5 Squares and Quadratic Reciprocity

5.1 Polynomial Congruences and Hensel’s Lemma

• We discussed briefly the problem of solving higher-degree congruences in an earlier chapter: the Chinese Remainder Theorem reduces the problem of solving any polynomial congruence \(q(x) \equiv 0 \pmod{m}\) to solving the individual congruences \(q(x) \equiv 0 \pmod{p^d}\), where the \(p^d\) are the prime-power divisors of \(m\).

• To solve a polynomial congruence of the form \(q(x) \equiv 0 \pmod{p^d}\), we first observe that any solution modulo \(p^d\) “descends” to a solution modulo \(p\) (namely, by considering it modulo \(p\)).

  ◦ Thus, one way to find the solutions modulo \(p^d\) is to start by finding all solutions modulo \(p\), then “lift” each of these solutions to get all of the solutions modulo \(p^2\), then “lift” these to obtain all solutions modulo \(p^3\), and so forth.
• **Example:** Solve the congruence \( x^3 + 4x \equiv 4 \pmod{7^3} \).
  ○ We first solve the congruence modulo 7.
    * By trying all the residue classes, we see that \( x^3 + 4x \equiv 4 \pmod{7} \) has the single solution \( x \equiv 3 \pmod{7} \).
  ○ Next we “lift” to find the solutions modulo \( 7^2 \): any solution must be of the form \( x = 3 + 7k \) for some \( k \).
    * Plugging in yields \((3 + 7k)^3 + 4(3 + 7k) \equiv 4 \pmod{7^2}\), which, after expanding, is equivalent to \( 27 + 9 \cdot 7k + 12 + 28k \equiv 4 \pmod{7^2} \).
    * Rearranging yields \( 21k \equiv 14 \pmod{7^2} \).
    * Cancelling the factor of 7 yields \( 3k \equiv 2 \pmod{7} \), which has the single solution \( k \equiv 3 \pmod{7} \).
    * Hence we obtain \( x \equiv 24 \pmod{49} \).
  ○ Now we “lift” to find the solutions modulo \( 7^3 \): any solution must be of the form \( x = 24 + 49k \) for some \( k \).
    * Plugging in yields \((24 + 7^2k)^3 + 4(24 + 7^2k) \equiv 4 \pmod{7^3}\).
    * After expanding, reducing, and rearranging, we obtain the congruence \( 147k \equiv 147 \pmod{7^3} \).
    * Cancelling the factor of \( 7^2 \) yields \( 3k \equiv 3 \pmod{7} \), which has the single solution \( k \equiv 1 \pmod{7} \).
    * Hence we obtain \( x \equiv 73 \pmod{7^3} \).
  ○ Hence there is a unique solution: \( x \equiv 73 \pmod{7^3} \).

• **Example:** Solve the congruence \( x^3 + 4x \equiv 12 \pmod{7^3} \).
  ○ We first solve the congruence modulo 7.
    * By trying all the residue classes, we see that \( x^3 + 4x \equiv 5 \pmod{7} \) has two solutions, \( x \equiv 1 \pmod{7} \) and \( x \equiv 5 \pmod{7} \).
  ○ Next we try to “lift” to find the solutions modulo \( 7^2 \): any solution must be of the form \( x = 1 + 7k \) or \( x = 5 + 7k \) for some \( k \).
    * In the first case, plugging in yields \((1 + 7k)^3 + 4(1 + 7k) \equiv 12 \pmod{7^2}\), which, after expanding, is equivalent to \( 1 + 3 \cdot 7k + 4 + 28k \equiv 12 \pmod{7^2} \).
    * Rearranging yields \( 49k \equiv 7 \pmod{7^2} \), which is equivalent to \( 0 \equiv 7 \pmod{7^2} \). This has no solutions.
    * In the second case, plugging in yields \((5 + 7k)^3 + 4(5 + 7k) \equiv 12 \pmod{7^2}\), which, after expanding, is equivalent to \( 125 + 15 \cdot 7k + 20 + 28k \equiv 12 \pmod{7^2} \).
    * Rearranging yields \( 14k \equiv 14 \pmod{7^2} \).
    * Cancelling the factor of \( 7 \) yields \( 2k \equiv 2 \pmod{7} \), which has the single solution \( k \equiv 1 \pmod{7} \).
    * Hence we obtain \( x \equiv 12 \pmod{7^2} \).
  ○ Now we “lift” to find the solutions modulo \( 7^3 \): any solution must be of the form \( x = 12 + 49k \) for some \( k \).
    * Plugging in yields \((12 + 7^2k)^3 + 4(12 + 7^2k) \equiv 4 \pmod{7^3}\).
    * Expanding gives \( 12^3 + 3 \cdot 12 \cdot 7^2k + 4 \cdot 12 + 4 \cdot 7^2k \equiv 4 \pmod{7^3} \).
    * Some arithmetic and rearranging eventually gives the congruence \( 98k \equiv 294 \pmod{7^3} \).
    * Cancelling the factor of \( 7^2 \) yields \( 2k \equiv 3 \pmod{7} \), which has the single solution \( k \equiv 5 \pmod{7} \).
    * Hence we obtain \( x \equiv 257 \pmod{7^3} \).
  ○ Hence there is a unique solution: \( x \equiv 257 \pmod{7^3} \).

• In the examples above, two of the solutions modulo 7 lifted to a single solution modulo \( 7^2 \), which in turn lifted to a single solution modulo \( 7^3 \). However, one solution modulo 7 failed to yield any solutions modulo \( 7^2 \). We would like to know what causes the lifting process to fail.
  ○ To motivate our proof of the general answer, consider the polynomial \( q(x) = x^3 + 4x \) and suppose we have a solution \( x \equiv a \pmod{p} \) to \( q(x) \equiv c \pmod{p} \) that we would like to “lift” to a solution modulo \( p^2 \).
  ○ Then we substitute \( x = a + pk \) into the equation, and look for solutions to \( q(a + pk) \equiv 0 \pmod{p^2} \).
  ○ This is equal to \( (a + pk)^3 + 4(a + pk) \), which we can expand out using the binomial theorem to obtain \( a^3 + 3a^2pk + 4a + 4pk \pmod{p^2} \).
○ Rearranging this shows that we need to solve the equation \((a^3 + 4a) + (3a^2 + 4)pk \equiv c \pmod{p^2}\).

○ Since by hypothesis, \(a^3 + 4a \equiv c \pmod{p}\), we can rearrange the above congruence and then divide through by \(p\) to obtain the congruence \(\frac{a^3 + 4a - c}{p} + (3a^2 + 4)k \equiv 0 \pmod{p}\).

○ We see that this congruence will have a unique solution for \(k\) as long as \(3a^2 + 4 \not\equiv 0 \pmod{p}\).

○ We recognize the expression \(3a^2 + 4\) as the derivative \(q'(a)\). So the above computations suggest that we should expect that our ability to lift a solution \(x \equiv a \pmod{p}\) to a solution modulo \(p^d\) will depend on the value of the derivative \(q'(a)\). Indeed, this is precisely what happens in general:

- **Theorem** (Hensel’s Lemma): Suppose \(q(x)\) is a polynomial with integer coefficients. If \(q(a) \equiv 0 \pmod{p^d}\) and \(q'(a) \not\equiv 0 \pmod{p}\), then there is a unique \(k\) (modulo \(p\)) such that \(q(a + kp^d) \equiv 0 \pmod{p^{d+1}}\). Explicitly, if \(u\) is the inverse of \(q'(a)\) modulo \(p\), then \(k = -u \cdot \frac{q(a)}{p^d}\).

○ The idea of the proof is the same as in all of the examples we discussed above: to determine when we can lift to find a solution modulo \(p^{d+1}\), we substitute \(x = a + kp^d\) into the equation, and look for solutions \(k\) to the congruence \(q(a + kp^d) \equiv 0 \pmod{p^{d+1}}\). The only difficulty is expanding out \(q(a + kp^d)\) modulo \(p^{d+1}\).

○ **Proof:** Suppose \(x \equiv a \pmod{p^d}\) is a solution to the congruence \(q(x) \equiv 0 \pmod{p^d}\), where \(q(x)\) has degree \(r\). (By definition, note that this means \(\frac{q(a)}{p^d}\) is an integer.)

○ Set \(q(x) = \sum_{n=0}^{r} c_n x^n\), and observe that \(q'(x) = \sum_{n=0}^{r} c_n \cdot nx^{n-1}\).

  * First observe that by the binomial theorem, we have \((a + kp^d)^n = a^n + n \cdot p^d k \cdot a^{n-1} + p^{2d} \cdot \text{other terms}\).
  * But since all of the binomial coefficients are integers, the reduction modulo \(p^{d+1}\) of \((a + kp^d)^n\) is simply \(a^n + (n \cdot a^{n-1})p^d k\).

○ We then compute
  \[
  q(a + kp^d) \equiv \sum_{n=0}^{r} c_n (a + kp^d)^n \pmod{p^{d+1}}
  \equiv \sum_{n=0}^{r} c_n \left[a^n + (n \cdot a^{n-1})p^d k\right] \pmod{p^{d+1}}
  \equiv \sum_{n=0}^{r} c_n a^n + p^d k \sum_{n=0}^{r} c_n \cdot n a^{n-1} \pmod{p^{d+1}}
  = q(a) + p^d k \cdot q'(a) \pmod{p^{d+1}}.
  \]

○ Hence, solving \(q(a + kp^d) \equiv 0 \pmod{p^{d+1}}\) is equivalent to solving \(q(a) + p^d k \cdot q'(a) \equiv 0 \pmod{p^{d+1}}\).

