The Multiplication Table Problem and its Generalizations

by

Alexander (Sacha) Mangerel

A thesis submitted in conformity with the requirements
for the degree of Masters of Science
Graduate Department of Mathematics
University of Toronto

Abstract

The Multiplication Table Problem and its Generalizations

Alexander (Sacha) Mangerel
Masters of Science
Graduate Department of Mathematics
University of Toronto
2014

Motivated by an old question investigated by Erdős (colloquially referred to as the "Multiplication Table" problem) and recent developments in its study by Ford and Tenenbaum, we investigate the fundamental problem of locating the divisors of "most" integers in certain intervals. We generalize Erdős' problem to a certain class of Arithmetical Semigroups using Ford's techniques. We generalize this problem in a different direction by providing explicit estimates of "restricted multiplication tables" in various interesting cases.

Acknowledgements

I would like to thank Dr. J.B. Friedlander for his patience, encouragement and numerous useful mathematical conversations during the development of this thesis. I am tremendously indebted to my parents Libbie and Xavier for their unwavering love and support that has given me the mental and emotional wherewithal to produce this work, as well as for their edits and comments. I would also like to acknowledge my brother Joshua, without whose friendship I could not have accomplished what I have thus far.

Contents

Notation

The letters x, y, z will denote positive real numbers, assumed large, while k, l, m, n, a, b, d will denote (usually positive) integers, or elements of an arithmetical semigroup (see Definition 2.6 or Appendix C). The letters p, q will denote prime numbers or prime elements. The letters C or C' will denote positive, absolute constants, although the identity of these constants may change from line to line. The letter ϵ will be used to denote an arbitrarily small quantity which also may change from line to line. A letter written in bold typeface such as $\mathbf{a}$ will denote a vector, the number and type of its components made clear by the context. We use Landau's standard notations: if f and g are functions of a complex argument z, then: i)$f(z) = O(g(z))$ whenever there exists a positive constant $C > 0$ such that $|f(z)| \leq Cg(z)$ for each z of large enough modulus; ii) $f(z) = o(g(z))$ if the quotient $\frac{f(z)}{g(z)} \to 0$ as $z \to \infty$ (assuming $g(z) \neq 0$ from some point onwards). We will also use the Vinogradov notational conventions: $f(z) \ll g(z)$ if $f(z) = O(g(z))$, $f(z) \gg g(z)$ if $g(z) \ll f(z)$, $f(z) \sim g(z)$ if $\frac{f(z)}{g(z)} \to 1$ as $|z| \to \infty$ and $f(z) \asymp g(z)$ if $g(z) \ll f(z) \ll g(z)$. The implicit constants will always be independent of other variables, unless otherwise indicated using subscripts (e.g. $f(n) \asymp_M g(n)$ denotes the dependence of the implicit constants on the variable M).

In the setting of Algebraic Number Theory, $I, J, \mathfrak{a}, \mathfrak{b}$ etc. will always denote generic integral ideals, while $P, \mathfrak{p}$ will always denote generic prime ideals.

For $d, n \in \mathbb{N}$, we will write $d|n$ if there exists an integer k such that $n = kd$; by analogy, we will write $\mathfrak{a}|\mathfrak{c}$ if there exists an integral ideal $\mathfrak{b}$ such that $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$, noting that this means that $\mathfrak{c} \subseteq \mathfrak{a}$. The Galois group of a number field $K/\mathbb{Q}$ will be denoted $\mathrm{Gal}(K/\mathbb{Q})$ as is standard, or by G, where the context is clear.

We will write $P^+(n)$ and $P^-(n)$ to denote the largest and smallest prime divisors of n, respectively, and in the general context of arithmetical semigroups (which are defined in Chapter 2 and discussed in detail in Appendix C), $P^{\pm}(n)$ will refer to the largest and smallest prime divisors n according to the size of their norms. The functions $\Omega(n) := \sum_{p^\nu || n} \nu$ and $\omega(n) := \sum_{p|n} 1$ will denote the number of prime factors of n, counted with and without multiplicity, respectively. We will label the arithmetic functions defined on arithmetical semigroups that generalize the classical integer counterparts by labelling the functions according to the semigroup, e.g. $\tau_X(n)$ denotes the number of divisors of an element n of an arithmetical semigroup X.

If $a, b \in X$, we denote by $(a, b) \in X$ the *greatest common divisor* of a and b, i.e., an element d of largest norm (which is unique up to multiplication by elements with norm 1) such that $d|a$ and $d|b$. We denote by $[a, b]$ the *least common multiple* of a and b, i.e., the element of smallest norm c such that $a|c$ and $b|c$. When more than one argument is considered, we write $(a_1, \dots, a_k)$ and $[a_1, \dots, a_k]$ to denote the gcd and lcm, respectively, of the k-tuple of elements $a_1, \dots, a_k \in X$.

We will use $\log_k n$ to denote the k-fold iterated *natural* logarithm, i.e., $\log e = 1$, $\log_1 n = \log n$ and $\log_k n = \log(\log_{k-1} n)$ for each $k \geq 2$.

If S is a finite set, then $|S|$ will denote the cardinality of S. Whenever we deal with a sequence of integers $\mathcal{A}$, we refer to the function $A(x) := \sum_{\substack{n \leq x \\ n \in \mathcal{A}}} 1$ as the *counting function* of $\mathcal{A}$.

Chapter 1

Introduction

1.1 The Classical Multiplication Table Problem

Much of Analytic Number Theory is concerned with the behaviour of the primes, which generate the multiplicative semigroup of natural numbers. By studying the nature and size of the prime factors dividing integers, one can analyze the anatomy of integers. The problem of analyzing the divisors of an integer, however, is not approachable with these methods. While the distribution and statistics of prime numbers, described quantitatively by the Prime Number Theorem (PNT) can be used to supply information regarding the number of integers with prime factors with certain constraints, the analogous properties relating to divisors of integers in place of primes is much less tractable, as there is no analogue of the PNT in this scenario.

In the 1930's, a common investigation in Number Theory concerned the study of integer sequences and their sets of multiples. Let $\mathcal{A} \subseteq \mathbb{N}$. The *set of multiples* of $\mathcal{A}$, written $\mathcal{M}(\mathcal{A})$ is the set of all integers $\{na : a \in \mathcal{A}, n \in \mathbb{N}\}$. It is not difficult to see that if $\mathcal{B} \subseteq \mathcal{A}$ is the sequence obtained by removing, in order, the elements of $\mathcal{A}$ that are divisible by smaller elements of $\mathcal{A}$ then $\mathcal{M}(\mathcal{B}) = \mathcal{M}(\mathcal{A})$ (for if $b|a$ then $a \in \mathcal{M}(\{b\})$ and hence $\mathcal{M}(\{a, b\}) = \mathcal{M}(\{b\})$; using this observation repeatedly, one arrives at the above assertion). The sequence $\mathcal{B}$ with this property i.e., such that no two of its elements divide one another, is said to be *primitive*. The study of such sequences was undertaken by Behrend, Pillai and others [12].

Definition 1.1. Let $\mathcal{A} \subseteq \mathbb{N}$ and set $A(x) := \sum_{a \leq x,\ a \in \mathcal{A}} 1$. The *upper and lower natural densities* of $\mathcal{A}$ are $\overline{d}(\mathcal{A}) := \limsup_{x\to\infty} x^{-1}A(x)$ and $\underline{d}(\mathcal{A}) = \liminf_{x\to\infty} x^{-1}A(x)$, respectively. If $\overline{d}(\mathcal{A}) = \underline{d}(\mathcal{A})$, their common value is called the *natural density* of $\mathcal{A}$ and is denoted $d(\mathcal{A})$. A sequence of natural density zero is called a *null sequence*.

It was conjectured that $d\mathcal{M}(\mathcal{A})$ existed for every primitive sequence $\mathcal{A}$. In 1934, Besicovitch gave the following counterexample (see Appendix A for a proof): consider intervals of integers of the form $(y, 2y]$ for y fixed. This is indeed a primitive sequence since $\frac{1}{2} < |u/u'| < 2$ for any $u, u' \in (y, 2y]$. For any $\epsilon > 0$, it is possible to choose a sequence $\{y_k\}_k$ growing sufficiently quickly that the sets of multiples $\mathcal{M}((y_k, 2y_k])$ exist but vanish as $k \to \infty$, and that by taking $\mathcal{A} := \mathbb{N} \cap \bigcup_{k\geq 0}(y_k, 2y_k]$, $\underline{d}(\mathcal{M}(\mathcal{A})) < \epsilon$, while $\overline{d}(\mathcal{M}(\mathcal{A})) \geq \frac{1}{2}$. Hence, if $\epsilon \in (0, \frac{1}{2})$, then $\mathcal{M}(\mathcal{A})$ does not possess natural density.

A consequence of this result is that the sequence of integers with a divisor in an interval of the form $(y, 2y]$ becomes null, as $y \to \infty$ (Erdős provided a more precise formulation of the above counterexample, proving that if $\psi(x) \to 0$ but $x^{\psi(x)} \to \infty$ as $x \to \infty$ (e.g. $\psi(x) = (\log\log x)^{-1}$), any interval of the form

$(y, y^{1+\psi(y)}]$ also has the property that $(y, 2y]$ does [3]). That such a result was surprising suggests that knowledge regarding the statistics of the divisors was limited.

In a seminal paper [16], Hooley introduced the function $\Delta(n) := \max_{u\in\mathbb{R}} \sum_{d|n:v<d\leq ev} 1$ and utilized it in various applications in Number Theory. In the language of probability theory, $\Delta(n)$ is essentially a concentration function for the divisor distribution function $F_n(t) := \tau(n)^{-1} \sum_{d|n,d\leq t} 1$. From this perspective, $\Delta(n)$ provides a tool to study the distribution of divisors of n in fixed intervals. In the early 1980's, Hall (and subsequently Tenenbaum) systematically studied $\Delta(n)$ and its intrinsic connection to divisor problems [13].

The following problem (colloquially christened "The Multiplication Table Problem" by Erdős in the 1950s [4]) is relevant to the study of the distribution of divisors of an integer. Given $N \in \mathbb{N}$, let $A(N)$ denote the set of all products ab, where $1 \leq a, b \leq N$. These are precisely the entries in an N-by-N multiplication table. How many distinct products occur, i.e., what is $|A(N)|$? It is an elementary fact that on a sequence of natural density 1, the number of prime factors (counted with multiplicity) $\Omega(n) \sim \log_2 n$, and for the significant (with respect to natural density) set of integers $\sqrt{x} < n \leq x$, $\Omega(n) \sim \log_2 x$. Therefore, on one hand $\sqrt{x} < a, b \leq x$ implies that $x < ab \leq x^2$ and for most such products, $\Omega(ab) \sim \log_2 x^2 \sim \log_2 x$. On the other hand, the complete additivity of Ω implies that $\Omega(ab) = \Omega(a) + \Omega(b) \sim 2\log_2 x$. This observation (made by Erdős) therefore suggests that the products ab are not generally elements of this density 1 sequence (and thus, in the main, belong to a null sequence). This immediately implies that, at least, $|A(N)| = o(N^2)$. Later work, in particular by Tenenbaum, was done to refine this to a more quantitative statement.

The following device was introduced, both for its independent interest and in order to approach this problem.

Definition 1.2. Let $2 \leq y \leq z \leq x$. The *divisor distribution function* is

$$H(x, y, z) := |\{n \leq x : \exists\ d|n \text{ s.t. } d \in (y, z]\}|.$$

In light of the above remarks regarding the distribution of divisors of integers, a systematic investigation of $H(x, y, z)$ has intrinsic value and lends itself to various applications, among which (Ch. 2 [13], see Appendix B for proofs):

i) The fundamental identity of the Möbius function is that $\sum_{d|n} \mu(d) = 0$ for each $n \geq 2$. In sieving applications, one must often limit the set of divisors of n in this sum to those bounded above by a given parameter y, and it is natural to ask how much the sum over this truncated set of divisors deviates from zero in such a case. For $y \geq 1$, Erdős and Kataí attacked this problem by studying the function $M(n, y) := \sum_{\substack{d|n \\ d\leq y}} \mu(d)$. Erdős and Hall showed [5] that $\limsup_{y\to\infty} d\{n : M(n, y) \neq 0\} = 0$. The following is a quantitative improvement, derived using knowledge of $H(x, y, z)$.

Theorem (Hall,Tenenbaum)**.** *Let* $\epsilon_y := d\{n : M(n, y) \neq 0\}$ *for* $y > 1$. *Then* $\epsilon_y \ll (\log y)^{-\frac{\delta}{1+\delta}}$, *with* $\delta > 0$ *a computable constant.*

The idea behind the proof is that the integers with non-zero $M(n, y)$ must have a divisor $m \leq y$, such that $qm > y$ for any prime $q|n$ not dividing m (otherwise $\mu(m) + \mu(qm) = 0$, since μ is multiplicative and $\mu(q) = -1$). This means that n is counted by $H(x, y/q, y)$, where $q := P^-(n)$.

ii) One can ask how large the divisors of an integer are in proportion to the integer itself. The following theorem, whose proof relies on the asymptotics of $H(x, y, z)$, addresses this question.

Theorem (Hall,Tenenbaum). *Let $t \geq 1, u \in [0,1]$. Then $h(u,t) := d\{n : n^{\frac{1-u}{t}} < d \leq n^{\frac{1}{t}}\}$ is well-defined.*

To prove this, one first replaces the bounds on d in terms of n by bounds in terms of x when $x/\log x < n \leq x$, the remaining values of n being negligible with respect to density. By choosing $y := x^{\frac{1-u}{t}}$ and $z := x^{\frac{1}{t}}$, one can use (modulo technical refinements related to sieve methods) $H(x,y,z)$ to count them. Subject to the precision of the estimates being used for $H(x,y,z)$, one can even provide quantitative bounds for $h(u,t)$.

The seminal paper [27] by Tenenbaum gave strong upper and lower bounds for $H(x,y,z)$, according to the sizes of y and z relative to x. In particular, when $(y,z] \cap \mathbb{N}$ fails to be a primitive set in the sense given earlier, say for $z > 2y$, there is increased interdependence among divisors $d, d' \in (y,z]$ of n, and hence, such n will be overcounted if they are enumerated naïvely among the $\lfloor \frac{x}{d} \rfloor$ integers divisible by d, necessitating the use of different techniques to count them (we give an indication of these difficulties in Appendix D). The main heuristic in Tenenbaum's work is the following: suppose n is squarefree for simplicity. Since $n = \prod_{p|n} p$ and any divisor d of n is a product $\prod_{p \in A} p$, where A is a subset of the prime factors of n, $\log d$ is a partial sum of $\log n = \sum_{p|n} \log p$. Relying on ideas that carry over rigorously to the setting of divisors (Ch. 1 of [13]), Tenenbaum asserted that $\log d$ is uniformly distributed in the logarithmic interval $[0, \log n]$ (this is discussed further below).

Tenenbaum's estimates were later improved to an essentially best possible result by Ford. Using more elaborate probabilistic arguments regarding so-called *order statistics* (see [8] for a description) and ingenious technical manipulations, he removed the uniformity assumption, leading to upper and lower bounds that are sharp up to multiplicative constants (depending on the values of y and z relative to x). The main theorem in [9], in the single case $z = 2y$ used in the applications mentioned above and in the Multiplication Table Problem, is the following:

Theorem (Ford). *Let $3 \leq y \leq \sqrt{x}$. Then*

$$H(x,y,z) \asymp x(\log y)^{-\delta}(\log\log y)^{-\frac{3}{2}}, \tag{1.1}$$

where $\delta := 1 - (1 + \log\log 2)(\log 2)^{-1} > 0$.

(The most general result, valid for all $z \leq \sqrt{x}$, is found in [8]; it is worth mentioning that Koukoulopoulos [20] more recently generalized the Multiplication Table problem to a count of how many distinct products $d_1 \cdots d_k$ emerge from multiplying k-tuples of integers $(d_1, \ldots, d_k) \in \{1, \ldots, N\}^k$, for $k \geq 3$). One can deduce from this theorem the following corollary:

Corollary (Ford). *Let $N \geq 3$. We have*

$$|A(N)| \asymp \frac{N^2}{(\log N)^{\delta}}(\log\log N)^{-\frac{3}{2}}. \tag{1.2}$$

(The proof uses arguments similar to those in Proposition 2.13).

Ford's strategy in estimating $H(x,y,z)$ in the context of (rational) integers is to recast the problem in terms of the clustering of divisors. Define, for $a \in \mathbb{N}$,

$$\mathcal{L}(a) := \bigcup_{d|a} (\log(d/2), \log d], \tag{1.3}$$

and let $L(a)$ denote the Lebesgue measure of $\mathcal{L}(a)$. It is clear that $L(a) \leq (\log 2)\sum_{d|a} 1 = \tau(a)\log 2$, and a large deviation from this number suggests that many intersections $(\log(d'/2), \log d'] \cap (\log(d/2), \log d]$ are non-trivial, and therefore either $d < d' \leq 2d$ or $d' < d \leq 2d'$. Occurrences of this kind undermine the hypothesis that $\{\log d : d|n, d \leq z\}$ is uniformly distributed in $[0, \log n]$. Indeed, with this hypothesis, one expects that the interval $(\log y, \log z]$, of logarithmic length $\log(z/y) = \log 2$, in our case, contains a proportion of size $\frac{\log 2}{\log a}$ of the $\tau(a)$ divisors of a over the interval $[0, \log a]$. Thus, the expectation value of the measure would be $\tau(a)\log 2$, which is not the case when many intersections occur. By establishing estimates for $L(a)$ for appropriate choices of a, he arrives at (1.1).

1.2 A Generalization to Algebraic Number Fields

Algebraic Number Theory demonstrates an analogy between the roles of integral ideals in number fields and integers. Let $K/\mathbb{Q}$ be a number field, i.e., a finite extension field of the field of rational numbers, and let $\mathcal{O}_K$ denote its ring of integers, i.e. the set of all $\alpha \in K$, such that there exists $f(X) \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. The Krull-Schmidt theorem ([7], Ch. 5.3) asserts that any ideal $I \subseteq \mathcal{O}_K$ factors uniquely (up to a permutation in order) into prime ideals, just as rational integers factor uniquely into rational primes, as asserted by the Fundamental Theorem of Arithmetic. The statistics of these prime ideals also follow a Prime Number Theorem of sorts, called the Prime Ideal Theorem (see Chapter 2), proven by Landau in the early 1900's [22]. There are, therefore, many generalizations of results in rational Number Theory to algebraic number fields.

Let $K/\mathbb{Q}$ be a number field of degree M with discriminant Δ_K. For an ideal $\mathfrak{a}$, let $N(\mathfrak{a}) = N_K(\mathfrak{a}) := |\mathcal{O}_K/\mathfrak{a}|$ be its ideal norm (finite because any integral ideal is a torsion-free, finitely generated $\mathbb{Z}$-module with the same free rank as the $\mathcal{O}_K$, and thus has finite index), and let $\mathcal{B}(N) := \{\mathfrak{a} \subset \mathcal{O}_K : N_K(\mathfrak{a}) \leq N\}$, i.e., the set of ideals with norm at most N. Define $A_K(N) := \{\mathfrak{ab} : \mathfrak{a}, \mathfrak{b} \in \mathcal{B}(N)\}$. In analogy to $A(N)$, one might ask how large $A_K(N)$ is with respect to $B(N)^2$.

A related problem is to consider the set $A'_K(N) := \{N(\mathfrak{ab}) : \mathfrak{a}, \mathfrak{b} \in \mathcal{B}(N)\}$ of integers equal to norms of products of ideals. In contrast to a study of $A_K(N)$, studying $A'_K(N)$ requires, in essence, counting the products of ideals without accounting for the multiplicity of prime ideals lying above a given rational prime (as discussed below). To begin a discussion of the strategy behind tackling this problem in the particular case where K is a Galois extension of the rational numbers, we need some preliminaries from Algebraic Number Theory and Galois Theory (see, for example, [1]).

$\mathcal{O}_K$ is a Dedekind domain and therefore admits unique factorization of integral ideals into prime ideals. Let $p \in \mathbb{N}$ be a rational prime. Then the principal ideal $p\mathcal{O}_K$ factors in K as a product $P_1^{k_1} \cdots P_r^{k_r}$, where each P_j is a distinct prime ideal of the extension, with $P_j \cap \mathbb{Z} = (p)$. Moreover, $k_j = 1$ if and only if $p \nmid \Delta_K$, where Δ_K denotes the discriminant of K. Because $\Delta_K \in \mathbb{Z}$, it has only finitely many prime factors and therefore, with the exception of finitely many rational primes, we need only speak of *unramified* primes for which $k_j = 1$ for all j. Let $f(P) := [\mathcal{O}_K/P : \mathbb{Z}/p\mathbb{Z}]$ denote the *relative degree* of the field extension induced by p for P lying above it. Since K is Galois, $\mathrm{Gal}(K/\mathbb{Q})$ acts transitively on the primes lying above a rational prime, and thus $f(P) = f(P')$ for each $P, P'|p\mathcal{O}_K$. We may therefore refer to the relative degree of $f(P)$ as a function of the rational prime p above which it lies. The prime ideals dividing $p\mathcal{O}_K$ satisfy the relation $\sum_{P|p\mathcal{O}_K} f(P) = M$, and thus, according to the previous observation, we may define $\omega_K(p) := M/f(p)$ to be the number of prime ideals in the factorization of an unramified prime p.

Because the extension $K/\mathbb{Q}$ is normal, via a projection of the minimal polynomial, implicitly defined for K, modulo P, the extension of quotient fields $(\mathcal{O}_K/P)/(\mathbb{Z}/p\mathbb{Z})$ is Galois, and its Galois group is cyclic, generated by the Frobenius element σ_P of P, which lifts to an element of $\mathrm{Gal}(K/\mathbb{Q})$. As mentioned, the Galois group of $K/\mathbb{Q}$ acts transitively on the primes in the factorization of p, and, under the action of $\mathrm{Gal}(K/\mathbb{Q})$ induced on the Frobenius elements of these primes, we have $\tau\sigma_P\tau^{-1} = \sigma_{\tau(P)}$. When the Galois group is Abelian, this implies that $\sigma_P = \sigma_{P'}$ for every $P, P'|p\mathcal{O}_K$. Otherwise, the action of conjugation of $\mathrm{Gal}(K/\mathbb{Q})$ generates a non-trivial conjugacy class $\mathcal{C}_P$ containing σ_P, called the *Frobenius class* of P. Because conjugation is an automorphism, all elements of the conjugacy class have the same group order. Hence, the sizes of Frobenius classes depend on the isomorphism class of the Galois group. Let D be the union of a set of Frobenius classes. Then (Ch. 3 of [17]):

Theorem (Chebotarev)**.** *With the notation above,* $|\{p \le x : \sigma_P \in D\}| \sim \frac{|D|}{|Gal(K/\mathbb{Q})|}\frac{x}{\log x}$.

The remarks above imply that the set of all primes with a given relative degree form a union of conjugacy classes, and we may thus partition the set of all prime ideals in K according to these degrees. Let S denote the set of all rational integers that are admissible as relative degrees of primes. This set is finite because any $s \in S$ divides the degree of the extension $[K : \mathbb{Q}]$, which is assumed to be finite. We can assign a number $C_s \le |\mathrm{Gal}(K/\mathbb{Q})|$ to the cardinality of the union of conjugacy classes of primes with relative degree s, and set $\rho_s := C_s[K : \mathbb{Q}]^{-1}$, its density relative to the set of all primes in K, as prescribed by Chebotarev's theorem.

The ideal norm satisfies the formula $N_K(\mathfrak{ab}) = N_K(\mathfrak{a})N_K(\mathfrak{b})$ for any two integral ideals $\mathfrak{a}, \mathfrak{b}$. Further, the ideal norm of a prime P lying over a rational prime with $f(p) = r$ satisfies $N_K(P) = p^r$. Therefore, one may express the norm of any ideal $\mathfrak{I}$ as

$$N(\mathfrak{I}) = \prod_{P|\mathfrak{I}} N_K(P)^\nu = \prod_{s\in S}\left(\prod_{\substack{P|\mathfrak{I}\\ f(P)=s,\, P\cap\mathbb{Z}=(p)}} p^\nu\right)^s . \tag{1.4}$$

Let $\mathcal{P}$ denote the set of all rational primes, and for $s \in S$, let $\mathcal{P}_s := \{p \in \mathcal{P} : f(p) = s\}$. Also, let $\mathcal{N}_s := \{n \in \mathbb{N} : p|n \Rightarrow p \in \mathcal{P}_s\}$. It is clear that $N(\mathfrak{I}) = \prod_{s\in S} m_s^s$, where $m_s \in \mathcal{N}_s$. Moreover, because $\{\mathcal{P}_s : s \in S\}$ forms a partition of $\mathcal{P}$, every ideal norm can be written uniquely in the form of (1.4), up to permutations of divisors. Therefore, the maps

$$\pi_s : \mathbb{N} \to \mathcal{N}_s,\ n \mapsto \prod_{\substack{p^\nu||n\\ p\in\mathcal{P}_s}} p^\nu$$

are well-defined for each s. By determining the number of divisors of $\pi_s(n)$ for each $s \in S$, we can determine the size of $A'_K(N)$.

The above technicalities do not, however, factor into a determination of the order of magnitude of $|A_K(N)|$. Indeed, it will be apparent that with no more than the Prime Ideal Theorem and $|\mathcal{B}(N)|$, referred to above, we can solve that problem using Ford's methodology. In fact, his argument can be applied to a much broader range of settings, namely a certain class of arithmetical semigroups (for a discussion, see Appendix C).

We will prove the following results:

Theorem 1.3. *Let $K/\mathbb{Q}$ be a number field (not necessarily Galois). Then with the notation above, for*

$x \geq 4$ and $3 \leq y \leq \sqrt{x}$,

$$H_K(x, y, 2y) \asymp_K \frac{x}{(\log y)^{\delta}(\log_2 y)^{\frac{3}{2}}}. \tag{1.5}$$

Therefore, we have the estimate

$$|A_K(N)| \asymp_K \frac{N^2}{(\log N)^{\delta}(\log_2 N)^{\frac{3}{2}}}. \tag{1.6}$$

The deduction of the second assertion from the first is made in Chapter 2 (see Proposition 2.13). Note that this order of magnitude has the same form as that given in (1.2), modulo the dependence of implicit constants on the choice of the number field K. The proof, as mentioned, follows Ford's method closely and is, at the very least, expository of his strategy.
Next, we have the following upper and lower bounds on the divisor distribution functions $H_s(x, y, z)$, defined for each $s \in S$, when $z = 2y$.

Theorem 1.4. *Let $N \in \mathbb{N}$ and let $K/\mathbb{Q}$ be a Galois number field of degree $M := [K : \mathbb{Q}]$. Let $s \in S$. Then, uniformly for $2 \leq y \leq \sqrt{x}$,*

$$H_s(x, y, 2y) \asymp_s \frac{x}{(\log x)^{1-\rho_s}(\log y)^{1-\rho_s(1-\delta)}(\log_2(y))^{\frac{3}{2}}}. \tag{1.7}$$

In the next section, we will deduce the following estimate for $|A'_K(N)|$ as a corollary of this last theorem (which we quote again as Proposition 2.14).

