1. List all of the (nonzero) quadratic residues, and all of the quadratic nonresidues, modulo 19.
   - From our discussion, the quadratic residues are \( \{1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2\} = \{1, 4, 9, 16, 6, 17, 11, 7, 15\} \).
   - Then the quadratic nonresidues are the remaining nonzero residue classes \( \{2, 3, 7, 8, 10, 12, 13, 14, 18\} \).

2. Find all solutions to each of the following polynomial congruences:
   (a) \( x^3 + 2x^2 + 3 \equiv 0 \pmod{132} \).
      - Note that 132 = 2^2 \cdot 3 \cdot 11. So by the Chinese remainder theorem, we just need to solve the congruence \( \pmod{2^2} \), \( \pmod{3} \), and \( \pmod{11} \), and then glue the results back together.
      - We can solve each individual congruence just by testing all possible residue classes to see if \( q(x) = x^3 + 2x^2 + 3 \) is zero on one.
      - Mod 4, we have \( q(0) = 3 \), \( q(1) = 2 \), \( q(2) = 3 \), \( q(3) = 0 \) so the solution is \( x \equiv 3 \pmod{4} \).
      - Mod 3, we have \( q(0) = 0 \), \( q(1) = 0 \), \( q(2) = 1 \), so the solutions are \( x \equiv 0, 1 \pmod{3} \).
      - Mod 11, we have \( q(0) = 3 \), \( q(1) = 6 \), \( q(2) = 8 \), \( q(3) = 4 \), \( q(4) = 0 \), \( q(5) = 2 \), \( q(6) = 5 \), \( q(7) = 4 \), \( q(8) = 5 \), \( q(9) = 3 \), \( q(10) = 4 \), so the solution is \( x \equiv 4 \pmod{11} \).
      - We will then have two solutions modulo 132, obtained by solving the simultaneous congruences \( x \equiv 3 \pmod{4} \), \( x \equiv 0, 1 \pmod{3} \), \( x \equiv 4 \pmod{11} \).
      - The resulting two solutions are \( x \equiv 15, 103 \pmod{132} \).

   (b) \( x^3 + x + 4 \equiv 0 \pmod{49} \).
      - Since 49 = 7^2, we first solve the congruence modulo 7.
      - If \( q(x) = x^3 + x + 4 \), we can compute \( q(0) = 4 \), \( q(1) = 6 \), \( q(2) = 0 \), \( q(3) = 6 \), \( q(4) = 2 \), \( q(5) = 1 \), \( q(6) = 2 \pmod{7} \).
      - Thus, the only solution to \( q(x) \equiv 0 \pmod{7} \) is \( x \equiv 2 \pmod{7} \).
      - Now we lift to find the solutions modulo 7^2; we know we must have \( x = 2 + 7a \).
      - Plugging in yields \( (2 + 7a)^3 + (2 + 7a) + 4 \equiv 0 \pmod{49} \), which, upon expanding and reducing, simplifies to \( 42a \equiv 35 \pmod{49} \).
      - Cancelling the factor of 7 yields \( 6a \equiv 5 \pmod{7} \), which has the single solution \( a \equiv 2 \pmod{7} \).
      - This yields the single solution \( x \equiv 16 \pmod{49} \) to our original congruence.

