HOMEWORK 1

(1) Perform the following operations.

(a) $(1+i)(3+i+k)$
(b) $(2 \mod 11)(8 \mod 11)$
(c) $(a+bi+cj+dk)(a-bi-cj-dk)$
(d) $(1+i+k)^{-1}$
(e) $7^{-1} \mod 11$
(f) $-5 \mod 13$.
(g) $(1002)(1000) \mod 1003$.[1]
(h)

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

(i)

$$\begin{pmatrix} 1 \mod 7 & 2 \mod 7 \\ 3 \mod 7 & 2 \mod 7 \end{pmatrix}^{-1}$$

(j)

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix}$$

(k)

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}^{-1}$$ [2]

Sol'n

(a)

$$\begin{aligned}(1+i)(3+i+k) &= 1(3+i+k)+i(3+i+k)\\ &= 3+i+k+3i+iI+ik\\ &= 3+i+k+3i+(-1)+(-j)\\ &= 2+4i-j+k.\end{aligned}$$

(b)

$$(2 \mod 11)(8 \mod 11) = 16 \mod 11 = 5 \mod 11$$

(c)

$$\begin{aligned}&(a+bi+cj+dk)(a-bi-cj-dk)\\ &= a(a-bi-cj-dk)+bi(a-bi-cj-dk)+cj((a-bi-cj-dk)+dk(a-bi-cj-dk)\\ &= (a^2-abi-acj-adk)+(abi-b^2ii-bcij-bdik)+(acj-bcji-c^2jj-cdjk)+(adk-bdki-cdjk-d^2kk)\\ &= (a^2-abi-acj-adk)+(abi+b^2-bck+bdj)+(acj+bck+c^2-cdi)+(adk-bdj-cdi+d^2)\\ &= (a^2 \quad -acj-adk)+(\quad b^2-bck+bdj)+(acj+bck+c^2-cdi)+(adk-bdj-cdi+d^2)\\ &= (a^2 \quad -adk)+(\quad b^2-bck+bdj)+(\quad bck+c^2-cdi)+(adk-bdj-cdi+d^2)\\ &= (a^2 \quad)+(\quad b^2-bck+bdj)+(\quad bck+c^2-cdi)+(\quad -bdj-cdi+d^2)\\ &= (a^2 \quad)+(\quad b^2 \quad +bdj)+(\quad c^2-cdi)+(\quad -bdj-cdi+d^2)\\ &= (a^2 \quad)+(\quad b^2 \quad)+(\quad c^2 \quad)+(\quad d^2)\\ &= a^2+b^2+c^2+d^2.\end{aligned}$$

[1] use a trick!

[2] Since Quaternions are not commutative, one cannot use the usual formula, and we must do this "by hand"

(d) We have

$$\overline{(1+i+k)} = 1 - i - k$$

and

$$||(1+i+k)||^2 = 1+1+1 = 3$$

Thus

$$(1+i+k)^{-1} = \frac{1}{3}(1-i-k).$$

(e) Since $(7 \mod 11)(3 \mod 11) = 21 \mod 11 = -1 \mod 11$, we have $(7 \mod 11)(3 \mod 11)(7 \mod 11)(3 \mod 11) = 1 \mod 11$. Hence $(7 \mod 11)(3 \cdot 7 \cdot 3 \mod 11) = 1 \mod 11$. But $(3 \cdot 7 \cdot 3 \mod 11) = (-2)(-4) = 8 \mod 11$. Hence $7^{-1} \mod 11 = 8 \mod 11$. (note this could be verified directly since $7 \cdot 8 = 56$ which indeed does equal 1 mod 11).

(f) $-5 \mod 13 = 8 \mod 13$.

(g) $(1002)(1000) \mod 1003 = (-1 \mod 1003)(-3 \mod 1003) = 3 \mod 1003$.

