HOMEWORK 1: SOLUTIONS - MATH 341
INSTRUCTOR: George Voutsadakis

Problem 1 *(a) Is the map $f : \mathbf{Q}^* \to \mathbf{Q}^*$, defined by $f(\frac{n}{m}) = \frac{m}{n}$, where $\mathbf{Q}^*$ is the set of nonzero rational numbers, a one to one map?*

(b) Is the map $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 - 4$, an onto map?

(c) Let $f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$, where $f(i) = i + 2$, for $1 \leq i \leq n - 2$, and $f(n-1) = 1$ and $f(n) = 2$ invertible?

(d) Let $f : A \to B$ and $g : B \to C$ be two maps. Show that

- *(i) If $g \circ f$ is onto, then g must be onto.*
- *(ii) If $g \circ f$ is one-to-one, then f must be one-to-one.*

(e) Show that $|\mathbf{Z} \times \mathbf{Z}| = |2\mathbf{Z} \times 2\mathbf{Z}|$.

Solution:

(a) The map is one to one: Let $\frac{n}{m}, \frac{p}{q} \in \mathbf{Q}^*$. Then $f(\frac{n}{m}) = \frac{p}{q}$ implies $\frac{m}{n} = \frac{q}{p}$ implies that $(\frac{m}{n})^{-1} = (\frac{q}{p})^{-1}$ implies $\frac{n}{m} = \frac{p}{q}$.

(b) $f : \mathbb{R} \to \mathbb{R}$, defined by $f(x) = x^2 - 4$, is not onto, since $x^2 \geq 0$ implies $x^2 - 4 \geq -4$, i.e., $f(x) \geq -4$. Hence, for instance, $-5 \notin f(\mathbb{R})$.

(c) The given function is invertible since one very easily verifies that it is one to one and onto.

(d) (i) Suppose that $g \circ f : A \to C$ is onto. To show that $g : B \to C$ must be onto, let $c \in C$. Since $g \circ f$ is onto, there exists $a \in A$, such that $c = (g \circ f)(a)$, i.e., $c = g(f(a))$. But then, there exists $b = f(a) \in B$, such that $c = g(b)$, which proves that g is onto.

(ii) Suppose that $g \circ f : A \to C$ is one to one. To show that $f : A \to B$ must be one to one, let $a_1, a_2 \in A$, such that $f(a_1) = f(a_2)$. Then $g(f(a_1)) = g(f(a_2))$. Hence $(g \circ f)(a_1) = (g \circ f)(a_2)$. Now, since $g \circ f : A \to C$ is one to one, $a_1 = a_2$. Hence f must be one to one as well.

(e) To show that $|\mathbf{Z} \times \mathbf{Z}| = |2\mathbf{Z} \times 2\mathbf{Z}|$, it suffices to exhibit a one to one and onto function $f : \mathbf{Z} \times \mathbf{Z} \to 2\mathbf{Z} \times 2\mathbf{Z}$. Define f by

$$f(m, n) = (2m, 2n), \quad \text{for all } (m, n) \in \mathbf{Z} \times \mathbf{Z}.$$

f is onto by the definition of $2\mathbf{Z} \times 2\mathbf{Z}$ and it is one to one, since, for all $(m, n), (p, q) \in \mathbf{Z} \times \mathbf{Z}$, $f(m, n) = f(p, q)$ implies $(2m, 2n) = (2p, 2q)$, whence $2m = 2p$ and $2n = 2q$, and, therefore, $m = p$ and $n = q$, i.e., $(m, n) = (p, q)$. ■

Problem 2 *(a) Determine whether the following relations are equivalent relations and, if so, describe the equivalence classes:*

(i) In $\mathbb{R}$*,* $a \sim b$ *if and only if* $|a| = |b|$.

(ii) In $\mathbb{R}$*,* $a \sim b$ *if and only if* $|a - b| \leq 1$.

(iii) In $\mathbb{R} \times \mathbb{R}$*,* $(x_1, y_1) \sim (x_2, y_2)$ *if and only if* $x_1^2 + y_1^2 = x_2^2 + y_2^2$.

