A BRIEF INVESTIGATION INTO QUOTIENT RINGS

JACOB TERKEL

Abstract. A concept nearly omnipresent in mathematics is the simultaneous tool and idea of modular arithmetic. Modular arithmetic is almost always done over the integers, and in most scenarios, cyclical arithmetic is quite intuitive. However, it is by no means the only way to examine remainder groups. Very interesting, yet elegant results arise when the ambient ring is shifted to something more complex. In this paper, we take a deep dive to answer questions about the structure of the underlying additive group of $R/(\alpha)$, as well as its group of units where R is one of the ring of Gaussian integers, the ring of Eisenstein integers, or various polynomial rings.

Contents

1. Introduction

One of the most important concepts in number theory, and in mathematics in general, is the idea of modular arithmetic. To do modular arithmetic one must first select a modulus or divisor to work under. There are many ways this can be done, but the most interesting outcome is when you restrict the domain of the modular arithmetic to a ring similar to the integers. If we hone in our focus to only the integers, under the operation of addition modulo some integer n a set of congruence classes are formed. These congruence classes constitute the cyclic group of order n. Similarly, the set of all congruence classes which

Date: January 13, 2022.

Key words and phrases. Number Theory, Algebra, Eisenstein Integers, Gaussian Integers, Remainder Groups, Polynomial Rings, Quotient Rings, Totients, Nontotients, Modular Arithmetic, Primitive Roots, Finite Abelian Groups.

have a multiplicative inverse (i.e., a congruence class which can be multiplied by to get the congruence class defined by the multiplicative identity, 1) also constitute a group under the operation multiplication mod n, this group is well known as $\mathbb{Z}_n^\times$ which has a well-known structure. However, what if instead of studying just the integers, we instead ask the same questions about other rings? For example, what is the isomorphism class of the group of units $\mathbb{Z}[i]$ mod some Gaussian integer? Which Eisenstein Integers have primitive roots? And many other questions.

In this paper, we provide answers for many of the questions of the nature described above and utilize them to further our understanding of quotient rings as a whole by making overarching connections.

2. The Gaussian Integers

The Gaussian integers are defined as follows:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

The norm of $a + bi$ is $a^2 + b^2$

Beginning with our primary question: what is the isomorphism class of $\mathbb{Z}[i]$ mod α under addition for some Gaussian integer α? We denote this group as $\mathbb{Z}[i]/(\alpha)^+$.[1] First, notice that we may assume without loss of generality that both components of α are not negative. It is easy to see that $\mathbb{Z}[i]/(\alpha) \cong \mathbb{Z}[i]/(-\alpha)$, and for conjugation, let $\phi(\beta) = \overline{\beta}$ be the function with domain $\mathbb{Z}[i]/(\alpha)$ and codomain $\mathbb{Z}[i]/(\overline{\alpha})$. See that we have

$$\phi(x + y) = \overline{x + y} = \overline{x} + \overline{y} = \phi(x) + \phi(y),$$

$$\phi(1) = \overline{1} = 1,$$

and for $x = x_1 + x_2 i$ and $y = y_1 + y_2 i$ we have that

$$\phi(xy) = \overline{(x_1 + x_2 i)(y_1 + y_2 i)} = x_1 y_1 - x_2 y_2 - (x_1 y_2 + y_1 x_2)i = (x_1 - x_2 i)(y_1 - y_2 i) = \phi(x)\phi(y).$$

This means ϕ satisfies the ring homomorphism conditions, and is a bijection (as ϕ has an inverse being conjugation as well.), meaning $\mathbb{Z}[i]/(\alpha)$, it associates, and conjugates all fall within the same ring isomorphism class.

Our first part to this answer comes from [Conrad] with the following

Theorem 2.1 (Theorem 7.14 from [Conrad])**.** *For Gaussian integer α where $\alpha \neq 0$ we have that*

$$|\mathbb{Z}[i]/(\alpha)^+| = N(\alpha)$$

where $N(\alpha)$ is the norm of α.

[1] Throughout this paper, we refer to the underlying additive group in a ring R as R^+.