(h)

$$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2+1 & 0+1 \\ 1+1 & 0+1 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}$$

(i) The determinant of

$$\begin{pmatrix} 1 \mod 7 & 2 \mod 7 \\ 3 \mod 7 & 2 \mod 7 \end{pmatrix}$$

is $2 - 6 \mod 7 = -4 \mod 7 = 3 \mod 7$. Moreover $3^{-1} \mod 7 = 5 \mod 7$. Thus, if we use the formula for the inverse we get that

$$\begin{aligned}
\begin{pmatrix} 1 \mod 7 & 2 \mod 7 \\ 3 \mod 7 & 2 \mod 7 \end{pmatrix}^{-1} &= 5\begin{pmatrix} 2 \mod 7 & -2 \mod 7 \\ -3 \mod 7 & 1 \mod 7 \end{pmatrix} \\
&= 5\begin{pmatrix} 2 \mod 7 & 5 \mod 7 \\ 4 \mod 7 & 1 \mod 7 \end{pmatrix} \\
&= \begin{pmatrix} 10 \mod 7 & 25 \mod 7 \\ 20 \mod 7 & 5 \mod 7 \end{pmatrix} \\
&= \begin{pmatrix} 3 \mod 7 & 4 \mod 7 \\ 6 \mod 7 & 5 \mod 7 \end{pmatrix}
\end{aligned}$$

(j)

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ k & 1 \end{pmatrix} = \begin{pmatrix} i+(i+j)k & ik+i+j \\ 1+k & 1+k \end{pmatrix} = \begin{pmatrix} 2i-j & i \\ 1+k & 1+k \end{pmatrix}$$

(k) To find

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}^{-1}$$

we need to resort to basic techniques (since our formula does not work since quaternions are **not** commutative). Consider a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

which satisfies

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} ia+(i+j)c & ib+(i+j)d \\ a+c & b+d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

This leads to 4 equations over the quaternions:

$$ia + (i+j)c = 1 \tag{1}$$
$$a + c = 0 \tag{2}$$
$$ib + (i+j)d = 0 \tag{3}$$
$$b + d = 1 \tag{4}$$

Multiplying (1) by i and adding it to (2) yields:

$$-a + (-1+k)c + a + c = i + 0 \Rightarrow kc = i. \tag{5}$$

Now multiplying this new equation by $-k$ on both sides tells us that $c = -j$. Now using equation (2) tells us that $a = j$. Now let us deal with b and d. For those two we use the same trick and multiply (3) by i and add it to (4) which yields $kd = 1$ or $d = -k$. This time when we use (4) we get $b = 1 + k$. In summary:

$$\begin{pmatrix} i & i+j \\ 1 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} j & 1+k \\ -j & -k \end{pmatrix}.$$

(2) Let

$$\omega := \frac{(1+i+j+k)}{2}.$$

(a) Show that $\omega \in \mathbb{S}^3$.

Sol'n
$\omega\overline{\omega} = 1/4 + 1/4 + 1/4 + 1/4 = 1.$

(b) Compute the multiplicative order of ω.

Sol'n
ω can also be written as

$$\omega = \cos(\pi/3) + \sin(\pi/3)\frac{1}{\sqrt{3}}(i+j+k) = cos(\pi/3) + sin(\pi/3)v$$

with $v \in \mathbb{S}^2$. From the result in class this implies that ω has order $2 \cdot 3 = 6$.

(c) Find ω^{-1}.

Sol'n

$$\omega^{-1} = \overline{\omega} = \frac{(1-i-j-k)}{2}$$

(3) Let $q \in \mathbb{H}$. Show that $q \in \mathbb{S}^3$ if and only if $q^{-1} = \overline{q}$.

Sol'n
In general, $q^{-1} = \overline{q}/||q||^2$. Thus the result holds if and only if $||q||^2 = 1$, or since $||q|| > 0$ we must have that $||q|| = 1$, i.e. $q \in \mathbb{S}^3$ as desired.

(4) A quaternion is called *real* if and only if it equals its own conjugate (i.e., the given quaternion's i, j and k components are each 0.) Show that a quaternion q commutes with every other quaternion if and only if q is real. (**Hint:** Take this slowly! First, figure out what it means for q to commute with i, then figure out what it means for it to commute with j.)

Sol'n

Clearly real quaternions commute with every other quaternion. Conversely, write q as $a+bi+cj+dk$ where $a, b, c, d \in \mathbb{R}$. Now $qi = ai-b-ck+dj$ while at the same time $iq = ai - b + ck - dj$. Hence if q is to commute with i, we must have that both c and d are equal to 0. If we did the same trick with j instead of i we would see that, in addition, $b = 0$. Hence $q = a$, i.e. q is a real quaternion.