ABSTRACT

Title of dissertation: Eventually Stable Quadratic Polynomials over $\mathbb{Q}(i)$

Jermain McDermott, Doctor of Philosophy, 2024

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

Let f be a polynomial or a rational function over a field K. Arithmetic dynamics studies the algebraic and number-theoretic properties of its iterates $f^n := f \circ f \circ ... \circ f$.

A basic question is, if f is a polynomial, are these iterates irreducible or not? We wish to know what can happen when considering iterates of a quadratic $f = x^2 + r \in K[x]$. The most interesting case is when $r = \frac{1}{c}$, which we will focus on, and discuss criteria for irreducibility, i.e. *stability* of all iterates. We also wish to prove that if 0 is not periodic under f, then the number of factors of f^n is bounded by a constant independent of n, i.e. f is *eventually stable*. This thesis is an extension to $\mathbb{Q}(i)$ of the paper [1], which considered f over $\mathbb{Q}$.

This thesis involves a mixture of ideas from number theory and arithmetic geometry. We also show how eventual stability of iterates ties into the density of prime divisors of sequences.

Eventually Stable Quadratic Polynomials over $\mathbb{Q}(i)$

by

Jermain McDermott

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: *Advisor, Chair*
Professor William Gasarch: *Dean's Representative*
Professor Niranjan Ramachandran
Professor Amin Gholampour
Professor Patrick Brosnan

Acknowledgments

It is impossible to assign a well-ordering to the set of all the thanks. However, I must first offer my sincerest gratitude to my advisor Larry Washington. His guidance, knowledge, patience, and availability for my end-of-week drop-ins have all been indispensable to me. I'll also be continuously grateful for him as a role model outside of this thesis.

I also owe a huge thank you to my mentors at George Mason University. Without them I wouldn't have made it this far. My undergraduate thesis advisors and Geometry Lab inductors, Drs. Sean Lawton and Chris Manon, I would like to thank first. I would also like to thank Dr. Daniel Anderson for Friday Chill Math practice, and ping pong sessions at the Walker's house on Thanksgivings (I'd like to thank them as well for including me in their family!). I would also like to thank Dr. Ellen O'Brien for taking a chance hiring me at the GMU Math Tutoring Center as a sophomore.

I would like to thank my defense committee: Dr. Niranjan Ramachandran, who first suggested the topic of this thesis after my preliminary exam, and for inspiring in me a love of algebraic number theory, and Dr. Amin Gholampour for also reinforcing that love of algebra. Thanks must also go to Dr. Rodrigo Trevino for rekindling my love of dynamics. I certainly also owe thanks to Dr. Art Drisko and the NSA for their financial support throughout grad school, and for their continued elective support through the pandemic. Their vote of confidence went a long way getting me to this point.

My friends and student mentors also played a major role in this journey. A huge thank you first goes to Sam Mendelson, who can take most of the credit for my becoming a math major and inspiring many others; Charles Daly, my tutor-turned-coworker at the Tutoring Center, for our Chill Math, our skating and hackey-sacking sessions, and for letting me follow him to UMD in his giant footsteps; Ishfaaq Imtiyas, Noah Chrein, and Stavros Papathanasiou, my entering peers/trinities in College Park; Keagan Callis for housing me during a low, unfortunate period and helping me pass my first qual exam as a result; Jacob Kressel for doing the same and being my brother since GMU; Beer Crew for the weekly beer o'clock; and Liam Fowl, Andrew Hornstra, Shashank Sule, Meenakshi Krishnan, and Michael Rozowski for their friendship. I'd also like to thank my tattooed brothers for taking me under their wings when I had just moved to Virginia in 2009 and didn't know anyone; Michael Armstrong and Zack Hargreaves just to name a few.

I owe an infinity to my partner Maeve Wildes, who has sacrificed and put up with *a lot* during this time. Her support means everything to me. Finally, I must thank my parents and family. Because of them,

cogito, ergo sum.

Table of Contents

Chapter 1: Introduction

Suppose K is a field with algebraic closure $\overline{K}$. In this thesis we study the arithmetic dynamics of quadratic polynomials $f(x) = x^2 + r \in K[x]$ under iteration, i.e.

$$f^n(x) = (f \circ f \circ ... \circ f)(x) \text{ } (n \text{ compositions}) \qquad \text{with } f^0(x) = x.$$

Fix $\alpha \in K$ and denote by $f^{-n}(\alpha) := \{\beta \in \overline{K} : f^n(\beta) = \alpha\}$. If $f^n(x) - \alpha$ is separable, the disjoint union $T_{f,\infty}(\alpha) := \{\alpha\} \sqcup f^{-1}(\alpha) \sqcup f^{-2}(\alpha) \sqcup \cdots$ is a rooted tree with root vertex α, and edges assigned according to the action of f. Denote by $\mathrm{Aut}(T_f(\alpha))$ the tree automorphisms of $T_f(\alpha)$. Since the natural action of the Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ on $f^{-n}(\alpha)$ commutes with $f \in K[x]$, we obtain a homomorphism $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}(T_f(\alpha))$ called the arboreal Galois representation associated to (f, α). One of the central problems in arithmetic dynamics is whether the image of this homomorphism has finite index in $\mathrm{Aut}(T_f(\alpha))$; a dynamical analogue of the renowned Serre open image theorem. This question has generated a large literature, see [2] for a summary of this and other current research in the field.

In this thesis, we attempt to characterize factorizations of $f^n(x) - \alpha$ for $\alpha = 0$.

The polynomial function f is called *stable over* K if every iterate f^n is irreducible over K.

Definition 1. *Let K be a field, $f \in K[x]$, and $\alpha \in K$. For $n \geq 1$ let k_n denote the number of irreducible factors of $f^n(x) - \alpha$ over K.*

*We call the pair (f, α) (resp. f) **eventually stable over K** if there is a constant $C(f, \alpha)$ (resp $C(f, 0)$) such that for all n,*

$$k_n \leq C(f, \alpha).$$

Eventual stability is applied in some finite-index results for certain arboreal Galois representations [3, 4], and is equivalent to a bound independent of n on the number of Galois orbits on $f^{-n}(\alpha)$ [5, Proposition 2.2]. However, this is a straightforward consequence of the image of the arboreal representation associated to (f, α) having finite index, so finite index of the arboreal representation implies eventual stability. The reverse implication is much less clear. Other applications include finiteness of S-integer points in backwards orbits; see [5, Section 3] for a discussion of these and other results surrounding the topic.

The following theorem of Hamblen, Jones, and Madhu [6] establishes eventual stability of a large class of polynomials over number fields:

Theorem 1.0.1. *(Hamblen, Jones and Madhu, [6, Theorem 5]) Let $d \geq 2$, let K be a field of characteristic not dividing d, and let $f(x) = x^d + r \in K[x]$. If there is a discrete non-archimedean absolute value on K with $|r| < 1$, then f is eventually stable over K.*

The following corollary is an extension of [6, Corollary 6] considered by DeMark et al.:

Corollary 1.0.1. *Let $f(x) = x^d + r \in \mathbb{Q}(i)[x]$, and suppose that r is non-zero and is not the reciprocal of an element of $\mathbb{Z}[i]$. Then f is eventually stable over $\mathbb{Q}(i)$.*

This thesis is an attempt at proving eventual stability when $d = 2$ and a non-zero $r \neq -1$ *is* a reciprocal of an element of $\mathbb{Z}[i]$. In this case, the following conjecture attempts to fully describe the situation. It is an extension of [1, Conjecture 1.7] which considered $r \in \mathbb{Q}$:

Conjecture 1. *Let $f_r = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then f_r is eventually stable over $\mathbb{Q}(i)$ with constant $C(f_r, 0) = 4$:*

(1) *If $c = m^2$ with $1 \pm im \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ then $k_n = 2$ for all $n \geq 1$.*

(2) *If $c \in \{\pm 8i, -16\}$, then $k_1 = k_2 = 2$, $k_n = 3$ for all $n \geq 3$.*

(3) *If $c = -(s^2-1)^2$ for $\pm s \in \mathbb{Z}[i]\backslash\{3, 5, 56\}$ then $k_1 = 2$ and $k_n = 3$ for all $n \geq 2$.*

(4) *If $c = -(s^2 - 1)^2$ for $\pm s \in \{3, 5, 56\}$ then $k_1 = 2$, $k_2 = 3$ and $k_n = 4$ for all $n \geq 3$.*

(5) *If $c \neq 48$ and $c = -m^2(m^2 \pm 2i)$, then $k_1 = 1$ and $k_n = 2$ for all $n \geq 2$.*

(6) *If $c = 48$, then $k_1 = 1, k_2 = 2$, and $k_n = 3$ for all $n \geq 3$.*

(7) *If $c \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ and $c \neq -m^2(m^2 \pm 2i)$ then $k_n = 1$ for all $n \geq 1$.*

Case (7) is precisely the case where $f_r^2(x)$ is irreducible and thus case (7) asserts that if $f_r^2(x)$ is irreducible, then $f_r^n(x)$ is irreducible for all $n \geq 1$. We state this as a $\mathbb{Z}[i]$ analogue of [1, Conjecture 1.8]:

Conjecture 2. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$. If $f_r^2(x)$ is irreducible then $f_r^n(x)$ is irreducible for all $n > 2$.*

The main result of this thesis is a $\mathbb{Z}[i]$ analogue of [1, Theorem 1.2]:

Theorem 1.0.2. *Let $K = \mathbb{Q}(i)$ and $f_r(x) = x^2 + r$ with $r = 1/c$ for $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$. If $N(c) \leq 10^9$, then f_r is eventually stable over $\mathbb{Q}(i)$ and $C(f_r, 0) \leq 4$. In particular, Conjecture 1 below holds for all c with $N(c) \leq 10^9$.*

In Chapter 3, we fully prove cases (2) and (4) of Conjecture 1 as the following $\mathbb{Z}[i]$ analogue of [1, Theorem 1.5]):

Theorem 1.0.3. *Let $f_r = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then,*

(1) We have $k_1 = k_2 = 2$ and $k_3 = 3$ if and only if $c \in \{\pm 8i, -16\}$. In this case $k_n = 3$ for all $n \geq 3$.

(2) We have $k_3 \geq 4$ if and only if $c = -(s^2 - 1)^2$ for $\pm s \in \{3, 5, 56\}$. In this case $k_n = 4$ for all $n \geq 3$.

Whether $f_r^n(0)$ is a square or not is of central importance in this result and for most of this thesis. To this end, we use tools such as the non-linear recurrence relation

$$a_1 = 1, \quad a_n(c) = c^{2^{n-1}-1} + a_{n-1}^2(c) \quad \text{for } n \geq 2$$

describing the numerator of $f_r^n(0) = \frac{a_n}{c^{2^{n-1}}}$ for $n \geq 1$ (note $c^{2^{n-1}}$ is a square when $n \geq 2$).

In Chapter 4, we prove another irreducibility test involving the a_n sequence. It is a $\mathbb{Z}[i]$ analogue of [1, Lemma 1.10]:

Lemma 1.0.1. *Suppose that $c \in \mathbb{Z}[i]\backslash\{0\}$, $r = 1/c$ and f_r^2 is irreducible. Let $a_n = a_n(c)$ be defined as above and set*

$$b_n^{\pm}(c) = i(a_{n-1} \pm \sqrt{a_n}) \in \bar{\mathbb{Q}}. \tag{1.1}$$

If $b_n^{\pm}$ is not a square in $\mathbb{Z}[i]$ (which holds in particular if a_n is non-square in $\mathbb{Z}[i]$) for all $n \geq 3$, then $f_r^n(x)$ is irreducible for all $n \geq 1$.

This leads us to prove the following $\mathbb{Z}[i]$ extension of [1, Conjecture 1.11]:

Conjecture 3. *Let $b_n^{\pm}(c)$ be defined as in 1.1. If $c \in \mathbb{Z}[i]\backslash\{0, -1\}$, then $b_n^{\pm}(c)$ is non-square in $\mathbb{Z}[i]$ for all $n \geq 3$.*

The $\{b_n^{\pm}(c)\}$ square test of Lemma 1.0.1 allows us to prove a $\mathbb{Z}[i]$ analogue of [1, Theorem 1.3]:

Theorem 1.0.4. *Let $f_r(x) = x^2 + r$ with $r = 1/c$. Then f_r^n is irreducible for all $n \geq 1$ if c satisfies one of the following conditions:*

(1) $c, c+1 \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$, $2 \nmid c$ *and* $16 \nmid c+1$;

(2) $c \equiv i \bmod a+bi$ *with*

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 9 \bmod 16) \text{ or} \\ \\ (i \bmod 2, 5 \bmod 8, 1 \bmod 16) \end{cases}$$

or $c \equiv -i \bmod a+bi$, *with*

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 1 \bmod 16) \text{ or} \\ \\ (i \bmod 2, 5 \bmod 8, 9 \bmod 16) \end{cases}$$

(3) $c \neq -1 \pm 2i$ *and* $v_\pi(c)$ *is odd for all primes* $\pi \mid c$.

In Chapter 5, we prove another result allowing us to check irreducibility of f^k for some finite k to determine stability of f. It is the extension to $\mathbb{Z}[i]$ of [1, Theorem 1.4]. In the statement, $\epsilon : \mathbb{R} \to \mathbb{R}$ is a monotonically decreasing function with $2 \leq \epsilon \leq 4$ (see Definition 4):

Theorem 1.0.5. *Let* $f_r(x) = x^2 + r$ *with* $r = 1/c$ *for* $c \in \mathbb{Z}[i]$ *with* $|c| \geq 5$. *If* f^k *is irreducible for*

$$k = 1 + \left\lfloor \log_2 \left(1 + \frac{\log 4 + \epsilon(|c|)/\sqrt{|c|}}{\log \sqrt{1 + 1/|c|}} \right) \right\rfloor,$$

then all f^n *are irreducible.*

Now, we define the orbit of $t \in \mathbb{Q}(i)$ under f_r to be the set $O_{f_r}(t) = \{t, f_r(t), f_r^2(t), ...\}$, and we say that a prime π divides $O_{f_r}(t)$ if there is at least one nonzero $\alpha \in O_{f_r}(t)$ with $v_\pi(\alpha) > 0$. In Chapter 6, we prove the following $\mathbb{Z}[i]$ analogue of [1, Proposition 6.1], showing that the natural density of prime divisors of orbits is 0 when $b_n^{\pm}$ is non-square for all $n \geq 2$:

Theorem 1.0.6. *Let* $f_r(x) = x^2 + r$ *for* $r = 1/c$ *for* $c \in \mathbb{Z}[i] \backslash \{0, -1\}$, *with* $c, c+1$ *both non-square in* $\mathbb{Z}[i]$. *If Conjecture 3 above holds for* c, *then for any* $t \in \mathbb{Q}(i)$ *we have*

$$D(\{\pi \text{ prime in } \mathbb{Z}[i] : \pi \text{ divides } O_{f_r}(t)\}) = 0.$$

Chapter 2: Background

We list some theorems that will make our work considerably easier:

Theorem 2.0.1. *If $p(x) \in \mathbb{Q}(i)[x]$, then any factorization of p into irreducible polynomials over $\mathbb{Q}(i)$ has the same number of factors as $\bar{p}(x)$, $p(x)$ with conjugated coefficients.*

Proof. Since conjugation is a field automorphism of $\mathbb{Q}(i)$, it extends to a ring automorphism of $\mathbb{Q}(i)[x]$. Ring automorphisms preserve irreducibility. □

Corollary 2.0.1. *The polynomial $f_r^n(x)$ has the same number of factors irreducible over $\mathbb{Q}(i)$ as $f_{\bar{r}}^n(x)$.*

This corollary allows us to only consider c in quadrants 1 and 3, reducing our work load by "half".

We also will need some way of inferring irreducibility of iterated polynomials. To this end, Capelli's Lemma is foundational to our study and an important criterion.

Lemma 2.0.1. *(Capelli's Lemma) Let K be a field, $f(x), g(x) \in K[x]$ and let $\alpha \in \overline{K}$ be a root of g. Then $g(f(x))$ is irreducible over K if and only if g is irreducible over K and $f(x) - \alpha$ is irreducible over $K(\alpha)$.*

Proof. Let $n = \deg g$, $m = \deg f$, and β be a root of $f(x) - \alpha$. Note β is a root of $g(f(x))$, since $g(f(x)) = \prod_i (f(x) - \alpha_i)$ over $\overline{K}$ where $\{\alpha_i\}$ are all the roots of g including α. Now, g is irreducible over K and $f(x) - \alpha$ is irreducible over $K(\alpha)$ iff $[K(\alpha) : K] = n$ and $[K(\beta) : K(\alpha)] = m$. Since $\deg g(f(x)) = mn$, we have that $g(f(x))$ is irreducible over K iff

$$[K(\beta) : K] = mn = [K(\beta) : K(\alpha)] \cdot [K(\alpha) : K].$$

□

For a helpful application of Capelli's Lemma, [1, Lemma 2.2] uses the lemma together with the fact that a quadratic polynomial of non-square discriminant is irreducible over K. It translates irreducibility of the list $\{g(f^n(x))\}_{n\geq 1}$ to a property of a sequence in K. We include the proof here for completeness:

Lemma 2.0.2. *(Demark-Hindes-Jones-Misplon-Stoll-Stoneman, [1, Lemma 2.2]) Let K be a field with $char(K) \neq 2$, $g \in K[x]$ a monic, irreducible polynomial with $d := \deg(g) \geq 1$, and $f(x)$ monic and quadratic with critical point β. If the set*

$$\{(-1)^d g(f(\beta))\} \cup \{g(f^n(\beta))\}_{n\geq 2}$$

contains no squares in K, then $g(f^n(x))$ is irreducible over K for all $n \geq 1$.

Proof. Let $f(x) = x^2 + bx + c$, so that $\gamma = -b/2$. We proceed by induction on n, with the $n = 0$ case covered by the irreducibility of $g(x)$. Assume then that $g(f^{n-1}(x))$ is irreducible over K for some $n \geq 1$, and let d_1 be the degree of $g(f^{n-1}(x))$. By

Capelli's Lemma (2.0.1), $g(f^n(x))$ is irreducible over K if and only if for any root β of $g(f^{n-1}(x))$, we have $f(x) - \beta$ is irreducible over $K(\beta)$, or equivalently (because K has characteristic different from 2), $\mathrm{Disc}(f(x) - \beta) = b^2 - 4c + 4\beta$ is not a square in $K(\beta)$.

This must hold if $N_{K(\beta)/K}(b^2 - 4c + 4\beta)$ is not a square in K. The Galois conjugates of $b^2 - 4c + 4\beta$ are precisely $b^2 - 4c + 4\alpha$ as α varies over all roots of $g(f^{n-1}(x))$. Thus

$$\begin{aligned} N_{K(\beta)/K}(b^2 - 4c + 4\beta) &= (-4)^{d_1} \prod_{\alpha \text{ root of } g \circ f^{n-1}} \left[\left(-\frac{b^2}{4} + c \right) - \alpha \right] \\ &= (-4)^{d_1} \cdot g(f^{n-1}(-b^2/4 + c)) \\ &= (-4)^{d_1} \cdot g(f^{n-1}(\gamma))), \end{aligned}$$

where the second equality holds because $g(f^{n-1}(x))$ is monic. Now d_1 is odd if and only if $n = 1$ and d is odd, which proves the Lemma. □

Remark. *It is shown in this theorem that if $g(f^n(x))$ is irreducible for some $n \geq 1$ and $g(f^{n+1}(0))$ is non-square in K, then $g(f^{n+1}(x))$ is irreducible.*

2.1 Rigid divisibility

One can show inductively that $f^n_{1/c}(0) = a_n / c^{2^{n-1}}$, where

$$a_1(c) = 1, \quad a_n(c) = a(c)^2_{n-1} + c^{2^{n-1}-1} \quad \text{for } n \geq 2.$$

Note that the numerator a_n is relatively prime to the denominator $c^{2^{n-1}-1}$, a square when $n > 1$. This recurrence relationship will be essential in this analysis. Many of our results hinge on this relationship paired with the notion of "rigid divisibility".

Rigid divisibility is a property of some sequences $\{z_n\}_{n\geq 1}$ yielding that the prime divisors of z_j are related to those of z_{jk} in the following way:

Definition 2. *Let $A = \{z_n\}_{n\geq 1}$ be a sequence in a field K. We say A is a* ***rigid divisibility sequence over K*** *if for each non-archimedean absolute value $|\cdot|$ on K, the following hold:*

(1) if $|z_n| < 1$, then $|z_n| = |z_{kn}|$ for any $k \geq 1$.

(2) if $|z_n| < 1$ and $|z_j| < 0$, then $|z_{gcd(n,j)}| < 0$.

The following is [6, Lemma 12], establishing rigid divisibility of the forward orbit of 0:

Theorem 2.1.1. *(Hamblen, Jones and Madhu, [6, Lemma 12]) Let K be a field and $f(x) = x^d + r \in K[x]$ for some $d \geq 2$. Then $\{f^n(0)\}_{n\geq 1}$ is a rigid divisibility sequence over K.*

Proof. Let $|\cdot|$ be a non-archimedean absolute value on K. We begin with the observation that either $|f^n(0)| > 1$ for all $n \geq 1$ or $|f^n(0)| \leq 1$ for all $n \geq 1$. Indeed, assume that $|f^n(0)| > 1$ for some $n \geq 1$ and without loss let n be minimal with this property. Write $c = f^n(0) - (f^{n-1}(0))^d$, taking $f^0(x) = x$ in the case $n = 1$. Then $|c| = |f^n(0)|$ by the ultrametric property. Therefore $|f(0)| = |r| > 1$, whence $n = 1$. We now have $|f^i(0)| = |f^{i-1}(0)|^m > |f^{i-1}(0)|$ for each $i \geq 2$, proving that $|f^n(0)| > 1$ for all $n \geq 1$.

To prove property (1) of rigid divisibility, suppose that $|f^n(0)| < 1$. By the previous paragraph, this gives $1 \geq |f(0)| = |r|$. We induct on k, noting first that if $k = 1$, then trivially $|f^{kn}(0)| = |f^n(0)|$. Suppose that $|f^{(k-1)n}(0)| = |f^n(0)| < 1$. Write $f^n(x) = f^n(0) + \sum_{i=1}^{d^{n-1}} r_i x^{d_i}$ and note that the r_i are elements of $\mathbb{Z}[r]$ and thus $|r_i| \leq 1$ because $|r| \leq 1$. Observe that $f^{kn}(0) = f^n(f^{(k-1)n}(0))$ implies

$$|f^{kn}(0)| = \left| f^n(0) + \sum_{i=1}^{d^{n-1}} r_i (f^{(k-1)n}(0))^{d_i} \right| = |f^n(0)|$$

where the last equality follows from the fact that $|f^{(k-1)n}(0)|^{d_i} < |f^n(0)|$ for $i \geq 1$.

To prove property (2), assume $|f^m(0)| < 1$ for some $m \geq 1$, and let m be the minimal positive integer with this property. By the argument at the beginning of this proof, $|f^n(0)| \leq 1$ for all i. Therefore the sequence $\overline{0}, \overline{f(0)}, \overline{f^2(0)}, ...$ in the residue field of K is a cycle containing precisely m distinct elements. Hence for any $j = \ell m + r$, $\overline{f^k(0)}$ will be zero if and only if $r = 0$. So if both $|f^j(0)| < 1$ and $|f^n(0)| < 1$, then $m \mid \gcd(j, n)$, yielding property (2). □

Thus we have that if a_n is the numerator of $f^n(0)$, then a_n is a rigid divisibility sequence.

In our case $K = \mathbb{Q}(i)$, and if $\{s_n\}$ is a sequence in $\mathbb{Q}(i)$, we may translate the rigid divisibility sequence definition to this setting. It is the condition that for any prime $\pi \in \mathbb{Z}[i]$ we have:

(1) if $v_\pi(s_n) = e > 0$ then $v_\pi(s_{mn}) = e$ for all $m \geq 1$, and

(2) if $v_\pi(s_n) > 0$ and $v_\pi(s_j) > 0$, then $v_\pi(s_{\gcd(n,j)}) > 0$.

