Exploring Number Theory

A blog on elementary number theory

The Legendre symbol

Posted on November 28, 2015

The law of quadratic reciprocity is a beautiful result. It is also an excellent tool to answer the question: given an odd prime p, and given that a is an integer such that a and p are relatively prime, is a is a quadratic residue modulo p, in other words, is the equation $x^2 \equiv a \ (\text{mod} \ p)$ solvable? Using the law of quadratic reciprocity requires the evaluation of the Legendre symbol. The focus of this post is on the Legendre symbol as well as related concepts of quadratic residues and the law of quadratic residues. The versatility of the law of quadratic reciprocity is demonstrated with examples.

Quadratic Residues

The setting is that the modulus in question is an odd prime p. Consider an integer a such that a and p are relatively prime, i.e. having no common prime factor. The number a is said to be a quadratic residue modulo p if the equation $x^2 \equiv a \ (\text{mod} \ p)$ has an integer solution in x. Another way to say this is that a is a quadratic residue modulo p if there exists a square root of a modulo p (a square root would be a solution to the equation). If the integer a is not a quadratic residue modulo p, we say that a is a quadratic nonresidue modulo p. If the context is clear, the word quadratic can be omitted. We can then say a is a residue modulo p or a is a nonresidue modulo p.

Since every integer is congruent modulo p to one of the numbers in the set $\mathbb{Z}_p=\{0,1,2,\cdots,p-1\}$, the integers a can be considered from the set $\mathbb{Z}_p^*=\{1,2,\cdots,p-1\}$ (the non-zero elements of $\mathbb{Z}_p$).

Let's look at a quick example. Let $p=11$. Squaring each number in $\mathbb{Z}_{11}$ produces the set $\{0^2,1^2,2^2,\cdots,10^2\}$. Reducing modulo 11 produces the set $\{0,1,4,9,5,3\}$. Thus the integers 1, 3, 4, 5 and 9 are quadratic residues modulo 11. The square roots of each residue are the solutions to the equation $x^2 \equiv a \ (\text{mod} \ 11)$. For $a=3$, the solutions are x = 5 and 6. There are two square roots of 3 modulo 11, namely 5 and 6.

When the modulus is small, it is easy to find all quadratic residues simply by squaring all the numbers in $\mathbb{Z}_p^*$. The focus in this post is on how to use the law of quadratic reciprocity to determine whether a given a is a quadratic residue modulo a large odd prime p.

To check whether the integer a is a quadratic residue modulo an odd prime p, the most important idea, before considering the law of reciprocity, is to check the modular exponentiation $a^{(p-1)/2} \pmod p$. If the result is congruent to 1 modulo p, then a is a quadratic residue modulo p. If the result is congruent to -1 modulo p, then a is a quadratic nonresidue modulo p. This is called Euler's Criterion (proved here). For clarity, it is stated below.

Theorem 1 (Euler's Criterion)
Let p be an odd prime. Let a be an integer that is relatively prime to p. Then the integer a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1 \pmod p$. On the other hand, the integer a is a quadratic nonresidue modulo p if and only if $a^{(p-1)/2} \equiv -1 \pmod p$.

According to Euler's Criterion, the task of checking for the status of quadratic residue is a matter of performing a modular exponentiation. This can be done using software or a calculator for modular arithmetic. If so desired, the exponentiation can also be programmed using the fast powering algorithm.

Though Euler's Criterion (with a calculator for modular arithmetic) is a sure fire way for checking the status of quadratic residues, the law of quadratic reciprocity can simplify the task even further. As the examples below will show, checking the status of quadratic residues using the law of reciprocity may require no modular exponentiation at all and if exponentiation is required, it is of a much smaller size.

Euler's Criterion also gives us several basic facts about quadratic residues.

