Rose-Hulman Undergraduate Mathematics Journal

Volume 21 | Issue 2 Article 3

A Case Study on Hooley's Conditional Proof of Artin's Primitive Root Conjecture

Shalome Kurian
University of Warwick, Coventry, shalomekurian98@gmail.com

A Case Study on Hooley's Conditional Proof of Artin's Primitive Root Conjecture

Cover Page Footnote

I would like to thank my supervisor Dr Samuel Le Fourn for his support and advice, the URSS for facilitating the project during which this paper was completed and the Warwick Mathematics Institute for funding the project.

Rose-Hulman Undergraduate Mathematics Journal
Volume 21, Issue 2, 2020

A Case Study on Hooley's Conditional Proof of Artin's Primitive Root Conjecture

By *Shalome Kurian*

Abstract. Artin's Primitive Root Conjecture represents one of many famous problems in elementary number theory that has resisted complete solution thus far. Significant progress was made in 1967, when Christopher Hooley published a conditional proof of the conjecture under the assumption of a certain case of the Generalised Riemann Hypothesis. In this survey we present a description of the conjecture and the underlying algebraic theory, and provide a detailed account of Hooley's proof which is intended to be accessible to those with only undergraduate level knowledge. We also discuss a result concerning the $qx+1$ problem, whose proof requires similar techniques to those used by Hooley.

1 Introduction

The question of which integers generate the group $(\mathbb{Z}/p\mathbb{Z})^*$ for prime numbers p is a longstanding open problem in number theory. We call these generators *primitive roots modulo p*. Gauss proved that primitive roots exist for every prime p in his Disquisitiones Arithmeticae (1801), but the proof was not constructive, so determining whether a given integer is a primitive root remained a difficult problem. In articles 315-317 of the same text, he considered the decimal expansions of fractions of the form $\frac{1}{p}$, and in particular which expansions had the maximal period length $p-1$, which amounts to determining whether 10 is a primitive root modulo p. For example, $\frac{1}{7} = 0.\overline{142857}$ has period length 6, which shows that the order of 10 in the group $(\mathbb{Z}/7\mathbb{Z})^*$ is 6, thus 10 is a primitive root modulo 7. It is likely that Gauss asked himself with what frequency this occurred, but he did not provide even a conjectural answer to this question.

Over a century later, Emil Artin (1927) provided a precise conjecture based on heuristic analysis: for a nonsquare integer $g \neq -1$, the density (in a sense to be made precise later) of primes p for which g is a primitive root modulo p is given by

$$A(h) := \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right),$$

Mathematics Subject Classification. 11A07
Keywords. Artin Conjecture

where q goes through all prime numbers and h is the largest integer for which g is a perfect h-th power. The above quantity is easily shown to be nonzero, so a consequence is that g is a primitive root modulo p for infinitely many primes p. To put it in the language of Gauss: for these g, the period of the expansion of $\frac{1}{p}$ in base g is of maximal length infinitely often.

Later it was found that the conjecture as stated above was not consistent with numerical calculations when the squarefree part g_1 of g satsified $g_1 \equiv 1 \bmod 4$. This was due to an incorrect assumption in Artin's heuristic, namely that the fields $\mathrm{K}_q := \mathbb{Q}(\zeta_q, g^{1/q})$ (where $\zeta_q = e^{\frac{2\pi i}{q}}$) for primes q are pairwise linearly disjoint; that is, $\mathrm{K}_{q_1} \cap \mathrm{K}_{q_2} = \mathbb{Q}$. The proposed density was therefore modified in this case, and the reformulated conjecture was more consistent with numerical data and heuristics. Several results were soon published in support of the conjecture. Most notable are perhaps Hooley's proof (1967) of the conjecture under the assumption of the Generalised Riemann Hypothesis (GRH), and Heath-Brown's unconditional result (1986) that any nonsquare integer $g \neq -1$ is a primitive root modulo p for infinitely many primes p, with at most three exceptions. However, the conjecture is still not known to hold unconditionally for any specific choice of g.

The goal of this survey is to provide a description of the conjecture together with the underlying theory, and a detailed presentation of Hooley's conditional proof which is accessible to those with only a basic understanding of Galois theory and algebraic number theory. Some results in the survey are left unproved; in most cases this is because they are quite long or technical and do not contribute much to the overall understanding of the proof. The most noteworthy result of this kind is Chebotarev's Density Theorem. In each case we provide a reference for reader to view the proof if he/she is interested.

The survey is structured as follows. Section 2 is a discussion of the basic Hilbert ramification theory required to understand the statement of Chebotarev's Density Theorem, one version of which is presented at the end of the section. The next two sections are largely based on the relevant part of the survey by Moree [Mor12, pages 9-12]. In Section 3 we give the precise statement of Artin's Primitive Root Conjecture along with some key theoretical results and heuristics. In Section 4 we present Hooley's conditional proof, for the most part following the presentation in Hooley's original paper [Hoo67], but in more detail. There are two main steps in the proof. The first is establishing a different characterisation of the primes for which g is a primitive root, in terms of splitting of those primes in the number fields K_k. The second is more analytic, using a quantitative version of Chebotarev's Density Theorem (which holds under the assumption of GRH) to estimate the densities of the primes which split in each K_k. The latter forms the bulk of Hooley's work, though it is important to note that Hooley did not have access to such a precise form of Chebotarev's Density Theorem at the time - he instead used theory of the Riemann zeta function and applied GRH directly to obtain the estimate. Finally, we mention an interesting related problem in Section 5 which is linked to the famous

Collatz Conjecture.

2 Algebraic Preliminaries

2.1 Hilbert's ramification theory

Let L/K be an extension of number fields. It is a well known and central result in algebraic number theory that for any nonzero prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$, the ideal $\mathfrak{p}\mathcal{O}_L$ of $\mathcal{O}_L$ factorises uniquely as a product of prime ideals of $\mathcal{O}_L$. Let us consider what happens when L/K is a Galois extension. In this case, for any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, we have a natural action of the Galois group $G := \mathrm{Gal}(L/K)$ on the prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$ (that is, $\mathfrak{p}\mathcal{O}_L \subseteq \mathfrak{P}$). For convenience we will generally assume that $\mathfrak{p}$ denotes a nonozero prime ideal of $\mathcal{O}_K$ and $\mathfrak{P}$ (or $\mathfrak{P}_i$) denotes a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$.

Lemma 2.1. *For any prime ideal $\mathfrak{P}$ lying above $\mathfrak{p}$ and any $\sigma \in G$, the image $\sigma(\mathfrak{P})$ is also a prime ideal lying above $\mathfrak{p}$.*

Proof. It is clear that $\sigma(\mathfrak{P})$ is an ideal of $\mathcal{O}_L$, and it contains $\mathfrak{p}$ because σ fixes K. To see that it is prime, note that if $x, y \in \mathcal{O}_L$ and $xy \in \sigma(\mathfrak{P})$ then $\sigma^{-1}(xy) \in \mathfrak{P}$, so $\sigma^{-1}(x)$ or $\sigma^{-1}(y)$ belongs to $\mathfrak{P}$ as it is prime, and applying σ again, either x or y belongs to $\sigma(\mathfrak{P})$. □

In fact, the Galois group acts transitively on the prime ideals $\mathfrak{P}$ above $\mathfrak{p}$.

Proposition 2.2. *For any two prime ideals $\mathfrak{P}, \mathfrak{P}'$ lying above $\mathfrak{p}$, there is a $\sigma \in G$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Proof. We argue as in [Neu13, Proposition I.9.1], by assuming that $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$ for all $\sigma \in G$. By the Chinese Remainder Theorem, there exists $x \in \mathcal{O}_L$ such that

$$x \equiv 0 \bmod \mathfrak{P}' \quad \text{and} \quad x \equiv 1 \bmod \sigma(\mathfrak{P}) \quad \text{for all } \sigma \in G.$$

Observe that the norm $\mathrm{Nm}_{L/K}(x) = \prod_{\sigma\in G} \sigma(x) \in \mathfrak{P}' \cap \mathcal{O}_K = \mathfrak{p}$ (note that $x \in \mathfrak{P}'$ and one of the σ is the identity). But $x \notin \sigma^{-1}(\mathfrak{P})$ for any $\sigma \in G$, so $\sigma(x) \notin \mathfrak{P}$ for any $\sigma \in G$. Since $\mathfrak{P}$ is a prime ideal, it follows that $\prod_{\sigma\in G} \sigma(x) \notin \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}$ which is a contradiction. □

We recall some terminology before discussing more of the ramification theory. Suppose L/K is a (not necessarily Galois) extension of number fields and the prime ideal $\mathfrak{p}$ decomposes in L as

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}$$

(We will usually write $(\mathfrak{p})$ instead of $\mathfrak{p}\mathcal{O}_L$ from now on.) For each $\mathfrak{P} = \mathfrak{P}_i$, we call

$$e(\mathfrak{P}_i/\mathfrak{p}) := e_i, \quad f(\mathfrak{P}_i/\mathfrak{p}) := f_i := [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$$

respectively the *ramification index* and *inertia degree* of $\mathfrak{P}_i$. Note that the latter quantity makes sense as $\mathcal{O}_K/\mathfrak{p}$ naturally embeds into $\mathcal{O}_L/\mathfrak{P}_i$ since $\mathfrak{p} \subseteq \mathfrak{P}_i$, so $(\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$ is an extension of finite fields and thus has finite degree. An important relation between these quantities and the degree $n := [L:K]$ of the extension is the following formula [Neu13, Proposition I.8.2].

Proposition 2.3 (Fundamental Identity)**.** $\sum_{i=1}^{r} e_i f_i = n$.

We say that $\mathfrak{p}$ *splits completely* (or is *totally split*) if $r = n$, which by the identity above is equivalent to $e_i = f_i = 1$ for all i. On the other hand we call $\mathfrak{p}$ *inert* if $r = 1$ and $e_1 = 1$ (in other words, if $\mathfrak{p}\mathcal{O}_L$ is prime). As for prime ideals in the decomposition of $\mathfrak{p}$, we call $\mathfrak{P}_i$ *ramified* (over K) if $e_i > 1$, and *totally ramified* if we also have $f_i = 1$. We say that $\mathfrak{p}$ is *ramified* if at least one $\mathfrak{P}_i$ is ramified, and *unramified* otherwise.

In the case that L/K is a Galois extension, the situation simplifies considerably.

