Contents

5 Squares and Quadratic Reciprocity

In this chapter, we discuss a number of results relating to the squares modulo m. We begin by studying the quadratic residues (squares) and quadratic nonresidues (nonsquares) modulo a prime p, which leads to the Legendre symbol, a tool that provides a convenient way of determining when a residue class a modulo p is a square. We establish some basic properties of the Legendre symbol with an ultimate goal of proving Gauss's celebrated law of quadratic reciprocity, which describes an unexpected and stunning relation between when p is a square modulo q and when q is a square modulo p for primes p and q.

We provide a detailed motivation of quadratic reciprocity, in order to build up to the statement and proof of the theorem, and then discuss a number of applications to related number-theoretic questions. We close with a brief discussion of several different generalizations of quadratic reciprocity: we construct the Jacobi symbol and discuss squares modulo m for non-prime m, and then examine quadratic reciprocity in $\mathbb{Z}[i]$ and $\mathbb{F}_p[x]$.

5.1 Quadratic Residues and the Legendre Symbol

- Our goal is to discuss solutions to quadratic equations modulo m. We begin by treating the special case where the modulus is a prime.
  - 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 (just test $x \equiv 0, 1$), so we can 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, which we can easily solve.
  - So assume $a \not\equiv 0 \pmod{p}$: then a is invertible modulo p.
  - We may then complete the square to write $4af(x) = (2ax + b)^2 + (4ac - b^2)$.
  - Since $4a$ is invertible modulo p, the congruence $f(x) \equiv 0 \pmod{p}$ is equivalent to $(2ax + b)^2 \equiv (b^2 - 4ac) \pmod{p}$.
  - Solving for x then amounts to finding all solutions to $y^2 \equiv D \pmod{p}$, where $y = 2ax + b$ and $D = b^2 - 4ac$.
- To summarize the observations above: aside from some minor business about the leading coefficient and when $p = 2$, solving a general quadratic equation is equivalent to computing arbitrary square roots modulo p.

5.1.1 Quadratic Residues and Nonresidues

- Let us start by discussing the (seemingly) simpler question of determining whether the congruence $y^2 \equiv D \pmod{p}$ has a solution at all, when p is a prime.
- 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.
  - Remark: 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 immediate from the definition that $y^2 \equiv D \pmod{p}$ has a solution for y precisely when D is a quadratic residue modulo p (or when $D = 0$).
- 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 quadratic nonresidues are 2 and 3.
  - Example: Modulo 13, the quadratic residues are 1, 4, 9, 3, 12, and 10, while the quadratic nonresidues are 2, 5, 6, 7, 8, and 11.
  - Example: Modulo 21, the quadratic residues are 1, 4, and 16, while the quadratic 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 quadratic nonresidues are 2, 7, 12, 17, 22, 3, 8, 13, 18, and 23.
- Here are some of the basic properties of quadratic residues:
- Proposition (Properties of Quadratic Residues): Let p be an odd prime. Then the following hold:

1. 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.
   - For the converse, we will show inductively that if a is a quadratic residue modulo p^d then a is also a quadratic residue modulo p^{d+1}, for any d. By chaining together these implications we see that if a is a quadratic residue modulo p then a is also a quadratic residue modulo p^d for all $d \geq 1$.
   - So suppose that $a \equiv b^2 \pmod{p^d}$. Since p^d is odd, by shifting b by p^d if needed we may assume b has the same parity as a, and so we may write $a - b^2 = p^d \cdot 2k$ for some integer k. Then we have $(b + p^d k)^2 = b^2 + 2p^d k + p^{2d} k^2 \equiv b^2 + 2p^d k = a \pmod{p^{d+1}}$, and so a is also a quadratic residue modulo p^{d+1} as required.

2. If m is any odd positive integer, then a unit a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for each prime p dividing m.
   - Proof: By the Chinese Remainder Theorem, there is a solution to $x^2 \equiv a \pmod{m}$ if and only if there is a solution to $x^2 \equiv a \pmod{p^d}$ for each prime power p^d appearing in the prime factorization of m.
   - But by (1), there is a solution to $x^2 \equiv a \pmod{p^d}$ if and only if there is a solution to $x^2 \equiv a \pmod{p}$.
   - In other words, a is a quadratic residue modulo m if and only if a is a quadratic residue modulo p for each prime p dividing m, as claimed.
3. If p is an odd prime, the quadratic residues modulo p are 1^2, 2^2, ... , $(\frac{p-1}{2})^2$. Hence, half of the invertible residue classes modulo p are quadratic residues, and the other half are quadratic nonresidues.
   - Example: The quadratic residues modulo 11 are 1^2, 2^2, 3^2, 4^2, 5^2 (i.e., 1, 4, 9, 5, 3).
   - Proof: If p is prime, then $p|(a^2-b^2)$ implies $p|(a-b)$ or $p|(a+b)$: thus, $a^2 \equiv b^2 \pmod{p}$ is equivalent to $a \equiv \pm b \pmod{p}$.
   - We conclude that 1^2, 2^2, ... , $(\frac{p-1}{2})^2$ are distinct modulo p.
   - Furthermore, the other squares $(\frac{p+1}{2})^2$, ... , $(p-1)^2$ are equivalent to these in reverse order, since $k^2 \equiv (p-k)^2 \pmod{p}$.
4. If p is an odd prime and u is a primitive root modulo p, then a is a quadratic residue modulo p if and only if $a \equiv u^{2k} \pmod{p}$ for some integer k.
   - In other words, the quadratic residues are the even powers of the primitive root, while the quadratic nonresidues are the odd powers of the primitive root.
   - Example: 2 is a primitive root mod 11, and the quadratic residues mod 11 are $2^2 \equiv 4$, $2^4 \equiv 5$, $2^6 \equiv 9$, $2^8 \equiv 3$, and $2^{10} \equiv 1$.
   - Proof: Clearly, if $a \equiv u^{2k} \pmod{p}$ then $a \equiv (u^k)^2$ is a quadratic residue.
   - Conversely, suppose a is a quadratic residue, with $a \equiv b^2 \pmod{p}$. Then because u is a primitive root, we can write $b \equiv u^k \pmod{p}$ for some k: then $a \equiv b^2 \equiv u^{2k} \pmod{p}$, as required.

5.1.2 Legendre Symbols

- From items (1) and (2) in the proposition above, we are essentially reduced to wanting to study the quadratic residues modulo p. We now introduce notation that will help us distinguish between quadratic residues and quadratic nonresidues:
- 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 quadratic nonresidue modulo 7.
  - Example: We have $\left(\frac{3}{13}\right) = \left(\frac{-3}{13}\right) = +1$, and $\left(\frac{2}{13}\right) = 1$, since 3 and -3 are quadratic residues modulo 13, while 2 is not.
  - Note that the quadratic equation $x^2 \equiv a \pmod{p}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions modulo p.
- We would like to give an easy way to calculate the Legendre symbol.
- Theorem (Euler's Criterion): If p is an odd prime, then for any residue class a, it is true that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

- Proof: If $p|a$ then the result is trivial (since both sides are 0 mod p), so now assume a is a unit modulo p and let u be a primitive root modulo p.
- If a is a quadratic residue, then by item (4) of the proposition above, we know that $a = u^{2k}$ for some integer k.
- Then $a^{(p-1)/2} \equiv (u^{2k})^{(p-1)/2} = (u^{p-1})^k \equiv 1^k = 1 = \left(\frac{a}{p}\right) \pmod{p}$, as required.
- If a is a quadratic nonresidue, then again by item (4) of the proposition above, we know $a = u^{2k+1}$ for some integer k.
- We first observe that $u^{(p-1)/2} \equiv -1 \pmod{p}$: to see this, observe that $x = u^{(p-1)/2}$ has the property that $x^2 \equiv 1 \pmod{p}$.
- The two solutions to this quadratic equation are $x \equiv \pm 1 \pmod{p}$, but $x \not\equiv 1 \pmod{p}$ since otherwise u would not be a primitive root (its order would be at most $(p-1)/2$), so we have $x \equiv -1 \pmod{p}$.
- Now we can compute $a^{(p-1)/2} \equiv (u^{2k+1})^{(p-1)/2} = (u^{p-1})^k \cdot u^{(p-1)/2} \equiv u^{(p-1)/2} \equiv -1 = \left(\frac{a}{p}\right) \pmod{p}$, again as required.
- We conclude that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ in all cases, so we are done.