Theorem 2
Let p be an odd prime. The following properties are true:

- If a and b are both residues modulo p, then the product $a \times b$ is a residue modulo p.
- If If a and b are both nonresidues modulo p, then the product $a \times b$ is a residue modulo p.
- If a and b are such that one of them is a residue modulo p and the other is a nonresidue modulo p, then the product $a \times b$ is a nonresidue modulo p.

Theorem 2 says that the product of two integers of the same types (both residues or both nonresidues) is always a residue modulo the odd prime p. The product of two integers of different types is always a nonresidue modulo the odd prime p. The theorem follows from Euler's criterion and from the fact that $(ab)^{(p-1)/2} = a^{(p-1)/2} \times b^{(p-1)/2}$.

In arithmetic modulo a prime p, there exists a primitive root modulo p and that any primitive root generates by powering all the integers that are relatively prime to the modulus p. Let g be a primitive root modulo an odd prime p. It then follows that the quadratic residues modulo p are the even powers of g and the nonresidues are the odd powers of g. A related fact is that when p is an odd prime and when a and p are relatively prime, the equation $x^2 \equiv a \pmod p$ either has two solutions or has no solutions.

Theorem 3

Let g be a primitive root modulo an odd prime p. For any a that is relatively prime to p, the following is true:

- a is a quadratic residue modulo p if and only if a is of the form $a \equiv g^{2k} \pmod p$ for some positive integer k,
- a is a quadratic nonresidue modulo p if and only if a is of the form $a \equiv g^{2k+1} \pmod p$ for some positive integer k.
  (proved here)

Theorem 4

Let p be an odd prime. For any a that is relatively prime to p, the equation $x^2 \equiv a \pmod p$ either has two solutions or has no solutions (proved here).

Legendre Symbol

The law of quadratic reciprocity is stated using the Legendre symbol. For an odd prime p and for an integer a that is relatively prime to p, the symbol $\left(\frac{a}{p} \right)$ is defined as follows:

$$\left(\frac{a}{p} \right) = \begin{cases} \ \ 1 & \text{if } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

One obvious and important observation is that Euler's Criterion can be restated as follows:

Theorem 1a (Euler's Criterion)

Let p be an odd prime. Let a be an integer that is relatively prime to p. Then

$\left(\frac{a}{p} \right) \equiv a^{\frac{p-1}{2}} \pmod p$.

In the above definition, the lower argument of the Legendre symbol is always an odd prime and the upper argument is an integer that is relatively prime to the lower argument. To smooth out some statements involving the Legendre symbol and to make it easier to define the Jacobi symbol in the next post, we relax the Legendre symbol by making $\left(\frac{a}{p} \right) = 0$ whenever a and

p are not relatively prime, i.e. $a \equiv 0 \pmod{p}$. The Legendre symbol can be broaden slightly by the following:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \pmod{p} \\ 1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and } a \text{ is a quadratic residue modulo } p \\ -1 & \text{if } a \not\equiv 0 \pmod{p} \text{ and } a \text{ is a quadratic nonresidue modulo } p \end{cases}$$

Here’s some useful basic facts about the Legendre symbol.

Theorem 5
Let p be an odd prime. The following properties hold:

- The Legendre symbol is periodic with respect to the top argument, i.e. if $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
- The Legendre symbol is multiplicative with respect to the top argument, i.e. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \times \left(\frac{b}{p}\right)$.
- If $a \equiv 0 \pmod{p}$, then $\left(\frac{a^2}{p}\right) = 0$. If $a \not\equiv 0 \pmod{p}$, then $\left(\frac{a^2}{p}\right) = 1$.

The first bullet point in Theorem 5 is easily verified based on the definition of the Legendre symbol. For the case $a \equiv 0 \pmod{p}$, the other facts in Theorem 5 are easily verified. For the case $a \not\equiv 0 \pmod{p}$, the second bullet point follows from Theorem 2, i.e. the fact that the product of two residues and the product of two nonresidues are both residues modulo an odd prime and that the product of a residue and a nonresidue is a nonresidue modulo an odd prime. The second part of the third bullet point is true since any integer that is a square is a quadratic residue.