We extend [7, Proposition 5.4] to polynomials over $\mathbb{Q}(i)[x]$, showing that when $g \mid f$ and $\{a_n\} = \{\text{numerator of } f^n(0)\}_{n\geq 1}$ is a rigid divisibility sequence, then

$$\{w_n\} = \{\text{numerator of } g(f^{n-1}(0))\}_{n\geq 1}$$

is a rigid divisibility sequence as well:

Proposition 2.1.1. *Suppose that $f \in \mathbb{Q}(i)[x]$ has all iterates separable, 0 is a critical point of f, and $\{a_n\} = \{$numerator of $f^n(0)\}_{n\geq 1}$ is a rigid divisibility sequence with infinitely many values. If $g \mid f$ in $\mathbb{Q}(i)[x]$, then the sequence*

$$\{w_n\} = \{\textit{numerator of } g(f^{n-1}(0))\}_{n\geq 1}$$

is a rigid divisibility sequence.

Proof. This is the proof of [7, Proposition 5.4] with minor modifications.

Suppose that $gh = f$, and for $n \geq 1$ denote the numerators of $f^n(0)$ and $g(f^{n-1}(0))$ respectively by a_n and w_n. By convention $f^0(x) = x$, and note that we have $a_n = w_n w'_n$ for some $w'_n \in \mathbb{Z}[i]$. If $v_\pi(w_i) = e > 0$, then we have $a_i = f^i(0) \equiv 0 \bmod \pi^e$, whence 0 is periodic mod π^e under f, with period dividing i. Hence in particular $f^{mi-1}(0) \equiv f^{i-1}(0) \bmod \pi^e$ for all $m \geq 1$. Now $v_\pi(w_i) = e > 0$ implies that $g(f^{i-1}(0)) \equiv 0 \bmod \pi^e$, and thus $f^{i-1}(0)$ is a root of $g \bmod \pi^e$. Therefore $f^{mi-1}(0)$ is also a root of $g \bmod \pi^e$, implying that $v_\pi(w_{mi}) \geq e$. Similarly, if $v_\pi(w'_i) = e > 0$, then $v_\pi(w'_{mi}) \geq e$ for all $m \geq 1$.

Now suppose that $v_\pi(w_i) = e_1 > 0$. Then $v_\pi(w'_i) = e_2 \geq 0$, and $v_\pi(a_i) = e_1 + e_2$. Since $\{a_n\}$ is a rigid divisibility sequence over $\mathbb{Q}(i)$, we have $v_\pi(a_{mi}) = e_1 + e_2$ for

all $m \geq 1$. But by the previous paragraph $v_\pi(w_{mi}) \geq e_1$ and $v_\pi(w'_{mi}) \geq e_2$. Thus $a_{mi} = w_{mi}w'_{mi}$ implies $v_\pi(w_{mi}) = e_1$ and $v_\pi(w'_{mi}) = e_2$.

To show that $\pi^e \mid w_n$ and $\pi^e \mid w_m$ implies $\pi^e \mid w_{\gcd(m,n)}$, note

$$g(f^{n-1}(0)) \equiv g(f^{m-1}(0)) \equiv 0 \bmod \pi^e,$$

so

$$g(f^{m-1}(0)) \cdot h(f^{m-1}(0)) = f^m(0) \equiv 0 \bmod \pi^e$$

and

$$g(f^{n-1}(0)) \cdot h(f^{n-1}(0)) = f^n(0) \equiv 0 \bmod \pi^e.$$

Without loss of generality suppose that $n > m$, whence

$$0 \equiv g(f^{n-1}(0)) \equiv g(f^{n-m-1}(f^m(0))) \equiv g(f^{n-m-1}(0)) \bmod \pi^e.$$

Applying this repeatedly and using the Euclidean algorithm yields

$$\pi^e \mid g(f^{\gcd(m,n)-1}(0)).$$

Hence $\{w_n\}$ is a rigid divisibility sequence, as desired. □

Chapter 3: When f_r or f_r^2 is reducible

We first give necessary and sufficient conditions for the irreducibility of f_r and f_r^2 when f_r is irreducible. We thus prove the following $\mathbb{Z}[i]$ analogue of [1, Proposition 2.1]:

Proposition 3.0.1. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0\}$. Then $f_r(x)$ is reducible if and only if c is a square. If $f_r(x)$ is irreducible, then $f_r^2(x)$ is reducible if and only if $c = -m^2(m^2 \pm 2i)$ for some $m \in \mathbb{Z}[i]$.*

Proof. To prove the first statement, note that $f_r(x) = x^2 + r = (x + i\sqrt{r})(x - i\sqrt{r})$ over $\mathbb{Q}(i)$ if and only if $\pm i\sqrt{r} \in \mathbb{Q}(i)$, if and only if r is square in $\mathbb{Q}(i)$. Then $c = 1/r$ is a square in $\mathbb{Z}[i]$.

If $c = -m^2(m^2 + 2i)$, then

$$f_r^2(x) = \left(x^2 - \frac{1-i}{m}x - \frac{im^2 - 1}{m^2(m^2+2i)}\right)\left(x^2 + \frac{1-i}{m}x - \frac{im^2 - 1}{m^2(m^2+2i)}\right).$$

Similarly, if $c = -m^2(m^2 - 2i)$, then

$$f_r^2(x) = \left(x^2 - \frac{1+i}{m}x + \frac{im^2 + 1}{m^2(m^2-2i)}\right)\left(x^2 + \frac{1+i}{m}x + \frac{im^2 + 1}{m^2(m^2-2i)}\right).$$

The factors when $c = -m^2(m^2 \pm 2i)$ have discriminant $\frac{2i}{m^2+2i}$ and $\frac{-2i}{m^2-2i}$ (respectively). These factors are irreducible if and only if their discriminant is non-square in $\mathbb{Q}(i)$,

if and only if $m^2 \pm 2i$ is a square in $\mathbb{Z}[i]$.

When $c = -m^2(m^2 \pm 2i)$, suppose $m^2 + 2i = y^2$. Then $2i = (y-m)(y+m)$. If $\{y+m, y-m\} = \{-1+i, 1-i\}$, this implies $\pm 2m = -2+2i$, so $m = 1 \pm i$. Since $c \neq 0$, $m = 1+i$, but then the discriminant is $\frac{2i}{m^2+2i} = \frac{2i}{2i+2i} = 1/2$, non-square in $\mathbb{Q}(i)$. We obtain similar contradictions when $\{y-m, y+m\} \in \pm\{\{1+i, 1+i\}, \{1, 2i\}, \{i, 2\}\}$. Note $y-m = 1+i = y+m$ is impossible since m is nonzero, but $(y+m)-(y-m) = 2m = 0 = (1+i)-(1+i)$. If $\{y+m, y-m\} = \{1, 2i\}$, then $\pm 2m = 1-2i$, a contradiction since $2 \nmid 1+2i$. If $\{y+m, y-m\} = \{i, 2\}$, then $\pm 2m = -2+i$, again a contradiction.

Since $\overline{\frac{-2i}{m^2-2i}} = \frac{2i}{\bar{m}^2+2i}$ and we've just shown the latter is non-square in $\mathbb{Q}(i)$, the discriminant of the factors when $c = -m^2(m^2-2i)$ is also non-square. Thus the factors of $f_r^2(x)$ are irreducible over $\mathbb{Q}(i)$ when $c = -m^2(m^2 \pm 2i)$.

Conversely, suppose $f_r(x)$ is irreducible but $f_r^2(x)$ is reducible, with β a root of $f_r^2(x)$. Then $f_r(\beta)$ is a root of $f_r(x)$, so $[\mathbb{Q}(f_r(\beta)) : \mathbb{Q}(i)] = 2$ by the irreducibility of f_r. A sufficient and necessary condition for $f_r^2(x)$ to be irreducible over $\mathbb{Q}(i)$ is $[\mathbb{Q}(i)(\beta) : \mathbb{Q}(i)] = 4$. Equivalently,

$$[\mathbb{Q}(i)(\beta) : \mathbb{Q}(i)(f_r(\beta))] = 2.$$

This is true if and only if $f_r(\beta) - r$ is not a square in $\mathbb{Q}(i)(f_r(\beta))$, since β is also a root of $f_r(x) - f_r(\beta) = x^2 + r - f_r(\beta)$.

Suppose $f_r(\beta) = i\sqrt{r}$, without loss of generality (since $f_r(\beta)$ is a root of $f_r(x)$). Then $f_r(\beta) - r$ is a square in $\mathbb{Q}(i)(f_r(\beta))$ if and only if there are $a, b \in \mathbb{Q}(i)$ such that

$$-r + i\sqrt{r} = (a + bi\sqrt{r})^2 = a^2 - rb^2 + 2abi\sqrt{r}.$$

This is true if and only if $2ab = 1$ and $a^2 - rb^2 = -r$. Then after $b = \frac{1}{2a}$ is replaced in the second equation and we multiply that equation through by a^2, we obtain $a^4 + ra^2 - \frac{r}{4} = 0$. By the quadratic formula, this is true if and only if $a^2 = \frac{-r \pm \sqrt{r^2+r}}{2}$, or since $r = 1/c$, substituting yields $a^2 = \frac{-1/c \pm \sqrt{(c+1)/c^2}}{2}$. Then, multiplying both sides by $4c^2$, we obtain $4c^2a^2 = (2c)(-1 \pm \sqrt{c+1})$, a square in $\mathbb{Q}(i)$ if and only if $c+1$ is a square in $\mathbb{Q}(i)$, say $c + 1 = C^2$. Then

$$(2c)(-1 \pm \sqrt{c+1}) = 2(C^2 - 1)(-1 \pm C).$$

For the case $2(C^2 - 1)(-1 + C) = 2(C + 1)(C - 1)^2$ is a square, we must have $C + 1 = im^2$ for some $m \in \mathbb{Q}(i)$, since the prime factorization of 2 in $\mathbb{Q}(i)$ is $2 = i(1 + i)^2$. For the case $2(C^2 - 1)(-1 - C) = -2(C + 1)^2(C - 1)$ is a square, we must have $C - 1 = im^2$ for some $m \in \mathbb{Q}(i)$. Thus, in the first case (when $C + 1 = im^2$), then

$$c = C^2 - 1 = (im^2 - 1)^2 - 1 = (-m^4 - 2im^2 + 1) - 1 = -m^2(m^2 + 2i).$$

Similarly, when $C - 1 = im^2$,

$$c = (-m^4 + 2im^2 + 1) - 1 = -m^2(m^2 - 2i).$$

Thus $f_r(x)$ is irreducible with $f_r^2(x)$ reducible if and only if $c = -m^2(m^2 \pm 2i)$. $\square$

Remark. *Since*

$$-m^2(m^2 + 2i) = \overline{-\bar{m}^2(\bar{m}^2 - 2i)},$$

by Corollary 2.0.1 we may restrict our study to $-m^2(m^2 - 2i)$, since k_n for $f_{\bar{r}}^n$ (the number of factors over $\mathbb{Q}(i)$ when $\bar{r} = 1/\bar{c}$) is the same as k_n for f_r^n.

Since f_r is reducible if and only if $c = m^2$, we see that in this case f splits into

$$f_r(x) = x^2 + 1/m^2 = (x - i/m)(x + i/m) =: g_1(x) \cdot g_2(x). \tag{3.1}$$

We now prove the $\mathbb{Z}[i]$ analogue of [1, Proposition 2.3]:

Proposition 3.0.2. *Let $r = 1/c$ and $c = m^2 \in \mathbb{Z}[i]\backslash\{0\}$. Let $g_1(x) = x - \frac{i}{m}$, $g_2(x) = x + \frac{i}{m}$. Then $f = g_1 \cdot g_2$. Moreover, $g_1(f_r(x))$ factors if and only if $1 - im$ is a square in $\mathbb{Z}[i]$, while $g_2(f_r(x))$ factors if and only if $1 + im$ is a square in $\mathbb{Z}[i]$.*

Proof. First observe that $g_1(f_r(x)) = x^2 + \frac{1-im}{m^2}$ and $g_2(f_r(x)) = x^2 + \frac{1+im}{m^2}$, hence g_1 splits if and only if $\frac{1-im}{m^2}$ is a square in $\mathbb{Q}(i)$, if and only if $1 - im$ is a square in $\mathbb{Z}[i]$. The g_2 case is clear. $\square$

The following proposition is the $\mathbb{Z}[i]$ analogue of [1, Proposition 2.4]. It requires that we consider a few extra r values with $g_2(f_r^2(0))$ square in K:

Proposition 3.0.3. *Let $r = 1/c$, $c = m^2 \in \mathbb{Z}[i]\backslash\{0\}$ and let g_1, g_2 be as above. If $g_2(f_r(x))$ is irreducible, then $g_2(f_r^2(x))$ is reducible if and only if*

$$m \in \{4i, \pm 2 + 2i\} = S.$$

Similarly, if $g_1(f_r(x))$ is irreducible, then $g_1(f_r^2(x))$ is reducible iff $m \in -S$.

Proof. Note $g_2(f_r^2(0)) = \frac{im^3+m^2+1}{m^4} = \frac{(-im)^3-(-im)^2+1}{m^4}$ and $g_1(f_r^2(0)) = \frac{-im^3+m^2+1}{m^4} = \frac{(im)^3-(im)^2+1}{m^4}$. Thus $g_2(f_r^2(0))$ or $g_1(f_r^2(0))$ being a square in $\mathbb{Q}(i)$ corresponds to a $\mathbb{Z}[i]$-integral point on the elliptic curve Q:

$$Q : y^2 = ix^3 + x^2 + 1 = (-ix)^3 - (-ix)^2 + 1 = z^3 - z^2 + 1.$$

This curve has label 2.0.4.1-4232.1-a1 in the LMFDB [8] and has Mordell-Weil generators

$$\langle (-i + 1 : 2i - 1 : 1), (0 : -i : 1) \rangle.$$

We can compute integral points over number fields in MAGMA [9] with code from Thongjunthug's thesis [10]. This curve thus has $\mathbb{Z}[i]$-integral points

$$\{(x, \pm y)\} = \{(0, 1), (1, 1), (-1, i), (-1 - i, 2 - i), (-1 + i, 2 + i), (1 \pm i, i),$$

$$(2 - 2i, 1 - 4i), (2 + 2i, 1 + 4i), (-1 - 3i, 6 + i), (-1 + 3i, 6 - i), (4, 7),$$

$$(3 - 9i, 10 + 27i), (3 + 9i, 10 - 27i), (-13 - 4i, 22 - 47i), (-13 + 4i, 22 + 47i)\}.$$

The x coordinates correspond to m values where $g_2(f_{1/m^2}^2(x))$ potentially splits. Let S'' denote the set of all these x coordinates:

$$S'' = \{0, \pm 1, 4, \pm 1 \pm i, -1 \pm 3i, 2 \pm 2i, 3 \pm 9i, -13 \pm 4i\}.$$

We made the substitution $x = -im$ to obtain the equation of Q. Denote by S' the corresponding m values:

$$S' = \{0, \pm i, 4i, \pm 1 \pm i, \pm 3 - i, \pm 2 + 2i, \pm 9 + 3i, \pm 4 - 13i\}.$$

By inspection, the only values of $m \in S'$ that yield $g_2(f_r^2(x))$ reducible are $S := \{4i, \pm 2 + 2i\}$. The corresponding m-values such that $g_1(f_r^2(x))$ is reducible are the negatives of these: $-S = \{-4i, \pm 2 - 2i\}$.

Conversely, if $m = 4i$, then

$$g_2(f_r^2(x)) = (x^2 - x + \frac{7}{16})(x^2 + x + \frac{7}{16}).$$

If $m = \pm 2 + 2i$, then

$$g_2(f_r^2(x)) = (x^2 - ix - \frac{4 \pm i}{8})(x^2 + ix - \frac{4 \pm i}{8}).$$

This shows that $g_2(f_r^2(x))$ is reducible for these m values. □

3.1 When f_r is reducible

In this section, we suppose $c = m^2 \in \mathbb{Z}[i] \backslash \{0, -1\}$ so that $f_r = g_1 \cdot g_2 = (x - i/m)(x + i/m)$ is reducible. If w_n is the numerator of $g_2(f^{n-1}(0))$, then by Proposition 2.1.1, we have $\{w_n\}_{n \geq 1}$ is a rigid divisibility sequence.

First suppose $g_i(f^n(x))$ is irreducible. By the remark following Lemma 2.0.2, for $n \geq 2$, $g \circ f_r^n$ is irreducible provided that $g \circ f_r^{n-1}$ is irreducible and $g \circ f_r^n(0)$ is not a square in $\mathbb{Q}(i)$. Recall that

$$S' = \{0, \pm i, 4i, \pm 1 \pm i, \pm 3 - i, \pm 2 + 2i, \pm 9 + 3i, \pm 4 - 13i\}$$

is the set of m values such that $g_2(f^2_{1/m^2}(0))$ has a square numerator: we handle these cases in the next subsection.

The following $\mathbb{Z}[i]$ analogue of [1, Proposition 2.7] gives us equivalence classes for m that will yield $g_i(f^n(x))$ irreducible for all n. We rely solely on Mathematica [11] code to determine the following and all other Gaussian integer congruence arguments for the rest of this thesis.

Proposition 3.1.1. *Let $r = 1/c$ and $c = m^2 \in \mathbb{Z}[i]\backslash\{0, -1\}$ with $m \notin S'$ from Proposition 3.0.3. Let g_1, g_2 as in eq. (3.1). Then $g_2(f^n_r(x))$ is irreducible for all $n \geq 2$ if m is in one of the following equivalence classes. For g_1, replace the equivalence class m mod z with $-m$ mod z:*

$m \equiv 1,\ 1+i$	$(\text{mod } 2)$	$m \equiv -1$	$(\text{mod } 2+i)$
$m \equiv \pm 1$	$(\text{mod } 2+2i)$	$m \equiv \pm 1$	$(\text{mod } 3)$
$m \equiv -1+i,\ 1$	$(\text{mod } 3+i)$	$m \equiv -2$	$(\text{mod } 3+2i)$
$m \equiv \pm 2-i$	$(\text{mod } 4)$	...	(cont'd in Appendix Table A.1)

Table 3.1: Congruences that ensure w_n is non-square for $n \geq 2$, provided that $m \notin S'$

If in addition $1+im$ and $m-i$ are non-square in $\mathbb{Z}[i]$, then the following congruences also suffice:

$m \equiv 1$	$(\text{mod } 3+2i)$	$m \equiv \pm 2 + i$	$(\text{mod } 4)$
$m \equiv -1-2i,$	$(\text{mod } 4+i)$	$m \equiv -3i$	$(\text{mod } 4+4i)$
$-2i,\ 1,\ 2$			
$m \equiv -1, 2-2i$	$(\text{mod } 5+i)$	$m \equiv -3+i,$	$(\text{mod } 5+2i)$
		$-1 \pm 2i$	
		...	(cont'd in Appendix Table A.2)

Table 3.2: Congruences that ensure w_n is non-square for $n \geq 2$, provided that $m \notin S'$ and $1 + im$ and $m - i$ are non-square in $\mathbb{Z}[i]$

Proof. Denote by w_n the numerator of $g_2(f_r^{n-1}(0))$, we wish to show that w_n is non-square for all n. Then by Lemma 2.0.2, $g_2(f_r^n(x))$ is irreducible.

Note that for $n \geq 2$, the denominator of $g_2(f_r^{n-1}(0))$ is $m^{2^{n-1}}$, hence square. Following Proposition 2.1.1, $\{w_n\}_{n>0}$ is a rigid divisibility sequence. By the proof of Proposition 3.0.3, $m \notin S'$ implies that w_3, the numerator of $g_2(f^2(0))$, is non-square. We now show w_3 has a prime divisor of odd multiplicity, i.e $w_3 \neq i\alpha^2$ for any $\alpha \in \mathbb{Z}[i]$. We thus consider a twist of the elliptic curve Q defining w_3 from Proposition 3.0.3; we show there are no $\mathbb{Z}[i]$ points on the elliptic curve $C_3 : iy^2 = x^3 - x^2 + 1$. Note that

$$y^2 = -ix^3 + ix^2 - i = (ix)^3 - i(ix)^2 - i = z^3 - iz^2 - i.$$

Sage [12] tells us that the elliptic curve above has rank 0 and trivial torsion, hence $C_3(\mathbb{Q}(i)) = \{\infty\}$. Thus if w_3 is non-square, it is not of the form $i\alpha^2$, so it must have a prime divisor of odd multiplicity. Rigid divisibility then states that w_{3j} is non-square in $\mathbb{Z}[i]$ for all $j \geq 1$.

We know $g_2(f_r^2(x))$ is irreducible when $m \notin S'$ by Proposition 3.0.3. By the remark after Lemma 2.0.2, $g \circ f_r^n$ is irreducible provided that $g \circ f_r^{n-1}$ is irreducible and $g \circ f_r^n(0)$ is not a square in $\mathbb{Q}(i)$. Since the sequence $\{w_n \bmod z\}_{n\geq 1}$ eventually cycles, we find moduli z and values for $m \not\equiv 0 \bmod z$ ensuring that this cycle consists of non-square values modulo z. Since w_{3j} is non-square in $\mathbb{Z}[i]$ for all $j \geq 1$, we only need to find primes $\pi \in \mathbb{Z}[i]$ ensuring that w_{3j+1}, w_{3j+2} are non-square mod π for all $j \geq 1$ for table A.1.

If in addition $w_2 = 1 + im$ is non-square, then $1 + im$ has some prime divisor with odd multiplicity if and only if $m - i$ is non-square: note

$$1 + im \neq i\alpha^2 \iff i(m-i) \neq i\alpha^2 \iff m - i \neq \alpha^2.$$

Hence $1 + im$ has a prime divisor of odd multiplicity since itself and $m - i$ are non-square by hypothesis. This prime divisor of odd multiplicity divides w_{2j} with that same multiplicity by rigid divisibility, so w_{2j} is non-square for all $j \geq 1$. Now the congruences in the second table suffice.

□

3.1.1 The case $m \in S'$

We consider now m in the set

$$S' = \{0, \pm i, 4i, \pm 1 \pm i, \pm 3 - i, \pm 2 + 2i, \pm 9 + 3i, \pm 4 - 13i\}$$

from Proposition 3.0.3. These are m-values such that $g_2(f^2_{1/m^2}(0))$ has a square numerator, while

$$m \in S = \{4i, \pm 2 + 2i\} \subset S'$$

are the only such values where $g_2(f^2_{1/m^2}(x))$ is indeed reducible, provided $g_2(f_r)$ was irreducible (i.e. $1 + im \notin \mathbb{Z}[i]^2$). The case $m \in S$ is handled in Propositions 3.1.3 and 3.1.4. We'll show that the remaining m values with $c = m^2 \notin \{0, -1\}$ pose no issue.

We need only consider $m \in \{1 + i, 3 - i, 9 + 3i, 4 - 13i\}$ by Corollary 2.0.1; note

$$(-3 - i)^2 = 8 + 6i = \overline{(3 - i)^2} = \overline{8 - 6i},$$

but f_{1/m^2} and $f_{1/\bar{m}^2}$ have the same number of factors sequence $\{k_n\}_{n>0}$.

Proposition 3.1.2. *Let $r = 1/c$ and $c = m^2 \in \mathbb{Z}[i]\backslash\{0, -1\}$, and let g_2 as in eq. (3.1). If $1 + im$ is non-square in $\mathbb{Z}[i]$ and $m \in S'\backslash S$, then $g_2(f^n_r(x))$ is irreducible for all $n \geq 1$.*

Proof. Since $1 + im \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ and $m \in S'\backslash S \implies m \notin S$, $g_2(f_r)$ and $g_2(f^2_r)$ are irreducible by Propositions 3.0.2 and 3.0.3. By the remarks preceding, we consider

$m \in \{1+i, 3-i, 9+3i, 4-13i\}$. However $g_2(f^2_{1/m^2}(0))$ and thus w_3 is a square in $\mathbb{Q}(i)$. For the rest of this proof, showing that $g_2(f^n_{1/m^2}(0))$ is non-square for all $n \geq 3$ suffices: inductively, we prove $g_2(f^n_{1/m^2}(x))$ is irreducible for $n \geq 2$. Since $g_2(f^n_{1/m^2}(x))$ is irreducible for some $n \geq 2$ and $g_2(f^{n+1}_{1/m^2}(0))$ is non-square, we have $g_2(f^{n+1}_{1/m^2}(x))$ is irreducible by Lemma 2.0.2.

