---

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) $\left(\frac{5}{51}\right)$.

   - From the definition, we have $\left(\frac{5}{51}\right) = \left(\frac{5}{3}\right)\left(\frac{5}{17}\right)$. Using Euler's criterion to evaluate the Legendre symbols gives $\left(\frac{5}{3}\right) = -1$ and $\left(\frac{5}{17}\right) = -1$, so we see $\left(\frac{5}{51}\right) = \boxed{+1}$.
   - Using quadratic reciprocity, we have $\left(\frac{5}{51}\right) = \left(\frac{51}{5}\right) = \left(\frac{1}{5}\right) = \boxed{+1}$.

   (b) $\left(\frac{3}{51}\right)$.

   - From the definition, we have $\left(\frac{3}{51}\right) = \left(\frac{3}{3}\right)\left(\frac{3}{17}\right) = \boxed{0}$ since the first term is zero.
   - Using quadratic reciprocity, we have $\left(\frac{3}{51}\right) = -\left(\frac{51}{3}\right) = \left(\frac{0}{3}\right) = \boxed{0}$.

   (c) $\left(\frac{433}{777}\right)$.

   - From the definition, we have $\left(\frac{433}{777}\right) = \left(\frac{433}{3}\right)^2\left(\frac{433}{7}\right)\left(\frac{433}{37}\right)$. Evaluating the Legendre symbols gives $\left(\frac{433}{3}\right) = \left(\frac{1}{3}\right) = +1$, $\left(\frac{433}{7}\right) = \left(\frac{-1}{7}\right) = -1$, and $\left(\frac{433}{37}\right) = +1$ by Euler's criterion, so we see $\left(\frac{433}{777}\right) = \boxed{-1}$.
   - Using quadratic reciprocity, we have $\left(\frac{433}{777}\right) = \left(\frac{777}{433}\right) = \left(\frac{-89}{433}\right) = \left(\frac{-1}{433}\right)\left(\frac{89}{433}\right) = \left(\frac{433}{89}\right) = \left(\frac{-12}{89}\right) = \left(\frac{-1}{89}\right)\left(\frac{2}{89}\right)^2\left(\frac{3}{89}\right) = \left(\frac{89}{3}\right) = \left(\frac{2}{3}\right) = \boxed{-1}$.

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

   - The approach using quadratic reciprocity is much easier in essentially all situations, because to use the definition we must first factor the bottom number, and then we need to evaluate several Legendre symbols (each of which takes nearly as much effort as just doing one Jacobi symbol).

---

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) $\left(\frac{15}{47}\right)$.

- Using factoring: $\left(\frac{15}{47}\right) = \left(\frac{3}{47}\right)\left(\frac{5}{47}\right) = -\left(\frac{47}{3}\right)\left(\frac{47}{5}\right) = -\left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = -(-1)(-1) = \boxed{-1}$.
- Using Jacobi symbols: $\left(\frac{15}{47}\right) = -\left(\frac{47}{15}\right) = -\left(\frac{2}{15}\right) = \boxed{-1}$.

(b) $\left(\frac{231}{1423}\right)$.

- Using factoring: $\left(\frac{231}{1423}\right) = \left(\frac{3}{1423}\right)\left(\frac{7}{1423}\right)\left(\frac{11}{1423}\right) = -\left(\frac{1423}{3}\right)\left(\frac{1423}{7}\right)\left(\frac{1423}{11}\right) = -\left(\frac{1}{3}\right)\left(\frac{2}{7}\right)\left(\frac{4}{11}\right) = -(+1)(+1)(+1) = \boxed{-1}$.
- Using Jacobi symbols: $\left(\frac{231}{1423}\right) = -\left(\frac{1423}{231}\right) = -\left(\frac{37}{231}\right) = -\left(\frac{231}{37}\right) = -\left(\frac{9}{37}\right) = \boxed{-1}$.

(c) $\left(\frac{1633}{6733}\right)$.

