Topics in divisibility: pairwise coprimality, the GCD of shifted sets and polynomial irreducibility

Randell Heyman

A dissertation submitted in fulfilment
of the requirements for the degree of
Doctor of Philosophy

The School of Mathematics and Statistics
The University of New South Wales

31 July 2015

Originality Statement

I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published or written by another person, or substantial proportions of material which have been accepted for the award of any other degree or diploma at UNSW or any other educational institution, except where due acknowledgement is made in the thesis. Any contribution made to the research by others, with whom I have worked at UNSW or elsewhere, is explicitly acknowledged in the thesis. I also declare that the intellectual content of this thesis is the product of my own work, except to the extent that assistance from others in the project's design and conception or in style, presentation and linguistic expression is acknowledged.

Signed Randell Heyman
Date 31 July 2015

Copyright Statement

Signed Randell Heyman
Date 31 July 2015

Authenticity Statement

I certify that the Library deposit digital copy is a direct equivalent of the final officially approved version of my thesis. No emendation of content has occurred and if there are any minor variations in formatting, they are the result of the conversion to digital format.

Signed Randell Heyman
Date 31 July 2015

Acknowledgements

I thank Professor Igor Shparlinski for his help and support. He has suggested many interesting mathematical questions for me to pursue. He has freely given his time, knowledge and experience. I feel very fortunate to have had such supervision.

I thank my co-supervisor, Professor Michael Cowling, who was also my honours supervisor, for his support over many years.

I thank various anonymous referees for their comments on journal submissions. Many of their comments have been incorporated in this thesis.

I thank my mother, Shirley, for her enthusiasm for education.

Finally, I thank my wife Hilary, daughter Carly and son Jay for their enduring love and support.

Abstract

By 3,000 B.C. there is evidence of the use of divisibility in Egypt and Mesopotamia, see for example [58]. Divisibility naturally led to the concepts of primality, common divisors and eventually, polynomial irreducibility. In this thesis, we explore some modern results regarding these three concepts.

In Chapter 2, we explore pairwise coprimality and pairwise non-coprimality. Given a subset A of the set $\{1,\ldots,k\}^2$ we say that $(a_1,\ldots,a_k) \in \mathbb{Z}^k$ exhibits *pairwise coprimality over A* if $\gcd(a_i,a_j) = 1$ for all $(i,j) \in A$. When the set A is obvious we might just say that $(a_1,\ldots,a_k)$ exhibits *pairwise coprimality.* We say that $(a_1,\ldots,a_k)$ is *totally pairwise coprime* if $\gcd(a_i,a_j) = 1$ for all $1 \leq i < j \leq k$. We say that $(a_1,\ldots,a_k)$ is *pairwise non-coprime* if $\gcd(a_i,a_j) \neq 1$ for all $1 \leq i < j \leq k$. Pairwise coprimality has a long history. It is a requirement of the Chinese remainder theorem whose proof has been known for at least 750 years (see [58, p. 131–132]). The Chinese remainder theorem is important in many areas of modern day mathematics. Some applications in modular multiplication, bridging computations, coding theory and cryptography can be found in [22, p. 33–184] and some comments regarding modular multiplication applications can be found in [59, p. 287–290]. To date pairwise coprimality calculations have also been necessary for quantifying k-tuples that are pairwise non-coprime (see [51], [43] and [70] and its comments regarding [32]).

We start Chapter 2 by giving pairwise primality results for triples and show that the methods are not generally suitable for larger tuples. We then use more advanced techniques to give general results for larger tuples. This leads to results for tuples of polynomials over finite fields that exhibit pairwise coprimality. We finish the chapter with a brief discussion regarding tuples with both pairwise coprime and pairwise non-coprime conditions.

In Chapter 3, we study the greatest common divisor of shifted sets. Our main result is a dual problem to the approximate common divisor problem which has applications in cryptography. Given a set of k positive integers $\{a_1,\ldots,a_k\}$ and an integer parameter H, we study the greatest common divisor of small additive shifts of its elements by integers h_i with $|h_i| \leq H$, $i = 1,\ldots,k$. In particular, we show that for any choice of $a_1,\ldots,a_k$ there are shifts of this type for which the greatest common divisor of $a_1+h_1,\ldots,a_k+h_k$ is much larger than H. We end the chapter with some related results.

In Chapter 4, we consider integer coefficient polynomial irreducibility. Some of the analysis could be the basis for further results for polynomials with rational coefficients, due to Gauss's lemma [36, Article 42]. It is well known that almost all polynomials in rather general families of $\mathbb{Z}[x]$ are irreducible, see [1, 20, 84] and references therein. There are also known polynomial time irreducibility tests and polynomial time factoring algorithms, see for example [60]. However, it is always interesting to study large classes of polynomials that are known to be irreducible.

In Section 4.1, we study the number of polynomials of bounded height that are irreducible by the Eisenstein criterion. In Section 4.2 we study the number of polynomials of bounded height that are irreducible by the Eisenstein criterion after the additive shift of a variable. In Section 4.3 we consider the Dumas criterion; in this context a generalisation of the Eisenstein criterion. Our main results in this section are estimates of the number of polynomials of bounded height that are irreducible due to the Dumas criterion. Finally, in Section 4.4, we give various enumerations of the number of irreducible binomials in finite fields.

Contents

Chapter 1

Notation

We indicate below notation that is common to chapters in this thesis.

For any integer $s \geq 1$, we denote by $\omega(s)$, $\varphi(s)$ and $\tau(s)$ the number of distinct prime factors, the Euler totient function and the number of divisors of s respectively (we also set $\omega(1) = 0$). We also use μ to denote the Möbius function, that is

$$\mu(s) = \begin{cases} (-1)^{\omega(s)} & \text{if } s \text{ is square free,} \\ 0 & \text{otherwise.} \end{cases}$$

As usual, the Riemann zeta function is given by

$$\zeta(s) = \sum_{j=1}^{\infty} \frac{1}{j^s},$$

for all complex numbers s whose real part is greater than 1.

We recall that the notation $f(x) = O(g(x))$ or $f(x) \ll g(x)$ is equivalent to the assertion that there exists a constant $c > 0$ such that $|f(x)| \leq c|g(x)|$ for large enough x. The notation $f(x) = o(g(x))$ is equivalent to the assertion that

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

The notation $f(x) \sim g(x)$ is equivalent to the assertion that

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1.$$

We use p, with or without subscript, to denote a prime number and q, with or without subscript, to denote a prime power (that is, $q = p^r$ for some positive integer r).

Finally, we use $|A|$ to denote the cardinality of a set A.

Chapter 2

Pairwise coprimality

2.1 Pairwise non-coprimality of triples

2.1.1 Introduction

Let a_1, a_2, a_3 be positive integers less than H. We obtain an asymptotic formula for the number of (a_1, a_2, a_3) that are pairwise non-coprime. We do this by estimating the number of triples that possess certain pairwise coprimality conditions and applying the inclusion-exclusion principle. The density of pairwise non-coprime positive integer triples is approximately 17.4%. We also give an upper bound on the error term in an asymptotic formula for $\sum_{n=1}^{H}(\varphi(n)/n)^m$ for $m \geq 2$ and as $H \to \infty$.

The result regarding the density of pairs of coprime positive integers is generally ascribed to E. Cesáro, although J. J. Sylvester and P. D. L. Dirichlet also contributed to the result (for a recent comment see [66, page 1320]). A proof of the result is given in [41, Theorem 332]). More formally, if

$$C(H) = \sum_{\substack{1 \leq a_1, a_2 \leq H \\ \gcd(a_1, a_2) = 1}} 1, \quad P(H) = \sum_{1 \leq a_1, a_2 \leq H} 1 = H^2,$$

then

$$\lim_{H \to \infty} \frac{C(H)}{P(H)} = \frac{6}{\pi^2}.$$

Nymann [72] gave the following result.

$$\sum_{\substack{1 \leq a_1, \ldots, a_k \leq H \\ \gcd(a_1, \ldots, a_k) = 1}} 1 = \frac{H^k}{\zeta(k)} + \begin{cases} O(H \log H) & \text{if } k = 2, \\ O\left(H^{k-1}\right) & \text{if } k \geq 3. \end{cases} \tag{2.1}$$

This naturally leads to the enumeration of tuples with pairwise coprimality.

Tóth [81] showed that for each integer $k \geq 2$

$$\sum_{\substack{1 \leq a_1, \ldots, a_k \leq H \\ \gcd(a_i, a_j) = 1 \\ i \neq j}} 1 = \vartheta(k) H^k + O(H^{k-1} (\log H)^{k-1}), \tag{2.2}$$

where

$$\vartheta(k) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{k-1} \left(1 + \frac{k-1}{p}\right). \tag{2.3}$$

In this section we enumerate the number of triples of maximum height H that are pairwise non-coprime. Let

$$\mathcal{N}_k(H) = \sum_{\substack{1 \leq a_1, \ldots, a_k \leq H \\ \gcd(a_i, a_j) \neq 1 \\ 1 \leq i < j \leq k}} 1.$$

Our main result is the following.

Theorem 2.1.1. *Suppose H is a positive integer. We have*

$$\mathcal{N}_3(H) = \rho H^3 + O\left(H^2 (\log H)^2\right),$$

where

$$\rho = 1 - \frac{3}{\zeta(2)} + 3 \prod_{p \text{ prime}} \left(1 - \frac{2p-1}{p^3}\right) - \prod_{p \text{ prime}} \left(1 - \frac{3p-2}{p^3}\right).$$

The three products (where $\zeta(2)$ can, of course, be expressed as a product over primes) are easily checked against the more general Theorem 2.2.1 in the next section. According to Moree [70, Page 9], Freiberg [32] also gives a result for the density of triples of positive integers that are pairwise non-coprime.

For the remainder of this section we will ease notation in summations by using (a, b) to indicate the greatest common divisor of integers a and b.

2.1.2 Preparatory Lemma

Kac [57] attributes to I. Schur the following result. For $m \geq 2$,

$$\lim_{H \to \infty} \frac{1}{H} \sum_{n=1}^{H} \left(\frac{\varphi(n)}{n}\right)^m = \prod_{p \text{ prime}} \left(1 + \frac{(1 - 1/p)^m - 1}{p}\right).$$

For Theorem 2.1.1 we require an upper bound on the error term in an asymptotic formula for

$$\sum_{n=1}^{H} \left(\frac{\varphi(n)}{n}\right)^2.$$

An upper bound on the error term in the general case is known (see [12]) and it has since been improved using analytic tools (see, for example, [7], [62]). We provide a different elementary proof to that of [12].

Lemma 2.1.2. *Let $m \geq 2$. We have*

$$\sum_{n=1}^{H} \left(\frac{\varphi(n)}{n}\right)^m = H \prod_{p \text{ prime}} \left(1 + \frac{(1-1/p)^m - 1}{p}\right) + O\left((\log H)^m\right).$$

Proof. Let $m \geq 2$. Then

$$\begin{aligned}\sum_{n=1}^{H} \left(\frac{\varphi(n)}{n}\right)^m &= \sum_{n=1}^{H} \prod_{p|n} (1-1/p)^m \\ &= \sum_{n=1}^{H} \prod_{p|n} (1+f(p)), \qquad (2.4)\end{aligned}$$

where

$$f(n) = \begin{cases} \prod_{p|n} \left((1-1/p)^m - 1\right) & \text{if } n \text{ is square free,} \\ 0 & \text{otherwise.} \end{cases}$$

We will freely use the fact that

$$|f(n)| \leq \prod_{p|n} \frac{m}{p} = \frac{m^{\omega(n)}}{n}.$$

Returning to (2.4) we have

$$\begin{aligned}\sum_{n=1}^{H} \left(\frac{\varphi(n)}{n}\right)^m &= \sum_{n=1}^{H} \sum_{d|n} f(d) \\ &= \sum_{d \leq H} f(d) \left(\frac{H}{d} + O(1)\right) \\ &= H \sum_{d \leq H} \frac{f(d)}{d} + O\left(\sum_{d \leq H} |f(d)|\right). \qquad (2.5)\end{aligned}$$

For the error term in (2.5) we note from [80, III.3 Theorem 6] that

$$\sum_{l=1}^{H} m^{\omega(l)} = O\left(H(\log H)^{m-1}\right). \qquad (2.6)$$

Using (2.6) and partial summation the error term in (2.5) can given by

$$\sum_{d \leq H} |f(d)| = O\left((\log H)^m\right). \qquad (2.7)$$

For the main term in (2.5) we observe that

$$\sum_{d\leq\infty} \frac{f(d)}{d}$$

is absolutely convergent since

$$\sum_{d>H} \left|\frac{f(d)}{d}\right| \leq \sum_{d>H} \frac{m^{\omega(d)}}{d^2} \leq \sum_{d>H} \frac{d^{o(1)}}{d^2} \leq \sum_{d>H} \frac{1}{d^{2+o(1)}} = H^{-1+o(1)}.$$

Thus

$$\begin{aligned}\sum_{d\leq H} \frac{f(d)}{d} &= \sum_{d<\infty} \frac{f(d)}{d} - \sum_{d>H} \frac{f(d)}{d} \\ &= \prod_{p \text{ prime}} \left(1 + \frac{f(p)}{p}\right) + O\left(H^{-1+o(1)}\right) \\ &= \prod_{p \text{ prime}} \left(1 + \frac{(1-1/p)^m - 1}{p}\right) + O\left(H^{-1+o(1)}\right). \qquad (2.8)\end{aligned}$$

Combining (2.5), (2.7) and (2.8) completes the proof. □

2.1.3 Proof of Theorem 2.1.1

It is clear that

$$\mathcal{N}_3(H) = H^3 - \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_i,a_j)=1 \\ \text{for some } 1\leq i<j\leq 3}} 1.$$

Then, using the inclusion-exclusion principle, we have

$$\begin{aligned}\sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_i,a_j)=1 \\ \text{for some } 1\leq i<j\leq 3}} 1 = &\sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ 1\leq i<j\leq 3}} \sum_{(a_i,a_j)=1} 1 - \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ 1\leq i<j<k\leq 3}} \sum_{\substack{(a_i,a_j)=1 \\ (a_j,a_k)=1}} 1 \\ &+ \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_1,a_2)=1 \\ (a_1,a_3)=1 \\ (a_2,a_3)=1}} 1.\end{aligned}$$

Using symmetry, we obtain

$$\mathcal{N}_3(H) = H^3 - 3 \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_1,a_2)=1}} 1 + 3 \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_1,a_2)=1 \\ (a_1,a_3)=1}} 1 - \sum_{\substack{1\leq a_1,a_2,a_3\leq H \\ (a_1,a_2)=1 \\ (a_1,a_3)=1 \\ (a_2,a_3)=1}} 1. \qquad (2.9)$$

Using (2.1), the first summation of (2.9) is given by

$$\sum_{\substack{1\le a_1,a_2,a_3\le H\\ (a_1,a_2)=1}} 1 = \frac{H^3}{\zeta(2)} + O\left(H^2\log H\right). \tag{2.10}$$

Using (2.2), the third summation of (2.9) is given by

$$\sum_{\substack{1\le a_1,a_2,a_3\le H\\ (a_1,a_2)=1\\ (a_1,a_3)=1\\ (a_2,a_3)=1}} 1 = \vartheta(3)H^3 + O\left(H^2(\log H)^2\right), \tag{2.11}$$

where $\vartheta(3)$ is calculated using (2.3).

It remains to express the middle summation of (2.9) as a multiple of H^3 and a suitable error term. If we let

$$\varphi(n,H) = \sum_{\substack{1\le a\le H\\ (a,n)=1}} 1, \tag{2.12}$$

then we have

$$\begin{aligned}\sum_{\substack{1\le a_1,a_2,a_3\le H\\ (a_1,a_2)=1\\ (a_1,a_3)=1}} 1 &= \sum_{1\le n\le H}\ \sum_{\substack{1\le a_2,a_3\le H\\ (n,a_2)=1\\ (n,a_3)=1}} 1 = \sum_{1\le n\le H}\ \sum_{\substack{1\le a_3\le H\\ (n,a_3)=1}} 1 \sum_{\substack{1\le a_2\le H\\ (n,a_2)=1}} 1\\ &= \sum_{1\le n\le H} \varphi(n,H)^2. \end{aligned}\tag{2.13}$$

The following is well-known (or see [44, Lemma 4]).

$$\varphi(n,H) = \frac{H\varphi(n)}{n} + O\left(2^{\omega(n)}\right).$$

Substituting into (2.13) we have

$$\begin{aligned}\sum_{\substack{1\le a_1,a_2,a_3\le H\\ (a_1,a_2)=1\\ (a_1,a_3)=1}} 1 &= \sum_{1\le n\le H}\left(\frac{H\varphi(n)}{n} + O\left(2^{\omega(n)}\right)\right)^2\\ &= H^2\sum_{1\le n\le H}\left(\frac{\varphi(n)}{n}\right)^2 + O\left(H\sum_{1\le n\le H}\frac{\varphi(n)2^{\omega(n)}}{n}\right)\\ &\quad + O\left(\sum_{1\le n\le H}\left(2^{\omega(n)}\right)^2\right). \end{aligned}\tag{2.14}$$

Appealing to (2.6) we have

$$O\left(\sum_{1\le n\le H}\frac{\varphi(n)2^{\omega(n)}}{n}\right)=O\left(\sum_{1\le n\le H}2^{\omega(n)}\right)=O\left(H\log H\right), \tag{2.15}$$

and also

$$\sum_{1\le n\le H}\left(2^{\omega(n)}\right)^2=O\left(H\left(\log H\right)^3\right). \tag{2.16}$$

Substituting equations (2.15) and (2.16) into (2.14) yields

$$\sum_{\substack{1\le a_1,a_2,a_3\le H\\(a_1,a_2)=1\\(a_1,a_3)=1}}1=H^2\sum_{1\le n\le H}\left(\frac{\varphi(n)}{n}\right)^2+O\left(H\left(\log H\right)^3\right). \tag{2.17}$$

Using Lemma 2.1.2, setting $m=2$, and substituting into (2.17) we obtain

$$\sum_{\substack{1\le a_1,a_2,a_3\le H\\(a_1,a_2)=1\\(a_1,a_3)=1}}1=H^3\prod_{p\text{ prime}}\left(1-\frac{2p-1}{p^3}\right)+O\left(H^2\left(\log H\right)^2\right). \tag{2.18}$$

Substituting (2.10), (2.11) and (2.18) into (2.9) completes the proof.

2.1.4 Comments

By using Theorem 2.1.1, we see that the density of triples of positive integers that are pairwise non-coprime is given by $\rho\approx 0.1742$.

In this section we have only considered $\mathcal{N}_3(H)$. Our approach does not seem particularly well suited to higher tuples (that is $\mathcal{N}_k(H)$ for $k>3$). If we examine (2.9) we observe that finding a suitable expression for $\mathcal{N}_3(H)$ involved 3 different summations. The expression of two of these summations as a multiple of H^3 with a suitably bound error term was provided by previously known results. For $\mathcal{N}_4(H)$ we have 10 summations (each summation corresponds to one of the, up to isomorphism, 10 non-null undirected graphs of 4 vertices). Of these 10 summations 6 can be obtained by natural extensions of the techniques in this section. The remaining 4, namely

$$\sum_{\substack{1\le a_1,\dots,a_4\le H\\(a_1,a_2)=1\\(a_2,a_3)=1\\(a_3,a_4)=1}}1,\quad \sum_{\substack{1\le a_1,\dots,a_4\le H\\(a_1,a_2)=1\\(a_2,a_3)=1\\(a_3,a_4)=1\\(a_4,a_1)=1}}1,\quad \sum_{\substack{1\le a_1,\dots,a_4\le H\\(a_1,a_2)=1\\(a_2,a_3)=1\\(a_2,a_4)=1\\(a_3,a_4)=1}}1\quad\text{and}\quad \sum_{\substack{1\le a_1,\dots,a_4\le H\\(a_1,a_2)=1\\(a_1,a_3)=1\\(a_1,a_4)=1\\(a_2,a_3)=1\\(a_2,a_4)=1}}1,$$

would appear to require techniques such as those shown in Section 2.2.

2.2 Tuples of integers with pairwise coprimality conditions

2.2.1 Introduction

This section is entirely based on [2]. We study tuples whose elements are positive integers of maximum value H and impose certain coprimality conditions on pairs of elements. In contrast to the rest of this thesis, we will use v, rather than k, to denote the number of elements of arrays due to the strong link to the number of vertices of various graphs.

Fernández and Fernández, in [31] and in subsequent discussions with the author, have shown how to calculate the density of v-tuples of positive integers that exhibit coprimality across given pairs. That is, how to calculate ρ_G in Theorem 2.2.1 below. In Appendix 1, we give an example of these calculations. Their approach is non-inductive. Hu [51] has estimated the number of $(a_1, \ldots, a_v)$ with $1 \leq a_1, \ldots, a_v \leq H$ that satisfy given coprimality conditions on pairs of elements of the v-tuple. His inductive approach gives an asymptotic formula with an upper bound on the error term of $O(H^{v-1} \log^{v-1} H)$.

In significantly many cases, our main result gives a better error term than that of [51]. Unlike [51] our approach is non-inductive.

We use a graph to represent the required primality conditions as follows. Let $G = (V, E)$ be a graph with v vertices and e edges. The set of vertices, V, will be given by $V = \{1, \ldots, v\}$ whilst the set of edges of G, denoted by E, is a subset of the set of pairs of elements of V. That is, $E \subseteq \{\{1,2\}, \{1,3\}, \ldots, \{r,s\}, \ldots, \{v-1, v\}\}$. We admit isolated vertices (that is, vertices that are not adjacent to any other vertex). An edge is always of the form $\{r,s\}$ with $r \neq s$ and $\{r,s\} = \{s,r\}$. For each real $H > 0$ we define the set of all tuples that satisfy the primality conditions by

$$G(H) := \{(a_1, \ldots, a_v) \in \mathbb{N}^v : a_r \leq H,\ \gcd(a_r, a_s) = 1 \text{ if } \{r,s\} \in E\}.$$

We also let $g(H) = |G(H)|$ and denote with d the maximum degree of the vertices of G. Finally, let $Q_G(z) = 1 + B_2 z^2 + \cdots + B_v z^v$ be the polynomial associated to the graph G, defined by

$$Q_G(z) = \sum_{F \subseteq E} (-1)^{|F|} z^{v(F)}, \tag{2.19}$$

where $v(F)$ is the number of non-isolated vertices of graph F.

Our main result is as follows.

Theorem 2.2.1. *For real $H > 0$ we have*

$$g(H) = H^v \rho_G + O(H^{v-1} \log^d H),$$

where

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{p}\right).$$

The quantity ρ_G gives the asymptotic proportion of v random positive integers that exhibit the given pairwise coprimality conditions. This proportion is calculable. For example, consider the 'square' 4-tuple. That is, 4-tuples with $\gcd(a_1, a_2) = \gcd(a_2, a_3) = \gcd(a_3, a_4) = \gcd(a_4, a_1) = 1$. Then the asymptotic proportion of such 4-tuples is given by

$$\rho_G = \prod_{p \text{ prime}} \left(1 - \frac{4}{p^2} + \frac{4}{p^3} - \frac{1}{p^4}\right) = 0.217778\ldots \tag{2.20}$$

Further details can be found in Subsection 2.2.5.

2.2.2 Preparations

Let $P^+(s)$ denote the largest prime factor of any integer $s > 1$. By convention $P^+(1) = 1$.

For each $F \subseteq E$, a subset of the edges of G, let $v(F)$ be the number of non-isolated vertices of F. We define two polynomials $Q_G(z)$ and $Q_G^+(z)$ by

$$Q_G(z) = \sum_{F \subseteq E} (-1)^{|F|} z^{v(F)}, \qquad Q_G^+(z) = \sum_{F \subseteq E} z^{v(F)}.$$

In this way, we associate two polynomials to each graph. It is clear that the only $F \subseteq E$ for which $v(F) = 0$ is the empty set. Thus, the constant terms of $Q_G(z)$ and $Q_G^+(z)$ are always 1. If F is non-empty then there is some edge $a = \{r, s\} \in F$ so that $v(F) \geq 2$. Therefore, the coefficients of z in $Q_G(z)$ and $Q_G^+(z)$ are zero. Since we do not allow repeated edges the only case in which $v(F) = 2$ is when F consists of one edge. Thus, the coefficient of z^2 in $Q_G^+(z)$ is e, that is, the number of edges e in G. The corresponding z^2 coefficient in $Q_G(z)$ is $-e$.

As a matter of notation we shall sometimes use r and s to indicate vertices. The letter v will always denote the last vertex and the number of vertices in a given graph. Edges will sometimes be denoted by a or b. As previously mentioned, we use d to denote the maximum degree of any vertex and e to denote the number of edges. We use terms like e_j to indicate the j-th edge.

We associate several multiplicative functions to any graph. To define these functions we consider functions $E \to \mathbb{N}$. That is, to any edge a in the graph we associate a natural number n_a. We call any of these functions, $a \mapsto n_a$, an *edge numbering* of the graph. Given an edge numbering we assign a corresponding *vertex numbering* function $r \mapsto N_r$ by the rule $N_r = \operatorname{lcm}(n_{b_1}, \ldots, n_{b_u})$, where $E_r = \{b_1, \ldots, b_u\} \subseteq E$ is the set of edges incident to r. We note that in the case where r is an isolated vertex we will have $E_r = \emptyset$ and $N_r = 1$. With these notations we define

$$f_G(m) = \sum_{N_1 N_2 \cdots N_v = m} \mu(n_1) \cdots \mu(n_e) \tag{2.21}$$

and

$$f_G^+(m) = \sum_{N_1 N_2 \cdots N_v = m} |\mu(n_1) \cdots \mu(n_e)|. \tag{2.22}$$

In this and similar summations in this section, the summation is extended to all edge numberings (that is, for all $1 \le n_1, \ldots, n_e < \infty$) satisfying the condition written under the summation symbol, usually expressed in terms of the corresponding vertex numberings. As an example, again consider the 'square' 4-tuple. That is, 4-tuples with $\gcd(a_1, a_2) = \gcd(a_2, a_3) = \gcd(a_3, a_4) = \gcd(a_4, a_1) = 1$. We have $f_G(p^4) = -1$ and $f_G^+(p^4) = 7$. Detailed calculations of both $f_G(p^4)$ and $f_G^+(p^4)$ for this 'square' 4-tuple are shown in Subsection 2.2.5. We will see in Lemma 2.2.3 that it is not a coincidence that $f_G(p^4)$ is the coefficient of $1/p^4$ in (2.20).

The following is interesting in its own right but will also be used to prove Theorem 2.2.1.

Lemma 2.2.2. *Let $h : \mathbb{N} \to \mathbb{C}$ be a multiplicative function. For any graph G the function*

$$g_{h,G}(m) = \sum_{N_1 N_2 \cdots N_v = m} h(n_1) \cdots h(n_e)$$

is multiplicative.

