Math 446 - Homework # 6 Solutions

1. Do the following calculations in $\mathbb{Z}[i]$.

   (a) $(2 + 10i) + (-3 + 15i)$
   Solution: $-1 + 25i$

   (b) $(-13 + i) - (2 - 3i)$
   Solution: $-15 + 4i$

   (c) $(1 + 3i)(2 - 10i)$
   Solution: $2 - 10i + 6i - 30i^2 = 2 - 4i + 30 = 32 - 4i$

   (d) $\dfrac{1+i}{i}$
   Solution: $\dfrac{1+i}{i} \cdot \dfrac{-i}{-i} = \dfrac{-i - i^2}{-i^2} = \dfrac{1-i}{1} = 1 - i$

   (e) $\dfrac{2-3i}{1-2i}$
   Solution: $\dfrac{2-3i}{1-2i} \cdot \dfrac{1+2i}{1+2i} = \dfrac{2 + 4i - 3i - 6i^2}{1 + 2i - 2i - 4i^2} = \dfrac{8+i}{5} = \dfrac{8}{5} + \dfrac{1}{5}i$

2. Calculate the norms of the following elements of $\mathbb{Z}[i]$.

   (a) i
   Solution: $N(i) = N(0 + 1 \cdot i) = 0^2 + 1^2 = 1$.

   (b) $2 - i$
   Solution: $N(2 - i) = N(2 - 1 \cdot i) = 2^2 + (-1)^2 = 5$.

   (c) 15
   Solution: $N(15) = N(15 + 0 \cdot i) = 15^2 + 0^2 = 225$.

   (d) $15 + 102i$
   Solution: $N(15 + 102i) = 15^2 + 102^2 = 225 + 10,404 = 10,629$.

3. List all the associates of $-1 + 2i$.

   Solution:

$$
\begin{aligned}
&-1 + 2i \\
&-(-1 + 2i) = 1 - 2i \\
&i \cdot (-1 + 2i) = -2 - i \\
&(-i) \cdot (-1 + 2i) = 2 + i
\end{aligned}
$$

4. List all the associates of 10.

   Solution: 10, -10, $10i$, $-10i$.

5. Carry out the division algorithm for z and w. That is, find q and r in $\mathbb{Z}[i]$ with $z = wq + r$.

   (a) $z = -8 - i$ and $w = 3 + 2i$

   Solution: $z/w = \dfrac{-8-i}{3+2i} \cdot \dfrac{3-2i}{3-2i} = \dfrac{-24+16i-3i-2}{9+4} = -2+i$.
   Hence, $q = -2 + i$ and $r = 0$ since w divides z.

   (b) $z = 5 + i$ and $w = -1 - 2i$

   Solution: $z/w = \dfrac{5+i}{-1-2i} \cdot \dfrac{-1+2i}{-1+2i} = \dfrac{-5+10i-i+2i^2}{1+4} = \dfrac{-7}{5} + \dfrac{9}{5} \cdot i = -1.4 + 1.8i$. Let, $q = -1 + 2i$. Then $r = z - wq = 5 + i - (-1-2i)(-1+2i) = i$. Note that $N(r) = N(i) = 1 < 5 = N(w)$.

   (c) $z = 33 + 5i$ and $w = 10 - 2i$

   Solution: $z/w = \dfrac{33+5i}{10-2i} = \dfrac{40}{13} + \dfrac{29}{26} \cdot i \approx 3.08 + 1.12i$. Let, $q = 3 + i$. Then $r = z - wq = 33 + 5i - (10-2i)(3+i) = 1 + i$. Note that $N(r) = N(1+i) = 1^2 + 1^2 = 2 < 104 = N(w)$.

6. Determine whether or not $2 + 3i$ divides $10 - 11i$ in $\mathbb{Z}[i]$.

   Solution: Yes, $\dfrac{10-11i}{2+3i} = -1 - 4i \in \mathbb{Z}[i]$.

