Final Report
Arithmetic of Polynomials in Knot Theory
Fall 2025

Faculty Mentor: Yi Wang
Project Leader: Levi Poon
IML Scholars: Derek Zeng, Martin Jiang, Michael Yin, Sreehaas Chinnala [*]

December 24, 2025

Abstract

We used cyclotomic polynomials to prove the irreducibility of several common factors in $P_{a,b}$, labeled as equation 1. We divide the a, b pairs by their properties in the division of a series of prime numbers, especially $2, 3$. The key theorem is a can be categorized by odd and even as two groups, and $P_{a,b}$ has common factors of $(x+1)^2$ when a is odd, and $(x^2 - x + 1)$ when a is odd and divisible by 3. We formed our conjectures around findings in $P_{a,b}$ that the common factors are irreducible for a, b relative primes. And $P_{a,b}$ has ≥ 2 non-panlindromic irreducible factors in $\mathbb{F}_2[x]$ for $b \geq \frac{a}{4}$, $a \equiv 5, 19 \pmod{24}$.

1 Introduction

A central theme in modern knot theory is that subtle topological information about a knot $K \subset S^3$ is encoded in the geometry and arithmetic of its complement $M := S^3 \setminus K$. For a large class of knots, including the figure-eight knot, the complement admits a complete finite-volume hyperbolic metric, so that

$$M \cong \mathbb{H}^3/\Gamma, \quad \Gamma \leq \mathrm{SL}(2, \mathbb{C})$$

with Γ a lattice. By Mostow–Prasad rigidity, the hyperbolic structure is uniquely determined by the topology of M, and consequently geometric quantities (e.g. volume, cusp shape, holonomy) become topological invariants that are computable from explicit gluing and deformation equations coming from ideal triangulations [1, 2, 3]. This computability is one of the main reasons hyperbolic geometry has become a practical engine for producing and testing conjectures in 3-manifold topology. Among the most consequential operations in 3-manifold topology is Dehn filling. If M has a torus cusp, then $\partial M \cong T^2$ carries a preferred

[*] in alphabetical order

homology basis (meridian–longitude once the knot is fixed). A slope α is an unoriented primitive isotopy class of essential simple closed curves on ∂M, and the Dehn filling $M(\alpha)$ is obtained by gluing in a solid torus so that α bounds a meridional disk. Thurston's hyperbolic Dehn surgery theorem states that all but finitely many slopes produce a hyperbolic manifold again, and the new hyperbolic structure arises as a controlled deformation of the original cusp geometry [1, 2]. In particular, Dehn fillings provide an infinite family of closed (or less-cusped) hyperbolic manifolds generated from a single cusped parent, making them an ideal setting for systematic arithmetic experiments.

From an arithmetic perspective, one studies number fields naturally attached to Γ. The (invariant) trace field is generated by traces of elements of a suitable lift of Γ to $\mathrm{SL}(2, \mathbb{C})$; it is a commensurability invariant and often serves as a concise algebraic summary of the hyperbolic structure. For Dehn fillings of the figure-eight knot complement, Filaseta [4] gives an explicit description of the relevant trace field in terms of a lacunary Palindromic polynomial: for a slope written as $-a/b$ (with $\gcd(a, b) = 1$), the trace field can be expressed as $\mathbb{Q}(x + x^{-1})$ where x is a root of

$$P_{a,b}(x) = x^{4b} - x^{2b} - x^{a} - 2 - x^{-a} - x^{-2b} + x^{-4b}. \tag{1}$$

Thus, understanding the factorization of $P_{a,b}$ over $\mathbb{Q}$ directly informs the algebraic degree and structure of the trace field under Dehn filling. Concretely, irreducible factors correspond to field subextensions generated by algebraic relations among $x + x^{-1}$, and systematic factorization patterns suggest hidden constraints that depend on the residue classes of (a, b).

A second motivation comes from reduction modulo primes. For an integer polynomial, factoring over $\mathbb{F}_p$ often reveals structure that is invisible over $\mathbb{Q}$ at small computational scales, and it is a standard strategy to use mod-p behavior to guide (or obstruct) conjectures about rational factorization. In this project, we focus on $\mathbb{F}_2$ because Palindromic/symmetric phenomena interact in a particularly rigid way in characteristic 2, producing a clean trichotomy of observed behaviors (all symmetric factors; a mix of symmetric and asymmetric factors; all asymmetric factors). This is closely tied to the fact that $P_{a,b}$ is Palindromic (palindromic) and to the special role played by the involution $x \mapsto x^{-1}$ in characteristic 2.

In the remainder of the paper, we first record basic divisibility and parity constraints over $\mathbb{Q}$, then we develop the symmetric/asymmetric framework over $\mathbb{F}_2$ and summarize the resulting case-by-case distributions in terms of (a, b).

2 Results

2.1 Methodology

From the paper in by Michael Filaseta, the former mathematicians all tried to classify the reducibility of polynomials with respects to different values of a and b, which becomes one of the breakthrough points we have [4]. We utilized the powerful mathematics library to code our calculations. We want to divide a good number of pairs of a and b, and the polynomials grow exponentially when the values of a and b increase. The first step is finding a convenient tool to calculate the reducibility of a and b. Notice that this is a much more complicated job in rational fields comparing to the field 2 which is also a field we are interested in.

We will brief review some of the problems and highlights in the running of the following mathematical tools.

