*Bull. Aust. Math. Soc.* **108** (2023), 86–98
doi:10.1017/S0004972722001216

# AN AMAZING IDENTITY OF GAUSS AND JENKINS' LEMMA

HENG HUAT CHAN and SONG HENG CHAN✉

(Received 23 August 2022; accepted 16 September 2022; first published online 8 November 2022)

**Abstract**

We prove several finite product-sum identities involving the $q$-binomial coefficient, one of which is used to prove an amazing identity of Gauss. We then use this identity to evaluate certain quadratic Gauss sums and, together with known properties of quadratic Gauss sums, we prove the quadratic reciprocity law for the Jacobi symbol. We end our article with a new proof of Jenkins' lemma, a lemma analogous to Gauss' lemma. This article aims to show that Gauss' amazing identity and the properties of quadratic Gauss sums are sufficient to establish the quadratic reciprocity law for the Jacobi symbol.

2020 *Mathematics subject classification*: primary 11L05; secondary 11A07, 11A15.

*Keywords and phrases*: Gauss sum, Jacobi symbol, quadratic reciprocity law, cyclotomic unit.

## 1. Introduction

We begin with a short discussion on finite sum-product identities involving the $q$-binomial coefficient. We prove four such identities in Section 2, two of which are due to Gauss and are evaluations of special values of the Rogers–Szegö polynomials. The other two identities, (2.4) and (2.5), are possibly new.

In Section 3, we prove an amazing identity of Gauss (3.3) using (2.4).

In Section 4, we evaluate certain quadratic Gauss sums using identity (3.3). This proof is not new and we are essentially filling in the details of the proof given by Jenkins [6].

Next, in Section 5, we reproduce a proof of another identity on quadratic Gauss sums (5.1) which can be found in several classical textbooks. We chose to reproduce this proof and the proof of (3.3) to make this article as self-contained as possible. These two results then lead to a new proof of the quadratic reciprocity law for the Jacobi symbol.

Jenkins [6] gave a different proof of the quadratic reciprocity law for the Jacobi symbol using a formula for the Jacobi symbol. We will refer to Jenkins' formula, which is an analogue of Gauss' lemma, as Jenkins' lemma. In Section 6, we give a new proof of Jenkins' lemma using identities (3.3) and (5.1).

## 2. The $q$-binomial coefficient

Let $q$ be a complex variable. Let $(a;q)_0 = 1$ and

$$(a;q)_n = \prod_{k=1}^{n}(1 - aq^{k-1}), \quad n \in \mathbf{Z}^+.$$

The $q$-binomial coefficient is given by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{cases} \dfrac{(q;q)_n}{(q;q)_k(q;q)_{n-k}} & \text{if } n, k \text{ are integers}, 0 \le k \le n, \\ 0 & \text{otherwise.} \end{cases}$$

The Rogers–Szegö polynomial is defined by

$$h_n(x,q) = \sum_{j=0}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_q x^j.$$

We note that as $q \to 1$, $h_n(x,q) \to (1+x)^n$. However, $h_n(x,q)$ does not seem to have representations in terms of products except for a few special cases such as the two evaluations

$$h_{2n}(-1,q) = \sum_{j=0}^{2n} \begin{bmatrix} 2n \\ j \end{bmatrix}_q (-1)^j = (q;q^2)_n \tag{2.1}$$

and

$$h_n(q,q^2) = \sum_{j=0}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_{q^2} q^j = (-q;q)_n, \tag{2.2}$$

which were both discovered by Gauss.

Identities (2.1) and (2.2) were proved by Gauss [3, Sections 6–9] using recurrence relations. It turns out that these identities can also be established using Euler's identity [4, Theorem 349],

$$\sum_{j=0}^{\infty} \frac{x^j}{(q;q)_j} = \frac{1}{(x;q)_\infty}, \tag{2.3}$$

where

$$|q| < 1 \quad \text{and} \quad (a;q)_\infty = \prod_{k=1}^{\infty}(1 - aq^{k-1}).$$

