The quadratic reciprocity law and the Gauss–Schering lemma

Heng Huat Chan and Teoh Guan Chua

Abstract. In this article, we present a proof of the Gauss–Schering Lemma using the Quadratic Reciprocity Laws for the Jacobi symbol.

1. Introduction

Definition 1.1 (Legendre symbol). Let p be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)_L$ is defined to be

$$\left(\frac{a}{p}\right)_L = \begin{cases} 0 & \text{if } (a,p)\neq 1, \\ 1 & \text{if } x^2 \equiv a \pmod{p} \text{ is solvable}, \\ -1 & \text{otherwise.} \end{cases}$$

The main part of the famous Gauss's Law of Quadratic Reciprocity is the following.

Theorem 1.2 (Law of Quadratic Reciprocity). *If p and q are distinct odd primes then*

$$\left(\frac{p}{q}\right)_L \left(\frac{q}{p}\right)_L = (-1)^{(p-1)(q-1)/4}. \tag{1.1}$$

There are many proofs of (1.1) and several of these proofs involve a lemma, now known as Gauss's Lemma. Before we state Gauss's Lemma, we introduce some notations.

Let

$$\begin{aligned} r_n(s) &= \text{ the least non-negative residue of } s \text{ modulo } n, \\ H_n &= \{j | 1 \leqslant j \leqslant (n-1)/2\}, \\ S_{a,n} &= \{r_n(aj) | j \in H_n\}, \end{aligned}$$

and

$$\mu(a,n) = |\{s \in S_{a,n} | s \notin H_n\}|.$$

Gauss's Lemma gives a relation between the Legendre symbol and $\mu(a,p)$.

2020 *Mathematics Subject Classification.* Primary 11A15.

Lemma 1.3 (Gauss's Lemma). *Let p be an odd prime number and a be any positive integer such that $(a,p)=1$. Then*

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

A usual proof of Lemma 1.3 uses Euler's criterion which states that (see for example [**5**, p. 101, Corollary 2.38])

$$\left(\frac{a}{p}\right)_L \equiv a^{(p-1)/2} \pmod{p}. \tag{1.2}$$

Remark 1.4. Another proof of Gauss's Lemma which involves the "transfer map" in group theory can be found in [**10**, p. 91, Section 7.3].

The Legendre symbol has a natural extension to composite odd positive integers. It is now known as the Jacobi symbol.

Definition 1.5 (Jacobi symbol). Let a be any integer. The Jacobi symbol $\left(\frac{a}{b}\right)_J$ is defined for odd positive integer b by

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

if $b = \prod_{j=1}^{k} p_j^{\alpha_j}$.

Surprisingly, the Jacobi symbol satisfies a relation similar to (1.1).

Theorem 1.6 (Law of Quadratic Reciprocity for the Jacobi symbol). *If a and b are odd positive integers satisfying $(a,b)=1$, then*

$$\left(\frac{a}{b}\right)_J \left(\frac{b}{a}\right)_J = (-1)^{(a-1)(b-1)/4}. \tag{1.3}$$

Remark 1.7. The proof of (1.3) follows from (1.1) and requires only the simple congruence

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod{2},$$

where a and b are odd positive integers. See [**5**, p. 145] for more details.

Since the discovery of (1.3), there are proofs of (1.3) which are independent of (1.1). Two of the earliest published works on proving (1.3) directly are due to M. Jenkins [**3**] and E. Schering [**8**] (see also [**4**] for a modern treatment of Schering's work). Both Jenkins and Schering used a lemma analogous to Lemma 1.3 but Schering's version is an exact analogue of Lemma 1.3 with the prime p replaced by a composite odd positive integer b. As such, the following lemma is sometimes known as Gauss–Schering Lemma (see [**2**]).

