ABSTRACT

Title of Dissertation: Polynomials with Equal Images over Number Fields

Jordan H Hirsh
Doctor of Philosophy, 2024

Dissertation Directed by: Professor Lawrence C. Washington
Department of Mathematics

Chapman and Ponomarenko [1] characterized when two polynomials $f, g \in \mathbb{Q}[x]$ have the same image $f(\mathbb{Z}) = f(\mathbb{Z})$. We extend this result to rings of integers in number fields. In particular, if K is a finite extension of $\mathbb{Q}$ and $\mathcal{O}$ is the ring of algebraic integers in K, we characterize when polynomials $f, g \in K[x]$ satisfy $f(\mathcal{O}) = g(\mathcal{O})$. As part of our proof, we give a variant of Hilbert's irreducibility theorem.

Polynomials with Equal Images over Number Fields

by

Jordan H Hirsh

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2024

Advisory Committee:
Professor Lawrence C. Washington, Chair/Advisor
Professor Patrick Brosnan
Professor Amin Gholampour
Professor Niranjan Ramachandran
Professor William Gasarch

Acknowledgments

I would like to first thank my father, who's exuberance was always welcome!

I'd then like to thank Ishfaaq, Jerry, Liam, Stavros, Jon, and Andrew for being my good friends here at the math department!

I'd like to thank Jemma, Trystan and Jackie for believing in me and for being great conversationalists. It was always a pleasure!

I'd like to thank John, Alex, Or, and Matt for being great undergrad friends who are excited for me to succeed!

I'd like thank Rich and Neville for being great internet friends and always having something from pop-culture to talk about.

I'd like to thank William Gasarch for teaching me Ramsey Theory (which was very useufl in this paper). And I'd like to thank Amin Gholampour, Patrick Brosnan, and Niranjan Ramachandran for working with me over the course of my eight years at University of Maryland.

And last but certainly not least, I'd like thank Larry Washington for being my advisor and especially putting up with me. I hope you can put up with me on a few projects more.

Table of Contents

Chapter 1: Introduction

Given polynomials $f, g \in \mathbb{Q}[x]$, Chapman and Ponomarenko [1] showed that $f(\mathbb{Z}) = g(\mathbb{Z})$ if and only if one of the following holds:

1. $f(x) = g(x + b)$ for some $b \in \mathbb{Z}$
2. $f(x) = g(-x + b)$ for some $b \in \mathbb{Z}$
3. There is an odd integer k such that $f(x - \frac{k}{2})$ is even, and $g(x) = f(2x + b)$ or $g(x) = f(-2x + b)$ for some $b \in \mathbb{Z}$.

Let $\mathcal{O}$ be the ring of integers in a number field K and let $f(x)$ and $g(x)$ be in $K[x]$. We extend this result to all such $\mathcal{O}$. If we have f, g, we can produce new examples by replacing $g(x)$ with $g(ux + b)$ where u is a unit and $b \in \mathcal{O}$, or by using $f(x) + c$ and $g(x) + c$ for any $c \in K$. Therefore, for ease of exposition, we may assume $f(0) = g(0) = 0$.

Theorem 1.0.1. *Let $f, g \in K[x]$ such that $f(\mathcal{O}) = g(\mathcal{O})$. Normalize f and g so that $f(0) = g(0) = 0$. Then:*

1. $\deg f = \deg g$
2. *If $\deg f > 1$ and there is no unit u such that $f(x) = g(ux)$ then there are two possibilities:*

(a) There exists a prime power $p^h \geq 2$ *dividing* $\deg f$ *with* $\zeta_{p^h} \in \mathcal{O}$ *and there exist* $\beta, c \in K$ *such that* $f(x)$ *is a polynomial in* $(x + \frac{c}{1-\zeta_{p^h}})^{p^h}$ *and* $g(x) = f(\beta x)$

(b) or in a special case where $p = 2$ *and* $f(x)$ *is a polynomial in* $(x + \frac{c}{1-\zeta_{2^h}})^{2^h}$ *and* $g(x) = f(\beta^2 x)$.

Here ζ_p *denotes a primitive* p*th root of unity.*

3. *In case (a), there are primes* $\mathcal{P}_1, \mathcal{P}_2$ *dividing* p *such that the prime ideal factorization of* (β) *is* $\mathcal{P}_1^{\delta_1}\mathcal{P}_2^{-\delta_2}$ *where* $\delta_i \in \{0, 1\}$, $v_{\mathcal{P}_1}(c) = 0$, $v_{\mathcal{P}_2}(c) = -\delta_2$, *and the norms of* $\mathcal{P}_1$ *and* $\mathcal{P}_2$ *are* p.

   In case (b), there are primes $\mathcal{P}_1, \mathcal{P}_2$ *dividing* 2 *such that the prime ideal factorization of* (β) *is* $\mathcal{P}_1^{\delta_1}\mathcal{P}_2^{-\delta_2}$ *where* $\delta_i \in \{0, 1, 2\}$, $v_{\mathcal{P}_1}(c) = 0$, $v_{\mathcal{P}_2}(c) = -\delta_2$, *and the norms of* $\mathcal{P}_1$ *and* $\mathcal{P}_2$ *are* p.

It will be clear from the proof that, up to specifying the possible values of c, this gives a complete classification of possible pairs of polynomials f, g such that $f(\mathcal{O}) = g(\mathcal{O})$.

Remark: If we reverse the roles of f, g we get that $f(x) = g(\frac{1}{\beta}x)$ and $g(x)$ is a polynomial in $(x + \frac{c}{\beta(1-\zeta_{p^h})})^{p^h}$. Note that $v_{\mathcal{P}_2}(c/\beta) = 0$ and $v_{\mathcal{P}_1}(c/\beta) = -\delta_1$. So the theorem in a sense is symmetric in f, g.

This problem is similar to but distinct from the problem of characterizing polynomials that map $\mathcal{O}$ to $\mathcal{O}$. These are explored in depth in [2].

We start our proof using a modification of Hilbert's irreducibility for linear factors instead of just general factorization. We use the fact that we can always get a linear factor to state $f(x) = \sum_j d_j(x + \frac{c}{1-\zeta_{p^h}})^{jp^h}$ where $d_j \in \mathcal{O}$. Then the remainder of the proof is an analysis of the possible numerators and denominators of the coefficients of linear factors.

Chapter 2: A Variant on Hilbert Irreducibility

The classical Hilbert Irreducibility Theorem [3] states that if sufficiently many specializations of a polynomial are reducible than the polynomial itself is reducible. We need a variant of this that yields linear factors. This can be deduced inductively from various forms of the theorem [4]. We choose to give a proof based on Ramsey theory, following the proof of Hilbert Irreducibility given in [5].

