2015

On the Characterization of Prime Sets of Polynomials by Congruence Conditions

Arvind Suresh
Claremont McKenna College

CLAREMONT MCKENNA COLLEGE

On the Characterization of Prime Sets of Polynomials by Congruence Conditions

SUBMITTED TO

Professor David Krumm

AND

DEAN NICHOLAS WARNER

BY

Arvind Suresh

for

SENIOR THESIS

Fall 2014

December 1st

Contents

Abstract

This project is concerned with the set of primes modulo which some monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$ has a root, called the Prime Set of f. We completely characterise these sets for degree 2 polynomials, and develop sufficient machinery from algebraic number theory to show that if the Galois group of a monic, irreducible polynomial in $\mathbb{Z}[x]$ is abelian, then its Prime Set can be written as the union of primes in some congruence classes modulo some integer.

1 Preliminaries

1.1 Introduction

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. For a prime p, the *reduction of f modulo p*, denoted $\bar{f}(x)$, is the polynomial over the finite field $\mathbb{Z}/p\mathbb{Z}$ (or $\mathbb{F}_p$) that is obtained by reducing each coefficient of f modulo p. We say that $f(x)$ has a root modulo p if $\bar{f}(x) \in \mathbb{F}_p[x]$ has a root in $\mathbb{F}_p$, or equivalently, there is some $n \in \mathbb{Z}$ such that $p \mid f(n)$. For the rest of the document, $\mathbb{P}$ denotes the set of all prime numbers in $\mathbb{Z}$.

Definition 1.1.1. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. We define the Prime Set of f to be*

$$P(f) = \{p \in \mathbb{P} \mid \ f \text{ has a root mod } p\}.$$

This project is an introductory investigation of the set $P(f)$ for monic, irreducible polynomials $f(x) \in \mathbb{Z}[x]$. The question that drives the project is the following: "When can $P(f)$ be characterised by congruence conditions. In other words, for which monic, irreducible $f(x) \in \mathbb{Z}[x]$ can we find an integer m such that $p \in P(f)$ if and only p lies in the union of some (but not all) congruence classes modulo m?

Recall that the Galois group $\mathrm{Gal}(f)$ of a polynomial $f(x) \in \mathbb{Z}[x]$ is the Galois group of its splitting field extension over $\mathbb{Q}$. The main Theorem of the paper is the following.

Theorem A. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with abelian Galois group,. Then there exists an integer m and*

$$\frac{[K_m : \mathbb{Q}]}{\deg f} = \frac{\phi(m)}{\deg f}$$

many integers a_i that are relatively prime to m and pairwise incongruent modulo m, such that, for any rational prime p that does not divide m, f has a root modulo p if and only if $p \equiv a_i \pmod{m}$ for some $0 \leqslant i \leqslant \phi(m)/\deg f$

Theorem A is proved in the third section. The proof requires some facts from algebraic number theory, and a summary of these is given in the second section.

For the case when $\deg f = 2$, which is a special case of Theorem A, we are able to exhibit $P(f)$ as a union of primes in congruence classes, and in fact, the proof is constructive and draws only from classical number theory. Following this introduction, we quickly deal with the cases of $\deg f = 0, 1$, then review the requisite theorems from number theory and conclude the first section with the following.

Theorem B. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree 2, and let d be the square-free part of the discriminant of f. Set $m = d$, if d is odd and positive, and $m = 4|d|$ otherwise. Then, there exist $\phi(m)/2$ pairwise co-prime integers a_i that are relatively prime to m, such that for all $p \in \mathbb{P}$,*

$$p \in P(f) \text{ if and only if } p \equiv a_i \pmod{m}$$

for some $1 \leqslant i \leqslant \frac{\phi(m)}{2}$.

Along the way, we will encounter Density theorems of varying strengths, and we will also get to see some nice facts about the "size" of $P(f)$. The project concludes with a very brief discussion of possible other lines of inquiry into prime sets of polynomials.

1.2 $P(f)$ when $\deg f = 0, 1,$ or 2

If we restrict our attention to monic polynomials, the characterisation of $P(f)$ is almost trivial when f is degree 0 or 1. If $\deg f = 0$, then $f(x) = 1$ is constant and clearly irreducible modulo every prime, and if $f(x) = x - a$ is of degree 1, then $\bar{a}$ is a root of f modulo every prime p. We summarise this in the following Theorem.

Theorem 1.2.1. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. Then*

$$P(f) = \begin{cases} \emptyset & \text{if } \deg f = 0 \\ \mathbb{P} & \text{if } \deg f = 1. \end{cases}$$

For the case of degree 2, let $f(x) = x^2 + bx + c$, for some $b, c \in \mathbb{Z}$. In investigating the primes $p \in P(f)$, it is convenient to deal separately with the case when $p = 2$, since the fact that

$$n^2 \equiv n \pmod 2, \quad \text{for all } n \in \mathbb{Z},$$

implies $\bar{f}(\alpha) = (1 + \bar{b})\alpha + \bar{c}$ for any $\alpha \in \mathbb{F}_2$. Then it is easy to see that $2 \in P(f)$ if and only if bc is even.

The case for odd primes is determined by the following proposition.

Proposition 1.2.1. *Let K be a field with characteristic not equal to 2. If $f(x) \in K[x]$ is a monic, quadratic polynomial, then f has a root in K if and only if the* discriminant

$$\Delta_f = b^2 - 4c$$

of f is a square in K.

Proof. We have $f(x) = x^2 + bx + c$, with $b, c \in K$. If $\alpha \in K$ is a root of f, then we have

$$f(\alpha) = \alpha^2 + b\alpha + c = 0.$$

Multiplying on both sides by 4, and then adding b^2, we get

$$\begin{aligned} &(2\alpha)^2 + 2 \cdot 2\alpha \cdot b + b^2 + 4c = b^2 \\ \implies &(2\alpha + b)^2 = b^2 - 4c = \Delta_f, \end{aligned}$$

that is, Δ_f is a square in K.
Conversely, if $\Delta_f = \beta^2$ is a square in K, then

$$\alpha = \frac{-b \pm \beta}{2}$$

are the roots of f in K. □

Corollary 1.2.1. *$f(x) \in \mathbb{Z}[x]$ has a root modulo a prime p if and only if $\bar{\Delta}_f$ is a square in $\mathbb{F}_p$.*

With the above Corollary, it becomes clear that $P(f)$ would be characterised by congruence conditions if we could characterise the squares in $\mathbb{F}_p$ by congruence conditions. Thankfully, the theory of quadratic reciprocity allows us to do exactly this. We now introduce some definitions and facts from number theory that we use to conclude the section with a combinatorial proof of Theorem B. A good reference for these facts is Rosen [1].