Law of Quadratic Reciprocity

The law of reciprocity can ease the calculation of the Legendre symbol when both the upper and lower arguments are distinct odd primes. Theorem 6 is the law of reciprocity and Theorem 7 and Theorem 8 are two supplements to the law that can round out the calculation. After stating the theorems, we demonstrate with some examples.

Theorem 6 (the law of quadratic reciprocity)

Let p and q be two distinct odd prime numbers. Both of the following statements hold.

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{(p-1)/2 \times (q-1)/2}$$

Equivalently and more explicitly,

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \pmod 4 \text{ or } q \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \pmod 4 \end{cases}$$

Theorem 7 (first supplement to the law of quadratic reciprocity)

Let p be an odd prime number. The following statement holds.

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$$

Theorem 8 (second supplement to the law of quadratic reciprocity)

Let p be an odd prime number. The following statement holds.

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \end{cases}$$

Theorem 6 shows how to flip the Legendre symbol if both the upper and lower arguments are distinct odd primes. As long as one of the primes is congruent to 1 modulo 4, we can safely flip the symbol. If both primes are not congruent to 1 modulo 4, we can still flip the symbol except that we have to attach a minus sign. Theorem 7 (the first supplement) indicates when -1 (or $p-1$) is a quadratic residue an odd prime p. In words, -1 is a residue modulo p if dividing p by 4 gives the remainder of 1. Otherwise -1 is a nonresidue modulo p. Theorem 8 (the second supplement) indicates when 2 is a residue modulo an odd prime p. In words, 2 is a residue modulo p if dividing p by 8 leaves a remainder of 1 or 7. Otherwise 2 is a nonresidue modulo p.

Examples

Example 1

Evaluate $\left(\frac{1783}{7523}\right)$, an example where both the upper and lower arguments in the Legendre symbol are primes.

$$\begin{aligned}
\left(\frac{1783}{7523}\right) &= -\left(\frac{7523}{1783}\right) \\
&= -\left(\frac{391}{1783}\right) \\
&= -\left(\frac{17}{1783}\right) \times \left(\frac{23}{1783}\right) \\
&= -\left(\frac{1783}{17}\right) \times (-1)\left(\frac{1783}{23}\right) \\
&= \left(\frac{15}{17}\right) \times \left(\frac{12}{23}\right) \\
&= \left(\frac{3}{17}\right) \times \left(\frac{5}{17}\right) \times \left(\frac{2}{23}\right)^2 \times \left(\frac{3}{23}\right) \\
&= \left(\frac{17}{3}\right) \times \left(\frac{17}{5}\right) \times \left(1\right)^2 \times (-1)\left(\frac{23}{3}\right) \\
&= -\left(\frac{2}{3}\right) \times \left(\frac{2}{5}\right) \times \left(\frac{2}{3}\right) \\
&= -\left(\frac{2}{5}\right) \\
&= -(-1) \\
&= 1
\end{aligned}$$

The above derivation is a repeated use of Theorems 5, 6 and 8. The idea is to flip the Legendre symbols to make the lower arguments smaller. Then reduce the upper arguments and then factor the upper arguments. Then flip again until reaching a Legendre symbol of $\left(\frac{2}{5}\right)$, which is easy to solve.

It then follows that 1783 is a quadratic residue modulo the odd prime 7523. The answer can be confirmed by using Euler’s Criterion. Note that $1783^{3761} \equiv 1 \pmod{7523}$. □

Example 2

Evaluate $\left(\frac{a}{p}\right)$ where $p =$ 1298351, an odd prime and $a =$ 756479.