7. Determine whether or not $3 - 2i$ divides $10 + i$ in $\mathbb{Z}[i]$.

   Solution: No, $\dfrac{10+i}{3-2i} = \dfrac{28}{13} + \dfrac{23}{13} \cdot i \notin \mathbb{Z}[i]$.

8. Determine whether or not $2 + i$ is prime in $\mathbb{Z}[i]$. Find all the divisors of $2 + i$.

   Solution: Since $N(2+i) = 5$ and 5 is prime in $\mathbb{Z}$, by exercise 18, we know that $2 + i$ is prime in $\mathbb{Z}[i]$. Hence the only divisors of $2 + i$ are the units of $\mathbb{Z}[i]$ and the associates of $2 + i$, which are 1, -1, i, $-i$, $2 + i = (1)(2+i)$, $-2 - i = (-1)(2+i)$, $-1 + 2i = (i)(2+i)$, and $1 - 2i = (-i)(2+i)$.

9. Let w and v be Gaussian integers with $w \neq 0$ and $v \neq 0$. If w divides v and $N(w) = N(v)$, then w is an associate of v.

   Solution: Since w divides v we have that $v = wz$ where z is a Gaussian integer. The associates of v are $1 \cdot v$, $(-1) \cdot v$, $i \cdot v$, and $(-i) \cdot v$. Thus our goal is to show that $w = uv$ where u is a unit. Applying the norm to the equation $v = wz$ we get that $N(v) = N(wz) = N(w)N(z)$. Since $w \neq 0$ we know that $N(w) \neq 0$. Dividing $N(v) = N(w)N(z)$ by $N(w)$, and using the fact that $N(v) = N(w)$ we get that $1 = N(z)$. Thus z is a unit. So $z = 1, -1, i,$ or $, -i$. Since $1^{-1} = 1, (-1)^{-1} = -1, i^{-1} = -i$, and $(-i)^{-1} = i$ we have that $z^{-1} = 1, -1, -i,$ or i. Thus z^{-1} is a unit. Multiplying $v = wz$ by z^{-1} we get that $w = z^{-1}v$ Thus w is an associate of v.

10. Can there exist Gaussian integers z and w where $N(z)$ divides $N(w)$, but z does not divide w ? Try to find some cases that are non-trivial, ie where $1 < N(z) < N(w)$. [Hint: You might need to write a computer program.]

    Solution: I used a Mathematica program to find these examples.

    Let $z = 3 + i$ and $w = 4 + 2i$. Then $N(z) = 3^2 + 1^2 = 10$ and $N(w) = 4^2 + 2^2 = 20$. So $N(z)|N(w)$. However,

$$\frac{4+2i}{3+i} = \frac{(4+2i)(3-i)}{(3+i)(3-i)} = \frac{7}{5} + \frac{1}{5} \cdot i \notin \mathbb{Z}[i]$$

    Therefore, z does not divide w.

    Here's another example. Let $z = 1 + 2i$ and $w = -3 + i$. Then $N(z) = 1^2 + 2^2 = 5$ and $N(w) = (-3)^2 + 1^2 = 10$. So $N(z)|N(w)$. However,

$$\frac{-3+i}{1+2i} = \frac{(-3+i)(1-2i)}{(1+2i)(1-2i)} = \frac{-1}{5} + \frac{7}{5} \cdot i \notin \mathbb{Z}[i]$$

    Therefore, z does not divide w.

    <u>What have we learned from this exercise?</u>. Suppose that we want to find the divisors of $w = -3 + i$ for example. We say, ok, if z divides w then $w = zv$ and so $10 = N(w) = N(z)N(v)$. So, $N(z)$ divides 10. So, $N(z)$ is either 1, 2, 5, or 10. Then we look for say elements of norm 5 and we find one. It is $z = 1+2i$. Then we say, ok, $z = 1+2i$ is a divisor

of w. This is wrong. When solving these norm equations, we only find *possible* divisors of w. We must actually check that we have a divisor by trying to divide it into w. The only exceptions to this rule are when you find the elements with $N(z) = 1$ and $N(z) = N(w) = 10$. These are the units, and by exercise 9, the associates of w. These never need to be checked because we know from class that they always divide w.