Theorem 2.0.1. *Let $\mathcal{O}$ be the ring of integers of a finite extension K of $\mathbb{Q}$. Let $F(x,y) \in \mathcal{O}[x,y]$ and suppose for all sufficiently large $b \in \mathbb{Z}$ there exists $a \in \mathcal{O}$ such that $F(a,b) = 0$. Then $F(x,y)$ has a factor of the form $x - h(y)$ for some $h(y) \in K[y]$.*

Proof. First we normalize. We say $F(x,y) = \sum_{i=0}^{n} g_i(y)x^i$. Then we can define $\tilde{F}(x,y) = F(x,y)/g_n(y)$. We may now assume $F(x,y)$ is a monic polynomial in x with rational function coefficients in y.

Let L be the Galois closure of $K/\mathbb{Q}$ and let $G = \mathrm{Gal}(L/\mathbb{Q})$. For each $\sigma \in G$ let F^σ be the result of applying σ to each of the coefficients of F. By Puiseux's theorem [6, section 14],

$$F^\sigma(x,y) = \prod_i (x - f_{\sigma,i}(y))$$

where $f_{\sigma,i}$ is a Puiseux series of the form $\sum_{-\infty}^{N} b_j y^{j/k}$ for some k. We can replace k by the lcm

of the values of k for all the possible σ's and i's and use that k for all of the possible $f_{\sigma,i}$. These all converge for $|y|$ sufficiently large.

For $\sigma = 1$ we have

$$F(x, y) = \prod_i (x - f_i(y)),$$

Let $y = n^k$ where $n \in \mathbb{Z}$ is sufficiently large. By hypothesis, we know there exists $a \in \mathcal{O}$ such that $F(a, n^k) = 0$. This implies that for each such n we may choose i_n such that $F(f_{i_n}(n^k), n^k) = 0$ and $f_{i_n}(n^k) \in \mathcal{O}$.

Let $\sigma \in G$. Then

$$F^\sigma \left(\sigma \left(f_{i_n}(n^k)\right), n^k\right) = 0,$$

so

$$\sigma(f_{i_n}(n^k)) = f_{\sigma,i_{\sigma,n}}(n^k)$$

for some $i_{\sigma,n}$. We can choose $i_{\sigma,n} = i_n$ when $\sigma = 1$.

We assign to n the color $(i_n, \ldots, i_{\sigma,n}, \ldots)_{(\sigma \in G)}$. There are only finitely many possible colors, so we have colored all sufficiently large natural numbers with a finite coloring. The cube lemma states the following:

Lemma 2.0.2. *Given a finite coloring of the integers and a number m, there exists $\mu_1, \ldots, \mu_m$ such that for infinitely many integers γ all numbers of the form $\gamma + \sum_{i=1}^m \epsilon_i \mu_i$ where $\epsilon_i = 0$ or 1 are the same color.*

Proof. For a proof see [5]. □

Using the cube lemma, we have that there exist sufficiently large n such that $\{n + \sum \epsilon_i \mu_i | \epsilon_i \in$

$\{0,1\}\}$ are colored the same. This means there are i_1 and i_σ independent of n such that

$$\sigma(f_{i_1}((n+\sum_i \epsilon_i\mu_i)^k)) = f_{\sigma,i_\sigma}((n+\sum_i \epsilon_i\mu_i)^k)$$

for a sequence of sufficiently large n and $f_{i_1}((n+\sum_i \epsilon_i\mu_i)^k)$ is in $\mathcal{O}$.

We can write

$$f_{\sigma,i_\sigma}(n^k) = g_{\sigma,i_\sigma}(n) = p_{\sigma,i_\sigma}(n) + \ell_{\sigma,i_\sigma}(n),$$

where $p_{\sigma,i_\sigma}(z) \in \mathbb{C}[z]$ and $\ell_{\sigma,i_\sigma}(z) \in \mathbb{C}[[1/z]]$ with no constant term. Because there are only finitely many choices for p_{σ,i_σ} we may assume that m is larger than the degree of all such choices. Because the Puiseux series has a positive radius of convergence, there exists N such that for all $|\ell(n)| < \epsilon$ for all $n \geq N$.

For a function $h(x)$ define $\Delta_i h(x) = h(x+\mu_i) - h(x)$. Consider

$$\Delta_1\Delta_2\cdots\Delta_m g_{\sigma,i_\sigma}(n) = \Delta_1\Delta_2\cdots\Delta_m p_{\sigma,i_\sigma}(n) + \Delta_1\Delta_2\cdots\Delta_m \ell_{\sigma,i_\sigma}(n).$$

Because $m > \deg p_{\sigma,i_\sigma}$, the general theory of finite differences implies that

$$\Delta_1\Delta_2\cdots\Delta_m p_{\sigma,i_\sigma}(z) = 0.$$

It is easy to show that

$$|\Delta_1\Delta_2\cdots\Delta_m g_{\sigma,i_\sigma}(n)| = |\Delta_1\Delta_2\cdots\Delta_m \ell_{\sigma,i_\sigma}(n)| < 2^m\epsilon$$

when $n \geq N$. Because of our coloring choice,

$$\sigma\left(\Delta_1 \Delta_2 \cdots \Delta_m g_{i_1}(n)\right) = \Delta_1 \Delta_2 \cdots \Delta_m g_{\sigma, i_\sigma}(n)$$

and these are algebraic integers. Therefore, when ϵ is sufficiently small, $\Delta_1 \Delta_2 \cdots \Delta_m g_{\sigma, i_\sigma}(n)$ is an algebraic integer whose conjugates all have absolute value less than 1 and thus their product is 0. We conclude that

$$\Delta_1 \Delta_2 \cdots \Delta_m g_{i_1}(n) = 0$$

for a sequence of $n \to \infty$.

Since g is an analytic function in $1/n$, this means that

$$\Delta_1 \Delta_2 \cdots \Delta_m g_{i_1}(z) = 0$$

for all sufficiently large z.

We now work backwards by induction. Suppose we have that

$$\Delta_a \Delta_{a+1} \cdots \Delta_m g_{i_1}(z)$$

a polynomial $P_a(z)$ of degree $\leq a - 2$. We can write

$$P_a(n) = P_{a+1}(n + \mu_a) - P_{a+1}(n)$$

for some polynomial $P_{a+1}(n)$ of degree $\leq a-1$. Then

$$\Delta_a \left(\Delta_{a+1} \cdots \Delta_m g_{i_1}(n) - P_{a+1}\right)(n) = 0$$

for a sequence of $n \to \infty$. By the above the reasoning,

$$\Delta_{a+1} \cdots \Delta_m g_{i_1}(z) = P_{a+1}(z).$$

By induction, $g_{i_1}(z)$ is a polynomial.

