some $m \le x/p$ not divisible by p, so that $\sigma(n) = \sigma(m)(p+1) \equiv \sigma(m) \pmod{p}$. By Lemma 5.1.2, we obtain

$$\sum_{\substack{n\le x \text{ convenient}\\ p\mid n,\ p\mid\sigma(n)}} 1 \;=\; \frac{x}{p} \;-\; \sum_{\substack{m\le x/p\\ p\nmid\sigma(m)}} 1 \;+\; o\left(\frac{x}{p}\right) \;=\; \frac{x}{p} \;-\; (1+o(1))\frac{x}{p(\log x)^{1/(p-1)}} \;+\; o\left(\frac{x}{p}\right). \tag{5.7}$$

To deal with the first sum in (5.6), we proceed as in the case $a \in U_p$, by first obtaining an analogue of (5.3) and then using the last case of Lemma 5.1.4. Noting that $p \nmid n\sigma(n)$ also forces $p \nmid m\sigma(m)$, we deduce that

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv 0 \pmod p\\ p\nmid n\sigma(n)}} 1 \;=\; (1+o(1))\,\frac{\alpha(p)^J}{\varphi(p)} \sum_{\substack{m\le x\\ p\nmid m\sigma(m)}} \left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J > L_m\\ P_1\cdots P_J \le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) \;+\; o\left(\frac{x}{p}\right).$$

An entirely analogous argument also gives

$$\sum_{\substack{n\le x \text{ convenient}\\ p\nmid n\sigma(n)}} 1 \;=\; \alpha(p)^J \sum_{\substack{m\le x\\ p\nmid m\sigma(m)}} \left(\frac{1}{J!} \sum_{\substack{P_1,\dots,P_J > L_m\\ P_1\cdots P_J \le x/m\\ P_1,\dots,P_J \text{ distinct}}} 1\right) \;+\; o\left(\frac{x}{p}\right),$$

where the aforementioned application of Lemma 5.1.4 is replaced by the easy observation that the number of tuples $(v_1, \dots, v_J) \in U_p^J$ for which $\prod_{j=1}^J (v_j + 1) \in U_p$ is exactly $(\alpha(p)\varphi(p))^J$. Comparing the last two displays shows that

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv 0 \pmod p\\ p\nmid n\sigma(n)}} 1 \;=\; \frac{1+o(1)}{\varphi(p)} \sum_{\substack{n\le x \text{ convenient}\\ p\nmid n\sigma(n)}} 1 \;+\; o\left(\frac{x}{p}\right) \;=\; \frac{1+o(1)}{\varphi(p)} \sum_{\substack{n\le x\\ p\nmid\sigma(n)}} 1 \;+\; o\left(\frac{x}{p}\right),$$

where the last equality follows from the first assertion of Lemma 5.1.5. Finally,

invoking Lemma 5.1.2 shows that

$$\sum_{\substack{n\le x \text{ convenient}\\ s(n)\equiv 0 \pmod p\\ p\nmid n\sigma(n)}} 1 \;=\; (1+o(1))\frac{x}{p(\log x)^{1/(p-1)}} \;+\; o\left(\frac{x}{p}\right).$$

Inserting this and (5.7) into (5.6) establishes Proposition 5.2.1. □

Hence to complete the proof of Theorem 5.0.1, it suffices to show that the number of inconvenient $n \le x$ satisfying $s(n) \equiv a \pmod p$ is $o(x/p)$ uniformly in $x, p \to \infty$ with $p \le (\log x)^{K_0}$.

Section 5.3

Bounding the contribution of inconvenient n

Let $z = x^{1/\log_2 x}$. By the arguments given towards the start of the proof of Lemma 2.3.2, there are $o(x/p)$ many $n \le x$ which are either z-smooth or have a repeated prime factor exceeding y. Any remaining inconvenient n must have $P_J(n) \le y$. Splitting these n into S_1 and S_2 depending on whether or not $P_2(n) > y$ (respectively), it suffices to show that both S_1 and S_2 are $o(x/p)$.