- Matlab: Matlab is a highly developed tool that performs well in the early investigation. One of the strength in Matlab concentrates on the fast results of finding roots for the polynomials. We can investgate in small samples which leads to finding out how some polynomial forces roots to be $x \in \mathbb{C}$. This is important for $\mathbb{Q}(x + x^{-1})$ trace field analysis.

  However, Matlab has some significant downsides as it is bad in high degree analysis. Also hard to store a huge number of values, and not visualizing friendly.

- Wolfram Mathematica: This is a great tool that has a packages for visualization of knots and complex geometric shape. It is also good at reducing polynomials. However, in a similar problem of Matlab, it is not portable. It is not convienent for long time running as well,

- SageMath [5]: This is our main tool, which is a package that usable with python library which makes it extra powerful as we can preprocess the polynomials and postprocess the factorizing results. Although SageMath is not finding the exact roots as Matlab and Mathematica do, SageMath find the irreducible factors in polynomials product forms. This helps us to discover the common polynomials in the list, and the general form of irreducible leftover part of the irreducible part.

In terms of running SageMath, we find ubuntu build of runable SageMath challenging as too many prerequisite packages are required. We have few alternatives, including images in jupiter notebook, github codespaces, and docker containers.

2.2 Theorems in Rational Fields

We begin with the investigations of common factors in rational fields by considering whether $\{(x^{2^n} + 1) \mid n \in \mathbb{N}\}$ is a possible factor for some a, b pairs.

For positive integers a, b, consider the polynomial

$$P_{a,b}(x) = x^{4b} - x^{2b} - x^{a} - 2 - x^{-a} - x^{-2b} + x^{-4b}$$

Clear denominators by multiplying with x^{4b}:

$$Q_{a,b}(x) := x^{4b} P_{a,b}(x) = x^{8b} - x^{6b} - x^{4b+a} - 2x^{4b} - x^{4b-a} - x^{2b} + 1 \in \mathbb{Z}[x]$$

Since $Q_{a,b}(\xi) = \xi^{4b} P_{a,b}(\xi)$ for every $\xi \in \mathbb{C}^{\times}$, the two polynomials have the same zero set on the unit circle. We will work with $Q_{a,b}$ (a Palindromic polynomial with constant term 1).

Classify exactly for which $k \geq 1$ the cyclotomic factor $\Phi_{2^k}(x) = x^{2^{(k-1)}} + 1$ divides $Q_{a,b}(x)$, and show that for a fixed pair (a, b) at most one such k occurs.

Theorem 1. *Let $a, b \in \mathbb{Z}_{>0}$ and $k \geq 1$. Then $\Phi_{2^k}(x) \mid Q_{a,b}(x)$ if*

$$\begin{cases} \text{(A)} & 2^{k-1} \mid b \ \ \textit{and} \ \ a \equiv 2^{k-1} \pmod{2^k}, \\ \text{or (B)} & k \geq 2, \ b \equiv 2^{k-2} \pmod{2^{k-1}} \ \ \textit{and} \ \ 2^k \mid a. \end{cases}$$

Moreover, for a given (a, b) there is at most one k *for which $\Phi_{2^k} \mid Q_{a,b}$.*

For $k = 1$, $\Phi_2 = x + 1$: condition (A) says $a \equiv 1 \pmod 2$; (B) is void.

For $k = 2$, $\Phi_4 = x^2 + 1$: either $b \equiv 0 \pmod 2$ and $a \equiv 2 \pmod 4$, or $b \equiv 1 \pmod 2$ and $a \equiv 0 \pmod 4$

For $k = 3$, $\Phi_8 = x^4 + 1$: either $b \equiv 0 \pmod 4$ and $a \equiv 4 \pmod 8$, or $b \equiv 2 \pmod 4$ and $a \equiv 0 \pmod 8$. Higher k follow the same 2-adic pattern.

Fix $k \geq 1$ and let $\theta := \pi/2^{k-1}$, $\zeta := e^{i\theta}$, so ζ is a primitive 2^k-th root of unity. Consider ζ^t with t odd modulo 2^k.

We've also noticed that when we set $a \equiv 1 \pmod 2$, then $(x + 1) \mid P_{a,b}$. Likewise, if we let $a \equiv 0 \pmod 4$ and $b \equiv 1 \pmod 2$, we see that $(x^2 + 1) \mid P_{a,b}$.

The proof of the theorem above is simply substitution using the union roots $e^{\mathrm{i}\pi/2^k}$ for $k \in \mathbb{Z}$, and expanding both sides using Euler's formula to obtain the condition.

Theorem 2.

$$(x^2 - x + 1)^2 \mid P_{3,b}(x) \iff 3 \mid b.$$

Proof. Multiply by x^{4b} to clear denominators:

$$Q_{3,b}(x) := x^{4b} P_{3,b}(x) = x^{8b} - x^{6b} - x^{4b+3} - 2x^{4b} - x^{4b-3} - x^{2b} + 1 \in \mathbb{Z}[x].$$

Clearly $P_{3,b}$ and $Q_{3,b}$ have the same nontrivial irreducible factors.