(b) Fix an integer n *and define on* $\mathbf{Z}$ *the relation* $a \sim b$ *if and only if* $a - b$ *is divisible by* n*. Show that this is an equivalence relation on* $\mathbf{Z}$ *and describe the equivalence classes.*

(c) Let $f : S \to T$ *be any map and define the relation* $\sim$ *on* S *by letting* $a \sim b$ *if and only if* $f(a) = f(b)$*. Show that* $\sim$ *is an equivalence relation on* S.

Solution:

(a) (i) $a \sim a$ since $|a| = |a|$, hence $\sim$ is reflexive. $a \sim b$ implies $|a| = |b|$ whence $|b| = |a|$, i.e., $b \sim a$. Thus, $\sim$ is also symmetric. Finally, $a \sim b$ and $b \sim c$ imply $|a| = |b|$ and $|b| = |c|$, whence $|a| = |c|$. Therefore $\sim$ is also transitive. Thus, $\sim$ is an equivalence relation on $\mathbb{R}$. To describe the equivalence classes, let $a \in \mathbb{R}$. Then

$$
\begin{aligned}
[a] &= \{x \in \mathbb{R} : x \sim a\} \\
&= \{x \in \mathbb{R} : |x| = |a|\} \\
&= \{x \in \mathbb{R} : x = -a \text{ or } x = a\} \\
&= \{-a, a\}
\end{aligned}
$$

Hence the equivalence classes consist of all doubletons consisting of the reals and their negatives.

(ii) This is not an equivalence relation because it fails to be transitive. For instance, $0 \sim 1$ and $1 \sim 2$ but $0 \not\sim 2$.

(iii) $(x, y) \sim (x, y)$ since $x^2 + y^2 = x^2 + y^2$, hence $\sim$ is reflexive. $(x_1, y_1) \sim (x_2, y_2)$ implies $x_1^2 + y_1^2 = x_2^2 + y_2^2$ whence $x_2^2 + y_2^2 = x_1^2 + y_1^2$, i.e., $(x_2, y_2) \sim (x_1, y_1)$. Thus, $\sim$ is also symmetric. Finally, $(x_1, y_1) \sim (x_2, y_2)$ and $(x_2, y_2) \sim (x_3, y_3)$ imply $x_1^2 + y_1^2 = x_2^2 + y_2^2$ and $x_2^2 + y_2^2 = x_3^2 + y_3^2$, whence $x_1^2 + y_1^2 = x_3^2 + y_3^2$, i.e., $(x_1, y_1) \sim (x_3, y_3)$. Therefore $\sim$ is also transitive. Thus, $\sim$ is an equivalence relation on $\mathbb{R}^2$. To describe the equivalence classes, let $(a, b) \in \mathbb{R}^2$. Then

$$
\begin{aligned}
[(a, b)] &= \{(x, y) \in \mathbb{R}^2 : (x, y) \sim (a, b)\} \\
&= \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 = a^2 + b^2\}
\end{aligned}
$$

Hence the equivalence classes are all circles centered at the origin.

(b) $a \sim a$ since $0 = a - a$ is divisible by n. So $\sim$ is reflexive. $a \sim b$ implies $a - b$ is divisible by n, whence $b - a = -(a - b)$ is also divisible by n, and, therefore $b \sim a$, i.e., $\sim$ is symmetric. Finally, if $a \sim b$ and $b \sim c$, Then, both $a - b$ and $b - c$ are divisible by n, whence $a-c=(a-b)+(b-c)$ is divisible by n. Hence $a\sim c$ and $\sim$ is also transitive. Thus $\sim$ is an equivalence relation on $\mathbf{Z}$. Suppose that $a\in\mathbf{Z}$. Then

$$\begin{aligned}[a] &= \{x\in\mathbf{Z} : x\sim a\}\\ &= \{x\in\mathbf{Z} : x-a \text{ is divisible by } n\}\\ &= \{x\in\mathbf{Z} : x-a=kn, k\in\mathbf{Z}\}\\ &= \{a+kn : k\in\mathbf{Z}\}.\end{aligned}$$

Thus, the equivalence class of a consists of all integers that leave the same remainder as a when divided by n. Hence there are n distinct equivalence classes corresponding to the different remainders $0,1,\ldots,n-1$ of the division by n.

