STROLLING ALONG GAUSSIAN LINES

Elsa Magness[1]
Department of Mathematics, Seattle University, Seattle, WA 98122, USA
magnesse@seattleu.edu

Brian Nugent[2]
Department of Mathematics, Seattle University, Seattle, WA 98122, USA
nugentb@seattleu.edu

Leanne Robertson
Department of Mathematics, Seattle University, Seattle, WA 98122, USA
robertle@seattleu.edu

Abstract

If you walked to infinity along the real line stepping on consecutive integers you could discover the infinitude of the primes, arbitrarily large gaps in the sequence of primes, the periodicity of divisibility by every integer, the truth of Bertrand's postulate, arbitrarily long sequences of consecutive integers where none is relatively prime to all the others, and other properties of the integers. What could you discover if instead you walked to infinity along an arbitrary line in the complex plane stepping only on consecutive Gaussian integers? How different or similar would this stroll to infinity be? In the *Monthly* article, "A Stroll Through the Gaussian Primes," Gethner, Wagon, and Wick [2] show that you could similarly discover arbitrarily large gaps in the sequence of Gaussian primes, but would you ever observe infinitely many Gaussian primes or is even encountering one Gaussian prime guaranteed? Would you see a periodicity of divisibility similar to that on the real line? Would you stroll along arbitrarily long sequences of consecutive Gaussian integers where none is relatively prime to all the others?

This paper investigates these and related questions. We study properties of lines in the complex plane that contain two, and hence infinitely many, Gaussian integers. We call these *Gaussian lines* and show that several divisibility properties of the rational integers on the real line, including the Chinese remainder theorem, extend to divisibility properties of Gaussian integers on Gaussian lines. We investigate the distribution of Gaussian primes on Gaussian lines and a generalization of Bertrand's Postulate. We leave the reader with several open problems. (TO DO: Make most important results clearer in abstract and intro)

[1]Elsa's funding?
[2]Brian's funding?

1. TO DO/IDEAS

1. THIS IS THE COCALC VERSION
2. change to Monthly style file
3. Changed: $\alpha_0 = a + bi$ and $\delta = c + di$. Check correct everywhere. Also note $\delta \notin \mathbb{Z}$ since real and im parts are rel prime.
4. Twin primes as in Vatwani
5. Some theorems have been changed. Be sure to check they are referred to correctly.
6. Make sure $\mathcal{GP}(L)$ notation correctly incorporated throughout paper.
7. Use pmod in equations – check consistency
8. Question: For a fixed primitive Gaussian line L, is there a $k \in \mathbb{Z}^+$ that depends on L such that for $n < k$ every set of n consecutive Gaussian integers on L contains an integer that is relatively prime to all the others, and for $n \geq k$ there is always a counterexample?
9. Change notation for Morm?
10. Thank Steve

2. Introduction and Notation

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. In 1970, Jordan and Rabung [**?**] showed that steps of length at least 4 would be required, and in 1998, Gethner, Wagon, and Wick [2] showed that steps of length 5 or less are insufficient to reach infinity. In the same paper they showed that it is impossible to walk to infinity on any line in the complex plane by stepping only on Gaussian primes and taking steps of bounded length. We further investigate this idea of strolling along lines.

Instead of wondering freely on Gaussian integers in the complex plane, we ask what would happen if you walk along a straight line stepping only on Gaussian integers. What facts about the Gaussian integers would such a walker observe? How similar would the walk be to that of walking to infinity along the real line stepping only on the integers? Would you stroll on infinitely many Gaussian primes,

or perhaps none at all? In this paper we consider these questions by investigating properties of the Gaussian integers on lines in the complex plane.

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. We call a line in the complex plane a *Gaussian line* if it contains two, and hence infinitely many, Gaussian integers. A Gaussian line is called *primitive* if the integers on the line do not all share a common divisor. One special example of a primitive Gaussian line is the real line, where the set of Gaussian integers on the line is just the set $\mathbb{Z}$ of rational integers. In general, several important properties of the rational integers extend to analogous properties of the Gaussian integers on a primitive Gaussian line. We study these analogies in this paper. We prove divisibility properties of the Gaussian integers on Gaussian lines, as well as investigate properties of sets of consecutive integers, provide a generalization of the Chinese remainder theorem, discuss experimental results on an extension of Bertrand's Postulate, and investigate the distribution of Gaussian primes on these lines.

We begin with some background on Gaussian integers. The unit group of $\mathbb{Z}[i]$ is $\{\pm 1, \pm i\}$, so two Gaussian integers, α and β, are *associates* if and only if $\alpha = \pm\beta$ or $\alpha = \pm i\beta$. The *norm* of a Gaussian integer $\alpha = a + bi$ is defined to be $N(a + bi) = \alpha \cdot \overline{\alpha} = a^2 + b^2$, where the "bar" denotes complex conjugation. Unique factorization 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 natural numbers $\mathbb{Z}^+$, and *Gaussian prime* for a prime in $\mathbb{Z}[i]$. The Gaussian primes can be classified in terms of the factorization of rational primes $p \in \mathbb{Z}^+$ into Gaussian prime factors 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 and any other element of norm 2 is an associate of $1 + i$.

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 a unit multiple 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. Two Gaussian integers are *relatively prime* if they only have unit factors in common.