Proof. Let $m = m_1 m_2$ where $\gcd(m_1, m_2) = 1$. Let us assume that for a given edge numbering of G we have $N_1 \cdots N_v = m$. For any edge $a = \{r, s\}$ we have $n_a | N_r$ and $n_a | N_s$. Therefore, $n_a^2 | m$. It follows that we may express n_a as $n_a = n_{1,a} n_{2,a}$ with $n_{1,a} | m_1$ and $n_{2,a} | m_2$. In this case $\gcd(n_{1,a}, n_{2,a}) = 1$, and we will have

$$N_r = \operatorname{lcm}(n_{b_1}, \ldots, n_{b_v}) = \operatorname{lcm}(n_{1,b_1}, \ldots, n_{1,b_v}) \operatorname{lcm}(n_{2,b_1}, \ldots, n_{2,b_v}),$$

$$h(n_1) \cdots h(n_e) = h(n_{1,1}) \cdots h(n_{1,e}) \cdot h(n_{2,1}) \cdots h(n_{2,e}).$$

Since each edge numbering n_a splits into two edge numberings $n_{1,a}$ and $n_{2,a}$, we have

$$m_1 = N_{1,1} \cdots N_{1,v}, \quad m_2 = N_{2,1} \cdots N_{2,v}.$$

Thus

$$\begin{aligned}
g_{h,G}(m_1 m_2) &= g_{h,G}(m) \\
&= \sum_{N_1 N_2 \cdots N_v = m} h(n_1) \cdots h(n_e) \\
&= \sum_{N_{1,1} \cdots N_{1,v} \cdot N_{2,1} \cdots N_{2,v} = m_1 m_2} h(n_{1,1}) \cdots h(n_{1,e}) \cdot h(n_{2,1}) \cdots h(n_{2,e}) \\
&= \sum_{N_{1,1} \cdots N_{1,v} = m_1} h(n_{1,1}) \cdots h(n_{1,e}) \sum_{N_{2,1} \cdots N_{2,v} = m_2} h(n_{2,1}) \cdots h(n_{2,e}) \\
&= g_{h,G}(m_1) g_{h,G}(m_2),
\end{aligned}$$

which completes the proof. □

For $h = \mu$ we will denote $g_{h,G}$ by f_G and for $h = |\mu|$ we will denote $g_{h,G}$ by f_G^+. We now draw the link between $f_G^+(p^k)$ and $Q_G^+(z)$.

Lemma 2.2.3. *For any graph G and prime p the value $f_G^+(p^k)$ is equal to the coefficient of z^k in $Q_G^+(z)$. In the same way the value of $f_G(p^k)$ is equal to the coefficient of z^k in $Q_G(z)$.*

Proof. First we consider the case of $f_G(p^k)$. Recall that

$$Q_G(z) = \sum_{F\subseteq E} (-1)^{|F|} z^{v(F)}, \qquad f_G(p^k) = \sum_{N_1\cdots N_v = p^k} \mu(n_1)\cdots\mu(n_e),$$

where the last sum is on the set of edge numberings of G. In the second sum we shall only consider edge numberings of G giving a non null term. This means that we only consider edge numberings with n_a squarefree numbers. Notice also that if $N_1\cdots N_v = p^k$, then each $n_a \mid p^k$. So the second sum extends to all edge numbering with $n_a \in \{1, p\}$ for each edge $a \in E$ and satisfying $N_1\cdots N_v = p^k$.

We need to prove the equality

$$\sum_{F\subseteq E,\ v(F)=k} (-1)^{|F|} = \sum_{N_1\cdots N_v = p^k} \mu(n_1)\cdots\mu(n_e). \tag{2.23}$$

To this end we shall define for each $F \subseteq E$ with $v(F) = k$ a squarefree edge numbering $\sigma(F) = (n_a)$ with $N_1\cdots N_v = p^k$, $n_a \in \{1,p\}$ and such that $(-1)^{|F|} = \mu(n_1)\cdots\mu(n_e)$. We will show that σ is a bijective mapping between the set of $F \subseteq E$ with $v(F) = k$ and the set of edge numberings (n_a) with $N_1\cdots N_v = p^k$. Thus, equality (2.23) will be established and the proof finished.

Assume that $F \subseteq E$ with $v(F) = k$. We define $\sigma(F)$ as the edge numbering (n_a) defined by

$$n_a = p \text{ for any } a \in F, \quad n_a = 1 \text{ for } a \in E \smallsetminus F.$$

In this way it is clear that $\mu(n_1)\cdots\mu(n_e) = (-1)^{|F|}$. Also $N_r = p$ or $N_r = 1$. We will have $N_r = p$ if and only if there is some $a = \{r, s\} \in F$. So that $N_1\cdots N_v = p^{v(F)}$ because by definition $v(F)$ is the cardinality of the union $\bigcup_{\{r,s\}\in F}\{r, s\}$.

The map σ is invertible. For let (n_a) be an edge numbering of squarefree numbers with $N_1\cdots N_v = p^k$ and $n_a \in \{1,p\}$. If $\sigma(F) = (n_a)$ necessarily we will have $F = \{a \in E : n_a = p\}$. It is clear that defining F in this way we will have $v(F) = k$ and $\sigma(F) = (n_a)$.

Therefore the coefficient of z^k in $Q_G(z)$ coincides with the value of $f_G(p^k)$.

The proof for f_G^+ is the same observing that for $\sigma(F) = (n_a)$ we will have $1 = |(-1)^{|F|}| = |\mu(n_1)\cdots\mu(n_e)|$. □

2.2.3 Proof of Theorem 2.2.1

We prove the theorem in the following steps.

1. We show that

$$g(H) = \sum_{n_1,\dots,n_e} \mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}\left\lfloor \frac{H}{N_r}\right\rfloor.$$

2. We show that

$$g(H) = H^v \sum_{n_1=1}^{\infty}\cdots\sum_{n_e=1}^{\infty} \mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}\frac{1}{N_r} + R + O\left(H^{v-1}\log^d H\right),$$

where

$$|R| \le H^{v-1}\sum_{j=1}^{e}\sum_{n_1=1}^{\infty}\cdots\sum_{n_{j-1}=1}^{\infty}\sum_{n_j>H}\sum_{n_{j+1}=1}^{\infty}\cdots\sum_{n_e=1}^{\infty}\mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}\frac{1}{N_r}.$$

3. We show that $|R| = O(H^{v-1}\log^d H)$.

We start with the following sieve result which generalises the sieve of Eratosthenes.

Lemma 2.2.4. *Let X be a finite set, and let $A_1, A_2, \dots, A_k \subseteq X$. Then*

$$|X\backslash \bigcup_{j=1}^{k} A_j| = \sum_{J\subseteq\{1,2,\dots,k\}} (-1)^{|J|} B_J,$$

where $B_\emptyset = X$, and for $J \subseteq \{1, 2, \dots, k\}$ nonempty

$$B_J = \bigcap_{j\in J} A_j.$$

To prove Theorem 2.2.1, let X be the set

$$X = \{(a_1, \dots, a_v) \in \mathbb{N}^v : a_r \le H, 1 \le r \le v\}.$$

Our set $G(H)$, associated to the graph G, is a subset of X. Now for each prime $p \le H$ and each edge $a = \{r, s\} \in G$ define the following subset of X.

$$A_{p,a} = \{(a_1, \dots, a_v) \in X : p|a_r, p|a_s\}.$$

Therefore, the tuples in $A_{p,a}$ are not in $G(H)$. In fact it is clear that

$$G(H) = X\backslash \bigcup_{\substack{a\in E\\ p\le H}} A_{p,a},$$

where E denotes the set of edges in our graph G. We note that we have an $A_{p,a}$ for each prime number less than or equal to H and each edge $a \in E$. Denoting P_H as the set of prime numbers less than or equal to H we can represent each $A_{p,a}$ as A_j with $j \in P_H \times E$. We now apply Lemma 2.2.4 and obtain

$$g(H) = \sum_{J \subseteq P_H \times E} (-1)^{|J|} B_J. \tag{2.24}$$

We compute B_J and then $|J|$. For B_J, we have

$$J = \{(p_1, e_1), \dots, (p_m, e_m)\}, \quad B_J = \bigcap_{j=1}^{m} A_{p_j, e_j}.$$

Therefore $(a_1, \dots, a_v) \in B_J$ is equivalent to saying that $p_j | a_{r_j}, p_j | a_{s_j}$ for all $1 \leq j \leq m$, where $e_j = \{r_j, s_j\}$. We note that if $p_{i_1}, \dots, p_{i_\ell}$ are the primes associated in J with a given edge $a = \{r, s\}$, then the product of $p_{i_1} \cdots p_{i_\ell}$ must also divide the values a_r and a_s associated to the vertices of a. Let $T_a \subseteq P_H$ consist of the primes p such that $(p, a) \in J$. In addition, we define

$$n_a = \prod_{p \in T_a} p,$$

observing that when $T_a = \emptyset$ we have $n_a = 1$. Then $(a_1, \dots, a_v) \in B_J$ is equivalent to saying that for each $a = \{r, s\}$ appearing in J we have $n_a \mid a_r$ and $n_a \mid a_s$. In this way, we can define J by giving a number n_a for each edge a. We note that n_a will always be squarefree, and all its prime factors will be less than or equal to H. We also note that $(a_1, \dots, a_v) \in B_J$ is equivalent to saying that $n_a | a_r$ for each edge a that joins vertex r with another vertex.

Then for each vertex r, consider all the edges a joining r to other vertices, and denote the least common multiple of the corresponding n_a's by N_r. So $(a_1, \dots, a_v) \in B_J$ is equivalent to saying that $N_r | a_r$. The number of multiples of N_r that are less than or equal to H is $\lfloor H/N_r \rfloor$, so we can express the number of elements of B_J as

$$B_J = \prod_{r=1}^{v} \left\lfloor \frac{H}{N_r} \right\rfloor. \tag{2.25}$$

We now compute $|J|$. This is the total number of prime factors across all the n_j. As mentioned before n_j is squarefree, so

$$(-1)^{|J|} = (-1)^{\sum_{j=1}^{e} \omega(n_j)} = \mu(n_1) \cdots \mu(n_e), \tag{2.26}$$

where the summations are over all squarefree n_j with $P^+(n_j) \leq H$. Substituting (2.25) and (2.26) into (2.24) yields

$$g(H) = \sum_{n_1=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1) \cdots \mu(n_e) \prod_{r=1}^{v} \left\lfloor \frac{H}{N_r} \right\rfloor.$$

At first the sum extends to the $(n_1,\dots,n_e)$ that are squarefree and have all prime factors less than or equal to H. But we may extend the sum to all $(n_1,\dots,n_e)$, because if these conditions are not satisfied then the corresponding term is automatically 0. In fact we may restrict the summation to the $n_a \le H$, because otherwise for $a=\{r,s\}$ we have $n_a \mid N_r$ and $\lfloor H/N_r \rfloor = 0$. Therefore,

$$g(H) = \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \left\lfloor \frac{H}{N_r} \right\rfloor .$$

We now seek to express $g(H)$ as a multiple of H^v plus a suitable error term. Observe that for all real $z_1, z_2, z_3 > 0$,

$$\lfloor z_1 \rfloor \lfloor z_2 \rfloor \lfloor z_3 \rfloor = z_1z_2z_3 - z_1z_2\{z_3\} - z_1\{z_2\}\lfloor z_3 \rfloor - \{z_1\}\lfloor z_2 \rfloor \lfloor z_3 \rfloor,$$

where $\{y\}$ denotes the fractional part of a number y.

Applying a similar procedure, with v factors instead of 3, we get

$$\begin{aligned} g(H) &= \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{H}{N_r} \\ &- \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \left\{ \frac{H}{N_1} \right\} \prod_{r=2}^{v} \left\lfloor \frac{H}{N_r} \right\rfloor \\ &- \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \frac{H}{N_1} \left\{ \frac{H}{N_2} \right\} \prod_{r=3}^{v} \left\lfloor \frac{H}{N_r} \right\rfloor \\ &\cdots \\ &- \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \frac{H}{N_1} \cdots \frac{H}{N_{v-1}} \left\{ \frac{H}{N_v} \right\} \\ &= H^v \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r} + \sum_{k=1}^{v} R_k, \end{aligned} \tag{2.27}$$

where for $1 \le k \le v$,

$$R_k = - \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \frac{H}{N_1} \cdots \frac{H}{N_{k-1}} \left\{ \frac{H}{N_k} \right\} \left\lfloor \frac{H}{N_{k+1}} \right\rfloor \cdots \left\lfloor \frac{H}{N_v} \right\rfloor,$$

with the obvious modifications for $j=1$ and $j=v$. We then have

$$\begin{aligned} |R_k| &\le \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} |\mu(n_1)\cdots\mu(n_e)| \frac{H}{N_1} \cdots \frac{H}{N_{k-1}} \frac{H}{N_{k+1}} \cdots \frac{H}{N_v} \\ &\le H^{v-1} \sum_{P^+(m)\le H} \frac{C_{G,k}(m)}{m}, \end{aligned}$$

where

$$C_{G,k}(m) = \sum_{m=\prod_{1\le r\le v, r\ne k} N_r} |\mu(n_1)\cdots\mu(n_e)|.$$

By similar reasoning to that of Lemma 2.2.2 the function $C_{G,k}(m)$ can be shown to be multiplicative. The numbers $C_{G,k}(p^\alpha) = C_{G,k,\alpha}$ do not depend on p, and $C_{G,k}(p^\alpha) = C_{G,k,\alpha} = 0$ for $\alpha > v$. So we have

$$\begin{aligned}\sum_{P^+(m)\le H} \frac{C_{G,k}(m)}{m} &\le \prod_{p\le H}\left(1 + \frac{C_{G,k,1}}{p} + \frac{C_{G,k,2}}{p^2} + \cdots \frac{C_{G,k,v}}{p^v}\right)\\ &= O(\log^{C_{G,k,1}} H),\end{aligned}$$

where $C_{G,k}(m)$ is the number of solutions $(n_1,\ldots,n_e)$, with n_j squarefree, to

$$\prod_{1\le r\le v, r\ne k} N_r = m. \tag{2.28}$$

Let h_k denote the degree of vertex k. It is easy to see that for a prime p we have $C_{G,k,1} = C_{G,k}(p) = h_k$. The solutions are precisely those with all $n_j = 1$, except one $n_\ell = p$, where ℓ should be one of the edges meeting at vertex k. Therefore, the maximum number of solutions occurs when k is one of the vertices of maximum degree. So if we let d be this maximum degree, then the maximum value of $C_{G,k}(p)$ is d. Therefore,

$$|R_k| = O(H^{v-1}\log^d H). \tag{2.29}$$

Substituting (2.29) into (2.27) we obtain

$$g(H) = H^v \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}\frac{1}{N_r} + O(H^{v-1}\log^d H). \tag{2.30}$$

We require the following lemma.

Lemma 2.2.5. *We have*

$$\lim_{H\to\infty} \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} |\mu(n_1)\cdots\mu(n_e)|\prod_{r=1}^{v}\frac{1}{N_r} < \infty.$$

Proof. Let

$$f_G^+(m) = \sum_{m=\prod_{r=1}^{v} N_r} |\mu(n_1)\cdots\mu(n_e)|.$$

We note that $f_G^+(m)$ is multiplicative by Lemma 2.2.2. It is clear that $f_G^+(1) = 1$. Also, each edge joins two vertices r and s and thus $n_j|E_r$ and $n_j|E_s$. This means that

$$n_j^2|\prod_{r=1}^{v} N_r.$$

It follows that

$$\prod_{r=1}^{v} N_r \neq p,$$

for any prime p and so $f_G^+(p) = 0$. We also note that a multiple $(n_1, \ldots, n_e)$ only counts in $f_G^+(m)$ if $|\mu(n_1)\cdots\mu(n_e)| = 1$. Therefore each n_j is squarefree. So each factor in

$$\prod_{r=1}^{v} N_r \tag{2.31}$$

brings at most a p. So the greatest power of p that can divide (2.31) is p^v. So $f_G^+(p^\alpha) = 0$ for $\alpha > v$. Recall that $f_G^+(p^\alpha)$ is equal to the coefficient of x^α in $Q_G^+(x)$. So, by Lemma 2.2.3, we note that $f_G^+(p^\alpha)$ depends on α but not on p. Putting all this together we have

$$\sum_{m=1}^{\infty} \frac{f_G^+(m)}{m} = \prod_{p \text{ prime}} \left(1 + \frac{f_G^+(p^2)}{p^2} + \ldots + \frac{f_G^+(p^v)}{p^v}\right) < \infty. \tag{2.32}$$

Next, we observe that the sequence

$$\Big\{ \sum_{1\le n_1 \le H} \cdots \sum_{1 \le n_e \le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r} \Big\}_{H=1}^{\infty}$$

is an increasing sequence. It is also a bounded sequence since

$$\sum_{1\le n_1 \le H} \cdots \sum_{1 \le n_e \le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r} \le \sum_{m=1}^{\infty} \frac{f_G^+(m)}{m}$$

for any $H \in \mathbb{N}$. So, by the monotone convergence theorem, the limit

$$\lim_{H\to\infty} \sum_{1\le n_1 \le H} \cdots \sum_{1 \le n_e \le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r} \tag{2.33}$$

exists and is bounded by

$$\sum_{m=1}^{\infty} \frac{f_G^+(m)}{m}.$$

□

With a little more work one can show that

$$\lim_{H\to\infty} \sum_{1\le n_1 \le H} \cdots \sum_{1 \le n_e \le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r} = \sum_{m=1}^{\infty} \frac{f_G^+(m)}{m}.$$

Returning to (2.30), it is now clear from Lemma 2.2.5 that

$$\rho_G = \lim_{H\to\infty} \sum_{1\le n_1\le H} \cdots \sum_{1\le n_e\le H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r}$$

is absolutely convergent. In fact,

$$g(H) = H^v \rho_G + R + O(H^{v-1}\log^d H), \tag{2.34}$$

where

$$\rho_G = \sum_{n_1=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \frac{1}{N_r},$$

and

$$|R| \le H^{v-1} \sum_{j=1}^{e} \sum_{n_1=1}^{\infty} \cdots \sum_{n_{j-1}=1}^{\infty} \sum_{n_j>H} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r}.$$

Now

$$\rho_G = \sum_{m=1}^{\infty} \frac{1}{m} \sum_{N_1\cdots N_v=m} \mu(n_1)\cdots\mu(n_e) = \sum_{m=1}^{\infty} \frac{f_G(m)}{m}.$$

We note that $f_G(m)$ is multiplicative by Lemma 2.2.2. In a similar way to Lemma 2.2.5, we have $f_G(1) = 1, f_G(p) = 0$ and $f_G(p^\alpha) = 0$, for all $\alpha > v$. Thus, by the multiplicativity,

$$\rho_G = \sum_{m=1}^{\infty} \frac{f_G(m)}{m} = \prod_{p \text{ prime}} \left(1 + \frac{f_G(p^2)}{p^2} + \ldots + \frac{f_G(p^v)}{p^v}\right).$$

Therefore, by Lemma 2.2.3, we have

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{p}\right). \tag{2.35}$$

Substituting (2.35) into (2.34), it only remains to show that $|R| = O(H^{v-1}\log^d H)$.

We have

$$|R| \le H^{v-1} \sum_{j=1}^{e} \sum_{n_1=1}^{\infty} \cdots \sum_{n_{j-1}=1}^{\infty} \sum_{n_j>H} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r}.$$

All terms in the sum on j are analogous; so assuming that the first is the largest, we have

$$|R| \le C_1 H^{v-1} \sum_{n_1>H} \sum_{n_2=1}^{\infty} \sum_{n_{j+1}=1}^{\infty} \cdots \sum_{n_e=1}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} \frac{1}{N_r},$$

where C_1 is a function of e and not H. So it will suffice to show that

$$R_1 := \sum_{n_1>H}\sum_{n_2=1}^{\infty}\cdots\sum_{n_e=1}^{\infty}|\mu(n_1)\cdots\mu(n_e)|\prod_{r=1}^{v}\frac{1}{N_r} = O(\log^d H). \tag{2.36}$$

We will treat an edge $e_1 = \{u, s\}$ differently to the other edges. For a given $(n_1, \ldots, n_e)$ of squarefree numbers we have two special integers,

$$N_u = \operatorname{lcm}(n_1, n_{\alpha_1}, \ldots n_{\alpha_k}), \quad N_s = \operatorname{lcm}(n_1, n_{\beta_1}, \ldots n_{\beta_k}).$$

We also remark that we may have $N_u = \operatorname{lcm}(n_1)$ or $N_s = \operatorname{lcm}(n_1)$.

For any edge e_j with $2 \le j \le e$ we define $d_j = \gcd(n_1, n_j)$. Since the n_j are squarefree, we have

$$n_j = d_j n_j', \quad d_j | n_1, \quad \gcd(n_1, n_j') = 1.$$

Then it is clear that

$$N_u = \operatorname{lcm}(n_1, d_{\alpha_1}n_{\alpha_1}', \ldots, d_{\alpha_k}n_{\alpha_k}') = n_1 \operatorname{lcm}(n_{\alpha_1}', \ldots, n_{\alpha_k}')$$

and

$$N_s = n_1 \operatorname{lcm}(n_{\beta_1}', \ldots, n_{\beta_l}').$$

For any other vertex with $t \ne u$ and $t \ne s$, we have

$$\begin{aligned} N_t &= \operatorname{lcm}(n_{t_1}, \ldots, n_{t_m}) = \operatorname{lcm}(d_{t_1}n_{t_1}', \ldots, d_{t_m}n_{t_m}') \\ &= \operatorname{lcm}(d_{t_1}, \ldots, d_{t_m}) \operatorname{lcm}(n_{t_1}', \ldots, n_{t_m}'), \end{aligned}$$

where m will vary with t. Substituting the equations for N_u, N_s and N_t into the definition of R_1 in (2.36) we obtain

$$\begin{aligned} R_1 &= \sum_{n_1>H}\sum_{n_2=1}^{\infty}\cdots\sum_{n_e=1}^{\infty}|\mu(n_1)\cdots\mu(n_e)|\frac{1}{N_u}\frac{1}{N_s}\prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}}\frac{1}{N_t} \\ &= \sum_{n_1>H}\frac{|\mu(n_1)|}{n_1^2}\sum_{d_2|n_1}\cdots\sum_{d_e|n_1}\sum_{n_2'=1}^{\infty}\cdots\sum_{n_e'=1}^{\infty}\frac{|\mu(n_2)\cdots\mu(n_e)|}{\operatorname{lcm}(n_{\alpha_1}', \ldots, n_{\alpha_k}')\operatorname{lcm}(n_{\beta_1}', \ldots, n_{\beta_l}')} \\ &\qquad\times\prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}}\frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m})\operatorname{lcm}(n_{t_1}', \ldots, n_{t_m}')} \\ &= \sum_{n_1>H}\frac{|\mu(n_1)|}{n_1^2}\sum_{d_2|n_1}\cdots\sum_{d_e|n_1}\prod_{\substack{1\le t\le v\\ t\ne r,\ t\ne s}}\frac{1}{\operatorname{lcm}(d_{t_1}, \ldots, d_{t_m})} \\ &\qquad\times\sum_{n_2'=1}^{\infty}\cdots\sum_{n_e'=1}^{\infty}\left(\frac{|\mu(d_2n_2')\cdots\mu(d_en_e')|}{\operatorname{lcm}(n_{\alpha_1}', \ldots, n_{\alpha_k}')\operatorname{lcm}(n_{\beta_1}', \ldots, n_{\beta_l}')}\right. \\ &\qquad\qquad\left.\times\prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}}\frac{1}{\operatorname{lcm}(n_{t_1}', \ldots, n_{t_m}')}\right). \end{aligned}$$

It follows that

$$
\begin{aligned}
R_1 \le \sum_{n_1 > H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})} \\
\times \sum_{n_2'=1}^{\infty} \cdots \sum_{n_e'=1}^{\infty} \left(\frac{|\mu(n_2') \cdots \mu(n_e')|}{\operatorname{lcm}(n_{\alpha_1}', \dots, n_{\alpha_k}') \operatorname{lcm}(n_{\beta_1}', \dots, n_{\beta_l}')} \right. \\
\left. \times \prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} \frac{1}{\operatorname{lcm}(n_{t_1}', \dots, n_{t_m}')} \right).
\end{aligned}
$$

The expression

$$
\sum_{n_2'=1}^{\infty} \cdots \sum_{n_e'=1}^{\infty} \frac{|\mu(n_2') \cdots \mu(n_e')|}{\operatorname{lcm}(n_{\alpha_1}', \dots, n_{\alpha_k}') \operatorname{lcm}(n_{\beta_1}', \dots, n_{\beta_l}')} \prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} \frac{1}{\operatorname{lcm}(n_{t_1}', \dots, n_{t_m}')}
$$

is finite by Lemma 2.2.5 (but this time considering the graph G without the edge $\{u, s\}$). Thus, for some constant C_2, we have

$$
\begin{aligned}
R_1 &\le C_2 \sum_{n_1 > H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})} \\
&= C_2 \sum_{n_1 > H} \frac{|\mu(n_1)|}{n_1^2} f_{G,e}(n_1), \qquad (2.37)
\end{aligned}
$$

where the arithmetic function $f_{G,e}$ is defined as follows.

$$
f_{G,e}(n) = \sum_{d_2 | n} \cdots \sum_{d_e | n} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})}.
$$

We note that there is a factor $\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})$ for each vertex other than u or s. The function $f_{G,e}$ is a multiplicative function. We have $f_{G,e}(p^k) = f_{G,e}(p)$ for any power of a prime p with $k \ge 2$, because in the definition of $f_{G,e}(p^k)$ only the divisors 1 and p of p^k give non null terms. When $n = p$ we have

$$
f_{G,e}(p) = 1 + \frac{A_1}{p} + \cdots + \frac{A_{v-2}}{p^{v-2}},
$$

where A_i is the number of ways that

$$
\prod_{\substack{1 \le t \le v \\ t \ne u,\ t \ne s}} |\mu(d_2) \cdots \mu(d_e)| \operatorname{lcm}(d_{t_1}, \dots, d_{t_m}) = p^i,
$$

where every divisor in the product $d_h \mid n = p$ can only be 1 or p. The inequality $A_i \leq 2^{e-1}$ does not depend on p, and so there must be a number w, independent of p, such that

$$f_{G,e}(p^k) = f_{G,e}(p) \leq \left(1 + \frac{1}{p}\right)^w .$$

Since $f_{G,e}$ is multiplicative we have, for any squarefree n,

$$f_{G,e}(n) \leq \prod_{p|n} \left(1 + \frac{1}{p}\right)^w = \left(\frac{\sigma(n)}{n}\right)^w, \quad |\mu(n)| = 1. \tag{2.38}$$

Substituting (2.38) into (2.37) yields

$$R_1 \leq C_2 \sum_{n>H}^{\infty} \frac{|\mu(n)|}{n^2} \left(\frac{\sigma(n)}{n}\right)^w \leq C_2 \sum_{n>H}^{\infty} \frac{1}{n^2} \left(\frac{\sigma(n)}{n}\right)^w .$$

It is well known that $\sigma(n) = O(n \log\log n)$ (see, for example, [40]), and thus

$$R_1 = O\left(\frac{(\log\log H)^w}{H}\right). \tag{2.39}$$

Comparing (2.39) with (2.36) completes the proof of Theorem 2.2.1.

2.2.4 The spectrum of ρ_G

For any $n > 1$, let $S_n = \{\rho_G : |G| = n\}$. We state some obvious results without proof. For any $n > 1$, we have $0 \notin S_n$ and $1 \in S_n$. We also observe that

$$\min S_n = \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^{n-1} \left(1 + \frac{n-1}{p}\right) \to 0 \text{ as } n \to \infty,$$

and

$$S_2 \subsetneq S_3 \subsetneq \cdots .$$

Next, we obtain an upper bound for $|S_n|$.