Proposition 2.4. *If* L/K *is Galois then the ramification indices and inertia degrees* $e(\mathfrak{P}/\mathfrak{p})$, $f(\mathfrak{P}/\mathfrak{p})$ *are independent of the prime ideal* $\mathfrak{P}$ *above* $\mathfrak{p}$ *chosen. If we denote them by* e, f *and by* r *the number of those prime ideals, we thus have*

$$efr = [L:K].$$

Proof. Since G acts transitively on prime ideals above $\mathfrak{p}$, for each i there exists $\sigma_i \in G$ such that $\sigma_i(\mathfrak{P}_1) = \mathfrak{P}_i$. Then we have an isomorphism $\mathcal{O}_L/\mathfrak{P}_1 \to \sigma_i(\mathcal{O}_L)/\sigma_i(\mathfrak{P}_1) = \mathcal{O}_L/\mathfrak{P}_i$ given by $x + \mathfrak{P}_1 \mapsto \sigma_i(x) + \sigma_i(\mathfrak{P}_1)$. This gives us an isomorphism of quotients $(\mathcal{O}_L/\mathfrak{P}_1)/(\mathcal{O}_K/\mathfrak{p}) \cong (\mathcal{O}_L/\mathfrak{P}_i)/(\mathcal{O}_K/\mathfrak{p})$ which establishes that $f_i = f_1$. Using that $\sigma_i(\mathfrak{p}\mathcal{O}_L) = \mathfrak{p}\mathcal{O}_L$ we see that $\mathfrak{P}_1^k | \mathfrak{p}\mathcal{O}_L \iff \sigma_i(\mathfrak{P}^k) | \sigma_i(\mathfrak{p}\mathcal{O}_L) \iff \mathfrak{P}_i^k | \mathfrak{p}\mathcal{O}_L$ which implies that $e_i = e_1$.

The formula is then a direct application of the Fundamental Identity in this special case. □

Let us take a look at a concrete example with quadratic fields. Consider the extension L/$\mathbb{Q}$, where $L := \mathbb{Q}(\sqrt{d})$ and d is a nonzero squarefree integer not equal to 1 (note that L/$\mathbb{Q}$ is Galois). We want to know how for a given rational prime p, the ideal $p\mathcal{O}_L$ factors as a product of prime ideals of $\mathcal{O}_L$. In this case we have $n = 2$, so by the Fundamental Identity there are only three possibilities: $p\mathcal{O}_L = \mathfrak{P}_1\mathfrak{P}_2$ with $\mathfrak{P}_1, \mathfrak{P}_2$ distinct prime ideals, $p\mathcal{O}_L = \mathfrak{P}_1^2$ and $p\mathcal{O}_L = \mathfrak{P}_1$; that is, $p\mathcal{O}_L$ is itself a prime ideal of $\mathcal{O}_L$. A very useful tool for this problem is the Dedekind-Kummer Theorem [Neu13, Proposition I.8.3].

Theorem 2.5 (Dedekind-Kummer)**.** *Let* $K = \mathbb{Q}(\alpha)$ *be a number field, where* α *is an algebraic integer. Let* p *be a rational prime which does not divide* $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. *Let* $P(X) \in \mathbb{Z}[X]$

be the minimal polynomial of α*, and let* $\overline{P}(X) \in \mathbb{F}_p[X]$ *denote the reduction of* P *modulo* p*. Let the factorisation of* $\overline{P}$ *into monic irreducible polynomials be*

$$\overline{P} = \overline{P_1}^{e_1}\overline{P_2}^{e_2}\dots\overline{P_r}^{e_r},$$

where the $\overline{P_i}(X) \in \mathbb{F}_p[X]$ *are pairwise distinct. For each* i*, choose a polynomial* $P_i(X) \in \mathbb{Z}[X]$ *such that* $\overline{P_i} \equiv P_i \bmod p\mathbb{Z}[X]$*. Let* $\mathfrak{P}_i$ *denote the ideal* $(p, P_i(\alpha))$ *in* $\mathcal{O}_K$*. Then:*
(i) the $\mathfrak{P}_i$ *are pairwise distinct prime ideals of* $\mathcal{O}_K$*;*
(ii) the $\mathfrak{P}_i$ *are the only prime ideals in* $\mathcal{O}_K$ *dividing* (p)*;*
(iii) $\mathrm{Nm}(\mathfrak{P}_i) = p^{\deg(\overline{P_i})}$*;*
(iv) $(p) = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\dots\mathfrak{P}_r^{e_r}$*.*

Example 2.6. For $L = \mathbb{Q}(\sqrt{10})$, the discriminant is 40 and the integer ring is $\mathbb{Z}[\sqrt{10}]$, with the generator having minimal polynomial $X^2 - 10$. We thus have three cases for the decomposition of a prime number p in $\mathcal{O}_L$:

- If $p = 2$ or 5, p is ramified in L; more precisely $p\mathcal{O}_L = (p, \sqrt{10})^2$.
- If 10 is a quadratic residue mod p (e.g. $p = 3$), p is totally split in L; more precisely $p\mathcal{O}_L = (p, \sqrt{10} + a)(p, \sqrt{10} - a)$ where $a \in \mathbb{Z}$ is chosen such that $a^2 \equiv 10 \bmod p$.
- If 10 is not a quadratic residue mod p (e.g. $p = 7$), p is inert in L, i.e. $p\mathcal{O}_L$ is a prime ideal.

The conditions of 10 being a square or not modulo p can of course be checked via quadratic reciprocity, and amount to congruence conditions of p modulo 40.

Remark 2.7. Notice that $f(\mathfrak{P}_i/p) = \deg(\overline{P_i})$, so the Dedekind-Kummer Theorem provides a more concrete interpretation of the inertia degrees as the degrees of the corresponding polynomials in the factorisation of the minimal polynomial over $\mathbb{F}_p$.

It is also easy to show using the theorem in the quadratic case that p is ramified in $\mathbb{Q}(\sqrt{d})$ if and only if $p|\Delta_K$ (noting that $\Delta_K = d$ if $d \equiv 1 \bmod 4$ and $\Delta_K = 4d$ otherwise). In fact this result holds in full generality: given an extension of number fields L/K, a prime ideal $\mathfrak{p}$ is ramified in K if and only if it divides the relative discriminant $\Delta_{L/K}$ [Neu13, Corollary III.2.12]. In particular this shows that only finitely many prime ideals are ramified in K.

Let us return to looking at the action of the Galois group $G = \mathrm{Gal}(L/K)$ on the prime ideals $\mathfrak{P}$ lying above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. We can assume these prime ideals are unramified because as we saw earlier, there are only finitely many that are ramified, so

this makes no difference to the densities discussed later on. For each prime $\mathfrak{P}$ above $\mathfrak{p}$, define the *decomposition subgroup* $D_{\mathfrak{P}}$ of G by

$$D_{\mathfrak{P}} := \{\sigma \in G \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

made up with the elements of G which fix $\mathfrak{P}$ setwise. By the Orbit-Stabiliser Theorem, as G acts transitively on the prime ideals above $\mathfrak{p}$ by Proposition 2.2, it is of order $n/r = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ using Proposition 2.4. We then consider the map

$$\Phi_{\mathfrak{P}} : D_{\mathfrak{P}} \to \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$$

given by $\sigma \mapsto \overline{\sigma}$. Here, $\overline{\sigma}$ is defined by $\overline{\sigma}(\overline{x}) := \overline{\sigma(x)}$ for $x \in \mathcal{O}_L$, where the bar denotes the class in the quotient $\mathcal{O}_L/\mathfrak{P}$. The extension $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$ is indeed Galois as any extension of finite fields is. The map $\overline{\sigma}$ is well-defined: if $x - y \in \mathfrak{P}$ then $\sigma(x) - \sigma(y) = \sigma(x-y) \in \mathfrak{P}$ because $\sigma \in D_{\mathfrak{P}}$, and it is easy to see that $\overline{\sigma} \in \mathrm{Gal}((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p}))$ and that $\Phi_{\mathfrak{P}}$ is a group homomorphism.

Proposition 2.8. *The homomorphism $\Phi_{\mathfrak{P}}$ is surjective.*

Proof. This is proven in [Neu13, Proposition I.9.4]; we restate the ideas here for our own purposes.

First, consider the extension $L/L^{D_{\mathfrak{P}}}$. Its Galois group is $D_{\mathfrak{P}}$ by Galois correspondence; in particular every element of it fixes $\mathfrak{P}$. In other words, there is only one prime ideal of $\mathcal{O}_L$ above $\mathfrak{P}_D := \mathfrak{P} \cap \mathcal{O}_{L^{D_{\mathfrak{P}}}}$ which is $\mathfrak{P}$ itself, so

$$e(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}/\mathfrak{P}_D) = [L : L^{D_{\mathfrak{P}}}] = e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p}).$$

By multiplicativity of the indices and degrees, we have $e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}/\mathfrak{P}_D)e(\mathfrak{P}_D/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{P}_D)f(\mathfrak{P}_d/\mathfrak{p})$. Combined with the previous equalities, this implies that $e(\mathfrak{P}_D/\mathfrak{p}) = f(\mathfrak{P}_D/\mathfrak{p}) = 1$; in particular $\mathcal{O}_{L^{D_{\mathfrak{P}}}}/\mathfrak{P}_D = \mathcal{O}_K/\mathfrak{p}$ when they are both seen as subfields of $\mathcal{O}_L/\mathfrak{P}$.

By the Primitive Element Theorem, there exists $\overline{\theta} \in \mathcal{O}_L/\mathfrak{P}$ which generates this field over $\mathcal{O}_K/\mathfrak{p}$. Let $\theta \in \mathcal{O}_L$ be a lift of this element so that $\overline{\theta} = \theta \bmod \mathfrak{P}$. We call $\overline{g}$ the minimal polynomial of $\overline{\theta}$ over $\mathcal{O}_K/\mathfrak{p}$, and f the minimal polynomial of θ over $L^{D_{\mathfrak{P}}}$, with algebraic integral coefficients because θ is integral over $\mathbb{Z}$ so over $\mathcal{O}_{L^{D_{\mathfrak{P}}}}$ as well. As the extension $L/L^{D_{\mathfrak{P}}}$ is Galois, f is split into linear factors in $\mathcal{O}_L$, and putting this modulo $\mathfrak{P}_D$, $f \bmod \mathfrak{P}_D \in (\mathcal{O}_K/\mathfrak{p})[X]$ is split into linear factors in $\mathcal{O}_L/\mathfrak{P}$, so every root of this reduction can be lifted to a root of f in $\mathcal{O}_L$. Furthermore, as $\overline{f} := f \bmod \mathfrak{P}_D \in (\mathcal{O}_K/\mathfrak{p})[X]$ and vanishes on $\overline{\theta}$, $\overline{g}$ divides $\overline{f}$ as the former is the minimal polynomial.

