On Square-Free Values of Polynomials over Integers and Function Fields

Bachelor's Thesis, TWIN

Jasper Van den Neste (3908100)
Supervisor: dr. D. Schindler

June 13, 2018

Utrecht University

Abstract

Square-free values are of significant interest to number theorists, partly due to their close connection to the Möbius function. However, little is known about square-free values of polynomials with integer coefficient when the degree of the polynomial is greater than 3. For instance, it has yet to be proved that the polynomial $f(x) = x^4 + 2$ takes infinitely many square-free values, let alone that an asymptotic density of square-free values is known.

The main purpose of this thesis is to show how to prove the density of square-free values for polynomials of degree 1 and 2, after which the focus shifts to polynomials in one variable over the field $\mathbb{F}_q$. We show that, when considering the latter, a certain asymptotic density can be proved for square-free polynomials of any degree. Furthermore, we compare this proof to the strategy used to prove the asymptotic density of polynomials with integer coefficients. Finally, we investigate the density of square-free values of polynomials with large varying coefficients, making use of Brun's sieve, and again find similar densities.

Contents

1 Introduction.

1.1 Introduction.

Number theory is a perplexing branch of mathematics. Few other fields ponder questions that seem eminently simple and find that they turn out to be so difficult to answer. When looking at the almost trivial definition of the positive integer, a beautiful simplicity is found. On the other hand, when attempting to isolate the fundamental building blocks of these integers, the prime numbers, and their distribution, we find a complexity that bewilders mathematicians even nowadays. It is well know that prime numbers form the basis for the multiplicative structure of $\mathbb{Z}$ and because of that, prime numbers play a central role in many of the questions which arise in classical number theory. For example, the importance of primes in multiplication is undeniable, but what in addition? The famous *Goldbach Conjecture* ponders this question. Is it true that every even positive integer greater than 2 can be written as the sum of two primes? A prime example of an easy question to ask and nevertheless it remains unsolved to this day. For another example, two primes are called *twins* if they are two apart (e.g., 3 and 5, 11 and 13, etc). Here we might ask: Are there infinitely many such pairs? The answer to this "Twin Primes Question" remained unknown for a long time but has recently been solved, putting a boundary on the distance between two consecutive prime pairs [25]. Now we know that $\mathbb{Z}$ is a unique factorization domain (which is defined later), but it turns out that there are many others which are interesting in their own right. The one that we focus on in this paper is the class of polynomials in one variable x with coefficients in a field K, denote $K[x]$, and observe that it is in fact a unique factorization domain[16].

As we shall see, integers are not the only ring that have baffled mankind over the years. Can we now answer the same number theoretic problems for $\mathbb{F}_q[x]$ as for $\mathbb{Z}$? For instance, can we state some analogue to the Goldbach Conjecture in this new setting, and can we answer it? A first try might be: "Can every even monic polynomial be written as a sum of two monic irreducible polynomials?" Though we have not yet defined the meaning of this conjecture (i.e. what are even polynomials?), it does seem to make some sense. If, however, we try the Twin Prime Conjecture, it is definitely not clear what "twin irreducible polynomials" might be. If we take for example the size of a prime $|f|, f \in \mathbb{F}_q[x]$, we note that there are several $f \in \mathbb{F}_q[x]$ which have the same size. How then would we characterize the distance between these primes? An interesting discussion on the subject in given by Lior Bary-Soroker.[4]

If we want to answer questions like the two presented above about polynomials, we need to know something about the irreducible elements within the setting. The basic idea would be: If irreducibles are more dense among the polynomials than primes are among the integers, then questions like the *Goldbach Conjecture* should be easier to answer in the polynomial case; if irreducibles are less dense than primes, the answers might be more difficult to find; and if the densities are similar, then the questions may be comparably hard to answer. But the nature and density of irreducible polynomials depends completely on the field K, so we need to consider some specific fields.

The fundamental Theorem of Algebra gives us some insight on irreducible

polynomials in $\mathbb{C}[x]$. Since every polynomial of degree n over $\mathbb{C}$ has n roots in $\mathbb{C}$, we see that every polynomial over $\mathbb{C}$ factors completely into linear polynomials. Continuing this reasoning, we see that the only irreducible elements over $\mathbb{C}$ are the linear polynomials. By using a similar reasoning, over $\mathbb{R}$, $f(x)$ factors into a product of linear and/or quadratic polynomials; that is, the irreducibles over $\mathbb{R}$ are either linear or quadratic. Thus we see that, in some sense, irreducibles in $\mathbb{C}[x]$ and $\mathbb{R}[x]$ are relatively scarce, and thus it is quite difficult to solve an analogue to the Goldbach Conjecture.

In this thesis, we contrast and compare the ring of integers and the ring of polynomials in a single variable over a finite field. Mainly, the focus lies on square-free values and we try to answer analogous versions of problems in both rings.

Definition 1.1. (Square-free integer). We define an integer $n \in \mathbb{N}$ to be square-free if, for any integer $a \in \mathbb{N}, a > 1$, n is not divisible by the square of a.

For the relevance of square-free integers in number theory we look at the Möbius function $\mu(n)$, Definition 2.10, a function which is closely related to square-free values since $\mu^2(n)$ is the indicator function for square-free values. Now $\mu(n)$ turns out to be a very well-connected function in number theory and also finds many applications in combinatorics[24]. It shows up in the Möbius inversion formula and encodes one of the most important mysteries in mathematics, the Riemann hypothesis. On the other hand, square-free values also are related to another mystery, a mystery connected to the distribution of prime factors as well, the ABC conjecture. Most these concepts are explained later in this thesis. But in short, from an interest in number theory, inevitably an interest in the Möbius function rises, and an interest in the Möbius function results in an interest in square-free values.

Another reason why people study the Möbius function is due to the fact that its behavior is directly linked to the Prime Number Theorem, stating that, when taking the limit $x \to \infty$, the number $\pi(x)$ of primes below x is asymptotically equal to $\frac{x}{\log x}$. It turns out that the Prime Number Theorem is "equivalent" to the fact that $\mu(n)$ has average value ("mean value") zero, i.e., $\lim_{x\to\infty} \frac{1}{x} \sum_{n\leq x} \mu(n) = 0$.[2, Chapter 3.9] We can interpret this final statement as follows: If we randomly pick a square-free integer n, then, since $\mu(n) = \pm 1$ depending only on an even or odd number of factors, it is equally likely to have an even and an odd number of prime factors.

However, in the end a substantial part of the interest in square-free values, as with prime numbers, is probably from an aesthetical and metaphysical viewpoint. Nearly everybody shares the feeling that numbers are important, and the integers in particular. Prime numbers are a crucial part of the integers: they tell you how you can break numbers down and build them up. To anyone studying mathematics, investigating integers feels like discovering the atoms of the universe. And analyzing their behaviour and connection is like putting together the skeleton of the universe. Now often, it turns out to be quite difficult to study prime numbers. Therefore the focus sometimes shifts to a related subject, in this case, square-free values. We hope that a profound understanding of square-free values helps us to better grasp the behaviour of

prime numbers as well.

As mentioned earlier, the nature and density of irreducible polynomials depends completely on the field over which we speak. This thesis focuses mainly on the field $\mathbb{F}_q$ (which is defined later in 3.1). The polynomial ring $\mathbb{F}_q[x]$ and the ring of integers $\mathbb{Z}$ has several common characteristics. For instance, both have a Euclidean algorithm, hence are unique factorization domains. Also, there are some quantitative aspects for which we find similarities in both rings: Units of the ring of integers are ± 1, and every nonzero integer can be multiplicatively built up by a unit and a positive integer. Analogously, the units of $\mathbb{F}_q[x]$ are the nonzero scalars $\mathbb{F}_q^\times$, and every nonzero polynomial can be multiplicatively built up by a unit and monic polynomial. The counterpart of a prime in $\mathbb{Z}$ is a monic irreducible polynomial. Analyzing arithmetic properties of integers is done by sampling these integers uniformly in the interval $[A, 2A]$ in the limit $A \to \infty$; Analogously, analyzing arithmetic properties of polynomials is done by sampling these polynomials uniformly from the monic polynomials M_n of degree n in the limit $\#M_n = q^n \to \infty$. The Prime *Number* Theorem tells us that the number of primes $p \leq x$ is $\pi(x) \sim \frac{x}{\log x}$ in the limit $x \to \infty$. If the Riemann Hypothesis if true, this would tell us that $\pi(x) = \int_2^x \frac{\mathrm{d}x}{\log x} + O\left(x^{1/2+o(1)}\right)$. The Prime *Polynomial* Theorem, analogously, tells us that the number of monic irreducible polynomials of degree n is $\pi_q(n) = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right)$. This corresponds to Prime Number Theorem (and to Riemann Hypothesis) if we map $x \leftrightarrow q^n$, recalling that x is the number of positive integers up to x and q^n is the number of monic polynomials of degree n. In many situations, it seems to make sense to compare number theoretic questions in these two fields, as we do in this paper.

Our main focus lies on the issue of representing square-free integers by polynomials with integer coefficients. This thesis has the following structure: In Section 2, we investigate square-free values of integer polynomials of degree 1 and discuss the density (as defined is the aforementioned section) of these values. Thereafter we examine the same density for polynomials of degree 2. In Section 3, having addressed the problems in the ring of integers $\mathbb{Z}$, we shift our focus to function fields, specifically the finite field $\mathbb{F}_q$. In this chapter, a basis for ring theory is displayed, after which the analogue for square-free values of polynomials of degree 2 is laid out. Throughout this chapter, a comparison between $\mathbb{Z}$ and $\mathbb{F}_q[x]$ is drawn. After establishing the analogue and, thus having a basis in finite fields, we analyse the article by Dan Carmon 'On Square-Free Values of Large Polynomials over the Rational Function Field'[6].

2 Square-free values of Integer Polynomials.

When we talk about how "often" square-free values occur within the range of a polynomial, a useful definition is that of a *density*:

Definition 2.1 (Density of square-free values of a polynomial)**.** First we define, for a polynomial $f \in \mathbb{Z}[x]$,

$$\mathcal{N}_f(n) := \{k \in \mathbb{Z}, 1 \leq k \leq n : f(k) \text{ square-free}\}.$$

We define the density c_f of square-free values of the polynomial f to be the proportion of values n in an interval $A = [0, b] \subset \mathbb{Z}$, where $f(n)$ is square-free:

$$c_f := \lim_{n\to\infty} \frac{\#\mathcal{N}_f(n)}{n}$$

Definition 2.2 (Density of square-free values in the positive integers)**.** Suppose $C_n = \{k \in \mathbb{Z} : 1 \leq k \leq n, k \text{ is square-free}\}$. If the limit

$$D = \lim_{n\to\infty} \frac{|C_n|}{n}$$

exists, we define this limit to be the density D of square-free values in the positive integers. $\mathbb{N}$

Remark. Combining Definition 2.1 and 2.2, we see that $D = c_x$.

Definition 2.3 (Square-free polynomial)**.** For a polynomial $f \in \mathbb{Z}[x]$, this polynomial is *square-free* if:

For every prime $p \in \mathbb{Z}$, there exists an x, depending on p, such that $p^2 \nmid f(x)$.

Remark. We make two assumptions, as to make sure our quest for finding square-free values of polynomials doesn't end before we start.

i) $f(x)$ is not divisible by the square of some non-constant polynomial $g \in \mathbb{Z}[x]$. Since, if $f(x)$ is divisible by $g(x)$, then $f(a)$ can be only square-free if $g(a) = \pm 1$. Since we stated that g is non-constant, this $g(k) = \pm 1$ for a finite number of $k \in \mathbb{Z}$. For example, if

$$f(x) = (2x + 1)^2(x^2 - 9x + 6),$$

we see that there are no square free values for $x \in \mathbb{Z}\backslash\{0\}$.

ii) $f(x)$ cannot be written as $f(x) = p^2 g(x)$, where $g(x) \in \mathbb{Z}[x]$ and $p \in \mathbb{Z}\backslash\{1, -1, 0\}$. Since, if $f(x)$ can be written as $f(x) = p^2 g(x)$, then we see that for every $k \in \mathbb{Z}$, $f(k)$ is not square-free.

However, not all functions that meet above assumptions are square-free polynomials. For example, $f(x) = x(x+1)(x+2)(x+3)$, meets the requirements, but we see that $2^2 \mid f(x), \forall x \in \mathbb{Z}\backslash\{0\}$, and thus f is not a square-free polynomial.

Given these definitions an interesting question would be:

Question 1. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n. Are there infinitely many positive integers k such that $f(k)$ is square-free? If so, can we find the density c_f of square-free values of a given function f?

Remark. If one of the aforementioned assumptions is not met, the density $c_f \to 0$. These situations are therefore not discussed any further.

Since we're interested in calculating the density of square-free values, we define a function $\rho_f(d)$ that counts the number of values $a \in \{0, \dots, d-1\}$ for which $d \mid f(a)$:

Definition 2.4.

$$\rho_f(d) := \#\{a \in \frac{\mathbb{Z}}{d\mathbb{Z}} : f(a) \equiv 0 \bmod d\}.$$

Then, for small primes p, the probability that $f(a)$ is not divisible by some p^2 is $\left(1 - \frac{\rho_f(p^2)}{p^2}\right)$. If we assume that the probability of a function evaluated at a being divisible by p^2 is independent for every different $p \in \mathcal{P}$ ($\mathcal{P}$ being all primes $\in \mathbb{N}$), we have the following conjecture:

Conjecture 2.1. Let $f \in \mathbb{Z}[x]$ be a square-free polynomial of degree n. Then there are infinitely many square-free values taken by $f(k)$. The density of square-free values of a polynomial f is

$$c_f := \prod_{p \in \mathcal{P}} \left(1 - \frac{\rho_f(p^2)}{p^2}\right).$$

Remark. Note that, if we can write $f(x) = p^2 g(x)$ where $p \in \mathbb{N}$ as mentioned above, we find $\rho_f(p^2) = p^2$ and thus we now see that $c_f = 0$.

In Section 2.1 and 2.2, we focus mainly on the density of square-free values of polynomials with non-varying coefficients, and solve Conjecture 2.1 for a number of cases. But an interesting question might be: How will varying coefficient change the density of square free values, considering that the coefficients might be tending to infinity faster than the arguments?

Question 2. Assume $N \in \mathbb{Z}$ to be "sufficiently" large, can N be written as a sum of a positive k-th power and a positive square-free: $N = x^k + r$? How many values of x can we find, asymptotically?

We can translate this problem to finding $\#\{x \in \mathbb{N} : f(x) = N - x^k \text{ is square-free}, x^k \leq N\}$. Looking at Conjecture 2.1, using the logic as displayed before, we could state that the number of values x is $c_f N^{1/k} \geq 0$. Considering that in this situation both c_f and f depend on N, an answer to Question 2 is not obvious from Conjecture 2.1. Yet it has been solved in a similar fashion by Estermann in [14] for $k = 2$, and a case was stated by Hooley in [19, §4.6, Theorem 4] for $k = 3$. This proof is unfortunately unsuccessful in determining the number of representations of Question 2, nor can it be used when x^3 is replaced with a general polynomial of degree 3. In this day and age, the case for $k \geq 4$ is still unsolved.

We now investigate Conjecture 2.1 for a number of different types of polynomials.

2.1 Polynomials of degree 1 [26].

For polynomials of degree *1*, we show that the density of Conjecture 2.1 equals the regular density of square-free values in $\mathbb{Z}$. Therefore we focus on the density D first. Before this density is be calculated, some basic definitions are stated:

Definition 2.5 (Dirichlet series)**.** Given an arithmetic function $a : \mathbb{N} \to \mathbb{C}$ and suppose there is an $s \in \mathbb{C}$ for which the infinite series

$$D_a(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

converges, then this series is called the *Dirichlet series of* a.

Definition 2.6 (Riemann Zeta function)**.** The Riemann Zeta function $\zeta(s)$ is defined for complex arguments s with $\mathrm{Re}(s) > 1$ as

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

Theorem 2.1 (Regular density of square-free values)**.** *The probability that a large random integer is square-free — that is, the density* D *— is* $\frac{1}{\zeta(2)}$.

To prove Theorem 2.1, Lemma 2.1 is used.

Lemma 2.1. Given two random positive integers $j, k \in \{1, \ldots, n\}$. The asymptotic probability that j and k are relatively prime as $n \to \infty$ — that is, their greatest common factor is 1 — is $\frac{6}{\pi^2}$.

We use the asymptotic density of square-free numbers D, as defined in Definition 2.2. Say we have any two distinct numbers $j, k \in \mathbb{Z}$ where $j < k < n$. The set of all the possible combinations we call B_n and is therefore defined as:

$$B_n = \left\{(j, k) \in \mathbb{Z}^2 : 1 \leq j < k \leq n\right\}.$$

Then

$$|B_n| = \frac{n!}{2!(n-2)!} = \frac{n(n-1)}{2}.$$

Now we define A_n to be the pairs which are relatively prime:

$$A_n = \left\{(j, k) \in \mathbb{Z}^2 : 1 \leq j < k \leq n,\ \gcd(j, k) = 1\right\}.$$

Dividing A_n and B_n defines the probability p_n that two selected integers are relatively prime:

$$p_n = \frac{|A_n|}{|B_n|} = \frac{2|A_n|}{n(n-1)}. \tag{1}$$

To calculate this probability p_n, several *arithmetic* functions are used.

2.1.1 Arithmetic functions and Dirichlet products.

In this section, we introduce some mathematical background on arithmetic functions, Dirichlet series and Dirichlet products. These basics are then used in the proof of Lemma 2.1.

Definition 2.7 (Arithmetic function)**.** Any real- or complex valued function function a is called an *arithmetic* function if it is defined on the set $\mathbb{N}$ of positive integers.

Definition 2.8 ("Big Oh" estimate)**.** "$f(x) = O(g(x))$" means that there exist constants x_0 and c such that $|f(x)| \leq c|g(x)|$ for all $x \geq x_0$.

Definition 2.9 ("Small Oh" estimate)**.** "$f(x) = o(g(x))$" means that for sufficiently large x, $g(x) \neq 0$ and $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Definition 2.10 (Möbius function μ)**.** The Möbius function μ is the arithmetic function defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1; \\ (-1)^m, & \text{if } n = \prod_{j=1}^{m} p_j, \text{ where } \{p_j\}_{j=1}^{m} \text{ are distinct primes;} \\ 0, & \text{otherwise.} \end{cases}$$

In other words, the function is 0 if the argument is not a square-free value and $(-1)^k$ if the argument is composed of k distinct prime factors.

Definition 2.11 (Multiplicativity)**.** An arithmetic function a is called *multiplicative* if $a \not\equiv 0$ and $a(nm) = a(n)a(m)$ whenever $\gcd(n, m) = 1$.

From this definition, we see that for a multiplicative function $a \not\equiv 0$, then $a(1) = a(1 \cdot 1) = a(1)a(1) = 1$. For the same a, it holds that its value depends only on its values on the prime powers; if $n = \prod_{j=1}^{m} p_j^{k_j}$ is the factorization of n into a product of distinct prime powers, then $a(n) = a(\prod_{j=1}^{m} p_j^{k_j}) = \prod_{j=1}^{m} a(p_j^{k_j})$.

Lemma 2.2. The arithmetic function μ is multiplicative.

Proof. We look at three possibilities

i) We note that $\mu(1) = 1$. So for any n, we see that $\mu(n \cdot 1) = \mu(n) = 1 \cdot \mu(n) = \mu(1) \cdot \mu(n)$.

ii) $\mu(n) = 0$ or $\mu(m) = 0$. Then either m or n has a factor p_i^k with $k \geq 2$. Then also $\mu(nm) = 0 = \mu(n)\mu(m)$.

iii) $m = p_1 p_2 \dots p_r$ and $n = q_1 q_2 \dots q_s$. Since we look at m and n being relative prime, this translates to $q_i \neq p_j$ for all $(i, j) \in \mathbb{Z}^2$. Then $\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(n)\mu(m)$.

This then completes the proof that μ is multiplicative. □

Three more arithmetic functions need to be introduced:

Definition 2.12.

$$\mathbf{1}(n) = 1, \text{for all } n; \quad e(n) = \begin{cases} 1, & \text{if } n = 1; \\ 0, & \text{otherwise.} \end{cases}, \quad i(n) = n, \text{for all } n;$$

Definition 2.13 (Dirichlet convolution)**.** For two arithmetic functions a and b, the Dirichlet convolution of a and b, denoted by $a * b$ is the arithmetic function defined by

$$(a * b)(n) = \sum_{d|n} a(d) b\left(\frac{n}{d}\right), \ n \in \mathbb{N}.$$

The convolution arises naturally in the following context:

Lemma 2.3. Given the (absolutely convergent) Dirichlet series

$$D_a(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}, \tag{2}$$

and

$$D_b(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^s}, \tag{3}$$

their product is as follows:

$$D_a(s)D_b(s) = \sum_{n=1}^{\infty} \frac{(a*b)(n)}{n^s}.$$

Proof.

$$\begin{aligned} D_a(s)D_b(s) = \left(\sum_{d=1}^{\infty} \frac{a(d)}{d^s}\right)\left(\sum_{k=1}^{\infty} \frac{b(k)}{k^s}\right) &= \sum_{d,k=1}^{\infty} \frac{a(d)b(k)}{(d\,k)^s} \\ = \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d,k:\ d\cdot k=n} a(d)b(k) &= \sum_{n=1}^{\infty} \frac{1}{n^s} \sum_{d|n} a(d)b(\frac{n}{d}) \\ = \sum_{n=1}^{\infty} \frac{(a*b)(n)}{n^s}. & \end{aligned} \tag{4}$$

□

One argument for defining the equation (4) in that way is due to the fact many arithmetic functions are defined by a Dirichlet product. Also many identities among arithmetic functions can be written as identities involving Dirichlet products. Proofs are given later, but some examples are:

i) $D_e(s) = \sum_{n=1}^{\infty} \frac{e(n)}{n^s} = 1$.

ii) $D_\mu(s)D_{\mathbf{1}}(s) = \sum_{n=1}^{\infty} \frac{(\mu*\mathbf{1})(n)}{n^s} = \sum_{n=1}^{\infty} \frac{e(n)}{n^s} = 1$, where the second equality is true since $\sum_{d|n} \mu(d) = e(n)$.

iii) $\sum_{d|n} \mu(d)\frac{n}{d} = \phi(n)$, so $\mu * i = \phi$.

