1. Solve $4^x \equiv 28 \mod 37$ by hand using Shanks algorithm.

   You can use Mathematica to calculate multiplicative orders and to perform modular multiplication.

2. Download the Mathematica notebook for today, and use it and Shanks to solve the following DLPs. How long are your lists in each case?

   (a) $4^x \equiv 28 \mod 37$

   (b) $6^x \equiv 5660 \mod 7951$

   (c) $637\,239\,129^x \equiv 182\,583\,899 \mod 2\,043\,290\,489$

3. Use the Chinese Remainder Theorem to solve the following system:

$$x \equiv 6 \mod 7$$
$$x \equiv 4 \mod 8$$
$$x \equiv 10 \mod 15$$

4. The point of this problem is to illustrate the utility of Exercise 1.33 from Problem Set #1, which asked you to consider elements $a \in \mathbb{F}_p^*$ and $b \equiv a^{(p-1)/q} \mod p$.

   (a) i. Let $p = 13$ and $q = 3$. Notice that p and q are primes where $q \mid (p-1)$.
   Using these values of p and q, form the list of 12 elements

$$\{b_1, b_2, \ldots, b_{12}\} \text{ where } b_a \equiv a^{(p-1)/q} \mod p$$

   Notice there will be some repeat elements in this list.

   ii. Now form the list $\{\text{ord}(b_1), \text{ord}(b_2), \ldots, \text{ord}(b_{12})\}$

   iii. What is the probability that a randomly chosen value $a \in \mathbb{F}_{13}^*$ will produce an element $b \in \mathbb{F}_{13}^*$ such that $\text{ord}(b) = q = 3$?
   Hint: It better be $\frac{q-1}{q} = \frac{2}{3}$ or else part b of the exercise is wrong!

   (b) Let $p = 104759$ and $q = 52379$. You may assume that both of these values are prime.

   Find five elements of $\mathbb{F}_p^*$ with order q *by hand.* i.e. no Mathematica, no WolframAlpha, no calculator, etc.