MATH 115: ELEMENTARY NUMBER THEORY
HOMEWORK # 3

JOHN VOIGHT

This homework is *not due*! It is just for fun.

Homework #8 (Freebie):

- §13.1: 1, 2, 8
- Elliptic Curves:
  EC1: Let $E : y^2 = x^3 - x + 1$ over $\mathbb{Z}/3\mathbb{Z}$.
  (a) Determine $\#E(\mathbb{Z}/3\mathbb{Z})$.
  (b) Alice and Bob do a Diffie-Hellman key exchange using the group $E(\mathbb{Z}/3\mathbb{Z})$, where $E : y^2 = x^3 - x + 1$, with $g = (1, 1)$. They use secret exponents $a = 2$ and $b = 3$. What is the secret common key that they exchange?