

# Modeling Random Walks to Infinity on Primes in $\mathbb{Z}[\sqrt{2}]$

Bencheng Li

Department of Mathematics  
University of Michigan  
Ann Arbor, MI 48105  
USA  
[benchenl@umich.edu](mailto:benchenl@umich.edu)

Steven J. Miller

Department of Mathematics and Statistics  
Williams College  
Williamstown, MA 01267  
USA  
[sjm1@williams.edu](mailto:sjm1@williams.edu)

Tudor Popescu

Department of Mathematics  
Brandeis University  
Waltham, MA 02453  
USA  
[tudorpopescu@brandeis.edu](mailto:tudorpopescu@brandeis.edu)

Daniel Sarnecki

Department of Mathematics  
Cornell University  
Ithaca, NY 14850  
USA  
[dbs263@cornell.edu](mailto:dbs263@cornell.edu)

Nawapan Wattanawanichkul

Department of Mathematics  
University of Illinois, Urbana-Champaign  
Urbana, IL 61801  
USA  
[nawapan2@illinois.edu](mailto:nawapan2@illinois.edu)

## Abstract

An interesting question, known as the Gaussian moat problem, asks whether it is possible to walk to infinity on Gaussian primes with steps of bounded length. Our work examines a similar situation in the real quadratic integer ring  $\mathbb{Z}[\sqrt{2}]$  whose primes cluster near the asymptotes  $y = \pm x/\sqrt{2}$  as compared to Gaussian primes, which cluster near the origin. We construct a probabilistic model of primes in  $\mathbb{Z}[\sqrt{2}]$  by applying the prime number theorem and a combinatorial theorem for counting the number of lattice points whose absolute values of their norms are at most  $r^2$ . We then prove that it is impossible to walk to infinity if the walk remains within some bounded distance from

the asymptotes. Lastly, we perform a few moat calculations to show that the longest walk is likely to stay close to the asymptotes; hence, we conjecture that there is no walk to infinity on  $\mathbb{Z}[\sqrt{2}]$  primes with steps of bounded length.

# 1 Introduction

## 1.1 Background

It is known that one cannot walk to infinity along real prime numbers with steps of bounded length, i.e., there is no finite number  $N$  such that there exists an infinite sequence of increasing real primes  $p_1, p_2, \dots$  where  $p_{i+1} - p_i \leq N$  for any  $i \in \mathbb{N}$ . One can prove this by using the *primorial*  $p\#$ , which is the product of all primes  $p_i$  less than or equal to  $p$ , i.e.,

$$p\# := \prod_{p_i \text{ prime, } p_i \leq p} p_i.$$

For any real prime  $p$ , consider the sequence

$$(p\# + j)_{j=2,3,\dots,p}.$$

All numbers in this sequence are composite, so we have a gap of length at least  $p - 1$  between  $p$  and the next prime. Thus, it is impossible to walk to infinity along primes taking steps of bounded length because there are infinitely many primes.

This classical problem is clearly one-dimensional as we only need to find an arbitrarily large gap on the number line. However, one can ask the more flavorful question of whether there exists a prime walk to infinity in *two dimensions*, for example, in the integer ring of a quadratic field [2, p. 368].

**Definition 1.** For a square-free integer  $d$ , the *quadratic integer ring of a quadratic field*  $\mathbb{Q}(\sqrt{d})$ , denoted by  $\mathbb{Z}[\sqrt{d}]$ , is the set

- (i)  $\{a + b\left(\frac{1+\sqrt{d}}{2}\right) \mid a, b \in \mathbb{Z}\}$  if  $d \equiv 1 \pmod{4}$ , or
- (ii)  $\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$  if  $d \equiv 2, 3 \pmod{4}$ .

We note that for any  $d$ , the *norm* of an element  $a+b\sqrt{d}$  in  $\mathbb{Z}[\sqrt{d}]$  is defined as  $a^2 - b^2d$ . We call an element in  $\mathbb{Z}[\sqrt{d}]$  a *unit* if its norm is  $\pm 1$ , and two numbers in  $\mathbb{Z}[\sqrt{d}]$  are *associates* if one is a multiple of the other by a unit. Lastly, in a unique factorization domain (UFD), for example,  $\mathbb{Z}[i]$  and  $\mathbb{Z}[\sqrt{2}]$ , a *prime* is defined as a non-zero, non-unit number that is divisible only by its associates and the units of such UFD [7, p. 268].

In particular, the *ring of Gaussian integers*  $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$  is a special case of quadratic integer rings when  $d = -1$ , and primes in  $\mathbb{Z}[i]$  are simply called *Gaussian primes*. With the notion of primes established, one can ask the earlier question regarding the existence of a prime walk to infinity in this setting. This problem is also known as the *Gaussian moat problem*.

## 1.2 Gaussian moat problem and our motivation

According to Guy [3, Problem A.16] and Gethner and Stark [4], Basil Gordon first posed the *Gaussian moat problem* in 1962, asking whether one can walk to infinity starting at the origin, and thereafter stepping only on primes in  $\mathbb{Z}[i]$  with steps of bounded length. Equivalently, the problem discusses the existence of a  $k$ -moat for any finite real  $k$ , where a  $k$ -moat is a region of composite Gaussian integers that encloses the origin with width at least  $k$ . A more general version of this problem also considers any starting point besides the origin [4].

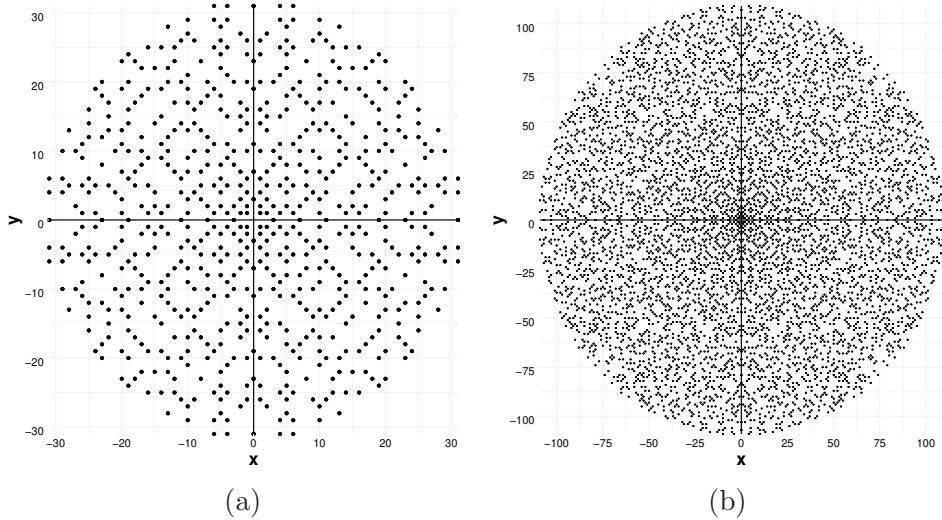


Figure 1: Gaussian primes in disks of radius 30 (Figure 1a) and 100 (Figure 1b).

To simplify the Gaussian moat problem, one can exploit the *8-fold symmetry* of the geometric structure of Gaussian primes as manifested in Figures 1a and 1b. Such symmetry can be explained by the following characterization of Gaussian primes [2, p. 378].

**Theorem 2.** *An element  $a+bi \in \mathbb{Z}[i]$  is a Gaussian prime if and only if the element satisfies one of the following requirements up to associates:*

- (i)  $a+bi$  is  $1+i$ ,
- (ii)  $a+bi$  is such that  $a^2+b^2$  is a real prime, and  $a^2+b^2 \equiv 1 \pmod{4}$ , or
- (iii)  $a+bi$  is such that  $b=0$ ,  $|a|$  is a real prime, and  $a \equiv 3 \pmod{4}$ .

Since the norm of  $a+bi$  is defined as  $a^2+b^2$ , any element  $a+bi$  is a unit if  $a^2+b^2=1$ . This gives us exactly four units in  $\mathbb{Z}[i]$ , namely,  $\pm 1$  and  $\pm i$ . Thus, for each prime in  $\mathbb{Z}[i]$ , its other three associates are also primes. Moreover, it is known that any real prime  $p$  congruent to 1 modulo 4 can be expressed as a unique sum  $a^2+b^2$  [7, p. 284]. Thus, by Theorem 2 (ii), each real prime  $p \equiv 1 \pmod{4}$  yields eight Gaussian primes:  $a+bi$ ,  $a-bi$ , and their six

associates, which implies the 8-fold symmetry. Then one can reduce the problem to finding a strip of some width at least  $k$  sweeping across the first octant.

