Finding Factors of Factor Rings over the Gaussian Integers

Greg Dresden and Wayne Dymàček

1. INTRODUCTION AND HISTORY. The Gaussian integers are defined to be the set $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i = \sqrt{-1}\}$. These sit inside the complex numbers $\mathbb{C}$ and thus obey the usual rules of addition and multiplication; indeed, despite the presence of the imaginary i, they are quite similar to the "traditional" integers. In fact, in the set $\mathbb{Z}[i]$ one can define (Gaussian integer) primes, construct analogues of the Euclidean division algorithm and the Euler ϕ function, discuss Pythagorean triples, generalize the twin-prime problem, and much more. In this paper, we will generalize the idea of factor rings from the integers to the Gaussian integers and discuss what new objects can be found in this manner. (Recall that integer factor rings are the familiar objects $\mathbb{Z}/\langle n\rangle$, for $\langle n\rangle$ the ideal in $\mathbb{Z}$ generated by n. These rings are also written as $\mathbb{Z}/n\mathbb{Z}$ or $\mathbb{Z}_n$.)

If the Gaussian integers were no more than a practice area for generalizing concepts from the "traditional" integers, they would still be of great interest to students and researchers alike. Yet these numbers have been (and still are) far more than just a convenient teaching tool. They have played roles in the development of two of the great theorems of mathematics of the last two centuries (the reciprocity theorems and Fermat's Last Theorem) and have helped inspire the creation of algebraic number theory. Taking a minute to provide a brief review of this fascinating history will be time well spent. (Much of what follows can be found in [9]; see also [7].)

Our story begins over two hundred years ago, long before either abstract algebra or modern number theory came into existence. In the late 1700s, Leonhard Euler noticed some intriguing patterns that arose in his study of the equation $x^2 \equiv p \pmod{q}$. Euler called p a quadratic residue or nonresidue modulo q depending on the existence of a solution to this equation, and he surmised that, for odd primes p and q with $p \equiv 1 \pmod{4}$, p is a quadratic residue modulo q if and only if q is a quadratic residue modulo p. This remarkable conjecture on quadratic reciprocity (and others like it) established a test for the solvability of $x^2 \equiv p \pmod{q}$ by looking at the reciprocal equation $x^2 \equiv q \pmod{p}$. Moreover, if $q > p$ this new equation could be simplified and the process repeated. Euler was able to prove some nice partial results (for example, that -1 is a quadratic residue modulo an odd prime p if and only if $p \equiv 1 \pmod{4}$) and Adrien-Marie Legendre attempted a proof a few years later. The first appearance, however, of a full and complete proof of the quadratic reciprocity theorem was in Carl Friedrich Gauss's seminal work of 1801, the *Disquisitiones Arithmeticae.*

It was only natural that after settling the matter of quadratic reciprocity Gauss should then turn to higher reciprocity theorems, and he spent many years trying to establish relationships between, say, $x^4 \equiv p \pmod{q}$ and $x^4 \equiv q \pmod{p}$. This proved to be exceptionally difficult, and Gauss realized that he needed to look beyond the "traditional" integers. Here is how in Gauss's 1832 paper [5, p. 102] a new set of numbers makes its first appearance in print:

> [N]umeri formae $a + bi$, denotantibus i, pro more quantitatem imaginariam $\sqrt{-1}$, atque a, b indefinite omnes numeros reales integros inter $-\infty$ et $+\infty$. Tales numeros vocabimus *numeros integros complexos.* ...

Gauss called them *numeros integros complexos* (*complex integer numbers*), but of course we now know them as Gaussian integers. He proceeded to develop an entire arithmetic in $\mathbb{Z}[i]$; first, by defining primes and illustrating which Gaussian integers are prime, and then by proving the existence of unique factorization into these primes. (This can now be recognized as the beginning of algebraic number theory, which seeks to do for $\mathbb{Z}[\xi] = \{a + b\xi + c\xi^2 + \cdots\}$ what Gauss did for $\mathbb{Z}[i] = \{a + bi\}$.) Gauss was then able to state a general theorem for quartic (also called biquadratic) reciprocity in the language of Gaussian integers. Still, as with Euler before him, even the great Gauss was unable to prove the reciprocity theorems he had so painstakingly developed. This was finally achieved by the young mathematician Ferdinand G. Eisenstein, who produced five different proofs in the 1840s.

A general theorem for higher (quintic, etc.) reciprocity proved to be even more difficult, but more on that in a moment. Since we find ourselves in the 1840s, let us turn our attention to the 1847 meeting of the Paris Academy of Science, where for a few moments Fermat's Last Theorem seemed to have been solved. (Edwards's book [3] gives a full and lengthy description of that exciting time; what follows here is a condensed version of his account.)

