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 3

Due Tuesday, October 26 in class.

Recall that $\mathbb{Z}[i]$ is the number system consisting of formal expressions of the form $a + bi$ where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$.

Definition HW.3.1. Given $x, y \in \mathbb{Z}[i]$ and $d \in \mathbb{Z}[i]$, we say that d is *a GCD of x and y* if:

- $d|x$ and $d|y$, and [d is a common divisor]
- if $e|x$ and $e|y$, then $e|d$. [every common divisor divides d]

The reason we say "a GCD" is that if d is a GCD of x and y, then so are $-d$, id, and $-id$. [compare with Theorem 1.30]

Question 1.

a) Let a, b be nonzero elements of $\mathbb{Z}[i]$. If we apply the Division Algorithm sequentially:

$$\begin{aligned} a &= bq_1 + r_1 & 0 < N(r_1) < N(b) \\ b &= r_1q_2 + r_2 & 0 < N(r_2) < N(r_1) \\ r_1 &= r_2q_3 + r_3 & 0 < N(r_3) < N(r_2) \\ &\vdots \\ r_{k-2} &= r_{k-1}q_k + r_k & 0 < N(r_k) < N(r_{k-1}) \\ r_{k-1} &= r_kq_{k+1} \end{aligned}$$

then r_k is a GCD of a and b. [compare with Theorem 1.37]

b) Prove that if d is a GCD of x and y, then we can write $d = ax + by$ for some $a, b \in \mathbb{Z}[i]$. [compare with Theorem 1.31]

Definition HW.3.2. Given $x, y \in \mathbb{Z}[i]$, we say that x and y are relatively prime if 1 is a GCD of x and y. [compare with Definition 1.34]

Recall that x is *associated* to y if $x|y$ and $y|x$ (you proved this means $x = \pm y$ or $\pm iy$).

Definition HW.3.3. A nonzero element $x \in \mathbb{Z}[i]$ is called *irreducible* if every divisor of x is associated to 1 or associated to x. [compare with Definition 2.1]

Definition HW.3.4. A nonzero element $x \in \mathbb{Z}[i]$ is called a *unit* if it is associated to 1.

c) Let x be an irreducible element of $\mathbb{Z}[i]$. Prove that if $x|ab$, then $x|a$ or $x|b$. (Hint: show that if $x \nmid a$, then x and a are relatively prime.) [compare with Theorem 2.4]

d) Prove that every nonzero element of $\mathbb{Z}[i]$ which is not a unit has at least one irreducible factor. [compare with Theorem 2.2]

e) Prove that every nonzero element $a \in \mathbb{Z}[i]$ can be factored into a product of irreducible elements times a unit: $a = u \cdot x_1 \cdots x_k$, where u is a unit and each x_i is irreducible. [compare with Theorem 2.3]

f) **Unique factorization in** $\mathbb{Z}[i]$. Prove that every nonzero element $a \in \mathbb{Z}[i]$ can be factored into a product of irreducibles in a unique way, up to units and the order of the factors.

   In other words, if $a = u \cdot x_1 \cdots x_k$ and $a = v \cdot y_1 \cdots y_\ell$ are two factorizations of a as in part e), then $k = \ell$ and there is a reordering of the factors so that x_i is associated to y_i for all $i = 1, 2, \ldots, k$. [compare with Theorem 2.5]

Question 2. We define the number system $\mathbb{Z}[\sqrt{-5}]$ to be the collection of formal expressions of the form $a + b\sqrt{-5}$, where $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$. For example, $2 + 0\sqrt{-5}$, $3 + 2\sqrt{-5}$, and $-2 + 7\sqrt{-5}$ are all elements of $\mathbb{Z}[\sqrt{-5}]$.

If $x \in \mathbb{Z}[\sqrt{-5}]$ and $y \in \mathbb{Z}[\sqrt{-5}]$ are two elements of $\mathbb{Z}[\sqrt{-5}]$, we define addition and multiplication as follows:

$$\text{if } x = a + b\sqrt{-5} \quad \text{and} \quad y = c + d\sqrt{-5}, \quad \text{then} \qquad x + y = (a + c) + (b + d)\sqrt{-5}$$

$$\text{if } x = a + b\sqrt{-5} \quad \text{and} \quad y = c + d\sqrt{-5}, \quad \text{then} \qquad x \cdot y = (ac - 5bd) + (ad + bc)\sqrt{-5}$$

These operations are commutative, associative, and distribute (they satisfy all the axioms up through Axiom D). The additive identity is $0 = 0 + 0\sqrt{-5}$, and the multiplicative identity is $1 = 1 + 0\sqrt{-5}$.

a) Come up with a definition of a function $N \colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ with the following properties.

   I. $N(0) = 0$

   II. $N(1) = 1$ and $N(-1) = 1$

   III. $N(x) \neq 1$ for some nonzero x (just to rule out silly answers)

   IV. $N(x \cdot y) = N(x) \cdot N(y)$ for any $x, y \in \mathbb{Z}[\sqrt{-5}]$ (this is the important condition)

b) One way to factor $6 = 6 + 0\sqrt{-5}$ into irreducibles is

$$6 = 2 \cdot 3.$$

   Find a <u>different</u> way to factor 6 as a product of irreducibles,[1] showing that ***we do not have unique factorization*** in $\mathbb{Z}[\sqrt{-5}]$.

[1] Writing it as $6 = (-2)(-3)$ does not count as "different".