Theorem 2.2.6. *For any $\epsilon > 0$ and sufficiently large n we have*

$$|S_n| \leq (1+\epsilon)\left(\frac{2^{\binom{n}{2}}}{n!}\right).$$

Proof. For any $n > 1$ let T_n be the equivalence set of graphs with n vertices partitioned by isomorphism. It is clear that

$$|S_n| \leq |T_n|. \tag{2.40}$$

Harary and Palmer [42, Equation 9.1.1] credit Pólya with the following.

$$|T_n| \sim 2^{\binom{n}{2}}/n!. \tag{2.41}$$

Combining (2.40) and (2.41) concludes the theorem. □

We note that non-isomorphic graphs do not necessarily yield different densities. That is, $G_1 \not\sim G_2 \not\Rightarrow \rho_{G_1} \neq \rho_{G_2}$. To see this, we exhibit graphs

$$G_1 = (\{\{1,2\},\{2,3\},\{3,4\},\{1,4\}\},\{1,2,3,4\})$$

and

$$G_2 = (\{\{1,2\},\{2,3\},\{1,3\},\{1,4\}\},\{1,2,3,4\}).$$

It is clear that G_1 is not isomorphic to G_2. As shown in Subsection 2.2.5

$$\rho_{G_1} = \prod_{p \text{ prime}} \left(1 - \frac{4}{p^2} + \frac{4}{p^3} - \frac{1}{p^4}\right),$$

and using similar calculations we can show that ρ_{G_2} gives an identical result (alternatively see the calculations in Chapter 5). A consequence is that equation (2.40) can be improved to a strict inequality for $n > 3$.

2.2.5 Calculations

We calculate the asymptotic proportion that 4 random positive integers exhibit 'square' pairwise coprimality conditions. That is, 4-tuples with

$$\gcd(a_1, a_2) = \gcd(a_2, a_3) = \gcd(a_3, a_4) = \gcd(a_4, a_1) = 1. \tag{2.42}$$

Here $G(V, E)$ is given by

$$V = \{1,2,3,4\}, \quad E = \{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}.$$

As shown in equation (2.19),

$$Q_G\left(\frac{1}{p}\right) = \sum_{F \subseteq E} (-1)^{|F|} \left(\frac{1}{p}\right)^{v(F)},$$

where $v(F)$ is the number of non-isolated vertices of F.

Next we examine each $F \subseteq E$ to compute its contribution to $Q_G(z)$. This is shown in Table 2.1.

Table 2.1: Subsets of edges and calculation of the polynomial $Q_G(z)$

$F \subseteq E$	$\lvert F\rvert$	$v(F)$	$(-1)^{\lvert F\rvert} z^{v(F)}$
$\emptyset$	0	0	1
$\{\{1,2\}\}$, $\{\{2,3\}\}$, $\{\{3,4\}\}$, $\{\{4,1\}\}$	1	2	$-4z^2$
$\{\{1,2\},\{2,3\}\}$, $\{\{2,3\},\{3,4\}\}$, $\{\{3,4\},\{4,1\}\}$, $\{\{4,1\},\{1,2\}\}$	2	3	$4z^3$
$\{\{1,2\},\{3,4\}\}$, $\{\{2,3\},\{4,1\}\}$,	2	4	$2z^4$
$\{\{1,2\},\{2,3\},\{3,4\}\}$, $\{\{2,3\},\{3,4\},\{4,1\}\}$, $\{\{3,4\},\{4,1\},\{1,2\}\}$, $\{\{4,1\},\{1,2\},\{2,3\}\}$	3	4	$-4z^4$
E	4	4	z^4
			$Q_G(z) = 1 - 4z^2 + 4z^3 - z^4$

Putting this all together we have

$$\rho_G = \prod_{p \text{ prime}} \left(1 - \frac{4}{p^2} + \frac{4}{p^3} - \frac{1}{p^4}\right).$$

This gives ρ_G as an Euler product. As shown in [83], Euler products such as ρ_G can be computed to high precision.

As foreshadowed in Subsection 2.2.2, we now give an example of the calculation of f_G and f_G^+. In particular, we calculate $f_G(p^4)$ and $f_G^+(p^4)$. Again G is the 'square' 4-tuple (see (2.42)). Using (2.21) we have the following 2 tables.

Table 2.2: Calculation of $f_G(p^4)$

$F \subseteq E$	$(n_1, \dots, n_4)$	$(N_1, \dots, N_4)$	$\mu(n_1) \cdots \mu(n_4)$
$\{\{1,2\},\{3,4\}\}$	$(p,1,p,1)$	(p,p,p,p)	1
$\{\{2,3\},\{4,1\}\}$	$(1,p,1,p)$	(p,p,p,p)	1
$\{\{1,2\},\{2,3\},\{3,4\}\}$	$(p,p,1,p)$	(p,p,p,p)	-1
$\{\{2,3\},\{3,4\},\{4,1\}\}$	$(1,p,p,p)$	(p,p,p,p)	-1
$\{\{1,2\},\{3,4\},\{4,1\}\}$	$(p,1,p,p)$	(p,p,p,p)	-1
$\{\{1,2\},\{2,3\},\{4,1\}\}$	$(p,p,1,p)$	(p,p,p,p)	-1
$\{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$	(p,p,p,p)	(p,p,p,p)	1
			$f_G(p^4) = -1$

Table 2.3: Calculation of $f_G^+(p^4)$

$F \subseteq E$	$(n_1, \dots, n_4)$	$(N_1, \dots, N_4)$	$\lvert\mu(n_1) \cdots \mu(n_4)\rvert$
$\{\{1,2\},\{3,4\}\}$	$(p,1,p,1)$	(p,p,p,p)	1
$\{\{2,3\},\{4,1\}\}$	$(1,p,1,p)$	(p,p,p,p)	1
$\{\{1,2\},\{2,3\},\{3,4\}\}$	$(p,p,1,p)$	(p,p,p,p)	1
$\{\{2,3\},\{3,4\},\{4,1\}\}$	$(1,p,p,p)$	(p,p,p,p)	1
$\{\{1,2\},\{3,4\},\{4,1\}\}$	$(p,1,p,p)$	(p,p,p,p)	1
$\{\{1,2\},\{2,3\},\{4,1\}\}$	$(p,p,1,p)$	(p,p,p,p)	1
$\{\{1,2\},\{2,3\},\{3,4\},\{4,1\}\}$	(p,p,p,p)	(p,p,p,p)	1
			$f_G^+(p^4) = 7$

2.3 Tuples of polynomials over finite fields with pairwise coprimality conditions

2.3.1 Introduction

Given that this thesis canvasses pairwise coprimality and polynomial irreducibility, it is natural to consider arrays of monic polynomials over finite fields that satisfy certain pairwise coprimality conditions. Another motivation arises from the very recent articles, [24] and [67], that use function fields over a finite field to calculate densities of integer coefficient polynomials that are irreducible by the Eisenstein criterion and the shifted Eisenstein criterion respectively. In this subsection we seek to estimate the number of arrays of degree bounded monic polynomials $(b_1, \dots, b_v) \in (\mathbb{F}_q[x])^v$ with q a prime power that satisfy given pairwise coprimality conditions. We use the methods of Section 2.2. This section is joint work with Igor Shparlinski.

For the remainder of this section all references to polynomials will refer to monic polynomials. We use a graph to represent the required primality conditions as follows. Let $G = (V, E)$ be a graph with v vertices and e edges. The set of vertices, V, will be given by $V = \{1, \dots, v\}$ whilst the set of edges of G, denoted by E, is a subset of the set of pairs of elements of V. That is, $E \subseteq \{\{1,2\}, \{1,3\}, \dots, \{r,s\}, \dots, \{v-1, v\}\}$. We admit isolated vertices (that is, vertices that are not adjacent to any other vertex). An edge is always of the form $\{r, s\}$ with $r \neq s$ and $\{r,s\} = \{s,r\}$. Let

$$\mathbf{b} = \{(b_1, \dots, b_v) \in (\mathbb{F}_q[x])^v : b_r \text{ monic}, 1 \leq r \leq v\}.$$

For each real $H > 0$ and any prime power q, we define the set of all tuples that satisfy the primality conditions by

$$G(H) := \{b \in (\mathbb{F}_q[x])^v : \deg b_r \leq H, \ \gcd(b_r, b_s) = 1 \text{ if } \{r,s\} \in E\},$$

We also let $g(H) = |G(H)|$, and denote with d the maximum degree of the vertices of G. Finally, let $Q_G(z) = 1 + B_2 z^2 + \cdots + B_v z^v$ be the polynomial associated to the graph G, defined by

$$Q_G(z) = \sum_{F \subseteq E} (-1)^{|F|} z^{v(F)}, \tag{2.43}$$

where $v(F)$ is the number of non-isolated vertices of graph F.

Our main result is as follows.

Theorem 2.3.1. *For real $H > 0$ and a constant w we have*

$$g(H) = q^{Hv} \rho_G + O\left(\frac{q^{Hv} (\log\log H)^w}{H} \right),$$

where

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{q^p}\right).$$

2.3.2 Preparations

Denote the degree of the maximum prime factor of a polynomial b with $\deg b > 0$ by

$$\deg P^+(b) = \max_{\substack{b_i | b \\ \deg b_i \neq \deg b}} \deg b_i.$$

By convention, $P^+(b) = 1$ for any b with $\deg b = 0$.

As a matter of notation we shall sometimes use r and s to indicate vertices. The letter v will always denote the last vertex and the number of vertices in a given graph. Edges will sometimes be denoted by a or b. As previously mentioned, we use d to denote the maximum degree of any vertex and e to denote the number of edges. We use terms like e_j to indicate the j-th edge.

We associate several multiplicative functions to any graph. To define these functions, we consider functions $E \to \mathbb{F}_q[x]$, that is, to any edge a in the graph we associate a polynomial n_a. We call any of these functions, $a \mapsto n_a$, an *edge labeling* of the graph. Given an edge labeling, we assign a corresponding *vertex labeling* function $r \mapsto N_r$ by the rule $N_r = \operatorname{lcm}(n_{c_1}, \dots, n_{c_u})$, where $E_r = \{c_1, \dots, c_u\} \subseteq E$ is the set of edges incident to r. We note that in the case where r is an isolated vertex we will have $E_r = \emptyset$ and $N_r = 1$. In this and similar summations in this section, the summation is extended to all edge labels (that is, for all $0 \leq \deg n_1, \dots, \deg n_e < \infty$) satisfying the condition written under the summation symbol, usually expressed in terms of the corresponding vertex labeling.

2.3.3 Proof of Theorem 2.3.1

We start by showing that

$$g(H) = \sum_{\deg n_1, \dots, \deg n_e} \mu(n_1) \cdots \mu(n_e) \prod_{r=1}^{v} \lfloor q^{H - \deg N_r} \rfloor,$$

where $\mu(n)$, with n a polynomial over a finite field, is calculated analogously to μ of an integer.

Let X be the set

$$X = \{\mathbf{b} : \deg b_r \leq H, 1 \leq r \leq v\}.$$

Our set $G(H)$, associated to the graph G, is a subset of X. Now for each prime polynomial p with $\deg p \leq H$ and each edge $a = \{r, s\} \in G$ define the following subset of X.

$$A_{p,a} = \{(b_1, \dots, b_v) \in X : p | a_r, p | a_s\}.$$

Therefore, the tuples in $A_{p,a}$ are not in $G(H)$. In fact it is clear that

$$G(H) = X \setminus \bigcup_{\substack{a \in E \\ \deg p \leq H}} A_{p,a},$$

where E denotes the set of edges in our graph G. We note that we have an $A_{p,a}$ for each prime polynomial with degree less than or equal to H and each edge $a \in E$. Denoting P_H as the set of prime polynomials with degree less than or equal to H we can represent each $A_{p,a}$ as A_j with $j \in P_H \times E$. We now apply Lemma 2.2.4 and obtain

$$g(H) = \sum_{J \subseteq P_H \times E} (-1)^{|J|} B_J. \tag{2.44}$$

We compute B_J and then $|J|$. For B_J, we have

$$J = \{(p_1, e_1), \ldots, (p_m, e_m)\}, \quad B_J = \bigcap_{j=1}^{m} A_{p_j, e_j}.$$

Therefore, $(b_1, \ldots, b_v) \in B_J$ is equivalent to saying that $p_j | b_{r_j}, p_j | b_{s_j}$ for all $1 \leq j \leq m$, where $e_j = \{r_j, s_j\}$. We note that if $p_{i_1}, \ldots, p_{i_\ell}$ are the prime polynomials associated in J with a given edge $a = \{r, s\}$, then the product of $p_{i_1} \cdots p_{i_\ell}$ must also divide the polynomials a_r and a_s associated to the vertices of a. Let $T_a \subseteq P_H$ consist of the prime polynomials p such that $(p, a) \in J$. In addition, we define

$$n_a = \prod_{p \in T_a} p,$$

observing that when $T_a = \emptyset$ we have $n_a = 1$. Then $(b_1, \ldots, b_v) \in B_J$ is equivalent to saying that for each $a = \{r, s\}$ appearing in J we have $n_a \mid b_r$ and $n_a \mid b_s$. In this way we can define J by giving a polynomial n_a for each edge a. We note that n_a will always be squarefree, and all its prime factors will have degree less than or equal to H. We also note that $(b_1, \ldots, b_v) \in B_J$ is equivalent to saying that $n_a | b_r$ for each edge a that joins vertex r with another vertex.

Then for each vertex r, consider all the edges a joining r to other vertices, and denote the least common multiple of the corresponding n_a's by N_r. So $(b_1, \ldots, b_v) \in B_J$ is equivalent to saying that $N_r | a_r$. If $\deg N_r \leq \deg H$ then the number of multiples of N_r that are of degree less than or equal to H is $q^{H - \deg N_r}$ If $\deg N_r > \deg H$ then the number of multiples of N_r that are of degree less than or equal to H is zero. So we can express the number of elements of B_J as

$$B_J = \prod_{r=1}^{v} \lfloor q^{H - \deg N_r} \rfloor. \tag{2.45}$$

We now compute $|J|$. This is the total number of prime factors across all the n_j. As mentioned before n_j is squarefree, so

$$(-1)^{|J|} = (-1)^{\sum_{j=1}^{e} \omega(n_j)} = \mu(n_1) \cdots \mu(n_e), \tag{2.46}$$

where the summations are over all squarefree n_j with $\deg P^+(n_j) \leq H$. Substituting (2.45) and (2.46) into (2.44) yields

$$g(H) = \sum_{\deg n_1=0}^{\infty} \cdots \sum_{\deg n_e=0}^{\infty} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} \lfloor q^{H-\deg N_r} \rfloor.$$

At first, the sum extends to the $(n_1, \ldots, n_e)$ that are squarefree and have all prime factors with degree less than or equal to H. But we may extend the sum to all $(n_1, \ldots, n_e)$, because if these conditions are not satisfied then the corresponding term is automatically 0. In fact, we may restrict the summation to n_a with $\deg n_a \leq H$, because otherwise for $a = \{r, s\}$ we have $n_a \mid N_r$ and $\lfloor q^{H-\deg N_r} \rfloor = 0$. Therefore,

$$\begin{aligned} g(H) &= \sum_{0\leq \deg n_1 \leq H} \cdots \sum_{0\leq \deg n_e \leq H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} q^{H-\deg N_r} \\ &= q^{Hv} \sum_{0\leq \deg n_1 \leq H} \cdots \sum_{0\leq \deg n_e \leq H} \mu(n_1)\cdots\mu(n_e) \prod_{r=1}^{v} q^{-\deg N_r}. \qquad (2.47) \end{aligned}$$

We require the following lemmas to show absolute convergence before proceeding.

Lemma 2.3.2. *For any graph G the function*

$$h_{\mu,G}(m) = \sum_{\deg(N_1\cdots N_v)=m} \mu(n_1)\cdots\mu(n_e)$$

is multiplicative.

Proof. Let $m = m_1 m_2$ where $\gcd(m_1, m_2) = 1$. Let us assume that for a given edge numbering of G we have $\deg(N_1 \cdots N_v) = m$. For any edge $a = \{r, s\}$ we have $n_a | N_r$ and $n_b | N_s$. Therefore $n_a^2 | m$. It follows that we may express n_a as $n_a = n_{1,a} n_{2,a}$ with $n_{1,a} | m_1$ and $n_{2,a} | m_2$. In this case $\gcd(n_{1,a}, n_{2,a}) = 1$, and we will have

$$N_r = \operatorname{lcm}(n_{b_1}, \ldots, n_{b_v}) = \operatorname{lcm}(n_{1,b_1}, \ldots, n_{1,b_v}) \operatorname{lcm}(n_{2,b_1}, \ldots, n_{2,b_v}),$$

$$h(n_1)\cdots\mu(n_e) = \mu(n_{1,1})\cdots\mu(n_{1,e}) \cdot \mu(n_{2,1})\cdots\mu(n_{2,e}).$$

Since each edge numbering n_a splits into two edge numberings $n_{1,a}$ and $n_{2,a}$, we have

$$m_1 = \deg(N_{1,1}\cdots N_{1,v}), \quad m_2 = \deg(N_{2,1}\cdots N_{2,v}).$$

Thus,

$$\begin{aligned}
h_{\mu,G}(m_1m_2) &= h_{\mu,G}(m)\\
&= \sum_{\deg(N_1\cdots N_v)=m} \mu(n_1)\cdots\mu(n_e)\\
&= \sum_{\deg(N_{1,1}\cdots N_{1,v}\cdot N_{2,1}\cdots N_{2,v})=m_1m_2} \mu(n_{1,1})\cdots\mu(n_{1,e})\cdot\mu(n_{2,1})\cdots\mu(n_{2,e})\\
&= \sum_{\deg(N_{1,1}\cdots N_{1,v})=m_1} \mu(n_{1,1})\cdots\mu(n_{1,e}) \sum_{\deg(N_{2,1}\cdots N_{2,v})=m_2} \mu(n_{2,1})\cdots\mu(n_{2,e})\\
&= h_{\mu,G}(m_1)h_{\mu,G}(m_2),
\end{aligned}$$

which completes the proof. □

Lemma 2.3.3.

$$\lim_{H\to\infty} \sum_{0\le\deg n_1\le H} \cdots \sum_{0\le\deg n_e\le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} q^{-\deg N_r} < \infty.$$

Proof. Let

$$h_G^+(m) = \sum_{\deg(N_1\cdots N_v)=m} |\mu(n_1)\cdots\mu(n_e)|.$$

We note that $h_G^+(m)$ is multiplicative by a similar proof to that shown in Lemma 2.3.2. It is clear that $h_G^+(0)=1$ and $h_G^+(1)=0$. Also, each edge joins two vertices s and t and thus $n_j|N_s$ and $n_j|N_t$. This means that

$$n_j^2|\prod_{r=1}^{v} N_r.$$

It follows that

$$\prod_{r=1}^{v} N_r \neq p,$$

for any prime p and so $h_G^+(p)=0$. We also note that a multiple $(n_1,\dots,n_e)$ only counts in $h_G^+(m)$ if $|\mu(n_1)\cdots\mu(n_e)|=1$. Therefore, each n_j is squarefree. So each factor in

$$\prod_{r=1}^{v} N_r \tag{2.48}$$

brings at most a p. So the greatest power of p that can divide (2.48) is p^v. So $h_G^+(p^\alpha)=0$ for $\alpha>v$. Recall that $h_G^+(p^\alpha)$ is equal to the coefficient of x^α in $Q_G^+(x)$. So, by Lemma 2.2.3, we note that $h_G^+(p^\alpha)$ depends on α but not on p. Next, we observe that the sequence

$$\left\{ \sum_{0\le\deg n_1\le H} \cdots \sum_{0\le\deg n_e\le H} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} q^{-\deg N_r} \right\}_{H=0}^{\infty}$$

is an increasing sequence. It is also a bounded sequence since

$$\sum_{0\le\deg n_1\le H}\cdots\sum_{0\le\deg n_e\le H}|\mu(n_1)\cdots\mu(n_e)|\prod_{r=1}^{v}q^{-\deg N_r}\le\sum_{m=0}^{\infty}\frac{h_G^+(m)}{q^m}$$

for any $H\in\mathbb{N}$. So, by the monotone convergence theorem, the limit

$$\lim_{H\to\infty}\sum_{0\le\deg n_1\le H}\cdots\sum_{0\le\deg n_e\le H}|\mu(n_1)\cdots\mu(n_e)|\prod_{r=1}^{v}q^{-\deg N_r}\tag{2.49}$$

exists and is bounded above by

$$\sum_{m=0}^{\infty}\frac{h_G^+(m)}{q^m}.$$

□

With a little more work one can show that

$$\lim_{H\to\infty}\sum_{0\le\deg n_1\le H}\cdots\sum_{0\le\deg n_e\le H}|\mu(n_1)\cdots\mu(n_e)|\prod_{r=1}^{v}q^{-\deg N_r}=\sum_{m=0}^{\infty}\frac{h_G^+(m)}{q^m}.$$

Now combining the lemma with (2.47) we obtain

$$g(H)=q^{Hv}\rho_G+R,\tag{2.50}$$

where

$$\rho_G=\sum_{0\le\deg n_1\le\infty}\cdots\sum_{0\le\deg n_e\le\infty}\mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}q^{-\deg N_r},$$

and

$$\begin{aligned}|R|=q^{Hv}&\sum_{0\le\deg n_1\le\infty}\cdots\sum_{0\le\deg n_e\le\infty}\mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}q^{-\deg N_r}\\&-q^{Hv}\sum_{0\le\deg n_1\le H}\cdots\sum_{0\le\deg n_e\le H}\mu(n_1)\cdots\mu(n_e)\prod_{r=1}^{v}q^{-\deg N_r}.\end{aligned}$$

Now

$$\rho_G=\sum_{m=0}^{\infty}\frac{1}{q^m}\sum_{\deg(N_1\cdots N_v)=m}\mu(n_1)\cdots\mu(n_e)=\sum_{m=0}^{\infty}\frac{h_G(m)}{q^m},$$

where for $m\ge 0$ we have

$$h_G(m)=\sum_{\deg(N_1\cdots N_v)=m}\mu(n_1)\cdots\mu(n_e).$$

We note that the function $h_G(m)$ is multiplicative by Lemma 2.3.2. In a similar way to Lemma 2.2.5 we have $h_G(0) = 1, h_G(1) = 0, h_G(p) = 0$ and $h_G(p^\alpha) = 0$, for all $\alpha > v$. Thus, by the multiplicativity,

$$\rho_G = \sum_{m=0}^{\infty} \frac{h_G(m)}{m} = \prod_{p \text{ prime}} \left(1 + \frac{f_G(p^2)}{q^{2p}} + \ldots + \frac{f_G(p^v)}{q^{pv}}\right).$$

Therefore, by Lemma 2.2.3, we have

$$\rho_G = \prod_{p \text{ prime}} Q_G\left(\frac{1}{q^p}\right). \tag{2.51}$$

It only remains to estimate $|R|$.

Lemma 2.3.4. *We have* $|R| = O\left(\frac{q^{Hv}(\log\log H)^w}{H}\right)$, *for some constant* w *that does not depend on* H.

Proof. We have

$$|R| \leq q^{H(v-1)} \sum_{j=1}^{e} \sum_{\deg n_1=0}^{\infty} \cdots \sum_{\deg n_{j-1}=0}^{\infty} \sum_{\deg n_j > H} \sum_{\deg n_{j+1}=0}^{\infty} \cdots \sum_{\deg n_e=0}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} q^{-N_r}.$$

All terms in the sum on j are analogous; so assuming that the first is the largest, we have

$$|R| \leq C_1\ q^{H^(v-1)} \sum_{\deg n_1 > H} \sum_{n_2=0}^{\infty} \sum_{n_{j+1}=0}^{\infty} \cdots \sum_{n_e=0}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} q^{-N_r}, \tag{2.52}$$

where C_1 is a function of e and not H. Let

$$R_1 := \sum_{\deg n_1 > H} \sum_{\deg n_2=0}^{\infty} \cdots \sum_{\deg n_e=0}^{\infty} |\mu(n_1)\cdots\mu(n_e)| \prod_{r=1}^{v} q^{-N_r}. \tag{2.53}$$

We will treat an edge $e_1 = \{u, s\}$ differently to the other edges. For a given $(n_1, \ldots, n_e)$ of squarefree numbers we have two special integers,

$$N_u = \operatorname{lcm}(n_1, n_{\alpha_1}, \ldots n_{\alpha_k}), \quad N_s = \operatorname{lcm}(n_1, n_{\beta_1}, \ldots n_{\beta_k}).$$

We also remark that we may have $N_u = \operatorname{lcm}(n_1)$ or $N_s = \operatorname{lcm}(n_1)$.