When $m = 1+i$, we find that $\{w_n \bmod 6+i\}_{n\geq 2}$ is the following sequence:

$$\{i, -1, -3i, 2-2i, 3i, 2+i, i, 3i, 3-2i, 2-i, 2-2i, 1-2i, 2, -2+2i, -2+i,$$

$$-1-i, 1+3i, -i, i, 3i, 3-2i...\}$$

where a cycle of non-squares begins at $w_8 \equiv i \equiv w_{20} \bmod 6+i$. The only squares mod $6+i$ in this sequence occur at $w_2 \equiv -1$ and $w_6 \equiv 2+i \equiv (2i)^2 \bmod 6+i$ However, we have that $w_6 \equiv -i \bmod 2+i$ is non-square. Thus $g_2(f^n_{1/2i}(0))$ is non-square for all $n \geq 3$.

When $m \in \{3-i, 9+3i\}$, note that

$$\{w_n\}_{n\geq 2} \equiv \{-1+i, -1+i, -i, -1-i, -i, -1-i, ...\} \bmod 3+2i.$$

Since i and $-1-i$ are non-square mod $3+2i$, we have a cycle of non-squares beginning at w_4. Thus $g_2(f^n_{1/m^2}(0))$ is non-square for all $n \geq 3$.

Lastly, when $m = 4-13i$, again note that

$$\{w_n\}_{n\geq 2} \equiv \{-i, -1, -2, 1, i, 2, i, 2, ...\} \bmod 3+2i.$$

Since $\pm i$ and ± 2 are non-squares mod $3+2i$, we have a cycle of non-squares beginning at $w_6 \equiv i \bmod 3+2i$. We need only show that w_5 is non-square. However,

note $w_5 \equiv 1 + 3i \bmod 5 + 2i$ is non-square. Thus $g_2(f^n_{1/m^2}(0))$ is non-square for all $n \geq 3$ and we're done. □

The following is a $\mathbb{Z}[i]$ analogue of [1, Corollary 2.9], giving conditions such that the number of factors sequence for f is $\{k_n\} = \{2, 2, 2..\}$ when $N(c) \leq 10^9$.

Corollary 3.1.1. *Let $r = 1/c$ and $c = m^2 \in \mathbb{Z}[i]\backslash\{0, -1\}$, and let g_2 as in eq. (3.1). Suppose that $m \notin S = \{4i, \pm 2 + 2i\}$ and $N(c) = N(m^2) \leq 10^9$. If $1 + im$ is non-square in $\mathbb{Z}[i]$ then $g_2(f^n_r(x))$ is irreducible for all $n \geq 1$. If in addition $1 - im$ is non-square in $\mathbb{Z}[i]$ and $m \notin -S$, then $f^n_r(x)$ is a product of two irreducible factors for all $n \geq 1$.*

Proof. By hypothesis, $1 + im \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ and $m \notin S$ so $g_2(f_r)$ and $g_2(f^2_r)$ are irreducible over $\mathbb{Z}[i]$ by Propositions 3.0.2 and 3.0.3. If $m \in S'\backslash S$ we may apply Proposition 3.1.2 to conclude $g_2(f^n_r(x))$ is irreducible for all $n \geq 1$.

Now suppose $m \notin S'$, with $N(m^2) \leq 10^9$, so $|m| \leq 10^{9/4} \approx 178$. It suffices to show that $g_2(f^n_r(0))$ is non-square in $\mathbb{Q}(i)$ for all $n \geq 3$ by Lemma 2.0.2. The first group of congruences in Proposition 3.1.1 applies to all $m \notin S'$ with $|m| \leq 10^{9/4}$ except for a set of 2,429 values. Of these, 58 have the property that $\{1 + im, m - i\}$ contains a square. We apply the second group of congruences in Proposition 3.1.1 to the remaining 2,371 values, and only 186 survive. This leaves 244 values that we must handle via other methods.

To do this, we search for primes $\pi \in \mathbb{Z}[i]$ such that

$$\{g(f^n(0))\}_{n\geq 1} \text{ eventually cycles between non-squares modulo } \pi. \qquad (\circledast)$$

If we find such a π, it implies that all but finitely many terms of the sequence $\{g_2(f_r^n(0))\}_{n\geq 2}$ are non-squares in $\mathbb{Q}(i)$. We then reduce modulo other primes to show that the remaining terms are non-squares.

Of the 244 m-values left over from the first paragraph of this proof, all have a prime $|\pi| < 141$ that satisfies condition $\circledast$ and reduce modulo small primes until all have been proven non-square. The m-value producing the largest number of such terms is $m = -14 - 176i$, where we must check that each of $g_2(f_r(0))$, $g_2(f_r^2(0))$, ... $g_2(f_r^{50}(0))$ is a non-square. In all cases the desired result is achieved by reducing modulo primes of norm less than 100.

The case for irreducibility of $g_1(f_r^n(x))$ is identical. However note if (m, z) is a moduli class that is used to prove irreducibility of $g_2(f_r^n(x))$, $(-m, z)$ can be used to prove irreducibility of $g_1(f_r^n(x))$ by Proposition 3.1.1. □

Note $m = 4i$, $\pm 2 + 2i$ are the only values with $g_2(f_{1/m^2}^2(x))$ reducible. When $m = 4i$,

$$g_2(f_{-1/16}^2(x)) = (x^2 - x + 7/16)(x^2 + x + 7/16) =: g_{21}(x)g_{22}(x) \tag{3.2}$$

and when $m = \pm 2 + 2i$,

$$\begin{aligned} g_2(f_{1/(\pm 2+2i)^2}^2(x)) &= (x^2 - ix - (4 \pm i)/8)(x^2 + ix - (4 \pm i)/8) \\ &=: g_{23}(x)g_{24}(x), \end{aligned} \tag{3.3}$$

These factors have discriminants $\mathrm{Disc}_x(g_{21}) = \mathrm{Disc}_x(g_{22}) = \frac{11}{4}$ and $\mathrm{Disc}_x(g_{23}) =$

$\frac{2\pm i}{2} = \mathrm{Disc}_x(g_{24})$, all non-squares in $\mathbb{Q}(i)$, hence they are irreducible polynomials over $\mathbb{Q}(i)$.

Remark. *We'll consider only the case $m = 2+2i$ since $c = (-2+2i)^2 = -8i = \bar{8}i = (2+2i)^2$, and since $\{f_r^n\}$ and $\{f_{\bar{r}}^n\}$ have the same number of factors over $\mathbb{Q}(i)$ by Corollary 2.0.1.*

The following analogue of [1, Proposition 2.10] uses the same method of proof. In the rest of this thesis, $\left[\frac{\cdot}{\alpha}\right]$ and $\left[\frac{\cdot}{\pi}\right]_2$ refer to the Gaussian Jacobi and Gaussian Legendre symbols (respectively) as in [13]. Thus if $\alpha = \pi_1^{a_1} \cdot \pi_2^{a_2} \cdots \pi_n^{a_n}$ is a prime factorization of $\alpha \in \mathbb{Z}[i]$, then

$$\left[\frac{\beta}{\alpha}\right] = \left[\frac{\beta}{\pi_1}\right]_2^{a_1} \cdot \left[\frac{\beta}{\pi_2}\right]_2^{a_2} \cdots \left[\frac{\beta}{\pi_n}\right]_2^{a_n} = -1 \quad \text{if } \beta \text{ is a non-residue mod } \alpha.$$

Proposition 3.1.3. *Let $r = -1/16$ and let g_{21} and g_{22} be as in eq. (3.2). For all $n \geq 1$, both $g_{21}(f_r^n(x))$ and $g_{22}(f_r^n(x))$ are irreducible for all $n \geq 1$. In particular $f_{-1/16}^n(x)$ has $k_n = 3$ irreducible factors for all $n \geq 3$.*

Proof. By Lemma 2.0.2 it suffices to prove that neither $g_{21}(f_r^n(0))$ nor $g_{22}(f_r^n(0))$ is a square for all $n \geq 1$. Observe that $f_r^n(0) \equiv 5i \bmod 6+5i$ for $n \geq 5$, and $g_{21}(5i) \equiv -2+3i \bmod 6+5i$, with $\left[\frac{-2+3i}{6+5i}\right] = -1$. Thus we need only show $\{g_{21}(f_r^n(0))\}$ is non-square for $1 \leq n \leq 4$. Note $g_{21}(f_r^n(0))$ is non-square modulo $6+i$ for $1 \leq n \leq 3$, and $g_{21}(f_r^4(0))$ is non-square modulo $10+i$. Thus $g_{21}(f_r^n(0))$ is non-square for all $n \geq 1$.

For $g_{22}(f_r^n(0))$ we have a simpler argument using $p = 2+i$: observe that

$$g_{22}(0) \equiv g_{22}(-1) \equiv -i \bmod 2+i$$

and $f_r^n(0) \equiv 0$ or $-1 \bmod 2+i$ for all $n \geq 1$, with $\left[\frac{i}{2+i}\right] = -1$. □

We also prove the following $\mathbb{Z}[i]$ analogue of [1, Proposition 2.10], requiring only minor modifications:

Proposition 3.1.4. *Let $r = \pm 1/(8i)$ and let g_{23} and g_{24} be as in eq. (3.3). For all $n \geq 1$, both $g_{23}(f_r^n(x))$ and $g_{24}(f_r^n(x))$ are irreducible. In particular $f^n_{\pm 1/(8i)}(x)$ has $k_n = 3$ irreducible factors for all $n \geq 3$.*

Proof. We prove this for $r = 1/(8i)$ since the same conclusion holds for $r = -1/(8i)$ by Corollary 2.0.1.

As in Proposition 3.1.3 it suffices to prove that neither $g_{23}(f^n_{1/(8i)}(0))$ nor $g_{24}(f_r^n(0))$ is a square for all $n \geq 1$. Observe that $f^n_{1/(8i)}(0) \equiv 3+2i \bmod 8+3i$ for $n \geq 4$, and $g_{23}(3+2i) \equiv 3+3i \bmod 8+3i$, with $\left[\frac{3+3i}{8+3i}\right] = -1$. Thus we need only show $\{g_{21}(f_r^n(0))\}$ is non-square for $1 \leq n \leq 3$, but $g_{23}(f_r^n(0))$ is still non-square modulo $8+3i$ for $1 \leq n \leq 2$, and $g_{23}(f_r^3(0))$ is non-square modulo 3. Thus $g_{23}(f_r^n(0))$ is non-square for all $n \geq 1$.

For $g_{24}(f_r^n(0))$, observe that $g_{24}(-2+3i) \equiv 5i \bmod 8+7i$, and $g_{24}(1+3i) \equiv 6+i \bmod 8+7i$ while $f_r^n(0) \equiv -2+3i$ or $1+3i \bmod 8+7i$ for all $n \geq 2$, with $\left[\frac{5i}{8+7i}\right] = \left[\frac{6+i}{8+7i}\right] = -1$. When $n = 1$, we can reduce mod 3 to see that $g_{24}(f_r(0))$ is non-square.

For g_{24}, the same argument as that for g_{22} in Proposition 3.1.3 applies modulo $2+i$. □

We can sum up the results of this section (3.1.1) as the proof of item (2) of Conjecture 1, and the proof of item (1) of the same conjecture up to our norm bound:

Theorem 3.1.1. *Let $f_r = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then,*

(1) *Suppose $N(c) \leq 10^9$. We have $k_n = 2$ for all n if and only if $c = m^2 \notin \{\pm 8i, -16\}$ and $1 \pm im$ is non-square.*

(2) *We have $k_1 = k_2 = 2$ and $k_3 = 3$ if and only if $c \in \{\pm 8i, -16\}$. In this case $k_n = 3$ for all $n \geq 3$.*

3.1.2 The case when $c = -(s^2 - 1)^2$

Now suppose $1 \pm im$ is square, so $1 \pm im = s^2$ with $s \neq \pm 1$, so that $m = \pm i(s^2 - 1)$ and $f_r(x) = x^2 + 1/m^2 = x^2 - 1/(s^2 - 1)^2$. If $1 - im = s^2$, we then have

$$\begin{aligned} g_1(f_r(x)) = (x^2 + 1/m^2) - i/m &= \left(x^2 - \frac{1}{(s^2-1)^2}\right) - \frac{i}{i(s^2-1)} \\ &= x^2 - \frac{s^2}{(s^2-1)^2} \\ &= \left(x - \frac{s}{s^2-1}\right)\left(x + \frac{s}{s^2-1}\right) \\ &:= h_1(x)h_2(x). \end{aligned} \tag{3.4}$$

and if $1+im = s^2$ with $|s|>1$, so $m = -i(s^2-1)$, we then have

$$\begin{aligned} g_2(f_r(x)) = (x^2+1/m^2) + \frac{i}{m} &= \left(x^2 - \frac{1}{(s^2-1)^2}\right) + \frac{i}{-i(s^2-1)} \\ &= x^2 - \frac{s^2}{(s^2-1)^2} \\ &= \left(x - \frac{s}{s^2-1}\right)\left(x + \frac{s}{s^2-1}\right) \\ &= h_1(x)h_2(x). \end{aligned} \tag{3.5}$$

Now

$$h_1(f_r(x)) = x^2 - \frac{1}{(s^2-1)^2} - \frac{s}{s^2-1} = x^2 + \frac{-s^3+s-1}{(s^2-1)^2} = x^2 - \frac{s^3-s+1}{(s^2-1)^2}$$

while

$$h_2(f_r(x)) = x^2 - \frac{1}{(s^2-1)^2} + \frac{s}{s^2-1} = x^2 + \frac{s^3-s-1}{(s^2-1)^2}.$$

Note $h_1(f_r(x))$ is irreducible unless s is the x-coordinate of an integral point on the elliptic curve $C : y^2 = x^3 - x + 1$. This curve has label 2.0.4.1-2116.1-a1 in the LMFDB [8] with free rank 1 and trivial torsion. The Mordell-Weil generator is $(1:1:1)$, which is also the generator of $E(\mathbb{Q})$ (label 92.a1 in the LMFDB). Thus the $\mathbb{Z}[i]$-integral points are the $\mathbb{Z}$-integral points:

$$\{(x, \pm y)\} = \{(\pm 1, 1), (0,1), (3,5), (5,11), (56, 419)\}.$$

Note $s \neq \pm 1$ since $c \neq 0$. Thus, if $s \notin \{3, 5, 56\}$, then $h_1(f_r(x))$ is irreducible.

Note $h_2(f_r(x))$ is irreducible unless s is the x-coordinate of an integral point on the elliptic curve $y^2 = x^3 - x - 1 = -(-x^3 + x + 1) = -((-x)^3 - (-x) + 1)$, so

$(iy)^2 = (-x)^3 - (-x) + 1$. This is a reparametrization of the curve C above. Again $s \neq \pm 1$, so if $-s \notin \{3, 5, 56\}$, then $h_2(f_r(x))$ is irreducible.

Now [1, Corollary 2.11] translates into the following $\mathbb{Z}[i]$ analogue:

Corollary 3.1.2. *Let $r = 1/c$ and $c = -(s^2-1)^2$ for $s \in \mathbb{Z}[i]/\{0, \pm 1\}$, and let g_1, g_2 be as in eq. (3.1) and h_1, h_2 be as in eq. (3.4). Suppose that $N(c) = N((s^2-1)^2) \leq 10^9$. If $s \notin \{3, 5, 56\}$ then for all $n \geq 1$ we have $h_1(f_r^n(x))$ irreducible. If $s \notin \{-3, -5, -56\}$ then $h_2(f_r^n(x))$ irreducible. In particular, if $N((s^2-1)^2) \leq 10^9$ and $\pm s \notin \{3, 5, 56\}$, then $f_r^n(x)$ has $k_n = 3$ irreducible factors for all $n \geq 2$.*

Proof. Note $N(c) = |(s^2-1)^2|^2 \leq 10^9 \iff |s^2 - 1| \leq 10^{9/4} \approx 178$ implies $|s| < 14$. To show that $h_k(f_r^n(x))$ is irreducible for $n \geq 1$, we show that $\{h_k(f_r^n(0))\}$ contains no squares in $\mathbb{Q}(i)$. To verify that $h_k(f_r^n(0))$ is non-square in $\mathbb{Q}(i)$ for all $n \geq 2$, we search for primes p so that $\{h_k(f^n(0))\}_{n \geq 1}$ satisfies condition $\circledast$.

By the discussion above this theorem, $s \notin \{3, 5, 56\} \implies h_1(f_r(x))$ is irreducible. Now, for each $s \in \mathbb{Z}[i] \backslash \{0, \pm 1\}$ with $|s| < 14$, we find there exists a prime $|p| \leq 141$ with this desired property.

For each such s and p, we take the finitely many terms of the sequence $\{h_1(f^n(0))\}_{n \geq 2}$ that have not been proven non-square, and reduce modulo small primes until all have been proven non-square. The s-values producing the most terms to check are from $s = -66 + 14i$ or $s = 37 - 24i$, where we must check that

each of $h_1(f_r(0)), h_1(f_r^2(0)), ..., h_1(f_r^{89}(0)))$ is a non-square. In all cases, the desired result is achieved by reducing modulo primes π with $|\pi| < 141$.

The analysis for h_2 is analogous: $s \notin \{-3, -5, -56\} \implies h_2(f_r(x))$ is irreducible; there exists a prime so that $\{h_2(f_r(x) \bmod p)\}_{n\geq 2}$ cycles between non-squares; and we find that the largest number of such terms are from $s = -37 + 24i$, $66 - 14i$ where we must check also that $h_2(f_r(0))$,..., $h_2(f_r^{89}(0))$ are non-square.

□

When $\pm s \in \{3, 5, 56\}$, $h_k(f(x))$ is no longer guaranteed to be irreducible; indeed for $s \in \{3, 5, 56\}$ we have

$$h_1(f(x)) = \left(x - \frac{\sqrt{s^3 - s + 1}}{s^2 - 1}\right)\left(x + \frac{\sqrt{s^3 - s + 1}}{s^2 - 1}\right) =: h_{11}(x)h_{12}(x). \tag{3.6}$$

while for $s \in \{-3, -5, -56\}$ we have

$$h_2(f(x)) = \left(x - \frac{\sqrt{(-s)^3 - (-s) + 1}}{s^2 - 1}\right)\left(x + \frac{\sqrt{(-s)^3 - (-s) + 1}}{s^2 - 1}\right) =: h_{21}(x)h_{22}(x). \tag{3.7}$$

We now prove the $\mathbb{Z}[i]$ analogue of [1, Proposition 2.12]:

Proposition 3.1.5. *Let $r = 1/c$ and $c = -(s^2 - 1)^2 \in \mathbb{Z}[i]\backslash\{0, \pm 1\}$. Let $j, k \in \{1, 2\}$, g_j, h_k, and h_{kj} be as in eqs. 3.1, 3.4 and 3.6-3.7. If $s \in \{3, 5, 56\}$ and $1 - im = s^2$, then for all $n \geq 1$ we have $g_2(f_r^n(x))$, $h_2(f_r^n(x))$, $h_{11}(f_r^n(x))$ and $h_{12}(f_r^n(x))$ irreducible. If $1 + im = s^2$, replace g_2 with g_1. If $s \in \{-3, -5, -56\}$ and $1 - im = s^2$, then for all $n \geq 1$ we have $g_2(f_r^n(x))$, $h_1(f_r^n(x))$, $h_{21}(f_r^n(x))$ and*

$h_{22}(f_r^n(x))$ irreducible. If $1+im=s^2$, replace g_2 with g_1. In particular, $f_r^n(x)$ has $k_n=4$ irreducible factors for all $n\geq 3$.

Proof. We'll show this is the case for $s\in\{3,5,56\}$; the case that $s\in\{-3,-5,-56\}$ is analogous.

First note that if $1+im=s^2$ then $g_2(f_r(x))$ is reducible while $g_1(f_r(x))$ is irreducible, and vice-versa for $1-im=s^2$. To show they cannot both be a square in $\mathbb{Z}[i]$, suppose $1+im=s^2$ with $1-im=j^2$. Then we have $2=j^2+s^2=(j+is)(j-is)$. If $j+is=\pm i$, then $j-is=\mp 2i$, so $2j=\mp i$, a contradiction since $j\in\mathbb{Z}[i]$. We obtain a similar contradiction when $j+is=\pm 1$. Then $j+is=1+i$, $j-is=1-i$ without loss of generality. In this case, $2j=2$, $2is=2i$ so $j=1=s$, and $1+im=1-im$, impossible unless $m=0$.

Suppose now that $1-im=s^2$ to show $g_2(f_r^n(x))$ is irreducible for all $n\geq 2$ for $s\in\{3,5,56\}$. Note $1+im$ is therefore non-square by the above remarks, thus $g_2(f_r(x))$ is irreducible by Proposition 3.0.2.

Since $g_2(f_r(x))$ is irreducible and $m\in\{8i,24i,(56^2-1)i\}$ when $s\in\{3,5,56\}$, we have $g_2(f_r^2(x))$ is irreducible by Proposition 3.0.3. We'll show that $\{g_2(f_r^n(0))\}_{n\geq 3}$ contains no squares, so that by Lemma 2.0.2, $g_2(f_r^n(x))$ is irreducible for all $n\geq 3$.

First let $s=3$ so that $m=8i$. We'll show that w_n (the numerator of

$g_2(f_r^{n-1}(0)) = \frac{w_n}{m^{2^{n-1}}}$) is non-square for all $n \geq 3$. Consider

$$\{w_n \bmod 24+i\}_{n\geq 3} \equiv \{6-6i, -2+8i, -3, -1, -5i, 6+4i, -5i, 6+4i, ...\},$$

and note that $-5i$ and $6+4i$ are non-square mod $24+i$. Since $-2+8i$ is non-square mod $24+i$ as well, we need only verify that w_n is non-square for $n \in \{3,5,6\}$. However, we find that $w_3 \equiv w_6 \equiv -i \bmod 2+i$ and $\left[\frac{-i}{2+i}\right] = -1$, and $w_5 \equiv 1+i \bmod 3+2i$ with $\left[\frac{1+i}{2+i}\right] = -1$.

When $s = 5$, then $m = (5^2-1)i = 24i$, so $m \equiv 2-i \mod 4+i$. Note that

$$\{w_n \bmod 4+i\}_{n\geq 3} \equiv \{1-i, 1+i, 1+2i, 1-i, 1+i, 1+2i, ...\},$$

and that $1 \pm i$ and $1+2i$ are non-square mod $4+i$, so w_n is non-square for all $n \geq 3$.

When $s = 56$, then $m = (56^2-1)i$. Again, $m \equiv 2-i \mod 4+i$, so

$$\{w_n \bmod 4+i\}_{n\geq 3} \equiv \{1-i, 1+i, 1+2i, 1-i, 1+i, 1+2i, ...\}.$$

Thus $g_2(f_r^n(x))$ is irreducible for all $n \geq 3$ when $s \in \{3,5,56\}$.

Now, we show $h_2(f_r^n(x))$ is irreducible for $n \geq 1$ for $s \in \{3,5,56\}$. By the above discussion, if $s \in \{3,5,56\}$, then $h_2(f_r(x))$ irreducible. Again, we'll show that $\{h_2(f_r^n(0))\}_{n\geq 2}$ contains no squares in $\mathbb{Q}(i)$.

When $s = 3$, consider

$$\{h_2(f_r^n(0)) \bmod 24+i\}_{n\geq 2} \equiv \{-6+5i, 7+8i, 8+17i, -10+16i, 6+11i, -6+7i, -6+7i, ...\},$$

so that $\left[\frac{-6+5i}{24+i}\right] = \left[\frac{-10+16i}{24+i}\right] = \left[\frac{6+11i}{24+i}\right] = \left[\frac{-6+7i}{24+i}\right] = -1$. Now we need only verify that $h_2(f_r^3(0))$ and $h_2(f_r^4(0))$ are non-square, however, $h_2(f_r^3(0)) \equiv 2 \bmod 7+2i$ and $h_2(f_r^3(0)) \equiv 3 \bmod 7+2i$, both non-squares mod $7+2i$.

When $s = 5$, consider

$$\{h_2(f_r^n(0)) \bmod 28+5i\}_{n\geq 1} \equiv \{5-i, 2-18i, -10+3i, -3-9i, 5-i, 2-18i, ...\},$$

a cycle of non-squares mod $28+5i$. Thus $\{h_2(f_r^n(0))\}_{n\geq 1}$ contains no squares in $\mathbb{Q}(i)$.

When $s = 56$, consider

$$\{h_2(f_r^n(0)) \bmod 6+5i\}_{n\geq 2} \equiv \{i, -5+4i, 2+6i, 1+6i, -4+2i, 1+6i, ...\}.$$

Since $\left[\frac{i}{6+5i}\right] = \left[\frac{2+6i}{6+5i}\right] = \left[\frac{1+6i}{6+5i}\right] = \left[\frac{-4+2i}{6+5i}\right] = -1$, we need only verify that $h_2(f_r^3(0))$ is non-square in $\mathbb{Q}(i)$. However, $h_2(f_r^n(0)) \equiv 2 \bmod 7+2i$ is non-square so we're done.