Let $\zeta = e^{\pi i/3}$ be a primitive 6th root of unity, satisfying $\zeta^6 = 1$ and $\zeta^3 = -1$. Substituting into $Q_{3,b}$ gives

$$\begin{aligned} Q_{3,b}(\zeta) &= \zeta^{8b} - \zeta^{6b} - \zeta^{4b+3} - 2\zeta^{4b} - \zeta^{4b-3} - \zeta^{2b} + 1 \\ &= \zeta^{8b} - \zeta^{6b} + (\zeta^{4b} - 2\zeta^{4b} + \zeta^{4b}) - \zeta^{2b} + 1 \\ &= \zeta^{8b} - \zeta^{6b} - \zeta^{2b} + 1. \end{aligned}$$

Since $\zeta^6 = 1$, we have $\zeta^{8b} = \zeta^{2b}$, hence $Q_{3,b}(\zeta) = 0$. Similarly $Q_{3,b}(\zeta^5) = 0$. Thus the minimal polynomial of ζ, namely $\Phi_6(x) = x^2 - x + 1$, divides $Q_{3,b}(x)$ for all b.

To determine the multiplicity, compute the derivative:

$$\begin{aligned} Q'_{3,b}(x) = 8b\, x^{8b-1} - 6b\, x^{6b-1} - (4b+3)x^{4b+2} \\ - 8b\, x^{4b-1} - (4b-3)x^{4b-4} - 2b\, x^{2b-1}. \end{aligned}$$

At $x = \zeta$ this simplifies (after using $\zeta^6 = 1$ and setting $u = \zeta^{2b}$) to

$$Q'_{3,b}(\zeta) = 6b\, \zeta^{-1}(u - 1) = 6b\, \zeta^{-1}(\zeta^{2b} - 1).$$

Therefore $Q'_{3,b}(\zeta) = 0$ if and only if $\zeta^{2b} = 1$, i.e. $3 \mid b$. Hence Φ_6 has multiplicity ≥ 2 exactly when $3 \mid b$.

Finally, a direct computation of the second derivative shows that when $b = 3k$,

$$Q''_{3,3k}(\zeta) = -\zeta\,(216k^2 + 18) \neq 0,$$

so the multiplicity is exactly 2 in this case.

Thus $(x^2-x+1) \mid P_{3,b}(x)$ always, $(x^2-x+1)^2 \mid P_{3,b}(x) \iff 3 \mid b$., which completes the proof of the theorem. □

Lemma 3. $(x^2 + x + 1) \nmid P_{a,b}$ *for any* $a, b \in \mathbb{Z}$

Proof. The roots of the polynomial $x^2 + x + 1$ are $\alpha = \text{cis}(\frac{2\pi}{3})$ and $\beta = \text{cis}(\frac{4\pi}{3})$. The powers of these roots are $1, \alpha$, or β. Select a root $\hat{x}$ of the polynomial. If b is congruent with 1 or 2 mod 3, then $\hat{x}^b$ is also a root of the polynomial $x^2 + x + 1$, and thus, $(\hat{x}^{\pm 2b})^2 + \hat{x}^{\pm 2b} = -1$. Thus, the polynomial $P_{a,b}(\hat{x})$ becomes $-1 - \hat{x}^a - 2 - \hat{x}^{-a} - 1 = 0 \implies |\hat{x}^a + \hat{x}^{-a}| = 4$, which is not possible since $|\hat{x}| = 1$.

Now, consider $b \equiv 0 \pmod 3$. Then, $\hat{x}^b = 1$, and $P_{(a,b)}(\hat{x}) = 1 - 1 - \hat{x}^a - 2 - \hat{x}^{-a} - 1 + 1 = 0 \implies \hat{x}^a + \hat{x}^{-a} = -2$. Now, since $|\hat{x}| = 1$, this means that $\hat{x}^{\pm a} = -1$, however, remember that $\hat{x} = \alpha$ or β and $a \in \mathbb{Z}$. There is no integer a such that either root of $x^2 + x + 1$ can be -1, so it is not possible for $\hat{x}^a + \hat{x}^{-a} = -2$. Thus, whatever b is, it is not possible for $x^2 + x + 1$ to divide $P_{(a,b)}$. □

Corollary 1. $(x^6 - 1) \nmid P_{a,b}$

This is also the case for any other multiples of $x^2 + x + 1$.

Lemma 4. $P_{a,b} = \frac{(x^{6b}-1)(x^{2b}-1)}{x^{4b}} - \frac{(x^a+1)^2}{x^a}$

Theorem 5. *From lemma 4, we separate polynomial $P_{a,b}$ into 2 parts, and assume that $a \equiv 1 \pmod 2$ and $\gcd(a, b) = 1$. The common factors between two parts are*

$$(x + 1)^2 \mid P_{a,b} \quad \textit{always,}$$

$$(x^2 - x + 1) \mid P_{a,b} \quad \textit{only when} \quad 3 \mid a$$

Proof. By the previous lemma, we shall write that

$$P_{a,b} = \frac{(x^{6b} - 1)(x^{2b} - 1)}{x^{4b}} - \frac{(x^a + 1)^2}{x^a}$$

For a polynomial $x^m - 1$, we can write it as the product of several cyclotomic polynomials.

$$x^m - 1 = \prod_{d|m} \Phi_d(x) \tag{2}$$

So,

$$x^{6b} - 1 = \prod_{d|6b} \Phi_d(x), \quad x^{2b} - 1 = \prod_{d|2b} \Phi_d(x),$$

$$(x^a + 1)^2 = (\frac{x^{2a} - 1}{x^a - 1})^2 = \prod_{d|2a, d\nmid a} \Phi_d(x)$$

Since the polynomials are factored into cyclotomic polynomials, any common factor must be a cyclotomic polynomial $\Phi_d(x)$ for some integer d.

