Quadratic Reciprocity Law

Preyarnsi Saikia

Indian Institute of Technology Delhi

1. Introduction & History

The Quadratic Reciprocity law or the 'Golden Theorem' is a result in Number Theory about modular arithmetic. The law was conjectured by Euler and Legendre and was first proved by Gauss. Later, Gauss gave seven more proofs of the Quadratic Reciprocity law. The best current count finds 246 proofs which makes this law one of the most proved results of Number Theory. The Law was also mentioned in David Hilbert's influential opening speech of the International Congress of Mathematicians in Paris in the year 1900 in which he outlined 23 major mathematical problems to lead mathematics in the coming century.

In 1640, Fermat was inspired by the book 'Diophantos' Arithmetica' to study about prime numbers which could be represented as the sum of two squares which induced the first complementary law of the Quadratic Reciprocity Theorem. Around 1741, Euler was led to the Quadratic Reciprocity law through his study of quadratic forms inspired by Fermat's investigations on primes p represented as $p = x^2 + Ny^2$ for $N = \pm 1, \pm 2, \pm 3$ with integers $x, y \in \mathbb{Z}$. Legendre was the first mathematician who gave a partial proof of the Law and coined the term 'Quadratic Reciprocity law'. His work on the Quadratic Reciprocity Law can be found in his two books: *Recherches d' Analyse Indeterminee (1785/88)* and *Essai sur la Theorie des Nombres (1798)*. In 1801 Gauss gave the first complete proof of the Quadratic Reciprocity Law in his treatise 'Disquisitiones Arithmeticae', where he, in fact, furnished two entirely different proofs. Altogether Gauss found 8 different proofs, six of which were published by him and two others were found after his death in his papers. For some background history, we refer to the article [1].

In this article, we will state and prove the quadratic reciprocity law and show some applications. We follow mainly the treatment given in Hardy and Wright's iconic textbook [2].

2. Definitions and Preliminary Lemmas

Definition 1. If p is an odd prime ($p \nmid a$), and x is one of the numbers $1, 2, 3, \ldots, p-1$. Then, one of the numbers $1.x, 2.x, \ldots, (p-1)x$ is congruent to $a \pmod p$. There is, therefore a unique x' such that $xx' \equiv a \pmod p$, $\quad 0 < x' < p$. Here, x' is the **associate** of x.

Definition 2. If the congruence

$$x^2 \equiv a \pmod p$$

has a solution $x = x_1$, we say that a **is a quadratic residue of** p and write $a\mathrm{R}p$.

Definition 3. If the congruence

$$x^2 \equiv a \pmod p$$

does not have a solution, we say that a **is a quadratic non-residue of** p and write $a\mathrm{N}p$.

Definition 4. Legendre's symbol $\left(\frac{a}{b}\right)$, where p is an odd prime and a is any number not divisible by p, is defined by

$$\left(\frac{a}{b}\right) = +1, \text{ if } a\mathrm{R}p,$$

$$\left(\frac{a}{b}\right) = -1, \text{ if } a\mathrm{N}p.$$

Definition 5. If p is an odd prime, there is just one residue of $n \pmod p$ between $-\frac{1}{2}p$ and $\frac{1}{2}p$. We call this residue the **minimal residue of** $n \pmod p$. It is positive or negative according as the least non-negative residue of n lies between 0 and $\frac{1}{2}p$ or between $\frac{1}{2}p$ and p.

Lemma 6. *If p is an odd prime and a is not a multiple of p, then*

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

Proof. Given, p is an odd prime and $p \nmid a$. If x' is the associate of x then there are two possibilities: either there is at least one x associated with itself, so that $x' = x$, or there is no such x.

Case 1: Suppose that the first alternative is true and that x_1 is associated with itself. In this case the congruence $x^2 \equiv a \pmod p$ has the solution $x = x_1$; and a is a quadratic residue of p. Plainly,

$$x = p - x_1 \equiv -x_1 \pmod p$$

is another solution of the congruence. Also, if $x' = x$ for any other value x_2 of x, we have

$$x_1^2 \equiv a, \;\; x_2^2 \equiv a, \quad (x_1 - x_2)(x_1 + x_2) = x_1^2 - x_2^2 \equiv 0 \pmod p.$$

Hence, either $x_1 \equiv x_2$ or $x_2 \equiv -x_1 \equiv p - x_1$; and there are just two solutions of the congruence, namely x_1 and $p - x_1$.