   (c) \( x^4 - x^2 + 3 \equiv 0 \pmod{125} \).
      - Since 125 = 5^3, we first solve the congruence modulo 5.
      - If \( q(x) = x^4 - x^2 + 3 \), we can compute \( q(0) = 3 \), \( q(1) = 3 \), \( q(2) = 0 \), \( q(3) = 0 \), \( q(4) = 3 \pmod{5} \).
      - Thus, the solutions to \( q(x) \equiv 0 \pmod{5} \) are \( x \equiv 2, 3 \pmod{5} \).
      - Now we lift to find the solutions modulo 5^2.
      - If \( x = 2 + 5a \) we obtain \( (2 + 5a)^4 - (2 + 5a)^2 + 3 \equiv 0 \pmod{25} \), which, upon expanding and reducing, simplifies to \( 15a \equiv 10 \pmod{25} \). Cancelling the factor of 5 yields \( 3a \equiv 2 \pmod{5} \) giving \( a = 4 \pmod{5} \) and so \( x \equiv 22 \pmod{25} \).
      - If \( x = 3 + 5a \) we obtain \( (3 + 5a)^4 - (3 + 5a)^2 + 3 \equiv 0 \pmod{25} \), which, upon expanding and reducing, simplifies to \( 10a \equiv 0 \pmod{25} \). Cancelling the factor of 5 yields \( 2a \equiv 0 \pmod{5} \) giving \( a \equiv 0 \pmod{5} \) and so \( x \equiv 3 \pmod{25} \).
      - Now we lift each solution to the modulus 5^3.
      - If \( x = 22 + 25a \) we obtain \( (22 + 25a)^4 - (22 + 25a)^2 + 3 \equiv 0 \pmod{125} \), which, upon expanding and reducing, simplifies to \( 75a \equiv 100 \pmod{125} \). Cancelling the factor of 25 yields \( 3a \equiv 4 \pmod{5} \) giving \( a = 3 \pmod{5} \) and so \( x \equiv 97 \pmod{125} \).
      - If \( x = 3 + 25a \) we obtain \( (3 + 25a)^4 - (3 + 25a)^2 + 3 \equiv 0 \pmod{125} \), which, upon expanding and reducing, simplifies to \( 50a \equiv 50 \pmod{125} \). Cancelling the factor of 25 yields \( 2a \equiv 2 \pmod{5} \) giving \( a \equiv 1 \pmod{5} \) and so \( x \equiv 28 \pmod{25} \).
      - This yields the two solutions \( x \equiv 22, 97 \pmod{125} \) to our original congruence.
3. Calculate the following Legendre symbols (i) using Euler’s criterion, and (ii) using quadratic reciprocity for Jacobi symbols:

(a) \( \left( \frac{3}{17} \right) \).
   - Using Euler’s criterion, we have \( 3^{(17-1)/2} \equiv 3^8 \equiv -1 \) (mod 17).
   - Using quadratic reciprocity, we have \( \left( \frac{3}{17} \right) = \left( \frac{17}{3} \right) = \left( \frac{2}{3} \right) = -1 \).

(b) \( \left( \frac{15}{23} \right) \).
   - Using Euler’s criterion, we have \( 15^{(23-1)/2} \equiv 15^{11} \equiv -1 \) (mod 23).
   - Using quadratic reciprocity for Jacobi symbols, we have \( \left( \frac{15}{23} \right) = - \left( \frac{23}{15} \right) = - \left( \frac{8}{15} \right) = - \left( \frac{2}{15} \right)^3 = -1 \) since \( \left( \frac{2}{15} \right) = 1 \) because 15 is 7 mod 8.

(c) \( \left( \frac{11}{733} \right) \).
   - Using Euler’s criterion, we have \( 11^{(733-1)/2} \equiv 11^{366} \equiv -1 \) (mod 733).
   - Using quadratic reciprocity for Jacobi symbols, we have \( \left( \frac{11}{733} \right) = \left( \frac{733}{11} \right) = \left( \frac{7}{11} \right) = - \left( \frac{11}{7} \right) = - \left( \frac{4}{7} \right) = -1 \).

(d) \( \left( \frac{-5}{67} \right) \).
   - Using Euler’s criterion, we have \( (-5)^{(67-1)/2} \equiv (-5)^{33} \equiv +1 \) (mod 67).
   - Using quadratic reciprocity for Jacobi symbols, we have \( \left( \frac{-5}{67} \right) = \left( \frac{-1}{67} \right) \left( \frac{5}{67} \right) = -1 \cdot \left( \frac{67}{5} \right) = -1 \cdot \left( \frac{2}{5} \right) = +1 \) since \( \left( \frac{2}{5} \right) = 1 \) because 67 is 3 mod 8.

