# Section 3.8 Exercises
# Herstein's Topics In Algebra

Spencer T. Parkin

April 18, 2016

## Thoughts

I had some trouble with a part of the proof of Theorem 3.8.1. For integers $a$ and $n$, the division algorithm can give us integers $t$ and $r$ such that $a = tn+r$ with $|r| < |n|$, but Herstein asserts that such can be found where $|r| \leq |n|/2$. Well, what about $a = 40$ and $n = 7$? Here, $t = 5$ and $r = 5$, and clearly $5 \leq 7/2$ does not hold.

## Problem 1

Find all the units in $J[i]$.

In the field of complex numbers $\mathbb{C}$, multiplicative inverses are unique. That is, letting $a + bi \in \mathbb{C}$, we have

$$(a+bi)^{-1} = \frac{a-bi}{a^2+b^2}.$$

Now since $\mathbb{C}$ contains $J[i]$, this too must hold true. Thus, if $x = a+bi \in J[i]$ is a unit, we must have $d(x)|\Re(x)$ and $d(x)|\Im(x)$. But this is only possible for $x = 1, -1, i, -i$.

## Problem 2

If $a + bi$ is not a unit of $J[i]$ prove that $a^2 + b^2 > 1$.

Perhaps Herstein forgot to exclude $0 + 0i$.

If $a$ and $b$ are non-zero, then by Problem 1, they're not units, and $d(a + bi) > 1$. If $a = 0$, then by Problem 1, $|b| > 1$. Similarly, if $b = 0$, then $|a| > 1$.

# Problem 3

Find the greatest common divisor in $J[i]$ of $3 + 4i$ and $4 - 3i$, then $11 + 7i$ and $18 - i$.

Let's consider for a moment the general problem of finding $\gcd(a+bi, c+di)$. Since $J[i]$ is a Euclidean ring with unit element, we know by Theorem 3.7.1 that it is a principle ideal ring. Then by Lemma 3.7.1, we know that any greatest common divisor of $a + bi$ and $c + di$ is a generator of the ideal $A$ given by

$$A = \{u(a + bi) + v(c + di)|u, v \in J[i]\}.$$

That generator being $x + yi$, we must have

$$A = \{(x + yi)(s + ti)|s, t \in \mathbb{Z}\}.$$

Continue on...

# Problem 8

Determine all prime elements in $J[i]$.

Maybe show that for $a, b \in J[i]$, $\langle a\rangle$ and $\langle b\rangle$ are properly contained in the ideal $I$ given by

$$I = \{ua + vb|u, v \in J[i]\},$$

if coprime. Now if $a$ is prime in $J[i]$, then we must have $I = J[i]$. Where am I going with this? I'm trying to find another way to characterize a prime. I want to say that $a \in J[i]$ is prime if and only if blank, where blank is something other than the definition. By definition, $a \in J[i]$ is prime if whenever we write $a = uv$ for $u, v \in J[i]$, we have at least one of $u$ and $v$ a unit of $j[i]$. It's hard to come somewhere straight from the definition.