We have now shown that $F(x,y)$ has a factor $x - f_{i_1}(y)$ where $f_{i_1}(y)$ is a polynomial of degree d in $y^{1/k}$ with $f_i(m^k) \in \mathcal{O}$ for infinitely many m. Take $d+1$ distinct integers m_i with $f(m_i^k) \in \mathcal{O}$. We have

$$f_{i,\sigma}(m_j^k) = C_d m_j^d + \ldots + C_1 m_j + C_0$$

is an element of $\mathcal{O}$. This yields

$$\begin{bmatrix} 1 & m_0 & \ldots & m_0^d \\ 1 & m_1 & \ldots & m_1^d \\ \vdots & \ddots & \ldots & \vdots \\ 1 & m_d & \ldots & m_d^d \end{bmatrix} \begin{bmatrix} C_0 \\ C_1 \\ \vdots \\ C_d \end{bmatrix} = \begin{bmatrix} f_{i,\sigma}(m_0) \\ f_{i,\sigma}(m_1) \\ \vdots \\ f_{i,\sigma}(m_d) \end{bmatrix}.$$

The first matrix is a Vandermonde matrix with determinant

$$\prod_{0 \leq j < k \leq d} (m_k - m_j).$$

Since the m_j's are distinct, the determinant is non-zero, which means the Vandermonde matrix is invertible. Since all the $f_{i,\sigma}(m_j)$ are in $\mathcal{O}$, the C_j's must be in K.

We have shown that if $F(x, y)$ is such that for each sufficiently large $y \in \mathbb{Z}$, there exists an x such that $F(x, y) = 0$ then there exists a polynomial $g(x) \in K[x]$ such that $x - g(y^{1/k})$ is a factor of $F(x, y)$. We want to show that there are no fractional powers. To do so we will apply what we've shown to modifications of $F(x, y)$.

Let p be a prime in $\mathbb{Z}$ and consider $G(x, y) = F(x, py)$. Since $G(x, y)$ satisfies the conditions we put on $F(x, y)$, there must be an $h_p \in K[x]$ such that $x - h_p(y^{1/\ell_p})$ is a factor of $G(x, y)$. Thus $x - h_p((y/p)^{1/\ell_p})$ is one of the Puiseux factors of $F(x, y)$ (not necessarily $x - g(y^{1/k})$). If $F(x, y)$ is of degree b in x, there are at most b possible such factors. So we choose $b + 1$ unramified primes and by the pigeonhole principle, there are p_1 and p_2 such that h_{p_1} and h_{p_2} correspond to the same Puiseux factor. Thererfore,

$$h_{p_1}((y/p_1)^{1/\ell_1}) = h_{p_2}((y/p_2)^{1/\ell_2}).$$

Let $h_{p_1}(x) = \sum_i a_i x^i$ and $h_{p_2}(x) = \sum_j b_j x^j$. From the above, we know the coefficients of h_{p_1} and h_{p_2} are in K. Suppose a_i is non-zero for some i such that $i/\ell_1 \notin \mathbb{Z}$. Then there exists b_j such that

$$a_i(y/p_1)^{i/\ell_1} = b_j(y/p_2)^{j/\ell_2}.$$

Therefore $i/\ell_1 = j/\ell_2$ and

$$\left(\frac{p_2}{p_1}\right)^{i/\ell_1} = \frac{b_j}{a_i} \in K.$$

Since each p_j is unramified, we have a factorization $p_1\mathcal{O} = P_1P_2 \dots P_g$ into distinct prime ideals.

But a fractional power of P_1 cannot appear in the prime factorization of b_j/a_i. So the non-integral power coefficients must be 0. Therefore $h_{p_1}((y/p_1)^{1/\ell_1}) = h_1(y/p_1)$ for some $h_1 \in K[x]$. Therefore, $x - h_1(y/p_1)$ is a Puiseux factor of $F(x, y)$. This completes the proof of Theorem 2.0.1. □

Chapter 3: A Tale of Two Polynomials

Let $f(x)$ and $g(x)$ be polynomials in $K[x]$ such that

$$f(\mathcal{O}) = g(\mathcal{O}).$$

In other words, for every $x \in \mathcal{O}$ there exists a $y \in \mathcal{O}$ such that $f(x) = g(y)$ and vice-versa.

Lemma 3.0.1. $\deg f = \deg g$ *and they differ by a linear change of variables.*

Proof. By Theorem 2.0.1, $f(x) - g(y)$ has a factor $(x - k(y))$. This means $f(k(y)) = g(y)$. So deg $f \leq$ deg g. The opposite direction yields deg $f \geq$ deg g and thus the degrees are equal and deg $k = 1$. □

From now on we'll let $n = \deg f = \deg g$.

A linear factor of $f(x) - g(y)$ must be of the form $ax - by + c$ where $a, b \neq 0$. Otherwise, $f(x)$ would contain y or $g(y)$ would contain x. Therefore we can put all linear factors into the form $x - by + c$. Write $f(x) - g(y) = h(x, y) \prod_i (x - b_i y + c_i)$ where $h(x, y)$ has no linear factors in $K[x, y]$. Suppose $c_i \notin \mathcal{O}$ for all i. Choose $t \in \mathcal{O}$ so that $tb_i \in \mathcal{O}$ for all i. Then $\prod_i (x - b_i ty + c_i) \neq 0$ when $x, y \in \mathcal{O}$. Therefore there exists an x such that $h(x, ty) = 0$. This happens for all y so by Theorem 2.0.1, $h(x, ty)$ has a linear factor, so $h(x, y)$ has a linear factor. This is a contradiction, so $c_i \in \mathcal{O}$ for some i. Therefore we can translate x by c_i, which is in $\mathcal{O}$,

and assume some $c_i = 0$.

Henceforth we will assume $x - \beta y$ is a factor of $f(x) - g(y)$.

