WALKING TO INFINITY ALONG GAUSSIAN LINES

Elsa Magness
Department of Mathematics, Seattle University, Seattle, WA 98122, USA
emagness@brynmawr.edu

Brian Nugent [1]
Department of Mathematics, Seattle University, Seattle, Washington
bnugent@uw.edu

Leanne Robertson
Department of Mathematics, Seattle University, Seattle, Washington
robertle@seattleu.edu

Received: 1/6/20, Accepted: 1/27/21, Published: 2/1/21

Abstract

We study analogies between the rational integers on the real line and the Gaussian integers on other lines in the complex plane. This includes a Gaussian analog of Bertrand's Postulate, the Chinese Remainder Theorem, and the periodicity of divisibility. We also computationally investigate the distribution of Gaussian primes along these lines and leave the reader with several open problems.

1. Introduction

Is it possible to walk from the origin in the complex plane to infinity using steps of bounded length and stepping only on Gaussian primes? Several authors have worked on this intriguing question since it was first posed by Basil Gordon in 1962. Erdös conjectured that such a walk to infinity is impossible, but the problem remains unsolved today (see [1] for a discussion of the contradictory references to Erdös' role in this problem). In 1970, Jordan and Rabung [3] showed that steps of length at least 4 would be required, and in 1998, Gethner, Wagon, and Wick [1] showed that steps of length $\sqrt{26}$ or less are insufficient to reach infinity. In the same paper they showed that it is impossible to walk to infinity along any line in the complex plane by stepping only on Gaussian primes and taking steps of bounded length, and thus established the Gaussian analog of the classical result that there are arbitrarily long sequences of composites on the real line. In 2017, West and Sittinger [7] generalized

[1]Brian Nugent's research was partially supported by NSF grant DMS-16000048.

this result and showed that in any imaginary quadratic field (with class number 1) it is similarly impossible to walk to infinity along any line using steps of bounded length and stepping only on primes in the ring of integers of the field. Motivated by these results, we further investigate the idea of walking to infinity along lines in the complex plane stepping only on Gaussian integers, and analogies to walking to infinity along the real line.

Recall that the ring $\mathbb{Z}[i]$ of *Gaussian integers* consists of all complex numbers of the form $\alpha = a + bi$, where a and b are rational integers. Following Gethner et al., we call a line in the complex plane a *Gaussian line* if it contains two, and hence infinitely many, Gaussian integers. We call a Gaussian line *primitive* if the Gaussian integers on the line do not all share a common divisor. With these definitions, we ask what we might discover if instead of wandering freely on Gaussian integers in the complex plane, we walked along a primitive Gaussian line stepping only on Gaussian integers? How different or similar would this stroll to infinity be to that of walking to infinity along the real line stepping only on rational integers? Would we stroll on infinitely many Gaussian primes, or perhaps none at all? Could we observe an analog of Bertrand's postulate on our walk? Would we see a periodicity of divisibility similar to that on the real line? What other properties of the Gaussian integers might we discover?

An overview of the paper and our results is as follows. In Section 2, we establish the background and notation used throughout. In Section 3, we investigate the distribution of Gaussian primes on Gaussian lines. We discuss what a theorem of Tao says about primes on Gaussian lines and formulate and computationally support an extension of Bertrand's Postulate to these lines. The main questions posed in this section are equivalent to famous open problems about quadratic polynomials representing prime numbers, so we turn to more tractable problems in subsequent sections. In Section 4, we prove key divisibility properties of Gaussian integers on Gaussian lines that are important for the rest of the paper. This includes an analogy of the periodicity of divisibility of rational integers on the real line and a characterization of the rational integers and Gaussian primes that divide some Gaussian integer on a given Gaussian line. In Section 5, we extend the Chinese Remainder Theorem to Gaussian lines and prove a theorem that shows there are always infinitely many Gaussian lines that satisfy any given CRT-type divisibility properties. Finally, in Section 6, we return to questions raised in Section 4 and completely characterize the set of Gaussian integers that divide some Gaussian integer on a given Gaussian line.

2. Background and Notation

We begin with some background on Gaussian integers and by establishing the notation concerning Gaussian lines that is used throughout the paper.

Since the unit group of the Gaussian integers $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$, two Gaussian integers, α and β, are *associates* if and only if $\alpha = \pm\beta$ or $\alpha = \pm i\beta$. The *norm* of the Gaussian integer $\alpha = a + bi$ is defined by $N(a+bi) = \alpha \cdot \overline{\alpha} = a^2 + b^2 \in \mathbb{Z}$, where the "bar" denotes complex conjugation, and its *trace* is defined by $Tr(a + bi) = \alpha + \overline{\alpha} = 2a \in \mathbb{Z}$. Unique factorization into Gaussian primes holds in $\mathbb{Z}[i]$, and this gives the Gaussian integers a well-defined notion of primality. To avoid confusion, we use the terminology *rational prime* for a prime in the rational integers $\mathbb{Z}$, and *Gaussian prime* for a prime in $\mathbb{Z}[i]$.

The Gaussian primes can be classified in terms of the factorization of the rational primes $p \in \mathbb{N}$ into Gaussian primes as follows:

1. If $p = 2$, then p ramifies in $\mathbb{Z}[i]$. Specifically, $2 = -i(1 + i)^2$, so $1 + i$ is a Gaussian prime of norm 2.

2. If $p \equiv 1 \pmod 4$, then $p = \pi \cdot \overline{\pi}$ splits as a product of two conjugate Gaussian primes of norm p that are not associates in $\mathbb{Z}[i]$.

3. If $p \equiv 3 \pmod 4$, then p remains prime in $\mathbb{Z}[i]$ and has norm p^2.

Every Gaussian prime is an associate of one of the Gaussian primes described above. If π is a Gaussian prime then we say π *lies over* p if π divides the rational prime p.

For every Gaussian line L, we distinguish two Gaussian integers, $\alpha_0 = a + bi$ and $\delta = c + di$, that define L as follows. Let α_0 be the Gaussian integer on L of minimum norm, and if there are two such integers, let α_0 be the one with the larger real part. If L is vertical, then take $\delta = i$. Otherwise, let α_1 be the Gaussian integer on L closest to α_0 (so $N(\alpha_1 - \alpha_0)$ is minimal) and with $\mathrm{Re}(\alpha_1) > \mathrm{Re}(\alpha_0)$. Then take $\delta = \alpha_1 - \alpha_0$. Thus α_0 is on the line L, but δ is not, provided $\alpha_0 \neq 0$. Note that there are only two primitive Gaussian lines with $\alpha_0 = 0$, namely the real line $\mathrm{Im}(z) = 0$ and the imaginary line $\mathrm{Re}(z) = 0$.

With α_0 and δ defined in this way, the lemma below describes all Gaussian integers on L. This lemma is essentially Lemma 4.2 in [1], except that we describe the primitive case and specify α_0 and δ, since this is convenient for our work.

Lemma 1. *Let L be a Gaussian line, and let $\alpha_0 = a + bi$ and $\delta = c + di$ be as defined above. Then c and d are relatively prime, $c \geq 0$, and the Gaussian integers on L are exactly the Gaussian integers α_n given by*

$$\alpha_n = \alpha_0 + \delta n, \ n \in \mathbb{Z}.$$

Moreover, L is primitive if and only if α_0 and δ are relatively prime over $\mathbb{Z}[i]$.

Proof. If L is vertical then $\delta = i$ and $\alpha_0 = k$ for some $k \in \mathbb{Z}$. Then the Gaussian integers on L are given by $\alpha_n = k + ni$, where $n \in \mathbb{Z}$, L is primitive, and α_0 and δ are relatively prime. Thus, the lemma holds for all vertical Gaussian lines.