11. Determine whether or not 2 is prime in $\mathbb{Z}[i]$. Find all the divisors of 2.

    Solution: Note that $N(2) = 4$. Suppose that $w \in \mathbb{Z}[i]$ is a divisor of 2, then $2 = zw$ where $z \in \mathbb{Z}[i]$. Hence $4 = N(2) = N(zw) = N(z)N(w)$. Since $N(z)$ and $N(w)$ are positive integers, we see that $N(w)$ divides 4 in $\mathbb{Z}$. Hence $N(w)$ can be 1, 2, or 4.

    We first deal with the trivial cases of $N(w)$ equal to 1 or 4. Then we do the $N(w)$ equal to 2 case.

    Case 1: If $N(w) = 1$, then w is a unit, so w must be 1, -1, i, or $-i$. All of these Gaussian integers divide 2 because every unit divides every Gaussian integer.

    Case 2: Suppose that $N(w) = 4$. By Exercise 9, since $w|2$ and $N(w) = 4 = N(2)$, we must have that w is an associate of 2, that is w is one of 2, -2, $2i$, and $-2i$. Each of these is a divisor of 2 since the associates of a Gaussian integer g always divide g.

    Case 3: Suppose that $w = a + bi \in \mathbb{Z}[i]$. If $N(w) = 2$, then $a^2 + b^2 = 2$. The only solutions to this equation with a and b integers are $(a, b) = (\pm 1, \pm 1)$. This gives us the solutions $1 + i$, $-1 + i$, $1 - i$ and $-1 - i$. By exercise 10, we must be careful here and verify that these all actually divide 2. We do this below:

$$\begin{aligned} \frac{2}{1+i} &= 1 - i \in \mathbb{Z}[i] \\ \frac{2}{-1+i} &= -1 - i \in \mathbb{Z}[i] \\ \frac{2}{1-i} &= 1 + i \in \mathbb{Z}[i] \\ \frac{2}{-1-i} &= -1 + i \in \mathbb{Z}[i] \end{aligned}$$

    Hence the divisors of 2 are 1, -1, i, $-i$, $1 + i$, $-1 + i$, $1 - i$, $-1 - i$, 2, -2, $2i$, and $-2i$. Since 2 has divisors other than its associates and units, we have that 2 is not prime.

12. Determine whether or not 13 is prime in $\mathbb{Z}[i]$. Find all the divisors of 13.

    Solution: Note that $N(13) = 13^2 = 169$. Suppose that $w \in \mathbb{Z}[i]$ is a divisor of 13, then $13 = zw$ where $z \in \mathbb{Z}[i]$. Hence $169 = N(13) = N(zw) = N(z)N(w)$. Since $N(z)$ and $N(w)$ are positive integers, we see that $N(w)$ divides 169 in $\mathbb{Z}$. Hence $N(w)$ can be 1, 13, or 169.

    We first deal with the trivial cases of $N(w)$ equal to 1 or 169. Then we do the $N(w)$ equal to 13 case.

    Case 1: If $N(w) = 1$, then w is a unit, so w must be 1, -1, i, or $-i$. All of these Gaussian integers divide 13 because every unit divides every Gaussian integer.

    Case 2: Suppose that $N(w) = 169$. By Exercise 9, since $w|13$ and $N(w) = 169 = N(13)$, we must have that w is an associate of 13, that is w is one of 13, -13, $13i$, and $-13i$. Each of these is a divisor of 13 since the associates of a Gaussian integer g always divide g.

