

# MATH 356 Number Theory

## Solutions to Homework Assignment 11

Keep:

1. Compute in the quaternions.

(a)  $(3 + 2\mathbf{i} - 4\mathbf{j} + 6\mathbf{k})(2 - 3\mathbf{i} + \mathbf{k})$

**Solution:**

$$\begin{aligned} (3 + 2\mathbf{i} - 4\mathbf{j} + 6\mathbf{k})(2 - 3\mathbf{i} + \mathbf{k}) &= 6 - 9\mathbf{i} + 3\mathbf{k} + 4\mathbf{i} - 6\mathbf{i}^2 + 2\mathbf{i}\mathbf{k} - 8\mathbf{j} + 12\mathbf{j}\mathbf{i} \\ &\quad - 4\mathbf{j}\mathbf{k} + 12\mathbf{k} - 18\mathbf{k}\mathbf{i} + 6\mathbf{k}^2 \\ &= 6 - 9\mathbf{i} - 28\mathbf{j} + 3\mathbf{k} \end{aligned}$$

(b)  $(2 + 6\mathbf{i} - \mathbf{j})(2 - 6\mathbf{i} + \mathbf{j})$

**Solution:**

$$\begin{aligned} (2 + 6\mathbf{i} - \mathbf{j})(2 - 6\mathbf{i} + \mathbf{j}) &= \begin{bmatrix} 2 + 6i & -1 \\ 1 & 2 - 6i \end{bmatrix} \begin{bmatrix} 2 - 6i & 1 \\ -1 & 2 + 6i \end{bmatrix} \\ &= \begin{bmatrix} 41 & 0 \\ 0 & 41 \end{bmatrix} \\ &= 41. \end{aligned}$$

(c)  $4 - \mathbf{i} + 3\mathbf{j} + 2\mathbf{k}$  divided by  $1 - 2\mathbf{i} + 2\mathbf{j} + 3\mathbf{k}$  (find quotient and remainder).

**Solution:**

$$\begin{aligned} \begin{bmatrix} 4 - i & 3 + 2i \\ -3 + 2i & 4 + i \end{bmatrix} \begin{bmatrix} 1 - 2i & 2 + 3i \\ -2 + 3i & 1 + 2i \end{bmatrix}^{-1} &= \begin{bmatrix} 4 - i & 3 + 2i \\ -3 + 2i & 4 + i \end{bmatrix} \frac{1}{18} \begin{bmatrix} 1 + 2i & -2 - 3i \\ 2 - 3i & 1 - 2i \end{bmatrix} \\ &= \frac{1}{18} \begin{bmatrix} 18 + 2i & -4 - 14i \\ 4 - 14i & 18 - 2i \end{bmatrix} \end{aligned}$$

I gave bad directions on this – it should be “Compute in the Hurwitz integers.”

With that in mind, we need to find the nearest half-integers to each entry. I will

use  $\gamma = \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix}$ . Sadly, these are all integers. But now, we take

$$\begin{aligned} \rho &= \begin{bmatrix} 4 - i & 3 + 2i \\ -3 + 2i & 4 + i \end{bmatrix} - \begin{bmatrix} 1 & -i \\ -i & 1 \end{bmatrix} \begin{bmatrix} 1 - 2i & 2 + 3i \\ -2 + 3i & 1 + 2i \end{bmatrix} \\ &= \begin{bmatrix} -i & -1 \\ 1 & i \end{bmatrix}. \end{aligned}$$

Thus  $4 - \mathbf{i} + 3\mathbf{j} + 2\mathbf{k} = (1 - \mathbf{k})(1 - 2\mathbf{i} + 2\mathbf{j} + 3\mathbf{k}) + (-\mathbf{i} - \mathbf{j})$ .

Keep in mind that the order matters. Notice that the norm of the remainder is  $2 < 18$ .

2. Show that  $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ .

**Solution:** Represent each one in matrix form and check. For example:  $\mathbf{k}^2 = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = -1$ .