Much progress towards the Gaussian moat problem has been made over decades. Jordan and Rabung [8], in 1970, constructed a  $\sqrt{10}$ -moat when starting at the origin while Gethner et al. [5] proved the existence of 4,  $\sqrt{18}$ , and  $\sqrt{26}$ -moats in 1998. The latter result implies that steps of length 5 are not sufficient for a walk to infinity. Moreover, in 2004, Tsuchimura [13] showed the existence of a 6-moat. While the problem remains open, there is a strong inclination from the literature [4, 5] that the answer to the Gaussian moat problem is *no*.

As mentioned earlier, the Gaussian moat problem is just a variation of the prime walk to infinity problem. Hence, in this paper, we would like to shift our focus to another quadratic ring of integers, namely,  $\mathbb{Z}[\sqrt{2}]$ . In other words, we attempt to answer *whether it is possible to walk to infinity on primes in  $\mathbb{Z}[\sqrt{2}]$  with steps of bounded length*. To begin with, we recall the following characterization of the primes in  $\mathbb{Z}[\sqrt{2}]$  [2, p. 378].

**Theorem 3.** *An element  $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$  is a prime if and only if the element satisfies one of the following requirements up to associates:*

- (i)  $a + b\sqrt{2}$  is  $\sqrt{2}$ ,
- (ii)  $a + b\sqrt{2}$  is such that  $|a^2 - 2b^2|$  is a real prime, and  $a^2 - 2b^2 \equiv 1, 7 \pmod{8}$ , or
- (iii)  $a + b\sqrt{2}$  is such that  $b = 0$ ,  $a$  is a real prime, and  $a \equiv 3, 5 \pmod{8}$ .

It is known that  $1 + \sqrt{2}$  is the *fundamental unit* of  $\mathbb{Z}[\sqrt{2}]$ , meaning that all units of  $\mathbb{Z}[\sqrt{2}]$  are of the form  $\pm(1 + \sqrt{2})^k$ , where  $k \in \mathbb{Z}$  [7, p. 270]. Thus, for each prime  $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ , its associates  $\pm(a + b\sqrt{2})(1 + \sqrt{2})^k$  are also primes. In addition, using Theorem 3 (ii), one can show that every prime number  $p \equiv 1, 7 \pmod{8}$  can be expressed as  $a^2 - 2b^2$ , for some  $a, b \in \mathbb{Z}$  by using Thue's lemma [12, p. 43].

**Lemma 4** (Thue's lemma). *Let  $a, n > 1$  be integers with  $\gcd(a, n) = 1$ . Then there exist  $x, y \in \mathbb{Z}$  with*

$$0 < |x|, |y| < \sqrt{n}$$

and

$$x \equiv ay \pmod{n}.$$

*Proof.* Let  $r = \lfloor \sqrt{n} \rfloor$ . Then  $r^2 \leq n < (r+1)^2$ . Note that the number of pairs  $(x, y)$  with  $0 \leq x, y \leq r$  is  $(r+1)^2 > n$ . Therefore, by the pigeonhole principle, there exist  $(x_1, y_1)$  and  $(x_2, y_2)$  as above such that

$$x_1 - ay_1 \equiv x_2 - ay_2 \pmod{n}.$$

In particular, we obtain that  $x_1 - x_2 \equiv a(y_1 - y_2) \pmod{n}$ . Setting  $x = x_1 - x_2$  and  $y = y_1 - y_2$ , we get the condition in the above statement, and we only have to prove that  $0 < |x|, |y| < \sqrt{n}$ .

Since  $\gcd(a, n) = 1$ , we have that if  $x = 0$ , then  $y = 0$ . However, if  $x = y = 0$ , then  $(x_1, y_1) = (x_2, y_2)$ , contradicting the fact that they are different pairs. Since  $0 \leq x_i, y_i \leq r$  for  $i \in \{1, 2\}$ , we conclude that  $0 < |x|, |y| < r \leq \sqrt{n}$  and  $x \equiv ay \pmod{n}$ .  $\square$

With the above lemma established, we now obtain the following theorem.

**Theorem 5.** *Let  $p$  be a prime number. Then  $p$  can be written as  $a^2 - 2b^2$ ,  $a, b \in \mathbb{Z}$  if and only if  $p \equiv 1, 7 \pmod{8}$ .*

*Proof.* If  $p = a^2 - 2b^2$  where  $a, b \in \mathbb{Z}$ , then  $a^2 \equiv 2b^2 \pmod{p}$ . Hence, 2 is a quadratic residue modulo  $p$ , but this is equivalent to  $p \equiv 1, 7 \pmod{8}$ .

On the other hand, if  $p \equiv 1, 7 \pmod{8}$ , then 2 is a quadratic residue modulo  $p$ , so there exists  $c$  such that  $c^2 \equiv 2 \pmod{p}$ . Using Lemma 4, there exist  $a, b \in \mathbb{Z}$  with  $0 < |a|, |b| < \sqrt{p}$  and  $a \equiv bc \pmod{p}$ . We then square the previous expression and obtain

$$a^2 \equiv b^2 c^2 \equiv 2b^2 \pmod{p} \Rightarrow a^2 - 2b^2 \equiv 0 \pmod{p}.$$

Since  $0 < a, b < \sqrt{p}$  and  $p|(a^2 - 2b^2)$ , then  $a^2 - 2b^2 = \pm p$ . If  $a^2 - 2b^2 = p$ , we have proved the theorem. Otherwise,  $-p = a^2 - 2b^2$ , and note that

$$p = 2b^2 - a^2 = (a + 2b)^2 - 2(a + b)^2.$$

$\square$

Therefore, by using Theorem 3 (ii) and the fundamental unit  $1 + \sqrt{2}$ , each prime  $p \equiv 1, 7 \pmod{8}$  contributes infinitely many  $\mathbb{Z}[\sqrt{2}]$  primes of the form  $\pm(x \pm y\sqrt{2})(1 + \sqrt{2})^{2k}$ , where  $p = x^2 - 2y^2$  and  $k$  is any integer. However, there are only four associates with the same Euclidean norm, namely,  $\pm(x \pm y\sqrt{2})$ . This implies the 4-fold symmetry of primes in  $\mathbb{Z}[\sqrt{2}]$  as contrast to the 8-fold symmetry of  $\mathbb{Z}[i]$ . Hence, it is sufficient to study walks on  $\mathbb{Z}[\sqrt{2}]$  primes in the first quadrant. In Figures 2a and 2b, we notice that primes in  $\mathbb{Z}[\sqrt{2}]$  tend to cluster near the asymptotes  $y = \pm x/\sqrt{2}$ , whereas Gaussian primes only cluster near the origin. Because of this distinct geometric structure of primes in  $\mathbb{Z}[\sqrt{2}]$ , if there exists an unbounded walk in  $\mathbb{Z}[\sqrt{2}]$  that steps on the primes with steps of bounded length, then the walk is expected to stay close to the asymptotes.

### 1.3 Results

We observe in Figure 3 that the number of primes in the disk centered at the origin with radius  $n < 60$  in  $\mathbb{Z}[\sqrt{2}]$  is greater than that of  $\mathbb{Z}[i]$ . The observation leads us to Theorem 18 in Section 2, in which we show that the density of primes in  $\mathbb{Z}[\sqrt{2}]$  is higher than that in  $\mathbb{Z}[i]$ . We also deduce from Theorem 18 and Figures 2a and 2b that a prime walk in  $\mathbb{Z}[\sqrt{2}]$  in the first quadrant is more likely to exist near the asymptote  $y = x/\sqrt{2}$ . In Section 3, we then present the main theorem of this paper, Theorem 21, which states that it is impossible to perform a walk to infinity taking steps of bounded length on primes in  $\mathbb{Z}[\sqrt{2}]$  if the walk