If L is not vertical, then by our choice of $\delta = c + di$ we have $c > 0$ and L has slope d/c. Thus c and d must be relatively prime since otherwise there would be a Gaussian integer on L between α_0 and α_1, contradicting our choice of α_1. Let β be a Gaussian integer on L. Then $\beta = \alpha_0 + r\delta$ for some real number r. But, $r = (\beta - \alpha_0)/\delta$ is in the quotient field $\mathbb{Q}(i)$, so $r \in \mathbb{Q}$. Now $r\delta = rc + rdi = \beta - \alpha_0 \in \mathbb{Z}[i]$ implies $rc, rd \in \mathbb{Z}$. Since c and d are relatively prime, it follows that $r \in \mathbb{Z}$ as needed.

For the second part of the lemma, first suppose α_0 and δ have a common Gaussian prime divisor π. Then π divides $\alpha_0 + \delta n$ for all $n \in \mathbb{Z}$, *i.e.*, π divides all Gaussian integers α_n on L and L is not primitive. Conversely, if α_0 and δ are relatively prime, then α_0 and $\alpha_1 = \alpha_0 + \delta$ are also relative prime. Thus, L is primitive in this case since it contains at least two Gaussian integers that do not share a common divisor. □

Throughout this paper, we define a Gaussian line L by its values of α_0 and δ as given in Lemma 1. Given these values, we also define a rational integer Δ associated to L by

$$\Delta = ad - bc. \tag{1}$$

Note that if $\alpha_n = x + yi = \alpha_0 + n\delta$, $n \in \mathbb{Z}$, is any other Gaussian integer on L, then $x = a + nc$, $y = b + nd$, and Δ can also be computed by $\Delta = xd - yc$. That is, Δ can be computed from the values of α_n and δ for any $n \in \mathbb{Z}$, not just from α_0 and δ. In Section 4, we use Δ to characterize the set of rational integers that divide some Gaussian integer on L. Another use of Δ is given by the following easy lemma.

Lemma 2. *Let L be a primitive Gaussian line. Then $\Delta = 0$ if and only if L is the real or imaginary line, which holds if and only if $\alpha_0 = 0$.*

Proof. The only part of the lemma that doesn't follow directly from the definitions is the fact that if $\Delta = 0$ then L is the real or imaginary line. For this assume $\Delta = 0$, so $ad = bc$. Since c and d are relatively prime, it follows that c divides a and d divides b. Thus, $a = cx$ and $b = dy$ for some $x, y \in \mathbb{Z}$. This gives $cdx = cdy$. We may assume c and d are both nonzero since otherwise a or b is equal to zero and L is the real or imaginary line. Thus, it follows that $x = y$ and $\alpha_0 = x\delta$. Hence, $x = 0$ since α_0 and δ are relatively prime and $\delta \neq 0$. Therefore, $\alpha_0 = 0$, and L is either the real or imaginary line. □

3. Primes on Gaussian Lines

One of the first questions we had when we began our study of Gaussian lines was about the distribution of Gaussian primes on these lines. We wondered whether every primitive Gaussian line contains infinitely many Gaussian primes, or if the existence of even one prime is guaranteed. This led us to consider what Tao's [6] beautiful theorem about arbitrarily shaped constellations in the Gaussian primes says about primes on Gaussian lines, and to formulate and computationally support an analog of Bertrand's Postulate to Gaussian lines.

Since the real and imaginary lines contain infinitely many primes, it is natural to wonder whether every primitive Gaussian line similarly contains infinitely many Gaussian primes. Finding even one other primitive Gaussian line that contains infinitely many Gaussian primes is a very difficult problem, however, since this is equivalent (by taking norms) to finding a quadratic polynomial that takes on infinitely many rational prime values and no such polynomials are known. For example, determining whether or not there are infinitely many Gaussian primes on the Gaussian line with $\alpha_0 = 1$ and $\delta = i$ (*i.e.* Gaussian primes of the form $\alpha_n = 1 + ni$) is equivalent to determining whether or not there are infinitely many rational primes of the form $1 + n^2$, which is Landau's fourth problem given at the 1912 International Congress of Mathematicians and remains open today. In general, it is also not known whether every irreducible quadratic polynomial attains at least one prime value, so similarly we cannot easily decide whether every primitive Gaussian line contains at least one Gaussian prime.

Despite the difficulty of finding a Gaussian line that contains infinitely many Gaussian primes, we can apply a result of Iwaniec and Lemke Oliver to prove that infinitely many Gaussian lines contain infinitely many elements that are the product of at most two Gaussian primes. For example, it is a deep theorem of Iwaniec [2] that there are infinitely many values of n such that $1 + n^2$ is the product of at most two rational primes, from which it is immediate that the vertical Gaussian line defined by $\alpha_0 = 1$ and $\delta = i$ contains infinitely many elements that are the product of at most two Gaussian primes. Iwaniec notes that his proof generalizes to show that if $G(n) = An^2 + Bn + C$ is an irreducible polynomial with $A > 0$ and C odd, then there exist infinitely many integers n such that $G(n)$ has at most two rational prime factors. This theorem also follows from a result of Lemke Oliver [4] generalizing Iwaniec's work. Applied to Gaussian lines, this result yields the following:

Theorem 1. *Let L be a primitive Gaussian line such that $1+i$ does not divide α_0. Then L contains infinitely Gaussian integers that are the product of at most two Gaussian primes.*

Proof. Let L be a primitive Gaussian line with $\alpha_0 = a + bi$, $\delta = c + di$, and $\Delta = ad - bc$ as defined in Equation (1). Assume $1+i$ does not divide α_0. The norm

of an arbitrary Gaussian integer α_n on L can be viewed as a quadratic polynomial $f(n)$ as follows:

$$f(n) = N(\alpha_n) = N(\alpha_0 + \delta n) = N(\delta)n^2 + Tr(\alpha_0\overline{\delta})n + N(\alpha_0) \qquad (2)$$
$$= (c^2 + d^2)n^2 + 2(ac + bd)n + a^2 + b^2.$$

The discriminant of f is equal to $-4\Delta^2$, which is negative unless $\Delta = 0$. Thus, f is irreducible over $\mathbb{Z}$ unless L is the real or imaginary line, by Lemma 2. Moreover, the leading coefficient of f is positive and the constant term $N(\alpha_0)$ is odd, since we are assuming $1 + i$ does not divide α_0. It follows from Iwaniec's theorem discussed above that there are infinitely many n such that $f(n) = N(\alpha_n)$ is a product of at most two rational primes; *i.e.*, α_n is a product of at most two Gaussian primes. □

Unfortunately Theorem 1 does not say anything about the distribution of Gaussian primes on Gaussian lines. For this, we first apply Tao's [6] astonishing theorem about arbitrarily shaped constellations in the Gaussian primes to Gaussian lines.

