PMATH 340 Number Theory, Exercises for Chapter 5 (Prime Numbers)

1: (a) Let $p = 47$, $q = 61$, $e = 43$ and $n = pq$. Encrypt the 2-letter message GO using the RSA public key (e, n) (first replace GO by the number $m = 0715$ because G and O are the 7^{th} and 15^{th} letters of the alphabet).

(b) Let $p = 41$, $q = 67$, $e = 217$ and $n = pq$. Decrypt the cyphertext $c = 811$ which was encoded from a 2-letter message using the RSA public key (e, n).

2: (a) Let $n = 459061$. Given that $n = pq$ for some primes $p < q$ and that $\varphi(n) = 457612$, find the prime factorization of n.

(b) Let $n = 806437$. Given that $n = pq$ for some primes $p < q$ with $q - p \leq 100$, find the prime factorization of n.

3: (a) Show that 91 is a pseudo-prime in the base 3.

(b) Find a prime p such that $n = 5 \cdot 29 \cdot p$ is a Carmichael number.

(c) Show that 217 is a strong pseudoprime in the base 6.

4: (a) Show that there are infinitely many primes of the form $6k + 5$, where k is an integer.

(b) Show that the sequence $\{6k + 5\}$ contains arbitrarily long strings of consecutive terms which are all composite. In other words, show that for every positive integer n there exists a value of k such that the n integers $6k + 5, 6k + 11, 6k + 17, \cdots, 6k + 6n - 1$ are all composite.

5: (a) Show that there are infinitely many primes of the form $8k - 1$ with $k \in \mathbf{Z}$.
Hint: suppose that $p_1, p_2, \cdots, p_l$ are the only such primes, and consider $(p_1 p_2 \cdots p_l)^2 - 2$.

(b) Show that there are infinitely many primes of the form $8k + 5$ with $k \in \mathbf{Z}$.