For any edge e_j with $2 \leq j \leq e$ we define $d_j = \gcd(n_1, n_j)$. Since the n_j are squarefree, we have

$$n_j = d_j n_j', \quad d_j | n_1, \quad \gcd(n_1, n_j') = 1.$$

Then it is clear that

$$N_u = \operatorname{lcm}(n_1, d_{\alpha_1} n'_{\alpha_1}, \dots, d_{\alpha_k} n'_{\alpha_k}) = n_1 \operatorname{lcm}(n'_{\alpha_1}, \dots, n'_{\alpha_k})$$

and

$$N_s = n_1 \operatorname{lcm}(n'_{\beta_1}, \dots, n'_{\beta_l}).$$

For any other vertex with $t \neq u$ and $t \neq s$, we have

$$\begin{aligned} N_t &= \operatorname{lcm}(n_{t_1}, \dots, n_{t_m}) = \operatorname{lcm}(d_{t_1} n'_{t_1}, \dots, d_{t_m} n'_{t_m}) \\ &= \operatorname{lcm}(d_{t_1}, \dots, d_{t_m}) \operatorname{lcm}(n'_{t_1}, \dots, n'_{t_m}), \end{aligned}$$

where m will vary with t. Substituting the equations for N_u, N_s and N_t into the definition of R_1 in (2.54) we obtain

$$\begin{aligned} R_1 = &\sum_{\deg n_1 > H} \sum_{\deg n_2 = 0}^{\infty} \cdots \sum_{\deg n_e = 0}^{\infty} |\mu(n_1) \cdots \mu(n_e)| q^{-\deg N_u} q^{-\deg N_s} \prod_{\substack{1 \le t \le v \\ t \neq u,\ t \neq s}} q^{-N_t} \\ = &\sum_{\deg n_1 > H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} \sum_{\deg n'_2 = 0}^{\infty} \cdots \sum_{\deg n'_e = 0}^{\infty} \frac{|\mu(n_2) \cdots \mu(n_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \dots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \dots, n'_{\beta_l})} \\ &\times \prod_{\substack{1 \le t \le v \\ t \neq u,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m}) \operatorname{lcm}(n'_{t_1}, \dots, n'_{t_m})} \\ = &\sum_{\deg n_1 > H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} \prod_{\substack{1 \le t \le v \\ t \neq r,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})} \\ &\times \sum_{\deg n'_2 = 0}^{\infty} \cdots \sum_{\deg n'_e = 0}^{\infty} \left(\frac{|\mu(d_2 n'_2) \cdots \mu(d_e n'_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \dots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \dots, n'_{\beta_l})} \right. \\ &\left. \times \prod_{\substack{1 \le t \le v \\ t \neq u,\ t \neq s}} \frac{1}{\operatorname{lcm}(n'_{t_1}, \dots, n'_{t_m})} \right) \\ \le &\sum_{\deg n_1 > H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2 | n_1} \cdots \sum_{d_e | n_1} |\mu(d_2) \cdots \mu(d_e)| \prod_{\substack{1 \le t \le v \\ t \neq u,\ t \neq s}} \frac{1}{\operatorname{lcm}(d_{t_1}, \dots, d_{t_m})} \\ &\times \sum_{\deg n'_2 = 0}^{\infty} \cdots \sum_{\deg n'_e = 0}^{\infty} \left(\frac{|\mu(n'_2) \cdots \mu(n'_e)|}{\operatorname{lcm}(n'_{\alpha_1}, \dots, n'_{\alpha_k}) \operatorname{lcm}(n'_{\beta_1}, \dots, n'_{\beta_l})} \right. \\ &\left. \times \prod_{\substack{1 \le t \le v \\ t \neq u,\ t \neq s}} \frac{1}{\operatorname{lcm}(n'_{t_1}, \dots, n'_{t_m})} \right). \end{aligned}$$

The expression

$$\sum_{\deg n_2'=0}^{\infty} \cdots \sum_{\deg n_e'=0}^{\infty} \frac{|\mu(n_2')\cdots\mu(n_e')|}{\operatorname{lcm}(n_{\alpha_1}',\ldots,n_{\alpha_k}')\operatorname{lcm}(n_{\beta_1}',\ldots,n_{\beta_l}')} \prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}} \frac{1}{\operatorname{lcm}(n_{t_1}',\ldots,n_{t_m}')}$$

is finite by Lemma 2.3.3 (but this time considering the graph G without the edge $\{u,s\}$). Thus, for some constant C_1, we have

$$\begin{aligned} R_1 &\le C_2 \sum_{\deg n_1>H} \frac{|\mu(n_1)|}{n_1^2} \sum_{d_2|n_1} \cdots \sum_{d_e|n_1} |\mu(d_2)\cdots\mu(d_e)| \prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}} \frac{1}{\operatorname{lcm}(d_{t_1},\ldots,d_{t_m})} \\ &= C_2 \sum_{\deg n_1>H} \frac{|\mu(n_1)|}{n_1^2} f_{G,e}(n_1), \end{aligned} \tag{2.54}$$

where the arithmetic function $f_{G,e}$ is defined as follows.

$$f_{G,e}(n) = \sum_{d_2|n} \cdots \sum_{d_e|n} |\mu(d_2)\cdots\mu(d_e)| \prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}} \frac{1}{\operatorname{lcm}(d_{t_1},\ldots,d_{t_m})}.$$

We note that there is a factor $\operatorname{lcm}(d_{t_1},\ldots,d_{t_m})$ for each vertex other than u or s. The function $f_{G,e}$ is a multiplicative function. We have $f_{G,e}(p^k) = f_{G,e}(p)$ for any power of a prime p with $k \ge 2$, because in the definition of $f_{G,e}(p^k)$ only the divisors 1 and p of p^k give non null terms. When $n = p$ we have

$$f_{G,e}(p) = 1 + \frac{A_1}{p} + \cdots + \frac{A_{v-2}}{p^{v-2}},$$

where A_i is the number of ways that

$$\prod_{\substack{1\le t\le v\\ t\ne u,\ t\ne s}} |\mu(d_2)\cdots\mu(d_e)| \operatorname{lcm}(d_{t_1},\ldots,d_{t_m}) = p^i,$$

where every divisor in the product $d_h \mid n = p$ can only be 1 or p. The inequality $A_i \le 2^{e-1}$ do not depend on p, and so there must be a number w, independent of p, such that

$$f_{G,e}(p^k) = f_{G,e}(p) \le \left(1+\frac{1}{p}\right)^w.$$

Since $f_{G,e}$ is multiplicative we have, for any squarefree n,

$$f_{G,e}(n) \le \prod_{p|n} \left(1+\frac{1}{p}\right)^w = \left(\frac{\sigma(n)}{n}\right)^w, \quad |\mu(n)| = 1. \tag{2.55}$$

Substituting (2.55) into (2.54) yields

$$\begin{aligned} R_1 &\le C_2 \sum_{\deg n > H}^{\infty} \frac{|\mu(n)|}{n^2} \left(\frac{\sigma(n)}{n} \right)^w \le C_2 \sum_{\deg n > H}^{\infty} \frac{1}{n^2} \left(\frac{\sigma(n)}{n} \right)^w \\ &\le C_2 \; q^H \sum_{j > H}^{\infty} \frac{1}{j^2} \left(\frac{\sigma(j)}{j} \right)^w . \end{aligned}$$

It is well known that $\sigma(j) = O(j \log\log j)$ (see, for example, [40]), and thus

$$R_1 = O\left(\frac{q^H (\log\log H)^w}{H} \right). \tag{2.56}$$

Combining (2.56), (2.52) and (2.53) completes the proof of Lemma 2.3.4. □

Combining (2.50), (2.51) and Lemma 2.3.4 concludes the proof of Theorem 2.3.1.

2.4 Combined pairwise coprime and non-coprime conditions

Section 2.2 and Subsection 2.1.4 suggest that counting arrays that are pairwise non-coprime can be done via the counting of arrays that possess pairwise coprimality conditions. In fact, we can easily generalise our analysis to tuples with coprimality conditions on some pairs of elements and non-coprimality conditions on other pairs of elements.

Suppose we wish to estimate the number of arrays with a fixed number of bounded elements that have both pairwise coprimality and pairwise non-coprimality conditions. Using the notation of Section 2.2, we consider a set G_1 with vertices $V = \{1, \dots, v\}$ and edges $E_1 \subseteq \{\{1,2\}, \{1,3\}, \dots, \{v-1, v\}\}$. The set E_1 dictates the required pairwise coprimality conditions, as shown below. Another set G_2 with vertices V and edges $E_2 \subseteq \{\{1,2\}, \{1,3\}, \dots, \{v-1, v\}\}$ is used to determine the pairwise non-coprimality conditions, as shown below. Clearly, $E_1 \cap E_2 = \emptyset$ since no pair of elements can be both coprime and non-coprime. Next, we define

$$G_1(H) := \{(a_1, \dots, a_v) \in \mathbb{N}^v : a_r \leq H,\ \gcd(a_r, a_s) = 1 \text{ if } \{r,s\} \in E_1\},$$

and

$$G_2(H) := \{(a_1, \dots, a_v) \in \mathbb{N}^v : a_r \leq H,\ \gcd(a_r, a_s) \neq 1 \text{ if } \{r,s\} \in E_2\}.$$

Since we want to estimate arrays that satisfy both pairwise coprimality and pairwise non-coprimality conditions, we want to estimate $|G_1(H) \cap G_2(H)|$. We select an arbitrary $\{r_1, s_1\} \in E_2$. Let

$$\begin{aligned}&(G_1 \cup \{r_1, s_1\})(H)\\ &:= \{(a_1, \dots, a_v) \in \mathbb{N}^v : a_r \leq H,\ \gcd(a_r, a_s) = 1 \text{ if } \{r,s\} \in (E_1 \cup \{r_1, s_1\})\},\end{aligned}$$

and

$$\begin{aligned}&(G_2/\{r_1, s_1\})(H)\\ &:= \{(a_1, \dots, a_v) \in \mathbb{N}^v : a_r \leq H,\ \gcd(a_r, a_s) \neq 1 \text{ if } \{r,s\} \in E_2/\{r_1, s_1\}\},\end{aligned}$$

It clear that

$$\begin{aligned}&|G_1(H) \cap G_2(H)|\\ &= |G_1(H) \cap (G_2/\{r_1, s_1\})(H)| - |(G_1 \cup \{r_1, s_1\})(H) \cap (G_2/\{r_1, s_1\})(H)|.\end{aligned}$$

Notice that $|E_2/\{r_1, s_1\}| = |E_2| - 1$. If $|(G_2/\{r_1, s_1\})(H)| \neq 0$ we repeat the process for both $G_1(H) \cap (G_2/\{r_1, s_1\})(H)$ and $(G_1 \cup \{r_1, s_1\})(H) \cap (G_2/\{r_1, s_1\})(H)$. Eventually, the process will terminate. We will be left with a calculation only involving subsets of $G_1(H)$; all whose cardinality can be estimated by Section 2.2.

Chapter 3

GCD of shifted sets

3.1 The GCD of shifted sets

3.1.1 Introduction

With the exception of Section 3.2, this section is entirely based on [47]. Section 3.2 is joint work with Igor Shparlinski. Let $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ be a nonzero vector. The *approximate common divisor problem*, introduced by Howgrave-Graham [49] for $n = 2$, can generally be described as follows. Suppose we are given two bounds $D > H \geq 1$. Assuming that for some h_i with $|h_i| \leq H$, $i = 1, \ldots, n$, we have

$$\gcd(a_1 + h_1, \ldots, a_n + h_n) > D, \tag{3.1}$$

the task is to determine the shifts $h_1, \ldots, h_n$. If it is also requested that $h_1 = 0$, then we refer to the problem as the *partial approximate common divisor problem* (certainly in this case the task is to find the shifts faster than via complete factorisation of $a_1 \neq 0$).

This problem has a strong cryptographic motivation as it is related to some attacks on the RSA and some other cryptosystems, see [11, 15, 18, 49, 77] and references therein for various algorithms and applications. In particular, much of the current motivation for studying approximate common divisor problems stems from the search for efficient and reliable *fully homomorphic encryption*, that is, encryption that allows arithmetic operations on encrypted data, see [21, 37, 67]. In Subsection 3.1.7, we give a brief overview of the approximate common divisor problem and its application to an attack on RSA and to fully homomorphic encryption.

Here we consider a dual question and show that for any $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{Z}^n$, there are shifts $|h_i| \leq H$, $i = 1, \ldots, n$, for which (3.1) holds with a relatively large value of D. We also give results for some related questions.

Throughout we use $\gcd(\mathbf{x})$ to mean $\gcd(x_1, \ldots, x_n)$ for any $\mathbf{x} \in \mathbb{Z}^n$. We also denote the height of $\mathbf{x}$ with $\mathfrak{H}(\mathbf{x}) = \max\{|x_1|, \ldots, |x_n|\}$.

The implied constants in the symbols 'O', '$\ll$' and '$\gg$' may occasionally, where obvious, depend on the integer parameter n and the real positive parameter ε, and are absolute otherwise.

Our treatment of this question is based on some results of Baker and Harman [5] (see also [4]). For an integer $n > 1$ and real positive $\varepsilon < 1$, we define $\kappa(n, \varepsilon)$ as the solution $\kappa > 0$ to the equation

$$\frac{n(\varepsilon\kappa - 1)}{n-1} = \frac{1}{2^{2+\max\{1,\kappa\}} - 4}. \tag{3.2}$$

The solution is unique, as the left hand side of (3.2) is monotonically increasing (as a function of κ) from $-n/(n-1)$ to $+\infty$ on $[0, \infty)$ whilst the right hand side of (3.2) is positive and monotonically non-increasing.

We also set

$$\vartheta(n, \varepsilon) = \frac{1}{(n-1)} \left(1 - \frac{1}{\varepsilon\kappa(n, \varepsilon)}\right).$$

It easy to see from (3.2) that $\varepsilon\kappa(n, \varepsilon) > 1$, so $\vartheta(n, \varepsilon) > 0$.

Our main results is as follows.

Theorem 3.1.1. *For any vector* $\mathbf{a} \in \mathbb{Z}^n$*, any real positive* $\varepsilon < 1$ *and*

$$H \geq \mathfrak{H}(\mathbf{a})^{\varepsilon},$$

there exists a vector $\mathbf{h} = (h_1, \ldots, h_n) \in \mathbb{Z}^n$ *of height*

$$\mathfrak{H}(\mathbf{h}) \leq H$$

such that

$$\gcd(\mathbf{a} + \mathbf{h}) \gg \mathfrak{H}(\mathbf{h}) H^{\vartheta(n,\varepsilon)}.$$

Next, we are interested in asking for which $\mathbf{h}$ the shifted set is pairwise coprime.

For $\mathbf{a} \in \mathbb{Z}^n$ we denote by $L(\mathbf{a})$ the smallest H such that there is an $\mathbf{h} \in \mathbb{Z}^n$ with $\mathfrak{H}(\mathbf{h}) = H$ such that

$$\gcd(a_i + h_i, a_j + h_j) = 1, \qquad 1 \leq i < j \leq n.$$

For $n = 2$, and thus $\mathbf{a} = (a_1, a_2) \in \mathbb{Z}^2$, Erdős [30, Equation (3)] has given the bound

$$L(\mathbf{a}) \ll \frac{\log \min\{|a_1|, |a_2|\}}{\log \log \min\{|a_1|, |a_2|\}}.$$

However the method of [30] does not seem to generalise to $n \geq 3$.

Theorem 3.1.2. *For an arbitrary* $\mathbf{a} \in \mathbb{Z}^n$ *we have*

$$L(\mathbf{a}) \ll \log^2 \mathfrak{H}(\mathbf{a}).$$

Note that our argument allows the replacement of $\mathfrak{H}(\mathbf{a})$ by $\mathfrak{H}^*(\mathbf{a})$, where $\mathfrak{H}^*(\mathbf{a})$ is the second largest $|a_i|$, $i = 1, \ldots, n$.

It is also interesting to investigate as for Theorem 3.1.2 but with a relative primality condition. For $\mathbf{a} \in \mathbb{Z}^n$ we denote by $\ell(\mathbf{a})$ the smallest H such that there is a vector $\mathbf{h} \in \mathbb{Z}^n$ with $\mathfrak{H}(\mathbf{h}) = H$ and

$$\gcd(a_1 + h_1, \ldots, a_n + h_n) = 1.$$

A very simple argument, based on the Chinese Remainder Theorem, implies the following result, which generalises [30, Equation (2)].

Theorem 3.1.3. *For infinitely many* $\mathbf{a} \in \mathbb{Z}^n$ *we have*

$$\ell(\mathbf{a}) \gg \left(\frac{\log \mathfrak{H}(\mathbf{a})}{\log \log \mathfrak{H}(\mathbf{a})} \right)^{1/n}.$$

Note that Theorem 3.1.3 is essentially an explicit version of a result of Huck and Pleasants [52].

Finally, we give a result regarding the greatest common divisor of a set of integers. A probabilistic method using random sets of integers, as shown below, was discussed in 1999, see [17]. It is clear that for non-zero vector $\mathbf{a} \in \mathbb{Z}^n$ and arbitrary vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ we have

$$\gcd(a_1, \ldots, a_n) \mid \gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y}),$$

where

$$\mathbf{a} \cdot \mathbf{x} = \sum_{i=1}^{n} a_i x_i \qquad \text{and} \qquad \mathbf{a} \cdot \mathbf{y} = \sum_{i=1}^{n} a_i y_i.$$

Let $R(\mathbf{a}, h)$ be the number of vectors $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ with positive components and of height $\mathfrak{H}(\mathbf{x}), \mathfrak{H}(\mathbf{y}) \le h$ for which

$$\gcd(a_1, \ldots, a_n) = \gcd(\mathbf{a} \cdot \mathbf{x}, \mathbf{a} \cdot \mathbf{y}). \tag{3.3}$$

By [35, Theorem 3] we have

$$|R(\mathbf{a}, h) - \zeta(2)^{-1} h^{2n}| \le h^{2n - 1/n} (h \mathfrak{H}(\mathbf{a}))^{o(1)}$$

as $\max\{h, \mathfrak{H}(\mathbf{a})\} \to \infty$, and where $\zeta(s)$ is the Riemann zeta function.

We now claim the following (rather modest) improvement.

Theorem 3.1.4. *Let* $n \ge 2$ *and let* $\mathbf{a} \in \mathbb{Z}^n$*. Then, for* $\max\{h, \mathfrak{H}(\mathbf{a})\} \to \infty$*,*

$$|R(\mathbf{a}, h) - \zeta(2)^{-1} h^{2n}| \le h^{2n - n/(n^2 - n + 1)} (h \mathfrak{H}(\mathbf{a}))^{o(1)}.$$

3.1.2 Proof of Theorem 3.1.1

Let $\|\xi\|$ denote the distance between a real ξ and the closest integer.

We first give a short outline of the proof. Our argument is based on a result of Baker and Harman [5]. In particular, we infer from [5, Theorem 1] that for an arbitrary R, not too small compared to $\mathfrak{H}(\mathbf{a})$ and another parameter Q, not too large compared to R there is an integer $r \in [R, QR]$ such that

$$\left\|\frac{a_i}{r}\right\| \le Q^{-1/n}, \qquad i = 1, \ldots, n. \tag{3.4}$$

This means that for some integers $h_i \in [-rQ^{-1/n}, rQ^{-1/n}]$ we have

$$\frac{a_i}{r} + \frac{h_i}{r} \in \mathbb{Z}, \qquad i = 1, \ldots, n,$$

which immediately implies that

$$r \mid \gcd(a_1 + h_1, \ldots, a_n + h_n).$$

We now give qualitative estimates and optimise the parameters.

We note that by [5, Theorem 1], see also [5, Equation (2.1)] that gives an explicit formula for the constant $\gamma(K)$ below, we have

Lemma 3.1.5. *Suppose that for fixed $n > 1$ and $K > 0$, and for some sufficiently large real positive Q and R we have*

$$\left(\sum_{i=1}^{n} a_i^2\right)^{1/2} \le R^K \qquad \textit{and} \qquad C_1(K,n) \le Q \le R^{\gamma(K)},$$

where

$$\gamma(K) = \frac{1}{2^{2+\max\{1,K\}} - 4}.$$

Let $\psi_1, \ldots, \psi_n$ be positive real numbers with

$$\psi_i \le c_2(K,n)(\log Q)^{-n}, \quad i = 1, \ldots, n, \qquad \textit{and} \qquad \psi_1 \cdots \psi_n = Q^{-1}.$$

Then there exists a positive integer $r \in [R, 2QR]$ with

$$\left\|\frac{a_i}{r}\right\| \le \psi_i, \quad i = 1, \ldots, n,$$

where $C_1(K,n)$ and $c_2(K,n)$ depend on at most K and n.

To prove Theorem 3.1.1, we choose some parameters Q and R that satisfy the assumptions of Lemma 3.1.5 with $K = \kappa(n,\varepsilon)$, where $\kappa(n,\varepsilon)$ is given by (3.2), and we then set $\psi_i = Q^{-1/n}$, $i = 1, \ldots, n$. Then by Lemma 3.1.5, there exists an integer r with $R \le r \le 2QR$ such that (3.4) holds. So for some integers h_i with $|h_i| \le rQ^{-1/n}$ we have

$$a_i + h_i \equiv 0 \pmod{r}, \qquad i = 1, \ldots, n.$$

More precisely, suppose that for some constant $A \ge 1$ we choose R such that for

$$Q = (0.5)^{n/(n-1)} A^{-1} R^{\gamma(K)}, \tag{3.5}$$

we have

$$2Q^{1-1/n} R = H. \tag{3.6}$$

We note from (3.5) that $Q \le R^{\gamma(K)}$. Then, we see from (3.5) and (3.6) that

$$R = A^{(n-1)/(n\gamma(K)-\gamma(K)+n)} H^{n/(n\gamma(K)-\gamma(K)+n)}.$$

Then, taking A to satisfy

$$A^{(n-1)/(n\gamma(K)-\gamma(K)+n)} = n^{1/2K},$$

due to our choice of $K = \kappa(n, \varepsilon)$, we have

$$R = n^{1/2K} H^{n/(n\gamma(K)-\gamma(K)+n)} = n^{1/2K} H^{1/\varepsilon K}. \tag{3.7}$$

Using (3.7), we derive

$$\left(\sum_{i=1}^{n} a_i^2 \right)^{1/2} \le n^{1/2} H^{1/\varepsilon} = R^K.$$

Thus, R satisfies the conditions of Lemma 3.1.5. We also have

$$Q^{1/n} \gg R^{\gamma(K)/n} \gg H^{\gamma(K)/\varepsilon n K}. \tag{3.8}$$

In particular, by increasing H, we can make sure that $Q \ge C_1(K, n)$ and $Q^{-1/n} \le c_2(K, n)(\log Q)^{-n}$. Therefore, Lemma 3.1.5 indeed applies. Hence for $\mathbf{h} = (h_1, \ldots, h_n)$ we have

$$\mathfrak{H}(\mathbf{h}) \le rQ^{-1/n} \le 2Q^{1-1/n} R = H$$

and

$$\gcd(\mathbf{a} + \mathbf{h}) \ge r \ge \mathfrak{H}(\mathbf{h}) Q^{1/n}. \tag{3.9}$$

We now see from (3.2) that

$$\frac{\gamma(K)}{\varepsilon n K} = \frac{\varepsilon K - 1}{\varepsilon (n-1) K},$$

which together with (3.9) and (3.8) completes the proof.

3.1.3 Proof of Theorem 3.1.2

We recall the following well-known result of Iwaniec [54] on the *Jacobsthal problem.* For a given r, let $C(r)$ be the maximal length of a sequence of consecutive integers, each divisible by one of r arbitrarily chosen primes. Iwaniec [54] gives the following bound on $C(r)$.

Lemma 3.1.6. *For a given $r > 1$ we have*

$$C(r) \ll (r \log r)^2.$$

We are now ready to prove Theorem 3.1.2. It is based on the following inductive construction.

We set $h_1 = 0$. Now, for $i = 2, \ldots, n$, assuming that $h_1, \ldots, h_{i-1}$ are chosen and we define h_i, as the smallest non-negative integer with

$$\gcd\left(\prod_{j=1}^{i-1}(a_j + h_j), a_i + h_i\right) = 1.$$

We consider the Jacobsthal sequence starting at a_i with the prime factors of

$$\prod_{j=1}^{i-1}(a_j + h_j).$$

Therefore, h_i can be bounded by the maximal length of such a sequence with

$$r = \omega\left(\prod_{j=1}^{i-1}(a_j + h_j)\right)$$

prime factors.

We now show that if n is a positive integer and $a = \mathfrak{H}(\mathbf{a})$ then

$$\mathfrak{H}(\mathbf{h}) \ll \log^2 a. \tag{3.10}$$

Let $\omega(k)$, as usual, denote the number of distinct prime divisors of an integer $k \geq 1$. So, by Lemma 3.1.6,

$$C(\omega(k)) \ll (\omega(k) \log(\omega(k))^2 \ll \log^2 k.$$

for any $k > 1$. From the trivial bound $\omega(k)! \leq k$ and the Stirling formula we have

$$\omega(k) \ll \frac{\log k}{\log \log k}$$

for any integer $k \geq 1$. Now a straight forward inductive argument, after simple calculations, implies (3.10) and concludes the proof.

3.1.4 Proof of Theorem 3.1.3

Let us choose a sufficiently large parameter H and the first $(2H+1)^n$ primes $p_{i_1,\ldots,i_n} > H$ for $-H \le i_1, \ldots, i_n \le H$.

For each $k = 1, \ldots, n$ we define a_k as the smallest positive integer with

$$a_k \equiv -i_k \pmod{p_{i_1,\ldots,i_n}}, \qquad -H \le i_1, \ldots, i_n \le H.$$

Set $\mathbf{a} = (a_1, \ldots, a_n)$. For any $\mathbf{h} \in \mathbb{Z}^n$ with $\mathfrak{H}(\mathbf{h}) \le H$, we have

$$p_{h_1,\ldots,h_n} \mid \gcd(a_1 + h_1, \ldots, a_n + h_n).$$

This implies that $\ell(\mathbf{a}) \ge H$.

It remains to estimate $\mathfrak{H}(\mathbf{a})$. We have $p_{i_1,\ldots,i_n} \ll H^n \log H$ for $-H \le i_1, \ldots, i_n \le H$. Therefore,

$$\mathfrak{H}(\mathbf{a}) \le \prod_{-H \le i_1,\ldots,i_n \le H} p_{i_1,\ldots,i_n} = \exp(O(H^n \log H)) = \exp(O(\ell(\mathbf{a})^n \log \ell(\mathbf{a}))),$$

which completes the proof.

3.1.5 Proof of Theorem 3.1.4

It is enough to consider the case where $\gcd(a_1, \ldots, a_n) = 1$.

We can certainly assume that $n \le \log h$, for otherwise the bound is trivial.

Let μ denote the Möbius function, that is $\mu(1) = 1$, $\mu(d) = 0$ if $d \ge 2$ is not squarefree, and $\mu(d) = (-1)^{\omega(d)}$ otherwise, where $\omega(d)$, as before, is the number of prime divisors of an integer $d \ge 1$.

As in the proof of [35, Theorem 3], by the inclusion exclusion principle we have

$$R(\mathbf{a}, h) = \sum_{d \ge 1} \mu(d) U_d(\mathbf{a}, h)^2,$$

where for an integer $d \ge 1$, we denote by $U_d(\mathbf{a}, h)$ the number of vectors $\mathbf{x} \in \mathbb{Z}^n$ with positive components and of height $\mathfrak{H}(\mathbf{x}) \le h$ for which $d \mid \mathbf{a} \cdot \mathbf{x}$.

We now recall from [35] some estimates on $U_d(\mathbf{a}, h)$.

More precisely, for $1 \le d \le 2h/3n$ we have

$$\left| U_d(\mathbf{a}, h)^2 - \frac{h^{2n}}{d^2} \right| \le 8nd^{-1}h^{2n-1}, \tag{3.11}$$

see [35, Equation (8)]. The proof of (3.11) also relies on the bound

$$U_d(\mathbf{a}, h) \le d^{n-1} \left(h/d + 1 \right)^n . \tag{3.12}$$

that holds for any integer $d \ge 1$.

For any squarefree $d \ge 1$ we also have the bound

$$U_d(\mathbf{a}, h) \le h^{n-1} \left(hd^{-1/n} + 1 \right), \tag{3.13}$$

see [35, Equation (10)].