With This incredibly useful information, we can prove the following

Proposition 2.2. *Let $\alpha = a + bi$ where $\alpha \neq 0$ where $\delta = \gcd(a, b)$.*

$$\mathbb{Z}[i]/(\alpha)^+ \cong \mathbb{Z}_{N(\alpha)/\delta} \times \mathbb{Z}_\delta$$

Proof. First, note that $ai \equiv b\ (\alpha)$, and $bi \equiv -a\ (\alpha)$, therefore, by the linear representation of the gcd every element of $\mathbb{Z}[i]/(\alpha)^+$ is equivalent to one with imaginary component in $\mathbb{Z}_\delta$ where $\delta = \gcd(a, b)$ over the integers. Furthermore, we have that

$$(a + bi)\left(\frac{a}{\delta} + \frac{bi}{\delta}\right) = \frac{a^2 + b^2}{\delta} \equiv 0\ (\alpha).$$

From this it follows that every element in $\mathbb{Z}[i]/(\alpha)^+$ is equivalent to a number of the form $x + yi$ for $x \in \mathbb{Z}_{N(\alpha)/\delta}$ and $y \in \mathbb{Z}_\delta$. There are exactly $N(\alpha)$ ways to represent a number like this, and by Theorem 2.1 it follows that this representation is unique for every congruence class. Furthermore, it is clear that addition is pointwise, and thus our claim follows.

■

The isomorphism is not as predictable as one may initially expect, for example the elements of order 2 in $\mathbb{Z}[i]/(4 + 2i)^+$ are $5, 2 + i$ and $7 + i$ (Seen Figure 1 as $-1 + 2i$, $2 + i$, and $1 + 3i$ respectively) which may be confusing as it is isomorphic to $\mathbb{Z}_{10} \times \mathbb{Z}_2$, but the elements of order 2 in this group are $(0, 1)$, $(5, 0)$, and $(5, 1)$.

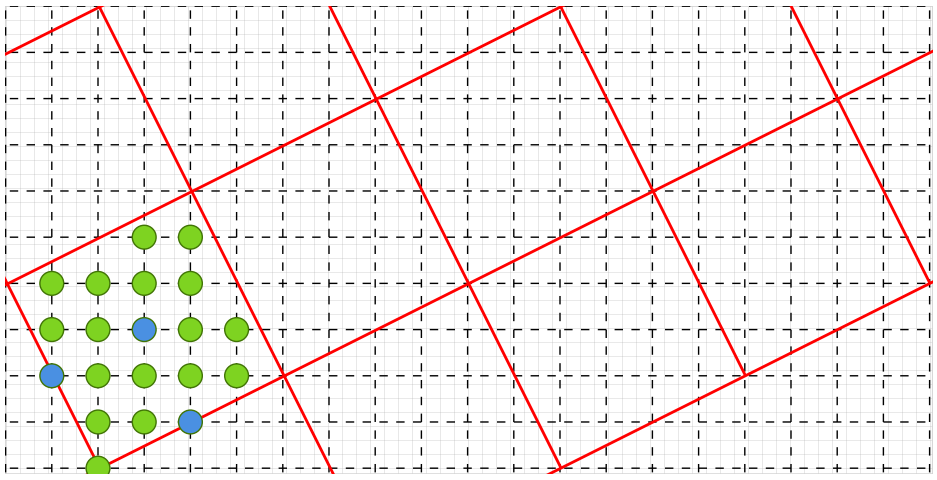

FIGURE 1. Depiction of $\mathbb{Z}[i]/(4 + 2i)^+$ with the elements of order 2 colored blue, and the other 17 colored green. The dotted grid is $\mathbb{Z}[i]$ with the horizontal axis being the value of the real component, and the vertical being the imaginary component with the bottom-most green point is $0 + 0i$.

Now we shift our focus to the multiplicative question. That is, identifying the isomorphism class of $(\mathbb{Z}[i]/(\alpha))^\times$. This was answered for all Gaussian prime powers in $\mathbb{Z}[i]$ in [Cross] the following theorems.