To show that $h_{11}(f_r^n(x))$ and $h_{12}(f_r^n(x))$ are irreducible for $n \geq 1$, it suffices by Lemma 2.0.2 to show that none of

$$\{h_{11}(f_r^n(0)) : n \geq 1\} \cup \{h_{12}(f_r^n(0)) : n \geq 1\}$$

is a square in $\mathbb{Q}(i)$. Note that $h_{11}(f_r(0)) = -((s^2-1)(\sqrt{s^3-s+1})+1)/(s^2-1)^2$. For $s = 5, 56$ respectively, the prime factorization of the numerator of $h_{11}(f_r(0))$ is

$$41265 = (1+2i)\cdot(2+i)\cdot(2+7i)\cdot(7+2i), \quad 1313566 = i(1+i)^2 \cdot 656783,$$

none of which is a square.

For $s = 3$, $\{h_{11}(f_r^n(0))\}_{n\geq 1} \equiv \{2-i, 1-i, 1+i, 1-i, ..\} \bmod 4+i$ for all $n \geq 2$, all non-squares modulo $4 + i$.

For $s = 5$,

$$\{h_{11}(f_r^n(0)) \bmod 6 + 5i\}_{n\geq 2} \equiv \{-2 - 3i, 4 - i, 2i, -1 + 2i, 3i, -1 + 2i, 3i, ...\}$$

with $\left[\frac{-2-3i}{6+5i}\right] = \left[\frac{4-i}{6+5i}\right] = \left[\frac{-1+2i}{6+5i}\right] = \left[\frac{3i}{6+5i}\right] = -1$, all non-square except $2i$ when $n = 4$. However, $h_{11}(f_r^4(0)) \equiv i \bmod 3 + 2i$ with $\left[\frac{i}{3+2i}\right] = -1$. Thus $\{h_{11}(f_r^n(0))\}_{n\geq 1}$ is non-square for all n.

For $s = 56$, $\{h_{11}(f_r^n(0)) \bmod 10 + 3i\}_{n\geq 2} \equiv \{3i, 5 + i, 1 - 3i, 1 - 3i, ...\}$ with $\left[\frac{3i}{10+3i}\right] = \left[\frac{1-3i}{10+3i}\right] = -1$, while for $n = 3$ we find that $h_{11}(f_r^3(0)) \equiv -2+4i \bmod 10+i$ with $\left[\frac{-2+4i}{10+i}\right] = -1$. Thus $\{h_{11}(f_r^n(0))\}_{n\geq 1}$ is non-square for all n.

To show $h_{12}(f_r(0))$ is non-square, note that for $s = 3, 5, 56$ respectively, it has numerators

$$39 = -3i(2 + 3i)(3 + 2i), \quad 263, \quad \text{and } 1313564 = -(1 + i)^4 \cdot 7 \cdot 43 \cdot 1091,$$

all non-squares in $\mathbb{Q}(i)$.

For $s = 3$, we reduce the sequence $\{h_{12}(f_r^n(0))\}_{n\geq 2}$ modulo 29 and find that it cycles among the four values 17, 15, 26, 21, none of which is a square modulo 29. For $s = 5$, we reduce modulo $10 + i$ and find that it cycles among the set $\{5 - 3i, i, 2 + i, 1 + 3i\}$, all non-squares modulo $10 + i$. For $s = 56$, we reduce the

sequence modulo $5+2i$; then $h_{12}(f_r^n(0)) \equiv -1-3i$ for all $n \geq 5$, while one verifies directly that $h_{12}(f_r^n(0))$ is non-square for $2 \leq n \leq 4$. □

We can sum up the results of this section (3.1.2) as the proof of item (4) of Conjecture 1 and the proof of item (3) of the same conjecture up to our bound 10^9 for $N(c)$:

Theorem 3.1.2. *Let $f_r = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0,-1\}$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then,*

(3) *Suppose $N(c) \leq 10^9$. We have $c = -(s^2-1)^2$ with $\pm s \in \mathbb{Z}[i]\backslash\{3,5,56\}$ if and only if $k_1 = 2$ and $k_n = 3$ for all $n \geq 2$.*

(4) *We have $k_3 \geq 4$ if and only if $c = -(s^2-1)^2$ for $\pm s \in \{3,5,56\}$. In this case $k_n = 4$ for all $n \geq 3$.*

3.2 The case when f_r is irreducible but f_r^2 reducible

If $r = 1/c$, with c satisfying $0 \neq c = -m^2(m^2-2i)$ for some $m \in \mathbb{Z}[i]$, then f is irreducible but f^2 is reducible as seen in Proposition 3.0.1:

$$\begin{aligned} f_{1/c}^2(x) &= \left(x^2 - \frac{1+i}{m}x + \frac{im^2+1}{m^2(m^2-2i)}\right)\left(x^2 + \frac{1+i}{m}x + \frac{im^2+1}{m^2(m^2-2i)}\right) \\ &=: q_1(x)q_2(x). \end{aligned} \tag{3.8}$$

These polynomials are irreducible as stated in Proposition 3.0.1. When $m = 2+2i$ however, we have $c = 48$ and obtain the factorization

$$q_2(f_{1/48}(x)) = (x^2 - \frac{x}{2} + \frac{19}{48})(x^2 + \frac{x}{2} + \frac{19}{48}) =: v_1(x)v_2(x).$$

When $m = -2 - 2i$, this is the factorization of $q_1(f_{1/48}(x))$.

This ($c = 48$) is the only c with $N(c) \leq 10^9$ such that any $q_j(f_r)$ splits, as the following $\mathbb{Z}[i]$ analogue of [1, Proposition 2.13] confirms.

Proposition 3.2.1. *Let $r = 1/c$ with $0 \neq c = -m^2(m^2 - 2i)$ for some $m \in \mathbb{Z}[i]$. If f_r^3 has strictly more than two irreducible factors, then*

$$im^6 + 3m^4 + (1+i)m^3 - (2i)m^2 + (2-2i)m + 1,$$

or

$$im^6 + 3m^4 - (1+i)m^3 - (2i)m^2 - (2-2i)m + 1.$$

is a square in $\mathbb{Q}(i)$.

Proof. The proof requires only the following modifications from [1, Proposition 2.13]: we now consider $c = -m^2(m^2 \pm 2i) \in \mathbb{Z}[i]$ governing f_r^2 irreducibility instead of $c = 4m^2(m^2 - 1) \in \mathbb{Z}$, and we use $N_{K/\mathbb{Q}(i)}$ rather than $N_{K/\mathbb{Q}}$ for a field K.

Note $f^3(x)$ has three or more irreducible factors if and only if $q_j(f_r(x))$ is reducible for some j. If $q_j(f_r(x))$ is reducible, let α be a root of $q_i(f_r(x))$, noting $\beta := f_r(\alpha)$ is a root of $q_i(x)$. By the irreducibility of $q_j(x)$, we have $|\mathbb{Q}(i)(\beta) : \mathbb{Q}(i)| = 2$. Since $q_j(f_r(x))$ is reducible, we have $|\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)| < 4$, which implies $|\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)(\beta)| = 1$, and thus $\alpha \in \mathbb{Q}(i)(\beta)$. But α is a root of $f_r(x) - \beta = x^2 + r - \beta$, and so $\alpha \in \mathbb{Q}(i)(\beta)$ is equivalent to $r - \beta$ being a square in $\mathbb{Q}(i)(\beta)$. Letting β' be the other root of q_j, then for $r = \frac{1}{-m^2(m^2-2i)}$ we have

$$N_{\mathbb{Q}(i)(\beta)/\mathbb{Q}(i)}(r - \beta) = q_j(r) = \frac{im^6 + 3m^4 \pm (1+i)m^3 - (2i)m^2 \pm (2-2i)m + 1}{m^2(m^2 - 2i)^2}.$$

The multiplicativity of the norm map implies that the numerator is square in $\mathbb{Q}(i)$.

□

In [1], the authors find values of $c = 4m^2(m^2-1)$ (yielding f^2 reducible over $\mathbb{Q}$ when f was irreducible over $\mathbb{Q}$) such that $f^3(x)$ has more than 2 irreducible factors. These correspond to integral points on the related hyperelliptic curve

$$C : y^2 = 8x^6 - 12x^5 - 4x^3 + 4x^2 + 4x^2 + 1$$

however, they find all the rational points. Note that the map $(x, y) \to ((1+i)x, y)$ is a birational transformation from our curve

$$C_{\mathbb{Z}[i]} : y^2 = ix^6 + 3x^5 - (1+i)x^3 - (2i)x^2 - (2-2i)x^2 + 1$$

to the curve C.

Rather than trying to find all $\mathbb{Q}(i)$-rational points on $C_{\mathbb{Z}[i]}$, we opt instead to brute force the search for integral points with norm less than our bound 10^9.

A computer search of the curve $C_{\mathbb{Z}[i]}$ yields our Gaussian integer analogue of Theorem 2.14 of [1]:

Theorem 3.2.1. *The only $\mathbb{Z}[i]$-points on the curve $C : y^2 = ix^6 + 3x^4 - (1+i)x^3 - (2i)x^2 - (2-2i)x + 1$ with $N(x) \leq 10^9$ are those with $x \in \{0, 1, i, \pm(1+i), 2+2i\}$.*

The following theorem is the Gaussian integer analogue of [1, Proposition 2.15]:

Corollary 3.2.1. *Let $r = 1/c$ and $c = -m^2(m^2 - 2i) \neq 0$, with $N(c) \leq 10^9$. Then $f_r^3(x)$ has more than 2 irreducible factors if and only if $m = \pm(2 + 2i)$.*

Proof. That $m = \pm(2 + 2i)$ is sufficient follows from the discussion above. To see that $m = \pm(2 + 2i)$ is necessary, assume that $f_r^3(x)$ has more than two irreducible factors. By Proposition 3.2.1, $\pm m$ is the x-coordinate on $y^2 = im^6 + 3m^4 - (1 + i)m^3 - (2i)m^2 - (2 - 2i)m + 1$. Since $c = -m^2(m^2 - 2i) \neq 0$ and $N(c) \leq 10^9$, we have $\pm m \in \{0, \pm(1 + i), 2 + 2i\}$ by Theorem 3.2.1. Since $c \neq 0$, $m = \pm(2 + 2i)$. □

Recall that k_n denotes the number of factors of $f_r^n(x)$ over $\mathbb{Z}[i]$. For $N(c) \leq 10^9$, we now prove that $\{k_n\}_{n\geq 1} = \{1, 2, 3, 3, 3, ...\}$ for $-m^2(m^2 - 2i)$ if and only if $m = \pm(2 + 2i)$.

Since for $m = 2 + 2i$ we have $q_2(f_{1/48}(x)) = v_1(x)v_2(x)$, it suffices to show that $q_1(f_{1/48}^n(x))$ and $v_j(f_{1/48}^n(x))$ (for $j \in \{1, 2\}$) are irreducible for all n. This is because q_1 for $m = -2 - 2i$ is the same as q_2 for $m = 2 + 2i$ (as q_1 and q_2 only differ by a sign of the x term). By Lemma 2.0.2, it suffices to show that $q_1(f_{1/48}^n(0))$ and $v_j(f_{1/48}^n(0))$ are non-square in $\mathbb{Q}(i)$ for all n.

Note

$$\{v_1(f_{1/48}^n(0)) \bmod 10 + 3i\}_{n\geq 1} \equiv \{-1 - 5i, 1 + 5i, -3i, -1 - 4i, 2 + 3i, -5i, -3i, ...\}$$

cycles between the non-squares $-1 - 4i$, $2 + 3i$, $-5i$, and $-3i$, while the first two entries are also non-square. Similarly,

$$\{v_2(f_{1/48}^n(0)) \bmod 10 + 3i\}_{n\geq 1} \equiv \{1 - i, -5i, -2 - 5i, 4 - 2i, 1 - 2i, 1 + 5i, -2 - 5i, ...\}$$

cycles between the non-squares $-2-5i$, $4-2i$, $1-2i$, and $1+5i$, while the first two entries again are also non-squares modulo $10+3i$.

To show that $q_1(f^n_{1/48}(0))$ is non-square for all n when $m = 2+2i$, note that $q_1(f_{1/48}(0)) \equiv -2 \bmod 3+2i$ is non-square. For $n \geq 2$, $\{q_1(f^n_{1/48}(0)) \bmod 2+i\}_{n\geq 2} \equiv \{-i, -i, ...\}$, and note $-i$ is non-square modulo $2+i$, so $q_1(f^n_{1/48}(0))$ is non-square for all n.

When $c = -m^2(m^2-2i)$ and $m \neq \pm(2+2i)$, we wish to show that $q_j(f^n_r(x))$ is irreducible for all n. We thus prove the Gaussian integer analogue of Proposition 2.16 of [1]:

Proposition 3.2.2. *Let $r = 1/c$ and $c = -m^2(m^2-2i) \notin \{0, 48\}$, and let q_j be as in (3.8). Suppose that $N(c) \leq 10^9$. Then for all $n \geq 1$ we have $q_1(f^n_r(x))$ and $q_2(f^n_r(x))$ irreducible. Hence $f^n_r(x)$ is a product of two irreducible factors for all $n \geq 2$.*

Proof. Observe that $N(c) = |-m^2(m^2-2i)|^2 \leq 10^9$ implies $|m| < 14$. By Lemma 2.0.2 we show that $\{q_j(f^n_r(0))\}_{n\geq 1}$ contains no squares in $\mathbb{Q}(i)$. For $q_j(f^n_r(0))$, we find that there exists a prime with $|p| \leq 52$ satisfying condition $\circledast$ for all permissible m with $|m| < 14$. For each such m and p, we take the finitely many terms of the sequence $\{q_1(f^n_r(0))\}_{n\geq 2}$ (resp. $\{q_2(f^n_r(0))\}_{n\geq 2}$) that have still not been proven non-square, and reduce modulo small primes until all have been proven non-square. □

We can sum up the results of this section (3.1.3) as the proofs of items (5) and (6) of Conjecture 1 up to our bound 10^9 for $N(c)$:

Theorem 3.2.2. *Let $f_r = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0, -1\}$, $N(c) \leq 10^9$, and let k_n denote the number of irreducible factors of $f_r^n(x)$. Then,*

(5) *Suppose $c \neq 48$. Then $c = -m^2(m^2 \pm 2i)$ if and only if $k_1 = 1$ and $k_n = 2$ for all $n \geq 2$.*

(6) *We have $k_1 = 1$ and $k_3 \geq 3$ if and only if $c = 48$. In this case, $k_2 = 2$ and $k_n = 3$ for all $n \geq 3$.*

Chapter 4: The proof of Theorem 1.0.4

The Gaussian integer analogue of Lemma 3.2 of [1] is also central to our analysis, with an identical proof:

Lemma 4.0.1. *Suppose that $r = 1/c$ and $f_r^2(x)$ is irreducible. Let $a_n = a_n(c)$ and*

$$b_n^{\pm} = i(a_{n-1} \pm \sqrt{a_n}).$$

If for every $n \geq 3$, $\{b_n^+, b_n^-\}$ contains no squares in $\mathbb{Z}[i]$ (which holds if a_n is non-square in $\mathbb{Z}[i]$), then $f_r^n(x)$ is irreducible for all $n \geq 1$.

Proof. Assume inductively that $f_r^n(x)$ is irreducible for some $n \geq 2$. Let α be a root of $f_r^{n+1}(x)$, and observe that $\beta := f_r(\alpha)$ is a root of $f_r^n(x)$. By our inductive assumption, we have

$$[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)(\beta)] = 2.$$

Now $f_r^{n+1}(x)$ is irreducible if and only if $[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)] = 2^{n+1}$, which is equivalent to $[\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)(\beta)] = 2$. This holds if and only if $f_r(x) - \beta$ is irreducible over $\mathbb{Q}(i)(\beta)$, i.e. if $r - \beta$ is not a square in $\mathbb{Q}(i)(\beta)$. Now factor $f_r^n(x)$ over $K_1 := \mathbb{Q}(i)(\sqrt{r})$. We have

$$f_r^n(x) = (f_r^{n-1}(x) - i\sqrt{r})(f_r^{n-1}(x) + i\sqrt{r}),$$

and because $[\mathbb{Q}(i)(\beta) : \mathbb{Q}(i)] = 2^n$, we must have $[\mathbb{Q}(i)(\beta) : K_1] = 2^{n-1}$, which implies that the minimal polynomial of β over K_1 is one of $f_r^{n-1}(x) \pm i\sqrt{r}$. Suppose it is $f_r^{n-1}(x) + i\sqrt{r}$ without loss of generality. It follows that $N_{\mathbb{Q}(i)(\beta)/K_1}(r - \beta)$ is the product of $(r - \beta')$, where β' varies over all roots of $f_r^{n-1}(x) + i\sqrt{r}$; this product is just $f_r^{n-1}(r) + i\sqrt{r}$. To summarize, we have

$$N_{\mathbb{Q}(i)(\beta)/K_1}(r - \beta) = f_r^{n-1}(r) + i\sqrt{r} = f_r^n(0) + i\sqrt{r}$$

Suppose now that $f_r^{n+1}(x)$ is reducible, and hence $r - \beta$ is a square in $\mathbb{Q}(i)(\beta)$. Because the norm map is multiplicative, this implies $N_{\mathbb{Q}(i)(\beta)/K_1}(r - \beta)$ is a square in K_1, i.e. there exist s_1, $s_2 \in \mathbb{Q}(i)$ with

$$(s_1 + s_2\sqrt{r})^2 = s_1^2 + rs_2^2 + 2s_1s_2\sqrt{r} = f_r^n(0) + i\sqrt{r}.$$

This last equality implies $s_1^2 + rs_2^2 = f_r^n(0)$ and $s_2 = i/(2s_1)$, whence

$$s_1^2 - \frac{r}{4s_1^2} = f_r^n(0) \iff s_1^2 = \frac{f_r^n(0) \pm \sqrt{f_r^{n+1}(0)}}{2} = \frac{a_n \pm \sqrt{a_{n+1}}}{2c^{2^{n-1}}}$$

Now $n \geq 2$, so $c^{2^{n-1}}$ is a square. Thus one of $(a_n \pm \sqrt{a_{n+1}})/2$ is a square in $\mathbb{Q}(i)$. Since $2 = -i(1+i)^2$ in $\mathbb{Z}[i]$, we have that $i(a_n \pm \sqrt{a_{n+1}})$ is a square in $\mathbb{Z}[i]$. This expression is $b_{n+1}^{\pm}$, but $b_n^{\pm}$ is not a square in $\mathbb{Z}[i]$ any all $n \geq 3$ by hypothesis. This contradiction yields $f_r^{n+1}(x)$ is irreducible. □

Remark. *In this proof, we showed that if $f_{1/c}^n(x)$ is irreducible and the set $\{b_{n+1}^+(c), b_{n+1}^-(c)\}$ contains no squares in $\mathbb{Z}[i]$, then $f_{1/c}^{n+1}(x)$ is irreducible for $n \geq 2$.*

The proof of [1, Proposition 3.3] is also easily adapted to the Gaussian integer setting:

Proposition 4.0.1. *If* $c \in \mathbb{Z}[i]\backslash\{0, -1, \pm 2i, -89\}$, *then* a_3 *is non-square in* $\mathbb{Z}[i]$.

Proof. We have $a_3(c) = c^3 + c^2 + 2c + 1$, and so if $a_3(c) = y_0^2$ for $y_0 \in \mathbb{Z}[i]$, then necessarily (c, y_0) is an integer point on the elliptic curve $y^2 = x^3 + x^2 + 2x + 1$. This curve has conductor norm 2116 with label 2.0.4.1-2116.1-b2 in the LMFDB [8]. It has Mordell-Weil group generator $(-1 : i : 1)$ and torsion isomorphic to $\mathbb{Z}/3\mathbb{Z}$ with generator $(0 : -1 : 1)$. We determine all $\mathbb{Z}[i]$-integral points using MAGMA [9] with code from Thongjunthug's thesis [10], :

$$\{(x, \pm y)\} = \{(-1, i), (0, 1), (-2i, 1 + 2i), (2i, 1 - 2i), (-89, 835i)\}$$

Note $c \in \{0, -1, \pm 2i, -89\}$ is excluded by hypothesis. □

For a table of congruences for c yielding $a_n(c)$ non-square for all $n \geq 2$, we prove the following $\mathbb{Z}[i]$ analogue of [1, Proposition 3.5]:

Proposition 4.0.2. *Suppose that* $c \in \mathbb{Z}[i]\backslash\{0\}$. *If* c *satisfies any of the congruences in Table 4.1, or* $c+1 \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ *and* c *satisfies any of the congruences in Table 4.2, then* a_n *is not a square in* $\mathbb{Z}[i]$ *for all* $n \geq 2$.

Table 4.1: Congruences that ensure a_n is non-square for $n \geq 2$

$c \equiv i,\ 1 + i$	$\pmod 2$
$c \equiv -i$	$\pmod{2 + i}$
$c \equiv -1 - i$	$\pmod{3 + i}$

$c \equiv i,\ \pm 1 + i$	$(\mathrm{mod}\ 3 + 2i)$
$c \equiv 1 + 2i$	$(\mathrm{mod}\ 4)$
$c \equiv 2 - i$	$(\mathrm{mod}\ 4 + i)$
$c \equiv i,\ 2,\ \text{-}3,\ -(1 + i),\ 1 - 2i$	$(\mathrm{mod}\ 4 + 3i)$
$c \equiv 1$	$(\mathrm{mod}\ 4 + 4i)$
$c \equiv -2 + 2i,\ -1 - i,\ 1 - 2i$	$(\mathrm{mod}\ 5)$
$c \equiv -2 + i,\ \pm 1 - i,\ -i,\ 1 + 2i,\ 2 + 2i$	$(\mathrm{mod}\ 5 + i)$
$c \equiv -i,\ 2,\ 2 + i$	$(\mathrm{mod}\ 5 + 2i)$
$c \equiv -2 + 2i,\ 2 + i$	$(\mathrm{mod}\ 5 + 3i)$
$c \equiv 1 + 3i$	$(\mathrm{mod}\ 5 + 4i)$
$c \equiv -2 + 2i,\ i,\ -3i$	$(\mathrm{mod}\ 6 + i)$
$c \equiv -1 \pm 3i,\ -i,\ 2 - 3i$	$(\mathrm{mod}\ 6 + 5i)$
$c \equiv 3 \pm i$	$(\mathrm{mod}\ 7)$

Table 4.2: Congruences that ensure a_n is non-square for $n \geq 2$, provided that $c+1$ is non-square.

$c \equiv i,\ 1+i$	$(\mathrm{mod}\ 2)$
$c \equiv \pm i$	$(\mathrm{mod}\ 2+i)$
$c \equiv -1 \pm i$	$(\mathrm{mod}\ 3)$
$c \equiv \pm i,\ \pm(1+i)$	$(\mathrm{mod}\ 3+i)$
$c \equiv \pm i,\ -2,\ -2i,\ \pm 1+i$	$(\mathrm{mod}\ 3+2i)$
$c \equiv \pm 1 \pm 2i$	$(\mathrm{mod}\ 4)$
$c \equiv -2,\ 1+i,\ 1+2i,\ 2-i$	$(\mathrm{mod}\ 4+i)$
$c \equiv \pm i,\ \pm 2,\ \pm 3,\ \pm(1+i),\ \pm(1-2i),$	$(\mathrm{mod}\ 4+3i)$
$c \equiv 1,\ 3$	$(\mathrm{mod}\ 4+4i)$
$c \equiv \pm(2-2i),\ \pm(1+i),\ \pm(1-2i)$	$(\mathrm{mod}\ 5)$
$c \equiv -2, -2 \pm i, \pm 1-i, \pm i, 2i, 1 \pm 2i, \pm(2+2i)$	$(\mathrm{mod}\ 5+i)$
$c \equiv \pm i, 1-i, \pm 2, 2+i$	$(\mathrm{mod}\ 5+2i)$
$c \equiv -3, -2, 1-i, 1-2i, 2 \pm i, \pm 2+2i$	$(\mathrm{mod}\ 5+3i)$
$c \equiv \pm 2+i, -1+i, 4i, 1+2i, 1+3i, 2-2i, 3-i$	$(\mathrm{mod}\ 5+4i)$
$c \equiv -2, -2+2i, \pm i, 2i, -3i, 1+i$	$(\mathrm{mod}\ 6+i)$
$c \equiv -1 \pm 3i, \pm i, 1-2i, 1+3i, 1+4i, 2, 2+i, 2-3i, 3, 4+i$	$(\mathrm{mod}\ 6+5i)$
$c \equiv -2 \pm 3i, \pm 3i, 2 \pm 3i, 3 \pm i$	$(\mathrm{mod}\ 7)$

Proof. Let $f(x) = x^2 + 1/c$ and take z to be a fixed Gaussian integer with $z \nmid c$. Let $k := \mathbb{Z}[i]/z\mathbb{Z}[i]$, with $c_0 \in k$ satisfying $(1/c) \equiv c_0 \bmod z$ and put $\bar{f} = x^2 + c_0 \in k[x]$.

