Homework - 03

Terrence Randall

January 31st

1 Problem 1

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

Z_{12} forms a group with modulo addition: $\{Z_{12}, +\}$
-Closure: $(\forall x)(\forall y)$ x,y $\in Z_{12}$ then x + y $\in Z_{12}$
-Associative: $(\forall x)(\forall y)(\forall w)$ x,y,w $\in Z_{12}$ [(x + y) + w] mod 12 = [x + (y + w)] mod 12
-Identity Element: $(\forall x)$ x $\in Z_{12}$ such that x + 0 = x
-Inverse Element: $(\forall x)(\exists y)$ x,y $\in Z_{12}$ such that x + y = 0

2 Problem 2

Compute gcd(29495, 16983) using Euclid's algorithm. Show all the steps

gcd(29495, 16983)
gcd(16983, 12512)
gcd(12512, 4471)
gcd(4471, 3570)
gcd(3570, 901)

gcd(901, 867)
gcd(867, 34)
gcd(34, 17)
gcd(17, 0)

3 Problem 3

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)).

Given:
c $|$ a
c $|$ b
If q and z are integers
Since gcd(a,b) $=$ (q)a $+$ (z)b
Then c $|$ (q)a $+$ (z)b
and c $|$ gcd(a, b)

4 Problem 4

Use the Extended Euclid's Algorithm to compute by hand the multiplicative inverse of 25 in Z28 . List all of the steps.
gcd(25, 28)
gcd(28, 25)
gcd(25, 3) : residue 3 $=$ 1x28 - 1x25
gcd(3, 1) : residue 1 $=$ 1x25 - 8*(1x28 - 1x25)
9x25 - 8x28

5 Problem 5

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

Process: Find the multiplicative inverse of the first number, multiply this by the value on the right, take the modulus of this value, and the result is our x value

(a) $8x \equiv 11 \pmod{13}$
8^{-1} in mod $13 = 5$
$11 \text{ x } 5 = 55 \implies 55 \bmod 13 = 3$
$8 \text{ x } 3 = 24 \implies 24 \bmod 13 = 11$

(b) $5x \equiv 3 \pmod{21}$
5^{-1} in mod $21 = 17$
$3 \text{ x } 17 = 51 \implies 51 \bmod 21 = 9$
$5 \text{ x } 9 = 45 \implies 45 \bmod 21 = 3$

(c) $8x \equiv 9 \pmod{7}$
8^{-1} in mod $7 = 1$
$9 \text{ x } 1 = 9 \implies 9 \bmod 7 = 2$
$8 \text{ x } 2 = 16 \implies 16 \bmod 7 = 2$