CISC 203 Problem Set 4

Amy Brons

April 3, 2022

1. Let a = 54, and b = 231. Use Euclid's algorithm to find gcd(a,b) and to find integers m and n such that gcd(a,b) = am + bm.

   To do this, we can follow the following steps in the Euclidean Algorithm :

   $231 = 4(54) + 15$

   $54 = 3(15) + 9$

   $15 = 1(9) + 6$

   $9 = 1(6) + 3$

   $6 = 2(3) + 0$

   Therefore because the last line has no remainder, the gcd can be determinined one above that.

   $gcd(54, 231) = 3$

   Next from these lines of calculation we can determine that:

   $3 = 1(9) + -1(6)$

   $6 = 1(15) + -1(9)$

   $9 = 1(54) + -3(15)$

   $15 = 231 + -4(54)$

   These determinations will act as replacements in determining our final solution:

   $3 = 1(9) + -1(6)$

   $= 1(9) + -1(1(15) - 1(9))$

   $= -1(15) + 2(9)$

   $= -1(15) + 2(1(54) - 3(15))$

   $= -1(15) + 2(54) - 6(15)$

   $= -7(15) + 2(54)$

$= -7(1(231) - 4(54)) + 2(54)$

$= -7(231) + 28(54) + 2(54)$

$= -7(231) + 30(54)$

$3 = 30(54) - 7(231)$

To check the math:

$3 = 30(54) - 7(231)$

$3 = 1620 - 1617$

$3 = 3$

Therefore it can be determined that:
$gcd(54, 231) = 30(54) - 7(231)$

Such that:

$m = 30$
$n = -7$

2. i) Given that $x \in \mathbb{N}$ and $0 < x < n$, we can try to find the congruences for $3x \equiv 12(mod 39)$

This can be done by first rearranging the equation:

$3x \equiv 12(mod 39)$
$3x - 12 \equiv 0(mod 39)$

$0(mod 39)$ can also be written as 39k, given $k \in \mathbb{Z}$ so:

$3x - 12 \equiv 39k$

$3x = 39k + 12$

$x = \frac{39k+12}{3}$

$x = 13k + 4$

Given the calculations completed, it can be known that $x = 13k + 4$ and $0 < x < 39$

Therefore:
When k = 0, $x = 13(0) + 4 = 4$
When k = 1, $x = 13(1) + 4 = 17$
When k = 2, $x = 13(2) + 4 = 30$
When k = 3, $x = 13(3) + 4 = 43$, which is outside of our x range and therefore too large.

Therefore it is known that the congruences are equal to $x = 4, 17, 30$

ii) Given that $x \in \mathbb{N}$ and $0 < x < n$, we can try to find the congruences for $6x \equiv 3(mod12)$

This can be done by first rearranging the equation:

$6x \equiv 3(mod12)$
$6x - 3 \equiv 0(mod12)$

$0(mod12)$ can also be written as 12k, given $k \in \mathbb{Z}$ so :

$6x - 3 \equiv 12k$
$6x = 12k + 3$

$x = \frac{12k}{6} + \frac{3}{6}$

$x = 2k + \frac{1}{2}$

Therefore there is no solutions to the equivalence because $n \notin \mathbb{N}$, given that a fraction is added to the integer k. Therefore there are no possible congruences.

3. Let gcd(a,b) = d. Prove that $gcd(\frac{a}{d}, \frac{b}{d}) = 1$
For this explanation, we can look to Module 10, Theorem 11.Theorem 11 states that:
Let a and b be integers, at least one of them not 0. The gcd d of a and b can be written as:

d = ax + by

for some integers x and y; and d is the smallest integer that can be written in this form.

Now to look at this Theorem related to our equation if $gcd(a, b) = d$, this can be rewritten as $d = ax+bx$. Therefore:

$gcd(\frac{a}{ax+bx}, \frac{b}{ax+bx} = gcd(\frac{1}{x(1+b)}, \frac{1}{x(a+1)})$

Given that both of these values are fractions, to find the gcd, the common divisor must be equal to one. This the mathematically logical solution for this problem, given that both the a and b values become present in the divisor, meaning they need to be relatively prime to each other, and therefore the value of $gcd(\frac{a}{d}, \frac{b}{d}) = 1$.

