involve
a journal of mathematics

On the distribution of
the greatest common divisor of Gaussian integers

Tai-Danae Bradley, Yin Choi Cheng and Yan Fei Luo

msp

2016 vol. 9, no. 1

INVOLVE 9:1 (2016)
dx.doi.org/10.2140/involve.2016.9.27

On the distribution of the greatest common divisor of Gaussian integers

Tai-Danae Bradley, Yin Choi Cheng and Yan Fei Luo

(Communicated by Kenneth S. Berenhaut)

For a pair of random Gaussian integers chosen uniformly and independently from the set of Gaussian integers of norm x or less as x goes to infinity, we find asymptotics for the average norm of their greatest common divisor, with explicit error terms. We also present results for higher moments along with computational data which support the results for the second, third, fourth, and fifth moments. The analogous question for integers is studied by Diaconis and Erdős.

1. Introduction

In this paper, we study questions related to the size of the greatest common divisor of pairs of randomly chosen Gaussian integers. In particular, in Theorem 1, we first calculate the probability that a pair of random Gaussian integers, chosen uniformly and independently from the set of all Gaussian integers with norm x or less, has greatest common divisor $\pm\kappa$ or $\pm i\kappa$ for a fixed Gaussian integer κ. The main term for this probability in the case where $\kappa=1$ was first given by Collins and Johnson [1989, Theorem 8]. We refine their results by providing the expression for the more general case in addition to giving an explicit error term for all cases. In Theorem 2 we derive the expected norm of the greatest common divisor between a pair of Gaussian integers with norm x or less. Finally, in Theorem 3 and Conjecture 4, we present an expression for higher moments of the norm of the greatest common divisor between a pair of Gaussian integers with norm x or less. We expect our results to generalize to principal ideal domains without too much difficulty. More generally, our results should hold for the ring of integers in an algebraic number field, though our techniques will need to be modified to deal with class number greater than one and infinite unit group. We expect the ideas in [Micheli and Ferraguti 2015] could help address this question and would be an interesting direction to explore further. Of further interest are function field analogues. Some interesting results in this direction may be found in [Micheli and Schnyder 2015].

MSC2010: 11N37, 11A05, 11K65, 60E05.
Keywords: Gaussian integer, gcd, moment, Dedekind zeta function.

Similar questions have also been studied for the case of rational integers. Originally, Mertens [1874] proved that the probability that a pair of rational integers chosen uniformly and independently at random from $\{1, 2, \dots, x\}$ are relatively prime is asymptotic to $1/\zeta(2)$, as x tends to infinity, where ζ is the Riemann zeta function. Christopher [1956, Theorem 1] generalized Mertens' result by finding the probability that two integers have greatest common divisor k for a fixed k larger than 1. An asymptotic expression for the moments of the greatest common divisor was first derived by Cesàro [1885], and Diaconis and Erdős [2004, Theorem 2] later extended his work by explicitly calculating the error term. In particular, the expected value for the greatest common divisor between a pair of random integers chosen independently and uniformly from the set $\{1, 2, \dots, x\}$ is

$$\frac{1}{\zeta(2)} \log x + O(1), \tag{1}$$

while the n-th moment is given by

$$\frac{x^{n-1}}{n+1}\left(\frac{2\zeta(n)}{\zeta(n+1)} - 1\right) + O(x^{n-2}\log x) \quad \text{for } n \geq 2. \tag{2}$$

The goal of the present paper is to show that (1) has an analogous counterpart in the ring of Gaussian integers as stated in Theorem 2 at the end of this section. Further, we show that (2) also has an analogous form as presented in Theorem 3 and Conjecture 4. Before proceeding, we first give the following preliminary definitions and remark.

Definition. The norm of a Gaussian integer $\alpha = a + bi$ for rational integers a and b is defined by $N(\alpha) = a^2 + b^2$.

Most of our results will be in terms of the norms of Gaussian integers and not the integers themselves.

Remark. Given two Gaussian integers η and μ, a greatest common divisor, denoted (η, μ), is defined to be a Gaussian integer κ such that κ is a divisor of both η and μ, and if there is any other common factor between η and μ, then it must also be a factor of κ. From this definition, it becomes clear that (η, μ) is unique only up to its associates. In other words, $(\eta, \mu) = \kappa, -\kappa, i\kappa$, and $-i\kappa$. Our calculations, however, will be performed via ideals for reasons that will soon become apparent. For a Gaussian integer η, we say $\mathfrak{n}$ is the ideal such that

$$\mathfrak{n} = (\eta) = (-\eta) = (i\eta) = (-i\eta),$$

and the norm of $\mathfrak{n}$ is defined by $N(\mathfrak{n}) = N(\eta)$. Accordingly, the definition of the greatest common divisor for a pair of ideals is this:

Definition (greatest common divisor of two ideals). For a ring R, let $\mathfrak{n}$, $\mathfrak{m} \subset R$ be ideals. The greatest common divisor $(\mathfrak{n}, \mathfrak{m})$ is defined to be the ideal $\mathfrak{K} \subset R$ which satisfies the following:

(1) $\mathfrak{n} \subset \mathfrak{K}$ and $\mathfrak{m} \subset \mathfrak{K}$.

