

1. How many different functions $f : \{1, 2, 3\} \rightarrow \{4, 5, 6, 7\}$ are there? How many of them are injective? Surjective? (In all three cases, you don't have to — nor should you — list them all, but you should explain where your answer comes from.)
2. Define an injective function from the interval $(0, 1)$ to the real numbers \mathbb{R} . Next find a *surjective* function from $(0, 1)$ to \mathbb{R} . This can indeed be done, but it's tricky and you should leave this until you've finished your other problems. If it's easier, you can use any other finite open interval (a, b) in place of $(0, 1)$, such as $(-1, 1)$, $(10, 11)$, and so on.
3. Write out the multiplication tables for mod 2, mod 3, mod 4, and mod 5 arithmetic. (Hint: This goes fast, because they have a certain kind of symmetry.) How does the table for mod 4 multiplication differ from the other three? Which numbers have mod-4 multiplicative inverses? Which numbers have mod-5 multiplicative inverses? Write down any ideas for why 4 might be different.
4. Do the following problems with the Affine Cipher $E_{a,b}(x) = a \cdot x + b \pmod{26}$.
 - (a) Encrypt “meet me at midnight” with the key $(a, b) = (3, 7)$.
 - (b) Determine the decryption key $(a^{-1}, -a^{-1}b)$ for this system and show that it works by decrypting your ciphertext from (a).
 - (c) Known plaintext attack: suppose $E_{a,b}(3) = 5$ $E_{a,b}(6) = 7$. Find a and b .