Math 240: Discrete Structures I (W18) – Assignment 5

Solutions must typed or very neatly written and uploaded to MyCourses no later than **6 pm** on **Saturday, February 24, 2018**. Up to 4 bonus marks will be awarded for solutions typeset in LaTeX; both the .tex file and .pdf file must be uploaded.

You may use theorems proven or stated in class, but you must state the theorem you are using.

[18] 1. **Solving equations**

For each equation, either find all solutions or explain why none exist.

(a) $235x \equiv 12 \pmod{243}$

(b) $235x \equiv 12 \pmod{245}$

(c) $235x \equiv 10 \pmod{245}$

[7] 2. **Congruence**

(a) There is a divisibility rule for dividing an integer n by 11:

> Label the digits (starting with the ones place and moving right to left) with the labels $0, 1, 2, \ldots$ and so on. Sum the digits with even labels, sum the digits with the odd labels, and subtract one sum from the other. The result is divisible by 11 if and only if n is divisible by 11.

For example, consider $5, 195, 407, 283$. We check $(3+2+0+5+1)-(8+7+4+9+5) = (11) - (33) = -22$. Since $11 \mid -22$, we also have $11 \mid 5, 195, 407, 283$.

Prove this rule is correct. HINT: Find an appropriate way to represent a number in terms of its digits, and think modulo 11.

[15] 3. **Cryptography**

You have stumbled across a (bad) RSA encryption system with public key $n = 221, e = 113$.

(a) Find primes p, q such that $n = pq$.

(b) You intercept the message $E = 2$. Decode it using the single private key d as described in the handout.

(c) Decode E using two private keys and the Chinese Remainder Theorem as described in the handout.