Another argument for defining the Dirichlet product in the the form of equation (4) is that the product has useful algebraic properties. For following theorems, see [2, Chapter 2].

Theorem 2.2 (Properties of Dirichlet convolution)**.**

i) The function e acts as a unit element for $*$, i.e., $a * e = e * a = a$ for all arithmetic functions a.

ii) The Dirichlet product is commutative, i.e., $a * b = b * a$ for all arithmetic functions a and b.

iii) The Dirichlet product is associative, i.e., $(a * b) * c = a * (b * c)$ for all arithmetic functions a, b and c.

iv) If $a(1) \neq 0$, then a has a unique Dirichlet inverse, i.e., there is a unique function b such that $a * b = e$.

Theorem 2.3 (Products and quotients of multiplicative functions)**.** *Assume a and b are multiplicative functions. Then:*

i) The (pointwise) product of a and b defined by $(a \cdot b)(n) = a(n)b(n)$ is multiplicative.

ii) If b is non-zero, then the quotient a/b is multiplicative.

Proof. The proof follows directly from the definition of multiplicativity. □

Theorem 2.4 (Dirichlet product and multiplicative functions)**.**

i) If a and b are multiplicative, then so is $a * b$.

ii) If a is multiplicative, then so is the Dirichlet inverse a^{-1}.

iii) If $a * b = c$ and if a and c are multiplicative, then so is b.

iv) If a is multiplicative, then $a(b * c) = (a\,b) * (a\,c)$ for any functions b and c.

Remark. Note that the set of multiplicative arithmetic functions form a ring for which the operation of addition is the Dirichlet convolution and the operation of multiplication corresponds to point-wise multiplication. In other words, the statements of Theorems 2.2 - 2.4 are essentially some ring axioms. [12]

Also, we can now see that for $\mathcal{D}$ being the set of all formal Dirichlet series and $\mathcal{F}$ being the set of all arithmetic functions, $(\mathcal{D}; +; \cdot)$ is a commutative ring with identity. Furthermore we see that there is a ring homomorphism from arithmetic functions $(\mathcal{F}; +; *)$ to Dirichlet series $(\mathcal{D}; +; \cdot)$ as $f \mapsto D_f$ which satisfies $D_f \cdot D_g = D_{f*g}$.

A key result we need is the Möbius inversion formula.

Proposition 2.5. Let a be an arithmetic function. Define $b = a * \mathbf{1}$. Then $a = b * \mu$.

Remark. The result of this proposition is essentially stating that if

$$b(n) := \sum_{d|n} a(d),$$

then $a(n) = \sum_{d|n} b(d)\mu(\frac{n}{d})$.

Proof. A proof for the proposition, requires merely proving

$$\mathbf{1} * \mu = e, \tag{5}$$

which we have already done. Indeed, using (5) and remembering that the convolution is associative, we end up with

$$b * \mu = (a * \mathbf{1}) * \mu = a * (\mathbf{1} * \mu) = a * e = a.$$

Since both μ and $\mathbf{1}$ are multiplicative, their convolution must also be multiplicative. We know that e is a multiplicative function and per definition $e(1) = 1$

and $e(p^k) = 0$, p being prime and $k \in \mathbb{N}$. Therefore, $\sum_{d|1} \mu(d) = \mu(1) = 1$. And since a nonzero, multiplicative, arithmetic function depends only on the value of its prime powers, We need only to prove that $\sum_{d|p^k} \mu(d) = 0$, to complete the proof that $1 * \mu = e$. We write $\sum_{d|p^k} \mu(d) = \sum_{j=0}^{k} \mu(p^j) = \mu(1) + \mu(p) = 1 - 1 = 0$, and see that the proof is complete. □

Lemma 2.4. The arithmetic function $\sum_{d|n} \mu(d)$ is multiplicative.

Remark. This follows directly from Proposition 2.5, since $\mu * \mathbf{1} = e$. An alternative proof is given below.

Proof. Let n and m be positive integers such that $\gcd(m, n) = 1$. We have

$$\sum_{d_1|n} \mu(d_1) \sum_{d_2|m} \mu(d_2) = \sum_{d_1|n, d_2|m} \mu(d_1)\mu(d_2) = \sum_{d_1|n, d_2|m} \mu(d_1 d_2) = \sum_{d|n\cdot m} \mu(d).$$

The second equality follows from the fact that μ is multiplicative and the fact that if $\gcd(n, m) = 1$, $d_1 \mid n$ and $d_2 \mid m$, then $\gcd(d_1, d_2) = 1$, while the final equality follows from the fact that if $\gcd(n, m) = 1$ and $d \mid n \cdot m$, then d can be written as $d = d_1 d_2$ for a unique pair d_1, d_2 satisfying $d_1 \mid n$ and $d_2 \mid m$. □

Remark. Since $(a * \mathbf{1})(n) = \sum_{d|n} a(d)\mathbf{1}(\frac{n}{d}) = \sum_{d|n} a(d)$.

To finalize the proof of Lemma 2.1, we need another arithmetic function:

Definition 2.14 (Euler ϕ function)**.**

$$\phi(n) = \#\left\{k : 1 \le k \le n,\ \gcd(k, n) = 1\right\}.$$

That is, $\phi(n)$ counts the number of positive integers less than of equal to n which are relatively prime to n. For our calculation of $\lim_{n\to\infty} p_n$, we use a result that is a corollary of the following proposition.

Proposition 2.6. $\phi * \mathbf{1} = i$; In other words,

$$\sum_{d|n} \phi(d) = n.$$

Proof of proposition 2.6. Suppose $F(n) = \phi(n_1) + \phi(n_2) + \ldots + \phi(n_r)$, where n_i is a divisor of n. We have

$$\begin{aligned} F(p^k) &= \phi(1) + \phi(p) + \phi(p^2) + \ldots + \phi(p^k) \\ &= 1 + (p-1) + (p^2 - p) + \ldots + p^k - p^{k-1} \\ &= p^k. \end{aligned}$$

Since we can prime factor any number n, these terms are relative prime and the function F is multiplicative, we find

$$\begin{aligned} F(n) &= F(p_1^{k_1}) \cdot F(p_2^{k_2}) \cdots F(p_s^{k_s}) \\ &= p_1^{k_1} \cdots p_s^{k_s} \\ &= n. \end{aligned}$$

□

Proposition 2.6 and the Proposition 2.5, we derive the following corollary:

Corollary 2.6.1. $\mu * i = \phi$; that is,

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Remark. Ultimately, the proof of Theorem 2.1 and Lemma 2.1 makes use Corollary of 2.6.1 only, not Proposition 2.6.

Many arithmetic functions display disorganized behaviour when their values are plotted as functions of their arguments, and trying to find an "asymptotic formula" seems to be that straightforward a task. The Möbius function also falls into this category. Nevertheless, the functions do "behave" well when analyzing their arithmetic means $M_a(x) = (\frac{1}{x})\sum_{n\leq x} a(n)$. [2, Chapter 3] This gives us enough background to prove Lemma 2.1.

2.1.2 Proof of Lemma 2.1.

Proof of Lemma 2.1. Recall that $\phi(k)$ counts the amount of numbers relative prime to k. Therefore, for each $k \geq 2$, there are $\phi(k)$ integers j satisfying $1 \leq j < k$ and $\gcd(j,k) = 1$. Rewriting this in the form of Equation (1),

$$|A_n| = \#\left\{(j,k) \in \mathbb{Z}^2 : 1 \leq j < k \leq n,\ \gcd(j,k) = 1\right\} = \sum_{k=2}^{n} \phi(k).$$

From (1), we find

$$p_n = \frac{2\sum_{k=2}^{n}\phi(k)}{n(n-1)}. \tag{6}$$

We only need to analyze $\sum_{k=1}^{n}\phi(k)$ for large n to ultimately calculate

$$\lim_{n\to\infty} p_n = \lim_{n\to\infty} \frac{2\sum_{k=2}^{n}\phi(k)}{n(n-1)}. \tag{7}$$

Remark. We can also write the function ϕ in the quite familiar form:

$$\phi(n) = n\prod_{p|n}(1-\frac{1}{p}), \quad n \geq 2,\ p \text{ prime} \tag{8}$$

However, for analyzing $\sum_{k=1}^{n}\phi(k)$, we may not directly use (8).

To analyze $\sum_{k=1}^{n}\phi(k)$, we make use of Corollary 2.6.1. Recall that from Corollary 2.6.1, we can state

$$\begin{aligned}\sum_{k=1}^{n}\phi(k) &= \sum_{k=1}^{n}(\mu * i)(k) = \sum_{k=1}^{n}\sum_{d|k}\mu(d)\frac{k}{d} \\ &= \sum_{k=1}^{n}\sum_{d\cdot d'=k} d'\mu(d) = \sum_{d=1}^{n}\mu(d)\sum_{d'\leq\frac{n}{d}} d'.\end{aligned}$$

Since $\sum_{j=1}^{n} j = \frac{1}{2}n(n+1)$, we have

$$\sum_{k=1}^{n} \phi(k) = \sum_{d=1}^{n} \mu(d) \sum_{d' \leq \frac{n}{d}} d' = \frac{1}{2} \sum_{d=1}^{n} \mu(d)[\frac{n}{d}]([\frac{n}{d}]+1), \tag{9}$$

where $[a]$ indicates the greatest integer $\leq a$, i.e. the floor function. We know

$$\left[\frac{n}{d}\right]\left(\left[\frac{n}{d}\right]+1\right) \leq \frac{n}{d}(\frac{n}{d}+1) = (\frac{n}{d})^2 + \frac{n}{d};$$
$$\left[\frac{n}{d}\right]\left(\left[\frac{n}{d}\right]+1\right) \geq (\frac{n}{d}-1)\frac{n}{d} = (\frac{n}{d})^2 - \frac{n}{d}.$$

This combines into,

$$(\frac{n}{d})^2 - \frac{n}{d} \leq \left[\frac{n}{d}\right]\left(\left[\frac{n}{d}\right]+1\right) \leq (\frac{n}{d})^2 + \frac{n}{d}. \tag{10}$$

Substituting (10) in (9) gives us

$$\frac{n^2}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d^2} - \frac{n}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d} \leq \sum_{k=1}^{n}\phi(k) \leq \frac{n^2}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d^2} + \frac{n}{2}\sum_{d=1}^{n}\frac{\mu(d)}{d}. \tag{11}$$

Recall that $|\mu(d)| \leq 1$. We can say that $\sum_{d=2}^{n}\frac{1}{d}$ is a lower Riemann sum for $\int_1^n \frac{1}{x}dx$. This gives us

$$|\sum_{d=1}^{n}\frac{\mu(d)}{d}| \leq \sum_{d=1}^{n}\frac{1}{d} = 1 + \sum_{d=2}^{n}\frac{1}{d} \leq 1 + \log n. \tag{12}$$

Using (11) and (12), and taking the term $B_n = n(n-1)$ into account, we end up with

$$\lim_{n\to\infty}\frac{\sum_{k=2}^{n}\phi(k)}{n(n-1)} = \frac{1}{2}\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}. \tag{13}$$

We now need to find an expression for $\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}$. Initially, looking at the definition of μ, it would seem very difficult to evaluate this explicitly. Fortunately, a solution is provided by the Möbius inversion. Substituting $a = 1$, $b = \mu$ and $x = 2$ into Equations (2) - (4), we find that the right hand side of (2) and (3) is absolutely convergent. Recalling equation (5), we then find $\mathbf{1} * \mu = e$; In other words, $a * b = e$. Therefore, we end up with

$$\left(\sum_{d=1}^{\infty}\frac{1}{d^2}\right)\left(\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2}\right) = 1. \tag{14}$$

Equation (14) can be solved as follows. Recall:

$$\begin{aligned}\frac{\sin x}{x} &= 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \cdots \\ &= (1-\frac{x}{\pi})(1+\frac{x}{\pi})(1-\frac{x}{2\pi})(1+\frac{x}{2\pi})\cdots \\ &= (1-\frac{x^2}{\pi^2})(1-\frac{x^2}{4\pi^2})\cdots\end{aligned}$$

Multiplying these terms out, we end up with

$$-\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2},$$

for the coefficients of x^2. The original Taylor expansion of $\frac{\sin x}{x}$ tells us that the coefficient of $x^2 = -\frac{1}{3!} = -\frac{1}{6}$, which gives us the following equality:

$$-\frac{1}{6} = -\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}. \tag{15}$$

Using (15), we end up with:

$$\sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}. \tag{16}$$

From (14) and (16), we obtain

$$\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} = \frac{6}{\pi^2}. \tag{17}$$

Combining (17) with (13) and (7) gives

$$\lim_{n\to\infty} p_n = \frac{6}{\pi^2},$$

completing the proof of lemma. □

We are now in a position to prove Theorem 2.1

2.1.3 Proof of Theorem 2.1.

Proof of Theorem 2.1. As stated earlier, the Möbius function acts as the indicator function for square free values, we write

$$\mu^2(n) = \begin{cases} 1, & \text{if } n \text{ is square-free;} \\ 0, & \text{otherwise.} \end{cases} \tag{18}$$

We recall that

$$C_n = \{k \in \mathbb{Z} : 1 \leq k \leq n, k \text{ is square-free}\}.$$

Since a value of ± 1 for the Möbius function gives us a square-free, we have

$$|C_n| = \sum_{j=1}^{n}\mu^2(j). \tag{19}$$

To prove Theorem 2.1, we should find that

$$D = \lim_{n\to\infty}\frac{|C_n|}{n} = \frac{6}{\pi^2}. \tag{20}$$

Before we can go about finding that, we prove the following lemma.

Lemma 2.5. The indicator function of square-free values is $\mathbf{1}_{SF}(n)$, where

$$\mathbf{1}_{SF}(n) = \mu^2(n) = \sum_{k^2|n} \mu(k).$$

Proof. If n is a square-free value, then only integer k of which the square divides n, i.e. $k^2 \mid n$, is the integer $k = 1$ (per definition of square-free values). Since $\mu(1) = 1$, we end up with $\mu^2(n) = 1$. Now suppose n is not a square-free value. Since n can then be written in the form $n = d^2 l$, where $d > 1$ and l is a square-free value. Then $k^2 \mid m^2 l$ if and only if $k \mid d$. We write

$$\mu^2(n) = \sum_{k^2|n} \mu(k) = \sum_{k^2|d^2 l} \mu(k) = \sum_{k|d} \mu(k) = (\mu * 1)(d) = 0.$$

In the last equality we use Equation (5) and the fact that we stated that $d > 1$. The lemma now follows from (18). □

Lemma 2.5 then gives us,

$$\sum_{j=1}^{n} \mu^2(j) = \sum_{j=1}^{n} \sum_{k^2|j} \mu(k). \tag{21}$$

Before we go any further, we recall the *Inclusion-exclusion principle*.

Definition 2.15 (Inclusion-exclusion principle)**.** For finite sets $A_1, A_2, \ldots, A_n$, one has the identity

$$\bigcup_{i=1}^{n} A_i = \sum_{k=1}^{n} (-1)^{k+1} \left(\sum_{1 \le i_1 \le \cdots \le i_k \le n} |A_{i_1} \cap \ldots \cap A_{i_k}| \right). \tag{22}$$

Remark. The Inclusion-exclusion principle in this example essentially states that if we want the number of values $N_{a_2,\ldots,a_n}$ with a_i meaning $i^2 \nmid f(n)$, this equals $N - \sum_{i=2}^{n} N_{a_i'} + \sum_{2 \le i < j \le n}^{n} N_{a_i', a_j'} - \ldots$ We define a_i' being not a_i.

We now attempt to evaluate (21). If $k^2 > n$, then in (21) there is no value of k such that $k^2 \mid j$. If $k^2 \le n$, then there are $\lceil \frac{n}{k^2} \rceil$ values of k such that $k^2 \mid j$, times, namely, when $j = k^2, 2k^2, \ldots, \lceil \frac{n}{k^2} \rceil k^2$. We can then rewrite (21):

$$\begin{aligned} \sum_{j=1}^{n} \mu^2(j) = \sum_{j=1}^{n} \sum_{k^2|j} \mu(k) = \sum_{k^2 \le n} \lceil \frac{n}{k^2} \rceil \mu(k) = \sum_{k \le \lceil n^{\frac{1}{2}} \rceil} \lceil \frac{n}{k^2} \rceil \mu(k) \\ = n \sum_{k \le \lceil n^{\frac{1}{2}} \rceil} \frac{\mu(k)}{k^2} + \sum_{k \le \lceil n^{\frac{1}{2}} \rceil} \left(\lceil \frac{n}{k^2} \rceil - \frac{n}{k^2} \right) \mu(k). \end{aligned} \tag{23}$$

Since both $\left| \left(\lceil \frac{n}{k^2} \rceil - \frac{n}{k^2} \right) \right|$ and $|\mu(k)|$ in the right hand side of (23) are bounded by 1, we find

$$\left| \sum_{k \le \lceil n^{\frac{1}{2}} \rceil} \left(\lceil \frac{n}{k^2} \rceil - \frac{n}{k^2} \right) \mu(k) \right| \le n^{\frac{1}{2}}. \tag{24}$$

Combining equations (19), (23) and (24), we end up with

$$D = \lim_{n\to\infty} \frac{|C_n|}{n} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2}.$$

Using this with (17) gives (20) and completes the theorem.

Remark. When proving the number of square-free values of *any* function $f \in \mathbb{Z}[x]$ with degree 1 (and not just $f(x) = x$), we follow a similar route, interchanging j and $aj + b$. We would then solve:

$$\sum_{j=0}^{k} \mu^2(aj + b) = \sum_{j=0}^{n} \sum_{k^2|aj+b} \mu(k).$$

An interesting discussion on the matter can be found in the article by Hooley [18]. This states that if $S(x; a, k)$ is the number of square-free integers below x that are congruent to a mod k, then

$$S(x; a, k) \sim \frac{6x}{p^2 k} \prod_{p|k} \left(1 - \frac{1}{p^2}\right)^{-1} \quad (x \to \infty),$$

only if $\gcd(a, k) = 1$ and $k \leq x^{2/3-\epsilon}$.

□

2.2 Polynomials of degree 2[34].

We now focus on polynomials of degree 2. Let's assume that $f \in \mathbb{Z}[x]$ is a square-free polynomial, as defined in Definition 2.3.

Question 3. Can we again say something about the density c_f of square-free values in these polynomials?

Theorem 2.7 (Chinese Remainder Theorem)**.** *Let m and n be relative prime positive integers. For any integers a and b, the pair of congruences*

$$x \equiv a \bmod m, \quad x \equiv b \bmod n,$$

has a solution, and this solution is uniquely determined modulo mn.

In the following argumentation, we use the fact that $d \mapsto \rho(d)$ (Definition 2.4) is a multiplicative function, this is due to the Chinese Remainder Theorem[10].

For quadratic equations, the problem (which is essentially proving Conjecture 2.1) becomes more difficult. It was Erdös who established that if f is a square-free polynomial that has a degree ≤ 3, then there are infinitely many integers n for which $f(n)$ is square-free [13]. Estermann focused specifically on polynomials of the form $f(x) = x^2 + k$ and found an expression for the positive density of these polynomials [14]. However, beyond that astonishingly little is known unequivocally for irreducible f. For example, for polynomials of the form $a^4 + 2$ the infinitude of square free values, let alone the actual density, is still an open problem. A problem to which a solution has been found is how

often the value of an irreducible polynomial $f \in Z[x]$ of degree n is free of $(n-1)-$th powers, either when evaluated at integers or at primes, see [29]. Also, the general quadratic case was solved by Ricci [31]. We first take a look at some examples of local densities of the quadratic case, after which we discuss the general case.

2.2.1 Example 1.

Lemma 2.6. For $f \in \mathbb{Z}[x], f(x) = x(x+1)$, we have that for all primes p, and $k \geq 1$, $\rho_f(p^k) = 2$.

