Name: ______________________________

Math/CS 467, Midterm 2
Fall 2020, John Lesieutre

- Write your exam on a separate sheet of paper and submit on Gradescope.
- You may consult the textbook, your notes, my slides, and the homework solutions during the exam. However, you may not consult other references on the internet.
- No calculators or other aids are allowed.
- Justifications or proofs are required for all problems except where indicated otherwise.
- If you aren't sure how to do a problem, don't leave it blank! I will give you a point or two if you define some of the terms appearing in the problem.
- If you need more space, continue on the back of the page. Mark your work clearly.
- You have 50 minutes to complete the exam.
- Good luck!

Problem 1. a) Compute the value of the Jacobi symbol $\left(\frac{621}{101}\right)$.

b) Suppose that p is a prime congruent to 5 (mod 8). Prove that $\left(\frac{2}{p}\right) = -1$.

Problem 2. a) Suppose that you wanted to factor the number 667 using Pollard's $p - 1$ method. Tell me what you would do, clearly stating each step. Please use specific numbers for the parameters. (You do not need to actually compute anything, just explain the steps of the algorithm.)

b) The actual factorization is $667 = 23 \cdot 29$. For what value of the variables will your algorithm find a factor? Which factor will it find? (You are looping over some number, which we have called "i" or "k". I want to know for which value of this number the $p - 1$ algorithm would find a factor.)

Problem 3. The number 85 is a base-67 pseudoprime.

a) State the *strong* base-67 pseudoprime test for $n = 85$. Tell me exactly what you would check. You do not need to compute anything.

b) Another way to test whether 85 is prime is to just factor it. Factor 85 using Fermat's algorithm. (No credit for other methods.)

Problem 4. The number 1063 is prime, and according to Fermat's little theorem, $5^{1062} \equiv 1 \pmod{1063}$.

a) It follows that either $5^{531} \equiv 1 \pmod{1063}$ or $5^{531} \equiv -1 \pmod{1063}$. How would you figure out which it is, without actually computing any exponentials? Describe a method.

b) Now figure it out: determine the value of $5^{531} \pmod{1063}$.

Problem 5. a) Suppose that p is an odd prime which is the largest number in a Pythagorean triple. This means there are integers x and y, both positive and less than p, such that $x^2 + y^2 = p^2$. Prove that $\left(\frac{-1}{p}\right) = 1$.

b) For which odd primes p is -1 a quadratic residue modulo p?