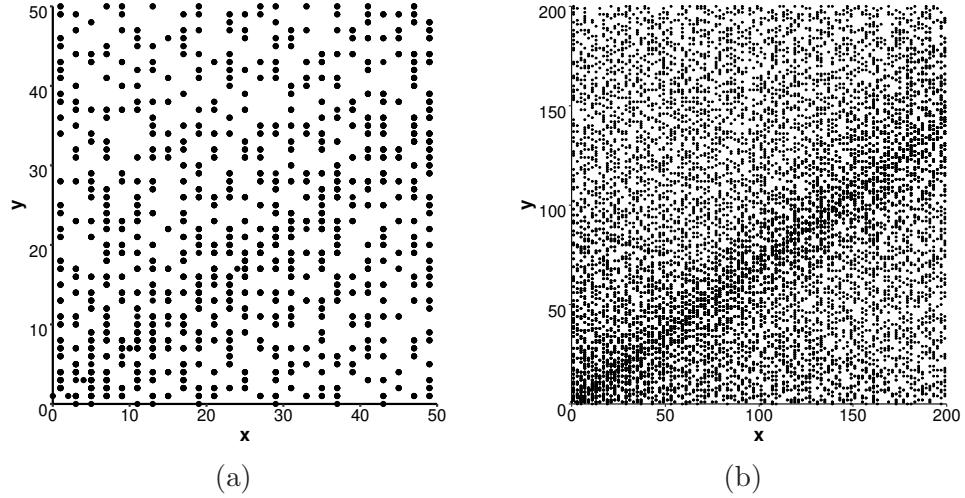


Figure 2: Primes in  $\mathbb{Z}[\sqrt{2}]$  where  $0 \leq x, y \leq 50$  (Figure 2a) and  $0 \leq x, y \leq 200$  (Figure 2b).

remains within some bounded distance from the asymptote  $y = x/\sqrt{2}$ . Lastly, in Section 4, we present some evidence that the longest walk possible must stay close to the asymptote. We are therefore led to Conjecture 22, which states that it is impossible to have such a walk to infinity in  $\mathbb{Z}[\sqrt{2}]$ .

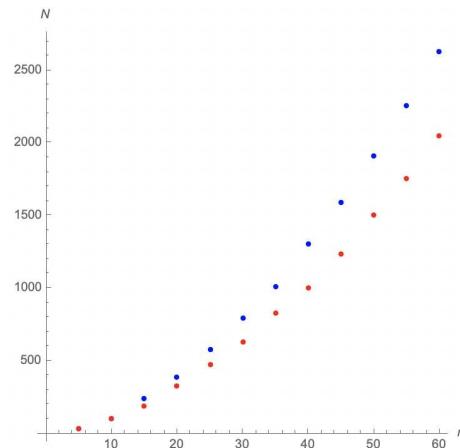


Figure 3: The number of primes ( $N$ ) in  $\mathbb{Z}[i]$  (red, bottom) and  $\mathbb{Z}[\sqrt{2}]$  (blue, top) within the disk centered at the origin with radius  $n$ .

## 2 Modeling primes in $\mathbb{Z}[\sqrt{2}]$

### 2.1 Density of Gaussian primes

Our goal in this section is to obtain an asymptotic count for the density of primes in  $\mathbb{Z}[\sqrt{2}]$ . To do so, we adapt Loh's approximation of Gaussian primes in the disk of radius  $r$  centered at the origin [9, p. 143], which relies on the *prime number theorem* [7, p. 10] and *Dirichlet's theorem on arithmetic progressions* [10, pp. 542–545].

**Theorem 6** (Prime number theorem, PNT). *Let  $\pi(x)$  be the number of primes not exceeding a real number  $x$ . Then*

$$\pi(x) \sim \frac{x}{\log x}.$$

We note that here, as well as throughout the paper,  $\log$  refers to the natural logarithm, and  $f(x) \sim g(x)$  means that  $\lim_{x \rightarrow \infty} f(x)/g(x) = 1$ .

**Definition 7** (Dirichlet density). For two sets of positive integers  $S \subseteq T$ , with  $\sum_{n \in T} n^{-1}$  divergent, the *Dirichlet density of  $S$  in  $T$* , denoted by  $d(S, T)$ , exists if and only if

$$\liminf_{s \rightarrow 1^+} \frac{\sum_{n \in S} n^{-s}}{\sum_{n \in T} n^{-s}} = d(S, T) = \limsup_{s \rightarrow 1^+} \frac{\sum_{n \in S} n^{-s}}{\sum_{n \in T} n^{-s}}.$$

**Definition 8.** We let  $\mathbb{P}$  be the set of positive primes and  $\mathbb{P}(a; m)$  the set of positive primes  $p$  such that  $p \equiv a \pmod{m}$ .

**Theorem 9** (Primes in arithmetic progressions). *Suppose  $a, m \in \mathbb{Z}$ , with  $\gcd(a, m) = 1$ . Then  $d(\mathbb{P}(a; m), \mathbb{P}) = 1/\varphi(m)$ , where  $\varphi$  is Euler's totient function.*

Using the above tools, Loh [9, p. 143] has obtained the following theorem.

**Theorem 10.** *The number of Gaussian primes contained within the disk of sufficiently large radius  $r$  about the origin is asymptotic to*

$$\frac{2r^2}{\log r}.$$

*Proof.* Theorem 9 implies that the densities of primes of the forms  $4k + 1$  and  $4k + 3$  are the same since  $d(\mathbb{P}(1; 4), \mathbb{P}) = d(\mathbb{P}(3; 4), \mathbb{P}) = 1/\varphi(4) = 1/2$ . As in Theorem 2, all the Gaussian primes can be derived from real primes as follows:

- (i) the real prime 2 gives us four Gaussian primes:  $1+i, 1-i, -1+i$ , and  $-1-i$ ,
- (ii) any real prime  $p = 4k + 3$  supplies four Gaussian primes:  $p, -p, pi$ , and  $-pi$ ,
- (iii) any real prime  $p = 4k + 1$  supplies eight Gaussian primes as  $p$  can be written as a unique sum  $a^2 + b^2 = (a+bi)(a-bi)$ , i.e., each  $p$  gives  $a+bi, -(a+bi), (a+bi)i, -(a+bi)i, a-bi, -(a-bi), (a-bi)i$ , and  $-(a-bi)i$ .

Now, consider the disk centered at the origin with radius  $r \geq 1$ . From (ii), any real  $(4k + 3)$ -prime supplies four Gaussian primes on the real and imaginary axes. We derive from the PNT and Theorem 9 that there are asymptotically  $r/(\varphi(4) \log r)$   $(4k + 3)$ -primes, so the number of Gaussian primes lying on the axes within the disk is asymptotic to

$$4 \cdot \frac{r}{\varphi(4) \log r} = \frac{2r}{\log r}. \quad (1)$$

Next, consider the disk excluding the axes. For positive integers  $1, 2, \dots, r^2$ , there are asymptotically  $r^2/\log r^2$  primes. Note that we consider the integers from 1 to  $r^2$  since each lattice point in the disk has the norm of at most  $r^2$ . By Theorem 9, asymptotically half of them are primes of the form  $4k + 1$ . From (iii), the number of Gaussian primes supplied by these  $(4k + 1)$ -primes is asymptotic to

$$8 \cdot \frac{r^2}{2 \log r^2} = \frac{2r^2}{\log r}. \quad (2)$$

Combining the results from (i), (1), and (2) gives the desired estimate.  $\square$

Thus, the density of Gaussian primes in the disk of radius  $r$  centered at the origin can be obtained by dividing the estimate in Theorem 10 by the number of lattice points in the disk, which is known to be  $\pi r^2 + O(r)$  [6, p. 67].

**Theorem 11.** *The density of Gaussian primes in the disk of radius  $r$  centered at the origin is asymptotic to*

$$\frac{2}{\pi \log r},$$

i.e., the probability that a Gaussian integer in the disk is prime is asymptotically  $2/(\pi \log r)$ .

## 2.2 Density of primes in $\mathbb{Z}[\sqrt{2}]$

In generalizing the PNT to the Gaussian primes, we consider primes whose norms lie within an interval. In particular, we estimate the number of Gaussian primes of the form  $a + bi$  such that  $a^2 + b^2 \leq r^2$ . We follow this line of thinking in generalizing further to primes in  $\mathbb{Z}[\sqrt{2}]$ , where we take the absolute value of the norm as the norm can be negative. Here, we estimate the number of primes of the form  $a + b\sqrt{2}$  such that

$$|a^2 - 2b^2| \leq r^2. \quad (3)$$

**Definition 12.** Let  $\text{NR}(r^2)$  be the *norm region* defined by  $|x^2 - 2y^2| \leq r^2$  where  $x, y \in \mathbb{R}$ .