○ Dividing through by \(p^d\) yields the equivalent congruence \(k \cdot q'(a) \equiv -\frac{q(a)}{p^d} \pmod{p}\).

○ This congruence has exactly one solution for \(k\), by the assumption that \(q'(a) \not\equiv 0 \pmod{p}\), and its value is as claimed.

○ Hence: the solution \(x \equiv a \pmod{p^d}\) lifts to a unique solution \(x \equiv a + p^d k \pmod{p^{d+1}}\), whose value is as claimed.

○ **Remark:** The presence of the derivative \(q'(a)\) is not accidental. Instead of using the binomial theorem, we could have instead written out the Taylor expansion of \(q(x + b)\):
  \[
  q(x + b) = q(x) + b q'(x) + b^2 q''(x) \frac{2}{2!} + b^3 q'''(x) \frac{3}{3!} + \cdots + b^r q^{(r)}(x) \frac{r}{r!} + \cdots.
  \]

Since the higher derivatives of \(q(x)\) are all zero, this is actually a finite sum. If we then set \(b = p^d k\), reducing modulo \(p^{d+1}\) eliminates everything except the first two terms. (This is not completely obvious because there are factorials in the denominators, but it can be shown that \(q^{(r)}(a)/r!\) is always an integer.)
Using the explicit description of the parameter $k$ from Hensel’s lemma, we see that as long as $q'(a) \neq 0 \pmod{p}$, any solution $x = a$ to $q(x) \equiv 0 \pmod{p}$ will lift to a unique solution $x \equiv a_j \pmod{p^j}$ for any $j$.

- This sequence of residues is explicitly given by $a_{j+1} = a_j - u \cdot q(a_j)$, where $u$ is the inverse of $q'(a)$ modulo $p$.
- Observe that this is precisely the same procedure as in Newton’s method for finding a sequence converging to a root of a differentiable function $f(x)$.

### 5.2 Quadratic Residues and the Legendre Symbol

- We now turn our attention to studying the zeroes of quadratic polynomials modulo $m$.
  - By the Chinese Remainder Theorem, this is equivalent to studying the zeroes of quadratic polynomials modulo prime powers.
  - Furthermore, Hensel’s lemma allows us (essentially) to reduce to the case of finding the zeroes of quadratic polynomials modulo $p$. In this case, since we are now working over a field, we have the added advantage of knowing that there will be at most 2 zeroes.
  - So let $f(x) = ax^2 + bx + c$, and consider the general quadratic congruence $f(x) \equiv 0 \pmod{p}$. If $p = 2$ then this congruence is easy to solve, so also assume $p$ is odd.
  - If $a \equiv 0 \pmod{p}$, then the congruence $f(x) \equiv 0 \pmod{p}$ reduces to a linear congruence. If $a \not\equiv 0 \pmod{p}$, then $a$ is invertible modulo $p$.
  - Now we can complete the square and write $4a f(x) = (2ax+b)^2 + (4ac-b^2)$; then the congruence $f(x) \equiv 0 \pmod{p}$ is equivalent to $(2ax+b)^2 \equiv (b^2-4ac) \pmod{p}$, since $4a$ is invertible modulo $p$.
  - Solving for $x$ then amounts to finding all solutions to $y^2 \equiv D \pmod{p}$, where $y = 2ax+b$ and $D = b^2-4ac$. In other words, aside from some minor issues that could arise in the application of Hensel’s lemma, solving a general quadratic equation is equivalent to computing square roots.

- An obvious first question is: how can we determine whether the congruence $y^2 \equiv D \pmod{p}$ has a solution at all?

**Definition:** If $a$ is a unit modulo $m$, we say $a$ is a quadratic residue modulo $m$ if there is some $b$ such that $b^2 \equiv a \pmod{m}$. If there is no such $b$, then we say $a$ is a quadratic nonresidue modulo $m$.

- It is a matter of taste whether to include nonunits in the definition of quadratic residues/nonresidues. For the moment, we will only consider units.

- It is straightforward to list the quadratic residues modulo $m$ by squaring all of the invertible residue classes.

  - **Example:** Modulo 5, the quadratic residues are 1 and 4, while the nonresidues are 2 and 3.
  - **Example:** Modulo 13, the quadratic residues are 1, 4, 9, 3, 12, and 10, while the nonresidues are 2, 5, 6, 7, 8, and 11.
  - **Example:** Modulo 21, the quadratic residues are 1, 4, and 16, while the nonresidues are 2, 5, 8, 10, 11, 13, 17, 19, and 20.
  - **Example:** Modulo 25, the quadratic residues are 1, 6, 11, 16, 21, 4, 9, 14, 19, and 24, while the nonresidues are 2, 7, 12, 17, 22, 3, 8, 13, 18, and 23.

- We note that if $m$ is composite, then (by the Chinese Remainder Theorem) $a$ is a quadratic residue modulo $m$ if and only if $a$ is a quadratic residue modulo each of the prime powers dividing $m$. Using Hensel’s lemma, we can reduce things further.

**Proposition:** If $p$ is an odd prime, then a unit $a$ is a quadratic residue modulo $p^d$ for $d \geq 1$ if and only if $a$ is a quadratic residue modulo $p$.

- **Proof:** Clearly, if there exists a $b$ such that $a \equiv b^2 \pmod{p^d}$ then $a \equiv b^2 \pmod{p}$, so the forward direction is trivial.
If we have (Euler’s criterion): If \( q(x) = x^2 - a \), we then want to apply Hensel’s lemma to lift the solution \( x \equiv b \) (mod \( p \)) of the congruence \( q(x) \equiv 0 \) (mod \( p \)) to a solution modulo \( p^4 \).

We can do this as long as \( q'(b) \neq 0 \) (mod \( p \)): but \( q'(b) = 2b \), and this is nonzero because \( b \neq 0 \) (mod \( p \)) and because \( p \) is odd.

- Thus, we are essentially reduced to considering quadratic residues modulo \( p \). A first observation is that exactly half of the invertible residue classes are quadratic residues:

- **Proposition:** If \( p \) is an odd prime, the quadratic residues modulo \( p \) are \( 1^2, 2^2, \ldots, \left( \frac{p-1}{2} \right)^2 \). Hence, half of the invertible residue classes modulo \( p \) are quadratic residues, and the other half are nonresidues.

  - **Proof:** If \( p \) is prime, then \( p|a^2 - b^2 \) implies \( p|(a-b) \) or \( p|(a+b) \); thus, \( a^2 \equiv b^2 \) (mod \( p \)) is equivalent to \( a \equiv \pm b \) (mod \( p \)).

  - We conclude that \( 1^2, 2^2, \ldots, \left( \frac{p-1}{2} \right)^2 \) are distinct modulo \( p \).

  - Furthermore, the other squares \( \left( \frac{p+1}{2} \right)^2, \ldots, (p-1)^2 \) are equivalent to these in reverse order, since \( k^2 \equiv (p-k)^2 \) (mod \( p \)).

- **Definition:** If \( p \) is an odd prime, the Legendre symbol \( \left( \frac{a}{p} \right) \) is defined to be 1 if \( a \) is a quadratic residue, -1 if \( a \) is a quadratic nonresidue, and 0 if \( p|a \).

  - The notation for the Legendre symbol is somewhat unfortunate, since it is the same as that for a standard fraction. When appropriate, we may write \( \left( \frac{a}{p} \right)_L \) to emphasize that we are referring to a Legendre symbol rather than a fraction.

  - **Example:** We have \( \left( \frac{2}{7} \right) = +1 \), \( \left( \frac{3}{7} \right) = -1 \), and \( \left( \frac{0}{7} \right) = 0 \), since 2 is a quadratic residue and 3 is a nonresidue modulo 7.

  - **Example:** We have \( \left( \frac{3}{13} \right) = \left( \frac{-3}{13} \right) = +1 \), and \( \left( \frac{2}{15} \right) = 1 \), since 3 and -3 are quadratic residues modulo 13, while 2 is not.

  - Note that the quadratic equation \( x^2 \equiv a \) (mod \( p \)) has exactly \( 1 + \left( \frac{a}{p} \right) \) solutions modulo \( p \).

- **Theorem** (Euler’s criterion): If \( p \) is an odd prime, then for any residue class \( a \), it is true that \( \left( \frac{a}{p} \right) = a^{(p-1)/2} \) (mod \( p \)).

  - We will start with a useful proposition, whose proof we present separately.

  - **Proposition:** If \( p \) is an odd prime and \( u \) is a primitive root modulo \( p \), then \( a \) is a quadratic residue if and only if \( \log_u(a) \) is even.

    - **Proof:** If \( \log_u(a) = 2k \) is even, then clearly \( a = u^{2k} = (u^k)^2 \) is a quadratic residue.

    - Conversely, suppose \( a \equiv b^2 \) (mod \( p \)). Then since \( u \) is a primitive root, we can write \( b = u^k \) for some \( k \): then \( a = u^{2k} \), so \( \log_u(a) \) is even.

  - **Proof** (of Theorem): If \( p|a \) then the result is trivial, so assume \( a \) is a unit modulo \( p \) and let \( u \) be a primitive root modulo \( p \).