For every Gaussian line L, we distinguish two Gaussian integers, $\alpha_0 = a + bi$ and $\delta = c + di$ 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 $\Re(\alpha_1) > \Re(\alpha_0)$. Then take

$\delta = \alpha_1 - \alpha_0$. Thus α_0 is on the line L, but in general δ is not. Note that there are only two primitive Gaussian lines with $\alpha_0 = 0$, namely the real line $\Im(z) = 0$ and the complex line $\Re(z) = 0$.

With α_0 and δ defined in this way, the proposition below describes all Gaussian integers on L. Note that this proposition is very similar to Lemma 4.2 in [2], except that we specify α_0 and δ, and describe the primitive case, since this is convenient for our later work.

Proposition 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, 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 $\alpha_n = k + in, n \in \mathbb{Z}$, L is primitive, and α_0 and δ are relatively prime. Thus the proposition holds for all vertical Gaussian lines.

If L is a non-vertical Gaussian line, then by our choice of $\delta = c+di$ we have $c \neq 0$ and the Gaussian line 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. 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 proposition, first suppose α_0 and δ have a common divisor $\tau \in \mathbb{Z}[i]$ that is not a unit. Then τ divides $\alpha_0 + \delta n$ for all $n \in \mathbb{Z}$, *i.e.* τ 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, and L must be primitive since it contains at least two Gaussian integers that do not share a common divisor. □

Throughout this paper we use the notation in Proposition 1 to describe Gaussian lines. In Section 4 we prove analogies of divisibility properties of the rational integers on the real line to Gaussian integers on Gaussian lines. In Section 5 we extend the Chinese remainder theorem (CRT) to Gaussian lines and prove a theorem that shows you can always find a Gaussian line that satisfies certain CRT-type divisibility properties. In Section 6 we establish divisibility properties of sets of consecutive Gaussian integers on Gaussian lines. In Section 7 we investigate the distribution of Gaussian primes on Gaussian lines, and discuss experimental results on an extension of Bertrand's Postulate to Gaussian lines.

3. Definitions and Notation

This section establishes notation, definitions, and convention that we will follow for the remainder of the paper.

In this paper, L denotes an arbitrary primitive Gaussian line. We will study three sets of Gaussian integers associated to L. We define 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. The second set we will discuss is the *rational divisor set of* L, denoted $\mathbb{Z}(L)$ which we define to be the set of all rational integers that divide some Gaussian integer on L. The last set we study is the *divisor set of* L, denoted $\mathcal{D}(L)$), which we define to be the set of all Gaussian integers that divide some element of L. In Section 4, we completely classify the Gaussian integers that are in each of these three sets. Note that the elements of these sets may not lie on L, but rather divide some Gaussian integer that lies on L. Below is the formal definitions of these sets.

$$\begin{aligned}\mathcal{D}(L) &= \{\beta \in \mathbb{Z}[i] : \beta | \alpha_n \text{ for some } n \in \mathbb{Z}\}\\ \mathbb{Z}(L) &= \{d \in \mathbb{Z} : d | \alpha_n \text{ for some } n \in \mathbb{Z}\}\\ \mathcal{GP}(L) &= \{\pi \in \mathbb{Z}[i] : \pi \text{ is prime } \pi \notin \mathbb{Z}, \pi | \alpha_n \text{ for some } n \in \mathbb{Z}\}\end{aligned}$$

For any Gaussian integer $\beta = x + iy$, we would like to describe the smallest positive rational integer that β divides. If we take $\beta = 2 + 4i$, then the smallest integer that β divides is 10, which we note is $N(\beta)/2$. In general, we define a function $\nu : \mathbb{Z}[i] \to \mathbb{Z}$ by

$$\nu(\beta) = \frac{N(\beta)}{\gcd(x, y)}.$$

Then the smallest integer that β divides is $\nu(\beta)$.

4. Divisibility on Gaussian Lines

In this section we establish divisibility properties of primitive Gaussian lines. These properties are used throughout the rest of the paper.

Throughout this section, let L be a primitive Gaussian line and $\alpha_0 = a + bi$, $\delta = c + di$ be defined as in Section 3. Then c and d are relatively prime rational integers and the Gaussian integers on L are exactly the integers $\alpha_n = \alpha_0 + \delta n$, $n \in \mathbb{Z}$. Also recall from Section 3 that the prime set $\mathcal{GP}(L)$ of L is defined to be the set of Gaussian primes that divide some Gaussian integer on L.

In the special case where L is the real line, we have $\alpha_0 = 0$, $\delta = 1$, and $\alpha_n = n$, $n \in \mathbb{Z}$. In this case, divisibility of integers on the line L by a rational prime p is

periodic with period p, since here p divides α_n iff $n \equiv 0 \pmod{p}$. Our first theorem shows that this periodicity generalizes to arbitrary primitive Gaussian lines.

Theorem 1. *Let L be a primitive Gaussian line and $\omega \in \mathbb{Z}[i]$. Suppose $\omega|\alpha_t$ for some t. Then $\omega|\alpha_n$ if and only if $n \equiv t \pmod{\nu(\omega)}$.*

Proof. Suppose ω divides α_t for some t. Then ω does not divide δ, since otherwise it would also divide $\alpha_0 = \alpha_t - \delta t$, which is not possible since δ and α_0 are relatively prime by assumption. Thus, since $\alpha_n - \alpha_t = \delta(n-t)$, we have that

$$\omega|\alpha_n \Leftrightarrow \omega|(\alpha_n - \alpha_t) \Leftrightarrow \omega|(n-t).$$

But $n - t \in \mathbb{Z}$, so $\omega|(n-t)$ if and only if $\nu(\omega)|(n-t)$, as needed. □

Notice that in particular if π is a Gaussian prime that lies over the rational prime p and $\pi|\alpha_t$ for some t, then $\pi|\alpha_n$ if and only if $n \equiv t \pmod{p}$.