Now $a_n = c^{2^{n-1}} f^n(0)$, and it follows that if $\bar{f}^n(0)$ is not a square in k for $n \geq 2$, then a_n is not a square in $\mathbb{Z}[i]$. The sequence $(\bar{f}^n(0) \bmod z)_{n\geq 1}$ eventually lands in a repeating cycle. When this sequence is such that $\bar{f}^n(0)$ is a non-square in k for all $n \geq 2$, then a_n is a non-square in $\mathbb{Z}[i]$ for all $n > 1$. Table 4.1 consists of such pairs c, z. Since $c \in \{i, 1+i\} \bmod 2$ is in this table, for the rest of this thesis we may assume $c \in \{0, 1\} \bmod 2$.

When $c \equiv 0 \bmod 2$, and p is an integer prime, a_p has a prime divisor of odd multiplicity when it is non-square: note that $a_1(c) = 1$ and for all $n \geq 2$, $a_n = a_{n-1}^2 + c^{2^{n-1}-1} \equiv 1 + 0 \equiv 1 \bmod 2$. Thus if a_p is non-square in $\mathbb{Z}[i]$, it cannot be of the form $i\alpha^2 \in \{0, i\} \bmod 2$ since $a_p \equiv 1 \bmod 2$.

Now suppose $c \equiv 1 \bmod 2$. Then $a_2 = c + 1 \equiv 0 \bmod 2 \implies a_{2n} \equiv 0 \bmod 2$ by rigid divisibility. We show a_{2n} is non-square when a_2 is non-square: if $a_2 = c+1$ has some prime divisor π with $v_\pi(c+1) = j$ odd, rigid divisibility of $\{a_n\}$ then implies that $v_\pi(a_{2k}) = j$ as well, hence a_{2k} is non-square for all $k \geq 1$. Now suppose $c + 1 = i\alpha^2$. Since $a_{2n}(c) = (c+1)P_{2n}(c)$ over $\mathbb{Z}$, the only way $a_{2n}(c)$ is a square in $\mathbb{Z}[i]$ is if $P_{2n}(c) = i\alpha_1^2$ for some $\alpha_1 \in \mathbb{Z}[i]$. However, by rigid divisibility $v_{1+i}(a_{2n}) = v_{1+i}(c+1)$, so $1 + i \nmid P_{2n}(c)$. Since $P_{2n}(c) \in \mathbb{Z}[c]$, $1 + i \nmid P_{2n}(c)$, and $c \equiv 1 \bmod 2$, we must have $P_{2n}(c) \equiv 1 \bmod 2$. Thus $P_{2n}(c) \neq i\alpha_1^2$, so $a_{2n}(c)$ is non-square.

Also, $a_{2n+1} \equiv c^{2^{n-1}-1} + a_{2n}^2 \equiv 1 \bmod 2$, so if a_{2n+1} is non-square in $\mathbb{Z}[i]$,

$a_{2n+1} \neq i\alpha^2$. We have thus shown $a_p(c)$ non-square implies $a_{kp}(c)$ is non-square for all integer primes p when $c \in \{0, 1\} \mod 2$.

Many pairs c, z in Table 4.2 hinge only on $a_{2k+1} \iff \bar{f}^{2k+1}(0)$ being non-square mod z. For instance, when $z = 2 + i$ and $c \equiv i \mod z$, we have the sequence

$$\{a_n(c)\}_{n\geq 1} \equiv \{1, -1, i, 1, i, 1, ..., \} \mod 2 + i.$$

Since i is non-square mod $2 + i$, $\bar{f}^{2k+1}(0)$ is non-square mod $2 + i$ for all $k > 1$, and thus $f^{2k+1}(0)$ is non-square in $\mathbb{Q}(i)$. When $c + 1$ is non-square in $\mathbb{Z}[i]$, a_{2k} is non-square in $\mathbb{Z}[i]$, so $f^{2k}(0)$ is non-square in $\mathbb{Q}(i)$. Therefore $f^n(0)$ is non-square in $\mathbb{Q}(i)$ for all n.

The remaining pairs c, z in Table 4.2 satisfy the condition that both $\bar{f}^{3n+1}(0)$ and $\bar{f}^{3n+2}(0)$ are non-squares mod z for $n \geq 1$, thus a_{3n+1} and a_{3n+2} are non-squares in $\mathbb{Z}[i]$ for all $n \geq 1$. We've shown that if a_3 is non-square then it has an odd prime divisor, but by Proposition 4.0.1, a_3 is not a square when $c \in \mathbb{Z}[i]\backslash\{0, -1, \pm 2i, -89\}$. It follows from Proposition 2.1.1 that a_{3n} is a non-square for all $n \geq 1$ for such a c. An example is when $z = 7$ and $c \equiv 3i \mod z$:

$$\{\bar{f}^n(0) \mod 7\}_{n\geq 1} \equiv \{2i, 3+2i, -2, -3+2i, -2-3i, 2, -3+2i, -2-3i, 2, -3+2i, ...\}.$$

The only squares mod 7 in this sequence with $n > 1$ are $\pm 2 \equiv \bar{f}^{3n}(0) \mod 7$ with $2 \equiv 3^2 \mod 7$, but a_{3n} is known to be non-square in $\mathbb{Z}[i]$. □

The following is a $\mathbb{Z}[i]$ analogue of [1, Theorem 3.6] giving simple criteria for $b_n^{\pm}(c)$ to be non-square for all $n \geq 3$:

Theorem 4.0.1. *Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\{0\}$. Let a_n and $b_n^{\pm}$ as in eq. (1.1). Assume that c satisfies one of the following conditions:*

(1) $c, c+1 \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$, $2 \nmid c$ *and* $16 \nmid c+1$;

(2) $c \equiv i \bmod a+bi$ *with*

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 9 \bmod 16) \text{ or} \\ (i \bmod 2, 5 \bmod 8, 1 \bmod 16) \end{cases}$$

or $c \equiv -i \bmod a+bi$, with

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 1 \bmod 16) \text{ or} \\ (i \bmod 2, 5 \bmod 8, 9 \bmod 16) \end{cases}$$

(3) $c \neq -1 \pm 2i$ *and $v_\pi(c)$ is odd for all primes π dividing c.*

In item (2), a_n is non-square for $n \geq 2$, while in items (1) and (3), $\{b_n^+(c), b_n^-(c)\}$ contains no squares in $\mathbb{Z}[i]$ for all $n \geq 3$. In all cases, f_r^n is irreducible for all $n \geq 1$.

We break this theorem into three lemmas.

4.1 Case (1)

Lemma 4.1.1. *Suppose* $c, c+1 \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$. *If* $2 \nmid c$ *and* $16 \nmid c+1$, *then* f_r^n *is irreducible for all* $n \geq 1$.

Proof. Note that by Table 4.1, we may assume $c \notin \{i, 1+i\} \bmod 2$. Note also that f_r^2 is irreducible since $c+1$ is non-square in $\mathbb{Z}[i]$, but $c = -m^2(m^2 \pm 2i)$ implies $c+1 = (im \pm 1)^2$.

Since $2 \nmid c$ and $c \notin \{i, 1+i\} \bmod 2$, $c \equiv 1 \bmod 2$. By the recurrence relation $a_k = a_{k-1}^2 + c^{2^{k-1}-1}$, we must have $a_k \in \{0,1\} \bmod 2$ for all $k \geq 1$. If a_k is non-square then $b_k^{\pm}$ is as well, so suppose a_k is square. If $\sqrt{a_k} \in \{0,1\} \bmod 2$, then

$$\sqrt{a_k} \equiv a_k \equiv a_{k-1}^2 + c^{2^{k-1}-1} \equiv a_{k-1} + 1 \bmod 2.$$

Now,

$$b_k^{\pm} \equiv i(a_{k-1} \pm \sqrt{a_k}) \equiv i(a_{k-1} + (a_{k-1}+1)) \equiv i \bmod 2,$$

so $b_k^{\pm}$ is non-square modulo 2, hence is non-square in $\mathbb{Z}[i]$. We now impose restrictions on c mod 4 that imply $\sqrt{a_k} \notin \{i, 1+i\} \bmod 2$.

Note $c \equiv 1 \bmod 2$ implies $c \in \{\pm 1, \pm 1 + 2i\} \bmod 4$ and $c+1 \in \{0, 2, 2i, 2+2i\} \bmod 4$. Now,

$$\{a_k\}_{k\geq 1} \equiv \{1, c+1, c, c+1, c, ...\} \bmod 4 \tag{4.1}$$

since c has order 2 mod 4, so $a_k = c^m + a_{n-1}^2 \equiv c + a_{k-1}^2 \bmod 4$, and since $2 \mid c+1 \implies 2 \mid a_{2k} \implies 4 \mid a_{2k}^2$ by rigid divisibility of $\{a_k\}_{k\geq 1}$.

Suppose $\sqrt{a_k} \equiv i \bmod 2$. Then $a_k \equiv -1 \bmod 4$, since $\sqrt{a_k} = 2z + i \implies a_k = 4z^2 + 4iz - 1$. Since $c \equiv 1 \bmod 2$, we have $c + 1 \equiv 0 \bmod 2$, thus eq. (4.1) implies $c \equiv a_k \equiv -1 \bmod 4$.

Suppose $\sqrt{a_k} \equiv 1 + i \bmod 2$. Then $a_k \equiv 2i \bmod 4$, so since $1 + i \mid a_k$, we must have $1 + i \nmid c$ since $\gcd(c, a_k) = 1$ for all k. Since $c \equiv 1 \bmod 2$, $c + 1 \equiv a_n \equiv 2i \bmod 4$ by eq. (4.1), and $c + 1 \equiv 2i \bmod 4 \iff c \equiv -1 + 2i \bmod 4$. Since c is non-square mod 4 in this case, by eq. (4.1) we have $a_{2n+1} \equiv c \bmod 4$ non-square as well. Since $a_2 = c + 1$ is non-square by hypothesis and $c \in \{0, 1\} \bmod 2$, a_{2n} is also non-square by the proof of Proposition 4.0.2. Thus a_k is non-square for all $k \geq 2$ in this case.

Thus $c \not\equiv -1 \bmod 4$ implies $b_k^{\pm}$ is non-square in $\mathbb{Z}[i]$ for all $k \geq 3$. Now suppose $c \equiv -1 \bmod 4$. By eq. (4.1), we have $c + 1 \equiv a_{2k} \equiv 0 \bmod 4$, hence if a_{2k} is a square, then $\sqrt{a_{2k}} \equiv 0 \bmod 2 \implies b_{2k}^{\pm} \equiv i \bmod 2$ is not a square in $\mathbb{Z}[i]$. Now we must show $b_{2k+1}^{\pm}$ is non-square.

Since $c \equiv -1 \bmod 4$, $c \in \{-1, -1 + 4i, 3, 3 + 4i\} \bmod 8$, so $c + 1 \in \{0, 4i, 4, 4 + 4i\} \bmod 8$. Again

$$\{a_k\}_{k \geq 1} \equiv \{1, c + 1, c, c + 1, c, ...\} \bmod 8 \tag{4.2}$$

by the same reasoning as eq. (4.1).

If $c \in \{-1 + 4i, 3\} \bmod 8$ we're done, these are non-square and would imply

a_{2k+1} is non-square in $\mathbb{Z}[i]$ by eq. (4.2), thus $b^{\pm}_{2k+1}(c)$ is not a square in $\mathbb{Z}[i]$.

If $c \equiv 3+4i \equiv (2+i)^2 \bmod 8$, then $a_{2k+1} \equiv 3+4i \bmod 8$ by eq. (4.2) and

$$\sqrt{a_{2k+1}} \in \{-2-i, -2+3i, 2+i, 2-3i\} \bmod 8$$

when a_{2k+1} is a square in $\mathbb{Z}[i]$. Also, $c+1 \equiv a_{2k} \equiv 4+4i \bmod 8$ and thus

$$b^{\pm}_{2k+1}(c) \equiv i(4+4i \pm \sqrt{3+4i}) \in \{-3+2i, -7+2i, -5+6i, -1+6i\} \bmod 8.$$

Since this set consists of non-squares mod 8, $b^{\pm}_{2k+1}$ is not a square in $\mathbb{Z}[i]$ when $c \not\equiv -1 \bmod 8$.

If $c \equiv -1 \bmod 8$, then $c \equiv a_{2k+1} \bmod 8$ by eq. (4.2). Therefore $\sqrt{a_{2k+1}} \in \{\pm i, \pm 3i\} \bmod 8$. If $\sqrt{a_{2k+1}} \equiv \pm 3i \bmod 8$, then since $a_{2k} \equiv 0 \bmod 8$, we have

$$b^{\pm}_{2k+1}(c) \equiv i(a_{2k} \pm \sqrt{a_{2k+1}}) \equiv \pm 3 \bmod 8$$

and is thus non-square. Thus we may assume $\sqrt{a_{2k+1}} \equiv \pm i \bmod 8$, hence $\sqrt{a_{2k+1}} = 8z+i \implies a_{2k+1} = 64z^2 + 16iz - 1$, so $a_{2k+1} \equiv -1 \bmod 16$. Also,

$$\{a_k\}_{k\geq 1} \equiv \{1, c+1, c, c+1, ...\} \bmod 16$$

again by the same reasoning as eq. (4.1). Thus $c \equiv a_{2k+1} \equiv -1 \bmod 16$.

Now, when $c, c+1 \in \mathbb{Z}[i] \backslash \mathbb{Z}[i]^2$, $2 \nmid c$, and $16 \nmid c+1$, we have that $c \not\equiv -1 \bmod 16$ must land into an above case. Thus $\{b^+_n(c), b^-_n(c)\}$ contains no squares in $\mathbb{Z}[i]$ for each $n \geq 3$. Since f_r^2 is irreducible, f_r^n is irreducible for all $n \geq 1$ by Lemma 2.0.2.

□

Remark. *If* $c \equiv -1 \bmod 16$, *then* $\sqrt{a_{2k+1}} \in \pm\{i, 7i\} \bmod 16$ *with*

$$b^{+}_{2k+1}(c) \equiv i(a_{2k} + \sqrt{a_{2k+1}}) \equiv \begin{cases} i(0 \pm 7i) \equiv \pm 7 \\ \\ i(0 \pm i) \equiv \pm 1 \end{cases} \bmod 16$$

(the same is true of b^{-}_{2k+1}*) but* ± 1 *and* ± 7 *are all squares mod 16: note* $-1 = i^2$, *while* $7 \equiv (3i)^2 \bmod 16$. *Thus the method of proof of Lemma 4.1.1 cannot conclude that* $b^{\pm}_{2k+1}(c)$ *is non-square for such* c.

4.2 Case (2)

Lemma 4.2.1. *If* $c \equiv i \bmod a+bi$ *with*

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 9 \bmod 16) \text{ or} \\ \\ (i \bmod 2, 5 \bmod 8, 1 \bmod 16) \end{cases}$$

or $c \equiv -i \bmod a+bi$, *with*

$$(a+bi, a^2+b^2, (a+b)^2) \equiv \begin{cases} (1 \bmod 2, 5 \bmod 8, 1 \bmod 16) \text{ or} \\ \\ (i \bmod 2, 5 \bmod 8, 9 \bmod 16) \end{cases}$$

then $\{a_n\}_{n\geq 2}$ *contains no squares in* $\mathbb{Z}[i]$. *Thus* f_r^n *is irreducible for all* $n \geq 1$.

Proof. Let $f_r(x) = x^2 + r$ with $r = 1/c$ for $c \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$. If $c \equiv i \bmod a+bi$ then

$$\{a_n(c) \bmod a+bi\}_{n\geq 1} \equiv \{1, 1+i, i, -1-i, i, -1-i, ...\}. \tag{4.3}$$

Note that $\left[\frac{\pm i}{a+bi}\right] = (-1)^{(a^2+b^2-1)/4}$ when a is odd, b is even by [13, Theorem 17]. I claim the same is true when a and b are reversed: note that

$$\begin{aligned} i = \gamma^2 + z(a+bi) \iff -i &= \bar{\gamma}^2 + \bar{z}(a-bi) \\ &= \bar{\gamma}^2 + \bar{z}(-i \cdot i)(a-bi) \\ &= \bar{\gamma}^2 - i\bar{z}(b+ai), \end{aligned}$$

so

$$\left[\frac{\pm i}{a+bi}\right] = \left[\frac{\pm i}{b+ai}\right] = (-1)^{(a^2+b^2-1)/4} \tag{4.4}$$

when a and b have opposite parity.

First suppose

$$(a+bi, a^2+b^2, (a+b)^2) \equiv (1 \bmod 2, 5 \bmod 8, 9 \bmod 16).$$

Since $a+bi \equiv 1 \bmod 2$, a is odd and b is even, and a, b having opposite parity and $a^2+b^2 \equiv 5 \mod 8$ implies $\left[\frac{\pm i}{a+bi}\right] = -1$ by eq. (4.4). Thus $a_{3+2k} \equiv i \bmod a+bi$ is non-square for all $k \geq 1$ by eq. (4.3).

Since $(a+b)^2 \equiv 9 \bmod 16$, we have $\pm(1+i)$ is non-square mod $a+bi$ when a is odd and b is even by [13, Theorem 17]:

$$\left[\frac{1+i}{a+bi}\right] = (-1)^{\frac{(a+b)^2-1}{8}} = \begin{cases} -1 & \text{if } (a+b)^2 \equiv 9 \bmod 16 \\ 1 & \text{if } (a+b)^2 \equiv 1 \bmod 16. \end{cases}$$

Thus $\{a_n \bmod a+bi\}_{n\geq 1} \equiv \{1, 1+i, i, -1-i, i, ...\}$ is non-square for all $n \geq 2$.

Now suppose

$$(a+bi, a^2+b^2, (a+b)^2) \equiv (i \bmod 2, 5 \bmod 8, 1 \bmod 16).$$

Since $a+bi \equiv i \bmod 2$, a is even and b is odd. Now, if $(a+b)^2 \equiv 1 \bmod 16$, then $\pm(1-i)$ is a non-residue mod $b+ai$:

$$\left[\frac{1-i}{b+ai}\right] = \left[\frac{-i}{b+ai}\right]\left[\frac{1+i}{b+ai}\right]$$

$$= -\left[\frac{1+i}{b+ai}\right] = -(-1)^{\frac{(a+b)^2-1}{8}} = \begin{cases} 1 & \text{if } (a+b)^2 \equiv 9 \bmod 16 \\ -1 & \text{if } (a+b)^2 \equiv 1 \bmod 16 \end{cases}$$

again by [13, Theorem 17], and since $\left[\frac{\pm i}{a+bi}\right] = \left[\frac{\pm i}{b+ai}\right] = -1$ when $N(a+bi) \equiv 5 \bmod 8$.

Note $1-i$ is a residue mod $b+ai$ if and only if $1+i$ is a residue mod $a+bi$:

$$\begin{aligned} 1 - i = \gamma^2 + z(b+ai) \iff 1 + i &= \bar{\gamma}^2 + \bar{z}(b-ai) \\ &= \bar{\gamma}^2 + \bar{z}(-i \cdot i)(b-ai) \\ &= \bar{\gamma}^2 - i\bar{z}(a+bi). \end{aligned}$$

Then a_n is non-square for all $n \geq 2$ in either case.

In the case $c \equiv -i \bmod a+bi$ we have

$$\{a_n(c)\}_{n\geq 1} \equiv \{1, 1-i, -i, -1+i, -i, -1+i, ...\} \bmod a+bi,$$

so the claim is true with a switch of 9 mod 16 and 1 mod 16 in the congruence.

Since a and b have opposite parity and $a^2+b^2 \equiv 5 \mod 8$ in all cases, we have $\left[\frac{\pm i}{a+bi}\right] = -1$. Since, $c \equiv \pm i \bmod a+bi$ by hypothesis, c is non-square mod $a+bi$, so c is non-square in $\mathbb{Z}[i]$. Thus f_r is irreducible. Since $\{a_n\}_{n\geq 2}$ contains no squares in all cases, f_r^n is irreducible for all $n \geq 1$ by Lemma 2.0.2.

□

4.3 Case (3)

Lemma 4.3.1. *If $c \neq -1 \pm 2i$ and $v_\pi(c)$ is odd for all primes π dividing c, then f_r^n is irreducible for all $n \geq 1$.*

Proof. Note that by Table 4.1, we may assume $c \in \{0, 1\} \bmod 2$. Also, note that $c \neq -m^2(m^2 \pm 2i)$ unless m is a unit in $\mathbb{Z}[i]$ with $c = -1 \pm 2i$, contrary to our hypothesis. First we disprove some edge cases.

If $b_n^\pm = 0$, then $\sqrt{a_n} = \pm a_{n-1}$. Then $a_n = a_{n-1}^2 + c^{2^{n-1}-1} = a_{n-1}^2$, so $c^{2^{n-1}-1} = 0$, impossible. If $b_n^\pm = \pm 1$, then $a_{n-1} \pm \sqrt{a_n} = \pm i$. Then $\pm\sqrt{a_n} = \pm i - a_{n-1}$, so $a_n = -1 \mp 2ia_{n-1} + a_{n-1}^2$, so $a_{n-1}^2 + c^{2^{n-1}-1} = -1 \mp 2ia_{n-1} + a_{n-1}^2$. Then $c^{2^{n-1}-1} = -1 \pm 2ia_{n-1}(c)$. Since $a_{n-1} \equiv 1 \bmod c$, we must then have $0 \equiv -1 \pm 2i \bmod c$, so $c = \mu \cdot (-1 \pm 2i)$ for some $\mu \in \mathbb{Z}[i]^\times$ since $-1 \pm 2i$ is prime in $\mathbb{Z}[i]$. However, $c = \pm 2 + i$ and $c = 1 + 2i$ are found in Table 4.1 as pairs $(c \bmod z, z) = (i, 2)$ and $(1 + 2i, 4)$ respectively, so a_n is non-square for all $n \geq 2$ for these c. Thus $f_{1/(\pm 2+i)}$, and $f_{1/(1+2i)}$ are stable by Lemma 2.0.2. Note f_r for $c = 1-2i$ has the same behavior by Corollary 2.0.1.

We may thus assume that f^2 is irreducible. First suppose $c \equiv 1 \bmod 2$. Note that if a_n is non-square in $\mathbb{Z}[i]$ then $b_n^\pm$ is not a square in $\mathbb{Z}[i]$ and we're done, so suppose $a_n \in \mathbb{Z}[i]^2$. Then $b_n^\pm$ are $\mathbb{Z}[i]$-factors of $c^{2^{n-1}-1}$:

$$\begin{aligned} a_n - a_{n-1}^2 = c^{2^{n-1}-1} &= (\sqrt{a_n} - a_{n-1})(\sqrt{a_n} + a_{n-1}) \\ &= i(a_{n-1} - \sqrt{a_n})i(a_{n-1} + \sqrt{a_n}) = b_n^- b_n^+. \end{aligned}$$

Also, note that

$$\gcd(b_n^-, b_n^+) = \gcd(i(a_{n-1} - \sqrt{a_n}), i(a_{n-1} + \sqrt{a_n})) \mid \gcd(2ia_{n-1}, 2i\sqrt{a_n}) = 2$$

since $\gcd(a_n, a_{n-1}) = \gcd(c^m, a_{n-1}) = 1$. When $c \equiv 1 \bmod 2$, c is coprime to 2, so $\gcd(b_n^-, b_n^+) = 1$.

