Math 350, Sections 01,03, Fall 2021

Optional Handout: A Theorem on Norms

Problem 17.18 in Saracino, which I considered but did not actually assign, asks you to count the number of elements in $\mathbb{Z}[i]/\langle 2+2i\rangle$. The number of elements is 8. Here is one way to prove that.

Let $I = \langle 2+2i\rangle$. We will show that

$$0+I, 1+I, 2+I, 3+I, i+I, 1+i+I, 2+i+I, 3+i+I$$

are (eight) **distinct** cosets, and that together they cover all of $\mathbb{Z}[i]$.

First, we claim that I is precisely the set

$$I = \{2m+2ni : m, n \in \mathbb{Z} \text{ are both odd or both even}\}.$$

For the $\subseteq$ direction, given any $a+bi \in \mathbb{Z}[i]$, the corresponding element of I is $(a+bi)(2+2i) = 2(a-b)+2(a+b)i$. Letting $m = a-b$ and $n = a+b$, clearly m and n are either both odd or both even, as desired. For the $\supseteq$ direction, given m and n both odd or both even, let $a = (n+m)/2$ and $b = (n-m)/2$, which are both integers. Then $2m+2ni = (a+bi)(2+2i)$; the claim is proven.

Next, we observe that each $x+iy \in \mathbb{Z}[i]$ lies in one of the eight cosets listed above. Indeed, by adding an integer multiple of $2+2i$, we can change the y to either a 1 or 0, so that $x+iy$ lies in the same coset as n or as $n+i$, for some integer $n \in \mathbb{Z}$. Then, since $4 = (1-i)(2+2i) \in I$, we can add an integer multiple of 4 to see that $n+i$, and therefore also $x+iy$, lies in the same coset as either k or $k+i$, where k is one of $0, 1, 2, 3$. Thus, $\mathbb{Z}[i]$ is completely covered by the eight cosets above, so that those eight cosets do indeed comprise all elements of $\mathbb{Z}[i]/I$.

It only remains to show that the eight cosets are distinct. However, any two distinct cosets representatives from the list of eight above differ by an element $a+bi$, where either $b = 1$ and a is one of $0, 1, 2, 3$, or else $b = 0$ and a is one of $1, 2, 3$. The only case where both a and b are even is $2+0i$; but $2 = 2 \cdot 1$ and $0 = 2 \cdot 0$, and 1 and 0 do not have the same parity. By the claim, then, any such $a+bi$ is not in I. Thus, the eight cosets are indeed distinct, because any two of their representatives differ by an element not in I. QED

I imagine that's roughly the kind of argument Saracino had in mind when he wrote that problem. However, it turns out there's nothing special about the ideal $\langle 2+2i\rangle$ except that one can pull off an ad hoc proof as above. Far more generally, we have the following theorem.

Theorem. Let $a+bi \in \mathbb{Z}[i] \setminus \{0\}$ be a nonzero Gaussian integer, and let $I = \langle a+bi\rangle$ be the principal ideal in $\mathbb{Z}[i]$ that it generates.

Then the quotient ring $\mathbb{Z}[i]/I$ has exactly a^2+b^2 elements.

That is, the norm function $N(a+bi) = a^2+b^2$ counts the number of elements in the quotient of $\mathbb{Z}[i]$ by the corresponding principal ideal.

There are a number of ways to prove this theorem. One way is to prove it using the ideas of Section 21. Even though we haven't gotten to that section, we have a lot of the terminology already. The strategy is first to prove the Theorem for irreducible elements $a + bi$. [For an integral domain R, we say $a \in R$ is *irreducible* if for any $x, y \in R$ such that $a = xy$, we have that either x or y is a unit. That is, irreducible elements are the generalizations of prime numbers.]

It turns out that there are three types of irreducibles in $\mathbb{Z}[i]$, classified by their norm. First, $1 + i$ is an irreducible element; so are all of its unit multiples — that is, $1 + i$, $1 - i$, $-1 + i$, and $-1 - i$. (These are precisely the elements of norm 2.) Second, if $p \in \mathbb{Z}$ is an odd prime number satisfying $p \equiv 3 \pmod 4$, then p is still an irreducible when viewed as an element of $\mathbb{Z}[i]$; of course, then, so are $-p$, pi, and $-pi$. (There are precisely the elements of norm p^2, for a prime congruent to 3 mod 4.) The remaining irreducibles are those elements of the form $a+bi$ for which $a^2+b^2 = p$ is an odd prime satisfying $p \equiv 1 \pmod 4$; they are precisely the elements of norm p, for a prime p congruent to 1 mod 4.

For example, $1 + 2i$ is an irreducible in $\mathbb{Z}[i]$ (because its norm is $1^2 + 2^2 = 5$, which is an integer prime congruent to 1 modulo 4). And it's easy to check that $0, 1, 2, 3, 4$ (viewed as elements of $\mathbb{Z}[i]$) are all in different cosets of $I = \langle 1 + 2i \rangle$, once you prove that $I \cap \mathbb{Z} = 5\mathbb{Z}$. Furthermore, some similar messing around shows that anything in $\mathbb{Z}[i]$ is in the same coset as one of $0, 1, 2, 3, 4$. So $\mathbb{Z}[i]/I$ has exactly 5 elements. The proof for any other irreducible $a + bi$ where $a^2 + b^2 = p$ is a prime congruent to 1 modulo 4 is similar. It's even easier to show (by exactly the same strategy) that $\mathbb{Z}[i]/\langle 1 + i \rangle$ has exactly $2 = 1^2 + 1^2$ elements. Meanwhile, if $p \equiv 3 \pmod 4$ is a prime integer, then $N(p) = p^2$, and it's not hard to check that $I = \{px + pyi : x, y \in \mathbb{Z}\}$, so that the p^2 coset representatives of the form $a + bi$ with $a, b \in \{0, 1, \ldots, p-1\}$ will do the trick. Thus, assuming you believe all that, we have verified that the Theorem is true if $a + bi$ is irreducible.

It also turns out that, just as is true in $\mathbb{Z}$, any element of $\mathbb{Z}[i]$ can be written as a product of irreducibles. So to extend the Theorem to arbitrary (e.g., non-irreducible) $a + bi$ is "just" a matter of proving that the function taking $a + bi$ to the order of $\mathbb{Z}[i]/\langle a + bi \rangle$ is also multiplicative. See me if you're curious about that but can't figure out the proof.

Actually, we can generalize the previous theorem *even further*.

Theorem. Let $d \in \mathbb{Z}$ be an integer that is not a perfect square, and let $R = \mathbb{Z}[\sqrt{d}]$. Let $a + b\sqrt{d} \in R \setminus \{0\}$ be a nonzero element of R, and let $I = \langle a + b\sqrt{d} \rangle$ be the principal ideal in R that it generates. Then the quotient ring R/I has exactly $|a^2 - db^2|$ elements.

What's going on here is that, just as we had $N : \mathbb{Z}[i] \to \mathbb{Z}$ given by $N(a + bi) = a^2 + b^2$, we can more generally define a "norm" on $\mathbb{Z}[\sqrt{d}]$ by $N(a + b\sqrt{d}) = a^2 - db^2$. Thus, once again, *even if the ring does not have nice factorization properties*, the absolute value of the norm (which is always the norm itself if d is negative) counts the number of elements in the quotient ring formed by modding out by the associated principal ideal.

FYI: The theorem above can be made even *more* general, to apply to any *order* in a *number field* (whatever that means). See, for example, Exercises 7.14 and 7.15 of David Cox's book, *Primes of the Form* $x^2 + ny^2$.