MATH 467 FACTORIZATION AND PRIMALITY TESTING, FALL 2023, PROBLEMS 8

Return by Monday 23rd October

1. Prove that if n is odd and $p|n$, then

$$\sum_{\substack{m=1\\(m,n)=1}}^{\phi(n)} \left(\frac{m}{p}\right)_L = 0.$$

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.

2. Determine which of the following numbers are prime and which are composite.
(i) 3215031751,
(ii) 341550071728321,
(iii) 1234567891234567919,
(iv) 3825123056546413051,
(v) 1296001987165015643369032371289,

3. (i) Find the primes p with $83 \le p \le 113$ 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.

4. Consider the numbers

$$a_1 = 234567890234567899234567899234545666777888990189,$$

$$a_2 = 234567890234567899234567899234545666777888990190,$$

$$m_1 = 2447952037112100847479213118326022843437705003126289,$$

$$m_2 = 59545797598759584957498579859585984759457948579595794859456799501.$$

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)

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