By definition of S_1, any n counted in it can be written as $n = mP_2P_1$, where $P_1 > z$, where $\max\{y, P(m)\} < P_2 < P_1$, and $P_J(m) \le y$. The congruence $s(n) \equiv a \pmod p$ can be rewritten as $(P_1, P_2) \equiv (v_1, v_2) \bmod p$ for some (v_1, v_2) in $\mathcal{V}_2(m) \coloneqq \mathcal{V}_2(p, a; \sigma(m), m)$. Now given m and (v_1, v_2), the number of possible (P_1, P_2) can be bounded by familiar Brun–Titchmarsh and partial summation arguments. This gives

$$S_1 \;\ll\; \frac{x(\log_2 x)^2}{\log x} \sum_{\substack{m\le x\\ P_J(m)\le y}} \frac{1}{m}\cdot\frac{\#\mathcal{V}_2(m)}{\varphi(p)^2}. \tag{5.8}$$

We now claim that uniformly in primes p and in residues $a, r, s \bmod p$, we have

$$\#\mathcal{V}_2(p,a;r,s) \ \leq \ \mathbb{1}_{r\equiv s\equiv a\equiv 0 \,(\mathrm{mod}\ p)}\ \varphi(p)^2 \ \ + \ \ 2\varphi(p). \tag{5.9}$$

Indeed, writing $r(v_1+1)(v_2+1) - sv_1v_2 = (r(v_1+1) - sv_1)\cdot v_2 \ + \ r(v_1+1)$ and differentiating the possibility of whether or not the coefficient of v_2 is invertible mod p, we obtain

$$\#\mathcal{V}_2(p,a;r,s) \ \leq \sum_{\substack{v_1\in U_p\\ r(v_1+1)\not\equiv sv_1 \,(\mathrm{mod}\ p)\\ r(v_1+1)\not\equiv a \,(\mathrm{mod}\ p)}} 1 \ \ + \ \varphi(p)\cdot \sum_{\substack{v_1\in U_p\\ r(v_1+1)\equiv sv_1\equiv a \,(\mathrm{mod}\ p)}} 1$$

The first sum is always at most $\varphi(p)$. As for the second sum, if $a \in U_p$, then the congruence $sv_1 \equiv a \pmod p$ forces v_1 into a unique coprime residue class mod p, in which case the second sum is at most 1. Moreover, if $a \equiv 0 \pmod p$ but $r \in U_p$, then the congruence $r(v_1+1) \equiv a \equiv 0 \pmod p$ forces $v_1 \equiv -1 \pmod p$, so that the second sum again at most 1. Inserting all these observations into the displayed bound above shows that $\#\mathcal{V}_2(p,a;r,s) \leq 2\varphi(p)$ except when $a \equiv r \equiv 0 \pmod p$. Now if $a \equiv r \equiv 0 \pmod p$, then for $\mathcal{V}_2(p,a;r,s)$ to be nonempty, we must also have $s \equiv 0 \pmod p$, thus proving (5.9).

Now if $a \in U_p$, then (5.8) and (5.9) show that $S_1 \ll x(\log_2 x)^2/p\sqrt{\log x}$; here the sum $\sum_{\substack{m\leq x\\ P_J(m)\leq y}} 1/m$ has been bounded by writing $m = AB$ with $P(B) \leq y < P^-(A)$, and handling $\sum 1/A$ and $\sum 1/B$ in a manner analogous to the proof of Lemma 2.3.2.

On the other hand, if $a \equiv 0 \pmod p$, then (5.8) and (5.9) show that

$$S_1 \ \ll \ \frac{x(\log_2 x)^2}{\varphi(p)\log x} \sum_{\substack{m\leq x\\ P_J(m)\leq y}} \frac{1}{m} \ \ + \ \ \frac{x(\log_2 x)^2}{\log x} \sum_{\substack{m\leq x:\ p\mid m\\ P_J(m)\leq y}} \frac{1}{m}.$$

Handling the first sum as above, writing any m in the second sum as $m = Mp$ with $P_J(M) \le y$, and handling $\sum 1/M$ as above, now shows that $S_1 \ll x(\log_2 x)^2/p\sqrt{\log x}$ in the case $a \equiv 0 \pmod p$ as well. Hence we always have $S_1 = o(x/p)$.