The famous conjecture of Fermat (from about 1636) concerns integer solutions to the equation $x^n + y^n = z^n$ for $n \geq 3$. It was not until 1994 that Andrew Wiles proved that no solutions except the obvious trivial ones exist. Prior to the 1847 Paris meeting only a few partial results had been found, so it was quite a shock when Gabriel Lamé announced that he had a complete proof. A key part of his method involved the factoring of $x^p + y^p$ as $(x + y)(x + \xi y)(x + \xi^2 y) \cdots (x + \xi^{p-1} y)$, where ξ is a complex number (called a *primitive* pth *root of unity*) such that $\xi^p = 1$ but $\xi^q \neq 1$ when $0 < q < p$. Lamé had made the assumption that arithmetic in this extended set of numbers would be the same as in $\mathbb{Z}$ or in $\mathbb{Z}[i]$, and, in particular, that one would have unique factorization into prime elements. Joseph Liouville spoke next, however, and said that this assumption of Lamé might not be true. Much work was carried out by Lamé and others over the ensuing days in an attempt to bridge this gap, until it was eventually discovered that Ernst Kummer had already proved that unique factorization fails in some of these extended sets of numbers (for instance, when ξ is a primitive 23rd root of unity). Kummer was working on his proof of the aforementioned higher reciprocity laws when he made this disappointing discovery, and this led him to define ideal numbers. This led directly to Richard Dedekind's development of algebraic number theory in the 1870s and the restoration of a form of unique factorization using ideals instead of numbers.

We see that the Gaussian integers are quite deceptive in their similarity to the "traditional" integers. They both have primes, as well as unique factorization into primes; both are principal ideal domains; and they both even have norms and division algorithms, making them Euclidean domains (see [16]). It is thus not surprising that Lamé and others thought (incorrectly!) that their numbers of the form $a_0 + a_1\xi + a_2\xi^2 + \cdots$ would always behave in a similar manner.

2. MOTIVATIONAL REMARKS. There are, of course, fundamental differences even between $\mathbb{Z}$ and $\mathbb{Z}[i]$ and one place where these differences can be observed is in the types of factor rings that can be produced. As mentioned earlier, factor rings in the "traditional" integers are the familiar objects $\mathbb{Z}_n$, and these are isomorphic to the rings $\{0, 1, \ldots, n-1\}$ modulo n. These rings are easily understood; not only is the underlying group cyclic, but one can also show that if n factors as $p_1^{e_1} \cdots p_k^{e_k}$, then $\mathbb{Z}_n$ "factors" as $\mathbb{Z}_{p_1^{e_1}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{e_k}}$. This is a consequence of the Chinese Remainder Theorem, which asserts the existence of a unique solution (mod $p_1^{e_1} \cdots p_k^{e_k}$) to systems of congruences such as $x \equiv a_1$ (mod $p_1^{e_1}$), $\ldots$, $x \equiv a_k$ (mod $p_k^{e_k}$). Using this theorem, we can create a well-defined isomorphism between $\mathbb{Z}_n$ and the direct sum of the respective $\mathbb{Z}_{p_i^{e_i}}$.

In the Gaussian integers $\mathbb{Z}[i]$ factor rings can be much more complicated, and many interesting questions arise. These two exercises are taken from a popular modern algebra text [4]:

> Show that the characteristic of $\mathbb{Z}[i]/\langle a+bi\rangle$ divides a^2+b^2. (Exercise 38, page 269)
> Show that $\mathbb{Z}[i]/\langle 2+i\rangle$ is a field. How many elements does it have? (Exercise 11, page 331)

Further reading turned up many similar exercises dealing with factor rings over the Gaussian integers, and further investigation by us and by our students (Matt Kozora and Michael Riley) revealed that there was a general theory behind all these problems, a theory that could easily handle these exercises in just one or two steps. Indeed, what we show in this article is that many of these questions about factor rings can be answered by simply understanding how a general factor ring like $\mathbb{Z}[i]/\langle a+bi\rangle$ "factors" into direct products of smaller, simpler rings, usually of the form $\mathbb{Z}_n$ or $\mathbb{Z}_n[i]$. Our purpose is to present this general theory, along with its ramifications and applications, in a manner that is accessible to capable algebra students and in a form that could be used either as an extended homework problem or in a classroom presentation. Indeed, much of this work can be generalized to other rings containing $\mathbb{Z}$, which might make a good honors thesis or senior project (see the conclusion for further remarks).

We remark that the problem of factoring the (multiplicative) group of units of $\mathbb{Z}[i]/\langle a+bi\rangle$ has been completely solved in [2]. For an extension of this topic beyond the Gaussian integers (with references to other papers), see [15]. For a study of the group of units in $\mathbb{Z}/\langle n\rangle$, see [8, chap. 4].