Definition 1.2.1. *Let $p \in \mathbb{Z}$ be prime, and $a \in \mathbb{Z}$ such that $p \nmid a$. We say that a is a* Quadratic Residue modulo p *(short: QR modulo p) if there is some $y \in \mathbb{Z}$ such that $a \equiv y^2 \pmod{p}$, or equivalently, $\bar{a}$ is a square in $\mathbb{F}_p$.*

Definition 1.2.2. *Let $a, p \in \mathbb{Z}$, and $p \in \mathbb{P}$. Then, we define the* Legendre Symbol of a on p *as follows*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a QR modulo } p \\ -1 & \text{if } a \text{ is not a QR modulo } p \\ 0 & \text{if } p \mid a. \end{cases}$$

A moment of thought should convince the reader that the Legendre Symbol possesses the following convenient properties:

- $a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Thanks to these properties, we can compute the Legendre Symbol for any a and p by using the following.

Theorem 1.2.2 (Law of Quadratic Reciprocity)**.** *Let $p, q \in \mathbb{Z}$ be odd primes. Then*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 8 \\ -1 & \text{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \pmod 4 \text{ and } q \equiv 3 \pmod 4 \end{cases}$$

The last fact we need is the following:

Theorem 1.2.3 (Chinese Remainder Theorem)**.** *If $m_1, \ldots, m_n$ are pairwise relatively prime positive integers, then*

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \;\cong\; \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_n\mathbb{Z}$$

In other words, every set of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

where each a_i is relatively prime to m_i and the m_i's are pairwise co-prime, has a unique solution modulo $m_1 \cdots m_n$.

We now make some pertinent observations that will help the proof of Theorem B flow smoothly. Observe that If we let Δ_f denote the discriminant of f, then Proposition 3 assures us that f has a root modulo p if and only if Δ_f is QR modulo p, that is,

$$\left(\frac{\Delta_f}{p}\right) = 1.$$

Due to the strong multiplicativity of the Legendre symbol, we have

$$\left(\frac{\Delta_f}{p}\right) = \left(\frac{d}{p}\right),$$

where d is the square-free part of Δ_f. If we write $d = (-1)^{e_1} 2^{e_2} p_1 \cdots p_n$, where $e_i \in \{0, 1\}$ and the p_i are distinct odd primes, then we have

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)^{e_1} \left(\frac{2}{p}\right)^{e_2} \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_n}{p}\right).$$

We may invert the symbols using Theorem 4, to get

$$\left(\frac{d}{p}\right) = \pm \left(\frac{-1}{p}\right)^{e_1} \left(\frac{2}{p}\right)^{e_2} \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right).$$

Thanks to the Law of Quadratic Reciprocity, it is evident that the sign of $\left(\frac{d}{p}\right)$ is determined by congruence class conditions modulo each p_i, and modulo 4 or 8 (depending on the parity and sign of d). Note also that due to the Chinese Remainder Theorem, if a given prime p lies in some congruence class $\bar{a}_i$ modulo p_i for $1 \leqslant i \leqslant n$, then there is a unique congruence class $\bar{a}$ modulo

$p_i \cdots p_n$ such that $p \in \bar{a}$.

With this setup, we are ready to give a combinatorial proof of the claim. We only prove it for the cases when d is odd and positive and when it is even and negative. The proofs for the other cases are identical.

Theorem B. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial of degree 2, and let d be the square-free part of the discriminant of f. Set $m = d$, if d is odd and positive, and $m = 4|d|$ otherwise. Then, there exist $\phi(m)/2$ pairwise co-prime integers a_i that are relatively prime to m, such that for all $p \in \mathbb{P}$,*

$$p \in P(f) \text{ if and only if } p \equiv a_i \pmod{m}$$

for some $1 \leqslant i \leqslant \frac{\phi(m)}{2}$.

Proof. Since f is irreducible over $\mathbb{Q}$, d is non-trivial.
Suppose that d is odd and positive. Then we can write $d = p_1 \cdots p_n$ as a product of distinct, odd primes. As we saw in the discussion, we then have that

$$\left(\frac{d}{p}\right) = \pm\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right).$$

First, we count the number of ways we can assign values of $+1$ or -1 to each individual Legendre Symbol $\left(\frac{p}{p_i}\right)$ such that the resulting product $\pm\left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right)$ is positive. Observe that we can freely assign the signs of $n-1$ of the symbols, at which point the final symbol can equal only one of $+1$ or -1 in order to make the resulting product $+1$. That is, there are 2^{n-1} distinct assignments that make $\left(\frac{d}{p}\right) = 1$.

Now, suppose we have chosen a particular assignment, and let $\left(\frac{p}{p_i}\right) = l_i$. Recall that for a prime q, half of the numbers $1, 2, \ldots, q-1$ are quadratic residues modulo q, and the other half are non-residues modulo q. So, for each p_i, there are

$$\frac{p_i - 1}{2} = \frac{\phi(p_i)}{2}$$

many congruence classes modulo p_i such that $\left(\frac{p}{p_i}\right) = l_i$ if and only if p is in one of these classes. It follows due to the Chinese Remainder Theorem that there are

$$\prod_{i=1}^{n} \frac{\phi(p_i)}{2} = \frac{\phi(d)}{2^n}$$

many congruence classes modulo d such that the assignment is satisfied if and only if p is in one of these classes modulo d. Multiplying the above by the number of assignments, we conclude that there are

$$\frac{\phi(d)}{2^n} \cdot 2^{n-1} = \frac{\phi(d)}{2}$$

congruence classes modulo d such that $\left(\frac{d}{p}\right) = 1$ (i.e: $p \in P(f)$) if and only p is in one of these classes mod d.

Suppose that d is even and negative. Then we can write $d = -2p_1 \cdots p_n$, where the p_i's are distinct, odd primes. As above, we see that

$$\left(\frac{d}{p}\right) = \pm\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{p}{p_1}\right)\cdots\left(\frac{p}{p_n}\right).$$

We can freely assign values to the n symbols $\left(\frac{p}{p_i}\right)$, at which point there is only one value we can assign to $\left(\left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\right)$ that makes the resultant product $\pm\left(\frac{d}{p}\right)$ equal $+1$. So there are 2^n assignments.

Now, suppose we have fixed an assignment. As above, there are $\phi(p_1)/2$ congruence classes modulo p_i and 2 congruence classes modulo 8 that satisfy the assignment, so we conclude that there are

$$2\prod_{i=1}^{n} \frac{\phi(p_i)}{2} = \frac{\phi(d)}{2^{n-1}}$$

many congruence classes modulo $8p_1 \cdots p_n = 4|d|$ such that the assignment is satisfied if and only if p is in one of these classes. Multiplying by the number of assignments, we conclude that there are $2\phi(d)$ congruence classes modulo $4|d|$ such that $p \in P(f)$ is and only if p is in one of these classes mod $4|d|$. Note that

$$\phi(4|d|) = \phi(8p_1 \cdots p_n) = 4\phi(p_1 \cdots p_n) = 4\phi(d),$$

so we are done. □

1.3 Preliminary Investigations for higher degrees

We begin by asking some basic questions about the size of $P(f)$- can it be empty or finite? In the general case (for *all non-constant* polynomials in $\mathbb{Z}[x]$) we have the following (the argument is due to Sury [2]).

