Question 1:

i. 150*92 mod 14 ***Answer = 10***

((150 mod 14)*(92mod14) mod 14) > ((10)*(8) mod 14) > (80 mod 14) > **10**

(150/14 has a remainder of 10, while 92/14 has a remainder of 8. Multiple them, the divide the product by 14 to get the remainder and the final answer: 10)

ii. 6 * (4/11) mod 14 ***Answer = 6***

Convert (4/11) to (88/11) because 88 follows mod 14 + 14 and is divisible by 11 > ((6 mod 14) * (8 mod 14) mod 14) > ((6)*(8) mod 14 > ((48)mod14) > (48-14= 34-14 = 20 – 14 = 6

Added 14 to 4 until I got a number that could divide into 11, and used it to sub in for the fraction.

iii. 24/17 mod 14 ***Answer = 8***

Convert 24 to a multiple of 17 using mod 14 > ((136/17) mod 14) > (8) mod 14)) = 8

This one was pretty straight forward. Add 14 to 24 until you find 17 can divide it, and go from there.

iv. $4^8 * 5^{12}$ mod 14 ***Answer = 2***

$(((4^4) * (4^4)) * ((5^6) *(5^6))$ mod 14)

a. **$((4^2$ mod 14) $(4^2$ mod 14) $(4^2$ mod 14) $(4^2$ mod 14))> ((2)(2)(2)(2)) =16 mod 14= 2**

b. $((5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14) > ((11)(11)(11)(11)(11)) \bmod 14$ > CONVERT TO EQUIV CLASS > $((1)(1)(1)(1)(1)(1) \bmod 14) = 1$

c. $2*1 \bmod 14 = 2$

I was able to convert part 1 fine, but part b I ended up using the equiv classes conversion from Professor Paar to convert the 11 to 1.

v. $5^{10} * 6^8 \bmod 14$ ***Answer = 2***

a. $((5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14)(5^2 \bmod 14) \bmod 14) > ((11)(11)(11)(11)(11) \bmod 14$ > CONVERT WITH EQUIV CLASS > $((1)(1)(1)(1)(1) \bmod 14 = 1$

b. $((6^2 \bmod 14)(6^2 \bmod 14)(6^2 \bmod 14)(6^2 \bmod 14) \bmod 14) > ((8)(8)(8)(8)) \bmod 14$ > CONVERT > $((-2)(-2)(-2)(-2)) \bmod 14 > 16 \bmod 14 = 2$

c. $1*2 \bmod 14 = 2$

Question 2:

i. Show the elements of groups Z_{13} and Z^*_{13}

Answer:

Z13 elements would be {0,1,2,3,4,5,6,7,8,9,10,11,12}

Z*13 would be {1,2,3,4,5,6,7,8,9,10,11,12}

For Z_{13}, 0-12 can all go into 13, but 0 wouldn't go into Z^*_{13} because it would be 0 of multiplied. 13 is a prime number, so for Z*13, every number 1-12 has a GCD of 1.

ii. Show the elements of groups Z_{18} and Z^*_{18}

Answer:

Z_{18} elements would be {0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17}

Z*18 would be {1, 5, 7, 11, 13, 17}

Z_{18} can still use 0-17, BUT Z*18 cannot, because the number itself is not prime. Z*18's answer would exclude numbers that have some common factor with 18.

iii. Find the order of 5 in Z^*_{13} ***Answer= Order(5) is 4***

$5^1 = 5$ | $5^2 = 25 \bmod 13 = 12$ | $5^3 = 125 \bmod 13 = 8$ | $5^4 = 625 \bmod 13 = 1$

The order of 5 in z*13 is 4

iv. Find (if it exists) the multiplicative inverse of $5 \in Z_{13}$ (integer ring) ***Answer: MI = 8***

We start by rewriting it as 5*x = 1 mod 13. We will keep replacing X with 1 number up until we can calculate 5*x = 1 after calculating it with mod 13. Example being:

5*1 = 1 > 5=1 – Not the answer

5*2 = 1 > 10 = 1 – Not the Answer

5*3 = 1 > 15 mod 13 > 2 = 1 - Not the Answer

5*4 = 1 > 20 mod 13 > 7 = 1 – Not the Answer

5*5 = 1 > 25 mod 13 > 12 = 1 – Not the Answer

5*6 = 1 > 30 mod 13 > 4 = 1 – Not Answer

5*7 =1 > 35 mod 13 > 9 = 1 – Not Answer

5*8=1 > 40 mod 13 > 1= 1 – Answer!

V. Is Z^{*}_{13} a cyclic group? If so, what is its order and the generator element?

Z*13 would be {1,2,3,4,5,6,7,8,9,10,11,12} |Z*13| would be 12 ord (1) = 1. Ord (2) = 12

2^{12} mod 13 = 1 | 3^{12} mod 13 = 1 | 4^{12} mod 13 = 1 | 5^{12} mod 13 = 1 | 6^{12} mod 13 = 1

7^{12} mod 13 = 1 | 8^{12} mod 13 = 1 | 9^{12} mod 13 = 1 | 10^{12} mod 13 = 1 | 11^{12} mod 13 = 1

12^{12} mod 13 = 1

Answer:

The maximum order we got was 12, so it is cyclical, I think.

The generators would be: {1,2,3,4,5,6,7,8,9,10,11,12}

This question really confuses me since the examples in the notes used non-prime numbers as examples.