(2) If there exists some ideal $\mathfrak{a} \subset R$ such that $\mathfrak{n} \subset \mathfrak{a}$ and $\mathfrak{m} \subset \mathfrak{a}$, then $\mathfrak{K} \subset \mathfrak{a}$.

In other words, $(\mathfrak{n}, \mathfrak{m})$ is the smallest ideal that contains all the elements of both $\mathfrak{n}$ and $\mathfrak{m}$. When applied to the ring of Gaussian integers, a Dedekind domain, it is clear that $(\mathfrak{n}, \mathfrak{m})$ is unique.

Definition (the Dedekind zeta function of $\mathbb{Q}(i)$). For the number field $\mathbb{Q}(i)$, the complex-valued Dedekind zeta function is defined for $\operatorname{Re}(s) > 1$ by

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{\mathfrak{a} \subset \mathbb{Z}[i]} \frac{1}{N(\mathfrak{a})^s} = \frac{1}{4} \sum_{\substack{(a,b) \in \mathbb{Z} \\ (a,b) \neq (0,0)}} \frac{1}{(a^2+b^2)^s},$$

where the first summation is over the nonzero ideals $\mathfrak{a}$ of the ring of Gaussian integers $\mathbb{Z}[i]$.

In order to find the expression for the expected norm of a greatest common divisor between a pair of Gaussian integers of norm x or less, we will first derive the necessary probability distribution function of Theorem 1:

Theorem 1. *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[i]$ with norm x or less. The probability that $(\mathfrak{n}, \mathfrak{m}) = \mathfrak{K}$ is*

$$\frac{1}{\zeta_{\mathbb{Q}(i)}(2) N(\mathfrak{K})^2} + O\left(\frac{1}{x^{2/3} N(\mathfrak{K})^{4/3}}\right).$$

This probability will allow us to calculate the expected norm of the greatest common divisor between a pair of ideals:

Theorem 2. *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[i]$ with norm x or less. The expected norm of the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ is*

$$\frac{\pi}{4\zeta_{\mathbb{Q}(i)}(2)} \log x + O(1).$$

We will then prove the following result regarding the n-th moment for $n > 2$:

Theorem 3. *Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals chosen independently and uniformly at random from the set of ideals in $\mathbb{Z}[i]$ with norm x or less. For $n > 2$, there exists a constant $c_n \in \mathbb{R}$ such that*

$$E_x\{N(\mathfrak{n}, \mathfrak{m})^n\} \sim c_n x^{n-1},$$

where $E_x\{N(\mathfrak{n}, \mathfrak{m})^n\}$ denotes the n-th moment of the norm of the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$.

Lastly, we will present numerical data which provide strong evidence for the following conjecture regarding the constant of Theorem 3 for all $n \geq 2$:

Conjecture 4. *For* $n \geq 2$,

$$E_x\{N(\mathfrak{n}, \mathfrak{m})^n\} \sim \frac{4}{\pi(n+1)}\left(\frac{2\zeta_{\mathbb{Q}(i)}(n)}{\zeta_{\mathbb{Q}(i)}(n+1)} - 1\right)x^{n-1}.$$

The proof of Theorem 1 will be given in Section 2 and that of Theorem 2 will be given in Section 3. Finally, in Section 4, we prove Theorem 3 and present Conjecture 4 along with computational data which support the conjecture for the second, third, fourth, and fifth moments.

2. Probability distribution function

Before deriving the expression for the probability of Theorem 1, we first define the following two functions:

Definition (the Möbius function). For an ideal $\mathfrak{n}$, the Möbius Function $\mu(\mathfrak{n})$ is defined by

$$\mu(\mathfrak{n}) = \begin{cases} 1 & \text{if } \mathfrak{n} = (1), \\ (-1)^t & \text{if } \mathfrak{n} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t \text{ for distinct prime ideals } \mathfrak{p}_i, \\ 0 & \text{otherwise.} \end{cases}$$

We will use the following identity

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu(\mathfrak{d}) = \begin{cases} 1 & \text{if } \mathfrak{n} = (1), \\ 0 & \text{if } \mathfrak{n} \neq (1), \end{cases} \tag{3}$$

as well as the generating function

$$\sum_{\mathfrak{n}\subset\mathbb{Z}[i]} \frac{\mu(\mathfrak{n})}{N(\mathfrak{n})^s} = \frac{1}{\zeta_{\mathbb{Q}(i)}(s)} \quad \text{for } \operatorname{Re}(s) > 1.$$

Definition (the sum-of-two-squares function). For $n \in \mathbb{Z}$, let the sum-of-two-squares function $r(n, 2)$ represent the number of ways that n can be expressed as a sum of two squares. Thus,

$$r(n, 2) = \tfrac{1}{4}\#\{\mathfrak{a} \subset \mathbb{Z}[i] : N(\mathfrak{a}) = n\}.$$

We will need the result of Sierpiński [1906] (for a statement in English, see [Schinzel 1972, (1)])

$$\sum_{n=1}^{x} r(n, 2) = \pi x + O(x^{1/3}). \tag{4}$$

The error term $O(x^{1/3})$ has been improved by Huxley [2003] to $O(x^{131/416+\epsilon})$, but the former is sufficient for our purposes. We shall also use

$$\sum_{n=1}^{x} \frac{r(n,2)}{n} = \pi(S + \log x) + O(x^{-1/2}) \tag{5}$$

[Sierpiński 1907], where S denotes Sierpiński's constant $S \approx 2.58/\pi$. This also has the alternate expressions

$$S = \frac{1}{\pi} \lim_{z\to\infty}\left(4\zeta(z)\beta(z) - \frac{\pi}{z-1}\right) = \gamma + \frac{\beta'(1)}{\beta(1)}$$

[Finch 2003, p. 123], where $\beta(z)$ is the Dirichlet beta function and γ is the Euler–Mascheroni constant.