We've shown that we may assume $b_n^\pm \notin \{0, \pm 1\}$. If say $b_n^+ \in \{-i, i\}$, then b_n^+ is non-square in $\mathbb{Z}[i]$, with $b_n^+ \equiv b_n^- \equiv i \bmod 2$, so $b_n^\pm$ is non-square in $\mathbb{Z}[i]$.
Now suppose $|b_n^\pm| > 1$. Then $b_n^\pm$ has a prime divisor π with $\pi \nmid b_n^\mp$, since $\gcd(b_n^-, b_n^+) = 1$. This prime divisor is of odd multiplicity since $v_\pi(b_n^\pm) = v_\pi(c^m) = m \cdot v_\pi(c)$ and both m and $v_\pi(c)$ are odd by hypothesis. Thus $b_n^\pm$ is non-square.

Now suppose $c \equiv 0 \bmod 2$. By hypothesis we have $v_{1+i}(c) \geq 3$, since if $v_{1+i}(c) = 1$ then $c \equiv 1 + i \bmod 2$ from Table 4.1. Again, if $a_n \in \mathbb{Z}[i]^2$, then $b_n^\pm$ are $\mathbb{Z}[i]$-factors of $c^{2^{n-1}-1}$:

$$a_n - a_{n-1}^2 = c^{2^{n-1}-1} = b_n^- b_n^+.$$

with $\gcd(b_n^-, b_n^+) \mid 2$. Again, since $\gcd(b_n^+, b_n^-) \mid 2$ then for a prime $\pi \neq 1 + i$ we have either $\pi \mid b_n^+$ or $\pi \mid b_n^-$ but not both.

We now show $b_n^\pm(c) \neq \pm 2i$ unless $c \mid 8$ or $c \mid 2^{n-1}$.

Suppose $b_n^\pm(c) = \pm 2i$. Then $a_{n-1} \pm \sqrt{a_n} = \pm 2$, so $\pm\sqrt{a_n} = \pm 2 - a_{n-1}$, so $a_n = 4 \mp 4a_{n-1} + a_{n-1}^2$. Then $c^{2^{n-1}-1} + a_{n-1}^2 = 4(1 \pm a_{n-1}) + a_{n-1}^2$, so

$$c^{2^{n-1}-1} = 4(1 \pm a_{n-1}).$$

Note that the constant term of $\frac{a_{n-1}(c)-1}{c}$ is 2^{n-3} for $n \geq 3$ by induction: when $n = 3$, we have $\frac{a_2(c)-1}{c} = \frac{(c+1)-1}{c} = 1$. Now suppose $k \geq 3$, and $\frac{a_{k-1}(c)-1}{c}$ has a constant term of 2^{k-3} to show $\frac{a_k(c)-1}{c}$ has constant term 2^{k-2}. In particular, by the hypothesis we know

$$a_{k-1}(c) = p_{k-1}(c) + 2^{k-3}c + 1$$

for some polynomial $p_{k-1}(c)$ divisible by c^2. Then

$$\begin{aligned} a_k(c) = c^{2^{k-1}-1} + a_{k-1}^2(c) &= c^{2^{k-1}-1} + (p_{k-1}(c) + 2^{k-3}c + 1)^2 \\ &= c^{2^{k-1}-1} + p_{k-1}^2 + 2p_{k-1} \cdot 2^{k-3}c + 2p_{k-1} + 2 \cdot 2^{k-3}c + 1 \\ &= p_k(c) + 2^{k-2}c + 1 \end{aligned}$$

where p_k is a polynomial divisible by c^2 which was the claim to be shown.

Since $c^{2^{n-1}-1} = 4(1 \pm a_{n-1})$, first suppose $c^{2^{n-1}-1} = 4(a_{n-1} + 1)$. Since $a_{n-1} \equiv 1 \bmod c$, then $4(a_{n-1} + 1) \equiv 8 \equiv c^{2^{n-1}-1} \equiv 0 \bmod c$, so $c \mid 8 = i(1+i)^6$.

Otherwise, we have $c^{2^{n-1}-1} = 4(1 - a_{n-1})$. Then

$$0 \equiv c^{2^{n-1}-2} \equiv 4\frac{1 - a_{n-1}(c)}{c} \equiv 4 \cdot -2^{n-3} \equiv -2^{n-1} \bmod c$$

since the constant term of $\frac{a_{n-1}(c)-1}{c}$ is 2^{n-3}. Then we must have $c \mid 2^{n-1}$.

We now show that if $\pi \neq 1 + i$ divides c then $b_n^{\pm}(c)$ is non-square in $\mathbb{Z}[i]$.

Suppose $\pi \neq 1+i$ is prime with $\pi \mid c$. Then $c \nmid 2^{n-1}$ for any n, so $b_n^{\pm}(c) \neq \pm 2i$.

We've shown that we may assume $|b_n^{\pm}| > 1$, so there is a prime divisor of $b_n^{\pm}$, and $b_n^{\pm} \neq \pm 2i$.

Note $b_n^- b_n^+ = c^{2^{n-1}-1}$, so without loss of generality suppose $1+i \neq \pi \mid b_n^+$. Since $\gcd(b_n^+, b_n^-) \mid 2$, $\pi \nmid b_n^-$, so $v_\pi(b_n^+) = v_\pi(c^{2^{n-1}-1}) = v_\pi(c)(2^{n-1}-1)$, an odd number since by hypothesis $v_\pi(c)$ is odd. Thus b_n^+ is non-square.

To show b_n^- is non-square, suppose $v_{1+i}(b_n^-) > 2$, we show $v_{1+i}(b_n^-)$ is odd. Since $v_{1+i}(c)$ is odd by hypothesis, $v_{1+i}(c^{2^{n-1}-1})$ is odd, say M. Since $b_n^+ \equiv b_n^- \bmod 2$, we have $v_{1+i}(b_n^+) = 2$ since $b_n^{\pm} \equiv 0 \bmod 2$ and $\gcd(b_n^+, b_n^-) \mid 2$. Since $v_{1+i}(b_n^+) = 2$, $v_{1+i}(b_n^-) = M - 2$ because $b_n^+ b_n^- = c^{2^{n-1}-1}$. Since $M-2$ is also odd, b_n^- is non-square in $\mathbb{Z}[i]$. Suppose now that $v_{1+i}(b_n^-) \leq 2$.

If $v_{1+i}(b_n^-) = 0$, then since $|b_n^-| > 1$, we must have a prime divisor $\pi \neq 1+i$ of b_n^-. Since $c^m = b_n^+ b_n^-$, π is a prime divisor of c, but c is divisible by primes only to odd multiplicities by hypothesis. A prime divisor $\pi \neq 1+i$ of c divides b_n^- or b_n^+ but not both, so $v_\pi(b_n^-) = v_\pi(c^m) = m \cdot v_\pi(c)$ is odd since both $v_\pi(c)$ and $m = 2^{n-1} - 1$ are odd. Thus b_n^- is not a square in $\mathbb{Z}[i]$.

If $v_{1+i}(b_n^-) = 1$, then b_n^- is clearly non-square.

If $v_{1+i}(b_n^-) = 2$, then since $b_n^- \neq \pm 2i$, $b_n^- = \pm 2$ or has a prime divisor of odd multiplicity other than $1+i$ (since $b_n^+ b_n^- = c^{2^{n-1}-1}$), both indicating that it is non-square in $\mathbb{Z}[i]$.

Now suppose $c \mid 2^{n-1}$. Then c or $\bar{c}$ is of the form $\pm 2^k(1+i)$, both non-square so f_r is irreducible. By Corollary 2.0.1, f_r^n has the same number of factors over $\mathbb{Q}(i)$ as $f_{\bar{r}}^n$, so from now on we assume $c = \pm 2^k(1+i)$.

Note that $c+1 = \pm 2^k + 1 \pm (2^k)i$ is non-square when $c \neq -4-4i$: if

$$\pm 2^k + 1 \pm (2^k)i = (x+iy)^2 = x^2 - y^2 + 2xyi,$$

then $2xy = 2^k$, so x or y is ± 1 or else $x^2 - y^2$ is even. If $x = \pm 2^{k-1}$, $y = \pm 1$, then

$$x^2 - y^2 = 2^{2k-2} - 1 \neq \pm 2^k + 1 = \mathrm{Re}(c+1)$$

for any integer $k \geq 1$.

However, if $x = \pm 1$ and $y = \pm 2^{k-1}$, then

$$x^2 - y^2 = 1 - 2^{2k-2} \neq \pm 2^k + 1 = \mathrm{Re}(c+1)$$

unless $c = -2^k(1+i)$ and $k = 2$. Then $c = -4-4i$ where $a_2 = c+1 = -3-4i = (-1+2i)^2$ is square.

Note also that $a_n(-4-4i) \equiv -1-i \bmod 3$. If $c \equiv -1-i \bmod 3$, we obtain the list

$$\{a_n\}_{n\geq 1} \equiv \{1, -i, 1+i, 1+i, ...\} \bmod 3$$

and note that $1+i$ is non-square mod 3. Thus a_n is non-square for $n \geq 3$, so $b_n^{\pm}$ is non-square for all $n \geq 3$.

Now we may assume $a_2 = c+1$ is non-square. Note $c \equiv 0 \bmod 2$ implies we have $c+1 \equiv 1 \bmod 2$. Since a_2 is non-square, it is not of the form $i\alpha^2$ since

$i\alpha^2 \in \{0, i\} \bmod 2$, hence a_2 has a prime divisor of odd multiplicity.

Also note that $c = \pm 2^k(1+i) \equiv \pm(1+i) \bmod 3$. When $c \equiv -1 - i \bmod 3$, we've shown above that $b_n^{\pm}(c)$ is not a square in $\mathbb{Z}[i]$ for all $n \geq 3$.

From here on assume $c \equiv 1 + i \bmod 3$. We show that $b_n^{\pm} \neq \pm 2i$; it will follow that $b_n^{\pm}$ is non-square. Suppose for now that $b_n^{\pm} \neq \pm 2i$ to show this implication. Recall that $a_n = a_{n-1}^2 + c^m$ for $m = 2^{n-1} - 1$. Note $\gcd(b_n^-, b_n^+) \mid 2$ and $c^m = \pm(1+i)^{(2k+1)m} = b_n^- b_n^+$ with $b_n^{\pm} \notin \{\pm 1, \pm 2i\}$. If $v_{1+i}(b_n^{\pm}) = 2$, suppose without loss of generality that $v_{1+i}(b_n^+) = 2$. Since $b_n^+ \neq \pm 2i$, we then must have $b_n^+ = \pm 2$ and $v_{1+i}(b_n^-)$ odd (since N and $2k+1$ are odd), so both $b_n^{\pm}$ are non-square.

If $v_{1+i}(b_n^+) = 1$, then $b_n^+ \equiv b_n^- \equiv 1 + i \bmod 2$, so both $b_n^{\pm}$ are non-square.

Note that $v_{1+i}(b_n^+) = 0$ is a contradiction since $b_n^- \equiv b_n^+ \equiv 1 \bmod 1 + i$ while

$$b_n^- \cdot b_n^+ = c^m \equiv 0 \bmod 1 + i.$$

In all cases, $b_n^{\pm}$ is non-square.

Recall that if $b_n^{\pm} = \pm 2i$, we have $c^m = 4(1 \pm a_{n-1}) \implies c \mid 2^{n-1}$ or 8. We first show that the $c \mid 8$ cases pose no obstruction, obtained when $c^m = 4(1 + a_{n-1})$.

If $c = \pm 2^k(1+i)$ divides 8, then $k \in \{1, 2\}$ since by assumption $v_{1+i}(c) \geq 3$. The values of c also satisfying $c \equiv 1 + i \bmod 3$ are $c \in \{-2 - 2i, 4 + 4i\}$. When

$c = -2-2i$, we have that $c+1 = -1-2i$ is non-square in $\mathbb{Z}[i]$. We find from Table 4.2 that the modulus $5+i$ ensures a_n is non-square for $n \geq 2$. When $c = 4+4i$, we find from Table 4.1 the modulus $3+i$. Thus $b_n^{\pm}(c)$ is non-square for all non-square $c \mid 8$ and $n \geq 2$.

When $c^m = 4(1-a_{n-1})$, we obtained $c \mid 2^{n-1}$. We now show that $b_n^{\pm} = \pm 2i$ and $c \equiv 1+i \mod 3$ leads to a contradiction.

Recall $c \equiv \pm(1+i) \mod 3$ when $c \mid 2^{n-1}$ and $v_{1+i}(c)$ is odd. Now, we have

$$c^m = 4(1-a_{n-1}) \implies c^{2^{n-1}-1} = 4(1-a_{n-2}^2 - c^{2^{n-2}-1}) \tag{4.5}$$

Note we may assume $n > 4$ since $a_3(c)$ is non-square by Proposition 4.0.1 and since a_4 is non-square when a_2 is non-square, implying that $b_j^{\pm}$ is non-square in $\mathbb{Z}[i]$ for $j \in \{2,3,4\} \cup 2\mathbb{Z}^+$.

Note that

$$\{c^k \mod 3\}_{k\geq 1} \equiv \{(1+i)^k \mod 3\}_{k\geq 1} \equiv \{1+i, -i, 1-i, 2, -1-i, i, -1+i, 1, ...\}$$

so $1+i$ and thus c has multiplicative order 8 mod 3. Since $8 \mid 2^k$ when $k \geq 3$, we have

$$c^{2^{n-1}-1} \equiv c^{-1} \equiv -1+i \mod 3.$$

Since $n > 4$, we have $2^{n-1} - 1 \equiv 2^{n-2} - 1 \equiv -1 \bmod 8$ and we obtain the following from eq. (4.5):

$$-1+i \equiv 1 - a_{n-2}^2 - (-1+i) \mod 3$$

We obtain $a_{n-2}^2 \equiv -2i \bmod 3$, implying $a_{n-2} \equiv \pm(1-i) \bmod 3$. Since

$$\{a_n(c) \bmod 3\}_{n\geq 1} \equiv \{1, -1+i, 1, i, 1+i, -1, i, 1+i, -1, ...\},$$

we must have $n-2=2$ in this case, so $n=4$. Since $n>4$ by assumption, this is a contradiction.

Thus $b_n^{\pm} \neq 2i$; we've shown that this implies $b_n^{\pm}$ is non-square. Note that since c is non-square, f_r is irreducible. Since $\{b_n^+(c), b_n^-(c)\}$ contains no squares in $\mathbb{Z}[i]$ for each $n \geq 3$, it follows that $f_{1/c}^n(x)$ is irreducible for all $n \geq 1$ by Lemma 4.0.1. □

Remark. *We can now apply Theorem 4.0.1 to $c=-89$, a case with a_3 square in $\mathbb{Z}[i]$ by Proposition 4.0.1. Since $-89 \equiv 3 \bmod 4$ is a Gaussian prime, item (3) of this proposition applies (item (1) also applies since $2 \nmid c$ and $16 \nmid c+1 = -88 \notin \mathbb{Z}[i]^2$), hence we have $f_{-1/89}^n(x)$ is irreducible for all $n \geq 1$ by Lemma 4.0.1.*

Chapter 5: A useful factorization of c

We first note the following extension of [1, Lemma 4.1] to the Gaussian integers (where $N : \mathbb{C} \to \mathbb{R}$ is the field norm $N_{\mathbb{C}/\mathbb{R}}(a + ib) = a^2 + b^2$):

Lemma 5.0.1. *Let $c \in \mathbb{Z}[i]$ with $|c| > 1$, and $n \geq 2$ such that $a_n(c)$ is a square. Then we may write $c = uv$ with $\gcd(u, v) = 1$ such that*

$$dv^{2^{n-1}-1} - \frac{u^{2^{n-1}-1}}{d} = 2a_{n-1}(uv).$$

If in addition $b_n^{\pm} = i(a_{n-1} \pm \sqrt{a_n(c)})$ is a square, then $N(u)$ or $N(v)$ is a square.

Proof. This is essentially the proof of [1, Lemma 4.1] with minor modifications. Let $m = 2^{n-1} - 1$. Since $a_n(c)$ is square, there is $s \in \mathbb{Z}[i]$ such that $a_n(c) = s^2$. Since $a_n(c) = c^m + a_{n-1}(c)^2 = s^2$, we have

$$c^m = (s + a_{n-1}(c))(s - a_{n-1}(c)).$$

Set $t_+ = s + a_{n-1}(c)$ and $t_- = s - a_{n-1}(c)$, so $t_+ \cdot t_- = c^m$, and let $d = \gcd(t_+, t_-)$. Note $a_1(c) = 1$, so inductively $a_m(c) \equiv 1 \bmod c$ for all $m \geq 1$. Since $s^2 = a_n(c) \equiv 1 \bmod c$, a_{n-1} and s are relatively prime to c. Since $\gcd(a_{n-1}(c), s) \mid c^m$, we must have $\gcd(a_{n-1}(c), s) = 1$, so $a_{n-1}(c)$ and s are relatively prime.

Then we may conclude that

$$\gcd(s + a_{n-1}(c), s - a_{n-1}(c)) \mid \gcd(2s, 2a_{n-1}(c)) = 2.$$

and thus $d = \gcd(t_+, t_-) \in \{1, 1+i, 2\}$.

We have the following possibilities: $c = uv$ with $t_+ = dv^m$ and $t_- = u^m/d$, or $t_+ = u^m/d$ and $t_- = dv^m$. In the first case we have

$$t_+ - t_- = dv^m - u^m/d = 2a_{n-1}(c),$$

while in the second case we have (since m is odd)

$$d(-v)^m - \frac{(-u)^m}{d} = (-t_- + t_+) = 2a_{n-1}((-u)(-v))$$

so by switching the signs of u, v the claim is true.

If $c \in \{i, 1+i\} \bmod 2$, then a_n is non-square in $\mathbb{Z}[i]$ by Table 4.1 of Theorem 4.0.1. Thus, if $b_n^{\pm}$ is a square in $\mathbb{Z}[i]$, then $c \in \{0, 1\} \bmod 2$.

If $c \equiv 1 \bmod 2$, then $d = 1$ and $t_+ = v^m$ and $t_- = u^m$ with $b_n^+ = it_+ = iv^m$ and $b_n^- = -it_- = -iu^m$. If b_n^+ is a square in $\mathbb{Z}[i]$, then $N(b_n^+)$ is a square in $\mathbb{Z}$, while

$$N(b_n^+) = N(it_+) = N(t_+) \in \{N(v)^m, N(u)^m\},$$

so one of $\{N(u), N(v)\}$ is square in $\mathbb{Z}$ since m is odd.

When $c \equiv 0 \bmod 2$, $d \in \{1+i, 2\}$ since $1+i$ divides one of $s \pm a_{n+1}$ (because $t_+ t_- = c^m$), while $s + a_{n-1} \equiv s - a_{n-1} \bmod 2$, so both are $1+i$ or $0 \bmod 2$.

Note $b_n^+ = i(a_{n-1} + \sqrt{a_n}) = i \cdot t_+$ and $b_n^- = -i \cdot t_-$. If $d = 1+i$, then

$$s \pm a_{n-1}(c) \equiv s \mp a_{n-1}(c) \equiv 1+i \bmod 2.$$

In this case, $b_n^\pm = i(a_{n-1} \pm s) \equiv 1+i \bmod 2$ is non-square mod 2, so is non-square in $\mathbb{Z}[i]$.

Thus if $b_n^\pm$ is a square and $c \equiv 0 \bmod 2$, then $d = 2$. Then

$$u^m = \mp 2i \cdot b_n^\pm \quad \text{and} \quad v^m = \pm i \cdot b_n^\mp / 2 = \pm b_n^\mp / (1-i)^2$$

without loss of generality. Again, $N(u)^m$ or $N(v)^m$ is a square, but m is odd so either $N(u)$ or $N(v)$ is a square. □

Remark. *Note that $d = 1+i$ is impossible when $n > 2$: since*

$$s + a_{n-1}(c) \equiv s - a_{n-1}(c) \equiv 1+i \bmod 2$$

in this case, we have $v_{1+i}(s \pm a_{n-1}(c)) = 1$. However,

$$v_{1+i}(c^m) = m \cdot v_{1+i}(c) = v_{1+i}(s + a_{n-1}(c)) + v_{1+i}(s - a_{n-1}(c)) = 2,$$

so m odd implies $m = 2^{n-1} - 1 = 1$, hence $n = 2$, and $v_{1+i}(c) = 2$.

Assume $t \geq 4$ in $\mathbb{R}$, and let $F(t) = \frac{1}{2}(1 - \sqrt{1 - \frac{4}{t}}) = \frac{2}{t(1+\sqrt{1-\frac{4}{t}})}$. Note that $F(t) \leq 1/2$, and that from the first expression we see that $F(t)$ decreases

monotonically to 0. From the second expression we see that for large t, $F(t) \approx \frac{1}{t}$.

Lemma 5.0.2. *(Demark-Hindes-Jones-Misplon-Stoll-Stoneman, [1, Lemma 4.2])* *Let $t \geq 4$ in $\mathbb{R}$. Then the sequence*

$$\bar{a}_n(t) = \frac{a_n(t)}{t^{2^{n-1}-1}} \quad \text{for } n \geq 1$$

satisfies

$$1 = \bar{a}_1(t) < \bar{a}_2(t) < \ldots \quad \text{and} \quad lim_{n\to\infty}\bar{a}_n(t) = tF(t).$$

Proof. This is the proof of [1, Lemma 4.2] included here for completeness. We have that $\bar{a}_{n+1}(c) = 1 + \bar{a}_n^2(c)/c$. When $1 \leq x < cF(c)$, then $cF(c) > 1 + x^2/c > x$, so that the sequence is strictly increasing and bounded by $cF(c)$. Since $cF(c)$ is the smallest fixed point ≥ 1 of $x \to 1 + x^2/c$, it must be the limit.

□

We extend [1, Definition 4.3] over $\mathbb{Z}[i]$:

Definition 3. *Let $c \in \mathbb{Z}[i]$ with $|c| > 1$. We set*

$$Q(c) := \min\{N(v/u) : u, v \in \mathbb{Z}[i] \text{ coprime with } |v| > |u| \text{ and } c = uv\}$$

$$\tilde{Q}(c) := \min\{N(v/u) : u, v \in \mathbb{Z}[i] \text{ coprime with } |v| > |u|,\ c{=}uv,$$
$$\text{and } \{N(v),\ N(u)\} \text{ contains a square}\}$$

and

$$q(c) := \sqrt{Q(c)}, \quad \tilde{q}(c) := \sqrt{\tilde{Q}(c)}.$$

If $Q(c) = N(v/u)$, then since $N(v) > N(u)$, $N(v) \geq N(u)+1$, thus $N(v/u) \geq 1 + 1/N(u)$.

Note $N(u) < N(\sqrt{c})$, since $N(u^2) < N(u)N(v) = N(c)$, so

$$\tilde{Q}(c) \geq Q(c) = N(\frac{v}{u}) > 1 + \frac{1}{N(\sqrt{c})} = 1 + \frac{1}{|c|} \quad \text{and} \quad \tilde{q}(c) \geq q(c) > \sqrt{1 + \frac{1}{|c|}}.$$

We also make use of the following $\mathbb{Z}[i]$ extension of [1, Definition 4.4]:

Definition 4. *Let $c \in \mathbb{Z}[i]\backslash\{0,-1\}$ and $n \geq 2$. Define $\epsilon(n,c)$ so that*

$$\log \frac{\sqrt{a_n(c)} + a_{n-1}(c)}{\sqrt{a_n(c)} - a_{n-1}(c)} = \frac{\epsilon(n,c)}{\sqrt{c}}$$

Note that

$$\begin{aligned}\epsilon(n,c) &= \sqrt{c} \log \frac{(\sqrt{a_n(c)} + a_{n-1}(c))/c^{2^{n-2}-1}}{(\sqrt{a_n(c)} - a_{n-1}(c))/c^{2^{n-2}-1}} \\ &= \sqrt{c} \log \frac{\sqrt{a_n(c)/c^{2^{n-1}-2}} + a_{n-1}(c)/c^{2^{n-2}-1}}{\sqrt{a_n(c)/c^{2^{n-1}-2}} - a_{n-1}(c)/c^{2^{n-2}-1}}\end{aligned}$$

and for $|c| \geq 4$,

$$\bar{a}_n(|c|) = \frac{a_n(|c|)}{|c|^{2^{n-1}-1}} \text{ has } \lim_{n\to\infty} \bar{a}_n(|c|) = |c|F(|c|)$$

by Lemma 5.0.2. Thus, for $|c| \geq 4$ we have

$$\epsilon(|c|) := \lim_{n\to\infty} \epsilon(n,|c|) = \sqrt{|c|} \log \frac{\sqrt{|c|^2 F(|c|)} + |c|F(|c|)}{\sqrt{|c|^2 F(|c|)} - |c|F(|c|)} = \sqrt{|c|} \log \frac{1 + \sqrt{F(|c|)}}{1 - \sqrt{F(|c|)}}.$$

Since $0 \leq F(|c|) \leq 1/2$, we have $0 \leq \sqrt{F(|c|)} \leq \sqrt{2}/2$.