Proposition 1.3.1. *For every non-constant polynomial $f(x) \in \mathbb{Z}[x]$, $P(f)$ is infinite.*

Proof. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x]$, with $n > 0$ and $a_n \neq 0$. Let $d \in \mathbb{Z}$, and consider the polynomial

$$f(a_0 dx) = a_0 + a_0 a_1 dx + \cdots + a_0 a_n d^n x^n.$$

Setting

$$g(x) = 1 + a_1 dx + \cdots + a_n d^n x^n,$$

we have that $f(a_0 dx) = a_0 g(x)$. Since $g(x) = 0, \pm 1$ for at most finitely many values of x, there exists some $m \in \mathbb{Z}$ such that $|g(m)| > 1$. Then there is some prime p that divides $g(m)$, that is, $g(m)$ has a root modulo p, from which follows that $p \in P(g) = P(f)$. Because $g(m) \equiv 1 \pmod{d}$, we also have $p \equiv 1 \pmod{d}$.

In summary, for any d, there exists some $p \in \mathbb{P}$ co-prime to d such that $p \in P(f)$. We conclude the argument with an algorithm to enumerate an infinite list of primes in $P(f)$:

Start by picking any non-zero integer d_0 and find the prime $p_0 \in P(f)$ as described above. Then, for each $i \in \mathbb{N}$, set $d_i = d_{i-1} p_{i-1}$, and let each $p_i \in P(f)$ be the prime whose existence is guaranteed by the above argument. Then observe that the p_i's have to be distinct, from which we conclude that there are infinitely many of them. □

A natural follow-up question is whether $P(f) = \mathbb{P}$ for some $f(x)$, or weaker than that, whether $P(f)$ is cofinite in $\mathbb{P}$. In order to further investigate $P(f)$, we introduce the notion of *density*.

Definition 1.3.1. *Let $A \subseteq B$ be subsets of $\mathbb{N}$. The* natural *or* asymptotic density of A in B *is*

$$d(A) = \lim_{n \to \infty} \frac{\#\{x \in A \mid x \leqslant n\}}{\#\{x \in B \mid x \leqslant n\}},$$

if the limit exists. In the case when A is a set of primes and $B = \mathbb{P}$, we simply call the above expression the natural density of A. The Dirichlet density of A in B *is*

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{n \in A} n^{-s}}{\sum_{n \in B} n^{-s}},$$

if it exists. In the case when A is a set of primes and $B = \mathbb{P}$, we simply call the above expression the Dirichlet density of A.

The reader may consult Rosen [1, Ch. 16] or Janusz [3, IV.4] for a discussion of Dirichlet density.

Density provides us with a measure of the fraction of primes in $\mathbb{P}$ that is contained in $P(f)$. Dirichlet Density is a slightly weaker notion than Natural Density - Whenvever the latter exists, so does the former, and they are equal. Dirichlet density has the following (noticeably measure-theoretic) properties:

- $\delta(\mathbb{P}) = 1$.
- If $A \subset B$ and $\delta(A)$ and $\delta(B)$ exist, then $\delta(A) \leq \delta(B)$.
- If A, B are disjoint and $\delta(A), \delta(B)$ exist, then $\delta(A \cup B) = \delta(A) + \delta(B)$.
- If A is finite, then $\delta(A) = 0$.
- If $\delta(A)$ exists and B differs from A by only finitely many elements, then $\delta(A) = \delta(B)$.

We quickly provide a simple corollary to Theorem B.

Corollary 1.3.1. *Let $f(x) \in \mathbb{Z}[x]$ be monic, and irreducible. If $\deg f = 2$, then $\delta(P(f)) = 1/2$.*

Proof. By Theorem B, there exist $\phi(m)/2$ congruence classes modulo some m, such that $p \in P(f)$ if and only if p is in one of those congruence classes. By Dirichlet's Theorem, the density of primes in each of these congruence classes is $1/\phi(m)$. Since the classes are disjoint, it follows immediately that

$$\delta(P(f)) = \frac{1}{\phi(m)} \cdot \frac{\phi(m)}{2} = \frac{1}{2}.$$

□

Thus, when $f(x)$ is linear and monic, then $\delta(P(f)) = 1$. In general, $P(f)$ is cofinite only if $\delta(P(f)) = 1$, so we want to know if there are any polynomials f with $\deg f > 1$ such that $\delta(P(f)) = 1$. The answer to this is *no*, and it follows as a consequence of the *Frobenius Density Theorem*. Before we state the theorem and prove the claim, we review some basic facts from Galois Theory.

Every polynomial $f(x) \in \mathbb{Z}[x]$ has a unique (up to isomorphism) *splitting field* $K \supset \mathbb{Q}$, which has the property that $f(x)$, when regarded as a polynomial in $K[x]$, splits into linear factors (we say f splits over K), and if $E \subset K$ is an intermediate field, then $f(x)$ does not split over E. The *Galois group* of $f(x)$ is the group of field automorphisms of K. We denote it by $\mathrm{Gal}(K/\mathbb{Q})$ or $\mathrm{Gal}(f)$. It is a fact that $|\mathrm{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}]$.

When we have $f(x) \equiv g_1(x) \cdots g_r(x) \pmod{p}$, where the g_i's are irreducible over $\mathbb{F}_p$, and $d_i := \deg g_i$, then the sequence $d_1, \ldots, d_r$ is called the *decomposition type* of f modulo p. Note that this is a partition of $n := \deg f$. On the other hand, we can realize $\mathrm{Gal}(f)$ as a subgroup of S_n acting on the roots $\alpha_1, \ldots, \alpha_n$ of $f(x)$, in which case the cycle types of elements in $\mathrm{Gal}(f)$ also give partitions of n. The following theorem links these two partitions. See Janusz [3, IV,5] for a proof.

Theorem 1.3.1 (Frobenius Density Theorem)**.** *The density of the set of primes p modulo which a monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$ has a given decomposition type $d_1, \ldots, d_r$ exists, and is equal to $|H|/|\mathrm{Gal}(f)|$, where*

$$H = \{\sigma \in \mathrm{Gal}(f) \mid \sigma \text{ has cycle pattern } d_1, \cdots, d_r\}.$$

Notice that Corollary 1.3.1 is implied by Frobenius' Density Theorem, since $\mathrm{Gal}(f) \cong \mathbb{Z}/2\mathbb{Z}$, in which the non-identity element swaps the roots of f. The following argument is due to Sury [2].