Therefore, choosing some parameter D, we write

$$R(\mathbf{a},h) = M + O(\Delta_1 + \Delta_2) \tag{3.14}$$

where

$$\begin{aligned} M &= \sum_{d\le 2h/3n} \mu(d) U_d(\mathbf{a},h)^2, \\ \Delta_1 &= \sum_{2h/3n<d\le D} \mu(d) U_d(\mathbf{a},h)^2, \\ \Delta_2 &= \sum_{d>D} \mu(d) U_d(\mathbf{a},h)^2. \end{aligned}$$

Using (3.11), we derive

$$\begin{aligned} M &= \sum_{d\le 2h/3n} \mu(d) \left(\frac{h^{2n}}{d^2} + O\left(h^{2n-1}d^{-1}\right)\right) \\ &= h^{2n} \sum_{d\le 2h/3n} \frac{\mu(d)}{d^2} + O\left(h^{2n-1}\log h\right). \end{aligned}$$

Since

$$\sum_{d\le 2h/3n} \frac{\mu(d)}{d^2} = \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} + O\left(1/h\right) = \zeta(2)^{-1} + O\left(1/h\right),$$

see [41, Theorem 287], we derive

$$M = h^{2n}\zeta(2)^{-1} + O\left(h^{2n-1}\log h\right). \tag{3.15}$$

To estimate Δ_1 we apply the bound (3.12), which for $d \ge 2h/3n$ can be simplified as $U_d(\mathbf{a},h) = O(d^{n-1})$. Therefore,

$$\Delta_1 \ll \sum_{2h/3n<d\le D} d^{n-1} U_d(\mathbf{a},h) \le D^{n-1} \sum_{2h/3n<d\le D} U_d(\mathbf{a},h). \tag{3.16}$$

Using the same argument as the proof of [35, Theorem 3], based on a bound of the divisor function $\tau(k)$, we obtain

$$\begin{aligned} \sum_{d>2h/3n} U_d(\mathbf{a},h) &= \sum_{d>2h/3n} \sum_{\substack{\mathfrak{H}(\mathbf{x})\le h \\ d\mid \mathbf{a}\cdot\mathbf{x}}} 1 \\ &= \sum_{h(\mathbf{x})\le h} \sum_{\substack{d>2h/3n \\ d\mid \mathbf{a}\cdot\mathbf{x}}} 1 \le \sum_{h(\mathbf{x})\le h} \tau(\mathbf{a}\cdot\mathbf{x}) \le h^n (h\mathfrak{H}(\mathbf{a}))^{o(1)}, \end{aligned} \tag{3.17}$$

where $\mathbf{x}$ runs through integral vectors with positive components. Hence, we see that (3.16) yields the estimate

$$\Delta_1 \ll D^{n-1}h^n(h\mathfrak{H}(\mathbf{a}))^{o(1)}. \tag{3.18}$$

Finally, to estimate Δ_2 we apply the bound (3.13) and, as before, derive

$$\Delta_2 \ll h^{n-1}\left(hD^{-1/n}+1\right)\sum_{d>D} U_d(\mathbf{a},h) \le h^{2n-1}\left(hD^{-1/n}+1\right)(h\mathfrak{H}(\mathbf{a}))^{o(1)}. \tag{3.19}$$

Substituting the bounds (3.15), (3.18) and (3.19) into (3.14), we obtain

$$R(\mathbf{a},h) = h^{2n}\zeta(2)^{-1} + O\left(\left(h^{2n-1}+D^{n-1}h^n+h^{2n}D^{-1/n}\right)(h\mathfrak{H}(\mathbf{a}))^{o(1)}\right).$$

Now, choosing

$$D = h^{n^2/(n^2-n+1)},$$

we conclude the proof.

3.1.6 Comments

We remark that it is also interesting to study analogous questions for polynomials with integer coefficients or over finite fields, see [29, 34, 71] for some polynomial versions of the approximate common divisor problem. Some of our techniques can be extended to this case. However some important ingredients, such as the results of Baker and Harman [4, 5], are missing.

3.1.7 The approximate common divisor problem and cryptography

In this subsection, we make a few comments about solving the approximate common divisor problem. We also discuss the problem's applications to both an attack on RSA and fully homomorphic encryption. Given that this subsection is peripheral to this chapter, the comments are neither comprehensive nor rigorous.

Howgrave-Graham [49] discussed two methods of solving the approximate common divisor problem; the continued fraction approach and the lattice approach. To illustrate the continued fraction approach, consider the following algorithm. We wish to input two similar bit-sized integers a_0, b_0. The algorithm outputs all integers $d = b_0^\alpha,\ \alpha > 1/2$ such that there exist integers x_0, y_0 with

$$|x_o|, |y_0| < X = b_0^{\max\{2\alpha-1,1-\alpha\}},$$

and d divides both $a_0 + x_0$ and $b_0 + y_0$, or report that no such d exists. We recall from the study of continued fractions that for a_0/b_0 there are only finitely many $g_i, h_i,\ i = 1, \ldots, m$ such that

$$\left|\frac{a_0}{b_0} - \frac{g_i}{h_i}\right| < \frac{1}{2h_0^2}.$$

Moreover each fraction g_i/h_i is a convergent of a_0/b_0. The values of d can then be calculated as

$$d_i = \min_k\{\max\{|kg_i - a_0|, |kh_i - b_0|\}\},\ i = 1, \ldots, m.$$

Next we illustrate the lattice approach method on the partial approximate common divisor problem. Here we input integers a_0, b_0 and $\epsilon, \alpha \in (0,1)$ and seek to output all integers $d < M = b_0^\alpha$ such that there exists an x_0 with $|x_0| < X = b_0^{\alpha^2-\epsilon},\ d|(a_0 + x_0),\ d|b_0$, or report no such d exists. We start by reframing the problem from integers to polynomials. Let $q_1(x) = a_0 + x$ and $q_2(x) = b_0$. We require a x_0 such that $q_1(x_0) \equiv q_2(x_0) \equiv 0 \pmod{d}$. Now let

$$\begin{aligned} r(x) &= r_0 + r_1(x) + \ldots + r_h x^h \\ &= \sum_{0 \leq i \leq u} \mu_i(x) q_1(x)^{u-i} q_2(x)^i, \end{aligned}$$

where u, h are functions of α and ϵ. Note that if $q_1(x_0) \equiv q_2(x_0) \equiv 0 \pmod{d}$ then $r(x) \equiv 0 \pmod{d^u}$. Also there is considerable scope to vary $\mu_i(x)$. So we now use lattice/matrix methods to find a $r(x)$ with small enough coefficients $r_0, \ldots, r_h$ so that the roots of $r(x)$ over $\mathbb{Z}$ are less than d^u. Thus, $r(x) \equiv 0 \pmod{d^u}$ when x is a root of $r(x)$ (in practice we can use the LLL algorithm to find the roots, see [60]). The roots of this $r(x)$ are therefore possible roots of $q_1(x)$ and $q_2(x)$.

Coron and May [18] outline a possible attack on RSA code using the approximate common divisor problem. For RSA, we keep two primes p and q private but we let $N = pq$ and N is made public. We also make public an encoding key e and keep private a decoding key f. The decoding key f is calculated (privately) as the inverse of e modulo $\varphi(N)$. To use RSA we take a message and raise it to a power modulo N. The power to be used is e to encode, and f to decode.

The attack on RSA we discuss was the first polynomial time algorithm to find p, q given N, e, f with p, q being the same bit-size. We have $N = pq$ and we let $s = p+q-1$. Given N, s it is easy to find p, q. We let $U = ef - 1$ and note that since $ef \equiv 1 \pmod{\varphi}(N)$, it follows that $\varphi(n)|U$. Also $N - s = \varphi(n)$. So we have $(N - s)|(N - s)$ and $(N - s)|U$. Letting $a_0 = N,\ x_0 = -s$ and $b_0 = U$ allows us to use the Howgrave-Graham algorithm to solve what is now an approximate common divisor problem.

Finally, we make some comments about fully homomorphic encryption based on [21]. This encryption is described as the holy grail of encryption, see [67]. This form of encryption allows repeated addition and multiplication of encoded data. In turn this holds the prospect of many applications such as minimizing non-interactive zero-knowledge proofs, see [39], improved delegation of computing, see [13], cloud computing, see [63] and voting, see [67].

A simple example of fully homomorphic encryption would be to pick an arbitrary odd integer, p, not necessarily prime. To encode a message $m \in \{0,1\}$, pick random $s, r \in \mathbb{Z}$ with $2r < p/2$, and encode m to $ps + 2r + m$. To decode the encoded message, we calculate $(ps + 2r + m \pmod{p}) \pmod{2}$. Since modular arithmetic respects addition and multiplication so will this one addition or multiplication encryption (we discuss multiple operations shortly). Specifically, suppose we encode m_1 and m_2 to get n_1 and n_2 respectively and pass the two encoded messages on to a separate entity. The entity responds with $n_1 + n_2$ and $n_1 n_2$. On decoding these two messages, we obtain $m_1 + m_2$ and $m_1 m_2$ respectively.

To turn this into a public key system, we publicise arbitrary $x_i = ps_i + 2r_i,\ i = 1, \ldots, n$ such that $x_{\alpha_1} + \cdots + x_{\alpha_k} + m,\ x_{\alpha_i} \in \{x_1, \ldots, x_k\}$ sufficiently masks the value of m for certain choices of x_i. To encode m, we calculate $x_{\alpha_1} + \cdots + x_{\alpha_k} + m$ using one of these choices. To decode, we simple proceed as before, by the application of modulo p and then modulo 2. The recovery of p from the public values of x_i, and hence an attack on the encryption, is then a classic approximate common divisor problem. The p can be calculated from the values of x_i using the algorithm ideas proposed by Howgrave-Graham mentioned previously.

For repeated addition and/or multiplication this encryption will fail as the r_i terms will exceed p, thereby invalidating the process. Gentry [37] proposed a solution for repeated addition and/or multiplication using the ideas of ‘bootstrapping’ and ‘squashing the decryption circuit’.

3.2 The GCD of sets shifted by a positive integer

In this subsection, we study positive integer translations applied to $\mathbf{a}$. That is,

$$(a_1, \ldots, a_n), (a_1 + 1, \ldots, a_n + 1), \ldots$$

We investigate $t(\mathbf{a})$; the smallest non-negative integer j such that

$$\gcd(a_1 + j, \ldots, a_n + j) = 1.$$

We note for all $\mathbf{a}$ with $\gcd(\mathbf{a}) = 1$ we have $t(\mathbf{a}) = 0$. So a lower bound for $t(\mathbf{a})$ is $t(\mathbf{a}) \geq 0$. We also note that $t(\mathbf{a})$ always exists; we just take j to be the distance from $\mathfrak{H}(\mathbf{a})$ to the lowest prime number greater than $\mathfrak{H}(\mathbf{a})$. Using this fact and [6, Theorem 1] gives $t(\mathbf{a}) = O(\mathfrak{H}(\mathbf{a})^{0.525})$.

Denote by $j(s)$ the Jacobsthal function; the smallest integer t such that any sequence of t consecutive integers contains an element that is coprime to s.

Theorem 3.2.1. *Let $\boldsymbol{a} = (a_1, \ldots, a_n)$ consist of at least 2 distinct elements. Then*

$$t(\boldsymbol{a}) \ll (\log \mathfrak{H}(\boldsymbol{a}))^2. \tag{3.20}$$

Proof. We start by showing that

$$t(\mathbf{a}) < L(\mathbf{a}) := \min_{\substack{a_r, a_s \in \{a_1, \ldots, a_n\} \\ a_r > a_s}} j(a_r - a_s).$$

Without loss of generality rearrange the elements of $\mathbf{a}$, so that $a_1 \geq a_2 \geq \ldots \geq a_n$. Suppose to the contrary we have $t(\mathbf{a}) \geq L(\mathbf{a})$. Fix two integers, r and s, such that $L(\mathbf{a}) = j(a_r - a_s)$. It follows that there exists positive integers q_j such that

$$\gcd(a_r + j, a_s + j) = q_j \neq 1, \quad 0 \leq j \leq L(\mathbf{a}) - 1.$$

Since $a_r + j = (a_s + j) - (a_r - a_s)$, we have

$$\gcd(a_r + j, a_s + j) = \gcd(a_r - a_s, a_s + j).$$

So

$$\gcd(a_r - a_s, a_s + j) = q_j \neq 1, \quad 0 \leq j \leq L(\mathbf{a}) - 1.$$

But now the $j(a_r - a_s)$ consecutive integers $a_s, a_s + 1, \ldots, a_s + j(a_r - a_s) - 1$ are all not coprime to $a_r - a_s$; contradicting the definition of the Jacobsthal function. This proves that $t(\mathbf{a}) < L(\mathbf{a})$.

Using the corollary in [54], we have

$$\begin{aligned} t(\mathbf{a}) &\ll \min_{\substack{a_r, a_s \in \{a_1, \dots, a_n\} \\ a_r > a_s}} \left(\omega(a_r - a_s) \log \omega(a_r - a_s)\right)^2 \\ &\ll \left(\omega(\mathfrak{H}(\mathbf{a})) \log \omega(\mathfrak{H}(\mathbf{a}))\right)^2 . \end{aligned} \tag{3.21}$$

By taking logarithms of both sides of the inequalities

$$\left(\frac{\omega(m)}{2}\right)^{\frac{\omega(m)}{2}} \leq \omega(m)! \leq m$$

we obtain $\omega(m) \log \omega(m) \ll \log m$. Combining this result with (3.21) yields

$$t(\mathbf{a}) \ll \left(\log \mathfrak{H}(\mathbf{a})\right)^2 ,$$

which completes the proof. □

Chapter 4

Polynomial irreducibility

4.1 The Eisenstein criterion

4.1.1 Introduction

This section is entirely based on [44]. We obtain a more precise version of an asymptotic formula of A. Dubickas for the number of monic Eisenstein polynomials of fixed degree d and of height at most H, as $H \to \infty$. In particular, we give an explicit bound for the error term. We also obtain an asymptotic formula for arbitrary Eisenstein polynomials of height at most H. The Eisenstein criterion [28] is a simple well-known sufficient criterion to establish that an integer coefficient polynomial (and hence a polynomial with rational coefficients) is irreducible, see also [19]. We recall that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \tag{4.1}$$

is called an *Eisenstein polynomial* if for some prime p we have

(i) $p \mid a_i$ for $i = 0, \ldots, n-1$,

(ii) $p^2 \nmid a_0$,

(iii) $p \nmid a_n$.

For integers $d \geq 2$ and $H \geq 1$, we let $\mathcal{E}_n(H)$ be the set of all Eisenstein polynomials with $a_n = 1$ and of height at most H, that is, satisfying $\max\{|a_0|, \ldots, |a_{n-1}|\} \leq H$.

Dubickas [26] has given an asymptotic formula for the cardinality $E_n(H) = |\mathcal{E}_n(H)|$, see also [23]. Here we address this question again and obtain a more precise version of this result with an explicit error term. Using techniques different to those in [26], we also obtain an asymptotic formula for the number of polynomials, whether monic or non-monic, that satisfy the Eisenstein criterion. We also observe that, since the publication of [44], Dotti and Micheli [24] have used a function field analogue of these results to calculate densities for both monic and arbitrary Eisenstein polynomials (that is, ϑ_n in Theorem 4.1.1 and ρ_n in Theorem 4.1.2).

Theorem 4.1.1. *We have,*

$$E_n(H) = \vartheta_n 2^n H^n + \begin{cases} O\left(H^{n-1}\right), & \text{if } n > 2, \\ O(H(\log H)^2), & \text{if } n = 2, \end{cases}$$

where

$$\vartheta_n = 1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{n+1}}\right).$$

We remark that our argument is quite similar to that of Dubickas [26], and in fact the method of [26] can also produce a bound on the error term in an asymptotic formula for $E_n(H)$. However we truncate the underlying inclusion-exclusion formula differently. This allows us to get a better bound on the error term than that which follows from the approach of [26].

We also obtain an asymptotic formula for the cardinality $F_n(H) = |\mathcal{F}_n(H)|$ of the set $\mathcal{F}_n(H)$ of Eisenstein polynomials of the form (4.1) of height at most H, that is, satisfying $\max\{|a_0|, \ldots, |a_n|\} \le H$. This result does not seem to have any predecessors.

Theorem 4.1.2. *We have,*

$$F_n(H) = \rho_n 2^{n+1} H^{n+1} + \begin{cases} O\left(H^{n}\right), & \text{if } n > 2, \\ O(H^2(\log H)^2), & \text{if } n = 2, \end{cases}$$

where

$$\rho_n = 1 - \prod_{p \text{ prime}} \left(1 - \frac{(p-1)^2}{p^{n+2}}\right).$$

4.1.2 Preparations

We start by deriving a formula for the number of monic polynomials for which a given positive number satisfies conditions that are similar, but not equivalent, to the Eisenstein criterion. Let s be a positive integer. Let $\mathcal{G}_n(s, H)$ be the set of monic polynomials of the form (4.1), of height at most H, and such that

(i) $s \mid a_i$ for $i = 0, \ldots, n-1$,

(ii) $\gcd(a_0/s, s) = 1$.

It is easy to see that [26, Lemma 2] immediately implies the following result.

Lemma 4.1.3. *For $s \le H$, we have*

$$|\mathcal{G}_n(s,H)| = \frac{2^n H^n \varphi(s)}{s^{n+1}} + O\left(\frac{H^{n-1}2^{\omega(s)}}{s^{n-1}}\right).$$

We now derive a version of Lemma 4.1.3 for arbitrary polynomials. Let $\mathcal{H}_n(s,H)$ be the set of polynomials of the form (4.1), of height at most H, and such that

(i) $s \mid a_i$ for $i = 0, \ldots, n-1$,

(ii) $\gcd(a_0/s, s) = 1$,

(iii) $\gcd(a_n, s) = 1$.

We also use the well-known identity

$$\sum_{d|s} \frac{\mu(d)}{d} = \frac{\varphi(s)}{s}, \tag{4.2}$$

see [41, Section 16.3].

We now define the following generalisation of the Euler function,

$$\varphi(s,H) = \sum_{\substack{|a| \le H \\ \gcd(a,s)=1}} 1,$$

and use the following well-known consequence of the sieve of Eratosthenes.

Lemma 4.1.4. *For any integer $s \ge 1$, we have*

$$\varphi(s,H) = \frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right).$$

Proof. Using the inclusion-exclusion principle we write

$$\varphi(s,H) = \sum_{d|s} \mu(d) \sum_{\substack{|a| \le H \\ d|a}} 1 = \sum_{d|s} \mu(d) \left(2 \left\lfloor \frac{H}{d} \right\rfloor + 1\right).$$

Therefore,

$$\varphi(s,H) = \sum_{d|s} \mu(d) \left(\frac{2H}{d} + O(1)\right) = 2H \sum_{d|s} \frac{\mu(d)}{d} + O\left(\sum_{d|s} |\mu(d)|\right).$$

Recalling (4.2) and that

$$\sum_{d|s} |\mu(d)| = 2^{\omega(s)},$$

see [41, Theorem 264], we obtain the desired result. □

We also recall that

$$2^{\omega(s)} \le \tau(s) = s^{o(1)} \tag{4.3}$$

as $s \to \infty$, see [41, Theorem 317].

Next, we obtain an asymptotic formula for $|\mathcal{H}_n(s,H)|$.

Lemma 4.1.5. *For $s \le H$, we have*

$$|\mathcal{H}_n(s,H)| = \frac{2^{n+1}H^{n+1}\varphi^2(s)}{s^{n+2}} + O\left(\frac{H^n}{s^{n-1}}2^{\omega(s)}\right).$$

Proof. Fix a $n > 1$. For every $i = 1, \ldots, n-1$, the number of admissible values of a_i (that is, with $|a_i| \le H$ and $s \mid a_i$) is equal to

$$2\left\lfloor \frac{H}{s} \right\rfloor + 1 = \frac{2H}{s} + O(1). \tag{4.4}$$

We now consider the admissible values of a_0. Writing $a_0 = sm$ with an integer m satisfying $|m| \le H/s$ and $\gcd(m,s) = 1$, we see from Lemma 4.1.4 that a_0 takes

$$\varphi(s, \lfloor H/s \rfloor) = \frac{2H\varphi(s)}{s^2} + O\left(2^{\omega(s)}\right) \tag{4.5}$$

distinct values.

Lemma 4.1.4 also implies that a_d takes

$$\varphi(s, H) = \frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right) \tag{4.6}$$

distinct values.

Combining (4.4), (4.5) and (4.6), we obtain

$$\begin{aligned}|\mathcal{H}_n(s,H)| &= \left(\frac{2H}{s} + O(1)\right)^{n-1}\left(\frac{2H\varphi(s)}{s^2} + O\left(2^{\omega(s)}\right)\right)\\ &\qquad\qquad\left(\frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right)\right)\\ &= \left(\left(\frac{2H}{s}\right)^{n-1} + O\left(\left(\frac{H}{s}\right)^{n-2}\right)\right)\left(\frac{2H\varphi(s)}{s^2} + O\left(2^{\omega(s)}\right)\right) \qquad (4.7)\\ &\qquad\qquad\left(\frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right)\right).\end{aligned}$$

Hence, using the trivial bound $\varphi(s) \le s$ and that by (4.3) we have $2^{\omega(s)} = O(H)$, we see that

$$\left(\frac{2H\varphi(s)}{s^2} + O\left(2^{\omega(s)}\right)\right)\left(\frac{2H\varphi(s)}{s} + O\left(2^{\omega(s)}\right)\right) = \frac{4H^2\varphi^2(s)}{s^3} + O\left(H2^{\omega(s)}\right).$$

Substituting into (4.7), and using that $\varphi(s) \le s$ again, we obtain

$$|\mathcal{H}_n(s,H)| = \frac{2^{n+1}H^{n+1}\varphi^2(s)}{s^{n+2}} + O\left(\frac{H^n}{s^{n-1}} + \frac{H^{n-1}}{s^{n-2}}2^{\omega(s)} + \frac{H^n}{s^{n-1}}2^{\omega(s)}\right).$$

Taking into account that $s \le H$, we conclude the proof. □

4.1.3 Proof of Theorem 4.1.1

We now prove the main result for monic Eisenstein polynomials.

The inclusion-exclusion principle implies that

$$E_n(H) = -\sum_{s=2}^{H} \mu(s)\, |\mathcal{G}_n(s,H)|.$$

Substituting the asymptotic formula of Lemma 4.1.3 for $|\mathcal{G}_n(s,H)|$, yields

$$\begin{aligned} E_n(H) &= -\sum_{s=2}^{H} \mu(s) \left(\frac{2^n H^n \varphi(s)}{s^{n+1}} \right) + O\left(\sum_{s=2}^{H} \left(\frac{H}{s} \right)^{n-1} 2^{\omega(s)} \right) \\ &= -2^n H^n \sum_{s=2}^{\infty} \frac{\mu(s)\varphi(s)}{s^{n+1}} + O\left(H^n \sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{n+1}} + H^{n-1} \sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{n-1}} \right). \end{aligned} \tag{4.8}$$

(since $\varphi(s) \le s$, the series in the main term converges absolutely for $n \ge 2$). Since $\mu(s)\varphi(s)/s^{n+1}$ is a multiplicative function, it follows that

$$\begin{aligned} -\sum_{s=2}^{\infty} \frac{\mu(s)\varphi(s)}{s^{n+1}} &= 1 - \sum_{s=1}^{\infty} \frac{\mu(s)\varphi(s)}{s^{n+1}} \\ &= 1 - \prod_{p \text{ prime}} \left(1 - \frac{\varphi(p)}{p^{n+1}} \right) = 1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{n+1}} \right). \end{aligned} \tag{4.9}$$

We also have

$$\sum_{s=H+1}^{\infty} \frac{\varphi(s)}{s^{n+1}} \le \sum_{s=H+1}^{\infty} \frac{1}{s^n} = O\left(H^{-n+1} \right). \tag{4.10}$$

Recalling (4.3), for $n > 2$ we immediately obtain

$$\sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{n-1}} = O(1). \tag{4.11}$$

For $n = 2$, we recall that

$$\sum_{s \le t} 2^{\omega(s)} \le \sum_{s \le t} \tau(s) = (1 + o(1)) t \log t$$

as $t \to \infty$, see [41, Theorem 320].

Thus, via partial summation, we derive

$$\sum_{s=2}^{H} \frac{2^{\omega(s)}}{s} = O\left(\sum_{t=2}^{H} \frac{\log t}{t} \right) = O\left((\log H)^2 \right). \tag{4.12}$$

Substituting (4.9), (4.10), (4.11) and (4.12) into (4.8), we conclude the proof.

4.1.4 Proof of Theorem 4.1.2

The inclusion-exclusion principle implies that

$$|\mathcal{F}_n(H)| = -\sum_{s=2}^{H} \mu(s)|\mathcal{H}_n(s,H)|.$$

Using the asymptotic formula of Lemma 4.1.5 yields

$$\begin{aligned}|\mathcal{F}_n(H)| &= -\sum_{s=2}^{H} \mu(s)\left(\frac{2^{n+1}H^{n+1}\varphi^2(s)}{s^{n+2}}\right) + O\left(\sum_{s=2}^{H} \frac{H^n\, 2^{\omega(s)}}{s^{n-1}}\right) \\ &= -2^{n+1}H^{n+1}\sum_{s=2}^{\infty} \frac{\mu(s)\varphi^2(s)}{s^{n+2}} \\ &\qquad + O\left(H^{n+1}\sum_{s=H+1}^{\infty} \frac{\varphi^2(s)}{s^{n+2}} + H^n \sum_{s=2}^{H} \frac{2^{\omega(s)}}{s^{n-1}}\right)\end{aligned} \tag{4.13}$$

(since $\varphi(s) \le s$, the series in the main term converges absolutely for $n \ge 2$). In a similar manner to that used for (4.9), we note that $\mu(s)\varphi^2(s)/s^{n+2}$ is a multiplicative function, so it follows that

$$\begin{aligned}-\sum_{s=2}^{\infty} \frac{\mu(s)\varphi^2(s)}{s^{n+2}} &= 1-\sum_{s=1}^{\infty} \frac{\mu(s)\varphi^2(s)}{s^{n+2}} \\ &= 1 - \prod_{p \text{ prime}} \left(1 - \frac{\varphi^2(p)}{p^{n+2}}\right) = 1 - \prod_{p \text{ prime}} \left(1 - \frac{(p-1)^2}{p^{n+2}}\right).\end{aligned} \tag{4.14}$$

Since $\varphi(s) \le s$, we also have

$$\sum_{s=H+1}^{\infty} \frac{\varphi^2(s)}{s^{n+2}} \le \sum_{s=H+1}^{\infty} \frac{1}{s^n} = O\left(H^{-n+1}\right). \tag{4.15}$$

Substituting (4.14) and (4.15) into (4.13), and recalling (4.11) and (4.12), we conclude the proof.

4.1.5 Further Comments on ϑ_n and ρ_n

As $n \to \infty$,

$$\begin{aligned}\vartheta_n &= 1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{n+1}}\right) = \sum_{s=2}^{\infty} \frac{\mu(s)\varphi(s)}{s^{n+1}} \\ &= \frac{1}{2^{n+1}} - \frac{2}{3^{n+1}} + \sum_{s=4}^{\infty} \frac{\mu(s)\varphi(s)}{s^{n+1}} = \frac{1}{2^{n+1}} - \frac{2}{3^{n+1}} + O\left(\int_3^{\infty} \frac{1}{\sigma^{n-1}} d\sigma\right) \\ &= \frac{1}{2^{n+1}} - \frac{2}{3^{n+1}} + O\left(\frac{1}{n3^n}\right) = \frac{1}{2^{n+1}} + O\left(\frac{1}{3^n}\right).\end{aligned}$$

Similarly,

$$\rho_n = \frac{1}{2^{n+2}} + O\left(\frac{1}{3^n}\right), \qquad n \to \infty.$$

We have computed in Table 4.1 the approximate values of ϑ_n and ρ_n for $n = 2, \ldots, 10$. The first 10,000 primes have been used in the calculations. The values of ϑ_n are consistent with those given in [26], but the values of ρ_n seems to be new.

Table 4.1: Approximate values of ϑ_n and ρ_n for $n = 2, \ldots, 10$.

n	ϑ_n	ρ_n
2	0.2515	0.1677
3	0.0953	0.0556
4	0.0409	0.0224
5	0.0186	0.0099
6	0.0088	0.0046
7	0.0042	0.0022
8	0.0021	0.0010
9	0.0010	0.0005
10	0.0005	0.0003

4.2 Eisenstein shifted polynomials

4.2.1 Introduction

This section is entirely based on [45]. We study polynomials with integer coefficients which become Eisenstein polynomials after the additive shift of a variable. We call such polynomials *shifted Eisenstein polynomials.* We determine an upper bound on the maximum shift that is needed given a shifted Eisenstein polynomial and also provide a lower bound on the density of shifted Eisenstein polynomials, which is strictly greater than the density of classical Eisenstein polynomials. We also show that the number of irreducible degree n polynomials that are not shifted Eisenstein polynomials is infinite.