Theorem 2.3 (Theorems 3 and 4 from [Cross]). *Let π be a Gaussian integer prime that is not an integer prime, and has norm greater than 2. If $(\mathbb{Z}[i]/(\pi))^\times$ is the group of units in $\mathbb{Z}[i]/(\pi)$ then*

$$(\mathbb{Z}[i]/(\pi^n))^\times \cong \mathbb{Z}_{q^n-q^{n-1}}$$

where $q = N(\pi)$.

Let p be a Gaussian integer prime that is also an integer prime. We have that

$$(\mathbb{Z}[i]/(p^n))^\times \cong \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^{n-1}} \times \mathbb{Z}_{p^2-1}.$$

Theorem 2.4 (Theorems 5 and 6 from [Cross]). *If α is a Gaussian integer prime with norm 2 then*

$$(\mathbb{Z}[i]/(\alpha))^\times \cong \mathbb{Z}_1,$$
$$(\mathbb{Z}[i]/(\alpha^2))^\times \cong \mathbb{Z}_2,$$
$$(\mathbb{Z}[i]/(\alpha^3))^\times \cong \mathbb{Z}_4,$$
$$(\mathbb{Z}[i]/(\alpha^4))^\times \cong \mathbb{Z}_2 \times \mathbb{Z}_4,$$

if $n \geq 5$ is even with $n = 2m$ then

$$(\mathbb{Z}[i]/(\alpha^n))^\times \cong \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_4,$$

and if $n \geq 5$ is odd with $n = 2m+1$ then

$$(\mathbb{Z}[i]/(\alpha^n))^\times \cong \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_{2^{m-1}} \times \mathbb{Z}_4.$$

While the above theorems do not themselves yield a result regarding the group of units mod composite Gaussian integers, we can utilize a specified form of the Chinese remainder theorem for rings.

Theorem 2.5 (Chinese Remainder Theorem For Rings (Proposition 12.3.1 in [Ireland, Rosen])). *Let α and β be relatively prime elements of a ring R*

$$(R/(\alpha\beta))^\times \cong (R/(\alpha))^\times \times (R/(\beta))^\times$$

This is theorem is utilized in the following section, but in this section, it can be used to prove one direction of the complete characterization of primitive roots found in [Cross].

Theorem 2.6 (Theorem 8 from [Cross]). *The Gaussian integers with primitive roots (i.e., α such that $\mathbb{Z}[i]/(\alpha)^\times$ is cyclic) are as follows:*

- *The Gaussian integer primes that are also integer primes*

- *non-integer Gaussian integer primes with norm greater than 2, and all of their positive powers*
- $1 + i$
- 2
- *any of the above multiplied by* $1 + i$

With this, we have answered a large portion of the central questions posed about this ring.

But, I still have a tangential question that arises from noticing a pattern in Cross's results. It is easily seen that with the exception of the first two equations in Theorem 2.4 that the order of $\mathbb{Z}[i]/(\alpha)^\times$ for all prime powers α is divisible by 4. Thus, by Theorem 2.5 if $n > 2$ is 2 mod 4, then no group of units mod any Gaussian integer has size n. This invites us to ask the following question.

Which even natural numbers are not the order of the group of units for any Gaussian integer?

We call these integers Gaussian nontotients. In addition to the aforementioned 2 mod 4 case, there are Gaussian nontotients that are 0 mod 4 as well. We can develop an entire class of nontotient numbers 0 mod 4.

Proposition 2.7. *Let $r \neq 5$ be a prime 1 mod 4 and $m = 4r$. If $m + 1$ is not prime, then m is nontotient.*

Proof. Let r be a prime congruent to 1 mod 4. Let $m = 4r$. See that m's only factorizations are m, $2 \cdot 2r$, $2 \cdot 2 \cdot r$, and $4 \cdot r$. Furthermore, if m is totient, then in at least one of its factorizations every factor must be totient as well. But r and $2r$ cannot be totient as r is odd and $2r$ is 2 mod 4. Therefore m is totient if and only if it takes one of the following two forms

$$m = q^n - q^{n-1}$$

for some integer prime q equivalent 1 mod 4, or

$$m = p^{2n-2}(p^2 - 1)$$

for some integer prime p equivalent 3 mod 4.