Proposition 1.3.2. *If $f(x) \in \mathbb{Z}[x]$ is a monic, irreducible polynomial such that $\delta(P(f)) = 1$, then $f(x)$ is linear.*

Proof. Let $K \supseteq \mathbb{Q}$ be the splitting field of $f(x)$. Note that $f(x)$ has a root modulo p if and only if a 1 occurs in its decomposition type modulo p. It follows by due to Frobenius that if f is irreducible and has a roots modulo all but finitely many primes, then each $\sigma \in \mathrm{Gal}(f)$ has a cycle pattern that contains a 1, that is, each $\sigma \in \mathrm{Gal}(f)$ fixes a root. The action of $\mathrm{Gal}(f)$ on the roots of f is transitive, so if we fix an i and j, then there is some $\sigma \in \mathrm{Gal}(f)$ such that $\sigma(\alpha_i) = \alpha_j$. Observe that if $\tau \in \mathrm{Gal}(f)$ fixes α_i, then we have

$$\sigma\tau\sigma^{-1}(\alpha_j) = \sigma\tau(\alpha_i) = \sigma(\alpha_i) = \alpha_j.$$

Since every element of $\mathrm{Gal}(f)$ fixes a root of f, it follows that if $H \leqslant \mathrm{Gal}(f)$ is the subgroup that fixes some α_i, then

$$\mathrm{Gal}(f) = \bigcup_{\sigma \in \mathrm{Gal}(f)} \sigma H \sigma^{-1}.$$

But it is an elementary result from group theory that a finite group cannot be the union of conjugates of a proper subgroup, so we must have $H = \mathrm{Gal}(f)$. Since our choice of i was arbitrary, it follows that $\mathrm{Gal}(f) = H$ fixes every root of f, which implies that it is trivial. We therefore conclude that

$$\deg f = [K : \mathbb{Q}] = |\mathrm{Gal}(f)| = 1.$$

□

To summarise, we have established that $P(f)$ is always infinite if $\deg f > 0$, and $\delta(P(f)) < 1$ if $\deg f > 1$. Observe also that for any polynomial f, the identity of $\mathrm{Gal}(f)$ fixes every root of f, so Frobenius's Density Theorem implies there is also a lower bound on $\delta(P(f))$. We state this as a Corollary.

Corollary 1.3.2. *For any monic, irreducible polynomial $f(x) \in \mathbb{Z}[x]$,*

$$\delta(P(f)) \geqslant \frac{1}{|\mathrm{Gal}(f)|}.$$

A lot more can be said about $\delta(P(f))$, but we have restricted ourselves to the bare minimum needed to ensure that our search for congruence classes of primes is not in vain.

2 Review of Algebraic Number Theory

In this section, we provide a short summary (mostly without proofs) of the basic tools from algebraic number theory that we intend to use. There are a number of standard reference texts for this material. The reader may wish to consult Lang [4] or Janusz [3].

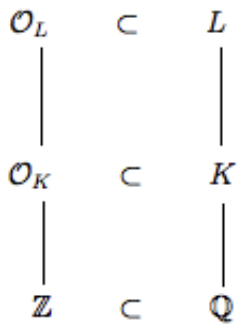
2.1 Number fields/rings

Definition 2.1.1. *A field K is called a number field if it is a finite extension of $\mathbb{Q}$.*

Recall that $\alpha \in \mathbb{C}$ is an algebraic number if it is the root of a monic polynomial in $\mathbb{Q}[x]$. The ring of integers $\mathbb{Z}$ and the field of rationals $\mathbb{Q}$ share a special relationship, which is generalised to arbitrary number fields. This relationship is founded on the notion of *integrality*.

Definition 2.1.2. *An algebraic number is called an* algebraic integer *if it is the root of a monic polynomial in $\mathbb{Z}[x]$.*

It is a fact that the set of all algebraic integers in some number field K form a subring of K. This is called the *ring of integers of K*, and is denoted $\mathcal{O}_K$. A ring is called a *number ring* if it is the ring of integers of some number field. Number rings have the useful structural property that if $\mathbb{Q} \subseteq K \subseteq L$ is a chain of number field, then we also have $\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \mathcal{O}_L$, giving rise to the following chain diagram:



From the above diagram, it would seem to be the case that the ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, and this is true. This is easily deduced by assuming that

$p/q \in \mathbb{Q}$ (written in lowest terms) is a root of a monic polynomial in $\mathbb{Z}[x]$ and then showing using basic algebraic manipulations that q must divide p, which forces q to be ± 1.

Number rings are usually not PIDs or even UFDs. However, they are *Dedekind rings*. For our purposes, it suffices to say that this ensures that ideals 'factor' nicely in them.

Recall that if $\mathfrak{a} = (a_1, \ldots, a_m)$ and $\mathfrak{b} = (b_1, \ldots, b_n)$ are ideals of a ring R, then the product $\mathfrak{ab}$ is defined to be the ideal generated by

$$\{a_i b_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}.$$

If R is a Dedekind Ring and $\mathfrak{a}$ is an ideal of R, then $\mathfrak{a}$ factors uniquely (up to order) as a product of prime ideals of R. We care about this because the decomposition type of $f(x)$ mod p is closely related (by Kummer's Theorem, as we shall see) to the way (p) factors in $K = \mathbb{Q}(\alpha)$, where α is a root of $f(x)$.

Example 2.1.1. *Let $K = \mathbb{Q}(\sqrt{-5})$. We state without proof that $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Then each of the elements $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ is irreducible in R. Observe that we can then write*

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}),$$

so $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ is not a UFD.

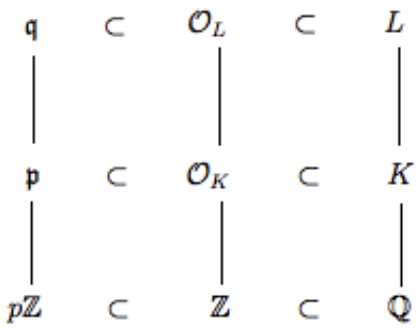
Let $\mathfrak{p}_1 = (2, 1+\sqrt{-5}), \mathfrak{p}_2 = (2, 1-\sqrt{-5}), \mathfrak{p}_3 = (3, 1+\sqrt{-5})$, and $\mathfrak{p}_4 = (3, 1-\sqrt{-5})$. These are prime ideals of $\mathcal{O}_K$, and we have $\mathfrak{p}_1\mathfrak{p}_2 = (2)$, $\mathfrak{p}_3\mathfrak{p}_4 = (3)$, $\mathfrak{p}_1\mathfrak{p}_3 = (1+\sqrt{-5})$, and $\mathfrak{p}_2\mathfrak{p}_4 = (1-\sqrt{-5})$. Then, observe that although the number 6 does not factor uniquely in $\mathcal{O}_K$, the ideal (6) factors uniquely as:

$$(6) = (2) \cdot (3) = (\mathfrak{p}_1\mathfrak{p}_2)(\mathfrak{p}_3\mathfrak{p}_4) = (\mathfrak{p}_1\mathfrak{p}_3)(\mathfrak{p}_2\mathfrak{p}_4) = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Henceforth, we refer to a prime ideal $\mathfrak{p}$ of a ring R as a prime of R (in the case of number rings, we say prime of K rather than prime of $\mathcal{O}_K$).