Theorem 1.5. *Let $K/\mathbb{Q}$ be a Galois number field and let S be the set of all possible relative degrees of prime ideals of $\mathcal{O}_K$. Set $t := |S|$ and let $A'_K(N)$ denote the set of all norms $N(\mathfrak{ab})$ for $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}(N)$. Then*

$$|A'_K(N)| \asymp N^2 \sum_{A \subseteq \{1,\dots t\}} \frac{N^{2|A|^{-1}(\sum_{\substack{j \in A \\ j \neq 1}} s_j^{-1} - 1)}}{(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}}. \tag{1.8}$$

(The leading order term in any such sum depends on the nature of S, so we leave it in this form in general).
Broadly, the outline of this thesis is as follows. In Chapter 2, we provide lemmata (giving full proofs wherever necessary) to be used in the development of our main theorems. In particular, we prove that, in order to study $|A_K(N)|$ in a general number field and $|A'_K(N)|$ in a Galois number field, it is sufficient to quantitatively describe the functions $H_K(x, y, 2y)$ and $H_s(x, y, 2y)$, respectively. In Chapter 3, we walk through Ford's strategy in a general setting which simultaneously addresses the problems of determining $|A_K(N)|$ and $|A'_K(N)|$ by providing estimates for H_K and for H_s. In Chapter 4, we show how some of the prior arguments apply in the setting of rational integers, to cases in which the set of products is restricted to shifted sums of squares, i.e., $u^2 + v^2 + s = ab$ for s fixed and $a, b \leq N$, as well as shifted squarefree numbers, i.e., $n + s = ab$ where $\mu^2(n) = 1$. Chapter 5 is split into four appendices in which, among other things, we discuss: i) applications of the function $H(x, y, z)$ due to Hall and Tenenbaum; ii) the subject of Arithmetical Semigroups, the theory of which provides the framework for our general treatment of the Multiplication Table problem.

Chapter 2

Preliminaries

In this section, we prove (or cite references to proofs of) results that will be useful in Chapters 3 and 4, with a focus on clarity and completeness. Throughout, we assume that $K/\mathbb{Q}$ is an arbitrary (unless otherwise specified to be Galois) number field, with discriminant Δ_K and degree $[K:\mathbb{Q}]$. All implied constants, unless otherwise indicated, will depend at most on K.
It will be necessary to estimate the number of ideals with norm bounded by x that satisfy a certain constraint on their prime ideal factors. To this end, we need an estimate for the number of ideals with norm bounded by x.

Theorem 2.1 (Dedekind-Weber)**.** *There exists a constant A_K depending only on K such that for any $x \geq 1$,*

$$\sum_{N(\mathfrak{a}) \leq x} 1 = A_K x + O_K\left(x^{1-\frac{1}{m}}\right),$$

where $m := [K:\mathbb{Q}]$.

Proof. See Theorem 11.1.5 of [7] for a guided exposition, and the precise statement of the value of A_K (the error term here is not best possible, but suffices for our application). □

One relevant constraint is that an integral ideal have a large squarefull part. By a *squarefree ideal*, we mean an integral ideal $\mathfrak{a} = \mathfrak{p}_1^{k_1} \cdots \mathfrak{p}_m^{k_m}$, where each $k_j = 1$; in contrast, a *squarefull ideal* has $k_j \geq 2$ for each $1 \leq j \leq m$. It is thus clear that we can decompose any integral ideal $\mathfrak{a}$ as $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$, where $\mathfrak{b}$ is squarefull, $\mathfrak{c}$ is squarefree and the two parts are coprime, by taking $\mathfrak{b}$ to be the product of prime divisors with $k_j \geq 2$.

Corollary 2.2. *For any $3 \leq y \leq \sqrt{x}$, the number of integral ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \leq x$ and squarefull part having norm at least $(\log y)^4$ is $O_K\left(\frac{x}{(\log y)^2}\right)$.*

Proof. This number is clearly

$$\sum_{\substack{N(\mathfrak{b}\mathfrak{c}) \leq x \\ N(\mathfrak{b}) > (\log y)^4}} 1 = \sum_{N(\mathfrak{d}) > (\log y)^2} \sum_{N(\mathfrak{c}) \leq x/N(\mathfrak{d})^2} 1,$$

where $\mathfrak{d}^2 = \mathfrak{b}$. Applying Theorem 2.1, we get a bound of

$$\leq 2A_K x \sum_{N(\mathfrak{d})>(\log y)^2} \frac{1}{N(\mathfrak{d})^2} \leq 2A_K x \int_{(\log y)^2}^{\infty} \frac{du}{u^2} = O_K\left(\frac{x}{(\log y)^2}\right),$$

as claimed. □

As in many problems in classical multiplicative Number Theory, the statistics of prime ideal divisors are important to the arithmetic of ideals. We will thus need a description of these statistics.

Theorem 2.3 (Landau's Prime Ideal Theorem)**.** *Let $\pi_K(x)$ denote the counting function of prime ideals with norm $\leq x$. Then*

$$\pi_K(x) = \frac{x}{\log x}\left(1 + O_K\left(\frac{1}{\log x}\right)\right)$$

Proof. See [23]. □

From Theorem 2.3, we may deduce the following consequences, which shall be play a role in this chapter and the next.

Corollary 2.4 (Mertens' Theorems for Ideals)**.** *The following holds:*
i) There exists a constant c_K depending at most on K such that

$$\sum_{N(\mathfrak{p})\leq x} \frac{1}{N(\mathfrak{p})} = \log_2 x + c_K + O_K\left(\frac{1}{\log x}\right). \tag{2.1}$$

Hence, for any $u < N(\mathfrak{p}) \leq v$,

$$\prod_{u<N(\mathfrak{p})\leq v} (1 - N(\mathfrak{p})^{-1})^{-1} \sim \frac{\log v}{\log u}.$$

ii) For any $\alpha > 1$, $\sum_{N(\mathfrak{p})\leq x} \frac{1}{N(\mathfrak{p})^\alpha} = O_{K,\alpha}(1)$.
iii) We have

$$\sum_{N(\mathfrak{p})\leq x} \log(N(\mathfrak{p})) = x\left(1 + O_K\left(\frac{1}{\log x}\right)\right),$$

as well as

$$\sum_{N(\mathfrak{p})\leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \log x + O_K(1).$$

Proof. These are standard exercises in partial summation. The details are provided below for the sake of completeness.
i) From the theory of Stieltjes integration, we can write

$$\begin{aligned}\sum_{N(\mathfrak{p})\leq x} \frac{1}{N(\mathfrak{p})} &= \int_{2^-}^{x} \frac{1}{t} d\left\{\sum_{N(\mathfrak{p})\leq t} 1\right\} = \int_{2^-}^{x} \frac{1}{t} d\left\{\frac{t}{\log t}(1 + O_K(1/\log t))\right\} \\ &= \int_{2^-}^{x} \frac{dt}{t\log t} - b_K \int_{2^-}^{x} \frac{dt}{t(\log t)^2} + O_K\left(\frac{1}{\log x}\right) \\ &= \log_2 x - \log_2 2 - b_K \frac{1}{\log 2} + O_K\left(\frac{1}{\log x}\right),\end{aligned}$$

where b_K is a constant implied by the error term of Theorem 2.2. This establishes the first claim, where $c_K := -\log_2 2 - b_k \frac{1}{\log 2}$.
We prove ii) and use it to show the second part of i). Since $t^{-(1+\epsilon)}$ is an integrable function on $(1,\infty)$, letting $\epsilon := \alpha - 1 > 0$ (completely determined by α), we have

$$\sum_{N(\mathfrak{p})\leq x} \frac{1}{N(\mathfrak{p})^{1+\epsilon}} = \int_{2^-}^{x} \frac{1}{t^{1+\epsilon}} d\left\{ \sum_{N(\mathfrak{p})\leq t} 1 \right\} \ll \int_{2^-}^{x} \frac{1}{t^{1+\epsilon}} dt \ll_\epsilon 1.$$

The second statement of i) now follows:

$$\begin{aligned}\prod_{u<N(\mathfrak{p})\leq v} (1-N(\mathfrak{p})^{-1})^{-1} &= \exp\left(- \sum_{u<N(\mathfrak{p})\leq v} \log(1-N(\mathfrak{p})^{-1}) \right) = \exp\left(\sum_{u<\mathfrak{p}\leq v} N(\mathfrak{p})^{-1} + \sum_{u<N(\mathfrak{p})\leq v} \sum_{k\geq 2} \frac{1}{kN(\mathfrak{p})^k} \right) \\ &= \exp\left(\log\left(\frac{\log v}{\log u}\right)(1+o(1)) \right) \sim \frac{\log v}{\log u},\end{aligned}$$

since the double sum in the second last line clearly satisfies

$$\sum_{N(\mathfrak{p})\leq v} \sum_{k\geq 2} \frac{1}{kN(\mathfrak{p})^k} \leq \sum_{u<N(\mathfrak{p})\leq v} \frac{1}{N(\mathfrak{p})^2} \frac{1}{1-N(\mathfrak{p})^{-1}} \ll \sum_{u<N(\mathfrak{p})\leq v} \frac{1}{N(\mathfrak{p})^2} = O\left(\frac{1}{u}\right),$$

by ii).
iii) Similarly, we have

$$\sum_{N(\mathfrak{p})\leq x} \log N(\mathfrak{p}) = \int_{2^-}^{x} \log t d\left\{ \sum_{N(\mathfrak{p})\leq t} 1 \right\} = \int_{2^-}^{x} dt + O_K\left(\int_{2^-}^{x} \frac{dt}{\log t} \right) = x + O_K\left(\frac{x}{\log x} \right), \tag{2.2}$$

since $\mathrm{li}(x) := \int_1^x \frac{dt}{\log t} \sim \frac{x}{\log x}$ as $x \to \infty$. The second assertion now follows from

$$\sum_{N(\mathfrak{p})\leq x} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})} = \int_{2^-}^{x} \frac{1}{t} d\left\{ \sum_{N(\mathfrak{p})\leq t} \log N(\mathfrak{p}) \right\}$$

by applying (2.2). □

To evaluate $|A'_K(N)|$, i.e. the number of integers representing products of prime ideals, using Ford's argument, we will need an effective form (with the error term given below) of Chebotarev's theorem in the form of (2.1), valid for each $s \in S$ (for the appropriate definitions, see Chapter 1.2).

Lemma 2.5. *Let $x \geq 3$ and $s \in S$. Then*

$$\sum_{\substack{p\leq x \\ p\in\mathcal{P}_s}} \frac{1}{p} = \rho_s \log_2 x + c_0 + O_s\left(e^{-c_1\sqrt{\log x}} \right)$$

where c_0, c_1 are constants depending at most on s, and ρ_s is the ratio of the size of the union of all conjugacy classes containing Frobenius elements of primes of relative degree s to $|Gal(K/\mathbb{Q})|$ (see Chapter 1.2).

Proof. Define

$$\psi_s(x) := \sum_{\substack{N(\mathfrak{p}^m)\le x \\ \mathfrak{p}\nmid\Delta_K,\ f(\mathfrak{p})=s}} \log(N_K(\mathfrak{p})).$$

Consider the subgroup $H = \langle g\rangle \le \mathrm{Gal}(K/\mathbb{Q})$ for g an element of a conjugacy class counted by C_s, and denote by $\hat{H}$ its group of its characters. Invoking the exact formula derived by Lagarias and Odlyzko (Thm 7.1 in [21]), we have for any $2 \le T \le x$,

$$\psi_s(x) = \rho_s \left(x - \sum_{\chi\in\hat{H}} \overline{\chi}(g) \left(\sum_{\substack{\rho=\beta+i\gamma:\zeta_K(\rho)=0 \\ |\gamma|\le T}} \frac{x^\rho}{\rho} - \sum_{\substack{\rho:\zeta_K(\rho)=0 \\ |\rho|\le\frac{1}{2}}} \frac{1}{\rho} \right) \right) + O\left(\frac{x(\log x)^2}{T}\right),$$

where ζ_K is the Dedekind zeta function for the extension $K/\mathbb{Q}$, and the sum over ρ includes only non-trivial zeros, i.e., excluding $\{-2k : k \in \mathbb{N}\}$. The sum over ρ in brackets will be included in the error term, and we may therefore ignore the contribution of the various characters of $\hat{H}$.
Let $\epsilon > 0$. Heath-Brown's theorem [15] regarding zeros of Hecke L-functions shows that, uniformly in the interval $\sigma \in [\frac{1}{2}, 1]$,

$$N(\sigma, T) := |\{\rho = \beta + i\gamma : \zeta_K(\rho) = 0,\ \beta \in [\sigma, 1],\ |\gamma| \le T\}| \ll T^{(c+\epsilon)(1-\sigma)}(\log T)^A,$$

where $c = c(T) \ge 2$ is a positive constant depending at most on T. By the symmetry of zeros about the line $\sigma = \frac{1}{2}$ and about the real axis,

$$\begin{aligned}
\sum_{\rho:|\gamma|\le T} \frac{x^\rho}{\rho} &= 4 \sum_{1\le k\le \log_2 x} \sum_{\substack{1-2^{-k}\le\rho<1-2^{-(k+1)} \\ |\gamma|\le T}} \frac{x^\rho}{\rho} \le 4x \sum_{1\le k\le\log_2 x} \frac{x^{-2^{-(k+1)}}}{1-2^{-k}} N(1-2^{-k}, T) \\
&\ll x\log^A T \sum_{1\le k\le\log_2 x} \frac{x^{-2^{-(k+1)}}}{1-2^{-k}} T^{(c+\epsilon)2^{-k}} = x\log^A T \sum_{1\le k\le\log_2 x} \frac{(x/T^{2(c+\epsilon)})^{-2^{-(k+1)}}}{1-2^{-k}} \\
&\le x\log_2 x \log^A T \exp\left(\frac{\log 2}{\log x}(\log x - 2(c+\epsilon)\log T)\right) \ll x\log^A T \exp\left(-2(c'+\epsilon)\frac{\log T}{\log x}\right),
\end{aligned}$$

where c' is chosen slightly smaller than c to compensate for the $\log_2 x$ factor in the previous expression. Choosing T such that $\log T = \sqrt{\log x}$, one arrives at

$$\psi_s(x) = \rho_s x + O\left(C_s x(\exp\left(-c''\sqrt{\log x}\right)(\log^{\frac{A}{2}} x + \log^2 x))\right) = \rho_s x + O\left(C_s x \exp\left(-c_1\sqrt{\log x}\right)\right).$$

Note, from the definition of ψ_s, that

$$\psi_s(x) = \sum_{\substack{N_K(\mathfrak{p})\le x \\ \mathfrak{p}\nmid\Delta_K,\ f(\mathfrak{p})=s}} \log(N_K(\mathfrak{p})) + O\left(s \sum_{\substack{p^{ks}\le x \\ k\ge 2}} \log p\right) = \sum_{\substack{N_K(\mathfrak{p})\le x \\ \mathfrak{p}\nmid\Delta_K,\ f(\mathfrak{p})=s}} \log(N_K(\mathfrak{p})) + O_s(x^{\frac{1}{2}}\log x).$$

Thus, by partial summation, we get

$$\begin{aligned}\sum_{\substack{p\leq x\\ p\in\mathcal{P}_s}}\frac{1}{p} &= \sum_{\substack{N_K(\mathfrak{p})\leq x^{\frac{1}{s}}\\ \mathfrak{p}\nmid\Delta_k, f(\mathfrak{p})=s}}\frac{1}{N_K(\mathfrak{p})} = \int_{2^{\frac{1}{s}}}^{x^{\frac{1}{s}}}\frac{1}{t\log t}d\psi_s(t)\\ &= \rho_s\int_{2^{\frac{1}{s}}}^{x^{\frac{1}{s}}}\frac{dt}{t\log t} + O\left(\left(\int_1^{x_0}+\int_{x_0}^{x^{\frac{1}{s}}}\right)\frac{dt}{\log t}\exp\left(-c_1\sqrt{\log t}\right)\right)\\ &= \rho_s\log_2 x + \rho_s(\log\frac{1}{s}-\log_2 2) + O\left(\exp\left(-c_1'\sqrt{\log x}\right)\right),\end{aligned}$$

where x_0 was chosen as large as possible, such that $\log x_0 \geq \exp(c_1\sqrt{\log x_0})$, and c_1' is chosen to bound $(\log x)^{-1}\exp(-c_1\sqrt{\log x})$. This completes the proof. □

We note here that the error term in the above is stronger (i.e., smaller) than $O\left(\frac{1}{\log x}\right)$, which will be needed later (see Lemma 2.4).

We have therefore demonstrated that the semigroups of: i) integral ideals of a number field $K/\mathbb{Q}$; and ii) integers with prime factors constrained to have a fixed relative degree, both have an associated set of prime elements that are statistically well-described. We may therefore prove sieve estimates in the following, more general framework, with subsequent application to our problems (for a more detailed discussion, see Appendix C).

Definition 2.6. An *arithmetical semigroup* is a triple $(X, \mathcal{P}_X, N_X)$ where X is a semigroup (i.e. a multiplicative monoid with identity) generated by a set of elements $\mathcal{P}_X$ and $N_X : X \to \mathbb{N}$ is a function that satisfies the following properties:

a) If 1_X denotes the identity element of X then $N_X(1_X) = 1$;

b) For any $M > 0$, the set $\{x \in X : N_X(x) \leq M\}$ has finite cardinality (informally, the ball induced by N_X of radius x in X is finite).

c) For any $x, y \in X$, $N_X(xy) = N_X(x)N_X(y)$.

When the generating set and norm function N_X are understood, we abuse notation and say that X is an arithmetical semigroup.

With this greater level of generality, we will be able to tackle the estimation of both $|A_K(N)|$ in a general number field K, and $|A_K'(N)|$ when K is Galois, using a single argument, provided in Chapter 3. We note that by assuming Axiom A (see Definition 5.6), which is the analogue of Theorem 2.1 for the number of elements of norm $N_X(a) \leq x$ in a general arithmetical semigroup X, we may prove the analogues of Corollaries 2.2 and 2.4 in X (see Appendix C for an overview). These results are proven the same way, using the norm N_X in place of the norm $N = N_K$. In our subsequent treatment, therefore, we use the more general language of arithmetical semigroups.

Let $(X, \mathcal{P}_X, N_X)$ be an arithmetical semigroup. We will need a way to quantify the number of elements in X whose prime divisors have large norm. This will be shown to be small, and therefore relegated to the error term. To this end, we use the following analogue of a classical sieve result proven by Halberstam and Richert. In the statement below, a *multiplicative function* is a homomorphism f from X into the unit group of a field, i.e., satisfying $f(ab) = f(a)f(b)$, provided that a and b share no prime divisors .

Lemma 2.7. *Suppose f is a real-valued, non-negative, multiplicative function for which there exist $A, B > 0$ such that:*

i) $\sum_{N_X(p)\le x} f(p)\log N_X(p) \le Ax$
ii) $\sum_{\nu\ge 2}\sum_p f(p^\nu)N_X(p)^{-\nu}\log(N_X(p)^\nu) \le B$. *Then for any* $x > 1$,

$$\sum_{N_X(a)\le x} f(a) \le (A+B+1)\frac{x}{\log x}\sum_{N_X(a)\le x}\frac{f(a)}{N_X(a)}$$

Proof. Set $S(x) := \sum_{N_X(a)\le x} f(a)$ and $M(x) := \sum_{N_X(a)\le x}\frac{f(a)}{N_X(a)}$. Then we have

$$S(x)\log x = \sum_{N_X(a)\le x} f(a)\log N_X(a) + \sum_{N_X(a)\le x} f(a)\log\frac{x}{N_X(a)} = S_1 + S_2 + S_3,$$

where, as a consequence of the equation $\log N_X(a) = \sum_{p^\nu||a}\log N_X(p^\nu)$, we have set

$$S_1 := \sum_{N_X(a)\le x}\sum_{\substack{a=mp\\(m,p)=1}} f(mp)\log N_X(p)$$
$$S_2 := \sum_{N_X(p)\le x}\sum_{\nu\ge 2} f(p^\nu)\sum_{\substack{N_X(m)\le\frac{x}{N_X(p)^\nu}\\(m,p^\nu)=1}} f(m)\log(N_X(mp^\nu))$$
$$S_3 := \sum_{N_X(a)\le x} f(a)\log\frac{x}{N_X(a)}.$$

By the trivial inequality $\log y \le y$ for $y \ge 1$, $S_3 \le xM(x)$. Since $\log(N_X(mp^\nu)) \le x\log N_X(p^\nu)$,

$$S_2 \le x\sum_{N_X(p)\le x}\sum_{\nu\ge 2}\frac{f(p^\nu)\log N_X(p)^\nu}{N_X(p)^\nu}M(xN_X(p)^{-\nu}) \le BxM(x).$$

Finally,

$$S_1 \le \sum_{N_X(m)\le x} f(m)\sum_{N_X(p)\le\frac{x}{N_X(m)}} f(p)\log N_X(p) \le AxM(x)$$

and the lemma follows immediately upon division by $\log x$. □

Using Lemma 2.7, we will be able to provide the upper bound implied by the following statement which allows us to focus on elements with prime factors of small norm with negligible losses.

Theorem 2.8. *Let* $\alpha \in (0,1]$ *and let* $(X, \mathcal{P}_X, N_X)$ *be an arithmetical semigroup satisfying an* α*-prime element theorem, i.e.,*

$$\pi_X(x) := |\{N_X(p) \le x : p \in \mathcal{P}_\alpha\}| = \alpha\frac{x}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Write $\Phi_X(x,z) := |\{N_X(n) \le x : N_X(P^-(n)) > z\}|$. *Then, uniformly for* $2 \le y \le \frac{1}{2}x$,

$$\Phi_X(x,z) \asymp_\alpha \frac{x}{(\log x)^{1-\alpha}(\log z)^\alpha}. \tag{2.3}$$

Note that by partial summation (as in Corollary 2.4), the hypothesis on $\pi_X(x)$ implies the estimates

$$\sum_{\substack{N_X(p)\le x\\ p\in\mathcal{P}_X}} N_X(p)^{-1} = \alpha\log_2 x + O(1) \tag{2.4}$$

$$\prod_{\substack{u<N_X(p)\le v\\ p\in\mathcal{P}_X}} (1-N_X(p)^{-1})^{-1} \asymp \left(\frac{\log v}{\log u}\right)^{\alpha}. \tag{2.5}$$

Proof. The proof follows a line of argument suggested in Ch. 0 of [13]. Let $\chi(a,z)$ be the characteristic function of the set $\{N_X(n)\le x : N_X(P^-(n))>z\}$, and note that this is a multiplicative function. It is easy to see that $|\chi(p,z)|\le 1$, with $|\chi(p,z)|=1$ whenever $N_X(p)>z$. For any $\epsilon\in(0,\frac{1}{2})$, and uniformly for $z\le\sqrt{x}$,

$$\sum_{N_X(p)\le x}\chi(p,z)\log N_X(p) = \sum_{z<N_X(p)\le x}\log N_X(p) \ll x$$

$$\sum_{p,\nu\ge 2}\chi(p^\nu,z)\log N_X(p^\nu)N_X(p)^{-\nu} \le \sum_p N_X(p)^{-2(1-\epsilon)}\sum_{\nu\ge 0}N_X(p)^{-\nu} \ll \sum_p \frac{1}{N_X(p)^{2(1-\epsilon)}} \ll 1.$$

Applying Lemma 2.7 and using (2.4) and (2.5), we have

$$\begin{aligned}\Phi_X(x,z) = \sum_{a\le x}\chi(a,z) &\ll \frac{x}{\log x}\sum_{N_X(a)\le x}\frac{\chi(a,z)}{N_X(a)} \le \frac{x}{\log x}\sum_{z<N_X(P^-(a))\le N_X(P^+(a))\le x}\frac{1}{N_X(a)}\\ &= \frac{x}{\log x}\prod_{z<N_X(p)\le x}(1-N_X(p)^{-1})^{-1} \ll \frac{x}{\log x}\cdot\left(\frac{\log x}{\log z}\right)^{\alpha} = \frac{x}{(\log x)^{1-\alpha}(\log z)^{\alpha}}.\end{aligned}$$

This last upper bound holds for all x and z satisfying $x>z$.
For the lower bound, we consider two cases, according to whether or not $x^{\frac{1}{4}}<z\le\frac{1}{2}x$. In the first case, the hypothesis on $\mathcal{P}_X$ implies (counting only prime elements among those with norm $>z$)

$$\Phi_X(x,z) = \sum_{\substack{N_X(a)\le x\\ N_X(P^-(a))>z}} 1 \ge \pi_K(x)-\pi_K(z) = \int_z^x d\pi_K(t) \gg \int_z^x \frac{dt}{\log t} \gg \frac{x-z}{\log x} \gg \frac{x}{(\log x)^{1-\alpha}(\log z)^{\alpha}}.$$

In the second case, i.e., when $2\le x\le x^{\frac{1}{4}}$, let $g(a)$ be a multiplicative function defined by $g(p^\nu)=1$ or 0 according to whether or not $\nu=1$ and $z<N_X(p)\le x^{\frac{1}{3}}$. From Corollary 2.4,

$$\begin{aligned}\Phi_X(x,z)\log x &\ge \sum_{N_X(a)\le x}\chi(a,z)\log N_X(a) \ge \sum_{N_X(a)\le x}\chi(a,z)\sum_{p^k||a}\log N_X(p^k)\\ &= \sum_{z<N_X(p)\le x}\log N_X(p)\sum_{\substack{N_X(m)\le \frac{x}{N_X(p)}\\ N_X(P^-(m))>z}} 1 = \sum_{\substack{N_X(m)\le x\\ N_X(P^-(m))>z}}\ \sum_{z<N_X(p)\le\frac{x}{N_X(m)}}\log N_X(p)\\ &\gg x\sum_{\substack{N_X(m)\le x\\ N_X(P^-(m))>z}}\frac{1}{N_X(m)} \ge x\sum_{N_X(m)\le\sqrt{x}}\frac{g(m)}{N_X(m)},\end{aligned}$$

where the last z term has been dropped because it is small compared to $x/N_X(m)$. Since g is supported

on squarefree elements, we have

$$\Phi_X(x,z)\log x = \prod_{z<N_X(p)\le x^{\frac13}}\left(1+\frac{1}{N_X(p)}\right) - \sum_{N_X(m)>\sqrt{x}}\frac{g(m)}{N_X(m)}$$
$$> \prod_{z<N_X(p)\le x^{\frac13}}\left(1+\frac{1}{N_X(p)}\right) - \frac12\sum_{N_X(m)\ge 1}\frac{g(m)}{N_X(m)}\frac{\log N_X(m)}{\log x}. \tag{2.6}$$

This last term is expressible as

$$\sum_{N_X(m)\ge1} g(m)\frac{\log N_X(m)}{N_X(m)^s} = -\frac{d}{ds}\left(\sum_{N_X(m)\ge1} g(m)N_X(m)^{-s}\right) = -\frac{d}{ds}\exp\left(\sum_{z<p\le x^{\frac13}}\sum_{k\ge1}(-1)^{k-1}N_X(p)^{-sk}k^{-1}\right)$$
$$= \exp\left(\sum_{z<N_X(p)\le x^{\frac13}}\sum_{k\ge1}(-1)^{k-1}N_X(p)^{-sk}k^{-1}\right)\sum_{z<N_X(p)\le x^{\frac13}}(\log N_X(p))\sum_{k\ge1}N_X(p)^{-sk}(-1)^{k-1}$$
$$= \prod_{z<N_X(p)\le x^{\frac13}}\left(1+N_X(p)^{-s}\right)^{-1}\sum_{z<N_X(p)\le x^{\frac13}}\frac{\log N_X(p)}{N_X(p)^s+1}, \tag{2.7}$$

where $s\in\mathbb{C}$ satisfies $\mathrm{Re}(s)=\sigma>1$. In (2.7), the inner sum is $\log(x^{\frac13}z^{-1})+O(1)$ when $s=1$, by Corollary 2.4. In this case, comparing (2.7) to (2.6),

$$\Phi_X(x,z)\log x > \prod_{z<N_X(p)\le x^{\frac13}}(1+N_X(p)^{-1})\left(1-\frac{\log(x^{\frac13}z^{-1})+O(1)}{2\log x}\right)$$
$$= \left(\frac56+O((\log x)^{-1})\right)\prod_{z<N_X(p)\le x^{\frac13}}(1+N_X(p)^{-1}).$$

Again using Corollary 2.4, upon dividing by $\log x$ we get

$$\Phi_X(x,z) \gg \frac{x}{\log x}\prod_{z<N_X(p)\le x^{\frac13}}\frac{1+N_X(p)}{N_X(p)} = \frac{x}{\log x}\prod_{z<N_X(p)\le x^{\frac13}}(1-(1+N_X(p))^{-1})^{-1}$$
$$\asymp \frac{x}{\log x}\left(\frac{\log x}{\log z}\right)^{\alpha} = \frac{x}{(\log x)^{1-\alpha}(\log z)^{\alpha}},$$

and the lower bound implicit in (2.3) holds in the case $2\le z\le x^{\frac14}$ as well.
The uniformity in z then follows by taking constants for which all of the various upper and lower bounds apply. □

The special cases which are of relevance to the determination of $|A_K(N)|$ and $|A'_K(N)|$, respectively, are as follows.

