Intro to Number Theory (Fall 2024)
Final Practice Problems

Instructions: Write your name at the top. No notes, text, calculators, etc. are allowed. Please answer the questions in the space provided below. You may continue an answer on the back, but if you do so, please write SEE BACK in the space provided.

Quadratic reciprocity: Let p, q be distinct odd primes. Then

- Main law: $\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & p, q \text{ not both } 3 \mod 4 \\ -\left(\frac{p}{q}\right) & p \equiv q \equiv 3 \mod 4 \end{cases}$
- First supplementary law: $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4 \end{cases}$

Remarks: A couple of the problems are longer or more involved than an individual problem on the final exam would be.

0. Review your midterm exam, and the midterm practice problems to review up through Section 3.3. (The review problems below do not cover this material.)
1. State the following:
   (a) Lagrange's Theorem
   (b) Fermat's Little Theorem
   (c) Euler's Theorem
2. Compute $\phi(4 \cdot 5 \cdot 7)$. Briefly justify your work.
3. Determine the invertible elements mod 8, and for each of them state what their inverses are.
4. Compute $5^9 \mod 11$ by repeated squaring (show your work).
5. (a) Bob is making a public key for RSA. He chooses $p = 7$ and $q = 11$. He chooses $d = 43$ for his private decryption key. Determine Bob's public key.
   (b) Alice wants to securely send the message $m = 8$ to Bob. Encrypt m using Bob's public key.
6. Prove that $100! \equiv -1 \mod 101$.
7. Determine, with proof, which of the following numbers are sums of 2 squares, i.e., of the form $x^2 + y^2$ with $x, y \in \mathbb{Z}$:
   (a) 101
   (b) 23
   (c) 5050
8. Determine the squares mod 11 (show your work).
9. Determine, with proof, whether 11 is a square mod 103.
10. Determine, with proof, whether 7 is a square mod 103.