  - First suppose \( a \) is a quadratic residue, so that \( \left( \frac{a}{p} \right) = +1 \).

    - Then by the proposition above, we know that \( a = u^{2k} \) for some integer \( k \).
* We compute \( a^{(p-1)/2} \equiv (u^{2k})^{(p-1)/2} = (u^{p-1})^{k} \equiv 1^{k} = 1 \pmod{p} \), which agrees with the value of \( \left( \frac{a}{p} \right) \).

○ Now suppose \( a \) is a quadratic nonresidue, so that \( \left( \frac{a}{p} \right) = -1 \).

* Then by the proposition above, we know \( a = u^{2k+1} \) for some integer \( k \).
* We compute \( a^{(p-1)/2} \equiv (u^{2k+1})^{(p-1)/2} = (u^{p-1})^{k} \cdot u^{(p-1)/2} \equiv u^{(p-1)/2} \).
* Now observe that \( x = u^{(p-1)/2} \) has the property that \( x^2 \equiv 1 \pmod{p} \).
* The two solutions to this quadratic are \( x \equiv \pm 1 \pmod{p} \), but \( x \not\equiv 1 \pmod{p} \) since otherwise \( u \) would not be a primitive root.
* Hence \( u^{(p-1)/2} \equiv -1 \pmod{p} \), meaning that \( a^{(p-1)/2} \equiv -1 \pmod{p} \) as well, and this agrees with the value of \( \left( \frac{a}{p} \right) \).

• Euler’s criterion provides us with a fairly efficient way to calculate Legendre symbols, since it is easy to find \( a^{(p-1)/2} \pmod{p} \) with successive squaring.

**Example:** Determine whether \( 5 \) is a quadratic residue or nonresidue modulo \( 29 \).

○ By Euler’s criterion, \( \left( \frac{5}{29} \right) = 5^{14} \pmod{29} \).

○ With successive squaring, we see that \( 5^2 \equiv -4, 5^4 \equiv -13, 5^8 \equiv -5, \) so \( 5^{14} \equiv (-4) \cdot (-13) \cdot (-5) \equiv 1 \pmod{29} \).

○ Thus, since the Legendre symbol is \( +1 \), we see that \( 5 \) is a quadratic residue mod \( 29 \).

• Euler’s criterion also yields an extremely useful corollary about the product of Legendre symbols:

**Corollary:** If \( p \) is a prime, then for any \( a \) and \( b \), \( \left( \frac{ab}{p} \right) = \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right) \).

○ In particular: the product of two quadratic residues is a quadratic residue, the product of a residue and nonresidue is a nonresidue, and (much more unexpectedly) the product of two nonresidues is a residue.

○ **Proof:** Simply use Euler’s criterion to write \( \left( \frac{ab}{p} \right) = (ab)^{(p-1)/2} = a^{(p-1)/2}b^{(p-1)/2} = \left( \frac{a}{p} \right) \cdot \left( \frac{b}{p} \right) \).

○ **Remark** (for those who like group theory): This corollary is saying that the Legendre symbol is a group homomorphism from the group \( \mathbb{Z}/p\mathbb{Z}^\times \) of units modulo \( p \) to the group \( \{\pm 1\} \). The preimage of \( +1 \) under this map is the coset of quadratic residues, while the preimage of \( -1 \) under this map is the coset of quadratic nonresidues.

### 5.3 Motivation for Quadratic Reciprocity

• Euler’s criterion provides us with a way to compute whether a residue class \( a \) modulo \( p \) is a quadratic residue or nonresidue.

• We will now examine the reverse question: given a particular value of \( a \), for which primes \( p \) is \( a \) a quadratic residue? For one value of \( a \), we can answer this question immediately:

**Proposition:** \(-1\) is a quadratic residue modulo \( p \) if and only if \( p = 2 \) or \( p \equiv 1 \pmod{4} \).

○ **Proof:** Clearly \(-1\) is a quadratic residue mod \( 2 \). If \( p \) is odd, apply Euler’s criterion to write \( \left( \frac{-1}{p} \right) = (-1)^{(p-1)/2} \), and notice that this is \( +1 \) when \( (p-1)/2 \) is even and \(-1\) when \( (p-1)/2 \) is odd.

• For most \( a \), however, the answer is far from obvious. Let us examine a few particular values of \( a \), modulo primes less than 50, to see whether there are any patterns. (We can do the computations with Euler’s criterion, or by making a list of all the squares modulo \( p \).)
Consider \( a = 2 \). Some short calculations show that \( a \) is a quadratic residue modulo 7, 17, 23, 31, 41, and 47, while \( a \) is a nonresidue modulo 3, 5, 11, 13, 19, 29, 37, and 43.

Consider \( a = 3 \). Some short calculations show that \( a \) is a quadratic residue modulo 11, 13, 23, 37, and 47, while \( a \) is a nonresidue modulo 5, 7, 17, 19, 29, 31, 41, and 43.

Consider \( a = 5 \). Some short calculations show that \( a \) is a quadratic residue modulo 11, 19, 29, 31, and 41, while \( a \) is a nonresidue modulo 3, 7, 13, 17, 23, 37, 43, and 47.

Consider \( a = 7 \). Some short calculations show that \( a \) is a quadratic residue modulo 3, 17, 23, and 29, while \( a \) is a nonresidue modulo 5, 7, 11, 13, 19, 31, 37, 41, and 43.

Consider \( a = 13 \). Some short calculations show that \( a \) is a quadratic residue modulo 3, 17, 23, and 29, while \( a \) is a nonresidue modulo 5, 11, 13, 17, 23, and 41.

- We can see a few patterns in these results.
  
  For \( a = 5 \) there is an obvious pattern: the primes where 5 is a quadratic residue all end in 1 or 9, while the primes where 5 is a nonresidue all end in 3 or 7.

  We see that the primes where 5 is a quadratic residue are 1 or 4 modulo 5, while the primes where 5 is a nonresidue are 2 or 3 modulo 5. We also notice the rather suspicious fact that 1 and 4 are the quadratic residues modulo 5, while 2 and 3 are the nonresidues.

  This suggests searching for a similar pattern with a small modulus in the other examples. Doing this eventually uncovers the fact that all of the primes where 2 is a quadratic residue are either 1 or 7 modulo 8, while the primes where 2 is a nonresidue are all 3 or 5 modulo 8.

  Similarly, we can see that all of the primes where 3 is a quadratic residue are either 1 or 11 modulo 12, while the primes where 3 is a nonresidue are all 5 or 7 modulo 12. However, there is nothing obvious about how these residues are related, unlike in the case \( a = 5 \).

  A similar pattern does not seem to be as forthcoming for when 7 is a quadratic residue.

  We can see that the primes where 13 is a quadratic residue are 3, 4, or 10 modulo 13, and the primes where 13 is a nonresidue are 2, 5, 6, 7, 8, or 11 modulo 13. Notice that 3, 4, and 10 are all quadratic residues modulo 13, while 2, 5, 6, 7, 8, and 11 are nonresidues.

  It seems that we have found natural patterns for \( a = 5 \) and \( a = 13 \): for these two primes, it appears that \( \left( \frac{5}{p} \right) = 1 \) if and only if \( \left( \frac{p}{5} \right) = 1 \), and similarly for 13.

  However, we have not found such a “reciprocity” relation for \( a = 3 \) and \( a = 7 \).

- Let us try looking at negative integers, to see if results are more obvious there:

  For \( a = -3 \), some short calculations show that \( a \) is a quadratic residue modulo 7, 13, 19, 31, and 37, while \( a \) is a nonresidue modulo 5, 11, 17, 23, 29, 41, and 47. This shows a much more natural pattern: the primes with \( \left( \frac{a}{p} \right) = 1 \) are all 1 modulo 3, while the values where \( \left( \frac{a}{p} \right) = -1 \) are all 2 modulo 3.

  Notice that 1 is a quadratic residue modulo 3, and 2 is a nonresidue.

  For \( a = -7 \), some short calculations show that \( a \) is a quadratic residue modulo 11, 23, 29, and 37, while \( a \) is a nonresidue modulo 3, 5, 13, 17, 19, 31, 41, and 47. Again, we see a pattern: the primes where \( \left( \frac{a}{p} \right) = 1 \) are all 1, 2, or 4 modulo 7, while the values where \( \left( \frac{a}{p} \right) = -1 \) are all 3, 5, or 6 modulo 7.

  Notice that the quadratic residues modulo 7 are 1, 2, and 4, while the nonresidues are 3, 5, and 6.

  Based on this evidence, it seems that \( \left( \frac{-3}{p} \right) = 1 \) if and only if \( \left( \frac{p}{3} \right) = 1 \), and similarly \( \left( \frac{-7}{p} \right) = 1 \) if and only if \( \left( \frac{p}{7} \right) = 1 \).

- We notice that the “reciprocity” relation appears to be different for the primes 5 and 13 versus the primes 3 and 7.

  Based on our previous ideas of looking for simple congruence relations, we observe that 3 and 7 are both 3 modulo 4, while 5 and 13 are both 1 modulo 4.
• If \( p \equiv 1 \pmod{4} \), it appears that \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = 1 \), if \( q \neq p \) is any odd prime. Note that this is symmetric in \( p \) and \( q \), so this should actually hold if \( p \) or \( q \) is 1 modulo 4.

