Math 3527 (Number Theory 1)

Lecture #31

Quadratic Reciprocity and Jacobi Symbols:

- Motivation for Quadratic Reciprocity
- Examples of Quadratic Reciprocity
- Jacobi Symbols

This material represents §5.3 + §5.4 from the course notes.

Legendre Symbols

Recall some basic properties of the Legendre symbol:

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 divides a.

Theorem (Euler's Criterion)

If p is an odd prime, then for any residue class a, it is true that $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

In particular, Euler's criterion implies that $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Quadratic Reciprocity Motivation, I

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, namely $a = -1$ we can also answer this question immediately.

Quadratic Reciprocity Motivation, II

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 $p \equiv 1$ (mod 4).

Quadratic Reciprocity Motivation, II

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 $p \equiv 1$ (mod 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 (when p is odd) we see immediately that -1 is a quadratic residue precisely when $p \equiv 1 \pmod 4$.

Quadratic Reciprocity Motivation, III

For other $a \neq \pm 1$ (or at least the ones that are not obvious squares like $a = 4$), it is much less clear when a will be a quadratic residue. Let's work out some examples with primes less than 50:

- For $a = 2$, a is a QR modulo 7, 17, 23, 31, 41, and 47, while a is an NR modulo 3, 5, 11, 13, 19, 29, 37, and 43.
- For $a = 3$, a is a QR modulo 11, 13, 23, 37, and 47, while a is an NR modulo 5, 7, 17, 19, 29, 31, 41, and 43.
- For $a = 5$, a is a QR modulo 11, 19, 29, 31, and 41, while a is an NR modulo 3, 7, 13, 17, 23, 37, 43, and 47.
- For $a = 7$, a is a QR modulo 3, 23, 31, 37, and 47, while a is an NR modulo 5, 11, 13, 17, 23, and 41.
- For $a = 13$, a is a QR modulo 3, 17, 23, and 29, while a is an NR modulo 5, 7, 11, 19, 31, 37, 41, and 47.

Quadratic Reciprocity Motivation, IV

We can see a few patterns in these results. The easiest one to spot is for $a = 5$:

- 5 is a quadratic residue mod 11, 19, 29, 31, and 41, while 5 is a quadratic nonresidue mod 3, 7, 13, 17, 23, 37, 43, and 47.
- Notice that 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.
- Another way of saying this is: the primes where 5 is a quadratic residue are all 1 or 4 mod 5, while the primes where 5 is a nonresidue are all 2 or 3 mod 5.
- Suspiciously, that 1 and 4 are the quadratic residues mod 5, while 2 and 3 are the nonresidues.
- This suggests searching for a similar pattern with a small modulus in the other examples.

Quadratic Reciprocity Motivation, V

We can identify a few other patterns now:

- 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, 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 $a = 5$.
- We can also 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.

Quadratic Reciprocity Motivation, VI

Some of the patterns are still elusive.

- It seems that we have found natural patterns for $a = 5$ and $a = 13$: for these two primes, it appears that a is a quadratic residue modulo p if and only if p is a quadratic residue modulo a.
- Another way of saying this is 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 yet found such a "reciprocity" relation for $a = 3$ and $a = 7$.

Quadratic Reciprocity Motivation, VII

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

- For $a = -3$, a is a QR modulo 7, 13, 19, 31, and 37, while a is an NR modulo 5, 11, 17, 23, 29, 41, and 47.
- We see here that the primes where a is a QR are all 1 mod 3, while the ones where a is an NR are all 2 mod 3.
- Notice that 1 is a quadratic residue modulo 3, and 2 is a quadratic nonresidue.
- For $a = -7$, a is a QR modulo 11, 23, 29, and 37, while a is an NR modulo 3, 5, 13, 17, 19, 31, 41, and 47.
- Again, we see a pattern: the primes where a is a QR are all 1, 2, or 4 mod 7, while the ones where a is an NR are all 3, 5, or 6 mod 7.
- Notice that the quadratic residues modulo 7 are 1, 2, and 4, while the nonresidues are 3, 5, and 6.

Quadratic Reciprocity Motivation, VIII: Are We Motivated Yet?

Let us summarize the information we have gathered so far:

- From $a = 5$, it seems $\left(\frac{5}{p}\right) = 1$ if and only if $\left(\frac{p}{5}\right) = 1$.
- From $a = 13$, it seems $\left(\frac{13}{p}\right) = 1$ if and only if $\left(\frac{p}{13}\right) = 1$.
- From $a = -3$, it seems $\left(\frac{-3}{p}\right) = 1$ if and only if $\left(\frac{p}{3}\right) = 1$.
- From $a = -7$, it seems $\left(\frac{-7}{p}\right) = 1$ if and only if $\left(\frac{p}{7}\right) = 1$.
- In each case, we have a "reciprocity relation" between the values of the two Legendre symbols $\left(\frac{p}{q}\right)$ and $\left(\frac{q}{p}\right)$.
- But the reciprocity relation appears to be different for the primes 5 and 13 versus the primes 3 and 7.

