

# Why We ♥ Gaussian Integers

M. L. Smedinghoff and S. G. Smedinghoff

November 22, 2005

## 1 Introduction

Throughout the study of the integers, a recurring theme is the uniqueness of prime factorization. Unique prime factorization is so important that number theorists have named it the Fundamental Theorem of Arithmetic. Unique prime factorization is the property that tells us that any integer can be expressed as a product of powers of prime numbers. Moreover there is only one possible such expression for each integer. The idea of unique prime factorization is so important that number theorists study it in other number systems besides the integers. Some number systems do not have unique prime factorization. Consider the ring  $\mathbb{Z}[\sqrt{-5}]$ . In this ring, the number 21 can be factored into  $7 \cdot 3$  which are both primes in  $\mathbb{Z}[\sqrt{-5}]$ , but it can also be factored into  $(4 + \sqrt{-5})(4 - \sqrt{-5})$  which are also both primes in  $\mathbb{Z}[\sqrt{-5}]$ . Since we can factor 21 into primes in more than one way, there is no unique prime factorization in  $\mathbb{Z}[\sqrt{-5}]$ . Now consider the ring  $\mathbb{Z}[i]$ . The elements of this set are known as the Gaussian Integers. In the remaining sections of this paper, we will prove that that the Gaussian Integers have unique prime factorization.

## 2 Lemma 1

Recall that in the integers, we have the division algorithm that says if we have positive integers  $a$  and  $b$ , we can find positive integers  $q$  and  $r$  such that  $a = bq + r$  where  $0 \leq r < b$ . We can define a similar algorithm for the Gaussian Integers.

**Lemma 1 (Division Algorithm for the Gaussian Integers):** If  $\alpha, \beta \in \mathbb{Z}[i]$ ,  $\beta \neq 0$ , then there exist  $\gamma, \rho \in \mathbb{Z}[i]$  such that

$$\alpha = \beta\gamma + \rho,$$

and  $N(\rho) < N(\beta)$ .

**Proof:** If we choose  $\gamma$  to be any element of the Gaussian integers, then if we let  $\rho = \alpha - \beta\gamma$  then  $\alpha = \beta\gamma + \rho$ . Thus there exists a  $\gamma, \rho \in \mathbb{Z}[i]$  such that  $\alpha = \beta\gamma + \rho$ . Now to prove that  $N(\rho) < N(\beta)$  assume  $\alpha = \beta\gamma + \rho$ . Thus  $\frac{\alpha}{\beta} = \gamma + \frac{\rho}{\beta}$ . Note that as the Gaussian Integers are not closed under division we are using the complex numbers.  $\frac{\alpha}{\beta}$  and  $\frac{\rho}{\beta}$  will be members of the complex numbers since  $\beta \neq 0$ . Now choose  $\gamma$  to be the Gaussian Integer whose real and imaginary components are the nearest integers to the real and imaginary components of  $\frac{\alpha}{\beta}$  respectively. Hence the absolute value of both the real and imaginary components of  $\frac{\rho}{\beta}$  must be less than or equal to  $\frac{1}{2}$ . Thus  $|\frac{\rho}{\beta}| \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2}$ . We can write  $|\frac{\rho}{\beta}| = \frac{|\rho|}{|\beta|}$ . Note that for Gaussian Integers, the magnitude is equivalent to the norm so  $\frac{N(\rho)}{N(\beta)} \leq \frac{1}{2}$ . Therefore  $N(\rho) \leq \frac{N(\beta)}{2}$  and  $N(\rho) < N(\beta)$ .

## 3 Lemma 2

For our next lemma, we need to define the concept of a unit. A unit is an element  $\alpha$  of a ring if there exists a  $\beta$  in the ring such that  $\alpha\beta = 1$ .

