Elementary Number Theory

Math 175, Section 30, Autumn 2010

Shmuel Weinberger (`shmuel@math.uchicago.edu`)

Tom Church (`tchurch@math.uchicago.edu`)

`www.math.uchicago.edu/~tchurch/teaching/175/`

Homework 5

Due Tuesday, November 9 in class.

Recall that given $x, y \in \mathbb{Z}[i]$, we say that $y|x$ if there exists $z \in \mathbb{Z}[i]$ such that $x = yz$.

Definition HW5.1. Fix a nonzero element $x \in \mathbb{Z}[i]$. We say that two elements y and z are *congruent modulo* x and write $y \equiv z \pmod{x}$ if and only if $x \mid (y - z)$.

Congruence modulo x is an equivalence relation.[1]

Definition HW5.2. For $y \in \mathbb{Z}[i]$, the *residue class of* y *modulo* x is the set of all elements $z \in \mathbb{Z}[i]$ which are congruent to y modulo x:

$$[y] = \left\{ z \in \mathbb{Z}[i] \middle| y \equiv z \pmod{x} \right\}$$

Question 1. Prove that for any nonzero $x \in \mathbb{Z}[i]$, there are only finitely many different residue classes modulo x.

Question 2. If $x = a + bi$, how many residue classes are there modulo x?

Definition HW5.3. Fix a nonzero element $x \in \mathbb{Z}[i]$. We define the number system $\mathbb{Z}[i]/(x)$ to be the set of residue classes modulo x. We define addition and multiplication in $\mathbb{Z}[i]/(x)$ as follows:

$$[y] + [z] = [y + z] \qquad \text{for } y, z \in \mathbb{Z}$$
$$[y] \cdot [z] = [y \cdot z] \qquad \text{for } y, z \in \mathbb{Z}$$

These operations are well-defined and make $\mathbb{Z}[i]/(x)$ into a commutative ring with identity; the additive identity is $[0]$, and the multiplicative identity is $[1]$.[1]

[1] You may assume this without proving it.

(Thus Question 1 asked you to prove that the ring $\mathbb{Z}[i]/(x)$ is finite, and Question 2 asked you to find its cardinality $\left|\mathbb{Z}[i]/(x)\right|$.)

Question 3. The following questions should be answered by concrete computations. For example, if one of these rings is not a field, you should give an explicit example of an nonzero element and a justification of why it does not have a multiplicative inverse.

a) For $x = 2$, is $\mathbb{Z}[i]/(x)$ a field?

b) For $y = 3$, is $\mathbb{Z}[i]/(y)$ a field?

c) For $z = 5$, is $\mathbb{Z}[i]/(z)$ a field?

In any commutative ring with identity, there are two related kinds of elements: *irreducibles* and *primes*. For $\mathbb{Z}$ and $\mathbb{Z}[i]$ these notions coincide and the terms can be (and are) used interchangably, but it is good to be familiar with the right general terminology.

Definition HW5.4. Let R be a commutative ring with identity.
An element $x \in R$ is called *prime* if

$$x|ab \quad \text{implies that either} \quad x|a \;\text{ or }\; x|b.$$

An element $x \in R$ is called *irreducible* if

$$d|x \quad \text{implies that either} \quad d|1 \;\text{ or }\; x|d.$$

Question 4. We proved in Question HW3.1(c) that irreducible elements of $\mathbb{Z}[i]$ are prime. Prove the converse: if $x \in \mathbb{Z}[i]$ is prime, then x is irreducible.

Question 5. Given $x \in \mathbb{Z}[i]$, prove that $\mathbb{Z}[i]/(x)$ is a field if and only if x is a prime in $\mathbb{Z}[i]$.

Question 6. Prove that 2 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but 2 is not a prime in $\mathbb{Z}[\sqrt{-5}]$.
(So in general, the notions of "irreducible" and "prime" can be different.)