Lemma 1.8 (Gauss–Schering Lemma). *Let b be a positive odd integer and a be any positive integer such that $(a,b)=1$. Then*

$$\left(\frac{a}{b}\right)_J = (-1)^{\mu(a,b)}.$$

The beauty of Lemma 1.8 is that it is exactly Lemma 1.3 with the prime p replaced by a composite odd positive integer b. The proofs of Lemma 1.3, however, cannot be adapted to prove Lemma 1.8. This is due to the fact that Euler's criterion (1.2) is false when the prime p is replaced by a composite odd integer n. Since (1.3) follows from (1.1), we would like to know if we could deduce Lemma 1.8 from (1.3). This will be discussed in the next section.

2. A proof of the Gauss–Schering Lemma

One of the proofs of (1.1) which is due to Eisenstein (see [**9**, p. 10]) uses the following trigonometric identity:

Lemma 2.1. *Let m be an odd positive integer. Then*

$$\frac{\sin mx}{\sin x} = (2i)^{m-1} \prod_{j\in H_m} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right). \tag{2.1}$$

Lemma 2.1 can be proved using the identity

$$x^m - 1 = \prod_{j=1}^{m} (x - \zeta_m^j),$$

where $\zeta_m = e^{4\pi i/m}$ where m is odd. By writing the identity in terms of the sine function, one arrives at the identity

$$\sin mx = (2i)^{m-1} \sin x \prod_{j=1}^{(m-1)/2} \sin(x - 2\pi j/m)\sin(x + 2\pi j/m)$$

and Lemma 2.1 follows by using the identity

$$\sin(a+b)\sin(a-b) = (\sin a + \sin b)(\sin a - \sin b).$$

We now use Lemma 2.1 to show the following:

Lemma 2.2. *Let a and b be odd positive integers such that $(a,b) = 1$. Then*

$$\prod_{s\in H_b} \frac{\sin(2as\pi/b)}{\sin(2s\pi/b)} = (-1)^{\mu(a,b)}.$$

Proof. Let

$$S_1 = \{s | s \in S_{a,b} \cap H_b\}$$

and

$$S_2 = \{b - s | s \in S_{a,b} \text{ but } s \notin H_b\}.$$

Note that $|S_2| = \mu(a,b)$.

If $s \in S_1$ then $\sin(2as\pi/m) = \sin(2u\pi/m)$ for some $u \in H_b$. If $s \in S_2$ then $\sin(2as\pi/m) = -\sin(2u\pi/m)$ for some $u \in H_b$. Note that since $S_1 \cup S_2 = H_b$,

$$\prod_{u\in H_b} \sin(2au\pi/b) = (-1)^{\mu(a,b)} \prod_{u\in H_b} \sin(2u\pi/b),$$

and this completes the proof of the lemma. □

Reversing the roles of a and b, we find by Lemma 2.2 that

$$\prod_{t\in H_a}\sin(2bt\pi/a)=(-1)^{\mu(b,a)}\prod_{t\in H_a}\sin(2t\pi/a).$$

By Lemma 2.1, we conclude that

$$\begin{aligned}(-1)^{\mu(a,b)+\mu(b,a)}&=(-1)^{\mu(a,b)-\mu(b,a)}=\prod_{s\in H_a}\prod_{t\in H_b}\frac{\sin^2(2s\pi/b)-\sin^2(2\pi t/a)}{\sin^2(2t\pi/a)-\sin^2(2s\pi/b)}\\&=(-1)^{(a-1)(b-1)/4}.\end{aligned}$$

By (1.3),

$$\left(\frac{a}{b}\right)_J\left(\frac{b}{a}\right)_J=(-1)^{(a-1)(b-1)/4}=(-1)^{\mu(a,b)+\mu(b,a)}. \tag{2.2}$$

We are now ready to prove Lemma 1.8. Let q be an odd prime and b be any positive odd integer such that $(b,q)=1$. Then by Lemma 1.3, we find that

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

By (2.2), we conclude that

$$\left(\frac{q}{b}\right)_J=(-1)^{\mu(q,b)}. \tag{2.3}$$

Next, suppose a is any odd positive integer. Since $(a,b)=1$, by the Dirichlet Theorem on primes in arithmetic progression (see for example [**1**, Chapter 7]), there exists a prime Q of the form $a+bn$. By (2.3),

$$\left(\frac{a}{b}\right)_J=\left(\frac{Q}{b}\right)_J=(-1)^{\mu(Q,b)}.$$

But $\mu(Q,b)=\mu(a,b)$ since $S_{Q,b}=S_{a,b}$ Therefore,

$$\left(\frac{a}{b}\right)_J=(-1)^{\mu(a,b)}$$

and the proof of Lemma 1.8 is complete.

