QUANTUM ALGORITHMS
HOMEWORK 3 SELECTED SOLUTIONS

PROF. MATTHEW MOORE

AP 1. Implement the Miller-Rabin probabilistic primality testing algorithm as presented in class (or in the textbook). Fill in the function `is_prime_MR(q)` in the python source file. You need only submit your function with the homework, not the entire source file.

Solution:

```
def is_prime_MR(q):
  if q <= 1:
    return False

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

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

  # Step 3
  a = randrange(2, q-1)

  # Step 4
  a_powers = [ (a**l) % q ]
  for _ in range(k):
    a_powers.append( ( a_powers[-1]**2 ) % q )

  # Test 1
  if a_powers[-1] != 1:
    return False

  # Test 2
  for j in range(1, len(a_powers)):
    if a_powers[j] == 1 and a_powers[j-1] not in [1, q-1]:
      return False

  return True
```

Date: February 18, 2021.

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

Solution: The smallest such pairs of numbers are given in the table below, along with the sequence of powers a^ℓ, $a^{2\ell}$, $\ldots$, $a^{2^k\ell}$.

q	a	k	ℓ	$a^\ell, a^{2\ell}, \ldots, a^{2^k\ell}$
25	7	3	3	$18, 24, 1, 1$
25	18	3	3	$7, 24, 1, 1$
49	18	4	3	$1, 1, 1, 1, 1$
49	19	4	3	$48, 1, 1, 1, 1$
49	30	4	3	$1, 1, 1, 1, 1$