CISC 203 Problem Set 1

Cain J. B. Susko

November 22, 2021

1. (a) using euclids algorithim:

$$(a \mod b) = c$$

if $c = 0$ **then the answer is** b **else, the answer is** $gcd(b, c)$

we are given $a = 34,\ b = 55$, therefore:

$$\begin{aligned}
34 \mod 55 &= 34 \\
55 \mod 34 &= 21 \\
34 \mod 21 &= 13 \\
21 \mod 13 &= 8 \\
13 \mod 8 &= 5 \\
8 \mod 5 &= 3 \\
5 \mod 3 &= 2 \\
3 \mod 2 &= 1 \\
2 \mod 1 &= 0
\end{aligned}$$

thus the $\gcd(34, 55) = 1$
to then find the numbers m, n in the equation:

$$\gcd(34, 55) = 34m + 55n$$

we would first rearrange for m:

$$m = \frac{1}{34}(1 - 55n)$$

and then substitute it in the equation:

$$1 = 34\left(\frac{1}{34}(1 - 55n)\right) \Rightarrow \qquad n = 0$$

$$1 = 34m + (55 \times 0) \Rightarrow \qquad m = \frac{1}{34}$$

therefore: $1 = 34 * \frac{1}{34} + 55 * 0$

(b) there are no integer solutions because in $6x \equiv 2 \mod 12$, $6x$ can only be multiples of 6 (and 12) and because of this:

$$6x \mod 12 = \{6, 0\}$$

therefore it is not possible for $6x$ to be congruent with 2 in mod 12

(c) if $\gcd(a, b) = 1$ then a and b are relatively prime. this means that a and b's only divisor in common are 1. because we know that $a|bc$, we can definitively say that c is a denominator of a as we know for sure that any divisor save 1 is not shared between a and b. therefore, for the conditions to be satisfied $(a|bc)$ it must be true that $a|c$.

(d) presume it is possible for $n^2 + 1 \not\equiv 0 \mod 6$. the answers for this equation are as follows:

$$n = 0 \to 1 \qquad n = 1 \to 2$$
$$n = 2 \to 5 \qquad n = 3 \to 4$$
$$n = 4 \to 5 \qquad n = 5 \to 2$$

this pattern repeats forever, as is the nature of modular arithmetic. thus, we have reached a contradiction as no number n within mod 6 can evaluate to 0
therefore, we have shown that $n^2 + 1 \not\equiv 0 \mod 6$.

2. (a) the problem can be refactored into a system of congruences like so:

$$x \equiv 1 \mod 5 \tag{1}$$
$$x \equiv 3 \mod 7 \tag{2}$$
$$x \equiv 7 \mod 8 \tag{3}$$

(b) we start with finding an x that satisfies (1) and (2) by substituting one equation in the other:

$$(1)\ x = 1 + 5k \qquad (2)\ x = 3 + 5l$$

$$x \equiv 31 \mod 35 \tag{4}$$

now, buy substituting (4) into (3)

$$(4)\ x = 31 + 35s \qquad (3)\ x = 7 + 8p$$

$$x \equiv 31 \mod 280 \tag{5}$$
$$x = 31 + 280n \tag{6}$$

and thus we have found (5), the solution to the congruence system using the Chinese remainder theorem. using (6) we can find the greatest number of groups n mod 280 where $x < 1000$, which is $n = 3$ where $x = 871$

3. (a) we know that any combination of integers in addition and subtraction result in an integer. therefore it must be true that $x + xy \in \mathbb{Z}$ for all $x, y \in \mathbb{Z}$

(b) show that: $(x * y) * z = x * (y * z)$

$$(x * y) * z = x * (y * z)$$
$$(x + xy) + (x + xy) \times z = x + x \times (y + yz)$$
$$x + xy + xz + xyz = x + xy + xyz$$

as you can see we cannot alter the LHS or RHS to equal the other as the terms on each side are unequal. thus showing that $(\mathbb{Z}, *)$ is not associative.

(c) if the operation were: $x * y = xy$ then the identity element would be $1 \because 1 \times z = z$ for any integer if we assume that $xy = y$ then $x * y = x + y$

$$x + y \neq x \vee y$$

therefore there is no identity element

$$x * y \neq x \vee y$$

(d) we know that there is an inverse $\forall_x \forall_y (x, y \in \mathbb{Z})$ as the inverse of any integer a is $\frac{1}{a}$ or a^{-1}

(e) given:

$$x * y = y * x$$
$$x + xy = y + xy$$
$$x + xy \neq y + xy$$

thus showing * is not communative

4. (a) the multiplication table would be:

$\cdot$	I	A_1	A_2	A_3	A_4	A_5
I	$I \cdot I$	$I \cdot A_1$	$I \cdot A_2$	$I \cdot A_3$	$I \cdot A_4$	$I \cdot A_5$
A_1	$A_1 \cdot I$	$A_1 \cdot A_1$	$A_1 \cdot A_2$	$A_1 \cdot A_3$	$A_1 \cdot A_4$	$A_1 \cdot A_5$
A_2	$A_2 \cdot I$	$A_2 \cdot A_1$	$A_2 \cdot A_2$	$A_2 \cdot A_3$	$A_2 \cdot A_4$	$A_2 \cdot A_5$
A_3	$A_3 \cdot I$	$A_3 \cdot A_1$	$A_3 \cdot A_2$	$A_3 \cdot A_3$	$A_3 \cdot A_4$	$A_3 \cdot A_5$
A_4	$A_4 \cdot I$	$A_4 \cdot A_1$	$A_4 \cdot A_2$	$A_4 \cdot A_3$	$A_4 \cdot A_4$	$A_4 \cdot A_5$
A_5	$A_5 \cdot I$	$A_5 \cdot A_1$	$A_5 \cdot A_2$	$A_5 \cdot A_3$	$A_5 \cdot A_4$	$A_5 \cdot A_5$

(b) G must satisfy 3 properties:

Closure we can see that $(G, \cdot)$ is closed because:

$$\begin{aligned} x \cdot I &= x & x \cdot x &= x \\ A_1 \cdot A_2 &= A_3 & A_1 \cdot A_3 &= A_2 \\ A_1 \cdot A_4 &= A_5 & A_1 \cdot A_5 &= A_4 \\ A_2 \cdot A_3 &= A_4 & A_2 \cdot A_4 &= A_3 \\ A_2 \cdot A_5 &= A_1 & A_3 \cdot A_4 &= A_2 \\ A_3 \cdot A_5 &= A_4 & A_4 \cdot A_5 &= A_2 \end{aligned}$$

thus $G_x \cdot G_x \in G$

Identity Element G has an identity element I where $x \times I = I \times x = I$. for example:

$$A_2 \times I = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \qquad I \times A_2 = I \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \times \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Inverse one can determine if a 3×3 matrix has an inverse by finding the determinant of said matrix. if the determinant is 0 there is no inverse. and because we know G has closure, we only need to test the matrices in G:

$$\begin{aligned} \det(I) &= 1 & \det(A_1) &= -1 \\ \det(A_2) &= -1 & \det(A_3) &= 1 \\ \det(A_4) &= -1 & \det(A_5) &= 1 \end{aligned}$$

thus showing all matrices in G have an inverse

thus $(G, \times)$ satisfies the requirements to be a group

5. (a) the table would be:

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

(b) G must satisfy 4 properties to be an Abelian group:

Communative G is communative if for all elements, $a * b = b * a$:

$$1 \times 1 = 1 = 1 \times 1$$

$$i \times i = i = i \times i$$

$$-1 \times -1 = 1 = -1 \times -1$$

$$-i \times -i = -1 = -i \times -i$$
$$1 \times i = i = i \times 1$$
$$1 \times -1 = -1 = -1 \times 1$$
$$1 \times -i = -i = -i \times 1$$
$$i \times -1 = -i = -1 \times i$$
$$i \times -i = -i = -i \times i$$
$$-1 \times -i = i = -i \times -1$$

therefore showing that $x \times y = y \times x$

Closure if one were to look at the table, can see that each element in the table is also in $G = \{1, i, -1, -i\}$
therefore showing $(G, \times)$ is closed

Identity Element the identity element of $(G, \times)$ is:

$$1 \times 1 = 1$$
$$1 \times i = i$$
$$1 \times -1 = -1$$
$$1 \times -i = -i$$

therefore showing 1 is the identity element in $(G, \times)$

Inverse all numbers $G \in \mathbb{C}$ can be found using the formula: $\frac{1}{g}$ where $g \in G$

thus showing that $(G, \times)$ is an Abelian Group.

(c) to determine if G is cyclic we must find the generator element. this is an element where it, its inverse, and the group operation, can generate any number in $(G, \times)$:

$$i = i$$
$$i \times i = -1$$
$$i^{-1} = -i$$
$$i^{-1} \times i^{-1} = 1$$

therefore the generator element in $(G, \times)$ is i

(d) first, the group $(\mathbb{Z}_4, +)$ is:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

we can see that there are specific elements in $(\mathbb{Z}_4, +)$ map to specific elements in $(G, \times)$ such that:

$$f : G \to \mathbb{Z}_4$$

$$1 \to 0 \qquad i \to 1$$
$$-1 \to 2 \qquad -i \to 3$$

to show f is an isomorphism we must also show that it is injective and surjective:

Surjective we can see that each element in $(G, \times)$ is mapped to an element in $(\mathbb{Z}_4, +)$. therefore f is onto

Injective we can see that each element in $(G, \times)$ is mapped to a unique element in $(\mathbb{Z}_4, +)$. therefore f is one-to-one

thus we have shown that $f : G \to \mathbb{Z}_4$ is an isomorphism