Corollary 2.9. *a) Set $\Phi_K(x,z) := |\{\mathfrak{a}\subset\mathcal{O}_K : N(\mathfrak{a})\le x \text{ and } N(P^-(\mathfrak{a}))>z\}|$. We have, uniformly for $2\le z\le\frac12 x$, $\Phi_K(x,z)\asymp\frac{x}{\log z}$.*
b) For each $s\in S$, set $\Phi_s(x,z) := |\{n\le x : n\in\mathcal{N}_s \text{ and } P^-(n)>z\}|$. We have, uniformly for $2\le z\le\frac12 x$, $\Phi_s(x,z)\asymp\frac{x}{(\log x)^{1-\rho_s}(\log z)^{\rho_s}}$.

These will be implemented in the deductions of Theorems 1.3 and 1.4 in Chapter 3.

Proof. In part a), take X to be the semigroup of integral ideals of $K/\mathbb{Q}$ with norm function $\mathfrak{a} \mapsto N_K(\mathfrak{a})$ and $\mathcal{P}_X$ to be the set of all prime ideals. By Theorem 2.3, one may take $\alpha = 1$.
In part b), take X to be the semigroup of positive integers generated by $\mathcal{P}_s$ which, by definition, is $\mathcal{N}_s$, and take the trivial norm function, i.e. $n \mapsto n$. By Chebotarev's theorem and Lemma 2.5, one may take $\alpha = \rho_s$.

□

A second sieve bound, necessary for the evaluation of a sum in Chapter 3.2, has the following analogue in the general setting of arithmetical semigroups.

Proposition 2.10. *Let $f : X \to \mathbb{R}_+$ be an arithmetic function such that there is some $C > 0$ with $f(pm) \leq Cf(m)$ for each $(m, p) = 1$. Let $\mathcal{I}_x := \{a \in X : a \text{ is squarefree and } N_X(P^+(a)) \leq x\}$. Then for any real $h \geq 0$,*

$$\sum_{a \in \mathcal{I}_x} \frac{f(a)}{N_X(a) \log^h(N_X(P^+(a)) + x/N_X(a))} \ll_{C,h} (\log x)^{-h} \sum_{a \in \mathcal{I}_x} \frac{f(a)}{N_X(a)}. \tag{2.8}$$

Proof. We consider two cases according to whether or not $N_X(a) \leq x^{\frac{1}{2}}$. In the first case, $x/N_X(a) > x^{\frac{1}{2}}$, so that, trivially, $\log^h(N_X(P^+(a)) + x/N_X(a)) \geq 2^{-h} \log^h x$. This suffices to prove the bound in the first case.
In the second case, fix $\epsilon \in (0, \frac{1}{2})$. We may restrict ourselves to the event that $N_X(P^+(a)) \leq x^\epsilon$. Otherwise we have, as before, $\log^h(N_X(P^+(a)) + x/N_X(a)) \geq \epsilon^{-h} \log^h x$, which again suffices. In the event that $N_X(P^+(a)) \leq x^\epsilon$, by applying the hypothesis on f with $p = P^+(a)$, $m = ap^{-1}$ (m and p being coprime since a is squarefree), we have by partial summation,

$$\begin{aligned}
&\sum_{\substack{a \in \mathcal{I}_x \\ N_X(a) > x^{\frac{1}{2}}, N_X(P^+(a)) \leq x^\epsilon}} \frac{f(a)}{N_X(a) \log^h(N_X(P^+(a)) + x/N_X(a))} \\
&\leq C \sum_{\substack{m \in \mathcal{I}_x \\ N_X(a) > x^{\frac{1}{2}-\epsilon}, N_X(P^+(m)) \leq x^\epsilon}} \frac{f(m)}{N_X(m)} \sum_{\substack{N_X(p) \leq x^\epsilon \\ N_X(p) > N_X(P^+(m))}} \frac{1}{N_X(p) \log^h(N_X(p))} \\
&\leq 2C \sum_{\substack{m \in \mathcal{I}_x \\ N_X(m) > x^{\frac{1}{2}-\epsilon}, N_X(P^+(m)) \leq x^\epsilon}} \frac{f(m)}{N_X(m)} \int_{2^-}^{x^\epsilon} \frac{1}{t(\log t)^h} d\left\{ \frac{t}{\log t} \left(1 + O\left(\frac{1}{\log t}\right)\right)\right\} \\
&\leq 2C'(h) \sum_{\substack{m \in \mathcal{I}_x \\ N_X(m) > x^{\frac{1}{2}-\epsilon}, N_X(P^+(m)) \leq x^\epsilon}} \frac{f(m)}{N_X(m)} \int_{2^-}^{x^\epsilon} \frac{dt}{t(\log t)^{h+1}} \\
&= 2C\epsilon^{-h}(\log x)^{-h} \sum_{\substack{m \in \mathcal{I}_x \\ N_X(m) > x^{\frac{1}{2}-\epsilon}, N_X(P^+(m)) \leq x^\epsilon}} \frac{f(m)}{N_X(m)},
\end{aligned}$$

the latter being trivially bounded above by the right side of (2.8). Combining the estimates in these cases finishes the proof. □

Recall the definition (1.3) of the function $L(a)$, which, roughly, measures the amount of clustering of the

divisors of a. Define the following analogue:

$$L_K(\mathfrak{a}) := \text{meas}(\mathcal{L}_K(\mathfrak{a})) := \text{meas}\left(\bigcup_{\mathfrak{d}|\mathfrak{a}}(\log(N(\mathfrak{d})/2), \log N(\mathfrak{d})]\right).$$

Write $\tau_K(\mathfrak{a}) := \sum_{\mathfrak{d}|\mathfrak{a}} 1$, which is the ideal divisor counting function on K. The following inequalities readily follow from the definition:

Lemma 2.11. *Let $\mathfrak{a}, \mathfrak{b}$ be integral ideals in K.*
i) We always have $L_K(\mathfrak{a}) \leq \min(\tau_K(\mathfrak{a}) \log 2, \log N(\mathfrak{a}) + \log 2)$.
ii) If $(\mathfrak{a}, \mathfrak{b}) = 1$ then

$$L_K(\mathfrak{ab}) \leq \min(\tau_K(\mathfrak{a})L(\mathfrak{b}), \tau_K(\mathfrak{b})L(\mathfrak{a})).$$

iii) For any $k \in \mathbb{N}$,

$$L_K(\mathfrak{p}_1 \cdots \mathfrak{p}) \leq \min_{j \leq k} 2^{k-j}(\log 2 + \log N(\mathfrak{p}_1 \cdots \mathfrak{p}_j)).$$

Proof. i) For each divisor $\mathfrak{d}$ of $\mathfrak{a}$, the interval $(\log(N(\mathfrak{d})/2), \log(N(\mathfrak{d}))]$ has length $\log 2$ and there are $\tau_K(\mathfrak{a})$ divisors. Thus, the upper bound $L_K(\mathfrak{a}) \leq \tau_K(\mathfrak{a}) \log 2$ follows in the case of maximum measure when all of the intervals are disjoint. The other one, i.e., $L_K(\mathfrak{a}) \leq \log N(\mathfrak{a}) + \log 2$, follows, since $0 < \log N(\mathfrak{d}) \leq \log N(\mathfrak{a})$ for all $\mathfrak{d}|\mathfrak{a}$, whence $(\log(N(\mathfrak{d})/2), \log N(\mathfrak{d})] \subset (-\log 2, \log N(\mathfrak{a})]$.
ii) By the translation invariance of Lebesgue measure, we have

$$L_K(\mathfrak{ab}) = \text{meas}\left(\bigcup_{\mathfrak{d}|\mathfrak{b}} \{u + \log N(\mathfrak{d}) : u \in \mathcal{L}_K(\mathfrak{a})\}\right) \leq \text{meas}(\mathcal{L}_K(\mathfrak{a})) \sum_{\mathfrak{d}|\mathfrak{b}} 1 = \tau_K(\mathfrak{b})L_K(\mathfrak{a}).$$

Switching the roles of $\mathfrak{a}$ and $\mathfrak{b}$ in the above computation yields $L_K(\mathfrak{ab}) \leq \tau_K(\mathfrak{b})L_K(\mathfrak{a})$ as well, which proves the stated upper bound.
iii) We apply i) and ii) with $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_j$ and $\mathfrak{b} = \mathfrak{p}_{j+1} \cdots \mathfrak{p}_k$ for any $1 \leq j \leq k$. Using $\tau_K(\mathfrak{b}) = 2^{k-j}$ (as any divisor of $\mathfrak{b}$ corresponds to a subset of the $k - j$ primes defining it, of which there are 2^{k-j}), we complete the proof. □

When X is a general arithmetical semigroup with norm N_X we can similarly define $\mathcal{L}_X$ and L_X, changing the endpoints of the intervals in the definition of $\mathcal{L}_K$ to $\log N_X(a)/2$ and $\log N_X(a)$, for $a \in X$. The proof of Lemma 2.11 with L_X in place of L_K is the same.
In his lower bound estimate, Ford considers a specific set of integers $\mathcal{A}$, whose prime factors can be partitioned into disjoint classes. More precisely, he defines a set $\mathcal{B}$ of vectors $\mathbf{b}$ with a fixed number of entries (the sum of which is bounded), and indexes the size of the prime factors of $a \in \mathcal{A}$ according to each component of the vector described. The classes that he considers are selected in a manner that facilitates computation. We will construct these partitions, parametrized by $\alpha \in (0, 1]$, in order to treat all arithmetical semigroups satisfying an α-prime element theorem (see Theorem 2.8).
Let $\lambda_0(\alpha) \in (0, 2)$ and for each $j \geq 1$, select $\lambda_j(\alpha) > \lambda_{j-1}(\alpha)$ maximally such that

$$\sum_{\lambda_{j-1}(\alpha) < N_X(p) \leq \lambda_j(\alpha)} \frac{1}{N_X(p)} \leq \log 2. \tag{2.9}$$

Note that $\{\lambda_j(\alpha)\}_{j \geq 0}$ is well-defined by Corollary 2.4, since the sum over norms is indeed divergent.

Since $\lambda_j(\alpha)$ is chosen to be maximal, if p is the prime element with smallest norm larger than $\lambda_j(\alpha)$ then adding $N_X(p)^{-1}$ to (2.9) makes the sum exceed $\log 2$. We now define the sets $E_j := \{p : N_X(p) \in (\lambda_{j-1}(\alpha), \lambda_j(\alpha)]\}$ and set $\rho = \rho(\alpha) := 2^{\alpha^{-1}} \geq 2$ (this should not be confused with the notation ρ_s associated with $A'_K(N)$). These will serve to produce the partition in question,

Lemma 2.12. *There exists some constant $R > 0$ such that $\rho^{m-R} \leq \log \lambda_m(\alpha) \leq \rho^{m+R}$ for every $m \geq 1$.*

We henceforth fix R in this context.

Proof. Although this is proven in [20], we give a different proof. By Corollary 2.4 and telescoping, for any $m \geq 1$ we have

$$\begin{aligned}\alpha(\log_2 \lambda_m(\alpha) - \log_2 \lambda_0(\alpha)) &= \sum_{j=1}^{m} \sum_{\lambda_{j-1}(\alpha) < N_X(p) \leq \lambda_j(\alpha)} \frac{1}{N_X(p)} + O\left(1 + \sum_{j=1}^{m} \frac{1}{\log \lambda_j(\alpha)}\right) \\ &\leq m \log 2 + O\left(1 + \sum_{j=1}^{m} \frac{1}{\log \lambda_j(\alpha)}\right). \end{aligned} \tag{2.10}$$

Exponentiating, we have (henceforth omitting the dependence on α for convenience)

$$\log \lambda_m \leq C_0 \rho^m \exp\left(C_1 \sum_{j=1}^{m} \frac{1}{\log \lambda_j}\right).$$

Let ν_j denote the smallest norm of a prime larger than λ_j, for each $1 \leq j \leq m$. From (2.10), we have

$$\begin{aligned}\alpha(\log_2 \lambda_m - \log_2 \lambda_0) &\geq m \log 2 - \sum_{j=1}^{m} \frac{1}{\nu_j} + O\left(\frac{1}{\log \lambda_m}\right) \geq m \log 2 - \sum_{j=1}^{m} \rho^{-j/2} + O\left(\sum_{j=1}^{m} \frac{1}{\log \lambda_j}\right) \\ &\geq m \log 2 + O\left(1 + \sum_{j=1}^{m} \frac{1}{\log \lambda_j}\right). \end{aligned} \tag{2.11}$$

The second last inequality above holds because for any j large enough, we trivially have $\frac{1}{\lambda_j} < \frac{1}{2}\alpha^{-1} \log 2$ and hence

$$\lambda_j > \log \lambda_j \gg \exp(\frac{1}{2} j \alpha^{-1} \log 2) = \rho^{j/2}.$$

Exponentiating (2.11), we see that

$$\log \lambda_m \asymp \rho^m \exp\left(C_1 \sum_{j=1}^{m} \frac{1}{\log \lambda_j}\right) \asymp \rho^m \exp\left(C_1 \sum_{j=1}^{m} \rho^{-j}\right) \asymp \rho^m$$

uniformly in m. Therefore, there exists a constant R large enough that $\rho^{m-R} \leq \log \lambda_m(\alpha) \leq \rho^{m+R}$. □

We note here the deductions of $|A_K(N)|$ and $|A'_K(N)|$, i.e., the number of distinct products of integer ideals, and the number of distinct norms of products of integer ideals, respectively, from the expressions for H_K and H_s for each s.

Proposition 2.13. *Let $N \in \mathbb{N}$. Then*

$$H_K\left(\frac{N^2}{2}, \frac{N}{4}, \frac{N}{2}\right) \leq |A_K(N)| \leq 2 \sum_{0 \leq j \leq \frac{\log N}{2 \log 2}} H_K\left(\frac{N^2}{2^j}, \frac{N}{2^{j+1}}, \frac{N}{2^j}\right).$$

Proof. Suppose $\mathfrak{a}, \mathfrak{b}$ are integral ideals with $N(\mathfrak{a}) \in (N/4, N/2]$ and $\mathfrak{b} \in \mathcal{B}(N)$, so that $N(\mathfrak{ab}) \leq N^2/2$ (every ideal counted by $H_K(N^2/2, N/4, N/2)$ has this form). Then trivially, $\mathfrak{a} \in \mathcal{B}(N)$ as well; thus, $\mathfrak{ab} \in A_K(N)$ which, upon taking cardinalities, establishes the lower bound.
For the upper bound, if $\mathfrak{ab} \in A_K(N)$ then $N(\mathfrak{b}) \leq N$ and $N(\mathfrak{a}) \in (N/2^{j+1}, N/2^j]$ for some $j \geq 0$. Thus, $\mathfrak{ab}$ is counted by $H_K(N^2/2^j, N/2^{j+1}, N/2^j)$. It follows that the set $A_K(N)$ is covered by the union of all sets counted by $H_k(N^2/2^j, N/2^{j+1}, N/2^j)$, whose cardinality is bounded above by the sum of these terms over all $j \geq 0$. Note that if $\mathfrak{ab}$ is counted by a term with $j > \frac{\log N}{2 \log 2}$, then $N^2/2^j \leq N^{\frac{3}{2}}$, which gives us

$$\sum_{\frac{\log N}{2 \log 2} < j \leq \frac{\log N}{\log 2}} H_K(N^2/2^j, N/2^{j+1}, N/2^j) \ll N^{\frac{3}{2}} \log N = o(H_K(N^2/2, N/4, N/2)),$$

according to Theorem 1.3. Thus, multiplying each of the first $\frac{\log N}{2 \log 2}$ terms by two more than accounts for these and produces the desired upper bound. □

In light of equation (1.5) in Theorem 1.3 (which is proven in Chapter 3), we have:

$$|A_K(N)| \gg \frac{N^2}{2(\log N - \log 4)^\delta (\log(\log N - \log 4))^{\frac{3}{2}}} \gg \frac{N^2}{(\log N)^\delta (\log_2 N)^{\frac{3}{2}}},$$

and

$$\begin{aligned} |A_K(N)| &\ll \sum_{0 \leq j \leq \frac{\log N}{2 \log 2}} 2^{-j} \frac{N^2}{(\log N - (j+1)\log 2)^\delta (\log(\log N - (j+1)\log 2))} \\ &\ll \frac{N^2}{(\log N)^\delta (\log_2 N)^{\frac{3}{2}}} \sum_{j \geq 0} 2^{-j} \ll \frac{N^2}{(\log N)^\delta (\log_2 N)^{\frac{3}{2}}} \end{aligned}$$

whence follows (1.6) in Theorem 1.3.
The next proposition is a more technical analogue of Proposition 2.13 for $|A'_K(N)|$. For relevant definitions, see Chapter 1.2.

Proposition 2.14. *Let $N \in \mathbb{N}$, set $t := |S|$ and let $\{s_1, \ldots, s_t\}$ be the ordering of the elements of S according to size (and thus $s_1 = 1$). The following estimates hold:*

$$|A'_K(N)| \gg \sum_{\substack{A \subseteq \{1,\ldots,t\} \\ 1 \in A}} H_{s_1}\left(\frac{N^{2(1-\frac{1}{|A|})}}{4}, \frac{N^{1-\frac{1}{|A|}}}{4}, \frac{N^{1-\frac{1}{|A|}}}{2}\right) \prod_{\substack{j \in A \\ j \neq 1}} H_{s_j}\left(\frac{N^{\frac{2}{|A|s_j}}}{4}, \frac{N^{\frac{1}{|A|s_j}}}{4}, \frac{N^{\frac{1}{|A|s_j}}}{2}\right)$$

$$|A'_K(N)| \ll \sum_{\substack{A \subseteq \{1,\ldots,t\} \\ 1 \in A}} \sum_{\mathbf{r} \in [0, \frac{\log N}{2 \log 2}]^{|A|}} H_{s_1}\left(\frac{N^{2(1-\frac{1}{|A|})}}{2^{\sum_{j \in A} r_j}}, \frac{N^{1-\frac{1}{|A|}}}{2^{r_1+1}}, \frac{N^{1-\frac{1}{|A|}}}{2^{r_1}}\right) \prod_{\substack{j \in A \\ j \neq 1}} H_{s_j}\left(N^{\frac{2}{|A|s_j}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{r_j+1}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{r_j}}\right).$$

Note that wherever the sum over components r_j produces a power of 2 exceeding $N^{2(1-|A|^{-1})}$, it contributes nothing to the upper bound.

Proof. For the lower bound, suppose that $n = m_1^{s_1} m_2^{s_2} \cdots m_t^{s_t}$ is counted in the sum on the right side, and let A be the set of all $j \in \{1, \dots, t\}$ with $\pi_{s_j}(n) = 1$. Write $m_j = a_j b_j \le N^{\frac{2}{|A|s_j}}$, where $a_j \in (\frac{N^{\frac{1}{|A|s_j}}}{4}, \frac{N^{\frac{1}{|A|s_j}}}{2}]$ for each $j \neq 1$, and $a_1 \in (N^{(1-|A|^{-1})}/4, N^{(1-|A|^{-1})}/2]$. It follows that $b_j^{s_j} \le \frac{1}{2} N^{\frac{1}{|A|}}$ for each $j \in A$. Hence, $m_1 \le \frac{1}{2} N^{2(1-1/|A|)}$, $m_j \le \frac{1}{2} N^{\frac{2}{|A|s_j}}$ for $j \neq 1$ and $n = ab$, with

$$a := \prod_{j \in A} a_j^{s_j} \le \frac{N}{2^{d_A}} \le N,$$
$$b := \prod_{j \in A} b_j^{s_j} \le \prod_{\substack{j \in A \\ j \neq 1}} N^{\frac{1}{|A|}} = N,$$

where $d_A := \sum_{j \in A} s_j \ge s_1 = 1$. Thus, a and b both correspond to norms of ideals of the form

$$\mathfrak{a} := \prod_{j \in A} \left(\prod_{\substack{P \mid p\mathcal{O}_K \\ p \mid a_j}} P^{\nu_p(a_j)} \right)^{s_j},$$
$$\mathfrak{b} := \prod_{j \in A} \left(\prod_{\substack{P \mid p\mathcal{O}_K \\ p \mid b_j}} P^{\nu_p(b_j)} \right)^{s_j}$$

where ν_p is the p-adic valuation of a_j. Therefore, n is counted as an ideal norm in $A'_K(N)$.
To prove the upper bound, it should be noted that:
i) In light of Theorem 1.3, for any $j \neq 1$ (and hence $s_j \ge 2$) and $r_j \le \frac{\log y}{\log 2}$ (and hence smaller than $\frac{\log x}{2 \log 2}$ so that $\sqrt{x} \le x 2^{-r_j}$), we have

$$\begin{aligned} H_{s_j}(x^{\frac{1}{s_j}}, \frac{y^{\frac{1}{s_j}}}{2^{(r_j+1)}}, \frac{z^{\frac{1}{s_j}}}{2^{r_j}}) &\ll x^{\frac{1}{2}} ((\frac{1}{s_j} \log x)^{1-\rho_{s_j}} (\frac{1}{s_j} \log(y 2^{-(r_j+1)}))^{\rho_{s_j}})^{-\delta} (\rho_{s_j} \log_2(y 2^{-(r_j+1)}))^{-\frac{3}{2}} \\ &\ll x 2^{-r_j} ((\log x)^{1-\rho_{s_1}} (\log(y 2^{-(r_j+1)}))^{-\rho_{s_1}})^{-\delta} (\rho_{s_1} \log_2(y 2^{-(r_j+1)}))^{-\frac{3}{2}} \\ &\ll H_{s_1}(x 2^{-r_j}, y 2^{-(r_j+1)}, y 2^{-r_j}), \end{aligned}$$

because $\rho_{s_1} = M^{-1} \le \rho_{s_j}$ for each $s_j \in S$.
ii) If n_1, n_2 are integers counted by $H_{s_j}(x_j, y_j, z_j)$ for $j = 1, 2$, respectively, then $n_j \le x_j$ with (at least one) of its divisors in the interval $(y_j, z_j]$. This therefore implies that $n_1 n_2 \le x_1 x_2$ has a divisor $d_1 d_2 \in (y_1 y_2, z_1 z_2]$, meaning that $H_{s_1}(x_1, y_1, z_1) H_{s_1}(x_2, y_2, z_2) \le H_{s_1}(x_1 x_2, y_1 y_2, z_1 z_2)$. Inductively, the same inequality holds when we replace two factors n_1, n_2 by any finite number of such factors.
iii) Next, we note that for any $2 \le y \le \sqrt{x}$, if $k \le \frac{1}{2} \log y$ (such that $y 2^{-k} \ge 1$) then

$$H_{s_1}(x, y 2^{-k}, y) = \sum_{j=0}^{k-1} H_{s_1}(x, y 2^{-(j+1)}, y 2^{-j}) \ll_k H_{s_1}(x, y/2, y).$$

We now proceed to prove the upper bound. Suppose $n = N(\mathfrak{a}\mathfrak{b})$ for some $\mathfrak{a}, \mathfrak{b} \in \mathcal{B}(N)$, and write $n = m_1^{s_1} \cdots m_t^{s_t}$. Put $A := \{j \in \{1, \dots, t\} : \pi_{s_j}(n) \neq 1\}$ and $B := \{j \in A : m_j^{s_j} > N^{\frac{1}{|A|}}\}$. For $j \in B$, there is a $k_j \le \frac{|A|}{2}$ such that $m_j \in (N^{(2k_j-1)/|A|}, N^{2k_j/|A|}]$ and has a proper divisor $a_j \in (N^{\frac{k_j}{|A|s_j}} 2^{-(r_j+1)}, N^{\frac{k_j}{|A|s_j}} 2^{-r_j}]$ for some $r_j \ge 0$. For $j \in A \backslash B$, there is analogously some r_j such that m_j

has a divisor in $(N^{\frac{1}{|A|s_j}}2^{-(r_j+1)}, N^{\frac{1}{|A|s_j}}2^{-r_j}]$. If $A = B$ then

$$N^2 \geq m = \prod_{j\in A} m_j^{s_j} > N^{\frac{2}{|A|}\sum_{j\in A} 1} = N^2,$$

a clear contradiction. Thus, $|A\backslash B| \geq 1$. By construction, we have

$$2\log N \geq \log m = \sum_{j\in B} s_j \log m_j + \sum_{j\in A\backslash B} s_j \log m_j > 2|A|^{-1}\log N \sum_{j\in B}(k_j - 1).$$