We now wish to show $|\epsilon(n,c)| \leq \epsilon(n,|c|)$. To this end, let $g(z) = \frac{\sqrt{a_n}}{a_{n-1}}(z)$, a meromorphic function on $\mathbb{C}$. Call $D_g \subset \mathbb{C}$ the domain of g, then note that $\mathbb{R}^+ = (0,\infty)$ is a subset of D_g and $g(t) > 1$ on $\mathbb{R}^+$ by Theorem 5.0.1:

Theorem 5.0.1. *Let $n \geq 2$. If $t \in \mathbb{R}^+$, then $g(t) = \frac{\sqrt{a_n(t)}}{a_{n-1}(t)} > 1$.*

Proof. Note $\sqrt{a_n(t)} = \sqrt{a_{n-1}^2(t) + t^{2^{n-1}-1}} > a_{n-1}(t)$ whenever $t > 0$, therefore $\frac{\sqrt{a_n(t)}}{a_{n-1}(t)} > 1$ for all $t > 0$.

□

We now prove that $|c| \geq 5$ implies $|g(c)| > 1$:

Theorem 5.0.2. *Let $n \geq 2$. If $|g(c)| = |\frac{\sqrt{a_n}}{a_{n-1}}(c)| \leq 1$, then $|c| < 5$.*

Proof. When $|a_n(c)/a_{n-1}^2(c)| \leq 1$, we have $|a_n(c)| \leq |a_{n-1}^2(c)|$. By the reverse triangle inequality and the relationship $a_n(c) = c^m + a_{n-1}^2(c)$,

$$|c|^m - |a_{n-1}^2(c)| \leq |a_{n-1}^2(c) + c^m| = |a_n(c)| \leq |a_{n-1}^2(c)|$$

implies $|c|^m \leq 2|a_{n-1}^2(c)|$. Therefore $|c|^m \leq 2a_{n-1}^2(|c|)$ since $a_{n-1}(c)$ has non-negative coefficients, so

$$\frac{|c|^m}{a_{n-1}^2(|c|)} \leq 2 \implies 1/2 \leq \frac{a_{n-1}^2(|c|)}{|c|^m}.$$

Since $a_n(|c|) = a_{n-1}^2(|c|) + |c|^m$,

$$1/2 \leq \frac{a_{n-1}^2(|c|)}{|c|^m} = \frac{a_n(|c|) - |c|^m}{|c|^m} = \frac{a_n(|c|)}{|c|^m} - 1,$$

so

$$3/2 \leq \frac{a_n(|c|)}{|c|^m} = \bar{a}_n(|c|).$$

From Lemma 5.0.2 we know that $\{\bar{a}_n(|c|)\}_{n\geq 1}$ strictly increases to $|c|F(|c|)$. Now, we show that $tF(t)$ decreases on $(4, \infty)$:

$$\frac{\mathrm{d}}{\mathrm{d}t}(tF(t)) = F(t) - t \cdot \left(\frac{1}{t^2\sqrt{1-4/t}}\right) = F(t) - \frac{1}{t\sqrt{1-4/t}}.$$

Since $F(t) = \frac{2}{t(1+\sqrt{1-\frac{4}{t}})} = \frac{2}{t+t\sqrt{1-4/t}} < \frac{2}{2t\sqrt{1-4/t}} = \frac{1}{t\sqrt{1-4/t}}$ for $t \in (4,\infty)$, we have $\frac{\mathrm{d}}{\mathrm{d}t}(tF(t)) < 0$ on $(4,\infty)$. Thus $tF(t)$ decreases to 1 on this interval.

Since $5 \cdot F(5) \approx 1.38 < 3/2$, we have that all $|c| = t \in [5,\infty)$ have $\bar{a}_n(t) \leq 3/2$. Thus all c with $|c| \geq 5$ must have $|\frac{\sqrt{a_n}}{a_{n-1}}(c)| > 1$. □

Remark. *Note that $c \in \mathbb{Z}[i]$ with $|c| < 5$ implies $|c| \leq 2\sqrt{5}$, while*

$$2\sqrt{5} \cdot F(2\sqrt{5}) \approx 1.51 > 3/2,$$

so 5 is the minimum modulus for which we can guarantee $|\frac{\sqrt{a_n}}{a_{n-1}}(c)| > 1$ with this method.

Suppose $z \in D_g$ with $|z| \geq 5$, and $g'(t) > 0$ on $\mathbb{R}^+$. As in [14], the ML inequality yields

$$\left|\log \frac{g(z)+1}{g(z)-1}\right| = \left|2\int_z^\infty \frac{g'(\gamma)d\gamma}{g(\gamma)^2-1}\right| \leq 2\int_{|z|}^\infty \frac{|g'(t)|dt}{g(t)^2-1} = \log \frac{g(|z|)+1}{g(|z|)-1} \text{ for } |g(z)| > 1. \tag{5.1}$$

Since $z \in D_g$ and $|z| \geq 5$, $|g(z)| = |\frac{\sqrt{a_n}}{a_{n-1}}(z)| > 1$ by Theorem 5.0.2, so $\left|\log \frac{g(z)+1}{g(z)-1}\right|$ is defined at z. We now show that $g'(t) > 0$ on $\mathbb{R}^+$:

$$g'(t) = \frac{d}{dt}\sqrt{1+\frac{t^m}{a_{n-1}^2(t)}} = \frac{1}{2\sqrt{1+t^m/a_{n-1}^2(t)}}\left(\frac{mt^{m-1}}{a_{n-1}^2(t)} + t^m(-2a_{n-1}^{-3}(t))(a_{n-1}'(t))\right)$$

so

$$g'(t) = \frac{t^{m-1}}{2a_{n-1}^2(t)\sqrt{a_{n-1}^2(t)+t^m}}\left(ma_{n-1}(t) - 2ta_{n-1}'(t)\right).$$

Since the first factor is clearly all positive when $t > 0$, we now show that

$$ma_{n-1}(t) - 2ta'_{n-1}(t) > 0.$$

If $a_{n-1}(t) = t^{2^{n-2}-1} + A_{2^{n-2}-2}t^{2^{n-2}-2} + ... + A_1 t + A_0$, then $A_i \geq 0$ since $a_{k-1}^2(c) + c^{2^{k-1}-1} = a_k(c)$ and

$$\begin{aligned} 2ta'_{n-1}(t) &= 2(2^{n-2}-1)t^{2^{n-2}-1} + 2(2^{n-2}-2)A_{2^{n-2}-2}t^{2^{n-2}-2} + ... + 2\cdot 2A_2t^2 + 2A_1t \\ &= \sum_{k=0}^{2^{n-2}-1} 2kA_kt^k. \end{aligned} \tag{5.2}$$

Thus

$$ma_{n-1}(t) - 2ta'_{n-1}(t) = \sum_{k=0}^{2^{n-2}-1} (m-2k)A_kt^k.$$

However, $2k < m$ for all $k \leq \deg a_{n-1} = 2^{n-2} - 1$ since

$$2k \leq 2\cdot(2^{n-2}-1) = 2^{n-1} - 2 = m - 1.$$

Thus $ma_{n-1}(t) - 2ta'_{n-1}(t) > 0$ for $t > 0$ since there exists at least one $A_k > 0$.

Since $|g(c)| = |\frac{\sqrt{a_n}}{a_{n-1}}(c)| > 1$ when $|c| \geq 5$, and $g'(|c|) > 0$, eq. (5.1) gives us

$$\begin{aligned} |\epsilon(n,c)| = \left|\sqrt{c}\log\frac{\sqrt{a_n}(c) + a_{n-1}(c)}{\sqrt{a_n}(c) - a_{n-1}(c)}\right| &= \left|\sqrt{c}\log\frac{\frac{\sqrt{a_n}}{a_{n-1}}(c)+1}{\frac{\sqrt{a_n}}{a_{n-1}}(c)-1}\right| \\ &\leq \sqrt{|c|}\log\frac{\frac{\sqrt{a_n}}{a_{n-1}}(|c|)+1}{\frac{\sqrt{a_n}}{a_{n-1}}(|c|)-1} \\ &= \sqrt{|c|}\log\frac{\sqrt{a_n}(|c|) + a_{n-1}(|c|)}{\sqrt{a_n}(|c|) - a_{n-1}(|c|)} \\ &= \epsilon(n,|c|). \end{aligned}$$

and thus $|\epsilon(n,c)| \leq \epsilon(n,|c|)$ for all $|c| \geq 5$.

From the remarks following [1, Lemma 4.2] we know $\epsilon(n,|c|) \leq \epsilon(|c|)$, so

$$|\epsilon(n,c)| \leq \epsilon(n,|c|) \leq \epsilon(|c|)$$

for all $|c| \geq 5$.

5.1 The proof of Theorem 1.0.5

We now have the tools in place to prove the $\mathbb{Z}[i]$ analogue of [1, Proposition 4.5]:

Proposition 5.1.1. *Suppose $|c| > 1$ and $n \geq 4$. If $c \in \mathbb{Z}[i]\backslash\mathbb{Z}^-$, $c \equiv 1 \bmod 2$, and*

$$n \geq 1 + \log_2\left(1 + \frac{|\epsilon(n,c)/\sqrt{c}|}{\log q(c)}\right)$$

then $a_n(c)$ is not a square.

If $c \in \mathbb{Z}[i]\backslash\mathbb{Z}^-$, $c \equiv 0 \bmod 2$, and

$$n \geq 1 + \log_2\left(1 + \frac{|\epsilon(n,c)/\sqrt{c}|}{\log q(c)} + \frac{\log 4}{\log q(c)}\right)$$

then $a_n(c)$ is not a square.

If $c \in \mathbb{Z}[i]\backslash\mathbb{Z}^-$, with $c \equiv 1 \bmod 2$ or $c \equiv 0 \bmod 2$, and the weaker condition

$$n \geq 1 + \log_2\left(1 + \frac{|\epsilon(n,c)/\sqrt{c}|}{\log \tilde{q}(c)}\right) \quad \text{or} \quad n \geq 1 + \log_2\left(1 + \frac{|\epsilon(n,c)/\sqrt{c}|}{\log \tilde{q}(c)} + \frac{\log 4}{\log \tilde{q}(c)}\right)$$

holds (respectively), then $b_n^{\pm}(c)$ is non-square.

Proof. In the following, we write a_n for $a_n(c)$ since c is fixed, and assume that a_n is a square. Let $m = 2^{n-1} - 1$. Since $n > 2$, by Lemma 5.0.1 and the following remark we may write $c = uv$ with coprime u, v such that

$$(v^m, u^m) = (\frac{1}{d}(\pm\sqrt{a_n} + a_{n-1}), d(\pm\sqrt{a_n} - a_{n-1})) \quad \text{for } d \in \{1, 2\}.$$

We first show $|u| \neq |v|$ in all cases. Note $|u| \neq |v| \iff |u^m| \neq |v^m|$.

When $d = 1$, let $\sqrt{a_n} = A + Bi$, $a_{n-1} = C + Di$, so $N(u^m) = N(v^m)$ implies $N(\pm\sqrt{a_n} - a_{n-1}) = N(\pm\sqrt{a_n} + a_{n+1})$. This is the case if and only if

$$N(A + Bi - (C + Di)) = N(A + Bi + (C + Di)).$$

Then

$$\begin{aligned}(A - C)^2 + (B - D)^2 = (A + C)^2 + (B + D)^2 &\iff -2AC - 2BD = 2AC + 2BD \\ &\iff 0 = 4(AC + BD),\end{aligned}$$

so the vectors $\overrightarrow{\sqrt{a_n}} = \begin{bmatrix} A \\ B \end{bmatrix}$ and $\vec{a}_{n-1} = \begin{bmatrix} C \\ D \end{bmatrix}$ are perpendicular.

Then, we must have $\overrightarrow{\sqrt{a_n}} = \lambda \begin{bmatrix} -D \\ C \end{bmatrix}$ for some real λ, i.e.

$$\sqrt{a_n} = \lambda(-D + iC) = \lambda i(C + Di) = \lambda i a_{n-1}.$$

Then $A = -\lambda D$, $B = \lambda C$. Since a_n is a square, $A, B \in \mathbb{Z}$, so λ is a rational number $s/t \in \mathbb{Q}$. To have $\sqrt{a_n} \in \mathbb{Z}[i]$ we must have $t \mid a_{n-1}$. Let $\beta = a_{n-1}/t \in \mathbb{Z}[i]$,

so $\beta \mid a_{n-1}$. Then

$$\sqrt{a_n} = (s/t)ia_{n-1} = si\beta.$$

However, a_n is relatively prime to a_{n-1} as shown in the proof of Lemma 5.0.1. Since $\beta \mid \gcd(\sqrt{a_n}, a_{n-1}) = 1$, we have $\beta \in \{\pm 1, \pm i\}$. Thus $\sqrt{a_n}$ is either real or pure imaginary. If $\beta = \pm 1 = a_{n-1}/t$, then $a_{n-1} \in \mathbb{Z}$, and thus $\sqrt{a_n} = \lambda i a_{n-1} \in i\mathbb{Z}$. The reverse is true for $\beta = \pm i$. In either case, $a_n \in \mathbb{Z}$.

Since $a_n = a_{n-1}^2 + c^m$ and $a_n, a_{n-1}^2 \in \mathbb{Z}$, then $c^m \in \mathbb{Z}$. Since $m = 2^{n-1} - 1$ is odd, we must have $c \in \mathbb{Z}$. This contradicts a_{n-1} being pure imaginary, since $a_k(c) = a_{k-1}^2 + c^{2^{k-1}-1}, a_1(c) = 1$, and thus $a_k \in \mathbb{Z}$ whenever $c \in \mathbb{Z}$. Thus $\sqrt{a_n}$ is pure imaginary and $c \in \mathbb{Z}$ with $\beta = \pm 1$. The only way $\sqrt{a_n}$ is pure imaginary and $c \in \mathbb{Z}$ is when $a_n(c)$ is a negative integer. Then c is a negative integer, since $a_n(c) > 0$ when $c \in \mathbb{Z}^+$. In this case $A = D = 0$, with

$$N(\sqrt{a_n} - a_{n-1}) = N(\sqrt{a_n} + a_{n-1}) \iff N(iB - C) = N(iB + C).$$

Since $c \in \mathbb{Z}[i]$ is not a negative integer by hypothesis, we must have $N(u) \neq N(v)$.

When $d = 2$, we again show $|u| \neq |v|$. If $|v|^m = |u|^m$, we then have

$$|v^m/u^m| = \left| \frac{\sqrt{a_n} \pm a_{n-1}}{d^2(\sqrt{a_n} \mp a_{n-1})} \right| = 1.$$

Without loss of generality, suppose

$$\left| \frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}} \right| = |d^2| = 4.$$

Then $N(\frac{\sqrt{a_n}+a_{n-1}}{\sqrt{a_n}-a_{n-1}}) = 16$. Then,

$$N(\sqrt{a_n} + a_{n-1}) = 16 \cdot N(\sqrt{a_n} - a_{n-1}). \tag{5.3}$$

Since $d = \gcd(\sqrt{a_n} + a_{n-1}, \sqrt{a_n} - a_{n-1}) = 2$, we must have $v_{1+i}(\sqrt{a_n} - a_{n-1}) = 2$, hence in $\mathbb{Z}$,

$$v_2(N(\sqrt{a_n} - a_{n-1})) = 2.$$

Now $v_2(N(\sqrt{a_n}+a_{n-1})) = 6$ in $\mathbb{Z}$ by eq. (5.3). Since $(\sqrt{a_n}+a_{n-1})(\sqrt{a_n}-a_{n-1}) = c^m$,

$$8 = v_2(N(\sqrt{a_n} + a_{n-1})N(\sqrt{a_n} - a_{n-1})) = v_2(N(c^m)) = m \cdot v_{1+i}(c),$$

so $m \mid 8$. However, $m = 2^{n-1} - 1$ is odd number greater than 1 since $n > 2$, a contradiction. Thus $|v| \neq |u|$ in all cases.

Now, since $|v| \neq |u|$,

$$\begin{aligned}
m \log q(c) \leq m|\log(|v/u|)| &= |\log(|(v/u)^m|)| \\
&= \left|\log |d^{\pm 2} \frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}|\right| \\
&= \left|\log |d^{\pm 2}| + \log |\frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}|\right| \\
&\leq \left|\log |d^{\pm 2}|\right| + \left|\log |\frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}|\right| \\
&\leq \log d^2 + \left|\log \frac{\sqrt{a_n} + a_{n-1}}{\sqrt{a_n} - a_{n-1}}\right| \\
&= \log d^2 + |\epsilon(n,c)/\sqrt{c}| \\
&= \begin{cases} |\epsilon(n,c)/\sqrt{c}| & \text{if } d = 1, \\ \log 4 + |\epsilon(n,c)/\sqrt{c}| & \text{if } d = 2. \end{cases}
\end{aligned}$$

This is equivalent to the inequalities shown, since $m = 2^{n-1} - 1$.

Assuming that $b_n^{\pm}(c)$ is square in $\mathbb{Z}[i]$ yields $N(u)$ or $N(v)$ is square by Lemma 5.0.1,

hence the bound is valid for $\tilde{q}(c)$ in place of $q(c)$.

□

Remark. *Note that [1, Proposition 4.5] assumed c is a non-square positive integer $c = uv$, so $u \neq \pm v$ and thus $|u| \neq |v|$ is automatic.*

We now handle the negative integer case, including the proof of [1, Proposition 3.1] as a lemma:

Lemma 5.1.1. *(Demark-Hindes-Jones-Misplon-Stoll-Stoneman, [1, Proposition 3.1]) If $c \in \mathbb{Z}^-$, then $a_n \in \mathbb{Z}^-$ for all $n \geq 2$.*

Proof. Let $r = 1/c$ and $f_r(x) = x^2 + r$, and consider the image of the interval $I = (-\sqrt{-r}, 0)$ under $f_r : \mathbb{R} \to \mathbb{R}$. We have $f_r(-\sqrt{-r}) = 0$ and $f_r(0) = r \in I$, so as f_r is a continuous function with no critical points in I, it follows that $f_r(I) \subset I$. As $f_r(0) = r \in I$, inductively, $f_r^n(0) \in I$ for all $n \geq 1$. Hence $0 > f_r^n(0) = a_n/c^{2^n}$, and hence $a_n < 0$ for $n \geq 1$. □

We are now in the position to prove that if $c \in \mathbb{Z}^-$ is non-square in $\mathbb{Z}[i]$, then $b_n^{\pm}$ is not a square in $\mathbb{Z}[i]$:

Theorem 5.1.1. *Suppose $c \in \mathbb{Z}^- \backslash \mathbb{Z}[i]^2$ is a negative integer. Then $f_r^n(x)$ is irreducible for all $n \geq 1$.*

Proof. Since c is a negative integer, $a_n(c) \in \mathbb{Z}^-$ by Lemma 5.1.1. Thus, if $a_n(c)$ is a square in $\mathbb{Z}[i]$, $\sqrt{a_n(c)} \in i\mathbb{Z}$. If $b_n^{\pm}(c)$ is a square in $\mathbb{Z}[i]$ for some $n \geq 2$, then we may write $c = uv$ with $\gcd(u, v) = 1$ such that $\{N(u), N(v)\}$ contains a square by

Lemma 5.0.1, with

$$(v^m, u^m) = (\pm\sqrt{a_n} - a_{n-1}, \pm\sqrt{a_n} + a_{n-1}) = (iB - C, iB + C) \quad \text{for } B, C \in \mathbb{Z}.$$

Note $N(iB - C) = N(u^m) = N(v^m) = N(iB + C)$ is a square in $\mathbb{Z}$ since the norm is multiplicative, thus $N(u) = N(v)$ is a square. Then $|iB - C| = |iB + C| = \sqrt{C^2 + B^2} = s$ is an integer. Since $c^m = u^m v^m$, we have $|c^m| = |c|^m = s^2$. Since m is odd, we must have $|c| = -c$ a square in $\mathbb{Z}[i]$, contrary to our hypothesis. Thus $b_n^{\pm}(c)$ is not a square in $\mathbb{Z}[i]$ for all $n \geq 2$.

We now show $f_r^2(x)$ is irreducible to apply Lemma 4.0.1, it will follow that we have f_r^n irreducible over $\mathbb{Z}[i]$ for all $n \geq 1$. If $c \neq -m^2(m^2 \pm 2i) \in \mathbb{Z}^- \backslash \mathbb{Z}[i]^2$, then f_r^2 is irreducible by Proposition 3.0.1: suppose the opposite for a contradiction.

If $c = -m^2(m^2 \pm 2i) \in \{-1 \pm 2i, 0\} \bmod 4$, we may assume $c \equiv 0 \bmod 4$ since $c \in \mathbb{Z}^-$. Then $(1 + i) \mid m$, so $c = 4\alpha^2(\alpha^2 \pm 1)$ for some $\alpha \in \mathbb{Z}[i]$. Since $c \in \mathbb{Z}$, we may assume $\alpha \in \mathbb{Z} \cup i\mathbb{Z}$: if $\alpha = A + Bi$, then

$$0 = \mathrm{Im}(c) = \mathrm{Im}(4\alpha^2(\alpha^2 \pm 1)) = 16A^3B - 16AB^3 \pm 8AB.$$

If both A, B are non-zero, then $16A^2 - 16B^2 \pm 8 = 0$, so $\pm 8 = 16(B^2 - A^2)$. This is a contradiction, so we may assume A or $B = 0$.

Thus $\alpha \in \mathbb{Z} \cup i\mathbb{Z}$. If $|\alpha| > 1$ in $\mathbb{Z}$ or $i\mathbb{Z}$ we have $4\alpha^2(\alpha^2 \pm 1) \in \mathbb{Z}^+$. If $|\alpha| = 1$, we have $c \in \{0, 8\}$. Thus $c \notin \mathbb{Z}^-$ is a contradiction, so $c \neq -m^2(m^2 \pm 2i)$. □

The lower bound on n from Proposition 5.1.1 leads to the following $\mathbb{Z}[i]$ analogue of [1, Corollary 4.6]:

Corollary 5.1.1. *Let $f(x) = x^2 + 1/c$ for $c \in \mathbb{Z}[i]\backslash\mathbb{Z}[i]^2$ with $|c| \geq 5$.*

(1) *If $c \equiv 1 \bmod 2$ and f^k is irreducible for*

$$k = 1 + \left\lfloor \log_2 \left(1 + \frac{\epsilon(|c|)/\sqrt{|c|}}{\log \sqrt{1 + 1/|c|}} \right) \right\rfloor,$$

or $c \equiv 0 \bmod 2$ and f^k is irreducible for

$$k = 1 + \left\lfloor \log_2 \left(1 + \frac{\log 4 + \epsilon(|c|)/\sqrt{|c|}}{\log \sqrt{1 + 1/|c|}} \right) \right\rfloor,$$

then all f^n are irreducible.

(2) *If $c \equiv 1 \bmod 2$ or $c \equiv 0 \bmod 2$ (respectively) and $a_2(c) = c + 1$ and $a_p(c)$ are non-square for all prime numbers p with*

$$5 \leq p \leq 1 + \left\lfloor \log_2 \left(1 + \frac{\epsilon(|c|)/\sqrt{|c|}}{\log \sqrt{1 + 1/|c|}} \right) \right\rfloor$$

or

$$5 \leq p \leq 1 + \left\lfloor \log_2 \left(1 + \frac{\log 4 + \epsilon(|c|)/\sqrt{|c|}}{\log \sqrt{1 + 1/|c|}} \right) \right\rfloor,$$

then all f^n are irreducible.

Proof. Recall that all f^n are irreducible when f^k is irreducible for some k and $a_n(c)$ or $b_n^{\pm}(c)$ are non-square for all $n > k$.

(1) If $n > k$, then

$$n \geq 1 + \log_2 \left(1 + \frac{|\epsilon(n, c)/\sqrt{c}|}{\log q(c)} \right)$$

or

$$n \geq 1 + \log_2 \left(1 + \frac{|\epsilon(n,c)/\sqrt{c}|}{\log q(c)} + \frac{\log 4}{\log q(c)} \right)$$

since $q(c) > \sqrt{1+1/|c|}$ and $|\epsilon(n,c)| \leq \epsilon(n,|c|) \leq \epsilon(|c|)$ for $|c| \geq 5$. If $c \in \mathbb{Z}^-$, apply Theorem 5.1.1 to conclude the stability of f. Otherwise, Proposition 5.1.1 applies. Thus $a_n(c)$ is non-square, and the claim follows.