We now turn to S_2, the count of composite $n \le x$ not having any repeated prime factor exceeding y, and satisfying the three conditions $P_2(n) \le y$, $P(n) > z$, $s(n) \equiv a \pmod p$. From now on, we will be handling all residues a mod p simultaneously. Write $n = mP$ with $P = P(n) > \max\{z, P(m)\}$, so that $P(m) \le y$. Then $Ps(m) + \sigma(m) = s(n) \equiv a \pmod p$. Now if $s(m) \not\equiv 0 \pmod p$, then we must also have $\sigma(m) \not\equiv a \pmod p$, and by Brun–Titchmarsh, the total number of such (m, P) is

$$\ll \sum_{\substack{m \le x \\ P(m) \le y}} \frac{x/m}{\varphi(p)\log z} \ll \frac{x\log_2 x}{p\log x} \cdot \prod_{\ell \le y}\left(1 + \sum_{v \ge 1}\frac{1}{\ell^v}\right) \ll \frac{x\log_2 x}{p\log x} \cdot \exp\left(\sum_{\ell \le y}\frac{1}{\ell}\right),$$

which is $\ll x\log_2 x/p(\log x)^{3/4} = o(x/p)$.

It thus only remains to bound the contribution of (m, P) counted above that satisfy $s(m) \equiv 0 \pmod p$, so that $\sigma(m) \equiv a \pmod p$. This means two things: First, $m = \sigma(m) - s(m) \equiv a \pmod p$. Second, since n is composite, we have $m > 1$, so that $s(m) > 0$, whence the condition $s(m) \equiv 0 \pmod p$ forces $p \le s(m) \le \sigma(m) \ll m\log_2(3m)$, leading to to $m \gg p/\log_2 p$. (Here the bound on $\sigma(m)$ is a standard fact, see for instance [33, Theorem 323, p. 350].) Bounding the number of $P \in (z, x/m]$ via Chebyshev's estimate on the count of primes, and then summing over m shows that the total number of such possible (m, P) is

$$\ll \frac{x\log_2 x}{\log x}\left(\frac{\log_2 p}{p} + \sum_{\substack{p < m \le y^{10} \\ m \equiv a \pmod p}}\frac{1}{m} + \sum_{\substack{y^{10} < m \le x \\ P(m) \le y \\ m \equiv a \pmod p}}\frac{1}{m}\right). \tag{5.10}$$

By partial summation, the second sum is $\ll (\log x)^{1/4}/p$. To bound the third sum above, consider any $X \in (y^{10}, x]$ and note that any y-smooth $m \le x$ is certainly not divisible by any prime $\ell \in (y, X^{1/2}]$. This means that

$$\sum_{\substack{m\le X\\ P(m)\le y\\ m\equiv a \pmod p}} 1 \le \sum_{\substack{M\le X/p\\ y<\ell\le X^{1/2} \Longrightarrow M\not\equiv -ap^{-1} \bmod \ell}} 1 \ll \frac{X}{p}\cdot \prod_{y<\ell\le X^{1/2}} \left(1-\frac{1}{\ell}\right) \ll \frac{X(\log x)^{1/4}}{p\log X},$$

where we have written $m = Mp + a$ and invoked Lemma 5.1.1. By partial summation and the above bound, it now follows that the third sum in (5.10) is $\ll (\log x)^{1/4}(\log_2 x)/p$. Collecting all above estimates shows that the number of possible (m, P) with $s(m) \equiv 0 \pmod p$ is $\ll x(\log_2 x)^2/p(\log x)^{3/4} = o(x/p)$. This establishes that $S_2 = o(x/p)$, concluding the proof of Theorem 5.0.1. □

Section 5.4

Concluding remarks

Given our reliance on the Siegel–Walfisz theorem, it seems difficult to extend uniformity in our results past $(\log x)^{K_0}$. It would be interesting to have heuristics suggesting the "correct" range of uniformity to expect. Uniformity in Theorem 5.0.1 certainly fails as soon as p is a bit larger than $x^{1/2}$. To see this, let q, r run over primes up to $\frac{1}{3}\sqrt{x}$. Then each product $qr \le x$ and $s(qr) = q + r + 1 < \sqrt{x}$. Hence, some $m < \sqrt{x}$ has $\gg x^{1/2}(\log x)^{-2}$ preimages $n = qr \le x$. If now $p \ge x^{1/2}(\log x)^3$ (say), then the residue class m mod p contains $s(n)$ for many more than x/p composite $n \le x$.