We can now prove that $\Phi_{\mathfrak{P}}$ is surjective. Let $\overline{\sigma}$ be an automorphism of $(\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})$. As $\overline{g}$ is irreducible, $\overline{\sigma}$ sends $\overline{\theta}$ to another root of $\overline{g}$, but $\overline{g}$ divides $f \bmod \mathfrak{P}_D$, so to a

$\theta' \bmod \mathfrak{P}$ with $\theta' \in \mathscr{O}_L$ a root of f. Now, as f is irreducible over $L^{D_\mathfrak{P}}$ and the extension $L/L^{D_\mathfrak{P}}$ is Galois, there is an automorphism $\sigma \in D_\mathfrak{P}$ sending θ to θ'. Considering this modulo $\mathfrak{P}$, we have

$$\overline{\sigma}(\overline{\theta}) = \overline{\theta'} = \sigma(\theta) \bmod \mathfrak{P}$$

which proves that $\overline{\sigma} = \Phi_\mathfrak{P}(\sigma)$ because $\sigma \in D_\mathfrak{P}$ and $\overline{\theta}$ generates $\mathscr{O}_L/\mathfrak{P}$ over $\mathscr{O}_K/\mathfrak{p}$. □

It is a well known result that the Galois group of an extension of finite fields such as $(\mathscr{O}_L/\mathfrak{P})/(\mathscr{O}_K/\mathfrak{p})$ is cyclic, generated by the Frobenius element $x \mapsto x^{\#\mathscr{O}_K/\mathfrak{p}}$. By the above proposition, we deduce that there is an element $(\mathfrak{P}, L/K) \in D_\mathfrak{P}$ such that $\sigma((\mathfrak{P}, L/K)) = \overline{(\mathfrak{P}, L/K)}$ is the Frobenius element of $\mathrm{Gal}((\mathscr{O}_L/\mathfrak{P})/(\mathscr{O}_K/\mathfrak{p}))$.

Definition 2.9. When $\mathfrak{P}$ is unramified over K, the map $\Phi_\mathfrak{P}$ is an isomorphism and we thus define the *Frobenius symbol* (or *Frobenius* for short) $(\mathfrak{P}, L/K)$ as the unique element of G such that for all $x \in \mathscr{O}_L$,

$$(\mathfrak{P}, L/K)(x) \equiv x^{\#\mathscr{O}_K/\mathfrak{p}} \bmod \mathfrak{P}.$$

Proof of uniqueness. As the order of $D_\mathfrak{P}$ is $e(\mathfrak{P}/\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$ and $\Phi_\mathfrak{P}$ surjects onto a group of order $f(\mathfrak{P}/\mathfrak{p})$ by definition, its kernel is of order $e(\mathfrak{P}/\mathfrak{p})$. In particular, it is an isomorphism if and only if $\mathfrak{P}$ is unramified, and we can then define the Frobenius as above. □

The most important case of use of the Frobenius is the following.

Lemma 2.10. *If* $\mathfrak{p}$ *is unramified in* L/K*, then it is totally split if and only if* $(\mathfrak{P}, L/K) = 1$ *for one (all) prime ideal(s)* $\mathfrak{P}$ *above* $\mathfrak{p}$.

Proof. Let us fix a prime ideal $\mathfrak{P}$ above $\mathfrak{p}$. The Frobenius is well-defined because of the assumption, and of order $f = f(\mathfrak{P}/\mathfrak{p})$ because $\Phi_\mathfrak{P}(\mathfrak{P}, L/K)$ is by definition. It is thus the identity if and only if $f = 1$, which is equivalent to saying that $\mathfrak{p}$ is totally split (since $e = 1$). □

In general, $(\mathfrak{P}, L/K)$ depends on the choice of prime $\mathfrak{P}$ above $\mathfrak{p}$. Recall that for any two prime ideals $\mathfrak{P}$ and $\mathfrak{P}'$ above $\mathfrak{p}$, we can find $\sigma \in G$ such that $\mathfrak{P}' = \sigma(\mathfrak{P})$. Then we have $(\mathfrak{P}', L/K) = \sigma(\mathfrak{P}, L/K)\sigma^{-1}$. Indeed, by definition of $(\mathfrak{P}, L/K)$, for any $x \in \mathscr{O}_L$ we have

$$(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv \sigma^{-1}(x)^{\#\mathscr{O}_K/\mathfrak{p}} \bmod \mathfrak{P},$$

or

$$(\mathfrak{P}, L/K)\sigma^{-1}(x) \equiv \sigma^{-1}(x^{\#\mathscr{O}_K/\mathfrak{p}}) \bmod \sigma^{-1}(\mathfrak{P}'),$$

thus

$$\sigma(\mathfrak{P}, \mathrm{L}/\mathrm{K})\sigma^{-1}(x) \equiv x^{\#\mathscr{O}_\mathrm{K}/\mathfrak{p}} \bmod \mathfrak{P}'$$

and the result follows by uniqueness. We then define the Frobenius symbol $(\mathfrak{p}, \mathrm{L}/\mathrm{K})$ to be the conjugacy class $\{(\mathfrak{P}, \mathrm{L}/\mathrm{K}) \mid \mathfrak{P}|\mathfrak{p}\}$. Note that in the case of an abelian Galois group G, the Frobenius symbol $(\mathfrak{P}, \mathrm{L}/\mathrm{K})$ is independent of the choice of $\mathfrak{P}$, so we denote it by $(\mathfrak{p}, \mathrm{L}/\mathrm{K})$ and it may be viewed as the unique automorphism such that

$$(\mathfrak{p}, \mathrm{L}/\mathrm{K})(x) \equiv x^{\#\mathscr{O}_\mathrm{K}/\mathfrak{p}} \bmod \mathfrak{p}\mathscr{O}_\mathrm{L},$$

because

$$(\mathfrak{p}, \mathrm{L}/\mathrm{K})(x) \equiv x^{\#\mathscr{O}_\mathrm{K}/\mathfrak{p}} \bmod \mathfrak{P}$$

for all $\mathfrak{P} \mid \mathfrak{p}$ and $\mathfrak{P}_1 \cap \mathfrak{P}_2 \cap \ldots \cap \mathfrak{P}_r = \mathfrak{p}\mathscr{O}_\mathrm{L}$ by the Chinese Remainder Theorem.

We conclude this section with two lemmas on the splitting of prime ideals in subextensions and compositums (the latter of which holds even in the non-Galois case).

Lemma 2.11. *Let* L/K *be a Galois extension of number fields and* $\mathfrak{P}$ *be a prime ideal above* $\mathfrak{p}$. *For any subextension* K' *of* L/K, *let us denote* $\mathfrak{P}' = \mathfrak{P} \cap \mathscr{O}_{\mathrm{K}'}$ *the ideal below* $\mathfrak{P}$. *Then,* $\mathrm{K}' \subset \mathrm{L}^{\mathrm{D}_\mathfrak{P}}$ *if and only if* $e(\mathfrak{P}'/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p}) = 1$.

Proof. This is the first part of [Mar18, Chapter 2, Theorem 30]. □

It has an application to all extensions of number fields in the following shape:

Lemma 2.12. *Let* L/K *and* L'/K *be two (not necessarily Galois) extensions of number fields and* $\mathfrak{p}$ *a nonzero prime ideal of* $\mathscr{O}_\mathrm{K}$. *It is totally split in* LL' *if and only if it is totally split in* L *and in* L'.

Proof. Let M be a Galois extension of K containing L and L' (and thus LL'), and $\mathrm{M}_\mathrm{D} := \cap_\mathfrak{P} \mathrm{M}^{\mathrm{D}_\mathfrak{P}}$ where $\mathfrak{P}$ goes through the prime ideals of $\mathscr{O}_\mathrm{M}$ above $\mathfrak{p}$. By the previous lemma, for any subextension K' of M/K, $\mathfrak{p}$ is totally split in K' if and only if $\mathrm{K}' \subset \mathrm{M}_\mathrm{D}$ because every prime ideal of $\mathscr{O}_{\mathrm{K}'}$ above $\mathfrak{p}$ is of the shape $\mathfrak{P} \cap \mathscr{O}_{\mathrm{K}'}$.

Consequently, $\mathfrak{p}$ is totally split in LL' if and only if $\mathrm{LL}' \subset \mathrm{M}^{\mathrm{D}_\mathfrak{P}}$ which is equivalent to $\mathrm{L} \subset \mathrm{M}^{\mathrm{D}_\mathfrak{P}}$ and $\mathrm{L}' \subset \mathrm{M}^{\mathrm{D}_\mathfrak{P}}$, which in turn are equivalent to $\mathfrak{p}$ being totally split in L and in L'. □

2.2 The cyclotomic case

Now let $n \geq 1$ be an integer and consider the cyclotomic field extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, where $\zeta_n = e^{\frac{2\pi i}{n}}$ is a primitive n-th root of unity. Henceforth, φ denotes Euler's totient function.

Proposition 2.13.

• *The extension* $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ *is Galois of degree* $\varphi(n)$ *and there is a canonical isomorphism of groups* $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^*$ *defined by*

$$\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}.$$

• *The ring of integers of* $\mathbb{Q}(\zeta_n)$ *is* $\mathbb{Z}[\zeta_n]$.

• *The discriminant of* $\mathbb{Q}(\zeta_n)$ *has the same prime factors as* n*; in particular, the prime numbers which ramify in* $\mathbb{Q}(\zeta_n)$ *are exactly the ones that divide* n.

Proof. The first point (degree of the extension) is given in [Mar18], Chapter 2, and it is then easy to see that we can define automorphisms $\zeta_n \mapsto \zeta_n^k$ for k prime to n. We thus obtain $\varphi(n)$ field automorphisms, which proves that the extension is Galois and the isomorphism of groups.

The second point is [Neu13, Proposition III.10.2].

Finally, the precise discriminant computation is in [Was97, Proposition 2.7] and implies the third point. □

With these results, we know enough to prove the reciprocity law for cyclotomic fields.

Theorem 2.14. *For every prime number* p *not dividing* n, $\chi((p, \mathbb{Q}(\zeta_n)/\mathbb{Q})) = p$ *in* $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. Consider $\chi^{-1}(p)$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$. By definition of χ, it sends ζ_n to ζ_n^p, so for any prime ideal $\mathfrak{P}$ of $\mathbb{Z}[\zeta_n]$ above p, it sends the reduction of ζ_n to its p-th power. It is thus the Frobenius automorphism $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q})$, which proves the theorem. □

Corollary 2.15. *For any prime number not dividing* n, p *is totally split in* $\mathbb{Q}(\zeta_n)$ *if and only if* $p \equiv 1 \bmod n$.

This theorem also allows us to define a more general Frobenius: for any positive integer a coprime to n with prime factorisation $a = p_1^{k_1} \dots p_r^{k_r}$, we define

$$(a, \mathbb{Q}(\zeta_n)/\mathbb{Q}) := \prod_{i=1}^{r} (p_i, \mathrm{L/K})^{k_i} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}),$$

and by multiplicativity of χ, the previous theorem gives

$$\chi((a, \mathbb{Q}(\zeta_n)/\mathbb{Q})) = \overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*.$$

2.3 Chebotarev's Density Theorem

We are now ready to introduce a powerful theorem that will be useful later on (in a more quantitative version). In particular, it tells us that any element of G can be expressed as the Frobenius symbol of a prime (up to conjugacy). This version is proved in [Hei67, Theorem 5].

Theorem 2.16 (Chebotarev's Density Theorem)**.** *Suppose* L/K *is a Galois extension and* C *is a conjugacy class in* G*. Then the set*

$$\{\mathfrak{p} \mid \mathfrak{p} \text{ is a prime ideal of } \mathcal{O}_K \text{ unramified in L}, (L/K, \mathfrak{p}) \in C\}$$

has natural density $\frac{\#C}{\#G}$.

