QUIZ 3
(Math 258)

1.**Show that is *a, b, c,* and *d* are integers s.t. *a*|*c* and *b*|*d*, then *ab*|*cd*.**

If $a|c$, then there exists some integer s such that $c = sa$.
Similarly, if $b|d$, then there exists some integer t such that $d = tb$.
So multiplying c and d, we get:

$$cd = (sa)(tb) = (st)(ab)$$

And this is, by definition, $ab|cd$.

2.**Show that is 2^n-1 is prime, then *n* is prime.**

Suppose n is not prime. Then by definition, $n = ab$ for some integers a and b, each greater than 1. Since $a>1$, $2^a - 1$ is greater than 1. The second factor is greater than 1 also. Thus, $2^n - 1 = 2^{ab} - 1$ is the product of two integers greater than 1, and hence is not prime. But this is a contradiction.

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

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.Find the gcd(111, 201) using the Euclidean algorithm.

201 = (1)111 + 90 , and we know that gcd(111, 201) = gcd(111, 90)

111 = (1)90 + 21 , and we know that gcd(111, 90) = gcd(90, 21)

90 = (4)21 + 6 , and we know that gcd(90, 21) = gcd(21, 6)

21 = (3)6 + 3 , and we know that gcd(21, 6) = gcd(6, 3)

6 = (2)3 + 0 , and we know that gcd(6, 3) = gcd(3, 0) = 3

Hence, from above, gcd(111, 201) = 3.

5.Which of the following have an inverse and why; Find the inverse for the case that the inverse exists.

(a) 3 in Z_6

Since gcd(3, 6) = $2 \neq 1$, 3 has no inverse in Z_6. Since there are only 6 possibilities, let us check them all to be sure:

For $x = 0$, we have $0 \cdot 3 = 0 \neq 1$.
For $x = 1$, we have $1 \cdot 3 = 3 \neq 1$.
For $x = 2$, we have $2 \cdot 3 = 6 = 0 \neq 1$.
For $x = 3$, we have $3 \cdot 3 = 9 = 3 \neq 1$.

For $x = 4$, we have $4 \cdot 3 = 12 = 0 \neq 1$.
For $x = 5$, we have $5 \cdot 3 = 15 = 3 \neq 1$.

So, also, by trial and error, we see that 3 has no inverse.

(b) 4 in Z_5

Since gcd(4, 5) = 1, 4 has an inverse in Z_5.
We need to find a number x st $4x \equiv 1 \bmod 5$ (or, $4x = 1$ in Z_5)
It is not hard to see that $x = 4$ works, as $4 \cdot 4 = 16 \equiv 1 \bmod 5$.