(2) Now let k be as in (1). If $c \in \mathbb{Z}^-$, apply Theorem 5.1.1. Now suppose $c \notin \mathbb{Z}^-$, so $a_n(c)$ is non-square for $n > k$ by Proposition 5.1.1. If n is prime with $5 \leq n \leq k$, $a_n(c)$ is not a square by assumption. Otherwise, n is divisible by a prime $p \leq k$. By the proof of Proposition 4.0.2 we may assume $c \in \{0,1\} \bmod 2$, and thus if a_p is non-square, then a_{kp} is non-square. By assumption $a_p(c)$ is non-square, so $a_n = a_{kp}$ is non-square, and we're done.

□

The $\mathbb{Z}[i]$ analogue of [1, Proposition 5.4] is again proved with minor modifications:

Proposition 5.1.2. *Let $c \in \mathbb{Z}[i]$ and set $f(x) = x^2 + 1/c$. If $N(c) \leq 10^9$ and the second iterate f^2 is irreducible, then all iterates of f are irreducible.*

Proof. We consider the set of non-squares not of the form $-m^2(m^2 \pm 2i)$: this is a necessary and sufficient condition for f_r^2 to be irreducible by Proposition 3.0.1. When $|c| < 5$, those with $c \notin \{0,1\} \bmod 2$ or with $v_\pi(c)$ odd for all $\pi \mid c$ are handled by Theorem 4.0.1. The remaining cases with $c \in \{0,1\} \bmod 2$ are

$$c \in \pm\{2, 4i, 2+4i, 4+2i\},$$

but $c = -4i$ has the same behavior as $4i$ by Corollary 2.0.1.

Note that when $c \in \{2, 4i, \pm(4+2i), -2-4i\}$ we have that $c+1$ is prime in $\mathbb{Z}[i]$. Hence Table 4.2 applies to these c with the following congruence pairs (c, z): $(2, 4+3i)$ for $c = 2$, $(-i, 2+i)$ for $c = 4i \equiv -i \bmod 2+i$, $(\pm(1+i), 3+i)$ for $c = \pm(4+2i) \equiv \pm(1+i) \bmod 3+i$, and $(-1+i, 3+2i)$ for $c = -2-4i \equiv -1+i \bmod 3+2i$. Thus $a_n(c)$ is non-square in $\mathbb{Z}[i]$ for all $n \geq 2$ for these c.

This leaves $c \in \{-2, 2+4i\}$, values with $c+1$ a square. However, note that $c = -2$ is handled by Theorem 5.1.1. When $c = 2+4i$, consider $\{a_n\}_{n\geq 1} = \{1, i, 1-i, 1-i, ...\} \bmod 3$. Note that $1-i$ is non-square mod 3, so a_n is non-square for all $n \geq 3$. Since f^2 is irreducible by hypothesis, f^n is irreducible for all $n \geq 1$ by Lemma 4.0.1.

We now assume $|c| \geq 5$. By Theorem 4.0.1 it suffices to consider $2 \mid c$ or $16 \mid c+1$, with $\pm c$ in the first quadrant by Corollary 2.0.1. In either case, when $a_2(c)$, $a_p(c)$ are non-square for integer primes

$$5 \leq p \leq 1 + \left\lfloor \log_2 \left(1 + \frac{\log 4 + \epsilon(10^{4.5})/\sqrt{10^{4.5}}}{\log \sqrt{1 + 1/10^{-4.5}}} \right) \right\rfloor = 17 \tag{5.4}$$

then all f^n are irreducible by Corollary 5.1.1. This is a finite computation.

□

Chapter 6: Applications to the density of primes dividing orbits

Let K be a number field with ring of integers $\mathcal{O}_K$. Let $S \subset \mathcal{O}_K$ be a set of prime ideals, $\mathfrak{p} \in S$, and denote by $N(\mathfrak{p}) = \#\{\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K\}$ the absolute norm of the ideal $\mathfrak{p}$. We denote by $D(S)$ the Dirichlet density of the set S:

$$D(S) = \lim_{s \to 1^+} \frac{\sum_{\mathfrak{p} \in S} N(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}}$$

Since K is a number field, this density can be shown to be equivalent to the the natural density of S, denoted by

$$\delta(S) = \lim_{B \to \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq B\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) \leq B\}}.$$

The following is an extension to $\mathbb{Z}[i]$ of [1, Proposition 6.1], requiring minor modifications:

Theorem 6.0.1. *Let $c, c+1 \in \mathbb{Z}[i] \backslash \mathbb{Z}[i]^2$, $r = 1/c$, and assume that $b_n^{\pm}(c) = i(a_{n-1}(c) \pm \sqrt{a_n(c)})$ is non-square in $\mathbb{Z}[i]$ for all $n \geq 3$. Then for any $t \in \mathbb{Q}(i)$, we have*

$$D(\{\pi \text{ prime in } \mathbb{Z}[i] : \pi \text{ divides } O_{f_r}(t)\}) = 0.$$

Proof. Let $K := \mathbb{Q}(i)(\sqrt{r}, \sqrt{\bar{r}})$, and note $K_1 := \mathbb{Q}(i)(\sqrt{r})$ (from the proof of Lemma 4.0.1) is a subfield. Now $f_r = (x + i\sqrt{r})(x - i\sqrt{r})$ over K or K_1. Let

$g_1 = (x + i\sqrt{r})$, $g_2 = (x - i\sqrt{r})$. We'll show $g_i(f^{n-1}(0))$ is non-square in K for all $n \geq 2$. Note $g_i(f_r^{n-1}(0)) = f_r^{n-1}(0) \pm i\sqrt{r} \in K_1$, and that following the proof of Lemma 4.0.1, $f_r^{n-1}(0) \pm i\sqrt{r}$ is a square in K_1 if and only if $i(f_r^{n-1}(0) \pm \sqrt{f_r^n(0)})$ is a square in $\mathbb{Q}(i)$, which is equivalent to $b_n^{\pm} = i(a_{n-1} \pm \sqrt{a_n})$ being a square in $\mathbb{Z}[i]$. By assumption, $b_n^{\pm}$ is non-square in $\mathbb{Z}[i]$ for any $n \geq 3$, so $g_i(f_r^{n-1}(0))$ is not a square in K_1. If it were square in K, then there exist $a, b \in K_1$ such that $g_i(f_r^{n-1}(0)) = (a + b\sqrt{\bar{r}})^2$ with $b \neq 0$. Then $g_i(f_r^{n-1}(0)) = f_r^{n-1}(0) \pm i\sqrt{r}$ can be written as

$$a^2 + \bar{r}b^2 + 2ab\sqrt{\bar{r}} = f_r^{n-1}(0) \pm i\sqrt{r}.$$

In particular, $2ab = 0$ otherwise $2ab\sqrt{\bar{r}} \notin K_1$ can be written as $f_r^{n-1}(0) \pm i\sqrt{r} - (a^2 + \bar{r}b^2) \in K_1$, so $a = 0$ since $b \neq 0$ by assumption. Thus

$$f_r^{n-1}(0) \pm i\sqrt{r} = \bar{r} \cdot b^2 \in \mathbb{Q}(i)$$

is a contradiction since $f_r^{n-1}(0) \pm i\sqrt{r} \in K_1 \backslash \mathbb{Q}(i)$. Thus $f_r^{n-1}(0) \pm i\sqrt{r}$ is not a square in K.

Thus we may apply part (2) of [6, Theorem 1.1] twice to show

$$0 = \lim_{B \to \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) \leq B\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) \leq B\}} \tag{6.1}$$

where $N(\mathfrak{p}) = \#(\mathcal{O}_K/\mathfrak{p}\mathcal{O}_K)$ is the absolute norm of the ideal $\mathfrak{p}$ and S is the set of primes $\mathfrak{p}$ in the ring of integers $\mathcal{O}_K$ of K that divide $g_i(f_r^{n-1}(t))$ for at least one $i \in \{1, 2\}$ and at least one $n \geq 2$.

Note $K = \mathbb{Q}(i)(\sqrt{r}, \sqrt{\overline{r}})$ is a Galois extension of $\mathbb{Q}$ of degree 8. Excluding ramified primes $\mathfrak{p} \in \mathcal{O}_K$ (this is a finite set of primes), $\mathfrak{p} \in \mathcal{O}_K$ either has absolute norm $p \in \mathbb{Z}$ (when p splits in $\mathcal{O}_K$), or absolute norm p^k for $2 \leq k \leq 8$ otherwise. We may thus assume that $N(\mathfrak{p}) = p^k$ for some $1 \leq k \leq 8$.

Note that for $k \geq 2$, $\#\{n \leq B : n = p^k \text{ for some prime } p\}$ has asymptotic density zero relative to $\#\{n \leq B : n = p \text{ for some prime } p\}$ and so eq. (6.1) is equivalent to

$$0 = \lim_{B \to \infty} \frac{\#\{\mathfrak{p} \in S : N(\mathfrak{p}) = p \leq B\}}{\#\{\mathfrak{p} : N(\mathfrak{p}) = p \leq B\}} \tag{6.2}$$

Suppose $\mathfrak{p} \in S$, and say $\mathfrak{p} \mid g_i(f_r^{n-1}(t))$ for some $n \geq 2$. Then

$$N_{K/\mathbb{Q}(i)}(\mathfrak{p}) \mid N_{K/\mathbb{Q}(i)}(g_i(f_r^{n-1}(t))) = \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q}(i))} \sigma(g_i(f_r^{n-1}(t))) = (f_r^n(t))^2.$$

Let $(p) = \mathbb{Z} \cap \mathfrak{p}\mathcal{O}_K$, $(\pi) = \mathbb{Z}[i] \cap \mathfrak{p}\mathcal{O}_K$ be the primes lying below $\mathfrak{p}$, and note $\pi \mid N_{K/\mathbb{Q}(i)}(\mathfrak{p})$. Note that $N(\mathfrak{p}) = p$ if and only if p splits in $\mathcal{O}_K$. This is true if and only if π splits in $\mathcal{O}_K$, i.e. $N(\pi) = p$ and r is a quadratic residue mod π and $\overline{\pi}$. Otherwise, $N(\mathfrak{p}) = p^k$ for some $2 \leq k \leq 8$. But $\pi \mid (f_r^n(t))^2$, so $\pi \mid f_r^n(t)$ and thus $\overline{\pi} \mid \overline{f_r^n(t)} = f_{\overline{r}}^n(t)$ with

$$0 \equiv f_r(f_r^{n-1}(t)) \equiv (f_r^{n-1}(t))^2 + r \bmod \pi$$

and

$$0 \equiv f_{\overline{r}}(f_{\overline{r}}^{n-1}(t)) \equiv (f_{\overline{r}}^{n-1}(t))^2 + \overline{r} \bmod \overline{\pi}.$$

Thus r must be a quadratic residue mod π, and $\overline{r}$ is a quadratic residue mod $\overline{\pi}$

implies r is one as well. It follows that the numerator of eq. (6.2) is

$$4\#\{\pi \in \mathbb{Z}[i] : N(\pi) = p \leq B \text{ and } \pi \text{ divides } O_f(t)\}.$$

The denominator is

$$4\#\{\pi \in \mathbb{Z}[i] : N(\pi) = p \leq B \text{ and } r \text{ is a quadratic residue mod } \pi \text{ and } \overline{\pi}\}.$$

By Chebotarev's density theorem, the proportion of integer primes that split completely in a Galois extension of degree n is $1/n$, thus the latter is asymptotic to $C \cdot \#\{\pi \in \mathbb{Z}[i] : N(\pi) = p \leq B\}$ for some constant C. It follows that

$$D(\{\pi \text{ prime in } \mathbb{Z}[i] : \pi \text{ divides } O_f(t)\}) = 0$$

as desired. □

Remark. *The hypothesis that* $b_n^{\pm}(c) = i(a_{n-1}(c) \pm \sqrt{a_n(c)}$ *is non-square is strictly weaker than* $a_n(c)$ *being non-square for* $n \geq 2$*. When* $a_n(c)$ *is non-square for all* $n \geq 2$*, the conclusion follows by (2) of [6, Theorem 1.1].*

Appendix A: Tables

Table A.1: Congruences that ensure w_n is non-square for $n \geq 2$, provided that $m \notin S'$

$m \equiv 1,\ 1+i$	$(\mathrm{mod}\ 2)$	$m \equiv -1$	$(\mathrm{mod}\ 2+i)$
$m \equiv \pm 1$	$(\mathrm{mod}\ 2+2i)$	$m \equiv \pm 1$	$(\mathrm{mod}\ 3)$
$m \equiv -1+i,\ 1$	$(\mathrm{mod}\ 3+i)$	$m \equiv -2$	$(\mathrm{mod}\ 3+2i)$
$m \equiv \pm 2-i$	$(\mathrm{mod}\ 4)$	$m \equiv -2,\ 2i,\ 2-i$	$(\mathrm{mod}\ 4+i)$
$m \equiv 1,\ -2-i,\ -1+i,\ -2i,\ 3i$	$(\mathrm{mod}\ 4+3i)$	$m \equiv 3i$	$(\mathrm{mod}\ 4+4i)$
$m \equiv -2,\ -1+i,\ 1,\ 2+2i$	$(\mathrm{mod}\ 5)$	$m \equiv -1+2i,\ 2$	$(\mathrm{mod}\ 5+i)$
$m \equiv \pm(2-2i),\ 1+2i$	$(\mathrm{mod}\ 5+2i)$	$m \equiv -2 \pm i,\ -1-2i,\ 2i,\ 2,\ 2-2i$	$(\mathrm{mod}\ 5+3i)$
$m \equiv \pm 3,\ \pm(1-3i)$	$(\mathrm{mod}\ 5+4i)$	$m \equiv -3+i$	$(\mathrm{mod}\ 6+i)$
$m \equiv -2-3i$	$(\mathrm{mod}\ 6+5i)$	$m \equiv \pm 3-2i,\ \pm 1,\ \pm 1-2i$	$(\mathrm{mod}\ 7)$

$m \equiv -3-i,\ 2,\ 3-2i \pmod{7+2i}$

$m \equiv -2-2i,\ -1+2i,\ \pm 3i,\ 2+2i,\ 4 \pmod{7+3i}$

$m \equiv -4,\ \pm 3-i,\ -3+2i,\ -2-i,\ -1+i,\ -1+2i,\ -2i,\ \pm 3i,\ 1,\ \pm(1+4i),\ 1+5i,\ 2,\ 2\pm 2i,\ 2-3i,\ 4+i \pmod{7+4i}$

$m \equiv -3+2i,\ 3+i \pmod{7+5i}$

$m \equiv 4i,\ -6i,\ 1,\ 2,\ 2+3i,\ 3+3i \pmod{7+6i}$

$m \equiv \pm 4+i,\ \pm 2-3i \pmod{8}$

$m \equiv -4,\ -4+i,\ -3-3i,\ -2-i,\ -1+i,\ -1-4i,\ -2i,\ 3i,\ 1{,}2+2i,\ 2-3i,\ \pm(3-2i),\ 3+4i \pmod{8+i}$

$m \equiv -4+2i,\ 4i,\ \pm(2+3i),\ 5-2i \pmod{8+3i}$

$m \equiv 2+5i \pmod{8+4i}$

$m \equiv -5,\ \pm(1+2i) \pmod{8+5i}$

$m \equiv -6,\ -2-3i,\ 1-6i,\ \pm(2-2i),\ 3 \pmod{8+7i}$

$m \equiv \pm 6+i \pmod{8+8i}$

$m \equiv \pm 3,\ \pm(1+3i),\ \pm(2-4i),\ \pm(3+2i) \pmod{9+i}$

$m \equiv -4+3i,\ -3-5i,\ -2,\ -2+3i,\ -2-4i,\ -1+3i,\ 2i,\ 4i,\ \pm(1+2i),\ 2,\ 2-2i,\ \pm(3+3i),\ 3+4i,\ 4+i,\ 5-3i \pmod{9+2i}$

$m \equiv -5+3i,\ -2-2i,$	$(\mathrm{mod}\ 9+4i)$	$m \equiv -4+i,\ -3-2i,$	$(\mathrm{mod}\ 9+5i)$
$1-2i,\ 1+3i,\ 2-3i,$		$-2, -1+5i, 3-i, 5-2i$	
$3+2i$			
$m \equiv -4+i, -2-2i$	$(\mathrm{mod}\ 9+6i)$	$m \equiv -4+2i,\ -3-2i,$	$(\mathrm{mod}\ 9+7i)$
		$4+i,\ 5-3i$	
$m \equiv \pm 7, -7-i, -6+i,$	$(\mathrm{mod}\ 9+8i)$	$m \equiv \pm 4+2i,\ 3i$	$(\mathrm{mod}\ 10+i)$
$\pm 5+3i,\ \pm 4,\ -3+2i,$			
$-3-3i, -3+4i, -2+$			
$4i,\ -2-6i,\ -1+i,$			
$-1+2i, -1-3i, \pm 1-$			
$4i,\ -1+6i,\ -2i,\ \pm 3i,$			
$-7i,\ 8i,\ 1,\ 1 \pm 5i,\ 1+$			
$7i, \pm(2+i), \pm(2+2i),$			
$2-3i, \pm(2-5i), 3-i,$			
$3 \pm 4i,\ 4+i,\ 4-4i,$			
$\pm(5+i), \pm 5-2i, 6$			
$m \equiv -6,\ \pm(2-2i),$	$(\mathrm{mod}\ 8+7i)$	$m \equiv -3, -1-i, \pm(1-$	$(\mathrm{mod}\ 10+7i)$
$-2-3i, 1-6i, 3$		$4i)$	
$m \equiv -6i$	$(\mathrm{mod}\ 10+9i)$		

Table A.2: Congruences that ensure w_n is non-square for $n \geq 2$, provided that $m \notin S'$ and $1 + im$ and $m - i$ are non-square in $\mathbb{Z}[i]$

$m \equiv 1$	$(\text{mod } 3+2i)$	$m \equiv \pm 2 + i$	$(\text{mod } 4)$
$m \equiv -1-2i,\ -2i,\ 1,\ 2$	$(\text{mod } 4+i)$	$m \equiv -3i$	$(\text{mod } 4+4i)$
$m \equiv -1,\ 2-2i$	$(\text{mod } 5+i)$	$m \equiv -3+i,\ -1 \pm 2i$	$(\text{mod } 5+2i)$
$m \equiv -2,\ -1,\ -2i,\ 1 \pm 2i,\ 2-i,\ 2+2i,\ 3-i$	$(\text{mod } 5+3i)$	$m \equiv -2+i,\ -1+2i,\ \pm 3i,\ -4i$	$(\text{mod } 5+4i)$
$m \equiv \pm 1,\ 2+i$	$(\text{mod } 6+i)$	$m \equiv -1+i,\ -2i,\ -3i,\ 2+2i,\ \pm(2-3i),\ 3$	$(\text{mod } 6+5i)$
$m \equiv \pm 3, \pm 3 \pm i, \pm 3 - 3i$	$(\text{mod } 7)$	$m \equiv -2,\ 2-2i,\ 2-3i,\ 3+2i$	$(\text{mod } 7+2i)$
$m \equiv -4,\ -2+3i,\ -1-3i,\ 1 \pm 2i,\ 3+i$	$(\text{mod } 7+3i)$	$m \equiv -4+2i,\ -1,\ 1-i,\ 1+3i$	$(\text{mod } 7+4i)$
$m \equiv -2+i,\ \pm 1,\ 4,\ \pm(5-i)$	$(\text{mod } 7+5i)$	$m \equiv 2+i$	$(\text{mod } 8+i)$
$m \equiv -3-i,\ -2,\ -1,\ 2+2i,\ 2+4i,\ 3+3i$	$(\text{mod } 8+3i)$	$m \equiv -5+2i,\ -2-4i,\ 4-i$	$(\text{mod } 8+5i)$

$m \equiv -5-2i,\ -3+4i,$	$(\mathrm{mod}\ 8+7i)$	$m \equiv -3-3i,\ -2-4i,$	$(\mathrm{mod}\ 9+i)$
$-2,\ 2+2i,\ 3+3i$		$-1,\ \pm 3i,\ -4i,\ 1+2i,$	
		$2+i,\ 4+i,\ \pm(4+2i),$	
		$4-4i$	
$m \equiv -4-i,\ -3+3i,$	$(\mathrm{mod}\ 9+2i)$	$m \equiv -4, -4-3i, -3-$	$(\mathrm{mod}\ 9+4i)$
$-3-4i,\ -2,\ -1+4i,$		$2i, -2+3i, -1+2i, 5-i$	
$1-2i, 2+2i, 3-i, 4\pm 3i$			
$m \equiv -5+2i, -3+$	$(\mathrm{mod}\ 9+5i)$	$m \equiv -2+i, 6$	$(\mathrm{mod}\ 9+7i)$
$2i, -2-2i, -2-$			
$3i, 4i, 5i, 2, 4$			
$m \equiv -6-i, -4-$	$(\mathrm{mod}\ 9+8i)$	$m \equiv \pm(5-3i), -3-4i,$	$(\mathrm{mod}\ 10+i)$
$2i, -4+4i, -2+$		$1-3i,\ 2+i$	
$3i, -1-7i, 1-2i, 1+$			
$2i, 3+i, 3+3i$			
$m \equiv -4+i,\ -4+3i,$	$(\mathrm{mod}\ 10+3i)$	$m \equiv -8+i, \pm(4-3i),$	$(\mathrm{mod}\ 10+7i)$
$\pm(2-4i), -1-3i, 6-2i$		$\pm 1+i,\ -1-4i,\ 3+6i$	
$m \equiv -6+3i$, -5, $\pm(2+$	$(\mathrm{mod}\ 10+9i)$		
$2i), -2-5i,\ -1,\ 1+2i,$			
$2+i,\ 3+6i,\ 4-2i$			

Bibliography

[1] David DeMark, Wade Hindes, Rafe Jones, Moses Misplon, Michael Stoll, and Michael Stoneman. Eventually stable quadratic polynomials over $\mathbb{Q}$. *New York J. Math*, 26:526–561, 2020.

[2] Robert Benedetto, Laura DeMarco, Patrick Ingram, Rafe Jones, Michelle Manes, Joseph H. Silverman, and Thomas J. Tucker. Current trends and open problems in arithmetic dynamics. *Bull. Amer. Math. Soc.*, 56(4):611–685, October 2019.

[3] Andrew Bridy, John R. Doyle, Dragos Ghioca, Liang-Chung Hsia, and Thomas J. Tucker. Finite index theorems for iterated galois groups of unicritical polynomials, 2018.

[4] Andrew Bridy and Thomas J. Tucker. Finite index theorems for iterated galois groups of cubic polynomials, 2017.

[5] Rafe Jones and Alon Levy. Eventually stable rational functions. *Int. J. Number Theory*, 13(09):2299–2318, October 2017.

[6] Spencer Hamblen, Rafe Jones, and Kalyani Madhu. The density of primes in orbits of $z^d + c$. *International Mathematics Research Notices*, 2015(7):1924–1958, 2015.

[7] Rafe Jones. The density of prime divisors in the arithmetic dynamics of quadratic polynomials. *Journal of the London Mathematical Society*, 78(2):523–544, 2008.

[8] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2024. [Online; accessed 9 March 2024].

[9] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[10] Thotsaphon Thongjunthug. *Heights on elliptic curves over number fields, period lattices, and complex elliptic logarithms*. PhD thesis, University of Warwick, 2011. https://api.semanticscholar.org/CorpusID:118795819.

[11] Wolfram Research, Inc. Mathematica, Version 14.0. Champaign, IL, 2024.

[12] W. A. Stein et al. *Sage Mathematics Software (Version 10.2)*. The Sage Development Team, 2024. http://www.sagemath.org.

[13] Nancy Buck. Quadratic reciprocity for the rational integers and the gaussian integers. Master's thesis, The University of North Carolina at Greensboro, 2010. https://libres.uncg.edu/ir/uncg/f/Buck_uncg_0154M_10433.pdf.

[14] user53153. Maximize absolute value of complex logarithm. Mathematics Stack Exchange. URL:https://math.stackexchange.com/q/320169 (version: 2013-03-04).