We recall that

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in \mathbb{Z}[x] \tag{4.16}$$

is called an *Eisenstein polynomial*, or is said to be *irreducible by Eisenstein* if for some prime p we have

(i) $p \mid a_i$ for $i = 0, \ldots, n-1$,

(ii) $p^2 \nmid a_0$,

(iii) $p \nmid a_n$.

We sometimes say that f is *irreducible by Eisenstein with respect to prime* p if p is one such prime that satisfies the conditions (i), (ii) and (iii) above (see [19] regarding the early history of the irreducibility criterion).

Recently, motivated by a question of Dobbs and Johnson [23] several statistical results about the distribution of Eisenstein polynomials have been obtained. Dubickas [26] has found the asymptotic density for *monic* polynomials f of a given degree $\deg f = n$ and growing height

$$H(f) = \max_{i=0,\ldots,n} |a_i|. \tag{4.17}$$

In Section 4.1 we gave an improvement in the error term in the asymptotic formula of [26] and also calculated the density of general Eisenstein polynomials.

Clearly, the irreducibility of polynomials is preserved under shifting of the argument by a constant. Thus, it makes sense to investigate polynomials which become Eisenstein polynomials after shifting the argument. More precisely, here we study polynomials $f(x) \in \mathbb{Z}[x]$ for which there exists an integer s such that $f(x+s)$ is an Eisenstein polynomial. We call such $f(x) \in \mathbb{Z}[x]$ a *shifted Eisenstein polynomial.* We call the corresponding s an *Eisenstein shift of f with respect to p.*

For example, for $f(x) = x^2 + 4x + 5$, it is easy to see that $s = -1$ is an Eisenstein shift with respect to $p = 2$.

Here we estimate the smallest possible s which transfers a shifted Eisenstein polynomial $f(x)$ into an Eisenstein polynomial $f(x+s)$. We also estimate the density of shifted Eisenstein polynomials and show that it is strictly greater than the density of Eisenstein polynomials. On the other hand, we show that there are irreducible polynomials that are not shifted Eisenstein polynomials.

More precisely, let $\mathcal{I}_n$, $\mathcal{E}_n$ and $\overline{\mathcal{E}}_n$ denote the set of irreducible, Eisenstein and shifted Eisenstein polynomials, of degree n over the integers.

Trivially,

$$\mathcal{E}_n \subseteq \overline{\mathcal{E}}_n \subseteq \mathcal{I}_n.$$

We show that all inclusions are proper and that $\overline{\mathcal{E}}_n \setminus \mathcal{E}_n$ is quite "massive".

4.2.2 Notation

We define $\mathcal{I}_n(H)$, $\mathcal{E}_n(H)$ and $\overline{\mathcal{E}}_n(H)$ as the subsets of $\mathcal{I}_n$, $\mathcal{E}_n$ and $\overline{\mathcal{E}}_n$, respectively, consisting of polynomials of height at most H (where the height of a polynomial (4.16) is given by (4.17)).

Throughout Section 4.2, we will change our standard notation and use both letters p and q to represent primes.

Finally, we denote the discriminant of the function f by $D(f)$.

4.2.3 A bound on Eisenstein shifts via the discriminant

It is natural to seek a bound on the largest shift required to find a shift if it exists. In fact, for any polynomial, there is a link between the maximum shift that could determine irreducibility and the discriminant.

The following result is well-known and, in wider generality, can be proven by the theory of Newton polygons. Here we give a concise elementary proof.

Lemma 4.2.1. *Suppose $f \in \mathbb{Z}[x]$ is of degree n. If $f(x)$ is a shifted Eisenstein polynomial then there exists a prime p with $p^{n-1} \mid D(f)$ and $f(x+s)$ is irreducible by Eisenstein for some $0 \leq s < q$, where q is the largest of such primes.*

Proof. Since $f(x)$ is a shifted Eisenstein polynomial there exists an integer t and a prime p such that $f(x+t)$ is irreducible by Eisenstein with respect to p.

Recall that the discriminant of a n degree polynomial can be expressed as the determinant of the $2n-1$ by $2n-1$ Sylvester matrix. Using the Leibniz formula to express the determinant, and examining each summand, it immediately follows that $p^{n-1} \mid D(f(x+t))$. Also, the difference of any two roots of a polynomial is unchanged by increasing both roots by any integer u. So, using the definition of the discriminant, we get $D(f(x)) = D(f(x+u))$ for any integer u. So it follows that $p^{n-1} \mid D(f(x))$.

By expanding $f(x+t+kp)$ for an arbitrary integer k and examining the divisibility of coefficients, it follows that if $f(x+t)$ is Eisenstein with respect to prime p then so is $f(x+t+kp)$.

By appropriate choice of k, we can therefore find an integer s with

$$0 \le s < p \le \max\{p \text{ prime } : \ p^{n-1} \mid D(f)\}$$

such that the polynomial $f(x+s)$ is irreducible by Eisenstein. □

We also recall a classical bound of Mahler [64] on the discriminant of polynomials over $\mathbb{Z}$.

For $f(x)$ of the form (4.16), we define the *length* $L(f) = |a_0| + |a_1| + \ldots + |a_n|$.

Lemma 4.2.2. *Suppose $f \in \mathbb{Z}[x]$ is of degree n. Then*

$$|D(f)| \le n^n L(f)^{2n-2}.$$

Combining Lemmas 4.2.1 and 4.2.2 we derive the following.

Theorem 4.2.3. *Suppose $f(x) \in \mathbb{Z}[x]$. If $f(x+s)$ is not irreducible by Eisenstein for all s with*

$$0 \le s \le n^{n/(n-1)} L(f)^2,$$

then f is not a shifted Eisenstein polynomial.

We also remark that the shift s which makes $f(x+s)$ irreducible by Eisenstein with respect to prime p satisfies $f(s) \equiv 0 \pmod{p}$, which can further reduce the number of trials (however a direct irreducibility testing of $f(x)$ via the classical algorithm of Lenstra, Lenstra and Lovász [60] is still much more efficient).

4.2.4 Density of shifted Eisenstein polynomials

In this section, we show that as polynomial height grows, the density of polynomials that are irreducible by Eisenstein shifting is strictly larger than the density of polynomials that are irreducible by Eisenstein. We start by calculating a maximum height for $f(x)$ such that $f(x+1)$ is of height at most H.

Lemma 4.2.4. *For $f \in \mathbb{Z}[x]$ of degree n, we denote $f_{+1}(x) = f(x+1)$. Then $H(f_{+1}) \le 2^n H(f)$.*

Proof. Let $f(x)$ be of the form (4.16). For $i = 0, \ldots, n$, the absolute value of the coefficient of x^{n-i} in f_{+1} can be estimated as

$$\sum_{0 \le j \le i} \binom{n-j}{i-j} |a_{n-j}| \le 2^n H(f),$$

as required. □

We also need the number of polynomials, of given degree and maximum height, that are irreducible by Eisenstein. Let

$$\rho_n = 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}}\right). \tag{4.18}$$

In Section 4.1, we proved the following result.

Lemma 4.2.5. *We have,*

$$|\mathcal{E}_n(H)| = \rho_n 2^{n+1} H^{n+1} + \begin{cases} O\left(H^n\right), & \textit{if } n > 2, \\ O(H^2(\log H)^2), & \textit{if } n = 2. \end{cases}$$

We also require the following two lemmas.

Lemma 4.2.6. *Suppose that $f(x)$ is irreducible by Eisenstein with respect to prime p. Then $f(x+1)$ is not irreducible by Eisenstein with respect to p.*

Proof. Let

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{E}_n$$

be irreducible by Eisenstein with respect to prime p. The coefficient of x^0 in $f(x+1)$ is $a_n + a_{n-1} + \ldots + a_1 + a_0$, which is clearly not divisible by p. So $f(x+1)$ is not irreducible by Eisenstein with respect to p. □

Let

$$\tau_n = \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 - \sum_p \frac{(p-1)^4}{p^{2n+4}}. \tag{4.19}$$

Lemma 4.2.7. *Let*

$$\mathcal{F}_n(H) = \{f(x) \in \mathcal{E}_n(H) \ : \ f(x+1) \in \mathcal{E}_n\}.$$

Then for $n \geq 2$,

$$|\mathcal{F}_n(H)| \leq (\tau_n + o(1)) \, (2H)^{n+1}.$$

Proof. Fix some sufficiently large H and let

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathcal{E}_n(H).$$

Consequently,

$$f(x+1) = \sum_{i=0}^{n} A_i x^i,$$

with $A_i = a_i + L_i(a_n, a_{n-1}, \dots, a_{i+1})$ where $L_i(a_n, a_{n-1}, \dots, a_{i+1})$ is a linear form in $a_n, a_{n-1}, \dots, a_{i+1}$ for $i = 0, \dots, n$. In particular,

$$A_n = a_n, \quad A_{n-1} = na_n + a_{n-1}, \quad A_{n-2} = \frac{n(n-1)}{2}a_n + (n-1)a_{n-1} + a_{n-2}.$$

There are at most $O(H^n)$ polynomials $f \in \mathcal{I}_n(H)$ for which the condition

$$2A_{n-2} - (n-1)A_{n-1} = (n-1)a_{n-1} + 2a_{n-2} \neq 0. \tag{4.20}$$

is violated. Thus

$$|\mathcal{F}_n(H)| = |\mathcal{F}_n^*(H)| + O(H^n), \tag{4.21}$$

where $\mathcal{F}_n^*(H)$ is the set of polynomials $f \in \mathcal{F}_n(H)$ for which (4.20) holds.

Now, given two primes p and q, we calculate an upper bound on the number $N_n(H, p, q)$ of $f \in \mathcal{F}_n^*(H)$ such that

- $f(x)$ is irreducible by Eisenstein with respect to prime p;
- $f(x+1)$ is irreducible by Eisenstein with respect to prime q.

We see from Lemma 4.2.6 that $N_n(H, p, q) = 0$ if $p = q$. So we now always assume that $p \neq q$.

To do so, we estimate (inductively over $i = n, n-1, \dots, 0$) the number of possibilities for the coefficient a_i of f, provided that higher coefficients $a_n, \dots, a_{i+1}$ are already fixed.

- Possible values of a_n: We know that $a_n \not\equiv 0 \pmod p$ and $a_n \not\equiv 0 \pmod q$. Therefore, we conclude that the number of possible values of a_n is $2H(p-1)(q-1)/pq + O(1)$.
- Possible values of a_i, $1 \leq i < n$: Fix arbitrary $a_n, a_{n-1}, \dots, a_{i+1}$. The relations

  $$a_i \equiv 0 \pmod p \quad \text{and} \quad A_i = a_i + L_i(a_n, a_{n-1}, \dots, a_{i+1}) \equiv 0 \pmod q$$

  put a_i in a unique residue class modulo pq. It follows that the number of possible values of a_i for $i = n-1, n-2, \dots, 1$ cannot exceed $2H/pq + O(1)$.
- Possible values of a_0: We argue as before but also note that for a_0 we have the additional constraints that $A_0 \not\equiv 0 \pmod{p^2}$, $a_0 \not\equiv 0 \pmod{q^2}$ and so a_0 can take at most $2H(q-1)(p-1)/p^2q^2 + O(1)$ values.

So, for primes p and q we have

$$\begin{aligned} N_n(H, p, q) &\leq \left(\frac{2H(p-1)(q-1)}{pq} + O(1)\right)\left(\frac{2H}{pq} + O(1)\right)^{n-1} \\ &\qquad \left(\frac{2H(p-1)(q-1)}{p^2q^2} + O(1)\right) \\ &= \frac{2^{n+1}H^{n+1}(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + O(H^n). \end{aligned}$$

We also see from (4.20) that if $pq > (n+1)H$ then $N_n(H,p,q) = 0$. Hence,

$$\begin{aligned}
|\mathcal{F}_n^*(H)| &\le \sum_{\substack{p\neq q\\ pq\le (n+1)H}} \left(\frac{2^{n+1}H^{n+1}(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + O(H^n) \right)\\
&\le (2H)^{n+1} \sum_{\substack{p\neq q\\ pq\le (n+1)H}} \left(\frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} \right) + O\left(\frac{H^{n+1}\log\log H}{\log H} \right),
\end{aligned}$$

as there are $O(Q(\log Q)^{-1}\log\log Q)$ products of two distinct primes $pq \le Q$, see [80, Chapter II.6, Theorem 4]. Therefore,

$$|\mathcal{F}_n^*(H)| \le (2H)^{n+1} \sum_{\substack{p\neq q\\ pq\le (n+1)H}} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + o(H^{n+1}).$$

Since the above series converges, we derive

$$\begin{aligned}
|\mathcal{F}_n^*(H)| &\le (2H)^{n+1} \sum_{p\neq q} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} + o(H^{n+1})\\
&= (2H)^{n+1} \left(\sum_{p,q} \frac{(p-1)^2(q-1)^2}{p^{n+2}q^{n+2}} - \sum_{p} \frac{(p-1)^4}{p^{2n+4}} \right) + o(H^{n+1}),
\end{aligned}$$

which concludes the proof. □

We can now prove the main result of this section. We recall that ρ_n and τ_n are defined by (4.18) and (4.19), respectively.

Theorem 4.2.8. *For $n \ge 2$ we have*

$$\liminf_{H\to\infty} \frac{|\overline{\mathcal{E}}_n(H)|}{|\mathcal{E}_n(H)|} \ge 1 + \gamma_n,$$

where

$$\gamma_n = \frac{1}{2^{n^2+n}} \left(1 - \frac{\tau_n}{\rho_n} \right) > 0.$$

Proof. We see from Lemma 4.2.4 that for $h = H/2^n$ we have

$$\mathcal{E}_n(H) \bigcup (\mathcal{E}_n(h) \setminus \mathcal{F}_n(h)) \subseteq \overline{\mathcal{E}}_n(H),$$

where $\mathcal{F}_n(h)$ is defined as in Lemma 4.2.7. Therefore, since $\mathcal{F}_n(h) \subseteq \mathcal{E}_n(h)$, we have

$$|\overline{\mathcal{E}}_n(H)| \ge |\mathcal{E}_n(H)| + |\mathcal{E}_n(h)| - |\mathcal{F}_n(h)|.$$

Recalling Lemmas 4.2.5 and 4.2.7, we derive the desired inequality.

It now remains to show that $\gamma_n > 0$. So it suffices to show that

$$\rho_n - \tau_n > 0.$$

From (4.18) and (4.19), we have

$$\begin{aligned}
\rho_n - \tau_n &= 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}}\right) - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 + \sum_p \frac{(p-1)^4}{p^{2n+4}} \\
&\geq 1 - \prod_p \left(1 - \frac{(p-1)^2}{p^{n+2}}\right) - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 \\
&= \sum_{k=1}^{\infty} (-1)^{k+1} \sum_{p_1 < \ldots < p_k} \prod_{j=1}^{k} \frac{(p_j - 1)^2}{p_j^{n+2}} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 .
\end{aligned}$$

Discarding from the first sum all positive terms (corresponding to odd k) except for the first one, we obtain

$$\begin{aligned}
\rho_n - \tau_n &\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \sum_{p_1 < \ldots < p_{2k}} \prod_{j=1}^{2k} \frac{(p_j - 1)^2}{p_j^{n+2}} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 \\
&\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \frac{1}{(2k)!} \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^{2k} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 \\
&\geq \sum_p \frac{(p-1)^2}{p^{n+2}} - \sum_{k=1}^{\infty} \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^{2k} - \left(\sum_p \frac{(p-1)^2}{p^{n+2}}\right)^2 .
\end{aligned}$$

Hence, denoting

$$P_n = \sum_p \frac{(p-1)^2}{p^{n+2}},$$

we derive

$$\rho_n - \tau_n \geq P_n - \frac{P_n^2}{1 + P_n^2} - P_n^2.$$

Since

$$P_n \leq P_2 \leq 0.18,$$

the result now follows. □

It is certainly easy to get an explicit lower bound on γ_n in Theorem 4.2.8. Various values of γ_n using the first 10,000 primes are given in Table 4.2.

Table 4.2: Approximations to γ_n for some n

n	γ_n
2	1.33×10^{-2}
3	2.36×10^{-4}
4	9.44×10^{-7}
5	9.28×10^{-10}
10	7.70×10^{-34}

This prompts the following question. Is it possible to obtain tighter bound or exact values of

$$\liminf_{H\to\infty} \frac{|\overline{\mathcal{E}}_n(H)|}{(2H)^{n+1}} \qquad \text{and} \qquad \limsup_{H\to\infty} \frac{|\overline{\mathcal{E}}_n(H)|}{(2H)^{n+1}} \tag{4.22}$$

(they most likely coincide)? Very recently, prompted by [45], Micheli and Schnyder [68] have answered these questions using a local to global principle for density computations over a free $\mathbb{Z}$-module of finite rank.

4.2.5 Infinitude of $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$

We note that a consequence of Lemma 4.2.1 is that any polynomial belongs to $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ if its discriminant is $n-1$ free. Hence, we would expect the size of $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ to be "massive". In fact, for a fixed degree greater than or equal to 2, we can prove that the number of irreducible polynomials that are not shifted Eisenstein polynomials is infinite.

Theorem 4.2.9. *The set $\mathcal{I}_n \setminus \overline{\mathcal{E}}_n$ is infinite for all $n \geq 2$.*

Proof. Let $f(x) = x^n + x + p$ for some $n \geq 2$ and some prime p. Then f is irreducible (see [73, Lemma 9]). Since no prime can divide the coefficient of x it follows that f is not an Eisenstein polynomial.

We show that f cannot be an Eisenstein shift polynomial. Suppose this is not the case. Then for some integer s the polynomial $f(x+s)$ is an Eisenstein polynomial with respect to some prime q. We have

$$f(x+s) = x^n + nsx^{n-1} + \ldots + (ns^{n-1}+1)x + s^n + s + p.$$

However, the congruences $ns \equiv 0 \pmod q$ and $ns^{n-1} + 1 \equiv 0 \pmod q$ cannot hold simultaneously.

So we conclude that for any $n \geq 2$, the infinite set

$$\{f(x) = x^n + x + p \ : \ p \text{ prime}\}$$

consists of irreducible polynomials that are not shifted Eisenstein polynomials. □

We also expect that

$$\lim_{H\to\infty} \frac{|\mathcal{I}_n(H) \setminus \overline{\mathcal{E}}_n(H)|}{|\mathcal{I}_n(H)|} > 0.$$

For example, it is natural to expect that there is a positive proportion of polynomials $\mathcal{I}_n(H)$ with a square-free discriminant, which by Lemma 4.2.1 puts them in the set $\mathcal{I}_n(H) \setminus \overline{\mathcal{E}}_n(H)$. However, even the conditional (under the ABC-conjecture) results of Poonen [75] about square-free values of multivariate polynomials are not sufficient to make this claim.

We can, however, prove an inferior result, for degrees greater than 2, involving height constrained polynomials that can be shifted to a height constrained Eisenstein polynomial.

Theorem 4.2.10. *Let*

$$\overline{\mathcal{C}}_n(H) = \{f(x) \in \overline{\mathcal{E}}_n(H) \ : \ f(x+s) \in \mathcal{E}_n(H) \text{ for some } s \in \mathbb{Z}\}.$$

Then for $n > 2$,

$$\limsup_{H\to\infty} \frac{|\overline{\mathcal{C}}_n(H)|}{2H(2H+1)^n} < 1.$$

Proof. Let $\overline{\mathcal{C}}_n(d,H)$ be the set of all polynomials

$$f(x+s) = a_n(x+s)^n + a_{n-1}(x+s)^{n-1} + \ldots + a_1(x+s) + a_0 \in \mathbb{Z}[x]$$

such that

(i) $s \in \mathbb{Z}$,

(ii) $H(f(x+s)) \le H$,

(iii) $f(x)$ is Eisenstein with respect to all the prime divisors of d,

(iv) $H(f(x)) \le H$,

(v) $|s| < d$.

Note that each element of $\overline{\mathcal{C}}_n(d,H)$ may come from several pairs (f,s).

We also observe that the set of all $f(x)$ described in (iii) and (iv) is precisely $\mathcal{H}_n(d,H)$, where $\mathcal{H}_n(d,H)$ is the set of polynomials (4.16) of height at most H and such that

(a) $d \mid a_i$ for $i = 0,\ldots,n-1$,

(b) $\gcd(a_0/d, d) = 1$,

(c) $\gcd(a_n, d) = 1$.

It then follows from the condition (v) in the definition of $\overline{\mathcal{C}}_n(d,H)$ that

$$|\overline{\mathcal{C}}_n(d,H)| \leq 2d|\mathcal{H}_n(d,H)|.$$

Using the inclusion-exclusion principle implies that

$$|\overline{\mathcal{C}}_n(H)| \leq \sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} |\overline{\mathcal{C}}_n(d,H)|,$$

and so

$$|\overline{\mathcal{C}}_n(H)| \leq \sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} 2d\mathcal{H}_n(d,H). \tag{4.23}$$

From [44], we have

$$|\mathcal{H}_n(d,H)| = \frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+2}} + O\left(\frac{H^n}{d^{n-1}}2^{\omega(d)}\right). \tag{4.24}$$

Combining (4.23) and (4.24), we have

$$\begin{aligned}|\overline{\mathcal{C}}_n(H)| &\leq \sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} 2d\left(\frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+2}} + O\left(\frac{H^n 2^{\omega(d)}}{d^{n-1}}\right)\right)\\ &= 2\sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} \left(\frac{2^{n+1}H^{n+1}\varphi^2(d)}{d^{n+1}} + O\left(\frac{H^n 2^{\omega(d)}}{d^{n-2}}\right)\right).\end{aligned}$$

Hence,

$$\begin{aligned}\frac{|\overline{\mathcal{C}}_n(H)|}{2H(2H+1)^n} &\leq 2\sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} \left(\frac{\varphi^2(d)}{d^{n+1}} + O\left(\frac{2^{\omega(d)}}{Hd^{n-2}}\right)\right)\\ &= 2\sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} \frac{\varphi^2(d)}{d^{n+1}} + O\left(\frac{1}{H}\sum_{2\leq d\leq H}^{H} \frac{2^{\omega(d)}}{d^{n-2}}\right),\end{aligned}$$

for all $n > 2$. It's easy to see that

$$\sum_{d=2}^{H} \frac{2^{\omega(d)}}{d^{n-2}} = o(H),$$

for all $n > 2$. Hence,

$$\frac{|\overline{\mathcal{C}}_n(H)|}{2H(2H+1)^n} \leq 2\sum_{\substack{2\leq d\leq H\\ \mu(d)=-1}} \frac{\varphi^2(d)}{d^{n+1}} + o(1).$$

So

$$\begin{aligned}\limsup_{H\to\infty} \frac{|\overline{\mathcal{C}}_n(H)|}{2H(2H+1)^n} &\le 2\sum_{\mu(d)=-1} \frac{\varphi^2(d)}{d^{n+1}} \le 2\sum_{\mu(d)=-1} \frac{1}{d^{n-1}} = 2\sum_{k=0}^{\infty}\sum_{\omega(d)=2k+1} \frac{1}{d^{n-1}} \\ &\le 2\sum_{k=0}^{\infty}\left(\frac{1}{(2k+1)!}\left(\sum_p \frac{1}{p^{n-1}}\right)^{2k+1}\right) \\ &\le 2\sinh\left(\sum_p \frac{1}{p^{n-1}}\right) \le 2\sinh\left(\sum_p \frac{1}{p^2}\right).\end{aligned}$$

As direct calculations show that

$$\sum_p \frac{1}{p^2} < 0.46,$$

the result follows. □

We infer from [14, Theorem 1] that

$$\lim_{H\to\infty} \frac{|\mathcal{I}_n(H)|}{2H(2H+1)^n} = 1,$$

which when combined with Theorem 4.2.10 yields

$$\liminf_{H\to\infty} \frac{|\mathcal{I}_n(H)\setminus\overline{\mathcal{C}}_n(H)|}{|\mathcal{I}_n(H)|} > 0,$$

for $n > 2$.

4.2.6 Comments

It is easy to see that the results of the work can be extended to monic polynomials.

We note that testing whether $f \in \mathcal{E}_n$ can be done in an obvious way via several greatest common divisor computations. We, however, do not know any efficient algorithm to test whether $f \in \overline{\mathcal{E}}_n$. The immediate approach, based on Lemma 4.2.1 involves integer factorisation and thus does not seem to lead to a polynomial time algorithm. It is possible though, that one can get such an algorithm via computing greatest common divisor of pairwise resultants of the coefficients of $f(x+s)$ (considered as polynomials in s).

We also note that it is interesting and natural to study the *affine Eisenstein polynomials*, which are polynomials f such that

$$(cx+d)^n f\left(\frac{ax+b}{cx+d}\right) \in \mathcal{E}_n$$

for some $a, b, c, d \in \mathbb{Z}$. Very recently, prompted by [45], Micheli and Schnyder [68] have produced results regarding the density of affine Eisenstein polynomials. However the estimation of the number of polynomials of bounded height that are affine Eisenstein polynomials is still an interesting open question.

Studying the distribution of Galois groups of Eisenstein polynomials or the statistics of Eisenstein polynomials with bounded roots, are also of interest. For arbitrary monic polynomials, these questions are investigated in [20, 84] and [1], respectively.

4.3 The Dumas criterion

4.3.1 Introduction

This section on the Dumas criterion is entirely based on [46]. We study integer coefficient polynomials of fixed degree and maximum height H that are irreducible by the Dumas criterion. We call such polynomials *Dumas polynomials.* We derive upper bounds on the number of Dumas polynomials as $H \to \infty$. We also show that, for a fixed degree, the density of Dumas polynomials in the set of all irreducible integer coefficient polynomials is strictly less than 1.

The two most well-known polynomial irreducibility criteria based on coefficient prime divisibility are probably the Eisenstein criterion and the Dumas criterion. In this section, we explore densities of polynomials that satisfy the Dumas criterion. This criterion is a sufficient condition for polynomial irreducibility over $\mathbb{Z}$ (and hence $\mathbb{Q}$). It can be thought of as a generalization of the Eisenstein criterion since the Eisenstein criterion is an easy consequence of the Dumas criterion.

We can now state the Dumas criterion. Let

$$f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x] \tag{4.25}$$

be such that $a_0 a_n \neq 0$.

If the Newton polygon for f with respect to any prime is a single segment and contains no points with integer coordinates except the end points, then f is irreducible. The proof of the Dumas criterion is often based on the Newton diagram for a polynomial. The Newton diagram is similar to, but lesser known than, the Newton polygon. Construction of the Newton diagram and the proof of the Dumas criterion can be found in the book of Prasolov [76, Subsection 2.2.1]. Interested readers can also consult the 1906 paper by Dumas [27].

Whilst we will use the Newton polygon throughout this section, we note in passing that the Dumas criterion can also be expressed algebraically (see for example [9]) as follows. For any integer s and prime number p we denote by $\upsilon_p(s)$ the largest integer j such that $p^j \mid s$ (by convention $\upsilon_p(0) = 0$).