With these functions at hand, we may now proceed to calculate the desired probability. To do so, we will need two preliminary results. The first is the total number of pairs of ideals generated by Gaussian integers with norm at most x. The second result is the number of those pairs which have greatest common divisor $\mathfrak{K}$. The expressions for each of these are derived in the following two lemmas.

Lemma 5. *The total number of pairs of nonzero ideals* $\mathfrak{n}$ *and* $\mathfrak{m}$ *in* $\mathbb{Z}[i]$ *with norm* x *or less is*

$$\frac{\pi^2x^2}{16} + O(x^{4/3}).$$

Proof. Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals. Then

$$\#\left\{\mathfrak{n},\mathfrak{m} \subset \mathbb{Z}[i]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \le x\right\} = \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[i]\\ N(\mathfrak{n})\le x}} \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[i]\\ N(\mathfrak{m})\le x}} 1,$$

and we may rewrite this as

$$\frac{1}{16} \sum_{N(\mathfrak{n})=1}^{\lfloor x\rfloor} r(N(\mathfrak{n}),2) \sum_{N(\mathfrak{m})=1}^{\lfloor x\rfloor} r(N(\mathfrak{m}),2),$$

which by (4) equals

$$\tfrac{1}{16}(\pi x + O(\lfloor x\rfloor^{1/3}))^2.$$

Further, since $O(\lfloor x\rfloor) = O(x)$, we may expand $(\pi x + O(x^{1/3}))^2$ and obtain $\pi^2x^2 + 2\pi x\, O(x^{1/3}) + O(x^{2/3})$, which reduces to $\pi^2x^2 + O(x^{4/3})$. Thus, the total number of $\mathfrak{n}$ and $\mathfrak{m}$ with norm at most x is

$$\frac{\pi^2x^2}{16} + O(x^{4/3}). \qquad \square$$

Lemma 6. *The total number of pairs of nonzero ideals $\mathfrak{n}$ and $\mathfrak{m}$ in $\mathbb{Z}[i]$ with norm x or less having greatest common divisor $\mathfrak{K}$ is*

$$\frac{\pi^2 x^2}{16\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{x^{4/3}}{k^{4/3}}\right),$$

where $k = N(\mathfrak{K})$.

Proof. Let $\mathfrak{n}$ and $\mathfrak{m}$ be nonzero ideals. The number of pairs of $\mathfrak{n}$ and $\mathfrak{m}$ with norm x or less which are relatively prime is

$$\begin{aligned}\#\big\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[i]^2 : N(\mathfrak{n}), N(\mathfrak{m})\le x \text{ and } (\mathfrak{n},\mathfrak{m})=(1)\big\} &= \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[i]\\ N(\mathfrak{n})\le x}}\ \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[i]\\ N(\mathfrak{m})\le x\\ (\mathfrak{n},\mathfrak{m})=(1)}} 1\\ &= \sum_{\substack{\mathfrak{n}\subset\mathbb{Z}[i]\\ N(\mathfrak{n})\le x}}\ \sum_{\substack{\mathfrak{m}\subset\mathbb{Z}[i]\\ N(\mathfrak{m})\le x}}\ \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ \mathfrak{d}\mid(\mathfrak{n},\mathfrak{m})}} \mu(\mathfrak{d}),\end{aligned}$$

where in the last line we used identity (3). Reindexing with $\mathfrak{n} = \mathfrak{d}\mathfrak{n}'$ and $\mathfrak{m} = \mathfrak{d}\mathfrak{m}'$, where the norms of $\mathfrak{n}'$ and $\mathfrak{m}'$ range from 1 to $x/N(\mathfrak{d})$, we may rewrite this as

$$\begin{aligned}&\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \mu(\mathfrak{d}) \sum_{\substack{\mathfrak{n}'\subset\mathbb{Z}[i]\\ N(\mathfrak{n}')\le x/N(\mathfrak{d})}}\ \sum_{\substack{\mathfrak{m}'\subset\mathbb{Z}[i]\\ N(\mathfrak{m}')\le x/N(\mathfrak{d})}} 1\\ &\qquad= \frac{1}{16}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \mu(\mathfrak{d}) \sum_{N\mathfrak{n}'=1}^{\lfloor x/N\mathfrak{d}\rfloor} r(N(\mathfrak{n}'),2) \sum_{N\mathfrak{m}'=1}^{\lfloor x/N\mathfrak{d}\rfloor} r(N(\mathfrak{m}'),2).\end{aligned}$$

As in Lemma 5, this reduces to

$$\frac{1}{16}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \mu(\mathfrak{d})\left(\frac{\pi^2x^2}{N(\mathfrak{d})^2} + O\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right).$$