- Euler's criterion provides us with an efficient way to calculate Legendre symbols, since it is easy to find $a^{(p-1)/2}$ mod p using successive squaring.
- Example: Determine whether 5 is a quadratic residue or nonresidue modulo 29.
  - By Euler's criterion, $\left(\frac{5}{29}\right) \equiv 5^{14} \pmod{29}$.
  - 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 $\boxed{\text{quadratic residue}}$ modulo 29.
- Example: Determine whether 11 is a quadratic residue or nonresidue modulo 41.
  - By Euler's criterion, $\left(\frac{11}{41}\right) \equiv 11^{20} \equiv -1 \pmod{41}$ via successive squaring.
  - Thus, since the Legendre symbol is -1, we see that 11 is a $\boxed{\text{quadratic nonresidue}}$ modulo 41.
- We can extend these calculations to determine the quadratic residues and nonresidues for other moduli:
- Example: Determine whether 2 is a quadratic residue or nonresidue modulo 7^3.
  - Note that 7^3 is not prime, so we cannot use Euler's criterion directly. But because 7^3 is a prime power, we know that the quadratic residues modulo 7 are the same as the quadratic residues modulo 7^3.
  - By Euler's criterion, $\left(\frac{2}{7}\right) \equiv 2^3 \equiv 1 \pmod{7}$, so 2 is a quadratic residue modulo 7 hence also a $\boxed{\text{quadratic residue}}$ modulo 7^3.
- Example: Determine whether 112 is a quadratic residue or nonresidue modulo 675.
  - Note that $675 = 3^3 5^2$, so by our results, 112 is a quadratic residue modulo 675 if and only if it is a quadratic residue modulo 3 and modulo 5.
  - We have $\left(\frac{112}{3}\right) = \left(\frac{1}{3}\right) \equiv 1 \pmod{3}$, so 112 is a quadratic residue modulo 3.
  - However, $\left(\frac{112}{5}\right) = \left(\frac{2}{5}\right) \equiv 2^2 \equiv -1 \pmod{5}$, so 112 is a quadratic nonresidue modulo 5, hence also a $\boxed{\text{quadratic nonresidue}}$ modulo 675.

- Euler's criterion also yields an extremely useful corollary about the product of Legendre symbols:
- Corollary (Multiplicativity of Legendre Symbols): 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 quadratic residue and nonresidue is a nonresidue, and (much more unexpectedly) the product of two quadratic nonresidues is a quadratic 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.

5.2 The Law of Quadratic Reciprocity

- In this section we motivate and then prove Gauss's celebrated law of quadratic reciprocity, which describes an unexpected and stunning relation between when p is a quadratic residue modulo q and when q is a quadratic residue modulo p for primes p and q.
  - In other words, the law describes the relationship between the Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.
  - Before starting our discussion, we will point out that, based on what we have established so far, there is no obvious reason why there should be *any* relationship between these Legendre symbols at all!
  - Intuitively, it would seem like whether p is a square modulo q would have nothing at all to do with whether q is a square modulo p: these two questions are asking about different elements and different moduli, so why should there be any relationship between the answers?

5.2.1 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 $a = 1$ the answer is trivial, but for one other (less trivial) value of a, we can also answer this question immediately:
- Proposition (-1 and Quadratic Residues): If p is a prime, then -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 (since it is equal to 1), so assume p is odd.
  - By Euler's criterion, we have $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$. But the term on the right is $+1$ when $(p-1)/2$ is even and -1 when $(p-1)/2$ is odd.
  - Hence we deduce immediately that -1 is a quadratic residue precisely when $p \equiv 1 \pmod 4$.
- We also mention one interesting corollary of this result:
- Corollary (1 Mod 4 Primes): There are infinitely many primes congruent to 1 modulo 4.
  - Proof: By the proposition above, the congruence $n^2 + 1 \equiv 0 \pmod p$ has a solution if and only if $p = 2$ or $p \equiv 1 \pmod 4$.
  - We construct primes congruent to 1 modulo 4 using this polynomial $q(x) = x^2 + 1$ as follows: let $p_0 = 5$, and take $p_1, \ldots, p_k$ to be arbitrary primes congruent to 1 modulo 4.

- Now consider $q(2p_0p_1\cdots p_k)$, which is clearly an odd 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 1.
- Hence, by the above result, any prime divisor of $q(2p_0p_1\cdots p_k)$ must be a prime congruent to 1 modulo 4 that was not on our list. We conclude that there are infinitely many primes congruent to 1 modulo 4.

- For other $a \neq \pm 1$, however, the answer to our original question 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, 23, 31, 37, and 47, while a is a nonresidue modulo 5, 11, 13, 17, 23, and 41.
  - 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, 7, 11, 19, 31, 37, 41, and 47.

- 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 have units digits 1 or 9, while the primes where 5 is a nonresidue all have units digits 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.

- Theorem (Quadratic Reciprocity): If p and q are distinct odd primes, then $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$. 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).
  - This statement is often referred to as 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[1]; given Gauss's prodigious mathematical output, this is a very strong statement!

5.2.2 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, $2a$, ... , $\frac{p-1}{2}a$ whose least positive residue modulo p is bigger than $\frac{p}{2}$.
  - Proof: Let r_1, ... , r_k be the residues bigger than $\frac{p}{2}$ and s_1, ... , 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, we claim that these values $p - r_i$ are all distinct from the s_j.
  - To see this, suppose that $p - r_i = s_j$: then if $r_i \equiv c_1 a \pmod p$ and $s_j \equiv c_2 a \pmod p$, we would have $a(c_1 + c_2) \equiv 0 \pmod p$. So since a is a unit, this implies $c_1 + c_2 \equiv 0 \pmod p$. 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, ... , $\frac{p-1}{2}$ in some order.

[1] Gauss actually published six different proofs of quadratic reciprocity during his lifetime, and two more were found among his notes. There are now over 200 different proofs that have been collected.

