Section III.3. Supplement: The Gaussian Integers

Note. In this supplement, we define the Gaussian integers, show they form an integral domain. We define a multiplicative norm and use this to prove that the Gaussian integers form an integral domain. Our main references for this supplement are John Fraleigh's *A First Course In Abstract Algebra*, 7th edition (Addison-Wesley, 2003) and Thomas Hungerford's *Algebra* (Springer-Verlag, 1974).

Note III.3.GI.A. We now give a brief description of "reciprocity," which was the inspiration for the development of the Gaussian integers. This note is based on Isreal Kleiner's "From Numbers to Rings: The Early History of Ring Theory," *Elemente der Mathematik*, **53**, 18–35 (1998); this sources is available online on the European Mathematical Society Press website (accessed 3/19/2024).

Image from the MacTutor biography webpage of Gauss (accessed 3/19/2024)

Solving polynomial equations of the form

$$a_m x^m + a_{m-1} x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0 \equiv 0 \,(\text{mod } n),$$

where $a_i \in \mathbb{Z}$, plays a role in number theory. The case of $m = 2$ (i.e., the quadratic) was dealt with by Karl F. Gauss (April 30, 1777–February 23, 1855). In his famous 1801 book *Disquisitiones Arithmeticae*, Gauss showed that the quadratic case of solving $a_2x^2 + a_1x + a_0 \equiv 0 \pmod{n}$ requires only consideration of the congruence $x^2 \equiv q \pmod{p}$ where p and q are primes (the cases of odd primes and even primes handled separately). Gauss proved that $x^2 \equiv q \pmod{p}$ is solvable if and only if $x^2 \equiv p \pmod{q}$, unless $p \equiv q \equiv 3 \pmod{4}$ in which case $x^2 \equiv q \pmod{p}$ is solvable if and only if $x^2 \equiv p \pmod{q}$ is not solvable. This is Gauss' Quadratic Reciprocity Law. This is stated and proved in Elementary Number Theory (MATH 3120); see my online notes for that class on Section 12. Quadratic Reciprocity and notice Theorem 12.4, The Quadratic Reciprocity Theorem (beware that this expressed in terms of Legendre symbols of the forms (p/q) and (q/p); these are not quotients, and are defined in Section 11. Quadratic Congruences).

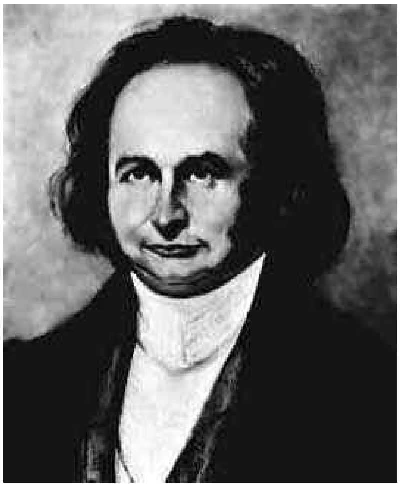

Image from the MacTutor biography webpage of Jacobi and the MacTutor biography webpage of Eisenstein (accessed 3/19/2024)

This initial work lead to the study of more general "reciprocity relations" between the solvability of $x^m \equiv q (\text{mod } p)$ and $x^m \equiv p \ (\text{mod } q)$ for $m > 2$. Carl Jacobi (December 10, 1804–February 18, 1851) and Ferdinand Eisenstein (April 16, 1823–October 1852) considered cubic reciprocity (Jacobi in a paper of 1827, and Eisenstein in three papers of 1844–45). In the process, they (primarily Eisenstein) considered the ring $\mathbb{Z}[\rho] = \{a + b\rho \mid a, b \in \mathbb{Z}\}$ where $\rho = (-1 + i\sqrt{3})/2 = e^{2\pi i/3}$ (so that $\rho^3 = 1$). This is now known as the *Eisenstein integers*. The Eisenstein integers form a unique factorization domain and the units are ± 1, $\pm\rho$, $\pm\rho^2$. With this tool, they formulated the cubic reciprocity law (as did Gauss, though he never published his result). Gauss considered quartic reciprocity in two papers. The first was "Theoria Residuorum Biquadraticorum, Commentatio Prima," *Commentationes Societatis Regiae Scientiarum Gottingensis recentiores*, **6**, 25–56 (April 5, 1825), and the second was "Theoria Residuorum Biquadraticorum, Commentatio Secunda," *Commentationes Societatis Regiae Scientiarum Gottingensis recentiores*, **7**, 89–148 (April 15, 1831). Copies of these (in Latin) are online on the HathiTrust website for the 1825 paper and the HathiTrust website for the 1831 paper. It was in the second of these two papers on quartic reciprocity ("*Residuorum Biquadraticorum*") that Gauss introduced the Gaussian integers: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$. It is straightforward to show that the Gaussian integers form a subring of $\mathbb{C}$ (and so form a commutative ring with identity). Since $\mathbb{C}$ has no zero divisors, then neither does $\mathbb{Z}[i]$. That is, the Gaussian integers form an integral domain. In summary, we have the following.