Proof. Recall $\rho(p^k)$ is defined as the amount of values a for which $p^k \mid a(a+1)$. Say p is prime and note that $\gcd(a, a+1) = 1$. Then for $p^k \mid a(a+1)$, since a and $a+1$ are coprime, it must mean that $p^k \mid a$ or $p^k \mid a+1$. Both of which contribute a solution. We end up with $\rho_f(p^k) = 2$. □

This result then gives us the density of square-free values for $f(x)$,

$$c_f = \prod_p \left(1 - \frac{\rho_f(p^2)}{p^2}\right) = \prod_p \left(1 - \frac{2}{p^2}\right).$$

2.2.2 Example 2.

Lemma 2.7. For $f \in \mathbb{Z}[x], f(x) = x^2 + 1$, we differentiate between three situations:

i) For $p \neq 2$, we have $\rho_f(p^k) = \rho_f(p)$ for all $k \geq 1$.

ii) For $p \neq 2$, there are two options:

$$\rho_f(p) = \begin{cases} 2, & p = 1 \bmod 4, \\ 0, & p = 3 \bmod 4. \end{cases}$$

iii) For $p^k = 4$, we have $\rho_f(4) = 0$.

Proof. Part (i) is a result from Hensel's Lemma. Part (ii) is a result from Fermat, that states every prime $p > 2$ can be written as $p = x^2 + y^2, (x, y) \in \mathbb{Z}^2$ if and only if $p \equiv 1 \bmod 4$[7]. Here we than try to answer the question when $x^2 \equiv -1 \bmod p$. Part (iii) is a result that follows from a direct computation. □

This result then gives us the density of square-free values for $f(x)$,

$$c_f = \prod_p \left(1 - \frac{\rho_f(p^2)}{p^2}\right) = \prod_{p \neq 2} \left(1 - \frac{1 - \left(\frac{-1}{p}\right)}{p^2}\right) = 0.894\ldots$$

2.2.3 General quadratic case.

In this section, we discuss the general quadratic polynomials. We do so by treating the easier cases also found in examples above and generalizing in the end of this section. For $n \in \mathbb{N}$, we recall

$$\mathcal{N}_f(n) := \{k \in \mathbb{N}, k \leq n : f(n) \text{ square-free}\}.$$

Theorem 2.8. *Suppose* $f(x) = x(x+1)$ *or* $f(x) = x^2+1$. *Then*

$$\#\mathcal{N}_f(n) = c_f n + O(n^{2/3}\log(n)), \quad \text{as } n \to \infty,$$

with $c_{x(x+1)} = \prod_p \left(1 - \frac{2}{p^2}\right)$ *and* $c_{x^2+1} = \prod_{p\neq 2}\left(1 - \frac{1+\frac{-1}{p}}{p^2}\right) = 0.894\ldots$.

Remark. Note that for $f(x) = x(x+1)$, we find $c_{x(x+1)} = \prod_p \left(1 - \frac{2}{p^2}\right)$. Furthermore, we know that since n and $n+1$ are coprime, our function $f(n) = n(n+1)$ is square-free if and only if both n and $n+1$ are square-free. Interestingly, we end up with a value that is smaller than the product of independently finding n and $n+1$ being square-free (see Theorem 2.1): $\frac{1}{\zeta(2)^2} = \prod_p \left(1 - \frac{2}{p^2} + \frac{1}{p^4}\right)$. We can therefore conclude that for $f(x) = x(x+1)$, the density of square-free values of n and $n+1$ cannot be considered as independent events.

2.2.4 General outline of the proof.

In this section, we describe in general terms what strategy is used to prove the Theorem. We make use of the sieve of Eratosthenes and Legendre. Recall, according to Lemma 2.5, that the indicator function of the square-free values is $\mathbf{1}_{SF}(n) = \sum_{k^2|n}\mu(k)$. Hence,

$$\#\mathcal{N}_f(n) = \sum_{a\leq n}\mathbf{1}_{SF}(f(a)) = \sum_{a\leq n}\sum_{k^2|f(a)}\mu(k) = \sum_{k\leq n}\mu(k)\#\{a\leq n : k^2 \mid f(a)\}. \tag{25}$$

Remark. Equation (25) is in effect the inclusion-exclusion principle. For $k=1$, we have $\mu(1) = 1$ all thus all n integers are added to the sum. We then subtract all values of a for which $f(a)$ can be divided by a prime, then add all values of a for which $f(a)$ can be divided by the distinct product of two primes, and so on. Note that we can constrain $k \ll n$ because k^2 divides the quadratic polynomial $f(a)$, which is $\ll n^2$ if $a \leq n$.

We introduce a value u (which ultimately is set to be $n^{1/3}$) and split the sum into two parts. The first part is the sum $\#\mathcal{N}'_f(n)$ which covers the "small" divisors $k \leq u$. The second part is the sum $\#\mathcal{N}''_f(n)$ which covers the "large" divisors $u < k \leq n$:

$$\begin{aligned}
\#\mathcal{N}_f(n) &= \#\mathcal{N}'_f(n) + \#\mathcal{N}''_f(n),\\
\#\mathcal{N}'_f(n) &= \sum_{k\leq u}\mu(k)\#\{a\leq n : k^2 \mid f(a)\},\\
\#\mathcal{N}''_f(n) &= \sum_{u<k\leq n}\mu(k)\#\{a\leq n : k^2 \mid f(a)\}.
\end{aligned}$$

Remark. We assume $a \in \mathbb{N}$. In the following, a is always a positive integer.

Our goal is to find a bound for $\#\mathcal{N}(n)$. To do so, we first find a bound for $\#\mathcal{N}'(n)$, specifically

$$\#\mathcal{N}'_f(n) = c_f n + O\left(\frac{n}{u}\log u + u\log u\right). \tag{26}$$

We then find a bound for $\#\mathcal{N}''(n)$, specifically

$$\#\mathcal{N}''_f(n) \ll \frac{n^2}{u^2}. \tag{27}$$

Substituting, as mentioned before, $u = n^{1/3}$, we end up with the correct result from Theorem 2.8:

$$\#\mathcal{N}_f(n) = c_f n + O(n^{2/3} \log n),$$

2.2.5 Bound for $\#\mathcal{N}'(n)$, the small divisors.

We find a bound for $\#\mathcal{N}'_f(n)$ (the main term) by using inclusion-exclusion. Recall

$$\#\mathcal{N}'_f(n) = \sum_{k \le u} \mu(k) \#\{a \le n : k^2 \mid f(a)\}.$$

To find a solution to the sum above, we again split the terms on the right hand side, and first find a different expression for $\#\{a \le n : k \mid f(a)\}$.

Lemma 2.8.

$$\#\{a \le n : k \mid f(a)\} = \frac{n\rho_f(k)}{k} + O\left(\rho_f(k)\right).$$

Proof. We rewrite

$$\#\{a \le n : k \mid f(a)\} = \sum_{\substack{c \bmod k: \\ k \mid f(c)}} \#\{a \le n : a = c \bmod k\}.$$

However, we know that

$$\#\{a \le n : a = c \bmod k\} = \frac{n}{k} + O(1).$$

This then gives us

$$\begin{aligned} \#\{a \le n : k \mid f(a)\} &= \sum_{\substack{c \bmod k: \\ k \mid f(c)}} \frac{n}{k} + O(1) \\ &= \frac{n\rho_f(k)}{k} + O\left(\rho_f(k)\right). \end{aligned} \tag{28}$$

□

Substituting Equation (28) back into our starting term gives us

$$\begin{aligned} N'_f(n) &= \sum_{k \le u} \mu(k) \left(\frac{n\rho_f(k^2)}{k^2} + O(\rho_f(k^2)) \right) \\ &= n \sum_{k \le u} \frac{\mu(k)\rho_f(k^2)}{k^2} + O\left(\sum_{k \le u} |\mu(k)| \rho_f(k^2) \right). \end{aligned} \tag{29}$$

We again decompose the sum

$$\sum_{k \le u} \frac{\mu(k)\rho_f(k^2)}{k^2} = \sum_{k=1}^{\infty} \frac{\mu(k)\rho_f(k^2)}{k^2} + O\left(\sum_{k > u} \frac{\mu(k)\rho_f(k^2)}{k^2} \right).$$

For the final step, we use that fact that both ρ_f and of μ are multiplicative (Lemma 2.2):

$$\sum_{k=1}^{\infty} \frac{\mu(k)\rho_f(k^2)}{k^2} = \prod_p \left(1 - \frac{\rho_f(p^2)}{p^2}\right) = c_f.$$

We now need to find a bound for the error term. Recall that in Lemma's 2.6 and 2.7, we stated that $\rho_f(p^2) \leq 2$, for p prime, and thus for k square-free

$$\rho_f(k^2) = \prod_{p|k} \rho_f(p^2) \leq \prod_{p|k} 2 = \sigma(k).$$

Note that σ in the above expression is the divisor function. We can now bound the error term by

$$\sum_{k>u} \frac{|\mu(k)|\rho_f(k^2)}{k^2} \leq \sum_{k>u} \frac{\sigma(k)}{k^2} \ll \frac{\log u}{u}.$$

Furthermore, for the error term in (29), we can find a bound by saying

$$\sum_{k\leq u} |\mu(k)|\rho_f(k^2) \leq \sum_{k\leq u} \sigma(k) \sim u \log u.$$

Since $\sum_{a\leq x} \sigma(a) = x(\log x + C) + O(x^{1/2})$, we have

$$\sum_{a>u} \frac{\sigma(a)}{a^2} = \frac{\log u + C + 2}{u} + O\left(\frac{1}{u^{3/2}}\right) \text{[35]}.$$

Combining the bounds, we end up with

$$\#\mathcal{N}'_f(n) = c_f n + O\left(\frac{n}{u}\log u\right) + O(u \log u),$$

which is exactly our term in Equation 26.

2.2.6 Bound for $\#\mathcal{N}''_f(n)$, the large divisors.

Suppose we rewrite $k^2 \mid f(a)$ as stating $f(a) = k^2 m$ for some integer $m \geq 1$. Then

$$\#\mathcal{N}''_f(n) = \sum_{a\leq n} \sum_{\substack{k^2|f(a),\\ k>u}} \mu(k) \leq \sum_{k>u} \#\{a \leq n : f(a) = k^2 m\}.$$

Instead of summing over values where $k > u$, we now sum over values m. If $k > u$ then $m = f(a)/k^2 \leq n^2/u^2$. If we neglect the bound on the size of k and the assumption that k is square-free, we have:

$$\#\mathcal{N}''_f(n) \leq \sum_{1\leq m\leq n^2/u^2} \frac{n^2}{u^2} \#\{(r,t) \in \mathbb{Z}^2 \text{ and } r,t \leq n : f(r) = t^2 m\}.$$

Remark. Note that we find a bound for $\#\mathcal{N}''_f(n)$ by switching the roles of k and m, such that, again, we have a bounded sum $\sum_{1\leq m\leq n^2/u^2}$ instead of an unbounded one $\sum_{k>u}$.

Suppose we look at the irreducible polynomial $f(x) = x^2 + 1$. Then the equation $f(r) = Dt^2$ becomes

$$r^2 - Dt^2 = -1.$$

This equation is also know as a (generalized, or negative) Pellian equation.

To find a bound to the amount of different solutions to this equation, given the limitations on the values r, t, we define the following:

$$S_m(n) := \#\{(r,t) \in \mathbb{Z}^2 \quad r,t \leq n : r^2 - mt^2 = -1\}.$$

Proposition 2.9. Suppose $1 < m < n$ is not a square of some other integer. Then

$$S_m(n) \ll \frac{\log n}{\log m}.$$

For the case that m is a square, there are no solutions of $r^2 - mt^2 = -1$ if $m > 1$. On the other hand, for the case that $m = 1$ there are two solutions.

Proof. Let $m > 1$ be no square of some other integer. Using the fact that we consider a Pell's equation, we know that if the equation $r^2 - mt^2 = -1$ can be solved by integers (r, t), all these solutions are of the form $r + \sqrt{m}t = \pm\epsilon_m^{2a+1}$, $a \in \mathbb{Z}$. The solution of this equation is $\epsilon_m = r_1 + t_1\sqrt{m}$, with $r_1, t_1 \geq 1$. We can therefore say that if $1 \leq r, t \leq n$ then $r + t\sqrt{m} = \epsilon_m^{2a+1}$ for some $a \geq 0$. Rewriting this yields

$$0 \leq a \leq \frac{\log r + \sqrt{m}t}{2\log \epsilon_m} = \frac{\log r + \sqrt{r^2+1}}{2\log \epsilon_m} \leq \frac{\log n}{\log \epsilon_m}.$$

Because $\epsilon_m = r_1 + t_1\sqrt{m} \geq \sqrt{m}$, we find a bound

$$S_m(n) \ll \frac{\log n}{\log m}.$$

If $m = C^2$ is a square, the equation $r^2 - Ct^2 = -1$ is rewritten into $r^2 - (Ct)^2 = -1$ or $(Ct - r)(Ct + r) = 1$. The solutions to this equation are $Ct - r = Ct + r = \pm 1$, which leaves us with $r = 0$. Finally, $C^2t^2 = 1$ is solvable only for $C = 1$ in which case there are two solutions. □

Inserting Proposition 2.9 into the bound of $\#\mathcal{N}_f''$ gives

$$\#\mathcal{N}_f'' \ll \sum_{1 \leq m < n^2/u^2} S_m(n) \ll 1 + \sum_{1 < m < n^2/u^2} \frac{\log n}{\log m} \ll \frac{n^2}{u^2},$$

as claimed, on using

$$\sum_{1 < m < y} \frac{1}{\log m} \ll \int_2^y \frac{1}{\log x} dx \sim \frac{y}{\log y}.$$

2.2.7 General case of quadratic polynomials.

For general quadratic polynomials of the form $f(x) = a_1x^2 + a_2x + a_3 \in \mathbb{Z}[x]$, for instance our example $f(x) = x(x+1)$. The only alteration that needs doing is to rewrite the equation $f(r) = mt^2$. Say we multiply the equation by $4a_1$ and factor a different term squared, we have

$$4a_1mt^2 = (2a_1r + a_2)^2 - \Delta_f,$$

Note that $\Delta_f = a_2^2 - 4a_1a_3$ is the discriminant of f, which is nonzero if and only if f has repeated roots. Equation $f(r) = mt^2$ is then rewritten into

$$(2a_1r + a_2)^2 - a_1m(2t)^2 = \Delta_f.$$

This leaves us with bounding the amount of solutions of

$$R^2 - (a_1m)T^2 = \Delta_f,$$

with $R, T \ll n$.

Remark. In the example $f(x) = x(x+1)$ we get $\Delta = +1$ and the equation becomes $R^2 - mT^2 = 1$, to which we apply a version of Proposition 2.9.

For polynomials of degree ≥ 3, this strategy of using the Sieve of Eratosthenes does not work as efficient. This is due to "large" primes p with p^2 dividing $f(n)$. In the quadratic case when p^2 divides $f(n)$, then p can be at most $O(n)$. However, in the cubic case, p can be considerably larger. This is where the strategy fails. Note that for polynomials of degree 3, a solution to this problem can be found without using the *ABC Conjecture*, but for polynomials of degree ≥ 4, this conjecture is necessary.

2.2.8 The ABC Conjecture.

Definition 2.16 (The ABC-Conjecture)**.** Granville proved that assuming the ABC Conjecture is correct, provides a closing proof for Conjecture 2.1. An interesting discussion on the matter is set out in his article [17]. Firstly, we introduce the radical of an integer N being the product of the primes dividing that integer: $\text{rad}(N) := \prod_{p|N} p$. Now, the ABC Conjecture states that for every $\epsilon > 0$, there exists a finite amount of coprime triples $(a, b, c) \in \mathbb{N}^3$, with $a+b = c$, such that

$$c > \text{rad}(abc)^{1+\epsilon}.$$

In other words, for every $\epsilon > 0$, there exists a constant K_ϵ such that for all coprime triples $(a, b, c) \in \mathbb{Z}^3$ with $a + b = c$ we have

$$c < K_\epsilon \cdot \text{rad}(abc)^{1+\epsilon}.$$

However, the ABC-conjecture has yet to be proven. Recently, some claims were made that such a proof had been found by the Japanese mathematician Shinichi Mochizuki. However, this theory makes use of an entirely new field of Mathematics which is not yet fully understood. Therefore, at this time the proof can neither be confirmed nor disproved [3].

2.2.9 Square-free integers in short intervals.

This density problem can also be translated to finding the density of square-free integers in short intervals, i.e. sets of the form $I(n,H) = \{a \in \mathbb{Z} : n \leq a < n+H\}$ where H is much smaller that n. When averaging over all n, we expect the density to be the same as that over all integers — in the case of the polynomial $f(x) = x$, where $c_f = \frac{1}{\zeta(2)}$. We would like to know how small we can take $H(n)$ such that the density is precise (up to smaller order deviations) for all n, and not just on average or almost all n. One motivation for this is that this might provide more insight in the finer distribution of square-free values.

Conjecture 2.2. Let $\epsilon > 0$ be fixed, let n be large, and let $H \gg n^{\epsilon}$. Then

$$\#\{a \in I(n,H) : a \text{ is square-free}\} = \frac{H}{\zeta(2)} + o\left(\frac{H}{\zeta(2)}\right).$$

This Conjecture follows from the ABC Conjecture by Granville's method [6, Appendix]. Granville [17] showed that asumming the ABC Conjecture is correct is essentially stating that for some fixed $\epsilon > 0$, there must be square-free integers in the interval $I(n, n^{\epsilon})$ for all large n. The most accurate result so far was found by Tolev [36], who proved the asymptotic for any $H(n)$ such that $\frac{H(n)}{n^{1/5}\log n} \to \infty$. Now, this question can also be translated to square-free values of polynomials instead of integers.

Question 4. Let $f \in \mathbb{Z}[x]$ be a square-free polynomial with $c_f > 0$. How small may we take $H(n)$ such that the asymptotic

$$\#\{a \in I(n,H) : f(a) \text{ is square-free}\} \sim c_f H,$$

holds for all n?

3 Square-free values of Polynomials over Function Fields.

Our goal in this section is to analyze some of the ideas of the sieve of Eratosthenes and Legendre in the context of the ring $\mathbb{F}_q[t]$ of polynomials over a finite field $\mathbb{F}_q$. Again we focus specifically on the questions on square-free values of polynomials and try to make a comparison with the ring of integers.

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ *and the ring of integers* $\mathbb{Z}$.
Note that some of the notation used here is defined later. We choose to cover some basic concepts here anyway since it does provide some intuition on the similarities. First, the most obvious analogies are the following:

i) The size of an integer (or the log of the size of the integer) compares to the degree of a polynomial. For instance, for $a, b \in \mathbb{Z}\backslash\{0\}$ we have

$$\log(|ab|) = \log(|a|) + \log(|b|),$$

and for any two polynomials f, g in $\mathbb{F}_q[t]$, we have

$$\deg(fg) = \deg(f) + \deg(g).$$

ii) Now in $\mathbb{F}_q[x]$, we would also like a way to measure the "size" of a monic polynomial of degree r. A natural such measure would be the following:

Definition 3.1. The norm or absolute value of a polynomial f of degree n in $\mathbb{F}_q[x]$ is defined as:

$$|f| := \#\frac{\mathbb{F}_q[t]}{(f)} = q^{\deg f} = q^n,$$

the number of residue classes modulo f and depends only on the degree of f.

So the Euclidean domain analogy is as follows:

$$|a| := \#\frac{\mathbb{Z}}{(a)} = \#\frac{\mathbb{Z}}{a\mathbb{Z}}, \quad \text{for } a \neq 0.$$

Note that whereas only one positive integer n has absolute value n, there are q^n monic polynomials of degree n over $\mathbb{F}_q$ with absolute value q^n.

iii) The Euclidean Algorithm also holds for polynomials. Suppose $a(x), b(x) \in \mathbb{F}_q[x]$ and $a(x), b(x) \neq 0$, then there are $q(x), r(x) \in \mathbb{F}_q[x]$ such that

$$a(x) = b(x)q(x) + r(x)$$

. Here it must hold that $r(x)$ is either 0 (in which case $b(x) \mid a(x)$ or $\deg r(x) < \deg b(x)$. Note that while the gcd of both polynomials and integers determine an element up to a *unit* of, respectively, $\mathbb{R}[x]$ (=non zero element of deg 0) and $\mathbb{Z}$, this means that the gcd of *polynomials* 2 and 4 is 1, whereas the gcd of *integers* 2 and 4 is 2.

3.1 The polynomial ring over a finite field.

Definition 3.2 (Ring)**.** A ring is a set R with two binary operations $+$ and $\cdot$ such that

i) $(R, +)$ is a commutative group;

ii) The operation $\cdot$ is associative, and there exists an element 1_R such that $a \cdot 1_R = a = 1_R \cdot a$, for all $a \in R$;

iii) the distributive law holds for both operations. That is, for any two elements $a, b \in R$, $a(b + c) = ab + ac$.

Remark. Not every ring R has to be commutative under the operation $\cdot$. If this is the case, we call R a *commutative ring.* If R has the multiplicative identity, we call R a *ring identity.*

Definition 3.3 (Zero-divisors)**.** If a, b are two ring elements with $a, b \neq 0$ but $ab = 0$ then a and b are called *zero-divisors.*

Remark. We see that the ring of all integers $\mathbb{Z}$ has no zero divisors, whereas a random integer ring $\mathbb{Z}_n$ (note that in this thesis, by $\mathbb{Z}_n$ we mean $\mathbb{Z}/n\mathbb{Z}$) or polynomial ring can have zero divisors. And example is the numbers 2 and 3 in the ring $\mathbb{Z}_6$. We have $2 \cdot 3 \equiv 0 \bmod 6$ and thus 2 and 3 are zero-divisors. More generally, the instead of every ring $\mathbb{Z}_n$ contains zero-divisors if and only if n is not prime.[23, Chapter 3]

Definition 3.4 (Integral domain)**.** An *integral domain* is a commutative ring with an identity with no zero-divisors.