Theorem 2 (Tao [6])**.** *Given any distinct Gaussian integers $v_1, \ldots, v_k$, there are infinitely many sets $\{\alpha + rv_1, \ldots, \alpha + rv_k\}$, with $\alpha \in \mathbb{Z}[i]$ and $r \in \mathbb{Z} \setminus \{0\}$, all of whose elements are Gaussian primes.*

By choosing $\delta = c + di \in \mathbb{Z}[i]$ with $\gcd(c, d) = 1$ as usual, we can apply Tao's theorem with $v_1 = \delta$, $v_2 = 2\delta, \ldots, v_k = k\delta$. The theorem guarantees the existence of infinitely many pairs (α, r) such that all the elements in the set

$$P_{\alpha,r} = \{\alpha + r\delta, \alpha + 2r\delta, \ldots, \alpha + kr\delta\}$$

are Gaussian primes. For each α, there is a primitive Gaussian line L_α with slope $m = d/c$ (*i.e.*, $\delta = c + di$) that contains all the elements in $P_{\alpha,r}$. Thus, L_α contains k Gaussian primes in arithmetic progression. It is possible that infinitely many of the sets $P_{\alpha,r}$ are actually on the same Gaussian line (that is, infinitely many of the lines L_α have the same α_0). In this case, we thus have a Gaussian line that contains infinitely many Gaussian primes. It follows that for a fixed slope $m \in \mathbb{Q}$, either there is a Gaussian line with slope m that contains infinitely many Gaussian primes or, for all $k \geq 1$, there are infinitely many Gaussian lines with slope m that contain k Gaussian primes in arithmetic progression. Considering this for all m and excluding the real and imaginary lines (the case $\alpha_0 = 0$), gives the following:

Corollary 1. *At least one of the following two statements is true:*

1. *There is a Gaussian line with $\alpha_0 \neq 0$ that contains infinitely many Gaussian primes.*
2. *For every rational integer m and every positive integer k, there are infinitely many distinct Gaussian lines with slope m that contain k Gaussian primes in arithmetic progression.*

Note that if the first statement in the corollary is true, then by taking norms it is also true that there is a quadratic polynomial that takes on infinitely many prime values. Regarding the second statement, note that it is not possible for a Gaussian line to contain infinitely many Gaussian primes in arithmetic progression. This follows from the result of Gethner et al. [1] mentioned earlier that every Gaussian line contains arbitrarily long sequences of consecutive Gaussian composites.

We also wondered where to look for primes on Gaussian lines. On the real line, Bertrand's Postulate guarantees the existence of a rational prime between n and $2n$ for every rational integer $n \geq 3$. In other words, there exists a prime between n and the next integer that is divisible by n. We wondered if the analogous statement holds on Gaussian lines. If α_n is on a Gaussian line L then to characterize the next Gaussian integer on L divisible by α_n, we define a function $\nu : \mathbb{Z}[i] \to \mathbb{Z}$ by

$$\nu(x+iy) = \frac{N(x+iy)}{\gcd(x,y)}. \tag{3}$$

The function ν is useful because if $\beta \in \mathbb{Z}[i]$ then the smallest positive rational integer divisible by β is $\nu(\beta)$, and furthermore, $\nu(\beta)$ divides every rational integer that is divisible by β. For example, if $\beta = 2 + 6i = 2(1 + 3i)$ then the smallest positive rational integer divisible by β is $2(1 + 3i)(1 - 3i) = 20 = \nu(\beta)$, and β divides a rational integer r if and only if r is divisible by 20. With regards to Bertrand's postulate, if α_n is on a Gaussian line L then the next Gaussian integer on L divisible by α_n is $\alpha_{n+\nu(\alpha_n)} = \alpha_n + \nu(\alpha_n) \cdot \delta$. Notice that $\nu(r) = r$ for all $r \in \mathbb{Z}$, so Conjecture 1 below is equivalent to Bertrand's Postulate when L is the real line. We include a second conjecture because $\alpha_{n+N(\alpha_n)} = \alpha_n + N(\alpha_n) \cdot \delta$ is also divisible by α_n and, as we discuss below, it is more efficient to use the norm when searching for Gaussian primes on lines. Thus, we make the following two conjectures that generalize Bertrand's Postulate.

Conjecture 1 (Strong Bertrand for Gaussian lines)**.** Let L be a primitive Gaussian line. If $n > 1$, then there is always at least one Gaussian prime on L that lies between α_n and $\alpha_{n+\nu(\alpha_n)}$.

Conjecture 2 (Weak Bertrand for Gaussian lines)**.** Let L be a primitive Gaussian line. If $n > 1$, then there is always at least one Gaussian prime on L that lies between α_n and $\alpha_{n+N(\alpha_n)}$.

We wrote a program in Sage [5] to search for lines L where Conjecture 2 fails for some Gaussian integer on L. We tested over 10^{10} consecutive Gaussian integers on about 700,000 lines and the conjecture held in every case. About 607,000 of the lines we checked had $\alpha_0 = 1$ and $\delta = c + di$, where c and d were relatively prime integers ranging from one to 1,000. Additionally, we checked over 24,000 lines where c and d were random integers between 300 and 10^{18}. Finally, we checked about 65,000 lines with $\alpha_0 \neq 1$.

Our algorithm for testing Conjecture 2 relies on the fact that if $\alpha_\ell = \pi$ is a Gaussian prime between α_n and $\alpha_{n+N(\alpha_n)}$ for some $0 < n < \ell$, then π is also between α_k and $\alpha_{k+N(\alpha_k)}$ whenever $n < k < \ell$. This holds because $N(\alpha_n) < N(\alpha_k)$ whenever $0 < n < k$ by our choice of α_0 being the element of smallest norm on L. The corresponding statement does not hold for $\nu(\alpha_n)$, which is why we focus on Conjecture 2. Specifically, for every line L that we tested, we found a sequence of 10^{10} Gaussian integers α_{ℓ_i}, $1 \leq i \leq 10^{10}$, on L such that the following three conditions are satisfied:

1. Each α_{ℓ_i} is a Gaussian prime;
2. The first Gaussian prime in the sequence, α_{ℓ_1}, lies between α_1 and $\alpha_{1+N(\alpha_1)}$, *i.e.*, $1 < \ell_1 < 1 + N(\alpha_1)$;
3. For $i \geq 1$, the Gaussian prime $\alpha_{\ell_{i+1}}$ lies between the previous prime α_{ℓ_i} and the Gaussian integer $\alpha_{\ell_i+N(\alpha_{\ell_i})}$ on L, *i.e.*, $\ell_i < \ell_{i+1} < 1 + N(\alpha_{\ell_i})$.

This verifies Conjecture 2 on the line L for all $1 < n \leq \ell_{10^{10}}$.

If either conjecture is true, then it would follow that there are infinitely many Gaussian primes on every Gaussian line. Unfortunately, proving either conjecture for even one Gaussian line (with $\alpha_0 \neq 0$) seems out of reach since this would give a Gaussian line with infinitely many Gaussian primes, and hence (as discussed earlier) a quadratic polynomial that takes on infinitely many rational prime values.

4. Divisibility on Gaussian Lines

Every second integer on the real line is divisible by 2, every third by 3, every fourth by 4, and so on. We wondered if this basic periodicity property of divisibility extends to Gaussian lines, and furthermore, if there is a simple way to characterize those Gaussian primes that occur as divisors on a particular Gaussian line. In this section we show that the answer to both of these questions is *YES*.

Throughout this section, let L be a primitive Gaussian line with $\alpha_0 = a + bi$ and $\delta = c + di$ as defined in Section 2. Then α_0 and δ are relatively prime Gaussian integers, c and d are relatively prime rational integers, and the Gaussian integers on L are exactly the numbers $\alpha_n = \alpha_0 + \delta n$, $n \in \mathbb{Z}$. Also, recall the definition and properties of the function $\nu : \mathbb{Z}[i] \to \mathbb{Z}$ defined in Equation (3) since this function is used here and throughout the rest of the paper.

In the special case where L is the real line, we have $\alpha_0 = 0$, $\delta = 1$, and $\alpha_n = n$ for all $n \in \mathbb{Z}$. In this case, divisibility of integers on the line L by a rational integer r is periodic with period r. Our first theorem shows that this periodicity generalizes to arbitrary primitive Gaussian lines, specifically that divisibility by a Gaussian

integer β is periodic with period $\nu(\beta)$. Note that the periodicity of divisibility on the real line is a special case of the following theorem.

