GROUP THEORY
PROBLEM SET 5
CONGRUENCE MODULO n

(1) Prove that if $a \equiv b \mod n$ and $c \equiv d \mod n$, then $a + c \equiv b + d \mod n$ and $ac \equiv bd \mod n$.
(2) If G is a finite set closed under an associative operation such that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$, for every $a, x, y, u, w \in G$, prove that G is a group.
(3) Using Fermat's Theorem, find the remainder of 3^{47} when it is divided by 23.
(4) Using Fermat's Theorem, find the remiainder of 37^{49} when it is divided by 7.
(5) Compute the remainder of $2^{(2^{17})} + 1$ when divided by 19.
(6) Compute $\varphi(p^2)$ where p is a prime.
(7) Compute $\varphi(pq)$ where both p and q are primes.
(8) If p is a prime, show that the only solutions of $x^2 \equiv 1 \mod p$ are $x \equiv 1 \mod p$ or $x \equiv -1 \mod p$.
(9) If G is a finite abelian group and $a_1, \cdots, a_n$ are all its elements, show that $x = a_1 a_2 \cdots a_n$ must satisfy $x^2 = e$.
(10) Using the results of Questions (8) and (9), prove that if p is an odd prime number, then $(p-1)! \equiv -1 \mod p$. This is known as Wilson's Theorem.
(11) In $\mathbb{Z}_{41}^*$, show that there is an element $[a]$ such that $[a]^2 = [-1]$, i.e. there is an integer a such that $a^2 \equiv -1 \mod 41$.
(12) Verify Euler's Theorem for $n = 14$ and $a = 3$, and for $n = 14$ and $a = 5$.
(13) If p is a prime number of the form $4n + 3$, show that we cannot solve

$$x^2 \equiv -1 \mod p.$$

Hint: Assume that there are solutions of $x^2 \equiv -1 \mod p$ where is p is a prime of the form $4n+3$. Then use Fermat's Theorem to get a contradiction.

(14) Show that the nonzero elements in $\mathbb{Z}_n$ form a group under the product $[a][b] = [ab]$ if and only if n is a prime.