We have the following two useful corollaries.

Corollary 1. *Let L be a primitive Gaussian line and ω be a Gaussian integer. Then the following are equivalent:*

1. *$\omega|\alpha_0$;*
2. *$\omega|\alpha_n$ for some n that is divisible by $\nu(\omega)$;*
3. *$\omega|\alpha_n$ iff $\nu(\omega)|n$.*

Proof. Immediate from Theorem 1. □

For rational integers x and y, we have the property that if x and y are relatively prime if and only if x and $x - y$ are relatively prime. In particular, consecutive rational integers are relatively prime. Our second corollary generalizes this property to primitive Gaussian lines.

Corollary 2. *Two Gaussian integers α_s and α_t on a primitive Gaussian line L are relatively prime if and only if α_s and $t - s$ are relatively prime over $\mathbb{Z}[i]$. In particular, consecutive Gaussian integers on L, α_s and α_{s+1}, are always relatively prime.*

Proof. Let π be a Gaussian prime that lies over the rational prime p. Then, by Theorem 1, π is a common divisor of α_s and α_t iff $\pi|\alpha_s$ and $p|(t-s)$. But $p|(t-s)$ iff $\pi|(t-s)$ since $t - s \in \mathbb{Z}$, so the latter condition holds iff p is a common divisor of α_s and $t - s$. □

We next turn to the problem of characterizing which Gaussian primes occur in the prime set $\mathcal{GP}(L)$ of the primitive Gaussian line L. We first consider which rational primes occur as divisors of some Gaussian integer on L. Note that some of these primes may not be in the prime set of L because here we are including the rational primes $p \equiv 1 \pmod 4$ and $p = 2$, which are not Gaussian primes. Of course, if L is the real or imaginary line (the special cases $\alpha_0 = 0$) then every rational prime divides some Gaussian integer on L. By contrast, the following lemma shows that for all other Gaussian lines only finitely many rational primes occur as divisors of some integer on L.

Lemma 1. *Let L be a primitive Gaussian line. Let β and γ be Gaussian integers in $\mathcal{D}(L)$. If $\nu(\beta)$ and $\nu(\gamma)$ are relatively prime then $\beta\gamma \in \mathcal{D}(L)$.*

Proof. Since β and γ are in $\mathcal{D}(L)$, by Theorem 1, there exists integers a and b such that $\beta|\alpha_x$ if and only if $x \equiv a \pmod{\nu(\beta)}$ and $\gamma|\alpha_x$ if and only if $x \equiv b \pmod{\nu(\gamma)}$. By the Chinese remainder theorem, there is an x that satisfies both congruences. Therefore, $\beta\gamma \in \mathcal{D}(L)$. □

Lemma 2. *Let L be a primitive Gaussian line with $\alpha_0 \neq 0$. Let α_0 and δ be as defined above, $\Delta = ad - bc$, and p be a rational prime. Then $p^n|\alpha_t$ for some $t \in \mathbb{Z}$ iff $p^n|\Delta$.*

Proof. Note that $p|\Delta$ includes $p|\alpha_0$. For any $t \in \mathbb{Z}$ we have that $\alpha_t = \alpha_0 + t\delta$, so $\Re(\alpha_t) = a + tc$ and $\Im(\alpha_t) = b + td$. Also, at least one of c or d is not divisible by p since $\gcd(c, d) = 1$. First suppose $p \nmid c$. Then:

$$\begin{aligned} p^n|\alpha_t \text{ for some } t \in \mathbb{Z} &\Leftrightarrow p^n|(a + tc) \quad \text{and} \quad p^n|(b + td) \\ &\Leftrightarrow b \equiv -td \pmod{p^n} \quad \text{where} \quad t \equiv -ac^{-1} \pmod{p^n} \\ &\Leftrightarrow b \equiv ac^{-1}d \pmod{p^n} \\ &\Leftrightarrow ad \equiv bc \pmod{p^n} \end{aligned}$$

Similarly, if $p|c$ and $p \nmid d$ then $p|\Im(\alpha_t)$ iff $t \equiv -bd^{-1} \pmod{p^n}$. The proof in this case is the same as above with this value of t.

□

Theorem 2. *Let L be a primitive Gaussian line. An integer d is in $\mathbb{Z}(L)$ if and only if $d|\Delta$.*

Proof. This follows directly from lemma 4 and lemma 1. □

By the Theorem 5, if a rational integer d divides some α_j, then d divides Δ. So if $\Delta \neq 0$, there are finitely many rational integers that appear as factors of elements on L. The only cases where $\Delta = 0$ are the real and imaginary axes.

The next theorem characterizes the Gaussian primes that occur in the $\mathcal{GP}(L)$. Recall from Theorem 1 that for such primes π, divisibility by π on L is periodic. Namely, if $\pi \in \mathcal{GP}(L)$ lies over the rational prime p, then there exists t, $0 \leq t < p$, such that π divides α_n if and only if $n \equiv t \pmod{p}$.

Theorem 3. *Let L be a primitive Gaussian line. Let $\pi \notin \mathbb{Z}$ be a Gaussian prime that divides the rational prime $p \neq 2$. Then $\pi \in \mathcal{GP}(L)$ iff $\pi \nmid \delta$.*

Proof. ($\Rightarrow$) Assume π divides δ. Since α_0 and δ are relatively prime, $\pi \not| \alpha_n$ for all n. So $\pi \notin \mathcal{GP}(L)$.