Lemma 3.0.2. *There exists an $m|n$ (recall n is the degree of f) and $c \in \mathcal{O}$ such that every linear factor (up to a multiplicative constant) of $f(x) - g(y)$ has the form $l(x, y) = x - \beta\zeta_m^i y + c\frac{1-\zeta_m^i}{1-\zeta_m}$, where ζ_m is a primitive mth root of unity, and each such linear factor with $0 \leq i < m$ appears in the factorization of $f(x) - g(y)$. If $m = 1$ we let $c = 0$ and omit the c term. We can write $f(x) = \sum d_j(x + \frac{c}{1-\zeta_m})^{jm}$ and $g(y) = \sum d_j(\beta y + \frac{c}{1-\zeta_m})^{jm}$ for some coefficients d_j.*

Proof. Since $f(x)$ and $g(y)$ have the same degree $f(x) - g(y)$ has the form $\alpha(x^n - \gamma y^n + \ldots)$. The fact that $x - \beta y$ is a factor implies that $\gamma = \beta^n$. Suppose we have a linear factor $ux + vy + w$. Then

$$f\left(\frac{-vy - w}{u}\right) = g(y) = f\left(\beta y\right).$$

Comparing highest terms yields $(-v/u)^n = (\beta)^n$. So every linear factor must be of the form $x - \beta\zeta_m y + c$. We need to evaluate c.

Note that we have also proved that if there is more than one linear factor then the factors must be distinct and if we have r linear factors in $K[x, y]$, there are at least r distinct roots of unity in $\mathcal{O}$.

Suppose we have two factors, $x - \beta y$ and $x - \beta\zeta_m y + c$. Then

$$f\left(\beta y\right) = g(y) = f\left(\beta\zeta_m y - c\right).$$

From this we have that $f(x) = f(\zeta_m x - c)$. So $f(x)$ is invariant under an affine transformation and we want to find the fixed point. So we solve $x = \zeta_m x - c$ for x and obtain $x = \frac{c}{\zeta_m - 1}$. We

now have that $f(x - \frac{c}{1-\zeta_m}) = f(\zeta x - \frac{c}{1-\zeta_m})$. If we take $h(x) = f(x - \frac{c}{1-\zeta_m})$ then we have $h(x) = h(\zeta_m x)$. Therefore, $h(x)$ has the form $\sum d_j x^{jm}$ and thus

$$f(x) = \sum d_j (x + \frac{c}{1-\zeta_m})^{jm} \text{ and } g(y) = \sum d_j (\beta y + \frac{c}{1-\zeta_m})^{jm}.$$

Therefore $f(x) - g(y)$ has the factor $(x + \frac{c}{1-\zeta_m})^m - (\beta y + \frac{c}{1-\zeta_m})^m$, which factors into the linear factors $x - \beta\zeta_m^i y + c\frac{1-\zeta_m^i}{1-\zeta_m}$ for $0 \leq i < m$. □

So we now have not only the structure of f and g but also the structure of their factors. We also have if there is more than one factor then $\zeta_m \in \mathcal{O}$ for some $m > 1$ and $m|n$. We want to show that there is a maximal such m.

Lemma 3.0.3. *Suppose f can be written in the form of Lemma 3.0.2 with $m = m_1$ and with $m = m_2$. Then $f(x)$ must be a polynomial of the form $f(x) = \sum d_j''(x + \frac{c}{1-\zeta_{m_3}})^{jm_3}$ where $m_3 = \operatorname{lcm}(m_1, m_2)$.*

Proof. The case $m_2 = 1$ is trivial so without loss of generality assume $1 < m_2 < m_1$. We have

$$f(x) = \sum d_j (x + \frac{c_1}{1-\zeta_{m_1}})^{jm_1} = \sum d_k' (x + \frac{c_2}{1-\zeta_{m_2}})^{km_2}.$$

If we shift by $\frac{c_1}{1-\zeta_{m_1}}$ we get

$$f(x - \frac{c_1}{1-\zeta_{m_1}}) = \sum d_j x^{jm_1} = \sum d_k' (x + \frac{c_2}{1-\zeta_{m_2}} - \frac{c_1}{1-\zeta_{m_1}})^{km_2}.$$

If $\frac{c_2}{1-\zeta_{m_2}} - \frac{c_1}{1-\zeta_{m_1}} \neq 0$, the coefficient of the x^{km_2-1} on the right will be non-zero while the coefficient of x^{jm_1-1} will be zero. If the above difference does equal 0, we have a polynomial in

x^{m_1} that is also a polynomial in x^{m_2} so it must be a polynomial in x^{m_3}. □

As in the previous lemma this gives us m_3 linear factors for $f(x) - g(y)$. Write

$$f(x) - g(y) = h(x, y) \prod (x - \beta\zeta_m^i y + c\frac{1 - \zeta_m^i}{1 - \zeta_m}) \tag{3.1}$$

where $h(x, y)$ has no linear factors and ζ_m is an element of K. The integer m is uniquely determined from the above lemma.

Lemma 3.0.4. *Let notation be as in Equation (3.1). For every $y \in \mathcal{O}$ there exists an $x \in \mathcal{O}$ and an i such that $x = \beta\zeta_m^i y - c\frac{1-\zeta_m^i}{1-\zeta_m}$.*

Proof. Fix y and suppose there isn't such an x. Choose $0 \neq D \in \mathcal{O}$ such that $D\beta \in \mathcal{O}$. Let $y_1 = y + Dt$ where $t \in \mathcal{O}$.

Let $x_i = \beta\zeta_m^i y_1 - c\frac{1-\zeta_m^i}{1-\zeta_m}$. If $x_i \in \mathcal{O}$ for some i then $x = x_i - D\beta\zeta_m^i t$ is in $\mathcal{O}$ and therefore

$$\beta\zeta_m^i y - c\frac{1 - \zeta_m^i}{1 - \zeta_m} = \beta\zeta_m^i(y_1 - Dt) - c\frac{1 - \zeta_m^i}{1 - \zeta_m} = x \in \mathcal{O}.$$

This is a contradiction. So for each such y_1 no linear factor can provide the required $x_i \in \mathcal{O}$.

Therefore for each such y_1 there must be $x \in \mathcal{O}$ such that $h(x, y_1) = 0$. Let $H(x, t) = h(x, y + Dt)$. For each t there exists x such that $H(x, t) = 0$. By Theorem 2.0.1 there must a linear factor, but this is a contradiction since $h(x, y)$ has no linear factors. So for each y there must exist an x as in the statement of the lemma. □

Proposition 3.0.5. *There exists a prime p dividing n such that*

$$(1 - \zeta_p)\beta \text{ is in } \mathcal{O}.$$

If $\beta \notin \mathcal{O}$, then $\zeta_p \in \mathcal{O}$.