- Thus, we may write

$$\begin{aligned} 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} &\equiv \prod_{i=1}^{k}(p-r_i) \cdot \prod_{j=1}^{l} s_j \pmod{p} \\ &\equiv (-1)^k \prod_{i=1}^{k} r_i \cdot \prod_{j=1}^{l} s_j \pmod{p} \\ &\equiv (-1)^k \prod_{n=1}^{(p-1)/2} (na) \pmod{p} \\ &\equiv (-1)^k a^{(p-1)/2} \cdot 1 \cdot 2 \cdot \cdots \cdot \frac{p-1}{2} \pmod{p} \end{aligned}$$

  and then cancelling the common $\left(\frac{p-1}{2}\right)!$ 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, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$. 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 roundoff analysis required to make an accurate accounting of how many residue classes reduce to lie in the interval $[p/2, p]$. Here is the formula for the general result:

- Lemma (Eisenstein): 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 greatest integer n with $n \leq x$, so for example $\lfloor \pi \rfloor = 3$ and $\lfloor -1.5 \rfloor = -2$. (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, $2a$, ... , $\frac{p-1}{2}a$ 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 mod 2.
  - As earlier, let r_1, ... , r_k be the residues bigger than $\frac{p}{2}$ and s_1, ... , s_l be the other residues, where $k + l = \frac{p-1}{2}$, and note that the elements $p - r_i$ and s_j are a rearrangement of 1, 2, ... , $\frac{p-1}{2}$.
  - 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 $p\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor+\sum_{i=1}^{k}r_j+\sum_{j=1}^{l}s_j=\sum_{j=1}^{(p-1)/2}ja=a\frac{p^2-1}{8}$.
- 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 $2\sum_{i=1}^{k}r_j$ are even, while p is odd, we obtain $\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{ja}{p}\right\rfloor\equiv k \pmod 2$, 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 $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{(p-1)(q-1)/4}$. 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 $n=\sum_{j=1}^{(p-1)/2}\left\lfloor\frac{jq}{p}\right\rfloor+\sum_{k=1}^{(q-1)/2}\left\lfloor\frac{kp}{q}\right\rfloor$.
  - The first sum is the number of lattice points (x,y) lying below the line $y=\frac{q}{p}x$, with $1\le x\le\frac{p-1}{2}$. The following figure illustrates this in the case $p=13$, $q=11$:

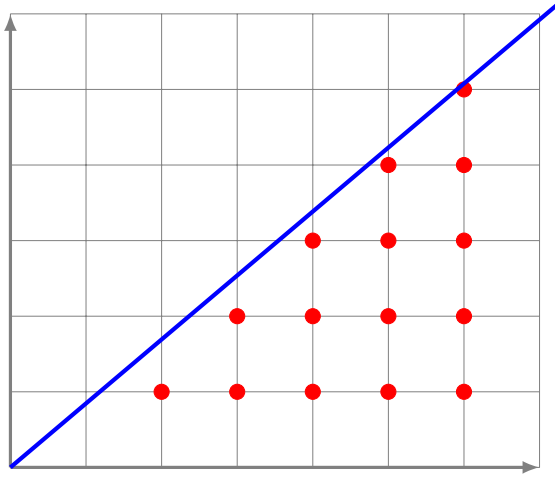

Figure 1: The lattice points underneath $y=\frac{q}{p}x$ with $1\le x\le\frac{p-1}{2}$.

  - 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 $1\le y\le\frac{q-1}{2}$. The following figure illustrates this in the case $p=13$, $q=11$:

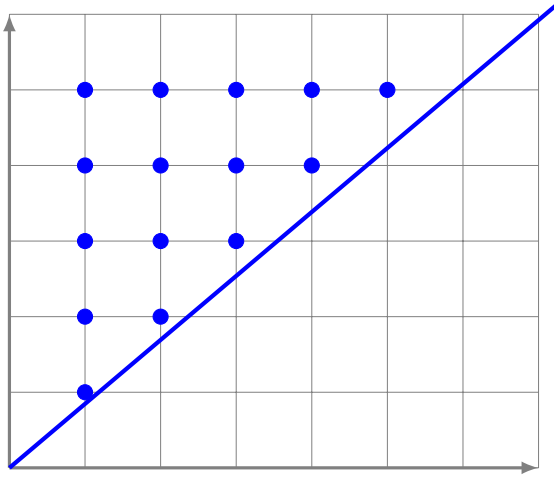

Figure 2: The lattice points to the left of $y = \frac{q}{p}x$ with $1 \leq y \leq \frac{q-1}{2}$.

- 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.
- 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 $\sum_{j=1}^{(p-1)/2} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{(q-1)/2} \left\lfloor \frac{kp}{q} \right\rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2}$, yielding the result.

- We now give a few examples of quadratic reciprocity for some particular primes p and q:
- Example: Verify quadratic reciprocity for the primes $p = 17$ and $q = 19$.
  - Using Euler's criterion, we evaluate $\left(\frac{17}{19}\right) \equiv 17^{(19-1)/2} \equiv 17^9 \equiv 1 \pmod{19}$. Indeed, 17 is a square modulo 19, since $17 \equiv 6^2 \pmod{19}$.
  - We also evaluate $\left(\frac{19}{17}\right) \equiv 19^{(17-1)/2} \equiv 19^8 \equiv 1 \pmod{17}$. Indeed, 19 is a square modulo 17, since $19 \equiv 6^2 \pmod{17}$.
  - This agrees with quadratic reciprocity, since 17 is congruent to 1 modulo 4, and $\left(\frac{17}{19}\right) \cdot \left(\frac{19}{17}\right) = 1$ as claimed.
- Example: Verify quadratic reciprocity for the primes $p = 23$ and $q = 43$.
  - Using Euler's criterion, we evaluate $\left(\frac{23}{43}\right) \equiv 23^{(43-1)/2} \equiv 23^{21} \equiv 1 \pmod{43}$. Indeed, 23 is a square modulo 43, since $23 \equiv 18^2 \pmod{43}$.
  - We also evaluate $\left(\frac{43}{23}\right) \equiv 43^{(23-1)/2} \equiv (-3)^{11} \equiv -1 \pmod{23}$. One can verify by writing down all of the quadratic residues modulo 23 that $43 \equiv 20$ is not among them.
  - This agrees with quadratic reciprocity, since both 23 and 43 are congruent to 3 modulo 4, and $\left(\frac{23}{43}\right) \cdot \left(\frac{43}{23}\right) = -1$ as claimed.

5.3 The Jacobi Symbol

- We can use quadratic reciprocity to give another method for computing Legendre symbols.
  - Explicitly, suppose we want $\left(\frac{p}{q}\right)$ where $p < q$. then since $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$, it suffices to find $\left(\frac{q}{p}\right)$. But now because $q > p$, $\left(\frac{q}{p}\right) = \left(\frac{r}{p}\right)$ where r is the remainder upon dividing q by p.
  - We have therefore reduced the problem to one of calculating a Legendre symbol with smaller terms.
  - By repeating this "flip and reduce" procedure, we can eventually winnow the terms down to values we can evaluate by inspection.
- Example: Determine whether 31 is a quadratic residue modulo 47.
  - We want to find $\left(\frac{31}{47}\right)$. Notice that 31 and 47 are both prime, so we can apply quadratic reciprocity.
  - 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 $\boxed{\text{is not}}$ a quadratic residue modulo 47.
- Example: Determine whether 357 is a quadratic residue modulo 661.
  - We want $\left(\frac{357}{661}\right)$. Although 661 is prime, 357 is not, so we cannot apply quadratic reciprocity directly.
  - Instead, we must first factor the top number: since $357 = 3 \cdot 7 \cdot 17$, we have $\left(\frac{357}{661}\right) = \left(\frac{3}{661}\right)\left(\frac{7}{661}\right)\left(\frac{17}{661}\right)$.
  - By quadratic reciprocity, since $661 \equiv 1 \pmod 4$ is prime, and 3, 7, 17 are also prime, we have

$$\begin{aligned}
\left(\frac{3}{661}\right) &= \left(\frac{661}{3}\right) = \left(\frac{1}{3}\right) = +1 \\
\left(\frac{7}{661}\right) &= \left(\frac{661}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1 \\
\left(\frac{17}{661}\right) &= \left(\frac{661}{17}\right) = \left(\frac{-2}{17}\right) = \left(\frac{-1}{17}\right) \cdot \left(\frac{2}{17}\right) = (+1) \cdot (+1) = +1
\end{aligned}$$

  - Thus, $\left(\frac{357}{661}\right) = \left(\frac{3}{661}\right) \cdot \left(\frac{7}{661}\right) \cdot \left(\frac{17}{661}\right) = -1$, so 357 $\boxed{\text{is not}}$ 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 now generalize the definition of the Legendre symbol to composite moduli, so as to provide a way around this problem.