    Case 3: Suppose that $w = a+bi \in \mathbb{Z}[i]$. If $N(w) = 13$, then $a^2+b^2 = 13$. The only solutions to this equation with a and b integers are $(a, b) = (\pm 2, \pm 3)$ and $(a, b) = (\pm 3, \pm 2)$. This gives us the solutions $2 + 3i$, $2 - 3i$, $-2 + 3i$, $-2 - 3i$, $3 + 2i$, $3 - 2i$, $-3 + 2i$, $-3 - 2i$. By exercise 10, we must be careful here and verify that these all actually divide 13.

We do this below:

$$\begin{aligned}
\frac{13}{2+3i} &= 2-3i \in \mathbb{Z}[i] \\
\frac{13}{2-3i} &= 2+3i \in \mathbb{Z}[i] \\
\frac{13}{-2+3i} &= -2-3i \in \mathbb{Z}[i] \\
\frac{13}{-2-3i} &= -2+3i \in \mathbb{Z}[i] \\
\frac{13}{3+2i} &= 3-2i \in \mathbb{Z}[i] \\
\frac{13}{3-2i} &= 3+2i \in \mathbb{Z}[i] \\
\frac{13}{-3+2i} &= -3-2i \in \mathbb{Z}[i] \\
\frac{13}{-3-2i} &= -3+2i \in \mathbb{Z}[i]
\end{aligned}$$

Hence the divisors of 13 are 1, -1, i, $-i$, $2+3i$, $-2+3i$, $2-3i$, $-2-3i$, $3+2i$, $-3+2i$, $3-2i$, $-3-2i$, 13, -13, $13i$, and $-13i$.

Since 13 has divisors other than its associates and units, we have that 13 is not prime.

13. Let z be a Gaussian integer. Suppose that z is not prime in $\mathbb{Z}[i]$. Suppose further that $z \neq 0$ and z is not a unit. Then there exist Gaussian integers w and v where

    (a) $z = wv$

    (b) w is not a unit and w is not an associate of z

    (c) v is not a unit and v is not an associate of z

    That is, z factors non-trivially.

    Solution: Suppose that z is not prime and $z \neq 0$ and z is not a unit. Since z is not prime and not a unit, there exists a Gaussian integer w that divides z, where w is not a unit and w is not an associate of z. Therefore, $z = wv$ where v is a Gaussian integer. The only thing left to show is that v is not a unit and not an associate of z.

Suppose v is a unit. Then $N(v) = 1$. So $N(z) = N(wv) = N(w)N(v) = N(w) \cdot 1 = N(w)$. Thus w divides z and $N(w) = N(z)$. By exercise 9, this implies that w is an associate of z, which can't happen.

Suppose that v is an associate of z. Then $v = uz$ where u is a unit. This implies that $N(v) = N(uz) = N(u)N(z) = 1 \cdot N(z) = N(z)$. Combining this with $N(z) = N(w)N(v)$ gives $N(v) = N(z) = N(w)N(v)$. Cancelling off the $N(v)$ term gives $N(w) = 1$. This implies that w is a unit, which can't happen.

Hence v is not a unit, and v is not an associate of z.

14. Let p be an odd prime in $\mathbb{Z}$ with $p \equiv 1 (\text{mod } 4)$. Prove that p is not prime in $\mathbb{Z}[i]$.

Solution: Since $p \equiv 1 (\text{mod } 4)$, we know from class that there exist integers a and b with $p = a^2 + b^2$. Thus $p = (a+bi)(a-bi) = wz$ where $w = a + bi$ and $z = a - bi$. Let's show that w is not a unit and is not an associate of p.

Note that a is non-zero, since if it was, then $p = b^2$. This can't happen since p is prime. Similarly, b is non-zero. Hence $N(w) = N(a + bi) = a^2 + b^2 \geq 1 + 1 = 2$. So w is not a unit. Similarly, $N(z) = N(a - bi) = a^2 + (-b)^2 \geq 1 + 1 = 2$. So z is not a unit.