(c) $a\sim a$ since $f(a)=f(a)$. So $\sim$ is reflexive. $a\sim b$ implies $f(a)=f(b)$, whence $f(b)=f(a)$, and, therefore $b\sim a$, i.e., $\sim$ is symmetric. Finally, if $a\sim b$ and $b\sim c$, Then, both $f(a)=f(b)$ and $f(b)=f(c)$, whence $f(a)=f(c)$, i.e., $a\sim c$ and $\sim$ is also transitive. Thus $\sim$ is an equivalence relation on S. ■

Problem 3 *(a) The Fibonacci sequence* $1,1,2,3,5,8,13,\ldots$ *is defined by* $F_1=F_2=1, F_{n+2}=F_{n+1}+F_n$, *for* $n\geq 1$. *Show that* $(F_{n+1})^2-F_nF_{n+2}=(-1)^n$.

(b) Use the Euclidean algorithm to calculate $\gcd(52,135)$ *and write it as a linear combination of 52 and 135.*

(c) Show that if $\gcd(n,r)=1$, *then there exists an integer* s *such that* $\gcd(n,s)=1$ *and* $rs\equiv 1 \bmod n$.

(d) Write the multiplication table mod 7 *of* $U(7)$ *and* mod 8 *of* $U(8)$.

Solution:

(a) We use induction on n. For the base of the induction, let $n=1$. Then

$$F_2^2-F_1F_3=1^2-1\cdot 2=-1=(-1)^1.$$

Now, for the inductive step, suppose that the relation is true for $n=k$, i.e., that $(F_{k+1})^2-F_kF_{k+2}=(-1)^k$. We will show that the relation is true for $n=k+1$:

$$\begin{aligned}(F_{k+2})^2-F_{k+1}F_{k+3} &= (F_{k+1}+F_k)^2-F_{k+1}(F_{k+2}+F_{k+1})\\ &= F_{k+1}^2+2F_{k+1}F_k+F_k^2-F_{k+1}F_{k+2}-F_{k+1}^2\\ &= F_k^2+2F_kF_{k+1}-F_{k+1}F_{k+2}\\ &= F_k^2+2F_kF_{k+1}-F_{k+1}(F_{k+1}+F_k)\\ &= F_k^2+2F_kF_{k+1}-F_{k+1}^2-F_{k+1}F_k\\ &= F_k^2+F_kF_{k+1}-F_{k+1}^2\\ &= -F_{k+1}^2+F_k(F_{k+1}+F_k)\\ &= -F_{k+1}^2+F_kF_{k+2}\\ &= -(F_{k+1}^2-F_kF_{k+2})\\ &= -(-1)^k\\ &= (-1)^{k+1}\end{aligned}$$

(b) We have

$$\begin{aligned} 135 &= 2 \cdot 52 + 31 \\ 52 &= 1 \cdot 31 + 21 \\ 31 &= 1 \cdot 21 + 10 \\ 21 &= 2 \cdot 10 + 1 \\ 10 &= 10 \cdot 1 + 0 \end{aligned}$$

Hence $\gcd(52, 135) = 1$. Following the steps above in the reverse direction one finds that $1 = 13 \cdot 52 - 5 \cdot 135$.

(c) Since $\gcd(n, r) = 1$, there exist $t, s \in \mathbf{Z}$, such that $tn + sr = 1$. We claim that this s satisfies the requirements. First

$$\begin{aligned} rs &= 1 - tn \\ &\equiv 1 \end{aligned}$$

Furthermore, if $d = \gcd(n, s)$, then, there exist $x, y \in \mathbf{Z}$, such that $n = dx$ and $s = dy$. Then $tdx + rdy = 1$, whence $(tx + ry)d = 1$, i.e., d is a positive divisor of 1, whence $d = 1$ and $\gcd(n, s) = 1$.