2 is always the divisor of $6b$ and $2b$, and 2 is the divisor of $2a$ but not the divisor of a when $a \equiv 1 \pmod 2$. So $(\Phi_2)^2 = (x+1)^2$ is always a common factor of both two parts.

6 is the divisor of $6b$, and 6 is the divisor of $2a$ but not the divisor of a when $a \equiv 1 \pmod 2$ and $3 \mid a$. So $\Phi_6 = x^2 - x + 1$ is the common factor of both parts only when $a \equiv 1 \pmod 2$ and $3 \mid a$.

Since a and b are relative primes, there is no other possible integer d such that $d \mid 6b$ or $6 \mid 2b$ and $d \mid 2a$ but $d \nmid a$. So, there is no common polynomial dividing $\frac{(x^{6b}-1)(x^{2b}-1)}{x^{4b}}$ and $\frac{(x^a+1)^2}{x^a}$. □

Corollary 2. *From the proof of Theorem 5, we can also notice that if $a \equiv 1 \pmod 2$ and $\gcd(a, b) \neq 1$, which means a is an odd number and a,b are not relative primes, we can also find some more cyclotomic polynomials as common factors by $\gcd(a, b)$. Thus, we are just focusing on $\gcd(a, b) = 1$ now.*

2.3 Conjectures in Rational Fields

There are few conjectures that we cannot prove in the given time. One reason is that there is no clear pattern in line. One other reason is that we cannot form the conjecture around a stronger case, where we can reduce the question to an easier form.

One of the most exciting conjectures we had is the following,

Conjecture 1. *In $\mathbb{Q}$, consider $a \equiv 1 \pmod 2$, and $\gcd(a, b) = 1$, we observed that,*

$$\begin{cases} \frac{P_{a,b}}{(x+1)^2(x^2-x+1)} & \textit{is irreducible when} \;\; a \equiv 0 \pmod 3 \\ \frac{P_{a,b}}{(x+1)^2} & \textit{is irreducible when} \;\; a \equiv 1, 2 \pmod 3 \end{cases}$$

We first verified this conjecture through an observation from Sage running results of a from 1 to 1000 and b from 1 to 200. We admit that this is a small number in the discussion of number theory, so later we tried to perform randomized verification in the range of $1 < \log_{10}(n) < 4.5$, where n could be either a or b. We do not observe any counterexample in this range. Meanwhile, we experience huge computational challenges as higher a, b make polynomials complexity grow exponentially. Thus, it is not really feasible to run large tests for higher a, b pairs. We ran out of memory very fast when we tried to run verification on Sage. Although one famous person claimed that 640K ought to be enough for anybody, we have obstacles in both running time and RAM for higher degree verification.

One family of polynomials we can observe in the irreducible polynomials is

$$\Phi_p := \left\{ \frac{x^p - 1}{x - 1} \mid p \text{ is a prime number} \right\}$$

For example, $\Phi_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.

Notice that this is always irreducible in the rational field, entertain the following proof [6].

Proof. Since p is a prime number, $x^p - 1 = \Phi_1(x)\Phi_p(x)$, so

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

Which completes the proof. $\square$

And a cyclotomic polynomial is an irreducible polynomial.

Unfortunately, this only covers a small amount of a, b pairs in the polynomials. However, we think it is a key breakthrough we can do, as there is the following property, where $n|k$, $\Phi_{nk}(x) = \Phi_n(x^k)$, and in our definition of $P_{a,b}$, we care about Φ_n [6].

Definition 1. *We call a polynomial* ***palindromic*** *if* $p(x) = x^{\deg(p)}p(\frac{1}{x})$. *We call a polynomial* ***non-palindromic*** *otherwise.*

Although we are not able to prove this conjecture, the result in [4] highly indicates that the conjecture is true, since we have the following theorem:

Theorem 6 (Palindromic compression)**.** *Fix an odd integer* $a \geq 1$. *There exists* $B(a) \geq 1$ *such that for every* $b \geq B(a)$ *with* $\gcd(a, b) = 1$, *if*

$$F_{a,b}(x) := x^{4b}\Big(x^{4b} - x^{2b} - x^a - 2 - x^{-a} - x^{-2b} + x^{-4b}\Big) \in \mathbb{Z}[x],$$

then the non-palindromic part of $F_{a,b}(x)$ *is* 1. *Equivalently, every irreducible factor of* $F_{a,b}(x)$ *(and hence of* $F_{a,b}(x)$ *with any cyclotomic factor removed) is Palindromic.*

Proof. Fix an odd integer $a \geq 1$ and consider, for $b \geq 1$,

$$P_{a,b}(x) = x^{4b} - x^{2b} - x^a - 2 - x^{-a} - x^{-2b} + x^{-4b} \in \mathbb{Z}[x^{\pm 1}],$$

and its integral (Laurent-cleared) polynomial

$$F_{a,b}(x) := x^{4b}P_{a,b}(x) = x^{8b} - x^{6b} - x^{4b+a} - 2x^{4b} - x^{4b-a} - x^{2b} + 1 \in \mathbb{Z}[x].$$

By inspection, $F_{a,b}$ is *palindromic* of degree $8b$, i.e.

$$F_{a,b}(x) = x^{8b}F_{a,b}(x^{-1}).$$

Set

$$n := 2b - a \qquad \text{(so } n \to \infty \text{ as } b \to \infty \text{ with } a \text{ fixed).}$$

Define a bivariate polynomial

$$F(x, y) := \sum_{j=0}^{4} f_j(x)\, y^j \quad \text{with} \quad \begin{cases} f_0(x) = 1, \\ f_1(x) = -x^a, \\ f_2(x) = -(x^a + 1)^2 x^a, \\ f_3(x) = -x^{3a}, \\ f_4(x) = x^{4a}. \end{cases}$$

A direct regrouping of exponents shows

$$F(x,x^n) \;=\; x^{4a}x^{4n} - x^{3a}x^{3n} - (x^a+1)^2x^ax^{2n} - x^ax^n + 1 \;=\; F_{a,b}(x).$$

Thus $F_{a,b}(x)$ is a lacunary specialization of the fixed bivariate polynomial $F(x,y)$ along the curve $y = x^n$.