Quadratic Reciprocity Motivation, IX: Now 100% Motivated!

Based on our previous ideas of looking for simple congruence relations, notice 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.
- In the other case, where $p, q \equiv 3 \pmod 4$, 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 $\left(\frac{-1}{q}\right) = -1$, we can rewrite this relation as $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = -1$.

Quadratic Reciprocity, I

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

Quadratic Reciprocity, I

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

This is precisely Gauss's Law of Quadratic Reciprocity:

Theorem (Gauss's Law of 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).*

Quadratic Reciprocity, II

We can summarize a bit of the history of quadratic reciprocity:

- The law of quadratic reciprocity was stated (without proof) by Euler in 1783, and the first correct proof was given by Gauss in 1796.
- Gauss actually published six different proofs of quadratic reciprocity during his lifetime, and two more were found among his notes.
- Indeed, Gauss remarked on several occasions that this theorem was one of his favorite results; given Gauss's prodigious mathematical output, this is a very strong statement!

Most proofs of quadratic reciprocity are fairly technically involved, so we will not present the proof here (the proof takes about 3 full pages in the notes).

Quadratic Reciprocity, III

Example: Verify quadratic reciprocity for $p = 17$ and $q = 19$.

Quadratic Reciprocity, III

Example: Verify quadratic reciprocity for $p = 17$ 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.

Quadratic Reciprocity, IV

Example: Verify quadratic reciprocity for $p = 23$ and $q = 43$.

Quadratic Reciprocity, IV

Example: Verify quadratic reciprocity for $p = 23$ 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.

Quadratic Reciprocity, V

We will also note one additional "basic evaluation":

Proposition (2 and Quadratic Residues)

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 $p \equiv 3, 5 \pmod 8$.

Quadratic Reciprocity, V

We will also note one additional "basic evaluation":

Proposition (2 and Quadratic Residues)

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 $p \equiv 3, 5 \pmod 8$.

Examples:

- 2 is a quadratic residue modulo the primes 7, 17, 23, 31, 41, 47, 71, 73, ... , since these primes are all congruent to 1 or 7 mod 8.
- 2 is a quadratic nonresidue modulo the primes 3, 5, 11, 13, 19, 29, 37, 43, 59, 61, 67, ... , since these primes are all congruent to 3 or 5 mod 8.

Quadratic Reciprocity, VI

We can use quadratic reciprocity to give another method for computing Legendre symbols.

- The idea is that if we want to compute $\left(\frac{p}{q}\right)$ where $p < q$, then by invoking quadratic reciprocity we can equivalently calculate the value of $\left(\frac{q}{p}\right)$.
- 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.

Quadratic Reciprocity, VII

Example: Determine whether 31 is a quadratic residue modulo 47.

Quadratic Reciprocity, VII

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 $16 = 4^2$ is clearly a quadratic residue.
- Since the Legendre symbol evaluates to -1, 31 is not a quadratic residue modulo 47.

Quadratic Reciprocity, VIII

Example: Determine whether 357 is a quadratic residue mod 661.

Quadratic Reciprocity, VIII

Example: Determine whether 357 is a quadratic residue mod 661.

- We want to find $\left(\frac{357}{661}\right)$. 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 know $\left(\frac{357}{661}\right) = \left(\frac{3}{661}\right) \cdot \left(\frac{7}{661}\right) \cdot \left(\frac{17}{661}\right)$.
- Then we can evaluate each of those Legendre symbols separately using quadratic reciprocity, since 661 is a prime congruent to 1 (mod 4) and 3, 7, and 17 are all prime.

Quadratic Reciprocity, VIII

- This yields

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

- 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 is not a quadratic residue modulo 661.

Quadratic Reciprocity, IX

Although this procedure can be applied to evaluate Legendre symbols with arbitrarily large numbers, we run into several computational issues.

- Specifically, we need to factor the top number every time we "flip and reduce", since quadratic reciprocity for Legendre symbols only makes sense when both terms are primes.
- We also need to remove factors of 2 and -1 once we reduce, although this is much more trivial since we know the values of $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ for all primes p.

What we will do now is generalize the Legendre symbol to composite moduli, so as to provide a way around this issue of needing to factor the top number.