In this case the numbers

$$1, 2, \ldots, p-1$$

may be grouped as $x_1, p - x_1$, and $\frac{p-3}{2}$ pairs of unequal associated numbers. Now

$$x_1(p - x_1) \equiv -x_1^2 \equiv -a \pmod{p},$$

while

$$xx' \equiv a \pmod{p}$$

for any associated pair x, x'. Hence

$$(p-1)! = \prod x \equiv -a.a^{\frac{p-3}{2}} \equiv -a^{\frac{p-1}{2}} \pmod{p}.$$

Case 2: If the second alternative is true and no x is associated with itself, a is a quadratic non-residue of p. In this case, the congruence

$$x^2 \equiv a \pmod{p}$$

has no solution, and the numbers

$$1, 2, \ldots, p-1$$

may be arranged in $\frac{p-1}{2}$ associated unequal pairs. Hence

$$(p-1)! = \prod x \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Using the Legendre symbol, we can conclude the following

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

□

Lemma 7. ***Wilson's Theorem:*** *For a prime p, we have $(p-1)! \equiv -1 \pmod{p}$.*

Proof. $x^2 \equiv 1 \pmod{p}$ has the solutions $x = \pm 1$; hence 1 is a quadratic residue of p and

$$\left(\frac{1}{p}\right) = 1.$$

If we put $a = 1$ in Lemma 6, we get

$$(p-1)! \equiv -1 \pmod{p}.$$

□

Lemma 8. *If p is an odd prime and a is not a multiple of p, then*

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

Proof. From Wilson's Theorem, we have,

$$(p-1)! \equiv -1 \pmod{p}.$$

Applying Wilson's Theorem to Lemma 6, we get

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

which can be rewritten as

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

□

Lemma 9. ***Gauss's Lemma:*** *Let m be an integer such that $p \nmid m$, $\left(\frac{m}{p}\right) = (-1)^{\mu}$, where μ is the number of members of the set*

$$m, 2m, 3m, \ldots, \frac{p-1}{2}m,$$

whose least positive residues$(\text{mod } p)$ *are greater than* $\frac{p}{2}$.

Proof. Given, m is an integer such that $p \nmid m$. Consider the minimal residues of the $\frac{p-1}{2}$ numbers

$$m, 2m, 3m, \ldots, \frac{p-1}{2}m.$$

We can write these residues in the form

$$r_1, r_2, \ldots, r_\lambda, \quad -r'_1, -r'_2, \ldots, -r'_\mu, \tag{2.1}$$

where

$$\lambda + \mu = \frac{p-1}{2}, \quad 0 < r_i < \frac{p}{2}, \quad 0 < r'_i < \frac{p}{2}.$$

Since the numbers $m, 2m, 3m, \ldots, \frac{p-1}{2}m$ are incongruent, no two r can be equal, and no two r'. If an r and an r' are equal, say $r_i = r'_j$, let am, bm be the two of the numbers such that

$$am \equiv r_i \pmod{p}, \quad bm \equiv -r'_j \pmod{p}.$$

Then

$$am + bm \equiv 0 \pmod{p},$$

and so

$$a + b \equiv 0 \pmod{p},$$

which is impossible because $0 < a < \frac{p}{2}, 0 < b < \frac{p}{2}$. Thus, we can say that the numbers r_i, r'_j are a rearrangement of the numbers

$$1, 2, 3, \ldots, \frac{p-1}{2};$$

and therefore

$$\begin{aligned} m.2m.3m\ldots\frac{p-1}{2}m &\equiv (-1)^{\mu}1.2.3\ldots\frac{p-1}{2}\pmod{p} \\ m^{\frac{p-1}{2}} &\equiv (-1)^{\mu}\pmod{p}. \end{aligned}$$

