Theory Problems

Solve the following problems.

1. **Show whether or not the set of remainders Z12 forms a group with either one of the modulo addition or modulo multiplication operations.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Z12 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Add | 0 | 11 | 10 | 9 | 8 | 7 | 6 | 5 | 4 | 3 | 2 | 1 |
| Multi | - | 1 | - | - | - | 5 | - | 7 | - | - | - | 11 |

\*modulo multiplication does not form a group but modulo addition does form a group.

1. **Compute gcd(29495, 16983) using Euclid’s algorithm. Show all the steps.** 
   1. gcd(29495, 16983)
   2. gcd(16983, 12512)
   3. gcd(12512, 4471)
   4. gcd(4471, 3570)
   5. gcd(3570, 901)
   6. gcd(901, 867)
   7. gcd(867, 34)
   8. gcd(34, 17)
   9. gcd(17, 0) = 17
2. **With the help of Bezout’s identity, show that if c is a common divisor of two integers a, b > 0, then c | gcd(a,b)**(i.e. c is a divisor of gcd(a,b)).   
     
   gcd(a,b) = x\*a + y\*b  
   x\*a/c + y\*b/c  
   (x\*a + y\*b)\*1/c = gcd(a,b)/c   
   therefore since the gcd is an integer and the left side of the equation has to be a integer, gcd(a,b)/c = integer and therefore c is a divisor of gcd(a,b)
3. **Use the Extended Euclid’s Algorithm to compute by hand the multiplicative inverse of 25 in Z28. List all of the steps.** 
   1. Gcd(25, 28) = 1

28 = 25\*1 + 3 3 = 28 – 25(1)  
25 = 3 \*8 + 1 1 = 25 – 3(8)   
8 = 1\*8

1 = 25 – 3(8)   
1 = 25 – (28-25(1))(8)  
1 = 25 – 28\*(8) + 25(8)   
1 = 25(9) – 28(8)

9

1. **In the following, find the smallest possible integer x. Briefly explain (i.e. you don’t need to list out all of the steps) how you found the answer to each. You should solve them without using brute-force methods:**\*How I solved it was basically euclids method  
   Quotient = dividend \* divisor + remainder  
   (coefficient)\*x = a\*mod + remainder make a = 1, see if you get no remainder and keep doing this until you get the right number.
   * 1. **8x ≡ 11 (mod 13)**

8x = (a)\*13 + 11  
8x = 24  
x = 3

* + 1. **5x ≡ 3 (mod 21)**5x = 21\*1 + 3 🡪 No   
       5x = 21\*2 + 3  
       5x = 42 + 3  
       5x = 45   
       x = 9
    2. **8x≡9(mod7)**8x = 7\*a + 9   
       8x = 16   
       x = 2