Proof. Let m be the maximum number of linear factors of $f(x) - g(y)$. These factors are of the form $x - \beta\zeta_m^i y + c\frac{1-\zeta_m^i}{1-\zeta_m}$. The previous lemma implies that for every $y = \zeta_m^j$ there must be an x coming from one of these linear factors. Suppose x comes from $x - \beta y$, then $x = \beta\zeta_m^j$. Since $x \in \mathcal{O}$, we have $\beta \in \mathcal{O}$ and trivially $(1 - \zeta_p)\beta$ is in $\mathcal{O}$ for every choice of p.

Now assume $\beta \notin \mathcal{O}$. There are m roots of unity and the $i = 0$ in Lemma 3.0.4 can never supply the x, so there are at most $m - 1$ linear factors remaining. We now have i, j, k such that $y = \zeta_m^j$ and $y = \zeta_m^k$ use the ith factor to produce their values of x and therefore

$$x_j = \beta\zeta_m^{i+j} + c\frac{1-\zeta_m^i}{1-\zeta_m} \quad \text{and} \quad x_k = \beta\zeta_m^{i+k} + c\frac{1-\zeta_m^i}{1-\zeta_m}$$

are both in $\mathcal{O}$. Therefore $x_j - x_k = \beta\zeta_m^i(\zeta_m^j - \zeta_m^k)$, which means $\beta(1 - \zeta_m^{j-k})$ is in $\mathcal{O}$. If ζ_m^{j-k} is not a prime power root of unity then $(1 - \zeta_m^{j-k})$ is a unit [7, Proposition 2.8] so $\beta \in \mathcal{O}$, which is assumed not to be true for the present case. Therefore $\zeta_m^{j-k} = \zeta_{p^h}$ for some p^h. Since $(1 - \zeta_{p^h})$ divides $(1 - \zeta_p)$ this means $\beta(1 - \zeta_p)$ is integral. □

Chapter 4: The Denominators' Names

In this section we use the assumption that for every $y \in \mathcal{O}$ there exists an $x \in \mathcal{O}$ such that $f(x) = g(y)$ in order to analyze the denominators of β and c in the factors $x - \beta\zeta_m^i y + c\frac{1-\zeta_m^i}{1-\zeta_m}$. By Lemma 3.0.4 one of these factors must give the desired x.

If $\beta \in \mathcal{O}$ then the $i = 0$ factor suffices, so we now assume that $\beta \notin \mathcal{O}$. By Lemma 3.0.5 the only prime factors of the denominator are primes dividing p.

Let $\mathcal{P}$ be a prime ideal of $\mathcal{O}$ in the denominator of β. Let $\mathcal{O}_\mathcal{P}$ be the localization and let π be a uniformizer. Let π^k be the exact power of π in the denominator of β and let π^ℓ be the exact power of π in the denominator of c:

$$v_\mathcal{P}(\beta) = -k < 0, \qquad v_\mathcal{P}(c) = -\ell.$$

Consider the factors

$$x - \zeta_m^i \beta y + c\left(\frac{1-\zeta_m^i}{1-\zeta_m}\right) = x - \zeta_m^i \beta y + c_i$$

By Lemma 3.0.4 for every y there exists an i such that

$$\zeta_m^i \beta y - c_i \in \mathcal{O} \subset \mathcal{O}_\mathcal{P}.$$

Multiply by $\pi^k \zeta_m^{-i}$ to obtain

$$\pi^k \beta y \equiv \pi^k \zeta_m^{-i} c_i = \pi^k c \frac{\zeta_m^{-i} - 1}{1 - \zeta_m} \bmod \pi^k \mathcal{O}_{\mathcal{P}}.$$

Let

$$c_i' = \pi^\ell c \frac{\zeta_m^{-i} - 1}{1 - \zeta_m}$$

and note that $\pi^\ell c$ is a unit. We need

$$\pi^k \beta y \equiv \pi^{k-\ell} c_i' \bmod \pi^k \mathcal{O}_{\mathcal{P}}.$$

Note that $\pi^k \beta$ is a unit in $\mathcal{O}_{\mathcal{P}}$. Therefore $\pi^k \beta y$ runs through all $N(\mathcal{P})^k$ integral congruence classes mod $\pi^k \mathcal{O}_{\mathcal{P}}$ as y takes all the values in $\mathcal{O}$ mod $\pi^k \mathcal{O}$. Therefore as i varies, $\pi^{k-\ell} c_i'$ has to run through at least $N(\mathcal{P})^k$ congruence classes mod π^k.

We now consider three cases: $\ell < k$, $\ell > k$, $\ell = k$.

4.1 $\ell < k$

If $\ell < k$ then $\pi^{k-\ell} c_i' \equiv 0 \mod \pi$, which means $\pi^{k-\ell} c_i'$ does not yield the non-zero congruence classes. Therefore $\ell \geq k$.

4.2 $\ell > k$

We need the following lemma.

Lemma 4.2.1. *Let v be the valuation of $\mathbb{Z}[\zeta_{p^h}]$ for the prime ideal $(1 - \zeta_{p^h})$ normalized by*

$v(1-\zeta_{p^h})=1$ *and let* v_p *be the usual* p*-adic valuation on* $\mathbb{Z}$*. If* $p^h \nmid i$ *then*

$$v(1-\zeta_{p^h}^i) = p^{v_p(i)}.$$

Proof. This follows easily from the equality of ideals $(1-\zeta_{p^h})^{p^s} = (1-\zeta_{p^{h-s}})$ when $s<h$. □

We need the integral values of $\pi^{k-\ell}c_i'$ to run through the $N(\mathcal{P})^k$ congruence classes mod π^k. The case $i=0$ takes care of the zero congruence class, so we assume $i \not\equiv 0 \bmod m$. Since $\ell > k$ we must have $v_{\mathcal{P}}(\zeta_m^{-i}-1) \geq \ell - k > 0$ so we must have ζ_m^i is a p-power root of unity. Write $m = p^h m_1$ with $p \nmid m_1$. We must have $m_1 | i$ so we write $i = m_1 i_1$ and $\zeta_m^i = \zeta_{p^h}^{i_1}$. Set $v_{\mathcal{P}}(1-\zeta_{p^h}) = M$. We need

$$Mp^{v_p(i)} = Mp^{v_p(i_1)} = v_{\mathcal{P}}(\zeta_{p^h}^{-i_1}-1) \geq \ell - k + v_{\mathcal{P}}(1-\zeta_m). \tag{4.1}$$

We want to see how many congruence classes mod π^k are represented by $\pi^{k-\ell}c_i'$. Suppose $j = j_1 m_1$ and

$$Mp^{v_p(i-j)} \geq v_{\mathcal{P}}(1-\zeta_m) + \ell. \tag{4.2}$$

This is equivalent to $\zeta_m^{i-j} - 1 \equiv 0 \mod (1-\zeta_m)\pi^\ell$, which implies

$$\pi^{k-\ell}c_i' \equiv \pi^{k-\ell}c_j' \mod \pi^k.$$

We need to count how many indices i satisfy (4.1) and such that no pair of distinct indices i, j satisfy (4.2). The condition (4.1) yields integrality and condition (4.2) guarantees the $\pi^{k-\ell}c_i'$'s are distinct mod π^k.