• If \( p, q \equiv 3 \pmod{4} \), it appears that \( \left( -\frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = 1 \), if \( q \neq p \) is any odd prime. Since \( \left( -\frac{p}{q} \right) = \left( -\frac{1}{q} \right) \cdot \left( \frac{p}{q} \right) \), and we know that \( \left( -\frac{1}{q} \right) = -1 \) from earlier, we can rewrite this relation as \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = -1 \).

• Thus: it appears that \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = 1 \) if \( p \) or \( q \) is 1 mod 4, and is \(-1\) if both \( p \) and \( q \) are 3 mod 4.

• This result is called “the law of quadratic reciprocity”.

• It was stated (without proof) by Euler in 1783, and the first correct proof was given by Gauss in 1796.

• This theorem was one of Gauss’s favorites: given Gauss’s prodigious mathematical output, this is a very strong statement! (He actually published six different proofs during his lifetime, and two more were found among his notes. There are now over 200 different proofs that have been collected.)

### 5.4 Proof of Quadratic Reciprocity

• The proof of quadratic reciprocity we will give is due to Eisenstein, and is a simplification of one of Gauss’s original proofs. The first ingredient is the following lemma:

• **Lemma** (Gauss’s Lemma): If \( p \) is an odd prime and \( p \nmid a \), then \( \left( \frac{a}{p} \right) = (-1)^k \), where \( k \) is equal to the number of integers among \( a, 2a, \ldots, \frac{p-1}{2} - a \) whose least positive residue modulo \( p \) is bigger than \( \frac{p}{2} \).

  • **Proof:** Let \( r_1, \ldots, r_k \) be the residues bigger than \( \frac{p}{2} \) and \( s_1, \ldots, s_l \) be the other residues, where \( k + l = \frac{p-1}{2} \).

  • Observe that \( 0 < p - r_i < p/2 \), and that each of these is distinct. Furthermore, these values \( p - r_i \) are all distinct from the \( s_j \):

    * If \( p - r_i = s_j \), then if \( r_i \equiv c_1 a \pmod{p} \) and \( s_j \equiv c_2 a \pmod{p} \), then we would have \( a(c_1 + c_2) = 0 \pmod{p} \).

    * So since \( a \) is a unit, this implies \( c_1 + c_2 = 0 \pmod{p} \). But this cannot happen, because \( c_1 \) and \( c_2 \) are both between 1 and \( \frac{p-1}{2} \).

  • Therefore, the \( \frac{p-1}{2} \) values among the \( p - r_i \) and \( s_j \) are all distinct and between 1 and \( p/2 \). Thus, they must simply be 1, 2, \ldots, \( \frac{p-1}{2} \) in some order.

  • Thus, we may write

\[
1 \cdot 2 \cdots \frac{p-1}{2} \equiv \prod_{i=1}^{k} (p - r_i) \cdot \prod_{j=1}^{l} s_j \pmod{p}
\]

\[
\equiv (-1)^k \prod_{i=1}^{k} r_i \cdot \prod_{j=1}^{l} s_j \pmod{p}
\]

\[
\equiv (-1)^k \prod_{n=1}^{(p-1)/2} (na) \pmod{p}
\]

\[
\equiv (-1)^k a^{(p-1)/2} \cdot 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p}
\]

and then cancelling the common \( \frac{p-1}{2} \) from both sides yields \( \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \equiv (-1)^k \pmod{p} \), as claimed.
We can use Gauss’s lemma to compute the Legendre symbol \( \left( \frac{a}{p} \right) \) for small values of \( a \).

**Corollary:** If \( p \) is an odd prime, \( \left( \frac{2}{p} \right) = (-1)^{\frac{3p^2-1}{8}} \). Equivalently, \( \left( \frac{2}{p} \right) = 1 \) if \( p \equiv 1, 7 \pmod{8} \), and \( \left( \frac{2}{p} \right) = -1 \) if \( p \equiv 3, 5 \pmod{8} \).

○ **Proof:** By Gauss’s lemma, we need only compute whether the number of residues among 2, 4, ... , \( p-3, \) \( p-1 \) that lie between \( p/2 \) and \( p \) is even or odd. (Conveniently, they already all lie between 0 and \( p \).)

○ If \( p \equiv 1 \pmod{4} \), the smallest such residue is \( (p+3)/2 \) and the largest is \( p-1 \), so the number is \( (p-5)/4 \). This is odd if \( p \equiv 5 \pmod{8} \) and even if \( p \equiv 1 \pmod{8} \).

○ If \( p \equiv 3 \pmod{4} \), the smallest such residue is \( (p+1)/2 \) and the largest is \( p-1 \), so the number is \( (p-3)/4 \). This is odd if \( p \equiv 3 \pmod{8} \) and even if \( p \equiv 7 \pmod{8} \).

We could make a similar analysis to compute \( \left( \frac{3}{p} \right) \), \( \left( \frac{5}{p} \right) \), and so forth. The only obstacle is the rather involved roundoff analysis required to make an accurate accounting of how many residue classes reduce to lie in the interval \( [p/2, p] \). Rather than doing this case-by-case, we will instead write down a formula for the general result:

**Lemma** (Eisenstein’s Lemma): If \( p \) is an odd prime and \( a \) is odd with \( p \nmid a \), then \( \left( \frac{a}{p} \right) = (-1)^s \) where

\[
s = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor.
\]

○ **Remark:** The notation \( \lfloor x \rfloor \) denotes the greatest integer function, defined as the largest integer \( n \) with \( n \leq x \). (In fact, this function was first introduced by Gauss in the course of one of his proofs of quadratic reciprocity!)

○ **Proof:** By Gauss’s lemma, \( \left( \frac{a}{p} \right) = (-1)^k \) where \( k \) is equal to the number of the residues \( a, 2a, \ldots, \frac{p-1}{2}a \) whose least positive residue modulo \( p \) is bigger than \( \frac{p}{2} \).

○ Thus, all we need to do is show that \( \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor \) is equivalent to \( k \pmod{2} \).

○ As in our earlier proof, we let \( r_1, \ldots, r_k \) be the residues bigger than \( \frac{p}{2} \) and \( s_1, \ldots, s_l \) be the other residues, where \( k+l=\frac{p-1}{2} \), and we note that the elements \( p-r_i \) and \( s_j \) are a rearrangement of 1, 2, \ldots, \( \frac{p-1}{2} \).

○ Thus, we have \( kp - \sum_{i=1}^{k} r_j + \sum_{j=1}^{l} s_j = \sum_{i=1}^{k} (p-r_j) + \sum_{j=1}^{l} s_j = \sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8} \).

○ Also, observe that the \( r_i \) and \( s_j \) are the remainders obtained when we divide \( ja \) by \( p \), for \( 1 \leq j \leq \frac{p-1}{2} \). The quotient when we do the division is clearly \( \lfloor ja/p \rfloor \).

○ Thus, we also have \( p \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{k} r_j + \sum_{j=1}^{l} s_j = \sum_{j=1}^{(p-1)/2} ja = \frac{p^2-1}{8} \).

○ Subtracting the first sum from the second sum yields \( p \left( \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{ja}{p} \right\rfloor - k \right) + 2\sum_{i=1}^{k} r_j = (a-1)\frac{p^2-1}{8} \).
Since we only care about \( k \) modulo 2, we can reduce everything mod 2: since \( \frac{p^2 - 1}{8} \) is an integer and \( a - 1 \) and \( 2 \sum_{i=1}^{k} r_j \) is even, while \( p \) is odd, we obtain \( \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{j a}{p} \right\rfloor \equiv k \pmod{2} \), as desired.

The above computation gives a seemingly useless expression for the Legendre symbol in terms of a sum involving the floor function, but it turns out that we can use it to prove quadratic reciprocity almost immediately:

**Theorem (Quadratic Reciprocity):** If \( p \) and \( q \) are distinct odd primes, then \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^{\frac{(p-1)(q-1)}{4}} \).

Equivalently, \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = 1 \) if \( p \) or \( q \) is 1 (mod 4), and \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = -1 \) if \( p \) and \( q \) are both 3 (mod 4).

**Proof:** By Eisenstein’s lemma, \( \left( \frac{p}{q} \right) \cdot \left( \frac{q}{p} \right) = (-1)^n \), where \( n = \sum_{j=1}^{(p-1)/2} \left\lfloor \frac{j q}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{k p}{q} \right\rfloor \).

The first sum is the number of lattice points \((x, y)\) lying below the line \( y = \frac{q}{p} x \), with \( 1 \leq x \leq \frac{p-1}{2} \). The following figure illustrates this in the case \( p = 13, q = 11 \):

![Figure 1: The lattice points underneath \( y = \frac{q}{p} x \) with \( 1 \leq x \leq \frac{p-1}{2} \).](image)

The second sum can be interpreted in a similar way as the number of lattice points below the line \( y = \frac{p}{q} x \).

More fruitfully, we can view it as the number of lattice points \((x, y)\) lying to the left of the line \( y = \frac{q}{p} x \), with \( 1 \leq y \leq \frac{q-1}{2} \). The following figure illustrates this in the case \( p = 13, q = 11 \):
Figure 2: The lattice points to the left of \( y = \frac{q}{p}x \) with \( 1 \leq y \leq \frac{q-1}{2} \).