Using (2.3), we find that

$$\Big(\sum_{k=0}^{\infty} \frac{(-x)^k}{(q;q)_k}\Big)\Big(\sum_{\ell=0}^{\infty} \frac{x^\ell}{(q;q)_\ell}\Big) = \frac{1}{(-x;q)_\infty}\frac{1}{(x;q)_\infty} = \frac{1}{(x^2;q^2)_\infty} = \sum_{n=0}^{\infty} \frac{x^{2n}}{(q^2;q^2)_n}.$$

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

Comparing the coefficients of $x^{2n}$,

$$\sum_{j=0}^{2n} \frac{(-1)^j}{(q;q)_j} \frac{1}{(q;q)_{2n-j}} = \frac{(q;q^2)_n}{(q;q)_{2n}},$$

which is equivalent to (2.1).

Similarly, by (2.3),

$$\Big(\sum_{k=0}^{\infty} \frac{(qx)^k}{(q^2;q^2)_k}\Big)\Big(\sum_{\ell=0}^{\infty} \frac{x^\ell}{(q^2;q^2)_\ell}\Big) = \frac{1}{(xq;q^2)_\infty} \frac{1}{(x;q^2)_\infty} = \frac{1}{(x;q)_\infty}$$
$$= \sum_{n=0}^{\infty} \frac{x^n}{(q;q)_n} = \sum_{n=0}^{\infty} \frac{(-q;q)_n}{(q^2;q^2)_n} x^n.$$

Comparing the coefficients of $x^n$,

$$\sum_{j=0}^{n} \frac{q^j}{(q^2;q^2)_j} \frac{1}{(q^2;q^2)_{n-j}} = \frac{(-q;q)_n}{(q^2;q^2)_n},$$

which is equivalent to (2.2).

There is a 'companion' of (2.3) [4, Theorem 348] given by

$$\sum_{j=0}^{\infty} \frac{q^{j(j-1)/2} x^j}{(q;q)_j} = \prod_{k=1}^{\infty} (1 + xq^{k-1}).$$

Since

$$\Big(\sum_{j=0}^{\infty} \frac{q^{j(j-1)/2}(-x)^j}{(q;q)_j}\Big)\Big(\sum_{j=0}^{\infty} \frac{q^{j(j-1)/2} x^j}{(q;q)_j}\Big) = \prod_{k=1}^{\infty} (1 - xq^{k-1})(1 + xq^{k-1})$$
$$= \prod_{k=1}^{\infty} (1 - x^2 q^{2k-2}) = \sum_{j=0}^{\infty} \frac{q^{j(j-1)}(-x^2)^j}{(q^2;q^2)_j},$$

we find, by comparing the coefficients of $x^{2n}$, that

$$\sum_{j=0}^{2n} \begin{bmatrix} 2n \\ j \end{bmatrix}_q (-1)^{n-j} q^{(n-j)^2} = (q;q^2)_n. \tag{2.4}$$

Similarly, since

$$\Big(\sum_{j=0}^{\infty} \frac{q^{j(j-1)}(qx)^j}{(q^2;q^2)_j}\Big)\Big(\sum_{j=0}^{\infty} \frac{q^{j(j-1)} x^j}{(q^2;q^2)_j}\Big) = \prod_{k=1}^{\infty} (1 + xq^{2k-2})(1 + xq^{2k-1})$$
$$= \prod_{k=1}^{\infty} (1 + xq^{k-1}) = \sum_{j=0}^{\infty} \frac{q^{j(j-1)/2} x^j}{(q;q)_j},$$

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

we find, by comparing the coefficients of $x^n$, that

$$\sum_{j=0}^{n} \begin{bmatrix} n \\ j \end{bmatrix}_{q^2} q^{(n-2j+1)(n-2j)/2} = (-q;q)_n. \tag{2.5}$$

## 3. Cyclotomic units and an identity of Gauss

It is known that if $(t,m)=1$, then $e^{2\pi it/m}$ is a primitive $m$th root of unity. We will use $\zeta_m$ to denote any primitive $m$th root of unity. It is often mentioned that as $q \to 1$,

$$\begin{bmatrix} n \\ k \end{bmatrix}_q \to \binom{n}{k},$$

the usual binomial coefficient. It is, however, more interesting to note that if we let $q=\zeta_{n+1}$, then

$$\begin{bmatrix} n \\ k \end{bmatrix}_{\zeta_{n+1}} = \prod_{j=1}^{k} \frac{1-\zeta_{n+1}^{n-j+1}}{1-\zeta_{n+1}^{j}} = \prod_{j=1}^{k} \frac{1-\zeta_{n+1}^{-j}}{1-\zeta_{n+1}^{j}} = \frac{(-1)^k}{\zeta_{n+1}^{k(k+1)/2}}. \tag{3.1}$$

This observation is due to Gauss [3, Section 12]. Using (3.1), Gauss deduced the following result from (2.1).