**Lemma 2:** The units in  $\mathbb{Z}[i]$  are precisely the numbers  $\pm 1$  and  $\pm i$ .

**Proof:** Let  $\alpha$  be a unit in  $\mathbb{Z}[i]$ . By definition there exists a  $\beta$  such that  $\alpha\beta = 1$ . Thus  $N(\alpha)N(\beta) = N(1) = 1$ . Since the norm of a Gaussian Integer must be a positive integer and  $N(\alpha)$  divides 1,  $N(\alpha) = 1$ . Expressing  $\alpha$  as  $a + bi$ , we know  $a^2 + b^2 = 1$ . Since  $a, b \in \mathbb{Z}$ , the only possibilities for  $a^2$  and  $b^2$  are for one of  $a^2$  and  $b^2$  to be 0 and the other to be 1. Thus the units in the Gaussian Integers are described by  $(a,b) = (0,1), (0,-1), (1,0),$  and  $(-1,0)$ . Therefore the units in the Gaussian Integers are  $1, -1, i,$  and  $-i$ .

## 4 Lemma 3

**Lemma 3:** A number  $a + bi$  in  $\mathbb{Z}[i]$  is prime in  $\mathbb{Z}[i]$  if and only if  $a + bi$  is a unit multiplied by one of the following:

- (i)  $1 + i$ ,
- (ii) a prime number  $p \in \mathbb{Z}$ , where  $p \equiv 3 \pmod{4}$ , or
- (iii)  $u + vi$ , where  $u^2 + v^2 = p$ , and  $p$  is a prime in  $\mathbb{Z}$  with  $p \equiv 1 \pmod{4}$ .

**Proof:** First we will prove that if  $a + bi$  is the product of a unit and one of the three cases then it is prime. In the first case,  $N(a + bi) = N(\text{unit})N(1 + i) = 2$ . Now note that since 2 is prime, the only way to multiply two integers together to get 2 is 1 times 2. Thus in order to write  $a + bi$  as the product of two Gaussian Integers, one of them must have a norm of 1. Therefore one of the Gaussian Integers must be a unit. Hence  $a + bi$  is prime.

Now consider the second case.  $N(a + bi) = N(\text{unit})N(p) = p^2$ . We can factor  $p^2$  as 1 times  $p^2$  or  $p$  times  $p$ . Thus if we multiply two Gaussian Integers to get  $a + bi$  the norms of the two Gaussian Integers must be 1 and  $p^2$  or  $p$  and  $p$ . Note that in fact, the norm of a Gaussian Integer cannot be  $p$  if  $p \equiv 3 \pmod{4}$  since we know that a prime number can only be expressed as the sum of two squares if it is congruent to 1 modulo 4. Hence the norms of the two Gaussian Integers are 1 and  $p^2$ . Therefore one of them is a unit and  $a + bi$  is prime.

Now consider the third case.  $N(a + bi) = N(\text{unit})N(u + vi) = p$ . Now since  $p$  is prime, the only way we can multiply two Gaussian Integers to get  $a + bi$  is if the norm of one is 1 and the norm of the other is  $p$ . Since one of the norms is 1, one of the Gaussian Integers is a unit and  $a + bi$  is prime.

Now we will prove the reverse direction by proving the contrapositive. Consider a Gaussian Integer  $a + bi$  that cannot be expressed in one of the three forms listed above. We know that if a number can be expressed as the sum of two squares then it is the product of a square number and distinct primes which are either 2 or congruent to 1 modulo 4. In other words,  $n = p_1 p_2 \dots p_t M^2$  is the sum of two squares if and only if every  $p_i$  is 2 or congruent to 1 modulo 4. Since the norm of any Gaussian Integer is the sum of two squares, we know the norm can be written in this form. In case 1, there is only one prime,  $p_1 = 2$  and  $M = 1$ . In case 2, there are no primes and  $M$  is a prime congruent to 3 modulo 4. In case 3, there is only one prime.  $p_1$  is a prime congruent to 1 modulo 4 and  $M = 1$ . Now we must consider all of the possibilities that do not fall into one of these cases. There are four in total. Case A is where there are at least two  $p_i$ 's. Case B is where there is only one prime but  $M \neq 1$ . Case C is where there are no primes and  $M$  is a composite number. Case D is where there are no primes and  $M$  is a prime congruent to 1 modulo 4.

Consider Case A. We know that any prime congruent to 1 modulo 4 can be expressed as the sum of two squares. Since we have two primes that are congruent to 1 modulo 4, we know that any norm of this form can be expressed as the product of the norms of two Gaussian Integers neither of which have a norm of 1. Since neither Gaussian Integer in the product is a unit,  $a + bi$  is not prime.