Let's now rule out the case that w is an associate of p. Suppose w is an associate of p. Then $w = up$ where u is a unit. Thus, $N(w) = N(u)N(p) = 1 \cdot p^2 = p^2$. We also know from the equation $p = wz$ that $p^2 = N(p) = N(w)N(z)$. Thus, $N(w) = p^2 = N(w)N(z)$. So $1 = N(z)$ and hence z is a unit. But this is contrary to what we know from above. Hence w is not an associate of p.

Therefore, we have shown that p has a divisor w that is not a unit and not an associate of p. Hence p is not prime in the Gaussian integers.

15. Let p be an odd prime in $\mathbb{Z}$ with $p \equiv 3 (\text{mod } 4)$. Prove that p is prime in $\mathbb{Z}[i]$.

Solution: Suppose that p is not prime in $\mathbb{Z}[i]$. By exercise 13, there exist Gaussian integers w and z where $p = wz$, z is not a unit, z is not an associate of p, w is not a unit, and w is not an associate of p.

Since w and z are not units, $N(w) \neq 1$ and $N(z) \neq 1$. Since w and z are divisors of p and they are not associates of p, by exercise 9, we must have that $N(w) \neq p^2$ and $N(z) \neq p^2$.

Since $p = wz$ we have that $p^2 = N(p) = N(wz) = N(w)N(z)$. Since p is prime in $\mathbb{Z}$, the only divisors of p^2 are 1, p, and p^2. Hence $N(w)$ and $N(z)$ must be either 1, p, or p^2. From the arguments above we see that we must have that $N(w) = N(z) = p$. Let $w = a + bi$ where $a, b \in \mathbb{Z}$. Then $p = N(w) = a^2 + b^2$. However from class, we know that a prime that is congruent to 3 modulo 4 cannot be the sum of two squares (we showed that the equation $\overline{3} = \overline{p} = \overline{a}^2 + \overline{b}^2$ has no solutions in $\mathbb{Z}_4$). Hence we have a contradiction. Thus p must be prime in $\mathbb{Z}[i]$.

16. Let $z, w \in \mathbb{Z}[i]$. Prove that w divides z if and only if $\overline{w}$ divides $\overline{z}$.

    Solution: Suppose that w divides z. Then there exists an element $q \in \mathbb{Z}[i]$ such that $wq = z$. Hence $\overline{wq} = \overline{z}$. Thus, $\overline{w} \cdot \overline{q} = \overline{z}$. Hence $\overline{w}$ divides $\overline{z}$.

    Conversely, suppose that $\overline{w}$ divides $\overline{z}$. Then there exists an element $q \in \mathbb{Z}[i]$ such that $\overline{w} \cdot q = \overline{z}$. Hence $\overline{\overline{w} \cdot q} = \overline{\overline{z}}$. Thus, $\overline{\overline{w}} \cdot \overline{q} = \overline{\overline{z}}$. So, $w \cdot \overline{q} = z$. Therefore w divides z.

17. (a) $N(v) = N(\overline{v})$ for all Gaussian integers v.

    Solution: Suppose that $v = a + bi \in \mathbb{Z}[i]$. Then

    $$N(v) = N(a + bi) = a^2 + b^2 = a^2 + (-b)^2 = N(a - bi) = N(\overline{v}).$$

    (b) For any Gaussian integer u we have the following: u is a unit iff $\overline{u}$ is a unit.

    Solution: We use exercise (17a). We have that u is a unit if and only if $N(u) = 1$ if and only if $N(\overline{u}) = 1$ if and only if $\overline{u}$ is a unit.

    (c) Let $z \in \mathbb{Z}[i]$. Prove that z is prime if and only if $\overline{z}$ is prime.

    Solution: We will prove the contrapositive: z is not prime if and only if $\overline{z}$ not is prime.