4. a) To find this system we need to find three congruences. Given the information listed in the question, it is known that:

$x = 5n + 1$
$x = 7k + 3$
$x = 9m + 7$

Therefore it can be determined that the system of congruences is:

$x \equiv 1(mod5)$
$x \equiv 3(mod7)$
$x \equiv 7(mod9)$

b) To solve this system, we need to determine the values of N, N_1, N_2, N_3:

$N = 5 \cdot 7 \cdot 9 = 315$

$N_1 = \frac{N}{5} = 63$

$N_2 = \frac{N}{7} = 45$

$N_3 = \frac{N}{9} = 35$

$N_i X_i \equiv 1(mod n_i)$

$N_1 X_1 \equiv 1(mod 5)$
$63 X_1 \equiv 1(mod 5)$
$63 \cdot 2 \equiv 1(mod 5)$
$X_1 = 2$

$N_2 X_2 \equiv 1(mod 7)$
$45 X_2 \equiv 1(mod 7)$
$45 \cdot 5 \equiv 1(mod 7)$
$X_2 = 5$

$N_3 X_3 \equiv 1(mod 9)$
$35 X_3 \equiv 1(mod 9)$
$35 \cdot 8 \equiv 1(mod 9)$
$X_3 = 8$

Next the following formula needs to be used:

$x = (n_1 N_1 X_1 + n_2 N_2 X_2 + n_3 N_3 X_3)(mod N)$
$= ((1 \cdot 63 \cdot 2) + (3 \cdot 45 \cdot 5) + (7 \cdot 35 \cdot 8))(mod 315)$
$= (126 + 675 + 1960)(mod 315)$
$= 2761(mod 315)$
$= 241$

Next it is known that we need to find the largest possible value that works for this, given the value must be under 700. To achieve this, we can add the value of N, so $241 < x < 700$

$241 + 315(1) = 556$
$241 + 315(2) = 871$ – This is over 700, so does not count.

Therefore the largest number of 'things' that can solve this system of congruences is 556.

To check this:
$556 - 1 = 5n$ - works as this is divisible by 5
$556 - 3 = 7k$ - works as this is divisible by 7
$556 - 7 = 9m$ - works as this is divisible by 9.

Therefore this is proved.

5. Consider the binary operation $*$ defined by $x * y = x + xy$ for $x, y \in \mathbb{Z}$. Show whether $*$ fulfills:

   (a) Closure:

Closure holds on a binary operation is $x * y \in S, \forall x, y \in S$

$x * y = x + xy$ for $x, y \in \mathbb{Z}$

So therefore if $x \in \mathbb{Z}$ and $y \in \mathbb{Z}$ then this means that $\in \mathbb{Z}$, and $x + xy \in \mathbb{Z}$ so $x * y \in \mathbb{Z}$.

Therefore closure holds.

(b) Associative property:

This means that rearranging the parenthesis will not change the result of the expression, and therefore is a rule of replacement. This can be disproven:

$(x * y) * n = (x + xy) * n$
$= (x + xy) + (x + xy) \cdot n$
$= x + xy + xn + xyn$

Now looking at this rearranged:

$x * (y * n) = x * (y + yn)$
$= x + x(y + yn)$
$= x + xy + xyn$

$x + xy + xn + xyn \neq x + xy + xyn$ Because of the addition of the xn term, these do not equal and therefore replacement is not valid.
Associativity does not hold.

(c) Identity element:

Finding the identity element for this can be done by finishing when an element is multiplied by an integer until it is equal to itself. So:

$x \cdot n = x = x + xn$
$xn = x - x$
$xn = 0$
$n = 0$

and

$y \cdot n = y = y + yn$
$yn = y - y = 0$
$yn = 0$
$n = 0$

Therefore the identity element is a zero.

(d) Existence of an inverse for all $x \in \mathbb{Z}$
To find the inverse of x, we must find x^{-1}.

$x + xy = 0$
$x = -xy$
$-1 = y$
$x = -x(-1)$

$x = x$

Therefore there is no inverse for x.