Lemma 4.2.2. *Let $0 \le A < B$ be real numbers. Let S be a set of integers such that $v_p(i) \ge A$ for all $i \in S$ and if $i, j \in S$ with $i \ne j$ then $v_p(i-j) < B$. Then the number of elements in S is at most $p^{\lceil B \rceil - \lceil A \rceil}$.*

Proof. The elements of S must be distinct mod $p^{\lceil B \rceil}$ and they must be multiples of $p^{\lceil A \rceil}$. There are $p^{\lceil B \rceil - \lceil A \rceil}$ such residue classes mod $p^{\lceil B \rceil}$. □

First assume ζ is not a p-power root of unity. Then $v_{\mathcal{P}}(1-\zeta_m) = 0$ since it is a unit. From (4.1) and (4.2), and Lemma 4.2.2, the number of i_1's that satisfy the inequalities is

$$p^{\lceil \log_p(\frac{\ell}{M}) \rceil - \lceil \log_p(\frac{\ell-k}{M}) \rceil}.$$

Because we have to represent all classes mod π^k (that is, mod $\mathcal{P}^k$) we must have

$$p^{\lceil \log_p(\frac{\ell}{M}) \rceil - \lceil \log_p(\frac{\ell-k}{M}) \rceil} \ge N(\mathcal{P})^k = p^{\nu k} \tag{4.3}$$

where

$$N(\mathcal{P}) = p^{\nu}.$$

So we have $\nu k \le \lceil \log_p(\frac{\ell}{M}) \rceil - \lceil \log_p(\frac{\ell-k}{M}) \rceil$ which implies $\nu k \le 1 + \log_p(\frac{\ell}{\ell-k})$ hence $p^{\nu k - 1} \le \frac{\ell}{\ell-k}$. Solving, we get $\ell \le \frac{k p^{\nu k-1}}{p^{\nu k-1}-1}$. Since $\ell > k$ we then have $k+1 \le \frac{k p^{\nu k-1}}{p^{\nu k-1}-1}$ which reduces to $p^{\nu k-1} \le k+1$. When $p \ge 5$ only $k=1$ and $\nu = 1$ works. When $p = 3$, we obtain $\nu = 1$ and $k \le 2$. When $p = 2$, we get only the following possibilities: $(\nu, k) = (1,1), (1,2), (1,3), (2,1)$.

If $p = 3$ and $k = 2$ then equations (4.1) and (4.2) say $M 3^{v_3(i)} \ge \ell - 2$ and $\ell > M 3^{v_3(i-j)}$. Since $1 < \frac{\ell}{\ell-2} \le 3$, we see that $v_p(i)$ and $v_p(i-j)$ take on the same unique value (or ∞), so we

can have only 3 values of i. But we need at least $N(\pi)^k$ values of i and $N(\pi)^k \geq 9$. Thus $p = 3$ and $k = 2$ does not work.

If $p = 2$ and $k = 3$ then our conditions become $\ell > M2^{v_2(i_1-j_1)}$ and $M2^{v_2(i_1)} \geq \ell - 3$. When $\ell \geq 4$ this determines at most four residue classes, but we need at least $2^k = 8$. So $p = 2$ and $k = 3$ does not work.

If $p = 2$ and $k = 2$ then our conditions become $\ell > M2^{v_2(i_1-j_1)}$ and $M2^{v_2(i_1)} \geq \ell - 2$. When $\ell \geq 4$ this determines only two residue classes, but we need at least $2^k = 4$. The case $(\nu, k, \ell) = (1, 2, 3)$ remains and we will eliminate this case later.

If $p = 2$ and $(\nu, k) = (2, 1)$ then our conditions become $\ell > M2^{v_2(i_1-j_1)}$ and $M2^{v_2(i_1)} \geq \ell - 1$. When $\ell \geq 2$ this determines at most two residue classes, but we need at least $2^{\nu k} = 4$.

To summarize, we have proved if $\ell > k$ and ζ is a non-p-power root of unity then $\nu = 1$. When $p \geq 3$, we have $k = 1$. When $p = 2$, the possibilities are $k = 1, 2$.

Now assume ζ is a p-power root of unity. Then the number of indices i's is

$$p^{\lceil \log_p(1+\frac{\ell}{M})\rceil - \lceil \log_p(1+\frac{\ell-k}{M})\rceil}.$$

The number of i's must be $\geq N(\pi)^k = p^{\nu k}$, so we have

$$\nu k \leq \lceil \log_p(1 + \frac{\ell}{M})\rceil - \lceil \log_p(1 + \frac{\ell - k}{M})\rceil.$$

This implies $\nu k \leq \log_p(\frac{M+\ell}{M+\ell-k}) + 1$ which means $p^{\nu k-1} \leq \frac{M+\ell}{M+\ell-k}$. Solving, we get $M + \ell \leq \frac{kp^{\nu k-1}}{p^{\nu k-1}-1}$. Since $M \geq 1$ and $\ell \geq k + 1$ we have $k + 2 \leq \frac{kp^{\nu k-1}}{p^{\nu k-1}-1}$ hence $p^{\nu k-1} \leq \frac{k}{2} + 1$. If $k \geq 3$ then this is impossible for all p. If $k \geq 2$ it's impossible for all $p \geq 3$. When $1 \leq k \leq 2$ we must

have $\nu = 1$ for all p.

To summarize, we have proved if $l > k$ and ζ is a p-power root of unity then $\nu = 1$. When $p \geq 3$, we have $k = 1$. When $p = 2$, the possibilities are $k = 1, 2$.

Now we determine all the possible values of ℓ.

When $k = 1$ we have $v_{\mathcal{P}}(1-\zeta_m) + \ell > Mp^{v_p(i-j)}$ and $Mp^{v_p(i)} \geq v_{\mathcal{P}}(1-\zeta_m) + \ell - 1$ with $M = v_{\mathcal{P}}(1-\zeta_{p^h})$. These bounds differ by 1 so we must have equality at the lower bound. If m is not a power of p then we must have $\ell = 1 + Mp^v$ for some $v \geq 0$. If m is a power of p then $\ell = 1 + M(p^v - 1)$ for some $v \geq 0$.