3. Show that  $\mathbf{ij} = \mathbf{k}$ ,  $\mathbf{jk} = \mathbf{i}$ , and  $\mathbf{ki} = \mathbf{j}$ .

**Solution:** See above. For example,  $\mathbf{ki} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \mathbf{j}$ .

4. Show that reversing the products in the previous parts changes the sign of the results.

**Solution:** Ditto.

5. Show that  $\mathbf{1}$ ,  $\mathbf{i}$ ,  $\mathbf{j}$ , and  $\mathbf{k}$  are linearly independent over  $\mathbb{R}$ .

**Solution:** Again consider these as matrices, and suppose that  $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = 0$ . Then

$$0 = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} = \begin{bmatrix} a + bi & c + di \\ -c + di & a - bi \end{bmatrix},$$

so  $a + bi = 0$  and  $c + di = 0$ . But we already know that  $a + bi = 0$  if and only if  $a = b = 0$ , and similarly  $c = d = 0$ . Therefore,  $\mathbf{1}$ ,  $\mathbf{i}$ ,  $\mathbf{j}$ , and  $\mathbf{k}$  are linearly independent.

6. Show that the Hurwitz integers form a ring with unity that has a multiplicative norm, a division algorithm, and no zero divisors.

**Solution:** The Hurwitz integers inherit commutativity of addition, associativity of multiplication and division, the distributive law(s), a multiplicative norm, and a lack of zero divisors (!) from  $Q$ . Also,  $0 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in \mathbb{H}$  and  $1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathbb{H}$ , and if  $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \in \mathbb{H}$ , then so is  $-a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$ . The only questions are about closure and a division algorithm. However, we covered the division algorithm in class (the center of each lattice hypercube is only  $1/2$  of a unit away from a vertex). Let  $a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k}, b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k} \in \mathbb{H}$ . If all of the coefficients are integers, the same is true for the sum and product, which are then in  $\mathbb{H}$ . If all of the coefficients are half-integers, then the coefficients of the sum are all integers, and the sum is again in  $\mathbb{H}$ . If the  $a_i$  are all integers and the  $b_i$  are all half-integers (or vice versa), then the coefficients in the sum and product are all half-integers as well.

We have a little more to do on multiplication before we can call it a day. Suppose the  $a_i$  are integers and the  $b_i$  are half integers; say  $b_i = \frac{2c_i + 1}{2}$  for some  $c_i \in \mathbb{Z}$ .

$$(a_1 + a_2\mathbf{i} + a_3\mathbf{j} + a_4\mathbf{k})(b_1 + b_2\mathbf{i} + b_3\mathbf{j} + b_4\mathbf{k}) = \dots$$

Life is too short. Do this by hand and see that it all works out. Note that if there is an even number of odd  $a_i$ , the result will be all integers, and if there is an odd number of odd  $a_i$ , the result will be all half-integers. In the case that all of the  $a_i$  and  $b_i$  are half-integers, the product has a 4 in the denominator, but the numerator has an even number of odd terms and is therefore even, which, when reduced, leaves a denominator of 2.

7. Show that if  $\alpha$  is a quaternion represented by the matrix  $A$ , then  $\bar{\alpha}$  is represented by  $\bar{A}^T$ . [Recall that  $\overline{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$  and translate to matrices.]

**Solution:**  $a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k} = \begin{bmatrix} a - bi & -c - di \\ c - di & a + bi \end{bmatrix}$ . Also,

$$\bar{A}^T = \begin{bmatrix} a - bi & c - di \\ -c - di & a + bi \end{bmatrix}^T = \begin{bmatrix} a - bi & -c - di \\ c - di & a + bi \end{bmatrix}.$$

8. Show that if  $q_1, q_2 \in Q$  (the quaternions), then  $\overline{q_1 q_2} = \bar{q}_2 \cdot \bar{q}_1$ .

**Solution:** Let  $A_1$  and  $A_2$  be matrices representing  $q_1$  and  $q_2$ , respectively. Then  $\overline{q_1 q_2} = \overline{A_1 A_2}^T = (\overline{A_1} \cdot \overline{A_2})^T = \overline{A_2}^T \overline{A_1}^T = \bar{q}_2 \cdot \bar{q}_1$ .