Theorem 3. *Suppose $\beta \in \mathbb{Z}[i]$ divides some Gaussian integer α_t on L. Then β divides α_n if and only if $n \equiv t \pmod{\nu(\beta)}$.*

Proof. Suppose β divides α_t for some t. Then β and δ are relatively prime, since any common divisor would also divide $\alpha_0 = \alpha_t - \delta t$, but δ and α_0 are relatively prime. Thus, β divides α_n if and only if β divides $\alpha_n - \alpha_t$, which in turn holds if and only if β divides $n - t$ since $\alpha_n - \alpha_t = \delta(n - t)$. But $n - t \in \mathbb{Z}$, so β divides α_n if and only if $\nu(\beta)$ divides $n - t$. □

Theorem 3 implies that consecutive Gaussian integers α_n and α_{n+1} on L are always relatively prime over $\mathbb{Z}[i]$, just as consecutive rational integers on the real line are always relatively prime over $\mathbb{Z}$. Also, because Theorem 3 is about Gaussian integers that divide some element on L, a natural follow-up problem is to characterize those Gaussian integers that occur as divisors of elements on L. In this section we specialize to rational integer and Gaussian prime divisors, and in Section 6 we give the complete characterization of the set of Gaussian integer divisors.

We define the *divisor set of* L, denoted $\mathcal{D}(L)$, to be the set of Gaussian integers that divide some Gaussian integer on L. Our main result in Section 6 (Theorem 11) is a complete characterization of this set. Here we begin by characterizing two of its subsets, the *rational set* and the *Gaussian-prime set*, which we need for our work in Section 5. We define the *rational set of* L, denoted $\mathcal{R}(L)$, to be the set of rational integers that divide some Gaussian integer on L, and the *Gaussian-prime set of* L, denoted $\mathcal{GP}(L)$, to be the set of non-rational Gaussian primes that divide some Gaussian integer on L. For easy reference, below are the set theoretical definitions of these three sets for a given Gaussian line L:

$$\mathcal{R}(L) = \{r \in \mathbb{Z} : r \mid \alpha_n \text{ for some } n \in \mathbb{Z}\};$$
$$\mathcal{GP}(L) = \{\pi \in \mathbb{Z}[i] : \pi \text{ is a Gaussian prime, } \pi \notin \mathbb{Z}, \text{ and } \pi \mid \alpha_n \text{ for some } n \in \mathbb{Z}\};$$
$$\mathcal{D}(L) = \{\beta \in \mathbb{Z}[i] : \beta \mid \alpha_n \text{ for some } n \in \mathbb{Z}\}.$$

Note that an element in any of these three sets does not necessarily lie on the line L, but simply divides some Gaussian integer that lies on L.

In general, the divisor set $\mathcal{D}(L)$ of L is not closed under multiplication. For example, suppose $1 + 2i$ divides α_0 and $1 - 2i$ divides α_1, so $1 + 2i, 1 - 2i \in \mathcal{D}(L)$. Since $\nu(1 + 2i) = \nu(1 - 2i) = 5$, it follows from Theorem 3 that $1 + 2i$ and $1 - 2i$ both divide every fifth Gaussian integer on L, starting with α_0 and α_1 respectively. Thus, no integer on L is divisible by their product *i.e.*, $(1 + 2i)(1 - 2i) = 5 \notin \mathcal{D}(L)$, and $\mathcal{D}(L)$ is not closed under multiplication. Our first lemma shows that this type of restriction from Theorem 3 is really the only property preventing the divisor set from being closed under multiplication.

Lemma 3. *Let β and γ be in the divisor set $\mathcal{D}(L)$ of L. If $\nu(\beta)$ and $\nu(\gamma)$ are relatively prime, then $\beta\gamma$ is in $\mathcal{D}(L)$.*

Proof. Suppose $\beta, \gamma \in \mathcal{D}(L)$. Then, by Theorem 3, there exist integers s and t such that β divides α_n if and only if $n \equiv s \pmod{\nu(\beta)}$ and γ divides α_n if and only if $n \equiv t \pmod{\nu(\gamma)}$. Since $\gcd(\nu(\beta), \nu(\gamma)) = 1$, the Chinese Remainder Theorem guarantees an integer n that satisfies both congruences. Therefore, $\beta\gamma \in \mathcal{D}(L)$. □

We use Lemma 3 to prove our next theorem and characterize the rational set of L. Recall from Equation (1) that $\Delta = ad - bc$ is a rational integer associated to L.

Theorem 4. *Let $r \in \mathbb{Z}$. Then r is in the rational set $\mathcal{R}(L)$ of L if and only if r divides Δ.*

Proof. Note that if $r, s \in \mathbb{Z}$ satisfy $rs \in \mathcal{R}(L)$, then $r \in \mathcal{R}(L)$ and $s \in \mathcal{R}(L)$ by the definition of the rational set. It follows from this and Lemma 3 that it is sufficient to prove Theorem 4 for prime powers.

Let $r = p^t$, where p is a rational prime and $t \in \mathbb{N}$. Then $r \in \mathcal{R}(L)$ if and only if p^t divides α_n for some $n \in \mathbb{Z}$. We have that $\alpha_n = \alpha_0 + n\delta$, so $\mathrm{Re}(\alpha_n) = a + nc$ and $\mathrm{Im}(\alpha_n) = b + nd$. Thus, p^t divides α_n if and only if p^t divides both $a + nc$ and $b + nd$. Recall that c and d are relatively prime, so at least one of them is not divisible by p. Without loss of generality, we assume that p does not divide c. Then c has a multiplicative inverse modulo p^t. Thus we have:

$$\begin{aligned}
p^t \mid \alpha_n &\iff a + nc \equiv 0 \pmod{p^t} \quad \text{and} \quad b + nd \equiv 0 \pmod{p^t} \\
&\iff b \equiv -nd \pmod{p^t}, \text{ where } n \equiv -ac^{-1} \pmod{p^t} \\
&\iff b \equiv ac^{-1}d \pmod{p^t} \\
&\iff ad \equiv bc \pmod{p^t} \\
&\iff p^t \mid \Delta,
\end{aligned}$$

as needed. □

Thus, the rational integers that divide some Gaussian integer α_n on L are exactly the divisors of Δ. Consequently, the rational set $\mathcal{R}(L)$ of L is finite unless $\Delta = 0$; that is, unless L is the real or imaginary line. Our next theorem characterizes the Gaussian prime set of L and shows, by contrast, that this set is always infinite.

Theorem 5. *Let π be a Gaussian prime with $\pi \notin \mathbb{Z}$. Then $\pi \in \mathcal{GP}(L)$ if and only if π does not divide δ.*

Proof. First suppose π divides δ. Then π does not divide $\alpha_n = \alpha_0 + \delta n$ for all $n \in \mathbb{Z}$ since α_0 and δ are relatively prime. Thus, $\pi \notin \mathcal{GP}(L)$ in this case.

Conversely, suppose π does not divide δ. Let π lie over the rational prime p. If p divides Δ, then p divides some Gaussian integer α_n on L by Theorem 4. Thus π

also divides α_n, and $\pi \in \mathcal{GP}(L)$ as needed. Thus, from now on we assume p does not divide Δ, and show that $\pi \in \mathcal{GP}(L)$ in this case as well.