When $k = 2$ then $p = 2$ and we have $v_{\mathcal{P}}(1-\zeta_m) + \ell > M2^{v_2(i-j)}$ and $M2^{v_2(i)} \geq v_{\mathcal{P}}(1-\zeta_m) + \ell - 2$. If $l \geq 4 - v_{\mathcal{P}}(1-\zeta_m)$ then we have only two possibilities for i that work but we need four.

The only case that remains is $l = 3$ and m is not a power of 2. From before, $\nu = 1$, that is $N(\mathcal{P}) = 2$. If $m = 2^h m_1$ then the m_1th roots of unity are distinct mod p, so $N(\mathcal{P}) \equiv 1 \bmod m_1$. It follows that $m_1 = 1$ and m is a power of 2 so this case cannot happen.

To summarize when $\ell > k$ we have shown that $k = 1$ and $\nu = 1$ for all primes and the values of ℓ are limited.

We will now show that these cases of $\ell > k$ are in fact just cases of $\ell = k$ in disguise. Let's consider the case where $m = p^h$. We must have $\ell = 1 + M(p^v - 1)$ where $v = v_p(i)$, so we can write $i = p^v i_2$. Our c_i can be written as

$$\frac{c'}{\pi^\ell}\frac{1-\zeta_{p^h}^i}{1-\zeta_{p^h}} = \frac{c'}{\pi}\frac{1-\zeta_{p^{h-v}}}{\pi^{\ell-1}(1-\zeta_{p^h})}\frac{1-\zeta_{p^{h-v}}^{i_2}}{1-\zeta_{p^{h-v}}}.$$

Note that

$$v_{\mathcal{P}}\left(\frac{c'}{\pi}\frac{1-\zeta_{p^{h-v}}}{\pi^{\ell-1}(1-\zeta_{p^h})}\right) = Mp^v - 1 - (\ell-1) - M = -1.$$

Therefore we have the $k = \ell = 1$ case with the p^{h-v}th roots of unity. In effect, we are using only p^{h-v} factors of $f(x) - g(y)$. The case where m is not a p-power is similar.

4.3 $\ell = k$

We now consider the case $\ell = k$. Write $m = p^h m_1$ with $p \nmid m_1$. Suppose

$$i \equiv j \mod p^{\lceil \log_p(k+1) \rceil} m_1.$$

Then ζ_m^{i-j} is a power of ζ_{p^h}. Lemma 4.2.1 implies

$$v_{1-\zeta_{p^h}}\left(\frac{1-\zeta_m^{i-j}}{1-\zeta_m}\right) \geq p^{v_p(i-j)} - 1 \geq p^{\lceil \log_p(k+1) \rceil} - 1 \geq k = \ell,$$

so $c_i' \equiv c_j'$ mod π^ℓ. Therefore the number of distinct c_i' mod π^ℓ is at most $p^{\lceil \log_p(k+1) \rceil} m_1$. To fill all residue classes we need

$$p^{\lceil \log_p(k+1) \rceil} m_1 \geq N(\mathcal{P})^k. \tag{4.4}$$

Since the m_1th roots of unity are distinct mod π, we have $N(\mathcal{P}) > m_1$. Therefore

$$N(\mathcal{P})^k = N(\mathcal{P})^{k-1} \cdot N(\mathcal{P}) > p^{\nu(k-1)} m_1, \tag{4.5}$$

where $p^\nu = N(\mathcal{P})$. We obtain $p(k+1)m_1 \geq p^{\nu k-\nu}m_1$, which implies

$$k+1 \geq p^{\nu k-\nu-1} \tag{4.6}$$

Suppose $p \geq 5$. Then we immediately obtain from (4.6) that $k \leq 2$. If $k \leq 2$ then $\lceil \log_p(k+1) \rceil = 1$ and (4.4) and (4.5) sharpen to $p > p^{\nu k-\nu}$ which implies $k = 1$.

Suppose $p = 3$. We similarly obtain from (4.6) that $k \leq 3$. When $k \leq 3$, inequalities (4.4) and (4.5) sharpen and yield $k = 1$.

Suppose $p = 2$. We again similarly obtain from (4.6) that $k \leq 4$. When $k \leq 4$, inequalities (4.4) and (4.5) sharpen and yield $k \leq 2$.

For all primes we have shown that if $k = \ell$ then $k = \ell = 1$, with the exception of $p = 2$ and $k = \ell = 2$. We now assume we are not in the exceptional case and show that $N(\mathcal{P})$ must be p and $m_1 = 1$. Suppose $m_1 > 1$. Then $1 - \zeta_m$ is a unit. If $i \equiv j \bmod m_1$ then $v_{1-\zeta_{p^h}}(1 - \zeta_m^{i-j}) \geq 1$. It follows that

$$c_i' \equiv c_j' \bmod \pi.$$

Therefore we get at most m_1 classes mod π from the c_i'. But the m_1th roots of unity are distinct and non-zero mod π, so $N(\pi) > m_1$. Therefore the c_i' cannot cover all the classes mod π. This contradiction implies $m_1 = 1$. By (4.4) we have $p \geq N(\pi)$, so $N(\pi) = p$.

Now suppose $p = 2$ and $k = \ell = 2$. If $i_1 \equiv j_1 \bmod 2m_1$, then $v_{1-\zeta_{2^h}}(1 - \zeta^{i_1-j_1}) \geq 2$. If $m_1 \neq 1$ we obtain $c_i' \equiv c_j' \mod \pi^2$, so we get at most $2m_1$ classes mod π^2. We must have

$$2m_1 \geq N(\mathcal{P})^2 > 2m_1$$

which is a contradiction. Therefore $m_1 = 1$. Putting $k = 2$ in (4.4) yields $4 \geq 2^{2\nu}$. Therefore $\nu = 1$.

To summarize, if $k = \ell$ then $k = \ell = 1$, with the exception of $p = 2$ and $k = \ell = 2$. For all cases, $m_1 = 1$ and $\nu = 1$.

4.4 There's only one prime p

Suppose β and $\frac{1}{\beta}$ are not in $\mathcal{O}$. Proposition 3.0.5 gives us a prime p such that $(1-\zeta_p)\beta \in \mathcal{O}$. This was obtained by using the assumption that for every $y \in \mathcal{O}$ there exists an x such that $f(x) = g(y)$. If we reverse the roles of x and y we get a prime q such that $\frac{(1-\zeta_q)}{\beta} \in \mathcal{O}$. We now show we may take $p = q$.