THEOREM 3.1. *Let $n$ be a positive integer and $(t,2n+1)=1$. Then,*

$$\sum_{j=0}^{2n} e^{2\pi itj^2/(2n+1)} = \prod_{k=1}^{n} (\zeta_{2n+1}^{2k-1} - \zeta_{2n+1}^{-(2k-1)}) \tag{3.2}$$

$$= (2i)^n \prod_{k=1}^{n} \sin\left(\frac{2t(2k-1)\pi}{(2n+1)}\right). \tag{3.3}$$

Instead of deducing (3.3) from (2.1) as Gauss did, we will now derive (3.3) from (2.4).

PROOF. Let $q=\zeta_{2n+1}$. From (2.4) and (3.1),

$$(-1)^n \sum_{j=0}^{2n} \frac{\zeta_{2n+1}^{(n-j)^2}}{\zeta_{2n+1}^{j(j+1)/2}} = \prod_{k=1}^{n} (1-\zeta_{2n+1}^{2k-1}). \tag{3.4}$$

Now if $\zeta_{2n+1}$ is a primitive $(2n+1)$th root of unity, then $\zeta_{2n+1}^2$ is also a primitive $(2n+1)$th root of unity. Therefore, we find from (3.4), after multiplying both sides by $(-1)^n$, that

$$\sum_{j=0}^{2n} \frac{\zeta_{2n+1}^{2(n-j)^2}}{\zeta_{2n+1}^{j(j+1)}} = \prod_{k=1}^{n} (\zeta_{2n+1}^{2(2k-1)} - 1).$$

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

This implies that

$$\zeta_{2n+1}^{-1-3-\cdots-2n-1}\sum_{j=0}^{2n}\zeta_{2n+1}^{2n^2+j^2-4nj-j}=\prod_{k=1}^{n}(\zeta_{2n+1}^{2k-1}-\zeta_{2n+1}^{-(2k-1)}).$$

Using the identity $1+3+\cdots+(2n-1)=n^2$ and the fact that $\zeta_{2n+1}^{-4nj-j}=\zeta_{2n+1}^{-2nj}$, we deduce that

$$\sum_{j=0}^{2n}\zeta_{2n+1}^{(n-j)^2}=\prod_{k=1}^{n}(\zeta_{2n+1}^{2k-1}-\zeta_{2n+1}^{-(2k-1)}).$$

Observing that

$$\sum_{j=0}^{2n}\zeta_{2n+1}^{(n-j)^2}=\sum_{j=0}^{2n}\zeta_{2n+1}^{j^2}$$

since the set of least nonnegative residues of $n-j$ modulo $2n$ for $0\le j\le 2n$ is $\{0,1,2,\dots,2n\}$, we deduce (3.2). Letting $\zeta_{2n+1}=e^{2\pi it/(2n+1)}$ with $(t,2n+1)=1$ and rewriting the right-hand side of (3.2) using $\sin x=(e^{ix}-e^{-ix})/2i$ completes the proof of (3.3). □

In a similar manner, from (2.2) and (3.1), we derive an analogue of (3.3), namely,

$$\sum_{j=0}^{n-1}(-1)^j e^{\pi ij^2/n}=e^{-\pi i(n-1)/4}2^{n-1}\prod_{k=1}^{n-1}\cos\frac{k\pi}{n}. \tag{3.5}$$

## 4. The quadratic Gauss sum

DEFINITION 4.1. Let $s$ and $t$ be positive integers. Define

$$g(s,t)=\sum_{j=0}^{t-1}e^{2\pi isj^2/t}.$$

The function $g(s,t)$ is sometimes referred to as the quadratic Gauss sum (see [1, page 177, Problem 16], [2, page 12]). It turns out that one can evaluate $g(1,m)$ for any odd positive integer $m$.