Clearly,  $\text{NR}(r^2)$  contains all the points  $(a, b) \in \mathbb{Z}[\sqrt{2}]$  that satisfy (3), so our goal is then to estimate the number of primes within  $\text{NR}(r^2)$ . However, unlike the disk norm region  $x^2 + y^2 \leq r^2$  that we use for counting the Gaussian primes,  $\text{NR}(r^2)$  is unbounded with infinite area as shown in Figures 4a and 4b. Thus, there might be infinitely many primes within  $\text{NR}(r^2)$ . To verify this statement and for convenience, we define the following notation:

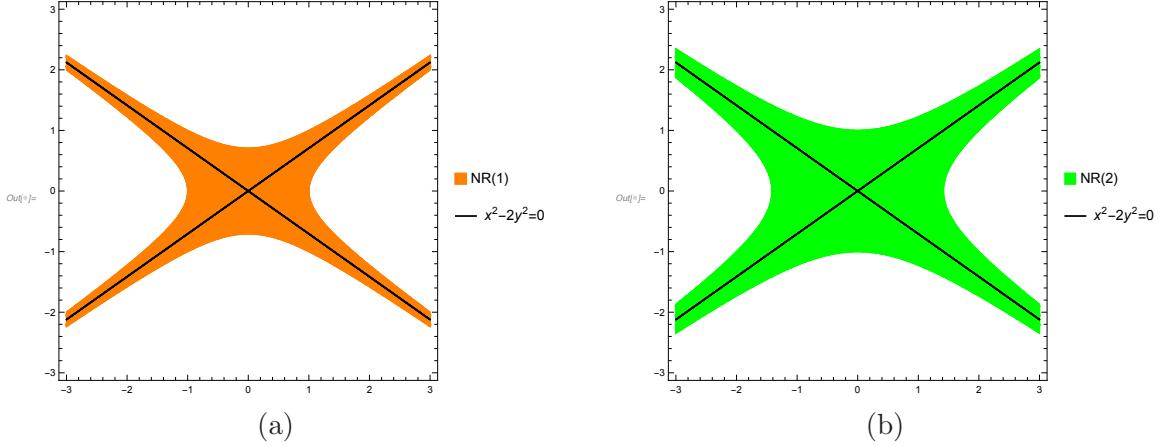


Figure 4: Norm regions  $\text{NR}(1)$  (orange; Figure 4a) and  $\text{NR}(2)$  (green; Figure 4b), enclosed by  $|x^2 - 2y^2| = 1$  and  $|x^2 - 2y^2| = 2$ , respectively, and the asymptotes  $y = \pm x/\sqrt{2}$ , i.e., the graph  $x^2 - 2y^2 = 0$  (black).

**Definition 13.** For any  $k \in \mathbb{Z}$ , let  $\text{NC}(k)$  denote the  $k$ -norm curve or the graph of the equation  $x^2 - 2y^2 = k$ .

**Lemma 14.** For any  $r^2 \geq 2$ , there exist infinitely many primes within  $\text{NR}(r^2)$ .

*Proof.* Notice that the  $k$ -norm curve that is closest to the origin and contains at least one prime is  $\text{NC}(-2)$  because  $\sqrt{2}$  and  $-\sqrt{2}$  lie on the curve. We know that, for every prime  $x + y\sqrt{2}$  in  $\mathbb{Z}[\sqrt{2}]$ , its associates of the form  $\pm(x + y\sqrt{2})(1 + \sqrt{2})^{2n}$ , where  $n \in \mathbb{Z}$ , are also primes on the same curve. In particular, there are infinitely many primes on  $\text{NC}(-2)$ , so any norm region  $\text{NR}(r^2)$  where  $r^2 \geq 2$  contains infinitely many primes.  $\square$

According to Lemma 14, it is impossible to approximate the number of primes in  $\mathbb{Z}[\sqrt{2}]$  within a certain norm region. However, as the number of  $k$ -norm curves within any  $\text{NR}(r^2)$  is finite, we now shift our goal to estimate the number of  $k$ -norm curves that contain primes in  $\mathbb{Z}[\sqrt{2}]$  and reside within the norm region  $\text{NR}(r^2)$ . For convenience, for any elements in  $\mathbb{Z}[\sqrt{2}]$  that lie on the same  $k$ -norm curve, we say that they are in the same *family*.

**Theorem 15.** The number of families of primes in  $\mathbb{Z}[\sqrt{2}]$  within  $\text{NR}(r^2)$  is asymptotic to

$$\frac{r^2}{2 \log r}.$$

*Proof.* According to Theorem 3 (iii), the number of primes in  $\mathbb{Z}[\sqrt{2}]$  within  $\text{NR}(r^2)$  that lie on the positive real axis is the same as the number of real primes  $\equiv 3, 5 \pmod{8}$  that are less than  $r$ . Hence, by the PNT and Theorem 9, there are asymptotically

$$2 \cdot \frac{r}{\varphi(8) \log r} = \frac{r}{2 \log r} \tag{4}$$

such primes. Since, for each prime  $p$  on positive real axis,  $-p$  and  $p$  are in the same family  $\text{NC}(p^2)$ , these primes then supply asymptotically  $r/(2 \log r)$  prime families within  $\text{NR}(r^2)$  when considering the entire real axis.

Similarly, there are asymptotically

$$2 \cdot 2 \cdot \frac{r^2}{\varphi(8) \log r^2} = \frac{r^2}{2 \log r} \quad (5)$$

real primes  $p \equiv 1, 7 \pmod{8}$  from  $-r^2$  to  $r^2$ . From Theorem 3 (ii), each norm  $p$  supplies a unique family  $\text{NC}(p)$ .

Combining (4), (5), and another family of primes containing  $\pm\sqrt{2}$ ,  $\text{NC}(-2)$ , there are asymptotically

$$\frac{r^2}{2 \log r}$$

distinct families of primes within the region  $\text{NR}(r^2)$ .  $\square$

The above analysis also confirms our observation that primes in  $\mathbb{Z}[\sqrt{2}]$  are most dense near the asymptotes  $y = \pm x/\sqrt{2}$ , since the region  $\text{NR}(r^2)$  for any  $r$  each straddles the asymptotes. The distribution of primes in  $\mathbb{Z}[\sqrt{2}]$  differs from the Gaussian primes which are most dense near the origin. This fact may have implications towards how to construct the longest walk possible in  $\mathbb{Z}[\sqrt{2}]$ .

Now that we have an estimate on the number of families of primes within  $\text{NR}(r^2)$ , we want to determine the total number of families of  $\mathbb{Z}[\sqrt{2}]$  integers within this region to make a statement about the probability of encountering a family of primes. Note that not every  $\text{NC}(k)$  such that  $|k| \leq r^2$  contains element of  $\mathbb{Z}[\sqrt{2}]$  because integer  $k$  may not be expressible as  $x^2 - 2y^2$  for some  $x, y \in \mathbb{Z}$ . Thus, to count the number of families of  $\mathbb{Z}[\sqrt{2}]$  integers within  $\text{NR}(r^2)$ , we refer to the following variation of a well-known theorem of Landau [11]. Note that a more general result can be found in Bernays' 1912 thesis [1].

**Theorem 16.** *For any integer  $m \neq -k^2$ . Let  $B_m(n)$  be the number of positive integers less than or equal to  $n$  that can be expressed as  $f(x, y) = x^2 + my^2$  where  $x, y \in \mathbb{Z}$ . Then*

$$B_m(n) \sim \frac{b_m n}{\sqrt{\log n}},$$

where  $b_m$  is some positive constant.

To apply Theorem 16, we take  $n = r^2$  and  $f(x, y) = x^2 - 2y^2$  and verify that  $m = -2$  is not a negative square. Then we can find an asymptotic estimate for the number of positive integers  $k < r^2$  such that

$$k = x^2 - 2y^2 = N(x + y\sqrt{2})$$

for some  $x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ . In other words, we have an estimate for the number of families of integers in  $\mathbb{Z}[\sqrt{2}]$  with positive norms that reside in  $\text{NR}(r^2)$ . We determine the number of families of integers with negative norms as follows.