3. SOME TECHNICAL BACKGROUND.

We begin by establishing some basic facts about elements and ideals in the Gaussian integers. First, since the units of $\mathbb{Z}[i]$ are 1, -1, i, and $-i$, we know that for a and b integers, the ideals $\langle a+bi\rangle$, $\langle -a-bi\rangle$, $\langle -b+ai\rangle$, and $\langle b-ai\rangle$ in $\mathbb{Z}[i]$ are one and the same. Thus, we can state:

Fact 1. $$\mathbb{Z}[i]/\langle a+bi\rangle \cong \mathbb{Z}[i]/\langle -a-bi\rangle \cong \mathbb{Z}[i]/\langle -b+ai\rangle \cong \mathbb{Z}[i]/\langle b-ai\rangle.$$

Also, by basic ring theory, we have:

Fact 2. $$\mathbb{Z}[i]/\langle 0\rangle \cong \mathbb{Z}[i] \qquad \text{and} \qquad \mathbb{Z}[i]/\langle 1\rangle \cong \{0\}.$$

Our first nontrivial statement about factor rings is:

Theorem 1. *If a is a positive integer larger than 1, then*

$$\mathbb{Z}[i]/\langle a\rangle \cong \mathbb{Z}_a[i].$$

Proof. Define $\phi : \mathbb{Z}[i] \to \mathbb{Z}_a[i]$ by $\phi(x+yi) = [x]_a + [y]_a i$, where $[\cdot]_a$ represents the equivalence class modulo a. This mapping is clearly a surjective ring homomorphism. Since $\phi(a) = [a]_a = [0]_a = 0$, a belongs to $\ker(\phi)$ and hence $\langle a\rangle \subseteq \ker(\phi)$. On the other hand, if $\phi(x+yi) = 0$, then both x and y are congruent to 0 modulo a, so we can write $x = ax'$ and $y = ay'$ for some integers x' and y'. Thus $x + yi = ax' + ay'i = a(x' + y'i)$ lies in $\langle a\rangle$. Therefore $\ker(\phi) = \langle a\rangle$, implying that $\mathbb{Z}[i]/\langle a\rangle \cong \mathbb{Z}_a[i]$. ■

Sometimes, $\mathbb{Z}_a[i]$ is actually a field, as pointed out by the next basic fact:

Fact 3. If a is a positive integer larger than 1, then $\mathbb{Z}_a[i]$ is a field if and only if a is a prime (in $\mathbb{Z}$) that is congruent to 3 modulo 4.

Proof. Suppose first that $\mathbb{Z}_a[i]$ is a field. Clearly a must be prime. Moreover, a cannot be 2, for if it were, then $(1+i)^2 \equiv 0 \pmod{a}$, a contradiction. So, let a be an odd prime, and consider the usual ring homomorphism $\phi : \mathbb{Z}_a[x] \to \mathbb{Z}_a[i]$ given by $\phi(x) = i$. Since a is an odd prime, $\ker(\phi) = \langle x^2+1\rangle$. By the standard isomorphism theorem, $\mathbb{Z}_a[i] \cong Z_a[x]/\langle x^2+1\rangle$, and this is a field if and only if x^2+1 is irreducible modulo a. This is equivalent to stating that there are no solutions to $x^2 \equiv -1 \pmod{a}$, and we recognize this as a question about quadratic reciprocity! As discussed in the introduction, Euler proved that this equation has solutions (for a an odd prime) if and only if $a \equiv 1 \pmod{4}$. Thus, we can conclude that $a \equiv 3 \pmod{4}$. Next, suppose that a is a prime congruent to 3 modulo 4, and consider again the ring homomorphism ϕ. Since x^2+1 is irreducible, the kernel $\langle x^2+1\rangle$ is a maximal ideal, and thus $\mathbb{Z}_a[i]$ is a field. ■

Since $\mathbb{Z}[i]$ is a Euclidean domain, we have the following corollary to Fact 3 and Theorem 1 about primes in $\mathbb{Z}[i]$ (a prime in $\mathbb{Z}[i]$, as first defined by Gauss, is exactly what one would expect– an element σ such that if $\sigma = xy$ then either x or y is a unit in $\mathbb{Z}[i]$, namely, one of the numbers ±1 or $\pm i$):

Corollary 1. *If a is a positive integer larger than 1, then a is prime in $\mathbb{Z}[i]$ if and only if a is a prime (in $\mathbb{Z}$) that is congruent to 3 modulo 4.*

We record several other bits of information about Gaussian integers that we meet later; some of these are interesting in their own right. The first is nothing more than the "division formula" in the complex numbers: for a, b, c, and d integers,

$$\frac{c+di}{a+bi} = \frac{ac+bd}{a^2+b^2} + i\left(\frac{ad-bc}{a^2+b^2}\right). \tag{1}$$

Next, we have an immediate consequence of equation (1):

Fact 4. If a and b are relatively prime integers, then $c + di$ belongs to the ideal $\langle ak + bki\rangle$ if and only if $k(a^2+b^2)$ divides both $ac + bd$ and $ad - bc$.