    Note that we only have to prove one direction of this exercise. Suppose that we prove the statement "Let w be a Gaussian integer. If w is not prime, then $\overline{w}$ is not prime." Plugging in $w = z$ gives one direction: If z is not prime, then $\overline{z}$ not is prime. Plugging in $w = \overline{z}$ and using the fact that $\overline{\overline{z}} = z$ we get the other direction: If $\overline{z}$ is not prime then if z not is prime.

    We now prove: If w is not prime, then $\overline{w}$ is not prime.

Suppose that w in not prime in the Gaussian integers. Then by negating the definition of prime, there exists a Gaussian integer α that divides w such that (i) α is not a unit and (ii) α is not an associate of w. Since α is a divisor of w, we have that $w = \alpha\beta$ where β is a Gaussian integer. Conjugating this equation we get that $\overline{w} = \overline{\alpha}\overline{\beta}$. Therefore, $\overline{\alpha}$ is a divisor of $\overline{w}$. If we now show that $\overline{\alpha}$ is not a unit and not an associate of $\overline{w}$ then we have shown that $\overline{w}$ is not a prime in the Gaussian integers.

Let us first show that $\overline{\alpha}$ is not a unit. If $\overline{\alpha}$ was a unit, by exercise 17b we would have that α was a unit. But from above we know that α is not a unit. Therefore, $\overline{\alpha}$ is not a unit.

We now show that $\overline{\alpha}$ is not an associate of $\overline{w}$. Suppose that $\overline{\alpha}$ was an associate of $\overline{w}$. Then $\overline{\alpha} = u\overline{w}$ where u is a unit of the Gaussian integers. Conjugating this equation we get that $\alpha = \overline{u}w$. By exercise 17b we have that $\overline{u}$ is a unit. Thus from $\alpha = \overline{u}w$ we get that α is an associate of w. But above we had that α was not an associate of w. Therefore, we must have that $\overline{\alpha}$ is not an associate of $\overline{w}$.

18. Let $z \in \mathbb{Z}[i]$. Prove that if $N(z)$ is a prime in $\mathbb{Z}$, then z is prime in $\mathbb{Z}[i]$.

Solution: We prove the contrapositive: If z is not prime, then $N(z)$ is not prime.

Suppose that z is not prime in $\mathbb{Z}[i]$. If $z = 0$, then $N(0) = 0$ which is not prime in $\mathbb{Z}$. If z is a unit, then $N(0) = 0$ which is not prime in $\mathbb{Z}$.

Henceforth, we assume that $z \neq 0$ and z is not a unit. This implies that $N(z)$ is an integer and $N(z) \geq 1$.

By exercise 13, there exists $w, x \in \mathbb{Z}[i]$ such that $z = wx$, where w is not a unit, w is not an associate of z, where x is not a unit, and x is not an associate of z.

Since w and x are not units, $N(w) \neq 1$ and $N(x) \neq 1$. Since w and x are divisors of z and they are not associates of z, by exercise 9, we must have that $N(w) \neq N(z)$ and $N(x) \neq N(z)$.

Since $z = wx$, we have that $N(z) = N(wx) = N(w)N(x)$. Thus $N(w)$ and $N(x)$ are divisors of $N(z)$ in $\mathbb{Z}$. From above, we have that $1 < N(w) < N(z)$ and $1 < N(x) < N(z)$. Therefore, we have factored $N(z) = N(w)N(x)$ non-trivially, and hence $N(z)$ is not a prime in $\mathbb{Z}$.

19. Let $w, y, z \in \mathbb{Z}[i]$. Prove that if w is a unit and z divides wy, then z divides y.

Solution: Suppose that w is a unit and z divides wy. This implies that there exists an element $k \in \mathbb{Z}[i]$ with $wy = zk$. Since w is a unit, we know that w^{-1} is in $\mathbb{Z}[i]$. Thus $w^{-1}(wy) = w^{-1}(zk)$. So $y = z(w^{-1}k)$. Since $w^{-1}k \in \mathbb{Z}[i]$ we know that z divides y.