As in Equation (2), the norm of an arbitrary Gaussian integer α_n on L can be viewed as a quadratic polynomial

$$f(n) = N(\alpha_0 + \delta n) = N(\delta)n^2 + Tr(\alpha_0\overline{\delta}\,)n + N(\alpha_0),$$

with discriminant $\text{Disc}(f) = -4\Delta^2$. If $p \neq 2$, then $p \equiv 1 \pmod 4$ since $\pi \notin \mathbb{Z}$. In this case, -1 is a square modulo p and so $\text{Disc}(f)$ is a non-zero square modulo p. Therefore, $f(n)$ has two distinct roots modulo p, so there are $r, s \in \mathbb{Z}$, $r \not\equiv s \pmod p$, such that $N(\alpha_r) \equiv N(\alpha_s) \equiv 0 \pmod p$. It follows from Theorem 3 that π and $\overline{\pi}$ both divide exactly one of α_r and α_s. Thus $\pi \in \mathcal{GP}(L)$ in this case. If $p = 2$, then $\text{Disc}(f) \equiv 0 \pmod p$ and f has a double root modulo p. It follows that π divides either α_0 or α_1. Thus, $\pi \in \mathcal{GP}(L)$ in this case as well. □

Since $\delta \neq 0$, it follows from Theorem 5 that the divisor set of a Gaussian line always contains infinitely many Gaussian primes. In particular, we have the following corollary to Theorem 5.

Corollary 2. *The divisor set $\mathcal{D}(L)$ of L contains at least one Gaussian prime that lies over p for every rational prime $p \equiv 1 \pmod 4$. Moreover, there are only finitely many rational primes $p \equiv 1 \pmod 4$ such that $\mathcal{D}(L)$ contains exactly one rational prime lying over p.*

Proof. Let π be a Gaussian prime that lies over the rational prime $p \equiv 1 \pmod 4$. Suppose that neither π nor $\overline{\pi}$ are in $\mathcal{D}(L)$. Then neither is in $\mathcal{GP}(L)$ and so both divide δ by Theorem 5. Thus p divides δ and p is a common divisor of c and d, which contradicts the definition of δ by Lemma 1. The second part of the corollary is immediate from Theorem 5 since δ has only finitely many Gaussian prime divisors. □

Taken together, Theorems 4 and 5 imply that if a Gaussian prime π divides δ, and π lies over p, then p does not divide Δ (or, equivalently, π does not divide Δ). This can also be seen directly: If π is a common divisor of both δ and Δ, then π divides d since $d\alpha_0 = \Delta + b\delta$ and α_0 and δ are relatively prime. Now, $\delta = c + di$, so π also divides c. But $c, d \in \mathbb{Z}$, so it follows that p is a common divisor of c and d, which contradicts L being primitive.

Theorems 4 and 5 characterize the rational and Gaussian prime sets of a given primitive Gaussian line. In Section 6, we use these theorems to give a complete characterization of the divisor set as well. First we use the theorems in this section to prove some results about Gaussian lines that involve the Chinese Remainder Theorem.

5. The Chinese Remainder Theorem for Gaussian Lines

In this section we prove a theorem about Gaussian lines that is analogous to the Chinese Remainder Theorem for $\mathbb{Z}$. We also use the Chinese Remainder Theorem for $\mathbb{Z}[i]$ to prove that there are always infinitely many Gaussian lines that satisfy any given CRT-type divisibility properties.

The Chinese Remainder Theorem (CRT) for $\mathbb{Z}$ implies that there will always be a solution to a system of linear congruences over $\mathbb{Z}$ when the moduli are pairwise relatively prime. It is well known that this theorem generalizes with the same proof to the Gaussian integers (or to any Euclidean domain). We state this more general version here since we will need it in our later work.

Theorem 6 (CRT for $\mathbb{Z}[i]$)**.** *Let $\mu_1, \mu_2, \ldots, \mu_k$ be pairwise relatively prime Gaussian integers and $\beta_1, \beta_2, \ldots, \beta_k$ be arbitrary Gaussian integers. Then the system of k congruences*

$$x \equiv \beta_j \pmod{\mu_j},\ 1 \leq j \leq k,$$

has a unique solution $\tau \in \mathbb{Z}[i]$ modulo $\mu_1\mu_2 \ldots \mu_k$.

Note that CRT for $\mathbb{Z}$ is just Theorem 6 with $\beta_j, \mu_j \in \mathbb{Z}$, $1 \leq j \leq k$. In the spirit of this paper, we extend CRT for $\mathbb{Z}$ to CRT for Gaussian lines. First we restate CRT for $\mathbb{Z}$ in terms of divisibility since the analogous statement for Gaussian lines is given in terms of divisibility.

Theorem 7 (CRT for $\mathbb{Z}$)**.** *Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime rational integers and $b_1, b_2, \ldots, b_k$ be arbitrary rational integers. Then there is a unique rational integer t modulo $m_1m_2 \cdots m_k$ such that*

$$m_1 \mid (t + b_1),\ m_2 \mid (t + b_2),\ \ldots,\ m_k \mid (t + b_k).$$

We use the function $\nu : \mathbb{Z}[i] \to \mathbb{Z}$ defined in Equation (3) to extend Theorem 7 to any Gaussian line. Since $\nu(n) = n$ for all $n \in \mathbb{Z}$, the following theorem reduces to CRT for $\mathbb{Z}$ when L is the real line.

Theorem 8 (CRT for Gaussian lines)**.** *Let L be a primitive Gaussian line, and suppose $\mu_1, \mu_2, \ldots, \mu_k$ are Gaussian integers in the divisor set $\mathcal{D}(L)$ of L such that $\nu(\mu_1), \nu(\mu_2), \ldots, \nu(\mu_k)$ are pairwise relatively prime. Let $b_1, b_2, \ldots, b_k \in \mathbb{Z}$. Then there is a unique rational integer t modulo $\nu(\mu_1)\nu(\mu_2) \cdots \nu(\mu_k)$ such that*

$$\mu_1 \mid \alpha_{t+b_1},\ \mu_2 \mid \alpha_{t+b_2},\ \ldots,\ \mu_k \mid \alpha_{t+b_k}.$$

Proof. Since $\mu_j \in \mathcal{D}(L)$, $1 \leq j \leq k$, it follows from Theorem 3 that for each j there exists $m_j \in \mathbb{Z}$ such that μ_j divides the Gaussian integer α_n on L if and only if $n \equiv m_j \pmod{\nu(\mu_j)}$. By Theorem 7, the system of k congruences

$$x \equiv m_j - b_j \pmod{\nu(\mu_j)},\ 1 \leq j \leq k,$$

has a unique solution $x \equiv t \pmod{\nu(\mu_1)\nu(\mu_2)\cdots\nu(\mu_k)}$. Thus, for $1 \leq j \leq k$, we have $t + b_j \equiv m_j \pmod{\nu(\mu_j)}$ and α_{t+b_j} is divisible by μ_j as needed. □

Now, suppose we want to find a primitive Gaussian line that satisfies certain CRT-type divisibility properties. For instance, suppose we want a line where $2+i$ divides α_1, $2+3i$ divides α_2, and $4080+1397i$ divides α_3. It follows from our next theorem that infinitely many such lines exist (one example in this case is the line defined by $\alpha_0 = 1$ and $\delta = 6297 + 8234i$), and the proof shows how to construct them.

Theorem 9. *Let $b_1, b_2, \ldots, b_k$ be rational integers and $\mu_1, \mu_2, \ldots, \mu_k$ be pairwise relatively prime Gaussian integers. Then there are infinitely many primitive Gaussian lines L such that μ_j divides the Gaussian integer α_{b_j} on L for all $1 \leq j \leq k$.*

Proof. To show there are infinitely many primitive Gaussian lines L that satisfy the desired divisibility conditions, we show that there are infinitely many Gaussian integers $\alpha_0 = a + bi$ and $\delta = c + di$ that satisfy all of the following properties:

(a) $N(\alpha_0 + n\delta) > N(\alpha_0)$ for all $n \neq 0$, $n \in \mathbb{Z}$;

(b) $\gcd(c, d) = 1$ and $c \geq 0$;

(c) α_0 and δ are relatively prime over $\mathbb{Z}[i]$;

(d) μ_j divides $\alpha_{b_j} = \alpha_0 + b_j\delta$ for all $1 \leq j \leq k$.