Consider Case B. We have one prime which is congruent to 1 modulo 4 and thus can be expressed as the sum of two squares. We can write  $M^2 = M^2 + 0$ . Since  $p_1$  is not 1 and  $M$  is not one, we know we can write any norm of this form as the product of the norms of two Gaussian Integers neither of which has a norm of 1. Since neither Gaussian Integer is a unit,  $a + bi$  is not prime.

Consider Case C. Since  $M$  is a composite number, let  $M = xy$ . We can write  $M_2$  as  $(x^2 + 0)(y^2 + 0)$ . Now we know that any Gaussian Integer with a norm of this form can be expressed as the product of the norms of two Gaussian Integers, neither of which has a norm of 1. Since neither of the Gaussian Integers is a unit,  $a + bi$  is not prime.

Consider Case D. Now  $M$  is a prime congruent to 1 modulo 4. Since any prime congruent to 1 modulo 4 can be expressed as the sum of two squares, we know  $M^2$  can be written as the product of two numbers that are both the sum of squares. Thus any norm of this form can be written as the product of the norms of two Gaussian Integers, neither of which has a norm of 1. Since neither of the Gaussian Integers is a unit,  $a + bi$  is not prime.

We have now shown that any Gaussian Integer that cannot be expressed as one of the three cases stated in the lemma is not prime.

## 5 Proof of Prime Factorization in $\mathbb{Z}[i]$

To begin our proof of Prime Factorization in  $\mathbb{Z}[i]$ , we need to define the concept of greatest common divisor (gcd).

**Definition:** If  $\alpha, \beta \in \mathbb{Z}[i]$  then the greatest common divisor of  $\alpha$  and  $\beta$  is a Gaussian Integer with the greatest possible norm that divides both  $\alpha$  and  $\beta$ .

Just as in the integers, the division algorithm will provide us with a way to find the gcd of two Gaussian Integers. We will need the analogue of the Euclidean Algorithm.

**Proof of Euclidean Algorithm for  $\mathbb{Z}[i]$ :** Just as in the integers, we will apply the Division Algorithm repeatedly as follows:

$$\alpha = \beta\gamma_1 + \rho_1 \quad (1)$$

$$\beta = \rho_1\gamma_2 + \rho_2 \quad (2)$$

$$\rho_1 = \rho_2\gamma_3 + \rho_3 \quad (3)$$

$$\vdots$$

$$\rho_{n-2} = \rho_{n-1}\gamma_n + \rho_n \quad (n)$$

$$\rho_{n-1} = \rho_n\gamma_{n+1} + 0 \quad (n+1)$$

First we will show that  $\rho_n$  divides  $\alpha$  and  $\beta$ . From Equation  $n+1$ , we know  $\rho_n | \rho_{n-1}$ . Since  $\rho_n | \rho_{n-1}$  and  $\rho_n | \rho_n$  we know that  $\rho_n$  divides  $\rho_{n-2}$ , a linear combination of  $\rho_n$  and  $\rho_{n-1}$  by Equation  $n$ . Note that the proof of the linear combination lemma is exactly analogous to the proof in the integers. Now we can work our way up the list of equations, noting the  $\rho_n | \rho_i$ . Now since  $\rho_n | \rho_1$  and  $\rho_n | \rho_2$ , we know that  $\rho_n | \beta$ , a linear combination of  $\rho_1$  and  $\rho_2$  by Equation 2. Finally, since  $\rho_n | \beta$  and  $\rho_n | \rho_1$ ,  $\rho_n | \alpha$ , a linear combination of  $\beta$  and  $\rho_1$  by Equation 1.

Let  $d$  be any divisor of  $\alpha$  and  $\beta$ . We will show that  $N(d) \leq N(\rho_n)$ . Since  $d | \alpha$  and  $d | \beta$ , we know that  $d | \rho_1$  as  $\rho_1$  can be expressed as a linear combination of  $\alpha$  and  $\beta$  by Equation 1. Similarly,  $d | \rho_2$  since  $\rho_2$  can be expressed as a linear combination of  $\beta$  and  $\rho_1$  by Equation 2. Now we can work down the list of equations to find that  $d | \rho_i$  for any  $i$ . Thus  $d | \rho_n$ . Hence  $\rho_n = dx$  for some Gaussian Integer  $x$ . Thus  $N(\rho_n) = N(d)N(x)$ . Since  $\rho_n$  is nonzero, the smallest possible value of  $N(x)$  is 1. Therefore,  $N(\rho_n) \geq N(d) * 1$ . Therefore,  $N(d) \leq N(\rho_n)$ . Thus  $\rho_n$  is the gcd of  $\alpha$  and  $\beta$ .

