J. Math. Univ. Tokushima
Vol. 43 (2009), 9–23

A Variation of Takagi's Proof for Quadratic Reciprocity Laws of Jacobi Symbols

By

Arata KUROKI and Shin-ichi KATAYAMA

Tokushima Prefectural Senior High School
of Science and Technology,
Tokushima 770-0006, JAPAN
and
Department of Mathematical Sciences,
Faculty of Integrated Arts and Sciences,
The University of Tokushima, Tokushima 770-8502, JAPAN

e-mail address : *tokushima-hst@mt.tokushima-ec.ed.jp*
: *katayama@ias.tokushima-u.ac.jp*

(Received September 30, 2009)

Abstract

It is well known that Gauss has found the first complete proof of quadratic reciprocity laws in [2] (1801) and many different proofs for quadratic reciprocity laws of *Legendre symbols* have been published after then (see for example Appendix B of Lemmermeyer's text [11]). In this paper, we shall write down a visual proof of quadratic reciprocity laws for *Jacobi symbols* depending on Schering's generalization of Gauss's lemma.

2000 Mathematics Subject Classification. Primary 11A15; Secondary 11A07

Introduction

As we have remarked in the above abstract, it was Gauss who firstly gave a complete proof of quadratic reciprocity laws in [2] (1801). He has published 6

different proofs, and two more unpublished proofs (see Werke II [4] 233-234). It is also remarked that there have been published over 200 proofs for quadratic reciprocity laws of *Legendre symbols* after Gauss's first proof. We also note that Gauss has already extended quadratic reciprocity laws for prime values p, q to composite values in [2] art 133, implicitly. On the other hand, the definition of *Jacobi symbol* $\left(\frac{m}{n}\right)$ for an odd positive integer n was firstly introduced in Jacobi's paper [6] in 1837 as follows:

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)\left(\frac{m}{p_2}\right)\cdots\left(\frac{m}{p_r}\right),$$

where n is decomposed into odd primes $n = p_1 p_2 \cdots p_r$. This definition does not suggest any relation to the number of the integer points in certain regions as in the case of Legendre symbols. It was 1883, E. Schering has published a proof of Gauss's lemma for the odd positive integer n, in which he has shown a relation between the Jacobi symbols and the number of lattice points in some region. Therefore one can easily see any proof depending on Gauss's lemma for prime values which works for Legendre symbols also works for Jacobi symbols. In his master thesis [10], the first author has shown that Takagi's proof for quadratic reciprocity laws for Legendre symbols also works for quadratic reciprocity laws of Jacobi symbols. Though it is only a slight modification of Takagi's proof, we could not find any article which write down these procedures explicitly. Therefore we have decided to write down these procedures here.

Let $n(>1)$ be any odd positive integer. Let S be the set of all the half system mod n. Let $(\mathbf{Z}/n\mathbf{Z})^\times$ be the reduced residue class group mod n. Then the group $(\mathbf{Z}/n\mathbf{Z})^\times$ acts on S in a natural way.

In section 1, we shall investigate fundamental properties of the action of $(\mathbf{Z}/n\mathbf{Z})^\times$ on the set of all the half systems S. In section 2, we shall recall Schering's proof of generalized Gauss's lemma. In section 3, we shall give a visual proof of Jacobi symbols which is a variation of Takagi's proof of quadratic reciprocity laws of Legendre symbols. Though these procedures are well known for specialists it will be of some interest, because, as we noticed as above, the article writing these procedures explicitly seems very rare in these days.

1. Properties of Half Systems

Let m, n be odd positive integers. In this section, we shall study fundamental properties of half systems. We shall abbreviate the residue class (a mod n) by $\overline{a}$. We shall denote $n_1 = (n-1)/2$. Then the usual Gauss's half system mod n H_0 is defined by putting

$$H_0 = \{\overline{1}, \overline{2}, \ldots, \overline{n_1} = \overline{(n-1)/2}\}.$$

Let $(\mathbf{Z}/n\mathbf{Z})^\times$ be the reduced residue class group mod n. Then $(\mathbf{Z}/n\mathbf{Z})^\times$ acts on $\mathbf{Z}/n\mathbf{Z}$ as follows.

For arbitrary $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^\times$ and any subset $X \subset \mathbf{Z}/n\mathbf{Z}$, we denote $aX = \{\overline{ax} \mid \overline{x} \in X\}$. We note that $\overline{0}$ is stable under the action of $(\mathbf{Z}/n\mathbf{Z})^\times$. We shall denote $(\mathbf{Z}/n\mathbf{Z})^\times$−orbit $\mathbf{Z}/n\mathbf{Z} - \overline{0}$ by $F(n)$. Then the number of elements in Gauss's half system H_0 is exactly the half of the number of elements in $F(n)$ and satisfy the following properties:

$$F(n) = H_0 \cup -H_0, \quad \text{and } H_0 \cap -H_0 = \emptyset.$$

One can generalize the definition of half system mod n as follows. The set $H = \{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{n_1}}\}$ satisfies that every $a(\not\equiv 0 \bmod n)$ is congruent to exactly one of a_j or $-a_j$. Thus the number of possible $H \in S$ is 2^{n_1} and every half system H satisfies