3. Two representations of the Jacobi symbol

In this section, we mention two other representations of the Jacobi symbol. These representations were established in the literature to provide direct proofs of (1.3). We will deduce these representations from Lemma 1.8.

THEOREM 3.1. *Let $\lfloor x\rfloor$ denote the largest integer less than x, where x is any real number. Define*

$$s(a,b)=\sum_{j=1}^{(b-1)/2}\left\lfloor\frac{aj}{b}\right\rfloor$$

and

$$t(a,b)=\sum_{j=1}^{(b-1)/2}\left\lfloor\frac{2aj}{b}\right\rfloor.$$

If a and b are odd positive integers such that $(a,b)=1$, then

$$\left(\frac{a}{b}\right)_J = (-1)^{s(a,b)} \tag{3.1}$$

$$= (-1)^{t(a,b)}. \tag{3.2}$$

Proof. For each $j \in H_b$ and odd positive integer a, write

$$ja = q_j b + r_j \tag{3.3}$$

with $1 \leqslant r_j \leqslant b-1$. Rewrite ja as

$$ja = \begin{cases} q_j b + r_j & \text{if } r_j \in H_b, \\ q_j b + b - s_j & \text{if } r_j = b - s_j \notin H_b. \end{cases}$$

Note that $s_j \in H_b$ and that there are exactly $\mu(a,b)$ number of j such that $r_j \notin H_b$. Therefore,

$$\begin{aligned} a\sum_{j=1}^{(b-1)/2} j &\equiv b\sum_{j=1}^{(b-1)/2} q_j + b\mu(a,b) + \sum_{r_j\in H_b} r_j - \sum_{r_k\notin H_b} s_k \\ &\equiv \sum_{j=1}^{(b-1)/2} q_j + \mu(a,b) + \sum_{j=1}^{(b-1)/2} j \pmod 2, \end{aligned}$$

where in the last relation, we have used the fact that

$$\{r_j | r_j \in H_b\} \cup \{s_k | r_k = b - s_k \notin H_b\} = H_b$$

and

$$\sum_{r_j\in H_b} r_j - \sum_{r_k\notin H_b} s_k \equiv \sum_{r_j\in H_b} r_j + \sum_{r_k\notin H_b} s_k \pmod 2.$$

This implies that

$$\sum_{j=1}^{(b-1)/2} \left\lfloor \frac{aj}{b} \right\rfloor \equiv \mu(a,b) \pmod 2,$$

and hence

$$\left(\frac{a}{b}\right)_J = (-1)^{\mu(a,b)} = (-1)^{s(a,b)}. \tag{3.4}$$

This completes the proof of (3.1).

To prove (3.2), we return to (3.3) and write

$$2ja = \begin{cases} 2q_j b + 2r_j = \lfloor 2ja/b \rfloor b + 2r_j & \text{if } r_j \in H_b, \\ (2q_j+1)b + b - 2s_j = \lfloor 2ja/b \rfloor b + b - 2s_j & \text{if } r_j = b - s_j \notin H_b. \end{cases}$$

The second case holds since

$$b + 1 \leqslant 2r_j = 2b - 2s_j < 2b$$

implies that

$$2ja = (2q_j+1)b + b - 2s_j, 1 \leqslant b - 2s_j < b.$$

Hence

$$2a\sum_{j=1}^{(b-1)/2} j \equiv b\sum_{j=1}^{(b-1)/2} \left\lfloor \frac{2ja}{b} \right\rfloor + \sum_{r_j\in H_b} 2r_j + b\mu(a,b) + 2\sum_{r_j\notin H_b} s_j \pmod 2,$$

which implies that

$$\sum_{j=1}^{(b-1)/2} \left\lfloor \frac{2aj}{b} \right\rfloor \equiv \mu(a,b) \pmod 2$$

and the proof of (3.2) is complete. □

REMARK 3.2. The identity (3.2) appears in the work of H. Rademacher in his study of the Dedekind sum [**6**, p. 159]. Rademacher established (3.2) using the reciprocity relations satisfied by the Dedekind sum. He then proved (1.3) using (3.2).