- As suggested by the picture, the union of these two sets of points yields all of the lattice points in the rectangle bounded by \( 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2} \). Clearly, there are \( \frac{p-1}{2} \cdot \frac{q-1}{2} \) such lattice points.
- Note that there are no lattice points lying on the line \( y = \frac{q}{p}x \) inside this rectangle: since \( p \) and \( q \) are prime, any lattice point \( (x, y) \) lying on \( py = qx \) must have \( q|y \) and \( p|x \), and this is not possible if \( 1 \leq x \leq \frac{p-1}{2} \).
- Hence, we conclude that

\[
\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kq}{p} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},
\]

yielding the result.

5.5 Applications of Quadratic Reciprocity

- In this section, we discuss several ways we can use quadratic reciprocity.

5.5.1 Computing Legendre Symbols

- The most immediate application of quadratic reciprocity is to give another method for computing Legendre symbols.
- **Example:** Determine whether 31 is a quadratic residue modulo 47.
  - We want to find \( \left( \frac{31}{47} \right) \).
  - By quadratic reciprocity, since both 47 and 31 are primes congruent to 3 (mod 4), we have \( \left( \frac{31}{47} \right) = -\left( \frac{47}{31} \right) = -\left( \frac{16}{31} \right) = -1 \), since 16 is clearly a quadratic residue.
  - Thus, 31 is not a quadratic residue modulo 47.
- **Example:** Determine whether 357 is a quadratic residue modulo 661.
  - Since 357 = 3 \cdot 7 \cdot 17, we want to find \( \left( \frac{357}{661} \right) = \left( \frac{3}{661} \right) \cdot \left( \frac{7}{661} \right) \cdot \left( \frac{17}{661} \right) \).
By quadratic reciprocity, since 661 is a prime congruent to 1 (mod 4), we then have
\[
\left( \frac{3}{661} \right) = \left( \frac{661}{3} \right) = \left( \frac{1}{3} \right) = +1
\]
\[
\left( \frac{7}{661} \right) = \left( \frac{661}{7} \right) = \left( \frac{3}{7} \right) = -\left( \frac{7}{3} \right) = -\left( \frac{1}{3} \right) = -1
\]
\[
\left( \frac{17}{661} \right) = \left( \frac{661}{17} \right) = -\left( \frac{2}{17} \right) = -\left( \frac{1}{17} \right) \cdot \left( \frac{2}{17} \right) = (+1) \cdot (+1) = +1
\]
Thus, \(\left( \frac{357}{661} \right) = -1\), so 357 is not a quadratic residue modulo 661.

One drawback of using quadratic reciprocity in this way is that we need to factor the top number every time we “flip and reduce”, since quadratic reciprocity only makes sense when both terms are primes. (We also need to remove factors of 2 and \(-1\), although this is much more trivial.)

We will fix this problem when we define the Jacobi symbol.

5.5.2 For Which \(p\) is \(a\) a Quadratic Residue Modulo \(p\)?

Another application is determining, given a particular value of \(a\), for which primes \(p\) is \(a\) a quadratic residue.

**Example:** Characterize the primes for which \(3\) is a quadratic residue.

We want to compute \(\left( \frac{3}{p} \right)\), for \(p \neq 3\).

By quadratic reciprocity, we know that if \(p \equiv 1 \pmod{4}\), then \(\left( \frac{3}{p} \right) = \left( \frac{p}{3} \right)\).

Note that \(\left( \frac{p}{3} \right)\) is +1 if \(p \equiv 1 \pmod{3}\), and -1 if \(p \equiv 2 \pmod{3}\).

Therefore, in this case, we see that \(\left( \frac{3}{p} \right) = +1\) only when \(p \equiv 1 \pmod{4}\) and \(p \equiv 1 \pmod{3}\) - i.e., when \(p \equiv 1 \pmod{12}\).

Also, if \(p \equiv 3 \pmod{4}\), then \(\left( \frac{3}{p} \right) = -\left( \frac{p}{3} \right)\).

As above, \(\left( \frac{p}{3} \right)\) is +1 if \(p \equiv 1 \pmod{3}\), and -1 if \(p \equiv 2 \pmod{3}\).

Therefore, in this case, we see that \(\left( \frac{3}{p} \right) = +1\) only when \(p \equiv 3 \pmod{4}\) and \(p \equiv 2 \pmod{3}\) - i.e., when \(p \equiv 11 \pmod{12}\).

We conclude that 3 is a quadratic residue modulo \(p\) precisely when \(p \equiv 1\) or 11 (mod 12).

**Example:** Characterize the primes for which \(6\) is a quadratic residue.

We want to compute \(\left( \frac{6}{p} \right) = \left( \frac{2}{p} \right) \cdot \left( \frac{3}{p} \right)\), for \(p \neq 2, 3\).

From the above computations, we know that \(\left( \frac{3}{p} \right)\) = +1 when \(p \equiv 1\) or 11 (mod 12), and \(\left( \frac{3}{p} \right)\) = -1 when \(p \equiv 5\) or 7 (mod 12).

We also know that \(\left( \frac{2}{p} \right)\) = +1 when \(p \equiv 1\) or 7 (mod 8), and \(\left( \frac{2}{p} \right)\) = -1 when \(p \equiv 3\) or 5 (mod 8).

Thus, \(\left( \frac{6}{p} \right)\) = +1 in the following cases:
\[ \left( \frac{3}{p} \right) = \left( \frac{2}{p} \right) = +1: \text{ then } p \equiv 1, 11 \pmod{12} \text{ and } p \equiv 1, 7 \pmod{8}. \text{ Solving these modulo 24 yields } p \equiv 1, 23 \pmod{24}. \]
\[ \left( \frac{3}{p} \right) = \left( \frac{2}{p} \right) = -1: \text{ then } p \equiv 5, 7 \pmod{12} \text{ and } p \equiv 3, 5 \pmod{8}. \text{ Solving these modulo 24 yields } p \equiv 5, 19 \pmod{24}. \]

- Therefore, 6 is a quadratic residue modulo \( p \) precisely when \( p \equiv 1, 5, 19, 23 \pmod{24} \).

### 5.5.3 Primes Dividing Values of a Quadratic Polynomial

- Another more surprising result of quadratic reciprocity is that we can characterize the primes dividing the values taken by a quadratic polynomial.
  - This should be unexpected, because polynomials can combine addition and multiplication in arbitrary ways.
  - There is no especially compelling reason, a priori, to think that the primes dividing the values of, say, the polynomial \( q(x) = x^2 + x + 7 \), should have any identifiable structure at all: for all we know, the set of primes dividing an integer of the form \( n^2 + n + 7 \) could be totally arbitrary.

- **Example:** Characterize the primes dividing an integer of the form \( n^2 + n + 7 \), for \( n \) an integer.
  - It is not hard to see that \( n^2 + n + 7 \) is always odd, so 2 is never a divisor.
  - Now suppose that \( p \) is an odd prime and that \( n^2 + n + 7 \equiv 0 \pmod{p} \).
  - We multiply by 4 and complete the square to obtain \((2n + 1)^2 \equiv -27 \pmod{p}\).
  - Since \( p \) is odd, there will be a solution for \( n \) if and only if \(-27\) is a square modulo \( p \). If \( p = 3 \), this clearly holds, so now assume \( p \geq 5 \).
  - We compute \( \left( \frac{-27}{p} \right) = \left( \frac{-1}{p} \right) \cdot \left( \frac{3}{p} \right)^3 = \left( \frac{-1}{p} \right) \cdot \left( \frac{3}{p} \right) \).
  - From earlier, we know that \( \left( \frac{-1}{p} \right) \) is +1 if \( p \equiv 1 \pmod{4} \) and is -1 if \( p \equiv 3 \pmod{4} \).
  - We also showed that \( \left( \frac{3}{p} \right) = +1 \) when \( p \equiv 1 \) or 11 \pmod{12} \), and \( \left( \frac{3}{p} \right) = -1 \) when \( p \equiv 5 \) or 7 \pmod{12} \).
  - Hence, \( \left( \frac{-3}{p} \right) = +1 \) precisely when \( p \equiv 1 \pmod{6} \).
  - Thus, by the above, we conclude that a prime \( p \) divides an integer of the form \( n^2 + n + 7 \) either when \( p = 3 \) or when \( p \equiv 1 \pmod{6} \).

- **Proposition:** There are infinitely many primes congruent to 1 modulo 6.
  - **Proof:** By the argument above, any prime divisor (other than 3) of an integer of the form \( n^2 + n + 7 \) must be congruent to 1 modulo 6. Let \( q(x) = x^2 + x + 7 \).
  - We construct primes congruent to 1 modulo 6 using this polynomial: let \( p_0 = 3 \), and take \( p_1, \ldots, p_k \) to be arbitrary primes congruent to 1 modulo 6, none of which is equal to 7.
  - Now consider \( q(p_0p_1 \cdots p_k) \), which is clearly an integer greater than 1: it is relatively prime to each of the \( p_i \) for \( 0 \leq i \leq k \), because none of the \( p_i \) divides the constant term 7.
  - Hence, by the above result, any prime divisor of \( q(p_0p_1 \cdots p_k) \) must be a prime congruent to 1 modulo 6 that was not on our list.
  - Thus, there are infinitely many primes congruent to 1 modulo 6.