5.3.1 Definition and Examples

- 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 $\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)_L \left(\frac{a}{p_2}\right)_L \cdots \left(\frac{a}{p_k}\right)_L$, where $\left(\frac{a}{p_k}\right)_L$ denotes the Legendre symbol.

- If b is itself prime, then the Jacobi symbol is simply the Legendre symbol. We will therefore just write $\left(\frac{a}{b}\right)$ since we may now always assume it is referring to the Jacobi symbol.
- Example: We have $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = +1$.
- Example: We have $\left(\frac{11}{45}\right) = \left(\frac{11}{3}\right)^2 \cdot \left(\frac{11}{5}\right) = (-1)^2 \cdot (+1) = -1$.
- Example: We have $\left(\frac{77}{33}\right) = \left(\frac{77}{3}\right) \cdot \left(\frac{77}{11}\right) = (-1) \cdot 0 = 0$.
- 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 $\gcd(a, b) > 1$.

- Proposition (Properties of Jacobi Symbols): Suppose b and b' are positive odd integers and a, a' are integers. Then the following hold:

1. The Jacobi symbol is multiplicative on top and bottom: $\left(\frac{aa'}{b}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a'}{b}\right)$ and $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$.
   - Proof: For the first statement, suppose $b = p_1 \cdots p_k$. Then $\left(\frac{aa'}{b}\right) = \left(\frac{aa'}{p_1}\right)_L \cdots \left(\frac{aa'}{p_k}\right)_L = \left(\frac{a}{p_1}\right)_L \left(\frac{a'}{p_1}\right)_L \cdots \left(\frac{a}{p_k}\right)_L \left(\frac{a'}{p_k}\right)_L = \left(\frac{a}{p_1}\right)_L \cdots \left(\frac{a}{p_k}\right)_L \left(\frac{a'}{p_1}\right)_L \cdots \left(\frac{a'}{p_k}\right)_L = \left(\frac{a}{b}\right)\left(\frac{a'}{b}\right)$, where we used the multiplicativity of the Legendre symbol in the middle.
   - For the second statement, suppose $b = p_1 \cdots p_k$ and $b' = q_1 \cdots q_k$.
   - Then $\left(\frac{a}{bb'}\right) = \left(\frac{a}{p_1}\right)_L \cdots \left(\frac{a}{p_k}\right)_L \left(\frac{a}{q_1}\right)_L \cdots \left(\frac{a}{q_k}\right)_L = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$ by definition of the Jacobi symbol.
2. If a is a quadratic residue modulo b and is relatively prime to b, then $\left(\frac{a}{b}\right) = +1$.
   - Proof: If $a \equiv r^2 \pmod{b}$, then $\left(\frac{a}{b}\right) = \left(\frac{r^2}{b}\right) = \left(\frac{r}{b}\right)^2 = +1$, since $\left(\frac{r}{b}\right)$ is either $+1$ or -1 by the assumption that a (hence r) is relatively prime to b.

- Item (2) in the proposition above tells us that the Jacobi symbol, like the Legendre symbol, evaluates to $+1$ on quadratic residues. However, unlike the Legendre symbol, which *only* evaluates to $+1$ on quadratic residues, the Jacobi symbol can also evaluate to $+1$ on quadratic nonresidues.
  - In other words, the converse to item (2) is not 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 because the only quadratic residues modulo 15 are 1 and 4.
  - 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 quadratic 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 quadratic nonresidues can still be a quadratic nonresidue.
  - For example, the quadratic residues modulo 15 are 1 and 4, while the quadratic nonresidues are 2, 7, 8, 11, 13, 14. Now observe that $2 \cdot 7 = 14 \pmod{15}$, but all three of 2, 7, and 14 are quadratic nonresidues.

- Ultimately, the problem is that a composite modulus has different types of quadratic nonresidues.
- To illustrate, an element a can be a quadratic nonresidue modulo 15 in three ways: (i) it could be a quadratic nonresidue mod 3 and a quadratic residue mod 5 [namely, $a = 11, 14$], (ii) a quadratic residue mod 3 and a quadratic nonresidue mod 5 [namely, $a = 7, 13$], or (iii) a quadratic nonresidue mod 3 and a quadratic nonresidue mod 5 [namely, $a = 2, 8$].
- The product of two quadratic nonresidues each in the same class above will be a quadratic residue modulo 15 (since it will be a quadratic residue mod 3 and mod 5), but the product of quadratic nonresidues from different classes will still be a quadratic nonresidue mod 15 (since it will be a quadratic nonresidue modulo 3 or modulo 5).

5.3.2 Quadratic Reciprocity for Jacobi Symbols

- Our main goal now is to establish that the Jacobi symbol also obeys the law of quadratic reciprocity. We first collect a few basic evaluations:
- Proposition (Basic Evaluations): If $b = p_1 p_2 \cdots p_k$ is a product of odd primes, then we have the following:
  1. $\left(\frac{-1}{b}\right) = (-1)^{(b-1)/2}$. Equivalently, $\left(\frac{-1}{b}\right)$ is $+1$ if $b \equiv 1 \pmod 4$ and is -1 if $b \equiv 3 \pmod 4$.
     - Proof: From our results on Legendre symbols, we know that $\left(\frac{-1}{p_k}\right) = (-1)^{(p_k-1)/2}$.
     - Then, by definition, $\left(\frac{-1}{b}\right) = \prod_{j=1}^{k} \left(\frac{-1}{p_k}\right) = \prod_{j=1}^{k} (-1)^{(p_k-1)/2} = (-1)^{\sum (p_k-1)/2}$.
     - It remains to verify that $\sum_{j=1}^{k} \frac{p_k - 1}{2} \equiv \prod_{j=1}^{k} \frac{p_k - 1}{2} \pmod 2$.
     - To see this observe that if m, n are odd then $\frac{mn-1}{2} - \frac{m-1}{2} - \frac{n-1}{2} = \frac{(m-1)(n-1)}{2}$ is even, and so $\frac{mn-1}{2} \equiv \frac{m-1}{2} + \frac{n-1}{2} \pmod 2$.
     - Then by an easy induction, we get $\sum_{j=1}^{k} \frac{p_k - 1}{2} \equiv \prod_{j=1}^{k} \frac{p_k - 1}{2} \pmod 2$, as required.
  2. $\left(\frac{2}{b}\right) = (-1)^{(b^2-1)/8}$. Equivalently, $\left(\frac{2}{b}\right)$ is $+1$ if $b \equiv 1, 7 \pmod 8$ and is -1 if $b \equiv 3, 5 \pmod 8$.
     - Proof: From our results on Legendre symbols, we know that $\left(\frac{2}{p_k}\right) = (-1)^{(p_k^2-1)/8}$.
     - Like above, $\left(\frac{2}{b}\right) = \prod_{j=1}^{k} \left(\frac{2}{p_k}\right) = \prod_{j=1}^{k} (-1)^{(p_k^2-1)/8} = (-1)^{\sum (p_k^2-1)/8}$.
     - It remains to verify that $\sum_{j=1}^{k} \frac{p_k^2 - 1}{8} \equiv \prod_{j=1}^{k} \frac{p_k^2 - 1}{8} \pmod 2$.
     - To see this observe that if m, n are odd then $\frac{m^2n^2-1}{8} - \frac{m^2-1}{8} - \frac{n^2-1}{8} = \frac{(m^2-1)(n^2-1)}{8}$, so $\frac{m^2n^2-1}{8} \equiv \frac{m^2-1}{8} + \frac{n^2-1}{8} \pmod 2$.
     - Then by an easy induction, we get $\sum_{j=1}^{k} \frac{p_k^2 - 1}{8} \equiv \prod_{j=1}^{k} \frac{p_k^2 - 1}{8} \pmod 2$, as required.
- Now we can prove quadratic reciprocity for the Jacobi symbol.
- Theorem (Quadratic Reciprocity for Jacobi Symbols): 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