- Using factoring: $\left(\frac{1633}{6733}\right) = \left(\frac{23}{6733}\right)\left(\frac{71}{6733}\right) = \left(\frac{6733}{23}\right)\left(\frac{6733}{71}\right) = \left(\frac{17}{23}\right)\left(\frac{59}{71}\right) = -\left(\frac{23}{17}\right)\left(\frac{71}{59}\right) = -\left(\frac{6}{17}\right)\left(\frac{12}{59}\right) = -\left(\frac{2}{17}\right)\left(\frac{3}{17}\right)\left(\frac{2}{59}\right)^2\left(\frac{3}{59}\right) = \left(\frac{17}{3}\right)\left(\frac{59}{3}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = \boxed{+1}$.
- Using Jacobi symbols: $\left(\frac{1633}{6733}\right) = \left(\frac{6733}{1633}\right) = \left(\frac{201}{1633}\right) = \left(\frac{1633}{201}\right) = \left(\frac{25}{201}\right) = \boxed{+1}$.

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

- Factoring produces smaller calculations a bit more quickly, but requires actually doing factorization, and the number of Legendre symbols produced tends to increase as the calculation progresses, requiring yet more calculations. The Jacobi symbol procedure is much easier with large numbers, since we don't need to do anything except pull out factors of 2 and -1 each time.

---

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 $x^2 - 38 \pmod{109}$.

- First, we can compute $\left(\frac{38}{109}\right) = +1$ (either via Euler's criterion or by using quadratic reciprocity), so 38 does have square roots modulo 109.
- To compute them we let $q(x) = x^2 - 38$ modulo $p = 109$.
- As noted in the lectures, $a = 0$ will not work, so we try $a = 1$, so that $q(x-1) = x^2 - 2x - 37$.
- Using successive squaring, we can calculate $x^{(p-1)/2} = x^{54} \equiv 34x + 75 \pmod{q}$.
- This means $x^{(p-1)/2} - 1 \equiv 34x + 74 \pmod{q}$, and so the first step of the Euclidean algorithm reads $x^{(p-1)/2} \equiv [\text{quotient}] \cdot q(x-a) + (34x + 74)$. The next step comes out evenly, so we get a gcd of $34x + 74$.
- Solving for the first root (i.e., solving $34n + 74 \equiv 0 \pmod{109}$) yields $n \equiv 94 \pmod{109}$.
- This means $n = 94$ is a root of $q(x-1)$, and therefore $n - 1 = 93$ is a root of the original polynomial $q(x)$.
- Indeed, we can check that $93^2 \equiv 38 \pmod{109}$. Therefore, the two roots are $r \equiv \boxed{\pm 93} \pmod{109}$.

(b) Use the Solovay-Strassen test with $a = 3$ to test whether $m = 2773$ is composite.

- With $a = 3$, we have $3^{(m-1)/2} \equiv 3^{1386} \equiv 635 \pmod{2773}$, whereas $\left(\frac{3}{2773}\right) = \left(\frac{2773}{3}\right) = \left(\frac{1}{3}\right) = +1$. Since these are unequal, we conclude that 2773 is $\boxed{\text{composite}}$.

(c) Use the Solovay-Strassen test with $a = 1149$ to test whether $m = 6601$ is composite.

- With $a = 1149$, we have $1149^{(m-1)/2} \equiv 1149^{3300} \equiv 1 \pmod{6601}$.
- On the other hand, $\left(\frac{1149}{6601}\right) = \left(\frac{6601}{1149}\right) = \left(\frac{856}{1149}\right) = \left(\frac{2}{1149}\right)^3 \left(\frac{107}{1149}\right) = -1 \cdot \left(\frac{1149}{107}\right) = -\left(\frac{-28}{107}\right) = -\left(\frac{-1}{107}\right)\left(\frac{2}{107}\right)^2 \left(\frac{7}{107}\right) = -\left(\frac{107}{7}\right) = -\left(\frac{2}{7}\right) = -1$. Since these are unequal, we conclude that 6601 is $\boxed{\text{composite}}$.
- Remark: In fact, 6601 is a Carmichael number, so it passes the Fermat test for every residue class.

