MATH 135 Winter 2017: Assignment 8 Due at 8:25 a.m. on Wednesday, March 15, 2017

It is important that you read the assignment submission instructions and suggestions available on LEARN.

1. Determine, with justification, the remainder when 2^{1000} is divided by 77.

2. Let

$$\begin{aligned} T &= \{\ x \in \mathbb{Z}\ :\ x \equiv 39 \pmod{90}\ \}, \\ U &= \{\ x \in \mathbb{Z}\ :\ x \equiv 4 \pmod{5}\ \wedge\ x \equiv 3 \pmod{9}\ \}, \text{ and} \\ V &= \{\ x \in \mathbb{Z}\ :\ x \equiv 4 \pmod{10}\ \wedge\ x \equiv 3 \pmod{9}\ \}. \end{aligned}$$

   Prove or disprove each of the following statements.

   (a) $T \cap V = \emptyset$

   (b) $U \subseteq T$

   (c) $V = U - T$

3. If m is an odd positive integer and $n \in \mathbb{N}$, prove that the system of congruences

$$\begin{aligned} 2x &\equiv 2n \pmod{m} \\ x &\equiv m \pmod{2^n} \end{aligned}$$

   has exactly one integer solution x with $0 \leq x < 2^n m$.

4. Find all the square roots of two in Z_{119} without using a calculator. That is, solve $[x]^2 = [2]$ in Z_{119}. Outline how you found your answer but you don't have to show all the steps.

5. Suppose that in setting up RSA, Alice chooses $p = 29$, $q = 43$ and $e = 125$.

   (a) What is Alice's public key?

   (b) What is Alice's private key?

   (c) Suppose Alice wishes to send Bob the message $M = 100$. Bob's public key is $(15, 391)$ and Bob's private key is $(47, 391)$. What is the cipher text corresponding to M? Show your work. (Not all of the information given with this question is needed to compute the correct answer.)

6. In this question, we ask you to successfully attack RSA in a special case. Let p and q be odd primes where $0 < p - q < 20$ and $pq = 330876019$. Determine p and q. You may only add, subtract, multiply, divide and take square-roots. Each of these operations may be performed at most 20 times. It must be possible to use your approach to break RSA when $0 < p - q < 20$ and pq is very large ($\approx 10^{300}$). Show your work.

7. Let z and w be complex numbers.

   (a) Prove that $\overline{zw} = \overline{z}\,\overline{w}$. (This is part of Exercise 1 in Chapter 31 of the notes.)

   (b) Prove by induction that $(\overline{z})^n = \overline{z^n}$ for all natural numbers n.