

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly and submit via Gradescope, making sure to select page submissions for each problem. Use of generative AI in any manner is not allowed on this or any other course assignments.

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 (factoring the bottom number), and (ii) using quadratic reciprocity for Jacobi symbols without factoring the bottom number:

(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 (no factoring):

(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 (make sure to give enough details to show that you actually used the requested algorithm):

- (a) Use Berlekamp's root-finding algorithm to find the roots of $x^2 - 38 \pmod{109}$.
 - (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. 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?]
-

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

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

6. As shown in problem 6 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, and $p > 3$. Show that $2^p - 1$ is composite.
 - (c) Deduce that $2^p - 1$ is composite for the primes $p = 11, 23, 83, 131, 179$.
-

7. 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 $(p-1)! = [1 \cdot 2 \cdots \frac{p-1}{2}] \cdot [(p - \frac{p-1}{2}) \cdots (p-2)(p-1)]$.]

(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.]

8. Recall (cf. Homework 1) that the Fibonacci 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 (i) and (ii) for the Fibonacci primes $F_5 = 5$, $F_7 = 13$, and $F_{11} = 89$.

(b) Show that F_{2n+2} is composite for $n > 1$. Deduce that if F_k is prime and $k > 4$ then k is odd. [Hint: Use problem 4(c) of homework 1.]

(c) 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. [Hint: Use problem 4(c) of homework 1.]

(d) 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 problem 4(b) of homework 1.]
