# TEST 3

**(Math 258)**

1. (a) The expression $a \equiv b \bmod m$ means: (40 pts)

A. $a = bm$ B. $m \mid a + b$ C. $m \mid a - b$ D. $a \mid b + m$

C

(b) Prove that if $a$|bc, where $a, b, c \in Z_{>0}$, and **gcd**($a$,$b$) = 1, then $a|c$ .

Since **gcd**($a$,$b$) = 1 $\Rightarrow \exists$ $s$, $t$ such that $sa + tb = 1$ . Multiply both sides by c to get: $sac + tbc = c$. Since $a|sac$ and $a|tbc$ , then $a|(sac + a|tbc)$ , i.e. $a|c$ .

(c) Prove or disprove: If $ac \equiv bc \bmod m$ , where $a, b, c, m \in Z_{>0}$ , then $a \equiv b \bmod m$ .

Disprove: Take $a$ = 7 , $b$ = 4 , $c$ = 2 and $m$ = 6 . Then, $7 \cdot 2 \equiv 4 \cdot 2 \bmod 6$
but $7 \neq 4 \bmod 6$ .
(It works only if **gcd**($c$,$m$) = 1).

(d) True or False: The expression $a \equiv b \bmod m$ means that $a$ and $b$ are equal in $Z_m$ .

True

(e) True or False: 10 = 2 in $Z_4$ .

True

(f) True or False: $Z_4$ is a field .

False, 2 has no multiplicative inverse.

(g) Is $F$ = {1, -1, $i$, - $i$ } an Abelian group with "+" ?

No, it is <u>not</u> closed under addition. For example, 1+i $\notin$ $F$ .

(h) Find the smallest field with 2 elements.

$F = Z_2$

2. Use the *Extended Euclidean Algorithm* to write the gcd(277,123) as a linear combination of 277 and 123. Use that relation to find the inverse of 123 in $Z_{277}$. (20 pts)

$277 = 2 \cdot 123 + 31$
$123 = 3 \cdot 31 + 30$
$31 = 1 \cdot 30 + 1$
$30 = 30 \cdot 1 + 0$

Hence, gcd( 277, 123 ) = 1 .

$1 = (1)\,31 + (-1)30$
$1 = (1)31 + (-1)(123 - 3 \cdot 31)$
$1 = (4)31 + (-1)123$
$1 = (4)31 + (-1)123$
$1 = (4)(277 - 2 \cdot 123) + (-1)123$
$1 = (4)277 - (8)123 + (-1)123$
$1 = (4)277 + (-9)123$

Since 277 = 0 in $Z_{277}$, the last equation gives: $1 = (-9) \cdot 123$, i.e. $123^{-1} = -9$ .

3. (a) Encrypt the message "MATH IS FUN" by translating the letters into numbers, applying the encryption function given below, and then translating the numbers back into letters. The function is: $f(x) = (p+13) \bmod 26$. (10 pts)

| Letter | Number Value | $f(x)$ | Value at $f(x)$ | New letter value |
|---|---|---|---|---|
| M | 13 | (13 + 13) mod 26 | 0 | Z |
| A | 1 | (1 + 13) mod 26 | 14 | N |
| T | 20 | (20 + 13) mod 26 | 7 | G |
| H | 8 | (8 + 13) mod 26 | 21 | U |
| I | 9 | (9 + 13) mod 26 | 22 | V |
| S | 19 | (19 + 13) mod 26 | 6 | F |
| F | 6 | (6 + 13) mod 26 | 19 | S |
| U | 21 | (21 + 13) mod 26 | 8 | H |
| N | 14 | (14 + 13) mod 26 | 1 | A |

(b) Decrypt the encrypted message below, using the Caesar cipher:

WHVW WRGDB

Caesar cipher is shifting the letter's number value by 3.

| Letter | Number Value | $f(x)$ | Value at $f(x)$ | New letter value |
|---|---|---|---|---|
| W | 23 | 23 - 3 | 20 | T |
| H | 8 | 8 - 3 | 5 | E |
| V | 22 | 22 – 3 | 19 | S |
| W | 23 | 23 – 3 | 20 | T |
| W | 23 | 23 – 3 | 20 | T |
| R | 18 | 18 - 3 | 15 | O |
| G | 7 | 7 - 3 | 4 | D |
| D | 4 | 4 - 3 | 1 | A |
| B | 2 | 2 - 3 | 25 | Y |

So, the message is: TEST TODAY

4. Show that if $a$ is an odd integer, then $a^2 \equiv 1 \bmod 8$. (10 pts)

$a$ odd $\Rightarrow a = 2k + 1$
$\Rightarrow a^2 = (2k + 1)^2 = 4k^2 + 4k + 1$
$\Rightarrow a^2 - 1 = 4k^2 + 4k = 4k(k + 1)$

Since k and k+1 consecutive, one of them is even, say k, then $k = 2\lambda$

$a^2 - 1 \Rightarrow 4(2\lambda)(k + 1)$
$\Rightarrow 8\lambda (k + 1)$
$\Rightarrow 8 \mid a^2 - 1$

5. Solve the congruence $4x \equiv 5 \bmod 9$. List at least three integers that are solutions of the congruence. (10 pts)

The inverse of 4 in $Z_9$ is 7. Indeed, $4 \cdot 7 = 28 = 1 + 3 \cdot 9 = 1 + 3 \cdot 0 = 1$
So,

$$7 \cdot 4x \equiv (7 \cdot 5) \bmod 9 \Rightarrow x \equiv 35 \bmod 9 \Rightarrow x \equiv 8 \bmod 9$$

Hence, 8 is a solution . Another two solutions are: 17 and 26. As a matter of fact, all numbers of the form $8 + 9k$ , $k \in Z$, are solutions.

6. Solve the system of congruences: $x \equiv 2 \bmod 3$ (10 pts)
$x \equiv 1 \bmod 4$
$x \equiv 3 \bmod 5$.

We have, $m = 3 \cdot 4 \cdot 5 = 60$

and

$M_1 = 60 / 3 = 20$
$M_2 = 60 / 4 = 15$
$M_3 = 60 / 5 = 12$

Then, 2 is the inverse of 20 modulo 3
3 is the inverse of 15 modulo 4
3 is the inverse of 12 modulo 5

The solution for of the system is: $x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \bmod 60$ .