We now proceed to an interesting isomorphism between rings. This is also an important step in developing our main theorem.

Theorem 2. *If a and b are relatively prime integers, then $\mathbb{Z}[i]/\langle a+bi\rangle$ is isomorphic to $\mathbb{Z}_{a^2+b^2}$.*

Observe the difference between Theorems 1 and 2. (Note also that Theorem 2 lets us solve the second exercise quoted earlier.) Theorem 2 admits the following corollary:

Corollary 2. *If a and b are relatively prime integers, then $a+bi$ is a prime in $\mathbb{Z}[i]$ if and only if a^2+b^2 is prime in $\mathbb{Z}$. (Note that in this case, $(a^2+b^2)\not\equiv 3 \pmod 4$.)*

Proof of Theorem 2. Thanks to Fact 1, we can assume without loss of generality that a and b are both positive. Observe that b is relatively prime to a^2+b^2, so b^{-1} exists in $\mathbb{Z}_{a^2+b^2}$. (We are being a bit sloppy with our notation; technically, we should be writing b^{-1} as $\left([b]_{a^2+b^2}\right)^{-1}$ to indicate that we are talking about the inverse of the equivalence class of b modulo a^2+b^2. It should be clear from the context, however, when we are talking about integers and when we are talking about equivalence classes modulo a^2+b^2.) Since $a^2+b^2\equiv 0 \pmod{a^2+b^2}$, $a^2\equiv -b^2 \pmod{a^2+b^2}$, implying that $(ab^{-1})^2\equiv -1$. Define $\phi:\mathbb{Z}[i]\to\mathbb{Z}_{a^2+b^2}$ by $\phi(x+yi)=x-(ab^{-1})y$ modulo a^2+b^2. Clearly ϕ is surjective and preserves addition.

Let $\alpha=x+yi$ and $\beta=w+zi$ be in $\mathbb{Z}[i]$. Since

$$\begin{aligned}\phi(\alpha)\cdot\phi(\beta)=\phi(x+yi)\cdot\phi(w+zi) &= \Big(x-ab^{-1}y\Big)\cdot\Big(w-ab^{-1}z\Big)\\ &\equiv (xw)+a^2b^{-2}(yz)-ab^{-1}(xz+yw)\\ &\equiv (xw-yz)-ab^{-1}(xz+yw)\\ &= \phi\left((xw-yz)+(xz+yw)i\right)\\ &= \phi\left((x+yi)\cdot(w+zi)\right)\\ &= \phi\left(\alpha\cdot\beta\right),\end{aligned}$$

ϕ preserves multiplication. Moreover, because $\phi(a+bi)=a-ab^{-1}b\equiv 0$, $\langle a+bi\rangle\subseteq\ker(\phi)$.

Let $c+di$ belong to $\ker(\phi)$ and let $c+di=(a+bi)(x+yi)$, where x and y are rational numbers. Since $0\equiv\phi(c+di)=c-ab^{-1}d$, $0\equiv bc-ad$, which by (1) makes y an integer. Multiplying the last equation by ab yields $0\equiv ab^2c-a^2bd$, which implies $0\equiv ac-a^2b^{-2}bd$. From $(ab^{-1})^2\equiv -1$, we have $0\equiv ac+bd$, so x is also an integer. We conclude $\ker(\phi)\subseteq\langle a+bi\rangle$, which means that $\ker(\phi)=\langle a+bi\rangle$ and thus demonstrates that $\mathbb{Z}[i]/\langle a+bi\rangle$ is isomorphic to $\mathbb{Z}_{a^2+b^2}$. ■

We can now identify all primes in the Gaussian integers:

Theorem 3. *Up to multiplication by units, the primes σ in $\mathbb{Z}[i]$ are of three types:*

(1) *$\sigma=a+bi$ and $\sigma'=b+ai$, where $p=a^2+b^2$ is a prime in $\mathbb{Z}$ and $p\equiv 1 \pmod 4$;*
(2) *$\sigma=p$, where p is a prime in $\mathbb{Z}$ and $p\equiv 3 \pmod 4$;*
(3) *$\sigma=1+i$.*

