Math 11N
Homework 6
Due Friday, February 18th, 2022

1. Solve the following systems of congruences. Your answer should be a single congruence class in each case: $x \equiv \_ \bmod \_$.

   (a)
   $$\begin{cases} x \equiv 6 \bmod 8 \\ x \equiv 3 \bmod 9 \\ x \equiv 8 \bmod 11 \\ x \equiv 7 \bmod 13 \end{cases}$$

   (b)
   $$\begin{cases} x \equiv 10 \bmod 12 \\ x \equiv 4 \bmod 15 \\ x \equiv 14 \bmod 50 \end{cases}$$

   Note: the moduli here are *not* pairwise coprime, so you'll have to do something different than usual. *(Hint: factor each modulus and turn each single congruence into a system of congruences. Then you can eliminate the redundant ones.)*

   (c) Show that the system below does *not* have a solution.
   $$\begin{cases} x \equiv 6 \bmod 12 \\ x \equiv 9 \bmod 15 \\ x \equiv 22 \bmod 50 \end{cases}$$

   Combined with the previous part, this demonstrates that the moduli not being pairwise coprime may or may not result in solutions to systems.

2. Prove for integers $m, n > 1$ that $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$ where $d = \gcd(m, n)$.

3. (a) Find, with proof, all solutions to $\varphi(n) = 6$.
   (b) Prove there is no solution to $\varphi(n) = 14$.

The goal of the remaining problems is finding solutions to the equation $x^2 = [1]$ in $\mathbb{Z}/N\mathbb{Z}$ for $N > 1$, which we know is equivalent to finding solutions to the congruence $x^2 \equiv 1 \bmod N$.

4. Let $p > 2$ be prime and $k \geq 1$. Prove that $x^2 \equiv 1 \bmod p^k$ if and only if $x \equiv \pm 1 \bmod p^k$.

5. The case of $p = 2$ is more complicated.

   (a) What are the solutions to $x^2 \equiv 1 \bmod 2$? $x^2 \equiv 1 \bmod 4$? $x^2 \equiv 1 \bmod 8$?

(b) Prove that for $k \geq 3$, $x^2 \equiv 1 \bmod 2^k$ has exactly four solutions: $x \equiv \pm 1 \bmod 2^k$, $x \equiv \pm 1 + 2^{k-1} \bmod 2^k$. *(Hint: prove this by induction on k. If $x^2 \equiv 1 \bmod 2^k$, note that $x^2 \equiv 1 \bmod 2^{k-1}$.)*

6. To finish up, we need to find a way of gluing together our information. For an integer $N > 1$, let $S_N = \{[x] \in \mathbb{Z}/N\mathbb{Z} : [x]^2 = [1]\}$, that is, S_N is the set of solutions to the congruence $x^2 \equiv 1 \bmod N$.

   (a) Let $m, n > 1$ be relatively prime integers. Prove the map $f : S_{mn} \to S_m \times S_n$ given by $f([x]_{mn}) = ([x]_m, [x]_n)$ is a bijection. *(Hint: you'll want to use the Chinese Remainder Theorem to show the map is surjective!)*

   (b) Let $N = 2^e p_1^{e_1} \dots p_k^{e_k}$ be the prime factorization of N. Set $N_2 = |S_{2^e}|$ and $N_{p_i} = |S_{p_i^{e_i}}|$. Write down a formula for the number of solutions to $x^2 \equiv 1 \bmod N$ in terms of N_2 and N_{p_i}, and use your formula to compute the number of solutions to $x^2 = [1]$ in $\mathbb{Z}/N\mathbb{Z}$ for $N = 60, 4410, 10!$.

   (c) Find all solutions to $x^2 \equiv 1 \bmod 39188$. *(Much like with the proof of the Chinese Remainder Theorem, your proof of part (a) will tell you how to do this!)*