Definition 2.1.3. *Suppose R is a ring, and $\mathfrak{a}, \mathfrak{b}$ are ideals of R. We say that $\mathfrak{b}$ divides $\mathfrak{a}$ (denoted $\mathfrak{b} \mid \mathfrak{a}$) or $\mathfrak{b}$ lies over $\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ of R such that $\mathfrak{a} = \mathfrak{bc}$.*

We use the unusual phrase "lies over" because in a Dedekind ring R, the fact that $\mathfrak{b}$ lies over or divides $\mathfrak{a}$ is equivalent to the fact that $\mathfrak{b} \supseteq \mathfrak{a}$. It is also convenient to think in these terms since the restrictions of prime ideals in number fields work nicely: If $K \subseteq L$ are number fields, $\mathfrak{p}$ is a prime of K and $\mathfrak{q}$ is a prime of L, then $\mathfrak{q} \cap K = \mathfrak{p}$. This gives the following addition to our earlier chain diagram:



where $p\mathbb{Z} = \mathfrak{p} \cap \mathbb{Z}$.

It turns out that for a number field K and any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite. This ensures that the following definition makes sense.

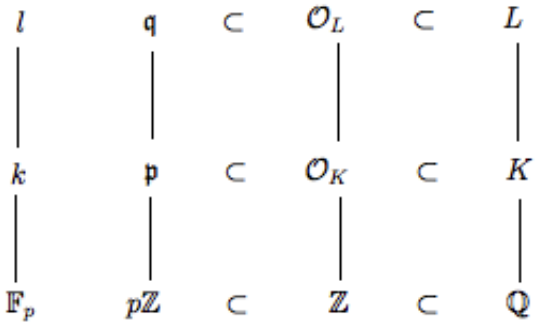
Definition 2.1.4. *Let R be a number ring and $\mathfrak{a}$ an ideal of R. Then the* norm *of $\mathfrak{a}$ is*

$$N(\mathfrak{a}) = |R/\mathfrak{a}|.$$

Recall that a prime $\mathfrak{p}$ of a number field K is maximal in $\mathcal{O}_K$, so that $k = \mathcal{O}_K/\mathfrak{p}$ is a finite field. We call k a residue field. If we have a chain of number rings $\mathbb{Z} \subseteq \mathcal{O}_K \subseteq \mathcal{O}_L$, then letting $l = \mathcal{O}_L/\mathfrak{q}$, we get an extension of residue fields $\mathbb{F}_p \subset k \subset l$. We can make l into a $k-$vector space by defining vector addition as usual and scalar multiplication naturally, that is, for $\alpha + \mathfrak{p} \in k$ and $x + \mathfrak{q} \in l$, we define

$$(\alpha + \mathfrak{p}) \cdot (x + \mathfrak{q}) = \alpha x + \mathfrak{q}.$$

It is an easy check to confirm that this is well-defined and does indeed satisfy the axioms for a vector space. We can similarly make l and k into $\mathbb{F}_p-$vector spaces. So we get the following addition to the diagram:



In the following definition, $\mathfrak{p}\mathcal{O}_L$ denotes the ideal of $\mathcal{O}_L$ generated by $\mathfrak{p}$.

Definition 2.1.5. *Let $K \subseteq L$ be number fields, and suppose $\mathfrak{p}$ is a prime of K. Write*

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \cdots \mathfrak{q}_r^{e_r},$$

where each $\mathfrak{q}_i$ is a prime of L. Let $k = \mathcal{O}_K/\mathfrak{p}$ and $l_i = \mathcal{O}_L/\mathfrak{q}_i$ for $i = 1, \ldots, r$. We define the residue degree *of $\mathfrak{q}_i$ over $\mathfrak{p}$ to be*

$$f(\mathfrak{q}_i/\mathfrak{p}) = f_i = [l_i : k]$$

and we define the ramification index of $\mathfrak{q}_i$ over $\mathfrak{p}$ to be

$$e(\mathfrak{q}_i/\mathfrak{p}) = e_i.$$

Theorem 2.1.2. *With notation as above. we have that*

$$\sum_{i=1}^{r} e_i f_i = \sum_{i=1}^{r} e(\mathfrak{q}_i/\mathfrak{p}) f(\mathfrak{q}_i/\mathfrak{p}) = [L : K].$$

From the preceding discussion of residue fields, it is easy to see that both f and e are multiplicative in towers. We introduce some relevant terminology:

Definition 2.1.6. *Using the same notation as above:*

- *If $e_i = 1$, then $\mathfrak{q}_i$ is* unramified *over $\mathfrak{p}$. If $e_i = \cdots = e_r = 1$, then $\mathfrak{p}$ is unramified in $\mathcal{O}_L$.*
- *If $r = n$, that is if $\mathfrak{p}\mathcal{O}_L$ is a product of n distinct primes of $\mathcal{O}_L$, then $\mathfrak{p}$* splits completely *in $\mathcal{O}_L$.*

- *If $e_i \geqslant 2$ for any i, then* $\mathfrak{p}$ ramifies *in* $\mathcal{O}_L$.

We are finally ready to state Kummer's Theorem, which provides us with the desired link to monic, irreducible polynomials in $\mathbb{Z}[x]$.

Theorem 2.1.3 (Kummer)**.** *Let $K = \mathbb{Q}(\theta)$ be a number field, where θ is an algebraic integer, and suppose that p is a prime number that does not divide $|\mathcal{O}_K/\mathbb{Z}[\theta]|$. Let $g(x) \in \mathbb{Z}[x]$ be the minimal polynomial of θ, and write*

$$g(x) \equiv g_1(x)^{e_1} \cdots g_r(x)^{e_r} \pmod{p},$$

where $g_i(x) \in \mathbb{Z}[x]$, $\overline{g_i(x)}$ is irreducible in $\mathbb{Z}_p[x]$, and the $\bar{g}_i$'s are pairwise distinct. Then

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r},$$

where $\mathfrak{p}_i = (p, g_i(\theta))\mathcal{O}_K = p\mathcal{O}_K + g_i(\theta)\mathcal{O}_K$ is a prime ideal, and $f_i = \deg g_i$.