Definition 3.5 (Field)**.** A field is a set F with two composition laws $+$ and $\cdot$ such that

i) All elements of F form an commutative group with operation $+$ and identity 0;

ii) All elements of $F\backslash\{0\}$ form a commutative group with operation $\times$ and identity 1;

iii) The distributive law holds.

Remark. Note that a field is therefore a commutative ring with identity in which every non-zero element has a multiplicative inverse. Every field is an integral domain but some integral domains are not fields. The example $\mathbb{Z}$ is not a field, since it does not have a multiplicative inverse. E.g. for an element $a \in \mathbb{Z}$, there need not be an element $a^{-1} \in \mathbb{Z}$ such that $a \cdot a^{-1} = 1$. However, every *finite* integral domain *is* a field. [5]

Definition 3.6 (Ideal)**.** An *(two-sided) ideal* I is a special kind of subset $I \subset R$ such that:

$$\forall b, a \in I, r \in R : a - b, ar, ra \in I.$$

Remark. A few remarks can be made about ideals

i) If R is a commutative ring and $S \subset R$, then the ideal generated by S is defined as follows:

$$\langle S \rangle = \{r_1 s_1 + r_2 s_2 + \ldots + r_k s_k \in R | r_i \in R, s_i \in S, i \in \{1, \ldots k\} \subset \mathbb{N}\}.$$

ii) If S has only one element s, this is called the *principal ideal generated by* s. For example, the ideal $2\mathbb{Z}(= \{0, 2, 4, \ldots\})$ of $\mathbb{Z}$ is the principal ideal $\langle 2 \rangle$.

iii) Every ideal of $\mathbb{Z}$ is principal (the proof makes use of the Euclidean Algorithm). Making the comparison between $\mathbb{Z}$ and $\mathbb{F}_q[t]$, we have

$$I = (a) \leftrightarrow I = ((f(x)),$$

where $a \neq 0, |a|$ minimum and $f \neq 0, |f| = q^{\deg f}$ minimum, so $\deg f$ minimum.

iv) A commutative ring R is called a *principal ideal domain* (*PID*) if

- $I \subset R$ is any ideal, then $I = (x)$ for some $x \in R$. (Let $(x_1, \ldots, x_n) \subset R$ denote the ideal generated by $x_1, \ldots, x_n$, explicitly $a_1 x_1 + \cdots + a_n x_n$ for all $a_i \in R$.
- The only zero divisor in R is 0.
- The word domain means there are no non-zero zero divisors. Sometimes you'll hear the term integral domain, which means a commutative ring with no non-zero zero divisors. The "principal ideal" part of the term means that every ideal is "principal"— i.e., generated by one element.

Remark. Therefore, also for $\mathbb{R}[x]$ it holds that every ideal is principal. In general, if F is a field, then any ideal $I \subset F[t]$ is generated by a single element.[5]

Definition 3.7 (Quotient-ring of ideal)**.** If I is an ideal of ring R, the set R/I is a ring under operations

i) $(a + I) + (b + I) = (a + b) + I$;

ii) $(a + I) \cdot (b + I) = ab + I$.

Remark. In words; R/I is the ring R in which all elements in the ideal I have been made 0. Take for example the ring

$$\frac{\mathbb{Z}_5[x]}{\langle x^2 + 1\rangle}.$$

This ring has 25 elements of the form $ax+b$ where $a, b \in \{0, 1, \ldots, 4\}$. However, it is not a field since $x^2 + 1$ can be factored in a product of lower degree polynomials in $\mathbb{Z}_5[x]$. Therefore $x^2+1 \equiv (x+3)(x+2) \bmod x^2+1 \equiv 0 \bmod x^2+1$ and we see that it has zero-divisors.

Lemma 3.1 (Unique factorization for principal ideal domains)**.** Let R be a PID. Then for any non-zero element $x \in R$, there exists a finite collection of distinct prime elements $p_1, \ldots, p_k$ so that $x = p_1^{n_1} \ldots p_k^{n_k}, \quad n_i \geq 1$ and so that no p_i is a unit multiple of p_j for $i \neq j$. Then the n_i are unique and the p_i are unique up to multiplication by units and reordering.[23]

Dictionary between the polynomial ring $\mathbb{F}_q$[x] *and the ring of integers* $\mathbb{Z}$*.*
The basic idea in any unique factorization domain is that there are certain (non-unit) elements, called *irreducible elements*, or in the case of $\mathbb{Z}$, *primes*, which form the "multiplicative building blocks" for the ring. So the Fundamental Theorem of Arithmetic holds for both rings:

- For $\mathbb{Z}$ recall that a prime element of R is simply a prime number or a negative of a prime number. Thus the theorem is saying that any integer $x \in \mathbb{Z}$ can be written as a product of powers of primes. The choice of p_i is only unique up to multiplying by units.
- For $\mathbb{F}_q[t]$ this is saying that every polynomial can be written as a product of a unit and irreducible polynomials p_i. We recall that the units of a field $\mathbb{F}_q$ are the non-zero elements of $\mathbb{F}_q$, i.e. the non-zero constant polynomials.

We consider two types of finite (Galois) fields $\mathbb{F}_{p^m}$. Suppose p prime, then either $m = 1$ (prime fields) or $m > 1$ (extension fields).

i) Prime Fields ($m = 1$). The elements of $\mathbb{F}_p$ are integers $\{0, 1, \ldots, p-1\}$. A different notation of this field is $\frac{\mathbb{Z}}{p\mathbb{Z}}$. Addition, subtraction and multiplication is all dealt with using modular reduction prime p. Inversion of $a \in \mathbb{F}_{p^1}$, denoted a^{-1} must satisfy $a \cdot a^{-1} = 1 \bmod p$, and can be computed using the Extended Euclidean Algorithm.

ii) Extension Fields ($m > 1$). To construct $\mathbb{F}_{p^m}$, we take an irreducible polynomial $P(x)$ of $\deg m$ with coefficient in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ and then define: $\mathbb{F}_{p^m} := \frac{\frac{\mathbb{Z}}{p\mathbb{Z}}[X]}{\langle P(X)\rangle}$. We can also define it as the field generated by the roots of $X^{p^m} - 1$

inside the algebraic closure of $\frac{\mathbb{Z}}{p\mathbb{Z}}$. The elements (residue classes) of $\mathbb{F}_{p^m}$ are polynomials $a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 = A(x)$, where $a_i \in \mathbb{F}_p$. Addition and subtraction of two elements $A(x), B(x) \in \mathbb{F}_{p^m}$ is done in the regular way, making sure the coefficients are again in $\mathbb{F}_p$. For multiplication, we use regular multiplication with modular reduction with an irreducible polynomial $P(x) \in \mathbb{F}_{p^m}$ — that is, a polynomial that cannot be factored into the product of two non-constant polynomials.

Lemma 3.2. Let p be a prime and $f(x)$ an irreducible polynomial of degree k in $\mathbb{Z}_p[x]$. Then $\frac{\mathbb{Z}_p[x]}{\langle f(x)\rangle}$ is a field with p^k elements. [11]

Remark. Note that some polynomials are irreducible in $\mathbb{R}[x]$ while they are reducible in $\mathbb{Z}_p[x]$. For example $x^2 + 1$ in $\mathbb{Z}_5[x]$. More generally, $x^2 + 1$ is irreducible in $\mathbb{Z}_p$ if and only if $p = 4k + 3, k \in \mathbb{Z}$ (see also part (ii) of the proof in Section 2.2.2.)

3.2 Basics for Function Field analogue of Conjecture 2.1.

When analyzing the proof for the function field analogue of Conjecture 2.1, we use the following notation. Suppose $\mathbb{F}_q$ is a finite field of q elements, and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$ where:

i) The units of $\mathbb{F}_q[t]$ are the scalars $\mathbb{F}_q^\times$ (being the multiplicative group of a field $(\mathbb{F}_q \backslash \{0\}, \cdot)$). Recall Lemma 3.1: Any nonzero polynomial may be uniquely written as the product of a unit and an element $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ — a *monic* polynomial.

ii) In further calculations, by M_n we mean the set of monic polynomials of degree n. We recall that every a_i must be an element in $\mathbb{F}_q$ and that $\mathbb{F}_q$ has q elements. Therefore, the cardinality of M_n is

$$\#M_n = q^n.$$

iii) The ring $\mathbb{F}_q[t]$ is a Euclidean ring, so the Euclidean Algorithm holds (see the beginning of Section 3)

Similar to considering integers over $\mathbb{Z}$, if an irreducible $A \in \mathbb{F}_q[t]$ divides, for $B, C \in \mathbb{F}_q[t]$, two other elements $A \mid BC$, then either $A \mid B$ or $A \mid C$.

Suppose we want to determine the amount of monic polynomials in an arithmetic progression. Recall that over the integers, this would be done by counting the number of integers $a \in \mathbb{N}, a \leq n$ such that $a = c \bmod k$. As seen in Section 2.1, the answer is $\lceil \frac{n}{k} \rceil = \frac{n}{|k|} + O(1)$. So we're looking at integers which are equivalent mod d. The analogues statement for $\mathbb{F}_q[t]$, where we are looking at the number of monic polynomials which are equivalent mod K, is

Lemma 3.3. Suppose we have a monic polynomial $K \neq 0, K \in \mathbb{F}_q[t]$, and $C \in \mathbb{F}_q[t]$. Then

$$\#\{A \in M_n : A = C \bmod K\} = \begin{cases} q^n/|K|, & \deg K \leq n, \\ O(1), & \text{otherwise.} \end{cases}$$

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ *and the ring of integers* $\mathbb{Z}$.
We have the following comparison:

$$\{a \in \mathbb{Z}, a \leq n : a = c \bmod k\} \leftrightarrow \{A \in M_n : A = C \bmod K\}.$$

Note that the error term for $\mathbb{F}_q[t]$ when $\deg K \leq n$ is zero whereas the corresponding error term for $\mathbb{Z}$ was $O(1)$. When used in further calculations for $\mathbb{Z}$, the error term ultimately becomes $O(\rho_f(k))$. That is one of the reasons why we can explain the behaviour of square-free values of polynomials over $\mathbb{F}_q$ better than over $\mathbb{Z}$.

Proof. We differentiate between two situations, n being smaller or greater than the degree of K. Suppose for one that $n \geq \deg D$. Using the Euclidean Algorithm, we know that $C = 0$ or $\deg C < \deg K$. We now claim the following bijection:

$$\begin{aligned} M_{n-\deg K} &\leftrightarrow \{A \in M_n : A = C \bmod K\}, \\ B &\mapsto C + BK. \end{aligned}$$

Suppose that $A \in M_n, A = C \bmod K$, then recall that we can write $A = C + BK$ for some $C \in \mathbb{F}_q[t]$. We know that A is monic and thus we need to check that B is monic, of degree $n - \deg K$. Now because $\deg C < \deg K$, it must be the case that

$$n = \deg A = \deg(C + BK) = \deg BK = \deg B + \deg K.$$

We see that $\deg B = n - \deg K$. Since both A and K are monic and $\deg C < \deg K$, we must have B monic. Note that we used the fact that since $\deg C < \deg BK$, we have $\deg C + BK = \deg BK$. We end up with

$$\#\{A \in M_n : A = C \bmod K\} = \#M_{n-\deg K} = q^{n-\deg K} = \frac{q^n}{q^{\deg K}} = \frac{q^n}{|K|},$$

which agrees with the result stated in Lemma 3.3. On the other hand, suppose now that $\deg K > n$, then the arithmetic progression $A \equiv C \bmod K$ has at most 1 $A \in M_n$ in the progression $A = C \bmod K$. Take, for example, two elements A and A' of the progression. These two elements have to differ by a multiple of $D : A - A' = BK$. If the degree of both are $n < \deg K$ then $\deg(A - A') \leq n < \deg K$, this results in $B = 0$ and thus $A = A'$. □

3.2.1 The Prime Polynomial Theorem[15].

Recall that in Section 1.1, we introduced $\pi(n)$, being the number of prime integers $a \in \mathbb{N}, a \leq n$. Now we introduce $\pi_q(n)$, being the number of monic irreducibles of degree n. The Prime Polynomial Theorem states that

$$\pi_q(n) = \frac{q^n}{n} + O_q\left(\frac{q^{n/2}}{n}\right).$$

Note that the implied constant here depends only on q. We see that the error term here is very strong. In fact, we only need the upper bound, corresponding to Chebyshev's Theorem

$$\pi_q(n) \leq \frac{q^n}{n},$$

(that we can achieve a constant of 1 here requires an additional argument). Now let us turn to the the field $\mathbb{F}_q$. Once again, the ring $\mathbb{F}_q[x]$ is a unique factorization domain. Recall that the number of monic polynomials of degree n is q^n. Can we again say something about how many of these polynomials are irreducibles? The answer turns out to be

$$N_q(n) = \frac{1}{n}\sum_{d|n}\mu(d)q^{n/d} \quad [22, \text{Theorem } 3.25].$$

The largest term in this sum, which we can denote by the order, is q^n. We can therefore state that the order of the amount of monic irreducibles of degree n over $\mathbb{F}_q$ is simply q^n/n. In effect, we see that one out of every n monic polynomials of degree n over $\mathbb{F}_q$ is irreducible. Note that an interesting similarity is observed when making the comparison with the density of primes in $\mathbb{Z}$? As stated before, the Prime Number Theorem tells us that the number of primes p less than a positive integer n is of order $n/\log n$. In fact, we can analyze the amount of primes $p \leq n$ by the so-called *logarithmic integral* ($\mathrm{Li}(n) := \int_2^n \frac{dt}{\log t} = \frac{n}{\log n} + O\left(\frac{n}{(\log n)^2}\right)$.

$$\pi(n) = \mathrm{Li}(n) + O\left(n\exp\left(-c\sqrt{\log}\right)\right) = \frac{n}{\log n} + O\left(\frac{n}{(\log n)^2}\right).$$

Above expression essentially states that "close" to an integer a, the density of primes is of order $1/\log a$ [30].

Remark. Note that when we look at polynomials of degree 1, the error term of $\pi_q(n)$ becomes $O\left(\frac{q^{1/2}}{1}\right)$ while assuming that the Riemann Hypothesis is correct yields an error term for $\pi(x)$ of $O\left(x^{1/2+o(1)}\right)$. We see that they are equivalent.

Interestingly, we see that, since $n = \log_q(q^n)$, in both $\mathbb{Z}$ and $\mathbb{F}_q[x]$, the density of irreducible elements "close" to an element is of order 1 over the log of the absolute value of that element. The difference between the two situations is that when looking at $\mathbb{Z}$, we use the natural log, while when looking at $\mathbb{F}_q[x]$, we use the log of base q. What does this mean for number theoretic problems? Well, it turns out that if we look at the factorization problem, for $\mathbb{Z}$ this remains notoriously hard, while for $\mathbb{F}_q[x]$ this is simpler, especially if q is small, i.e., less than n[15] (assuming that the Riemann Hypothesis is valid).

3.2.2 Separability.

Definition 3.8 (Separable polynomial)**.** A polynomial $f \in \mathbb{F}_q[t]$ is separable if it has no repeated roots of positive degree, i.e. if it is square-free in $\mathbb{F}_q[t]$. Equivalently, if it has no double roots in an algebraic closure of $\mathbb{F}_q$. The term "separable" comes from distinctness of the roots: they are separate in the sense that there are no multiple roots.

We define *separability* here since, in further function field analogues, we assume polynomials f to be separable. We need f to be separable in order to make sure that it does not have double roots in any extension of $\mathbb{F}_q$, since if it had, we end up with $c_f = 0$. Take for example the function $f(x) = x^2 + x + 4 \in \mathbb{F}_5[x]$, this function is not separable since it can be written as $f(x) = (x+3)(x+3) = x^2 + 6x + 9 \equiv x^2 + x + 4 \in \mathbb{F}_5[x]$ and thus is never square-free, i.e., $c_f = 0$. The density if positive if and only if f is square-free (i.e.,separable).[6, Theorem 2.1]

Remark. Note that even a *primitive* (i.e., the gcd of the coefficients of $f \in \mathbb{F}_q[t][x]$ is 1), separable f can have no square-free values. For example

$$f(x) = \prod_{a_1, a_2 \in \mathbb{F}_q} (x - a_1 t - a_2) = x^{q^2} + \cdots .$$

Then for every $a \in \mathbb{F}_q[t]$, our function f evaluated in that a is divisible by $\left(\prod_{a_3 \in \mathbb{F}_q}(t - a_3)\right)^2 = (t^q - t)^2$. This is true since $a \in \mathbb{F}_q[t]$ is congruent $\bmod (t - a_3)^2$ to some $a_1 t + a_2$. Therefore, $f(a) \equiv f(a_1 t + a_2) = 0 \bmod (t - a_3)^2$, which is not square-free. [32]

Definition 3.9 (Characteristic of a ring R)**.** The characteristic of ring R, denoted $\mathrm{char}(R)$, is the smallest number of times one must use the ring's multiplicative identity in a sum to get the additive identity, if this sum eventually attains 0. We can also say that for every element $x \in R$, $\mathrm{char}(R) \cdot x = 0$ in R, $\mathrm{char}(R)$ being the smallest value for which this holds.

Definition 3.10. We define the *derivative* of a polynomial $f = \sum_{i \geq 0} a_i t^i \in \mathbb{F}_q[t]$ is

$$a'(t) := \sum_{i \geq 1} i a_i t^{i-1}.$$

Suppose that the characteristic of $\mathbb{F}_q$, denoted $\mathrm{char}(\mathbb{F}_q)$ is p. We then have $(t^p)' = p t^{p-1} = 0$. In general, the following lemma holds:

Lemma 3.4. For p prime, suppose $q = p^k$ and $p = \mathrm{char}(\mathbb{F}_q)$. If for some polynomial $a \in \mathbb{F}_q[t]$, we have $a' = 0$, this is equivalent to saying there is a function $b(t^p)$ for which $a(t) = b(t^p)$.[23, Chapter 7]

Lemma 3.5. $f \in \mathbb{F}_q[t]$ is separable if and only if $\gcd(f, f') = 1$.[8]

Remark. Suppose we write some polynomial p as $p(x) = \prod_{i=1}^{n}(x - a_i)^{n_i}$ where $n_i = 1$ for all i, and take the derivative of p with respect to x. This results in $p(x)' = (x - a_2) \cdots (x - a_n) + (x - a_1)(x - a_3)(x - a_4) \cdots (x - a_n) + \ldots$. We see that none of the terms in $p(x)'$ has a common factor, thus resulting in $\gcd(p, p') = 1$.

3.3 Function Field analogue of Conjecture 2.1 [33].

Similar to when discussing polynomials over $\mathbb{Z}$, we now aim to prove a function field version of the conjecture stating that a square-free polynomial takes on infinitely many square-free values.

Remark. The separability here is the function field equivalent of saying a polynomial cannot be written as a square of a function.

Definition 3.11 (Square-free polynomial in $\mathbb{F}_q[t]$)**.** We call a polynomial $f \in \mathbb{F}_q[t]$ square-free, if it is not divisible by the square of any non-constant polynomial $g \in \mathbb{F}_q[t]$.

Suppose $f \in \mathbb{F}_q[t]$ is separable with $\deg f > 0$. Let $\mathcal{P}$ be the set of primes in $\mathbb{F}_q[t]$ (i.e. monic irreducible polynomials). Similar to the definition before, by $\mathcal{N}_f(n)$ we mean the set of monic polynomials $a(t) \in M_n$ such that $f(a(t)) \in \mathbb{F}_q[t]$ is square-free. Again, we define for a polynomial $K \in \mathbb{F}_q[t]$, the function ρ:

$$\rho_f(K) = \#\{a \in M_n, a \bmod K : f(a) \equiv 0 \bmod K\}.$$

Remark. Note that $a \bmod K$ means the natural projection of $a \in \mathbb{F}_q[t]$ to the quotient ring $\frac{\mathbb{F}_q[t]}{\langle K \rangle}$.

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ *and the ring of integers* $\mathbb{Z}$.
This again is a function field equivalent to the analysis seen in Lemma 2.8, where we were looking at:

$$\rho_f(k) := \#\{a \in \frac{\mathbb{Z}}{k\mathbb{Z}} : f(a) \equiv 0 \bmod k\}.$$

With this function we can again look at the amount of irreducibles mod K such that $P^2 \mid f(a)$, which then gives finally gives us a density function.

Theorem 3.1. *Suppose* $f \in \mathbb{F}_q[x]$ *is separable. Then*

$$\#\mathcal{N}_f(n) = c_f q^n + O_{f,q}\left(\frac{q^n}{n}\right), \quad \text{as } n \to \infty, \tag{30}$$

where, for irreducible elements $P \in \mathcal{P}$ *:*

$$c_f = \prod_{P \in \mathcal{P}} \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right).$$

The density c_f *is positive if and only if there is some* $a \in \mathbb{F}_q[t]$ *such that* $f(a)$ *is square-free.*

We prove in the following sections, using the same sieve strategy as in the number field case, that Theorem 3.1 is in fact correct. Only when considering the contribution of large primes, we introduce a new lemma paramount to the proof (cf Lemma 3.8). Note that this lemma is unavailable in our proof for the number field case. For Granville [17], the ABC Conjecture takes a similar role.

