EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai **Discussion 4M**

1. Modular decomposition of modular arithmetic

Complex systems are always broken down into simpler modules. In this problem you will learn how this might be done in modular arithmetic.

(a) Write down the addition and multiplication table for modular-6 arithmetic (the rows and columns should be labeled $0,1,2,3,4,5$).

(b) Each number $0,1,2,3,4,5$ has a remainder mod 2 and a remainder mod 3. For each number write down the pair (x,y) where x is its remainder mod 2 and y is its remainder mod 3. Obviously $0 \le x \le 1$ and $0 \le y \le 2$. Out of all possible pairs (x,y), where $0 \le x \le 1$ and $0 \le y \le 2$, how many times do you see each pair appear?

(c) Again write down the addition and multiplication table you wrote in part 1, but this time replace each number with its corresponding pair (when a number appears as a row/column label and also when it appears somewhere in the table). Describe how one can add or multiply two pairs without looking at the original numbers.

2. Proofs (or counterexamples) for dividing numbers

(a) Prove that if a prime number p divides $a \cdot b$, then p divides a or p divides b.

(b) If an integer m divides both a and b, prove that m divides $x \cdot a + y \cdot b$ for any integers x, y.

(c) If m and n both divide a, does this mean mn divides a?

(d) Now, assume m and n are prime. If m and n both divide a, does this mean mn divides a?

3. Does it Exist?

Can you find a number that is a perfect square and is a multiple of 2 but not a multiple of 4? Either give such a number or prove that no such number exists.