We then distribute the summation to obtain

$$\frac{\pi^2x^2}{16}\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} + O\left(\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}}\left(\frac{x}{N(\mathfrak{d})}\right)^{4/3}\right). \tag{6}$$

To evaluate the main term, we call on the generating function $\sum_{\mathfrak{n}\subset\mathbb{Z}[i]} \mu(\mathfrak{n})/N(\mathfrak{n})^s = 1/\zeta_{\mathbb{Q}(i)}(s)$ for $\mathrm{Re}(s) > 1$ to see that

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(i)}(2)} - \sum_{n=x+1}^{\infty}\ \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})=n}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2},$$

which implies

$$\left|\frac{1}{\zeta_{\mathbb{Q}(i)}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\right| \le \sum_{n=x+1}^{\infty} \frac{1}{n^2} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})=n}} 1 = \frac{1}{4}\sum_{n=x+1}^{\infty} \frac{r(n,2)}{n^2}.$$

Now we note that $r(n,2) \le 4\sigma_0(n) = o(n^{\epsilon})$ for all $\epsilon > 0$, where σ_0 represents the number of divisors of n. Thus

$$\frac{1}{4}\sum_{n=x+1}^{\infty} \frac{r(n,2)}{n^2} \le \sum_{n=x+1}^{\infty} \frac{o(n^{\epsilon})}{n^2} = o(x^{\epsilon-1}),$$

and so

$$\left|\frac{1}{\zeta_{\mathbb{Q}(i)}(2)} - \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2}\right| \le o(x^{\epsilon-1}) \quad \text{or} \quad \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \frac{\mu(\mathfrak{d})}{N(\mathfrak{d})^2} = \frac{1}{\zeta_{\mathbb{Q}(i)}(2)} + o(x^{\epsilon-1}).$$

For the error term of (6), we have

$$\sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})\le x}} \left(\frac{1}{N(\mathfrak{d})}\right)^{4/3} = \sum_{n=1}^{x} \frac{1}{n^{4/3}} \sum_{\substack{\mathfrak{d}\subset\mathbb{Z}[i]\\ N(\mathfrak{d})=n}} 1 = \frac{1}{4}\sum_{n=1}^{x} \frac{r(n,2)}{n^{4/3}}$$

and again use the bound $r(n,2) \le o(n^{\epsilon})$ to see that

$$\frac{1}{4}\sum_{n=1}^{x} \frac{r(n,2)}{n^{4/3}} \le \sum_{n=1}^{x} o(n^{\epsilon-4/3}),$$

which equals $o(x^{\epsilon-1/3}) + o(1)$. From this it is clear that

$$O\left(x^{4/3}\sum_{n=1}^{x} \frac{r(n,2)}{n^{4/3}}\right) = O(o(x^{4/3})) = O(x^{4/3}).$$

Thus (6) becomes

$$\frac{\pi^2 x^2}{16\zeta_{\mathbb{Q}(i)}(2)} + o(x^{\epsilon-1}) + O(x^{4/3}),$$

which allows us to conclude

$$\#\left\{\mathfrak{n},\mathfrak{m}\subset\mathbb{Z}[i]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \le x \text{ and } (\mathfrak{n},\mathfrak{m}) = (1)\right\} = \frac{\pi^2 x^2}{16\zeta_{\mathbb{Q}(i)}(2)} + O(x^{4/3}).$$

Having counted the number of relatively prime $\mathfrak{n}$ and $\mathfrak{m}$ within a given norm, we can now reindex to obtain the number of them which have $(\mathfrak{n},\mathfrak{m}) = \mathfrak{K}$. Letting $\mathfrak{n} = \mathfrak{n}'\mathfrak{K}$ and $\mathfrak{m} = \mathfrak{m}'\mathfrak{K}$, we see that $\mathfrak{n}'$ and $\mathfrak{m}'$ are relatively prime if and only if $\mathfrak{n}$ and $\mathfrak{m}$ have $\mathfrak{K}$ as their greatest common divisor. Hence, the number of relatively prime pairs $\mathfrak{n}'$ and $\mathfrak{m}'$ with norm y or less must be equivalent to the number of pairs $\mathfrak{n}$ and $\mathfrak{m}$

with norm yk or less (where $k = N(\mathfrak{K})$) having greatest common divisor $\mathfrak{K}$. Thus,

$$\begin{aligned}\#\{\mathfrak{n}, \mathfrak{m} \subset \mathbb{Z}[i]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \le x \text{ and } (\mathfrak{n}, \mathfrak{m}) = \mathfrak{K}\} \\ &= \#\{\mathfrak{n}', \mathfrak{m}' \subset \mathbb{Z}[i]^2 : N(\mathfrak{n}'), N(\mathfrak{m}') \le x/k \text{ and } (\mathfrak{n}', \mathfrak{m}') = (1)\} \\ &= \frac{\pi^2 x^2}{16\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{x^{4/3}}{k^{4/3}}\right), \qquad \square\end{aligned}$$