Here, the natural density of a set S of prime ideals of $\mathcal{O}_K$ is defined (if it exists) as

$$d(S) := \lim_{x\to\infty} \frac{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x, \mathfrak{p} \in S\}}{\#\{\mathfrak{p} \mid \mathrm{Nm}(\mathfrak{p}) \le x, \mathfrak{p} \text{ prime}\}}.$$

As an example application of the theorem, we deduce (a stronger form of) Dirichlet's Theorem on primes in arithmetic progression.

Corollary 2.17 (Dirichlet's Theorem)**.** *Let a and n be coprime positive integers. Then the set* $\{p \mid p \equiv a \bmod n\}$ *has natural density* $\frac{1}{\varphi(n)}$*. In particular, there infinitely many prime numbers congruent to a modulo n.*

Proof. We apply Chebotarev's Density Theorem to the cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. From section 1.2, we know that this extension is Galois with abelian Galois group isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ and by Theorem 2.14, $(p, \mathbb{Q}(\zeta_n)/\mathbb{Q}) = (a, \mathbb{Q}(\zeta_n)/\mathbb{Q})$ if and only if $p \equiv a \bmod n$. Therefore, Chebotarev's Density Theorem says that the set $\{p \mid p \equiv a \bmod n\}$ has natural density $\frac{1}{\#(\mathbb{Z}/n\mathbb{Z})^*} = \frac{1}{\varphi(n)}$ as required. □

3 Artin's Primitive Root Conjecture

3.1 Statement of the conjecture

We now introduce the main subject of the paper, Artin's Primitive Root Conjecture. Let us first look at an example. It is a standard result that for any prime p, the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. It has $\varphi(p-1)$ generators, given by g^k where k is coprime to $p-1$ and g is a fixed choice of generator. We refer to generators of $(\mathbb{Z}/p\mathbb{Z})^*$ as *primitive roots modulo* p. For example, the first ten powers of 2 modulo 11 are $2, 4, 8, 5, 10, 9, 7, 3, 6, 1$, thus 2 is a primitive root modulo 11. We may then ask:

For how many primes p is 2 *a primitive root modulo p?*

After computing many examples one may expect that the answer is "infinitely many" and that the same might be true for integers other than 2. Artin's conjecture addresses this question with an affirmative and even quantitative answer. For integers g we define

$$\mathcal{P}(g) := \{p \text{ prime} \mid g \text{ is a primitive root modulo } p\}$$

and $\mathscr{P}(g)(x) := \#\{p \in \mathscr{P}(g) \mid p \le x\}$. Then we have the following.

Conjecture (Artin's Primitive Root Conjecture)**.** Let $g \neq -1$ be a nonsquare integer. Then the set $\mathscr{P}(g)$ is infinite.
Moreover, if h is the largest integer for which g is a perfect h-th power (that is, $g = g_0^h$ for some integer g_0), g_1 is the squarefree part of g and

$$A(h) := \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right)$$

(where the products run over all primes q), then as $x \to +\infty$,

$$\mathscr{P}(g)(x) = \delta(g)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right),$$

where

$$\delta(g) := \begin{cases} A(h) & \text{if } g_1 \not\equiv 1 \bmod 4, \\ \left(1 - \mu(|g_1|) \displaystyle\prod_{q \mid g_1, q \mid h} \frac{1}{q-2} \prod_{q \mid g_1, q \nmid h} \frac{1}{q^2-q-1}\right) A(h) & \text{if } g_1 \equiv 1 \bmod 4. \end{cases}$$

Here μ is the Möbius function defined by $\mu(n) = (-1)^{\omega(n)}$ if n is squarefree and $\mu(n) = 0$ otherwise, where $\omega(n)$ is the number of distinct prime factors of n. The number $A := \prod_q \left(1 - \frac{1}{q(q-1)}\right)$ is called Artin's constant. Notice that it is nonzero as the sum of logarithms of $1 - 1/(q(q-1))$ converges to a real number (and then A is its exponential). It is also easy to see that the coefficient of $A(h)$ in the second part of the definition of $\delta(g)$ is always positive, thus so is $\delta(g)$ for any g.

Clearly the quantitative estimate implies the first statement. The quantity $\delta(g)$ can actually be interpreted as the "probability" that g is a primitive root modulo a given prime p due to the following fundamental result.

Theorem 3.1 (Prime Number Theorem)**.** *Let $\pi(x)$ be the prime-counting function, $\pi(x) = \#\{p \text{ prime} \mid p \le x\}$. Then*

$$\pi(x) \sim \frac{x}{\log x}.$$

The notation above means that the the two quantities are asymptotically equal, that is

$$\lim_{x \to \infty} \frac{\pi(x)}{\left(\frac{x}{\log x}\right)} = 1.$$

3.2 Standard results and heuristics

We will be making extensive use of the following different characterisation of the primes $p \in \mathscr{P}(g)$ which is easier to analyse and straightforward to prove.

Lemma 3.2. *For any prime p, we have $p \in \mathscr{P}(g)$ if and only if $g^{\frac{p-1}{q}} \not\equiv 1 \bmod p$ for each prime factor q of $p-1$.*

Proof. ($\Rightarrow$) Clear since the order of g modulo p is $p-1$.
($\Leftarrow$) If $p \notin \mathscr{P}(g)$ then by Lagrange's Theorem $g^m \equiv 1 \bmod p$ for some proper divisor m of $p-1$. Writing $k = \frac{p-1}{m} > 1$ and letting q be any prime factor of k (and thus of $p-1$), we have $g^{\frac{p-1}{q}} \equiv 1 \bmod p$ which is a contradiction. □

One of the key objects in Hooley's conditional proof of Artin's conjecture are the number fields $\mathrm{K}_q := \mathbb{Q}(\zeta_q, g^{\frac{1}{q}})$ (for a fixed choice of q-th root of g, which does not change K_q). This is because of the remarkable result that

Proposition 3.3. $(p \equiv 1 \bmod q,\ g^{\frac{p-1}{q}} \equiv 1 \bmod p) \iff p$ *splits completely in* K_q.

This equivalence is the main reason why we can apply the abstract algebraic theory discussed in Section 1 towards proving this conjecture, which on the surface looks elementary in nature. We can and will assume for the proof that p does not divide g because otherwise neither side holds (as p would then be ramified in K_q).

We will prove this result by establishing the intermediate equivalences

$$\left(p \equiv 1 \bmod q,\ g^{\frac{p-1}{q}} \equiv 1 \bmod p\right) \iff \mathrm{X}^q - g \text{ splits over } \mathbb{F}_p \iff p \text{ splits completely in } \mathrm{K}_q.$$

The case $q = 2$ can be done by itself, with $\mathrm{K}_2 = \mathbb{Q}(\sqrt{g})$ being a quadratic field (as we assumed g is not a square). Indeed, the left condition means that p is odd and $g^{(p-1)/2} \equiv 1 \bmod p$ which is equivalent to g being a quadratic residue modulo p, and it is equivalent (as p is odd) to p splitting completely in $\mathbb{Q}(\sqrt{g})$ by applying the Dedekind-Kummer Theorem to $\mathbb{Z}[\sqrt{g}]$ of index 1 or 2 in $\mathscr{O}_{\mathrm{K}_2}$.

Let us then fix a prime number $q > 2$ and an integer g assumed not to be a q-th power (otherwise, $\mathrm{K}_q = \mathbb{Q}(\zeta_q)$ and both sides of the equivalence hold by the proof of Corollary 2.17 for $a = 1$). The set of "bad" primes coming from q will be denoted by

$$\mathscr{B}_q(g) := \{p \in \mathscr{P}, \quad p \equiv 1 \bmod q \text{ and } g^{\frac{p-1}{q}} \equiv 1 \bmod p\}.$$

The link with Artin's conjecture is that p is a "good" prime for g (that is, g generates $(\mathbb{Z}/p\mathbb{Z})^*$) if and only if p does not belong to any of the $\mathscr{B}_q(g)$.

To make the proof easier to understand, we recall a basic lemma on cyclic groups.

Lemma 3.4. *Let $n \geq 1$ be an integer. Then for any integer $d \geq 1$:*

- *There exists an element of $\mathbb{Z}/n\mathbb{Z}$ of order exactly d if and only if $d|n$.*
- *Conversely, for any $d|n$, the multiples of d are the elements of $d\mathbb{Z}/n\mathbb{Z}$, which are also exactly the elements of order dividing n/d.*

Proof. The forward direction of the first item follows immediately from Lagrange's Theorem, and for the converse note that the element $\overline{n/d}$ has order d.
For the second item, consider $a \in \mathbb{Z}$ and its congruence class $\overline{a}$ modulo n. It is of order dividing n/d if and only if $(n/d)\overline{a} = 0 \bmod n$, which means that n divides $(n/d)a$ i.e $d|a$. We have thus proved that the elements of order dividing n/d are the multiples of d. Conversely, for any $a \in \mathbb{Z}$, $(n/d)\cdot(d\cdot\overline{a}) = n\cdot\overline{a} = 0 \bmod n$ which proves the other direction. □

Proof of Proposition 3.3. Let us recall that we assume that $q > 2$, g is not a q-th power and p does not divide g.

First we show that $p \in \mathscr{B}_q(g)$ if and only if the polynomial $X^q - \overline{g}$ is split (into distinct linear factors) in $\mathbb{F}_p$.

Indeed, if it has one root (say a) in $\mathbb{F}_p$ then g is a q-th power in $\mathbb{F}_p^*$, and then the other roots are of the shape $\zeta\cdot a$ with ζ a q-th root of unity. Consequently, $X^q - g$ is split in $\mathbb{F}_p^*$ if and only if in the latter group $\overline{g}$ is a q-th power, and there are elements of order exactly q. Using that $\mathbb{F}_p^* \cong \mathbb{Z}/(p-1)\mathbb{Z}$ and the previous lemma, this is equivalent to saying that q divides $p-1$ and $\overline{g}^{(p-1)/q} = 1$ which by definition means that p belongs to $\mathscr{B}_q(g)$.

The splitting field of $X^q - g$ is, for the same reasons, $K_q := \mathbb{Q}(\zeta_q, g^{1/q})$. We want to apply the Dedekind-Kummer Theorem to establish an equivalence with splitting of primes.

Firstly, $K := \mathbb{Q}(g^{1/q})$ is an extension of $\mathbb{Q}$ of degree exactly q: indeed, for d the degree of the extension, $|\mathrm{Nm}_{K/\mathbb{Q}}(g^{1/q})| = |g|^{d/q}$ (as the conjugates of $g^{1/q}$ must be amongst the $\zeta_q^k g^{1/q}$, so are of absolute value $|g|^{1/q}$) but it has to be an integer, which forces $q|d$ by hypothesis (as $|g|$ is not a q-th power either, q being odd), and as $X^q - g$ vanishes at $g^{1/q}$ and is of degree q, it must be the minimal polynomial, making the extension $K/\mathbb{Q}$ of degree exactly q.

