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 1

Due Tuesday, October 12 in class.

Question 1. The set $\mathbb{Z}[i]$ is the collection of formal expressions of the form $a + bi$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$. In this context, the plus sign and the symbol i are inert symbols with no meaning. For example, $2 + 0i$, $3 + 2i$, and $-2 + 7i$ are all elements of $\mathbb{Z}[i]$.

If $x \in \mathbb{Z}[i]$ and $y \in \mathbb{Z}[i]$ are two elements of $\mathbb{Z}[i]$, we define the operation of addition as follows:

$$\text{if } x = a + bi \quad \text{and} \quad y = c + di, \quad \text{then} \qquad x + y = (a + c) + (b + d)i$$

For example:

$$\begin{aligned}(2 + 0i) + (3 + 2i) &= 5 + 2i \\ (3 + 2i) + (-2 + 7i) &= 1 + 9i \\ (2 + 0i) + (-2 + 7i) &= 0 + 7i\end{aligned}$$

a) Prove that the addition operation on $\mathbb{Z}[i]$ is associative (that is, that $\mathbb{Z}[i]$ satisfies Axiom A2).

b) What is the additive identity in $\mathbb{Z}[i]$? Prove that the element you found satisfies Axiom A4: for any $x \in \mathbb{Z}[i]$, we have $x + 0 = x$ and $0 + x = x$.

c) What is the additive inverse of $3 + 4i$? In general, if $x = a + bi$, what is the additive inverse of x? Prove that your answer satisfies Axiom A5: $x + (-x) = 0$.

For $x \in \mathbb{Z}[i]$ and $y \in \mathbb{Z}[i]$, we define the operation of multiplication as follows:

$$\text{if } x = a + bi \text{ and } y = c + di, \text{ then } x \cdot y = (ac - bd) + (bc + ad)i$$

For example:

$$\begin{aligned}
(3+2i)\cdot(1+4i) &= (3-8) &&+ (2+12)i &&= -5+14i \\
(2+0i)\cdot(3+2i) &= (6-0) &&+ (0+4)i &&= 6+4i \\
(1-2i)\cdot(-2+5i) &= (-2+10) &&+ (4+5)i &&= 8+9i
\end{aligned}$$

d) Prove that the multiplication operation on $\mathbb{Z}[i]$ is associative (that is, $\mathbb{Z}[i]$ satisfies Axiom M2).

e) What is the multiplicative identity in $\mathbb{Z}[i]$? Prove that the element you found satisfies Axiom M4: for any $x \in \mathbb{Z}[i]$, we have $x \cdot 1 = x$ and $1 \cdot x = x$.

g) Prove that multiplication distributes over addition: if $x = a + bi$, $y = c + di$, and $z = e + fi$ are elements of $\mathbb{Z}[i]$, prove that

$$x \cdot (y + z) = x \cdot y \; + \; x \cdot z$$

Question 2. The set $\mathbb{Q}[i]$ is the collection of formal expressions of the form $a + bi$, where $a \in \mathbb{Q}$ and $b \in \mathbb{Q}$. (Recall that $\mathbb{Q}$ is the set of rational numbers.) For example, $\frac{1}{2} + 0i$, $3 + 2i$, and $-2 + \frac{7}{3}i$ are all elements of $\mathbb{Z}[i]$. We define addition and multiplication on $\mathbb{Q}[i]$ by the same formulas as before: if $x = a + bi$ and $y = c + di$, then

$$x + y = (a + c) + (b + d)i \qquad\qquad x \cdot y = (ac - bd) + (bc + ad)i$$

a) First, you should check that your proofs for Question 1(a–g) apply to $\mathbb{Q}[i]$ as well. You do not need to write anything for this part.

b) What is the multiplicative inverse of $3 + 4i$?

c) Which elements of $\mathbb{Q}[i]$ have a multiplicative inverse? Prove your answer is correct. (You may want to return to this after Question 3.)

Question 3. If $a + bi$ is an element of $\mathbb{Z}[i]$, its *norm* $N(a + bi) \in \mathbb{Z}$ is defined to be:

$$N(a + bi) = a^2 + b^2$$

If $a + bi$ is an element of $\mathbb{Q}[i]$, we define its norm $N(a + bi) \in \mathbb{Q}$ by the same formula: $N(a + bi) = a^2 + b^2$.

a) Find all elements $x \in \mathbb{Z}[i]$ with $N(x) = 1$.

b) Find all elements $x \in \mathbb{Z}[i]$ with $N(x) = 2$.

c) Prove that for any $x \in \mathbb{Z}[i]$ and $y \in \mathbb{Z}[i]$ we have

$$N(x \cdot y) = N(x) \cdot N(y).$$

(You should check that your proof also works for $\mathbb{Q}[i]$; you do not need to write the proof again.)