Questions 1-5

1:

Addition:

Closure: to prove closure we can look at (17+17) mod 18, since 17 + 17 is the biggest possible sum attainable within this set we will get 34 mod 18 = 16 which is also in our set so this is good under the closure requirement

Associativity: we can look at two different addition equations contained within the set [(17+16)+15] and [17+(16+15)] bot mod 18 will result in 12 so we can say it meets the requriements for Associativity

Identity: The identity matrix is something where some element a in Z18 and some other element x in Z18 we get (a+x) mod 18 = a for all elements a in Z18, for this specific we see that if x is 0 we get our answer for identity

Inverse: Under modulo addtion all elements have an inverse element, under addition we will just need to do some subtraction ie. for element a = 1 the inverse is 18 - a = 18 - 1 = 17, we then can say 1 + 17 = 18 mod 18 = 0 which satisfies our Inverse need, for 0 the inverse is 0

Is a set satisfies all 4 properties.

Multiplication:

Closure: similar to addition we will take two elements from the set Z18 and multiply them here we get (17 * 17) mod 18 = 1

Associativity: we also met the need by doing a similar grouping within the set Z18 [(17*16)*15] mod 18 = [17*(16*15)] mod 18 = 12

Identity: Much like addition there is one number that is the element for all integer sets, which is 1 since any element * 1 should result in itself

Inverse: Under modulo multiplcation not all elements have an inverse element, this is because for a number to have a multiplicative inverse the two elements must be relatively prime and by nature even numbers do not follow this rule there for we can say under multiplication Z18 is not a group

Is not a set does not satisfy the inverse property

2: gcd(36459,27828) -> gcd(27828,8631) -> gcd(8631,1935) -> gcd(1935,891) -> gcd(891,153) -> gcd(153,126) -> gcd(126,27) -> gcd(27,18) -> gcd(18,9) therefore the gcd(36459,27828) = 9

3: It is not because we are unable to find 2 elements, a and b, such that gcd(a,b) = 0 therefore it cant be a group

4: gcd(32,27) = res 5, 1x32 - 1x27 -> gcd(27,5) = res 2, 1x27 - 5(res 5) -> gcd(5,2) = res 1, 1(res 5) - 2(res 2) -> 11x32 - 13x27 additive inverse of -13 = 19 therefore 19 is the multiplicative inverse of 27

5: using the same method above to find the MI of the coefficents of x then multiplying both sides by that and solving x = c*MI mod z we get the answers below

a. MI of 9 mod 13 = 3 -> x = 33 mod 13 = 7

b. MI of 6 mod 23 = 4 -> x = 12 mod 23 = 12

c. MI of 5 mod 11 = 9 -> x = 81 mod 11 = 4

Explanation of code

The code that I have in mult_inv.py takes in 3 arguments the last two being the number and the modulo number it then tries to divide the number by the modulo if they are equal it returns 1 if it is less than the modulo it returns 0 if the number is greater than the modulo it divides it out and returns the quotient. From this point it then multiplies through to get the new numbers to see if it can go lower, if it does it continues until either a multiplicative inverse is found or if none are found then it will return a GCD for the two numbers.