Since we have defined the Euclidean Algorithm in much the same way as the integers, an analogue of Bezout's Identity exists for the Gaussian Integers. Thus we can write the gcd of two Gaussian Integers as a linear combination of the Gaussian Integers. The proof is identical to the proof for the integers.

The final ingredient of our proof of unique factorization of the Gaussian Integers is the Prime Divisibility Property. The Prime Divisibility Property for  $\mathbb{Z}[i]$  says that if  $\pi$  is a prime Gaussian Integer, and  $\pi | \alpha\beta$ , then  $\pi | \alpha$  or  $\pi | \beta$ .

**Proof of Prime Divisibility Property in  $\mathbb{Z}[i]$ :** Assume  $\pi|\alpha\beta$ . If  $\pi|\alpha$  we are done. Otherwise,  $\gcd(\pi,\alpha) = 1$ . By Bezout's Identity,  $1 = \rho\pi + \sigma\alpha$  for some  $\rho, \sigma \in \mathbb{Z}[i]$ . Multiplying both sides by  $\beta$ , we get  $\beta = \rho\pi\beta + \sigma\alpha\beta$ . Since  $\pi|\rho\pi\beta$  and  $\pi|\sigma\alpha\beta$ ,  $\pi|\beta$  as desired.

**Proof of Unique Factorization in  $\mathbb{Z}[i]$ :** First we will prove the existence of a prime factorization. We will proceed by induction. We will assume that every Gaussian Integer whose norm is greater than 1 and less than  $n$  has a prime factorization. A Gaussian Integer with norm  $n$  is either prime or composite. If it is prime, we have found a prime factorization. If it is composite, then we can factor it into two Gaussian Integers both of whose norms are less than  $n$ . Thus both of these Gaussian Integers will have prime factorizations, so the prime factorization of the Gaussian Integer in question will be the product of those two prime factorizations.

Now we will prove the uniqueness of prime factorization. Suppose there are Gaussian Integers with multiple prime factorizations. Let  $\alpha$  be a Gaussian Integer with the smallest possible norm that has multiple prime factorizations. Let the two factorizations be  $\alpha = \pi_1 \dots \pi_s$  and  $\alpha = \gamma_1 \dots \gamma_t$  where all the  $\pi_i$  and  $\gamma_i$  are prime and the two factorizations are not the same. Note that  $\alpha$  cannot be prime since a prime number has only one factorization. Thus  $s, t \geq 2$ . Notice that  $\pi_1 | \gamma_1 \dots \gamma_t$ . Thus by the Prime Divisibility Property,  $\pi_1 | \gamma_i$  for some  $i$ . Without loss of generality, assume  $\pi_1 | \gamma_1$ . However,  $\pi_1$  and  $\gamma_1$  are both prime, thus  $\pi_1 = \gamma_1$ . Hence  $\pi_2 \dots \pi_s = \frac{\alpha}{\pi_1} = \gamma_2 \dots \gamma_t$ . These two factorizations of  $\frac{\alpha}{\pi_1}$  are different. However, since  $N(\pi_1) > 1$ ,  $N(\frac{\alpha}{\pi_1}) < \alpha$ . But we assumed that  $\alpha$  had the smallest possible norm for a Gaussian Integer with multiple factorizations, a contradiction. Thus prime factorization is unique for the Gaussian Integers.

## 6 Conclusion

In order to prove that we love Gaussian Integers, we will proceed by induction. We will assume that we love all Gaussian Integers with norm less than  $n$ . Since we love all of the Gaussian integers with norm less than  $n$ , why should we not love just a few more with norm  $n$ ? Thus, if we love all Gaussian integers with norm less than  $n$ , we love all the Gaussian Integers with norm  $n$ . Hence, by induction, we love all Gaussian Integers. Tadah!