The latter is not a valid option unless $n = 1$, which gives us the modified criteria of

$$m = q^{n-1}(q - 1)$$

for some integer prime q 1 mod 4, or

$$m = (p + 1)(p - 1)$$

for some integer prime p 3 mod 4.

However, the latter is divisible by 8, but m is not leaving us with the sole criteria of

$$m = q^{n-1}(q-1)$$

Which could be valid in two scenarios

(A) $n = 1$

(B) $q = 5, n = 2$

The second scenario gives only the very specific $m = 20$, and the first scenario will work if and only if $m + 1$ is also prime. This proves our claim. ∎

To see the above proposition in action, look no further than 68, it is equal to four times 17, a prime, and 69 is not prime, from this it should follow that 68 is Gaussian nontotient, and sure enough, this can be easily verified empirically.

3. The Eisenstein Integers

Similarly to the Gaussian Integers, we have the ring $\mathbb{Z}[\omega]$, where

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\}$$

and $\omega = \frac{-1+\sqrt{-3}}{2}$. These are called the Eisenstein integers. The norm of $a+b\omega$ is a^2-ab+b^2. Similar to the Gaussian integers we need only consider when α has both components non-negative when examining $\mathbb{Z}[\omega]/(\alpha)$. The justification is nearly identical to the one for Gaussian integers, so we will not repeat it here.

We begin again by considering the group of Eisenstein under addition mod α, $\mathbb{Z}[\omega]/(\alpha)^+$.

In a near-identical fashion to the Gaussian Integers, the following statement can be proven.

Proposition 3.1. *For $\alpha \in \mathbb{Z}[\omega]$ with $\alpha = a + b\omega$, $N(\alpha) = a^2 + b^2 - ab$, and $\delta = \gcd(a, b)$ over the integers.*

$$\mathbb{Z}[\omega]/(\alpha)^+ \cong \mathbb{Z}_{N(\alpha)/\delta} \times \mathbb{Z}_\delta$$

Now, we shift our focus to the same question regarding the group of units in these quotient rings. This was partially answered [Gullerud, Mbirika] with the following theorem.

Theorem 3.2 (Theorem 4.3 and Theorem 5.3 from [Gullerud, Mbirika])**.** *If p is an integer prime that is also an Eisenstein prime then*

$$|(\mathbb{Z}[\omega]/(p^n))^\times| = p^{2n-2}(p^2-1).$$

If β is an Eisenstein prime with norm 3 then

$$|(\mathbb{Z}[\omega]/(\beta^n))^\times| = 2 \cdot 3^{n-1}.$$

And if π is an Eisenstein prime that has norm greater than 3, and is not an integer prime then

$$(\mathbb{Z}[\omega]/(\pi^n))^\times \cong \mathbb{Z}_{q^n-q^{n-1}}$$

where $q = N(\pi)$.

While this does result in the size of the group of units of $\mathbb{Z}[\omega]/(\alpha)$ when combined with Theorem 2.5 for all $\alpha \in \mathbb{Z}[\omega]$ it does not yield the isomorphism class for $\mathbb{Z}[\omega]/(\alpha)^\times$ for all α.

Remark 3.3. Using a computer program, I determined that all integer Eisenstein primes below 100 have a primitive root, and thus are cyclic

This leads me to conjecture the following.

Conjecture 3.4. *If p is an integer prime as well as an Eisenstein prime, then $(\mathbb{Z}[\omega]/(p))^\times$ is cyclic.*

However, even this would still leave the remaining powers of p, which leaves us with the unanswered question:

Question 3.5. What is the group structure of

$$(\mathbb{Z}[\omega]/(p^n))^\times$$

for prime p congruent to 2 mod 3, and natural n.

Moving on, in [Gullerud, Mbirika] the authors ask the following question:

Question 3.6 (Question 6.2 in [Gullerud, Mbirika])**.** What positive even integers are Eisenstein nontotient?