The number a is not a prime and is factored as $a = 353 \times 2143$. We have the following derivation.

$$
\begin{aligned}
\left(\frac{756479}{1298351}\right) &= \left(\frac{353}{1298351}\right) \times \left(\frac{2143}{1298351}\right) \\
&= \left(\frac{1298351}{353}\right) \times (-1)\left(\frac{1298351}{2143}\right) \\
&= -\left(\frac{17}{353}\right) \times \left(\frac{1836}{2143}\right) \\
&= -\left(\frac{17}{353}\right) \times \left(\frac{2}{2143}\right)^2 \times \left(\frac{3}{2143}\right)^3 \times \left(\frac{17}{2143}\right) \\
&= -\left(\frac{353}{17}\right) \times \left(1\right)^2 \times (-1)\left(\frac{2143}{3}\right)^3 \times \left(\frac{2143}{17}\right) \\
&= \left(\frac{13}{17}\right) \times \left(\frac{1}{3}\right)^3 \times \left(\frac{1}{17}\right) \\
&= \left(\frac{17}{13}\right) \times \left(1\right)^3 \times \left(1\right) \\
&= \left(\frac{4}{13}\right) \\
&= 1
\end{aligned}
$$

The evaluation of the Legendre symbols in this example does not start with a flipping since the upper argument 756479 is not a prime. Instead, we start with factoring the upper argument into prime factors and then proceed with a series of flipping, reducing and factoring. □

Example 3

Evaluate $\left(\frac{a}{p}\right)$ where $p = 569$, an odd prime and $a = 1610280$.

$$
\begin{aligned}
\left(\frac{1610280}{569}\right) &= \left(\frac{3}{569}\right)^4 \times \left(\frac{5}{569}\right) \times \left(\frac{7}{569}\right) \times \left(\frac{568}{569}\right) \\
&= \left(\frac{569}{3}\right)^4 \times \left(\frac{569}{5}\right) \times \left(\frac{569}{7}\right) \times \left(\frac{-1}{569}\right) \\
&= \left(\frac{2}{3}\right)^4 \times \left(\frac{4}{5}\right) \times \left(\frac{2}{7}\right) \times \left(1\right) \\
&= \left(-1\right)^4 \times \left(1\right) \times \left(1\right) \\
&= 1
\end{aligned}
$$

This example can also be evaluated by first reducing 1610280 modulo 569. □

Comment

The law of quadratic reciprocity is a deep and powerful result. It guides the evaluation of Legendre symbols in an attempt to answer whether a number is a quadratic residue modulo an odd prime. The law of reciprocity as represented above requires that the lower argument in the Legendre symbol is an odd prime. When the upper argument is an odd number that is not a prime, there is no way to flip it (based on the law of reciprocity using the Legendre symbol). In

Example 2, the evaluation of the Legendre symbol cannot begin until the top argument is factored. The factoring in Example 2 is possible since the number is small. When the number is large, factoring may not always be feasible. It turns out that the Legendre symbol has a generalization, called the Jacobi symbol, that is even more versatile and is defined in the next post.

SHARE THIS:

Twitter Facebook

Like

Be the first to like this.

RELATED

Solving quadratic congruences with odd prime moduli
In "Applied"

The Jacobi symbol
In "Basic"

Quadratic Residues
In "Basic"

This entry was posted in **Basic**, **Prime Numbers** and tagged **Euler's Criterion**, **Jacobi Symbol**, **Legendre Symbol**, **Mathematics**, **Number Theory**, **Quadratic Reciprocity**, **Quadratic Residue** by **Dan Ma**. Bookmark the **permalink [https://exploringnumbertheory.wordpress.com/2015/11/28/the-legendre-symbol/]** .

4 THOUGHTS ON “THE LEGENDRE SYMBOL”

Pingback: The Jacobi symbol | Exploring Number Theory

Pingback: Solving quadratic congruences with odd prime moduli | Exploring Number Theory

Pingback: Fermat numbers | Exploring Number Theory

Pingback: Pepin’s Primality Test | Mathematical Cryptography