(e) Commutative property

If the communicative property holds, it must be true that $x * y = y * x$

Given that $x * y = x + xy$

$y * x = y + yx = y + xy$

Because of this we can determine that $x * y \neq y * x$

and therefore the communicative property does not hold.

6. a) The completed Cayley table for G:

$\circ$	α	β	σ	π
α	β	σ	π	α
β	σ	π	α	β
σ	π	α	β	σ
π	α	β	σ	π

b) To show that $(G, \circ)$ is an Abelian group, the following properties must be proven:

Closed:
Closure is proven immediately, as a Cayley table would not be able to be produced without a closed group.

Commutativity:
As shown here in the table, this group is commutative. This is evidenced by the symmetric values along the tables diagonal line.

$\circ$	α	β	σ	π
α	β	σ	π	α
β	σ	π	α	β
σ	π	α	β	σ
π	α	β	σ	π

Associativity:
It must be proven that $(\alpha \circ \beta) \circ \sigma = \alpha \circ (\beta \circ \sigma)$

This can be seen that:

$(\sigma) \circ \sigma = \alpha \circ (\alpha)$

$\beta = \beta$
Therefore this is proven for this group. It can also be shown by proving associativity on any other elements. For example it can also be shown on:
$(\pi \circ \beta) \circ \alpha = \pi \circ (\beta \circ \alpha)$

This can be seen that:
$(\beta) \circ \alpha = \pi \circ (\sigma)$
$\sigma = \sigma$

Therefore associative property is proven.

Identity element:
The identity element occurs when an element on itself, produces itself.
The identity element here is π. This is evidenced on the table here, where $\pi \circ \pi = \pi$

$\circ$	α	β	σ	π
α	β	σ	π	α
β	σ	π	α	β
σ	π	α	β	σ
π	α	β	σ	π

Inverse for every element:
Here is shown each groups inverse. This is due to finding the relation to the identity element.

$\circ$	α	β	σ	π
α	β	σ	π	α
β	σ	π	α	β
σ	π	α	β	σ
π	α	β	σ	π

c) G is a cyclic group which is proven to Abelian, and because all elements can be produced from a single element. All groups can either be produced using the α group or the σ group. It is known that π and β are not generator elements because they produce the identity element when on themselves. Therefore either α or σ are the generator element. Given that there are n elements, the number of generator elements can be found through $\varphi(n)$. Through Euler's Totient we can tell that there must be two generator elements:

$\varphi(4) = 1 - (\frac{1}{2})$
$= 4 \cdot \frac{1}{2}$
$= 2$

Therefore this group is cyclic with 2 generator elements, α and σ

d) This group is isomorphic. This can be shown by looking at these Cayley tables and then providing the function $f : G \quad Z_4$

Here are the Cayley tables:

$\circ$	α	β	σ	π
α	β	σ	π	α
β	σ	π	α	β
σ	π	α	β	σ
π	α	β	σ	π

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Here we can now see how to map $G \quad Z_4$. When mapping elements it can be seen that because 0 is the identity element in Z_4, 0 is mapped to π. Next, because 2 on itself becomes the identity element, 2 is mapped onto β. When filling in the α and σ generator elements as 3 and 1, respectively, it becomes clear that these as isomorphic.

This is because of the fact that when the $G \quad Z_4$ function occurs, a Cayley table like this can be produced:

$\bigcirc$	0	1	2	3
0	π	σ	β	α
1	σ	β	α	π
2	β	α	π	σ
3	α	π	σ	β

This means that when rearranged, these Cayley table results would be identical, and therefore this is an isomorphism.

e) The order of the elements can be obtained by defining the order of the elements as their smallest positive integer.
When looking at the groups, and the relation in the group to the smallest integer (1) it can be seen that:
$\alpha 1 = 2$
$\beta 1 = 3$
$\sigma 1 = 4$
$\pi 1 = 1$

and therefore the order of the group is:
$G = \pi, \alpha, \beta, \sigma$

7. a) Let $\mathbb{Z}_{15}^* = 1, 2, 4, 7, 8, 11, 13, 15$

To show that $(H, \otimes)$ is a subgroup, lets first find it's size.
According to Module 11, Theorem 23, $(H, \otimes)$ is a subgroup of $(\mathbb{Z}_{15}^*, \otimes)$ such that $|H| = a, b = |\mathbb{Z}_{15}^*$ and then $a|b$.
This means that $|H||8$.
This means the size much have a size of 1, 2, 4, or 8.