Now, a classical discriminant formula [Mar18, Chapter 2, Theorem 8] gives that

$$\mathrm{disc}(1, g^{1/q}, \cdots, g^{(q-1)/q}) = \pm \mathrm{Nm}_{K/\mathbb{Q}}(q(g^{1/q})^{q-1}) = \pm q^q g^{q-1}.$$

On the other hand, this discriminant is also equal [Mar18, Chapter 2, proof of Theorem 11] to

$$\mathrm{disc}(\mathscr{O}_K)\cdot[\mathscr{O}_K : \mathbb{Z}[g^{1/q}]]^2,$$

which proves that for any prime p not dividing gq, p is unramified in K and we can apply the Dedekind-Kummer Theorem to $X^q - \overline{g} \in \mathbb{F}_p[X]$. It then says that p is totally split in $\mathbb{Q}(g^{1/q})$ if and only if the polynomial $X^q - \overline{g} \in \mathbb{F}_p[X]$ is split into q distinct linear factors;

in other words the equation $x^q = g \bmod p$ has exactly q solutions in $\mathbb{F}_p$. Notice this is a condition only on $\mathbb{Q}(g^{1/q})$ which is not Galois, but this is sufficient: if this polynomial is split as said, then in particular $p \equiv 1 \bmod q$ so p is totally split in $\mathbb{Q}(\zeta_q)$ as well, thus in the compositum K_q by Lemma 2.12. Conversely, if p is totally split in K_q, it must also be totally split in any subextension, hence in $\mathbb{Q}(g^{1/q})$ which means that $\mathrm{X}^q - \overline{g}$ is split into q distinct linear factors.

We have thus characterised the belonging of p to $\mathscr{B}_q(g)$. □

In what follows, we will actually be interested in the more general number fields $\mathrm{K}_k = \mathbb{Q}(\zeta_k, g^{1/k})$ for k squarefree, so the following two results will be useful.

Lemma 3.5. *Let k be a squarefree positive integer. Then K_k is the compositum of the fields K_q with $q|k$ and q prime.*

Proof. For any prime $q|k$, the field K_k contains K_q because $\zeta_q = \zeta_k^{k/q} \in \mathrm{K}_k$ and $g^{1/q} = (g^{1/k})^{k/q} \in \mathrm{K}_k$. Conversely, suppose F is a field containing $g^{1/q}$ for all primes $q|k$. We prove, by induction on the number of prime factors N of k, that $g^{1/k} \in \mathrm{F}$. The base case $\mathrm{N} = 1$ holds trivially. Now let $\mathrm{N} > 1$ and suppose that k is squarefree with N prime factors and $g^{1/q} \in \mathrm{F}$ for all primes $q|k$. Let q be one such prime and write $m = k/q$. By the inductive hypothesis, $g^{q/k} = g^{1/m} \in \mathrm{F}$. We also have $g^{m/k} = g^{1/q} \in \mathrm{F}$. Since k is squarefree, q and m are coprime, so there exist integers a, b such that $qa + mb = 1$. Therefore $g^{1/k} = (g^{q/k})^a (g^{m/k})^b \in \mathrm{F}$. The same argument (essentially the case $g = 1$) shows that if $\zeta_q \in \mathrm{F}$ for all primes $q|k$ then $\zeta_k \in \mathrm{F}$. Thus, K_k is contained in any field F that contains all of the K_q. We conclude that K_k is the compositum of the K_q. □

Lemma 3.6. *A prime p splits completely in K_q for some prime q if and only if it splits in K_k for some squarefree integer $k > 1$.*

Proof. (⇒) Obvious.
(⇐) Choose any prime factor q of k. Then K_q is a subextension of K_k. Since p is totally split in K_k, it follows that p is totally split in K_q. □

We now introduce some notation for quantities that we will want to estimate, in view of Proposition 3.3. For a fixed nonsquare integer $g \neq -1$, any parameter $\eta \geq 1$ and any squarefree positive integer k, define

$$\mathrm{N}_g(x, \eta) := \#\{p \leq x \mid \text{for all } q \leq \eta,\ p \text{ does not split completely in } \mathrm{K}_q\},$$

$$\mathrm{P}_g(x, k) := \#\{p \leq x \mid p \text{ splits completely in } \mathrm{K}_k\},$$

where p and q denote prime numbers.

Note that for $p \le q$ we have $q \nmid p-1$, so p does not split completely in K_q. Therefore to find good primes $p \le x$ we need only check primes q up to $x-1$, so

$$\mathscr{P}(g)(x) = N_g(x, x-1).$$

An important formula relating the two quantities is the following.

Proposition 3.7. *We have* $N_g(x,\eta) = \sum_l \mu(l) P_g(x,l)$*, where* l *ranges over all divisors of* $\prod_{q\le\eta} q$*.*

Proof. This is just a case of the Principle of Inclusion-Exclusion. Note that the only terms which contribute to the sum are those with squarefree l. Splitting up the sum on the right according to the number of prime factors of l, we have

$$\sum_l \mu(l) P_g(x,l) = \sum_{n=0}^{\pi(\eta)} \sum_{\omega(l)=n} (-1)^n P_g(x,l).$$

Since the $n=0$ term is simply $\pi(x)$, it suffices to show that expression

$$\sum_{n=1}^{\pi(\eta)} \sum_{\omega(l)=n} (-1)^{n+1} P_g(x,l)$$

correctly counts the number of primes $p \le x$ that split completely in K_q for at least one prime $q \le \eta$. Let p be such a prime which splits in exactly m of the K_q. Then in view of Lemma 3.5, the first sum ($n=1$) counts it $\binom{m}{1}$ times, the second $\binom{m}{2}$ times, and so on, for an overall count of $\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \ldots + (-1)^{m+1}\binom{m}{m} = 1-(1-1)^m = 1$ by the Binomial Theorem. □

By applying the Principle of Inclusion-Exclusion "in the infinite case", we can heuristically obtain a density for the set $\mathscr{P}(g)$. Recall that the elements of $\mathscr{P}(g)$ are precisely the primes that do not split in any of the K_q. Denote the degree of the extension $K_k/\mathbb{Q}$ by $n(k)$. Then by Chebotarev's Density Theorem 2.16, the density of the set of primes which split in K_k is $1/n(k)$. Therefore to compute the density of the set of primes which split in none of the K_q, we subtract the densities for each prime: $1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(5)} - \ldots$, then add the densities for products of two primes: $+\frac{1}{n(6)} + \frac{1}{n(10)} + \frac{1}{n(14)} + \ldots$, and so on. (Here we are making use of Lemmas 3.5 and 3.6.) In this way we obtain the heuristic formula

$$d(\mathscr{P}(g)) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)},$$

or put another way, as $x \to \infty$ we have

$$\mathscr{P}(g)(x) \sim \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} \right) \frac{x}{\log x}$$

in light of the Prime Number Theorem 3.1. This formula turns out to be conditionally true, and the sum is indeed equal to the quantity $\delta(g)$ in the statement of Artin's conjecture, as we will prove in the next section following the work of Hooley.

4 Hooley's Conditional Proof

In this section we present Hooley's conditional proof of Artin's Primitive Root Conjecture. Throughout, g denotes a nonsquare integer not equal to -1, g_1 the squarefree part of g, and h the largest integer for which g is an h-th power. Recall that $\mathscr{P}(g)(x) = \mathrm{N}_g(x, x-1)$ - the main idea of the proof is to estimate the latter quantity using a quantitative version of Chebotarev's Density Theorem, as well as several techniques from analysis.

We will be applying Chebotarev's theorem to the extensions $\mathrm{K}_k/\mathbb{Q}$ for squarefree k, so we begin by deriving an explicit formula for the degree $n(k)$.

4.1 Computation of the degree n(k)

Proposition 4.1. *We have*

$$n(k) = \frac{k\varphi(k)}{(h,k)\varepsilon(k)},$$

where

$$\varepsilon(k) := \begin{cases} 2 & \text{if } 2g_1 | k \text{ and } g_1 \equiv 1 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Note that the degree of $\mathbb{Q}(\zeta_k)$ over $\mathbb{Q}$ is equal to $\varphi(k)$ by Proposition 2.13. By multiplicity of degrees, it is thus enough to compute $m(k) := [\mathrm{K}_k : \mathbb{Q}(\zeta_k)]$.

We claim that $m(k)$ divides $k_1 := k/(h,k)$. Indeed, we can write $g = x^h$ for some integer x, and then $\mathbb{Q}(g^{1/k})$ is generated by a^{1/k_1} for $a := x^{h/(h,k)}$. We then have a group homomorphism

$$f : \mathrm{Gal}(\mathrm{K}_k/\mathbb{Q}(\zeta_k)) \to \langle \zeta_{k_1} \rangle$$

defined by $\sigma(a^{1/k_1}) = f(\sigma)a^{1/k_1}$. It is a group homomorphism because all the σ considered are trivial on the k_1-th roots of unity, and it is injective because if for some σ we have $f(\sigma) = 1$, then σ fixes a^{1/k_1} and ζ_{k_1}, so it fixes pointwise the whole field K_k. This proves that the Galois group $\mathrm{Gal}(\mathrm{K}_k/\mathbb{Q}(\zeta_k))$ injects into the group of k_1-th roots of unity, and in particular $m(k)$ divides k_1.

Let us now write

$$k_1 = m(k)r(k).$$

As k is squarefree, k_1 is too, so for a prime factor q of $r(k)$, the degree $[\mathbb{Q}(\zeta_k, a^{1/q}) : \mathbb{Q}(\zeta_k)]$ divides $m(k)$ so is coprime to q, but is 1 or q. Therefore, for all prime factors q of $r(k)$, $a^{1/q}$ belongs to $\mathbb{Q}(\zeta_k)$, which implies (as the cyclotomic extensions are abelian, so all their subextensions are Galois) that $q = 2$: it is the only situation where an extension of the shape $\mathbb{Q}(a^{1/q})$ can be Galois, because it has to contain all q-th roots of unity.

We have thus proved that in fact, $r(k) = 1$ or 2, and as it has to divide k_1, the latter case only occurs for k even. The same discussion proves more precisely that $r(k) = 2$ if and only if $\sqrt{a}$ belongs to $\mathbb{Q}(\zeta_k)$. Writing

$$a = g_1 b^2,$$

where g_1 is the also the squarefree (possibly negative, but not equal to 1) part of a because a is an odd power of g, this is equivalent to $\sqrt{g_1}$ belonging to $\mathbb{Q}(\zeta_k)$. The Galois group of this extension is $(\mathbb{Z}/k\mathbb{Z})^*$, with exactly $2^{\omega(k)-1}-1$ subgroups of index 2 so it has exactly $2^{\omega(k)-1}-1$ quadratic subextensions by Galois correspondence. The Gauss sum formulas [Neu13, pages 51-52] then prove that those extensions are the $\mathbb{Q}(\sqrt{(-1/\mathrm{D})\,\mathrm{D}})$ where D goes through the positive odd divisors of k other than 1 (here $(-1/\mathrm{D})$ is the Jacobi symbol).