$$\begin{aligned}\left(\frac{a}{b}\right) &= \prod_{j=1}^{k}\left(\frac{a}{p_j}\right) = \prod_{j=1}^{k}\prod_{i=1}^{l}\left(\frac{q_i}{p_j}\right) = \prod_{j=1}^{k}\prod_{i=1}^{l}\left(\frac{p_j}{q_i}\right)\cdot(-1)^{(p_j-1)(q_i-1)/4} \\ &= \prod_{i=1}^{l}\prod_{j=1}^{k}\left(\frac{p_j}{q_i}\right)\cdot(-1)^{\sum_{i,j}(p_j-1)(q_i-1)/4} = \left(\frac{b}{a}\right)\cdot(-1)^{\sum_{i,j}(p_j-1)(q_i-1)/4}.\end{aligned}$$

- But then $\sum_{i=1}^{l}\sum_{j=1}^{k}\frac{(p_i-1)(q_j-1)}{4} \equiv \left(\sum_{i=1}^{l}\frac{p_i-1}{2}\right)\cdot\left(\sum_{j=1}^{k}\frac{q_j-1}{2}\right) \equiv \frac{a-1}{2}\cdot\frac{b-1}{2} \pmod 2$ 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.

5.3.3 Calculating Legendre Symbols Using Jacobi Symbols

- We can use the Jacobi symbol to compute Legendre symbols using the "flip and reduce" 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.
  - But since 1009 is prime, the Jacobi symbol is the same as the Legendre symbol, so this means 247 is a $\boxed{\text{quadratic nonresidue}}$ modulo 1009.
- Example: Determine whether 1593 is a quadratic residue modulo the prime 2017.
  - By repeatedly using the "flip and reduce" procedure, we compute $\left(\frac{1593}{2017}\right) = \left(\frac{2017}{1593}\right) = \left(\frac{424}{1593}\right) = \left(\frac{2}{1593}\right)^3\left(\frac{53}{1593}\right) = \left(\frac{1593}{53}\right) = \left(\frac{3}{53}\right) = -\left(\frac{53}{3}\right) = -\left(\frac{2}{3}\right) = +1.$
  - Since 2017 is prime, the Jacobi symbol is the same as the Legendre symbol, so this means 1593 is a $\boxed{\text{quadratic residue}}$ modulo 2017.

5.4 Applications of Quadratic Reciprocity

- In this section, we discuss several applications of quadratic reciprocity to various classical and modern questions in number theory.

5.4.1 For Which p is a a Quadratic Residue Modulo p?

- Our first application of quadratic reciprocity is determining (given a particular value of a) for which primes p is a a quadratic residue.
  - To outline the procedure, if we want to compute $\left(\frac{a}{p}\right)$ for a fixed a, then after we find the prime factorization of a, we can convert the question to that of analyzing the Legendre symbols $\left(\frac{q_i}{p}\right)$ for the prime factors q_i of a.

- By using quadratic reciprocity, this is equivalent to analyzing the Legendre symbols $\left(\frac{p}{q_i}\right)$, which we can then do simply by listing all of the quadratic residues and nonresidues modulo q_i for each of the fixed values q_i.

- Example: Characterize the primes p for which 3 is a quadratic residue modulo p.
  - 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 $11 \pmod{12}$.

- Example: Characterize the primes p for which 6 is a quadratic residue modulo p.
  - 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 $11 \pmod{12}$, and $\left(\frac{3}{p}\right) = -1$ when $p \equiv 5$ or $7 \pmod{12}$.
  - We also know that $\left(\frac{2}{p}\right) = +1$ when $p \equiv 1$ or $7 \pmod 8$, and $\left(\frac{2}{p}\right) = -1$ when $p \equiv 3$ or $5 \pmod 8$.
  - Thus, $\left(\frac{6}{p}\right) = +1$ in the following cases:
  - Case 1: $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = +1$. This requires $p \equiv 1, 11 \pmod{12}$ and $p \equiv 1, 7 \pmod 8$. Solving these simultaneous congruences yields $p \equiv 1, 23 \pmod{24}$.
  - Case 2: $\left(\frac{3}{p}\right) = \left(\frac{2}{p}\right) = -1$. This requires $p \equiv 5, 7 \pmod{12}$ and $p \equiv 3, 5 \pmod 8$. Solving these simultaneous congruences yields $p \equiv 5, 19 \pmod{24}$.
  - Therefore, 6 is a quadratic residue modulo p precisely when $p \equiv 1, 5, 19, 23 \pmod{24}$.

5.4.2 Primes Dividing Values of a Quadratic Polynomial

- Another more surprising consequence 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 $p \equiv 1 \pmod{6}$.

- Using the characterization of the prime divisors of n^2+n+7, we can deduce the following interesting result:
- Proposition (1 Mod 6 Primes): 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 $q(p_0 p_1 \cdots p_k)$, 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 $q(p_0 p_1 \cdots p_k)$ 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, known as Dirichlet's theorem on primes in arithmetic progressions, that if a and m are relatively prime, there exist infinitely many primes congruent to a modulo m. This result is the special case with $a=1$ and $m=6$.

- Example: Characterize the primes dividing an integer of the form n^2+2n+6, for n an integer.
  - Observe that 2 is a divisor when $n=0$, so we may now restrict our attention to odd primes p.
  - Completing the square yields $(n+1)^2 \equiv -5 \pmod{p}$, which is equivalent to saying -5 is a quadratic residue modulo p. Clearly this has a solution when $p=5$, so also assume $p \neq 5$.
  - Then, to characterize these values we want to determine when $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{5}{p}\right)$ is equal to $+1$.
  - From earlier, we know that $\left(\frac{-1}{p}\right)$ is $+1$ if $p \equiv 1 \pmod{4}$ and is -1 if $p \equiv 3 \pmod{4}$.
  - By quadratic reciprocity, since 5 is congruent to 1 mod 4, we see $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, so $\left(\frac{5}{p}\right) = +1$ for $p \equiv 1, 4 \pmod{5}$ and $\left(\frac{5}{p}\right) \equiv -1$ for $p \equiv 2, 3 \pmod{5}$.
  - Combining the appropriate cases using the Chinese remainder theorem shows that $\left(\frac{-5}{p}\right) = +1$ precisely when $p \equiv 1, 3, 7, 9 \pmod{20}$.
  - Thus, by the above, we conclude that a prime p divides an integer of the form n^2+2n+6 either when $p=2$ or $p=5$ or when $p \equiv 1, 3, 7, 9 \pmod{20}$.