**Lemma 17.** *There exist  $a_1, b_1 \in \mathbb{Z}$  such that  $a_1^2 - 2b_1^2 = k$  if and only if there exist  $a_2, b_2 \in \mathbb{Z}$  such that  $a_2^2 - 2b_2^2 = -k$ .*

*Proof.* This can be proved using the fact that the norm in  $\mathbb{Z}[\sqrt{2}]$  is multiplicative. Since  $N(1 + \sqrt{2}) = -1$ , we simply have

$$N(a_1 + b_1\sqrt{2})N(1 + \sqrt{2}) = -k = N((a_1 + b_1\sqrt{2})(1 + \sqrt{2})).$$

□

In geometric terms, Lemma 17 tells us that if we have an integer that lies on the norm curve  $\text{NC}(k)$ , then there also exists an integer that lies on the related norm curve  $\text{NC}(-k)$ , and vice versa. Therefore, for any  $r \in \mathbb{N}$ , the number of families of  $\mathbb{Z}[\sqrt{2}]$  integers within  $\text{NR}(r^2)$  is asymptotic to

$$2 \cdot \frac{b_{-2}r^2}{\sqrt{\log r^2}}, \quad (6)$$

where  $b_{-2}$  is a constant as stated in Theorem 16.

Then we can divide our estimate of the number of families of primes in  $\text{NR}(r^2)$  from Theorem 15 by the total number of families of  $\mathbb{Z}[\sqrt{2}]$  integers in  $\text{NR}(r^2)$  in (6) to determine the probability of encountering a family of primes in  $\text{NR}(r^2)$ . Thus, our work culminates in the following estimate.

**Theorem 18.** *The probability that a  $\mathbb{Z}[\sqrt{2}]$  integer  $z \in \text{NR}(r^2)$  is in a family of prime is asymptotic to*

$$\frac{1}{2b_{-2}\sqrt{2 \log r}}.$$

It is worth noting that the analogous probabilities for  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  are asymptotic to  $1/\log r$  and  $2/(\pi \log r)$ , respectively, which indicates a greater density of primes for  $\mathbb{Z}[\sqrt{2}]$  within its respective norm-region.

### 3 Proof of main results

In the previous section, we have shown that, within a fixed norm region, the number of primes in  $\mathbb{Z}[\sqrt{2}]$  is infinite, yet the number of families of primes, i.e., the number of  $k$ -norm curves containing primes, is finite. While these curves have infinitely many primes, their exponential growth renders them increasingly and negligibly sparse as our walk of linear growth rate progresses. This observation leads to our main theorem in this section, which states that for any positive integers  $k$  and  $r$ , there is no unbounded walk in the first quadrant of  $\mathbb{Z}[\sqrt{2}]$  that steps on the primes, has step length bounded by  $k$ , and has distance from  $y = x/\sqrt{2}$  bounded by  $r$ .

We now introduce the following lemmas that are needed for the proof of the main theorem.

**Lemma 19.** For any norm curve  $\text{NC}(k)$  containing some prime  $P = x + y\sqrt{2}$ , another integer  $P'$  on the same curve is also a prime if and only if  $P'$  is of the form  $\pm(x \pm y\sqrt{2})(1 + \sqrt{2})^{2m}$  for some  $m \in \mathbb{Z}$ .

*Proof.* ( $\leftarrow$ ) If  $P'$  can be written as  $\pm(x + y\sqrt{2})(1 + \sqrt{2})^{2m}$ , then  $P'$  is a prime as it is an associate of  $x + y\sqrt{2}$ . Thus, we only need to show that any conjugate of a prime is also a prime, i.e.,  $x - y\sqrt{2}$  is a prime. Let us denote the conjugate of  $a + b\sqrt{2}$  by  $\overline{a + b\sqrt{2}}$ . Notice that

$$\overline{(a + b\sqrt{2})(c + d\sqrt{2})} = \overline{(a + b\sqrt{2})}\overline{(c + d\sqrt{2})}. \quad (7)$$

Hence, the conjugate of a product of elements in  $\mathbb{Z}[\sqrt{2}]$  is the product of the conjugate of each element.

From Theorem 3, we know that any prime  $P$  can be written as  $\pm Q(1 + \sqrt{2})^m$ ,  $m \in \mathbb{Z}$ , where  $Q$  is either  $\sqrt{2}$ , a real prime  $\equiv 3, 5 \pmod{8}$ , or  $x + y\sqrt{2}$  where  $x^2 - 2y^2$  is a real prime  $\equiv 1, 7 \pmod{8}$ . Then we can easily check that  $\overline{Q}$  is also a prime for each case. Hence, by (7),

$$\overline{P} = \pm \overline{Q(1 + \sqrt{2})^k} = \pm \overline{Q}\overline{(1 + \sqrt{2})^k} = \pm \overline{Q}(-1)^k(1 + \sqrt{2})^{-k},$$

which is an associate of the prime  $\overline{Q}$ . Therefore,  $\overline{P}$  is also a prime.

( $\rightarrow$ ) Suppose that  $P' = x' + y'\sqrt{2}$  is another prime on the same curve but not of the form  $\pm(x \pm y\sqrt{2})(1 + \sqrt{2})^{2m}$ . Since both  $P$  and  $P'$  are on the same norm curve, we have

$$N(P') = (x' + y'\sqrt{2})(x' - y'\sqrt{2}) = (x + y\sqrt{2})(x - y\sqrt{2}) = N(P). \quad (8)$$

By definition of primes in a UFD, both  $x + y\sqrt{2}$  and  $x - y\sqrt{2}$  are divisible only by its associates and the units of the UFD, so  $x' + y'\sqrt{2}$  is either a unit or an associate of  $x^2 - 2y^2$ . Either case implies that one of  $x' + y'\sqrt{2}$  and  $x' - y'\sqrt{2}$  must be a unit. Thus,  $|N(P')| = |N(x' + y'\sqrt{2})| = |N(x' - y'\sqrt{2})| = 1$ , a contradiction because  $|N(P)| \neq 1$ .  $\square$

Using the same argument as in the forward direction proof of Lemma 19, we can show that if  $P = x + y\sqrt{2}$  is a prime and  $Q = x' + y'\sqrt{2}$  is a  $\mathbb{Z}[\sqrt{2}]$  integer with the same norm, then  $Q$  is also a prime. This can be shown by considering (8) and noticing that neither  $x' + y'\sqrt{2}$  nor  $x' - y'\sqrt{2}$  can be a unit. Then each of them must be an associate of  $P$  or of the conjugate of  $P$ . Therefore, *if there is a prime on a k-norm curve, every integer on that curve is also a prime*.

**Lemma 20.** If  $P = x + y\sqrt{2}$  is a prime in  $\mathbb{Z}[\sqrt{2}]$  where  $x, y \in \mathbb{N}$ , then there is at most one prime between  $P$  and  $P' = P(1 + \sqrt{2})^2 = (3x + 4y) + (2x + 3y)\sqrt{2}$ , which are both on the same norm curve.

*Proof.* Consider the norm curve  $\text{NC}(x^2 - 2y^2)$  and, without loss of generality, suppose that  $x^2 - 2y^2 > 0$ , i.e., we examine the black curves in Figure 5. A similar proof can also be achieved for when  $x^2 - 2y^2 < 0$ , i.e., the blue curves in the same figure.

We first let  $S = \{x + y\sqrt{2} \in \mathbb{Z}[\sqrt{2}] | x, y > 0\} \cap \text{NC}(x^2 - 2y^2)$ , which is the set of all  $\mathbb{Z}[\sqrt{2}]$  integers on the norm curve  $\text{NC}(x^2 - 2y^2)$  in the first quadrant. There must be a

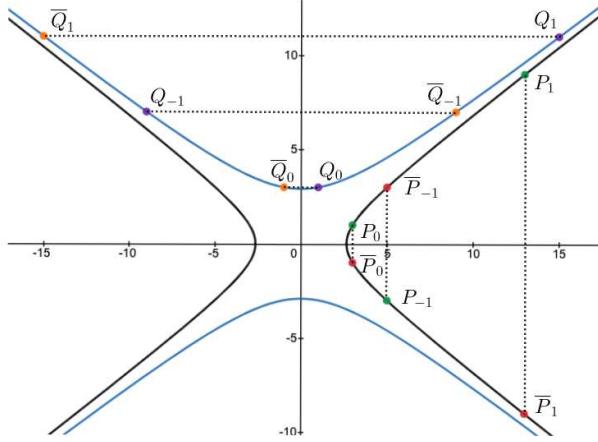


Figure 5: Positions of primes on the same norm curves.

prime  $P_0 = x_0 + y_0\sqrt{2}$  in the set  $S$  where  $x_0, y_0 > 0$  with the smallest Euclidean norm as the Euclidean norm of each element in  $S$  is of the form  $\sqrt{M}$ , where  $M \in \mathbb{N}$ .