($\Leftarrow$) The case where p divides Δ is handled by Lemma 4. We consider the case where p does not divide Δ. Then we let $x^2 \equiv -1 \pmod{p}$. Such an x exists because $p \equiv 1 \pmod{4}$. First we will assume that neither π nor $\overline{\pi}$ divides δ. One can verify that the values $s \equiv -(a+bx)(c+dx)^{-1} \pmod{p}$ and $t \equiv -(a-bx)(c-dx)^{-1} \pmod{p}$ are distinct solutions modulo p of the equation $N(\alpha_n) \equiv 0 \pmod{p}$. Note that $p \not| c^2+d^2 = (c+dx)(c-dx)$, so $(c+dx)^{-1}$ and $(c-dx)^{-1}$ exist. By Theorem 1, neither π nor $\overline{\pi}$ can divide both α_s and α_t. So, π divides α_s or α_t. Therefore, $\pi \in \mathcal{GP}(L)$.

Now we will assume that $\overline{\pi}$ divides δ. Suppose p divides both $c+dx$ and $c-dx$, then p divides $(c+dx)+(c-dx) = 2c$ and p divides $(c+dx)-(c-dx) = 2dx$. So $p|c$ and $p|d$. But we assumed $\pi \not| c+di$ so this cannot happen.

So p divides $c+dx$ or $c-dx$ but not both. So we have exactly one solution modulo p to the equation $N(\alpha_n) \equiv 0 \pmod{p}$, either $s \equiv -(a+bx)(c+dx)^{-1} \pmod{p}$ or $s \equiv -(a-bx)(c-dx)^{-1} \pmod{p}$. By the forward direction, $\overline{\pi} \notin \mathcal{GP}(L)$, so π must divide α_s. Therefore, $\pi \in \mathcal{GP}(L)$.

□

Lemma 3. *Let $\pi \notin \mathbb{Z}$ be a Gaussian prime that divides $p \neq 2$ and let L be a primitive Gaussian line. Then, $\pi^n \in \mathcal{D}(L)$ iff $\pi \in \mathcal{GP}(L)$.*

Proof. The forward direction is immediate. For the backward direction we use induction. If $\pi \in \mathcal{GP}(L)$ then $\pi \in \mathcal{D}(L)$ by definition. Now we assume $\pi^{n-1} \in \mathcal{D}(L)$. By Theorem 1, there exists a t such that for all k, π^{n-1} divides $\alpha_{t+p^{n-1}k}$. Let $\omega = \frac{\alpha_t}{\pi^{n-1}}$.

$\alpha_{t+p^{n-1}k} = \alpha_0 + \delta t + \delta p^{n-1}k = \pi^{n-1}(\omega + \delta\overline{\pi}^{n-1}k)$

Notice that $\delta\overline{\pi}^{n-1}$ has no rational integer factors. This means that $\omega + \delta\overline{\pi}^{n-1}k$ is a Gaussian line. Since $\pi \in \mathcal{GP}(L)$, $\pi \not| \delta$. So $\pi \not| \delta\overline{\pi}^{n-1}$. By theorem 3, π divides $\omega + \delta\overline{\pi}^{n-1}k_0$ for some k_0. Therefore, $\pi^n | \alpha_{t+p^{n-1}k_0}$. □

Corollary 3. *The prime set of every Gaussian line contains at least one of the Gaussian primes of norm p, for every rational prime $p \equiv 1 \pmod{4}$.*

Lemma 4. *Let L be a primitive Gaussian line. Let α_0 and δ be as defined above, $\Delta = ad - bc$, and p be a rational prime. Then $p^n \in \mathbb{Z}(L)$ iff $p^n | \Delta$.*

Proof. Note that $p|\Delta$ includes $p|\alpha_0$. For any $t \in \mathbb{Z}$ we have that $\alpha_t = \alpha_0 + t\delta$, so $\Re(\alpha_t) = a + tc$ and $\Im(\alpha_t) = b + td$. Also, at least one of c or d is not divisible by p since $\gcd(c, d) = 1$. First suppose $p \nmid c$. Then:

$$\begin{aligned} p^n|\alpha_t \text{ for some } t \in \mathbb{Z} &\Leftrightarrow p^n|(a+tc) \quad \text{and} \quad p^n|(b+td) \\ &\Leftrightarrow b \equiv -td \pmod{p^n} \quad \text{where} \quad t \equiv -ac^{-1} \pmod{p^n} \\ &\Leftrightarrow b \equiv ac^{-1}d \pmod{p^n} \\ &\Leftrightarrow ad \equiv bc \pmod{p^n} \end{aligned}$$

Similarly, if $p|c$ and $p \nmid d$ then $p|\Im(\alpha_t)$ iff $t \equiv -bd^{-1} \pmod{p^n}$. The proof in this case is the same as above with this value of t. □

Lemma 5. *Let L be a primitive Gaussian line. An integer d is in $\mathbb{Z}(L)$ if and only if $d|\Delta$.*

Proof. This follows directly from lemma 4 and lemma 1. □

Lemma 6. *Let $\pi \notin \mathbb{Z}$ be a Gaussian prime that divides $p \neq 2$ and let L be a primitive Gaussian line. Then, $\pi^n \in \mathcal{D}(L)$ iff $\pi \in \mathcal{GP}(L)$.*

Proof. The forward direction is immediate. For the backward direction we use induction. If $\pi \in \mathcal{GP}(L)$ then $\pi \in \mathcal{D}(L)$ by definition. Now we assume $\pi^{n-1} \in \mathcal{D}(L)$. By Theorem 1, there exists a t such that for all k, π^{n-1} divides $\alpha_{t+p^{n-1}k}$. Let $\omega = \frac{\alpha_t}{\pi^{n-1}}$.