5.4.3 Berlekamp's Root-Finding Algorithm

- We can also use some of the ideas of quadratic reciprocity to establish a fast root-finding algorithm for polynomials modulo p.
- Let $q(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be an element of $\mathbb{F}_p[x]$. We would like to describe a method for calculating a root of $q(x)$ in $\mathbb{F}_p$, if there is one.
  - As a starting point, consider the case where $q(x) = (x - r_1)(x - r_2)\cdots(x - r_n)$ factors into a product of linear terms in $\mathbb{F}_p[x]$.
  - We can detect if one of the r_i is equal to zero (since then q will have constant term 0), and also detect if any of the r_i are equal (since then q will have a common factor with its derivative q'), so assume that all of the r_i are distinct and nonzero.
  - Now, from Euler's criterion in $\mathbb{F}_p$, we know that $r^{(p-1)/2} \equiv \left(\frac{r}{p}\right) \bmod p$.
  - Therefore, the roots of the polynomial $x^{(p-1)/2} - 1$ in $\mathbb{F}_p$ are precisely the quadratic residues, while the roots of the polynomial $x^{(p-1)/2} + 1$ in $\mathbb{F}_p$ are precisely the quadratic nonresidues.
  - Thus, the greatest common divisor of $x^{(p-1)/2} - 1$ with $q(x)$ will be equal to the product of all the terms $x - r_i$ where r_i is a quadratic residue, while the greatest common divisor of $x^{(p-1)/2} + 1$ with $q(x)$ will be equal to the product of all the terms $x - r_i$ where r_i is a quadratic nonresidue.
  - This means that at least one root is a quadratic residue, and another is a quadratic nonresidue, then we will obtain a partial factorization of $q(x)$.
  - Our next insight is that we can repeat this procedure by performing the same calculation with $q(x - a)$ for an arbitrary $a \in \mathbb{F}_p$: the roots of this polynomial are simply the values $a + r_1, \ldots, a + r_n$. Since a can be arbitrary, and half of the residue classes modulo p are quadratic residues, we would expect to obtain at least one quadratic residue and one nonresidue with probability roughly $1 - 2/2^n$, which is always at least $1/2$ when $n \geq 2$.
  - Thus, if there are at least two roots of this polynomial, we expect to find a partial factorization with probability at least $1/2$ for each attempt. By iteratively applying this method for each factor, we can quickly calculate the polynomial's full list of roots.
- Here is a more formal description of this method:
- Algorithm (Berlekamp's Root-Finding): Let $q(x) \in \mathbb{F}_p[x]$ and suppose that $q(x) = (x - r_1)\cdots(x - r_n)$ for some distinct $r_i \in \mathbb{F}_p$. Choose a random $a \in \mathbb{F}_p$ and compute the greatest common divisor of $q(x - a)$ with the two polynomials $x^{(p-1)/2} - 1$ and $x^{(p-1)/2} + 1$. If one of these gcds is a constant, choose a different value of a and start over. Otherwise, if both gcds have positive degree, then each gcd gives a nontrivial factor of $q(x)$. Repeat the factorization procedure on each gcd, until the full factorization of $q(x)$ is found.
  - We note that the first step in the Euclidean algorithm's gcd calculation can be performed efficiently using successive squaring modulo $q(x - a)$: explicitly, to find the remainder upon dividing $x^{(p-1)/2}$ by $q(x - a)$, we use successive squaring (of powers of x) modulo $q(x - a)$.
  - As we noted above, the probability of failure on any given attempt should be (heuristically) roughly $2^{-(n-1)}$, which means that even in the worst case for a polynomial of degree 2, we have a 50% chance of success on each attempt.
  - Overall, this algorithm can be implemented in $O(n^2 \log p)$ time[2]. For large n, then, it is still fairly slow, but if n is small and p is large, it is much more efficient than a brute-force search for the roots.
- As a specific application, this method is quite efficient for computing square roots modulo p for arbitrary primes p.

[2]The components are as follows: (i) computing the coefficients of $q(x - a)$ in $\mathbb{F}_p[x]$ using the binomial theorem, (ii) applying the Euclidean algorithm to compute the gcd of two polynomials of degree n in $\mathbb{F}_p[x]$, (iii) summing over the expected number of applications until the complete factorization is found. Both the binomial theorem and Euclidean algorithm calculations can be done in $O(n^2 \log p)$ time, and the expected number of applications is essentially constant because of the exponential success probability.

- During our analysis of the Rabin cryptosystem, we showed that if $p \equiv 3 \pmod 4$, then $a^{(p+1)/4}$ is a square root of a modulo p, so in this case there is a simple formula for computing square roots.
- However, if $p \equiv 1 \pmod 4$ there is not such a nice formula. We will mention in particular that using $a = 0$ will never work for computing square roots modulo p if $p \equiv 1 \pmod 4$, since the two square roots will always be both quadratic residues or both quadratic nonresidues because -1 is a quadratic residue modulo p.

- Example: Find the roots of $x^2 \equiv 3 \pmod{13}$.
  - First, we can compute $\left(\frac{3}{13}\right) = +1$ (either via Euler's criterion or by using quadratic reciprocity), so 3 does have square roots modulo 13.
  - To compute them we let $q(x) = x^2 - 3$ modulo $p = 13$.
  - As noted above, $a = 0$ will not work, so we try $a = 1$, so that $q(x - a) = x^2 - 2x - 2$.
  - Using successive squaring, we can calculate $x^{(p-1)/2} = x^6 \equiv 3x + 10 \pmod{13}$.
  - This means $x^{(p-1)/2} - 1 \equiv 3x + 9 \pmod{13}$, and so the first step of the Euclidean algorithm reads $x^{(p-1)/2} \equiv [\text{quotient}] \cdot q(x - a) + (3x + 9)$.
  - Performing the next step shows that $3x + 9$ does indeed divide $x^2 - 2x - 2$ modulo 13 (the quotient is $9x + 7$).
  - Solving for the first root (i.e., solving $3n + 9 \equiv 0 \pmod{13}$) yields $n \equiv -3 \equiv 10 \pmod{13}$.
  - This means $n = 10$ is a root of $q(x-1)$, and therefore $n - 1 = 9$ is a root of the original polynomial $q(x)$.
  - Indeed, we can check that $9^2 \equiv 3 \pmod{13}$. Therefore, the two roots are $r \equiv \boxed{\pm 9} \pmod{13}$.

- Example: Find the roots of $x^2 \equiv 11 \pmod{2017}$.
  - First, we can compute $\left(\frac{11}{2017}\right) = +1$ (either via Euler's criterion or by using quadratic reciprocity), so 11 does have square roots modulo the prime 2017.
  - To compute them we let $q(x) = x^2 - 11$ modulo $p = 2017$.
  - As noted above, $a = 0$ will not work, so we try $a = 1$, so that $q(x - a) = x^2 - 2x - 10$.
  - Using successive squaring, we can calculate $x^{(p-1)/2} = x^{1008} \equiv 307x + 1710 \pmod{2017}$.
  - This means $x^{(p-1)/2} - 1 \equiv 307x + 1709 \pmod{2017}$, and so the first step of the Euclidean algorithm reads $x^{(p-1)/2} \equiv [\text{quotient}] \cdot q(x - a) + (307x + 1709)$.
  - Performing the next step shows that $307x + 1709$ does indeed divide $x^2 - 2x - 10$ modulo 2017 (the quotient is $1360x + 668$).
  - Solving for the first root (i.e., solving $307n + 1709 \equiv 0 \pmod{2017}$) yields $n \equiv 1361 \pmod{2017}$.
  - This means $n = 1361$ is a root of $q(x-1)$, and therefore $n - 1 = 1360$ is a root of the original polynomial $q(x)$.
  - Indeed, we can check that $1360^2 \equiv 11 \pmod{2017}$. Therefore, the two roots are $r \equiv \boxed{\pm 1360} \pmod{2017}$.