This can be easily seen by using Corollaries 1 and 2. For an alternate development (not involving quadratic reciprocity) of the Gaussian primes, see [2] or [11, chap. 9]. We remark that σ and σ' are distinct primes and that each prime σ in $\mathbb{Z}[i]$ has four distinct associates: $\sigma, -\sigma, i\sigma, -i\sigma$ (also, $-i\sigma$ is the complex conjugate of σ'). With this in mind, given a nonzero Gaussian integer $a + bi$, we can factor it in the manner

$$a + bi = i^d \cdot \prod {\sigma_m}^{u_m} \cdot \prod {\sigma'_m}^{v_m} \cdot \prod {p_m}^{e_m} \cdot (1+i)^n, \tag{2}$$

where $|\sigma_m|^2$ and $|\sigma'_m|^2$ are primes (in $\mathbb{Z}$) congruent to 1 modulo 4, p_m is a prime (in $\mathbb{Z}$) congruent to 3 modulo 4, and d, u_m, v_m, and n are nonnegative integers with $u_m \leq v_m$. (Recall that the absolute value $|x+yi|$ of a complex number $x+yi$ is defined to be $\sqrt{x^2+y^2}$.)

4. THE MAIN RESULTS. We can now prove a general statement about the elements of any factor ring of $\mathbb{Z}[i]$ (this result is a generalization of one part of Theorem 1 in [2], which covers only the case where one is factoring out by a power of a prime ideal in $\mathbb{Z}[i]$).

Theorem 4. *If a, b, and k are positive integers with a and b relatively prime, then the equivalence classes of $\mathbb{Z}[i]/\langle ak+bki\rangle$ are $\left\{[x+yi] : 0 \leq x < k(a^2+b^2),\ 0 \leq y < k\right\}$.*

Proof. We first show that the indicated equivalence classes are distinct. (Again, we are simplifying our notation; $[\cdot]$ will represent $[\cdot]_{ak+bki}$, an equivalence class modulo $ak+bki$.) If $[x_1+y_1i] = [x_2+y_2i]$ with $0 \leq x_1, x_2 < k(a^2+b^2)$ and $0 \leq y_1, y_2 < k$, then

$$(x_2 - x_1) + (y_2 - y_1)i \in \langle ak+bki\rangle. \tag{3}$$

Appealing to Fact 4, we conclude that $k(a^2+b^2)$ divides both $a(x_2-x_1)+b(y_2-y_1)$ and $a(y_2-y_1)-b(x_2-x_1)$. In particular, $k(a^2+b^2)$ divides

$$b\left\{a(x_2-x_1)+b(y_2-y_1)\right\} + a\left\{a(y_2-y_1)-b(x_2-x_1)\right\},$$

which simplifies to the statement that k divides y_2-y_1. Since both y_1 and y_2 are nonnegative and smaller than k, $y_1 = y_2$. Thus $k(a^2+b^2)$ divides both $a(x_2-x_1)$ and $b(x_2-x_1)$. Because a and b are relatively prime, $k(a^2+b^2)$ divides x_2-x_1, implying that $x_1 = x_2$ and ensuring that the equivalence classes are distinct.

We now demonstrate that any $x+yi$ falls into one of these equivalence classes. Since a and b are relatively prime, there exist integers s and t such that $aks+bkt = k$. Thus, after a brief calculation, $ki - (ak+bki)is - (ak+bki)t$ is found to be a real number. It follows that the complex number ki is congruent modulo $ak+bki$ to a real number in $\mathbb{Z}[i]$. This means that $[x+yi]$ coincides with $[x'+y'i]$ for some y' satisfying $0 \leq y' < k$. Finally, since the real number $k(a^2+b^2)$ is clearly in $\langle ak+bki\rangle$, we can conclude that $[x+yi] = [x''+y''i]$, with $0 \leq x'' < k(a^2+b^2)$ and $0 \leq y'' < k$. ■

Theorem 4 allows us to do the first of the two exercises posed earlier in this paper. We need only invoke the following corollary to Theorem 4:

Corollary 3. *For a and b relatively prime, the characteristic of the factor ring $\mathbb{Z}[i]/\langle ak+bki\rangle$ is $|k|(a^2+b^2)$.*

Returning to the general factorization of $a+bi$ in equation (2), we define $s_1 = \prod |\sigma_m|^{2u_m}$, $s_2 = \prod |\sigma'_m|^{2v_m}$, and $t = \prod {p_m}^{e_m}$. We observe that s_1, s_2, t, and n are nonnegative integers, that $|a+bi|^2 = s_1 s_2 \cdot t^2 \cdot 2^n$, and that s_1 divides s_2. We now state our main result.