$\alpha_{t+p^{n-1}k} = \alpha_0 + \delta t + \delta p^{n-1}k = \pi^{n-1}(\omega + \delta\overline{\pi}^{n-1}k)$

Notice that $\delta\overline{\pi}^{n-1}$ has no rational integer factors. This means that $\omega + \delta\overline{\pi}^{n-1}k$ is a Gaussian line. Since $\pi \in \mathcal{GP}(L)$, $\pi \not| \delta$. So $\pi \not| \delta\overline{\pi}^{n-1}$. By theorem 3, π divides $\omega + \delta\overline{\pi}^{n-1}k_0$ for some k_0. Therefore, $\pi^n|\alpha_{t+p^{n-1}k_0}$. □

Theorem 4. *A Gaussian integer ω is in $\mathbb{D}(L)$ if and only if $\omega = d\pi_1^{k_1}\pi_2^{k_2}\cdots\pi_m^{k_m}$ where $d \in \mathbb{Z}(L)$, $\pi_i \in \mathcal{GP}(L)$ and $\pi_i \neq \overline{\pi_j}$ for all i and j.*

Proof. ($\Rightarrow$) Suppose ω divides an element on our line. By lemmas 5 and 3, ω has only prime divisors in $\mathbb{Z}(L)$ and $\mathcal{GP}(L)$. So $\omega = d\pi_1^{k_1}\pi_2^{k_2}\cdots\pi_m^{k_m}$. Since d divides ω, $d \in \mathbb{Z}(L)$. Since π_i divides ω, $\pi \in \mathcal{GP}(L)$. □

TO DO: (1+i)

5. The Chinese remainder theorem for Gaussian Lines

In this section we prove a Chinese remainder theorem for 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 we can always find a primitive Gaussian line that satisfies a similar type of divisibility condition.

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) as follows:

Theorem 5 (CRT for Gaussian integers)**.** *Let $\mu_1, \ldots, \mu_k$ be pairwise relatively prime Gaussian integers and $\beta_1, \ldots, \beta_k$ be arbitrary Gaussian integers. Then the system of congruences*

$$\begin{aligned} x &\equiv \beta_1 \pmod{\mu_1} \\ x &\equiv \beta_2 \pmod{\mu_2} \\ &\vdots \\ x &\equiv \beta_k \pmod{\mu_k} \end{aligned}$$

has a unique solution $x_0 \in \mathbb{Z}[i]$ modulo $\mu_1\mu_2 \ldots \mu_k$.

Note that CRT for $\mathbb{Z}$ is just Theorem 5 with $\beta_i, \mu_i \in \mathbb{Z}$, $1 \leq i \leq k$. In the spirit of this paper, we extend CRT for $\mathbb{Z}$ to CRT for Gaussian integers on other Gaussian lines. To do this, we first restate CRT for $\mathbb{Z}$ in terms of divisibility:

Theorem 6 (CRT for $\mathbb{Z}$)**.** *Let $m_1, \ldots, m_k$ be pairwise relatively prime rational integers and $b_1, \ldots, b_k$ be arbitrary rational integers. Then there is a unique integer t modulo $m_1 m_2 \cdots m_k$ such that*

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

To extend Theorem 6 from integers on the real line to Gaussian integers on a Gaussian line we will use an important definition from Section 3. Recall, $\nu : \mathbb{Z}[i] \to \mathbb{Z}$ by

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

Then, in particular, $\nu(n) = n$ for all $n \in \mathbb{Z}$.

Theorem 7. *Let L be a Gaussian line. Suppose $\mu \in \mathbb{Z}[i]$ is only divisible by Gaussian primes in $\mathcal{GP}(L)$. Then $\mu | \alpha_m$ for some α_m on L. Moreover, μ divides α_n on L iff $n \equiv m \pmod{\nu(\mu)}$.*

Proof. TO DO: proof needed. Is statement correct? □

The following two corollaries are immediate, but stated here to emphasize analogies to the real line. The first extends the fact that divisibility by prime powers is periodic on the real line. Since $\nu(n) = n$ for all $n \in \mathbb{Z}$, the second Corollary extends the fact that on the real line the next integer divisible by $\alpha_n = n$ is $\alpha_{2n} = 2n$. This corollary is used in our work extending Bertrand's Postulate to Gaussian lines.

Corollary 4. *If $\pi \in \mathcal{GP}(L)$, then for every positive integer k there are infinitely many Gaussian integers on L that are divisible by π^k. Moreover, if π^k divides α_m then π^k divides α_n iff $n \equiv m \pmod{\nu(\pi^k)}$.*

TO DO??: Explain if π^k exactly divides α_m then π^t divides.....

Corollary 5. *If α_n is on L then the next Gaussian integer on L that is divisible by α_n is $\alpha_{n+\nu(\alpha_n)}$.*

We use Theorem 7 to prove an extension of the Chinese remainder theorem to Gaussian lines. Namely, Theorem 8 reduces to Theorem 6 in the special case where L is the real line.