- Although we have quoted this result for polynomials $q(x)$ that factor as a product of linear terms, we can in fact reduce the general problem of finding roots for arbitrary polynomials in $\mathbb{F}_p[x]$ to this case.
  - Explicitly, first we remove any repeated irreducible factors from q using its derivative, and then we apply the factorization algorithm above to the greatest common divisor of $q(x)$ and $x^p - x$.
  - Since $x^p - x$ is the polynomial whose roots are all the elements of $\mathbb{F}_p$, the greatest common divisor of $q(x)$ and $x^p - x$ will be the product of all the linear terms in the factorization of $q(x)$, which is the factor of $q(x)$ that contains all its roots.
  - Thus, to find roots of $q(x)$, we need only find the roots of the greatest common divisor of $q(x)$ and $x^p - x$, and we can do this using the algorithm described above.

5.4.4 The Solovay-Strassen Compositeness Test

- Another application of quadratic reciprocity is to give a compositeness test of similar flavor to the Miller-Rabin test.
  - From Euler's criterion, we know that if p is prime, then $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)$ modulo p.
  - Initially, we used this test to give a method for computing the Legendre symbol $\left(\frac{a}{p}\right)$. But we also have another way to compute this symbol, namely, by evaluating the Jacobi symbol $\left(\frac{a}{p}\right)$ using the "flip and reduce" procedure provided by quadratic reciprocity.
  - We therefore obtain a compositeness test by comparing the results of these two different methods: if $a^{(p-1)/2} \not\equiv \left(\frac{a}{p}\right)$ modulo p, then p is not prime.

- Test (Solovay-Strassen): If m is an odd integer such that $a^{(m-1)/2} \not\equiv \left(\frac{a}{m}\right)$ modulo m, then m is composite.
  - We remark that in order for the test to be useful, we need to calculate the Jacobi symbol $\left(\frac{a}{m}\right)$ using quadratic reciprocity. Thus, we will want to select a to be an odd residue class that is greater than 1.
  - This compositeness test was developed by Solovay and Strassen in 1978, and (as it slightly predated the unconditional version of the Miller-Rabin test) was one of the first primality tests demonstrating the feasibility of generating large primes for implementing cryptosystems like RSA.
  - Like with the Fermat and Miller-Rabin tests, this is a compositeness test only: each individual application for a single value of a can only produce the results "m is composite" or "no result".
  - In practice, the Solovay-Strassen test is used probabilistically, like with the Miller-Rabin test: we apply the test many times to the integer m, and if it passes sufficiently many times, we say m is probably prime.
  - It can be shown that any given residue has at least a $1/2$ probability of showing that m is composite, so the probability that a composite integer m can pass the test k times with randomly-chosen residues a is at most $1/2^k$.

- Example: Use the Solovay-Strassen test to decide whether 561 is prime.
  - We try $a = 5$: we have $5^{(m-1)/2} \equiv 5^{280} \equiv 67 \pmod{561}$, whereas $\left(\frac{5}{561}\right) = \left(\frac{561}{5}\right) = \left(\frac{1}{5}\right) = 1$. Since these are unequal, we conclude that 561 is $\boxed{\text{composite}}$.
  - Remark: Note that 561 is a Carmichael number, and passes the Fermat test for every residue class.

- Example: Use the Solovay-Strassen test with $a = 137$ to decide whether 35113 is prime.
  - With $m = 35113$, we have $137^{(m-1)/2} \equiv 137^{17556} \equiv 1 \pmod{2701}$.
  - Also, we have $\left(\frac{137}{35113}\right) = \left(\frac{35113}{137}\right) = \left(\frac{41}{137}\right) = \left(\frac{137}{41}\right) = \left(\frac{14}{41}\right) = \left(\frac{2}{41}\right) \cdot \left(\frac{7}{41}\right) = +1 \cdot \left(\frac{41}{7}\right) = \left(\frac{-1}{7}\right) = -1$. Since these are unequal, we conclude that 35113 is $\boxed{\text{composite}}$.

5.5 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 algebraic number theory in the early 20th century.

- Our goal is primarily to give a broad survey, so we will only sketch the basic ideas of the results.
  - A proper development that ties together all of these generalized reciprocity laws is properly left for a course in algebraic number theory, since the modern language of number theory (using ideals) is necessary to understand the broader picture.

5.5.1 Quadratic Residue Symbols in Euclidean Domains

- 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 π be a prime (equivalently, irreducible) element of R. We say that an element $a \in R$ is a quadratic residue modulo π 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 π 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 π, and -1 if a is a quadratic nonresidue modulo π.
  - 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 $a^{(N-1)/2} \equiv \pm 1 \pmod{\pi}$.

- The calculations above suggest a natural generalization of Euler's criterion:
- Proposition (Generalized Euler's Criterion): Let π 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 $a^{(N-1)/2} \equiv (u^{N-1})^k u^{(N-1)/2} \equiv u^{(N-1)/2} \equiv -1 \pmod{\pi}$.

- As an immediate corollary, we see that the quadratic residue symbol is multiplicative on top:

- Corollary: Let π 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 for any a and b, we have $\left[\frac{ab}{\pi}\right]_2 = \left[\frac{a}{\pi}\right]_2 \cdot \left[\frac{b}{\pi}\right]_2$.
  - Proof: We have $\left[\frac{ab}{\pi}\right]_2 = (ab)^{(N-1)/2} \equiv a^{(N-1)/2} b^{(N-1)/2} = \left[\frac{a}{\pi}\right]_2 \cdot \left[\frac{b}{\pi}\right]_2 \pmod{\pi}$.
  - Since both sides are ± 1 and π does not divide 2, we must then have $\left[\frac{ab}{\pi}\right]_2 = \left[\frac{a}{\pi}\right]_2 \cdot \left[\frac{b}{\pi}\right]_2$.
- In general, quadratic reciprocity will proscribe a relation between the value of $\left[\frac{\pi}{\lambda}\right]_2$ and $\left[\frac{\lambda}{\pi}\right]_2$ if λ and π 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.)

