

## MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2025, PROBLEMS 11

### To be submitted by Monday 10th November

Write programs to implement **LJ**, **QC** and the **Miller–Rabin** test in its deterministic form in which one assumes the Generalized Riemann Hypothesis, and use them to answer the following questions. The output from Miller-Rabin should read, for each number, either “ $n$  is composite.  $a$  is a witness.” where  $n$  is the number being tested and  $a$  is the value of the witness, or “ $n$  is prime”.

Submit any code you write to answer these questions.

1. Determine which of the following numbers are prime and which are composite.
  - (i) 3215031751,
  - (ii) 341550071728321,
  - (iii) 1234567891234567919,
  - (iv) 3825123056546413051,
  - (v) 1296001987165015643369032371289.
2. (i) Find the primes  $p$  with  $83 \leq p \leq 113$  for which  $a = 73$  is a quadratic residue modulo  $p$ ,  
(ii) Find the least quadratic residue  $a > 1$  and least positive quadratic non-residue  $b$  modulo  $p$  of whichever of 370370384407407431 and 370370384407407539 is prime  $p$ .
3. Consider the numbers

$$a_1 = 23456789023456789923456789923454566777888990189,$$

$$a_2 = 23456789023456789923456789923454566777888990190,$$

$$m_1 = 2447952037112100847479213118326022843437705003126289,$$

$$m_2 = 595457975987595849574985798595847594579485795794859456799501.$$

Use (LJ) to evaluate

$$\left( \frac{a_1}{m_1} \right)_J, \quad \left( \frac{a_2}{m_1} \right)_J, \quad \left( \frac{a_1}{m_2} \right)_J, \quad \left( \frac{a_2}{m_2} \right)_J$$

when  $m_j$  is prime (Miller-Rabin is useful here) and when the Legendre symbol is +1 solve (QC)

$$x^2 \equiv a_i \pmod{m_j}.$$