THEOREM 4.2. *Let $m$ be an odd positive integer. Then,*

$$g(1,m)=\sum_{j=0}^{m-1}e^{2\pi ij^2/m}=\begin{cases}\sqrt{m} & \text{if } m\equiv 1 \pmod 4,\\ i\sqrt{m} & \text{if } m\equiv 3 \pmod 4.\end{cases} \tag{4.1}$$
$$=i^{((m-1)/2)^2}\sqrt{m}.$$

Proofs of (4.1) can be found in many books. See [1, Ch. 9, Section 10] or [2, Lemma 1.2.1]. We will give a proof of Theorem 4.2 using (3.3). This proof is sketched in Jenkins' article [6].

We need the following lemma.

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

LEMMA 4.3. *Let $m$ be an odd positive integer. Then,*

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

Lemma 4.3 is a consequence of the identity

$$x^m - 1 = (x-1) \prod_{j=1}^{m-1} (x - \zeta_m^{2j}),$$

where we observed that $\{\zeta_m^j \mid 1 \le j \le (m-1)\} = \{\zeta_m^{2j} \mid 1 \le j \le (m-1)\}$ since $m$ is an odd positive integer and $\zeta_m^2$ is also a primitive $m$th root of unity.

PROOF OF THEOREM 4.2. Letting $x \to 0$ in Lemma 4.3, we deduce that

$$(-1)^{m-1}(2i)^{m-1} \prod_{j=1}^{m-1} \sin\left(\frac{2\pi j}{m}\right) = m.$$

This implies that

$$\left|(2i)^{m-1} \prod_{j=1}^{m-1} \sin\left(\frac{2\pi j}{m}\right)\right| = m. \tag{4.2}$$

Next, write

$$\begin{aligned}\prod_{j=1}^{m-1} \sin\left(\frac{2\pi j}{m}\right) &= \prod_{j=1}^{(m-1)/2} \sin\left(\frac{2\pi(2j-1)}{m}\right) \sin\left(\frac{2\pi(2j)}{m}\right) \\ &= (-1)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin\left(\frac{2\pi(2j-1)}{m}\right) \sin\left(\frac{2\pi(m-2j)}{m}\right) \\ &= (-1)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin^2\left(\frac{2\pi(2j-1)}{m}\right),\end{aligned}$$

where we have used $\sin y = -\sin(2\pi - y)$ in the second equality. By (4.2),

$$\left|(2i)^{(m-1)} \prod_{j=1}^{(m-1)/2} \sin^2\left(\frac{2\pi(2j-1)}{m}\right)\right| = m,$$

which implies that

$$(2i)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin\left(\frac{2\pi(2j-1)}{m}\right) = u_m \sqrt{m},$$

where $u_m$ is some power of $i$. By comparing both sides and using the fact that

$$\sin(2\pi(2j-1)/m) < 0 \quad \text{if } j > m/4 + 1/2,$$

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

we deduce immediately that if $m = 8k + 1$, then

$$u_m = i^{4k}(-1)^{2k} = 1.$$

Similarly, if $m = 8k + 3, 8k + 5$ and $8k + 7$, then $u_m = i, 1$ and $i$, respectively. Therefore,

$$(2i)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin\left(\frac{2\pi(2j-1)}{m}\right) = i^{((m-1)/2)^2}\sqrt{m}. \tag{4.3}$$

Substituting (4.3) into (3.3) with $t = 1$ and $m = 2n + 1$ completes the proof of Theorem 4.2. □

Trigonometric identities related to (4.3) can also be found in [9, Section 51].