Where "Eisenstein nontotient" is this chapter's analog to the previous chapter's "Gaussian nontotient."

We can easily prove the following in regards to this question.

Proposition 3.7. *If $n > 2$ is not divisible by 3 then n is Eisenstein nontotient.*

Proof. If α is divisible by an Eisenstein prime that is also an integer, then by the Chinese Remainder Theorem for rings and Theorem 3.2 we have $|\mathbb{Z}[\omega]/(\alpha)^\times|$ is divisible by 3 (as p^2 is always 1 mod 3). The same can be said if α is divisible by β^2 where β is some Eisenstein prime with norm 3 or π where π is an Eisenstein prime with prime norm 1 mod 3 using the same Theorems.

Therefore, we have that every Eisenstein totient is divisible by 3, with the exception of the totient of Eisenstein primes with norm 3, which has an Eisenstein totient of 2, proving our claim ∎

This completes the section on Eisenstein integers, and while not as well understood as its Gaussian counterpart, it has many parallels with it which seem to suggest a greater connection between these rings.

4. Polynomial Rings

This section will be quite different from the others. Let $\mathbb{F}[X]$ denote the ring of polynomials with coefficients in a field $\mathbb{F}$. Let the $N(P)$ be the norm for this ring where $N(P)$ is equal to the degree of P We have $N(PQ) = N(P) + N(Q)$. As stated in [Smith 1] and [Smith 2], $\mathbb{F}[X]$ also has a division algorithm and unique factorization.

It takes little effort to conjure a proof for an equivalence like $\mathbb{Z}_p[X]/(X)^+ \cong \mathbb{Z}_p$, or even more generally $\mathbb{Z}_p[X]/(X^k)^+ \cong \mathbb{Z}_p^k$.

However, what if select our modulus to be a non-monomial polynomial? Well in that case we have the following.

Proposition 4.1.

$$\mathbb{Z}_p[X]/(P(X))^+ \cong \mathbb{Z}_p^{\deg(P(X))}$$

Proof. First, we show that $|\mathbb{Z}_p[X]/(P(X))^+| = \deg(P(X))$. This is easily proven by seeing that for any polynomial $Q(X)$ with degree d where $\deg(P(X)) \leq d$ that there is some polynomial $R(X)$ with degree less than d such that

$$Q(X) - X^{d-\deg(P(X))}P(X) = R(X)$$

Which in turn supplies us with

$$Q(X) \equiv R(X) \ (P(X), p).$$

This can be repeated until we have a polynomial with a degree less than $\deg(P(X))$. It is also easily seen that no polynomial with degree less than $\deg(P(X))$ can be a multiple of $P(X)$, meaning that the set of polynomials with degree less than $\deg(P(X))$ are exactly the elements of $\mathbb{Z}_p[X]/(P(X))^+$, of which there are $p^{\deg(P(X))}$.

However, note that for any element A in $\mathbb{Z}_p[X]/(P(X))^+$ we have that $p \cdot A \equiv 0$, meaning every element of $\mathbb{Z}_p[X]/(P(X))^+$ has order that divides p, however, because p is prime that means either that A is the identity element, or it has order p, implying that $\mathbb{Z}_p[X]/(P(X))^+ \cong \mathbb{Z}_p^{\deg(k)}$.

■

However, what about the group of units? Well, under multiplication, we have the following.

Proposition 4.2.

$$|(\mathbb{Z}_p[X]/(X^2))^\times| = p^2 - p$$

Proof. Let U be some unit in $\mathbb{Z}_p[X]/(X^2)$ where $U \equiv ax + b$. Notice that b cannot be 0, as no multiple of x is congruent to 1. Otherwise, take the following steps

Because b is some non-zero integer, it has a multiplicative inverse, and this means we have the following

$$(ax + b)(b^{-1} - ab^{-2}x) \equiv ab^{-1}x - a^2b^{-2}x^2 + 1 - ab^{-1}x \equiv -a^2b^{-2}x^2 + 1 \equiv 1 \ (X^2, p)$$

Therefore, every element of $\mathbb{Z}_p[X]/(X^2)$ with non-zero b has an inverse, meaning we have proven our claim.