(e) \( \left( \frac{67}{101} \right) \).
   - Using Euler’s criterion, we have \( 67^{(101-1)/2} \equiv 67^{50} \equiv -1 \) (mod 101).
   - Using quadratic reciprocity for Jacobi symbols, we have \( \left( \frac{67}{101} \right) = \left( \frac{101}{67} \right) = \left( \frac{34}{67} \right) = \left( \frac{2}{67} \right) \left( \frac{17}{67} \right) = (-1) \cdot \left( \frac{17}{67} \right) = (-1) \cdot \left( \frac{-1}{67} \right) = -1 \) since \( \left( \frac{-1}{67} \right) = -1 \) and \( \left( \frac{-1}{17} \right) = +1 \).

(f) Which method is easier to implement by hand?
   - Although we only wrote one line for each Euler’s criterion calculation, the actual details are quite lengthy because we need to use successive squaring to evaluate each modular power. (The calculation for (a) is fairly short, but the rest are quite a bit more involved.)
   - The approach using quadratic reciprocity is actually much easier when the numbers are large, at least if the procedure is being done by hand, since it is effectively just using the Euclidean algorithm, which we know to be very fast and easy to perform by hand.
4. Calculate the following Jacobi symbols (i) using the definition in terms of Legendre symbols, and (ii) using quadratic reciprocity:

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

- 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 \( \left( \frac{5}{51} \right) = -1 \).
- Using quadratic reciprocity, we have \( \left( \frac{5}{51} \right) = \left( \frac{51}{5} \right) = \left( \frac{1}{5} \right) = +1 \).

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

- From the definition, we have \( \left( \frac{3}{51} \right) = \left( \frac{3}{3} \right) \left( \frac{3}{17} \right) = \left( \frac{1}{3} \right) = 0 \) since the first term is zero.
- Using quadratic reciprocity, we have \( \left( \frac{3}{51} \right) = - \left( \frac{51}{3} \right) = \left( \frac{0}{3} \right) = 0 \).

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

- From the definition, we have \( \left( \frac{433}{777} \right) = \left( \frac{433}{3} \right) \left( \frac{433}{7} \right) \left( \frac{433}{37} \right) \). 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 \( \left( \frac{433}{777} \right) = -1 \).
- Using quadratic reciprocity, we have \( \left( \frac{433}{777} \right) = \left( \frac{777}{433} \right) = \left( \frac{-89}{433} \right) = \left( \frac{-1}{433} \right) \left( \frac{89}{433} \right) = \left( \frac{433}{89} \right) = \left( \frac{-1}{89} \right) \left( \frac{2}{89} \right) \left( \frac{3}{89} \right) = \left( \frac{89}{3} \right) = \left( \frac{2}{3} \right) = -1 \).

(d) \( \left( \frac{881}{1101} \right) \).

- From the definition, we have \( \left( \frac{881}{1101} \right) = \left( \frac{881}{3} \right) \left( \frac{881}{367} \right) \). Evaluating the Legendre symbols gives \( \left( \frac{881}{3} \right) = \left( \frac{2}{3} \right) = -1 \), and \( \left( \frac{881}{367} \right) = \left( \frac{147}{367} \right) = -1 \) by Euler’s criterion, so we see \( \left( \frac{881}{1101} \right) = +1 \).
- Using quadratic reciprocity, we have \( \left( \frac{881}{1101} \right) = \left( \frac{1101}{881} \right) = \left( \frac{220}{881} \right) \left( \frac{2}{881} \right) \left( \frac{55}{881} \right) = \left( \frac{881}{55} \right) = \left( \frac{1}{55} \right) = +1 \).

(e) 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).
5. Do the following:

(a) Use Berlekamp’s root-finding algorithm to find the roots of the polynomial \(x^2 \equiv 38 \pmod{109}\).

- 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 \(r \equiv \pm 93 \pmod{109}\).

(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 \(\text{composite}\).