Remark. In Theorem 3.1, the case of large degree (i.e., limit $n \to \infty$) is discussed. This is analogous in nature to the number field problem. However, the case of a large finite field (i.e., limit $q \to \infty$, n fixed) is not easily solved using sieve theory. Rudnick found a solution to that case using algebrogeometric methods [32].

3.3.1 Proof that the density c_f is nonzero.

In this section, we use a version of Hensel's Lemma[9] to prove an equivalence relation of a positive density c_f.

Lemma 3.6. Suppose a polynomial $f \in \mathbb{F}_q[x]$ is separable. Denote by $P \in \mathbb{F}_q[t]$ an irreducible element. Now each $a_1 \in \mathbb{F}_q[t]/(P)$ such that $f(a_1) = 0 \bmod P$ has a unique $a_2 \in \mathbb{F}_q[t]$ such that $a_1 = a_2 \bmod P$ and $f(a_2) = 0 \bmod P^2$.

Proof. Suppose $a_2 = a_1 + Py$. If we expand f around a_1, this gives us:

$$f(a_2) = f(a_1) + f'(a_1)Py + P^2y^2g(a_1, y),$$

for some function g. We write

$$f(a_2) = f(a_1) + f'(a_1)Py \bmod P^2.$$

Note that higher order terms fall out because of the mod P^2, therefore the function g is of little interest to us and need not be defined any further. Then, saying $f(a_2) = 0 \bmod P^2$ is equivalent to

$$f(a_1) + f'(a_1)Py = 0 \bmod P^2.$$

We stated originally that $P \mid f(a_1)$, and thus above equation can be rewritten as

$$f'(a_1) \cdot y = -\frac{f(a_1)}{P} \bmod P.$$

Now, proving that $f'(a_1) \neq 0 \bmod P$ means we found a unique $y \bmod P$ and thus proves the Lemma.

Recall that we assumed $f \in \mathbb{F}_q[x]$ to be a separable polynomial. Therefore it has no double roots in any extension of $\mathbb{F}_q$. Here we consider $\mathbb{F}_q[t]/(P)$, which is an extension of degree equal to $\deg P$. We know that a_1 is a root of $f(x) \bmod P$. Therefore, it cannot be a root of $f'(x) \bmod P$. This gives us the necessary conclusion that $f'(a_1) \neq 0 \bmod P$.

Remark. A different, but also quite straightforward proof, makes use the fact that for separable f, it must hold that $\gcd(f, f') = 1$. Then we have $r, t \in \mathbb{F}_q[x]$ with $rf + tf' = 1$, more specifically, $r(a_1)f(a_1) + t(a_1)f'(a_1) = 1 \bmod P$. Recall that $f(a_1) = 0 \bmod P$, which gives us $v(a_1)f'(a_1) = 1 \bmod P$. This in turn means $f'(a_1) \neq 0 \bmod P$.

□

Recall

$$\rho_f(K) = \#\{a \in M_n, a \bmod K : f(a) = 0 \bmod K\}.$$

As a consequence of Lemma 3.6, we have the following corollary:

Corollary 3.1.1. Let $f \in \mathbb{F}_q[x]$ be a separable polynomial. For any prime $P \in \mathbb{F}_q[t]$

$$\rho_f(P^2) = \rho_f(P).$$

Recall that the density c_f was defined as follows:

$$c_f := \prod_P \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right).$$

We know that $\rho_f(P) \leq \deg f$, i.e. the amount of solutions to $f(a) \equiv 0 \bmod P$ equal the amount solutions of a polynomial equation over the field $\mathbb{F}_q[t]/\langle P \rangle$. Considering Corollary 3.1.1, we can then state that c_f is absolutely convergent. We now prove that $c_f \neq 0$:

Proposition 3.2. Let $f \in \mathbb{F}_q[t]$ be a separable polynomial. Then the following are equivalent:

1. There is some $a \in \mathbb{F}_q[t]$ such that $f(a)$ is square-free.
2. The density c_f is positive.
3. For all primes P, with $\deg P \leq \frac{1}{2}\log_q(\deg f)$, there is some $a_P \bmod P^2$ for which $f(a_P) \neq 0 \bmod P^2$.

Proof. Using Hensel's Lemma, we know that $\rho_f(P^2) = \rho_f(P) \leq \deg f$. Again we differentiate between two cases. If $|P|^2 > \deg f$, then the every factor $1 - \frac{\rho_f(P^2)}{|P|^2} > 0$ is nonzero. Now we need to analyze the primes for which $q^{\deg P^2} = q^{2\deg P} \leq \deg f$. Considering these irreducibles P, we can check that a factor equals zero if $\rho(P^2) = P^2$. Note that is the case if and only if $f(a) = 0 \bmod P^2$ for all $a \in \mathbb{F}_q[t]$. This means that the sequence $f(a)$ has a fixed square factor, which cannot be the case. □

3.4 General outline of the proof.

Suppose $f \in \mathbb{F}_q[t]$ is a separable polynomial. We recall that we defined $\mathcal{N}_f(n)$ to be the set of all monic polynomials $a(t) \in M_n$, such that $f(a(t)) \in \mathbb{F}_q[t]$ is square-free. We introduce the integer $\zeta > 0$, which purpose is to split the primes into two sets with degree greater or smaller than ζ. Ultimately, we choose ζ to be

$$\zeta = \log_q \frac{n}{4}. \tag{31}$$

Suppose

$$\mathcal{N}'_f(n) = \{a \in M_n : P^2 \nmid f(a),\ \forall P \text{ prime with} \deg P \leq \zeta\},$$

and

$$\mathcal{N}''_f(n) = \{a \in M_n : \exists P \text{ prime}, \deg P > \zeta, \text{ such that } P^2 \mid f(a)\}.$$

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ *and the ring of integers* $\mathbb{Z}$.
Note that in Section 2.2.4 we split $\mathcal{N}_f = \mathcal{N}'_f + \mathcal{N}''_f$ using the size of the primes $p \in \mathbb{Z}$ for which we checked if their square divided the function f, whereas now we split using the size of the prime $p \in M_n$ (which is equivalent to the degree).

Then

$$\mathcal{N}_f(n) \subseteq \mathcal{N}'_f(n) \subseteq \mathcal{N}_f(n) \cup \mathcal{N}''_f(n).$$

Remark. In words: $\mathcal{N}_f(n)$ is the set of all $a \in M_n$ for which $f(a)$ is square-free, which is contained in $\mathcal{N}'_f(n)$ (the set containing all $a \in M_n$ for which $f(a)$ is square-free when looking only at primes with $\deg P \leq \zeta$). Also $\mathcal{N}_f(n) \cup \mathcal{N}''_f(n)$ is the union of the set of all $a \in M_n$ such that $f(a)$ is square-free for all primes and the set of all $a \in M_n$ for which $f(a)$ is not square-free for primes with $\deg P > \zeta$, which contains $\mathcal{N}'_f(n)$.

This results in

$$\#\mathcal{N}'_f(n) - \#\mathcal{N}''_f \leq \#\mathcal{N}_f(n) \leq \#\mathcal{N}'_f(n).$$

Finding an upper bound for $\#\mathcal{N}$ depending only on $\#\mathcal{N}'$ allows us to give an asymptotic that term (the "main term"), which is easy if ζ is small. Since the lower bound depends on $\#\mathcal{N}'_f(n)$ and $\#\mathcal{N}''_f(n)$ (where we found an asymptotic for the former), we need only to find an upper bound for $\#\mathcal{N}''_f(n)$. We show that for $\zeta \leq \log_q \frac{n}{4}$,

$$\#\mathcal{N}'_f(n) = c_f q^n + O\left(\frac{q^n}{q^\zeta}\right). \tag{32}$$

And

$$\mathcal{N}''_f \ll q^{n/p} + \frac{q^n}{\zeta q^\zeta} + \frac{q^n}{n}. \tag{33}$$

Choosing $\zeta = \log_q \frac{n}{4}$ in (32) and (33), we eventually end up with Theorem 3.1.

3.5 Bound for $\#\mathcal{N}'(n)$, the small primes.

First, we introduce some notation. Suppose we define $A^{<k} = \{a \in A : \deg a < k\}$ for any set of polynomials A and any degree k. We define $A^{>k}$ and $A^{=k}$ in a similar way. To estimate $\mathcal{N}'(n)$ (the main term), one uses inclusion-exclusion, observing that if we put $\mathcal{P}_\zeta := \prod_{P \in \mathcal{P}^{\leq \zeta}} P$ then for $a \in M_n$,

$$\sum_{\substack{k | \mathcal{P}_\zeta, \\ k^2 | f(a)}} \mu(k) = \begin{cases} 1, & a \in \mathcal{N}'_f(n), \\ 0, & \text{otherwise.} \end{cases}$$

Remark. Note that this is the function field equivalence of the indicator function seen in Section 2.1.3, which was defined as

$$\mathbf{1}_{SF}(n) = \mu^2(n) = \sum_{k^2 | n} \mu(k).$$

This gives us

$$\#\mathcal{N}'(n) = \sum_{k | \mathcal{P}_\zeta} \mu(k) \#\{a \in M_n : k^2 \mid f(a)\}.$$

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ and the ring of integers $\mathbb{Z}$.
Note that this is equivalent to the $\mathbb{Z}$ case where we stated

$$\#\mathcal{N}'(n) = \sum_{k \leq u} \mu(k) \#\{a \leq n, a \in \mathbb{Z} : k^2 \mid f(a)\}.$$

Lemma 3.7. For $K \neq 0, K \in \mathbb{F}_q[t]$,

$$\#\{a \in M_n : f(a) \equiv 0 \bmod K\} = \begin{cases} \frac{q^n \rho_f(K)}{|K|,} & \deg K \leq n, \\ O\left(\rho_f(K)\right), & \text{otherwise.} \end{cases}$$

Dictionary between the polynomial ring $\mathbb{F}_q[\mathrm{x}]$ and the ring of integers $\mathbb{Z}$.
This lemma also is equivalent, interchanging n by q^n (the total number of monic polynomials with degree n).

Proof. We break the term down

$$\#\{a \in M_n : f(a) \equiv 0 \bmod K\} = \sum_{\substack{C \bmod K \\ K | f(C)}} \#\{a \in M_n : a = C \bmod K\}.$$

Note that we have proved already in Lemma 3.3:

$$\#\{a \in M_n : a = C \bmod K\} = \begin{cases} \frac{q^n}{|K|}, & \deg K \leq n, \\ O(1), & \text{otherwise.} \end{cases}$$

Furthermore, we know there are $\rho_f(K)$ solutions $C \bmod K$ of $f(C) = 0 \bmod K$. Multiplying this term to the term from Lemma 3.3 proves the lemma. □

Now we find a bound for $\deg \mathcal{P}_\zeta$. By our choice of (31):

$$\deg \mathcal{P}_\zeta = \sum_{P \in \mathcal{P}^{\leq \zeta}} \deg P = \sum_{j=1}^{\zeta} j \frac{q^j}{j} \leq \frac{q^\zeta - 1}{1 - \frac{1}{q}} \leq 2q^\zeta \leq \frac{n}{2}.$$

Remark. The second equality essentially looks at every degree j, and adds a term consisting of the number of primes with that degree times the degree itself.

Since $\deg \mathcal{P}_\zeta \leq \frac{n}{2} \leq n$, the error term $O(1)$ does not play a role and end up with

$$\#\{a \in M_n : k^2 \mid f(a)\} = \frac{q^n \rho_f(k^2)}{|k|^2}, \quad \forall k \mid \mathcal{P}_\zeta,$$

Which, equivalent to the $\mathbb{Z}[x]$ case, translates using multiplicativity of ρ_f to

$$\#\mathcal{N}'(n) = q^n \sum_{d \mid \mathcal{P}_\zeta} \frac{\mu(d)\rho_f(d^2)}{|d|^2} = q^n \prod_{P \in \mathcal{P}^{\leq \zeta}} \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right).$$

Recall again that by Hensel's Lemma (Corollary 3.1.1), we find that $\rho_f(P^2) = \rho_f(P) \leq \deg f = O(1)$. If we now take $c_f = \prod_P \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right)$, this gives us

$$\prod_{P \in \mathcal{P}^{\leq \zeta}} \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right) = c_f \prod_{P \in \mathcal{P}^{> \zeta}} \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right)^{-1} = c_f \exp O\left(\sum_{P \in \mathcal{P}^{> \zeta}} \frac{1}{|P|^2}\right).$$

Now we need to find a bound for the final term

$$\sum_{P \in \mathcal{P}^{> \zeta}} \frac{1}{|P|^2} \leq \sum_{\substack{F \text{ monic} \\ |F| > q^\zeta}} \frac{1}{|F|^2} \ll \frac{1}{q^\zeta},$$

which then results in

$$\prod_{P \in \mathcal{P}^{\leq \zeta}} \left(1 - \frac{\rho_f(P^2)}{|P|^2}\right) = c_f(1 + O(\frac{1}{q^\zeta})).$$

Thus giving us the required result

$$\#\mathcal{N}'(n) = c_f q^n + O\left(\frac{q^n}{q^\zeta}\right) = c_f q^n + O\left(\frac{q^n}{q^{\log_q n/4}}\right),$$

proving (32).

Remark. In effect, we see that the derivation of the main term is exactly the same for $\mathbb{F}_q$ as it is for $\mathbb{Z}$. We recall the latter showed a main term of

$$\#\mathcal{N}'(n) = c_f n + O\left(\frac{n}{u}\log u + u \log u\right).$$

3.6 Bound for $\#\mathcal{N}''(n)$, the large primes.

Now, the essential difference between the number field case and $\mathbb{F}_q[t]$, is the following lemma:

Lemma 3.8. Suppose $f \in \mathbb{F}_q[t]$ is a separable polynomial. For $a \in M_n$ such that its derivative $a' \neq 0$ and $k^2 \mid f(a)$ for monic $k \in \mathbb{F}_q[t]$, then $k \mid a'$ and hence $\deg k \leq \deg a' = n - 1$.

Proof. For f is a separable polynomial, it must hold that $\gcd(f, f') = 1$ in $\mathbb{F}_q[t]$ (Lemma 3.5). This means that there are $r, t \in \mathbb{F}_q[t]$ with $rf + tf' = 1$. If we now use $a \in M_n$, as the argument, we have $u(a)f(a) + v(a)f'(a) = 1$. This means that $f(a)$ and $f'(a)$ are coprime in $\mathbb{F}_q[t]$. Suppose $k^2 | f(a)$. Then also $k \mid f(a)$ but $\gcd(f, f') = 1$, this means that k is coprime to $f'(a)$. If we now differentiate, we end up with $k \mid \frac{d}{dt}(f(a)) = f'(a)a'$. As stated above, k is coprime to $f'(a)$ and now we see $k \mid f'(a)a'$, this means that $k \mid a'$. Since we assume that $a' \neq 0$, we obtain $\deg k \leq \deg a' \leq n - 1$. □

Suppose that for any polynomial K,

$$\mathcal{N}_{K,f}(n) = \{a \in M_n : f(a) \equiv 0 \bmod K\}.$$

We can now find a bound for $\mathcal{N}''_f(n)$

$$\mathcal{N}''_f(n) \subseteq \{a \in M_n : a' = 0\} \bigcup \bigcup_{P \in \mathcal{P}^{\geq \zeta} \cap \mathcal{P}^{\leq n-1}} \mathcal{N}_{P^2,f}(d). \tag{34}$$

Remark. In words: The set of all $a \in M_n$ for which $f(a)$ is not square-free for primes with $\deg P > \zeta$ is contained in the union of the set of all $a \in M_n$ such that exists a prime P with $\zeta < \deg P \leq n - 1$ for which $f(a)$ is not square-free and all non separable $a \in M_n$. The right term above is due to Lemma 3.8.

This just leaves us with finding bounds for the terms in (34). Suppose that $q = p^e$, saying $a' = 0$ is then equivalent to the existence of a new function $b(t^p)$ for which $a(t) = b(t^p)$. (which forces $p \mid n$). We know that $a \in M_n$ and thus $b \in M_{n/p}$. Now we know the number of elements in $M_{n/p}$ equals $q^{n/p}$. Therefore

$$\#\{a \in M_n : a' = 0\} = \#M_{n/p} = q^{n/p}.$$

Thus

$$\mathcal{N}''_f(n) \leq q^{n/p} + \sum_{P \in \mathcal{P}^{\geq \zeta} \cap \mathcal{P}^{\leq n-1}} \#\mathcal{N}_{P^2}(n).$$

Luckily, finding a bound for the remaining terms is something we already did (Lemma 3.7):

$$\#\mathcal{N}_{K,f}(n) = \begin{cases} q^n \frac{\rho_f(K)}{|K|}, & \deg K \leq n, \\ O(\rho_K(n)), & \text{otherwise.} \end{cases}$$

Recalling that the terms we are interested in only account for primes with degree $\leq n - 1$, this gives us

$$\begin{aligned} \mathcal{N}''_f(n) &\leq q^{n/p} + \sum_{P \in \mathcal{P}^{\geq \zeta} \cap \mathcal{P}^{\leq n-1}} \#\mathcal{N}_{P^2,f}(n) \\ &= q^{n/p} + \sum_{P \in \mathcal{P}^{\geq \zeta} \cap \mathcal{P}^{\leq n/2}} \frac{q^n}{|P|^2} \rho_f(P^2) + \sum_{P \in \mathcal{P}^{> n/2} \cap \mathcal{P}^{\leq n-1}} O(\rho_f(P^2)). \end{aligned}$$

Remark. The sum is again decomposed since we divide by $|P|^2$, which takes the place of $|D|$. We therefore must make sure that $\deg P^2 \leq n$, which is done by letting the degree of P go as far as $\frac{n}{2}$.

By Lemma 3.6, $\rho(P^2) = \rho(P) \leq \deg f$ and hence

$$\begin{aligned}\mathcal{N}_f''(n) &\ll_{\deg f} q^{n/p} + q^n \sum_{P \in \mathcal{P}^{\geq \zeta} \cap \mathcal{P}^{\leq n/2}} \frac{1}{|P|^2} + \sum_{P \in \mathcal{P}^{>n/2} \cap \mathcal{P}^{\leq n-1}} 1 \\ &\ll q^{n/p} + q^n \sum_{\zeta < m \leq n/2} \frac{1}{q^{2m}} \frac{q^m}{m} + \sum_{n/2 < m \leq n-1} \frac{q^m}{m} \\ &\ll q^{n/p} + q^n \frac{1}{\zeta q^\zeta} + \frac{q^n}{n}.\end{aligned}$$

This then proves (33). In the number field setting, Lemma 3.8 is not available, which renders the above argument useless once $\deg f > 2$.

Remark. Ramsay [28] proved Theorem 3.1 for polynomials $f \in \mathbb{F}_q[x]$, i.e. polynomials with constant coefficients. Poonen [27] proved the Theorem for all $\mathbb{F}_q[t, x]$, and generalized it to multivariate polynomials in $\mathbb{F}_q[t, x_1, \ldots, x_n]$.

4 New Results by Dan Carmon.

In this section, we discuss the new results of the paper by Dan Carmon, which aims to extend above results to polynomials f with large coefficients, giving quantitative answers to questions analogous to those presented in Section 2. This is done by the use of the methods presented in the papers of both Poonen's and Lando's [21] and a new element, the Brun sieve. Brun's sieve essential sieves out all small prime elements, leaving behind prime and almost prime elements with only large divisors. In then states that these almost prime elements are included between two sums with a relative small number of summands, which may be estimated from above and below, thus finding a bound on the error term. More about this sieve is found in Section 4.1.3.

Note that this section largely follows the proof and structure of the article by Carmon, simplifying some steps and adding remarks whenever necessary.

Theorem 4.1. *Suppose $q = p^e$ is a prime power, $k > 0$ is an integer, and $m, n > 0$ are integers with $m \gg \log_q n \log_q \log_q n$ and $m \to \infty$. Suppose $f \in \mathbb{F}_q[t, x]$ is a square-free polynomial with $\deg_x f \leq k, \deg_t f \leq n$. Let c_f be defined as before. Then*

$$\#\{a \in \mathbb{F}_q[t] : \deg a < m, f(a) \text{ is square-free}\} = c_f q^m + o(c_f q^m)).$$

Remark. Note that, as opposed to Section 3, now we look at the possibility that the coefficients vary. If n is bounded, we do find the Theorem discussed before (Theorem 4.1 reduces to Poonen's Theorem). As such, the interesting part is when $n \to \infty$. From $m \gg \log_q n \log_q \log_q n$, it then follows that $m \to \infty$. Note that since the error term depends on c_f, this provides us a more accurate estimate.

