MATH 3540 **Name:** _____
Day 6

Directions

1. Complete the following questions.

---

1. Prove the following is a negligible function.
   (a) $f(n) = 2^n$
   (b) $f(n) = 2^{\sqrt{n}}$

2. Show the following Theorem: Let n_1 and n_2 be negligible functions.
   (a) Then n_1+n_2 is negligible.
   (b) For any positive polynomial p, the function $p(n)n_2(n)$ is negligible.

3. Let G be a pseudorandom generator where $|G(s)| = 2|s|$.

   (a) Define $G_0(s) = G(so^{|s|})$. Is G_0 necessarily a pseudorandom generator?

   (b) Define $G_0(s) = G(s_1 \dots s_{n/2})$ where $s = s_1 \dots s_n$. Is G_0 necessarily a pseudorandom generator?

4. Define

   G by G(x) = x — x. (G maps inputs of length n to outputs of length 2n.) Which of the following algorithms A distinguishes the output of G from uniform?

   (a) An input y of length 2n, output 1 if the first bit of y is 1

   (b) An input y of length 2n, output 1 if the last bit of y is 1

   (c) An input y of length 2n, output 1 if the first and last bits of y are equal

   (d) An input y of length 2n, output 1 if the first bit of y is equal to the (n+1)st bit of y