5.5.2 Quadratic Reciprocity in $\mathbb{Z}[i]$

- We now examine quadratic reciprocity in $\mathbb{Z}[i]$. Like in $\mathbb{Z}$ we restrict attention to odd primes, meaning primes of odd norm (i.e., not associate to $1+i$).
- As we might hope, the quadratic residue symbol in $\mathbb{Z}[i]$ is closely related to the Legendre symbol in $\mathbb{Z}$.
- Proposition (Residue Symbols in $\mathbb{Z}[i]$): If p is a prime congruent to 1 mod 4 in $\mathbb{Z}$ factoring as $\pi\overline{\pi}$ 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 $\left[\frac{\pi}{l}\right]_2 = \left(\frac{p}{l}\right)$.
  - Proof: If $\pi | a$ or $\pi | l$ 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 $\pi | p$, this implies $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{\pi}$, so by the above, we see $\left(\frac{a}{p}\right) \equiv \left[\frac{a}{\pi}\right]_2 \pmod{\pi}$.
  - 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 $\pi | 2$, which is clearly not the case.
  - The second statement follows in exactly the same way.
- Theorem (Quadratic Reciprocity in $\mathbb{Z}[i]$): If π and λ 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 π and λ 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 λ and π are integers in $\mathbb{Z}$, then the result is immediate from quadratic reciprocity in $\mathbb{Z}$.
  - If λ is an integer l (i.e., an integer prime congruent to 3 modulo 4), and π is not, then by the above propositions we have $\left[\frac{\pi}{l}\right]_2 = \left(\frac{N(\pi)}{l}\right)$ and $\left[\frac{l}{\pi}\right]_2 = \left(\frac{l}{N(\pi)}\right)$, and these are equal by quadratic reciprocity in $\mathbb{Z}$. By symmetry, the result also holds if π is an integer, and λ is not.
  - Now assume that both $\pi = a + bi$ and $\lambda = c + di$ are nonintegers, with $\pi\overline{\pi} = p$ and $\lambda\overline{\lambda} = l$ two integral primes congruent to 1 modulo 4.

- By quadratic reciprocity in $\mathbb{Z}$, first observe that $\left(\frac{c}{l}\right) = \left(\frac{l}{c}\right) = \left(\frac{c^2+d^2}{c}\right) = \left(\frac{d}{c}\right)^2 = +1$.
- Also notice that $pl = (a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 \equiv (ad-bc)^2 \pmod{ac+bd}$.
- Thus, pl is a square modulo $ac+bd$, so $\left(\frac{l}{ac+bd}\right) = \left(\frac{p}{ac+bd}\right)$. Equivalently, this says $\left(\frac{ac+bd}{l}\right) = \left(\frac{ac+bd}{p}\right)$ by quadratic reciprocity.
- Then $\left[\frac{\lambda}{\pi}\right]_2 = \left[\frac{a}{\pi}\right]_2^2 \left[\frac{c+di}{\pi}\right]_2 = \left[\frac{a}{\pi}\right]_2 \left[\frac{ac+adi}{\pi}\right]_2 = \left(\frac{a}{p}\right)\left[\frac{ac+adi-di\pi}{\pi}\right]_2 = \left[\frac{ac+bd}{\pi}\right]_2 = \left(\frac{ac+bd}{p}\right)$.
- By the same argument, we have $\left[\frac{\pi}{\lambda}\right]_2 = \left(\frac{ac+bd}{l}\right)$, 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 $\left[\frac{1+i}{\lambda}\right]_2 = \left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right)$.
  - Then $2p = (a+b)^2 + (a-b)^2$, so $\left(\frac{2p}{a+b}\right) = 1$. Hence $\left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right)$, so $\left[\frac{1+i}{\lambda}\right]_2 = \left(\frac{2}{a+b}\right)$.

5.5.3 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 π 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 $(\alpha^{(N(\pi)-1)/2} - 1) \cdot (\alpha^{(N(\pi)-1)/2} + 1) \equiv 0 \pmod{\pi}$.
  - But now notice that $N(\pi) - 1$ is actually divisible by 4: so we can factor the expression even further, as $(\alpha^{(N(\pi)-1)/4} - 1) \cdot (\alpha^{(N(\pi)-1)/4} + 1) \cdot (\alpha^{(N(\pi)-1)/4} + i) \cdot (\alpha^{(N(\pi)-1)/4} - i) \equiv 0$.
  - By unique factorization, this means $\alpha^{(N(\pi)-1)/4}$ is equivalent to one of 1, -1, i, $-i$ modulo π.

- Definition: If π 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 $\pi | \alpha$, and otherwise to be the unique value among $\{\pm 1, \pm i\}$ satisfying $\left[\frac{\alpha}{\pi}\right]_4 \equiv \alpha^{(N(\pi)-1)/4} \pmod{\pi}$.
  - This residue symbol detects fourth powers, similarly to how the quadratic residue symbol detects squares.
  - If u is a primitive root modulo π, then $\left[\frac{\alpha}{\pi}\right]_4 = +1$ precisely when α is a power of u^4, which is clearly equivalent to α being a fourth power modulo π.

- 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 π and λ are both primes in $\mathbb{Z}[i]$ congruent to 1 modulo $2+2i$, then $\left[\frac{\pi}{\lambda}\right]_4 = \left[\frac{\lambda}{\pi}\right]_4 \cdot (-1)^{\frac{N(\pi)-1}{4} \cdot \frac{N(\lambda)-1}{4}}$.
  - 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.)

5.5.4 Reciprocity Laws in $\mathbb{F}_p[x]$

- We close with some brief remarks about 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 an odd prime.
- 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 $\left[\frac{f}{g}\right]_2 \cdot \left[\frac{g}{f}\right]_2 = (-1)^{\frac{p-1}{2}(\deg f)(\deg g)}$.
  - 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 field theory and algebraic number theory.
- We can also generalize the quadratic residue symbol to discuss general dth powers.
  - As we have shown, if f is irreducible in $\mathbb{F}_p[x]$, then the collection of residue classes modulo f forms a finite field with $p^{\deg(f)}$ elements.
  - By Euler's theorem, every element has order dividing $p^{\deg(f)} - 1$, and so (since this field has a primitive root) the possible powers of interest are dth powers where d divides $p^{\deg(f)} - 1$.
- Definition: If f is a monic irreducible polynomial in $\mathbb{F}_p[x]$ and d is a divisor of $n = p^{\deg(f)} - 1$, we define the dth-power residue symbol $\left[\frac{a}{f}\right]_d$ to be 0 if f divides a, and otherwise it is the unique element of $\mathbb{F}_p$ such that $a^{(n-1)/d} \equiv \left[\frac{a}{f}\right]_d \pmod{f}$.
  - The dth-power residue symbol shares most of the same properties as the other residue symbols we have defined: for example, it is multiplicative in the top element, and $\left[\frac{a}{f}\right]_d = 1$ if and only if a is a nonzero dth power modulo f.
  - We emphasize that the value of the dth-power residue symbol is an element in $\mathbb{F}_p$, rather than a complex number. In general, the possible values of this residue symbol are the elements of order dividing d in $\mathbb{F}_p$.
- Here is the corresponding reciprocity law for the dth-power residue symbol:
- Theorem (dth-Power Reciprocity in $\mathbb{F}_p[x]$): Let p be an odd prime and f, g be monic irreducible polynomials of positive degrees in $\mathbb{F}_p[x]$. Then $\left[\frac{f}{g}\right]_d = \left[\frac{g}{f}\right]_d (-1)^{\frac{p-1}{d}(\deg f)(\deg g)}$.
  - As with quadratic reciprocity, the proof of the dth-power reciprocity law requires a few more advanced tools from field theory, so we will not give it here.
- As a closing remark for this chapter, we will say that there are many other generalizations of quadratic reciprocity, and one of the major motivating problems of algebraic number theory in the early 20th century was to find a way to unify all of these disparate statements.
  - For example, in addition to the quartic reciprocity law in $\mathbb{Z}[i]$ known to Gauss, there is also a cubic reciprocity law in $\mathbb{Z}[\omega] = \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ that was first proven by Eisenstein in 1844 (although it was likely known to Gauss).
  - These various reciprocity laws were generalized and extended by other mathematicians, such as Kummer (with Kummer reciprocity), Hilbert (using his definition of the Hilbert symbol), and Artin (with the general formulation of Artin reciprocity).

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