An example that we can look at when discussing Theorem 4.1 is for instance $f(t, x) = tx + 1$, with $q = 2, k = 1, n = 1$ and $m = 5$. We see that $m = 5 \gg \log_2 1 \log_2 \log_2 1 = 0$. In the end we have to let $m \to \infty$. Furthermore, we see

that $\deg_x f = 1 = k$ and $\deg_t f = 1 = n$. So the assumptions there are met. We define c_f as usual. The theorem says that

$$\#\{a \in \mathbb{F}_2[t] : \deg a < 5, f(a) \text{ is square free}\} = c_f 2^5 + o(c_f 2^5).$$

We know there are $q^n - q^{n-1}$ square-free monic polynomials $a \in \mathbb{F}_2[t]$ of degree n. This allows us to calculate the number explicitly. Looking at Theorem 4.1, we are now in a position to state an analogue of Question 2:

Corollary 4.1.1. Suppose $q = p^e$ is a prime power, and $k > 0$ is an integer. Suppose that $N \in \mathbb{F}_q[t]$ is of "sufficiently" large degree n. Furthermore, let either k be coprime to p, or N not be a p-th power. Then the number of representations for $N = x^k + r$ N where $x, r \in \mathbb{F}_q[t]$, such that r is square-free and $\deg x < \frac{n}{k}$, is $c_{N,k}\ q^{\lceil n/k \rceil} + o\left(c_{N,k}\ q^{\lceil n/k \rceil}\right)$. Note that $c_{N,k} = \prod_{P \in \mathcal{P}} \left(1 - \frac{\rho_{N,k}(P^2)}{P^2}\right)$ and $\rho_{N,k}(D) = \#\{a \bmod D : a^k \equiv N \bmod D\}$.

Remark. Since, if N were a p-th power, and $p \mid k$, this would mean that $f(x)$ is also a p-th power. Then $f(x)$ is not square-free. Otherwise, f is square-free. We can check this by analyzing its derivatives in x and t. These derivatives must be coprime to f, whenever they are nonzero.

Now $c_{N,k}$ is the density of values which are not $\equiv N \bmod P^2$, for some P prime. This gives the number of square-free values of $f(x) = N - x^k$, which is square-free itself and has $\deg_x f = k, \deg_t f = n$. Here x can be any polynomial in $\mathbb{F}_q[t]$ with $\deg x < m = \lceil \frac{n}{k} \rceil$. Note that this agrees with the notion on m in Theorem 4.1. Now we look at the analogue to the short interval conjecture, Conjecture 2.2. We take interval length $H = q^m$, which consists of polynomials of size q^n. Using Theorem 4.1, we can see that we need $m \gg \log_q n \log_q \log_q n$, or equivalently, for $H \geq (\log_q q^n)^{C \log_q \log_q \log_q X} = n^{C \log_q \log_q n}$ for a certain constant C and all sufficiently large q^n, to get the correct result. In truth, we can let the interval be even smaller.

Theorem 4.2. *Suppose $q = p^e$ be a prime power, and $f \in \mathbb{F}_q[t, x]$ is a square-free polynomial with $\deg_x f = k$. Suppose n, m are large positive integers such that $m - p(\log_q n - \log_q \log_q n) \to \infty$, and $N(t) \in \mathbb{F}_q[t]$ is of degree n. Take the interval of size $H = q^m$ around N,*

$$I(N, m) = \{N + a : a \in \mathbb{F}_q[t], \deg a < m\}.$$

Then

$$\#\{a \in I(N, m) : f(a) \text{ is square-free}\} = c_f q^m + o\left(c_f q^m\right).$$

We see that $m - p(\log_p n - \log_q \log_q n) \to \infty)$ essentially means that $H \geq C \left(\frac{\log_q q^n}{\log_q \log_q q^n}\right)^p$ for any constant $C > 0$ and all sufficiently large q^n, i.e. a polylogarithmic relation. The fact that we see the characteristic of the field appear as the power of the term dependent on q^n, and thus taking such a prominent place in the allowed size of the interval, is rather odd. Moreover, note that there are intervals with $H \gg \frac{\log_q X}{\log_q \log_q X}$ that contain no square-free polynomials at all, by a straight forward application of the Chinese Remainder Theorem.

As with the proofs in Section 3, we see an analogues strategy for proving Theorem 4.1 and 4.2. However, we see that the differences in the context of

both proofs result in different leading error terms. This is the reason by both theorems have different lower bouds on m. Moreover, the two contributions are in fact mostly disjoint. Therefore we can unify the results into one theorem:

Theorem 4.3. *Suppose $q = p^e$ is a prime power, $k > 0$ is an integer, and $m, n_1, n_2 > 0$ are varying integers such that $m \gg \log_q n_1 \log_q \log_q n_1$ and $m - p(\log_q n2 \log_q \log_q n2 + 2k \log_q \log_q n_1) \to \infty$. Suppose $f \in \mathbb{F}_q[t, x]$ is a square-free polynomial with $\deg_x f \leq k, \deg_t f \leq n_1$. If $N(t) \in \mathbb{F}_q[t]$ is of degree n_2, and $I(N, m)$ is the interval of size q^m around N. We have*

$$\#\{a \in I(N,m) : f(a) \text{ square-free } \} = c_f q^m + o\left(c_f q^m\right).$$

4.1 Proof of Theorem 4.1.

First we introduce some notation. Let, for any set of polynomials A and any degree d, $A^{<d} = \{a \in A : \deg a < d\}$, and let us define $A^{>d}$ and $A^{=d}$ is a similar way. Furthermore, we write $\mathcal{N}_f(m) = \{a \in \mathbb{F}_q[t]^{<m} : f(a) \text{ is square-free}\}$. As with the proof of Theorem 2.8, we split $\#\mathcal{N}_f$ into a number of terms related to the contribution of certain primes and try to find bounds to find an appropriate estimate for $\mathcal{N}_f$. For constants m_0 and m_1, we let $m_1 = \lceil m/2 \rceil$ and define m_0 later.

$$\mathcal{N}' = \{a \in \mathbb{F}_q[t]^{<m} : \forall P \in \mathcal{P}^{<m_0}, P^2 \nmid f(a)\} \tag{35}$$

$$\mathcal{N}'' = \{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1}, P^2 \mid f(a)\} \tag{36}$$

$$\mathcal{N}''' = \{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_1}, P^2 \mid f(a)\} \tag{37}$$

Since $\mathcal{N} \subseteq \mathcal{N}' \subseteq \mathcal{N} \cup \mathcal{N}'' \cup \mathcal{N}'''$, it follows that $\#\mathcal{N}' - \#\mathcal{N}'' - \#\mathcal{N}''' \leq \#\mathcal{N} \leq \#\mathcal{N}'$.

Remark. In words: The set of all $a \in \mathbb{F}_q[t]^{<m}$ for which $f(a)$ is square-free for all primes P is contained in the set of values $a \in \mathbb{F}_q[t]^{<m}$ for which $f(a)$ is square-free for primes P with $\deg P < m_0$, which itself is contained in the union of the set of $a \in \mathbb{F}_q[t]$ for which $f(a)$ square-free for all primes, with the set of all $a \in \mathbb{F}_q[t]^{<m}$ for which there exists a prime P with $\deg P \geq m_0$ for which $f(a)$ is not square-free. We see that this is the same strategy as before. However, note that this last set is now split into one set looking only at primes with $m_0 \leq \deg P < m_1$ and the other set looking at the remaining primes, which differs from the approach in Section 3.4.

This gives us some boundary on $\#\mathcal{N}$. Our goal would then be to find the bounds $\#\mathcal{N}' = c_f q^m + o(c_f q^m)$ and $\#\mathcal{N}'', \#\mathcal{N}''' = o(c_f q^m)$. However, in order to do so, we have to determine some additional bounds relevant to our function f.

4.1.1 Preliminary bounds.

In this section, we derive three bounds which we need for calculating the bounds on $\mathcal{N}', \mathcal{N}'',$ and $\mathcal{N}'''$.

Definition 4.1 (Singular sum)**.** The *singular sum* of a polynomial f is

$$S = \sum_{P \in \mathcal{P}} \frac{\rho(P^2)}{|P|^2}.$$

Remark. Note that the fact that the singular sum converges follows from the proof of Lemma 4.1.

We define the tail (or remainder) $S(m_0)$ of this sum to be $S(m_0) = \sum_{P \in \mathcal{P}^{\geq m_0}} \frac{\rho(P^2)}{|P|^2}$. We attempt to find a bound for these sums, which in turn is used in the proof of Theorem 4.1.

Lemma 4.1. Suppose q is a prime power, $k > 0$ is an integer and $n, m_0 > 0$ are varying integers with $n \to \infty$. Suppose that $f \in \mathbb{F}_q[t, x]$ is a square-free polynomial with $\deg_x f \leq k$ and $\deg_t f \leq n$. Then the following bounds are correct

$$S \leq k \ln \log_q n + O(1) = O(\ln \ln n) \tag{38}$$

$$S(m_0) = O\left(\frac{n}{m_0 q^{m_0}}\right) \tag{39}$$

$$c_f \gg (\log_q n)^{-2k} \tag{40}$$

Remark. Note that, in effect, Equation (39) tells us about the speed of convergence of S. Furthermore, we need the lower bound on c_f in Equation 40 since we eventually want to prove that $\#\mathcal{N}'' = o(c_f q^m)$. The lower bound helps us to eventually find requirements on m_0.

We split the function $f(t, x)$ into two factors $f_i(t, x)$ and $f_s(t, x)$ such that $f(t, x) = f_i(t, x) f_s(t, x)$. Here $f_i(t, x) \in \mathbb{F}_q[t, x^p]$ denotes the product of all irreducible factors of $f(t, x)$ that are inseparable in x. That leaves $f_s(t, x)$ to have no x-inseparable factors. As stated, $f(t, x)$ is a square-free polynomial. Therefore, we know that f_i, f_s must be coprime (and square-free). Also f_i is coprime to $\frac{\partial f_i}{\partial t}$ and f_s is coprime to $\frac{\partial f_s}{\partial x}$ (see Lemma 3.5). Suppose that $P(t, x)$ is an irreducible common divisor of f_s and $\frac{\partial f_s}{\partial x}$. This leaves tho options. For one, $P^2 \mid f_s$. However, this disproves the fact that f_s is square-free. For another, $P \mid \frac{\partial P}{\partial x}$. However, this suggests that P is inseparable in x, which disproves f_s having no inseparable factors. We apply the same logic to f_i. Suppose that $P(t, x)$ is an irreducible common divisor of f_i and $\frac{\partial f_i}{t}$. This again leaves two options. For one, $P^2 \mid f_i$,. This disproves f_i being square-free. For another, P is inseparable in t. Since both $f_i, \frac{\partial f_i}{\partial t}$ are in $\mathbb{F}_q[t, x^p]$, either P^p is also a common divisor, disproving the fact that they are square free, or P is also in $\mathbb{F}_q[t, x^p]$. Now, we already stated that P is inseparable in t, so $P \in \mathbb{F}_q[t^p, x^p]$. This results P being a p-th power, contradicting its irreducibility. Therefore there exists no such irreducible common divisor.

Definition 4.2 (Resultant)**.** For the definition of the *resultant*, I advise to follow the discussion in the book by Gelfand [20].

Remark. In other words, the *resultant* of $k+1$ polynomials in k variables can be represented as an irreducible polynomial in the coefficients of $f_0, \ldots, f_k$. This polynomial vanishes if the $k+1$ polynomials have a common root.

Suppose $R(t) = \mathrm{Res}_x(f_i, \frac{\partial f}{\partial t}) \mathrm{Res}_x(f_s, \frac{\partial f}{\partial x}) \in \mathbb{F}_q[t]$. To check that this function is non vanishing, we check that the functions $f_i, \frac{\partial f}{\partial t}$ are coprime, as well as $f_s, \frac{\partial f}{\partial x}$. For the first term, we write $\frac{\partial f}{\partial t} = f_s \frac{\partial f_i}{\partial t} + f_i \frac{\partial f_s}{\partial t}$. We see that this is coprime to f_i by the argument above. Also, we write $\frac{\partial f}{\partial x} = f_i \frac{\partial f_s}{\partial x} + f_s \frac{\partial f_i}{\partial x}$. We see that this is coprime to f_s by the argument above. Then, we see that $R(t)$ is nonzero.

Remark. Recall that the x- and t-degrees of the polynomials f_i, f_s and their derivatives are all at most k and n, respectively. We can hen write the two terms of $R(t)$ as polynomials of degree $\leq 2k$ in the $\mathbb{F}_q[t]$-coefficients of their arguments, each of which is of degree at most n. Therefore, $\deg R \leq 4kn = O(n)$. Then the number of prime factors of R with degree $\geq m_0$ is at most $\frac{4kn}{m_0}$.

We now again apply a version of Hensel's Lemma. Suppose we have a prime $P \in \mathcal{P}$ such that $P \nmid R$. We want to show that for every residue $a_1 \bmod P \in \rho(P)$, there is at most one lifting modulo P^2 which is in $\rho(P^2)$. Since for every P such that $P \mid f$, also $P \mid R$. This, in turn, helps us to bound the contribution of $rho(P^2)$. Then the residue of $f \equiv c \bmod P \in \frac{\mathbb{F}_q[t]}{\langle P \rangle}[x]$ is non-trivial. Then c also has degree $\leq k$. As we saw before, this suggests that $\rho(P) \leq k$. Suppose $a_1 \in \mathbb{F}_q[t]$ is some residue class in $\rho(P)$, i.e. a_1 is such that $f(a_1) \equiv 0 \bmod P$. Suppose $\frac{\partial f}{\partial x}(a_1) \not\equiv 0 \bmod P$. Now we have every ingredient to apply Hensel's Lemma. This states that there is a unique lifting of a_1 to a residue $a_2 \bmod P^2$ such that $a_2 \equiv a_1 \bmod P$ and $f(a_2) \equiv 0 \bmod P^2$.

To the contrary, suppose $\frac{\partial f}{\partial x}(a_1) \equiv 0 \bmod P$. Now if $P \mid f_s(a_1)$, then a is a root of both f_s and $\frac{\partial f}{\partial x} \bmod P$. Therefore P would also divide $\mathrm{Res}_x(f_s, \frac{\partial f}{\partial x})$. We know this cannot be the case since we assumed $P \nmid R$. So $P \nmid f_s(a_1)$. Because P divides $f(a_1)$, this means that P divides $f_s(a_1) f_i(a_1)$. Since we just stated that $P \nmid f_s$, it must mean that $P \mid f_i$. Using a similar reasoning as before, this results in $\frac{\partial f}{\partial t}(a_1) \not\equiv 0 \bmod P$. Therefore

$$\frac{\mathrm{d}f(t, a_1(t))}{\mathrm{d}t} = \frac{\partial f}{\partial t}(a_1) + \frac{\partial f}{\partial x}(a_1)\frac{\mathrm{d}a}{\mathrm{d}t} \equiv \frac{\partial f}{\partial t}(a_1) \not\equiv 0 \bmod P.$$

We see that since $P \nmid \frac{\mathrm{d}f(t,a_1(t))}{\mathrm{d}t}$, also $P(t)^2 \nmid f(t, a_1(t))$, for any such a_1. Concluding, there is no residue $a_2 \bmod P^2$ where $a_2 = a_1 \bmod P$ such that $f(a_2) = 0 \bmod P^2$.
Thus our proof concludes that for all residues $a_1 \bmod P \in \rho(P)$, we have at most one lifting modulo P^2, which is in $\rho(P^2)$. This gives us a similar result as for the number field setting, i.e., primes P where $P \nmid R$, we have $\rho(P^2) \leq \rho(P) \leq k$.

Proof of Equation (39). Now using this knowledge, we attempt to find a bound for $S(m_0)$. Recalling $S(m_0) = \sum_{P \in \mathcal{P}^{\geq m_0}} \frac{\rho(P^2)}{|P|^2}$, we can split the primes over which we sum into those P such that $P \mid R$ and those P such that $P \nmid R$. For primes P such that $P \nmid R$, we have

$$\sum_{P \in \mathcal{P}^{\geq m_0} : P \nmid R} \frac{\rho(P^2)}{|P|^2} \leq k \sum_{d=m_0}^{\infty} \frac{1}{dq^d} = O\left(\frac{1}{m_0 q^{m_0}}\right).$$

Remark. The equalities hold since we know that $|P| = q^{\deg P} = q^d$ and the number of primes P, with $\deg P = d$, is $\frac{q^d}{d}$ (see Section 3.2.1).

Definition 4.3 (Primitive polynomial)**.** Let $q = p^m$ for some prime p. We define a *primitive polynomial* to be the minimal polynomial of a primitive element of the finite extension field $\mathbb{F}_q$. In other words, a polynomial $f(x)$ with coefficients in $\frac{\mathbb{Z}}{p\mathbb{Z}}$ is a primitive polynomial if it has a root α in $\mathbb{F}_q$ such that $\{0, 1, \alpha, \alpha^2, \ldots, a^{q-2}\}$ is the entire field $\mathbb{F}_q$, and $f(x)$ is the smallest degree polynomial having α as a root.

Remark. Note that a primitive polynomial f $f(x)$ must have a non-zero constant term, otherwise it is divisible by x.

Now, we focus on those primes P for which $P \mid R$. Recall f is square-free and therefore P^2 does not divide f. Therefore, if P divides the content of f, then $\frac{f}{P} \in \frac{\mathbb{F}_q[t]}{\langle P \rangle}[x]$ does not leave a residue 0. For these primes P, can therefore bound $\rho(P^2)$ by

$$\begin{aligned}\rho(P^2) &= \#\{a \bmod P^2 : f(a) \equiv 0 \bmod P^2\} \\ &= \#\{a \bmod P^2 : \frac{f(a)}{P} \equiv 0 \bmod P\} \\ &= \#\{a \bmod P : \frac{f(a)}{P} \equiv 0 \bmod P\} \cdot |P| \leq k|P|.\end{aligned}$$

On the other hand, for P such that $P \mid R$, if we now focus on primes P where P does divide the content of f, we simply have $\rho(P) \leq k$. Thus we find the bound $\rho(P^2) \leq |P|\rho(P) \leq k|P|$. we have $\rho(P^2) \leq k|P|$.

We are now in a position to find a bound for the primes P such that $P \mid R$

$$\begin{aligned}\sum_{\substack{P \in \mathcal{P}^{\geq m_0}, \\ P \mid R}} \frac{\rho(P^2)}{|P|^2} &\leq \sum_{\substack{P \in \mathcal{P}^{\geq m_0}, \\ P \mid R}} \frac{k|P|}{|P|^2} = \sum_{\substack{P \in \mathcal{P}^{\geq m_0}, \\ P \mid R}} \frac{k}{|P|} \\ &\leq \sum_{\substack{P \in \mathcal{P}^{\geq m_0}, \\ P \mid R}} \frac{k}{q^{m_0}} \leq \frac{4kn}{m_0} \frac{k}{q^{m_0}} = O\left(\frac{n}{m_0 q^{m_0}}\right).\end{aligned}$$

We can conclude our proof of Equation (39) □

Proof of Equation (38). Recalling $S = \sum_{P \in \mathcal{P}} \frac{\rho(P^2)}{|P|^2}$, we can again split the primes over which we sum into those P such that $P \mid R$ and those P such that $P \nmid R$. For primes P such that $P \nmid R$, we have

$$\begin{aligned}\sum_{P \in \mathcal{P} : P \nmid R} \frac{\rho(P^2)}{|P^2|} &\leq \sum_{P \in \mathcal{P}} \frac{k}{|P|^2} = \sum_{d=1}^{\infty} \sum_{P \in \mathcal{P}^{=d}} \frac{k}{q^{2d}} \\ &= \sum_{d=1}^{\infty} \frac{k}{q^{2d}} \frac{q^d}{d} = k \sum_{d=1}^{\infty} \frac{1}{dq^d} \leq \frac{k}{d-1} = O(1).\end{aligned}$$

On the other hand, for P such that $P \mid R$, we again try to find a bound on their contribution. We write for all $d > 0, u_d = \#\{P \in \mathcal{P}^{=d} : P \mid R\}$, and let $x_d = du_d$. We can again bound u_d by all the primes of degree d: $\pi_q(d)$, which results in $du_d \leq d\frac{q^d}{d}$. Also, $\sum_{d=1}^{\infty} du_d \leq \deg R \leq 4kn$, since there cannot be more than $\deg R$ prime factors that divide R. The bound then becomes

$$\sum_{\substack{P \in \mathcal{P} \\ P \mid R}} \frac{\rho(P^2)}{|P|^2} \leq \sum_{\substack{P \in \mathcal{P} \\ P \mid R}} \frac{k}{|P|^2} = k \sum_{d=1}^{\infty} \frac{u_d}{q^d} = k \sum_{d=1}^{\infty} \frac{x_d}{dq^d}.$$

Note that $\frac{1}{dq^d}$ is decreasing. Therefore, an upper bound on $\sum_{d=1}^{\infty} \frac{x^d}{dq^d}$, knowing $0 \leq x_d \leq q^d$ and $\sum_{d=1}^{\infty} x_d \leq 4kn$, is attained when $x_d = q^d$ for all $d < n_0$, and $x_{n_0} = 4kn - \sum_{d=1}^{n_0-1} x_d$, and $x_d = 0$, for all $d > n_0$. Note that n_0 is then determined uniquely by $0 \leq x_{n_0} \leq q^{n_0}$.

Remark. Such values would not necessarily correspond to any actual R, but do serve for obtaining an upper bound.