That is, the decomposition type of $f(x)$ modulo p is determined by the way (p) factors in $\mathbb{Q}(\theta)$, where θ is a root of f! The restriction on p rules out only finitely many p, because $\mathcal{O}_K/\mathbb{Z}[\theta]$ is always finite.

2.2 Decomposition Groups and the Artin Symbol

We henceforth assume that L/K is a Galois extension of number fields, and $[L : K] = n$. Observe that for any $\sigma \in G = \mathrm{Gal}(L/K)$, the set

$$\sigma(\mathfrak{q}) = \{\sigma(\alpha) \mid \alpha \in \mathfrak{q}\}$$

is a prime of $\mathcal{O}_L$, that is, elements of $\mathrm{Gal}(L/K)$ map prime ideals to prime ideals. It turns out that when L/K is Galois, then $\mathrm{Gal}(L/K)$ acts transitively on the set of prime ideals of $\mathcal{O}_L$ lying over $\mathfrak{p}$, for any fixed $p \in \mathbb{P}$. A consequence of this is the following.

Theorem 2.2.1. *In the setting of Theorem 2.1.2, if L/K is Galois, then $e_1 = \cdots = e_r$ and $f_1 = \cdots = f_r$. Letting e (resp. f) denote the common value of the e_i's (resp. f_i's) we have $ref = [L : K]$.*

Notice that for any prime $\mathfrak{q}_i$ of $\mathcal{O}_L$ that lies over $\mathfrak{p}$, the Orbit-Stabilizer Theorem from group theory implies that the stabilizer of $\mathfrak{q}$ in G is a subgroup of order $ref/r = ef$.

Definition 2.2.1. *With the notation as usual, we define the Decomposition Group of* $\mathfrak{q}$ *on* $\mathfrak{p}$*:*

$$D_{\mathfrak{q}/\mathfrak{p}} = \{\sigma \in G \mid \sigma(\mathfrak{q}) = \mathfrak{q}\}.$$

Let $H = \mathrm{Gal}(l/k)$. The reader may notice that $|H| = f(\mathfrak{q}/\mathfrak{p})$ divides $|D_{\mathfrak{q}/\mathfrak{p}}|$. This suggests that they are somehow related, and this is indeed the case:

Theorem 2.2.2. *There exists a surjective homomorphism from* $D_{\mathfrak{q}/\mathfrak{p}} \to H$*. Explicitly, we send* $\sigma \mapsto \bar{\sigma}$*, where* $\bar{\sigma} \in H$ *is defined by*

$$\bar{\sigma}(\bar{\alpha}) = \overline{\sigma(\alpha)}$$

where $\bar{\alpha} \in l$*,* $\alpha \in \mathcal{O}_L$ *is a lift of* $\bar{\alpha}$*, and* $\overline{\sigma(x)}$ *denotes the class of* $\sigma(x)$ *modulo* $\mathfrak{q}$*.*

Since l/k is an extension of finite fields, it is Galois, and H is cyclic. We also know from Galois Theory that H is generated by the Frobenius automorphism Frob, which is defined by

$$\mathrm{Frob}(\alpha) = \alpha^{|k|}.$$

Now, observe that if $\mathfrak{p}$ does not ramify in $\mathcal{O}_L$ and if L/K is Galois, then $e = 1$, and in particular $D_{\mathfrak{q}/\mathfrak{p}} \cong H$ is cyclic. Then, there is a unique element $\sigma \in D_{\mathfrak{q}/\mathfrak{p}}$ such that $\sigma \mapsto \mathrm{Frob}$ under the isomorphism. This σ has the unique property that

$$\sigma(a) \equiv a^{N(\mathfrak{p})} \pmod{\mathfrak{q}}, \quad \forall a \in \mathcal{O}_L.$$

Definition 2.2.2. *With notation as above, suppose* $\mathfrak{p}$ *is unramified in* $\mathcal{O}_L$ *and* $\mathfrak{q}$ *is a prime of* $\mathcal{O}_L$ *lying over* $\mathfrak{p}$*. We define the Artin symbol of* $\mathfrak{q}$ *in* L/K*:*

$$\left(\frac{L/K}{\mathfrak{q}}\right)$$

to be the unique element of $D_{\mathfrak{q}/\mathfrak{p}}$ *that is mapped to Frob* $\in H$ *under the isomorphism, where* $\mathfrak{q} \cap K = \mathfrak{p}$*.*

These are a few basic properties of the Artin Symbol:

Lemma 2.2.1. *Let* L/K *be a Galois extension of number fields. With notation as above:*

- *If* $\sigma \in \mathrm{Gal}(L/K)$*, then*

$$\left(\frac{L/K}{\sigma(\mathfrak{q})}\right) = \sigma\left(\frac{L/K}{\mathfrak{q}}\right)\sigma^{-1}$$

- *The order of* $((L/K)/\mathfrak{q})$ *in* $\mathrm{Gal}(L/K)$ *is* f*.*
- $\mathfrak{p}$ *splits completely in* L *if and only if* $((L/K)/\mathfrak{q}) = 1$
- *The Artin Symbol restricts nicely to Galois subfields. That is, if* $K \subset L \subset M$ *is a chain of Galois extensions, and* $\mathfrak{q}$ *is a prime of* M *with* $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$*, then* $((M/K)/\mathfrak{q}) \mid_L = ((L/K)/\mathfrak{p})$*.*

From this lemma, it follows that when G is abelian, every prime ideal lying over $\mathfrak{p}$ has the same Artin symbol, and if G is not abelian, then the Artin symbols of the prime ideals lying over $\mathfrak{p}$ at least form a conjugacy class $C \subseteq G$.
Thus, in general, we may extend the Artin symbol to primes of $\mathcal{O}_K$ by defining

$$\left(\frac{L/K}{\mathfrak{p}}\right) = C.$$

2.3 Density Theorems

Here, we extend the notion of density to apply to sets of prime ideals of a number ring. Since there is no linear ordering defined on prime ideals, we make use of the norm of an ideal.