■

This result allows us the extrapolate the following conclusion from the fundamental theorem of finite Abelian groups.

Corollary 4.3. *If p is some prime such that $p - 1$ is square free then $(\mathbb{Z}_p[X]/(X^2))^\times$ has a primitive root.*

However, this doesn't hold just for primes of this type, but every positive integer prime. Furthermore, we can identify every such primitive root

Theorem 4.4. *For prime p, an element $a + bx \in (\mathbb{Z}_p[X]/(X^2))^\times$ is a primitive root if and only if $a \neq 0$ and b is a primitive root in $\mathbb{Z}_p$.*

Proof. Let p be an integer prime Because p is prime, there is a primitive root in $\mathbb{Z}_p$, let r be one such primitive root. Now, consider the following expression.

$$(ax + r)^k \mod x^2, p$$

See that

$$(ax + r)^k \equiv kar^{k-1}x + r^k \mod x^2, p$$

Because r is a primitive root in $\mathbb{Z}_p$, we know that $r^k \equiv 1$ if and only if k is a multiple of $p - 1$. Furthermore, because r^{k-1} is never 0 mod p, $kar^{k-1}x \equiv 0$ if and only if k is a multiple of p or $a = 0$. However, if $a = 0$ then $ax + r$ would clearly not be a primitive root of $(\mathbb{Z}_p[X]/(X^2))^\times$. Therefore, we have that $|ax + r| = (p, p - 1) = p^2 - p$ for non-zero a and primitive root r in $\mathbb{Z}_p$.

Now, see that if r were not a primitive root of $\mathbb{Z}_p$ then $ax + r$ could not be a primitive root either, as $(ax + r)^x$ could not take on every value of $(\mathbb{Z}_p[X]/(X^2))^\times$.

Thus, for any element $ax + r \in (\mathbb{Z}_p[X]/(X^2))^\times$ we have that $ax + r$ is a primitive root if and only if r is a primitive root in $\mathbb{Z}_p$ and $a \neq 0$ ■

One implication of this is the following.

Corollary 4.5. *The number of primitive roots in* $(\mathbb{Z}_p[X]/(X^2))^\times$ *is equal to*

$$\varphi(p) \cdot \varphi(\varphi(p)) = (p-1) \cdot \varphi(p-1)$$

where φ *is the integer Euler totient function.*

The question of nontotients in these rings is much more complex, as the multiplicative structure in these polynomial groups is much harder to discern, but I do plan to look into this problem in the future.

5. Conclusion

With this investigation at its end, there are some surprising discoveries and observations that have arisen. For example, the very obvious parallels between the Gaussian and Eisenstein integers. In addition, we were also able to find a set of necessary and sufficient conditions for an element of $(\mathbb{Z}_p[X]/(X^2))^\times$ to be a primitive root, as well as other facts regarding remainder groups in polynomial quotient rings.

In the future, I would like to do more work on questions related to remainder groups. Specifically, Gaussian nontotients, and remainder groups in other classes of polynomial rings.

References

[Gullerud, Mbirika] Gullerud, E. & Mbirika, A. 2019, arXiv:1902.03483

[Cross] Cross, J. T. (1983). The Euler ϕ-Function in the Gaussian Integers.The American Mathematical Monthly, 90(8), 518–528. https://doi.org/10.2307/2322785

[Conrad] The Gaussian Integers Keith Conrad https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf

[Ireland, Rosen] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics (1982) Springer.

[Smith 1] Karen E. Smith 2018 UM Math Dept http://www.math.lsa.umich.edu/ kesmith/QuotientPolynomialRings-ANSWERS.pdf

[Smith 2] Karen E. Smith 2018 UM Math Dept http://www.math.lsa.umich.edu/ kesmith/MorePolynomialRingsOverField-ANSWERS.pdf

Department of Mathematics, Gettysburg College, Gettysburg, PA 17325, USA
Email address: terkja01@gettysburg.edu