Homework 3

8/8

1. Implement the Miller-Rabin probabalistic testing algorithm as presented in class (or in the text book).

```python
def is_prime_MR(q): # {{{
  # Fill in each step (as outlined in class or the textbook) below the relevant
  # comment.
  #
  # At Step 3, you will need to produce a random element of {1, ..., q-1}. Use
  # randrange() to do this: a = randrange(1, q). Note that modulus in python is
  # positive, so -1 should be represented as q-1.

  if q <= 1:
    return False

  # Step 1
  if ((q % 2) == 0):
    return False

  # Step 2
  l = q - 1
  k = 0
  while((l % 2) == 0):
    k += 1
    l = l // 2

  # Step 3
  a = randrange(2, (q - 1))
  a = 2   XX
  # Step 4
  p = [2**val for val in range(k+1)]
  al = a**l
  allist = [((al**val) % q) for val in p]
  print(allist)

  # Test 1
  if(allist[-1] != 1):
      return False

  # Test 2
  ind_1 = [i for i, e in enumerate(allist) if e == 1]
  if(len(ind_1) > 0):
    for val in ind_1:
      if(val > 0):
        if(allist[val-1] in [1,-1]):
          return False
```

4/4

---

2. Find five pairs of numbers $q \in Z$ and $a \in \{1, \ldots, q-1\}$ such that q is composite but passes the Miller-Rabin test with the given choice of a.

Below are the numbers and bases of Composite numbers which are categorized as primes by Miller-Rabin test. Also known as Pseudoprimes. Let n be the number and a be the base.

1. $n = 21$ for base $a = 20$. $21 = 3 * 7$ is a composite.
Test 1: $20^{20} \equiv 1(mod21)$. According to MR primality, this is not composite.

2. $n = 25$ for base $a = 7$. $25 = 5 * 5$ is a composite.
Test 2: $a^l = \{18, 24, 1, 1\}$. According to MR primality, this is not composite.

3. $n = 25$ for base $a = 18$. $25 = 5 * 5$ is a composite.
Test 2: $a^l = \{7, 24, 1, 1\}$. According to MR primality, this is not composite.

4. $n = 49$ for base $a = 18$. $49 = 7 * 7$ is a composite.
Test 2: $a^l = \{1, 1, 1, 1, 1\}$. According to MR primality, this is not composite.

5. $n = 49$ for base $a = 19$. $49 = 7 * 7$ is a composite.
Test 2: $a^l = \{48, 1, 1, 1, 1\}$. According to MR primality, this is not composite.

4/4