Definition 2.3.1. *Let* $A \subseteq B$ *be sets of primes of* $\mathcal{O}_K$*. We define the natural or asymptotic density of* A *in* B *to be*

$$\lim_{n\to\infty} \frac{\#\{\mathfrak{p} \in A \mid N(\mathfrak{p}) \leqslant n\}}{\#\{\mathfrak{p} \in B \mid N(\mathfrak{p}) \leqslant n\}},$$

if the limit exists. In the case when A *is a set of primes and* $\mathbb{P}_K$ *is the set of all primes of* K*, we simply call the above expression the Natural density of* A*.We define the Dirichlet density of* A *in* B *to be*

$$\lim_{s\to 1^+} \frac{\sum_{\mathfrak{p}\in A} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}\in B} N(\mathfrak{p})^{-s}}.$$

In the case when A *is a set of primes and* $\mathbb{P}_K$ *is the set of all primes of* K*, we simply call the above expression the Dirichlet density of* A*.*

An equivalent definition of Dirichlet density of a set A of primes of K is

$$\delta(A) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in A} N(\mathfrak{p})^{-s}}{-\log(s-1)}.$$

The following is a strengthened version of Frobenius' Density Theorem, since the latter cannot distinguish between multiple conjugacy classes in $\mathrm{Gal}(f)$ that have the same cycle-type. See Lang [4, VIII.8] for a proof.

Theorem 2.3.1 (Chebotarev Density Theorem)**.** *Let L/K be a Galois extension of number fields with Galois group G, and let C be a conjugacy class of G. Then, the set*

$$S = \{\mathfrak{p} \mid \mathfrak{p} \text{ is unramified in } L \text{ and } ((L/K)/\mathfrak{p}) = C\}$$

has Dirichlet density

$$\delta(S) = \frac{\#C}{\#G}.$$

We give a simple example of an application of Chebotarev's Density Theorem (in fact, Frbenius Density Theorem could have also been used here):

Theorem 2.3.2. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial, and let α be a root of $f(x)$ in the algebraic closure of $\mathbb{Q}$. If $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a Galois extension (or equivalently, if $|\mathrm{Gal}(f)| = \deg f$), then*

$$\delta(P(f)) = \frac{1}{\deg f}.$$

Proof. Since $K/\mathbb{Q}$ is Galois, $f(x)$ has a root modulo p if and only if (p) splits completely in K. By part (iii) of Lemma 9, this happens if and only if

$$\left(\frac{K/\mathbb{Q}}{p}\right) = 1,$$

the identity element of the group $G = \mathrm{Gal}(K/\mathbb{Q})$. By Chebotarev's Density Theorem, the set

$$S = \{p \mid p \text{ is a rational prime and } \left(\frac{K/\mathbb{Q}}{p}\right) = 1\}$$

has density

$$\delta(S) = \frac{1}{|\mathrm{Gal}(K/\mathbb{Q})|} = \frac{1}{[K:\mathbb{Q}]} = \frac{1}{\deg f}.$$

It is clear from the preceding comments that $S = P(f)$. The desired result follows. □

2.4 Cyclotomic fields

Let ζ_m denote a primitive mth root of unity. We denote the field $\mathbb{Q}(\zeta_m)$ by K_m. From Galois Theory, we know that the minimal polynomial $\Phi[x] \in \mathbb{Q}[x]$ of ζ_m has degree $\phi(m)$, where ϕ is Euler's Totient function. $K_m/\mathbb{Q}$ is Galois, with an abelian Galois group G that is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$, the group of units of the ring $\mathbb{Z}/m\mathbb{Z}$. The elements of G are of the form σ_a, for $1 \leqslant a < m$ and a co-prime to m, where $\sigma_a(\zeta_m) = \zeta_m^a$.

Things work very nicely in cyclotomic fields:

- $\mathcal{O}_{K_m} = \mathbb{Z}[\zeta_m]$.
- p ramifies in K_m if and only if $p \nmid m$.
- If $p \nmid m$, the factorisation of (p) into distinct prime ideals in $\mathbb{Z}[\zeta_m]$ has the form
$$(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_r,$$
where $f = f_i$ is the order of p in $(\mathbb{Z}/m\mathbb{Z})^\times$, and $r = \phi(m)/f$.

Cyclotomic fields are central to our discussion because of the following lemma.

Lemma 2.4.1. *Let $K_m = \mathbb{Q}(\zeta_m)$ be a cyclotomic field, and let $p \in \mathbb{P}$ such that $p \nmid m$. Then*
$$\left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma_p,$$
where $\sigma_p(\zeta_m) = \zeta_m^p$.

Proof. By the discussion preceding Definition 2.2.2, $((K_m/\mathbb{Q})/p) \in \mathrm{Gal}(K_m/\mathbb{Q})$ is the unique element such that for every $x \in \mathbb{Z}[\zeta_m]$
$$\left(\frac{K_m/\mathbb{Q}}{p}\right)(x) \equiv x^p \pmod{p}.$$

Every element of K_m and in particular every element of $\mathbb{Z}[\zeta_m]$ can be written in terms of the basis $\{1, \zeta_m, \ldots, \zeta_m^{m-1}\}$. Let $x = a_0 + a_1\zeta_m + \cdots +$

$a_{m-1}\zeta_m^{m-1}$. Then we have

$$\begin{aligned}\left(\frac{K_m/\mathbb{Q}}{p}\right)(x) &= \left(\frac{K_m/\mathbb{Q}}{p}\right)(a_0 + a_1\zeta_m + \cdots + a_{m-1}\zeta_m^{m-1}) \\ &= a_0 + a_1\zeta_m^p + \cdots + a_{m-1}\zeta_m^{(m-1)p} \\ &\equiv (a_0 + a_1\zeta_m + \cdots + a_{m-1}\zeta_m^{m-1})^p \pmod{p} \\ &= x^p,\end{aligned}$$

where the second congruence follows since the Binomial Theorem ensures that every other term in the expansion of x^p vanishes because its coefficient is divisible by p, and the coefficients are congruent to their own pth powers mod p (by Fermat's Little Theorem). □

Recall that we had used Dirichlet's Theorem to solve the case for quadratic polynomials. Dirichlet's Theorem actually follows as an easy consequence of Chebotarev's Density Theorem.

Theorem 2.4.1 (Dirichlet's Theorem)**.** *Let a and m be two positive, co-prime integers. Then the set*

$$S = \{p \in \mathbb{P} \mid p \equiv a \pmod{b}\}$$

has Dirichlet density $1/\phi(b)$, where ϕ denotes Euler's Totient function.

Proof. Let a and m be as above, and let $K_m = \mathbb{Q}(\zeta_m)$, where ζ_m is a primitive mth root of unity. Then $p \nmid m$ if and only if p is unramified in K_m. We also know that $K_m/\mathbb{Q}$ is Galois, and since $G = \mathrm{Gal}(K_m/\mathbb{Q})$ is abelian, the Artin symbol for each prime p of $\mathbb{Z}$ is a well-defined element of $\mathrm{Gal}(K_m/\mathbb{Q})$.