For convenience, we let  $P_k$  denote the prime  $x_k + y_k\sqrt{2} = (x_0 + y_0\sqrt{2})(1 + \sqrt{2})^{2k}$  and  $\bar{P}_k$  denote its conjugate. Then, from Lemma 19, each prime on the curve  $\text{NC}(x^2 - 2y^2)$  is either  $P_k$ ,  $-P_k$ ,  $\bar{P}_k$ , or  $-\bar{P}_k$  for some  $k \in \mathbb{Z}$ . We also note that since  $\text{NC}(x^2 - 2y^2)$  is symmetric about the  $y$ -axis, the  $x$ -coordinate of all primes on the right curve of  $\text{NC}(x^2 - 2y^2)$  must be positive.

We now show that all  $P_k$ 's and  $\bar{P}_k$ 's are on the right curve of  $\text{NC}(x^2 - 2y^2)$ , hence all  $-P_k$ 's and  $-\bar{P}_k$ 's are on the left. For any  $P_k = x_k + y_k\sqrt{2}$  where  $x_k, y_k > 0$ , we have that

$$P_{k+1} = P_k(1 + \sqrt{2})^2 = (3x_k + 4y_k) + (2x_k + 3y_k)\sqrt{2}.$$

Since  $x_k, y_k > 0$ , we obtain that  $3x_k + 4y_k > x_k$  and  $2x_k + 3y_k > y_k$ . Hence,  $x_{k+1} > x_k > 0$  and  $y_{k+1} > y_k > 0$  for any  $k \in \mathbb{N}$ . Therefore, all  $P_k$ 's for  $k \in \mathbb{N}$  are on the right curve.

Next, we consider  $P_{-k}$  where  $k > 0$ . In particular, we have

$$P_{-1} = x_{-1} + y_{-1}\sqrt{2} = P_0(1 + \sqrt{2})^{-2} = (3x_0 - 4y_0) + (3y_0 - 2x_0)\sqrt{2}.$$

Since we consider the norm curve  $x^2 - 2y^2 > 0$ , we have  $y_0 < x_0/\sqrt{2}$ . Hence,  $x_{-1} = 3x_0 - 4y_0 > 3x_0 - 2\sqrt{2}x_0 = (3 - 2\sqrt{2})x_0 > 0$ , so  $P_{-1}$  is still on the right curve of  $\text{NC}(x^2 - 2y^2)$ . If  $P_{-1}$  is on the upper half-curve, we would have  $x_{-1} > x_0$  and  $y_{-1} > y_0$  because the graph is increasing and  $P_0$  has the smallest Euclidean norm with  $x_0, y_0 > 0$ . However, this is impossible because we would have  $y_{-1} = 3y_0 - 2x_0 > y_0$  implying  $y_0 > x_0$ . Hence,  $y_{-1} < 0$ , i.e.,  $P_{-1}$  is on the lower half-curve. Similarly, we can show that  $x_{-k-1} > x_{-k}$  and  $y_{-k-1} < y_{-k}$  for  $k \geq 1$ .

Therefore, all  $P_k$ 's where  $k \in \mathbb{Z}$  lie on the right curve of  $\text{NC}(x^2 - 2y^2)$ , implying that all  $\bar{P}_k$ 's lie on the right norm curve while  $-P_k$ 's and  $-\bar{P}_k$ 's lie on the left curve. In particular,  $P_k$ 's and  $\bar{P}_{-k-1}$ 's for  $k \geq 0$  are all primes on the *right upper* half-curve, and their locations are shown in Figure 5.

Lastly, we show that there is at most one prime between  $P$  and  $P'$ . We note that  $P$  is either  $P_m$  or  $\bar{P}_m$  for some  $m \in \mathbb{Z}$ . Since these two cases have similar proofs, we only show the prior one. Suppose that there are at least two primes between  $P = P_m$  and  $P' = P_{m+1}$ , which are both on the upper half-curve, i.e.,  $m \geq 0$ . Then they must be  $\bar{P}_{-n}$  and  $\bar{P}_{-n-1}$  for some  $n > 0$ . However, we know that  $x_m < x_{-n}$ ,  $y_m < -y_{-n}$ ,  $x_{m+1} = 3x_m + 4y_m$ , and  $y_{m+1} = 3y_m + 2x_m$ . Hence, it follows that

$$x_{-n-1} = 3x_{-n} - 4y_{-n} > 3x_m + 4y_m = x_{m+1},$$

and

$$-y_{-n-1} = -3y_{-n} + 2x_{-n} > 3y_m + 2x_m = y_{m+1}.$$

Therefore,  $\bar{P}_{-n-1} = x_{-n-1} - y_{-n-1}\sqrt{2}$  is not between  $P_m$  and  $P_{m+1}$ , a contradiction. Thus, there can be at most one prime between  $P$  and  $P'$ .  $\square$

We are now ready to prove the main theorem.

**Theorem 21.** *For any positive integers  $k$  and  $r$ , there is no unbounded walk in the first quadrant of  $\mathbb{Z}[\sqrt{2}]$  that steps on the primes, has step length bounded by  $k$ , and has distance from  $y = x/\sqrt{2}$  bounded by  $r$ .*

*Proof.* Our goal is to construct a bounded region where every prime within it is of at most distance  $r$  from the line  $y = x/\sqrt{2}$  and then show that the number of primes in that region is clearly less than the minimum number of steps needed to walk across it.

Assume that any possible walk to infinity remains within some bounded distance  $r$  from  $y = x/\sqrt{2}$  and that we take steps of length at most  $k$ . Let  $S = (p, q)$  be some sufficiently large prime (in terms of its Euclidean norm) that belongs to the walk, and, without loss of generality,  $S$  is below the asymptote. We then construct the line perpendicular to  $y = x/\sqrt{2}$  passing through  $S$ . Let this line intersect  $y = x/\sqrt{2}$  at  $P = (x, y)$  as in Figure 6. Then we construct  $A$  and  $B$  on the line perpendicular to the asymptote such that  $AP = BP = r$ . By construction,  $S$  is between  $A$  and  $P$ .

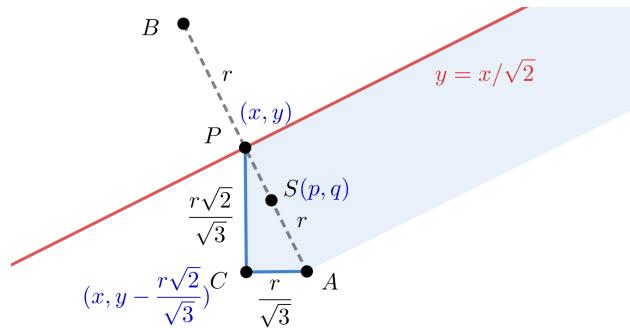


Figure 6: Constructing the desired bounded area.

Now, we construct  $C$  to be the point where the vertical line passing through  $P$  intersects the horizontal line passing through  $A$ . It follows that  $CA = \frac{r}{\sqrt{3}}$  and  $CP = \frac{r\sqrt{2}}{\sqrt{3}}$ . Hence,

$C = \left( x, y - \frac{r\sqrt{2}}{\sqrt{3}} \right)$ . Note that now, for any point in the shaded area in Figure 6, the point is always above and to the right of  $C$ .

We now consider any prime  $K = (m, n)$  in the shaded area and  $K'$  be the coordinates that represent the prime  $(m + n\sqrt{2})(1 + \sqrt{2})^2$ , i.e.,  $K' = (3m + 4n, 2m + 3n)$ . Then

$$d(K, K') = \sqrt{(2m + 4n)^2 + (2m + 2n)^2}.$$

On the other hand, if we define  $C'$  similarly to  $K'$ , i.e.,

$$C' = \left( 3x + 4 \left( y - \frac{r\sqrt{2}}{\sqrt{3}} \right), 2x + 3 \left( y - \frac{r\sqrt{2}}{\sqrt{3}} \right) \right),$$

we then have

$$d(C, C') = \sqrt{\left( 2x + 4 \left( y - \frac{r\sqrt{2}}{\sqrt{3}} \right) \right)^2 + \left( 2x + 2 \left( y - \frac{r\sqrt{2}}{\sqrt{3}} \right) \right)^2}. \quad (9)$$

Since  $m > x$  and  $n > y - \frac{r\sqrt{2}}{\sqrt{3}}$  because  $K$  is above and to the right of  $C$ , we have that  $d(K, K') > d(C, C')$ , for any  $K$  in the shaded region in Figure 6.