Let $g(x) \in \mathbb{Z}[x]$ be nonconstant. Write its factorization in $\mathbb{Q}[x]$ as

$$g(x) = c\prod_i q_i(x),$$

where $c \in \mathbb{Q}^\times$ and q_i are irreducible in $\mathbb{Q}[x]$. Denote by $q_i^*(x) := x^{\deg q_i}q_i(x^{-1})$ the palindromic of q_i. The *non-palindromic part* of g is, by definition, the product of those irreducible factors q_i which are not associates of a palindromic polynomial, i.e. $q_i \not\sim q_i^*$ in $\mathbb{Q}[x]$.

Theorem 1.1 in Filaseta's parper [4] (applied to the above $F(x,y)$; see also the verification in his Example 2) asserts the following: for each fixed a there exists an integer $n_0(a)$ such that, whenever $n \geq n_0(a)$ and $\gcd(a,b) = 1$ (equivalently, $\gcd(a,n) = 1$ since $n = 2b - a$ with a fixed and odd), the non-palindromic part of

$$F(x,x^n) = F_{a,b}(x)$$

is *not reducible* in $\mathbb{Q}[x]$, i.e. it is either 1 or an irreducible polynomial in $\mathbb{Q}[x]$.

We claim that if $f \in \mathbb{Q}[x]$ is palindromic and $q \in \mathbb{Q}[x]$ is an irreducible factor of f, then q^* is also a factor of f. Indeed, write $f = \prod_i q_i$ in $\mathbb{Q}[x]$ (up to a unit). Applying $x \mapsto x^{-1}$ and multiplying by a suitable power of x yields

$$f(x) \;\sim\; x^{\deg f}f(x^{-1}) \;=\; \prod_i q_i^*(x),$$

so the multiset of irreducible factors of f is invariant under $q \mapsto q^*$, hence $q^* \mid f$ whenever $q \mid f$.

Now apply this to $f = F_{a,b}$, which is palindromic. If $F_{a,b}$ had a non-palindromic irreducible factor q, then q^* would also divide $F_{a,b}$. Since q is non-palindromic, q^* is not an associate of q, hence the non-palindromic part of $F_{a,b}$ would contain at least the product $q\,q^*$, and therefore would be *reducible* in $\mathbb{Q}[x]$.

Consequently, for all $n \geq n_0(a)$ with $\gcd(a,b) = 1$, Filaseta's conclusion that the non-palindromic part is "not reducible" forces the only remaining possibility:

$$(\text{non-palindromic part of } F_{a,b}) \;=\; 1.$$

Equivalently, every irreducible factor of $F_{a,b}(x)$ in $\mathbb{Q}[x]$ is palindromic.

Let $C_{a,b}(x)$ denote the cyclotomic part of $F_{a,b}(x)$ (the product of all cyclotomic irreducible factors in $\mathbb{Q}[x]$). Cyclotomic polynomials are palindromic; removing $C_{a,b}$ cannot introduce any non-palindromic irreducible factor. Therefore, every irreducible factor of

$$\frac{F_{a,b}(x)}{C_{a,b}(x)}$$

is also palindromic.

Finally, since $n = 2b - a$, define

$$B(a) := \left\lceil \frac{n_0(a) + a}{2} \right\rceil .$$

Then for all $b \geq B(a)$ with $\gcd(a, b) = 1$, the above conclusions hold. $\square$

2.4 GF(2)

Similar to what we do in the rational field, we want to categorize the "behavior" of the same polynomial in $\mathbb{F}_2[x]$ (i.e., with coefficient mod 2) based on the value of a and b.

Directly from the definition of palindromic polynomials, we can know that the irreducible factor of a palindromic polynomial can be either:

- Another palindromic polynomial.
- A pair of non-palindromic polynomials with their product being palindromic.

Then, we can fit all the irreducible polynomials we find from conjecture 1 to the following cases. Factorize the polynomials in $\mathbb{F}_2$, we can categorize the results in disjoint sets of three,

Case 1:	All factorized polynomials are palindromic
Case 2:	Some factorized polynomials are palindromic and others are non-palindromic.
Case 3:	All factorized polynomials are not palindromic.

The first comment we can make is that case 2 is the most common scenario in this categorization. This is an observation and we cannot prove why such popularity exists. We think it is intuitively more common as more a, b pairs fit trace field of $\mathbb{Q}(x + x^{-1})$, where a pair of non-palindromic polynomials is required.

The general distribution of all three cases combined shows no clear patter, which is the reason why we want to divide all data into three subcases.

