E. Dummit's Math 3527 ~ Number Theory I, Spring 2023 ~ Homework 11, due Fri Apr 21st.

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. Submit scans of your responses via Canvas.

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

1. Calculate the following Jacobi symbols (i) using the definition in terms of Legendre symbols, and (ii) using quadratic reciprocity for Jacobi symbols:
   (a) $\left(\frac{5}{51}\right)$.
   (b) $\left(\frac{3}{51}\right)$.
   (c) $\left(\frac{433}{777}\right)$.
   (d) Which method is easier to implement by hand?

---

2. Calculate the following Legendre symbols (i) using quadratic reciprocity for Legendre symbols by factoring the top number at each stage, and (ii) using quadratic reciprocity for Jacobi symbols:
   (a) $\left(\frac{15}{47}\right)$.
   (b) $\left(\frac{231}{1423}\right)$.
   (c) $\left(\frac{1633}{6733}\right)$.
   (d) Which method is easier to implement by hand?

---

3. 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.
   (d) Use the Solovay-Strassen test with $a = 2, 3, 5$ to test whether $m = 1729$ is composite.

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

4. 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 Euler's criterion on $\left(\frac{(-1)^{(q-1)/2}}{p}\right)$.]

   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.

---

5. The goal of this problem is to classify the prime divisors of integers of the form $n^2 + n - 3$.

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

   (b) Prove that a prime p divides an integer of the form $q(n) = n^2 + n - 3$ if and only if $p = 13$ or p is congruent to 1, 3, 4, 9, 10, or 12 modulo 13. [Hint: What do you have to take the square root of?]

---

6. The goal of this problem is to prove that there are infinitely many primes congruent to 4 modulo 5.

   (a) Let n be a positive integer and let p be a prime dividing $5(n!)^2 - 1$. Show that $p > n$ and that $\left(\frac{5}{p}\right) = +1$.

   (b) Show that $5(n!)^2 - 1$ has at least one prime divisor not congruent to 1 modulo 5, and deduce that it has a prime divisor greater than n that is congruent to 4 modulo 5.

   (c) Deduce that there are infinitely many primes congruent to 4 modulo 5. [Hint: If P were the largest, apply (b) to $n = P$.]

---

7. As shown on problem 4 of homework 2, the only primes of the form $a^k - 1$ are those numbers $2^p - 1$ where p is prime, but as seen in problem 5 of homework 7, not all of these numbers actually are prime. The goal of this problem is to show the non-primality of some of these values $2^p - 1$.

   (a) Suppose that $q \equiv 7 \pmod 8$ is prime. Show that q divides $2^{(q-1)/2} - 1$. [Hint: Euler's criterion.]

   (b) Suppose that $p \equiv 3 \pmod 4$ is a prime such that $2p + 1$ is also prime. Show that $2^p - 1$ is composite.

   (c) Deduce that $2^p - 1$ is composite for the primes $p = 11, 23, 83, 131, 179, 183$.

---

8. The goal of this problem is to give several different proofs of the fact that if $p \equiv 1 \pmod 4$ is a prime, then the congruence $x^2 \equiv -1 \pmod p$ has a solution. In class, this was proven using primitive roots.

   (a) Show that if $x = \left(\frac{p-1}{2}\right)!$ then $x^2 \equiv -1 \pmod p$. [Hint: Note that $(p-1)! = [1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}] \cdot [(p - \frac{p-1}{2}) \cdots (p-2)(p-1)]$.]

   (b) Show that if $p \equiv 1 \pmod 4$, then -1 is a quadratic residue modulo p. [Hint: Euler's criterion.]

   (c) Suppose that a is any quadratic non-residue modulo p. Show that $x = a^{(p-1)/4}$ has $x^2 \equiv -1 \pmod p$. [Hint: Euler again.]

   (d) [Optional] Partition the $p - 1$ units modulo p into sets of the form $\{a, -a, a^{-1}, -a^{-1}\}$. Show that the only possible sizes of these sets are 2 and 4, and that a set can have size 2 only if $a = a^{-1}$ or $a = -a^{-1}$. Conclude that there must be 2 sets of size 2, namely $\{1, -1\}$ and $\{x, -x\}$ where $x^2 \equiv -1 \pmod p$.