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

- With \(a = 1149\), we have \(1149^{(m-1)/2} \equiv 1149^{4300} \equiv 1 \pmod{6601}\).
- On the other hand, \(\left(\frac{1149}{6601}\right) = \left(\frac{6601}{1149}\right) = \left(\frac{856}{1149}\right) = \left(\frac{2}{1149}\right)^3 \left(\frac{107}{1149}\right) = -1 \cdot \left(\frac{1149}{107}\right) = -\left(\frac{28}{107}\right) = -\left(\frac{-1}{107}\right) \cdot \left(\frac{2}{107}\right)^2 \left(\frac{7}{107}\right) = -\left(\frac{107}{7}\right) = -\left(\frac{2}{7}\right) = -1\). Since these are unequal, we conclude that 6601 is \(\text{composite}\).
- Remark: In fact, 6601 is a Carmichael number, so it passes the Fermat test for every residue class.

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?]

- By completing the square, or equivalently by using the quadratic formula, the roots of this polynomial are \(x = \frac{-1 \pm \sqrt{13}}{2}\).
- Therefore, since the modulus is odd, there is an integer solution if and only if 13 is a square modulo 2027; we can determine this by evaluating the Legendre symbol \(\left(\frac{13}{2027}\right)\).
- Using quadratic reciprocity, we see \(\left(\frac{13}{2027}\right) = \left(\frac{2027}{13}\right) = \left(\frac{-1}{13}\right) = +1\) since 13 is congruent to 1 mod 4.
- Since the Legendre symbol evaluates to +1, this means that 13 is a quadratic residue modulo 2027, and thus we may find its square root.
- Remark: Using Berlekamp’s root-finding algorithm, we can explicitly find the square roots of 13 as \(\pm 374 \pmod{2027}\), and so the solutions to the congruence are \(x = 392, 1634 \pmod{2027}\). In principle, identifying these solutions is also a way to solve this problem, but that approach does more work than was asked.

(b) Prove that there exists an integer solution \(n\) to the congruence \(q(n) \equiv 0 \pmod{2027^{2020}}\). [Hint: Hensel’s lemma.]
We follow the hint and use Hensel’s lemma, which assures us that a solution \( x = a \) to \( q(x) \equiv 0 \pmod{2027} \) will lift to a unique solution of \( q(x) \equiv 0 \pmod{2027^d} \) for any \( d \geq 1 \) provided that \( q(a) \neq 0 \pmod{2027} \).

Since \( q'(x) = 2x + 1 \), the only root of \( q'(x) = 0 \) is the value with \( 2r + 1 \equiv 0 \pmod{2027} \). This value is \( r \equiv 1013 \pmod{2027} \) and it is easy to see that it is not one of our roots.

Alternatively, we could notice that \( q(x) \) and \( q'(x) \) are relatively prime polynomials, since their polynomial greatest common divisor (with integer coefficients) is 13, so the only time that \( q \) and \( q' \) share a common root is when the modulus is 13.

Alternatively, we could observe that the quadratic has two roots by part (a), and since there is only one solution to \( q'(x) = 0 \), at least one of the roots must not be this root of the derivative.

In any case, we see that \( q'(a) \neq 0 \) for (at least) one root \( a \), and therefore by Hensel’s lemma, it lifts to a unique solution of \( q(x) \equiv 0 \pmod{2027^{2020}} \).

---

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.

- Clearly 13 is a quadratic residue modulo 2 (since 13 \( \equiv 1 \pmod{2} \)) and modulo 13 (since 13 \( \equiv 0 \pmod{13} \)), so we can now assume \( p \) is odd and that \( p \neq 13 \).
- We want to compute \( \left( \frac{13}{p} \right) \), 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 \( \left( \frac{p}{13} \right) = +1 \) exactly 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 \( \left( \frac{13}{p} \right) = \left( \frac{p}{13} \right) = +1 \) exactly when \( p \) is congruent to 1, 3, 4, 9, 10, or 12 modulo 13. This is exactly the required result, so we are done.

---

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.]