- **Remark:** It is a (not easy) Theorem of Dirichlet that if \( a \) and \( m \) are relatively prime, there exist infinitely many primes congruent to \( a \) modulo \( m \). The above result is a special case.
5.6 The Jacobi Symbol

- We would like to generalize the definition of the Legendre symbol to composite moduli.
- **Definition:** Let \( b \) be a positive odd integer with prime factorization \( b = p_1 p_2 \cdots p_k \) for some (not necessarily distinct) primes \( p_k \). The Jacobi symbol \( \left( \frac{a}{b} \right) \) is defined as \( \left( \frac{a}{b} \right) = \prod_{j=1}^{k} \left( \frac{a}{p_j} \right) \), where \( \left( \frac{a}{p_j} \right) \) denotes the Legendre symbol.

  - **Example:** \( \left( \frac{2}{15} \right) = \left( \frac{2}{3} \right) \cdot \left( \frac{2}{5} \right) = (-1) \cdot (-1) = +1. \)
  - **Example:** \( \left( \frac{11}{45} \right) = \left( \frac{11}{3} \right)^2 \cdot \left( \frac{11}{5} \right) = (-1)^2 \cdot (-1) = -1. \)
  - **Example:** \( \left( \frac{77}{33} \right) = \left( \frac{77}{3} \right) \cdot \left( \frac{77}{11} \right) = (-1) \cdot 0 = 0. \)

  - Observe that, by properties of the Legendre symbol, that \( \left( \frac{a}{b} \right) \) will always be +1, −1, or 0, and it will be 0 if and only if \( \gcd(a,b) > 1 \).

- The Jacobi symbol shares a number of properties with the Legendre symbol, the most important of which is that it is multiplicative on both the top and bottom: for any \( a, a' \) and any odd positive \( b, b' \), \( \left( \frac{aa'}{b} \right) = \left( \frac{a}{b} \right) \cdot \left( \frac{a'}{b'} \right) \) and \( \left( \frac{a}{bb'} \right) = \left( \frac{a}{b} \right) \cdot \left( \frac{a}{b'} \right) \).

  - This follows immediately from the definition and the fact that the Legendre symbol is multiplicative on the top.

- The Jacobi symbol can also detect squares: if \( a \) is a quadratic residue modulo \( b \) (and \( \gcd(a,b) = 1 \)), then \( \left( \frac{a}{b} \right) = +1. \)

  - This follows by observing that if \( a \equiv r^2 \ (\text{mod} \ b) \), then \( \left( \frac{a}{b} \right) = \left( \frac{r^2}{b} \right) = \left( \frac{r}{b} \right)^2 = +1. \)

- However, the converse is no longer true: it is not (!) the case that \( \left( \frac{a}{b} \right) = 1 \) implies that \( a \) is a quadratic residue modulo \( b \).

  - For example, \( \left( \frac{2}{15} \right) = +1 \) as computed above, but 2 is not a quadratic residue modulo 15.
  - Indeed, as we showed earlier, if \( b = p_1 p_2 \cdots p_k \), then \( a \) is a quadratic residue modulo \( b \) if and only if \( a \) is a quadratic residue modulo each \( p_i \).
  - We will note, though, that if \( b \) is an odd prime, then the Jacobi symbol and Legendre symbol are the same, and have the same value, and so in this case, \( \left( \frac{a}{b} \right) = +1 \) is equivalent to saying that \( a \) is a quadratic residue modulo \( b \).

- We might ask: why not instead define the Jacobi symbol \( \left( \frac{a}{b} \right) \) to be +1 if \( a \) is a quadratic residue and −1 if \( a \) is a nonresidue?

  - The reason we do not take this as the definition is that this new symbol is not multiplicative: with a composite modulus, the product of two nonresidues can still be a nonresidue.
  - For example, the quadratic residues modulo 15 are 1 and 4, while the nonresidues are 2, 7, 8, 11, 13, 14. Now observe that \( 2 \cdot 7 = 14 \ (\text{mod} \ 15) \), but all three of 2, 7, and 14 are quadratic nonresidues.
  - Ultimately, the problem is that a composite modulus has are “different kinds” of quadratic nonresidues.
To illustrate, an element \( a \) can be a nonresidue modulo 15 in three ways: (i) it could be a nonresidue mod 3 and a residue mod 5 [namely, \( a = 11, 14 \)], (ii) a residue mod 3 and a nonresidue mod 5 [namely, \( a = 7, 13 \)], or (iii) a nonresidue mod 3 and a nonresidue mod 5 [namely, \( a = 2, 8 \)].

The product of two nonresidues each in the same class above will be a quadratic residue modulo 15 (since it will be a residue mod 3 and mod 5), but the product of nonresidues from different classes will still be a nonresidue mod 15 (since it will be a nonresidue modulo 3 or modulo 5).

- The Jacobi symbol also obeys the law of quadratic reciprocity. We first collect a few basic evaluations:

**Proposition:** If \( b \) is odd and positive, \( \left( \frac{-1}{b} \right) = (-1)^{(b-1)/2} \) and \( \left( \frac{2}{b} \right) = (-1)^{(b^2-1)/8} \).

These statements are equivalent to the following: \( \left( \frac{-1}{b} \right) \) is +1 if \( b \equiv 1 \pmod{4} \) and is \( -1 \) if \( b \equiv 3 \pmod{4} \), and \( \left( \frac{2}{b} \right) \) is +1 if \( b \equiv 1, 7 \pmod{8} \) and is \( -1 \) if \( b \equiv 3, 5 \pmod{8} \).

**Proof:** Let \( b = p_1 p_2 \cdots p_k \) be a product of primes.

For the first statement, we know that \( \left( \frac{-1}{p_k} \right) = (-1)^{(p_k-1)/2} \).

* Then, by definition, \( \left( \frac{-1}{b} \right) = \prod_{j=1}^{k} \left( \frac{-1}{p_k} \right) = \prod_{j=1}^{k} (-1)^{(p_k-1)/2} = (-1)^{\sum (p_k-1)/2} \).

* Now we just need to verify that \( \sum_{j=1}^{k} \frac{p_k - 1}{2} = \prod_{j=1}^{k} \frac{p_k - 1}{2} \pmod{2} \).

* This follows from the observation that if \( m \) and \( n \) are any odd numbers, that \( m n - 1 = \frac{m - 1}{2} + \frac{n - 1}{2} \) is even.

* Thus, \( \frac{m n - 1}{2} \equiv \frac{m - 1}{2} + \frac{n - 1}{2} \pmod{2} \). Applying this repeatedly shows \( \sum_{j=1}^{k} \frac{p_k - 1}{2} \equiv \prod_{j=1}^{k} \frac{p_k - 1}{2} \pmod{2} \).

For the other statement, we know \( \left( \frac{2}{p_k} \right) = (-1)^{(p_k^2-1)/8} \).

* Like above, \( \left( \frac{2}{b} \right) = \prod_{j=1}^{k} \left( \frac{2}{p_k} \right) = \prod_{j=1}^{k} (-1)^{(p_k^2-1)/8} = (-1)\sum (p_k^2-1)/8 \).

* Now we just need to verify that \( \sum_{j=1}^{k} \frac{p_k^2 - 1}{8} = \prod_{j=1}^{k} \frac{p_k^2 - 1}{8} \pmod{2} \).

* This follows from the observation that if \( m \) and \( n \) are any odd numbers, that \( \frac{m^2 n^2 - 1}{8} - \frac{m^2 - 1}{8} - \frac{n^2 - 1}{8} = (m^2 - 1)(n^2 - 1)/8 \) is even.

* Thus, \( \frac{m^2 n^2 - 1}{8} \equiv \frac{m^2 - 1}{8} + \frac{n^2 - 1}{8} \pmod{2} \). Applying this repeatedly shows \( \sum_{j=1}^{k} \frac{p_k^2 - 1}{8} \equiv \prod_{j=1}^{k} \frac{p_k^2 - 1}{8} \pmod{2} \).

Now we prove quadratic reciprocity for the Jacobi symbol.

**Theorem:** If \( a \) and \( b \) are odd, relatively prime positive integers, then \( \left( \frac{a}{b} \right) \cdot \left( \frac{b}{a} \right) = (-1)^{(a - 1)(b - 1)/4} \).
○ The proof is essentially bookkeeping: we simply factor $a$ and $b$ and then use quadratic reciprocity on all of the prime factors. All of the actual work has already been done in proving quadratic reciprocity for the Legendre symbol.

○ Proof: Write $a = q_1 \cdots q_l$ and $b = p_1 \cdots p_k$ as products of primes.

○ Then, by definition, we have

$$ \left( \frac{a}{b} \right) = \prod_{j=1}^{k} \left( \frac{a}{p_j} \right) $$

$$ = \prod_{j=1}^{k} \prod_{i=1}^{l} \left( \frac{q_i}{p_j} \right) $$

$$ = \prod_{j=1}^{l} \prod_{i=1}^{k} \left( \frac{p_j}{q_i} \right) \cdot (-1)^{(p_j-1)(q_i-1)/4} $$

$$ = \prod_{i=1}^{k} \prod_{j=1}^{l} \left( \frac{p_j}{q_i} \right) \cdot (-1)^{\sum_{i,j}(p_j-1)(q_i-1)/4} $$

$$ = \left( \frac{b}{a} \right) \cdot (-1)^{\sum_{i,j}(p_j-1)(q_i-1)/4}. $$

○ But now observe that

$$ \sum_{i=1}^{l} \sum_{j=1}^{k} \frac{(p_i - 1)(q_j - 1)}{4} = \left( \sum_{i=1}^{l} \frac{p_i - 1}{2} \right) \cdot \left( \sum_{j=1}^{k} \frac{q_j - 1}{2} \right) $$

$$ \equiv \frac{a - 1}{2} \cdot \frac{b - 1}{2} \pmod{2} $$

using the same argument as in the previous proposition.