It thus happens if and only if g_1 is an odd divisor of k with $|g_1| > 1$ and the same sign as $\big(-1/|g_1|\big)$, which is equivalent to $g_1 \equiv 1 \bmod 4$. □

4.2 Evaluation of the series form of the density

Since we are dealing with multiplicative functions (functions f that satisfy $f(mn) = f(m)f(n)$ for any two coprime integers m, n) and Euler products, we will be making repeated use of the following elementary result.

Lemma 4.2. *If f is a multiplicative function such that $f(k) = 0$ for all non-squarefree k and $\sum_{k=1}^{\infty} |f(k)|$ converges, then*

$$\sum_{k=1}^{\infty} f(k) = \prod_{q} (1 + f(q)).$$

Proof. Writing $\mathrm{M}_n = \prod_{q \le n} q$, we have

$$\prod_{q \le n} (1 + f(q)) = \sum_{k=1}^{\mathrm{M}_n} f(k) - \sum_{\substack{k \le \mathrm{M}_n \\ \exists q > n, q \mid k}} f(k) \to \sum_{k=1}^{\infty} f(k)$$

as $n \to \infty$, because

$$\Big| \sum_{\substack{k \le \mathrm{M}_n \\ \exists q > n, q \mid k}} f(k) \Big| \le \sum_{k > n} |f(k)| \to 0.$$

□

We will also need a lower bound for the multiplicative function $\varphi(k)$.

Lemma 4.3. *For all $k \geq 1$, we have $\varphi(k) \geq \sqrt{k/2}$.*

Proof. For any prime p, we have $\varphi(p) = p-1 \geq \sqrt{p/2}$, and for any $\alpha \geq 2$ we have $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} \geq p^{\alpha-1} \geq \sqrt{p^\alpha/2}$. The result follows by multiplicativity. □

Proposition 4.4. *We have $\displaystyle\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \delta(g)$, where $\delta(g)$ is defined as in the statement of Artin's conjecture.*

Proof. For convenience, we restate here the definition of $\delta(g)$:

$$\delta(g) := \begin{cases} A(h) & \text{if } g_1 \not\equiv 1 \bmod 4, \\ \left(1 - \mu(|g_1|) \displaystyle\prod_{q \mid g_1, q \mid h} \frac{1}{q-2} \prod_{q \mid g_1, q \nmid h} \frac{1}{q^2-q-1}\right) A(h) & \text{if } g_1 \equiv 1 \bmod 4, \end{cases}$$

and also the definition of $\varepsilon(k)$:

$$\varepsilon(k) := \begin{cases} 2 & \text{if } 2g_1 \mid k \text{ and } g_1 \equiv 1 \bmod 4, \\ 1 & \text{otherwise.} \end{cases}$$

By Proposition 4.1, the series in question is $\displaystyle\sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\varphi(k)}$.

First, suppose that $g_1 \not\equiv 1 \bmod 4$, so that $\varepsilon(k) = 1$ for all k. Let $f(k) = \frac{\mu(k)(h,k)}{k\varphi(k)}$. It is easy to see that this function is multiplicative, and vanishes at non-squarefree k because of the factor $\mu(k)$. Furthermore, we have absolute convergence:

$$\sum_{k=1}^{\infty} |f(k)| = \sum_{k=1}^{\infty} \frac{(h,k)}{k\varphi(k)} \leq h\sqrt{2} \sum_{k=1}^{\infty} \frac{1}{k^{3/2}} < \infty$$

using Lemma 4.3. Thus by Lemma 4.2,

$$\begin{aligned} \sum_{k=1}^{\infty} \frac{\mu(k)(h,k)}{k\varphi(k)} &= \prod_q \left(1 + \frac{\mu(q)(h,q)}{q\varphi(q)}\right) \\ &= \prod_q \left(1 - \frac{(h,q)}{q(q-1)}\right) \\ &= \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right) \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \\ &= A(h) \end{aligned}$$

as required.

The case $g_1 \equiv 1 \bmod 4$ takes a bit more work. By definition of $\varepsilon(k)$, we have

$$\begin{aligned}\sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\varphi(k)} &= \sum_{2g_1 \nmid k} \frac{\mu(k)(h,k)}{k\varphi(k)} + \sum_{2g_1 \mid k} \frac{2\mu(k)(h,k)}{k\varphi(k)};\\ \sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\varphi(k)} &= A(h) + \sum_{2g_1 \mid k} \frac{\mu(k)(h,k)}{k\varphi(k)} \end{aligned} \tag{1}$$

as before. Since $\mu(k)$ vanishes for non-squarefree k, we have

$$\begin{aligned}\sum_{2g_1 \mid k} \frac{\mu(k)(h,k)}{k\varphi(k)} &= \sum_{k'=1}^{\infty} \frac{\mu(2|g_1|k')(h,2|g_1|k')}{2|g_1|k'\varphi(2|g_1|k')}\\ &= \sum_{(2g_1,k')=1}^{\infty} \frac{\mu(2|g_1|k')(h,2|g_1|k')}{2|g_1|k'\varphi(2|g_1|k')};\\ \sum_{2g_1 \mid k} \frac{\mu(k)(h,k)}{k\varphi(k)} &= \frac{\mu(2|g_1|)(h,2|g_1|)}{2|g_1|\varphi(2|g_1|)} \sum_{(2g_1,k')=1} \frac{\mu(k')(h,k')}{k'\varphi(k')}. \end{aligned} \tag{2}$$

Applying Lemma 4.2 to the latter sum, we obtain

$$\begin{aligned}\sum_{(2g_1,k')=1} \frac{\mu(k')(h,k')}{k'\varphi(k')} &= \prod_{q \nmid 2g_1} \left(1 + \frac{\mu(q)(h,q)}{q\varphi(q)}\right)\\ &= A(h) \prod_{q \mid 2g_1} \left(1 + \frac{\mu(q)(h,q)}{q\varphi(q)}\right)^{-1}\\ &= A(h) \prod_{q \mid h, q \mid 2g_1} \left(1 - \frac{1}{q-1}\right)^{-1} \prod_{q \nmid h, q \mid 2g_1} \left(1 - \frac{1}{q(q-1)}\right)^{-1}\\ &= A(h) \prod_{q \mid h, q \mid 2g_1} \frac{q-1}{q-2} \prod_{q \nmid h, q \mid 2g_1} \frac{q(q-1)}{q^2-q-1}. \end{aligned}$$

Note that $g_1 \equiv 1 \bmod 4$ implies that $2 \nmid g_1$, so $2g_1$ is squarefree. Therefore

$$\varphi(2|g_1|) = \prod_{q \mid 2g_1} \varphi(q) = \prod_{q \mid 2g_1} (q-1)$$

and from (2) we get

$$\begin{aligned}\sum_{2g_1 \mid k} \frac{\mu(k)(h,k)}{k\varphi(k)} &= A(h) \frac{\mu(2|g_1|)(h,2|g_1|)}{2|g_1|\varphi(2|g_1|)} \prod_{q \mid h, q \mid 2g_1} \frac{q-1}{q-2} \prod_{q \nmid h, q \mid 2g_1} \frac{q(q-1)}{q^2-q-1}\\ &= A(h) \frac{\mu(2|g_1|)(h,2|g_1|)}{2|g_1|} \prod_{q \mid h, q \mid 2g_1} \frac{1}{q-2} \prod_{q \nmid h, q \mid 2g_1} \frac{q}{q^2-q-1}\\ &= -A(h)\mu(|g_1|) \prod_{q \mid h, q \mid g_1} \frac{1}{q-2} \prod_{q \nmid h, q \mid g_1} \frac{1}{q^2-q-1}, \end{aligned}$$

using that

$$\frac{2|g_1|}{(h,2|g_1|)} = \prod_{q\nmid h, q|2g_1} q.$$

Plugging this back into (1) we obtain the desired result

$$\sum_{k=1}^{\infty} \frac{\mu(k)(h,k)\varepsilon(k)}{k\varphi(k)} = \left(1-\mu(|g_1|)\prod_{q|g_1,q|h}\frac{1}{q-2}\prod_{q|g_1,q\nmid h}\frac{1}{q^2-q-1}\right)\mathrm{A}(h).$$

□

4.3 Chebotarev's Density Theorem under GRH

The most important tool for the main computations is the quantitative version of Chebotarev's Density Theorem (which can be found in [Ser81, Theorem 2.4] for example), for which we need the assumption of GRH for the number fields K_k.

Let K be a Galois extension of $\mathbb{Q}$ with Galois group G and C a conjugacy class of G. For any $x \geq 1$, we write

$$\pi_{\mathrm{C}}(x) \quad := \quad \#\left\{\mathfrak{P} \text{ prime ideal of } \mathscr{O}_{\mathrm{K}} | \mathrm{Nm}(\mathfrak{P}) \leq x \text{ and } (\mathfrak{P}, \mathrm{K}/\mathbb{Q}) \in \mathrm{C}\right\}.$$

Theorem 4.5 (Explicit Chebotarev Density Theorem under GRH)**.** *Assuming the Riemann Hypothesis for the function* ζ_{K}*, for any conjugacy class* C *of* G *and any* $x \geq 2$*, we have*

$$\pi_{\mathrm{C}}(x) = \frac{\#\mathrm{C}}{\#\mathrm{G}}\mathrm{Li}(x) + \frac{\#\mathrm{C}}{\#\mathrm{G}}\mathrm{O}\left(\sqrt{x}(\log\Delta_{\mathrm{K}} + \#\mathrm{G}\log x)\right),$$

with absolute implicit constants which do not depend on the field K*, where* $\mathrm{Li}(x)$ *is the logarithmic integral defined by* $\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\,dt$*.*

Remark 4.6. This theorem is more precise with Li, but integration by parts shows that

$$\mathrm{Li}(x) = \frac{x}{\log x} + \mathrm{O}\left(\frac{x}{\log^2 x}\right)$$

The main interest for us is in the following:

Corollary 4.7. *With the same notation as before, let* $\pi_s(x)$ *be the number of prime numbers less than or equal to* x *which are totally split in* K*. Assuming the Riemann Hypothesis for* ζ_{K}*, we have*

$$\pi_s(x) = \frac{\mathrm{Li}(x)}{[\mathrm{K}:\mathbb{Q}]} + \mathrm{O}\left(\sqrt{x}\log x\right) + \mathrm{O}\left(\frac{\sqrt{x}\log\Delta_{\mathrm{K}}}{[\mathrm{K}:\mathbb{Q}]}\right),$$

again with absolute implicit constants.

Applying this to the number fields K_k and using Lemma 2.10, we obtain the estimate

$$P_g(x,k) = \frac{\mathrm{Li}(x)}{n(k)} + O(\sqrt{x}\log x) + O\left(\frac{\sqrt{x}\log \Delta_{K_k}}{n(k)}\right).$$

Computationally, we will need to have an estimate that is more explicit in its dependence on k. The following proposition gives us a much simpler error term in the above equation.