The reader interested in other work on the distribution of $s(n)$ in residue classes is referred to [6, 5, 57].

Bibliography

[1] A. Akande, *Uniform distribution of polynomially-defined additive functions to varying moduli*, submitted.

[2] L. Alaoglu and P. Erdős, *A conjecture in elementary number theory*, Bull. Amer. Math. Soc. **50** (1944), 881–882.

[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] S. Balasuriya, W. D. Banks, and I. E. Shparlinski, *Congruences and exponential sums with the sum of aliquot divisors function*, Int. J. Number Theory **4** (2008), 903–909.

[6] S. Balasuriya and F. Luca, *Character sums with the aliquot divisors function*, Unif. Distrib. Theory **2** (2007), 121–138.

[7] W. D. Banks, G. Harman, and I. E. Shparlinski, *Distributional properties of the largest prime factor*, Michigan Math. J. **53** (2005), 665–681.

[8] M. B. Barban, *The "large sieve" method and its application to number theory*, Uspehi Mat. Nauk **21** (1966), no. 1, 51–102 (Russian), English translation in Russ. Math. Surv. **21** (1966), no. 1, 49–103.

[9] W. Bruns and J. Herzog, *Cohen–Macaulay rings*, Cambridge Studies in Advanced Mathematics, vol. 39, Cambridge University Press, Cambridge, 1998.

[10] E. R. Canfield, P. Erdős, and C. Pomerance, *On a problem of Oppenheim concerning "factorisatio numerorum"*, J. Number Theory **17** (1983), 1–28.

[11] V. Chandee, X. Li, P. Pollack, and A. Singha Roy, *On Benford's law for multiplicative functions*, Proc. Amer. Math. Soc. **151** (2023), 4607–4619.

[12] B. Chang and G. Martin, *The smallest invariant factor of the multiplicative group*, Int. J. Number Theory **16** (2020), 1377–1405.

[13] J. Cilleruelo and M. Z. Garaev, *Least totients in arithmetic progressions*, Proc. Amer. Math. Soc. **137** (2009), 2913–2919.

[14] T. Cochrane, *Exponential sums modulo prime powers*, Acta Arith. **101** (2002), 131–149.

[15] 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.

[16] ———, *Upper bounds on character sums with rational function entries*, Acta Math. Sin. (Engl. Ser.) **19** (2003), 327–338.

[17] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums*, Acta Arith. **91** (1999), 249–278.

[18] H. Davenport, *On character sums in finite fields*, Acta Math. **71** (1939), 99–121.

[19] H. Delange, *On integral–valued additive functions*, J. Number Theory **1** (1969), 419–430.

[20] ———, *On integral–valued additive functions, II*, J. Number Theory **6** (1974), 161–170.

[21] T. Dence and C. Pomerance, *Euler's function in residue classes*, Ramanujan J. **2** (1998), 7–20.

[22] Z. Dvir, J. Kollár, and S. Lovett, *Variety evasive sets*, Comput. Complexity **23** (2014).

[23] P. Erdös and G. Szekeres, *Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisces Problem*, Acta Univ. Szeged **7** (1934–1935), 95–102.

[24] O. M. Fomenko, *The distribution of values of multiplicative functions with respect to a prime modulus (Russian)*, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **93** (1980), 218–224.

[25] J. B. Friedlander and F. Luca, *Residue classes having tardy totients*, Bull. Lond. Math. Soc. **40** (2008), 1007–1016.

[26] J. B. Friedlander and I. E. Shparlinski, *Least totient in a residue class*, Bull. Lond. Math. Soc. **39** (2007), 425–432, corrigendum in **40** (2008), 532.

[27] M. Z. Garaev, *A note on the least totient of a residue class*, Q. J. Math. **60** (2009), 53–56.