We end up with $q^{n_0-1} \leq 4kn$, and $n_0 \leq \log_q(4kqn) = \log_q(n) + O(1)$. We can now finalize the bound on primes P where $P \mid R$:

$$\sum_{\substack{P\in\mathcal{P}\\P|R}} \frac{\rho(P^2)}{|P|^2} \leq k\sum_{d=1}^{\infty}\frac{x_d}{dq^d} \leq k\sum_{d=1}^{n_0}\frac{1}{d} = k(\ln(n_0)+O(1))$$
$$= O(\ln\ln n).$$

□

Remark. Note that for both proofs, we see that the primes P where $P \mid R$ are provide the main term in the bound.

Proof of Equation (40). The final bound we need to prove is that of Equation (40). Recall we need to show the lower bound $c_f \gg (\log_q n)^{-k-o(1)}$. The reason we prove this bound last, is that we make use of the bound of Equation (38). Suppose $\epsilon > 0$, we now divide the summands of S into two sets. A set with those $x = \frac{\rho(P^2)}{|P|^2}$ greater than ϵ and a set with those lesser. Recall that each term is at most $\frac{k}{|P|}$. Then this means that only a finite amount of summands (corresponding to a finite amount of primes P) $x = \frac{\rho(P^2)}{|P|^2}$ are greater than ϵ. Furthermore, these primes are of finite degree and therefore, the amount that these terms add to the product $c_f = \prod_{P\in\mathcal{P}}\left(1-\frac{\rho(P^2)}{|P|^2}\right)$ can also be bounded below by some positive constant $C_\epsilon = C_{k,q,\epsilon} > 0$. Note that this constant does not depend on n (assuming no local obstructions exist, so that $1-\frac{\rho(P^2)}{|P|^2} \leq \frac{1}{|P|^2}$ for all P).
If we now focus on the summands x such that $x = \frac{\rho(P^2)}{|P|^2} < \epsilon$, we can expand this, which ultimately gives us the inequality $\ln 1 - x = -\int_0^x \frac{1}{1-x}\mathrm{d}x > -\int_0^x \frac{1}{1-\epsilon}\mathrm{d}x = -\frac{x}{1-\epsilon}$. This means that each of these terms $1-\frac{\rho(P^2)}{|P|^2} = 1-x$ in c_f is bounded below by $\exp -\frac{S}{1-\epsilon} \gg_{k,q} (\log_q n)^{-k/(1-\epsilon)}$. If now we look at the whole picture, using both the summands $x > \epsilon$, and the summands $x < \epsilon$, we end up with $c_f \gg_{k,q} C_\epsilon(\log_q n)^{-k+O(\epsilon)}$. Recall that C_ϵ depends only on ϵ (not n). Therefore, if we we let $\epsilon \to 0$ sufficiently slow as $n \to \infty$, we can replace the bound by $c_f \gg (\log_q n)^{-k-o(1)}$. Letting $\epsilon = \frac{1}{2}$ concludes our proof of Equation (40). □

We now attempt to find bounds on $\mathcal{N}', \mathcal{N}''$ and $\mathcal{N}'''$, which in turn helps us to prove Theorem 4.1. We start with the medium primes, $\mathcal{N}''$, since this is the most straightforward.

4.1.2 Bound for $\#\mathcal{N}''$, the medium primes.

Recall that we chose $m_1 = \lceil \frac{m}{2} \rceil$. This means that for any prime $P \in \mathcal{P}^{<m_1} = \mathcal{P}^{<\lceil \frac{m}{2} \rceil}$ we have $\deg(P^2) < m$. Using Lemma 3.7, we have $\#\{a \in \mathbb{F}_q[t]^{<m} : P^2 \mid$

$f(a)\} = \frac{\rho(P^2)}{|P|^2}q^m$. We now derive the bound for $\#\mathcal{N}''$:

$$\begin{aligned}
\#\mathcal{N}'' &= \#\{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1}, P^2 \mid f(a)\} \\
&= \# \bigcup_{P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1}} \{a \in \mathbb{F}_q[t]^{<m} : P^2 \mid f(a)\} \\
&\leq \sum_{P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1}} \#\{a \in \mathbb{F}_q[t]^{<m} : P^2 \mid f(a)\} \\
&= \sum_{P \in \mathcal{P}^{\geq m_0} \cap \mathcal{P}^{<m_1}} \frac{\rho(P^2)}{|P|^2} q^m \\
&\leq q^m \sum_{P \in \mathcal{P}^{\geq m_0}} \frac{\rho(P^2)}{|P|^2} = q^m S(m_0).
\end{aligned}$$

Remark. On the third line, the $\leq$ sign is due to the fact that there might elements $a \in \mathbb{F}_q[t]^{<m}$ for which $f(a)$ is not square-free for multiple primes P. Thus by summing each set, we overcount. The last equality is true per definition of $S(m_0)$.

Our aim was to prove that $\#\mathcal{N}'' = o\left(c_f q^m\right)$. We therefore need $S(m_0)$ to be $o(c_f)$. If we consider Lemma 4.1, we see that we need m_0 to be such that $\frac{m_0 q^{m_0}}{n(\log_q n)^{2k}} \to \infty$. This we can rewrite into saying that $m_0 - \log_q n - 2k \log_q \log_q n \to \infty$. We can, again, rewrite this as $m_0 \gg \log_q n$. If $n \to \infty$, the implied constant may be any constant greater than 1, and if n is bounded we only require $m_0 \to \infty$.

4.1.3 Bound for $\#\mathcal{N}'$, the small primes.

We recall writing $\mathcal{P}_{m_0} = \prod_{P \in \mathcal{P}^{<m_0}} P$. Using a sieve similar to the one we used in Sections 2.2.4 and 3.5, we write

$$\#\mathcal{N}' = \sum_{D \mid \mathcal{P}_{m_0}} \mu(D) \#\{a \in \mathbb{F}_q[t]^{<m} : D^2 \mid f(a)\}.$$

Suppose we can factorize a square-free polynomial $D \in \mathbb{F}_q[t]$, into $\nu(D)$ distinct primes. For $k \in \mathbb{N}$, we define

$$n_k = \sum_{\substack{D \mid \mathcal{P}_{m_0}, \\ \nu(D)=k}} \#\{a \in \mathbb{F}_q[t]^{<m} : D^2 \mid f(a)\}$$

so that $\#\mathcal{N}' = \sum_{k=0}^{\infty} (-1)^k n_k$.

Remark. In other words; n_k looks at any element dividing P_{m_0} (which is either a prime or the product of several primes), and finds the number of elements $a \in \mathbb{F}_q[t]^{<m}$ for which the polynomial is not square-free.

Here we start using the concept of Brun's sieve. In short, Brun's sieve makes use of the fact that the partial sum $\mathcal{N}_r = \sum_{k=0}^{r} (-1)^k n_k$ alternates around the limit of $\#\mathcal{N}'$. That is, for r even, we have $\#\mathcal{N}' \leq \mathcal{N}_r$, and for r odd, we have $\#\mathcal{N}' \geq \mathcal{N}_r$[1, Chapter 6]. Instead of having to find specific upper and lower bounds for $\#\mathcal{N}'$, we can concentrate on proving that $\mathcal{N}_r$ equals some

term, for sufficiently large r. In our case we want to prove that that term is $c_f q^m + o(c_f q^m)$. This then suffices as both upper and lower bounds for $\#\mathcal{N}'$.

The most straightforward calculation can be done by considering those elements $D|\mathcal{P}_{m_0}$ with $\nu(D) \leq r$ such that $\deg(D^2) \leq m$. For such D, we can make use of Lemma 3.7. We therefore let m_0 and r be such that $2m_0 r \leq m$. Then, for any $D \mid \mathcal{P}_{m_0}$ (since every factor of $\mathcal{P}_{m_0}$ has degree $< m_0$), $\deg D^2 = 2\deg D < 2m_0 r \leq m$. Then

$$\#\{a \in \mathbb{F}_q[t]^{<m} : D^2 \mid f(a)\} = \frac{\rho(D^2)}{|D|^2} q^m = \rho(D^2) q^{m-2\deg D}.$$

We can then write for every $k \leq r$, that $n_k = \sum_{\substack{D|\mathcal{P}_{m_0} \\ \nu(D)=k}} \rho(D^2) q^{m-2\deg D}$.

To evaluate this, we introduce the function U:

$$U(x,y) := \sum_{\substack{D|P_y \\ \nu(D)\leq x}} \mu(D) \frac{\rho(D^2)}{|D|^2}.$$

This gives us

$$\mathcal{N}_r = q^m \sum_{\substack{D|\mathcal{P}_{m_0} \\ \nu(D)\leq r}} \mu(D) \frac{\rho(D^2)}{|D|^2} = q^m U(r, m_0).$$

We now wish to estimate $U(r, m_0)$. Note that

$$\begin{aligned} U(\infty, m_0) &= \sum_{D|\mathcal{P}_{m_0}} \mu(D) \frac{\rho(D^2)}{|D|^2} = \prod_{P\in\mathcal{P}^{<m_0}} \left(1 - \frac{\rho(P^2)}{|P|^2}\right) \\ &= c_f \prod_{P\in\mathcal{P}^{\geq m_0}} \left(1 - \frac{\rho(P^2)}{|P|^2}\right)^{-1} = c_f(1 + O(S(m_0))) = c_f(1 + o(1)). \end{aligned}$$

Note that in finding the bound for $\#\mathcal{N}''$, we assumed that m_0 was chosen such that $S(m_0) = o(c_f) = o(1)$. If now we are able to bound $U(\infty, m_0) - U(r, m_0)$, we may conclude the proof. We write, for any $k \in \mathbb{N}$:

$$v_k = \sum_{\substack{D|\mathcal{P}_{m_0} \\ \nu(D)=k}} \frac{\rho(D^2)}{|D|^2}.$$

Remark. Note that v_k is the k-th elementary symmetric polynomial of the finite multiset $\left\{\frac{\rho(P^2)}{|P|^2} : P \in \mathcal{P}^{<m_0}\right\}$, whose elements are positive real numbers.

We then have $v_k \leq \frac{v_1^k}{k!}$. We can now again use the bound we found for S 38. Since v_1 takes only primes with degree $< m_0$, we have $v_1 \leq S$. We can therefore write $v_1 \leq \lambda = k \ln\log_q n + O(1)$. Let $r = \alpha\lambda$ for some $\alpha > 2$. Now we can find

our bound for $U(\infty, m_0) - U(r, m_0)$:

$$\begin{aligned}|U(\infty, m_0) - U(r, m_0)| &= \left|\sum_{k=r+1}^{\infty} (-1)^k v_k\right| \leq \sum_{k=r+1}^{\infty} v_k \leq \sum_{k=r+1}^{\infty} \frac{\lambda^k}{k!} \\ &< \sum_{k=r+1}^{\infty} \frac{\lambda^r}{r!}\alpha^{r-k} < \frac{\lambda^r}{r!} < \frac{\lambda^r}{(r/e)^r} \\ &= \left(\frac{e\lambda}{r}\right)^r = \left(\frac{e}{\alpha}\right)^{\alpha\lambda} = O\left((\log_q n)^{-\alpha \ln(a/e)k}\right).\end{aligned}$$

We need to choose $\alpha \ln(\alpha/e)$ such that (i.e., large enough), by (40),

$$|U(\infty, m_0) - U(r, m_0)| \ll (\log_q n)^{-k\alpha \ln(\alpha/e)} = o(c_f).$$

This proves that if we let r be such that $r \gg \log_q \log_q n$ and $r \to \infty$ then $\mathcal{N}_r = q^m c_f(1 + o(1))$. Use of Brun's sieve then concludes our proof that $\#\mathcal{N}' = c_f q^m + o(c_f q^m)$.

Remark. Note that we made some assumptions in Section 4.1.2 and 4.1.3 for the proofs to be correct, we sum them up right here. We need m_0 and r to be such that $m_0 \gg \log_q n$ and $r \gg \log_q \log_q n$, where $m_0, r \to \infty$ and $2m_0 r \leq m$. Combining these assumptions, we arrive at the conclusion that this means that $m \gg \log_q n \log_q \log_q n$ and $m \to \infty$. Note that this is one of the conditions in on m in Theorem 4.1.

4.1.4 Bound for $\#\mathcal{N}'''$, the large primes.

As we saw in Section 3.6, the bound for the large primes is, compared to the small and the medium primes, the most difficult to calculate. Poonen solved this problem by replacing the target polynomial by an equivalent multivariate polynomial with a simpler t-derivative, and carefully retrace Lando's bounds on the corresponding contributions to $\mathcal{N}'''$, noting the size of our coefficients.

Suppose we have the polynomial $f(x) \in \mathbb{F}_q[t][x]$, we then define a new polynomial F by

$$F(y_0, \ldots, y_{p-1}) = f(y_o^p, ty_1^p + \cdots + t^{p-1}y_{p-1}^p) \in \mathbb{F}_q[t][y_0^p, y_1^p, \ldots, y_{p-1}^p].$$

Recall that $\deg_x(f) \leq k$ and $\deg_t(f) \leq n$, these in turn provide a bound on F's coefficients and degrees: $\deg_t(F) < n + pk = O(n)$ and $\deg_{y_i}(F) < pk$. We use two lemma's from Poonen[27, Lemma 7.2 and Lemma 7.3]:

Lemma 4.2. If $f \in K[x_1, \ldots, x_n]$ is square-free, then

$$F := f(y_0^p + ty_1^p + \cdots + t^{p-1}y_{p-1}^p, x_2, x_3, \ldots, x_n) \in K[y_0, \ldots, y_{p-1}, x_2, \ldots, x_n]$$

is square-free.

Lemma 4.3. Suppose that $f \in K[x_1^p, \ldots, x_n^p]$ is square-free as an element of $K[x_1, \ldots, x_n]$. Then f and $\frac{\partial f}{\partial t}$ are relatively prime as elements of $K[x_1, \ldots, x_n]$.

Therefore, if f is a square-free polynomial, then F also is one. And if F is a square-free polynomial, this means that F and $\frac{\partial F}{\partial t}$ are coprime. Alternatively,

suppose that $y \in (\mathbb{F}_q[t])^p$ such that $P^2|F(y)$. Recall that the y_i-s appear in F only with exponents divisible by p, and $\frac{\partial F(y)}{\partial t}$. Thus $P^2|F(y)$ is equivalent to stating that $P \mid F(y)$ and $P \mid \frac{\partial F}{\partial t}(y)$. Furthermore, we note that $\deg_t(\frac{\partial F}{\partial t}) \leq \deg_t(F) = O(n)$ and $\deg_{y_i}(\frac{\partial F}{\partial t}) \leq \deg_{y_i}(F) \leq pk$.

Remark. Note that Lemma 4.3 proves F and $\frac{\partial F}{\partial t}$ are coprime in $\mathbb{F}_q(t)[y_0, \ldots, y_{p-1}]$ only. In our proof, we assume them to be coprime in $\mathbb{F}_q[t][y_0, \ldots, y_{p-1}]$. We can however check this is also true. To be coprime, we need to make sure that they have no common factor $P \in \mathbb{F}_q[t]$. If this P exists, then it must divide the contents of both $F(y_0, 0, \ldots, 0) = f(y_0^p)$ and $\frac{\partial F}{\partial t}(y_0, 0, \ldots, 0) = \frac{\partial f}{\partial t}(y_0^p)$. Then we can assume that P^2 divides f, which refutes the fact that f is square-free.

We are now in a position to find a bound for $\mathcal{N}'''$.

Suppose $m_p = \lceil \frac{m}{p} \rceil \leq \lceil \frac{m}{2} \rceil = m_1$. Observe that letting the p-tuple (that is, the sequence of p elements) y range over all $(\mathbb{F}_q[t]^{<m_p})^p$, implies $a = y_0^p + ty_1^p + \cdots t^{p-1}y_{p-1}^p$ ranges over all $\mathbb{F}_q[t]^{<pm_p}$. Note furthermore that $\mathbb{F}_q[t]^{<m} \subset \mathbb{F}_q[t]^{<pm_p}$. Therefore

$$\begin{aligned}
\#\mathcal{N}''' &= \#\{a \in \mathbb{F}_q[t]^{<m} : \exists P \in \mathcal{P}^{\geq m_1}, P^2 \mid f(a)\} \\
&\leq \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{p+1} : \exists P \in \mathcal{P}^{\geq m_1}, P^2 \mid f(y_0^p + ty_1^p + \cdots t^{p-1}y_{p-1}^p)\} \\
&= \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{p+1} : \exists P \in \mathcal{P}^{\geq m_1}, P^2 \mid F(y))\} \\
&= \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{p+1} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid F(y) \text{ and } P \mid \frac{\partial F}{\partial t}(y)\}. \qquad (41)
\end{aligned}$$

We need the following proposition to find a bound for (41), analogous to [21, Proposition 5]:

Proposition 4.4. Suppose $k, l, n, m_p, m_1 \in \mathbb{N}$ such that $m_1 \geq m_p$. Suppose that $f, g \in \mathbb{F}_q[t][y_0, \ldots, y_l]$ are coprime polynomials in $l+1$ variables with $\deg_{y_i}(f), \deg_{y_i}(g) \leq k$ and $\deg_t(f), \deg_t(g) \leq n$. If

$$\mathcal{N}_l(f, g) = \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid f(y) \text{ and } P \mid g(y)\}.$$

Then $\mathcal{N}_l(f, g) = O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right)$.

Proposition 4.4 allows us to write the following:

$$\#\mathcal{N}''' \leq O_{p,pk}\left(\frac{n+m_1}{m_1} q^{(p-1)m_p}\right) = O_{p,k}\left(\frac{n+m}{mq^{\frac{m}{p}-p}} q^m\right). \qquad (42)$$

Combining Equations (40) and (42) and assuming $m - p(\log_q n + 2k \log_q \log_q n) \to \infty$ (which we can assume in Theorem 4.1), we have $\#\mathcal{N}''' = o(c_f q^m)$. Before we prove Proposition 4.4, we first need a simpler bound, slightly generalizing [21, Proposition 6] and giving exact bounds.

Proposition 4.5. Suppose $k, l, n, m_p, m_1 \in \mathbb{N}$ such that $m_1 \geq m_p$. Suppose that $f \in \mathbb{F}_q[t][y_0, \ldots, y_l]$ is a polynomial such that $\deg_{y_i}(f) \leq k$ and $\deg_t(f) \leq n$, and f is not identically 0. Then

$$\#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f(y) = 0\} \leq k(l+1)q^{lm_p}.$$

Proof. We prove this proposition using induction. First we analyze the instance $l = 0$. This gives us the non vanishing polynomial $f(y_0)$ of degree at most k in y_0. This polynomial then has at most k roots in $\mathbb{F}_q[t]$. This means that $\#\{y \in (\mathbb{F}_q[t]^{<m_p})^{0+1} : f(y) = 0\} \leq k$. We conclude our proof for $l = 0$.

Assuming the proposition holds for $l-1$, we prove it must also hold for l. Let f be a polynomial in y_l, of degree at most k, with coefficients in $\mathbb{F}_q[t][y_0, \ldots, y_{l-1}]$. For simplicity, we denote this polynomial as $f(y', y_t)$, where $y' = (y_0, \ldots, y_{l-1})$. Suppose $f_0 \in \mathbb{F}_q[t][y_0, \ldots, y_{t-1}]$ is the leading coefficient of $f(y', y_t)$. Since f_0 also satisfies the degree requirements of Proposition 4.5, we find by induction

$$\#\{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} : f_0(y') = 0\} \leq klq^{(l-1)m_p}. \tag{43}$$

Furthermore, we know that every $y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1}$ with $f_0(y) \neq 0$, has at most $\deg_{y_l}(f) \leq k$ values of y_l in $\mathbb{F}_q[t]$ such that $f(y', y_l) = 0$. Therefore

$$\begin{aligned}\#\{(y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f_0(y') \neq 0, f(y', y_l) = 0\} &\leq k\#(\mathbb{F}_q[t]^{<m_p})^{l+1-1} \\ &= kq^{lm_p}.\end{aligned} \tag{44}$$

Combining (43) with (44), we end up with

$$\begin{aligned}&\#\{(y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f(y', y_l) = 0\} \\ &\leq \#\{(y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f_0(y') = 0\} \\ &+ \#\{(y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f_0(y') \neq 0, f(y', y_l) = 0\} \\ &= q^{m_p}\#\{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} : f_0(y') = 0\} \\ &+ \#\{(y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : f_0(y') \neq 0, f(y', y_l) = 0\} \\ &\leq q^{m_p}klq^{(l-1)m_p} + kq^{lm_p} = k(l+1)q^{lm_p}.\end{aligned}$$

□

In a similar fashion, we can show that:

Proposition 4.6. Suppose $k, l, n, m_p, m_1 \in \mathbb{N}$ such that $m_1 \geq m_p$. Suppose that $f \in \mathbb{F}_q[t][y_0, \ldots, y_l]$ is a polynomial such that $\deg_{y_i}(f) \leq k$ and $\deg_t(f) \leq n$. Let $P \in \mathcal{P}^{\geq m_1}$ be a large prime and suppose f is not identically 0 modulo P. Then

$$\mathcal{N}_l(f, P) = \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : P \mid f(y)\} \leq k(l+1)q^{lm_p}.$$

Remark. Observe that the assumption $m_1 \geq m_p$ is quite necessary in this proposition.In other words, each residue class modulo P has at most a single representative in $\mathbb{F}_q[t]^{<m_p}$.