There is another way of proving Lemma 1.8 without the use of (1.3) due to E. I. Zolotarev [**12**]. Zolotarev's proof took a different approach from Schering's proof. He defined

$$\left(\frac{a}{b}\right)_Z = \operatorname{sgn}(\lambda_a),$$

where λ_a is the permutation of $\mathbf{Z}/b\mathbf{Z}$ which sends $[x]_b$ to $[ax]_b$, and $\operatorname{sgn}(\sigma)$ is the "signum" of the permutation σ. Zolotarev then showed that for odd positive integers a and b satisfying $(a,b)=1$,

$$\left(\frac{a}{b}\right)_Z \left(\frac{b}{a}\right)_Z = (-1)^{(a-1)(b-1)/4}$$

and

$$\left(\frac{a}{b}\right)_Z = \left(\frac{a}{b}\right)_J.$$

For a modern treatment of Zolotarev's work, see [**7**] and [**11**].

References

[1] H. H. Chan, *Analytic number theory for undergraduates*, Monographs in Number Theory, vol. 3, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2009, DOI 10.1142/7252. MR2523579

[2] R. Hill, *Metaplectic covers of* GL_n *and the Gauss-Schering lemma* (English, with English and French summaries), J. Théor. Nombres Bordeaux **13** (2001), no. 1, 189–199. 21st Journées Arithmétiques (Rome, 2001). MR1838080

[3] M. Jenkins, *Proof of an Arithmetical Theorem leading, by means of Gauss's Fourth Demonstration of Legendre's Law of Reciprocity, to the extension of that Law*, Proc. Lond. Math. Soc. **2** (1866/69), 29–32, DOI 10.1112/plms/s1-2.1.29. MR1576676

[4] A. Kuroki and S.-i. Katayama, *A variation of Takagi's proof for quadratic reciprocity laws of Jacobi symbols*, J. Math. Univ. Tokushima **43** (2009), 9–23. MR2656202

[5] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991. MR1083765

[6] H. Rademacher, *Topics in analytic number theory*, Die Grundlehren der mathematischen Wissenschaften, Band 169, Springer-Verlag, New York-Heidelberg, 1973. MR364103

[7] G. Rousseau, *On the Jacobi symbol*, J. Number Theory **48** (1994), no. 1, 109–111, DOI 10.1006/jnth.1994.1057. MR1284879

[8] E. Schering, *Zur Theorie der Quadratischen Reste* (French), Acta Math. **1** (1882), no. 1, 153–170, DOI 10.1007/BF02391842. MR1554581

[9] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7, Springer-Verlag, New York-Heidelberg, 1973. Translated from the French. MR344216

[10] J.-P. Serre, *Finite groups: an introduction*, Surveys of Modern Mathematics, vol. 10, International Press, Somerville, MA; Higher Education Press, Beijing, 2016. MR3469786

[11] M. Szyjewski, *Zolotarev's proof of Gauss reciprocity and Jacobi symbols*, Serdica Math. J. **37** (2011), no. 3, 251–260. MR2951412

[12] E. I. Zolotarev. Nouvelle démonstration de la loi de réciprocité de Legendre. Nouv. Ann. Math (2) **11** (1872), 354–362.

Mathematical Research Center, Shandong University, No. 1 Building, 5 Hongjialou Road, Jinan, 250100, PR China
Email address: chanhh6789@sdu.edu.cn

Dept. of Mathematics, Ngee Ann Secondary School, Singapore, 529283, Singapore
Email address: teohguan.chua@gmail.com