Theorem 8 (CRT for Gaussian lines)**.** *Let L be a Gaussian line. Let $\mu_1, \ldots, \mu_k$ be Gaussian integers that are only divisible by primes in $\mathcal{GP}(L)$ and such that $\nu(\mu_1), \ldots, \nu(\mu_k)$ are pairwise relatively prime rational integers. Let $b_1, \ldots, b_k$ be arbitrary rational integers. Then there is a unique rational integer t modulo $\nu(\mu_1)\nu(\mu_2)\cdots\nu(\mu_k)$ such that*

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

Proof. By Theorem 7, for each μ_i, $1 \le i \le k$, there exists $m_i \in \mathbb{Z}$ such that μ_i divides α_{m_i}. Moreover, μ_i divides $\alpha_{m_i + s\nu(\mu_j)}$ for all $s \in \mathbb{Z}$. By CRT for $\mathbb{Z}$, the system of congruences

$$\begin{aligned} x &\equiv m_1 - b_1 \pmod{(\nu(\mu_1))} \\ x &\equiv m_2 - b_2 \pmod{(\nu(\mu_2))} \\ &\vdots \\ x &\equiv m_k - b_k \pmod{(\nu(\mu_k))} \end{aligned}$$

has a unique solution $t \in \mathbb{Z}$ modulo $\nu(\mu_1)\nu(\mu_2)\cdots\nu(\mu_k)$ that satisfies the following Thus, for $1 \le i \le k$, there is an $s_i \in \mathbb{Z}$ such that $\alpha_{t+b_i} = \alpha_{m_i + s_i\nu(\mu_i)}$. Hence, α_{t+b_i} is divisible by μ_i, $1 \le i \le k$, as needed.

□

Now suppose you want to construct a line that satisfies certain divisibility conditions, for instance that $2+i$ divides α_1, $2+3i$ divides α_2, and $4080+1397i$ divides the α_3. The following theorem says that such a line exists as long as your divisibility conditions adhere to Theorem 1.

Theorem 9. *Let $b_1, b_2, \ldots, b_k$ be non-negative integers and $\mu_1, \mu_2, \ldots, \mu_k$ be pairwise relatively prime Gaussian integers such that μ_i and b_i are relatively prime for $1 \leq i \leq k$. Then there exists infinitely many primitive Gaussian lines such that μ_i divides α_{b_i} for $1 \leq i \leq k$.*

Proof. (TO DO– check proof) To prove there exists such a line L, we find values for α_0 and δ that define L. If μ_i does not divide b_i for all i then take $\alpha_0 = 1$. Otherwise, let $v_1, v_2, \ldots, v_m$ be all the values for which μ_{v_i} divides b_i. We let $\alpha_0 = \prod_{i=1}^{m} \mu_{v_i}$. By Corollary 1, it suffices to find a value for δ. (TO DO: More here since the corollary is for prime divisors)

We start with a system of congruences as follows:

$$\begin{aligned} \delta &\equiv -\alpha_0 {b_1}^{-1} \pmod{\mu_1} \\ \delta &\equiv -\alpha_0 {b_2}^{-1} \pmod{\mu_2} \\ &\vdots \\ \delta &\equiv -\alpha_0 {b_k}^{-1} \pmod{\mu_k} \end{aligned}$$

Note that the inverse of $b_i \pmod{\mu_i}$ exists because b_i and μ_i are relatively prime for all i.

Notice that if δ satisfies the above system of congruences, then $\alpha_n = \alpha_0 + \delta n$ satisfies the condition of our Corollary, provided that it is indeed a line. Now, it suffices to find a solution that satisfies these congruences and also has real and imaginary parts that are relatively prime. In order to do this, we will first construct new values for each μ_i so that $\prod_{i=1}^{k} \mu_i$ is a rational integer. Note that since these new values will be multiples of the old values, a solution will still satisfy all of (**??**).

Let $\tau = \prod_{i=1}^{k} \mu_i$. Let $\pi_1, \pi_2, \ldots, \pi_g$ be the prime factors of τ. We will redefine the values of $\mu_1, \mu_2, \ldots, \mu_k$ by the following algorithm.

Suppose ${\pi_1}^t$ and $\overline{\pi_1}^s$ exactly divide τ. If π_1 is an associate of $1+i$ we handle this special case as follows. If t is even, we do not make any changes. So assume t is odd. Since $t > 0$, there exists a μ_i such that π_1^t exactly divides μ_i. Replace μ_i with $(1+i)\mu_i$. Now we handle the case when π_1 is not an associate of $1+i$. If $t < s$, then we do not make any changes. If $t \geq s$, then we proceed as follows. If

$s = 0$ then we let $\mu_{k+1} = \overline{\pi_1}^t$ and we include $\delta \equiv 1 \pmod{\mu_{k+1}}$ to our system of congruences. Then we replace k with $k+1$. If $s \neq 0$, then ${\pi_1}^s$ exactly divides μ_f for some f. We redefine μ_f by multiplying μ_f by $\overline{\pi_1}^{(t-s)}$. We repeat this process for π_i, where $j = 2, 3, \ldots, g$. Now, we let $T_0 = \prod_{i=1}^{k} \mu_i$. Note that these are our new values defined by the algorithm. Observe that T_0 is an associate of a positive rational integer since every factor of T_0 appears with exactly the same multiplicity as its conjugate. As it does not affect (**??**), we choose T to be the associate of T_0 that is a positive rational integer.