This gives us the subgroups:
$\{1\}, \{1,4\}, \{1,2,4,8,14\}, \{1,2,4,7,8,11,13,14\}$

Therefore, the generator element is found in the fourth subgroup, and the subgroup of H is shown to be:
$(H, \otimes) = \{1,4\}$

b) i) $|\mathbb{Z}^*_{330}|$ To find this, lets use Euler's Totient:

$\varphi(n) = n\Pi_{p|n}(1 - \frac{1}{p})$

where p is prime. Given the value 330 we can find the primes to be:
2, 3, 5, 11 as these are the numbers which divide 330 fully.
Therefore we can put this into Euler's Totient:

$\varphi(n) = n\Pi_{p|330}(1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{11})$

$= 330 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} \cdot \frac{10}{11}$
$= 80$

Therefore $|\mathbb{Z}^*_{330}| = 80$

ii) $|\mathbb{Z}^*_{121}|$ To find this, lets use Euler's Totient:

$\varphi(n) = n\Pi_{p|n}(1 - \frac{1}{p})$

where p is prime. Given the value 121 we can find the primes to be:
11. This is the only divisor of 121, so we can put this into the formula:
$\varphi(n) = n\Pi_{p|121}(1 - \frac{1}{11})$

$= 121 \cdot \frac{10}{11}$

$= 110$

Therefore $|\mathbb{Z}^*_{121}| = 110$

8. a) Let G be a simple graph with 11 vertices, in which the sum of the degrees of all the vertices is known to be at least 33. To solve this, we need to look back at the 2nd Module 6 principle, known as the Pigeonhole Principle. This principle states that if n pigeons are put into m holes where $n > m$, then at least one hold must contain more than one pigeon.
To relate this to the graph, we need to see what is the amount of pigeons(degrees) to fit in each hole (vertices).
There we can see that:

$\frac{33}{11} = 3$

Therefore we can prove that each vertices must have at least 3 degrees. However this does not prove that at least one vertex has a degree of 4.

In fact, the scenario in which each vertex has a degree of 3 is a direct counterexample to the claim that G must have one vertex with a degree of 4.

b) To determine the sum of the degrees of all vertices in T, given that T is a tree with n vertices, we must look at Module 12, Theorem 12. This is the handshake lemma, and it states that:

Given a graph $G = (V, E)$

$\sum_{u \in V} deg(u) = 2 \cdot |E|$

Therefore the sum of the degrees will be twice the number of edges. It is also known through Module 12, Theorem 45 that a tree graph that there must be $n - 1$ edges for n vertices.
Therefore the sum of degrees will be determined as:

$\sum_{n \in T} deg(n) = 2(n - 1)$

c) According to Module 12, Definition 46, a Eulerian tour is defined as a Eulerian trail that begins and ends at the same vertex. Additionally this can be viewed in tandem with module 12, Theorem 47. This states that a graph containing a Eulerian tour has every vertex of an even degree. Given that each vertex must have an even degree it can be said that the sum of the vertices must also be even because even + even = even.

Looking back now at Module 12, Theorem 12, the handshake lemma, it is stated that:

Given a graph $G = (V, E)$

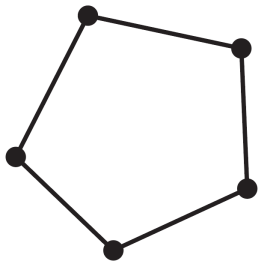
$\sum_{u \in V} deg(u) = 2 \cdot |E|$

Therefore the sum of the degrees is double the number of edges. This means that:

$2|v$ and $v = 2e$, where e is edges.

Therefore the number of edges can be odd or even because any number is even is it is multiplied by 2.

To disprove this we can look to a counter example. This graph would be an example of an Eulerian tour:



Evidently this graph is an Eluerian trail due to the fact that each edge can be walked exactly once to visit all of the vertices. However this graph also is an Eulerian tour, as the walk would start and end at the same vertices. This is all true and yet the graph contains an odd number of edges, therefore this is a counterexample.