COROLLARY 4.4. *Let $a$ and $b$ be two positive odd integers. Then,*

$$\frac{g(1, ab)}{g(1, a)g(1, b)} = (-1)^{(a-1)(b-1)/4}. \tag{4.4}$$

PROOF. From (4.1), we deduce that

$$\frac{g(1, ab)}{g(1, a)g(1, b)} = i^{((ab-1)/2)^2-((a-1)/2)^2-((b-1)/2)^2}.$$

Since

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

it follows that

$$\left(\frac{a-1}{2}\right)^2 + \left(\frac{b-1}{2}\right)^2 + \frac{(a-1)(b-1)}{2} - \left(\frac{ab-1}{2}\right)^2 \equiv 0 \pmod 4,$$

and this completes the proof of (4.4). □

Note that in (4.1), we evaluate the Gauss sum for odd positive integers. We end this section by giving an analogue of (4.1) for even positive integers, but with the corresponding Gauss sum 'weighted' by $(-1)^j$. Letting $x \to -1$ in the identity

$$\frac{x^{2n}-1}{x^2-1} = \prod_{\substack{j=1 \\ j\neq n,2n}}^{2n} (x - \zeta_{2n}^j),$$

gives

$$2^{n-1} \prod_{j=1}^{n-1} \cos\frac{\pi j}{2n} = \sqrt{n}. \tag{4.5}$$

Using (4.5) and (3.5), we deduce the following analogue of (4.1).

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

THEOREM 4.5. *If $n$ is any positive integer, then*

$$\sum_{j=0}^{n-1}(-1)^j e^{\pi i j^2/n} = e^{-\pi i(n-1)/4}\sqrt{n}.$$

## 5. The Jacobi symbol and the quadratic Gauss sum

DEFINITION 5.1. Let $p$ be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)_L$ is defined by

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

DEFINITION 5.2. The Jacobi symbol $\left(\frac{a}{b}\right)_J$ is defined for an odd positive integer $b$ by

$$\left(\frac{a}{b}\right)_J = \begin{cases} 1 & \text{if } b = 1, \\ \prod_{j=1}^{k}\left(\frac{a}{p_j}\right)_L^{\alpha_j} & \text{if } b = \prod_{j=1}^{k} p_j^{\alpha_j}. \end{cases}$$

We will write $\left(\frac{\cdot}{b}\right)$ to represent $\left(\frac{\cdot}{b}\right)_J$. Our aim is to prove the following theorem.

THEOREM 5.3. *Let $m$ be any positive odd integer and $a$ be an integer such that $(a,m) = 1$. Then,*

$$g(a,m) = \left(\frac{a}{m}\right) g(1,m). \tag{5.1}$$

Theorem 5.3 and its proof can be found in [2, Theorem 1.5.2]. The proof uses (4.1) and an automorphism $\sigma_m$ of the cyclotomic field $\mathbf{Q}(\zeta_k)$ which sends $\zeta_k$ to $\zeta_k^m$. The proof we present here follows closely the proof given in Hua's book [5, Section 7.5] and Lang's book [8, Ch. 4, Section 3]. We will prove two lemmas before proving Theorem 5.3.

Let $a$ and $b$ be two relatively prime positive integers. The Chinese remainder theorem implies that if an arithmetic function $f(j)$ satisfies $f(j+ab) = f(j)$, then

$$\sum_{j=0}^{ab-1} f(j) = \sum_{h=0}^{a-1}\sum_{k=0}^{b-1} f(ak+bh).$$

Now, since for any positive integer $c$, the function $e^{2\pi i c j^2/ab}$ is a function of $j$ with period $ab$, we find that

$$\begin{aligned} g(c,ab) &= \sum_{j=0}^{ab-1} e^{2\pi i c j^2/(ab)} = \sum_{h=0}^{a-1}\sum_{k=0}^{b-1} e^{2\pi i c(ak+bh)^2/(ab)} \\ &= \sum_{h=0}^{a-1} e^{2\pi i c b h^2/a} \sum_{k=0}^{b-1} e^{2\pi i c a k^2/b} = g(cb,a)g(ca,b). \end{aligned}$$

This yields the first lemma.

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

LEMMA 5.4. *Let $a, b$ and $c$ be positive integers with $(a, b) = 1$. Then,*

$$g(ca, b)g(cb, a) = g(c, ab).$$

Our next task is to establish the second lemma, which is a special case of Theorem 5.3.