Lemma 4.3.1. *Let p be a prime number and $f(x)$ as in* (4.25)*. If*

(i) $\frac{\upsilon_p(a_i)}{i} > \frac{\upsilon_p(a_n)}{i}$ *for* $i = 1, \ldots, n-1$,

(ii) $\upsilon_p(a_0) = 0$,

(iii) $\gcd(\upsilon_p(a_n), n) = 1$,

then f is irreducible over $\mathbb{Z}$.

By way of example, the polynomial $f(x) = x^4 + 8$ with respect to the prime number 2 has a Newton polygon without integer coordinates (other than endpoints). Therefore, f is irreducible by the Dumas criterion. By contrast, the reducible polynomial $f(x) = x^4 + 4$ cannot satisfy the Dumas criterion since the coordinate $(2, 2)$ or $(2, 0)$ will appear in any Newton polygon of f. So the determination of irreducibility using the Dumas criterion is not possible for $f(x) = x^4 + 4$. For integers $n \geq 2$ and $H \geq 1$, let $\mathcal{D}_n(H)$ be the number of Dumas polynomials of height at most H, that is, satisfying $\max\{|a_0|, \dots, |a_n|\} \leq H$. Our main result is the following theorem.

Theorem 4.3.2. *We have*

$$\mathcal{D}_n(H) \leq (2H)^{n+1}\tau_n + \begin{cases} O\left(H^2(\log H)^2\right), & \text{if } n = 2, \\ O\left(H^n\right), & \text{if } n \geq 3, \end{cases}$$

where

$$\tau_n = \begin{cases} 1 - \prod_{p \text{ prime}} \left(1 - \frac{1}{p}\right)^2 \left(1 + \frac{2}{p}\right), & \text{if } n = 2, \\ 1 - \frac{1}{\zeta(n-1)}, & \text{if } n \geq 3. \end{cases}$$

We have already noted that the number of polynomials that satisfy the Eisenstein criterion, calculated in Section 4.1, provides a lower bound on $\mathcal{D}_n(H)$. Specifically,

Lemma 4.3.3. *We have*

$$\mathcal{D}_n(H) \geq \vartheta_n 2^n H^n + \begin{cases} O\left(H^{n-1}\right), & \text{if } n > 2, \\ O(H(\log H)^2), & \text{if } n = 2, \end{cases}$$

where

$$\vartheta_n = 1 - \prod_{p \text{ prime}} \left(1 - \frac{p-1}{p^{n+1}}\right).$$

We note the appearance of values of the zeta function in the main term of the estimate in Theorem 4.3.2. This arises from the fact that estimates of the densities of k-tuples of positive integers that are relatively prime play a major role in the proof of Theorem 4.3.2.

In Theorem 4.3.2, we also observe that the result for quadratics is quite different to the result for higher degree polynomials. For polynomials of degree greater than 2, we can use gcd conditions about the coefficients of the non-leading and non-constant terms to enumerate the number of Dumas polynomials. This is clearly not possible for quadratics and we are forced to consider the coefficients of the leading and non-constant terms as well.

4.3.2 Notation

Let $f(x)$ be as in (4.25). We define the height of the polynomial f as

$$H(f) = \max_{0\le i\le n} |a_i|.$$

4.3.3 Preparations

Lemma 4.3.4. *Fix $n = 2$. Suppose that $f(x)$ is as in (4.25) with $H(f) \le H$ and $a_1 \ne 0$. If f is a Dumas polynomial then $\gcd(a_j, a_k) \ne 1$ for every $j, k \in \{0, 1, 2\}$.*

Proof. Suppose there exists a polynomial with the property that $\gcd(a_j, a_k) = 1$ for some distinct $j, k \in \{0, 1, 2\}$. If for any prime p we have $p \mid a_1$ then clearly $p \nmid a_0$ and $p \nmid a_2$. So the Newton polygon passes through the point $(1, 0)$, since it lies on the segment from $(0, 0)$ to $(2, 0)$. Thus, f is not a Dumas polynomial. On the other hand, if for any prime p we have $p \nmid a_1$ then the Newton polygon includes the point $(1, 0)$. So again f is not a Dumas polynomial, completing the proof. □

Lemma 4.3.5. *Fix $n \ge 2$. Suppose $f(x)$ is as shown in (4.25) with $H(f) \le H$, and we have $a_1a_2 \cdots a_{n-1} \ne 0$. If f is a Dumas polynomial then it follows that $\gcd(a_1, a_2, \ldots, a_{n-1}) \ne 1$.*

Proof. Suppose f is as described above with $\gcd(a_1, a_2, \ldots, a_{n-1}) = 1$. For any prime p, we must have $p \nmid a_i$ for some $1 \le i \le n - 1$. So the Newton diagram for f with respect to p includes the point $(a_i, 0)$. Thus, the Newton diagram with respect to any prime p does not consist of a single segment. Therefore f is not a Dumas polynomial. □

4.3.4 Proof of Theorem 4.3.2

Let $f(x)$ be as in (4.25) with $H(f) \le H$. We prove Theorem 4.3.2 for $n = 2$ and $n \ge 3$ separately.

We start with the $n = 2$ case. To ease notation we use $\gcd^*(a_0, a_1, a_2) \ne 1$ to mean that a_0, a_1 and a_2 are not pairwise coprime, that is, $\gcd(a_0, a_1) \ne 1$ or $\gcd(a_0, a_2) \ne 1$ or $\gcd(a_1, a_2) \ne 1$. We also use $\gcd_*(a_0, a_1, a_2) = 1$ to mean that a_0, a_1 and a_2 are pairwise coprime, that is, $\gcd(a_0, a_1) = \gcd(a_0, a_2) = \gcd(a_1, a_2) = 1$.

There are $O(H^2)$ polynomials with $a_0a_1a_2 = 0$. If we have $a_0a_1a_2 \ne 0$ then, by Lemma 4.3.4, the polynomial f can only be a Dumas polynomial if

$\gcd^*(a_0,a_1,a_2)\neq 1$. Therefore,

$$\begin{aligned}\mathcal{D}_2(H)-O(H^2) &\leq \sum_{\substack{1\leq|a_0|,|a_1|,|a_2|\leq H\\ \gcd^*(a_0,a_1,a_2)\neq 1}} 1\\ &= \sum_{\substack{1\leq a_0,a_1,a_2\leq H\\ \gcd^*(a_0,a_1,a_2)\neq 1}} 8\\ &= (2H)^3-\sum_{\substack{1\leq a_0,a_1,a_2\leq H\\ \gcd_*(a_0,a_1,a_2)=1}} 8. \qquad (4.26)\end{aligned}$$

From the paper of Tóth [81, Corollary 2] we have

$$\sum_{\substack{1\leq a_0,a_1,a_2\leq H\\ \gcd_*(a_0,a_1,a_2)=1}} 1 = H^3\prod_{p \text{ prime}}\left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}\right)+O\left(H^2(\log H)^2\right),$$

from which we obtain

$$\sum_{\substack{1\leq|a_0|,|a_1|,|a_2|\leq H\\ \gcd_*(a_0,a_1,a_2)=1}} 1 = (2H)^3\prod_{p \text{ prime}}\left(1-\frac{1}{p}\right)^2\left(1+\frac{2}{p}\right)+O\left(H^2(\log H)^2\right). \qquad (4.27)$$

Substituting (4.27) into (4.26) completes the proof for the $n=2$ case.

Now fix $n\geq 3$. There are $O(H^n)$ polynomials for which $a_1a_2\cdots a_{n-1}=0$. If $a_1a_2\cdots a_{n-1}\neq 0$ then, by Lemma 4.3.5, the polynomial f can only be a Dumas polynomial if $\gcd(a_1,a_2,\ldots,a_{n-1})\neq 1$. Therefore,

$$\mathcal{D}_n(H)-O(H^n)\leq \sum_{\substack{1\leq|a_1|,|a_2|,\ldots,|a_n|\leq H\\ \gcd(a_1,a_2,\ldots,a_{n-1})\neq 1}} 1. \qquad (4.28)$$

We infer from Nymann [72] that

$$\sum_{\substack{1\leq|a_1|,|a_2|,\ldots,|a_n|\leq H\\ \gcd(a_1,a_2,\ldots,a_{n-1})\neq 1}} 1 = (2H)^{n+1}\left(1-\frac{1}{\zeta(n-1)}\right)+O(H^n). \qquad (4.29)$$

Substituting (4.29) into (4.28) completes the proof for the $n\geq 3$ case. Thus Theorem 4.3.2 is proven.

4.3.5 Comments

Let $\mathcal{P}_n(H)$ be the number of polynomials of degree n and maximum height H. Let $\mathcal{I}_n(H)$ be the number of irreducible polynomials of degree n and maximum height H. Two results immediately follow from Theorem 4.3.2.

Firstly, we note that $\mathcal{P}_n(H)$ is precisely $(2H)(2H+1)^n$ and infer from Cohen [14, Theorem 1] that for $n \geq 2$

$$\lim_{H\to\infty} \frac{\mathcal{I}_n(H)}{\mathcal{P}_n(H)} = 1.$$

Thus, for $n \geq 2$,

$$\limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} = \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{I}_n(H)} \leq \tau_n.$$

Secondly, $\tau_n < 1$ for all $n \geq 2$ and so for $n \geq 2$

$$\limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} = \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{I}_n(H)} < 1.$$

Table 1 shows some calculated values of upper bounds on the limit superior of $\mathcal{D}_n(H)/\mathcal{P}_n(H)$ as H goes to infinity. It also includes limit inferior calculations derived from Section 4.1. Specifically, for various values of n, lower bounds on the limit inferior of $\mathcal{D}_n(H)/\mathcal{P}_n(H)$ as H goes to infinity. All summations are over all primes less than 100,000.

Table 4.3: Some lower bounds on $\liminf \mathcal{D}_n(H)/\mathcal{P}_n(H)$ as $H \to \infty$ and upper bounds on $\limsup \mathcal{D}_n H/\mathcal{P}_n(H)$ as $H \to \infty$

n	Lower bound	Upper bound
2	0.1677	0.7133
3	0.0556	0.3922
4	0.0224	0.1681
5	0.0099	0.0766
6	0.0046	0.0357
7	0.0022	0.0181
8	0.0010	0.0079
9	0.0005	0.0049
10	0.0003	0.0020

This prompts the following question. Is it possible to obtain tighter bounds or the exact values of

$$\liminf_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)} \qquad \text{and} \qquad \limsup_{H\to\infty} \frac{\mathcal{D}_n(H)}{\mathcal{P}_n(H)}$$

(they most likely coincide)?

We also note that it is possible to find upper bounds on

$$\limsup_{H\to\infty} \mathcal{D}_n(H)/\mathcal{P}_n(H)$$

by directly calculating the number of Dumas polynomials for an arbitrary single segment Newton polygon that contains no points with integer coordinates other than endpoints, and then summing over all possible single segment Newton polygons that contain no points with integer coordinates other than endpoints. There are substantial problems using the inclusion-exclusion principle with this approach; a Dumas polynomial with respect to more than one prime may exhibit a different Newton polygon for each of these primes. Whilst results for degree $n > 3$ are obtainable without the inclusion-exclusion principle, it has not been possible to find any results that are superior to Theorem 4.3.2.

We also note that it is also interesting to study polynomials f such that

$$(cx+d)^n f\left(\frac{ax+b}{cx+d}\right)$$

are Dumas polynomials for some $a, b, c, d \in \mathbb{Z}$. There does not seem to be enumeration results regarding these polynomials. But there has been some progress in determining which polynomials do and do not give Dumas polynomials after such an affine shift, see [56] and [8] and references therein.

4.4 Irreducible binomials in finite fields

4.4.1 Introduction

This section is entirely based on [48]. We consider various counting questions for irreducible binomials over finite fields. We use various results from analytic number theory to investigate these questions.

It is reasonably easy to obtain an asymptotic formula for the total number of irreducible polynomials over the finite field $\mathbb{F}_q$ of q elements, see [61, Theorem 3.25].

Studying irreducible polynomials with some prescribed coefficients is much more difficult, yet remarkable progress has also been achieved in this direction, see [16, 53, 74] and references therein.

Here we consider a special case of this problem and investigate some counting questions concerning irreducible binomials over the finite field $\mathbb{F}_q$ of q elements. More precisely, for an integer t and a prime power q, let $N_t(q)$ be the number of irreducible binomials over $\mathbb{F}_q$ of the form $X^t - a \in \mathbb{F}_q[X]$.

We use a well known characterisation of irreducible binomials $X^t - a$ over $\mathbb{F}_q$ of q elements to count the total number of such binomials on average over q or t. In fact, we consider several natural regimes, for example, when t is fixed and q varies or when both vary in certain ranges $t \le T$ and $q \le Q$. There has always been very active interest in binomials, see [61, Notes to Chapter 3] for a survey of classical results. Irreducible binomials have been used in [78] as building blocks for constructing other irreducible polynomials over finite fields, and in [10] for characterising the irreducible factors of $X^n - 1$ (see also [3, 65] and references therein for more recent applications). However, the natural question of investigating the behaviour of $N_t(q)$ has never been addressed in the literature.

Our methods rely on several classical and modern results of analytic number theory; in particular the distribution of primes in arithmetic progressions.

4.4.2 Notation

As usual, for any integer $n > 0$, let $\Lambda(n)$ denote the von Mangoldt function. That is,

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p \text{ and integer } k \ge 1, \\ 0 & \text{otherwise.} \end{cases}$$

For positive integers Q and s, we denote the number of primes in arithmetic progression by

$$\pi(Q; s, a) = \sum_{\substack{p \le Q \\ p \equiv a \pmod{s}}} 1.$$

We also denote

$$\psi(Q; s, a) = \sum_{\substack{p \le Q \\ p \equiv a \pmod s}} \Lambda(p).$$

In regard to big-Oh notation or $\ll$, the constant $c > 0$ may depend on the real parameter $\varepsilon > 0$.

We define $\log X$ as $\log X = \max\{\ln X, 2\}$ where $\ln X$ is the natural logarithm, For an integer $k \ge 2$, we define recursively $\log_k X = \log(\log_{k-1} X)$.

Finally, we use $\Sigma^\sharp$ to indicate that the summation is only over squarefree arguments in the range of summation.

4.4.3 Main results

We denote the radical of an integer $t \neq 0$, the largest square-free number that divides t, by $\mathrm{rad}(t)$. It is also convenient to define

$$\mathrm{rad}_4(t) = \begin{cases} \mathrm{rad}(t) & \text{if } 4 \nmid t, \\ 2\mathrm{rad}(t) & \text{otherwise.} \end{cases}$$

We start with an upper bound on the average value of $N_t(q)$ for a fixed t averaged over $q \le Q$.

Theorem 4.4.1. *For any fixed $\varepsilon > 0$ uniformly over real Q and positive integers t with $\mathrm{rad}_4(t) \le Q^{1-\varepsilon}$, we have*

$$\sum_{q \le Q} N_t(q) \le (1 + o(1)) \frac{Q^2}{\mathrm{rad}_4(t) \log(Q/\mathrm{rad}_4(t))}$$

as $Q \to \infty$.

We also present the following lower bound (which has $\varphi(\mathrm{rad}(t))^2$ instead of the expected $\varphi(\mathrm{rad}(t))$).

Theorem 4.4.2. *There exists an absolute constant $L > 0$ such that uniformly over real Q and positive integers t with $Q \ge t^L$ we have*

$$\sum_{q \le Q} N_t(q) \gg \frac{Q^2}{\varphi(\mathrm{rad}(t))^2 (\log Q)^2}.$$

We also investigate $N_t(q)$ for a fixed q averaged over $t \le T$.

Theorem 4.4.3. *For any fixed positive A and ε and a sufficiently large real q and T with*

$$T \ge (\log(q-1))^{(1+\varepsilon)A \log_3 q / \log_4 q}$$

we have

$$\sum_{t \le T} N_t(q) \le (q-1)T/(\log T)^A.$$

Finally, we obtain an asymptotic formula for the double average of $N_t(q)$ over $q \le Q$ and squarefree $t \le T$ in a rather wide range of parameters Q and T. With more work similar results can also be obtained for the average value of $N_t(q)$ over all integers $t \le T$. However, to exhibit the ideas and simplify the exposition, we limit ourselves to this special case, in particular we recall our notation $\Sigma^\sharp$ from Section 4.4.2.

Theorem 4.4.4. *For any fixed $\varepsilon > 0$ and any*

$$T \le Q^{1/2}/(\log Q)^{5/2+\varepsilon}$$

we have

$$\sum_{t \le T}{}^{\sharp} \sum_{q \le Q} N_t(q) = (1 + o(1)) \frac{Q^2 \log T}{2\zeta(2) \log Q},$$

as $T \to \infty$.

It seems difficult to obtain the asymptotic formula of Theorem 4.4.4 for larger values of T (even under the Generalised Riemann Hypothesis). However, here we show that a result of Mikawa [69] implies a lower bound of right order of magnitude for values of T of order that may exceed $Q^{1/2}$.

Theorem 4.4.5. *For any fixed $\beta < 17/32$ and $T \le Q^\beta$, we have*

$$\sum_{T \le t \le 2T}{}^{\sharp} \sum_{q \le Q} N_t(q) \gg \frac{Q^2}{\log Q}.$$

We note that Theorem 4.4.5 means that for a positive proportion of fields $\mathbb{F}_q$ with $q \le Q$ there is a positive proportion of irreducible binomials whose degrees do not exceed Q^β.

4.4.4 Characterisation of irreducible binomials

Let $\operatorname{ord}_q a$ denote the multiplicative order of $a \in \mathbb{F}_q^*$.

Our main tool is the following characterisation of irreducible binomials (see [61, Theorem 3.75]).

Lemma 4.4.6. *Let $t \ge 2$ be an integer and $a \in \mathbb{F}_q^*$. Then the binomial $X^t - a$ is irreducible in $\mathbb{F}_q[X]$ if and only if the following three conditions are satisfied.*

1. $\operatorname{rad}(t) \mid \operatorname{ord}_q a$,
2. $\gcd(t, (q-1)/\operatorname{ord}_q a) = 1$,
3. *if* $4 \mid t$ *then* $q \equiv 1 \pmod 4$.

Lemma 4.4.7. *Suppose that q is a prime power. Then*

$$N_t(q) = \begin{cases} \dfrac{\varphi(t)}{t}(q-1), & \textit{if } \operatorname{rad}_4(t) \mid (q-1), \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. We can assume that $\operatorname{rad}_4(t) \mid (q-1)$ (or equivalently $\operatorname{rad}(t) \mid (q-1)$ and if $4 \mid t$ then $q \equiv 1 \pmod 4$), as in the opposite case the result follows immediately from Lemma 4.4.6.

From Lemma 4.4.6 we see that

$$N_t(q) = \sum_{\substack{a \in \mathbb{F}_q^* \\ \operatorname{rad}(t) \mid \operatorname{ord}_q a \\ \gcd(t,(q-1)/\operatorname{ord}_q a)=1}} 1.$$

Since $\mathbb{F}_q^*$ is a cyclic group, there are $\varphi(\operatorname{ord}_q a)$ elements of $\mathbb{F}_q^*$ that have order equal to $\operatorname{ord}_q a$. Hence, we obtain

$$N_t(q) = \sum_{\substack{j \mid (q-1) \\ \operatorname{rad}(t) \mid j \\ \gcd(t,(q-1)/j)=1}} \varphi(j).$$

We now write $q-1 = RS$, where R is the largest divisor of $q-1$ with $\gcd(R, \operatorname{rad}(t)) = 1$ (thus all prime divisors of S also divide t). Now, for every integer $j \mid (q-1)$ the conditions $\operatorname{rad}(t) \mid j$ and $\gcd(t,(q-1)/j) = 1$ mean that $j = Sd$ for some $d \mid R$. Since $\gcd(S,R) = 1$, we have

$$N_t(q) = \sum_{d \mid R} \varphi(Sd) = \varphi(S) \sum_{d \mid R} \varphi(d) = \varphi(S)R = \frac{\varphi(t)}{t} SR = \frac{\varphi(t)}{t}(q-1),$$

which concludes the proof. □

4.4.5 Analytic number theory background

We recall a quantitative version of the Linnik theorem, see [55, Corollary 18.8], which is slightly stronger than the form which is usually used.

Lemma 4.4.8. *There is an absolute constant L such that if a positive integer k is sufficiently large and $Q \geq k^L$, then uniformly over all integers a with $\gcd(k,a) = 1$ we have*

$$\psi(Q; k, a) \gg \frac{Q}{\varphi(k)\sqrt{k}}.$$

On average over k, we have a much more precise result given by the *Bombieri–Vinogradov theorem* which we present in the form that follows from the work of Dress, Iwaniec, and Tenenbaum [25] combined with the method of Vaughan [82].

Lemma 4.4.9. *For any $A > 0$, $\alpha > 3/2$ and $T \le Q$ we have*

$$\sum_{t\le T} \max_{\gcd(a,t)=1} \max_{R\le Q} \left| \pi(R;t,a) - \frac{\pi(R)}{\varphi(t)} \right| \le Q(\log Q)^{-A} + Q^{1/2}T(\log Q)^{\alpha}.$$

The following result follows immediately from much more general estimates of Mikawa [69, Bounds (4) and (5)].

Lemma 4.4.10. *For any fixed $\beta < 17/32$, $u \le z^{\beta}$ and for all but $o(u)$ integers $k \in [u, 2u]$ we have*

$$\pi(2z;k,1) - \pi(z;k,1) \gg \frac{z}{\varphi(k)\log z}.$$

We also have a bound on the number $\rho_T(n)$ of integers $t \le T$ with $\mathrm{rad}(t) \mid n$, which is due to Grigoriev and Tenenbaum [38, Theorem 2.1]. We note that [38, Theorem 2.1] is formulated as a bound on the number of divisors $t \mid n$ with $t \le T$. However, a direct examination of the argument reveals that it actually provides an estimate for the above function $\rho_T(n)$. In fact, we present it in simpler form given by [38, Corollary 2.3]

Lemma 4.4.11. *For any fixed positive A and ε and a sufficiently large positive integer n and a real T with*

$$T \ge (\log n)^{(1+\varepsilon)A\log_3 n/\log_4 n}$$

we have $\rho_T(n) \le T/(\log T)^A$.

4.4.6 Proof of Theorem 4.4.1

For the case where $4 \nmid t$, we denote $s = \mathrm{rad}(t)$. Using Lemma 4.4.7, we have

$$\sum_{q\le Q} N_t(q) = \frac{\varphi(t)}{t} \sum_{\substack{q\le Q\\ s\mid(q-1)}} (q-1) = \frac{\varphi(t)}{t} \sum_{\substack{q\le Q\\ s\mid(q-1)}} q + O(Q/s). \tag{4.30}$$

So, with

$$\ell = \left\lfloor \frac{\log Q}{\log 2} \right\rfloor \qquad \text{and} \qquad \lambda = 2\varepsilon^{-1},$$

we have

$$\sum_{\substack{q\le Q\\ s\mid(q-1)}} q = \sum_{\substack{p\le Q\\ s\mid(p-1)}} p + \sum_{2\le r\le \ell} \sum_{\substack{p^r\le Q\\ s\mid(p^r-1)}} p^r. \tag{4.31}$$

Using the Brun-Titchmarsh bound, see [55, Theorem 6.6] and partial summation we obtain

$$\sum_{\substack{p\le Q\\ s\mid(p-1)}} p \le (1+o(1))\frac{Q^2}{\varphi(s)\log(Q/s)}, \tag{4.32}$$

provided that $s/Q \to 0$.

We now estimate the contribution from other terms with $r \geq 2$.

The condition $s \mid p^r - 1$ puts p in at most $r^{\omega(s)}$ arithmetic progressions modulo s. Extending the summation to all integers $n \leq Q^{1/r}$ in these progressions, we have

$$\sum_{\substack{p^r \leq Q \\ s|(p^r-1)}} p^r \ll r^{\omega(s)} Q(Q^{1/r}s^{-1} + 1).$$

We use this bound for $r \leq \lambda$. Since

$$\omega(s) \ll \frac{\log s}{\log\log(s+2)},$$

for $r \leq \lambda$ we have

$$r^{\omega(s)} = \exp\left(O\left(\frac{\log s}{\log\log(s+2)}\right)\right).$$

The total contribution from all terms with $2 \leq r \leq \lambda$ is at most

$$\begin{aligned}\sum_{2 \leq r \leq \lambda} \sum_{\substack{p^r \leq Q \\ s|(p^r-1)}} p^r &\leq Q(Q^{1/2}s^{-1} + 1) \exp\left(O\left(\frac{\log s}{\log\log(s+2)}\right)\right) \\ &= Q^{1+o(1)}(Q^{1/2}s^{-1} + 1). \qquad (4.33)\end{aligned}$$

For $\lambda \leq r \leq \ell$ we use the trivial bound

$$\sum_{\lambda \leq r \leq \ell} \sum_{\substack{p^r \leq Q \\ s|(p^r-1)}} p^r \leq \ell Q^{1+1/\lambda}. \qquad (4.34)$$

Combining (4.33) and (4.34), we see that

$$\begin{aligned}\sum_{2 \leq r \leq \ell} \sum_{\substack{p^r \leq Q \\ s|(p^r-1)}} p^r &\ll Q^{3/2+o(1)}s^{-1} + Q^{1+o(1)} + Q^{1+\varepsilon/2}\log Q \\ &\ll Q^{3/2+o(1)}s^{-1}, \qquad (4.35)\end{aligned}$$

provided that $s \leq Q^{1-\varepsilon}$ and $Q \to \infty$. Recalling (4.30), (4.31) and (4.32) and that

$$\frac{\varphi(t)}{t\varphi(s)} = \frac{1}{s},$$

we conclude the proof for the case where $4 \nmid t$.

In the event that $4 \mid t$ then, returning to (4.30), we have

$$\sum_{q \leq Q} N_t(q) = \frac{\varphi(t)}{t} \sum_{\substack{q \leq Q \\ s|(q-1) \\ 4|(q-1)}} (q-1) = \frac{\varphi(t)}{t} \sum_{\substack{q \leq Q \\ \mathrm{lcm}(4,\mathrm{rad}(t))|(q-1)}} (q-1).$$

Since $\mathrm{lcm}(4, \mathrm{rad}(t)) = 2\mathrm{rad}(t)$, the proof now continues as before, replacing s with $2s$.

4.4.7 Proof of Theorem 4.4.2

Combining (4.30) and (4.31), we have

$$\begin{aligned}\sum_{q\le Q} N_t(q) \ge \sum_{p\le Q} N_t(p) = \frac{\varphi(t)}{t} \sum_{\substack{p\le Q\\ \mathrm{rad}_4(t)|(p-1)}} (p-1)\\ \ge \frac{\varphi(t)}{t} \sum_{\substack{p\le Q\\ 2s|(p-1)}} (p-1), \qquad (4.36)\end{aligned}$$

where, as before, $s = \mathrm{rad}(t)$.

It immediately follows from Lemma 4.4.8 that

$$\pi(Q;2s,1) \gg \frac{Q}{\varphi(2s)\sqrt{2s}\log Q} \ge \frac{Q}{\varphi(s)\sqrt{s}\log Q}.$$

Thus

$$\sum_{\substack{p\le Q\\ 2s|(p-1)}} p \ge \sum_{k=1}^{\pi(Q;s,1)} (2ks+1) \ge 2s\frac{\pi(Q;s,1)^2}{2} \gg \frac{Q^2}{\varphi^2(s)(\log Q)^2}.$$

Combining this lower bound with (4.36) completes the proof.