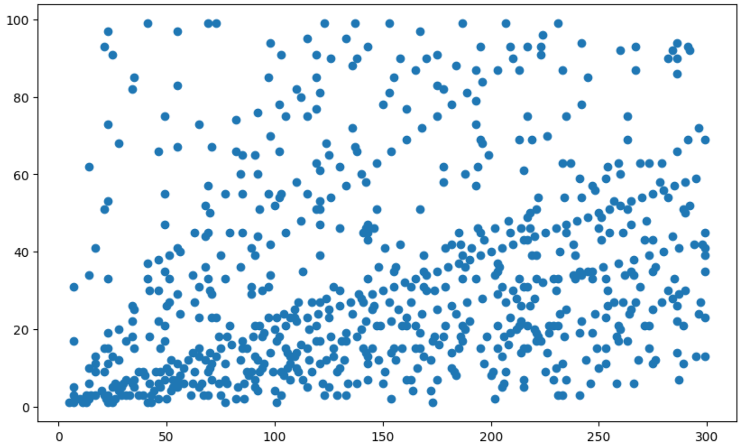

Figure 1: Distribution of all Cases Combined

Arguably, we can see clusters around $b \leq \frac{1}{5}a$. It is so controversial that the statistical analysis doesn't support the claim from eyeball. Fortunately, we are able to make some less controversial observations that fits a good range from $1 \leq a \leq 1000$ and $1 \leq b \leq 200$.

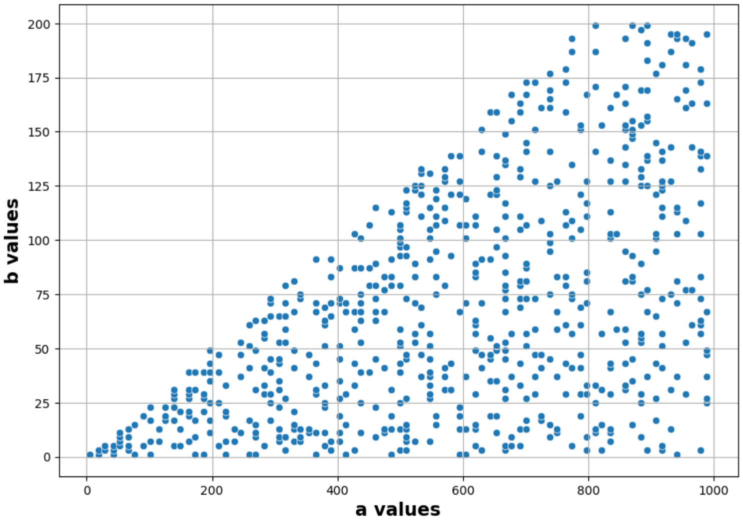

Figure 2: Distribution of Case 1 when $a \equiv 5, 19 \pmod{24}$

Conjecture 2. *$P_{a,b}$ has $\geq$ 2 non-panlindromic irreducible factors in $\mathbb{F}_2[x]$ for $b \geq \frac{a}{4}$, $a \equiv 5, 19 \pmod{24}$*

In other words, $P_{a,b}$ in case 1 for $a \equiv 5, 19 \pmod{24}$ only happens when $b < \frac{a}{4}$. This is an observation result, as we cannot induct the results for higher b. However, we guess from the cyclotomic polynomial, empirically, we should observe some patterns in a, b pair.

In figure 2, we draw out the conjecture 2 by a scatter plot. We can see an empty half triangle for $b \geq \frac{a}{4}$, as those entries is not observed with case 1.

Yet, we failed to find common factors for Case 1 in the graph. The closest observation we have is that they are formed by some cyclotomic polynomials where it's number could have some correlation, such as Φ_p are usually firstly observed in those cases. This is one of the future works we are interested in.

Moreover, we observed that,

Conjecture 3. *Case 3 exists* $\iff a \equiv 1 \pmod 2$ *and* $a \equiv 1, 2 \pmod 3$, $b \equiv 0 \pmod 2$

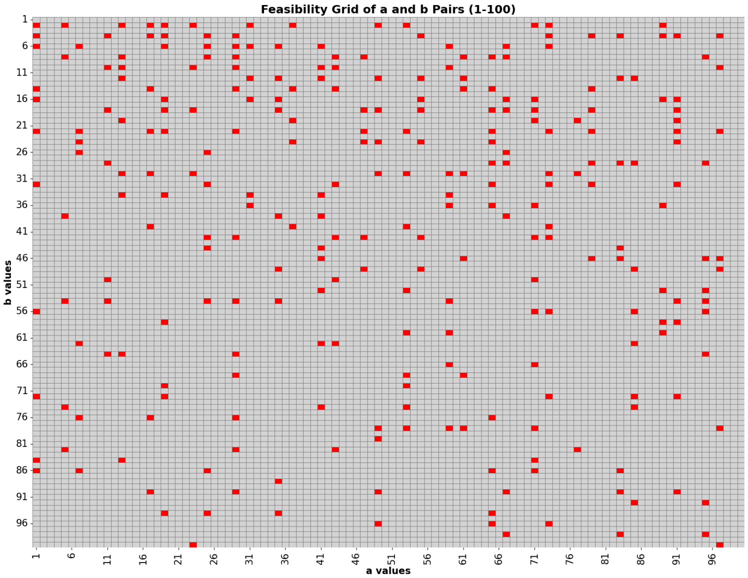

Figure 3: Distribution of Case 3 in Red

The graph also demonstrate such properties where we can clearly see gaps where $a \equiv 0 \pmod 3$ doesn't have any case 3. And we forced the properties of b as well. We should notice that this is the only conjecture in this report that forces both property of a and property of b. The future work could rely on even divide conjecture 3 into

- only one pair of non palindromic factors
- multiple pairs of non palindromic factors

This could future help understand the irreducibility.

