HOMEWORK 2
(Math 258)

1. Find the prime factorization of 126. (2 pts)

$126 = 2 \cdot 3^2 \cdot 7$

2. The **Euler function φ** is the function defined as follows: (4 pts)

$$\varphi(n) = |\{b \in Z \mid 0 < b \le n,\ \gcd(b,n) = 1\}|,\ n \in Z$$

(a) Find φ(10).

$\varphi(10) = |\{1, 3, 7, 9\}| = 4$

(b) Show that n is a prime if and only if $\varphi(n) = n - 1$.

"⇒" If n is prime, then the integers 1, 2, …, n-1 are $\le n$ and relatively prime to n. Since they are (n-1)-many of them, we have $\varphi(n) = n - 1$.

"⇐" Suppose n is not prime.
If $n = 1$, then $\varphi(n) = 1 = 1 - 1 = 0$ which is a contradiction.
If $n > 1$, then $n = ab$, where $1 < a < n$, $1 < b < n$. Since neither a nor b are relatively prime to n, then the number of integers which are $\le n$ and relatively prime to n must be at most n-3. (because we subtract from the at most n-1 two more, a and b). But then, $\varphi(n) \le n - 3 < n - 1$, i.e. $\varphi(n) \ne n - 1$, which is a contradiction.

3. Find the gcd and lcm of the following pair of integers: (2 pts)

$2^2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13$ and $2^3 \cdot 3^5 \cdot 11 \cdot 17^{13}$

$\gcd = 2^2 \cdot 3^3 \cdot 11$

$lcm = 2^3 \cdot 3^5 \cdot 5 \cdot 7 \cdot 11^2 \cdot 13 \cdot 17^{13} \cdot$

4. Show that if a,b,k and m are integers such that $k \ge 1, m \ge 2$ and $a \equiv b \bmod m$, then $a^k \equiv b^k \bmod m$. (*Hint*: Use the identity for $a^k - b^k$). (2 pts)

We know that $a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1})$.
Since $m \mid a - b \Rightarrow m \mid (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}) \Rightarrow m \mid a^k - b^k$
In other words, $a^k \equiv b^k \bmod m$.

5. Use the *extended Euclidean algorithm* to write the gcd(35, 78) as a linear combination of 35 and 78. Use that relation to find the inverse of 35 in Z_{78}. (4 pts)

Using the Euclidean Algorithm to find the GCD, we get:

$78 = 2 \cdot 35 + 8$
$35 = 4 \cdot 8 + 3$
$8 = 2 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$

So, working our way back up, we get:

$1 = 3 - 2$
$= 3 - (8 - 2 \cdot 3)$
$= 3 \cdot 3 - 8$
$= 3 \cdot (35 - 4 \cdot 8) - 8$
$= 3 \cdot 35 - 13 \cdot 8$
$= 3 \cdot 35 - 13 \cdot (78 - 2 \cdot 35)$
$= 29 \cdot 35 - 13 \cdot 78$

In other words, $1 = 29 \cdot 35 - 13 \cdot 78$.

Using this information, we can conclude that $29 \cdot 35 \equiv 1 (\mathrm{mod}\, 78)$, so 29 is the inverse of 35 in Z_{78}.

6. Solve the congruence $4x \equiv 5 \mathrm{mod}\ 9$. List at least three integers that are solutions of the congruence. (2 pts)

Writing 1 as a linear combination of 4 and 9, we get

$1 = 7 \cdot 4 - 3 \cdot 9$.

This tells us that 7 is the inverse of 4 modulo 9. So, to get the solution set, we multiply the congruence by 7 to get

$x \equiv 35 \pmod 9$

which is equivalent to

$x \equiv 8 \pmod 9$.

So the solution set is all numbers congruent to 8 modulo 9, or $8 + k \cdot 9$, where k is an integer.

7. Solve the system of congruences: $x \equiv 2 \mod 3$ (4 pts)
$x \equiv 1 \mod 4$
$x \equiv 3 \mod 5$.

Let $m = 3 \cdot 4 \cdot 5 = 60$.

So,

M1 = 60/3 = 20,
M2 = 60/4 = 15,

M3 = 60/5 = 12.

The inverse of 20 (mod 3) is 2.
The inverse of 15 (mod 4) is 3.
The inverse of 22 (mod 5) is 3.

The solution for x is:
$x = 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3 = 233 \equiv 53 \pmod{60}$.

i.e. $x \equiv 53 \pmod{60}$.