E. Dummit's Math 3527 $\sim$ Number Theory I, Spring 2020 $\sim$ Homework 11, due Fri Apr 17th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Either staple the pages of your assignment together and write your name on the first page, or paperclip the pages and write your name on all pages.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. List all of the (nonzero) quadratic residues, and all of the quadratic nonresidues, modulo 19.

---

2. Find all solutions to each of the following polynomial congruences:

   (a) $x^3 + 2x^2 + 3 \equiv 0 \pmod{132}$. (b) $x^3 + x + 4 \equiv 0 \pmod{49}$. (c) $x^4 - x^2 + 3 \equiv 0 \pmod{125}$.

---

3. Calculate the following Legendre symbols (i) using Euler's criterion, and (ii) using quadratic reciprocity for Jacobi symbols:

   (a) $\left(\frac{3}{17}\right)$. (b) $\left(\frac{15}{23}\right)$. (c) $\left(\frac{11}{733}\right)$. (d) $\left(\frac{-5}{67}\right)$. (e) $\left(\frac{67}{101}\right)$.

   (f) Which method is easier to implement by hand?

---

4. Calculate the following Jacobi symbols (i) using the definition in terms of Legendre symbols, and (ii) using quadratic reciprocity:

   (a) $\left(\frac{5}{51}\right)$. (b) $\left(\frac{3}{51}\right)$. (c) $\left(\frac{433}{777}\right)$. (d) $\left(\frac{881}{1101}\right)$.

   (e) Which method is easier to implement by hand?

---

5. Do the following:

   (a) Use Berlekamp's root-finding algorithm to find the roots of the polynomial $x^2 \equiv 38 \pmod{109}$.
   (b) Use the Solovay-Strassen test with $a = 3$ to test whether $m = 2773$ is composite.
   (c) Use the Solovay-Strassen test with $a = 1149$ to test whether $m = 6601$ is composite.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

6. Let $q(x) = x^2 + x - 4$ and let p be a prime.

   (a) Prove that there exists an integer solution n to the congruence $q(n) \equiv 0 \pmod{2027}$, given that the modulus 2027 is prime. [Hint: What do you have to take the square root of?]
   (b) Prove that there exists an integer solution n to the congruence $q(n) \equiv 0 \pmod{2027^{2020}}$. [Hint: Hensel's lemma.]

---

7. Let p be a prime. Prove that 13 is a quadratic residue modulo p if and only if $p = 2$, $p = 13$, or p is congruent to 1, 3, 4, 9, 10, or 12 modulo 13.

---

8. Suppose p and q are distinct odd primes, and define $q^* = (-1)^{(q-1)/2}q$. Prove that $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$. [Hint: Use quadratic reciprocity and break into 4 cases depending on whether p, q are 1 or 3 mod 4.]

   - Remark: This statement is in fact equivalent to the law of quadratic reciprocity, and is the version we actually found when we were discussing the motivation for the law.

---

9. Recall that if p is a prime congruent to 1 modulo 4, we proved in our study of factorization in $\mathbb{Z}[i]$ that there exist unique positive integers a and b such that $p = a^2 + b^2$. Suppose that a is odd and b is even, say with $b = 2k$. The goal of this problem is to show that both a and k are quadratic residues modulo p.

   (a) Verify that $\left(\frac{a}{p}\right) = +1$ and that $\left(\frac{k}{p}\right) = +1$ for the primes $p = 53$ and $p = 109$.

   (b) Show that the Legendre symbol $\left(\frac{a}{p}\right) = +1$. [Hint: Compute $\left(\frac{p}{a}\right)$ and use quadratic reciprocity.]

   (c) Show that the Legendre symbol $\left(\frac{2ab}{p}\right) = +1$ and deduce that $\left(\frac{k}{p}\right) = +1$. [Hint: Show explicitly that $2ab$ is the square of something mod p.]