LEMMA 5.5. *Let $a$ be any integer, $\alpha$ be any positive integer and $p$ be an odd prime with $(a, p) = 1$. Then,*

$$g(a, p^\alpha) = \left(\frac{a}{p^\alpha}\right) g(1, p^\alpha). \tag{5.2}$$

PROOF. For $\alpha = 1$, we observe that if $(j, p) = 1$, then

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

Note that we may then write

$$\begin{aligned} g(a, p) &= \sum_{j=0}^{p-1} e^{2\pi i a j^2/p} = 1 + 2 \sum_{j=1}^{(p-1)/2} e^{2\pi i a j^2/p} \\ &= 1 + 2 \sum_{\ell=1}^{p-1} \frac{1}{2}\left(1 + \left(\frac{\ell}{p}\right)\right) e^{2\pi i a \ell/p} \\ &= 1 + \sum_{\ell=1}^{p-1} e^{2\pi i a \ell/p} + \sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right) e^{2\pi i a \ell/p}. \end{aligned} \tag{5.3}$$

Now, since

$$1 + \sum_{\ell=1}^{p-1} e^{2\pi i a \ell/p} = 0 \tag{5.4}$$

and

$$\sum_{\ell=1}^{p-1} \left(\frac{\ell}{p}\right) e^{2\pi i a \ell/p} = \sum_{\ell=1}^{p-1} \left(\frac{a^2 \ell}{p}\right) e^{2\pi i a \ell/p} = \left(\frac{a}{p}\right) \sum_{\ell=1}^{p-1} \left(\frac{a\ell}{p}\right) e^{2\pi i a \ell/p}, \tag{5.5}$$

we conclude from (5.3), (5.4) and (5.5) that

$$g(a, p) = \left(\frac{a}{p}\right) g(1, p)$$

and (5.2) is true for $\alpha = 1$. We will next show that (5.2) is true for $\alpha = 2$. We will first show that

$$g(a, p^\alpha) = p g(a, p^{\alpha-2}).$$

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

This follows from the fact that the set of integers $\{0, 1, \ldots, p^\alpha - 1\}$ can be written as $\{s + tp^{\alpha-1} \mid 0 \le s \le p^{\alpha-1} - 1, 0 \le t \le p - 1\}$. Therefore,

$$\begin{aligned} g(a, p^\alpha) &= \sum_{s=0}^{p^{\alpha-1}-1} \sum_{t=0}^{p-1} e^{2\pi i a(s+tp^{\alpha-1})^2/p^\alpha} \\ &= \sum_{s=0}^{p^{\alpha-1}-1} e^{2\pi i a s^2/p^\alpha} \sum_{t=0}^{p-1} e^{4\pi i a s t/p} \\ &= p \sum_{\substack{s=0 \\ p|s}}^{p^{\alpha-1}-1} e^{2\pi i a s^2/p^\alpha} = p g(a, p^{\alpha-2}). \end{aligned}$$

If we follow the above argument with $\alpha = 2$, we conclude that $g(a, p^2) = p$, which means that $g(a, p^2)$ is independent of $a$ and we may write

$$g(a, p^2) = \left(\frac{a}{p^2}\right) g(1, p^2),$$

which is (5.2) for $\alpha = 2$.

Suppose (5.2) is true for all $1 \le k < \alpha$. Then,

$$g(a, p^\alpha) = p g(a, p^{\alpha-2}) = p\left(\frac{a}{p^{\alpha-2}}\right) g(1, p^{\alpha-2}) = \left(\frac{a}{p^\alpha}\right) g(1, p^\alpha). \qquad \square$$

We are now ready to prove Theorem 5.3.

PROOF OF THEOREM 5.3. Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. We prove the theorem by induction on $k$. Write $m = m' p_k^{\alpha_k}$. Then, by Lemma 5.4,

$$\begin{aligned} g(a, m) &= g(a, m' p_k^{\alpha_k}) = g(am', p_k^{\alpha_k}) g(a p_k^{\alpha_k}, m') \\ &= \left(\frac{am'}{p_k^{\alpha_k}}\right) g(1, p_k^{\alpha_k}) \left(\frac{a p_k^{\alpha_k}}{m'}\right) g(1, m') \\ &= \left(\frac{a}{m' p_k^{\alpha_k}}\right) \left(\frac{m'}{p_k^{\alpha_k}}\right) g(1, p_k^{\alpha_k}) \left(\frac{p_k^{\alpha_k}}{m'}\right) g(1, m') \\ &= \left(\frac{a}{m}\right) g(m', p_k^{\alpha_k}) g(p_k^{\alpha_k}, m') = \left(\frac{a}{m}\right) g(1, m). \end{aligned}$$

$\square$

We are now ready to prove the main part of the quadratic reciprocity law for the Jacobi symbol.