Aside, we want to share some difficulties in discuss of field 2. As we try to figure out the cyclotomic polynomials in conjecture 1, we observed no patterns in divisibility in cyclotomic polynomials in field 2. We try to run Φ_p in 2.3 in $\mathbb{F}_2[x]$, where we verified Artin's primitive root conjectures that were stated in 1927 [7]. The Artin constant,

$$A(1) = A = \prod_q \left(1 - \frac{1}{q(q-1)}\right) = 0.373958136192\ldots$$

represents the proportion of irreducible cyclotomic polynomials in the field 2. In our experiment, $S := \{\Phi_p \mid p \text{ is a prime}\}$ and $i := \{\Phi'_p \mid \Phi_p \text{ is irreducible in field 2}\}$, we tested up to 5761455 number of primes, and find $|i| = 2154734$ with an proportion of 0.37399.

Very close to the conjecture.

Since it has been almost 100 years, and the conjecture is open, we will try our best to find pattern and prove it next time.

3 Conclusions and future work

3.1 Conclusion

This project investigated the factorization behavior of the lacunary palindromic polynomial

$$P_{a,b}(x) = x^{4b} - x^{2b} - x^{a} - 2 - x^{-a} - x^{-2b} + x^{-4b}$$

(and its Laurent-cleared version $F_{a,b}(x) = x^{4b} P_{a,b}(x) \in \mathbb{Z}[x]$) motivated by Filaseta's description of trace fields for Dehn fillings of the figure-eight knot complement. Our goal was to identify systematic algebraic structure in $P_{a,b}$ as (a, b) vary, both over $\mathbb{Q}$ and after reduction to $\mathbb{F}_2$.

On the $\mathbb{Q}$-side, we focused on *cyclotomic obstructions* and isolated families of common factors that appear uniformly across large ranges of parameters. The main conceptual mechanism is that cyclotomic divisibility can be decided by evaluating at roots of unity and translating the resulting vanishing conditions into congruences on (a, b). Concretely, we established explicit 2-adic criteria for when $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$ divides the cleared polynomial $Q_{a,b}(x) = x^{4b} P_{a,b}(x)$ (Theorem 1), and we verified a sharp multiplicity criterion for $\Phi_6(x) = x^2 - x + 1$ in the special case $a = 3$, namely

$$(x^2 - x + 1)^2 \mid P_{3,b}(x) \iff 3 \mid b.$$

These results support the broader theme that, while $P_{a,b}$ has a highly sparse shape, its cyclotomic content is governed by rigid congruence patterns (especially 2-adic and mod-3 phenomena).

Beyond provable cyclotomic factors, we made extensive computational tests (primarily in SageMath) that lead to a strong global conjecture over $\mathbb{Q}$: after removing the forced factors $(x + 1)^2$ (for odd a) and, when applicable, $(x^2 - x + 1)$ (for $3 \mid a$), the remaining factor is typically irreducible when $\gcd(a, b) = 1$ (Conjecture 1). While we did not prove this conjecture, it is consistent with Filaseta's "palindromic compression" phenomenon (Theorem 6), which predicts that for fixed odd a and b sufficiently large (with $\gcd(a, b) = 1$), *all* irreducible factors are palindromic. This indicates that, asymptotically in b, rational factorizations should be constrained to cyclotomic factors and palindromic components, strongly limiting the possible shapes of nontrivial decompositions.

On the $\mathbb{F}_2$-side, we introduced a coarse but informative trichotomy based on whether irreducible factors are palindromic or occur in non-palindromic reciprocal pairs. Empirically, the "mixed" regime (both palindromic and non-palindromic factors present) dominates, and we identified two particularly clean patterns:

- a visible "forbidden region" for parameters $a \equiv 5, 19 \pmod{24}$ where Case 1 (having at least two non-palindromic irreducible factors) appears only when $b < \frac{a}{4}$ (Conjecture 2);
- a sharp residue-class characterization of when Case 3 occurs, namely the observed equivalence

$$\text{Case 3 exists} \iff a \equiv 1 \pmod{2},\ a \equiv 1, 2 \pmod{3},\ b \equiv 0 \pmod{2}.$$

These patterns suggest that reduction mod 2 is not merely a computational convenience: it exposes arithmetic constraints (parity and mod-3) that mirror the cyclotomic structure over $\mathbb{Q}$ and may ultimately be explainable by systematic congruences controlling reciprocal symmetry in characteristic 2.

Finally, we note the central practical limitation of our approach: direct factorization becomes computationally expensive as a, b grow (degrees scale like $8b$ after clearing), and exhaustive searches rapidly encounter time and memory bottlenecks. Nevertheless, the combination of (i) provable cyclotomic criteria via roots of unity and (ii) targeted large-scale sampling in $\mathbb{Q}$ and $\mathbb{F}_2$ provides a robust foundation for more theory-driven progress.

3.2 Future work: cyclotomic structure and beyond

There are several concrete directions that appear feasible and mathematically meaningful:

(1) Complete cyclotomic classification over $\mathbb{Q}$. We proved explicit criteria for Φ_{2^k} and analyzed Φ_6 in the $a = 3$ case. A natural next step is to classify *all* cyclotomic factors Φ_n that can divide $Q_{a,b}$ (or $F_{a,b}$) in terms of congruences on (a, b). A systematic approach is:

- Fix n and let ζ be a primitive nth root of unity.
- Evaluate $Q_{a,b}(\zeta)$ and reduce exponents modulo n to obtain an expression depending only on $a \bmod n$ and $b \bmod n$.
- Solve the resulting congruence conditions for vanishing, and then study multiplicity via $Q'_{a,b}(\zeta)$, $Q''_{a,b}(\zeta)$, etc.