Therefore, $\sum_{j\in B}(k_j - 1) \leq |A| - 1$, as the left side is an integer strictly smaller than $|A|$.
Denote by $\mathbf{k}$ the integer vector with components k_j for $j \in A$ (with the convention that $k_j = 1$ for $j \in A\backslash B$), and by $\mathbf{r}$ the integer vector with components r_j for $j \in A$. We then see that n is counted by

$$\sum_{A\subseteq\{1,\dots,t\}} \sum_{\mathbf{r}\in[0,\frac{\log N}{2\log 2}]^{|A|}} \sideset{}{^*}\sum_{\mathbf{k}} \prod_{j\in B} H_{s_j}\left(N^{\frac{k_j}{|A|s_j}}, \frac{N^{\frac{k_j}{|A|s_j}}}{2^{(r_j+1)}}, \frac{N^{\frac{k_j}{|A|s_j}}}{2^{r_j}}\right) \prod_{j\in A\backslash B} H_{s_j}\left(N^{\frac{1}{|A|s_j}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{(r_j+1)}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{r_j}}\right),$$

where the asterisk on the sum over $\mathbf{k}$ indicates that the condition $\sum_{j\in B}(k_j - 1) \leq |A| - 1$ holds.
Suppose $\pi_{s_1}(n) = 1$. The number of such n is at most N, as all such numbers must be squarefull. Thus, we may ignore this contribution (since it is negligible with respect to the upper bound being demonstrated). We may therefore assume that $\pi_{s_1}(n) \neq 1$.
To simplify notation, for $\mathbf{k}, \mathbf{r}$ and N fixed, we will write $H_j(\mathbf{k}, \mathbf{r}, N)$ to denote $H_{s_j}\left(\frac{N^{\frac{2k_j}{|A|s_j}}}{2^{r_j}}, \frac{N^{\frac{k_j}{|A|s_j}}}{2^{r_j+1}}, \frac{N^{\frac{k_j}{|A|s_j}}}{2^{r_j}}\right)$.
By applying remarks i), ii) and iii) successively (where $k_j \leq |B|$ for each j) , we have

$$\begin{aligned}
&\prod_{j\in B} H_j(\mathbf{k},\mathbf{r},N) \prod_{j\in A\backslash B} H_j(\mathbf{k},\mathbf{r},N) \leq \prod_{j\in B} H_1(\mathbf{k}-\mathbf{1},\mathbf{r},N) \prod_{j\in A\backslash\{1\}} H_j(\mathbf{1},\mathbf{r},N)\\
&\leq H_{s_1}\left(N^{\frac{2\sum_{j\in B}(k_j-1)}{|A|}}, \frac{N^{\frac{\sum_{j\in B}(k_j-1)}{|A|}}}{2^{r_1+1}}, \frac{N^{\frac{\sum_{j\in B}(k_j-1)}{|A|}}}{2^{r_1}}\right) \prod_{j\in A\backslash\{1\}} H_j(\mathbf{1},\mathbf{r},N)\\
&\leq |B| H_{s_1}\left(\frac{N^{\frac{2(|A|-1)}{|A|}}}{2^{\sum_{j\in A} r_j}}, \frac{N^{\frac{|A|-1}{|A|}}}{2^{r_1+1}}, \frac{N^{\frac{|A|-1}{|A|}}}{2^{r_1}}\right) \prod_{j\in A\backslash\{1\}} H_{s_j}\left(N^{\frac{2}{|A|s_j}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{r_j+1}}, \frac{N^{\frac{1}{|A|s_j}}}{2^{r_j}}\right)
\end{aligned}$$

for every vector $\mathbf{k}$ (where $\mathbf{1} := (1,\dots,1)$). Since each $k_j \leq |A|/2 \leq |S|/2$, there are only a finite number of such vectors. In addition, $|B| \leq [K : \mathbb{Q}]$; thus, the upper bound in the statement of the proposition holds. □

Using Theorem 1.4, we can deduce the appropriate order of magnitude for $|A'_K(N)|$ (as we did for $|A_K(N)|$). Since x and y are of the same order of magnitude, $(\log x)^{1-\alpha}(\log y)^{\alpha} \asymp \log x$. For the lower

bound in Theorem 1.5,

$$\begin{aligned}|A'_K(N)| &\gg \sum_{A\subseteq\{1,\dots,t\}} \frac{N^{2(1-|A|^{-1})}}{4(\log N)^{\delta(1-\rho_{s_1})}(\log N)^{\rho_{s_1}\delta}(\log_2 N^{\frac{3}{2}}} \prod_{\substack{j\in A\\ j\neq 1}} \frac{N^{\frac{2}{|A|s_j}}}{(\log N)^{\delta}(\log_2 N)^{\frac{3}{2}}} \\ &= \sum_{A\subseteq\{1,\dots,t\}} \frac{N^{2+2|A|^{-1}(\sum_{\substack{j\in A\\ j\neq 1}} s_j^{-1}-1)}}{4(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}} \\ &= N^2 \sum_{A\subseteq\{1,\dots,t\}} \frac{N^{|A|^{-1}\left(\sum_{\substack{j\in A\\ j\neq 1}} s_j^{-1}-1\right)}}{4(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}};\end{aligned}$$

for the upper bound,

$$\begin{aligned}|A'_K(N)| &\ll \sum_{A\subseteq\{1,\dots,t\}} \sum_{\mathbf{r}\in[0,\frac{\log N}{2\log 2}]^{|A|}} \frac{N^{2(1-|A|^{-1})}}{2^{\sum_{j\in A} r_j}(\log N)^{\delta}(\log_2 N)^{\frac{3}{2}}} \prod_{\substack{j\in A\\ j\neq 1}} \frac{N^{2|A|^{-1}s_j^{-1}}}{(\log N)^{\delta}(\log_2 N)^{\frac{3}{2}}} \\ &\ll N^2 \sum_{A\subseteq\{1,\dots t\}} \frac{N^{2|A|^{-1}(\sum_{\substack{j\in A\\ j\neq 1}} s_j^{-1}-1)}}{(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}} \sum_{\mathbf{r}\in[0,\frac{\log N}{2\log 2}]^{|A|}} 2^{-\sum_{j\in A} r_j} \\ &\ll N^2 \sum_{A\subseteq\{1,\dots t\}} \frac{N^{2|A|^{-1}(\sum_{\substack{j\in A\\ j\neq 1}} s_j^{-1}-1)}}{(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}}.\end{aligned}$$

We have therefore proven the following theorem:

Theorem 2.15. *Let $K/\mathbb{Q}$ be a Galois number field and let S be the set of all possible relative degrees of prime ideals of $\mathcal{O}_K$. Set $t := |S|$ and let $A'_K(N)$ denote the set of all norms $N(\mathfrak{ab})$ for $N(\mathfrak{a}), N(\mathfrak{b}) \leq N$. Then*

$$|A'_K(N)| \asymp N^2 \sum_{A\subseteq\{1,\dots t\}} \frac{N^{2|A|^{-1}(\sum_{\substack{j\in A\\ j\neq 1}} s_j^{-1}-1)}}{(\log N)^{|A|\delta}(\log_2 N)^{\frac{3}{2}|A|}}.$$

This reduces to Ford's theorem (1.1), as required, when $t = 1$.
Consider, for instance, the case when $K := \mathbb{Q}(\sqrt{d})$, where d is a squarefree integer. In this case, $S = \{1, 2\}$, and the sum above contains two terms (as we require all sets A to be non-empty and contain 1). The term corresponding to $A = S$ then yields the correct order of magnitude and we have:

Corollary 2.16. *If d is a squarefree integer then $|A'_{\mathbb{Q}(\sqrt{d})}(N)| \asymp \frac{N^{\frac{3}{2}}}{(\log N)^{2\delta}(\log_2 N)^3}$.*

Chapter 3

Bounding $H_X(x, y, z)$

We start by adapting Ford's argument ([9], Section 2) to the setting of arithmetical semigroups $(X, \mathcal{P}_X, N_X)$ with an α-prime element theorem, for $\alpha \in (0, 1]$ (see Definition 2.6 and Theorem 2.8 for definitions). As discussed in Chapter 2, this more general formalism has applications in the cases where: i) X is the semigroup of integral ideals, yielding an estimate for the number of distinct products of ideals $|A_K(N)|$; ii) X is the set of integers generated by the primes of the class $\mathcal{P}_s$ for a given $s \in S$, yielding an estimate for the number of distinct norms of products of ideals $|A'_K(N)|$. We deal with the lower bounds in 3.1 and the upper bounds in 3.2. Throughout Chapter 3, all bounds are dependent at most on X (e.g. via a dependence on α), unless otherwise indicated.

3.1 Lower Bounds

The proof of the lower bound consists of reducing the estimation of $H_X(x, y, 2y)$ to a combinatorial problem regarding sets of a partition (see the remarks preceding Lemma 2.12). This interpretation derives from an analysis of the values of $L_X(a)$ for an appropriate choice of semigroup elements $a \in X$. Some of Ford's argument is independent of the setting X, at which point his analysis is sufficient to complete the argument; therefore we need only make the preparatory steps towards this general combinatorial interpretation which is dealt with in his paper.

Theorem 3.1. *If $3 \leq y \leq \sqrt{x}$ then for any $\epsilon > 0$,*

$$H_X(x, y, 2y) \gg_\epsilon \frac{x}{(\log y)^{1+\alpha}(\log x)^{1-\alpha}} \sum_{\substack{N(a) \leq y^\epsilon \\ a \ squarefree}} \frac{L_K(a)}{N(a)}. \tag{3.1}$$

We may clearly assume that y is sufficiently large for the arguments below to make sense. Otherwise, if y is bounded by some fixed constant y_0, an inclusion-exclusion argument regarding the divisibility of an element a by elements $b \in X$ with $N_X(b) \in (y, 2y]$ (a bounded number of elements if we assume Axiom A, as described in Appendix C) akin to (5.1) in Appendix A, gives the lower bound $H_X(x, y, 2y) \gg x \gg \frac{x}{(\log x)^{1-\alpha}}$. For in this case the $\log^{1+\alpha} y$ term and the sum (which has only finitely many bounded terms) in (3.1) are bounded.

Proof. Consider the set of elements $I := apb$ with $N_X(I) \leq x$, where a is squarefree and $N_X(a) \leq y^\epsilon$, p

satisfies $\log(y/N_X(p)) \in \mathcal{L}_X(a)$, and the prime factors of b have norm either larger than $2y$ or contained in the interval $(y^\epsilon, y^{1-\epsilon}]$ (the choice of p makes it possible for b to be trivial if only one of the constraints on prime factors of b is assumed). We will call I with this form *good*. By definition, there is some $d|a$, such that $\log(N_X(d)/2) < \log(y/N_X(p)) \leq \log(N_X(d))$. Thus, exponentiating this inequality and rearranging, one arrives at $y < N_X(pd) \leq 2y$. The divisor pd of I thus belongs to $(y, 2y]$, and hence, any good element is counted by $H_X(x,y,2y)$. Therefore, counting the set of all good elements I provides a lower bound for $H_X(x,y,2y)$. By construction, $2y > p \geq y/N_X(d) \geq y^{1-\epsilon}$; thus, I has only one such representation, as pb contains only prime divisors that are either smaller than $2y$ or found in $(y^\epsilon, y^{1-\epsilon}]$. Thus, we may count good ideals according to the elements a, p and b of their unique factorizations.
Let us bound from below the number of such elements I. There are at least as many b with the above properties as there are elements J with $N_X(J) \leq x/N_X(ap)$ and $N_X(P^-(J)) > 2y$. Theorem 2.8 demonstrates that there are $\gg \frac{x}{N_X(ap)(\log y)^\alpha (\log x)^{1-\alpha}}$ of these. Such elements will occur if $x/N_X(ap) > 4y$, for example. If $N_X(b) \leq x/N_X(ap) \leq 4y$, however, the set of such b is at least as large as the set of elements with prime divisors $\geq y^\epsilon$. Theorem 2.8 also shows that the number of such b in this case is also

$$\gg_\epsilon \frac{x}{N_X(ap)(\log x)^{1-\alpha}(\log y)^\alpha}.$$

It therefore follows that

$$H_X(x,y,2y) \geq |\{I \in X : I \text{ is good}\}| \gg \frac{x}{(\log x)^{1-\alpha}(\log y)^\alpha} \sum_{N_X(a) \leq y^\epsilon} \frac{1}{N_X(a)} \sum_{\log(y/N_X(p)) \in \mathcal{L}_X(a)} \frac{1}{N_X(p)}. \tag{3.2}$$

Finally, note that, using the analogue of Corollary 2.4 for X and Lemma 2.11, the sum over p may be rewritten as

$$\begin{aligned}
&\sum_{d|a} \sum_{y/N_X(d) < N_X(p) \leq 2y/N_X(d)} \frac{1}{N_X(p)} \geq \sum_{d|a} \frac{N_X(d)}{2y} \sum_{y/N_X(d) < N_X(p) \leq 2y/N_X(d)} 1 \\
&= \sum_{d|a} \frac{N_X(d)}{2y} (\pi_X(2y/N_X(d)) - \pi_X(y/N_X(d))) \\
&\gg \frac{1}{\log y} \tau(a) \gg \frac{L_X(a)}{\log y}.
\end{aligned} \tag{3.3}$$

Inserting (3.3) into the lower bound (3.2) for $H_X(x,y,2y)$ yields (3.1). □

At this point, we make use of the partition over prime elements analyzed in Lemma 2.12. Let k, J and M be parameters to be chosen, assuming for the time being that $k \geq 1$ is an integer, $2^{J/2} > J$ and $2M < J$. Also, define

$$\mathcal{B} := \{\mathbf{b} \in (\mathbb{N} \cup \{0\})^J : b_j = 0 \text{ for } i < M, b_j \leq \min(Mj, M(J-j+1)) \text{ and } b_1 + \ldots + b_J = k\}.$$

For each $\mathbf{b} \in \mathcal{B}$, define $\mathcal{A}(\mathbf{b})$ to be the set of squarefree elements a, such that in the factorization of a into primes, b_j of them belong to the set $E_j := \{p : N_X(p) \in (\lambda_{j-1}, \lambda_j]\}$. An element $a \in \mathcal{A}(\mathbf{b})$ thus has no "small" prime factors and its distribution of prime factors is constrained in a symmetric manner. The following lemma shows that k can be choen in such a way that $a \in \mathcal{A}(\mathbf{b})$ contributes to the sum in (3.1).

Lemma 3.2. *There exists $k \in \mathbb{N}$ such that for all $a \in \mathcal{A}(\mathbf{b})$, $N_X(a) \ll_\epsilon y^\epsilon$.*

Proof. Since $p \in E_j$ implies that $N_X(p) \leq \lambda_j$,

$$\log N_X(a) = \sum_{j\leq J} \sum_{\substack{p|a \\ p\in E_j}} \log N_X(p) \leq \sum_{j\leq J} b_j \log \lambda_j \leq M\rho^R\Big(\sum_{M\leq j\leq J/2} j\rho^j + \sum_{J/2<j\leq J} (J-j+1)\rho^j\Big)$$
$$\leq M\rho^R(M\rho^M \sum_{j=0}^{J/2-M} \rho^j + \rho^M \sum_{j=0}^{J/2-M} j\rho^j + \rho^{J+1} \sum_{l=0}^{J/2} l\rho^{-l}).$$

Evaluating these geometric series using the elementary identity

$$\sum_{j\leq m} jx^j = x\frac{d}{dx}\sum_{j\leq m} x^j = x\frac{mx^{m-1}(x-1)-x^m}{(x-1)^2}$$

for $x = \rho$ in the middle sum and $x = 1/\rho$ in the last sum yields an upper bound

$$\log N_X(a) \ll M\rho^R(M\rho^{J/2} + \rho^{M+1}(J/2-M)\rho^{J/2-M-1} + \rho^{J+1}) \ll M\rho^{J+1},$$

where R is the constant introduced in Lemma 2.12. We fix M to be a large constant and set $J+1 = M+k$ with k such that $M\rho^{J+1} < \epsilon \log y$. The choice $k := \left\lfloor \frac{\log_2 y}{\log \rho} - M \right\rfloor$ is sufficient, because $M\rho^{-M} < \epsilon$ for any $\epsilon > 0$ when M is large enough. □

From Theorem 3.1, we derive the following:

Lemma 3.3. *Let $\mathbf{b} \in \mathcal{B}$. Then*

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{L_X(a)}{N_X(a)} \gg \left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)}\right)^2 \left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{W_X(a)}{N_X(a)}\right)^{-1}, \tag{3.4}$$

where

$$W_X(a) := |\{(d_1,d_2) : d_j|a \text{ and } |\log(N_X(d_1)/N_X(d_2))| \leq \log 2\}|.$$

Thus, W_X provides the number of intersections of intervals defining $\mathcal{L}_X$. The proposition below provides an upper bound for the second factor in (3.4).

Proposition 3.4. *For $\mathbf{b}$ as in the Lemma 3.3,*

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{W_X(a)}{N_X(a)} \leq \frac{(2\log 2)^k}{b_M!\cdots b_J!} \sum_{j=M}^{J} \rho^{-j+B_j},$$

where for each $M \leq j \leq J$, $B_j := b_M + \ldots + b_j$.

One sees that the upper bound in Proposition 3.4 is dependent only on the entries of the vector $\mathbf{b}$, and not its association to a set of primes. Defining the quantity

$$f(\mathbf{b}) := \sum_{j=M}^{J} \rho^{(b_M-1)+\ldots+(b_j-1)} = \sum_{j=M}^{J} \rho^{M-1-j+B_j}$$

for each $\mathbf{b} \in \mathcal{B}$, the upper bound in Proposition 3.4 becomes $\ll \frac{(2\log 2)^k}{b_M!\cdots b_J!} f(\mathbf{b})$ (since M is fixed).

Proof of Lemma 3.3. For each divisor $d|a$ define 1_d to be the characteristic function of $(\log N_X(d/2), \log N_X(d)]$. It follows that

$$\tau_X(a)(\log 2) = \sum_{d|a} \int_{\log(N_X(d)/2)}^{\log(N_X(d))} du = \sum_{d|a} \int_{\mathbb{R}} 1_d(u)du.$$

By construction, $L_X(a) = \text{meas}\left(\{u \in \mathbb{R} : \exists d|a \text{ s.t. } 1_d(u) \neq 0\}\right)$. Thus, by the Cauchy-Schwarz inequality,

$$(\log 2)^2 \left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)}\right)^2 \leq \left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{L_X(a)}{N_X(a)}\right)\left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{1}{N_X(a)} \sum_{d,d'|a} \int_{\mathbb{R}} 1_d(u)1_{d'}(u)du\right).$$

The second sum on the right side has non-zero contributions for a given a if and only if $1_d(u) = 1_{d'}(u) = 1$. This occurs on intervals of length at most $\log 2$ whenever $|\log(N_X(d)/N_X(d'))| \leq \log 2$. The cardinality of the set of such ordered pairs of divisors is precisely $W_X(a)$. It therefore follows upon rearrangement that

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{L_X(a)}{N_X(a)} \geq (\log 2)\left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)}\right)^2 \left(\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{W_X(a)}{N_X(a)}\right)^{-1},$$

which implies (3.4). □

Proposition 3.4 provides a bound on the sum over $\frac{W_X(a)}{N_X(a)}$; in order to evaluate the lower bound in (3.4) we will also need a bound for the sum over $\frac{\tau_X(a)}{N_X(a)}$, which is provided by the following lemma.

Lemma 3.5. *For $\mathbf{b} \in \mathcal{B}$, we have*

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)} \geq \frac{(2\log 2)^k}{eb_M! \cdots b_J!}. \tag{3.5}$$

Proof. Each a is a squarefree product of k distinct prime elements, b_j of which come from E_j for each j. As $\tau_X(a) = 2^k$,

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)} \geq 2^k \prod_{j=M}^{J} \frac{1}{b_j!} \left(\sum_{p_{B_j+1}\in E_j} \frac{1}{N_X(p_{B_j+1})}\right) \cdots \left(\sum_{p_{B_{j+1}}\in E_j \setminus \{p_{B_j+1}, \ldots, p_{B_{j+1}-1}\}} \frac{1}{N_X(p_{B_{j+1}})}\right), \tag{3.6}$$

where the normalization by $b_j!$ is needed since the tuples of distinct primes from E_j are permuted (and thus overcounted) in the above product in $b_j!$ ways. In each successive sum, we exclude the primes selected earlier so that all factors are distinct. From the construction of the sequence $\{\lambda_j\}_j$, for each $0 \leq j \leq J-1$ and $B_j + 1 \leq i \leq B_{j+1}$, we have

$$\sum_{p_i\in E_j \setminus \{p_{B_j+1}, \ldots, p_{i-1}\}} \frac{1}{N_X(p_i)} \geq \log 2 - (i - B_j - 1)\frac{1}{\lambda_j} \geq (\log 2 - b_j/\lambda_j).$$

Since there are b_j factors in (3.6) for each j, we may extract $(\log 2)^k$ from the product to get

$$\sum_{a\in\mathcal{A}(\mathbf{b})} \frac{\tau_X(a)}{N_X(a)} \geq \frac{(2\log 2)^k}{b_M! \cdots b_J!} \prod_{j=M}^{J} \left(1 - \frac{b_j}{\lambda_j \log 2}\right)^{b_j}.$$

For M sufficiently large, $b_j^2\lambda_j^{-1} \le (Mj)^2\rho^{-j+R} \le M^4\rho^{-M+R} \le 1$, so that $1-\frac{b_j}{\lambda_j \log 2} \ge 1-\frac{1}{b_j \log 2}$. As $x \mapsto x\log(1-1/x)$ is a convex function for any $x>1$,

$$\begin{aligned}\sum_{a\in\mathcal{A}(\mathbf{b})}\frac{\tau_X(a)}{N_X(a)} &\ge \frac{(2\log 2)^k}{b_M!\cdots b_J!}\exp\left(\sum_{j=M}^{J} b_j\log\left(1-\frac{1}{b_j\log 2}\right)\right) \ge \frac{(2\log 2)^k}{b_M!\cdots b_J!}\exp\left(k\log\left(1-\frac{1}{k\log 2}\right)\right)\\ &\ge \frac{(2\log 2)^k}{b_M!\cdots b_J!}\exp\left(-k\left(\frac{1}{k\log 2}+\frac{1}{(k\log 2)^2}\frac{1}{1-(k\log 2)^{-1}}\right)\right)\\ &\ge \frac{(2\log 2)^k}{b_M!\cdots b_J!}e^{-\frac{1}{2\log 2}},\end{aligned}$$

which yields (3.5). □

From Lemma 2.4 of [9] and its related comments, it follows that $\sum_{\mathbf{b}\in\mathcal{B}}\frac{1}{b_M!\cdots b_J! f(\mathbf{b})} \ge \frac{k^{k-1}}{2k!}$ (the only change to be made is to substitute $x_i = \rho^{-1+b_{M-i+1}}$ in place of the same power of 2, as the same equation $\sum_{i=M+1}^{k}(b_{M-i+1}-1)=0$ holds in both places). Thus, assuming the validity of Proposition 3.4, applying Lemma 3.3 and Stirling's formula,

$$\begin{aligned}\sum_{\mathbf{b}\in\mathcal{B}}\sum_{a\in\mathcal{A}(\mathbf{b})}\frac{L_X(a)}{N_X(a)} &\gg \sum_{\mathbf{b}\in\mathcal{B}}\frac{(2\log 2)^{2k}}{(b_M!\cdots b_J!)^2}\frac{b_M!\cdots b_J!}{(2\log 2)^k f(\mathbf{b})} \gg \frac{(2\log 2)^k k^{k-1}}{k!}\\ &\gg \frac{(2e\log 2)^k}{k^{\frac{3}{2}}} \gg \frac{(\log y)^{\alpha^{-1}(2-\delta)}}{(\log_2 y)^{\frac{3}{2}}},\end{aligned}$$

where $\delta := 1-\frac{\log_2 2+1}{\log 2}$ and $\rho := 2^{\alpha^{-1}}$. Theorem 3.1 then gives

$$\begin{aligned}H_X(x,y,2y) &\gg \frac{x}{(\log y)^{1+\alpha}(\log x)^{1-\alpha}}\frac{(\log y)^{\alpha^{-1}(2-\delta)}}{(\log_2 y)^{\frac{3}{2}}} = \frac{x}{(\log x)^{1-\alpha}(\log y)^{(1+\alpha)-\alpha(2-\delta)}(\log_2 y)^{\frac{3}{2}}}\\ &= \frac{x}{(\log x)^{1-\alpha}(\log y)^{1-\alpha(1-\delta)}(\log_2 y)^{\frac{3}{2}}},\end{aligned} \tag{3.7}$$

which, as we will see, is of the right form to prove Theorems 1.3 and 1.4. We must now verify Proposition 3.4.

Proof of Proposition 3.4. The set of divisors $d, d'|a$ counted by W_K are in 1-1 correspondence with tuples of subsets $\{Y_j(d)\}_{M\le j\le J}, \{Y_j(d')\}_{M\le j\le J}$ indexing the primes that divide them, such that

$$\Big|\sum_{p\in Y_j\triangle Y_j'}\log N_X(p)\Big| \le \log 2, \tag{3.8}$$

where $A\triangle B$ denotes the symmetric difference of the sets A and B. Setting $Y := \bigcup_{j=M}^{J} Y_j(d)$ and $Y' := \bigcup_{j=M}^{J} Y_j(d')$, we need to compute the number of pairs of subsets $Y, Y' \subseteq \{1,\dots,k\}$ that satisfy (3.8). If $Y = Y'$, the sum over the symmetric difference is empty and the bound on the sum is vacuous; thus, any of the 2^k subsets corresponding to divisors of a satisfy (3.8). If $Y \ne Y'$, we can partition the set of Y' into classes $C_j(Y)$ according to the first index $0 \le j \le k-1$ at which $p_{k-j} \in Y$ differs from $q_{k-j} \in Y'$ (the primes being ordered according to their norms). Only the last $j+1$ elements of the pair (Y, Y') differ when $Y' \in C_j(Y)$; we can thus choose Y' in 2^{j+1} ways for each Y. Allowing Y to vary over all 2^K subsets as before, there are thus $2^{j+1}2^k = 2^{k+j+1}$ pairs (Y, Y') that are equal in their first

$k-j-1$ elements.

Note that the bound in (3.8) restricts the choice of only one if all others are fixed. Thus, if we allow p_j to vary for $Y' \in C_{k-j+1}(Y)$, and fix the remaining symmetric difference sum to be $\log U$, then $\log U - \log 2 \le \log N_X(p_j) \le \log U + \log 2$, i.e., $U/2 \le N_X(p_j) \le 2U$. Letting μ_j denote the index l such that $N_X(p_j) \in (\lambda_{l-1}, \lambda_l]$, the α-prime element theorem and the error term in Lemma 2.12 imply that

$$\sum_{U/2 \le N_X(p_j) \le 2U} \frac{1}{N_X(p_j)} \ll \max\left(\frac{\pi_X(2U) - \pi_X(U/2)}{U/2}, \frac{1}{\log \lambda_{\mu_j - 1}} + \frac{1}{\log \lambda_{\mu_j}} \right)$$
$$\ll \frac{1}{\max(\log(2U), \log \lambda_{\mu_j - 1})} \ll \rho^{-\mu_j + 1}.$$

The second last inequality holds because π_X is monotone, while the last holds by Lemma 2.12. The remaining sum over primes will still contribute $(\log 2)^{k-1} \asymp (\log 2)^k$. With all of this data and the fact that $\rho \ge 2$ whenever $\alpha \le 1$, we have

$$\sum_{a \in \mathcal{A}(\mathbf{b})} \frac{W_X(a)}{N_X(a)} \ll \frac{1}{b_M! \cdots b_J!} \sideset{}{^*}\sum_{\substack{Y, Y' \subseteq \{1, \dots k\} \\ Y' \in C_j(Y)}} \prod_{i=M}^{J} \left(\sum_{p_i \in E_i} \frac{1}{N_X(p)} \right)^{b_j} \le \frac{(2 \log 2)^k}{b_M! \cdots b_J!} \left(1 + \sum_{j=1}^{k} \rho^{j+2-\mu_j} \right).$$

As $\mu_j = l$ whenever $B_{l-1} + 1 \le j \le B_l$, the last sum becomes

$$\sum_{j=1}^{k} \rho^{j+2-\mu_j} \le 4 \sum_{l=M}^{J} \rho^{-l} \sum_{B_{l-1}+1 \le j \le B_l} \rho^j \ll \sum_{l=M}^{J} \rho^{-l+b_1+\dots+b_l},$$

which completes the proof of the proposition. □

When X is the arithmetical semigroup of integral ideals in K and $\alpha = 1$, the results of this section give the lower bound for H_K implicit in Theorem 1.3; when X is the arithmetical semigroup of integers with prime factors belonging to the set $\mathcal{P}_s$ for a given $s \in S$ and $\alpha = \rho_s$, the above gives the lower bound for H_s implicit in Theorem 1.4.

