Math 312/ AMS 351 (Fall 2022)

Sample Midterm 1

1. Solve the following equations

   i) $3x + 2 \equiv 4 \mod 10$

   ii) $3x + 1 \equiv x + 4 \mod 10$

   iii) $3x + 1 \equiv 3 \mod 10$

   iv)

$$\begin{aligned} x &\equiv 2 \mod 17 \\ x &\equiv 3 \mod 20 \end{aligned}$$

2. a) Prove that no number of the form $8k+3$ can be written as a sum of two squares.

b) Show that a number n is divisible by 11 iff the alternating sum of its digits is divisible by 11 (e.g. 121 is divisible by 11 because $1-2+1 \equiv 0 \pmod{11}$).

3. Find the last two digits of
   i) 7^{123}

   ii) 6^{123}

4. Consider the RSA code with base $n = 55$, and the following alphabet:
   A=0, E=1, O=2, B=3, D=4, R=6, T=7

   a) Which of the following exponents is acceptable (choose one)?
      * $a = 15$
      * $a = 27$.
        Explain!

   b) Using the exponent that you selected in a) above, find the decryption key.

   c) Decrypt the message: **41, 1, 49**

5. Consider the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 9 & 1 & 7 & 2 & 3 & 4 & 6 & 5 \end{pmatrix}$$

i) Decompose σ into disjoint cycles.

ii) What is the order of σ? (Add a brief explanation, e.g. *the order of a cycle is ..., and then for the product of ... cycles, the order is ...*)

iii) What is the signature of σ? (Add a brief explanation.)

iv) Pick the correct answer: σ *can be written as product of*
   - 8 transpositions,
   - 9 transpositions.

   Explain.