We are now in a position to prove Proposition 4.4.

Proof of Proposition 4.4. We prove this proposition using induction. First we analyze the instance $l = -1$, to avoid repetition. Let f, g be polynomials in $\mathbb{F}_q[t]$, and observe that $(\mathbb{F}_q[t]^{<m_p})^{-1+1} = \{()\}$ is a unit set containing only the

empty tuple. Since we assumed f and g to be coprime, we know there does not exist a $P \in \mathcal{P}$ such that P divides both f and g. Therefore the set

$$\{y \in (\mathbb{F}_q[t]^{<m_p})^{-1+1} = \{()\} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid f(y) \text{ and } P \mid g(y)\}$$

is empty. Therefore $\mathcal{N}_l(f,g) = 0$. Since this also satisfies $O_k\left(\frac{n+m_1}{m_1} q^{-m_p}\right)$, we conclude our proof for $l = -1$.

Assuming the proposition holds for $l-1$, we prove it must also hold for l. We write $A_l = \mathbb{F}_q[t, y_0, \ldots, y_{l-1}]$. Let polynomials f and g be in $A_l[y_t]$, and suppose have only one variable, which is in y_l, with coefficients in the polynomial ring A_l. Suppose that $f_C, g_C \in A_l$ are their respective contents. This allows us to rewrite $f = f_C f_I$ and $g = g_C g_I$ (see Definition **??**). Then f_I and g_I are primitive polynomials in $A_l[y_l]$ and indivisible by any non-scalar polynomial in A_l. Since f and g are coprime, we also know that f_C and f_I are coprime to g_C and g_I. Also since we assumed f and g to have $\deg_{y_i}(f), \deg_{y_i}(g) \leq k$ and $\deg_t(f), \deg_t(g) \leq n$, we know all four polynomials f_C, f_I, g_C and g_I also have $\deg_{y_i} \leq k$ and $\deg_t \leq n$. Note that we can decompose

$$\mathcal{N}_l(f,g) \leq \mathcal{N}_l(f_I, g_I) + \mathcal{N}_l(f_I, g_C) + \mathcal{N}_l(g_I, f_C) + \mathcal{N}_l(f_C, g_C).$$

Remark. We can use the $\leq$ sign here, since there might be $y \in (\mathbb{F}_q[t]^{<m_p})^{l+1}$ that occur in more than one of the right hand terms.

This simplifies the process of finding the bound for $\mathcal{N}_l(f_C, g_C)$. Proving that the individual terms on the right are bounded by $O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right)$ suffices.

The term $\mathcal{N}_l(f_C, g_C)$. We defined f_C and g_C to be independent of y_l. Assuming the proposition is correct for $l-1$, results in

$$\begin{aligned}\mathcal{N}_l(f_C, g_C) = q^{m_p}\mathcal{N}_{l-1}(f_C, g_C) &= q^{m_p} O_{l-1,k}\left(\frac{n+m_1}{m_1} q^{(l-1)m_p}\right) \\ &= O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right).\end{aligned}$$

The terms $\mathcal{N}_l(f_C, g_I), \mathcal{N}_l(f_I, g_C)$ and $\mathcal{N}_l(f_I, g_I)$. For the terms $\mathcal{N}_l(f_C, g_I), \mathcal{N}_l(f_C, g_I)$, we have one polynomial in A_l and the another polynomial indivisible by any polynomial in A_l. We wish to bound $\mathcal{N}_l(f_I, g_I)$ by a term of this form as well.

Suppose $R = \mathrm{Res}_{y_l}(f_I, g_I) \in A_l$ be the resultant of f_I, g_I. Since f_I and g_I are coprime, we know that R is non-zero. Also by definition, if for $y_i \in \mathbb{F}_q[t]$ and $P \in \mathcal{P}$, we have $P \mid f_I(y)$ and $P \mid g_I(y)$, then this implies that $P \mid R(y)$. This gives us $\mathcal{N}_l(f_I, g_I) \leq \mathcal{N}_l(f_I, R)$. Also, since $\deg_{y_l}(f_I)$ and $\deg_{y_l}(g_I) \leq k$, we know that R can be written as a polynomial of degree $\leq 2k$ in the A_l coefficients of f_I, g_I. This in turn implies that $\deg_t(R) \leq 2kn$ and $\deg_{y_i}(R) \leq 2k^2$.

Lemma 4.4. Suppose $R \in A_l$ and $f \in A_l[y_l]$ such that f is indivisible by all non-scalar polynomials in A_l. Furthermore, let $\deg_t f \leq n, \deg_{y_i} f \leq k, \deg_t R \leq 2kn$ and $\deg_{y_i} R \leq 2k^2$. Let $\mathcal{N}_l(f, P)$ be defined as in Proposition 4.6. We have

$$\mathcal{N}_l(f, R) = O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right).$$

Remark. Note that we could then use this bound for $\mathcal{N}_l(f_I, g_C), \mathcal{N}_l(g_I, f_C)$ and $\mathcal{N}_l(f_I, g_I)$.

Proof of Lemma 4.4. Rewrite $R = \prod_{j\in J} R_j$. That is, we decompose R into its irreducible factors R_j. We have $\mathcal{N}_l(f, R) \leq \sum_{j\in J} \mathcal{N}_l(f, R_j)$. Again, we have the $\leq$ sign since some elements may in more than one term. Since all irreducible factors of R are in A_l, we have $R_j \nmid f$ and that f and R_j are coprime for all $j \in J$. Suppose now we decompose J into $J = J_1 \cup J_2 \cup J_3$, which splits the indices of the irreducible factors such that

$$\begin{aligned} J_1 &= \{j \in J : R_j \notin \mathbb{F}_q[t]\} \\ J_2 &= \{j \in J : R_j \in \mathbb{F}_q[t]^{\geq m_1}\} \\ J_3 &= \{j \in J : R_j \in \mathbb{F}_q[t]^{<m_1}\}. \end{aligned}$$

Recall that $\deg_t R \leq 2kn$ and that $\deg_{y_i}(R) \leq 2k^2 l$. Therefore, the number of elements in J_1 and J_2 is $\#J_1 \leq 2k^2 l$ and $\#J_2 \leq \frac{2kn}{m_1}$.

We focus on J_1 first. Suppose $f_0 \in A_l$ is some coefficient of f (as a polynomial in y_l) for which $R_j \nmid f_0$, for every $j \not\in J_1$. Since $R_j \nmid f$, we know that this coefficient exists. Now we turn to J_3. Note that every $j \in J_3$ and $y \in (\mathbb{F}_q[t]^{<m_p})^{l+1}$, we can write $R_j(y) = R_j$. This means that there exists no $P \in \mathcal{P}^{\geq m_1}$ such that $P \mid R_j$, i.e., $\mathcal{N}_l(f, R_j) = 0$. If now we turn to J_2, we observe that for every $j \in J_2$, we consider only primes P with $\deg P \geq m_1$. We therefore comply with all assumptions from Proposition 4.6 for f and $P = R_j$. This gives us $\mathcal{N}_l(f, R_j) \leq k(l+1)q^{lm_p} = O_{l,k}(q^{lm_p})$. We are now in a position to rewrite $\mathcal{N}_l(f, R_j)$ into terms, using the decomposition of J:

$$\begin{aligned} \mathcal{N}_l(f, R_j) &= \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid f(y) \text{ and } P \mid R_j(y)\} \\ &\leq \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : R_j(y) = 0\} \\ &+ \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : \exists P \in \mathcal{P}^{\geq m_1}, P \mid f_0(y) \text{ and } P \mid R_j(y)\} \\ &+ \#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : R_j(y) \neq 0, \exists P \in \mathcal{P}^{\geq m_1}, P \mid R_j(y), P \mid f(y) \text{ and } P \nmid f_0(y)\}. \end{aligned}$$

Since $\deg R_j \leq k$, we know that $\#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : R_j(y) = 0\} \leq k(l+1)q^{lm_p} = O_{l,k}(q^{lm_p})$. The second term equals $\mathcal{N}_l(f_0, R_j)$. Since we defined R_j to be irreducible, this means f_0, R_j are coprime. In order to be able to use Proposition 4.4, we need to check that all those assumptions are met. We have $\deg_{y_i}(f_0)$ and $\deg_{y_i}(R_i) \leq 2k^2$, and $\deg_t(f_0)$ and $\deg_t(R_j) \leq 2kn$.

Therefore we are allowed to use the proposition, and assuming this was correct for $l-1$, we have

$$\begin{aligned} \mathcal{N}_l(f_0, R_j) = q^{m_p}\mathcal{N}_{l-1}(f_0, R_j) &= q^{m_p} O_{l-1,2k^2}\left(\frac{2kn + m_1}{m_1} q^{(l-1)m_p}\right) \\ &= O_{l,k}\left(\frac{n + m_1}{m_1} q^{lm_p}\right) \end{aligned} \tag{45}$$

This leaves only the final summand. Suppose we write $y = (y', y_l) \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} \times (\mathbb{F}_q[t]^{<m_p})^{0+1} = (\mathbb{F}_q[t]^{<m_p})^{l+1}$. If for y, we have $R_j(y) = R_j(y') \neq 0$, this implies that $\deg_t(R_j(y')) \leq 2kn = 2k^2 l m_p$. Suppose we write

$\mathcal{P}_{y'} = \{P \in \mathcal{P}^{\geq m_1} : P \mid R_j(y'), P \nmid f_0(y')\}$, then

$$\#\mathcal{P}_{y'} \leq \frac{2kn + 2k^2 l m_p}{m_1} = O_{l,k}\left(\frac{n+m_1}{m_1}\right).$$

However, for each $y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1}$ and $P \in \mathcal{P}_{y'}$, we have that $f(y', y_l)$ is a polynomial of degree $\leq k$ in y_l. We know that this polynomial is non-vanishing mod P. Recalling that $\deg_t(P) \geq m_1 \geq m_p$, we then have $\#\{y_l \in (\mathbb{F}_q[t]^{<m_p})^{0+1} : P \mid f(y', y_l)\} \leq k$. Concluding

$$\begin{aligned}
&\#\{y \in (\mathbb{F}_q[t]^{<m_p})^{l+1} : R_j(y) \neq 0, \exists P \in \mathcal{P}^{\geq m_1}, P \mid R_j(y), P \mid f(y) \text{ and } P \nmid f_0(y)\} \\
&= \sum_{\substack{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} \\ R_j(y') \neq 0}} \#\{y_l \in B_0 : \exists P \in \mathcal{P}^{\geq m_1}, P \mid R_j(y'), P \mid f(y', y_l) \text{ and } P \nmid f_0(y')\} \\
&\leq \sum_{\substack{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} \\ R_j(y') \neq 0}} \sum_{P \in \mathcal{P}_{y'}} \#\{y_l \in B_0 : P \mid f(y', y_l)\} \leq \sum_{\substack{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} \\ R_j(y') \neq 0}} \sum_{P \in \mathcal{P}_{y'}} k \\
&= \sum_{\substack{y' \in (\mathbb{F}_q[t]^{<m_p})^{l+1-1} \\ R_j(y') \neq 0}} O_{l,k}\left(\frac{n+m_1}{m_1}\right) = O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right).
\end{aligned}$$

We now see that $\mathcal{N}_l(f, R_j) = O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right)$ for all $j \in J_1$. □

As mentioned before, this puts us in a position to find the final bound on $\mathcal{N}_l(f, g)$ and thus prove the theorem:

$$\begin{aligned}
\mathcal{N}_l(f, g) &\leq \sum_{j \in J_1} \mathcal{N}(f, R_j) + \sum_{j \in J_2} \mathcal{N}(f, R_j) + \sum_{j \in J_3} \mathcal{N}(f, R_j) \\
&\sum_{j \in J_1} O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right) + \sum_{j \in J_2} O_{l,k}\left(q^{lm_p}\right) + \sum_{j \in J_3} 0 \\
&\leq 2k^2 l \cdot O_{l,k}\left(\frac{n+m1+}{m_1} q^{lm_p}\right) + \frac{2kn}{m_1} \cdot O_{l,k}\left(q^{lm_p}\right) \\
&= O_{l,k}\left(\frac{n+m_1}{m_1} q^{lm_p}\right).
\end{aligned}$$

□

Remark. Note that while this error term was the most difficult to calculate, it actually contributes the smallest error.

4.2 Proof of Theorems 4.2 and 4.3.

Having proved Theorem 4.1 allows to explicitly prove Theorem 4.2 and 4.3. These proofs follow in this section.

Proof of Theorem 4.2. Introduce a function $f(x) = g(t, N(t) + x) \in \mathbb{F}_q[t][x]$. As was one of the assumptions, $\deg_x f = k$, therefore $\deg_x g = k$. For another assumption, $\deg N(t) = n$, therefore $\deg_t f \leq \deg_x g \cdot \deg_t N + \deg_t g = kn + \deg_t g = O(n)$. Since we get f from g by a fixed $\mathbb{F}_q[t]$ translation of the x variable,

g being square-free implies that f is square-free. Consequently, we have $\rho_f(D) = \rho_g(D) = \rho(D)$ for any polynomial D. Note that since the singular sum S and its tail $S(m_0)$ depend on P^2 and $\rho(P^2)$ only, we see both $S_f(m_0) = S_g(m_0)$ and $S_f = S_g$. Also, since the density is independent of the choice for $N(t)$ or its degree n, we have for f and g that $c_f = c_g$. In order to let $S_f(m_0)$ and $S_g(m_0)$ equal $o(1) = o(c_f)$, the only need to let $m_0 \to \infty, r \to \infty$. Similar to the argument used in 4.1.2 and 4.1.3, this in turn results in $\#\mathcal{N}' = c_f q^m + o(c_f q^m)$ and $\#\mathcal{N}'' = o(c_f q^m)$. The restriction our choice of r, m_0, leaves is that we must have $m \to \infty$. Finally, we need to analyze our bound $\mathcal{N}'''$. As c_f is now a constant, (41) implies that $\#\mathcal{N}''' = o(1) = o(c_f)$ when $\frac{mq^{m/p}}{n} \to \infty$, which is equivalent to $m - p(\log_q n \log_q \log_q n) \to \infty$, as we required in the theorem's statement. Note that this is the first time that n plays a role, as it still affects the relevant degrees. □

Proof of Theorem 4.3. We use an analogues approach as the one used in the proof of Theorem 4.2. Introduce a function $f(x) = g(t, N(t) + x) \in \mathbb{F}_q[t][x]$. Again, note that since the singular sum S and its tail $S(m_0)$ depend on P^2 and $\rho(P^2)$ only, we see both $S_f(m_0) = S_g(m_0)$ and $S_f = S_g$. Also, since the density is independent of the choice for $N(t)$ or its degree n, we have for f and g that $c_f = c_g$. Because of the independence of $S, S_f(m_0)$ and c_f on n, we may replace this n by any other of our choosing. For the same reason, the arguments used for finding the bounds on $\mathcal{N}''$ and $\mathcal{N}'$ hold for any choice of n. Our only restraint is that we have $r, m_0 \to \infty$ with $m_0 \gg \log_q n_1, r \gg \log_q \log_q n_1$ and $2m_0 r \leq m$. Note that this need not be a problem since we assumed $m \gg \log_q n_1 \log_q \log_q n_1$. Again, the only part that depends on our choice of n is the bound of $\#\mathcal{N}'''$. Note that $\deg_t f \leq kn_2 + n_1$ (n_2 being $\deg_t N$). Suppose $n_2 \ll n_1$, this results in $\deg_t f \leq \deg_x g \cdot \deg_t N + \deg_t g \ll n_1$ which is quite similar to our situation in Theorem 4.1. Note that we proved the effect of $\mathcal{N}'''$ on the total bound was quite slim. Alternatively, suppose $n_2 \gg n_1$. Then, using a similar reasoning, we have $\deg_t f \ll n_2$. Then (41) holds with the degree n replaced by n_2. Combining this with (40) where we let n_1 take the place of n, we need $\frac{mq^{m/p}}{n_2 \log_q n_1)}^{2k} \to \infty$ to end up with $\#N^m = o(c_f q^m)$. Note that the restriction $\frac{mq^{m/p}}{n_2 \log_q n_1)}^{2k} \to \infty$ is essentially stating $m - p(\log_q n_2 - \log_q \log_q n_2 + 2k \log_q \log_q n_1) \to \infty$, as is the restriction in the theorem. □

References

[1] M.R. Murthy A.C. Cojocaru. *An Introduction to Sieve Methods and their Applications*. Cambridge University Press, 2005.

[2] T. M. Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag Berlin Heidelberg, 1976. doi: 10.1007/978-3-662-28579-4.

[3] J. Aron. *Mathematicians left baffled after three-year struggle over proof. New Scientist*, 2015.

[4] L. Bary-Soroker. *Prime Tuples in Function Fields*. 2016. doi: 10.14760/SNAP-2016-010-EN.

[5] J. R. Bastida and R. Lyndon. *Field Extensions and Galois Theory*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1984. doi: 10.1017/CBO9781107340749.

[6] D. Carmon. *On Square-free Values of Large Polynomials over the Rational Function Field*. 2016. doi: arXiv:1605.07765[Math.NT].

[7] P.L. Clark. *Sums Of Two Squares, Lecture Notes*. University of Georgie, Department of Mathematics, 2009.

[8] K. Conrad. *Separability*. University of Connecticut, Department of Mathematics, 2014.

[9] K. Conrad. *Hensel's Lemma*. University of Connecticut, Department of Mathematics, 2016.

[10] K. Conrad. *The Chinese Remainder Theorem, Lecture Notes*. University of Connecticut, Department of Mathematics, 2017.

[11] K. Conrad. *Finite Fields*. University of Connecticut, Department of Mathematics, 2018.

[12] J. Elliot. *Ring structures on groups of arithmetic functions*. 2008. doi: 10.1016/j.jnt.2007.07.011.

[13] P. Erdös. *Arithmetical properties of polynomials*. J. London Math. Soc., 28:416–425, 1953.

[14] T. Estermann. *Einige Sätze über quadratfreie Zahlen*. Math. Ann., 105: 653–662, 1931.

[15] K. Hicks G. Effinger and G. L. Mullen. *Integers and polynomials: Comparing the close cousins* $\mathbb{Z}$ *and* $\mathbb{F}_q[x]$. Mathematical Intelligencer(2):28–33, 2005.

[16] J.A. Gallian. *Contemporary Abstract Algebra*. Houghton - Mifflin, 2002.

[17] A. Granville. *ABC allows us to count square-frees*. Internat. Math. Res. Notices, 19:991–1009, 1998.

[18] C. Hooley. *A Note on Square-Free Numbers in Arithmetic Progressions*. doi: 10.1112/blms/7.2.133.

[19] C. Hooley. *Applications of Sieve Methods to the Theory of Numbers*, volume 70 of *Cambridge Tracts in Mathematics*. Cambridge University Press, 1976.

[20] A. V. Zelevinsky I. M. Gelfand, M. M. Kapranov. *Discriminants, Resultants, and Multidimensional Determinants*. doi: 10.1007/978-0-8176-4771-1.

[21] G. Lando. *Square-free values of polynomials evaluated at primes over a function field. Q. J. Math. 66*, pages 205–224, 2015.

[22] R. Lidl and H. Niederreiter. *Finite Fields*. Cambridge Univ. Press, 1997.

[23] F. Lorenz and S. Levy. *Algebra: Volume I: Fields and Galois Theory.* Universitext. Springer New York, 2006. ISBN 9780387316086.

[24] R.P. Schneider M. Jameson. *Combinatorial Applications of Möbius Inversion.* ArXiv e-prints:1302.5744, 2013. doi: 10.1090/S0002-9939-2014-12020-X.

[25] J. Maynard. *Small gaps between primes.* ArXiv e-prints:1311.4600, 2013.

[26] R. G. Pinsky. *Problems from the Discrete to the Continuous.* Springer International Publishing, 2014. doi: 10.1007/978-3-319-07965-3.

[27] B. Poonen. *Square-free values of multivariable polynomials. Duke Math. J.*, 118:353–373, 2003.

[28] K. Ramsay. *Square-free values of polynomials in one variable over function fields. Int. Math. Res. Not. 4*, pages 225–234, 1992.

[29] T. Reuss. *Power-Free values of Polynomials.* Bull. London Math. Soc., 14: 21–26, 2015. doi: 10.1112/blms/bdul16.arXiv:1307.2802[Math.NT].

[30] P. Ribenboim. *The New Book of Prime Numbers.* Springer-Verlag, 1995.

[31] G. Ricci. *Ricerche arithmetische sui polinomi.* Rend. Circ. Mat. Palermo, 57:433–475, 1933.

[32] Z. Rudnick. *Square-free values of polynomials over the rational function field. Journal of Number Theory 135*, pages 60–66, 2014.

[33] Z. Rudnick. *Square-free Values of Polynomials over $\mathbb{F}_q[t]$, Course Notes.* School of Mathematical Sciences, Tel Aviv, 2015.

[34] Z. Rudnick. *Squarefree values of quadratic polynomials, Course Notes.* School of Mathematical Sciences, Tel Aviv, 2015.

[35] T Tao. *Erdos' Divisor Bound.* University of California - Los Angeles, 2011.

[36] D. Tolev. On the distribution of r-tuples of squarefree numbers in short intervals. *Int. J. Number Theory 2*, pages 225–234, 2006.