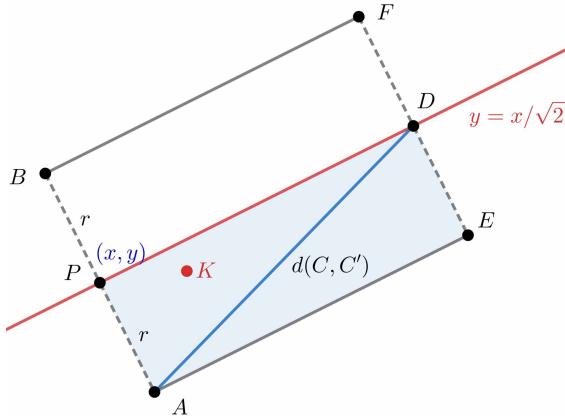


Figure 7: Constructing the bounded region  $APDE$ .

Next, we construct  $D$  on the asymptote such that  $AD = d(C, C')$  and let  $E$  be the point such that  $\overline{ED} \parallel \overline{AP}$  and  $ED = r$  as in Figure 7. Then, in the rectangle  $APDE$ , the greatest distance between any 2 points within the region is  $d(C, C')$ . As we have observed that  $d(K, K') > d(C, C')$  for any  $K$  in the shaded region in Figure 6, the same is true for any  $K$  in the rectangle  $APDE$ . Equivalently,  $d(K, K') > d(C, C')$  for any prime  $K = m + n\sqrt{2}$  in  $APDE$ .

In other words, within the rectangle  $APDE$ , if we step on some prime  $K$ , the prime  $K'$  will not lie inside  $APDE$ . This means *there are at most 2 primes on the same norm curve*

within APDE, namely  $K$  and the prime between  $K$  and  $K'$  if there is any, according to Lemma 20.

With the above fact, let us now estimate the minimum number of steps needed to walk across  $ABFE$ , where  $F$  is the reflection of  $E$  about the asymptote as in Figure 7, and the number of possible primes we can step on in the same area. Let  $g(x)$  be the vertical gap between the asymptote  $y = x/\sqrt{2}$  and the curve  $x^2 - 2y^2 = c$  in the first quadrant, which can be rewritten as  $y = \sqrt{x^2 - c}/\sqrt{2}$ . Then  $g(x)$  can be computed as

$$g(x) = \frac{x - \sqrt{x^2 - c}}{\sqrt{2}} = \frac{c}{\sqrt{2}(x + \sqrt{x^2 - c})} \geq \frac{c}{2\sqrt{2}x}.$$

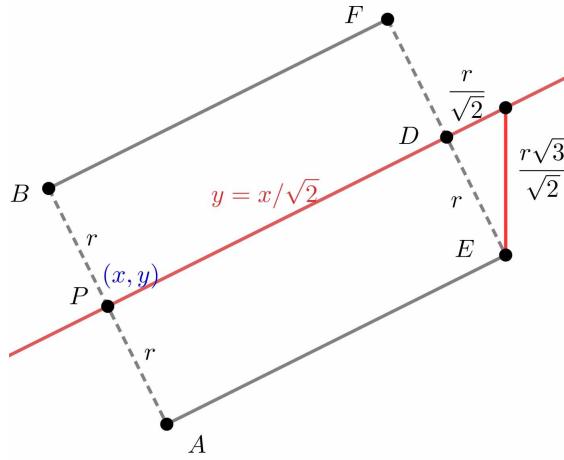


Figure 8: The vertical length from  $E$  to the asymptote  $y = x/\sqrt{2}$ .

To find the largest  $c$  such that the curve  $y = \sqrt{x^2 - c}/\sqrt{2}$  stays within APDE, we need  $g(x)$  not to exceed the vertical length from  $E$  to the asymptote, which is  $r\sqrt{3}/\sqrt{2}$  as shown in Figure 8. Thus

$$\frac{c}{2\sqrt{2}x} \leq g(x) \leq \frac{r\sqrt{3}}{\sqrt{2}},$$

so  $c \leq 2\sqrt{3}rx$ .

However, not all of the norm curves within the norm region  $\text{NR}(2\sqrt{3}rx)$  contain primes. From Theorem 15, within  $\text{NR}(2\sqrt{3}rx)$ , the number of norm curves that contain primes is asymptotic to

$$\frac{2\sqrt{3}rx}{2 \log \sqrt{2\sqrt{3}rx}} = O\left(\frac{x}{\log x}\right).$$

In particular, as we have observed that there are at most 2 primes on the same norm curve within APDE and hence  $ABFE$  by symmetry, the number of primes we can step on is at most twice of the estimate above, which is still  $O(x/\log x)$ .

On the other hand, we need to take as few as  $\lceil PD/k \rceil$  steps to go from the front  $\overline{AB}$  to the front  $\overline{EF}$ . Thus, from (9), the number of steps needed is bounded below by

$$\begin{aligned} \frac{PD}{k} &= \frac{\sqrt{AD^2 - AP^2}}{k} = \frac{\sqrt{d(C, C')^2 - r^2}}{k} \\ &= \frac{\sqrt{\left(2x + 4\left(y - \frac{r\sqrt{2}}{\sqrt{3}}\right)\right)^2 + \left(2x + 2\left(y - \frac{r\sqrt{2}}{\sqrt{3}}\right)\right)^2 - r^2}}{k}. \end{aligned}$$

Note that  $P = (x, y)$  is on  $y = x/\sqrt{2}$ , so replacing  $y$  with  $x/\sqrt{2}$  gives us that the number of steps needed is  $\Omega(x)$ , whereas the number of primes within  $ABFE$  is  $O(x/\log x)$ . Therefore, for a sufficiently large  $S$  hence  $x$ , the number of primes we can step on within  $ABFE$  is much less than the number of steps needed to walk across the same region.  $\square$

By the symmetry of primes in  $\mathbb{Z}[\sqrt{2}]$ , the theorem is also true for the third quadrant and the second and fourth quadrants when considering the asymptote  $y = -x/\sqrt{2}$  instead.

## 4 Visualizing prime walks

In this section, we present some evidence of why every prime walk in  $\mathbb{Z}[\sqrt{2}]$  with steps of bounded length is likely to stay close to the asymptote. We construct a random walk on primes in  $\mathbb{Z}[\sqrt{2}]$  with steps of length at most  $k$  by starting at  $\sqrt{2}$  and searching randomly for the next prime within distance  $k$  from the previous one. We also require the next prime has a larger Euclidean norm than the previous one to let the walk always spread further away from the origin. Figure 9 shows a collection of such random walks with step size  $\sqrt{8}$  starting from  $\sqrt{2}$ . It is interesting to discover that nearly all of the longest random walks are close to the asymptote  $y = \pm x/\sqrt{2}$ . When the starting point is chosen randomly and not necessarily  $\sqrt{2}$ , the resulting random walks also have the same property. In Figure 10, we have a collection of random walks with step size  $\sqrt{8}$  starting from  $13 + 15\sqrt{2}$ . Again, the longest walk is very close to the asymptote  $y = \pm x/\sqrt{2}$ .

We now describe the algorithm used to visualize all possible prime walks for step size  $k = \sqrt{8}$  starting from the origin. The algorithm consists of four main steps. The first step is to identify all primes in a disk of radius  $n$  for some large  $n$  by checking whether each element in the disk satisfies Theorem 3. Then, for each prime  $p$ , we find its  $k$ -neighbors which are primes within the distance  $k$  from  $p$ . Next, we form the road network connecting all primes and their  $k$ -neighbors, and find the connected component of  $\sqrt{2}$ , which is the prime closest to the origin. Finally, we can calculate all possible prime walks (ideally, if not limited by the running time) with steps of length at most  $k$  starting from the origin.

When  $k$  is  $\sqrt{8}$ , Figure 11 shows that the prime walks can go as far as  $x = 1500$ . Note that in reality the walks do not end there, but due to the limitation of our algorithm, the running time increases dramatically as the walks progress, so we need to stop the calculation after a certain point. Still, there is a clear trend that the longest walk is near the asymptote

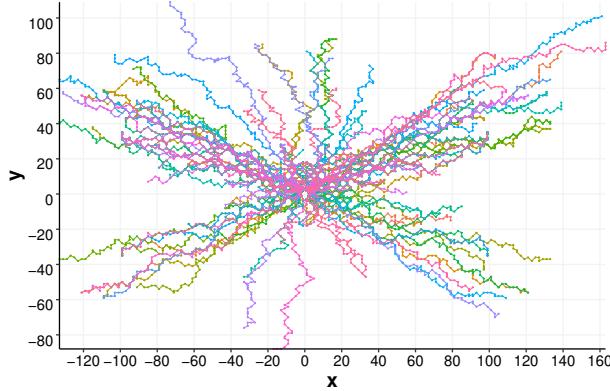


Figure 9: Random walks on primes with  $k = \sqrt{8}$  starting at  $\sqrt{2}$ .