○ Therefore, $\left( \frac{a}{b} \right) = \left( \frac{b}{a} \right) \cdot (-1)^{(a-1)(b-1)/4}$, which is equivalent to the desired result.

• We can use the Jacobi symbol to compute Legendre symbols using the “flip and invert” technique discussed earlier. The advantage of the Jacobi symbol is that we no longer need to factor the top number: we only need to remove factors of $-1$ and $2$.

• Example: Determine whether 247 is a quadratic residue modulo the prime 1009.

○ We have \( \left( \frac{247}{1009} \right) = \left( \frac{1009}{247} \right) = \left( \frac{21}{247} \right) = - \left( \frac{247}{21} \right) = - \left( \frac{16}{21} \right) = -1 \), where at each stage we either used quadratic reciprocity (to “flip”) or reduced the top number modulo the bottom.

○ Since the result is $-1$, this says the Jacobi symbol $\left( \frac{247}{1009} \right)$ is $-1$, so 247 is a quadratic nonresidue modulo 1009.

• Example: Determine whether 1593 is a quadratic residue modulo the prime 2017.

○ We have

$$ \left( \frac{1593}{2017} \right) = \left( \frac{2017}{1593} \right) = \left( \frac{424}{1593} \right) $$

$$ = \left( \frac{2}{1593} \right)^3 \cdot \left( \frac{53}{1593} \right) = \left( \frac{53}{53} \right) $$

$$ = \left( \frac{53}{3} \right) = - \left( \frac{2}{3} \right) = +1. $$

○ Therefore, since 2017 is prime, 1593 is a quadratic residue modulo 2017.
5.7 Some Generalizations of Quadratic Reciprocity

- A natural question is whether there is a way to generalize quadratic reciprocity to other Euclidean domains, such as $\mathbb{Z}[i]$ and $\mathbb{F}_p[x]$. It turns out that the answer is yes!
  - One natural avenue for generalization is to seek a version of the Legendre symbol that detects when a given element is a square modulo a prime, in more general rings.
  - Another avenue is to try to generalize to higher degree: to seek a version of the Legendre symbol that detects when a given element is equal to a cube, fourth power, etc., modulo a prime.
  - There are generalizations in each of these directions, and although we do not have the tools to discuss many of them, the program of finding and classifying these various “reciprocity laws” was a central idea that motivated much of the development of one branch of modern number theory through the 1930s.

- Our goal is primarily to outline the ideas involved, so we will only sketch the basic ideas, leaving some of the details as an exercise.
  - A proper development that ties together all of these generalized reciprocity laws is left for a course in algebraic number theory, since the modern language of number theory (using ideals) is necessary to understand the broader picture.

- We will first describe how the notion of quadratic residue extends to a general Euclidean domain.

**Definition:** Let $R$ be an arbitrary Euclidean domain, and $\pi$ be a prime (equivalently, irreducible) element of $R$. We say that an element $a \in R$ is a quadratic residue modulo $\pi$ if $\pi \nmid a$ and there is some $b \in R$ such that $b^2 \equiv a \pmod{\pi}$. If there is no such $b$, we say $a$ is a quadratic nonresidue.

- **Example:** With $R = \mathbb{Z}[i]$ and $\pi = 2 + i$, the nonzero residue classes are represented by $i$, $2i$, $1 + i$, and $1 + 2i$. The quadratic residues are $2i \equiv (1 + i)^2$ and $1 + i \equiv i^2$, and the nonresidues are $1 + i$ and $1 + 2i$.

- **Example:** With $R = \mathbb{F}_3[x]$ and $\pi = x^2 + 1$, the nonzero residue classes are represented by $1$, $2$, $x$, $x + 1$, $x + 2$, $2x$, $2x + 1$, and $2x + 2$. The quadratic residues are $1$, $2 \equiv x^2$, $x \equiv (x + 2)^2$, and $2x \equiv (x + 1)^2$, while the nonresidues are $x + 1$, $x + 2$, $2x + 1$, and $2x + 2$.

- If $R/\pi R$ is a finite field, we can formulate a generalized quadratic residue symbol:

**Definition:** Let $p$ be a prime element in the Euclidean domain $R$ such that $R/\pi R$ is a finite field. Then the quadratic residue symbol $\left( \frac{a}{\pi} \right)_2$ is defined to be $0$ if $\pi | a$, $+1$ if $a$ is a quadratic residue modulo $p$, and $-1$ if $a$ is a quadratic nonresidue.

- Since $R/\pi R$ is a finite field, it has a primitive root $u$. An element $a$ is then a quadratic residue if and only if it is an even power of the primitive root.
- If $R/\pi R$ has even size, then there are an odd number of units. Then the order of a primitive root $u$ is odd, so (it is easy to see) every unit is congruent to an even power of $u$.
- Thus, the only interesting case occurs when $R/\pi R$ has odd size $N$.
- In this case, by Euler’s theorem in $R/\pi R$, we see that $a^{N-1} \equiv 1 \pmod{\pi}$ for every unit $a$.
- We can factor this as $(a^{(N-1)/2} - 1)(a^{(N-1)/2} + 1) \equiv 0 \pmod{\pi}$, so since $R/\pi R$ is a field, we see that $a^{(N-1)/2} \equiv \pm 1 \pmod{\pi}$.
- This suggests a natural generalization of Euler’s criterion:

**Proposition** (Generalized Euler’s criterion): Let $\pi$ be a prime element in the Euclidean domain $R$ such that $R/\pi R$ is a finite field with $N$ elements, where $N$ is odd. Then $\left( \frac{a}{\pi} \right)_2 \equiv a^{(N-1)/2} \pmod{\pi}$ for any $a$.

- The proof is almost identical to the one over $\mathbb{Z}$.
- **Proof:** Let $u$ be a primitive root in $R/\pi R$. As remarked above, an element $a$ is a quadratic residue if and only if it is an even power of the primitive root.
* It is straightforward to see that \( u^{(N-1)/2} \equiv -1 \pmod{\pi} \), since by Euler’s theorem this element has square 1 but does not equal 1.
* Then if \( a \equiv u^{2k} \pmod{\pi} \), we see that \( a^{(N-1)/2} \equiv (u^{N-1})^k \equiv 1 \pmod{\pi} \).
* Furthermore, if \( u \equiv u^{2k+1} \pmod{\pi} \), we have \( a^{(N-1)/2} \equiv (u^{N-1})^k u^{(N-1)/2} \equiv u^{(N-1)/2} \equiv -1 \pmod{\pi} \).

- Using Euler’s criterion, we immediately see that the quadratic residue symbol is multiplicative on top: 
  \[
  \left[ \frac{ab}{\pi} \right]_2 = \left[ \frac{a}{\pi} \right]_2 \cdot \left[ \frac{b}{\pi} \right]_2.
  \]

- In general, we would like to find a relation between the value of \( \left[ \frac{\pi}{\lambda} \right]_2 \) and \( \left[ \frac{\lambda}{\pi} \right]_2 \) if \( \lambda \) and \( \pi \) are primes in \( R \). The precise statement will depend on the ring \( R \).

- Remark: We can also extend the definition of the quadratic residue symbol to cover cases where the bottom element is not a prime, in much the same way as we defined the Jacobi symbol as a product of Legendre symbols. (We will not concern ourselves with the details here.)

5.7.1 Quadratic Reciprocity in \( \mathbb{Z}[i] \)

- Let \( \pi \) be a prime of odd norm in \( \mathbb{Z}[i] \) (i.e., any prime not associate to \( 1 + i \)).
  - For brevity, we will call a prime of odd norm an “odd prime”.

- The quadratic residue symbol in \( \mathbb{Z}[i] \) is (as we might expect) closely related to the Legendre symbol in \( \mathbb{Z} \).

- **Proposition:** If \( p \) is a prime congruent to 1 mod 4 in \( \mathbb{Z} \) factoring as \( \pi \pi \) in \( \mathbb{Z}[i] \), and \( a \in \mathbb{Z} \) is any integer, then 
  \[
  \left[ \frac{a}{\pi} \right]_2 = \left( \frac{a}{p} \right),
  \]
  where the second symbol is the Legendre symbol in \( \mathbb{Z} \). Furthermore, if \( l \) is any odd prime integer, then 
  \[
  \left[ \frac{\pi}{l} \right]_2 = \left( \frac{l}{\pi} \right).
  \]

  - **Proof:** If \( \pi \mid a \) or \( \pi \mid l \) then the results are obvious.
  - By Euler’s criterion in \( \mathbb{Z}[i] \), we have \( \left[ \frac{a}{\pi} \right]_2 \equiv a^{(p-1)/2} \pmod{\pi} \).
  - By Euler’s criterion in \( \mathbb{Z} \), we also have \( \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{p} \).
  - Since \( \pi \mid p \), this implies \( \left( \frac{a}{p} \right) \equiv a^{(p-1)/2} \pmod{\pi} \), so by the above, we see \( \left( \frac{a}{\pi} \right) \equiv \left[ \frac{a}{\pi} \right]_2 \pmod{\pi} \).
  - Since each of these is either 1 or \(-1\), the only way they could be unequal is if \(-1 \equiv 1 \pmod{\pi} \); but this would mean that \( \pi \mid 2 \), which is clearly not the case.
  - The second statement follows in exactly the same way.