(d) We have $U(7) = \{1, 2, 3, 4, 5, 6\}$ and $U(8) = \{1, 3, 5, 7\}$ and

$\cdot$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

■

Problem 4 *(a) Calculate the value of* i^{38} *and express your answer in the form* $a + bi, a, b \in \mathbb{R}$.

(b) Calculate the value of $(1 + i)^7$ *and express your answer in the form* $a + bi, a, b \in \mathbb{R}$.

(c) Find all the solutions to the equation $z^4 = -1$.

Solution:

(a) $i^{38} = i^{4 \cdot 9 + 2} = (i^4)^9 i^2 = 1^9(-1) = -1$.

(b) We have $1 + i = \sqrt{2}(\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}) = \sqrt{2}(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4})$. Therefore, by De Moivre's formula

$$\begin{aligned} (1+i)^7 &= [\sqrt{2}(\cos\tfrac{\pi}{4} + i\sin\tfrac{\pi}{4})]^7 \\ &= \sqrt{2}^7(\cos\tfrac{7\pi}{4} + i\sin\tfrac{7\pi}{4}) \\ &= 8\sqrt{2}(\cos(-\tfrac{\pi}{4}) + i\sin(-\tfrac{\pi}{4})) \\ &= 8\sqrt{2}(\tfrac{\sqrt{2}}{2} - i\tfrac{\sqrt{2}}{2}) \\ &= 8 - i8. \end{aligned}$$

(c) Let $z = r(\cos\phi + i\sin\phi)$. Then

$$z^4 = r^4(\cos(4\phi) + i\sin(4\phi)) = \cos\pi + i\sin\pi.$$

Thus $r = 1$ and $4\phi = \pi + 2k\pi$, whence $\phi = \frac{\pi}{4} + k\frac{\pi}{2}$. The four different solutions are obtained by setting $k = 0, 1, 2, 3$. We have

k	ϕ	z
0	$\frac{\pi}{4}$	$\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$
1	$\frac{3\pi}{4}$	$-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$
2	$\frac{5\pi}{4}$	$-\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$
3	$\frac{7\pi}{4}$	$\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$

■

Problem 5 *(a) Perform the operation* $\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}\begin{bmatrix} 2i & i \\ -i & 1 \end{bmatrix}$ *in* $M(2, \mathbf{C})$.

(b) Calculate the determinant of $\begin{bmatrix} 5 & 1 \\ 2 & 2 \end{bmatrix}$ *in* $\mathbf{Z}_7$.

(c) Determine whether $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ *is invertible in* $M(2, \mathbf{C})$ *and, if so, calculate its inverse.*

(d) Determine whether $\begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix}$ *is invertible in* $M(2, \mathbf{Z}_5)$ *and, if so, calculate its inverse.*

(e) Find all the invertible matrices in $M(2, \mathbf{Z}_2)$.

Solution:

(a) $\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}\begin{bmatrix} 2i & i \\ -i & 1 \end{bmatrix} = \begin{bmatrix} 1+2i & 2i \\ -2+i & -2 \end{bmatrix}$.

(b) $\begin{vmatrix} 5 & 1 \\ 2 & 2 \end{vmatrix} = 5 \cdot 2 - 1 \cdot 2 = 3 - 2 = 1.$

(c) $\begin{vmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{vmatrix} = \cos^2\theta + \sin^2\theta = 1 \neq 0$. Hence, $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}$ is invertible and

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}^{-1} = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) \\ \sin(-\theta) & \cos(-\theta) \end{bmatrix}.$$

(d) $\begin{vmatrix} 4 & 1 \\ -3 & 2 \end{vmatrix} = 4 \cdot 2 - 1(-3) = 3 - 2 = 1 \neq 0$. Hence $\begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix}$ is invertible and its inverse is $\begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix}^{-1} = \begin{bmatrix} 2 & 4 \\ 3 & 4 \end{bmatrix}$.

(e) An easy analysis of the determinant of $ad - bc$ of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with $a, b, c, d \in \mathbf{Z}_2$ shows that it is nonzero for the following six matrices

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

■