Let $\mathcal{P}$ be the prime of $\mathcal{O}$ above p as in the previous sections. Since $N(\mathcal{P})$ factors through the norm from $\mathbb{Q}[\zeta_q]$ to $\mathbb{Q}$, we must have $N(P) \equiv 1 \bmod q$, since this is true for all norms from $\mathbb{Q}[\zeta_q]$ that are relatively prime to q [7, Theorem 2.13]. But we showed in previous sections that $N(P) = p$ so $p > q$. Reversing the roles of p and q yields $q > p$. This contradiction shows $p = q$.

If $\beta \in \mathcal{O}$ then $(1 - \zeta_p)\beta \in \mathcal{O}$ for all $\zeta_p \in \mathcal{O}$, so we choose $\zeta_q \in \mathcal{O}$ such that $\frac{(1-\zeta_q)}{\beta} \in \mathcal{O}$. We then take $p = q$.

4.5 There is only one prime in the denominator

Suppose $\mathcal{P}_1$ and $\mathcal{P}_2$ are distinct primes above p and both occur in the denominator of β. We will show that such a case cannot happen. Let

$$v_{\mathcal{P}_j}(\beta) = -k_j < 0, \qquad v_{\mathcal{P}_j}(c) = -\ell_j$$

for $j = 1, 2$. We work in the semi-localization $\mathcal{O}_{\mathcal{P}_1,\mathcal{P}_2}$, where we invert the complement of $\mathcal{P}_1 \cup \mathcal{P}_2$. If for every y there exists an x such that $f(x) = g(y)$ then the integral values of

$$\pi_1^{k_1-\ell_1}\pi_2^{k_2-\ell_2}c_i'$$

run through all congruence classes mod $\pi_1^{k_1}\pi_2^{k_2}$. By Section 4.1, we know that $\ell_1 \geq k_1$ and $\ell_2 \geq k_2$.

First assume $k_1 = k_2 = 1$. This always happens when $p \geq 3$.

Suppose $\ell_1 > k_1$ and $\ell_2 = k_2$. In the notation of Section 4.2, for $\pi_1^{k_1-\ell_1}c_i'$ to be integral, we must have $i \equiv 0 \bmod pm_1$. But this implies $c_i' \equiv 0 \bmod \pi_2$, so therefore $\pi_1^{k_1-\ell_1}\pi_2^{k_2-\ell_2}c_i' \equiv 0 \bmod \pi_2$. Therefore we don't get all residue classes mod $\pi_1^{k_1}\pi_2^{k_2}$. By symmetry we also eliminate the case $\ell_1 = k_1$ and $\ell_2 > k_2$.

Suppose $\ell_1 = k_1$ and $\ell_2 = k_2$. In the notation of Section 4.3, if $i \equiv j \bmod p$ (recall we showed $m_1 = 1$) then $c_i' \equiv c_j' \bmod \pi_1$ and mod π_2. Therefore we get at most p congruence classes mod $\pi_1\pi_2$, but there are $N(\mathcal{P}_1\mathcal{P}_2) = p^2$ such classes.

Suppose $\ell_1 > k_1$ and $\ell_2 > k_2$. From Equation (4.1) in Section 4.2,

$$M_1 p^{v_p(i)} \geq \ell_1 - 1 + v_{\mathcal{P}_1}(1 - \zeta_m)$$

and from Equation (4.2), every pair of distinct indices i, j must satisfy

$$M_1 p^{v_p(i-j)} < v_{\mathcal{P}_1}(1 - \zeta_m) + \ell_1.$$

This forces $v_p(i-j)$ and all but one value of $v_p(i)$ to take only one value, let's call it v_1. Similarly,

$\mathcal{P}_2$ gives us a value v_2.

We must have $v_p(i) \geq v_2$ for integrality of c'_i at $\mathcal{P}_2$. If $v_2 > v_1$ then $c'_i \equiv 0 \bmod \pi_1$, so we don't get all classes mod $\pi_1\pi_2$. Similarly we cannot have $v_1 > v_2$.

Suppose $v_1 = v_2$. Then we only get p values of i that satisfy our inequalities. Therefore we get only p values of $c'_i \bmod \pi_1\pi_2$. But there are p^2 classes.

We consider the exceptional case $p = 2$ and $\ell_1 = k_1 = 2$. In this case we have $m_1 = 1$ so m is a power of 2. From Section 4.3 we know that if $i \equiv j \bmod 4$ then $c'_i \equiv c'_j \bmod \pi_1^2$. We need to consider three cases.

Suppose $\ell_2 = k_2 = 1$. Then $i \equiv j \bmod 2$ implies $c'_i \equiv c'_j \bmod \pi_2$. Therefore if $i \equiv j \bmod 4$ then $c'_i \equiv c'_j \equiv \pi_1^2\pi_2$. But there are 8 classes mod $\pi_1^2\pi_2$.

Suppose $\ell_2 = k_2 = 2$. Then $i \equiv j \bmod 4$ implies $c'_i \equiv c'_j \bmod \pi_2^2$. Therefore if $i \equiv j \bmod 4$ then $c'_i \equiv c'_j \equiv \pi_1^2\pi_2^2$. But there are 16 classes mod $\pi_1^2\pi_2$.

Suppose $\ell_2 > k_2 = 1$. Since m is a power of 2, $v_{\mathcal{P}_2}(1 - \zeta_m) = M$. Equation (4.1) says

$$M2^{v_2(i)} \geq \ell_2 - 1 + M > M,$$

so $i \equiv 0 \bmod 2$. Recall that if $i \equiv j \bmod 4$ then $c'_i \equiv c'_j \bmod \pi_1^2$. Since i must be even we get only two classes for c'_i but we need 4.

Bibliography

[1] Scott T. Chapman and Vadim Ponomarenko. On image sets of integer-valued polynomials. *Journal of Algebra*, 348(1):350–353, 2011.

[2] Paul-Jean Cahen and Jean-Luc Chabert. *Integer-valued polynomials*, volume 48 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 1997.

[3] David Hilbert. Ueber die irreducibilität ganzer rationaler functionen mit ganzzahligen coefficienten. *Journal für die reine und angewandte Mathematik*, 110:104–129, 1892.

[4] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. A K Peters, Ltd., Wellesley, MA, second edition, 2008. With notes by Henri Darmon.

[5] William Gasarch, Mark B. Villarino, and Kenneth W. Regan. Hilbert's proof of his irreducibility theorem. *The American Mathematical Monthly*, 125(6):513–530, 2018.

[6] B. L. van der Waerden. *Einführung in die algebraische Geometrie (Grundlehren der mathematischen Wissenschaften, 51)*. Springer Verlag, 2nd edition, 1973.

[7] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.