Jacobi Symbols, I

Here is our generalization of the Legendre symbol:

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.

Jacobi Symbols, II

Examples:

- We have $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = +1.$
- We have $\left(\frac{11}{45}\right) = \left(\frac{11}{3}\right)^2 \cdot \left(\frac{11}{5}\right) = (-1)^2 \cdot (+1) = -1.$
- We have $\left(\frac{77}{33}\right) = \left(\frac{77}{3}\right) \cdot \left(\frac{77}{11}\right) = (-1) \cdot 0 = 0.$
- We have $\left(\frac{91}{75}\right) = \left(\frac{91}{3}\right)^2 \cdot \left(\frac{91}{5}\right) = (+1)^2 \cdot (+1) = +1.$

Jacobi Symbols, III

Here are some properties of Jacobi symbols:

Proposition (Properties of Jacobi Symbols)

Suppose b and b' are positive odd integers and a, a' are integers. Then the following hold:

1. $\left(\frac{a}{b}\right)$ *is* $+1$, -1, *or* 0, *and it is* 0 *if and only if* $\gcd(a, b) > 1$.
2. *If a is a quadratic residue modulo b and is relatively prime to b, then* $\left(\frac{a}{b}\right) = +1$.
3. *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* $\left(\frac{a}{bb'}\right) = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$.

Jacobi Symbols, IV

Proofs:

1. $\left(\frac{a}{b}\right)$ is $+1$, -1, or 0, and it is 0 if and only if $\gcd(a, b) > 1$.
   - Proof: This is immediate from the properties of the Legendre symbol, since each Legendre symbol is always $+1$, -1, or 0
   - Furthermore, there is a 0 term if and only if one of the prime divisors of b also divides a.

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.

Jacobi Symbols, V

3. 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: Suppose $b = p_1 \cdots p_k$ and $b' = q_1 \cdots q_k$.
   - 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.
   - Also, $\left(\frac{a}{bb'}\right) = \left(\frac{a}{p_1}\right)_L \cdots \left(\frac{a}{p_k}\right)_L \left(\frac{a}{q_1}\right)_L \cdots \left(\frac{a}{q_k}\right)_L = \left(\frac{a}{b}\right) \cdot \left(\frac{a}{b'}\right)$ by definition of the Jacobi symbol.

Jacobi Symbols, VI

Item (2) in the Proposition 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 squares, 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.

Jacobi Symbols, VII

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.

Jacobi Symbols, VIII

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).

Quadratic Reciprocity for Jacobi, I

Our next main result is that the Jacobi symbol also obeys the law of quadratic reciprocity:

Theorem (Quadratic Reciprocity for Jacobi Symbols)

If $b = p_1 p_2 \cdots p_k$ is a product of odd primes and a is odd, then

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* $b \equiv 3 \pmod 4$.
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* $b \equiv 3, 5 \pmod 8$.
3. *If a and b are odd, relatively prime positive integers, then* $\left(\frac{a}{b}\right) \cdot \left(\frac{b}{a}\right) = (-1)^{(a-1)(b-1)/4}$.

Quadratic Reciprocity for Jacobi, II

We will not go into the details of these proofs, but they are essentially just applications of the definition of the Jacobi symbol in terms of the Legendre symbol.

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.

Quadratic Reciprocity for Jacobi, III

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

Quadratic Reciprocity for Jacobi, III

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.
- Thus, 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.
- Therefore, 247 is a quadratic nonresidue modulo 1009.

Quadratic Reciprocity for Jacobi, IV

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

Quadratic Reciprocity for Jacobi, IV

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

- We have

$$\begin{aligned}\left(\frac{1593}{2017}\right) &= \left(\frac{2017}{1593}\right) = \left(\frac{424}{1593}\right) \\ &= \left(\frac{2}{1593}\right)^3 \cdot \left(\frac{53}{1593}\right) = \left(\frac{53}{1593}\right) \\ &= \left(\frac{1593}{53}\right) = \left(\frac{3}{53}\right) \\ &= -\left(\frac{53}{3}\right) = -\left(\frac{2}{3}\right) = +1.\end{aligned}$$

- Since 2017 is prime, the Jacobi symbol is the same as the Legendre symbol, so 1593 is a quadratic residue modulo 2017.

Summary

We motivated the statement of the law of quadratic reciprocity, and illustrated the law using some examples.

We defined the Jacobi symbol and showed that it also obeys the law of quadratic reciprocity.

We described how to use Jacobi symbols to evaluate Legendre symbols using quadratic reciprocity.

Next (and final) lecture: Applications of Quadratic Reciprocity