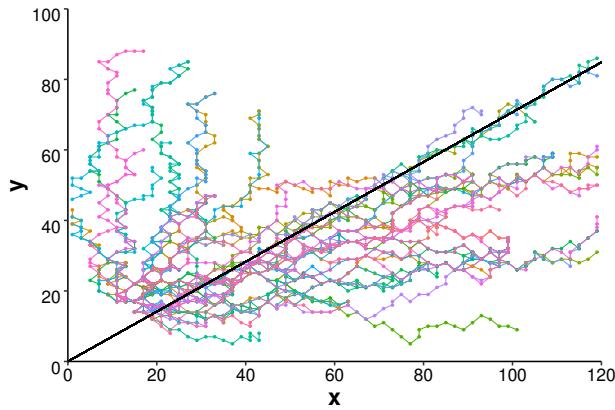


Figure 10: Random walks on primes with  $k = \sqrt{8}$  starting at  $13 + 15\sqrt{2}$  with the asymptote  $y = x/\sqrt{2}$  (black).

$y = x/\sqrt{2}$ , so the condition on the bounded distance from  $y = x/\sqrt{2}$  in Theorem 21 may not be necessary.

**Conjecture 22.** For any positive integers  $k$ , there is no unbounded walk in  $\mathbb{Z}[\sqrt{2}]$  that steps only on the primes and has step length bounded by  $k$ .

## 5 Conclusion

By estimating the number of primes near the asymptote  $y = x/\sqrt{2}$ , we have shown that there is no prime walk to infinity with steps of bounded length in  $\mathbb{Z}[\sqrt{2}]$  if every prime walk in  $\mathbb{Z}[\sqrt{2}]$  is guaranteed to stay within some bounded distance from  $y = x/\sqrt{2}$ . With several moat computations, we have demonstrated that the longest prime walks tend to cluster near the asymptote, which leads to Conjecture 22. One direction for future work is to prove Conjecture 22 and generalize this result to other quadratic integer rings that are UFDs, such

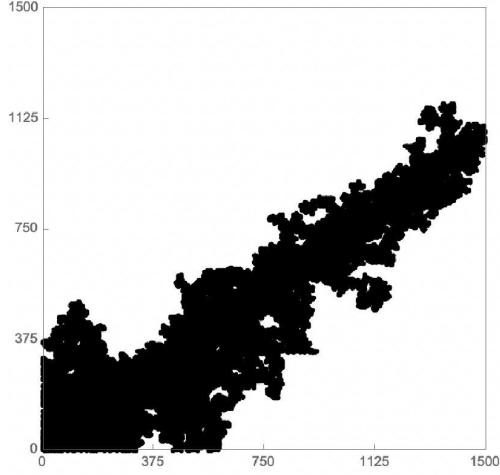


Figure 11: All prime walks with  $k = \sqrt{8}$  from the origin in the first quadrant.

as  $\mathbb{Z}[\sqrt{3}]$ ,  $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ , or  $\mathbb{Z}[\sqrt{7}]$ . Figures 12a and 12b show that primes in  $\mathbb{Z}[\sqrt{3}]$  also cluster near the asymptote  $x^2 - 3y^2 = 0$  similar to the case of  $\mathbb{Z}[\sqrt{2}]$ , and hence suggest that there should exist no prime walk to infinity with steps of bounded length in  $\mathbb{Z}[\sqrt{3}]$ . Another direction is to study prime walks in the quadratic integer rings that are not UFDs, such as  $\mathbb{Z}[\sqrt{-5}]$ , since our proof of the main theorem requires the ring to be a UFD.

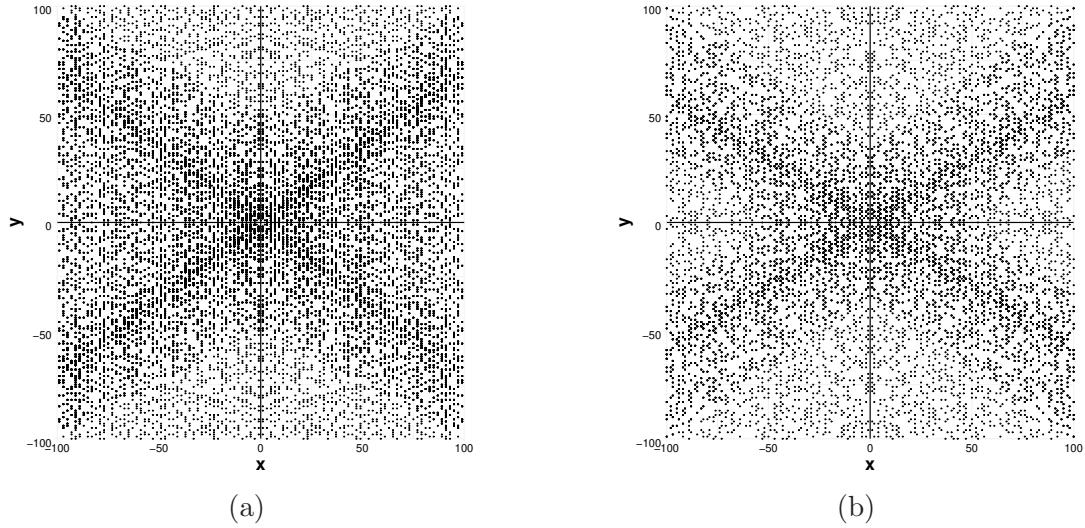


Figure 12: Primes in  $\mathbb{Z}[\sqrt{2}]$  (Figure 12a) and  $\mathbb{Z}[\sqrt{3}]$  (Figure 12b).

## 6 Acknowledgments

We thank other members of the collaborative team at the Polymath REU program for productive discussions and useful comments. We would like to thank our colleagues at the Young Mathematicians Conference in August 2020 for useful comments. We would also like to extend our gratitude to the editor and referees from the *Journal of Integer Sequences* for careful reading and comments on the manuscript.

## References

- [1] P. Bernays, *Über die Darstellung von positiven, ganzen Zahlen durch die primitiven binären quadratischen Formen einer nichtquadratischen Diskriminante*, Ph.D. dissertation, University of Göttingen, 1912.
- [2] T. J. Dekker, Prime numbers in quadratic fields, *CWI Quart.* **7** (1994), 367–394.
- [3] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, 1994.
- [4] E. Gethner and H. M. Stark, Periodic Gaussian moats, *Exp. Math.* **6** (1997), 289–292.
- [5] E. Gethner, S. Wagon, and B. Wick, A stroll through the Gaussian primes, *Amer. Math. Monthly* **105** (1998), 327–337.
- [6] G. H. Hardy, *Ramanujan: Twelve Lectures on Subjects Suggested by His Life and Work*, Amer. Math. Soc., 1999.
- [7] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., Oxford University Press, 2008.
- [8] J. H. Jordan and J. R. Rabung, A conjecture of Paul Erdős concerning Gaussian primes, *Math. Comp.* **24** (1970), 221–223.
- [9] P. Loh, Stepping to infinity along Gaussian primes, *Amer. Math. Monthly* **114** (2007), 142–151.
- [10] J. Neukirch, *Algebraic Number Theory*, Springer Science & Business Media, 2013.
- [11] D. Shanks and L. P. Schmid, Variations on a theorem of Landau, Part I, *Math. Comp.* **20** (1996), 551–569.
- [12] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2005.
- [13] N. Tsuchimura, Computational results for Gaussian moat problem, *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **88** (2005), 1267–1273.

---

2010 *Mathematics Subject Classification*: Primary 11A41; Secondary 11B05.

*Keywords*: walking to infinity, prime walk,  $\mathbb{Z}[\sqrt{2}]$ , real quadratic integer ring.

---

Received November 21 2020; revised version received July 12 2021; July 23 2021; November 3 2021; January 27 2022. Published in *Journal of Integer Sequences*, June 22 2022.

---

Return to [Journal of Integer Sequences home page](#).