We first choose α_0. For $1 \leq j \leq k$, let $\gamma_j \in \mathbb{Z}[i]$ be a common divisor of μ_j and b_j with maximal norm (each γ_j is uniquely defined up to multiplication by a unit in $\mathbb{Z}[i]$). Let λ be any Gaussian integer that is relatively prime to both $\mu_1\mu_2\cdots\mu_k$ and $b_1b_2\cdots b_k$. Define α_0 by

$$\alpha_0 = \lambda \prod_{j=1}^{k} \gamma_j \in \mathbb{Z}[i].$$

There are infinitely many possibilities for λ, so there are infinitely many possibilities for α_0.

For each α_0, we show there are infinitely many $\delta = c + di \in \mathbb{Z}[i]$ such that the above properties (a)–(d) are satisfied. Property (d) is equivalent to δ being a solution to the system of k congruences

$$\alpha_0 + b_j x \equiv 0 \pmod{\mu_j}, \quad 1 \leq j \leq k.$$

Dividing by γ_j for each j, this is equivalent to δ being a solution to the system

$$x \equiv -\left(\frac{\alpha_0}{\gamma_j}\right)\kappa_j^{-1} \pmod{\omega_j}, \quad 1 \leq j \leq k,$$

where each $\kappa_j = b_j/\gamma_j \in \mathbb{Z}[i]$ is relatively prime to $\omega_j = \mu_j/\gamma_j \in \mathbb{Z}[i]$. Note that each α_0/γ_j is also relatively prime to ω_j since $\omega_1, \omega_2, \ldots, \omega_k$ are pairwise relatively prime. Thus, any solution to this latter system of congruences is relatively prime to the product $\omega_1\omega_2\cdots\omega_k$. Since δ will be a solution, we include an additional congruence to insure that any solution is also relatively prime to α_0 and so property (c) will automatically be satisfied. Let β be the product of all the Gaussian primes that divide α_0 but do not divide $\omega_1\omega_2\cdots\omega_k$, and let $\beta = 1$ if no such Gaussian primes exist. Then δ is relatively prime to α_0 if it is relatively prime to both β and $\omega_1\omega_2\cdots\omega_k$. Thus, to insure that properties (c) and (d) are both satisfied, it is sufficient that δ be a solution to the following system of $k+1$ congruences:

$$\begin{aligned} &x \equiv 1 \pmod{\beta}, \quad \text{and} \\ &x \equiv -\left(\frac{\alpha_0}{\gamma_j}\right)\kappa_j^{-1} \pmod{\omega_j}, \quad 1 \le j \le k. \end{aligned}$$

This system has a unique solution $\tau = r + si \in \mathbb{Z}[i]$ modulo $\beta\omega_1\omega_2\cdots\omega_k$ by CRT for Gaussian integers (Theorem 6) since $\beta, \omega_1, \omega_2, \ldots, \omega_k$ are pairwise relatively prime. Thus, it remains to construct $\delta = c + di$ that satisfies properties (a) and (b), and such that $\delta \equiv \tau \pmod{\beta\omega_1\omega_2\cdots\omega_k}$, so that properties (c) and (d) hold as well.

To satisfy property (a), we construct $\delta = c + di$ such that

$$N(\alpha_n) = N(\alpha_0 + n\delta) = (c^2+d^2)n^2 + 2(ac+bd)n + a^2 + b^2, \quad n \in \mathbb{Z},$$

obtains its minimum value only when $n = 0$. For any $c, d \in \mathbb{Z}$, the quadratic function,

$$f(x) = (c^2+d^2)x^2 + 2(ac+bd)x + a^2 + b^2, \quad x \in \mathbb{R},$$

obtains its absolute minimum when $f'(x) = 0$, *i.e.*, when $x = -(ac+bd)/(c^2+d^2)$. Thus, since f is symmetric, for property (a) to be satisfied and $f(0)$ to be the minimum integer value of f, it is sufficient that c and d satisfy

$$-\frac{1}{2} < \frac{ac+bd}{c^2+d^2} < \frac{1}{2}. \tag{4}$$

For a fixed d,

$$\lim_{c\to\infty}\left(\frac{ac+bd}{c^2+d^2}\right) = 0,$$

so Equation (4) holds for all c larger than some bound that depends on d. We use this fact to complete the proof.

It is sufficient to choose $\delta = c + di$ such that Equation (4) holds, $\gcd(c, d) = 1$, $c \ge 0$, and $\delta \equiv \tau \equiv r + si \pmod{\beta\omega_1\omega_2\cdots\omega_k}$. Let $M = N(\beta\omega_1\omega_2\cdots\omega_k) \in \mathbb{Z}$. We first consider $s = 0$. In this case, $\tau = r$ is relatively prime to M since it is a non-zero rational integer that is relatively prime to $\beta\omega_1\omega_2\cdots\omega_k$. It follows from Dirichlet's Theorem on Primes in Arithmetic Progressions, that there are infinitely

many rational primes congruent to r modulo M. Thus, we can choose a rational prime p such that $p \equiv r \pmod{M}$, $p > M$, and p is large enough so that Equation (4) holds for $c = p$ and $d = M$. Define δ by $\delta = p + Mi$. Then, Equation (4) holds and $\gcd(c, d) = 1$, since p is prime and larger than M. Also, $\delta \equiv \tau \pmod{M}$, so $\delta \equiv \tau \pmod{\beta\omega_1\omega_2 \cdots \omega_k}$, since $\beta\omega_1\omega_2 \cdots \omega_k$ divides M. Thus, α_0 and δ define a primitive Gaussian line that satisfies the divisibility conditions stated in Theorem 9. Moreover, according to Dirichlet's Theorem, there are infinitely many choices of the prime p. Thus, there are infinitely many choices for δ, and so infinitely many primitive Gaussian lines with the same α_0 that satisfy the conditions.

Similarly, if $r = 0$, then $\tau = si$, where s is a non-zero rational integer that is relatively prime to M. Proceed as above to get a rational prime $p \equiv s \pmod{M}$, $p > M$, and p is large enough so that Equation (4) holds for $c = M$ and $d = p$. Define δ by $\delta = M + pi$. Then α_0 and δ define a primitive Gaussian line that satisfies the divisibility conditions stated in Theorem 9. Again, by Dirichlet's Theorem, there are infinitely many choices of the prime p and thus infinitely many primitive Gaussian lines with this α_0 that satisfy these conditions.

Finally, suppose r and s are both non-zero rational integers. Let h be the smallest positive rational divisor of r such that $\gcd(r/h, M) = 1$. Again, by Dirichlet's Theorem, we can find a rational prime $p > s$ such that $p \equiv r/h \pmod{M}$ and p is large enough so that Equation (4) holds for $c = ph$ and $d = s$. Define δ by

$$\delta = ph + si.$$

Then $\delta \equiv \tau \pmod{\beta\omega_1\omega_2 \cdots \omega_k}$. To see that $\gcd(ph, s) = 1$, first observe that $\gcd(p, s) = 1$ since $p > s$ is prime. Also, $\gcd(h, s) = 1$, since any common rational prime divisor q of h and s is also a common divisor of τ and M. Hence, there is a Gaussian prime that lies over q that divides both τ and $\beta\omega_1\omega_2 \cdots \omega_k$, which is a contradiction since they are relatively prime. Thus, as above, α_0 and δ define a primitive Gaussian line that satisfies the required divisibility conditions, and again there are infinitely many choices of δ by Dirichlet's Theorem.