- **Theorem (Quadratic Reciprocity in \( \mathbb{Z}[i] \))** \( \): If \( \pi \) and \( \lambda \) are distinct odd prime elements congruent to 1 modulo 2 in \( \mathbb{Z}[i] \), then 
  \[
  \left[ \frac{\pi}{\lambda} \right]_2 = \left[ \frac{\lambda}{\pi} \right]_2.
  \]

  - The statement that \( \pi \) and \( \lambda \) are congruent to 1 modulo 2 merely says that \( \pi = a + bi \) and \( \lambda = c + di \),
  where \( a \) and \( c \) are positive odd integers. (Any odd prime can be put into this form, so the statement is not much of a restriction.)
  - **Proof:** If both \( \lambda \) and \( \pi \) are integers in \( \mathbb{Z} \), then the result follows immediately from quadratic reciprocity in \( \mathbb{Z} \).
  - If \( \lambda \) is an integer \( l \) (i.e., an integer prime congruent to 3 modulo 4), and \( \pi \) is not, then by the above propositions we have 
    \[
    \left[ \frac{\pi}{l} \right]_2 = \left( \frac{N(\pi)}{l} \right) \quad \text{and} \quad \left[ \frac{l}{\pi} \right]_2 = \left( \frac{l}{N(\pi)} \right),
    \]
  and these are equal by quadratic reciprocity in \( \mathbb{Z} \). By symmetry, the result also holds if \( \pi \) is an integer, and \( \lambda \) is not.
Now assume that both \( \pi = a + bi \) and \( \lambda = c + di \) are nonintegers, with \( \pi \pi = p \) and \( \lambda \lambda = l \) two integral primes congruent to 1 modulo 4.

* By quadratic reciprocity in \( \mathbb{Z} \), first observe that \( \left( \frac{c}{7} \right) = \left( \frac{l}{c} \right) = \left( \frac{c^2 + d^2}{c} \right) = \left( \frac{d}{c} \right)^2 = +1. \)

* Also notice that \( pl = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \equiv (ad - bc)^2 \) (mod \( ac + bd \)).

* Thus, \( pl \) is a square modulo \( ac + bd \), so \( \left( \frac{l}{ac + bd} \right) = \left( \frac{p}{ac + bd} \right). \)

* By quadratic reciprocity, this says \( \left( \frac{ac + bd}{l} \right) = \left( \frac{ac + bd}{p} \right). \)

Now we can write

\[
\left[ \frac{\lambda}{\pi} \right]_2 = \left[ \frac{a^2}{\pi} \right]_2 \cdot \left[ \frac{c + di}{\pi} \right]_2 \\
= \left[ \frac{a}{\pi} \right]_2 \cdot \left[ \frac{ac + adi}{\pi} \right]_2 \\
= \left( \frac{a}{p} \right) \cdot \left[ \frac{ac + adi - d\pi}{\pi} \right]_2 \\
= \left( \frac{ac + bd}{\pi} \right) \cdot \left( \frac{ac + bd}{p} \right). 
\]

By the same argument, we have \( \left( \frac{\pi}{\lambda} \right) = \left( \frac{ac + bd}{l} \right) \), so, since this is equal to \( \left( \frac{ac + bd}{p} \right) \) as noted above, we conclude \( \left[ \frac{\lambda}{\pi} \right]_2 = \left[ \frac{\pi}{\lambda} \right]_2. \)

For completeness, we also remark that the argument above can be used to give simple formulas for the other remaining values of the quadratic residue symbol:

* If \( \pi = a + bi \) where \( a \) is odd and \( b \) is even, by Euler’s criterion, we have \( \left[ \frac{i}{\pi} \right]_2 = (-1)^{(N(\pi)-1)/4} = (-1)^{b/2}. \)

* Furthermore, by the argument above and quadratic reciprocity, we have \( \left[ \frac{1 + i}{\lambda} \right]_2 = \left( \frac{a + b}{p} \right) = \left( \frac{p}{a + b} \right). \)

* Now observe that \( 2p = (a + b)^2 + (a - b)^2 \), so \( \left( \frac{2p}{a + b} \right) = 1. \) Hence \( \left( \frac{p}{a + b} \right) = \left( \frac{2}{a + b} \right), \) meaning that \( \left[ \frac{1 + i}{\lambda} \right]_2 = \left( \frac{2}{a + b} \right). \)

### 5.7.2 Quartic Reciprocity in \( \mathbb{Z}[i] \)

* We can also write down a degree-4 variant of the quadratic residue symbol in \( \mathbb{Z}[i] \).

  * If \( \pi \) is a prime element of odd norm in \( \mathbb{Z}[i] \) and \( \pi \nmid \alpha \), we factored the expression \( \alpha^{N(\pi)-1} - 1 \equiv 0 \) in \( \mathbb{Z}[i]/\pi \) as \( (\alpha^{N(\pi)-1/2} - 1) \cdot (\alpha^{N(\pi)-1/2} + 1) \equiv 0 \) (mod \( \pi \)).
  
  * But now notice that \( N(\pi) - 1 \) is actually divisible by 4: so we can factor the expression even further, as \( (\alpha^{N(\pi)-1/4} - 1) \cdot (\alpha^{N(\pi)-1/4} + 1) \cdot (\alpha^{N(\pi)-1/4} + i) \cdot (\alpha^{N(\pi)-1/4} - i) \equiv 0. \)

  * Therefore, by unique factorization, we conclude that \( \alpha^{N(\pi)-1/4} \) is equivalent to one of 1, \(-1, i, -i \) modulo \( \pi \).

* **Definition:** If \( \pi \) is a prime element of odd norm, we define the **quartic residue symbol** \( \left[ \frac{\alpha}{\pi} \right]_4 \in \{0, \pm 1, \pm i\} \) to be 0 if \( \pi \nmid \alpha \), and otherwise to be the unique value among \( \{\pm 1, \pm i\} \) satisfying \( \left[ \frac{\alpha}{\pi} \right]_4 \equiv \alpha^{N(\pi)-1/4} \) (mod \( \pi \)).

  * This residue symbol detects fourth powers, in a similar way to how the quadratic residue symbol detects squares.
If \( u \) is a primitive root modulo \( \pi \), then \( \left[ \frac{\alpha}{\pi} \right]_4 = +1 \) precisely when \( \alpha \) is a power of \( u^4 \), which is clearly equivalent to \( \alpha \) being a fourth power modulo \( \pi \).

**Example:** Find the quartic residues modulo \( 2 + 3i \).

- The nonzero residue classes modulo \( \pi = 2 + 3i \) are represented by the elements 1, 2, 3, ... , 12. The quartic residues are \( 1, 3 \equiv (2 + i)^4 \), and \( 9 \equiv (1 + i)^4 \). The other 9 classes are quartic nonresidues.

- We can compute, for example, \( \left[ \frac{2}{2 + 3i} \right]_4 \equiv 2^3 \equiv i \pmod{\pi} \), and \( \left[ \frac{7}{2 + 3i} \right]_4 \equiv 7^3 \equiv -i \pmod{\pi} \).

This quartic residue symbol turns out to satisfy a reciprocity law much like the Legendre symbol in \( \mathbb{Z} \):

**Theorem** (Quartic Reciprocity in \( \mathbb{Z}[i] \)): If \( \pi \) and \( \lambda \) are both primes in \( \mathbb{Z}[i] \) congruent to 1 modulo \( 2 + 2i \), then

\[
\left[ \frac{\pi}{\lambda} \right]_4 \equiv \left[ \frac{\lambda}{\pi} \right]_4 \cdot (-1)^{\frac{N(\pi)-1}{4} \cdot \frac{N(\lambda)-1}{4}}.
\]

The proof, which we will not give here, involves more advanced machinery. (The result was known to Gauss, and a proof essentially appears in some of his unpublished papers.)

### 5.7.3 Quadratic Reciprocity in \( \mathbb{F}_p[x] \)

- As remarked earlier, all polynomials are quadratic residues modulo an irreducible polynomial \( f \) of positive degree in \( \mathbb{F}_2[x] \), since \( \mathbb{F}_2[x]/f \) has an even number of elements for any such \( f \).

- So we will restrict to the case of \( \mathbb{F}_p[x] \), where \( p \) is odd.

**Theorem** (Quadratic Reciprocity in \( \mathbb{F}_p[x] \)): Let \( p \) be an odd prime and \( f, g \) be monic irreducible polynomials of positive degree in \( \mathbb{F}_p[x] \). Then

\[
\left[ \frac{f}{g} \right]_2 \cdot \left[ \frac{g}{f} \right]_2 = (-1)^{\frac{p-1}{2} \cdot (\deg f) \cdot (\deg g)}.
\]

This result was originally stated by Dedekind in 1857, but a proof was not published until 1924.

- Most known proofs of this result (while fairly short) require more advanced results from algebraic number theory. To this author’s knowledge, an elementary proof of this theorem was not published until 1989.

- There is an elementary proof of this result, published in 2008, that relies only on the Chinese Remainder Theorem and the results we proved above, but it is fairly technical. (Perhaps the reader can devise a better one!)

Well, you're at the end of my handout. Hope it was helpful.

Copyright notice: This material is copyright Evan Dummit, 2014. You may not reproduce or distribute this material without my express permission.