Theorem 5. *If a and b are integers, not both zero, then with the notation just introduced and with $R_n = \mathbb{Z}[i]/\langle(1+i)^n\rangle$, the following hold:*

$$\mathbb{Z}[i]/\langle a+bi\rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \mathbb{Z}_t[i] \oplus \mathbb{Z}_{2^{n/2}}[i]$$

for even n, and

$$\mathbb{Z}[i]/\langle a+bi\rangle \cong \mathbb{Z}_{s_1} \oplus \mathbb{Z}_{s_2} \oplus \mathbb{Z}_t[i] \oplus R_n$$

for odd n.

Proof. First, by the factorization (2), we can write

$$\langle a+bi\rangle = \langle \prod {\sigma_m}^{u_m} \cdot \prod {\sigma'_m}^{v_m} \cdot \prod {p_m}^{e_m} \cdot (1+i)^n\rangle. \tag{4}$$

Since $\mathbb{Z}[i]$ is a Euclidean domain, we can apply the Euclidean algorithm to any two relatively prime elements x and y in $\mathbb{Z}[i]$ to find s and t such that $sx+ty=1$. It follows that $\langle x\rangle + \langle y\rangle = \mathbb{Z}[i]$. We can also state that $\langle x\rangle \cap \langle y\rangle = \langle xy\rangle$, and thus we can appeal to the Chinese Remainder Theorem for rings (a simple generalization of the "traditional" Chinese Remainder Theorem discussed earlier; see also [4, p. 331]) to obtain

$$\mathbb{Z}[i]/\langle xy\rangle \cong \mathbb{Z}[i]/\langle x\rangle \oplus \mathbb{Z}[i]/\langle y\rangle.$$

Applying this to (4), we arrive at

$$\mathbb{Z}[i]/\langle a+bi\rangle \cong \mathbb{Z}[i]/\langle \prod {\sigma_m}^{u_m}\rangle \oplus \mathbb{Z}[i]/\langle \prod {\sigma'_m}^{v_m}\rangle \oplus \mathbb{Z}[i]/\langle \prod {p_m}^{e_m}\rangle \oplus \mathbb{Z}[i]/\langle(1+i)^n\rangle. \tag{5}$$

We now show that (5) implies the stated result. For the first term on the right in (5), write $\prod {\sigma_m}^{u_m} = c+di$. Clearly, 2 does not divide $(c+di)$, for $2 = i^3(1+i)^2$, and likewise any prime p in $\mathbb{Z}$ such that $p \equiv 3 \pmod 4$ is also prime in $\mathbb{Z}[i]$, hence cannot divide $c+di$. Finally, for any prime q in $\mathbb{Z}$ with $q \equiv 1 \pmod 4$ we have $q = \sigma_m \cdot \sigma'_m$ for some m, whence q cannot divide $c+di$. As a result, c and d are relatively prime integers. We apply Theorem 2 to conclude that

$$\mathbb{Z}[i]/\langle \prod {\sigma_m}^{u_m}\rangle \cong \mathbb{Z}[i]/\langle c+di\rangle \cong \mathbb{Z}_{c^2+d^2} \cong \mathbb{Z}_{s_1}.$$

Similarly, the second term in (5) is isomorphic to $\mathbb{Z}_{s_2}$. Thanks to Theorem 1, the third term is $\mathbb{Z}_t[i]$. The fourth term is, by definition, R_n. For even n, R_n simplifies. Since $(1+i)^2 = 2i$, the ideal $\langle(1+i)^n\rangle$ can be rewritten as $\langle(1+i)^n\rangle = \langle(2i)^{n/2}\rangle = \langle 2^{n/2}\rangle$. Thus, $\mathbb{Z}[i]/\langle(1+i)^n\rangle = \mathbb{Z}[i]/\langle 2^{n/2}\rangle$, which by Theorem 1 is isomorphic to $\mathbb{Z}_{2^{n/2}}[i]$, as desired. ■

It is interesting to observe that for odd values of n greater than 1, R_n does not have a simple form.

Theorem 6. *For $k \geq 0$ the ring $R_{2k+1} = \mathbb{Z}[i]/\langle (1+i)^{2k+1}\rangle$ satisfies*

$$R_{2k+1} \cong \mathbb{Z}[x]/\langle 2^k x,\ 2^{k+1},\ x^2 + 2x + 2\rangle.$$

For $k > 0$, R_{2k+1} is not isomorphic to $\mathbb{Z}_c$, to $\mathbb{Z}_c[i]$, or to any direct sum of rings of these types.

Remark. For $k = 0$, the expression in Theorem 6 reduces to $\mathbb{Z}_2$. For an alternate proof of the case $k = 1$, one can combine [2, Theorem 5] with [6, Theorem 4]. Indeed, the case $k = 1$ (that is, the case of the ring R_3) gives one of only three rings of order 8 with additive group $\mathbb{Z}_4 \oplus \mathbb{Z}_2$. The others are the group $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ with standard multiplication, and that same group with trivial multiplication (see [6], [12], and [13]).