Proposition 4.8. *For any squarefree positive integer $k > 1$, we have*

$$\log(|\Delta_{K_k}|^{1/[K_k:\mathbb{Q}]}) = O(\log k)$$

with implicit constants depending on g (and both terms are 0 for $k = 1$).

Proof. As $K_k = \mathbb{Q}(\zeta_k, g^{1/k})$, the theorem of [TŠ55] implies that the (absolute value of the) discriminant of K_k divides

$$\Delta_{\mathbb{Q}(\zeta_k)}^{[K_k:\mathbb{Q}(\zeta_k)]} \Delta_{\mathbb{Q}(g^{1/k})}^{[K_k:\mathbb{Q}(g^{1/k})]},$$

hence its $[K_k:\mathbb{Q}]$-th root is less than kak_1 using that $\mathbb{Q}(g^{1/k}) = \mathbb{Q}(a^{1/k_1})$ and the computation for discriminant of cyclotomic fields [Was97, Proposition 2.7]. Its logarithm is then less than $2\log(k) + \log(g)$, which proves the result. □

Corollary 4.9. *Assuming the Riemann Hypothesis for the number fields K_k, we have the estimate*

$$P_g(x,k) = \frac{\mathrm{Li}(x)}{n(k)} + O(\sqrt{x}\log(kx)).$$

4.4 Some analytic preliminaries

Before the final computations, we would like to collect some useful analytic results. The first of these concerns products of prime numbers less than a given bound.

Lemma 4.10. *For any $x > 0$, we have $\prod_{p \le x} p \le 2^{2x}$.*

Proof. Let us define $\theta(x) = \sum_{p \le x} \log p$. For all $n \ge 1$, the binomial coefficient $\binom{2n+1}{n}$ is an integer less than 2^{2n} (e.g. by bounding its contribution in the binomial expansion of $(1+1)^{2n+1}$) and is divisible by all primes p between $n+1$ and $2n+1$, which proves that

$$\prod_{n+1 < p \le 2n+1} p < 2^{2n}.$$

Hence

$$\theta(2n+1) - \theta(n+1) < 2n\log 2,$$

after which we can obtain the logarithm of the inequality by induction (it is trivial for $n = 1$ and 2). Taking the exponential, we thus obtain the result. □

We will also be using the uniform version of the Brun-Titchmarsh estimate. It is proved using a delicate application of sieve methods; for example see [MV73, Theorem 2].

Proposition 4.11 (Brun-Titchmarsh)**.** *For any integer $x \geq 1$ and any prime $q < x$,*

$$\#\left\{p \leq x \text{ prime and } p \equiv 1 \bmod q\right\} \leq \frac{2x}{(q-1)\log(x/q)}.$$

Lastly, we will want to make use of a result known as Mertens' First Theorem:

Proposition 4.12 (Mertens)**.** $\displaystyle\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1)$

Proof. We follow [HW08, Theorem 425]). Recall that the definition of the von Mangoldt function Λ is $\Lambda(n) = \log p$ if n is a power of a prime number p, and 0 otherwise. It is then immediate that for all integers $n \geq 1$,

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

Let us define

$$\psi(x) = \sum_{n\leq x} \Lambda(n), \quad L(x) = \sum_{n\leq x} \log n.$$

By comparison between sum and integral (as log is increasing),

$$L(x) - \log x \leq \int_1^x \log t \, dt \leq L(x),$$

and that integral is equal to $x\log x - x$, so

$$L(x) = x\log x - x + O(\log x).$$

On the other hand, because of the von Mangoldt summation property

$$L(x) = \sum_{\substack{d,e\geq 1 \\ de\leq x}} \Lambda(d) = \sum_{d\geq 1} \Lambda(d)\lfloor x/d \rfloor = x \sum_{d\leq x} \frac{\Lambda(d)}{d} + O_1(\psi(x))$$

by approximating $\lfloor x/d \rfloor$ as $x/d + O_1(1)$. Now, by construction,

$$\psi(x) = \theta(x) + \theta(\sqrt{x}) + \cdots + \theta(x^{1/m})$$

with θ defined as in the previous proof, where m is the largest integer such that $2^m \leq x$, i.e. $\lfloor \log_2 x \rfloor$, so that

$$\psi(x) \leq 2x \log 2 + O(\sqrt{x} \log_2 x) = O(x).$$

The previous estimates combined thus lead to

$$\sum_{d \leq x} \frac{\Lambda(d)}{d} = \log x + O(1).$$

Finally, we have

$$\begin{aligned}
\sum_{p \leq x} \frac{\log p}{p} &= \sum_{d \leq x} \frac{\Lambda(d)}{d} - \sum_{m \geq 2} \sum_{p^m \leq x} \frac{\log p}{p^m} \\
&= \log x + O(1) + O\left(\sum_p \log p \cdot \left(\frac{1}{p^2} + \frac{1}{p^3} + \cdots \right) \right) \\
&= \log x + O(1) + O\left(\sum_p \frac{\log p}{p(p-1)} \right) \\
&= \log x + O(1).
\end{aligned}$$

□

4.5 Computation of the density

We now present the final part of the proof, that

$$\mathscr{P}(g)(x) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} \right) \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x} \right).$$

Combined with Proposition 4.4, this will establish Artin's Primitive Root Conjecture as stated in section 2.

It is worth noting that it is not possible to estimate $N_g(x, x-1)$ directly using the inclusion-exclusion formula in Proposition 3.7 because we end up with an error term of $O(\frac{x}{\log x})$ which is of course too large. But for smaller values of the parameter η it is possible, as we will see later on. The idea of the proof is therefore to introduce intermediate quantities and work with these individually before putting them together to arrive at the final result.

Recall that $\mathscr{P}(g)(x) = N_g(x, x-1)$. Consider the quantities

$$M_g(x, \eta_1, \eta_2) := \#\{p \leq x \mid p \text{ splits completely in some } K_q \text{ with } \eta_1 < q \leq \eta_2\}.$$

Observing that

$$N_g(x,\xi_1) - M_g(x,\xi_1,x-1) \le \mathscr{P}(g)(x) \le N_g(x,\xi_1),$$

we have

$$\mathscr{P}(g)(x) = N_g(x,\xi_1) + O(M_g(x,\xi_1,x-1)).$$

Furthermore,

$$M_g(x,\xi_1,x-1) \le M_g(x,\xi_1,\xi_2) + M_g(x,\xi_2,\xi_3) + M_g(x,\xi_3,x-1),$$

and we thus obtain the relation

$$\mathscr{P}(g)(x) = N_g(x,\xi_1) + O(M_g(x,\xi_1,\xi_2)) + O(M_g(x,\xi_2,\xi_3)) + O(M_g(x,\xi_3,x-1)), \tag{3}$$

with carefully chosen parameters $\xi_1 < \xi_2 < \xi_3$ (for sufficiently large x) defined by

$$\xi_1 = \frac{1}{6}\log x,\ \xi_2 = \sqrt{x}\log^{-2} x,\ \xi_3 = \sqrt{x}\log x.$$

Now we estimate separately each quantity on the right hand side of (3). Let us start with the first term $N_g(x,\xi_1)$, which will provide us with the main term in our estimation of $\mathscr{P}(g)(x)$.

By Lemma 4.10, the number of divisors l of $\prod_{q\le\xi_1} q$ may be crudely bounded by $\prod_{q\le\xi_1} q \le e^{2\xi_1} = x^{1/3}$ (indeed, this is why we chose $\xi_1 = \frac{1}{6}\log x$). It follows from Proposition 3.7 and Corollary 4.9 that

$$\begin{aligned} N_g(x,\xi_1) &= \sum_l \mu(l) P_g(x,l) \\ &= \sum_l \mu(l)\left(\frac{\mathrm{Li}(x)}{n(l)} + O(\sqrt{x}\log(lx))\right) \\ &= \left(\sum_l \frac{\mu(l)}{n(l)}\right)\mathrm{Li}(x) + O\left(\sum_{l\le x^{1/3}} \sqrt{x}\log x\right) \\ &= \left(\sum_l \frac{\mu(l)}{n(l)}\right)\mathrm{Li}(x) + O\left(\frac{x}{\log^2 x}\right). \end{aligned}$$

We can introduce the full sum by writing

$$\begin{aligned}\sum_l \frac{\mu(l)}{n(l)} &= \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} - \sum_{\exists q \mid k, q>\xi_1} \frac{\mu(k)}{n(k)} \\ &= \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} + O\left(\sum_{q>\xi_1} \left(\frac{1}{n(q)} \sum_j \frac{1}{n(j)}\right)\right) \\ &= \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} + O\left(\sum_{q>\xi_1} \frac{1}{q(q-1)}\right) \\ &= \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} + O\left(\frac{1}{\xi_1}\right),\end{aligned}$$

where j runs over all divisors of $\prod_{p<q} p$.

Using the relation $\mathrm{Li}(x) = \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right)$ from Remark 4.6, we conclude that

$$\begin{aligned}N_g(x,\xi_1) &= \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}\right) \mathrm{Li}(x) + O\left(\frac{\mathrm{Li}(x)}{\xi_1}\right) + O\left(\frac{x}{\log^2 x}\right) \\ &= \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}\right) \frac{x}{\log x} + O\left(\frac{x}{\xi_1 \log x}\right) + O\left(\frac{x}{\log^2 x}\right) \\ &= \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}\right) \frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right).\end{aligned}$$

We now turn our attention to the second quantity $M_g(x,\xi_1,\xi_2)$. Again we apply Corollary 4.9:

$$\begin{aligned}M_g(x,\xi_1,\xi_2) &\leq \sum_{\xi_1<q\leq\xi_2} P_g(x,q) \\ &= \sum_{\xi_1<q\leq\xi_2} \left(\frac{\mathrm{Li}(x)}{n(q)} + O(\sqrt{x}\log(qx))\right) \\ &= O\left(\frac{x}{\log x} \sum_{q>\xi_1} \frac{1}{q(q-1)}\right) + O\left(\sqrt{x}\log x \sum_{q\leq\xi_2} 1\right) \\ &= O\left(\frac{x}{\xi_1 \log x}\right) + O\left(\frac{\xi_2\sqrt{x}\log x}{\log \xi_2}\right) \\ &= O\left(\frac{x}{\log^2 x}\right),\end{aligned}$$

since $\log x = O(\log \xi_2)$.

The last two terms that we need to estimate, namely $\mathrm{M}_g(x,\xi_2,\xi_3)$ and $\mathrm{M}_g(x,\xi_3,x-1)$, do not even require the assumption of GRH.

