Due Friday, October 15 at 10:00 AM. Please turn in via email, in my mailbox in Hylan 913, or under my office door in Hylan 813. All chapter and exercise numbers refer to Silverman's *A Friendly Introduction to Number Theory*, 4th edition.

(1) Ex. 10.3(a). Do not do by brute force. Use the Chinese Remainder Theorem.

(2) Ex. 17.3(a)

(3) Ex. 17.4

(4) Ex. 18.2 (b)–(c). You do not need to include a solution to part (a) since it is a special case of part (b). However, you may find thinking about the classic RSA setup in part (a) to be helpful in solving part (b). Hint: use the results in the previous two exercises.

(5) Let $m = 92897091108461$. For the purpose of this exercise, suppose m is too large to factor. If we know m is the product of two distinct primes and $\varphi(m) = 92896611912924$, find the two prime factors of m.

(6) The message a is encrypted with the RSA algorithm using the encryption exponent $k = 3$ three times using three different moduli m_1, m_2, and m_3, which have no common factors. Explain a method for determining a. (Hint: use the Chinese Remainder Theorem and the fact that $a < \min\{m_1, m_2, m_3\}$.)

To convert words and phrases into sequences of numbers (and vice versa), use the conversion on page 123. Ignore all punctuation and spaces. For the following problems, you may use the spreadsheet developed in class or any other computational software (e.g. Wolfram Alpha). However, please give a detailed description of the steps you take.

(7) The following messages were encrypted with the RSA algorithm with prime factors $p = 2251$ and $q = 11939$, modulus $m = pq$, and encryption exponent $k = 2087$.

22611587, 22138420, 17726401, 7933697, 1440922,
18856207, 5646854, 19535715, 589184, 4890889,
17711308, 25716363, 14065813, 1554770

(a) What is the decryption exponent u?

(b) Decrypt the messages. Then concatenate and convert to letters.

(8) The following messages were encrypted with the RSA algorithm with modulus $m = 538937074901$ and encryption exponent $k = 314159$.

254717498112, 25011830619, 135117199315

Break the code and decrypt the messages. Then concatenate and convert to letters.