Assignment 7

True/False questions, not to turn in (but you should DO them):

- For every $n > 2$, and any $0 < a, b < n$, there is an x such that $ax = b \bmod n$.
- If $x = 0 \bmod 11$ and $x = 0 \bmod 13$, then it must be that $x = 0$.
- For any prime $p > 2$ there is an x such that $x + x = 1 \bmod p$.
- For any prime $p > 2$ there is an x such that $x \cdot x = 1 \bmod p$.
- For every prime $p > 2$ there is a solution to the equation $x^2 = -1 \bmod p$ (i.e. a square root of -1 exists).
- There are primes $p > 2$ for which there is a solution to the equation $x^2 = -1 \bmod p$.
- If $n > 2$ is not prime, there are integers $0 < x < n$ such that no power of x equals 1.

Questions to turn in:

1. Find all solutions to the equation $12x + 5 = 11 \bmod 57$.
2. Which congruence classes modulo 11 are third powers (i.e. they are equal to x^3 for some x)?
3. Using our base-26 representation of the english alphabet, encrypt the message “NUMBERSROCK” via the multiplication-by-11 algorithm. Then demonstrate how someone would go about decrypting the message.
4. In $\mathbb{Z}_3$ we want to consider all monic degree-2 polynomials, so all polynomials of the form $x^2 + bx + c$ where $b, c \in \mathbb{Z}_3$. There are 3×3 such polynomials. List them, then determine which of those polynomials have “roots” (i.e. values of $x \in \mathbb{Z}_3$ that would make the polynomial equal to 0), and how many roots they have.
5. Use Fermat’s theorem to compute $7^{2015} \bmod 11$.