From Lemma 8, we can write

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

Thus, we obtain,

$$\left(\frac{m}{p}\right) \equiv (-1)^{\mu}.$$

□

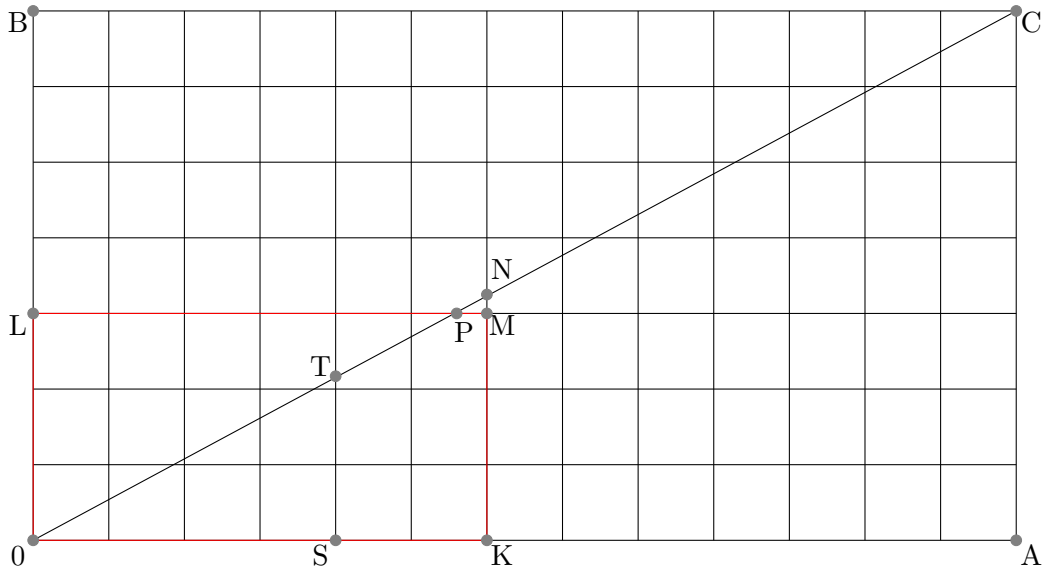
Lemma 10. *If p and q are odd primes and $p' = \frac{p-1}{2}$, $q' = \frac{q-1}{2}$ and*

$$S(p,q) = \sum_{s=1}^{p'} \left[\frac{sq}{p}\right],$$

then

$$S(p,q) + S(q,p) = p'q'.$$

Proof. We try to attempt the proof in a geometrical way. In the following figure, $AC = q, BC = p, KM = q', LM = p'$.



From the figure, we have $p > q$ and $\frac{q'}{p'} < \frac{q}{p}$ (as $q' < q$ and $p' < p$). Also, M falls below the

diagonal OC. Now,

$$\begin{aligned} \frac{q'}{p'} &< \frac{q}{p} \\ q' &< \frac{qp'}{p} \\ &= \frac{q}{p}\left(\frac{p-1}{2}\right) \\ &= \frac{q}{2} - \frac{1}{2} + \frac{1}{2} - \frac{q}{2p} \\ &= q' + \left(\frac{1}{2} - \frac{q}{2p}\right) \\ q' < \frac{qp'}{p} &< q' + 1. \end{aligned}$$

Thus, there is no integer between $KM = q'$ and $KN = \frac{qp'}{p}$. (From similarity of triangles OKN and OAC.)

We count the number of lattice points in the rectangle $OKML$ in two different ways. First, we count the points on KM and LM and find the number to be $p'q'$. There are no lattice points on OC (since p and q are primes) and none in the triangle PMN except perhaps on PM. Hence the number of lattice points in $OKML$ is the sum of those in the triangles OKN and OLP.

Number of lattice points on ST, the line $x = s$ is $\left[\frac{sq}{p}\right]$, as $\frac{sq}{p}$ is the ordinate of T (through similarity of triangles). Hence, the number in OKN is

$$\sum_{s=1}^{p'} \left[\frac{sq}{p}\right] = S(q, p).$$

Similarly, the number in OLP is $S(p, q)$ and the conclusion follows. □

3. The Quadratic Reciprocity Law

Theorem 11. *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'},$$

where $p' = \frac{p-1}{2}, q' = \frac{q-1}{2}$.

Proof. We can write,

$$kq = p\left[\frac{kq}{p}\right] + u_k, \tag{3.1}$$

where $1 \le k \le p'$, $1 \le u_k \le p - 1$.

Here u_k is the least positive residue of $kq \pmod p$. If $u_k = v_k \leq p'$, then u_k is one of the minimal residues r_i of the equation (2.1) in Gauss's Lemma, while if $u_k = w_k > p'$, then $u_k - p$ is one of the minimal residues $-r'_j$. Thus

$$r_i = v_k, \quad r'_j = p - w_k$$

for every i, j, and some k.