THEOREM 5.6. *Let $a$ and $b$ be two positive odd integers with $(a, b) = 1$. Then,*

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

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

PROOF. Note that by Theorem 5.3, Lemma 5.4 and Corollary 4.4,

$$\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = \frac{g(a,b)g(b,a)}{g(1,b)g(1,a)} = \frac{g(1,ab)}{g(1,b)g(1,a)} = (-1)^{(a-1)(b-1)/4}. \qquad \square$$

REMARK 5.7. Theorem 5.6 and all the identities for the quadratic Gauss sum leading up to (5.1) are known results that appear at different places in [5, 8]. We have seen here that these topics are connected via Gauss' amazing identity (3.3).

## 6. Jenkins' lemma

The proof of Theorem 5.6 given in the previous section is inspired by Jenkins [6]. Jenkins' proof involves (3.3), (4.1) but not (5.1). Instead, Jenkins uses a lemma analogous to a generalisation of Gauss' lemma. We now state Jenkins' lemma.

DEFINITION 6.1. For positive integers $N$ and $a$, let $r_N(a)$ denote the least nonnegative residue of $a$ modulo $N$.

LEMMA 6.2. *Let $m$ be an odd positive integer and $a$ be any integer with $(a,m)=1$. Let $S = \{2j-1 \mid 1 \le j \le (m-1)/2\}$. Let $T = \{r_m(a(2j-1)) \mid 1 \le j \le (m-1)/2\}$ and $\nu(a,m)$ be the number of integers in $T$ but not in $S$. Then,*

$$\left(\frac{a}{m}\right) = (-1)^{\nu(a,m)}.$$

We observe that $\nu(a,m)$ counts the number of even integers in $T$. We now give a proof of Lemma 6.2 as a corollary of (3.3) and (5.1).

PROOF. From (3.3), we deduce that

$$\begin{aligned} g(a,m) &= (2i)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin(2\pi a(2j-1)/m) \\ &= (-1)^{\nu(a,m)}(2i)^{(m-1)/2} \prod_{j=1}^{(m-1)/2} \sin(2\pi(2j-1)/m) \qquad (6.1) \\ &= (-1)^{\nu(a,m)} g(1,m), \end{aligned}$$

where we use that the fact that a 'minus' sign is introduced when $r_m(a(2j-1))$ is even, which explains the appearance of $(-1)^{\nu(a,m)}$ on the right-hand side of (6.1). The proof is completed by using (5.1). $\square$

The proof of Lemma 6.2 in the case when $m = p$ is an odd prime is easier and similar to the proof of Gauss' lemma, which states that if $S' = \{j \mid 1 \le j \le (p-1)/2\}$, $T' = \{r_p(aj) \mid 1 \le j \le (p-1)/2\}$ and $\nu'(a,p)$ is the number of integers in $T'$ that are not in $S'$, then

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

For completion, we will state this special case and give a direct proof.

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

LEMMA 6.3. *Let $p$ be an odd prime and $a$ be any integer with $(a, p) = 1$. Let*

$$S = \{2j - 1 \mid 1 \le j \le (p-1)/2\}, \quad T = \{r_p(a(2j-1)) \mid 1 \le j \le (p-1)/2\}$$