Theorem A. The *Gaussian integers*, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$, form an integral domain.

Note. We now introduce "multiplicative norms," which we will use to establish certain properties of the Gaussian integers. Most of this material is based on Fraleigh's book.

Definition. (Fraleigh's Definition 47.6) Let D be an integral domain. A *multiplicative norm* N on D is a function $N : D \to \mathbb{Z}$ such that the following conditions are satisfied:

1. $N(\alpha) = 0$ if and only if $\alpha = 0$.

2. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in D$.

Note III.3.GI.B. A "multiplicative norm" N on an integral domain need not be a norm is the usual sense (as seen in Linear Algebra or Analysis), because we do not require that N is nonnegative. Notice that *any* ring with such a mapping N defined on it (which satisfies the two given conditions) cannot have zero divisors.

Note. The usual norm on $\mathbb{C}$ is the *modulus* of each complex number: $|z| = |a+ib| = \sqrt{a^2 + b^2}$. This is shown to be a norm in Complex Variables (MATH 4337/5337) as an exercise from Section 1.4. Vectors and Moduli and a proof is given in Complex Analysis 1 (MATH 5510) in I.3. The Complex Plane (see Theorem I.3.A). This can be used to define a multiplicative norm on the Gaussian integers. We define multiplicative norm N on $\mathbb{Z}[i]$ as $N(a+bi) = |a+bi|^2 = a^2+b^2$. The next result allows us to find the Gaussian integers which are units.

Theorem B. (Fraleigh's Theorem 47.7) If D is an integral domain with a multiplicative norm N, then $N(1_D) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every α satisfying $|N(\alpha)| = 1$ is a unit in D, then an element $\pi \in D$ with $|N(\pi)| = p$, for a prime $p \in \mathbb{Z}$, is an irreducible of D.

Note III.3.GI.C. Theorem B let's us find the units of $\mathbb{Z}[i]$ using the multiplicative norm N. We simply need to find all Gaussian integers $a+bi$ such that $N(a+bi) = a^2+b^2 = 1$. Since $a, b \in \mathbb{Z}$ then we must have either $a = \pm 1$ and $b = 0$, or $a = 0$ and $b = \pm 1$. So the only units are 1, -1, i, and $-i$. Now every $\alpha \in \mathbb{Z}[i]$ such that $|N(\alpha)| = 1$ is a unit of $\mathbb{Z}[i]$ (since the only such α are 1, -1, i, $-i$), so Theorem B implies that any $\pi \in \mathbb{Z}[i]$ such that $|N(\pi)| = p$ where p is prime in $\mathbb{Z}$, is irreducible in $\mathbb{Z}[i]$. This may not allow us to classify the irreducible Gaussian integers, but we can observe, for example, that $5 \in \mathbb{Z}[i]$ is not irreducible. We have $5 = (1+2i)(1-2i)$ and, since $N(1+2i) = N(1-2i) = 1^2+2^2 = 5$ (and 5 is prime in $\mathbb{Z}$), $1+2i$ and $1-2i$ are irreducible. That is, $5 = (1+2i)(1-2i)$ is a factorization of 5 into irreducibles. We now shift over to material from Hungerford.

Note. A different ring is considered in Hungerford's Exercise III.3.3 and also analyzed using a multiplicative norm. Let R be the subring $\{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$

of the field of real numbers. As claimed in my online notes for Section III.3. Factorization in Commutative Rings; see Note III.3.B. Define $N : R \to \mathbb{Z}$ as $N(a+b\sqrt{10}) = (a+b\sqrt{10})(a-b\sqrt{10}) = a^2 - 10b^2$.

Lemma A. (Hungerford's Exercise III.3.3(a)) With $R = \{a+b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a+b\sqrt{10}) = (a+b\sqrt{10})(a-b\sqrt{10}) = a^2 - 10b^2$, we have that N is a multiplicative norm on R.

