UEE4611 Assignment #1, 2020 due March 24

1. Find the **multiplicative inverse** of each nonzero element in $\mathbb{Z}_7$. (10%)

2. The purpose of this problem is to set an upper bound on the number of iterations of the **Euclidean algorithm**.

   (a) Suppose that $m = qn + r$ with integers $q \geq 1$ and $0 \leq r < n$. Show that $m/2 > r$. (5%)

   (b) Let a_i be the value of a in the Euclidean algorithm after the ith iteration (see Figure 2.2 of the textbook or the lecture slide). Show that $a_{i+2} < a_i/2$. (5%)

   (c) Show that if m, n, and N are integers with $(1 \leq m, n \leq 2^N)$, then the Euclidean algorithm takes at most $2N$ steps to find $gcd(m, n)$. (5%)

3. Using the **extended Euclidean algorithm**, find the multiplicative inverse of

   (a) 135 mod 61 (10%)

   (b) 7465 mod 2464 (10%)

4. Use **Euler's theorem** to find a number a between 0 and 92 with a congruent to 7^{1013} modulo 93. (You should not need to use any brute-force searching.) (10%)

5. Use **Euler's theorem** to find a number a between 0 and 9 such that a is congruent to 9^{101} modulo 10. (10%)

$135 = 61 \times 2 + 13$

$61 = 13 \times 4 + 9$

$13 = 9 \times 1 + 4$

$9 = 4 \times 2 + 1$

$-14 \times 135 - 5 \times 61 = 1$