Homework #3

1. (a) Prove that if $m > n$ then $a^{2^n} + 1$ is a factor of $a^{2^m} - 1$.

   (b) Show that if a, m, n are positive integers with $m \neq n$, then

$$\gcd(a^{2^n} + 1, a^{2^m} + 1) = \begin{cases} 1 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd.} \end{cases}$$

   (c) Deduce that there are infinitely many primes considering the sequence

$$2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, ...$$

2. (a) For $n > 2$, show that every prime divisor of $n! - 1$ is greater than n.

   (b) Prove that if $n > 2$, then there exists a prime p satisfying $n < p < n!$.

3. (a) The product of two or more numbers of the form $4k + 1$, is also of that form.

   (b) There are infinitely many prime numbers of the form $4k + 3$.

4. Suppose $\gcd(a, b) = 1$. For any inter $k > 0$, prove that the arithmetic progression

$$a + b, a + 2b, ...$$

   contains k consecutive terms that are composite. [Hint: find a special integer n so that $a + (n + 1)b, ..., a + (n + k)b$ are all composite].

5. Let $f(x) = a_m x^m + ... + a_1 x + a_0$ be a polynomial of degree $m > 0$ with integer coefficients $a_0, a_1, ..., a_m$ all nonzero. The goal of this exercise is to show that the set

$$S = \{p \text{ prime: } p \text{ divides } f(n) \text{ for some integer } n\}$$

   is infinite. Assume on the contrary that S contains only finitely many primes, say $p_1, ..., p_k$. Consider the polynomial $g(y)$ in y defied by

$$g(y) = a_0^{-1} f(a_0 p_1 p_2 \cdots p_k y).$$

   (a) Show that $g(y)$ is a polynomial in y of degree m, with integer coefficients, constant term 1.

   (b) Suppose that p is a prime which divides $g(t)$ for some $t \in \mathbb{Z}$. Show that p divides $f(n)$ for some $n \in \mathbb{Z}$.

   (c) Show that none of $p_1, ..., p_k$ divides $g(y)$ when $y \in \mathbb{Z}$.

   (d) Deduce that $g(y)$ s either 1 or -1 for any $y \in \mathbb{Z}$, and that S must contain infinitely many primes.