Lastly, the probability that $\mathfrak{n}$ and $\mathfrak{m}$, having norm at most x, will have greatest common divisor $\mathfrak{K}$ is defined to be the number of pairs of ideals of norm x or less which have greatest common divisor $\mathfrak{K}$ divided by the total number of pairs of ideals of norm x or less. Thus, by Lemmas 5 and 6,

$$\begin{aligned}P_x\{\mathfrak{n}, \mathfrak{m} \subset \mathbb{Z}[i]^2 : N(\mathfrak{n}), N(\mathfrak{m}) \le x \text{ and } (\mathfrak{n}, \mathfrak{m}) = \mathfrak{K}\} \\ &= \left(\frac{\pi^2 x^2}{16} + O(x^{4/3})\right)^{-1}\left(\frac{\pi^2 x^2}{16\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{x^{4/3}}{k^{4/3}}\right)\right). \qquad (7)\end{aligned}$$

We can rewrite $(\pi^2 x^2/16 + O(x^{4/3}))^{-1}$ as $16\pi^{-2}x^{-2}(1 + O(x^{-2/3}))^{-1}$, which is equal to $16\pi^{-2}x^{-2}(1 + O(x^{-2/3}))$ since $(1 + f(x))^{-1} = 1 + O(f(x))$ for $f(x)$ tending towards 0 as x approaches infinity.

Line (7) then becomes

$$\begin{aligned}\pi^{-2}x^{-2}(1 + O(x^{-2/3}))\left(\frac{\pi^2 x^2}{\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{x^{4/3}}{k^{4/3}}\right)\right) \\ &= (1 + O(x^{-2/3}))\left(\frac{1}{\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{1}{x^{2/3}k^{4/3}}\right)\right) \\ &= \frac{1}{\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{1}{x^{2/3}k^{4/3}}\right) + O\left(\frac{1}{x^{2/3}k^{2}}\right) + O\left(\frac{1}{x^{4/3}k^{4/3}}\right),\end{aligned}$$

or finally

$$\frac{1}{\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{1}{x^{2/3}k^{4/3}}\right),$$

completing the proof of Theorem 1. The following corollary is a direct consequence of Theorem 1 for the special case when $\mathfrak{K} = (1)$.

Corollary 7. *The probability that a pair of Gaussian integers with norm x or less are relatively prime is*

$$\frac{1}{\zeta_{\mathbb{Q}(i)}(2)} + O\left(\frac{1}{x^{2/3}}\right).$$

In effect, Corollary 7 tells us that for x large, the probability that two Gaussian integers are relatively prime is asymptotic to $(\zeta_{\mathbb{Q}(i)}(2))^{-1}$ as x tends towards infinity. This is in agreement with the work of Collins and Johnson who state the probability as $(\zeta_{\mathbb{Q}(i)}(2))^{-1} = (\zeta(2)L(2, \chi))^{-1} \approx 0.6637$, where $L(2, \chi)$ is a Dirichlet L-series and χ the primitive Dirichlet character modulo 4.

3. Expected value

Having derived the probability distribution function found in Theorem 1, we are ready to find an expression for the expected value of our random variable, $N(\mathfrak{n}, \mathfrak{m}) = k$, where the norm of $\mathfrak{n}$ and $\mathfrak{m}$ ranges from 1 to x. To do this, we must express our probability in terms of k as well. The modification is simple, however. Since the number of ideals with norm k is equivalent to $r(k, 2)/4$, the probability that the greatest common divisor of $\mathfrak{n}$ and $\mathfrak{m}$ has norm k must be

$$P_x\{N(\mathfrak{n}, \mathfrak{m}) = k\} = \frac{r(k, 2)}{4\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{r(k, 2)}{x^{2/3}k^{4/3}}\right).$$

Then, by definition of expected value

$$\begin{aligned} E_x\{N(\mathfrak{n}, \mathfrak{m})\} &= \sum_{k=1}^{x} k P_x\{N(\mathfrak{n}, \mathfrak{m}) = k\} \\ &= \sum_{k=1}^{x} k\left(\frac{r(k, 2)}{4\zeta_{\mathbb{Q}(i)}(2)k^2} + O\left(\frac{r(k, 2)}{x^{2/3}k^{4/3}}\right)\right) \\ &= \frac{1}{4\zeta_{\mathbb{Q}(i)}(2)} \sum_{k=1}^{x} \frac{r(k, 2)}{k} + O\left(\frac{1}{x^{2/3}} \sum_{k=1}^{x} \frac{r(k, 2)}{k^{1/3}}\right). \end{aligned} \tag{8}$$

Using Stieltjes integration by parts to evaluate the error term, we obtain

$$\begin{aligned} \sum_{k=1}^{x} \frac{r(k, 2)}{k^{1/3}} &= x^{-1/3} \sum_{k=1}^{x} r(k, 2) - 4 - \int_1^x (\pi k + O(k^{1/3}))\left(-\tfrac{1}{3}k^{-4/3}\right) dk \\ &= \frac{3\pi}{2} x^{2/3} + O(\log x), \end{aligned}$$

which implies

$$O\left(x^{-2/3} \sum_{k=1}^{x} \frac{r(k, 2)}{k^{1/3}}\right) = O(1 + x^{-2/3} \log x) = O(1).$$

The main term of (8) can be rewritten using Sierpiński's identity from (5). Thus the expected value is equal to

$$\frac{1}{4\zeta_{\mathbb{Q}(i)}(2)}\left(\pi(S + \log x) + O\left(\frac{1}{x^{1/2}}\right)\right) + O(1)$$

or

$$\frac{\pi}{4\zeta_{\mathbb{Q}(i)}(2)} \log x + O(1).$$

This completes the proof of Theorem 2.