By Theorem 5, there exists a solution to our new system of congruences, which we will call $u + vi$. Recall, that this solution also satisfies our original system of congruences. Now it suffices to find a solution to the congruence $\delta \equiv u+vi \pmod{T}$ where δ has real and imaginary parts that are relatively prime. Let $H = gcd(u, T)$. Then $m = \frac{u}{H}$ is a rational integer. By Dirichlet's Theorem on Primes in Arithmetic Progression, there exists a prime q such that $q \equiv m \pmod{T}$ and $q > T$. Let $\delta = qH + di$. Since $qH \equiv u \pmod{T}$, δ satisfies our congruence so we now show that it has real and imaginary parts that are relatively prime. Observe that $\delta \not\equiv 0 \pmod{\mu_i}$ for all i, which implies that $gcd(u, v, T) = 1$. So, $gcd(H, v) = 1$. Since $v < T$, $gcd(q, v) = 1$. Therefore, δ has real and imaginary parts that are relatively prime as desired.

□

Example: We follow the proof above to construct a Gaussian line L such that $2+i$ divides α_1, $2+3i$ divides α_2, and $4080 + 1397i$ divides the α_3.

TO DO: THE CONSTRUCTION

Note that the line is not unique. Another line with these properties is given by $\alpha_0 = 1$ and $\delta = 6297 + 8234i$.

6. Sets of consecutive Gaussian integers on lines

In 1941, S.S. Pillai [3] proved that in every set of fewer than 17 consecutive integers there exists at least one integer that is relatively prime to all the others. He also conjectured that for every $k \geq 17$ there exists a set of k consecutive integers that does not have this property, and proved that this is the case for $17 \leq k \leq 430$. In the same year, Brauer [1] proved that Pillai's conjecture holds for all $k \geq 17$. In this section we investigate analogous questions about sets of consecutive Gaussian integers on Gaussian lines and leave the reader with two open problems.

For simplicity, we make the following definition, which is used throughout this section:

Definition. A set of Gaussian integers is said to have the *relatively prime property* if at least one Gaussian integer in the set is relatively prime to all the others.

Thus, by Pillai's result mentioned above, any set of 16 or fewer consecutive rational integers has the relatively prime property. We show that any set of six or fewer consecutive Gaussian integers on any primitive Gaussian line has this property, but there exist lines that contain sets of seven or more consecutive integers that do not.

Theorem 10. *Every set of 6 or fewer consecutive Gaussian integers on a primitive Gaussian line has the relatively prime property. Moreover, if $k \geq 7$, there is a primitive Gaussian line L and a set of k consecutive Gaussian integers on L that does not have this property.r*

Proof. To see that not every line has this property for $k \geq 7$, note that the real line with $\alpha_n = n$ does not have this property for $k \geq 17$ by Brauer's result mentioned above. For $7 \leq k \leq 17$, the L with $\alpha_n = 1+(83+672i)n$ does not have this property. To see this consider the set of k consecutive Gaussian integers on L beginning with α_1, that is $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$. Then:

TO DO: Say how line was formed or just use remark at end to prove statement and remark that this and Z could have done it.

Now let L be any Gaussian line and let $S = \{\alpha_s, \alpha_{s+1}, \ldots, \alpha_{s+k-1}\}$ be a set of k consecutive elements on L. To see that S contains at least one element that is relatively prime to all the others, first note that by Theorem 1, two elements of this sequence are relatively prime if and only if they have no common Gaussian prime factors that lie over a rational prime $p \leq k$.

If $k = 1, 2$, or 3 then S has the relatively prime property since two consecutive elements on L are always relatively prime. If $k = 4$. Then there are at exactly two elements in S that are divisible by $1 + i$ (α_s and α_{s+2}, or α_{s+1} and α_{s+3}) and at most two elements divisible by 3 (α_s and α_{s+3}, or only α_{s+1} or α_{s+2}). In all possible cases, there is at least one element that is not divisible by $1 + i$ or 3 and so is relatively prime to all other elements in S. Similarly, if $k = 5$ then there is an element in S that is not divisible by $1 + i$ or 3, and since there are no new Gaussian primes to consider this element is relatively prime to all other elements in S

If $k = 6$ then we must also consider divisibility by the two Gaussian primes that lie over 5. Note, however, that by Theorem 1 only α_s and α_{s+5} can share a common prime divisor that lies over 5. Thus, $1+i$ and 3 are the only possible common prime divisors of the elements $\alpha_{s+1}, \alpha_{s+2}, \alpha_{s+3}, \alpha_{s+4}$ to another element in S. But, as in the case $k = 4$, at least one of the elements $\alpha_{s+1}, \alpha_{s+2}, \alpha_{s+3}, \alpha_{s+4}$ is not divisible by $1 + i$ or 3. This element is relatively prime to all other elements in S.

□

Remark: For $k \geq 17$ the construction of the line L given by $\alpha_0 = 1$ and $\gamma =$

$83+672i$ in the proof of Theorem 10 generalizes to give a Gaussian line L such that the set $S = \{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ does not have the relatively prime property. Indeed, by Theorem 5, we can choose L to be a primitive Gaussian line such that α_1 is divisible by at least one Gaussian prime over p for all rational primes $p < k$ and α_2 is divisible by one Gaussian prime over 5. Then α_2 and α_7 have a common prime divisor that lies over 5 by Corollary 2. Similarly, for $t \geq 3$, α_1 and α_t have a common Gaussian prime divisor that lies over a rational prime dividing $t-1$.

