E. Dummit's Math 3527 ~ Number Theory I, Spring 2022 ~ Homework 10, due Fri Apr 22nd.

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 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?

---

2. 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?

---

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.

---

4. Show that there exists an integer solution to the congruence $x^2 + x \equiv 4 \pmod{2027}$, given that 2027 is prime. [Hint: What do you have to take the square root of?]

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

5. 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.

---

6. 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.

---

7. 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 $n = P$.]

---

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 $x^2 \equiv -1 \pmod p$.

---

9. Recall (cf. Homework 1) that the Fibonacci-Virahanka numbers F_n are defined by $F_1 = F_2 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geq 1$. The goal of this problem is to show that if F_k is a prime congruent to 1 modulo 4, then (i) F_k is the sum of two squares of Fibonacci numbers and (ii) the two square roots of -1 modulo F_k are also Fibonacci numbers.

   (a) Verify the results for the Fibonacci primes $F_5 = 5$, $F_7 = 13$, and $F_{11} = 89$.

   (b) Prove that $F_{2n+1} = F_{n+1}^2 + F_n^2$ and $F_{2n+2} = F_{n+1}(F_{n+2} + F_n)$ for all $n \geq 1$. [Hint: Show both statements together by induction.]

   (c) Suppose F_k is prime and $k > 4$. Show that k must be odd. [Hint: Use (b) if k is even.]

   (d) Suppose that F_k is a prime congruent to 1 modulo 4: then F_k can be written uniquely as the sum of two squares $F_k = a^2 + b^2$ for positive a, b. Show that both a and b are Fibonacci numbers.

   (e) Suppose that F_k is a prime congruent to 1 modulo 4: then -1 is a square modulo F_k. Show that the two square roots of -1 modulo F_k are F_{k-1} and F_{k-2}. [Hint: Use 5(c) from homework 1.]
