MATH 304: HOMEWORK 3 (due 3/1)

1. Find the smallest value of x (besides $x = 1$) that simultaneously satisfies the following congruences:

$$\begin{aligned} x &\equiv 1 \pmod 3 \\ x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 7. \end{aligned}$$

2. Find the value of (a) $\varphi(97)$ and (b) $\varphi(8800)$.

3. Consider the following reproduction of a historical document:

> "We have a number of things, but we do not know exactly how many. If we count them by threes, we have two left over. If we count them by fives, we have three left over. If we count them by sevens, we have two left over. How many things are there?"
> *Sun Tzu Suan Ching* (Master Sun's Mathematical Manual)
> circa AD 300, volume 3, problem 26

   This is the first recorded instance of Sun Tzu's theorem (the Chinese remainder theorem). Solve Sun Tzu's problem, i.e. find out how many things there are.

4. Let $n \geq 1$ be a natural number and let $p_1, \ldots, p_k$ be the distinct prime divisors of n (so this list contains exactly the prime divisors of n without any repetitions). Show that:

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\Big(1 - \frac{1}{p_3}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big)$$

5. Determine whether the system of congruences

$$\begin{aligned} x &\equiv 3 \pmod{10} \\ x &\equiv 8 \pmod{15} \\ x &\equiv 5 \pmod{84} \end{aligned}$$

   has a solution, and find them all (up to an appropriate modulus) if they exist.

   Recall the following definition: a group $(G, \square, e)$ consists of a set G of elements and a product

$$\begin{aligned} \square \colon G \times G &\longrightarrow G \\ (x, y) &\longmapsto x \square y \end{aligned}$$

   (this is a notationally heavy way of saying that for every pair of elements x and y in G, we get another element $x \square y$ of G) that satisfy the following conditions:

(i) $\square$ is associative: for all $x, y, z \in G$, the equation $x \square (y \square z) = (x \square y) \square z$ holds.

(ii) $\square$ is commutative: for all $x, y \in G$, the equation $x \square y = y \square x$ holds.

(iii) there is an element e, called the *unit* or *identity* element, that satisfies $x \square e = x$ for all $x \in G$.

(iv) existence of inverses: for every $x \in G$, there exists an element x^{-1} that satisfies the equation $x \square x^{-1} = e$.

6. Usually, mathematicians use the term "group" for an object G that satisfies (i), (iii), and (iv), but not necessarily (ii). Thus, in this course, we will use the term group to refer to commutative groups. But before we narrow our scope of inquiry, your task in this problem is to find an example of a group G that is NOT commutative. In other words, find a set G with a product $\square$ that satisfies (i), (iii) and (iv), but for which it is sometimes the case that $x \square y \neq y \square x$.

7. In class, we defined the notion of the subgroup $\langle x \rangle$ of a group G generated by an element x. When $\langle x \rangle = G$, i.e. the subgroup generated by x is the whole group G, we say that G is cyclic.

   Find an example of a group G that is NOT cyclic. In other words, it requires two or more elements to generate G.