We know that each $\sigma \in G$ is of the form σ_t, where $\sigma_t(\zeta_m) = {\zeta_m}^t$, and $1 \leq t < m$ is co-prime to m. Observe that for any $t_1, t_2 \in \mathbb{Z}_+$, we have that

$$\sigma_{t_1} = \sigma_{t_2} \quad \text{if and only if} \quad t_1 \equiv t_2 \pmod{m},$$

and in addition to this, we know that if $p \nmid m$, then $((K_m/\mathbb{Q})/p) = \sigma_p$. Combining the above, we see that for a rational prime p,

$$\left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma_a \quad \text{if and only if} \quad p \equiv a \pmod{m}.$$

Let S be the set of rational primes that have Artin symbol $\sigma_a \in G$. Then S is also the set of primes that are congruent to a modulo m. By Chebotarev, this set has Dirichlet density $1/|G| = 1/\phi(m)$.

□

3 Theorem A

3.1 Proof of Theorem A

We would now like to show that when $\mathrm{Gal}(f)$ is abelian, then $P(f)$ is characterisable by congruence conditions. We saw in Lemma 2.4.1 that the Artin symbol of a rational prime $((K_m/\mathbb{Q})/p)$ is determined by congruence classes modulo m. We make use of this fact. First note that $\mathrm{Gal}(K_m/\mathbb{Q})$ is always abelian, so every intermediate field is an *abelian extension* of $\mathbb{Q}$, that is, it is a Galois extension of $\mathbb{Q}$ with abelian Galois group. In fact, the following, amazing fact is true. The reader can find a proof in Cox [5, Ch. 2]

Theorem 3.1.1 (Kronecker-Weber Theorem)**.** *Every abelian extension (Galois extension with abelian Galois group) of the rationals is contained in some cyclotomic field.*

We will also need a part of the Fundamental Theorem of Galois Theory, which we state for completeness:

Theorem 3.1.2. *Let L/K be a Galois extension of fields with Galois Group G, and let $\phi(H)$ denote the fixed field of the subgroup H of G. If $H \triangleleft G$, then the restriction map*

$$\sigma \mapsto \sigma|_{\phi(H)}$$

is a surjective homomorphism of G onto $\mathrm{Gal}(\phi(H)/K)$, with kernel H.

Note that if $\mathrm{Gal}(f)$ is abelian, then $|\mathrm{Gal}(f)| = \deg f$. To see why, suppose α is a root of f, and let L denote its splitting field over $\mathbb{Q}$. Then, since $\mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f)$ is abelian, every subgroup is normal and in particular, ever intermediate field is a Galois over $\mathbb{Q}$. Then f must split in $\mathbb{Q}(\alpha)$, whence we conclude that $\mathbb{Q}(\alpha) = L$, so that

$$|\mathrm{Gal}(f)| = [L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f.$$

This fact is implicitly used in the following proof.

Theorem A. *Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible polynomial with abelian Galois group, and let m be an integer such that the splitting field of f is contained in $K_m = \mathbb{Q}(\zeta_m)$. Then, there exist*

$$\frac{[K_m : \mathbb{Q}]}{\deg f} = \frac{\phi(m)}{\deg f}$$

many integers a_i that are relatively prime to m and pairwise incongruent modulo m, such that, for any rational prime p that does not divide m, f has a root modulo p if and only if $p \equiv a_i \pmod{m}$ for some $0 \leqslant i \leqslant \phi(m)/\deg f$

Proof. We know that $G = \mathrm{Gal}(K_m/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ is cyclic, so every subgroup is normal, which implies that every intermediate field of K_m is Galois over $\mathbb{Q}$.
Let α be a root of $f(x)$, and set $K = f(\alpha)$. Then K is the fixed field of some subgroup H of G. We have that $((K_m/\mathbb{Q})/p)|_K = ((K/\mathbb{Q})/p)$, and applying Theorem 17, it follows that

$$\left(\frac{K/\mathbb{Q}}{p}\right) = 1 \text{ if and only if } \left(\frac{K_m/\mathbb{Q}}{p}\right) \in H.$$

We also know that elements of G are of the form σ_t, where $\sigma_t(\zeta_m) = \zeta_m^t$, and explicitly:

$$\left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma_p.$$

In the proof of Dirichlet's Theorem, we saw that

$$\left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma_a \quad \text{ if and only if } \quad p \equiv a \pmod{m}.$$

We combine all this information into the following.

$$\begin{aligned} f(x) \text{ has a root modulo } p &\iff p \text{ splits completely in } K \\ &\iff \left(\frac{K/\mathbb{Q}}{p}\right) = 1 \\ &\iff \left(\frac{K_m/\mathbb{Q}}{p}\right) = \sigma_a \in H \\ &\iff p \equiv a \pmod{m}. \end{aligned}$$

Finally, observe that

$$|H| = \frac{|G|}{[K:\mathbb{Q}]} = \frac{\phi(m)}{\deg f},$$

which completes the proof. □

3.2 Follow-up Questions

This project leads to some natural follow-up questions. The most pressing question is whether the converse of Theorem A is also true. That is, if the primes in $P(f)$ can be exhibited as the union of primes in some congruence classes modulo an integer, then is $\mathrm{Gal}(f)$ abelian? Another direction in which we can turn is to weaken project's question and ask whether $P(f)$ always *contains* the union of primes in some residue classes modulo an integer.

We finally conclude by giving the example of a polynomial whose Prime Set can be completely "characterised", but not simply by congruence conditions modulo some integer. For the polynomial $f(x) = x^3 - 2$, (see Cox [5, I.4]) it turns out that

$$P(f) = \{p \in \mathbb{P} \mid p \equiv 2 \pmod 3 \text{ or } p = x^2 + 27y^2 \text{ for some } x, y \in \mathbb{Z}\}.$$

This example suggests that broadening the definition of "characterisation" to include primes that can be expressed in different ways may yield some interesting results.

3.3 Acknowledgements

I would like to thank Prof. Krumm for his academic guidance and patient mentorship. I would also like to thank Prof. Matt Baker at Georgia Tech for his freely available lecture notes on Algebraic Number Theory, which I used extensively to become familiar with the material.

4 References

[1] Ireland, K. and Rosen, M. "A Classical introduction to modern number theory." Graduate Texts in Mathematics, Vol. 84. Springer-Verlag, New York, 1990.

[2] Sury, B., "Polynomials with Integer Values." *Resonance*, Vol. 6, No. 8. 2001.

[3] Janusz, Gerald J. "Algebraic Number Fields." Graduate Studies in Mathematics, Vol. 7. American Mathematical Society, 1996.

[4] Lang, S. "Algebraic Number Theory." Graduate Texts in mathematics, Vol. 110. Springer-Verlag, New York, 1994.

[5] Cox, David A. "Primes of the form $x^2 + ny^2$." Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., 2013.

[6] Baker, M. "Algebraic Number Theory, course notes, Fall 2006." link: *http://people.math.gatech.edu/ mbaker/pdf/ANTBook.pdf.*