3.2 Upper Bounds

The above combinatorial interpretation is applicable when z is any constant multiple of y (estimating $H_X(x,y,Cy)$ instead for $H_X(x,y,2y)$, for any fixed $C > 1$). In all other cases where $y < z \le \sqrt{x}$, the lower bound is analyzed using probabilistic methods independent of the setting of the problem. Ford treats the upper bound in this way in all cases. In this section, we will provide the arguments, in the context of a general semigroup X as in section 3.1, that lead to the application of these methods. This also requires estimating H_X, this time from above, in relation to the function L_X evaluated at squarefree arguments, where all prime divisors are distinct. The assumption of Axiom A (see Appendix C) will be crucial for this.

Theorem 3.6. *For $3 \le y \le \sqrt{x}$, we have uniformly*

$$H_X(x,y,2y) \ll \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y} \le t \le x} \frac{1}{(\log t)^{1+\alpha}} \sum_{\substack{N(P^+(m)) \le t \\ m \text{ squarefree}}} \frac{L_X(m)}{N_X(m)}. \tag{3.9}$$

Proof. As suggested by the (3.9), most of the analysis will involve squarefree elements. It will be convenient to consider a with a squarefull part bounded in norm by $(\log x)^{2\gamma}$, where $\gamma \geq 2$ is a constant to be chosen. By Corollary 2.2, there are $O\left(\frac{x}{(\log x)^{\gamma}}\right)$ elements with squarefull part not satisfying this. For large enough γ, these are negligible in number.

We decompose the remaining elements in the form $a = bm$, where b is squarefull, m is squarefree and b, m coprime. If a is counted by H_X, there is some pair of divisors $d|b, d'|m$, such that $N_X(dd') \in (y, 2y]$. Hence,

$$H_X(x,y,2y) = \sum_{N_X(b) \leq (\log x)^{2\gamma}} \sum_{d|b} H_X^*\left(x/N_X(b), y/N_X(d), 2y/N_X(d)\right) + O\left(\frac{x}{(\log x)^{\gamma}}\right), \tag{3.10}$$

where H_X^* is the analogue of H_X that counts only those *squarefree* elements with a divisor in a given interval. To bound each term H_X^* here, we will dyadically decompose $(x/(\log x)^{2\gamma}, x]$ into a partition of intervals of the form $(u/2, u]$ and count the number of contributing terms in each interval To do this, we consider the difference $H_X^*(u, v_1, 2v_1) - H_X^*(u/2, v_1, 2v_1)$ for some choice u, v_1 to be determined, assuming only that $2v_1^2 < u$.

The squarefree elements counted in the above difference are of the form mm' such that $N_X(mm') \in (\frac{1}{2}u, u]$ and either $N_X(m) \in (v_1, 2v_1]$ or $N_X(m') \in (v_1, 2v_1]$. We would like to decompose mm' according to the size of its prime divisors as we did in 3.1. To this end, we order the prime divisors of mm' according to norm, writing $mm' = I_1 I_2 I_3$, where $P^+(I_j) < P^-(I_{j+1})$ for $j = 1, 2$ and I_2 is prime. According to whether or not $N_X(P^(m)) < N_X(P^+(m'))$, if we choose I_2 to be the largest prime factor of m or m' then we have either $m|I_1 I_2$ or $m'|I_1 I_2$. If we set $w_1 := 2v_1$, $v_2 := u/4v_1$ and $w_2 := u/v_1$ (4 appears because the product of any two numbers from $(v_1, w_1]$ and $(v_2, w_2]$ is between $u/2$ and u), we have $\tau(I_1 I_2, v_j, w_j) \geq 1$ for either $j = 1$ or 2. In either case, the fact that $I_1 I_2$ has a divisor larger than v_j implies trivially that $I_1 I_2 > v_j$. Thus,

$$N_X(P^-(I_3)) > N_X(I_2) \geq v_j / N_X(I_1).$$

By Theorem 2.8, the number of I_3 with $N_X(I_3) \leq u$ and smallest prime divisor of norm at least $N_X(I_2)$ is $\ll \frac{u}{N_X(I_1 I_2)(\log u)^{1-\alpha}(\log N_X(I_2))^{\alpha}}$. If $j = 1$, $\log(2v_1/N_X(I_2))$ is in an interval of $\mathcal{L}_X(mm')$. If $j = 2$, then one of $c \in \{1, 2\}$, $\log(2cv_2/N_X(I_2))$ is an interval of $\mathcal{L}_X(mm')$. It follows that

$$\begin{aligned} H_X^*(u, v_j, w_j) - H_X^*(u/2, v_j, w_j) &\leq \sideset{}{^*}\sum_{N_X(I_1 I_2 I_3) \in (x/2, x]} 1 \\ &\ll \frac{x}{(\log x)^{1-\alpha}} \sum_{N_X(I_1) \leq x} \frac{1}{N_X(I_1)} \sum_{\substack{\log(cv_j/N_X(I_2)) \in \mathcal{L}_K(I_1) \\ N_X(I_2) > N_X(P^+(I_1))}} \frac{1}{N_X(I_2)(\log N_X(I_2))^{\alpha}}, \end{aligned} \tag{3.11}$$

where the asterisk on the sum indicates that: i) $N_X(P^+(I_j)) < N_X(P^-(I_{j+1}))$ for $j \in \{1, 2\}$; ii) I_2 is prime. In the second line, c is either 2 or 4. It will be convenient (in order to invoke the estimate from Proposition 2.10) to bound $\log N_X(I_2) \geq \max(\log(N_X(P^+(I_1))), \log(v_j/N_X(I_1))$. The inner sum of (3.11) becomes a sum over those primes in $(cv_j/N_X(I_1), 2cv_j/N_X(I_1)]$ that exceed $N_X(P^+(I_1))$. Therefore, by applying the α-prime element theorem as in section 3.1, on each of the $\leq \frac{L_K(I_1)}{\log 2}$ disjoint

intervals, we have

$$\sum_{I_2 \text{ prime}}^{*} \frac{1}{N_X(I_2)} \ll L_K(I_1)(\pi_K(2cv_j/N_X(I_1)) - \pi_K(cv_j/N_X(I_1))) \min\left(\frac{1}{N_X(P^+(I_1))}, \frac{1}{v_j/N_X(I_1)}\right)$$
$$\ll \frac{L_K(I_1)}{\log(\max(N_X(P^+(I_1)), v_j/N_X(I_1)))}.$$

By reinserting this last expression into (3.11), we get

$$H_X^*(u,v_j,w_j) - H_X^*(u/2,v_j,w_j) \leq \sum_{N_X(I_1I_2I_3)\in(u/2,u]}^{*} 1$$
$$\ll \frac{u}{(\log u)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \sum_{P^+(N_X(I_1))\leq t} \frac{L_K(I_1)}{N_X(I_1)\log^{1+\alpha}(\max(N_X(P^+(I_1)), v_j/N_X(I_1)))}. \tag{3.12}$$

Let $b \in X$ be a squarefull element that satisfies $N_X(b) \leq (\log x)^{2\gamma}$ and let $d|b$. Dyadically decomposing $(\frac{x}{(\log x)^{2\gamma}}, x]$ into subinterval $(x2^{-(l+1)}, x2^{-l}]$ with $l \leq 2\gamma \log_2 x$, as mentioned earlier, and applying this (3.12) with $u = 2^{-l}x$ for each l, we get

$$H_X\left(\frac{x}{N_X(b)}, \frac{y}{N_X(d)}, \frac{2y}{N_X(d)}\right) \ll \sum_{l\leq 4\log_2 x} \left(H_X^*\left(\frac{x2^{-l}}{N_X(b)}, \frac{y}{N_X(d)}, \frac{2y}{N_X(d)}\right) - H_X^*\left(\frac{x2^{-(l+1)}}{N_X(b)}, \frac{y}{N_X(d)}, \frac{2y}{N_X(d)}\right)\right)$$
$$\ll \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \sum_{l\leq 4\log_2 x} 2^{-l} \sum_{N_X(P^+(m))\leq t} \frac{L_X(m)}{N_X(mb)\log^{1+\alpha}(\max(N_X(P^+(m)), y/N_X(m)))}$$
$$\ll \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \sum_{N_X(P^+(m))\leq t} \frac{L_K(m)}{N_X(mb)\log^{1+\alpha}(\max(N_X(P^+(m)), y/N_X(m)))}.$$

Applying Proposition 2.10 with $h = 1+\alpha$ for each t, we can bound (3.10) as

$$H_X(x,y,2y) \ll \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \frac{1}{(\log t)^{1+\alpha}} \sum_{\substack{N_X(P^+(m))\leq t \\ m \text{ squarefree}}} \frac{L_X(m)}{N_X(m)} \sum_{N_X(b)\leq(\log y)^{2\gamma}} \sum_{d|b} \frac{1}{N_X(b)} + O\left(\frac{x}{(\log x)^{\gamma}}\right)$$
$$= \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \frac{1}{(\log t)^{1+\alpha}} \sum_{\substack{N_X(P^+(m))\leq t \\ m \text{ squarefree}}} \frac{L_X(m)}{N_X(m)} \sum_{N_X(b)\leq(\log y)^{2\gamma}} \frac{\tau_X(b)}{N_X(b)} + O\left(\frac{x}{(\log x)^{\gamma}}\right),$$

recalling that each b is a squarefull element. Note that the smallest possible value of the factor $(\log x)^{-(1-\alpha)}(\log t)^{-(1+\alpha)}$ is $(\log x)^{-2}$; we may thus choose $\gamma = 2+\epsilon$ for any $\epsilon > 0$. We will show that the inner sum over b is then finite, which proves (3.9).

Denoting by χ the characteristic function of the set of squarefull elements, it is easy to see that $a \mapsto \frac{\tau_X(a)}{N_X(a)}\chi(a)$ is a multiplicative function. We therefore have the Euler product

$$\sum_{a \text{ s.full}} \frac{\tau_X(a)}{N_X(a)^s} = \prod_{p \text{ prime}} \left(1 + \sum_{j\geq 2} \frac{\tau_X(p^j)}{N_X(p)^{js}}\right) \tag{3.13}$$

for $\mathrm{Re}(s) > 1$. This converges if, and only if,

$$\left| \sum_{\nu \geq 2} \sum_{p} \frac{\nu+1}{N_X(p)^{\nu s}} \right| \leq \sum_{\nu \geq 2} \sum_{p} \frac{1}{N_X(p)^{(\nu-\epsilon)\sigma}} < \infty.$$

for any $\epsilon \in (0,1)$ [28]. Corollary 2.2 implies that this also holds for $s = 1$. Thus, the bound claimed in our theorem holds uniformly over $y \leq \sqrt{x}$. □

In order to apply Ford's method (which involves statistics regarding the ordering of a fixed number of random variables distributed in an interval), we need to partition the sum on the right side of (3.9) according to the number of prime divisors of the element m. Let $\omega_X(m)$ denote the number of prime divisors of $m \in X$, and suppose $\omega_X(m) = k$, for some $k \in \mathbb{N}$. Let P be a real number with $P > e$, such that $N_X(P^+(m)) \leq P$. Let $\{p_1, \ldots, p_k\}$ be an enumeration of the prime divisors of m, such that $N_X(p_i) \leq N_X(p_{i+1})$, for each $1 \leq i \leq k-1$. Finally, let $Z_j(m) := \frac{\log_2 N_X(p_j)}{\log_2 P}$, for $1 \leq j \leq k$. The random variables $Z_1, \ldots, Z_k$ will be analyzed using Ford's method.
Set

$$T_k(P) := \sum_{\substack{N_X(P^+(m)) \leq P, \omega_X(m)=k \\ m \text{ squarefree}}} \frac{L_X(m)}{N_X(m)}.$$

Let $v := \left\lfloor \frac{\log_2 P}{\psi} \right\rfloor$ for $\psi := \alpha^{-1} \log 2$ and let $\beta := 2 \log 2$. Note that if P is fixed and $k \geq \beta v = 2\alpha \log_2 P$, we must have $\tau_X(m) = 2^k$ and $L_K(m) \leq 2^k \log 2$. Hence,

$$\begin{aligned} \sum_{k \geq \beta v} T_k(P) &\leq \sum_{k \geq \beta v} 2^k \log 2 \sum_{\substack{N_X(P^+(m)) \leq P \\ \omega_K(m)=k}} \frac{1}{N_X(m)} \\ &\leq \sum_{k \geq \beta v} \frac{2^k}{k!} \left(\sum_{N_X(p) \leq P} \frac{1}{N(p)} \right)^k = \sum_{k \geq \beta v} \frac{(2\alpha \log_2 P + O(1))^k}{k!}. \end{aligned}$$

Note that

$$\sum_{k \geq 2t} \frac{t^k}{k!} = \frac{t^t}{t!} \left(1 + \sum_{k \geq 2t+1} \prod_{j=1}^{k-t} \left(2 + \frac{j}{t} \right)^{-1} \right) \leq \frac{t^t}{t!} \left(1 + \sum_{l \geq 1} (2 + \frac{1}{t})^{-l} \right) = \frac{t^t}{t!} \left(1 + \frac{1}{1 + t^{-1}} \right) \ll \frac{t^t}{t!}. \tag{3.14}$$

Conversely, if $0 < \eta < 1$ and we set $m := \lfloor \eta t \rfloor + 1$,

$$\begin{aligned} \sum_{k \leq \delta t} \frac{t^k}{k!} &\leq \frac{t^m}{m!} \left(1 + \sum_{k \leq \delta t} \prod_{j=1}^{t-k} \left(1 - \frac{j}{t} \right) \right) = \frac{t^m}{m!} \left(1 + \sum_{k \leq \delta t} \exp \left(\sum_{j=1}^{t-k} \log(1 - j/t) \right) \right) \\ &\ll \frac{t^m}{m!} \sum_{k \leq \delta t} \exp \left(-\frac{(t-k)(t-k+1)}{2t} \right) = \frac{t^m}{m!} \sum_{k \leq \delta t} \exp \left(-\frac{1}{t} k^2 \right) \leq \frac{t^{m+1}}{m!}. \end{aligned} \tag{3.15}$$

For $\eta := \frac{1}{2 \log 2}$, for instance, $m + 1 < t$ when P is large enough. In this case, which occurs, in particular, when $t = \beta v$, the sum is bounded above by $\frac{t^t}{t!}$.

From (3.14), we have the bound

$$\sum_{k\geq 2\beta v} T_k(P) \ll \frac{(2\alpha \log_2 P + O(1))^{\beta v}}{(\beta v)!}.$$

Thus, it remains to bound $\sum_{1\leq k<2\beta v} T_k(P)$.

Theorem 3.7. *Suppose $1 \leq k < 2\beta v$. Then*

$$T_k(P) \ll (2\alpha \log_2 P)^k \frac{1+(v-k)^2}{(k+1)!(2^{k-v}+1)}. \tag{3.16}$$

Let us assume for the moment that this theorem is valid. There is a change in behaviour of (3.16) at $k = v$. For $k \leq v$, we have $1 + 2^{k-v} \leq 2$, and (3.15) (because the sum converges by comparison to the integral of x^2e^{-x}) and (3.16) therefore suggest that

$$\sum_{1\leq k\leq v} T_k(P) \ll \sum_{1\leq k\leq v} \frac{((v-k)^2+1)(2\alpha\log_2 P)^k}{(k+1)!} \ll \frac{(2\alpha\log_2 P)^v}{(v+1)!}.$$

When $v+1 \leq k \leq 2\beta v$,

$$\sum_{v+1\leq k\leq 2\beta v} T_k(P) \ll \sum_{v+1\leq k\leq 2\beta v} \frac{((v-k)^2+1)}{2^{k-v}} \frac{(2\alpha\log_2 P)^k}{(k+1)!} \leq \frac{(2\alpha\log_2 P)^v}{(v+1)!} \sum_{k\geq v} \frac{(v-k)^2+1}{(\log 2)^{-(k-v)}} \ll \frac{(2\alpha\log_2 P)^v}{(v+1)!}.$$

Hence, by Stirling's approximation,

$$\sum_{k\geq 1} T_k(P) \ll \frac{(2\alpha\log_2 P v^{-1})^v v^v}{(v+1)v!} \asymp \frac{(2\alpha e\psi)^v}{v^{\frac{3}{2}}} \asymp \frac{(\log P)^{\psi^{-1}(\log(2\alpha e\psi))}}{(\log_2 P)^{\frac{3}{2}}}. \tag{3.17}$$

Since $\psi = \alpha^{-1}\log 2$, the exponent of $\log P$ in (3.17) is

$$\frac{1+\log(2\log 2)}{\alpha^{-1}\log 2} - (1+\alpha) = \alpha(2-\delta) - (1+\alpha) = \alpha(1-\delta) - 1$$

which is clearly negative for any $\alpha \in (0,1]$. Thus, when P is selected from the interval $[\sqrt{y}, x]$, (3.17) is maximized at $P = \sqrt{y}$. Therefore,

$$\begin{aligned} H_X(x,y,2y) &\ll \frac{x}{(\log x)^{1-\alpha}} \max_{\sqrt{y}<t\leq x} \frac{1}{(\log t)^{1+\alpha}} \sum_{k\geq 1} T_k(t) \ll \max_{\sqrt{y}<t\leq x} \frac{x(\log t)^{\alpha(1-\delta)-1}}{(\log x)^{1-\alpha}(\log_2 t)^{\frac{3}{2}}} \\ &\ll \frac{x}{(\log x)^{1-\alpha}(\log y)^{1-\alpha(1-\delta)}(\log_2 y)^{\frac{3}{2}}}, \end{aligned}$$

which is equal in magnitude to the lower bound (3.7) from Chapter 3.1. We must now prove Theorem 3.7.

Proof of Theorem 3.7. The theorem is proven by applying Ford's order statistics method, which is essentially independent of the setting of the problem. We need only provide the setup for this application, as follows. Factor $m = p_1 \cdots p_k$, where $N_X(p_j) < N_X(p_{j+1})$ for each j and $N_X(p_k) \leq P$. Let μ_j denote the index l of λ_l such that $p_j \in (\lambda_{l-1}, \lambda_l]$. Let $\mu := (\mu_1, \ldots, \mu_k)$ and set $F(\mu) :=$

$\min_{1\le l\le k} 2^{-l}\,(\rho^{\mu_1}+\ldots+\rho^{\mu_k}+1)$. By Lemma 2.12,

$$L_X(m) \le \min_{1\le l\le k} \tau(p_1\cdots p_l)(\log 2+\log N_X(p_1)+\ldots+\log N_X(p_l)) \le \min_{1\le l\le k} 2^l(1+\log\lambda_{\mu_1}+\ldots+\log\lambda_{\mu_l})$$
$$\le 2^{k+R}\min_{1\le l\le k} 2^{-l}(1+\rho^{\mu_1}+\ldots+\rho^{\mu_l}) \le 2^k F(\mu).$$

Let $J := \{\mathbf{j}\in(\mathbb{N}\cup\{0\})^k : 0\le j_1\le\ldots\le j_k\le v+R+1\}$. Since $v+1\ge\frac{\log_2 P}{\log\rho}$ and $\mu_k\log\rho\log_2 N_X(p_{\mu_k})\le\log_2 P$, the set J contains all of the vectors μ that represent orderings of prime divisors of those m which are counted by $T_k(P)$. It follows that if b_j denotes the number of prime factors in the set E_j, we have

$$T_k(P) \le 2^{k+R}\sum_{\mathbf{j}\in J} F(\mathbf{j}) \sum_{\substack{N_X(p_1)<\ldots<N_X(p_k)\\ p_i\in E_{j_i}}} \frac{1}{N_X(p_1)\cdots N_X(p_k)}$$
$$\le 2^{k+R}\sum_{\mathbf{j}\in J} F(\mathbf{j}) \prod_{j=0}^{v+R+1}\frac{1}{b_j!}\left(\sum_{p\in E_j}\frac{1}{N_X(p)}\right)^{b_j} \le \frac{2^R(2\log 2)^k}{b_0!\cdots b_{v+R+1}!}\sum_{\mathbf{j}\in J}F(\mathbf{j}),$$

since $b_0+\ldots+b_{v+R+1}=k$ by construction. The remainder of the argument now follows from the end of Lemma 3.5 and Lemma 3.6 of [9] (the crucial point in the proof of Lemma 3.6 is that the series in the last line there converges. This is not affected by putting ρ in place of 2.). □

This concludes the proof of the upper bounds, with the applications to Theorems 1.3 and 1.4 described at the end of Chapter 3.1. In light of Propositions 2.13 and 2.14, the results of this section and the previous one are sufficient to prove (1.6) and (1.8).

Chapter 4

Restricted Multiplication Table Problems

In [8], the classical multiplication table problem for integers, described in chapter 1.1, is generalized to one in which the resulting products satisfy a particular condition. More precisely, suppose $\mathcal{B} \subseteq \mathbb{N}$ is an arbitrary sequence of integers. For $N \in \mathbb{N}$, let $A_{\mathcal{B}}(N) := |\mathcal{B} \cap \{ab : a, b \leq N\}|$. One now seeks to estimate $|A_{\mathcal{B}}(N)|$. Ford considered the particular case $\mathcal{B} := \{s + p : p \in \mathcal{P}\}$, where s is a fixed non-zero integer (a sequence of *shifted primes*). He quantitatively described the associated divisor distribution function $H(x, y, z; \mathcal{B}) := |\mathcal{B} \cap \{n \leq x : \exists d \in (y, z] \text{ s.t. } d|n\}|$, making certain assumptions regarding y and z. The problem was subsequently solved completely by Koukoulopoulos in [19]. He produced sharp order of magnitude estimates for all values of y and z. Naturally, there are endless ways to choose $\mathcal{B}$. In [10], for example, the choice of $\mathcal{B}$ as an arithmetic progression to a fixed modulus was considered. In this chapter, we investigate two examples of restricted multiplication table problems. In each case, we are shifting the sequence by some fixed non-zero integer s. We study: i) the sequence of shifted sums of squares $\mathcal{T}_s := \{u^2 + v^2 + s : u, v \in \mathcal{N} \cup \{0\}\}$; ii) the sequence of shifted squarefree numbers $\mathcal{U}_s := \{n + s : \mu^2(n) = 1\}$. In general, sequences that are equidistributed in residue classes modulo primes can be evaluated using similar methods to those worked out in the previous chapter, and i) is an example of this.

4.1 Shifted Sums of Squares

Euler proved that a rational prime p is representable as $a^2 + b^2$ for positive integers a, b if, and only if, $p \equiv 1 \pmod 4$. From the simple formula $(a^2 + b^2)(c^2 + d^2) = (ad - bc)^2 + (ac + bd)^2$ and induction, it follows that any product of sums of squares is itself a sum of squares. Thus, any squarefree integer composed of primes congruent to 1 mod 4 is a sum of squares. A converse of this also holds:

Theorem 4.1. *Let $m \in \mathbb{N}$. Then $m = a^2 + b^2$ for some $a, b \in \mathbb{N} \cup \{0\}$ if, and only if, any prime divisor p of m which is not congruent to 1 mod 4 satisfies $p^2|m$.*

Proof. See [14], Chapter XX. □

Based on this fact and basic techniques in Sieve Theory, we may arrive at a result reminiscent of Theorem 3.1:

Lemma 4.2. *If $3 \leq y \leq \sqrt{x}$ then for any $\epsilon > 0$,*

$$H(x, y, 2y; \mathcal{T}_s) \gg_{\epsilon,s} \frac{x}{(\log x)^{\frac{1}{2}}(\log y)} \sum_{\substack{a \leq y^{\epsilon} \\ \mu^2(a)=1}} \frac{L(a)}{\phi(a)}.$$

Proof. Let $\mathcal{T} := \mathcal{T}_0$. As before, we choose a set of integers apb such that $apb - s \in \mathcal{T}$, $a \leq y^{\epsilon}$ and $q|b \Rightarrow q \in (y^{\epsilon}, y^{1-\epsilon}]$ or $q > 2y$, and $\log(y/p) \in \mathcal{L}(a)$. This gives us

$$H(x, y, z; \mathcal{T}_s) \geq \sum_{\substack{a \leq y^{\epsilon} \\ \mu^2(a)=1}} \sum_{\log(y/p) \in \mathcal{L}(a)} \sum_{\substack{b \leq x/ap \\ P^-(b) > 2y, apb - s \in \mathcal{T}_s}} 1. \tag{4.1}$$

The inner sum can be computed as follows. For a and p fixed according to the conditions on the sums above, let $F \in \mathbb{Z}[X]$ denote the integer polynomial $F(X) := apX - s$. Set $\mathcal{A} := \{F(k) \leq x : P^-(k) > 2y\}$. Since F is linear, $\mathcal{A}$ is in bijection with the set of $k \leq \frac{x-s}{ap}$ satisfying $P^-(k) > 2y$. Hence, $|\mathcal{A}| \asymp \frac{x}{ap \log y}$ by Theorem 2.3 in the case $X = \mathbb{N}$ with $\alpha = 1$. Let z_0, D be constants to be chosen momentarily and let $\mathcal{P}(z_0) := \{p < z_0 : p \equiv 3 \pmod 4\}$. We let $S(\mathcal{A}, \mathcal{P}(z_0))$ be the *sifting function* for $\mathcal{A}$, i.e., the number of elements of $\mathcal{A}$ not divisible by any primes in $\mathcal{P}(z_0)$. We will show that this is, in fact, a good approximation for the inner sum in (4.1).