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

- With $a = 2$, we have $2^{(m-1)/2} \equiv 2^{864} \equiv 1 \pmod{1729}$ and $\left(\frac{2}{1729}\right) = +1$ since $1729 \equiv 1 \pmod 8$. Since these are equal, the test is $\boxed{\text{inconclusive}}$.
- With $a = 3$, we have $3^{(m-1)/2} \equiv 3^{864} \equiv 1 \pmod{1729}$ and $\left(\frac{3}{1729}\right) = \left(\frac{1729}{3}\right) = \left(\frac{1}{3}\right) = +1$ since $1729 \equiv 1 \pmod 4$. Since these are equal, the test is $\boxed{\text{inconclusive}}$.
- With $a = 5$, we have $5^{(m-1)/2} \equiv 5^{864} \equiv 1 \pmod{1729}$ and $\left(\frac{5}{1729}\right) = \left(\frac{1729}{5}\right) = \left(\frac{4}{5}\right) = +1$ since $1729 \equiv 1 \pmod 4$. Since these are equal, the test is $\boxed{\text{inconclusive}}$.

---

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.

- Clearly 13 is a square modulo 2 (since $13 \equiv 1^2 \bmod 2$) and modulo 13 (since $13 \equiv 0^2 \bmod 13$), so we can now assume p is odd and that $p \neq 13$.
- Now we just need to calculate $\left(\frac{13}{p}\right)$, for $p \neq 2, 13$, and in particular we want to know when this Legendre symbol is $+1$.
- Since $p \equiv 1 \pmod 4$, quadratic reciprocity says that $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right)$.
- But $\left(\frac{p}{13}\right) = +1$ precisely when p is a quadratic residue modulo 13.
- Since the quadratic residues modulo 13 are $\{1^2, 2^2, 3^2, 4^2, 5^2, 6^2\} \equiv \{1, 4, 9, 3, 12, 10\}$, this means that $\left(\frac{13}{p}\right) = \left(\frac{p}{13}\right) = +1$ precisely when p is congruent to 1, 3, 4, 9, 10, or 12 modulo 13. This is exactly the required result, so we are done.

(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?]

- Note that 2 divides no values of $q(n)$, since $q(0) \equiv q(1) \equiv 1 \pmod 2$. So now assume that p is an odd prime that divides $n^2 + n - 3$.
- By completing the square, or equivalently by using the quadratic formula, the roots of the polynomial $x^2 + x - 3 = 0$ are $x = \frac{-1 \pm \sqrt{13}}{2}$.
- Therefore, since p is odd, there is an integer solution to $q(n) \equiv 0 \pmod p$ if and only if 13 is a square modulo p. By (a), we know this happens for odd primes p precisely when $p = 13$ or p is congruent to 1, 3, 4, 9, 10, or 12 modulo 13.
- Hence putting this together with the lack of divisibility for $p = 2$ shows immediately that $n^2+n-3 \equiv 0 \pmod p$ has a solution if and only if $p = 13$ or p is congruent to 1, 3, 4, 9, 10, or 12 modulo 13.

---

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 $\left(\frac{5}{p}\right) = +1$.

   - If it were true that $p \leq n$ then p would divide $n!$ hence divide $5(n!)^2$, but then p would divide the difference $5(n!)^2 - [5(n!)^2 - 1] = 1$, impossible.
   - Additionally, we have $5(n!)^2 \equiv 1 \pmod{p}$, so since $(n!)^2$ is a unit mod p, we see $5 \equiv (n!)^{-2} \pmod{p}$ and so 5 is a quadratic residue modulo p. Since $p \neq 5$ since $5(n!)^2 - 1$ is not divisible by 5, we must have $\left(\frac{5}{p}\right) = +1$.

   (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.

   - Note that $5(n!)^2 - 1 \equiv -1 \pmod{5}$, so at least one prime divisor p is not congruent to 1 mod 5 (since otherwise the product would be 1 mod 5).
   - By (a), this prime is greater than n and $\left(\frac{5}{p}\right) = +1$. But by quadratic reciprocity we have $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, and $\left(\frac{p}{5}\right) = +1$ requires $p \equiv \pm 1 \pmod{5}$, so the only possibility is that $p \equiv 4 \pmod{5}$.

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

   - By (b), for any n we can construct a prime $p > n$ that is congruent to 4 modulo 5.
   - This implies there are infinitely many primes congruent to 4 modulo 5, for if there were only finitely many, if P were the largest, applying (b) to $n = P$ would yield a larger one.

---

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.]