[28] 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.

[29] A. Granville and K. Soundararajan, *Pretentious multiplicative functions and an inequality for the zeta-function*, Anatomy of integers, CRM Proc. Lecture Notes, vol. 46, Amer. Math. Soc., Providence, RI, 2008, pp. 191–197.

[30] G. Halász, *Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen*, Acta Math. Acad. Sci. Hungar. **19** (1968), 365–403.

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

[32] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.

[33] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, sixth ed., Oxford University Press, Oxford, 2008.

[34] I. Kátai, *On the average prime divisors*, Ann. Univ. Sci. Budapest. Sect. Comput. **27** (2007), 137–144.

[35] 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.

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

[37] L. Kuipers and J.-S. Shuie, *A Distribution Property of the Sequence of Fibonacci Numbers*, Fibonacci Quart. **10** (1972), no. 4, 375–376.

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

[39] S. Lang and A. Weil, *Number of points of varieties in finite fields*, American J. Math. **76** (1954), no. 4, 819—-827.

[40] 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. **74** (2024), 143–166.

[41] 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.

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

[43] N. McNew, P. Pollack, and A. Singha Roy, *Intermediate prime factors in specified subsets*, Monatsh. Math. **202** (2023), 837–855.

[44] 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.

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

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

[47] ———, *On a kind of uniform distribution for systems of multiplicative functions*, Litovsk. Mat. Sb. **22** (1982), no. 1, 127–137.

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

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

[50] ———, *Elementary and Analytic Theory of Algebraic numbers*, Springer–Verlag Berlin Heidelberg GmbH, 2004.

[51] W. Narkiewicz and F Rayner, *Distribution of values of $\sigma_2(n)$ in residue classes*, Monatsh. Math. **94** (1982), 133–141.

[52] H. Niederreiter, *Distribution of Fibonacci Numbers mod 5^k*, Fibonacci Quart. **10** (1972), no. 4, 373–374.

[53] I. Niven, *Uniform distribution of sequences of integers*, Trans. Amer. Math. Soc. **98** (1961), 52–61.

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

[55] S. E. Payne, *A second semester of linear algebra*, University of Colorado Denver, 2009.

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

[57] P. Pollack, *Some arithmetic properties of the sum of proper divisors and the sum of prime divisors*, Illinois J. Math. **58** (2014), 125–147.

[58] P. Pollack and C. Pomerance, *Paul Erdős and the rise of statistical thinking in elementary number theory*, Erdös centennial, Bolyai Soc. Math. Stud., vol. 25, János Bolyai Math. Soc., Budapest, 2013, pp. 515–533.

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

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

[61] ———, *Distribution in coprime residue classes of polynomially-defined multiplicative functions*, Math. Z. **303** (2023), no. 4, 20 pages.

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

[63] ———, *Popular values of Euler's function*, Mathematika **27** (1980), 84–89.

[64] F. Rayner, *Weak uniform distribution for divisor functions. I*, Math. Comp. **50** (1988), 335–342.

[65] ———, *Weak uniform distribution for divisor functions. II*, Math. Comp. **51** (1988), 331–337.

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

[67] W. Schwarz and J. Spilker, *Arithmetical functions*, London Mathematical Society Lecture Note Series, vol. 184, Cambridge University Press, Cambridge, 1994.

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

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

[70] S. Selberg, *Zur Theorie der quadratfreien Zahlen.*, Math. Z. **44** (1938), 306–318.

[71] A. Singha Roy, *Joint distribution in residue classes of families of multiplicative functions I*, submitted.

[72] ———, *Joint distribution in residue classes of families of multiplicative functions II*, submitted.

[73] ———, *Joint distribution in residue classes of families of polynomially-defined additive functions*, submitted.

[74] ———, *The Landau–Selberg–Delange method for products of Dirichlet L-functions and applications*, In preparation.

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

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

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

[78] A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 203–210.

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

[80] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen. II*, Acta Math. Acad. Sci. Hungar. **18** (1967), 411–467.

[81] A. Zame, *On a problem of Narkiewicz concerning uniform distribution of sequences of integers*, Colloq. Math. **24** (1972), 271–273.