Theorem 10 shows that every set of six consecutive integers on any primitive Gaussian line has the relatively prime property. On some primitive Gaussian lines (eg. the real line) every set of seven consecutive integers has this property, but on other lines (eg. the line discussed above with $\alpha_0 = 1$ and $\gamma = 83 + 672i$) there are sets of seven consecutive integers that do not. This lead us to ask the following question:

Question 1: For every $k \geq 7$ is there is a primitive Gaussian line L such that every set of k or fewer consecutive integers on L has the relatively prime property?

To investigate this question, for each k we consider a primitive Gaussian line L_k whose divisor set $\mathcal{D}(L_k)$ contains the minimum number of Gaussian primes π with $\nu(\pi) \leq k$. For $k \leq 100,000$, we show that every set of k or fewer consecutive integers on L_k has the relatively prime property. Thus, the answer to Question 1 is *YES* for $k \leq 100,000$. It is plausible that the answer is *YES* for all k.

For every positive integer k, we define L_k as follows. For each prime $p \equiv 1 \pmod 4$, let π_p be a Gaussian prime of norm p. Let δ_k be the product over all rational primes $p < k$,$p \equiv 1 \pmod 4$ of the Gaussian primes pi_p. Write $\delta_k = c + di$ as usual. Then δ_k has no rational prime divisors, so $\gcd(c, d) = 1$. Thus, by the Euclidean algorithm, there are $x, y \in \mathbb{Z}$ such that $cx + dy = 1$. Let L_k be the Gaussian line with $\delta = \delta_k$ and $\alpha_0 = y - xi$. Then δ and α_0 are relative prime, and $\Delta = 1$ (TO DO: EXPLAIN WHY).

Theorem 11. *For $7 \leq k \leq 100,000$ let L_k be the primitive Gaussian line described above. Then every set of k or fewer consecutive integers on L_k has the relatively prime property.*

Proof. TO DO: Finish proof

□

Returning to the real line, we have that $k = 17$ is a kind of "cut-off" value for the line. Namely, if $k < 17$ then every set of k consecutive integers has the relatively prime property, but if $k \geq 17$ then there exists a set of k consecutive integers that does not have this property. It would be interesting to know if the phenomenon of

having a "cut-off" value generalizes to all other Gaussian lines. This leads us to ask our second question:

Question 2: For every primitive Gaussian line L, does there exist a positive integer C_L such that every set of C_L or fewer consecutive integers on L has the relatively prime property, and if $k \geq C_L$ then there is a set of k consecutive integers on L that does not have this property?

We only know that such a cut-off value C_L exists when L is the real or imaginary line, in which cases $C_L = 17$.ut It would be interesting to determine a cut-off value C_L for even one more primitive Gaussian line. Notice that if the answer to both Question 1 and Questions 2 is *YES* then not only would every line have a cut-off value, but also the cut-off values would have to get arbritarily large.

7. Primes on Gaussian Lines

Mention: Klee et al, experimental results
Mention: Arbitrary long sets of Composites
Mention: Tao

In this section we formulate a conjecture that extends Bertrand's Postulate to Gaussian lines, and discuss experimental results that support this conjecture. In 1845, Joseph Bertrand conjectured that for every integer $n > 1$ there is at least one prime p such that $n < p < 2n$, and he verified his conjecture for .....

Bertrand's Postulate simply states that there is a rational prime between n and $2n$ for every rational integer n. In other words, there exists a prime number between any integer n and the next integer that is divisible by n. We have extended this idea through the following conjecture, which is supported by computer evidence detailed below.

Conjecture 1. *Let L be a Gaussian line with $\alpha_0 = 1$. Then there exists a Gaussian prime between α_n and $\alpha_{n+N(\alpha_n)}$ for every integer n.*

Our computer algorithm checks lines where $\alpha_0 = 1$ and $\delta = a + bi$ such that a and b are any pair of relatively prime integers ranging from one to one thousand, which totals to about 607,000 lines. Additionally, we checked over 24,000 lines where a, b, or both a and b were random integers greater than 300 and less than 10^{18}. On these lines, we checked 10^{10} elements beginning with α_1. Our algorithm runs as follows. First, we find $N(\alpha_1)$ and check for primes backwards beginning with $\alpha_{N(\alpha_1)}$. Once we find a Gaussian prime, α_k, we check for primes between α_k and $\alpha_{k+N(\alpha_k)}$ following the same method. Our algorithm ends if we fail to find a

Gaussian prime in this interval or if we have checked 10^{10} cases without failure. So far, our algorithm has never failed to find a prime in our desired interval.

We have also checked about 64,300 cases when $\alpha_0 \neq 1$, which makes it plausible that our extension of Bertrand's postulate holds for any Gaussian line.

If our conjecture is true, then it implies that there are infinitely many Gaussian primes on every Gaussian line, including horizontal and vertical lines. Note that a corollary of Conjecture 1 would yield a solution to Landau's fourth problem because if there are infinitely many primes on the line where $\alpha_n = 1 + in$, then the norm of these Gaussian prime elements are rational primes and have the form $1 + n^2$.

TO DO: Include open questions related to primes in this section (not a separate section)

It would be interesting to know much more about the analogies between the integers on the real line and the Gaussian integers on an arbitrary primitive Gaussian line. There are many questions one could ask:

References

[1] A. Brauer, On a property of k consecutive integers, *Bull. Amer. Math. Soc.* **47** (1941) 328–331.

[2] E. Gethner, S. Wagon, and B. Wick, A Stroll Through the Gaussian Primes, *Amer. Math. Monthly,* **105** (1998), 327–338.

[3] S. S. Pillai, On m consecutive integers-III, *Proceedings of the Indian Academy of Sciences* Vol 13 (1941), 530–533.

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

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