   - We know from our study of Legendre symbol values that $\left(\frac{2}{q}\right) = +1$ for $q \equiv 7 \pmod{8}$.
   - By Euler's criterion, we have $2^{(q-1)/2} \equiv \left(\frac{2}{q}\right) = +1 \pmod{q}$, meaning that q divides $2^{(q-1)/2} - 1$ as claimed.

   (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.

   - If $p \equiv 3 \pmod{4}$ then letting $q = 2p + 1$ we have $q = 2p + 1 \equiv 7 \pmod{8}$.
   - So applying (a) shows that $2^{(q-1)/2} - 1 = 2^p - 1$ is divisible by $q = 2p + 1$. Since $2^p - 1 > 2p + 1$ for $p > 3$ this means $2^p - 1$ is composite.

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

   - Observe that these primes are all 3 mod 4, and that for these p the value $2p+1 = 23, 47, 167, 263, 359$ is prime as well. Hence by (b), $2^p - 1$ is composite for all these p.

---

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 $(p-1)! = [1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}] \cdot [(p - \frac{p-1}{2}) \cdots (p-2)(p-1)]$.]
   - Per the hint, we break $(p-1)!$ into the product $(p-1)! = [1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2}] \cdot [(p - \frac{p-1}{2}) \cdots (p-2)(p-1)]$. But modulo p, the terms at the end are simply $-\frac{p-1}{2}$, ... , -2, -1.
   - Thus $(p-1)! = \left[\frac{p-1}{2}\right]! \cdot \left[\frac{p-1}{2}\right]! \cdot (-1)^{(p-1)/2} \equiv \left[\left[\frac{p-1}{2}\right]!\right]^2 \pmod p$ as $(p-1)/2$ is even.
   - So by Wilson's theorem, for $x = \left[\frac{p-1}{2}\right]!$ we have $x^2 \equiv (p-1)! \equiv -1 \pmod p$.

   (b) Show that if $p \equiv 1 \pmod 4$, then -1 is a quadratic residue modulo p. [Hint: Euler's criterion.]
   - By Euler's criterion, we have $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = 1 \pmod p$ since $(p-1)/2$ is even. But since $p > 2$, the only way these quantities can be congruent is if $\left(\frac{-1}{p}\right) = 1$, meaning that -1 is a quadratic residue modulo p.

   (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.]
   - Suppose that a is any quadratic non-residue modulo p. Then by Euler's criterion, we have $-1 = \left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod p$.
   - Therefore, for $x = a^{(p-1)/4}$, we have $x^2 \equiv a^{(p-1)/2} \equiv -1 \pmod p$.

---

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 $F_{11} = 89$.
   - We have $5 = 2^2 + 1^2$ and the square roots of -1 modulo 5 are 2 and 3.
   - Also, $13 = 3^2 + 2^2$ and the square roots of -1 modulo 13 are 5 and 8.
   - Finally, $89 = 8^2 + 5^2$ and the square roots of -1 modulo 89 are 34 and 55.

   (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.]
   - Problem 4(c) of homework 1 contained the identity $F_{2n+2} = F_{n+1}(F_{n+2} + F_n)$.
   - If $n > 1$ then $F_{n+1} > 1$ and also $F_{n+2} + F_n > 1$, so F_{2n+2} is composite.
   - Then the only way F_k can be prime with $k > 4$ is if k is odd, as claimed.

   (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.]
   - By (b), if F_k is a prime congruent to 1 modulo 4, then $k = 2n+1$ must be odd.
   - By 4(c) of homework 1, we have $F_k = F_{n+1}^2 + F_n^2$. Since the decomposition of F_k as a sum of two squares is unique because F_k is a prime congruent to 1 modulo 4, we must have $a = F_{n+1}$ and $b = F_n$.

   (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.]
   - By (b), if F_k is a prime congruent to 1 modulo 4, then k must be odd.
   - By 4(b) of homework 1, we have $F_{k-1}^2 - F_{k-2}F_k = (-1)^k$. Modulo F_k this yields $F_{k-1}^2 \equiv (-1)^k \equiv -1 \pmod{F_k}$ since k is odd.
   - Thus, F_{k-1} is one of the two square roots of -1 modulo F_k. The other is then its negative, $-F_{k-1} \equiv F_k - F_{k-1} = F_{k-2} \pmod{F_k}$, as claimed.