□

6. The Divisor Set of a Gaussian Line

We now return to questions about divisibility on Gaussian lines related to those discussed in Section 4. For a given primitive Gaussian line L, we first characterize those Gaussian-prime powers that exactly divide some Gaussian integer on L. Using this, our main theorem in this section gives a complete characterization of the divisor set $\mathcal{D}(L)$ of L.

Theorem 5 in Section 4 resolves the question of which Gaussian primes occur in the divisor set $\mathcal{D}(L)$ of a primitive Gaussian line L, but it does not address division

by prime powers. For example, Theorem 5 does not answer the following question: If $\pi \in \mathcal{D}(L)$, then is π^{100} guaranteed to be in $\mathcal{D}(L)$? Nor does it say anything about which prime powers π^k *exactly divide* some Gaussian integer α_n on L (*i.e.*, π^k divides α_n, but π^{k+1} does not). For example, if $\pi^{50} \in \mathcal{D}(L)$, then certainly $\pi, \pi^2, \ldots, \pi^{49} \in \mathcal{D}(L)$, but is π guaranteed to exactly divide some Gaussian integer on L? What about π^2 or π^3 or any other power of π? Our next theorem shows that the answer to all of these questions is *YES* whenever π lies over a rational prime $p \equiv 1 \pmod 4$, but is conditional for other values of p. We restrict to lines with $\Delta \neq 0$ since this simplifies the proof and exact division by all prime powers holds on the real and imaginary lines.

Theorem 10. *Let L be a primitive Gaussian line with $\Delta \neq 0$. Suppose π is a Gaussian prime that lies over the rational prime p.*

1. *If $p \equiv 1 \pmod 4$, then the following are equivalent:*
   (a) *π does not divide δ.*
   (b) *$\pi^k \in \mathcal{D}(L)$ for some positive integer k.*
   (c) *For every positive integers r, π^r exactly divides some Gaussian integer on L. In particular, $\pi^r \in \mathcal{D}(L)$ for all positive integers r.*
2. *If $p = 2$, then the following are equivalent:*
   (a) *$1 + i$ does not divide δ.*
   (b) *$(1 + i)^k \in \mathcal{D}(L)$ for some positive integer k.*
   (c) *Let 2^s be the exact power of 2 that divides Δ, and $\beta \in \mathbb{Z}[i]$ have 2-power norm. Then β exactly divides some Gaussian integer α_n on L if and only if β is an associate of $2, 2^2, \ldots, 2^s$, or $2^s(1+i)$. That is, $(1+i)^t \in \mathcal{D}(L)$ if and only if $0 \leq t \leq 2s + 1$, but $(1 + i)^t$ exactly divides a Gaussian integer on L if and only if in addition t is even or $t = 2s + 1$.*
3. *If $p \equiv 3 \pmod 4$ (so π is an associate of p), then p^k exactly divides some Gaussian integer α_n on L if and only if p^k divides Δ.*

Proof. We consider the three cases separately.
`Case 1`: Suppose $p \equiv 1 \pmod 4$. Statements 1(a) and 1(b) are equivalent by Theorem 5. Since 1(c) trivially implies 1(b), we only need to show that 1(b) implies 1(c). For this, suppose that $\pi^k \in \mathcal{D}(L)$, say π^k divides α_m. Then π^h exactly divides α_m for some $h \geq k$. Let r be a positive integer. If $r < h$, then 1(c) holds since π^r exactly divides α_n for $n = m + p^r q$, where q is any integer not divisible by p. To see this, write $\alpha_n = \alpha_0 + (m + p^r q)\delta = \alpha_m + p^r q\delta$, and use that π^h exactly divides α_m while π^r exactly divides $p^r q\delta$. Note that by considering the special case where

$r = 1$, this shows in general that if a Gaussian prime π does not divide δ then π *exactly* divides some Gaussian integer α_n on L.

We use induction and the general fact for $r = 1$ given above to show that 1(c) holds for $r \geq h$ as well. If $r = h$, then π^r exactly divides α_m by hypothesis, so 1(c) holds in this case. Suppose it holds for some $t \geq h$, say π^t exactly divides α_s. Let $\omega = \alpha_s/\pi^t \in \mathbb{Z}[i]$. For $q \in \mathbb{Z}$, consider

$$\alpha_{s+p^t q} = \alpha_s + p^t q\delta = \pi^t(\omega + \overline{\pi}^t \delta q),$$

where $p = \pi\overline{\pi}$ and $\overline{\pi}$ is not an associate of π since $p \equiv 1 \pmod 4$. Now, $\overline{\pi}^t\delta$ has no rational integer divisors since $\pi \nmid \delta$. Also, ω and $\overline{\pi}^t\delta$ are relatively prime since α_s and $p^t\delta$ are relatively prime. Thus, the numbers $\omega + \overline{\pi}^t\delta q$, $q \in \mathbb{Z}$, are the Gaussian integers on a different primitive Gaussian line L' with $\delta' = \overline{\pi}^t\delta$. Since $\pi \nmid \delta'$, it follows from the general result for $r = 1$, that there is a $q_0 \in \mathbb{Z}$ such that π exactly divides the Gaussian integer $\omega + \overline{\pi}^t\delta q_0$ on L'. Thus π^{t+1} exactly divides the Gaussian integer α_n on L for $n = s + p^t q_0$, and 1(c) holds for $r = t + 1$. By induction it holds for all r.

`Case 2`: Suppose $p = 2$. As above, it is sufficient to prove statement 2(b) implies 2(c). Suppose $(1 + i)^k \in \mathcal{D}(L)$ for some positive integer k. Then $(1 + i) \in \mathcal{D}(L)$ and $1 + i$ does not divide δ. Let 2^s, $s \geq 0$, be the exact power of 2 that divides Δ. Then $2^s \in \mathcal{D}(L)$, but $2^{s+1} \notin \mathcal{D}(L)$ by Theorem 4. Since 2 ramifies in $\mathbb{Z}[i]$, this is equivalent to $(1 + i)^{2s} \in \mathcal{D}(L)$, but $(1 + i)^{2s+2} \notin \mathcal{D}(L)$.

We first claim that $(1+i)^{2s+1} \in \mathcal{D}(L)$. For this, note that since $(1+i)^{2s} \in \mathcal{D}(L)$, there is a Gaussian integer α_m on L such that $(1 + i)^{2s}$ divides α_m. If $(1 + i)^{2s+1}$ divides α_m then $(1 + i)^{2s+1} \in \mathcal{D}(L)$ as claimed. So suppose $(1 + i)^{2s+1}$ does not divide α_m. By Theorem 3, $(1 + i)^{2s}$ divides α_{m+2^s} since $\nu((1 + i)^{2s}) = 2^s$. Now,

$$\alpha_{m+2^s} = \alpha_m + 2^s\delta = 2^s(\omega + \delta),$$

where $\omega = \alpha_m/2^s \in \mathbb{Z}[i]$ is not divisible by $1 + i$. Since neither ω nor δ is divisible by $1 + i$, their sum must be divisible by $1 + i$. Thus, $(1 + i)^{2s+1}$ divides α_{m+2^s}, and $(1 + i)^{2s+1} \in \mathcal{D}(L)$ in this case as well.