The r_i and r'_j (as we saw before) are the numbers $1, 2, \ldots, p'$ in some order. Hence, if

$$R = \sum r_i = \sum v_k, \quad R' = \sum r'_j = \sum (p - w_k) = \mu p - \sum w_k$$

(where μ is, as in Lemma 3.4, the number of the r'_j), we have

$$R + R' = \sum_{v=1}^{p'} v = \frac{1}{2}\frac{p-1}{2}\frac{p+1}{2} = \frac{p^2-1}{8},$$

and so

$$\mu p + \sum v_k - \sum w_k = \frac{1}{8}(p^2 - 1).$$

On the other hand, summing equation (3.1) from $k = 1$ to $k = p'$, we have

$$\frac{1}{8}q(p^2-1) = pS(q,p) + \sum u_k = pS(q,p) + \sum v_k + \sum w_k.$$

Subtracting the above two equations, we can deduce,

$$\frac{1}{8}(p^2-1)(q-1) = pS(q,p) + 2\sum w_k - \mu p.$$

Now $q - 1$ is even, and $p^2 - 1 \equiv 0 \pmod 8$ (as $p = 2n + 1$, so $p^2 - 1 = 4n(n + 1) \equiv 0 \pmod 8$); so that the left-hand side of the equation is even, and also the second term on the right. Hence (since p is odd)

$$S(p,q) \equiv \mu \pmod p,$$

and therefore, by Gauss's Lemma,

$$\left(\frac{q}{p}\right) = (-1)^{\mu} = (-1)^{S(q,p)}.$$

Finally,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S(q,p)+S(p,q)} = (-1)^{p'q'},$$

by Lemma 10. □

4. Applications

Lemma 12. *If p is an odd prime and $(p, 5) = 1$, then $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1$ or $4 \pmod 5$.*

Proof. By the Quadratic Reciprocity law, we have

$$\begin{aligned}\left(\frac{5}{p}\right) &= (-1)^{\frac{p-1}{2}\frac{5-1}{2}}\left(\frac{p}{5}\right)\\ &= (-1)^{p-1}\left(\frac{p}{5}\right)\\ &= \left(\frac{p}{5}\right)\end{aligned}$$

(as p is an odd prime). There are two quadratic residues of modulo 5 which are 1 and 4 and two quadratic non-residues 2 and 3. Thus,

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & if\ p \equiv 1\ or\ 4 \pmod 5 \\ -1 & if\ p \equiv 2\ or\ 3 \pmod 5. \end{cases}$$

Therefore, $\left(\frac{5}{p}\right) = 1$ if and only if $p \equiv 1$ or $4 \pmod 5$. □

Theorem 13. *There are infinitely many primes of the form* $5k + 4$.

Proof. Suppose there are finitely many primes congruent to 4 (mod 5), namely $p_1, p_2, \ldots, p_k$. Consider the number

$$N = (2p_1.p_2 \ldots p_k)^2 - 5.$$

First we claim that all prime divisors of N are congruent to 1 or 4 (mod 5). Let p be any prime divisor of N. Then $p \mid (2p_1.p_2 \ldots p_k)^2 - 5$ and $(2p_1.p_2 \ldots p_k)^2 \equiv 5 \pmod p$. Therefore, 5 is a quadratic residue mod p. By the previous lemma, $p \equiv 1$ or $4 \pmod 5$.

Next we claim that N has a prime divisor that is congruent to $p \equiv 4 \pmod 5$. If all the prime divisors of N are congruent to $1 \pmod 5$, as product of numbers of the form $5k + 1$ is also of the same form,

$$N \equiv 1 \pmod 5.$$

On the other hand, we know $p_i \equiv 4 \pmod 5$ for all i, so $p_i^2 \equiv 16 \equiv 1 \pmod 5$. Thus, $N = (2p_1.p_2 \ldots p_k)^2 - 5 \equiv 4 \pmod 5$, which is a contradiction. Therefore, there must be at least one odd prime p dividing N which is congruent to $4 \pmod 5$.

By assumption, $p_1, p_2, \ldots, p_k$ are all the primes congruent to $4 \pmod 5$. Then $p = p_i$ for some i. We have $p \mid N$ and $p \mid (2p_1.p_2 \ldots p_k)^2$, so $p \mid 5$, which is a contradiction. Hence, there are infinitely many primes $p \equiv 4 \pmod 5$. □

References

[1] Günther Frei. The reciprocity law from euler to eisenstein. In *The intersection of history and mathematics*. Springer, 1994.

[2] G. H. (Godfrey Harold) Hardy. *An Introduction to the Theory of Numbers*. Oxford mathematics. New York: Oxford University Press, 2008.