4. Higher moments

Finally, we show that there exists some constant $c_n \in \mathbb{R}$ such that the main term of the n-th moment of $N(\mathfrak{n}, \mathfrak{m})$ must be of the form $c_n x^{n-1}$ for $n > 2$. Let $N(\mathfrak{n}), N(\mathfrak{m}) \leq x$ with $(\mathfrak{n}, \mathfrak{m}) = \mathfrak{K}$ and restrict $N(\mathfrak{K})$ to the interval $\big(x/(j+1), x/j\big]$. We may then write $\mathfrak{n} = \mathfrak{n}'\mathfrak{K}$ and $\mathfrak{m} = \mathfrak{m}'\mathfrak{K}$, where $(\mathfrak{n}', \mathfrak{m}') = (1)$. The restriction on the norm of $\mathfrak{K}$ allows us to see that $N(\mathfrak{n}'), N(\mathfrak{m}') < x(j+1)/x$, which implies $N(\mathfrak{n}'), N(\mathfrak{m}') \leq j$. Now define

$$f(j) = \#\big\{(\mathfrak{n}', \mathfrak{m}') \subset \mathbb{Z}[i]^2 : N(\mathfrak{n}'), N(\mathfrak{m}') \leq j \text{ and } (\mathfrak{n}', \mathfrak{m}') = (1)\big\}$$

for $j \in \mathbb{N}$. By Lemma 6,

$$\begin{aligned} f(j) &= \frac{\pi^2 j^2}{16\zeta_{\mathbb{Q}(i)}(2)} + O(j^{4/3}) \\ &= O(j^2). \end{aligned}$$

Our reindexing above shows that this expression for $f(j)$ also gives us the number of pairs of ideals with norm x or less having greatest common divisor $\mathfrak{K}$, where $x/(j+1) < N(\mathfrak{K}) \leq x/j$. Thus the n-th moment of $N(\mathfrak{n}, \mathfrak{m})$ is given by

$$E_x\{N(\mathfrak{n}, \mathfrak{m})^n\} = \frac{1}{\pi^2 x^2/16 + O(x^{4/3})} \Bigg(\sum_{j=1}^{x} f(j) \sum_{\substack{\mathfrak{K} \subset \mathbb{Z}[i] \\ x/(j+1) < N(\mathfrak{K}) \leq x/j}} N(\mathfrak{K})^n \Bigg). \tag{9}$$

We next turn our attention to the inner sum of (9). First note that

$$\sum_{\substack{\mathfrak{K} \subset \mathbb{Z}[i] \\ x/(j+1) < N(\mathfrak{K}) \leq x/j}} N(\mathfrak{K})^n = \frac{1}{4} \sum_{k=\lceil x/(j+1) \rceil}^{\lfloor x/j \rfloor} k^n r(k, 2),$$

where $k = N(\mathfrak{K})$. Then Stieltjes integration by parts yields

$$\begin{aligned} \frac{1}{4} \sum_{k=\lceil x/(j+1) \rceil}^{\lfloor x/j \rfloor} k^n r(k,2) &= \left\lfloor \frac{x}{j} \right\rfloor^n \sum_{k=1}^{\lfloor x/j \rfloor} r(k,2) - \left\lceil \frac{x}{j+1} \right\rceil^n \sum_{k=1}^{\lceil x/(j+1) \rceil} r(k,2) \\ &\qquad - \int_{\lceil x/(j+1) \rceil}^{\lfloor x/j \rfloor} n t^{n-1} (\pi t + O(t^{1/3}))\, dt \\ &= \frac{\pi}{4(n+1)} x^{n+1} \left(\frac{1}{j^{n+1}} - \frac{1}{(j+1)^{n+1}} \right) + O\left(\frac{x}{j} \right)^{n+1/3}. \end{aligned}$$

The numerator of $E_x\{N(\mathfrak{n}, \mathfrak{m})^n\}$ is now equal to

$$\frac{\pi}{4(n+1)} x^{n+1} \sum_{j=1}^{x} O(j^2) \left(\frac{(j+1)^{n+1} - j^{n+1}}{j^{n+1}(j+1)^{n+1}} \right) + x^{n+1/3} \sum_{j=1}^{x} O(j^2) O\left(\frac{1}{j^{n+1/3}} \right). \tag{10}$$

The sum on the left is

$$\sum_{j=1}^{x} O(j^2) O\left(\frac{1}{j(j+1)^{n+1}}\right) = \sum_{j=1}^{x} O\left(\frac{1}{j^{-1}(j+1)^{n+1}}\right),$$

which is bounded above by $\sum_{j=1}^{x} O(1/j^n)$. For x tending toward infinity and $n \geq 2$, this converges to some constant $c'_n \in \mathbb{R}$. A similar argument shows that the second sum of (10) is likewise convergent for $n > 2$. We thus conclude that the main term of $E_x\{N(\mathfrak{n}, \mathfrak{m})^n\}$ is of the form $c'_n x^{n+1}$.