Thus we have $(1 + i)^t \in \mathcal{D}(L)$ if and only if $0 \leq t \leq 2s + 1$, and so it remains to consider exact division by $(1 + i)^t$. We consider t even and t odd separately. First suppose that $t = 2h$ is even. We claim that $(1 + i)^t$ exactly divides some Gaussian integer α_n on L, or equivalently, that 2^h divides α_n but $2^h(1 + i)$ does not. This is true when $t = s$ since $(1 + i)^{2s}$ exactly divides either α_m or α_{m+2^s} by the preceding paragraph. So suppose that for some h, $0 < h \leq s$, we have $(1+i)^{2h}$ exactly divides α_n for some n. Consider,

$$\alpha_{n+2^{h-1}} = \alpha_n + 2^{h-1}\delta = 2^{h-1}(\omega + \delta),$$

where $\omega = \alpha_n/2^{h-1} \in \mathbb{Z}[i]$ is divisible by $(1 + i)^2$ and δ is not divisible by $1 + i$. Thus, $\omega + \delta$ is not divisible by $1 + i$, and so $(1 + i)^{2h-2}$ exactly divides $\alpha_{n+2^{h-1}}$. The claim for odd t follows by induction.

Now suppose t is odd and $(1+i)^t$ exactly divides some Gaussian integer α_r on L. For instance, this holds for $t = 2s+1$ since $(1+i)^{2s+1}$ exactly divides either α_m or α_{m+2^s}. Write $t = 2j+1$, so $\nu((1+i)^t) = 2^{j+1}$. Thus, by Theorem 3, $(1+i)^t$ divides α_n for $n = r + 2^{j+1}q$, $q \in \mathbb{Z}$. Now,

$$\alpha_n = \alpha_{r+2^{j+1}q} = \alpha_r + 2^{j+1}\delta q = (1+i)^t\left(\omega + \mu(1+i)\delta q\right),$$

where $\omega = \alpha_r/(1+i)^t \in \mathbb{Z}[i]$ is not divisible by $1+i$ and $\mu \in \mathbb{Z}[i]$ is a unit. Now, the real and imaginary parts of $\mu(1+i)\delta$ must be relatively prime since $1+i$ does not divide δ and the real and imaginary part of δ are relatively prime. Also, ω and $\mu(1+i)\delta$ are relatively prime over $\mathbb{Z}[i]$ since $1+i$ does not divide ω and α_r and δ are relatively prime. Thus, the numbers $\omega + (1+i)\delta q$, $q \in \mathbb{Z}$, are the Gaussian integers on a different primitive Gaussian line L' with $\delta' = (1+i)\delta$. Since $1+i$ divides δ', it follows from Theorem 4 that none of the Gaussian integers $\omega + (1+i)\delta q$ are divisible by $1+i$, that is, $(1+i) \notin \mathcal{D}(L')$. Thus, $(1+i)^{t+1} \notin \mathcal{D}(L)$, or equivalently, $2^{j+1} \notin \mathcal{D}(L)$. This is a contradiction unless $j = s$. Therefore, if t is odd then $(1+i)^t$ exactly divides some Gaussian integer on L if and only if $t = 2s+1$.

`Case 3`: Suppose $p \equiv 3 \pmod 4$. Then p remains prime in $\mathbb{Z}[i]$ and π is an associate of p. By Theorem 4, we know that then p^k divides some Gaussian integer α_n on L if and only if p^k divides Δ. For *exact* divisibility, let s be such that p^s exactly divides Δ. Then p^s exactly divides some α_m on L since $p^{s+1} \notin \mathcal{D}(L)$. Then, as in the case $p = 2$, we have that p^{s-1} exactly divides

$$\alpha_{m+p^{s-1}} = \alpha_m + p^{s-1}\delta = p^{s-1}\left(\omega + \delta\right),$$

since $\omega = \alpha_m/p^{s-1}$ is divisible by p but δ is not. Continue in the same way to get that p^k exactly divides some Gaussian integer on L for all k with $0 \le k \le s$. □

Putting Theorem 10 together with the results in Section 4 yields a characterization of the divisor set $\mathcal{D}(L)$ of L as follows.

Theorem 11. *Let L be a primitive Gaussian line with $\Delta \neq 0$. A Gaussian integer β is in the divisor set $\mathcal{D}(L)$ of L if and only if β can be written as*

$$\beta = \mu r(1+i)^t \pi_1^{k_1}\pi_2^{k_2}\cdots\pi_m^{k_m},$$

where the variables in this expression are defined as follows:

(a) $\mu \in \{\pm 1, \pm i\}$ is a unit in $\mathbb{Z}[i]$;

(b) r is a rational integer that divides Δ;

(c) $t = 0$ if $1+i$ divides δ, and $t \in \{0, 1\}$ otherwise;

(d) For $1 \le j \le m$, π_j is a Gaussian prime such that π_j does not divide δ, $N(\pi_j) \neq 2$, and $N(\pi_j) \neq N(\pi_n)$ for $j \neq n$;

(e) For $1 \leq j \leq m$, $k_j \geq 0$ is a rational integer.

Proof. By Lemma 3, it is sufficient to characterize those $\beta \in \mathcal{D}(L)$ where $\nu(\beta)$ is a prime power. Thus, let p be a rational prime and $\beta \in \mathbb{Z}[i]$ satisfy $\nu(\beta) = p^n$ for some positive integer n.

First suppose $p \equiv 1 \pmod 4$, and let π be a Gaussian primes that lies over p. We may assume $\pi \in \mathcal{GP}(L)$ by Corollary 2 of Theorem 5. If $\overline{\pi} \notin \mathcal{GP}(L)$, then by Theorems 4 and 10, $\beta \in \mathcal{D}(L)$ if and only if $\beta = \mu p^t \pi^k$, where μ is a unit in $\mathbb{Z}[i]$ and t and k are non-negative integers, and p^t divides Δ. If, in addition, $\overline{\pi} \in \mathcal{GP}(L)$, then β can also be of the form $\mu p^t \overline{\pi}^k$.

If $p = 2$ then, up to associates, $1 + i$ is the only Gaussian prime that lies over p. Let 2^s be the power of 2 that exactly divides Δ. It follows from Theorem 10 that $\beta \in \mathcal{D}(L)$ if and only if $\beta = \mu 2^r (1 + i)^t$, where μ is a unit in $\mathbb{Z}[i]$, $0 \leq r \leq s$, and $t = 0$ if $1 + i$ divides δ and $t \in \{0, 1\}$ otherwise.

Finally, if $p \equiv 3 \pmod 4$, then p remains prime in $\mathbb{Z}[i]$. In this case, it follows from Theorem 4 that $\beta \in \mathcal{D}(L)$ if and only if $\beta = \mu p^r$, where μ is a unit in $\mathbb{Z}[i]$ and p^r divides Δ. □

References

[1] E. Gethner, S. Wagon, and B. Wick, A stroll through the Gaussian primes, *Amer. Math. Monthly,* **105** (1998), 327–338.

[2] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.* **47** (1978), no. 2, 171–188.

[3] J. Jordan and J. Rabung, A conjecture of Paul Erdös concerning Gaussian primes, *Math. Comp.* **24** (1970), 221–223.

[4] R. J. Lemke Oliver, Almost-primes represented by quadratic polynomials, Acta Arith. **151**, 241–261 (2012).

[5] *SageMath, the Sage Mathematics Software System (Version 6.8)*, The Sage Developers, 2015, http://www.sagemath.org.

[6] T. Tao, The Gaussian primes contain arbitrarily shaped constellations, *J. Anal. Math.* **99** (2006), 109–176.

[7] P. West and B. Sittinger, A further stroll into the Eisenstein primes, *Amer. Math. Monthly,* **124** (2017), 609–620.