For the first of these, we start off the same way as in the above computation, but this time we simply bound $\mathrm{P}_g(x,q)$ by the number of primes $p \le x$ for which $p \equiv 1 \bmod q$, which in turn is at most $\dfrac{2x}{(q-1)\log(x/q)}$ by the Brun-Titchmarsh estimate 4.11. Thus we have

$$\begin{aligned}
\mathrm{M}_g(x,\xi_2,\xi_3) &\le \sum_{\xi_2<q\le\xi_3} \frac{2x}{(q-1)\log(x/q)} \\
&= \mathrm{O}\left(\frac{x}{\log x}\sum_{\xi_2<q\le\xi_3}\frac{1}{q}\right) \\
&= \mathrm{O}\left(\frac{x}{\log^2 x}\sum_{\xi_2<q\le\xi_3}\frac{\log q}{q}\right) \\
&= \mathrm{O}\left(\frac{x}{\log^2 x}\left(\log\frac{\xi_3}{\xi_2}+\mathrm{O}(1)\right)\right) \\
&= \mathrm{O}\left(\frac{x\log\log x}{\log^2 x}\right),
\end{aligned}$$

using Mertens' estimate 4.12.

Recall that $\mathrm{M}_g(x,\xi_3,x-1)$ counts the number of primes $p \le x$ for which there exists $\xi_3 < q \le x-1$ such that $q \mid p-1$ and $g^{\frac{p-1}{q}} \equiv 1 \bmod p$. In particular these primes satisfy $g^{\frac{2(p-1)}{q}} \equiv 1 \bmod p$, where $\frac{p-1}{q} < \frac{x}{\log x}$, so they divide the product

$$\prod_{m<\frac{x}{\log x}} (a^{2m}-1).$$

Of course these primes are greater than or equal to 2, so it follows that

$$2^{\mathrm{M}_g(x,\xi_3,x-1)} < \prod_{m<\frac{x}{\log x}} (a^{2m}-1) < \prod_{m<\frac{x}{\log x}} a^{2m}.$$

Taking logs we obtain

$$\mathrm{M}_g(x,\xi_3,x-1) < 2\frac{\log|a|}{\log 2}\sum_{m<\frac{x}{\log x}} m = \mathrm{O}\left(\frac{x}{\log^2 x}\right),$$

since

$$\sum_{m<\mathrm{N}} m = \frac{1}{2}\mathrm{N}(\mathrm{N}-1) = \mathrm{O}(\mathrm{N}^2).$$

Putting these four estimates together gives the required formula for $\mathscr{P}(g)(x)$, thus completing the proof.

5 The $qx+1$ problem

We conclude with a discussion of another problem in number theory which makes use of similar methods to those outlined in the previous sections (closely following [FP95]).

Perhaps one of the most well-known unsolved elementary problems in mathematics is the Collatz Conjecture, also known as the $3x+1$ problem. If $C_3(m)$ denotes the largest odd factor of $3m+1$, the conjecture states that iterating C_3 will eventually result in an output of 1, no matter which positive integer m we start with. Much work has been done on this problem, especially computationally, and no counterexamples have been found thus far.

On the other hand, in the more general $qx+1$ problem for odd integers $q>3$ (with corresponding function C_q), we can sometimes find m for which the sequence of iterates $C_q^j(m)$ never reaches 1. In this case we call q a *Crandall number*. The name refers to Richard Crandall, who in 1978 conjectured that all odd integers $q>3$ are Crandall numbers, and gave the three examples 5, 13 and 1093. The first two are shown directly: taking $q=5$ and $m=13$ results in the cycle $13,33,83,13$, and taking $q=181$ and $m=27$ gives the cycle $27,611,27$. As we shall see shortly, the last follows from the fact that 1093 is a *Wieferich prime number*; that is, an odd prime q such that q^2 divides $2^{q-1}-1$. More generally, a Wieferich number is an odd q such that q and $(2^{\varphi(q)}-1)/q$ are not coprime. Note that by Lagrange's Theorem, it is always true that $q \mid 2^{\varphi(q)}-1$.

We will be making use of two different types of density in what follows, one of which is natural density but in the context of sets of integers, and the other is analytic density (also called Dirichlet density).

Definition 5.1. Let S, T be sets of positive integers with $S \subseteq T$. The *natural density* of S in T is defined to be

$$\lim_{x\to\infty} \frac{\#\{n \in S \mid n \le x\}}{\#\{n \in T \mid n \le x\}},$$

provided the limit exists.

Definition 5.2. Let S be a set of prime numbers. The *analytic density* of S is defined to be

$$\lim_{s\to 1^+} \frac{\sum_{p\in S} \frac{1}{p^s}}{\sum_{p} \frac{1}{p^s}},$$

provided the limit exists.

Lemma 5.3. *Every Wieferich number is a Crandall number.*

Proof. We prove the stronger result that every Wieferich number q is a 'strong' Crandall number in the sense that the set of positive integers m for which $C_q^j(m) = 1$ for some j has natural density 0 (in the positive integers). If $C_q(m) = 1$ for some m, then $qm+1$ is a power of 2, so we have $m = \frac{2^{k\varphi(q)}-1}{q}$ for some positive integer k. Hence, if $C_q^2(m) = 1$ for some m, then $C_q(m) = \frac{2^{k\varphi(q)}-1}{q}$, thus

$$qm+1 = 2^n\left(\frac{2^{k\varphi(q)}-1}{q}\right)$$

for some positive integers n and k. Noting that $2^{\varphi(q)-1}$ divides $2^{k\varphi(q)}-1$, we see that if q is a Wieferich number, then it is coprime to the left hand side of the equation but not the right hand side. It follows that we cannot have $C_q^2(m) = 1$ for any m, so if q is a Crandall number with $C_q^j(m) = 1$, we must have $C_q(m) = 1$ and thus $m = \frac{2^{k\varphi(q)}-1}{q}$ for some positive integer k. It is clear that the set of such m has natural density 0, since the powers of 2 have density 0. □

The above proposition is significant because 'almost all' odd numbers are Wieferich numbers and thus Crandall numbers.

Proposition 5.4. *The set of Wieferich numbers has natural density* 1 *in the odd numbers.*

Proof. For $B > 0$ we define

$$\mathscr{W}(B) := \{q \text{ odd} \mid \text{there is some prime } p_0 \le B \text{ with } p_0 | q, p_0^2 \nmid q\}.$$

Let d_B denote the natural density of the set $\mathscr{W}(B)$ in the odd numbers. The natural density in the odd numbers of the odd q which are divisible by p but not by p^2 is clearly $\frac{1}{p} - \frac{1}{p^2} = \frac{p-1}{p^2}$. Thus we have

$$d_B = 1 - \prod_{2<p\le B}\left(1 - \frac{p-1}{p^2}\right).$$

Note that the sum of the logarithms of $1-\frac{p-1}{p^2}$ diverges because the sum of the reciprocals of the primes diverges, so $d_B \to 1$ as $B \to \infty$.

Now for prime numbers p_0, write $\mathscr{P}(p_0)$ for the set of primes $p \equiv 1 \bmod p_0$ such that 2 is not a p_0-th power in $(\mathbb{Z}/p\mathbb{Z})^*$.

Recall that the condition that 2 is a p_0-th power modulo p is equivalent to the congruence $2^{\frac{p-1}{p_0}} \equiv 1 \bmod p$ (as a multiplicative consequence of Lemma 3.4).

By Proposition 3.3 this means that the primes $p \equiv 1 \bmod p_0$ such that 2 *is* a p_0-th power in $(\mathbb{Z}/p\mathbb{Z})^*$ are precisely the primes which split in K_{p_0}. Thus by Chebotarev's Density Theorem 2.3 and Proposition 4.1, they have natural density $1/n(p_0)$ with $n(p_0) = p_0(p_0-1)$ in the prime numbers. Furthermore, by Corollary 2.17, we know that the set of primes $p \equiv 1 \bmod p_0$ has natural density $\frac{1}{p_0-1}$ in the primes. Therefore the natural density of $\mathscr{P}(p_0)$ in the prime numbers is

$$\frac{1}{p_0-1} - \frac{1}{p_0(p_0-1)} = \frac{1}{p_0}.$$

This implies that the analytic density is also $\frac{1}{p_0}$ [Ten15, Theorems 2 and 3 of Chapter III]. As the sum of the reciprocals of the primes diverges, the sum of the reciprocals of the primes in $\mathscr{P}(p_0)$ must diverge as well (otherwise the analytic density would be zero). This has the consequence that the set of positive integers not divisible by any element of $\mathscr{P}(p_0)$ has natural density zero, because this density is at most $\prod_{p\in\mathscr{P}(p_0),\ p\le T}(1-\frac{1}{p})$ for any T, and this product tends to 0 as $T \to \infty$.

We deduce that the set

$$\mathscr{W}^*(B) := \{q \in \mathscr{W}(B) \mid \text{there are primes } p_0 \le B, p \in \mathscr{P}(p_0) \text{ with } p_0 | q, p_0^2 \nmid q, p | q\}$$

also has natural density d_B in the odd numbers. □

The last observation to make is that $\mathscr{W}^*(B)$ is a subset of the Wieferich numbers. Let $q \in \mathscr{W}^*(B)$ and choose p_0, p as in the definition. Clearly $\varphi(p_0), \varphi(p) | \varphi(q)$. Moreover, since $p \in \mathscr{P}(p_0)$, we have $p_0 | \varphi(p)$. Thus, both p_0 and $\varphi(p_0) = (p_0-1)$ divide $\varphi(q)$ so their product does as they are coprime. Note also that

$$2^{p_0\varphi(p_0)} - 1 = (2^{\varphi(p_0)} - 1)(2^{(p_0-1)\varphi(p_0)} + 2^{(p_0-2)\varphi(p_0)} + \ldots + 2^{\varphi(p_0)} + 1)$$

is divisible by p_0^2 because each term in the second factor is congruent to 1 modulo p_0 and there are p_0 of them. It follows that $p_0^2 | 2^{\varphi(q)} - 1$, hence that q is a Wieferich number, because $p_0^2 \nmid q$.

Thus the natural density of the Wieferich numbers in the odd numbers is at least d_B for every $B > 0$, and is therefore equal to 1 since $d_B \to 1$.

References

[FP95] Zachary Franco and Carl Pomerance, *On a conjecture of Crandall concerning the $qx+1$ problem.*, Math. Comput. **64** (1995), no. 211, 1333–1336.

[Hei67] H. Heilbronn, *Zeta-functions and* L*-functions*, Thompson, Washington, D.C., 1967, pp. 204–230.

[Hoo67] Christopher Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[HW08] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.

[Mar18] Daniel A. Marcus, *Number fields*, Universitext, Springer, Cham, 2018.

[Mor12] Pieter Moree, *Artin's primitive root conjecture—a survey*, Integers **12** (2012), no. 6, 1305–1416.

[MV73] H. L. Montgomery and R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

[Neu13] Jurgen Neukirch, *Algebraic number theory*, Springer Berlin Heidelberg, 2013.

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. (1981), no. 54, 323–401.

[T$\hat{5}$5] Hiraku Tôyama, *A note on the different of the composed field*, Kodai Math. Sem. Rep. **7** (1955), 43–44.

[Ten15] Gérald Tenenbaum, *Introduction to analytic and probabilistic number theory.* , vol. 163, Providence, RI: American Mathematical Society (AMS), 2015 (English).

[Was97] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

Shalome Kurian
University of Warwick
shalomekurian98@gmail.com