Problem Set #4

Due Friday, March 7, 2025 @ 2:00 pm

1. Show by hand that 4 is a Miller-Rabin witness for the compositeness of 153.

   You may use a computing tool for modular arithmetic, but you cannot use the Mathematica function mrWitness[ ] from class.

2. Use the Miller-Rabin test on each of the following numbers. In each case, either provide a Miller-Rabin witness for the compositeness of n, or conclude that n is probably prime by providing 5 numbers that are not Miller-Rabin witnesses for n.

   You can use the Mathematica function mrWitness[ ] from class in this problem.

   (a) $n = 930\,353$

   (b) $n = 267\,479$

   (c) $n = 3^{122} - 8$

   (d) $n = 110\,881$

   (e) n is the number from (d) read upside down

3. For each value n in #2 that you found was composite, use Pollard's ρ to completely factor n.

   You can use the Mathematica function pFactor[ ] from class.