This program should recover $(x+1)^2$ for odd a, explain the mod-3 phenomena more generally, and potentially identify "rare" cyclotomic factors that correlate with exceptional Dehn filling slopes.

(2) Using mod-p factorization to obstruct rational reducibility. A standard strategy for proving irreducibility over $\mathbb{Q}$ is to show that the reduction modulo a carefully chosen prime p remains irreducible in $\mathbb{F}_p[x]$. Our current focus on $\mathbb{F}_2$ is conceptually informative, but for proofs one may want to search for primes p where $F_{a,b}(x) \bmod p$ has strong irreducibility behavior (possibly after dividing out forced cyclotomic factors). A promising workflow is:

$$F_{a,b}(x) \in \mathbb{Z}[x] \longrightarrow \overline{F}^{(p)}_{a,b}(x) \in \mathbb{F}_p[x] \longrightarrow \text{irreducibility test in } \mathbb{F}_p[x].$$

If successful for infinitely many (a, b) (or for all $\gcd(a, b) = 1$ in a congruence class of a), this would convert computational evidence into unconditional theorems supporting Conjecture 1.

(3) Explaining the $\mathbb{F}_2$ "forbidden region" via symmetry and cyclotomy. Conjecture 2 suggests a sharp geometric boundary $b = \frac{a}{4}$ in the (a, b)-plane for certain residue classes of a. A principled explanation likely requires understanding how reciprocal pairing behaves in characteristic 2 for a palindromic polynomial with extreme lacunarity. One possible approach is to rewrite $F_{a,b}$ as a specialization $F(x, x^n)$ of a fixed bivariate polynomial (as in the proof of Theorem 6) and then analyze factorization in $\mathbb{F}_2[x]$ using:

- the Frobenius endomorphism $x \mapsto x^2$ and its effect on reciprocal symmetry,
- constraints on degrees of reciprocal pairs and how they must fit within total degree $8b$,
- cyclotomic subfactors over $\mathbb{F}_2$ (where Φ_n may split) and how that changes the "palindromic vs non-palindromic" count.

Even a partial theorem (e.g. a sufficient condition implying nonexistence of Case 1 beyond a linear boundary) would substantially strengthen the current experimental picture.

(4) Connecting factorization patterns to trace field degrees. Since the Dehn filling trace field is generated by $x + x^{-1}$ with x a root of $P_{a,b}$, factorization data for $P_{a,b}$ should translate into predictions for degrees and subfield structure. A useful next deliverable is a dictionary:

$$\text{irreducible factors of } P_{a,b} \quad \Longleftrightarrow \quad \text{subextensions of } \mathbb{Q}(x + x^{-1}),$$

including how palindromic factors constrain the Galois action induced by $x \mapsto x^{-1}$. This would reconnect the arithmetic experiments directly to hyperbolic geometry invariants and could be compared against computations from ideal triangulations as an external consistency check.

(5) Computational improvements and reproducibility. From a practical standpoint, it is worth implementing a more scalable pipeline:

- pre-factor out predicted cyclotomic parts using congruence tests before calling full factorization;
- switch to modular methods (factor mod several primes and lift) when working over $\mathbb{Q}$;
- store results as structured data (e.g. degrees, palindromicity flags, cyclotomic content) rather than full factorizations to reduce memory overhead.

This would enable exploration at significantly larger (a, b) without exceeding time/RAM limits, and would provide more reliable evidence for (or against) the conjectural boundaries reported here.

In summary, our results indicate that the arithmetic of $P_{a,b}$ is governed by a combination of rigid cyclotomic congruence phenomena and more subtle palindromic constraints that become visible both over $\mathbb{Q}$ and in characteristic 2. The most promising path forward is to turn the observed residue-class patterns into theorems by systematically classifying cyclotomic divisibility and using modular irreducibility criteria to control the remaining factor.

References

[1] William P. Thurston. “Three-dimensional manifolds, Kleinian groups and hyperbolic geometry”. In: *Bull. Amer. Math. Soc. (N.S.)* 6.3 (1982), pp. 357–381. DOI: 10.1090/S0273-0979-1982-15003-0.

[2] William P. Thurston. *The Geometry and Topology of Three-Manifolds*. Lecture notes, Princeton University (1978–1980); electronic edition. 1979.

[3] Walter D. Neumann and Don Zagier. “Volumes of hyperbolic three-manifolds”. In: *Topology* 24.3 (1985), pp. 307–332. DOI: 10.1016/0040-9383(85)90004-7.

[4] Michael Filaseta. *On the Factorization of lacunary polynomials*. 2022. arXiv: 2207.11648 [math.NT]. URL: https://arxiv.org/abs/2207.11648.

[5] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.8.beta0)*. https://www.sagemath.org. 2025.

[6] Jim Belk. *Fields and Cyclotomic Polynomials*. Lecture notes. 2025. URL: https://e.math.cornell.edu/people/belk/numbertheory/CyclotomicPolynomials.pdf.

[7] Pieter Moree. *Artin’s primitive root conjecture -a survey* -. 2012. arXiv: math/0412262 [math.NT]. URL: https://arxiv.org/abs/math/0412262.