Finally, we divide this by the total number of pairs of ideals $\mathfrak{n}$, $\mathfrak{m}$ with norm at most x to obtain the main term of the n-th moment of $N(\mathfrak{n}, \mathfrak{m})$ for $n > 2$

$$\frac{c'_n x^{n+1}}{\pi^2 x^2/16 + O(x^{4/3})} = c_n x^{n-1} \frac{1}{1 + O(x^{-2/3})},$$

where $c_n = 16c'_n/\pi^2$. Since

$$(1 + O(x^{-2/3}))^{-1} = 1 + O(x^{-2/3}),$$

it follows that for x tending to infinity

$$E_x\{N(\mathfrak{n}, \mathfrak{m})^n\} \sim c_n x^{n-1}.$$

With this, we bring the proof of Theorem 3 to an end and close by restating our conjecture regarding the constant of $E_x\{N(\mathfrak{n}, \mathfrak{m})^n\}$ for all $n \geq 2$. We also include numerical evidence below which provides support for the conjecture in the cases when $n = 2, 3, 4$ and 5.

Conjecture 4. *For $n \geq 2$,*

$$E_x\{N(\mathfrak{n}, \mathfrak{m})^n\} \sim \frac{4}{\pi(n+1)} \left(\frac{2\zeta_{\mathbb{Q}(i)}(n)}{\zeta_{\mathbb{Q}(i)}(n+1)} - 1\right) x^{n-1}.$$

Using Matlab, we first compiled a list of all pairs of Gaussian integers in the first quadrant with norm x or less and used the Euclidean algorithm to find all possible greatest common divisors. We determined the n-th moment by raising the norm of each greatest common divisor to the n-th power, summed the terms together, and then divided the result by the total number of pairs of Gaussian integers in the first quadrant with norm x or less. We have graphed the results in Figures 1–4 below for the cases when $n = 2, 3, 4$ and 5 with $x = 50,000$. In Table 1, we have listed the main term of the best fit curve corresponding to each graph as compared against the conjectured main term for each value of n.

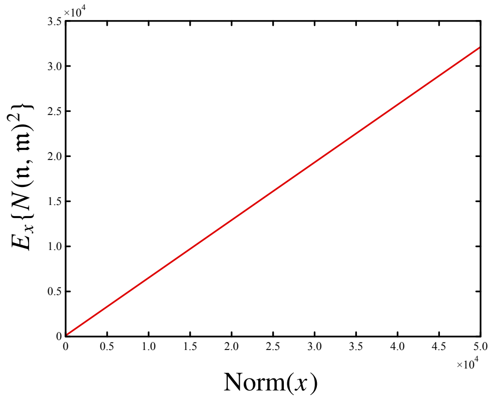

Figure 1. The graph of $E_x\{N(\mathfrak{n}, \mathfrak{m})^2\}$ for $1 \leq x \leq 50,000$. The best fit curve is $0.63952x + 0.5753$.

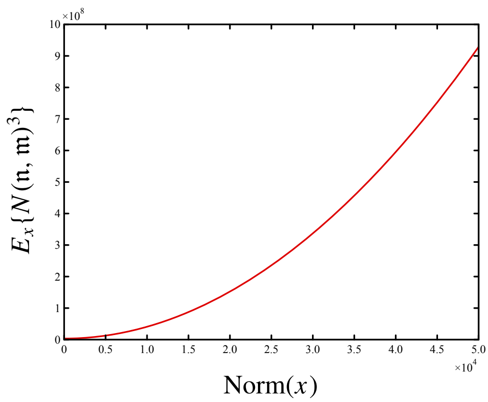

Figure 2. The graph of $E_x\{N(\mathfrak{n}, \mathfrak{m})^3\}$ for $1 \leq x \leq 50,000$. The best fit curve is $0.37018x^2 + 0.69337x - 584.8498$.

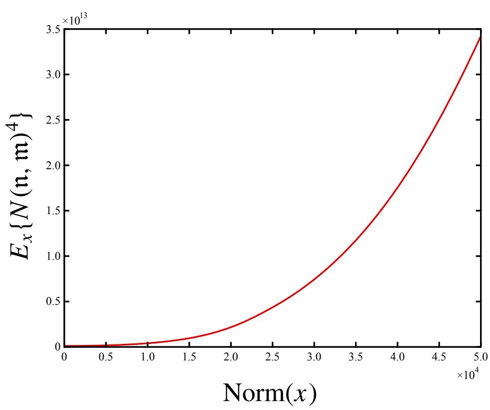

Figure 3. The graph of $E_x\{N(\mathfrak{n}, \mathfrak{m})^4\}$ for $1 \leq x \leq 50,000$. The best fit curve is $0.27238x^3 + 0.80149x^2 - 3723.1433x + 12324561.4508$.