Denote by $\rho(q)$ the number of solutions of $F(n) \equiv 0 \pmod q$, where q is a prime. Since s has only a finite number of prime factors, we may safely ignore these primes in what follows (they contribute only a constant multiplicative factor which, for our purposes is unimportant). The equation $apk \equiv s \pmod q$ has, at most, one solution, with equality if, and only if, $q \nmid ap$. Write

$$V(z_0) := \prod_{q \in \mathcal{P}(z_0)} \left(1 - \frac{\rho(q)}{q}\right) \asymp \prod_{\substack{q < z_0 \\ q \equiv 3 \pmod 4}} \left(1 - \frac{1}{q}\right) \prod_{q | ap} \left(1 - \frac{1}{q}\right)^{-1}.$$

By the Prime Number Theorem for the arithmetic progression $m \equiv 3 \pmod 4$ (which is, in fact, Theorem 2.3 when $K = \mathbb{Q}(i)$) and partial summation,

$$V(z_0) \asymp (\log z_0)^{-\frac{1}{2}} \frac{ap}{\phi(ap)}. \tag{4.2}$$

Let $D > 0$ and for each positive integer $d \leq D$ let $\mathcal{A}_d := \{a \in \mathcal{A} : a \equiv 0 \pmod d\}$. A result known as the *Fundamental Lemma* of Sieve Theory states that (see Corollary 6.10 of [11])

$$S(\mathcal{A}, \mathcal{P}(z_0)) = |\mathcal{A}| V(z_0) \left(1 + 4\theta(9\kappa + 1)^{\kappa} e^{9\kappa - s} K^{11}\right) + \theta \sum_{\substack{d < D \\ p|d \Rightarrow p \in \mathcal{P}(z_0)}} ||\mathcal{A}_d - \frac{\rho(d)}{d}|\mathcal{A}||, \tag{4.3}$$

where $s := \frac{\log D}{\log z_0}$, $\theta \in [0, 1)$ and $\kappa \geq 0$ and $K > 1$ are at our disposal. Since $\rho(d) = 1$ except for a finite number of $d < D$, and in other cases, $|\mathcal{A}_d| = \left\lfloor \frac{|\mathcal{A}|}{d} \right\rfloor$, the terms in (4.3) are less than 1 for all but a finite number of terms (and when y is larger than s, which we may assume as in Chapter 3.1, these terms are zero). If we choose $z_0 = x^{\frac{1}{2}+\eta}$ for $\eta > 0$, the only elements of $S(\mathcal{A}, \mathcal{P}(z_0))$ that are not sifted by $\mathcal{P}(z_0)$ (i.e., that are, in fact, divisible by primes congruent to 3 mod 4) are the primes in the interval $(z_0, x]$, since they can be divisible by at most one of these primes. This represents a remainder term of $O(x^{\frac{1}{2}+\eta'})$ for $\eta' \in (0, \eta)$, which is negligible. Moreover, by picking $D = z_0$, the sum over $d < D$ in (4.3)

also has this order of magnitude.
Suppose m is a composite sum of squares not counted by $S(\mathcal{A}, \mathcal{P}(z_0))$. Theorem 4.1 implies that it must be divisible by the square of a prime congruent to 3 mod 4. The size of these primes is at most $\sqrt{x}$. By an inclusion-exclusion argument, the number of $m \in \mathcal{A}$ that are composite and not counted by $S(\mathcal{A}, \mathcal{P}(z_0))$ is bounded below by

$$\geq |\mathcal{A}| \left(1 - \prod_{\substack{p \leq \sqrt{x} \\ p \equiv 3 \pmod 4}} \left(1 - \frac{1}{p^2}\right)\right) \gg |\mathcal{A}|.$$

Therefore, the sieve estimate derived using (4.3) has the right order of magnitude. Inserting (4.2) and (4.3) into (4.1) and noting that a and p are coprime by construction,

$$H(x, y, 2y; \mathcal{T}_s) \gg_\epsilon \frac{x}{(\log x)^{\frac{1}{2}} (\log y)} \sum_{\substack{a \leq y^\epsilon \\ \mu^2(a)=1}} \frac{1}{\phi(a)} \sum_{\log(y/p) \in \mathcal{L}(a)} \frac{1}{p-1}.$$

Lemma 4.1 now follows as in the conclusion of the proof of Theorem 3.1. □

Since the restrictions on a and p are independent of $\mathcal{T}_s$, in order to bound $H(x, y, 2y; \mathcal{T}_s)$ from below one can follow the same route as that used in the course of demonstrating Theorem 1.3. In this case, we may bound $\frac{1}{\phi(a)}$ by $\frac{1}{a}$ trivially, which will be proven to suffice.
To set up the proof of the upper bounds, we will show an analogue of Theorem 3.6.

Lemma 4.3. *For $3 \leq y \leq \sqrt{x}$, we have uniformly*

$$H(x, y, 2y; \mathcal{T}_s) \ll \frac{x}{(\log x)^{\frac{1}{2}}} \max_{\sqrt{y} < t \leq x} \frac{1}{(\log t)^2} \sum_{\substack{P^+(m) \leq t \\ \mu^2(m)=1}} \frac{L(m)}{\phi(m)}.$$

In Chapter 3, the inner sum had denominator m (when $X = \mathbb{N}$) and was bounded above on sets of the form $\{m : \omega(m) = k\}$, $k \geq 1$ by the products $\left(\sum_{p \leq P} \frac{1}{p}\right)^k$ with $k \geq 1$, estimated using Mertens' theorem. In this case, the resulting product will be $\left(\sum_{p \leq P} \frac{1}{p-1}\right)^k$, and an estimate of the form $\log_2 P + O(1)$, albeit with a different constant term, occurs as well. Therefore, all subsequent results pertaining to the upper bounds in Chapter 3 will apply once Lemma 4.3 has been proven.

Proof. We follow the method of proof of Theorem 3.6. Let $\gamma \geq 2$ be a parameter to be chosen. By Corollary 2.2, we can avoid all integers with a squarefull factor in excess of $(\log x)^{2\gamma}$ at the cost of a remainder term $O\left(\frac{x}{(\log x)^\gamma}\right)$. Decomposing the interval $(x/(\log x)^\gamma, x]$ dyadically as before, we get

$$\begin{aligned} H(x, y, 2y; \mathcal{T}_s) &= \sum_{b \leq (\log x)^{2\gamma}} \sum_{d \mid b} \sum_{\substack{a \leq x/b, \mu^2(a)=1 \\ \tau(a, y/d, z/d) \geq 1, ba - s \in \mathcal{T}_s}} 1 + O\left(\frac{x}{(\log x)^\gamma}\right) \\ &\leq \sum_{b \leq (\log x)^{2\gamma}} \sum_{d \mid b} \sum_{r \leq 2\log(x/b)} \sum_{\substack{2^{-(r+1)} x/b < a \leq 2^{-r} x/b \\ \mu^2(a)=1, ba - s \in \mathcal{T}_s, \tau(a; y/d, z/d) \geq 1}} 1 + O\left(\frac{x}{(\log x)^\gamma}\right). \end{aligned} \tag{4.4}$$

Write $a = I_1 I_2 I_3$, where I_2 is prime, $P^+(I_1) < I_2 < P^-(I_3)$, chosen such that $I_1 I_2$ has a divisor either

in $(y/d, 2y/d]$ or in $(\frac{xd}{4yb}, \frac{xd}{yb}]$. Then the arguments preceding (3.11), applied to (4.4), give

$$\sum_{\substack{I_1 \le 2^{-r}x/b \\ \mu^2(I_1)=1}} \sum_{\substack{\log(cw/I_2)\in\mathcal{L}(I_1) \\ P^+(I_1)<I_2, I_2 \text{ prime}}} \sum_{\substack{I_3 \le 2^{-r}x/bI_1I_2 \\ P^-(I_3)>I_2, \mu^2(bI_1I_2I_3-s)=1}} 1.$$

Using the method of Lemma 4.2 to derive an upper bound on the set of sums of squares represented by the polynomial $F(k) := bI_1I_2k - s$ for fixed b, I_1, I_2 and k having no small prime divisors, the inner sum becomes

$$\ll \frac{x}{2^r\phi(b)(\log x)^{\frac{1}{2}}} \sum_{\substack{I_1 \le 2^{-r}x/b \\ \mu^2(I_1)=1}} \frac{1}{\phi(I_1)\log(cw)} \sum_{\substack{\log(cw/I_2)\in\mathcal{L}(I_1) \\ P^+(I_1)<I_2, I_2 \text{ prime}}} \frac{1}{(I_2-1)\log(I_2)}.$$

Bounding $\log(I_2) \ge \max(\log(w/I_1), \log(I_1))$ as before, we use the same argument as in Theorem 3.6 to produce the overall estimate (putting m in place of I_1, so that m is hence squarefree)

$$\begin{aligned} H(x,y,2y;\mathcal{T}_s) &\ll \frac{x}{(\log x)^{\frac{1}{2}}} \max_{\sqrt{y}<t\le x} \sum_{b\le(\log x)^{2\gamma}} \frac{1}{\phi(b)} \sum_{d|b} \sum_{r\le 2\gamma\log_2 x} 2^{-r} \sum_{\substack{P^+(m)\le t \\ \mu^2(m)=1}} \frac{L(m)}{\phi(m)\log^2(\max(P^+(m), y/m))} \\ &\ll \frac{x}{(\log x)^{\frac{1}{2}}} \max_{\sqrt{y}<t\le x} \sum_{b\le(\log x)^{2\gamma}} \frac{1}{\phi(b)} \sum_{d|b} \sum_{\substack{P^+(m)\le t \\ \mu^2(m)=1}} \frac{L(m)}{\phi(m)\log^2(\max(P^+(m), y/m))}. \end{aligned}$$

Invoking Proposition 2.10 with the function $f(m) = L(m)/(m/\phi(m))$ (which is submultiplicative since $n \mapsto n/\phi(n)$ is multiplicative) and $h = 2$ and setting $\gamma = 2 + \epsilon$ for any ϵ as in Chapter 3.2, we derive

$$\begin{aligned} H(x,y,2y;\mathcal{T}_s) &\ll \frac{x}{(\log x)^{\frac{1}{2}}} \max_{\sqrt{y}<t\le x} \frac{1}{(\log t)^2} \sum_{b\le(\log x)^{2\gamma}} \frac{1}{\phi(b)} \sum_{d|b} \sum_{P^+(m)\le t} \frac{L(m)}{\phi(m)} \\ &\ll \frac{x}{(\log x)^{\frac{1}{2}}} \max_{\sqrt{y}<t\le x} \frac{1}{(\log t)^2} \sum_{P^+(m)\le t} \frac{L(m)}{\phi(m)}. \end{aligned} \tag{4.5}$$

The last equality follows by recognizing that, in general, $b/\phi(b) \le \prod_{p\le b}\left(1-\frac{1}{p}\right)^{-1} \ll \log b$ for any b. The Euler product here, analogous to (3.13) above is then

$$\begin{aligned} \sum_{\substack{b\ge 1 \\ b \text{ squarefull}}} \frac{\tau(b)}{\phi(b)^2} &= \prod_p \left(1 + \sum_{j\ge 2} \frac{\tau(p^j)}{\phi(p^j)^2}\right) \le \prod_p \left(1 + \sum_{j\ge 2} \frac{j(j+1)(\log p)^2}{p^{2j}}\right) \\ &\le \prod_p \left(1 + \sum_{j\ge 2} \frac{j(j+1)}{p^{(2-\epsilon)j}}\right), \end{aligned}$$

when $s = 2$. This is convergent for ϵ small enough, so (4.5) follows. □

From the comments preceding the proof of Lemma 4.2, we see that by carrying out all of the steps in Chapter 3 for the upper and lower bounds, we arrive at the following:

Theorem 4.4. *For $3 \le y \le \sqrt{x}$, we have*

$$H(x,y,2y;\mathcal{T}_s) \asymp \frac{x}{(\log x)^{\frac{1}{2}}(\log y)^{\delta}(\log_2 y)^{\frac{3}{2}}}.$$

4.2 Shifted Squarefree Numbers

We may apply the strategy used in Chapter 4.1 to determine the number of shifted squarefree integers. We need only change the sifting factors $\mathcal{P}(z_0)$ in Lemma 4.2. In this case, we seek squarefree values of the polynomial $F(X) = apX - s$, where a is squarefree and p is prime. To this end, we must sieve out any integer with a divisor of the form p^2, where $p < z_0$. Using the formalism above, the required sifting function takes the form

$$\mathcal{S}(\mathcal{A}, \mathcal{P}(z_0)) = |\mathcal{A}| \prod_{p<z_0} \left(1 - \frac{1}{p^2}\right) + O(x^{\frac{1}{2}+\epsilon}).$$

The product over primes is convergent as $z_0 \to \infty$ (to the value $\zeta(2)^{-1}$). We thus recover the estimate $S(\mathcal{A}, \mathcal{P}(z_0)) \asymp \frac{x}{\log y}$. This has the same order of magnitude as the number of integers with smallest prime factor strictly larger than y, by Theorem 2.8 when $X = \mathbb{N}$, and this was applied in Chapter 3 in the determination of $|A_X(N)$. Since the remainder of the argument from Chapter 3.1 is unchanged, we have:

Lemma 4.5. *If $3 \leq y \leq \sqrt{x}$ then for any $\epsilon > 0$,*

$$H(x, y, 2y; \mathcal{U}_s) \ll_\epsilon \frac{x}{\log y} \sum_{\substack{a \leq y^\epsilon \\ \mu^2(a)=1}} \frac{L(a)}{\phi(a)}.$$

By the same token, the upper bounds may also be deduced using this set-up. Since the upper and lower bounds agree for shifted sums of squares, they will also agree in this case, modulo the factor $(\log x)^{\frac{1}{2}}$ in the denominator. We therefore derive the same order of magnitude in this problem as in the unrestricted problem (see (1.1)).

Theorem 4.6. *We have, uniformly for $3 \leq y \leq \sqrt{x}$,*

$$H(x, y, 2y; \mathcal{U}_s) \asymp H(x, y, 2y).$$

Chapter 5

Appendices

5.1 Appendix A: Besicovitch's Counterexample

(This is a solution to Exercise III.3.7-8 in [28].)
Let $y \geq 2$ and $\mathcal{A} := \mathbb{N} \cap (y, 2y]$. Set $\mathcal{M}_y := \mathcal{M}(\mathcal{A})$ and $\epsilon_y := d\mathcal{M}y$. That ϵ_y exists follows from the inclusion-exclusion principle. Indeed, set $\mathcal{M}_y^{(j)} := \mathcal{M}(\{y+1, \dots, y+j\}) \backslash \mathcal{M}(\{y+1, \dots, y+j-1\})$ for each $j \geq 2$ (where $\mathcal{M}(\emptyset) = \emptyset$). These are disjoint sets of multiples which satisfy $\mathcal{M}_y = \bigcup_{1 \leq j \leq y} \mathcal{M}_y^{(j)}$; thus, we have

$$\begin{aligned} x^{-1} \sum_{\substack{n \leq x \\ n \in \mathcal{M}_y}} 1 &= \sum_{1 \leq j \leq y} x^{-1} \sum_{\substack{n \leq x \\ n \in \mathcal{M}_y^{(j)}}} 1 \\ &= \sum_{1 \leq j \leq y} x^{-1} \left(\left\lfloor \frac{x}{y+j} \right\rfloor + \sum_{1 \leq k \leq j-1} (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq j-1} \left\lfloor \frac{x}{\operatorname{lcm}(y+j, y+i_1, \dots, y+i_k)} \right\rfloor \right) \\ &= \sum_{1 \leq j \leq y} \left(\frac{1}{y+j} + \sum_{1 \leq k \leq j-1} (-1)^k \sum_{1 \leq i_1 < \dots < i_k \leq j-1} \frac{1}{\operatorname{lcm}(y+j, y+i_1, \dots, y+i_k)} \right) + o(1) \end{aligned} \tag{5.1}$$

which converges as $x \to \infty$, provided y is fixed. Let $\Omega(n, y) := \sum_{\substack{p^\alpha || n \\ p \leq y}} \alpha$, i.e., the truncation of $\Omega(n)$ to the set of prime divisors of n less than or equal to y. Setting $\mathcal{B}_y := \{n : \Omega(n, y) \geq \frac{\log_2 y}{\log 2}\}$, we will decompose $\mathcal{M}_y$ according to its intersection with $\mathcal{B}_y$. By construction, $n \in \mathcal{B}_y$ if, and only if, $n = ab$ with $P^+(b) \leq y < P^-(a)$ and $\Omega(b) \geq \frac{\log_2 y}{\log 2}$. It follows that

$$x^{-1} \sum_{\substack{n \leq x \\ n \in \mathcal{B}_y}} 1 = x^{-1} \sum_{\substack{b \leq x, P^+(b) \leq y \\ b \in \mathcal{B}_y}} \sum_{\substack{a \leq \frac{x}{b} \\ P^-(a) > y}} 1 = \sum_{\substack{b \leq x, P^+(b) \leq y \\ b \in \mathcal{B}_y}} \frac{1}{b} B_y(x/b),$$

where $B_y(x) := x^{-1} \sum_{a \leq x, P^-(a) > y} 1$. A similar inclusion-exclusion argument as that in (5.1) shows that $d\{n : P^-(n) > y\} = \prod_{p \leq y} (1 - \frac{1}{p})$ (by excluding multiples of $p \leq y$). Applying a discrete form of the Dominated Convergence Theorem (by defining the sequence of functions $\{g_n(t)\}_n$ as $g_n(t) :=$

$B_y(n/t)1_{(1,n]}(t)$, with Stieltjes integrals

$$\int_1^\infty g_n(t)1_{(1,n]}(t)d\{\sum_{b\le t, P^-(b)\le y}\frac{1}{b}\}),$$

(5.1) converges to

$$\lim_{x\to\infty} x^{-1}\sum_{\substack{m\le x\\ m\in\mathcal{B}_y}} 1 = \prod_{p\le y}\left(1-\frac{1}{p}\right)\sum_{\substack{P^+(b)\le y\\ b\in\mathcal{B}_y}}\frac{1}{b},$$

as $x\to\infty$ (forcing n to infinity as well).
We bound $d\mathcal{B}_y$ as follows, introducing a free parameter z to be optimized. The upper bound

$$1_{\mathcal{B}_y}(n) \le z^{\Omega(n,y)-\log_2 y/\log 2} = z^{\Omega(n,y)}(\log y)^{-\frac{\log z}{\log 2}}$$

is valid for each $z\ge 1$ and $n\in\mathbb{N}$. Thus,

$$x^{-1}\sum_{n\le x}1_{\mathcal{B}_y}(n) \le x^{-1}\exp\left(-\frac{\log z}{\log 2}\log_2 y\right)\sum_{n\le x} z^{\Omega(n,y)}. \tag{5.2}$$

Assume now that $z\in[1,2)$. Applying Lemma 2.7 to the setting $X=\mathbb{N}$ with the function $f(n):=z^{\Omega(n,y)}$ and noting that $z^{\Omega(p^\nu,y)}\le z^\nu$ if $p\le y$ and 1 otherwise, we have, by Corollary 2.4,

$$\begin{aligned}\sum_{n\le x} z^{\Omega(n,y)} &\ll \frac{x}{\log x}\prod_{p\le y}\left(1-\frac{z}{p}\right)^{-1}\prod_{y<p\le x}\left(1-\frac{1}{p}\right)^{-1} \ll \frac{x}{\log x}\exp\left(z\sum_{p\le y}\frac{1}{p}+\sum_{y<p\le x}\frac{1}{p}\right)\\ &\ll \frac{x}{\log x}\exp\left(z\log_2 y+\log\left(\frac{\log x}{\log y}\right)\right)\end{aligned} \tag{5.3}$$

Inserting (5.3) into (5.2), we find that

$$x^{-1}\sum_{n\le x}1_{\mathcal{B}_y}(n) \ll (\log y)^{-1}\exp\left(\left(-\frac{\log z}{\log 2}+z\right)\log_2 y\right). \tag{5.4}$$

The critical point of the exponent in (5.4), treated as a function of z, occurs at $z=\frac{1}{\log 2}$ (in $[1,2)$, as required). Inputting this optimal choice into (5.4) and taking $x\to\infty$, we get

$$d\mathcal{B}_y \ll (\log y)^{-\left(1-\frac{1+\log_2 2}{\log 2}\right)} = (\log y)^{-\delta}. \tag{5.5}$$

Consider now the set $\mathcal{B}'_y := \mathcal{M}_y\backslash\mathcal{B}_y$, i.e., those multiples of elements in $(y,2y]$ such that $\Omega(n,y)<\frac{\log_2 y}{\log 2}$. Since $\mathcal{M}_y$ and $\mathcal{B}_y$ both have natural density, $\mathcal{M}_y\cap\mathcal{B}_y$ does as well; hence, $d\mathcal{B}'(y)=d\mathcal{M}_y - d(\mathcal{M}_y\cap\mathcal{B}_y)$. In much the same way as we showed for $\mathcal{B}_y$, the majorization

$$1_{\mathcal{B}'_y}(n) \le z^{\Omega(n,y)-\log_2 y/\log 2}1_{\exists\ d|n: y<d\le 2y}(n)$$

holds when $z \in (0,1)$. Thus, when $x > 2y^2$ (so that $x/d > y$ for each $d \in (y, 2y]$),

$$\begin{aligned}
x^{-1}\sum_{n\le x} 1_{\mathcal{B}'_y}(n) &\le x^{-1} z^{-\frac{\log_2 y}{\log 2}} \sum_{d\in(y,2y]} z^{\Omega(d,y)} \sum_{m\le \frac{x}{d}} z^{\Omega(m,y)} \\
&\ll z^{-\frac{\log_2 y}{\log 2}} \frac{2y}{\log y} \sum_{d\in(y,2y]} \frac{z^{\Omega(d,y)}}{d} \frac{x}{d\log x} \sum_{P^+(m)\le \frac{x}{d}} \frac{z^{\Omega(m,y)}}{m} \\
&\ll (\log x \log y)^{-1} z^{-\frac{\log_2 y}{\log 2}} \prod_{y<p\le 2y} \left(1-\frac{1}{p}\right)^{-2} \prod_{p\le y} \left(1-\frac{z}{p}\right)^{-2} \prod_{2y<p\le \frac{x}{d}} \left(1-\frac{1}{p}\right)^{-1} \\
&\ll (\log x \log y)^{-1} \exp\left(2z\log_2 y - \log z \frac{\log_2 y}{\log 2} + \log\left(\frac{\log(x/d)}{\log y}\right)\right) \qquad (5.6) \\
&\ll (\log y)^{-2} \exp\left(\log_2 y \left(2z - \frac{\log z}{\log 2}\right)\right) \qquad (5.7)
\end{aligned}$$

The critical point of (5.7), as a function of z, is $z = \frac{1}{2\log 2}$, which is indeed in (0,1). Inputting this in (5.7) ad taking $x \to \infty$, we get $d\mathcal{B}'_y \ll (\log y)^{-\delta}$. Recalling that $\epsilon_y = d\mathcal{M}_y \le d\mathcal{B}_y + d\mathcal{B}'_y$, the above and (5.5) imply that $\epsilon_y \ll (\log y)^{-\delta}$. Thus, $\epsilon_y \to 0$ as $y \to \infty$.

Referring to the definitions stated in Chapter 1, we set $\mathcal{A} := \mathbb{N} \cap \bigcup_{k\ge 0}(y_k, 2y_k]$ and choose two infinite sequences $\{x_k\}_k$ and $\{x'_k\}_k$ with $x_k := y_k$ and $x'_k := 2y_k$. The first satisfies

$$x_k^{-1} \sum_{\substack{n\le x_k \\ n\in\mathcal{M}(\mathcal{A})}} 1 = y_k^{-1} \sum_{0\le j\le k-1} H(y_k, y_j) \le 2\epsilon \sum_{0\le j\le k-1} 2^{-(j+2)} \le \epsilon;$$

the second satisfies

$$x_k'^{-1} \sum_{\substack{n\le x'_k \\ n\in\mathcal{M}(\mathcal{A})}} 1 \ge (2y_k)^{-1} \sum_{n\in(y_k,2y_k]} 1 = \frac{1}{2},$$

as any set is a subset of its set of multiples. By definition, the lower and upper densities thus satisfy $\underline{d}\mathcal{M}(\mathcal{A}) \le \epsilon$ and $\overline{d}\mathcal{M}(\mathcal{A}) \ge \frac{1}{2}$. This establishes the claim asserted in Chapter 1.

5.2 Appendix B: Two Applications of $H(x, y, z)$

Recall the applications cited in Chapter 1 for the divisor distribution function $H(x, y, z)$. We will prove both (these are elaborations of the proofs given in Ch. 2.3-2.4 of [13]).

Theorem 5.1. *Let $\epsilon_y := d\{n : M(n, y) \ne 0\}$ for $y > 1$. Then $\epsilon_y \ll (\log y)^{-\frac{\delta}{1+\delta}}$, with $\delta = 1 - \frac{1-\log_2}{\log 2}$.*

Proof. The key observation is that if $m|n$ and m is squarefree and if there is some $q|n$, such that $q \nmid m$ and $qm \le y$, $\mu(m) + \mu(qm) = 0$. Therefore, in order to have non-zero contributions to $M(n, y)$, any squarefree divisor m of n not divisible by $P^-(n)$ must satisfy $P^-(n)m > y$. This forces $m \in (y/P^-(n), y]$. If $P^-(n)$ is large with respect to y, n will not satisfy $M(n, y) \ne 0$. If, however, $P^-(n) \le v$, $n \le x$ is counted by $H(x, y/v, y)$.

Set $v := \exp((\log y)^\alpha)$, where $\alpha \in (0, 1)$ is to be chosen. This choice is natural because according to the approach mentioned above, we expect the quantity $\Phi(x, v) = \Phi_{\mathbb{N}}(x, v)$ from Theorem 2.8 to appear, introducing a logarithmic factor $1/\log v$. If $P^-(n) > v$, then n is counted by $\Phi(x, v)$; conversely, if $P^-(n) \le v$ then n is counted by $H(x, y/v, y)$. Denoting by $\tau(n; y, z)$ the number of divisors of n in the

interval $(y,z]$, $H(x,y,z)$ counts the set of integers with $\tau(n;y,z)\geq 1$. We therefore have

$$\epsilon_y \leq \lim_{x\to\infty} x^{-1}\left(\sum_{\substack{n\leq x\\ P^-(n)\geq v}} 1 + \sum_{\substack{n\leq x\\ \tau(n;y/v,y)\geq 1}} 1\right) \ll \lim_{x\to\infty} x^{-1}\left(\frac{x}{\log v} + x\,(\log y)^{-\delta(1-\alpha)}\right),$$

by applying a frm of the upper bound implicit in (1.1). (We should mention that ϵ_y exists because y is fixed and $\epsilon_y = \sum_{f\leq y} d(\mathcal{M}((1,f])\backslash\mathcal{M}((1,f-1]))$, and each term in this sum exists by the inclusion/exclusion principle.) The optimal choice for α is $\alpha = \frac{\delta}{1+\delta}$, which proves the theorem. □

The second application has a much more elaborate proof.

Theorem 5.2. *Let $t\geq 1, u\in[0,1]$. Set*

$$S(u,t) := \{n\in\mathbb{N} : \exists\ m|n \text{ s.t. } n^{\frac{1-u}{t}} \leq m \leq n^{\frac{1}{t}}\}.$$

Then $h(u,t) := dS(u,t)$ is well-defined.