4.4.8 Proof of Theorem 4.4.3

Fix any positive T and q. For $q-1 \equiv 0 \pmod 4$ we have, using Lemma 4.4.7,

$$\sum_{t\le T} N_t(q) = (q-1) \sum_{\substack{t\le T\\ \mathrm{rad}(t)|(q-1)}} \frac{\varphi(t)}{t} \le (q-1) \sum_{\substack{t\le T\\ \mathrm{rad}(t)|(q-1)}} 1. \qquad (4.37)$$

For $q-1 \not\equiv 0 \pmod 4$ we have, using Lemma 4.4.7,

$$\begin{aligned}\sum_{t\le T} N_t(q) = (q-1) \sum_{\substack{t\le T\\ \mathrm{rad}(t)|(q-1)\\ 4\nmid t}} \frac{\varphi(t)}{t} \le (q-1) \sum_{\substack{t\le T\\ \mathrm{rad}(t)|(q-1)}} \frac{\varphi(t)}{t}\\ \le (q-1) \sum_{\substack{t\le T\\ \mathrm{rad}(t)|(q-1)}} 1. \qquad (4.38)\end{aligned}$$

Combining (4.37), (4.38) and Lemma 4.4.11 completes the proof.

4.4.9 Proof of Theorem 4.4.4

Using (4.30), (4.31) and (4.35), we have

$$\begin{aligned}\sum_{t\le T}{}^{\sharp}\sum_{q\le Q} N_t(q) &= \sum_{t\le T}{}^{\sharp}\frac{\varphi(t)}{t}\sum_{\substack{p\le Q\\ t\mid(p-1)}} p + O\left(Q^{3/2+o(1)}\sum_{t\le T} t^{-1}\right)\\ &= \sum_{t\le T}{}^{\sharp}\frac{\varphi(t)}{t}\sum_{\substack{p\le Q\\ t\mid(p-1)}} p + O\left(Q^{3/2+o(1)}\right), \qquad (4.39)\end{aligned}$$

as $T \le Q^{1/2}$.

Using partial summation, we have

$$\sum_{\substack{p\le Q\\ t\mid(p-1)}} p = (Kt+1)\pi(Kt+1;t,1) - t\sum_{1\le k\le K}\pi(kt;t,1), \qquad (4.40)$$

where $K = \lfloor (Q-1)/t \rfloor$.

We now write

$$\mathcal{E}(Q,t) = \max_{R\le Q}\left|\pi(R;t,1) - \frac{\pi(R)}{\varphi(t)}\right|.$$

With this notation, we derive from (4.40) that

$$\sum_{\substack{p\le Q\\ t\mid(p-1)}} p = \frac{Q\pi(Q)}{\varphi(t)} - \frac{t}{\varphi(t)}\sum_{1\le k\le K}\pi(kt) + O\left(tK\mathcal{E}(Q,t)\right). \qquad (4.41)$$

By the prime number theorem and [55, Corollary 5.29], and noting that for $1 \le k \le K$ we have $kt \le Q$, we also conclude that

$$\begin{aligned}\sum_{1\le k\le K}\pi(kt) &= t\sum_{1\le k\le K}\frac{k}{\log(kt)} + O(Q^2(\log Q)^{-2})\\ &= t\sum_{K/(\log Q)^2\le k\le K}\frac{k}{\log(kt)} + O(Q^2(\log Q)^{-2}).\end{aligned}$$

Now, for $K/(\log Q)^2 \le k \le K$ we have

$$\frac{1}{\log(kt)} = \frac{1}{\log Q + O(\log\log Q)} = \frac{1}{\log Q} + O\left(\frac{\log\log Q}{(\log Q)^2}\right).$$

Therefore,

$$\sum_{1\le k\le K}\pi(kt) = \left(\frac{1}{2}+o(1)\right)\frac{t}{\log Q}K^2 = \left(\frac{1}{2}+o(1)\right)\frac{Q^2}{t\log Q}.$$

Substituting this in (4.41) and using $\pi(Q) \sim Q/\log Q$, we obtain

$$\sum_{\substack{p \le Q \\ t|(p-1)}} p = \left(\frac{1}{2} + o(1)\right) \frac{Q^2}{\varphi(t)\log Q} + O\left(Q\mathcal{E}(Q,t)\right).$$

Using this bound in (4.39) yields

$$\sum_{t \le T}{}^{\sharp} \sum_{q \le Q} N_t(q) = \left(\frac{1}{2} + o(1)\right) \frac{Q^2}{2\log Q} \sum_{t \le T}{}^{\sharp} \frac{1}{t} \\ + O\left(Q^{3/2+O(1)} + Q\sum_{t \le T} \mathcal{E}(Q,t)\right).$$

By Lemma 4.4.9, with $A = 1 + \varepsilon$ and $\alpha = 3/2 + \varepsilon/2$, there is some $B > 0$ such that

$$\sum_{t \le T} \mathcal{E}(Q,t) \ll Q(\log Q)^{-A} + Q^{1/2}T(\log Q)^{\alpha} \ll Q(\log Q)^{-1-\varepsilon/2}.$$

Hence

$$\sum_{t \le T}{}^{\sharp} \sum_{q \le Q} N_t(q) = \left(\frac{1}{2} + o(1)\right) \frac{Q^2}{\log Q} \sum_{t \le T}{}^{\sharp} \frac{1}{t} + O\left(Q(\log Q)^{-1-\varepsilon/2}\right). \quad (4.42)$$

A simple inclusion-exclusion argument leads to the asymptotic formula

$$\sum_{t \le T}{}^{\sharp} \frac{1}{t} = \left(\frac{1}{\zeta(2)} + o(1)\right) \log T, \quad (4.43)$$

see [79] for a much more precise result. Substituting (4.43) into (4.42) completes the proof.

4.4.10 Proof of Theorem 4.4.5

We proceed as in the proof of Theorem 4.4.4, but instead of (4.39) we write

$$\sum_{T \le t \le 2T}{}^{\sharp} \sum_{q \le Q} N_t(q) \ge \sum_{T \le t \le 2T}{}^{\sharp} \sum_{Q/2 \le p \le Q} N_t(p) = \sum_{T \le t \le 2T}{}^{\sharp} \frac{\varphi(t)}{t} \sum_{\substack{Q/2 \le p \le Q \\ t|(p-1)}} p \\ \gg Q \sum_{T \le t \le 2T}{}^{\sharp} \frac{\varphi(t)}{t} \left(\pi(Q; t, 1) - \pi(Q/2; t, 1)\right).$$

Using Lemma 4.4.10, we easily conclude the proof.

Chapter 5

Appendix 1

We say that $(a_1, \dots, a_4)$ is pairwise non-coprime if $\gcd(a_i, a_j) \neq 1$ for all $1 \leq i < j \leq 4$. We use the methodology of [31] to calculate the densities of 4-tuples of positive integers that pairwise non-coprime.

This density is given by

$$N(4) = \lim_{H \to \infty} \frac{1}{H^4} \sum_{\substack{1 \leq a_1, \dots, a_4 \leq H \\ \gcd(a_i, a_j) \neq 1 \\ 1 \leq i < j \leq 4}} 1.$$

Let H be a positive integer and $\mathcal{A}$ a set of ordered pairs (i, j) with $1 \leq i < j \leq H$. Define

$$\mathcal{N}_{\mathcal{A}} = \lim_{H \to \infty} \frac{1}{H^4} \sum_{\substack{1 \leq a_1, \dots, a_4 \leq H \\ \gcd(a_i, a_j) = 1 \\ (i,j) \in \mathcal{A}}} 1.$$

Let

$$A_t = \left(\frac{1}{p}\right)^t \left(1 - \frac{1}{p}\right)^{4-t}, \; t = 0, 1, 2, 3,$$

and

$$C_{i_1, \dots, i_4} = \prod_{p \text{ prime}} \left(i_1 A_1 + \cdots + i_4 A_4\right).$$

We note that for each set $\mathcal{A}$ we have $\mathcal{N}_{\mathcal{A}} = C_{i_1, \dots, i_4}$, where $i_1, \dots i_4$ are calculated by the process outlined in [31] and shown below. Using the inclusion-exclusion principle, and appealing to symmetry, we have

$$\begin{aligned} N(4) = 1 &- 6\mathcal{N}_{\{(1,2)\}} + 12\mathcal{N}_{\{(1,2),(1,3)\}} + 3\mathcal{N}_{\{(1,2),(3,4)\}} - 12\mathcal{N}_{\{(1,2),(2,3),(3,4)\}} \\ &- 4\mathcal{N}_{\{(1,2),(2,3),(2,4)\}} - 4\mathcal{N}_{\{(1,2),(2,3),(3,1)\}} + 3\mathcal{N}_{\{(1,2),(2,3)(3,4),(4,1)\}} \\ &+ 8\mathcal{N}_{\{(1,2),(2,3),(1,3),(1,4)\}} - 6\mathcal{N}_{\{(1,2),(1,3),(1,4),(2,3),(2,4)\}} \\ &+ \mathcal{N}_{\{(1,2),(1,3),(1,4),(2,3),(2,4),(3,4)\}}. \end{aligned}$$

Then, using Figures 5.1 to 5.7 and Tables 5.1 to 5.7, we have

$$\begin{aligned} N(4) &= 1 - 6C_{1,4,5,2} + 12C_{1,4,4,1} + 3C_{1,4,4,0} - 12C_{1,4,3,0} - 4C_{1,4,3,1} - 4C_{1,4,3,0} \\ &\quad + 3C_{1,4,2,0} + 12C_{1,4,2,0} - 6C_{1,4,1,0} + C_{1,4,0,0} \\ &= 1 - 6C_{1,4,5,2} + 12C_{1,4,4,1} + 3C_{1,4,4,0} - 16C_{1,4,3,0} - 4C_{1,4,3,1} + 15C_{1,4,2,0} \\ &\quad - 6C_{1,4,1,0} + C_{1,4,0,0} \\ &\approx 0.0790, \end{aligned}$$

where the products are over all primes less than 100,000.

Figure 5.1: Graph for $\mathcal{N}_{\{(1,2)\}}$

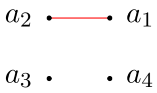

Table 5.1: Calculation of $\mathcal{N}_{\{(1,2)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 1 0
	1 0 0 1
	0 1 0 1
	0 1 1 0
	0 0 1 1
		$5A_2$

p divides exactly three a_i	1 0 1 1 0 1 1 1	$2A_3$
Required density		$C_{1,4,5,2}$

Figure 5.2: Graph for $\mathcal{N}_{\{(1,2),(1,3)\}}$

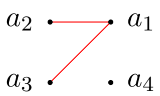

Table 5.2: Calculation of $\mathcal{N}_{\{(1,2),(1,3)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 0 1
	0 1 1 0
	0 1 0 1
	0 0 1 1
		$4A_2$

p divides exactly three a_i	0 1 1 1	A_3
Required density		$C_{1,4,4,1}$

Figure 5.3: Graph for $\mathcal{N}_{\{(1,2),(3,4)\}}$

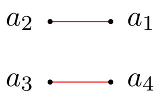

Table 5.3: Calculation of $\mathcal{N}_{\{(1,2),(3,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 1 0
	1 0 0 1
	0 1 0 1
	0 1 1 0
		$4A_2$

Required density		$C_{1,4,4,0}$

Figure 5.4: Graph for $\mathcal{N}_{\{(1,2),(2,3),(3,4)\}}$

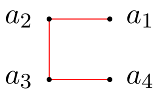

Table 5.4: Calculation of $\mathcal{N}_{\{(1,2),(2,3),(3,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 1 0
	0 1 0 1
	1 0 0 1
		$3A_2$

Required density		$C_{1,4,3,0}$

Figure 5.5: Graph for $\mathcal{N}_{\{(1,2),(2,3),(2,4)\}}$

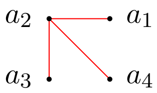

Table 5.5: Calculation of $\mathcal{N}_{\{(1,2),(2,3),(2,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 1 0
	0 0 1 1
	1 0 0 1
		$3A_2$

p divides exactly three a_i	1 0 1 1	A_3
Required density		$C_{1,4,3,1}$

Figure 5.6: Graph for $\mathcal{N}_{\{(1,2),(2,3),(1,3)\}}$

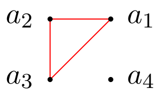

Table 5.6: Calculation of $\mathcal{N}_{\{(1,2),(2,3),(1,3)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	0 1 0 1
	0 0 1 1
	1 0 0 1
		$3A_2$

Required density		$C_{1,4,3,0}$

Figure 5.7: Graph for $\mathcal{N}_{\{(1,2),(2,3),(3,4),(1,4)\}}$

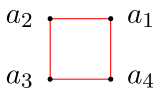

Table 5.7: Graph for $\mathcal{N}_{\{(1,2),(2,3),(3,4),(1,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	1 0 1 0 0 1 0 1	$2A_2$
Required density		$C_{1,4,2,0}$

Figure 5.8: Graph for $\mathcal{N}_{\{(1,2),(2,3),(1,3),(1,4)\}}$

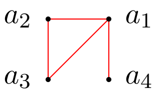

Table 5.8: Calculation of $\mathcal{N}_{\{(1,2),(2,3),(1,3),(1,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	0 0 1 1 0 1 0 1	$2A_2$
Required density		$C_{1,4,2,0}$

Figure 5.9: Graph for $\mathcal{N}_{\{(1,2),(1,3),(2,3),(2,4),(1,4)\}}$

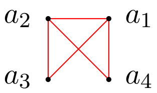

Table 5.9: Calculation of $\mathcal{N}_{\{(1,2),(1,3),(2,3),(2,4),(1,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

p divides exactly two a_i	0 0 1 1	A_2
Required density		$C_{1,4,1,0}$

Figure 5.10: Graph for $\mathcal{N}_{\{(1,2),(1,3),(2,3),(2,4),(1,4),(3,4)\}}$

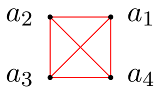

Table 5.10: Calculation of $\mathcal{N}_{\{(1,2),(1,3),(2,3),(2,4),(1,4),(3,4)\}}$

Element divisibility condition	Matrix	Formula
p does not divide any a_i	0 0 0 0	A_0

p divides exactly one a_i	1 0 0 0
	0 1 0 0
	0 0 1 0
	0 0 0 1
		$4A_1$

Required density		$C_{1,4,0,0}$

Bibliography

[1] S. Akiyama and A. Pethő, 'On the distribution of polynomials with bounded roots II. Polynomials with integer coefficients', Preprint, 2012.

[2] J. Arias de Reyna and R. Heyman, 'Counting tuples with coprimality conditions', J. Integer Seq., **18** (2014), 15.10.4.

[3] M. Ayad, K., Belghaba and O. Kihel, 'On permutation binomials over finite fields', Bull. Aust. Math. Soc., **89** (2014), 112–124.

[4] R. C. Baker and G. Harman, 'The sequence x/n and its subsequences', Rocky Mount. J. Math., **26** (1996), 795–814.

[5] R. C. Baker and G. Harman, 'Small remainder of a vector to suitable modulus', Math. Zeit., **221** (1996), 59–71.

[6] R. C. Baker, G. Harman and J. Pintz, 'The difference between consecutive primes, II', Proc. Lond. Math. Soc., **83** (2001), 532–562.

[7] U. Balakrishnan and Y. F. S. Pétermann, 'The Dirichlet series of $\zeta(s)\zeta^{\alpha}(s+1)f(s+1)$: On an error term associated with its coefficients', Acta Arith., **75** (1996), 39–69.

[8] A. Bishnoi and S. K. Khanduja, 'On Eisenstein-Dumas and generalized Schönemann polynomials', Comm. Algebra, **38** (2010), 3163–3173.

[9] N. C. Bonciocat, 'Schönemann-Eisenstein-Dumas-type irreducibility conditions that use arbitrarily many prime numbers', Preprint, 2014, available at arXiv:1304.0874 [math.NT].

[10] F. E. Brochero Martínez, C. R. Giraldo Vergara and L. Batista de Oliveira, 'Explicit factorization of $x^n - 1 \in \mathbb{F}_q[x]$', Preprint, 2014, available at arXiv:1404.6281 [math.NT].

[11] Y. Chen and P. Q. Nguyen, 'Faster algorithms for approximate common divisors: Breaking fully-homomorphic-encryption challenges over the integers', Advances in Cryptology-EUROCRYPT 2012, Lecture Notes Comput. Sci., **7237**, Springer, Berlin, 2012, 502–519.

[12] S. D. Chowla, ‘An order result involving the Euler φ-function’, J. Ind. Math. Soc. Old Ser., **18** (1929–1930), 138–141.

[13] K. Chung, Y. Kalai and S. Vadhan, ‘Improved delegation of computation using fully homomorphic encryption’, Advances in Cryptography-CYPTO 2010, Lecture Notes Comput. Sci., **6223**, Springer, Berlin, (2010), 483–501.

[14] S. D. Cohen, ‘The distribution of the Galois groups of integral polynomials’, Illinois J. of Math., **23** (1979), 135–152.

[15] H. Cohn and N. Heninger, ‘Approximate common divisors via lattices’, Preprint, 2011, available at arXiv:1108.2714 [math.NT].

[16] S. D. Cohen, ‘Explicit theorems on generator polynomials’, Finite Fields Appl., **11** (2005), 337–357.

[17] G. Cooperman, S. Feisel, J. von zur Gathen and G. Havas, ‘GCD of many integers (extended abstract)’, Computing and combinatorics 1999, Lecture Notes Comput. Sci., **1627**, Springer, Berlin, 1999, 310–317.

[18] J. Coron and A. May, ‘Deterministic polynomial-time equivalence of computing the RSA secret key and factoring’, J. Cryptology, **20** (2007), 39–50.

[19] D. A. Cox, ‘Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first’, Amer. Math. Monthly, **118** (2011), 3–21.

[20] R. Dietmann, ‘On the distribution of Galois groups’, Mathematika, **58** (2012), 35–44.

[21] M. van Dijk, C. Gentry, S. Halevi and V. Vaikuntanathan, ‘Fully homomorphic encryption over the integers’, Advances in cryptology-EUROCRYPT 2010, Lecture Notes Comput. Sci., **6110**, Springer, Berlin, 2010, 24–43.

[22] C. Ding, D. Pei and A. Salomaa, *The Chinese remainder theorem*, World Scientific, 1996.

[23] D. E. Dobbs and L. E. Johnson, ‘On the probability that Eisenstein’s criterion applies to an arbitrary irreducible polynomial’, 3rd Intern. Conf. Advances in Commutative Ring Theory, Lecture Notes in Pure and Appl. Math., **205**, Dekker, New York, 1999, 241–256.

[24] E. Dotti and G. Micheli, ‘Eisenstein polynomials over function fields’, Preprint, 2015, avaiable at arXiv:1506.05380 [math.NT].

[25] F. Dress, H. Iwaniec, and G. Tenenbaum, ‘Sur une somme liée à la fonction de Möbius’, J. Reine Angew. Math., **340** (1983), 53–58.

[26] A. Dubickas, ‘Polynomials irreducible by Eisenstein’s criterion’, Appl. Algebra Engin. Comm. Comput., **14** (2003), 127–132.

[27] G. Dumas, ‘Sur quelques cas d’irréductibilité des polynomes à coefficients rationnels’, J. Math. Pures Appl. (6), **2** (1906), 191–258.

[28] F. G. Eisenstein, *Mathematische werke, Vol. II*, AMS Chelsea, Providence, RI, 1989, 536–555.

[29] M. Elkadi, A. Galligo and T. L. Ba, ‘Approximate GCD of several univariate polynomials with small degree perturbations’, J. Symbolic Comput., **47** (2012), 410–421.

[30] P. Erdős, ‘On an elementary problem in number theory’, Canadian Math. Bull., **1** (1958), 5–8.

[31] J. L. Fernández and P. Fernández, ‘Equidistribution and coprimality’, Preprint, 2013, avaiable at arXiv:1310.3802 [math.NT].

[32] T. Freiberg, ‘The probability that 3 positive integers are pairwise noprime’, (unpublished manuscript).

[33] J. von zur Gathen and Jürgen Gerhard, *Modern computer algebra, (3rd edition)*, Cambridge University Press, 2013.

[34] J. von zur Gathen, M. Mignotte and I. E. Shparlinski, ‘Approximate polynomial GCD: Small degree and small height perturbations’, J. Symbolic Comput., **45** (2010), 879–886.

[35] J. von zur Gathen and I. E. Shparlinski, ‘GCD of random linear combinations’, Algorithmica, **46** (2006), 137–148.

[36] C. F. Gauss, *Disquisitiones arithmeticae (English Edition)*, Springer-Verlag, New York, 1986.

[37] C. Gentry, ‘Fully homomorphic encryption using ideal lattices’, Proc. of the ACM Intern. Symp. on Theory of Comp. 2009, ACM, New York, 2009, 169–178.

[38] D. Grigoriev and G. Tenenbaum, ‘A low complexity probabilistic test for integer multiplication’, J. Complexity, **26** (2010), 263–267.

[39] J. Goth, ‘Minimizing Non-interactive Zero-Knowledge Proofs Using Fully Homomorphic Encryption’, IACR Cyptology, ePrint Archive 2011, (2011).

[40] T. H. Gronwall, ‘Some asymptotic expressions in the theory of numbers’, Trans. Amer. Math. Soc., **14** (1913), 113–122.

[41] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers (6th Edition)*, Oxford University Press, Oxford, 2008.

[42] F. Harary and E. M. Palmer, *Graphical Enumeration*, Academic Press, New York, 1973.

[43] R. Heyman, ‘Pairwise non-coprimality of triples’, Preprint, 2014, available at arXiv: 1309.5578 [math.NT].

[44] R. Heyman and I. E. Shparlinski, ‘On the number of Eisenstein polynomials of bounded height’, Appl. Algebra Engrg. Comm. Comput., **24** (2013), 149–156.

[45] R. Heyman and I. E. Shparlinski, ‘On shifted Eisenstein polynomials’, Period. Math. Hungar., **69** (2014), 170–181.

[46] R. Heyman, ‘On the number of polynomials of bounded height that satisfy the Dumas criterion’, J. Integer Seq., **17** (2014), 14.2.4.

[47] R. Heyman and I. E. Shparlinski, ‘On the GCD of shifted sets’, J. Number Theory **154** (2015), 63–73.

[48] R. Heyman and I. E. Shparlinski, ‘Counting irreducible binomials over finite fields’, Preprint, 2105, avaiable at arXiv: 1504.01172 [math.NT].

[49] N. Howgrave-Graham, ‘Approximate integer common divisors’, Cryptology and lattices 2001, Lecture notes in Comput. Sci., **2146**, Springer, Berlin, 2001, 51–66.

[50] J. Hu, ‘The probability that random positive integers are k-wise relatively prime’, In. J. Number Theory, **9** (2013), 1263–1271.

[51] J. Hu, ‘Pairwise relative primality of positive integers’, Preprint, 2014, available at arXiv:1406.3113 [math.NT].

[52] C. Huck and P. A. B. Pleasants, ‘Entropy and diffraction of the k-free points in n-dimensional lattices’, Discrete Comput. Geom., **50** (2013), 39–68.

[53] S. Huczynska, ‘Existence results for finite field polynomials with specified properties’, *Finite fields and their applications: character sums and polynomials*, De Gruyter, Berlin, 2013, 65–87.

[54] H. Iwaniec, ‘On the problem of Jacobsthal’, Demonstratio Math., **11** (1978), 225–231.

[55] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.

[56] M. Juráš, 'Eisenstein-Dumas criterion for irreducibility of polynomials and projective transformations of the independent variable', JP Jour. Algebra, Number Theory & Appl., **6**, 2006, 221–236.

[57] M. Kac, Statistical independence in probability, analysis and number theory, The Carus Mathematical Monographs, No. 12. The Math. Assoc. of America, 1959.

[58] V. J. Katz, *A history of mathematics (brief edition)*, Pearson/Addison-Wesley, 2003.

[59] D. E. Knuth, *The Art of computer programming, Vol 2. Seminumerical algorithms (3rd Edition)*, Addison Wesley, Boston, 1998.

[60] A. K. Lenstra, H. W. Lenstra and L. Lovász, 'Factoring polynomials with rational coefficients', Mathematische Annalen, **261** (1982), 515–534.

[61] R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley 1983.

[62] J. Y. Liu, 'On an error term of Chowla, I', J. Number Theory, **64** (1997), 20–35.

[63] A. Lòpez, E. Tromer and V. Vaikuntanathan, 'On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption' Proc. of the 44th annual ACM symposium on theory of computing, ACM, (2012), 1219–1234.

[64] K. Mahler, 'An inequality for the discriminant of a polynomial', Michigan Math. J., **11** (1964), 257–262.

[65] A. Masuda and M. E. Zieve, 'Permutation binomials over finite fields', Trans. Amer. Math. Soc., **361** (2009), 4169–4180.

[66] G. Maze, J. Rosenthal and U. Wagner, 'Natural density of rectangular unimodular integer matrices', In. Linear Algebra Appl., **434** (2011), 1319–1324.

[67] D. Micciancio, 'A first glimpse of cryptography's holy grail', Comm. of the Assoc. of Comp. Machinery, **53** (2010), 96–96.

[68] G. Micheli and R. Schnyder, 'The density of shifted and affine Eisenstein polynomials', Preprint, 2015, available at arXiv:1507.02753 [math.NT].

[69] H. Mikawa, 'On primes in arithmetic progressions', Tsukuba J. Math., **25** (2001), 121–153.

[70] P. Moree, 'Counting carefree couples', Preprint, 2015, available at arXiv:0510003 [math.NT].

[71] K. Nagasaka, ‘Approximate polynomial GCD over integers’, J. Symbolic Comput., **46** (2011), 1306–1317.

[72] J. E. Nymann, ‘On the probability that k positive integers are relatively prime’, J. Number Theory, **4** (1972), 469–473.

[73] H. Osada, ‘The Galois groups of the polynomials $x^n + ax^l + b$’, J. Number Theory, **25** (1987), 230–238.

[74] P. Pollack, ‘Irreducible polynomials with several prescribed coefficients’, Finite Fields Appl., **22** (2013), 70–78.

[75] B. Poonen, ‘Squarefree values of multivariable polynomials’, Duke Math. J., **118** (2003), 353–373.

[76] V. V. Prasolov, *Polynomials*, Springer, 2004.

[77] S. Sarkar and S. Maitra, ‘Approximate integer common divisor problem relates to implicit factorization’, IEEE Trans. Inform. Theory, **57** (2011), 4002–4013.

[78] V. Shoup, ‘New algorithms for finding irreducible polynomials over finite fields’, Math. Comp., **54** (1990), 435–447.

[79] D. Suryanarayana, ‘Asymptotic formula for $\sum_{n\le x} \frac{\mu^2(n)}{n}$’, Indian J. Math., **9** (1967), 543–545.

[80] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.

[81] L. Tóth, ‘The probability that k positive integers are pairwise relatively prime’, Fibonacci Quart., **40** (2002), 13–18.

[82] R. C. Vaughan, ‘An elementary method in prime number theory’, Acta Arith., **37** (1980), 111–115.

[83] J. W. Wrench Jr., ‘Evaluation of Artin’s constant and the twin prime conjecture’, Math Comp., **15** (1961), 396–398.

[84] D. Zywina, ‘Hilbert’s irreducibility theorem and the larger sieve’, Preprint, 2010, available from arXiv/1011.6465 [math.NT].