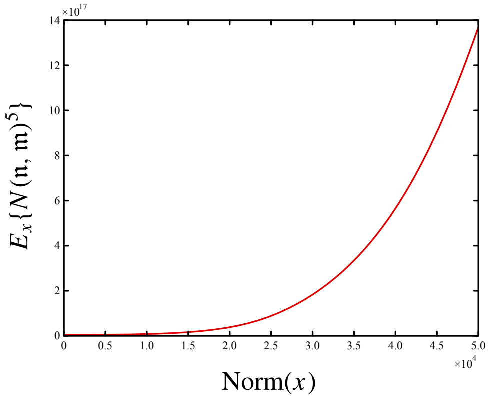

Figure 4. The graph of $E_x\{N(\mathfrak{n}, \mathfrak{m})^5\}$ for $1 \leq x \leq 50,000$. The best fit curve is $0.21914x^4 + 0.92436x^3 - 9773.8223x^2 + 92150266.2382x - 190551355734.3794$.

moment (n)	numerically derived term	conjectured term
2	$0.63952x$	$0.67364x$
3	$0.37018x^2$	$0.37444x^2$
4	$0.27238x^3$	$0.27309x^3$
5	$0.21914x^4$	$0.21928x^4$

Table 1. The main term of the n-th moment of the norm of the greatest common divisor of pairs of Gaussian integers with norm at most x.

Acknowledgements

The authors were supported by the Rich Summer Internship grant of the Dr. Barnett and Jean Hollander Rich Scholarship Fund and would like to thank both the selection committee and donors. For additional funding, the first author was supported by the NIH Maximizing Access to Research Careers (MARC) U-STAR grant [5T34 GM007639], the second author by the National Science Foundation [DMS-1201446] and the third author by the City College Fellowships Program. Gratitude also goes to Joseph Dacanay whose help with Matlab laid the groundwork for our experimental data. We thank Giacomo Micheli for making us aware of his work and for his comments on our paper. The authors are also grateful to the referee for helpful comments regarding the statement and proof of Theorem 3. We especially thank our advisor, Dr. Brooke Feigon, without whose patient instruction and insightful comments this work would not have been possible.

References

[Cesàro 1885] E. Cesàro, "Étude moyenne du plus grand commun diviseur de deux nombres", *Ann. Mat. Pura Appl.* **13**:2 (1885), 233–268. Zbl 17.0144.05

[Christopher 1956] J. Christopher, "The asymptotic density of some k-dimensional sets", *Amer. Math. Monthly* **63** (1956), 399–401. MR 20 #3832 Zbl 0070.04101

[Collins and Johnson 1989] G. E. Collins and J. R. Johnson, "The probability of relative primality of Gaussian integers", pp. 252–258 in *Symbolic and algebraic computation* (Rome, 1988), edited by P. Gianni, Lecture Notes in Comput. Sci. **358**, Springer, Berlin, 1989. MR 90m:11165

[Diaconis and Erdős 2004] P. Diaconis and P. Erdős, "On the distribution of the greatest common divisor", pp. 56–61 in *A festschrift for Herman Rubin*, edited by A. DasGupta, IMS Lecture Notes Monogr. Ser. **45**, Inst. Math. Statist., Beachwood, OH, 2004. MR 2005m:60011 Zbl 1268.11139

[Finch 2003] S. R. Finch, *Mathematical constants*, Encyclopedia of Mathematics and its Applications **94**, Cambridge University Press, 2003. MR 2004i:00001 Zbl 1054.00001

[Huxley 2003] M. N. Huxley, "Exponential sums and lattice points, III", *Proc. London Math. Soc.* (3) **87**:3 (2003), 591–609. MR 2004m:11127 Zbl 1065.11079

[Mertens 1874] F. Mertens, "Ueber einige asymptotische Gesetze der Zahlentheorie", *J. Reine Angew. Math.* **77** (1874), 289–338. MR 1579608

[Micheli and Ferraguti 2015] G. Micheli and A. Ferraguti, "On Mertens–Cesáro theorem for number fields", preprint, 2015. To appear in *Bull. Aust. Math. Soc.* arXiv 1409.6527

[Micheli and Schnyder 2015] G. Micheli and R. Schnyder, "On the density of coprime m-tuples over holomorphy rings", *Int. J. Number Theory* (online publication September 2015).

[Schinzel 1972] A. Schinzel, "Wacław Sierpiński's papers on the theory of numbers", *Acta Arith.* **21** (1972), 7–13. (errata insert). MR 46 #9b Zbl 0243.01028

[Sierpiński 1906] W. Sierpiński, "O pewnem zagadnieniu z rachunku funkcyj asymptotycznych", *Prace Matematyczno-Fizyczne* **17** (1906), 77–118.

[Sierpiński 1907] W. Sierpiński, "O sumowaniu szeregu $\sum_{n>a}^{n\le b} \tau(n) f(n)$, gdzie $\tau(n)$ oznacza liczbę rozkładów liczby n na sumę kwadratów dwóch liczb całkowitych", *Prace Matematyczno-Fizyczne* **18** (1907), 1–59. JFM 38.0319.02

Received: 2013-03-27 Revised: 2015-01-09 Accepted: 2015-01-28

tai.danae@gmail.com *Department of Mathematics, The Graduate Center, CUNY, 365 5th Avenue, New York, NY 10016, United States*

cycsano@hotmail.com *Department of Mathematics, The Graduate Center, CUNY, 365 5th Avenue, New York, NY 10016, United States*

fay.or.flymorning@gmail.com *GACE Consulting Engineers PC, 105 Madison Avenue, 6th Floor, New York, NY 10016, United States*

involve

msp.org/involve

See inside back cover or msp.org/involve for submission instructions. The subscription price for 2016 is US $160/year for the electronic version, and $215/year (+$35, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to MSP.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840, is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW® from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

involve

2016 vol. 9 no. 1

1944-4176(2016)9:1;1-4