Proof of Theorem 6. First, $(1+i)^{2k+1} = (1+i)(1+i)^{2k} = (1+i)2^k i^k$. Since i^k is a unit, $\langle (1+i)^{2k+1}\rangle = \langle 2^k + 2^k i\rangle$. In view of Theorem 4 (or, alternatively, [2, Theorem 1]), we know that the elements of R_{2k+1} are the equivalence classes $[a + bi]$ with $0 \leq a < 2^{k+1}$ and $0 \leq b < 2^k$, giving 2^{2k+1} elements in all.

Let $I = \langle 2^k x,\ 2^{k+1},\ x^2 + 2x + 2\rangle$. It is straightforward to show that $\mathbb{Z}[x]/I$ consists entirely of elements (really, equivalence classes) $c + dx$ with $0 \leq c < 2^{k+1}$ and $0 \leq d < 2^k$. Hence it has the same number of elements as R_{2k+1}.

Let $\phi : \mathbb{Z}[x] \to R_{2k+1}$ be defined by $\phi(p(x)) = [p(i-1)]$. This is clearly a surjective ring homomorphism. Since $\phi(2^k x) = [2^k(i-1)] = [i(2^k + 2^k i)] = [0]$, $2^k x$ is in $\ker(\phi)$. Also, both 2^{k+1} and $x^2 + 2x + 2$ are in $\ker(\phi)$. Hence $I \subseteq \ker(\phi)$. Let $p(x)$ belong to $\ker(\phi)$. Since $x^2 + 2x + 2$ is monic, $p(x) = (x^2 + 2x + 2)q(x) + r(x)$ where both $q(x)$ and $r(x)$ are in $\mathbb{Z}[x]$ and $r(x) = r_0 + r_1(x+1)$ for integers r_0 and r_1. Since $r(x)$ lies in $\ker(\phi)$, $[r_0 + r_1 i] = [0]$, so $r_0 + r_1 i$ is a member of $\langle 2^k + 2^k i\rangle$. This allows us to write $r_0 + r_1 i = (u + vi)(2^k + 2^k i)$. By comparing the real and imaginary parts of the two sides of this equation we see easily that we can write $r(x) = u2^{k+1} + (u+v)2^k x$, which is clearly in I. Therefore $p(x)$ is in I, so $\ker(\phi) = I$, making $\mathbb{Z}[x]/I$ isomorphic to R_{2k+1}.

We now suppose that $k > 0$ and show that R_{2k+1} is not isomorphic to one of the familiar rings listed in the statement of the theorem. The polynomial factor ring $\mathbb{Z}[x]/I$ (and thus R_{2k+1}) clearly has additive group $\mathbb{Z}_{2^{k+1}} \oplus \mathbb{Z}_{2^k}$ under the map taking 1 to $(1,0)$ and x to $(0,1)$ (for R_{2k+1}, we could map 1 to $(1,0)$ and i to $(1,1)$). Thus, R_{2k+1} cannot be ring-isomorphic to either $\mathbb{Z}_c$ or $\mathbb{Z}_c[i]$, and the only direct sum of these types of rings to which it could possibly be ring-isomorphic would be $\mathbb{Z}_{2^{k+1}} \oplus \mathbb{Z}_{2^k}$. The element 1 must map to the multiplicative identity $(1,1)$, and since i has additive order 2^{k+1}, it would have a nontrivial image a in $\mathbb{Z}_{2^{k+1}}$. This would imply that $a^2 \equiv -1 \pmod{2^{k+1}}$. Since 2^{k+1} is divisible by 4, we would have $a^2 \equiv -1 \equiv 3 \pmod 4$, an obvious impossibility. ■

5. EXAMPLES.

In what follows, all isomorphisms are *ring* isomorphisms.

Example 1. Since $2 + i$ is prime in $\mathbb{Z}[i]$ (by Theorem 3), Theorem 2 or 5 gives

$$\mathbb{Z}[i]/\langle 2 + i\rangle \cong \mathbb{Z}_5,$$

the finite field of five elements (thus working again the second of the two exercises mentioned earlier).

Example 2. Also prime in $\mathbb{Z}[i]$ is $2+5i$, yielding

$$\mathbb{Z}[i]/\langle 2+5i\rangle \cong \mathbb{Z}_{29}.$$

Example 3. The ring $\mathbb{Z}[i]/\langle 11\rangle$ is isomorphic to $\mathbb{Z}_{11}[i]$, while $\mathbb{Z}[i]/\langle 13\rangle \cong \mathbb{Z}_{13}[i]$. By Fact 3, only the first is actually a field. We can also see this by noting that Theorem 5 (and the factorization $13 = i^3 \cdot (3+2i) \cdot (2+3i)$) tells us that $\mathbb{Z}[i]/\langle 13\rangle$ is also isomorphic to $\mathbb{Z}_{13} \oplus \mathbb{Z}_{13}$, which clearly has zero divisors.

