Modular Arithmetic Practice Exercises - Solutions

1. For each of the following computations modulo , write the unique answer, , such that .

Answers: In each case, find the product, then divide by the modulus (“n”) and find down the remainder.

a)   
Solution: and , so 5+6 is equivalent to 3 (mod 8)

b)   
Solution: so is equivalent to 2 (mod 8)

c)   
Solution: so is equivalent to 0 (mod 8)

d)

Solution: , so is equivalent to 6 (mod 7)

e)

Solution: , so is equivalent to 2 (mod 6)

f) **0**  
Solution: so is equivalent to 0 (mod 5)

Comment: For [f], note that any number multiplied by 5 will be equivalent to 0 (mod 5), since the result will be a multiple of 5. Note also that ­. So, in some sense, multiplying by 5 (under mod 5 rules) is the same as multiplying by 0.

g) **3** (mod 5)

Solution: so is equivalent to 3 (mod 5)

Alternate Solution:   
, which is a multiple of 5 plus 8.

So, under “mod 5” arithmetic rules, Since , it follows (by transitivity) that .

h) **1** (mod 8)

Solution: , so is equivalent to 1 (mod 8).

Alternate solution (for #1h):

A trick for reducing large products like this mod n is to rewrite each factor in terms of its remainder when divided by n. In this case, we could rewrite as

that is, each factor is one more than a multiple of 8. If we distribute the first sum, rewriting as we get:

where we observe that, since the left-hand and right-hand sides differ by a multiple of 8, they must be equivalent mod 8. Proceeding similarly, we have:

2. For each of the following modulo “equations” (technically they are called “congruences”), find the mod solution set; that is, find all solutions, , such that , where is the modulus of the “equation.”

Answers: All of the following can be found by a trial and error approach, by substituting each possible value from 0 to in place of and seeing which one(s) make the congruence true. Additional comments can be found on the next page.

a)

Answer: is the only solution

b)

Answer: is the only solution

c)

Answer: is the only solution

d)

Answer: There is no solution to this congruence

e)

Answer: There are three solutions: and

Comments on answers for #2:

a) Answer:

We *could* also this answer using regular algebra – subtract 2 from both sides, then divide both sides by 3, as normal. This approach also works for part (b) below. This approach works for congruences SOMETIMES, but not always, as we’ll see below…

b) Answer:

We can solve this problem similarly to part [a] above – first subtract 5 from both sides, to get , then divide by 3 on both sides to get . This turns out to be the correct solution, since -1 is equivalent to 7 (mod 8).

c) Answer: .

Comment: Regular algebra doesn’t work here, as it does for parts [a] and [b]. That is, we can’t just divide both sides by 2, since there is no number 5/2 in modular arithmetic. (Only integers are allowed!) However, rather than dividing both sides by 2, we could actually multiply both sides by 5. Why 5? Because, on the left hand side, . This would give us…

Now, on the left hand side, note that , which is a multiple of 9; this means . On the right hand side, since . Thus, the above equivalence is logically equivalent to .

Note: the key to this approach is that there is a number we can multiply by 2 to get a result of 1 under (mod 9) arithmetic rules – specifically, . So, in some sense, 5 is the “reciprocal” of 2 under (mod 9) rules, which means multiplying by 5 under (mod 9) rules is analogous to dividing by 2 in “regular” arithmetic! (Weird, right? But it’s valid!)

d) Answer: No solution.

In order for to have a solution, we’d have to have for some integer . However, this would imply , which is impossible, since 3 is a factor of the left-hand side but not of the right-hand side.

e) Answer: .

Comment: Regular algebra rules can be used sometimes in congruences, but you need to be careful! If we just divided by 3 on both sides here, we’d get the solution – this is correct, but, as it turns out, incomplete.

To find all solutions (by a method other than trial and error), note that we are looking for all values of x for which for some integer . This equation is true iff , which in turn is true iff for some integer . This happens if x is 2, 5, 8, 11, 14, 17, etc… in general, whenever . In (mod 9) arithmetic, this means we must have a number that is 2, 5, or 8 more than a multiple of 9; thus, we get multiple (mod 9) solutions.

Question to think about: Why did “regular algebra rules” – in particular, dividing both sides of the congruence by 3 – work for parts [a] and [b], but not for part [e]?