Proof. First, note that we may assume that $u\in(0,1)$: when $u=0$, the two bounds are the same, $S(u,t)=\emptyset$ and $h(0,t)=0$ vacuously; when $u=1$, every positive integer is contained in $S(u,t)$, as 1 is one of its divisors. Thus, $h(1,t)=1$.
Next, suppose $t\in[1,2)$. Given any divisor $d|n$, $\frac{n}{d}$ is also a divisor of n. Thus, n has a divisor smaller than $n^{\frac{1}{2}}$ if, and only if, it has a divisor greater than $n^{\frac{1}{2}}$. Using, this observation, we may transform the pair (u,t) with $t\in[1,2)$ into a new pair (u',t') with $t'\geq 2$ as follows:
i) if $t\in[1,2(1-u))$, $\frac{1-u}{t}>\frac{1}{2}$; therefore, we can set $u' := \frac{u}{t+u-1}$ and $t' := \frac{t}{t+u-1} = \left(1-\frac{1-u}{t}\right)^{-1} > 2$;
ii) if $t\in[2(1-u),2-u)$, we can set $u' := \frac{2-t}{t}$ and $t' := 2$;
iii) if $t\in[2-u,2)$, we can set $u' := \frac{t+2u-2}{t}$ and $t' := 2$.
Thus, in the remainder of the proof, we assume that $t\geq 2$ and $u\in(0,1)$. To deal with the bounds on divisors depending on n, we find a suitable region in $[1,x]$, such that the set $\{n : \exists\ m|n \text{ s.t. } x^{\frac{1-u}{t}} < m \leq x^{\frac{1}{t}}\}$ is approximately the same size asymptotically in x as $S(u,t)$. To this end, we exclude the interval $[1,\frac{x}{\log x}]$, which is small with respect to $[1,x]$, and consider its complement $(x/\log x, x]$. Set

$$H(x) := |\{x/\log x < n \leq x : \exists\ d|n \text{ s.t. } n^{\frac{1-u}{t}} < d \leq n^{\frac{1}{t}}\}|.$$

Let $y := x^{\frac{1-u}{t}}$ and $z := x^{\frac{1}{t}}$, and suppose n is counted by $H(x)$ but not by $H(x,y,z)$. Thus, n has a divisor d that satisfies $n^{\frac{1-u}{t}} < d \leq y$. Since n is constrained to the interval $(x/\log x, x]$, it is counted by $H\left(x,\left(\frac{x}{\log x}\right)^{\alpha}, x^{\alpha}\right) + H\left(x,\left(\frac{x}{\log x}\right)^{\beta}, x^{\beta}\right)$, where $\alpha := \frac{1-u}{t}$ and $\beta := t^{-1}$. (1.1) implies that each of these terms is $\ll_{\alpha,\beta} x(\log x)^{-\delta}$. This is also negligibly small as $x\to\infty$. Therefore, indeed, $H(x,y,z)$ is a good approximation for $H(x)$ in this interval. By showing that $x^{-1}H(x,y,z)$ converges to a well-defined limit as $x\to\infty$, it will follow that $h(u,t)$ equals this limit, and the theorem will be proven.
It will be convenient to find an approximation for $H(x,y,z)$ itself, as follows. Let $\epsilon>0$ and set $H_\epsilon(x,y,z) := |\{n\leq x : \exists\ d\in(y,z] : P^-(d) > y^\epsilon\}|$. We will show that for small enough ϵ, $H_\epsilon(x,y,z)$ is sufficiently close to $H(x,y,z)$ that $x^{-1}\left(H(x,y,z) - H_\epsilon(x,y,z)\right)\to 0$ as $x\to\infty$. The extra constrain on the divisors of n will make the evaluation of H_ϵ tractable using techniques in Sieve Theory.
If n is counted by H but not by H_ϵ, there must be some divisor d of n that satisfies $y<d\leq z$ and $P^-(d)\leq y^\epsilon$. If it is the smallest such divisor of n, $\frac{d}{P^-(d)}\leq y$, as $\frac{d}{P^-(d)}$ itself is a divisor of n strictly

smaller than n. Thus, $d \leq y^{1+\epsilon}$ and n is counted by $H(x, y, y^{1+\epsilon})$. Results in section 1 of [8] show that

$$H(x, y, z) - H_\epsilon(x, y, z) \ll H(x, y, y^{1+\epsilon}) \ll \epsilon^\delta x,$$

and, as $\epsilon \to 0$, $x^{-1}(H(x, y, z) - H_\epsilon(x, y, z)) \to 0$, as claimed.
We may evaluate $H_\epsilon(x, y, z)$ using the inclusion/exclusion principle. Let $[a, b]$ denote the least common multiple of two positive integers a and b (this should hopefully not be confused with the closed interval whose endpoints are a and b). Then,

$$\begin{aligned} H_\epsilon(x, y, z) &= \sum_{k\geq 1}(-1)^{k-1} \sum_{\substack{y<d_1<\ldots<d_k\leq z \\ P^-(d_i)>y^\epsilon}} \left\lfloor \frac{x}{[d_1, \ldots, d_k]} \right\rfloor = \sum_{k\geq 1}(-1)^{k-1} \sum_{d\geq 1} \sum_{\substack{y<d_1<\ldots<d_k\leq z \\ P^-(d_i)>y^\epsilon, d=[d_1,\ldots,d_k]}} \left\lfloor \frac{x}{d} \right\rfloor \\ &= \sum_{k=1}^{\infty}(-1)^{k-1} \left(\sum_{\substack{d\geq 1 \\ P^-(d)>y^\epsilon}} \frac{\rho_k(d)}{d} x + O\left(\sum_{\substack{d\leq x \\ P^-(d)>y^\epsilon}} \rho_k(d) \right) \right), \end{aligned} \tag{5.8}$$

where $\rho_k(d)$ denotes the number of k-tuples of integers in $(y, z]$ with least common multiple d. Note that if $\rho_k(d) \neq 0$, then $k \leq \tau(d) \leq 2^{\Omega(d)}$ and, by construction,

$$\Omega(d) \leq \frac{\log x}{\epsilon \log y} = (\log x) \left(\epsilon t^{-1}(1-u) \log x\right)^{-1} = t(\epsilon(1-u))^{-1}.$$

Hence, for u, t and ϵ fixed, the number of k for which ρ_k contributes to (5.8) is uniformly bounded. Thus, $\tau(d)$ is also uniformly bounded and $\rho(d) \leq \binom{\tau(d)}{k} \ll_{u,t} 1$. The error term in (5.8) is then $\ll_{u,t} \Phi(x, y^\epsilon) \ll_{u,t} \frac{x}{\log x}$; therefore, it not factor into the density calculation.
The problem is thus reduced to evaluating

$$x^{-1} \sum_{r\geq 1} \sum_{j\geq 1} r \sum^{*} (p_1 \cdots p_j)^{-1},$$

where the asterisk over the inner sum indicates that we only consider $y^\epsilon < p_1 \leq \ldots \leq p_j \leq x$ with $\rho(p_1, \ldots, p_j) = r$. According to the observations above, j in (5.2) is bounded; hence, r can only take on finitely many values, and the double sum consists of only a finite number of pairs (r, j). Let $\chi_{r,j} : [0, 1]^j \to [0, 1]$ be the function which is 1 if its arguments are of the form $\frac{\log p_i}{\log x}$ and $p_1 \cdots p_j$ satisfies property $(*)$, and 0 otherwise. The following lemma shows that the inner sum in (5.2) corresponding to each of the finitely many pairs (r, j) converges to a limit, which proves the theorem.

Lemma 5.3. *Let $r, j \geq 1$. Let $\chi : \mathbb{R}^j \to \mathbb{R}$ be a Lebesgue integrable function with compact support. Then*

$$\lim_{x\to\infty} \sum^{*} \chi\left(\frac{\log p_1}{\log x}, \ldots, \frac{\log p_j}{\log x} \right) (p_1, \ldots, p_j)^{-1} = \int_0^\infty \cdots \int_0^\infty \chi(u_1, \ldots, u_j) \frac{du_1}{u_1} \cdots \frac{du_j}{u_j},$$

where the asterisk denotes the condition in (5.2) *for the pair (r, j).*

(The lemma applies to the functions $\chi_{r,j}$, for each relevant pair (r, j).)

Proof. Let $[a, b]^j$ be a hypercube containing the support of χ. Let ν and ν_x be measures on $[a, b]^j$ defined by $d\nu(u_1, \ldots, u_j) = \prod_{i=1}^j \frac{du_i}{u_j}$ and $d\nu_x(u_1, \ldots, u_j) = \prod_{i=1}^j x^{-u_i} d\pi(x^{u_i})$ respectively, where $\pi(x)$ is the usual prime counting function. Thus, ν_x has non-zero contributions occur when x^{u_i} is prime, i.e., when

$u_i = \frac{\log p}{\log x}$ for some prime p. We will show that the net $\{\nu_x\}_{x>0}$ converges weakly to ν as $x \to \infty$, i.e., given any integrable function g on $[a,b]^j$, we have $\int g d\nu_x \to \int g d\nu$, as $x \to \infty$.
First, if $P := \prod_{i=1}^{j}[a_i, b_i] \subseteq [a,b]^j$, then by Fubini's theorem,

$$\int_P d\nu_x(u_1,\dots,u_j) = \prod_{i\le j}\int_{[a_i,b_i]} x^{-u_i} d\pi(x^{u_i}) = \prod_{i\le j}\left(\frac{\pi(x^b)}{x^b} - \frac{\pi(x^a)}{x^a} + \log x \int_{[a_i,b_i]} \frac{\pi(x^{u_i})}{x^{u_i}} du_i\right)$$
$$= \prod_{i\le j}\left(\left(\frac{1}{b}-\frac{1}{a}\right)(\log x)^{-1} + \int_{[a_i,b_i]} \frac{du_i}{u_i}\right) = \int_P \frac{du_1}{u_1}\cdots\frac{du_j}{u_j} + O((\log x)^{-1}).$$

Thus, $\int_P d\nu_x \to \int_P d\nu$ as $x \to \infty$. By linearity of the integral, any simple measurable function f (i.e., a finite linear combination of characteristic functions of subsets of $[a,b]^j$) will also satisfy $\int f d\nu_x \to \int f d\nu$. Let $\eta > 0$. Recall that the simple measurable functions defined on $[a,b]^j$ are dense in $L^1([a,b]^j)$. In particular, if χ is Lebesgue integrable, we can choose s_1, s_2 simple and measurable, such that $s_1 \le \chi \le s_2$ and $\int_{[a,b]^j} |s_1 - s_2| d\nu < \eta$. It then follows that for x large enough,

$$\int_{[a,b]^j} s_1 d\nu - \eta \le \int_{[a,b]^j} s_1 d\nu_x \le \int_{[a,b]^j} \chi d\nu_x \le \int_{[a,b]^j} s_2 d\nu + \eta.$$

Because $\int_{[a,b]^j} s_1 d\nu \le \int_{[a,b]^j} \chi d\nu \le \int_{[a,b]^j} s_2 d\nu$, we produce

$$-\int_{[a,b]^j}(s_2 - s_1)d\nu - \eta \le \int_{[a,b]^j}\chi d\nu - \int_{[a,b]^j}\chi d\nu_x \le \int_{[a,b]^j}(s_2-s_1)d\nu + \eta$$

and thus $|\int_{[a,b]^j}\chi d\nu - \int_{[a,b]^j}\chi d\nu_x| < 2\eta$. This completes the proof of the lemma and the theorem. □

□

5.3 Appendix C: Arithmetical Semigroups

The purpose of this section is to provide a brief introduction to the "abstract" Analytic Number Theory that is used in Chapters 2 and 3.
As mentioned in Chapter 1.2, the defining property of the integral ideal space of a number field $K/\mathbb{Q}$, for instance, that makes it suitable for arithmetic is the existence and uniqueness of a factorization of integral ideals into a product of generating elements, namely the prime ideals of $\mathcal{O}_K$. The Dedekind-Weber theorem and the Prime Ideal Theorem (see the beginning of Chapter 2) describe, statistically, the distribution of integral ideals and prime ideals, respectively, according to their norms. The complete multiplicativity of the norm function $N : \{\text{ideal space of } K\} \to \mathbb{N}$ makes the arithmetic of ideals closely related to the arithmetic of positive integers.
By axiomatizing the above observations, Knopfmacher [18], introduced and developed the following general class of objects.

Definition 5.4. An *arithmetical semigroup* is a triple $(X, \mathcal{P}_X, N_X)$ where X is a semigroup (i.e. a multiplicative monoid with identity) generated by a set of elements $\mathcal{P}_X$ and $N_X : X \to \mathbb{N}$ is a function that satisfies the following properties:
a) If 1_X denotes the identity element of X then $N_X(1_X) = 1$;
b) For any $M > 0$, the set $\{x \in X : N_X(x) \le M\}$ has finite cardinality (informally, the ball induced by

N_X of radius x in X is finite).
c) For any $x, y \in X$, $N_X(xy) = N_X(x)N_X(y)$.
When the generating set $\mathcal{P}_X$ and norm function N_X are understood, we abuse notation and say that X is an arithmetical semigroup.

Property b), a general version of the Dedekind-Weber theorem, is at the heart of what makes analytic statements on X possible. The arithmetical semigroup $(\mathbb{N}, \mathcal{P}, \mathrm{id})$ is the usual setting for number theory, and property b) is equivalent to the statement that $\sum_{m \leq x} 1 = \lfloor x \rfloor < \infty$ for each x. Many of the definitions of arithmetic functions and Dirichlet series in classical Analytic Number Theory have analogues in this setting, provided that the notion of convergence is well-defined. (In general, arithmetical semigroups are naturally compatible with a discrete topology; thus, convergence issues are easy to handle. See Chapter 2 of [18]).

Definition 5.5. Let $\mathfrak{C}$ be a category with direct product for which there exists a subcollection of objects $\mathfrak{P}$ such that, up to isomorphism, any object A from $\mathfrak{C}$ is decomposable as a finite product $A = \prod_{j=1}^{k} P_j$, where P_j is an object belonging to $\mathfrak{P}$ (and P_i and P_j are not necessarily distinct). Let 0 denote the trivial object of the category (satisfying $A \times 0 \cong A$), and let $S_{\mathfrak{C}}$ denote the semigroup of isomorphism classes of objects of $\mathfrak{C}$ with the direct product operation and identity 0, generated by $\mathfrak{P}$. If there exists a norm function $N_{\mathfrak{C}}$ satisfying a), b) and c) in Definition 5.4 defined on $S_{\mathfrak{C}}$, such that $(S_{\mathfrak{C}}, \mathfrak{P}, N_{\mathfrak{C}})$ is an arithmetic semigroup, then $\mathfrak{C}$ is called an *arithmetical category*.

A non-trivial example of an arithmetical category is the category of finite Abelian groups. The set of cyclic p-groups of arbitrary prime power order forms a generating set with respect to direct products of groups, by the Classification Theorem (Ch. 1.7 of [24]). A natural norm function, which is indeed multiplicative by the Chinese Remainder Theorem, is the counting function of the group, i.e., $N(G) := |G|$. Another example is provided by function fields $\mathbb{F}_q(t)$ and their rings of integers $X = \mathbb{F}_q[t]$, i.e., polynomials in t over $\mathbb{F}_q$, where q the power of some prime p. The set of monic, irreducible polynomials in t over $\mathbb{F}_q$ provides the primes for X, and the map $f(t) \mapsto q^{\deg(f)}$ is a norm function N_X, as in Definition 5.4: noting that the number of monic polynomials of degree k is q^k (ranging over all q elements for each of the other k coefficients of the polynomial), the ball of radius x induced by N_X is necessarily finite, and property b) holds.
Quantitative statements regarding objects in arithmetical categories are available under certain assumptions. The following hypothesis quantifying property b) holds in a variety of different settings.

Definition 5.6. An arithmetical semigroup $(X, \mathcal{P}_X, N_X)$ is said to satisfy *Axiom A* if there exist positive real numbers A and δ_0, and $\eta \in [0, \delta_0)$, such that for any $y > 0$ large enough,

$$|\{a \in X : N_X(a) \leq y\}| = Ay^{\delta_0} + O(y^{\eta}).$$

In addition to the natural numbers (with $A = \delta_0 = 1$, $\eta = 0$) and the integral ideals of a number field $K/\mathbb{Q}$ (with $A = A_K$ in Theorem 2.1, $\delta_0 = 1$ and $\eta = 1 - [K : \mathbb{Q}]^{-1}$), the arithmetical category of finitely generated torsion modules over a finite integral domain of algebraic integers in a number field $K/\mathbb{Q}$ also satisfies Axiom A. Theorem 1.1 in Ch. 5 of [18] shows that if ζ_K denotes the Dedekind zeta function for K, this category induces an arithmetical semigroup with $A := A_K \prod_{r \geq 2} \zeta_K(r)$, $\delta_0 = 1$ and $\eta \leq 1 - 2(1 + [K : \mathbb{Q}])^{-1}$. (The famous Erdős-Szekeres [6], which describes the number of finitely-generated $\mathbb{Z}$-modules, i.e., Abelian group, of cardinality at most x, is an application of the aforementioned theorem when $K = \mathbb{Q}$.)

An abstract Prime Number Theorem can also be deduced by assuming Axiom A, using similar techniques to those needed in the case of rational integers (One such tool in classical Analytic Number Theory which has an analogue in the abstract theory is the Wiener-Ikehara Theorem, which yields information on the continuity of the Riemann zeta function $\zeta(s)$ on the line $\mathrm{Re}(s) = 1$; in particular, it allows us to deduce a zero-free region beyond this line. See Ch. 8.3 of [25].)

Theorem 5.7 ([18], Ch. 6.1)**.** *Suppose $(X, \mathcal{P}_X, N_X)$ is an arithmetical semigroup that satisfies Axiom A (with $A, \delta_0 > 0$ and $\eta \in [0, \delta_0)$). If $\pi_X(y)$ denotes the counting function of $\mathcal{P}_X$, then*

$$\pi_X(y) = \frac{y^{\delta_0}}{\delta_0 \log y}\left(1 + O\left(\frac{1}{\log y}\right)\right).$$

When $X = \mathbb{F}_q[t]$ and $lq^N \leq x < (l+1)q^N$ for $0 \leq l < q-1$,

$$|\{f(t) \in \mathbb{F}_q[t] : q^{\deg(f)} \leq x\}| = (q-1)\sum_{0 \leq k \leq N} q^{k-1} = q^N - 1 \asymp_q \frac{1}{l}x.$$

Therefore, X does not satisfy Axiom A, since l is variable as x changes. However, a Prime Number Theorem (counting irreducibles in X), i.e.,

$$\pi_{\mathbb{F}_q[t]}(y) = (\log q)\frac{x}{\log x} + O(x^{\frac{1}{2}+\epsilon})$$

does hold in this context ([26], see the remark following Thm 2.2 there), for any $\epsilon > 0$. Axiom A is used to determine $|A_K(N)|$ and $|A'_K(N)|$ in Chapters 2 and 3.

By analogy, we may define $A'_X(N) := \{N_X(A \cdot B) : N_X(A), N_X(B) \leq N\}$. The methods used to analyze $|A'_K(N)|$ in Chapter 3 have a generalization in this more abstract setting as in Ch. 9 of [18], which we describe below.

Let X be a commutative arithmetical semigroup. Define an equivalence relation $\sim$ on X with the property that $a \sim a'$ and $b \sim b'$ implies that $ab \sim a'b'$. Define $Y := X/\sim$ and a product structure on Y via $[x][x'] = [xx']$, where $[a]$ denotes the equivalence class of X in Y. This is well-defined because if $x_1 \sim x_2$ and $x'_1 \sim x'_2$ then $x_1x_2 \sim x'_1x'_2$ by construction; hence, the equivalence class of the product is the product of the equivalence classes. By construction, Y is a semigroup, and in certain applications will satisfy: i) a cancellation property $[x][y] = [x][z] \Rightarrow [y] = [z]$; ii) Y will contain a trivial class $[e]$, such that $[x][e] = [x]$ for each $x \in X$. In these applications, Y forms an Abelian group.

Definition 5.8. Let $(X, \mathcal{P}_X, N_X)$ be a commutative arithmetical semigroup with an equivalence relation $\sim$ as above. An *arithmetical formation* is an ordered pair (X, Y) where $Y := X/\sim$. When Y contains a trivial class and a cancellation property, the quotient Y is called the *class group* of X.

Two motivating examples are as follows:

a) Fix $m \in \mathbb{N}$ and let X be the semigroup generated by all positive integers coprime to m. Define the equivalence relation $\sim$ via $a \sim b$ if, and only if, $a \equiv b \pmod{m}$. Then, $Y = X/\sim \cong (\mathbb{Z}/m\mathbb{Z})^*$.

b) Let X be the semigroup of all integral ideals of a number field $K/\mathbb{Q}$. Let I be the set of all principal ideals of X. Define an equivalence relation $\sim$ on X via $\mathfrak{a} \sim \mathfrak{b}$ if, and only if, there exist $(\alpha), (\beta) \in I$ such that $(\alpha)\mathfrak{a} = (\beta)\mathfrak{b}$. This is an equivalence relation by the Krull-Schmidt theorem (as all non-zero ideals have inverses). Then, $Y = X/\sim$ is the familiar ideal class group of K, as I is the trivial class and all non-zero ideals are invertible. Moreover, Y has finite cardinality ([7], Ch. 11).

c) Using the formalism developed in Chapter 1, let X be the Galois group of $K/\mathbb{Q}$ in the previous example, and let $\sim$ be the equivalence relation defined by conjugation, i.e., $\sigma \sim \tau$ if, and only if, there is a $\sigma' \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma = \sigma'\tau\sigma'$. Then, $Y = X/\sim$ is the set of all conjugacy classes of automorphisms of K over $\mathbb{Q}$. For any finite extension, the coset space Y is finite (although Y may not be a group in this case).
When $|Y| < \infty$, one can define a set of characters $\hat{Y} := \mathrm{Hom}(Y, \mathbb{T})$ on Y, satisfying the usual orthogonality properties:

$$\sum_{[y]\in Y} \overline{\chi_1}([y])\chi_2([y]) = \begin{cases} |Y| & \text{if } \chi_1 = \chi_2 \\ 0 & \text{otherwise} \end{cases} \tag{5.9}$$

$$\sum_{\chi\in Y^*} \overline{\chi}([y'])\chi([y]) = \begin{cases} |Y| & \text{if } [y] = [y'] \\ 0 & \text{otherwise} \end{cases}. \tag{5.10}$$

For each $\chi \in \hat{Y}$ we may define an L-function $L(s,\chi)$ which is expressible as

$$L(s,\chi) := \sum_{a\in X} \chi(a) N_X(a)^{-s} = \prod_{p\in\mathcal{P}_X} \left(1 - \frac{\chi(p)}{N_X(p)^s}\right)^{-1}, \tag{5.11}$$

when $\sigma > \delta_0$. Here, $\chi(a) := \chi([a])$. The Euler product formula (5.11) implies that $L(s,\chi) \neq 0$ for $\sigma > \delta_0$ since, by definition, every prime element has $N_X(p) > 1$ by definition. Thus, $L(s,\chi)$ has a well-defined logarithm. It follows from (5.10) that for $[a] \in Y$,

$$\sum_{\chi\in Y^*} \overline{\chi(a)} \log L(s,\chi) = \sum_{m\geq 1} \sum_{p\in\mathcal{P}_X} \frac{1}{mN_X(p)^{ms}} \sum_{\chi\in Y^*} \overline{\chi(a)}\chi(p^m) = |Y| \sum_{p\in[a]} N_X(p)^{-s} + O(1), \tag{5.12}$$

where the remainder term comes from the terms p^m for $m \geq 2$ (as in Corollary 2.4). One can show that in fact $L(\delta_0,\chi) \neq 0$, provided $\chi^2 \neq \chi_0$. (When $\chi^2 = \chi_0$, the argument is not valid and an alternative must be found. This is not always possible for a given X, and may require assuming that $L(\delta_0,\chi)$ is non-vanishing, a hypothesis called "Axiom A^{**}"). Assuming Axiom A,

$$A_\chi(x) := \sum_{N_X(a)\leq x} \chi(a) = \sum_{[a]\in Y} \chi([a]) \sum_{\substack{N_X(b)\leq x \\ b\in[a]}} 1 \leq A_X x^\delta \sum_{[a]\in Y} \chi([a]) + O(|Y|x^\eta) = O(x^\eta)$$

by applying (5.9) for $\chi_1 = \chi_0$. Thus,

$$\begin{aligned} \left|\sum_{a\in X} \chi(a) N_X(a)^{-s}\right| &= \left|\sum_{n\geq 1} n^{-s} \left(\sum_{\substack{a\in X \\ N_X(a)=n}} \chi(a)\right)\right| = \left|\sum_{n\geq 1} n^{-s} \left(A_\chi(n) - A_\chi(n-1)\right)\right| \\ &= \left|\sum_{k\geq 1} A_\chi(k) \left(k^{-s} - (k+1)^{-s}\right)\right| = O\left(\sum_{k\geq 1} k^{-(2\sigma-\eta)}\right). \end{aligned} \tag{5.13}$$

Therefore, the series representation (5.11) of $L(s,\chi)$ converges even when $\eta < \sigma \leq \delta_0$. The left side of (5.13) is then asymptotically $L(s,\chi_0) = \sum_{a\in X} N_X(a)^{-s}$ as $s \to \delta_0^+$. As a result, the prime elements of X are uniformly distributed (i.e. with proportion $1/|Y|$) among the equivalence classes of Y. In the case

c) above, if we associate a prime $\mathfrak{p}$ with its Fröbenius class $\sigma_{\mathfrak{p}}$, we get an equidistribution statement of this type as in Chebotarev's theorem (1.2). Therefore, the theory of arithmetical formations leads to a generalization of Chebotarev's theorem when Axiom A is assumed.
The theory of arithmetical formations outlined above provides an approach for the determination of $|A'_X(N)|$, namely using the factorization idea presented in Chapter 1, that the arithmetical semigroup X has its prime factors partitioned according to their equivalence class in Y. By determining the asymptotics of each subsemigroup of X generated by the primes in a given equivalence class, one can compute $|A'_X(N)|$. Determining $|A'_X(N)|$ may follow the same line of argument as we have presented in Chapter 1. If D is a union of equivalence classes in Y, a number ρ_D, corresponding to the proportion of elements of $\mathcal{P}_X$ belonging to D can be used, in analogy to ρ_s (see Chapter 1.2).

5.4 Appendix D: Restricted Divisor Function for Shifted Sums of Squares

The purpose of this section is to show that a naïve study of the function $H(x, y, z; \mathcal{T}_s)$ (see Chapter 4), via the computation of the sums $\sum_{\substack{n\leq x\\ n\in\mathcal{T}_s}} \tau(n; y, z)$, is insufficient to provide precise order of magnitude estimates. This section describes an example of the shortcoming pointed out in Chapter 1, of Tenenbaum's contribution to this problem. It also complements the study of the shifted sum problem in Chapter 4. Specifically, we prove that

$$\sum_{\substack{n\leq x\\ n\in\mathcal{T}_s}} \tau(n; y, z) \sim (x-s)\pi M(s)\log(z/y),$$

for a suitable constant $M(s)$ (determined below) depending only on s. This shows, roughly speaking, that many integers have more than one divisor between y and z. In theory, such a bound would be useful in an inclusion-exclusion argument of the following nature:

$$\sum_{k=1}^{2l}(-1)^{k-1}\sum_{y<d_1<\ldots<d_k\leq z}\ \sum_{a^2+b^2+s\leq x}^{*} 1 \leq H(x, y, z; \mathcal{T}_s) \leq \sum_{k=1}^{2l-1}(-1)^{k-1}\sum_{y<d_1<\ldots<d_k\leq z}\ \sum_{a^2+b^2+s\leq x}^{*} 1,$$

where the asterisk in the sum implies that $a^2+b^2+s \equiv 0 \pmod{[d_1,\ldots,d_k]}$ for each k-tuple of divisors $(d_1,\ldots,d_k)$, for some $l \geq 1$. This would, however, necessitate a good pointwise estimate of the functions

$$R_k(m; y, z) := |\{(d_1,\ldots,d_k) \in (y, z]^k : m = [d_1,\ldots,d_k]\}|,$$

for each $k \in \mathbb{N}$ and $m \in (y^k, z^k]$. However, these are more complicated to bound directly than τ (see Ch. 2.7 of [13], for example).
Let $e(t) := e^{2\pi it}$ for $t \in \mathbb{R}$.