Example 4. Since $6+14i$ factors as $i^3 \cdot (5+2i) \cdot (1+i)^3$,

$$\mathbb{Z}[i]/\langle 6+14i\rangle \cong \mathbb{Z}_{29} \oplus R_3.$$

Example 5. There is often more than one representation for these factor rings, as seen in Example 3 (where $\mathbb{Z}[i]/\langle 13\rangle \cong \mathbb{Z}_{13}[i] \cong \mathbb{Z}_{13} \oplus \mathbb{Z}_{13}$). To continue this line of thought, we factor $3+9i$ as $(2+i) \cdot 3 \cdot (1+i)$. Thus, Theorem 5 gives

$$\mathbb{Z}[i]/\langle 3+9i\rangle \cong \mathbb{Z}_5 \oplus \mathbb{Z}_3[i] \oplus \mathbb{Z}_2,$$

which by the Chinese Remainder Theorem is also isomorphic to $\mathbb{Z}_{10} \oplus \mathbb{Z}_3[i]$. In a similar manner, $156 = i \cdot (3+2i) \cdot (2+3i) \cdot 3 \cdot (1+i)^4$, so

$$\mathbb{Z}[i]/\langle 156\rangle \cong \mathbb{Z}_{13} \oplus \mathbb{Z}_{13} \oplus \mathbb{Z}_3[i] \oplus \mathbb{Z}_4[i],$$

which by Theorem 1 is also isomorphic to $\mathbb{Z}_{156}[i]$.

6. CONCLUSION. We would like to point out that much of this work can be done in many different rings and algebraic number fields. For example, one might consider $\mathbb{Z}[\omega]$ for $\omega = (-1+i\sqrt{3})/2$, a primitive third root of unity. This, too, is a Euclidean domain, so one still has unique factorization into primes. Much of the theory presented in this article would carry over to this new ring, including the existence of the troublesome factor rings R_n (albeit in a slightly different form). These factor rings R_n arise because in the ring of integers for any algebraic number field K of degree 2 over $\mathbb{Q}$ there is always an integer prime p such that $\langle p\rangle = A^2$ for some prime ideal A. For $\mathbb{Z}[i]$, we see that $\langle 2\rangle = \langle 1+i\rangle^2$, and in $\mathbb{Z}[\omega]$ we have $\langle 3\rangle = \langle 2+\omega\rangle^2$. These primes p are called *ramified primes*, and while this is a topic beyond the scope of this article, it is entirely appropriate for further study by interested students. A good place to start might be [11] or [14] (see also [1] or [10]). Finally, the numbers $a+b\omega$ in $\mathbb{Z}[\omega]$ are sometimes called the *Eisenstein integers* and were used by him to develop cubic reciprocity. Eisenstein's proof, as well as a more modern version, can be found in [8, chap. 9].

REFERENCES

1. H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer-Verlag, Berlin, 1993.

2. J. T. Cross, The Euler φ-function in the Gaussian integers, *Amer. Math. Monthly* **90** (1983) 518–528.

3. H. M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, New York, 1996; corrected reprint of the 1977 original.

4. J. A. Gallian, *Contemporary Abstract Algebra*, 5th ed., Houghton Mifflin, Boston, 2002.

5. C. F. Gauss, Theoria residuorum biquadraticorum. Commentatio secunda., *Comm. Soc. Reg. Sci. Gottingen* **7** (1832) 1–34; reprinted in *Werke*, Georg Olms Verlag, Hildesheim, 1973, pp. 93–148.

6. R. W. Gilmer, Jr., Finite rings having a cyclic multiplicative group of units, *Amer. J. Math.* **85** (1963) 447–452.

7. J. R. Goldman, *The Queen of Mathematics*, A K Peters, Wellesley, MA, 1998.

8. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

9. V. J. Katz, *A History of Mathematics*, HarperCollins, New York, 1993.

10. R. A. Mollin, *Quadratics*, CRC Press, Boca Raton, FL, 1996.

11. I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, New York, 1991.

12. C. Nöbauer, The numbers of small rings (2002, preprint).

13. R. Raghavendran, Finite associative rings, *Compositio Math.* **21** (1969) 195–229.

14. P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer-Verlag, New York, 2001.

15. J. L. Smith and J. A. Gallian, Factoring finite factor rings, *Math. Mag.* **58** (1985) 93–95.

16. H. M. Stark, *An Introduction to Number Theory*, MIT Press, Cambridge, 1978.