This should help you prepare for the midterm.

1. Short answer questions.
   (a) Define what it means for a function \( f : A \rightarrow B \) to be injective.

   (b) Is it true that there is a solution to \( 3x \equiv 1 \) mod 9?

   (c) What is the definition of the gcd\((a, b)\)?

   (d) State Fermat’s little theorem.

   (e) Suppose that \([a]\) and \([b]\) are two distinct equivalence classes of an equivalence relation \(\sim\). Is it possible that \(a \sim b\)?

   (f) Consider the function \( f(x) = 3x^3 + 2^x \). True or false, \( f(x) \) is \( O(x^3) \)?
(g) Consider the system of congruences $x \equiv_{11} 7$ and $x \equiv_{13} 3$. How many solutions does this system have between 0 and $142 = 11 \cdot 13 - 1$?

(h) What’s the smallest prime integer bigger than 100?

(i) Define what it means that a relation is an equivalence relation.

(j) Do an insertion sort, showing all the steps, on the integers $\{3, 0, 5, -1\}$.

(k) Write the number 23 in base 6.

(l) Rewrite the base 5 integer $(401)_5$ as an integer in base 10.

(m) At most how many comparisons does a binary search do on a list of length $n$ (you may use big $O$ notation).

(n) If $\varphi$ is the Euler phi function, what is $\varphi(45)$?
2. Run the extended Euclidean algorithm on the integers 121 and 77 and use it to find integers $s$ and $t$ such that $s \cdot 121 + t \cdot 77 = 11$. Make sure to explain each step.

3. Solve the system of congruences

\[
\begin{align*}
2x &\equiv 3 \pmod{5} \\
x &\equiv 5 \pmod{3} \\
3x &\equiv 0 \pmod{4}
\end{align*}
\]
4. Describe an algorithm that determines if a function $f : \{1, 2, 3, 4, 5\} \rightarrow \{6, 7, 8, 9\}$ is surjective. You may use pseudo-code or sentences.

5. Describe an algorithm that computes $\varphi(n)$ where the input $n$ is an integer. How many times does it run the Euclidean Algorithm? (You may assume you already have a different function that has implemented the Euclidean Algorithm).
6. Fix an integer $n > 0$. Write $a \equiv_n b$ (for integers $a$ and $b$) if $n|(a - b)$. Prove carefully that $\equiv_n$ is an equivalence relation.

7. Consider the set $S = \mathbb{Z} \times \mathbb{Z}$ (the set of ordered pairs of two integers). We define an relation $\sim$ on $S$ by declaring $(a, b) \sim (c, d)$ if $a^2 + b^2 = c^2 + d^2$.

(a) Prove that $\sim$ is an equivalence relation.

(b) Compute $\lvert[(1, 0)]_\sim\rvert$ (the size of the equivalence class of $(1, 0)$).