*and $\nu(a, p)$ be the number of integers in $T$ but not in $S$. Then,*

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

PROOF. Let $\nu = \nu(a, p)$,

$$E = \{t \mid t \in T \text{ is even}\} = \{e_1, e_2, \ldots, e_\nu\}$$

and

$$O = \{t \mid t \in T \cap S\} = \{o_1, o_2, \ldots, o_{(p-1)/2-\nu}\}.$$

Let $O' = \{p - e \mid e \in E\}$. We claim that $O \cup O' = S$. First note that all integers in $O$ are distinct. For if $as \equiv as' \pmod p$ with $s, s' \in S$, then $s = s'$. Similarly, all integers in $E$ are distinct. Next, suppose $o = p - e \in O \cap O'$ for some $o \in O$ and $e \in E$. Suppose $o = as$ and $e = as'$ for some $s, s' \in S$. Then, $as \equiv p - as' \pmod p$, which implies that $s + s' \equiv 0 \pmod p$. This implies that $s + s' = 0$ since $s, s'$ are odd positive integers less than $p - 2$. However, these are both impossible because $s + s' > 0$. Thus, $O \cup O' = S$ and therefore,

$$1 \cdot 3 \cdots (p-2) \equiv a^{(p-1)/2}(-1)^{\nu(a,p)}(1 \cdot 3 \cdots (p-2)) \pmod p,$$

which implies that

$$a^{(p-1)/2} \equiv (-1)^{\nu(a,p)} \pmod p$$

and the proof is completed using Euler's criterion [1, Theorem 9.2]. □

REMARK 6.4. The generalisation of Lemma 6.3 is an analogue of the Gauss–Schering lemma [10], which is a generalisation of Gauss' lemma with the prime $p$ replaced by any odd positive integer $m$ and the Legendre symbol replaced by the Jacobi symbol. Kuroki and Katayama [7] showed that if we replace $S$ and $S'$ by any set $S^*$ such that $S^* \subset \{j \mid 1 \le j \le (m-1)\}$ with $|S^*| = (m-1)/2$ and define $T^* = \{r_m(as) \mid s \in S^*\}$, then

$$\left(\frac{a}{m}\right) = (-1)^{\nu^*(a,m)},$$

where $\nu^*(a, m)$ is the number of integers in $T^*$ but not in $S^*$.

REMARK 6.5. We observe that (5.1) follows from Jenkins' lemma and (6.1), namely,

$$g(a, m) = (-1)^{\nu(a,m)} g(1, m) = \left(\frac{a}{m}\right) g(1, m).$$

In other words, if we know Jenkins' lemma (see [6] for a proof), then we have a new proof of (5.1).

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press

## Acknowledgement

The authors would like to thank the referee for their invaluable suggestions.

## References

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Undergraduate Texts in Mathematics (Springer-Verlag, New York–Heidelberg, 1976).
[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums* (John Wiley, New York, 1998).
[3] C. F. Gauss, 'Summatio quarumdam serierum singularium', *Comment. Soc. Reg. Sci., Gottsingensis* **1** (1811), 40 pages.
[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th edn (Oxford University Press, Oxford, 1988).
[5] L. K. Hua, *Introduction to Number Theory* (Springer-Verlag, Berlin–Heidelberg, 1982).
[6] M. Jenkins, 'Proof of an arithmetical theorem leading, by means of Gauss' fourth demonstration of Legendre's law of reciprocity, to the extension of that law', *Proc. Lond. Math. Soc. (3)* **2** (1867), 29–32.
[7] A. Kuroki and S.-i. Katayama, 'A variation of Takagi's proof for quadratic reciprocity laws of Jacobi symbols', *J. Math. Tokushima Univ.* **43** (2009), 9–23.
[8] S. Lang, *Algebraic Number Theory* (Springer-Verlag, New York, 1986).
[9] T. Nagell, *Introduction to Number Theory* (John Wiley & Sons, New York, 1951).
[10] E. Schering, 'Zur Theorie der quadratischen Reste', *Acta Math.* **1** (1882), 153–170; Werke II, 69–86.

HENG HUAT CHAN, Department of Mathematics,
National University of Singapore, Singapore 119076, Republic of Singapore
e-mail: matchh@nus.edu.sg

SONG HENG CHAN, Division of Mathematical Sciences,
School of Physical and Mathematical Sciences, Nanyang Technological University,
21 Nanyang link, Singapore 637371, Republic of Singapore
e-mail: chansh@ntu.edu.sg

https://doi.org/10.1017/S0004972722001216 Published online by Cambridge University Press