Definition 5.9. Let $m \in \mathbb{N}$, $m \geq 2$ and let $a \in \mathbb{Z}/m\mathbb{Z}$. A *Gauss sum* is a sum of the form

$$g(a, m) := \sum_{k=0}^{m-1} e\left(\frac{ak^2}{m}\right).$$

Lemma 5.10. *Let $m \geq 2$ be a positive integer and let $a \in \mathbb{Z}/m\mathbb{Z}$. Let r denote the smallest non-negative*

integer in the residue class of m mod 4. Then

$$\delta(a,m) := m^{-1}g(a,m)^2 = \begin{cases} 1 & \text{if } r = 1 \\ 0 & \text{if } r = 2 \\ -1 & \text{if } r = 3 \\ (1+i^a)^2 & \text{otherwise} \end{cases}$$

Proof. See [2], section 1.5. □

Note that if t is the smallest non-negative integer in the residue class of a and $4|m$, we have: $\delta(a,m) = 0$ if $t = 2$; $\delta(a,m) = 4$ when $t = 0$; $\delta(a,m) = 2i$ when $t = 1$; and $\delta(a,m) = -2i$ when $t = 3$.

Theorem 5.11. *Fix $s \in \mathbb{Z}\backslash\{0\}$. Let $x > s$ and $m \geq 2$. Then*

$$\sum_{\substack{a^2+b^2+s \leq x \\ a^2+b^2+s \equiv 0 \ (mod\ m)}} 1 = \left(\left(\frac{x-s}{m^2}\right)\pi + O\left(\sqrt{\frac{x-s}{m^2}}\right)\right)\sum_{t|m} t\epsilon_s\left(\frac{m}{t}\right),$$

where, using the notation of the previous lemma,

$$\epsilon_s(m) := \sum_{\substack{a'=1 \\ (a',m)=1}}^{m} e\left(\frac{a's}{m}\right)\delta(a',m). \tag{5.14}$$

Proof. Using the orthogonality properties of exponentials, we have

$$\frac{1}{m}\sum_{x,y\in\mathbb{Z}/m\mathbb{Z}}\sum_{a=0}^{m-1} e\left(\frac{a}{m}\left(x^2+y^2+s\right)\right) = |\{(x,y) \in (\mathbb{Z}/m\mathbb{Z})^2 : x^2+y^2+s \equiv 0 \text{ (mod m)}\}|. \tag{5.15}$$

If we decompose the inner sum of (5.15) according to the gcd of a and m,

$$\begin{aligned}
\sum_{x,y\in\mathbb{Z}/m\mathbb{Z}}\sum_{a=0}^{m-1} e\left(\frac{a}{m}\left(x^2+y^2+s\right)\right) &= \sum_{t|m}\sum_{\substack{a'=0 \\ (a',m)=1}}^{m/t} e\left(\frac{a's}{m/t}\right)\left(\sum_{x=0}^{m-1} e\left(\frac{a'x^2}{m/t}\right)\right)^2 \\
&= \sum_{t|m}\sum_{\substack{a'=0 \\ (a',m)=1}}^{m/t} e\left(\frac{a's}{m/t}\right)\left(\sum_{u=0}^{m/t-1}\sum_{v=0}^{t-1} e\left(\frac{a'\left(\frac{vm}{t}+u\right)^2}{m/t}\right)\right)^2 \\
&= \sum_{t|m} t^2 \sum_{\substack{a'=0 \\ (a',m)=1}}^{m/t} e\left(\frac{a's}{m/t}\right)\left(\sum_{u=0}^{m/t-1} e\left(\frac{a'u^2}{m/t}\right)\right)^2 \\
&= \sum_{t|m} t^2 \sum_{\substack{a'=0 \\ (a',m)=1}}^{m/t} e\left(\frac{a's}{m/t}\right) g(a',m/t)^2.
\end{aligned}$$

The previous lemma then implies that

$$|\{(x,y)\in(\mathbb{Z}/m\mathbb{Z})^2 : x^2+y^2+s\equiv 0 \pmod{m}\}| = \sum_{t|m} t \sum_{\substack{a'=1\\(a',m/t)=1}}^{m/t} e\left(\frac{a's}{m/t}\right)\delta(a',m/t) = \sum_{t|m} t\epsilon_s(m/t).$$

Now,

$$\sum_{\substack{a^2+b^2+s\le x\\ a^2+b^2+s\equiv 0 \pmod m}} 1 = \sum_{\substack{(a,b)\in(\mathbb{Z}/m\mathbb{Z})^2\\ a^2+b^2+s\equiv 0 \pmod m}} \sum_{\substack{A^2+B^2+s\le x\\ (A,B)\equiv(a,b) \pmod m}} 1 = \sum_{\substack{(a,b)\in(\mathbb{Z}/m\mathbb{Z})^2\\ a^2+b^2+s\equiv 0 \pmod m}} \sum_{(u,v)\in\mathbb{Z}^2:(um+a)^2+(vm+b)^2\le x-s} 1. \tag{5.16}$$

Note that since $0\le a,b<m$, we have $m^2(u^2+v^2)\le(um+a)^2+(vm+b)^2<m^2((u+1)^2+(v+1)^2)$, for any pair (u,v) in the inner sum of (5.16). Thus, if the lattice point (A,B) is contained in the positive quadrant in $\mathbb{R}^2$, so is (u,v). The boundary points of the region defined by the set of pairs (u,v) are precisely those pairs for which $u^2+v^2\le\frac{x-s}{m^2}<(u+1)^2+(v+1)^2$. They therefore satisfy

$$u+v\le 2(u^2+v^2)^{\frac{1}{2}}\le 2\left(\frac{x-s}{m^2}\right)^{\frac{1}{2}}.$$

Let $L(a,b)$ denote the number of lattice points (A,B) such that $A\equiv a \pmod m$ and $B\equiv b \pmod m$ and $A^2+B^2+s\le x$. Then,

$$R\left(\sqrt{\frac{x-s}{m^2}}\right)\le L(a,b)<R\left(\sqrt{\frac{x-s}{m^2}+3\left(\frac{x-s}{m^2}\right)^{\frac{1}{2}}}\right), \tag{5.17}$$

where $R(r)=|\{(u,v)\in(\mathbb{N}\cup\{0\})^2 : u^2+v^2\le r^2\}|$ for $r>0$. From (5.17), it follows that

$$0\le L(a,b)-R\left(\sqrt{\frac{x-s}{m^2}}\right)\le R\left(\sqrt{\frac{x-s}{m^2}+3\left(\frac{x-s}{m^2}\right)^{\frac{1}{2}}}\right)-R\left(\sqrt{\frac{x-s}{m^2}}\right).$$

It is well-known that $R(r)=\left(\frac{x-s}{m^2}\right)\pi+O\left(\sqrt{\frac{x-s}{m^2}}\right)$ (for our purposes, a better error term is not needed; for a better error term, see [14]). Thus, for any pair (a,b),

$$L(a,b)=\left(\frac{x-s}{m^2}\right)\pi+O\left(\sqrt{\frac{x-s}{m^2}}\right).$$

Inserting (5.4) into (5.16), we get

$$\sum_{\substack{a^2+b^2+s\le x\\ a^2+b^2+s\equiv 0 \pmod m}} 1 = \sum_{\substack{(a,b)\in(\mathbb{Z}/m\mathbb{Z})^2\\ a^2+b^2+s\equiv 0 \pmod m}} L(a,b) = \left(\left(\frac{x-s}{m^2}\right)\pi+O\left(\sqrt{\frac{x-s}{m^2}}\right)\right)\sum_{t|m} t\epsilon_s(m/t),$$

which proves the theorem. □

We will need the following standard tool in Arithmetic Function Theory.

Definition 5.12. Let $r, d \in \mathbb{N}$. The *Ramanujan sum* $c_r(d)$ is the function

$$c_r(d) := \sum_{\substack{a=1 \\ (a,r)=1}}^{r} e\left(\frac{da}{r}\right).$$

The Ramanujan sums exhibit the following properties:

Lemma 5.13. *Fix $d \in \mathbb{N}$. The following holds:*
i) The map $r \mapsto c_r(d)$ is multiplicative.
ii) The Dirichlet series $\sum_{r\geq 1} c_r(d) r^{-s} = \sigma_{s-1}(d) d^{-(s-1)} \zeta(s)^{-1}$, when $Re(s) > 1$, where $\sigma_u(n) := \sum_{d|n} d^u$ for any $u \in \mathbb{C}$.
iii) Let χ denote the unique non-trivial Dirichlet character mod 4 and let $L(s,\chi)$ denote its L-function. Then,

$$\sum_{r\geq 1} \chi(r) c_r(d) r^{-s} = \sigma_{\chi,s-1}(d) d^{-(s-1)} L(s,\chi)^{-1},$$

where $\sigma_{\chi,u}(d) = \sum_{d|k} \chi(d) d^u$ for $u \in \mathbb{C}$.

It is well-known that the character in iii) satisfies $\chi(1) = 1$ and $\chi(3) = -1$.

Proof. These are straightforward observations which we will prove for the sake of completeness.
i) Observe that if $(r,s) = 1$, the Chinese Remainder Theorem implies that $a = br + cs$ for some unique pair $(b,c) \in \mathbb{Z}/s\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$. As $(a, rs) = 1$ if, and only if, $(b,s) = (c,r) = 1$, we have

$$\begin{aligned} c_r s(d) &= \sum_{\substack{a=1 \\ (a,rs)=1}}^{rs} e\left(\frac{ad}{rs}\right) = \sum_{\substack{b=1 \\ (b,s)=1}}^{s} \sum_{\substack{c=1 \\ (c,r)=1}}^{r} e\left(\frac{d(br+cs)}{rs}\right) \\ &= \left(\sum_{\substack{b=1 \\ (b,s)=1}}^{s} e\left(\frac{db}{s}\right)\right)\left(\sum_{\substack{c=1 \\ (c,r)=1}}^{r} e\left(\frac{dc}{r}\right)\right) = c_r(d) c_s(d), \end{aligned}$$

as asserted.
ii) Using the definition of $c_r(d)$ and the properties of the Möbius function,

$$\begin{aligned} \sum_{r\geq 1} c_r(d) r^{-s} &= \sum_{r\geq 1} r^{-s} \sum_{\substack{a=1 \\ (a,r)=1}}^{r} e\left(\frac{ad}{r}\right) = \sum_{r\geq 1} r^{-s} \sum_{a=1}^{r} e\left(\frac{ad}{r}\right) \sum_{\substack{e|r \\ e|a}} \mu(e) \\ &= \sum_{ek\geq 1} \mu(e)(ek)^{-s} \sum_{a'=1}^{k} e\left(\frac{a'd}{k}\right) \end{aligned} \tag{5.18}$$

where $a' := a/e$ and $k := r/e$ for each simultaneous divisor e of a and r. The inner exponential sum in (5.18) is zero unless $k|d$, in which case it is equal to k. Hence, we have

$$\sum_{r\geq 1} c_r(d) r^{-s} = \sum_{e\geq 1} \mu(e) e^{-s} \sum_{k|d} k k^{-s} = \zeta(s)^{-1} d^{-(s-1)} \sum_{l|d} l^{s-1},$$

where $l := d/k$ in the last equality. Thus, ii) follows. The proof of iii) is similar to that of ii), using the complete multiplicativity of χ. □

Thus, the function $\epsilon_s(m)$ in (5.14) is $\pm c_m(s)$ when m is odd and $(1+(-1)^s)c_m(s)+2i^s c_m(s)$ when $4|m$ (otherwise, $\epsilon_s(m)=0$). Hence $\epsilon_s(m)=\chi(m)c_m(s)$, with χ as above when $4\nmid m$.
Lemma 5.13 iii) will imply an expression for the inner sum in the statement of Theorem 5.11 when $s\equiv 2 \pmod 4$, in which case $\delta(s,m)=0$ for any m.

Lemma 5.14. *Let $s\equiv 2$ (mod 4) and let $h_m(s):=\sum_{t|m}\frac{m}{t}\epsilon_s(t)$. For $x\geq 1$ let $H_s(x):=\sum_{m\leq x}h_m(s)$. Then, for any $\epsilon>0$,*

$$H_s(x)=\frac{\sigma_\chi(s)}{2s}L(2,\chi)^{-1}x^2\left(1+O\left(exp\left(-(\log x)^{\frac{1}{3}-\epsilon}\right)\right)\right),$$

where $\sigma_\chi(s)=\sigma_{\chi,1}(s)$ with the notation in Lemma 5.13.

Proof. By construction, $h_m(s)$ is the Dirichlet convolution $h_m(s)=(\epsilon_s * id)(m)$, where id denotes the identity map, for each $m\in\mathbb{N}$. From Lemma 5.13, the above observations regarding ϵ_s and basic notions of Dirichlet series, it follows that when $\mathrm{Re}(w)>2$,

$$\begin{aligned}\sum_{m\geq 1}h_m(s)m^{-w}&=\left(\sum_{k\geq 1}\chi(k)c_k(s)k^{-w}\right)\left(\sum_{k\geq 1}id(k)k^{-w}\right)\\&=\sigma_{\chi,w-1}(s)s^{-(w-1)}L(w,\chi)^{-1}\zeta(w-1)=:F(w).\end{aligned}\tag{5.19}$$

$H_s(x)$ is determined via a standard application of the Effective Perron Formula (see, for example, section II.2 in [27]) along the line $\kappa:=2+(\log x)^{-1}$. For completeness, we give the details of this application. Fix $T\geq 2$, to be chosen later. When $\mathrm{Re}(w)=2$, every factor in (5.19) is absolutely convergent except for $\zeta(w-1)$ (which has a simple pole at $w=2$). It follows that

$$H_s(x)=\frac{1}{2\pi i}\int_{\kappa-iT}^{\kappa+iT}F(w)x^w\frac{dw}{w}+O\left(x^2T^{-1}\log x+B(2x)\left(1+x\frac{\log T}{T}\right)\right),\tag{5.20}$$

where B is some real-valued, non-decreasing function satisfying $|h_m(s)|\leq B(m)$ for each m. Note that for any d, the triangle inequality implies the trivial bound $|c_r(d)|\leq\phi(r)$. Hence, $|h_m(s)|\leq m\sum_{t|m}\phi(t)t^{-1}\leq m\tau(m)=O(m^{1+\epsilon})$ for any $\epsilon>0$. We may thus take $B(x)=x^{1+\epsilon}$ for some fixed ϵ.
A well-known theorem of Korobov and Vinogradov (see the notes of Chapter 6 of [29]) asserts that there is a $c>0$ such that $\zeta(s)\neq 0$ as long as $\mathrm{Re}(s)>1-\frac{c}{(\log x)^{\frac{2}{3}}(\log_2 x)^{\frac{1}{3}}}$. Set $\kappa_0:=2-c/(\log x)^{\frac{2}{3}+\epsilon}$ and let Γ denote the rectangular contour with corners at $\kappa\pm iT,\kappa_0\pm iT$, traversed counterclockwise. The interior of the contour contains only the pole at $w=2$ of $\zeta(w-1)$. By the Residue theorem, the main term of (5.20) is

$$\frac{1}{2\pi i}\left(\int_\Gamma+\int_{\kappa_0-iT}^{\kappa_0+iT}+\int_{\kappa_0+iT}^{\kappa+iT}-\int_{\kappa_0-iT}^{\kappa-iT}\right)F(w)x^w\frac{dw}{w}=\frac{\sigma_\chi(s)}{2s}L(2,\chi)^{-1}x^2+I_1+I_2-I_3,\tag{5.21}$$

where the integrals I_j are enumerated according to their order on the left side of (5.21). Their contribution remains to be determined.
Write $s=\sigma+i\tau$. From Chapter 5 in [29], $|\zeta(s)|\ll\log|\tau|$ whenever $\sigma>\kappa_0$. Thus, we may bound both

I_2 and I_3 (in which the imaginary part is held fixed with absolute value T) as follows:

$$|I_j| \ll \log T \int_{\kappa_0}^{\kappa} x^u \left| \frac{\sigma_{\chi,u-1+iT}(s)}{s^{u-1+iT} L(u+iT,\chi)} \right| \frac{d|w|}{(u^2+T^2)^{\frac{1}{2}}} \ll x^{\kappa} \frac{\log T}{T} \tau(s), \tag{5.22}$$

for $j \in \{2,3\}$. The last inequality holds because $|L(w,\chi)| \gg 1$ whenever $\mathrm{Re}(w) > 1$, and

$$\left| \frac{\sigma_{\chi,w-1}(s)}{s^{w-1}} \right| = s^{-\mathrm{Re}(w)+1} \sum_{t|s} t^{\mathrm{Re}(w)-1} \leq \tau(s).$$

To bound I_1, we note that the integrand is bounded in the compact subinterval $|\mathrm{Im}(w)| \leq t_0$ of the line $\kappa_0 \pm i\infty$, where $t_0 > 0$ is fixed. By the symmetry of the integral about the real axis, we have

$$|I_1| \ll x^{\kappa_0} \tau(s) \int_{t_0 < t \leq T} |\zeta(\kappa_0 + it)| \frac{dt}{(\kappa_0^2 + t^2)^{\frac{1}{2}}} \ll x^{\kappa_0} \tau(s) (\log T)^2. \tag{5.23}$$

The combined error term from (5.20), (5.22) and (5.23) is then

$$\ll x^{\kappa_0} \tau(s) (\log T)^2 + x^2 \frac{\log T}{T} \tau(s) + x^2 T^{-1} \log x + x^{1+\epsilon} \left(1 + x \frac{\log T}{T} \right). \tag{5.24}$$

It suffices (albeit perhaps not optimally) to select $T = x$. The largest error term in (5.24) is the first one, which satisfies

$$\ll_s x^{\kappa_0 + o(1)} = x^2 \exp\left(-\frac{\log x}{(\log x)^{\frac{2}{3}+\epsilon}} + o(1) \right) = x^2 \exp\left(-(\log x)^{\frac{1}{3}-\epsilon} \right).$$

The statement of the lemma now follows. □

When $s \not\equiv 2 \pmod 4$, in contrast to (5.19), the Dirichlet series for ϵ_s is instead

$$\begin{aligned} \sum_{m \geq 1} \epsilon_s(m) m^{-w} &= \sum_{m \equiv 1 \pmod 4} c_m(s) m^{-w} - \sum_{m \equiv 3 \pmod 4} c_m(s) m^{-w} + (1+i^s)^2 \sum_{m \equiv 0 \pmod 4} c_m(s) m^{-w} \\ &= \sum_{m \geq 1} \chi(m) c_m(s) m^{-w} + (1+i^s)^2 4^{-w} \sum_{k \geq 1} c_{4k}(s) k^{-w}. \end{aligned}$$

The same argument used to prove part ii) of Lemma 5.13 demonstrates that

$$\sum_{k \geq 1} c_{4k}(s) k^{-w} = 4 \sum_{d \geq 1} \mu(d) d^{-w} \sum_{4k | s} k^{-(w-1)}. \tag{5.25}$$

Clearly, this sum is zero unless $4|s$. In this case, the inner sum of (5.25) is $(s/4)^{-(w-1)} \sigma_{w-1}(s/4)$. Part iii) of Lemma 5.13 then implies that

$$\sum_{m \geq 1} \epsilon_s(m) m^{-w} = \sigma_{\chi,w-1}(s) s^{-w-1} L(w,\chi)^{-1} + H(w),$$

where

$$H(w) := \begin{cases} 4^w s^{-(w-1)} \sigma_{w-1}(s/4) \zeta(w)^{-1} & \text{if } s \equiv 0 \pmod 4 \\ 0 & \text{otherwise} \end{cases}.$$

The product $H(w)\zeta(w-1)$ is also evaluated with the method of Lemma 5.14 (where only the value of the residue, which is now $\left(8s^{-1}\sigma(s/4)\zeta(2)^{-1}+\frac{\sigma_\chi}{2s}L(2,\chi)^{-1}\right)x^2$, is different). We may thus restate Lemma 5.14 for $s\equiv 1,3 \pmod 4$ as well.

Lemma 5.15. *With the notation of Lemma 5.14,*

$$H_s(x)=M(s)x^2\left(1+O\left(exp\left(-(\log x)^{\frac{1}{3}-\epsilon}\right)\right)\right),$$

where $M(s)$ is defined as

$$M(s):=\begin{cases}\left(8s^{-1}\sigma(s/4)\zeta(2)^{-1}+\frac{\sigma_\chi(s)}{2s}L(2,\chi)^{-1}\right) & \text{if } 4|s\\ \frac{\sigma_\chi(s)}{2s}L(2,\chi)^{-1} & \text{otherwise}\end{cases}.$$

We immediately deduce the following:

Theorem 5.16. *Fix $s\in\mathbb{Z}\backslash\{0\}$. Let $\mathcal{T}_s:=\{a^2+b^2+s : a,b\in\mathbb{Z}\}$. Put $\tau(m;y,z):=|\{d|m : d\in(y,z]\}|$. Then, uniformly in $2\le y<z\le x^{\frac{1}{2}}$,*

$$\sum_{\substack{n\le x\\ n\in\mathcal{T}_s}}\tau(n;y,z)=(x-s)\pi M(s)\log(z/y)+O\left(x^{\frac{1}{2}}(z-y)\right). \tag{5.26}$$

Proof. The left side of (5.26) is

$$\sum_{\substack{n\le x\\ n\in\mathcal{T}_s}}\tau(n;y,z)=\sum_{a^2+b^2+s\le x}\ \sum_{\substack{d|a^2+b^2+s\\ d\in(y,z]}}1=\sum_{y<d\le z}\ \sum_{\substack{a^2+b^2+s\le x\\ a^2+b^2+s\equiv 0 \pmod d}}1.$$

By Theorem 5.11 and Lemma 5.15, we have (with the notation $h_d(s)$ from the proof of Lemma 6.3)

$$\begin{aligned}\sum_{\substack{n\le x\\ n\in\mathcal{T}_s}}\tau(n;y,z)&=\sum_{y<d\le z}\left(\left(\frac{x-s}{d^2}\right)\pi+O\left(x^{\frac{1}{2}}d^{-1}\right)\right)\sum_{t|d}\frac{d}{t}\epsilon_s(t)\\ &=(x-s)\pi\sum_{y<d\le z}\frac{1}{d^2}h_d(s)+O\left(x^{\frac{1}{2}}\sum_{y<d\le z}\frac{1}{d}h_d(s)\right)\\ &=(x-s)\pi\int_y^z u^{-2}dH_s(u)+O\left(x^{\frac{1}{2}}\int_y^z u^{-1}dH_s(u)\right)\\ &=(x-s)\pi\left(\frac{H_s(z)}{z^2}-\frac{H_s(y)}{y^2}\right)+2\int_y^z H_s(u)u^{-3}du+O\left(x^{\frac{1}{2}}(z-y)\right)\\ &=(x-s)\pi M(s)\int_y^z\frac{du}{u}+O\left(\int_y^z\exp\left(-(\log u)^{\frac{1}{3}-\epsilon}\right)\frac{du}{u}\right)+O\left(x^{\frac{1}{2}}(z-y)\right).\end{aligned}$$

With the change of variable $v=\log u$, the first error term becomes $\ll\int_{e^y}^{e^z}\exp(-v^{\frac{1}{3}-\epsilon})dv\ll 1$. The proof of (5.26) is now complete. □

Bibliography

[1] R. Ash. *A Course in Algebraic Number Theory.* 2001. Course notes available from: http://www.math.uiuc.edu/ r-ash/.

[2] B. Berndt, R. Evans, and K. Williams. *Gauss Sums and Jacobi Sums.* Canadian Mathematical Society Monographs, New York, NY, 2002.

[3] P. Erdős. A generalization of a theorem of Besicovitch. *J. London Math. Soc.*, pages 92–98, 1936.

[4] P. Erdős. Some remarks on number theory. *Riveon Lematematika*, 9:13–17, 1955. (Hebrew).

[5] P. Erdős and R. R. Hall. On the Möbius function. *J. Reine. Angew. Math.*, 315:121–126, 1980.

[6] P. Erdős and G. Szekeres. Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem. *Acta Litt. Sci. Szeged*, 7:95–102, 1934.

[7] J. Esmonde and M. R. Murty. *Problems in Algebraic Number Theory.* Graduate Texts in Mathematics, Springer, New York, NY, 2004.

[8] K. Ford. The distribution of integers with a divisor in a given interval. *Annals of Math.*, 168:367–433, 2008.

[9] K. Ford. Integers with a divisor in $(y, 2y]$. *Anatomy of Integers, CRM Proc. and Lect. Notes*, 46:65–80, 2008.

[10] K. Ford, M.R. Khan, I.E. Shparlinski, and C.L. Yankov. On the maximal difference between an element and its inverse in residue rings. *Proc. Amer. Math. Soc.*, 133:3463–3468, 2005.

[11] J. B. Friedlander and H. Iwaniec. *Opera de Cribro.* American Mathematical Soceity Colloquium Series, Volume 57, Providence, RI, 2010.

[12] R. R. Hall. *Sets of Multiples.* Cambridge University Press, Cambridge, UK, 1996.

[13] R. R. Hall and G. Tenenbaum. *Divisors.* Cambridge University Press, Cambridge, UK, 1988.

[14] G.H. Hardy and E.M. Wright. *An Introduction to the Theory of Numbers.* Oxford, UK, 1956.

[15] D. R. Heath-Brown. On the density of zeros of the Dedekind zeta-function. *Acta Arith.*, 33:169–181, 1977.

[16] C. Hooley. A new technique in the theory of numbers. *Proc. London Math. Soc.*, 38:115–151, 1979.

[17] G. Janusz. *Algebraic Number Fields.* American Mathematical Society, Providence, RI, 1996.

[18] J. Knopfmacher. *Abstract Analytic Number Theory.* Dover Publishing, New York, NY, 1975.

[19] D. Koukoulopoulos. Divisors of shifted primes. *Int. Math. Res. Not.*, 24:4585–4627, 2010.

[20] D. Koukoulopoulos. Localized factorizations of integers. *Proc. London Math. Soc.*, 101:392–426, 2010.

[21] J. Lagarias and A. Odlyzko. Effective versions of the Chebotarev density theorem. *in "Algebraic Number Fields", A. Fröhlich*, 1977.

[22] E. Landau. Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes. *Mathe. Ann.*, 56, 1903.

[23] E. Landau. *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale.* American Mathematical Society, Providence, RI, 2001.

[24] S. Lang. *Algebra.* Graduate Texts in Mathematics, Springer, New York, NY, 2002.

[25] H. Montgomery and B. Vaughan. *Multiplicative Number Theory: I. Classical Theory.* Cambridge University Press, Cambridge, UK, 2006.

[26] M. I. Rosen. *Number Theory in Function Fields.* Graduate Texts in Mathematics, Springer, New York, NY, 2001.

[27] G. Tenenbaum. Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné. *Compositio Math.*, 51:243–263, 1984.

[28] G. Tenenbaum. *Introduction to Analytic and Probabilistic Number Theory.* Cambridge University Press, Cambridge, UK, 1994.

[29] E. H. Titchmarsh. *The Theory of the Riemann Zeta Function (with notes by D.R. Heath-Brown).* Oxford University Press, Oxford, UK, 1986.