Homework 3

Due: Friday, February 11 at noon

Instructions: Submit a pdf of your solutions to the HW 3 assignment on Gradescope.
Note: Problems 4 and 5 require you to find multiplicative inverses. Since you are showing your skills in doing that by hand in problem 2, you can use whatever technique/computer tool you would like to find the needed inverses for problems 4 and 5. (In SAGE, the code $inverse\_mod(a, m)$ computes the multiplicative inverse of a modulo m.)

0. If you would like any of these problems to be graded for proficiency with the core skills, list the skill and the corresponding problem.

1. Use the Euclidean Algorithm to find $\gcd(65330, 5420)$.

2. Use the Euclidean Algorithm to find a multiplicative inverse of 206 modulo 5427.

3. Prove that, if a_1 and a_2 are units modulo m, then $a_1 a_2$ is also a unit modulo m.

4. Consider an affine cipher with key $(5, 4)$.

   (a) Encrypt the word "cryptology" using that cipher.

   (b) You recieve the ciphertext "DAROVSWR". What is the decrypted plaintext?

5. Two enemies of yours are passing messages using an affine cipher. You know that they always write formal notes starting with the greating "Hello" in the plaintext. You intercept a ciphertext that starts with "fkhhc." What key did they use?

6. (Exercise 1.6.16 in your textbook) Prove that $x^2 - y^2 = 102$ has no integer solutions. (Hint: Use the contrapositive of the following: If a, b are integers such that $a = b$, then $a \equiv b \pmod{m}$ for all nonzero integers m.)