Lemma B. (Hungerford's Exercise III.3.3(b)) With $R = \{a+b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a+b\sqrt{10}) = a^2 - 10b^2$, u is a unit in R if and only if $|N(u)| = \pm 1$.

Note. By Lemma B, we have that $3+\sqrt{10}$ is a unit because $N(3+\sqrt{10}) = 9-10 = -1$. In fact, the inverse of $3+\sqrt{10}$ is $-3+\sqrt{10}$ since $(3+\sqrt{10})(-3+\sqrt{10}) = -(3+\sqrt{10})(3-\sqrt{10}) = 1$.

Lemma C. (Hungerford's Exercise III.3.3(c)) With $R = \{a+b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a+b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4+\sqrt{10}$, and $4-\sqrt{10}$ are irreducible elements of R.

Lemma D. (Hungerford's Exercise III.3.3(d)) With $R = \{a+b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a+b\sqrt{10}) = a^2 - 10b^2$, we have that 2, 3, $4+\sqrt{10}$, and $4-\sqrt{10}$ are not prime elements of R.

Note. We saw in Example III.3.A that in the ring $\mathbb{Z}_n$, where $n \equiv 2 \pmod 4$, $\bar{2}$ is prime but not irreducible. Lemmas C and D show that, in R, there are irreducibles that are not prime. So, in general, irreducibility and primeness are distinct properties.

Theorem C. (Hungerford's Exercise III.3.4) Let $R = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$ and $N : R \to \mathbb{Z}$ as $N(a + b\sqrt{10}) = a^2 - 10b^2$. Then a and b are associates if and only if $|N(a)| = |N(b)|$. Every element of R can be factored into a product of irreducibles, though this factorization need not be unique (in the sense of Definition 3.5(ii)).

Note III.3.GI.D. Theorem C shows that even though every element of R can be factored into a product of irreducibles, the factorization may not be unique. We can establish this by example from Lemma C. Notice that $6 = 2 \cdot 3 = (4 + \sqrt{10})(4 - \sqrt{10})$ where 2, 3, $4 - \sqrt{10}$, and $4 + \sqrt{10}$ are irreducible. However, since $N(2) = 4$, $N(3) = 9$, $N(4 - \sqrt{10}) = 6$, and $N(4 + \sqrt{10}) = 6$ then by Theorem C neither of 2 and 3 is an associate of $4 - \sqrt{10}$ or $4 + \sqrt{10}$. That is, these factorizations of 6 into products of irreducibles are not the same in the sense of Definition III.3.5(ii).

Note. Next, we argue that the Gaussian integers form a Euclidean domain with $\varphi(a + bi) = a^2 + b^2$. First, we need a preliminary lemma which is given in Exercise III.3.6(a).

Lemma E. (Hungerford's Exercise III.3.6(a)) If a and n are integers, $n > 0$, then there exist integers q and r such that $a = qn + r$, where $|r| \le n/2$.

Note. Lemma E now allows us to prove the following.

Theorem D. (Hungerford's Exercise III.3.6(b)) The Gaussian integers $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ form a Euclidean domain with $\varphi(a + bi) = a^2 + b^2$.

Note III.3GI.E. By Theorem III.3.9, every Euclidean domain is a unique factorization domain, so we now have by Theorem D that the Gaussian integers form a unique factorization domain. In Mathematical Reasoning (MATH 3000), this appears as Fundamental Theorem of Arithmetic in the Gaussian integers; see my online notes for Mathematical Reasoning on Section 7.2. The Gaussian Integers and notice Theorem 7.20. It is also shown in those notes that the Division Algorithm holds in $\mathbb{Z}[i]$ (in Theorem 7.14) and the Euclidean Algorithm (for finding greater common divisors) holds in $\mathbb{Z}[i]$.

Note. In Fraleigh's *A First Course In Abstract Algebra*, 7th edition (Addison-Wesley, 2003), Section IX.47. Gaussian Integers and Multiplicative Norms (pages 409 and 410) it is stated:

> "…a suitably defined norm may be of help in determining the arithmetic structure of [integral domain] D. This is strikingly illustrated in *algebraic number theory*, where for a domain of *algebraic integers* we consider many different norms of the domain, each doing its part in helping to determine the arithmetic structure of the domain. …This is an example of the importance of studying properties of elements in an algebraic structure by means of mapping associated with them."

Revised: 3/28/2024