1. Bijections

Consider the function

$$f(x) = \begin{cases} x, & \text{if } x \geq 1; \\ 3x-2, & \text{if } \frac{1}{2} \leq x < 1; \\ -x, & \text{if } -1 \leq x < \frac{1}{2}; \\ 2x+3, & \text{if } x < -1. \end{cases}$$

1. If the domain and range of f are $\mathbb{N}$, is f injective (one-to-one), surjective (onto), bijective?
2. If the domain and range of f are $\mathbb{Z}$, is f injective (one-to-one), surjective (onto), bijective?
3. If the domain and range of f are $\mathbb{R}$, is f injective (one-to-one), surjective (onto), bijective?

2. RSA

In this problem you play the role of Amazon, who wants to use RSA to be able to receive messages securely.

1. Amazon first generates two large primes p and q. She picks $p = 13$ and $q = 19$ (in reality these should be 512-bit numbers). She then computes $N = pq$. Amazon chooses e from $e = 37, 38, 39$. Only one of those values is legitimate, which one? (N, e) is then the public key.

2. Amazon generates her private key d. She keeps d as a secret. Find d. Explain your calculation.

3. Bob wants to send Amazon the message $x = 102$. How does he encrypt his message using the public key, and what is the result?
   Note: For this problem you may find the following trick of fast exponentiation useful. To compute x^k, first write k in base 2 then use repeated squaring to compute each power of 2. For example, $x^7 = x^{4+2+1} = x^4 \cdot x^2 \cdot x^1$.

4. Amazon receives an encrypted message $y = 141$ from Charlie. What is the unencrypted message that Charlie sent her?

3. RSA Reasoning

In RSA, if Alice wants to send a confidential message to Bob, she uses Bob's public key to encode it. Then, Bob uses his private key to decode the message. Suppose that Bob chose $N = 77$ and $e = 3$, so his public key is $(3, 77)$. Bob chose $d = 26$, so his private key is $(26, 77)$.

Will this work for encoding and decoding messages? If not, where did Bob first go wrong in the above sequence of steps and what is the consequence of that error? If it does work, show that it works.

4. RSA with Multiple Keys

Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve, who is listening to all of their communications, notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e, N_1), \ldots, (e, N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

1. Suppose Eve sees the public keys $(7, 35)$ and $(7, 77)$ as well as the corresponding transmissions. How can Eve use this knowledge to break the encryption?

2. The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3, 5 \times 23)$, $(3, 11 \times 17)$, and $(3, 29 \times 41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.