- Recall that \( \left( \frac{-1}{p} \right) = +1 \) when \( p \equiv 1 \pmod{4} \) and \( \left( \frac{-1}{p} \right) = -1 \) when \( p \equiv 3 \pmod{4} \). Also note that \( q^* = q \) when \( q \equiv 1 \pmod{4} \) and \( q^* = -q \) when \( q \equiv 3 \pmod{4} \).
- If \( p \equiv 1 \pmod{4} \) and \( q \equiv 1 \pmod{4} \), then we have \( \left( \frac{q^*}{p} \right) = \left( \frac{q}{p} \right) = +1 \cdot \left( \frac{p}{q} \right) \) by quadratic reciprocity.
- If \( p \equiv 1 \pmod{4} \) and \( q \equiv 3 \pmod{4} \), then we have \( \left( \frac{q^*}{p} \right) = \left( \frac{-q}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) = +1 \cdot \left( \frac{p}{q} \right) \) by quadratic reciprocity.
- If \( p \equiv 3 \pmod{4} \) and \( q \equiv 1 \pmod{4} \), then we have \( \left( \frac{q^*}{p} \right) = \left( \frac{q}{p} \right) = \left( \frac{p}{q} \right) \) by quadratic reciprocity.
- If \( p \equiv 3 \pmod{4} \) and \( q \equiv 3 \pmod{4} \), then we have \( \left( \frac{q^*}{p} \right) = \left( \frac{-q}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{q}{p} \right) = -1 \cdot \left( \frac{p}{q} \right) = \left( \frac{p}{q} \right) \) by quadratic reciprocity.

In all four cases, we obtain the required equality \( \left( \frac{p}{q} \right) = \left( \frac{q^*}{p} \right) \).

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.
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 \( p = 109 \).

- First, \( 53 = 7^2 + 2^2 \), we have \( a = 7 \) and \( k = 2/2 = 1 \).
- Then indeed we have \( \left( \frac{7}{53} \right) = \left( \frac{53}{7} \right) = \left( \frac{4}{7} \right) = +1 \) and \( \left( \frac{1}{51} \right) = +1 \) using quadratic reciprocity for the first calculation.
- Also, since \( 109 = 10^2 + 3^2 \), we have \( a = 3 \) and \( k = 10/2 = 5 \).
- Again, we have \( \left( \frac{3}{109} \right) = \left( \frac{109}{3} \right) = \left( \frac{1}{3} \right) = +1 \) and \( \left( \frac{5}{109} \right) = \left( \frac{109}{5} \right) = \left( \frac{4}{5} \right) = +1 \) using quadratic reciprocity.

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

- Following the hint, by quadratic reciprocity for Jacobi symbols we have \( \left( \frac{a}{p} \right) = \left( \frac{p}{a} \right) \) since \( p \equiv 1 \) (mod 4).
- But then since \( p = a^2 + b^2 \), we see \( \left( \frac{p}{a} \right) = \left( \frac{a^2 + b^2}{a} \right) = \left( \frac{b^2}{a} \right) = +1 \). Thus, combining the two statements yields \( \left( \frac{a}{p} \right) = +1 \), as claimed.

(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 \( p \).]

- Following the hint, observe that \( 2ab = (a + b)^2 - (a^2 + b^2) \), so since \( p = a^2 + b^2 \), we see \( 2ab \equiv (a + b)^2 \) (mod \( p \)).
- This means \( 2ab \) is a quadratic residue modulo \( p \), so \( \left( \frac{2ab}{p} \right) = +1 \).
- For the second statement, note that \( \left( \frac{2ab}{p} \right) = \left( \frac{4ak}{p} \right) = \left( \frac{4}{p} \right) \left( \frac{a}{p} \right) \left( \frac{k}{p} \right) \).
- But \( \left( \frac{4}{p} \right) = +1 \) since 4 is a quadratic residue, and \( \left( \frac{a}{p} \right) = +1 \) by part (a), so we must have \( \left( \frac{k}{p} \right) = +1 \) as claimed.