PRACTICE PROBLEMS FOR THE FIRST MIDTERM

1. Give the definition of:

(i) The lowest common multiple of two integers, not both zero.
(ii) a congruent to b modulo m.
(iii) an equivalence relation.
(iv) a complete residue system.
(v) a reduced residue system.
(vi) Euler φ-function.
(vii) a multiplicative function
(viii) order of an integer a modulo m.
(ix) a singular solution.
(x) a quadratic residue.

2. (a) Let a and b be two coprime natural numbers and let $N = (a-1)(b-1)$. Show that every integer $c \geq N$ has a representation of the form $ax + by = c$, where x and y are non-negative integers. Show that $N - 1$ has no such representation.
(b) Show that exactly half of the integers $0, 1, \dots, N-1$ have such a representation.

3. Show that if $n > 1$ then $2^n - 1 \equiv 3 \mod 4$. Show that if $x^m \equiv 3 \mod 4$ then $x \equiv m \equiv 1 \mod 2$, in which case

$$\frac{x^m + 1}{x + 1} = x^{m-1} - x^{m-2} + \cdots - x + 1$$

is an odd integer. Conclude that the equation $2^n - x^m = 1$ has no solution with $x > 1$, $m > 1$ and $n > 1$.

4. Show that if $n > 1$ then the sum of the integers less than n and prime to n is

$$\frac{1}{2} n\varphi(n).$$

5. How many reduced fractions r/s are there with

$$0 \leq r < s \leq n?$$

6. Show that for every natural number k there are infinitely many blocks of length k of composite numbers.

7. State and prove the Chinese remainder theorem.