$$F(n) = H \cup -H \quad \text{and } H \cap -H = \emptyset.$$

Now we shall consider the action $(\mathbf{Z}/n\mathbf{Z})^\times$ on $F(n)$ and define a $(\mathbf{Z}/n\mathbf{Z})^\times$ orbit for any positive divisor d of n as follows

$$F(n,d) = \{\overline{a} \neq \overline{0} \mid (a,n) = n/d\},$$

where (a,n) denotes the greatest common divisor of a and n. We note that $F(n)$ decomposes into the following disjoint union

$$F(n) = \bigcup_{d|n} F(n,d).$$

For any half system H mod n, we shall define $H(n,d)$ by putting

$$H(n,d) = H \cap F(n,d).$$

Then H decomposes into the disjoint union as follows:

$$H = \bigcup_{d|n} H(n,d).$$

Now we shall define the number $\mu_H(\overline{a})$ (or simply $\mu_H(a)$) and $\mu_{H(n,d)}(\overline{a})$ (or simply $\mu_{H(n,d)}(a)$) by putting

$$\mu_H(a) = \#\{aH \cap -H)\},$$

$$\mu_{H(n,d)}(a) = \#\{aH(n,d) \cap -H(n,d)\}.$$

From the above decomposition $H = \bigcup_{d|n} H(n,d)$, we have

$$\mu_H(a) = \sum_{d|n} \mu_{H(n,d)}(a).$$

In the next section, we shall show

$$\mu_{H_1}(a) \equiv \mu_{H_2}(a) \mod 2,$$

for any half systems H_1 and H_2. This fact plays an important role in the generalization of Gauss's lemma for an odd positive integer n. We note that, for any $\overline{a} \in (\mathbf{Z}/n\mathbf{Z})^\times$ and for any half system H mod n, aH is also a half system mod n. Thus we can consider the reduced residue class group $(\mathbf{Z}/n\mathbf{Z})^\times$ acts on the set of half systems S. We note the number $\mu_H(a)$ is the number of elements in the intersection of two half systems aH and $-H$.

More generally, for any half systems H_1 and H_2, we shall define the number $\mu(H_1, H_2)$ by putting

$$\mu(H_1, H_2) = \#\{H_1 \cap H_2\}.$$

In the following, let us consider the elementary properties of the distribution of the numbers $\mu(H_1, H_2)$. For any a with $(a, n) = 1$, we know $\mu(aH_1, aH_2) = \mu(H_1, H_2)$. Thus we have shown that the above numbers satisfy

$$\mu_H(a) = \mu(aH, -H) = \mu(H, -aH).$$

Let M be the arithmetic mean of $\mu(H_1, H_2)$, that is,

$$M = \frac{\sum \mu(H_1, H_2)}{2^{2n_1}},$$

where H_1, H_2 run all of the half systems $H_1, H_2 \in S$,

Proposition 1. *With the above notation, we have*

$$M = \frac{n-1}{4}.$$

Proof. There are 2^{2n_1} pairs of H_1 and H_2 in S. Consider the case when $H_1 \cap H_2$ is the set $\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}\}$. Then k varies from 0 to n_1 and one can express H_1 and H_2 as follows:

$$H_1 = \{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}\} \cup \{\overline{y_1}, \ldots, \overline{y_{n_1-k}}\},$$

and

$$H_2 = \{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}\} \cup \{-\overline{y_1}, \ldots, -\overline{y_{n_1-k}}\}.$$

Hence there are
$\binom{n_1}{k}$ choices of $\{\overline{x_1}, \overline{x_2}, \ldots, \overline{x_k}\}$ from $\{\overline{1}, \ldots, \overline{n_1}\}$
and

2^k choices of the signs of $\overline{x_i}$,
and
2^{n_1-k} choices of the signs of $\overline{y_j}$.
Therefore there are

$$\left(\binom{n_1}{k}\cdot 2^k\right)\cdot 2^{n_1-k}=\binom{n_1}{k}\cdot 2^{n_1}$$

pairs of H_1, H_2 with $\mu(H_1,H_2)=k$.
Finally we have

$$M=\frac{\sum\mu(H_1,H_2)}{2^{2n_1}}=\frac{1}{2^{n_1}}\times\left(\sum_{k=0}^{n_1}k\cdot\binom{n_1}{k}\right)$$

$$=\frac{1}{2^{n_1}}\times n_1 2^{n_1-1}=\frac{n_1}{2}=\frac{n-1}{4}.$$

Now consider the special half systems of the form aH. Let H be any fixed half system and $m(H)$ be the mean value of the values of $\{\mu(H,aH)\mid \overline{a}\in(\mathbf{Z}/n\mathbf{Z})^\times\}$. Then we have

$$m(H)=\frac{\sum_a \mu_H(a)}{\phi(n)},$$

where a runs all of the representatives of the reduced residue class group $(\mathbf{Z}/n\mathbf{Z})^\times$. Here $\phi(n)$ is the Euler function and satisfies $\phi(n)=\#\{(\mathbf{Z}/n\mathbf{Z})^\times\}$.

Proposition 2. *With the above notation, we have*

$$m(H)=\frac{n-1}{4}.$$

Proof. For any $\overline{a}$, $\overline{-a}$ is also a residue class such that $\overline{-a}\in(\mathbf{Z}/n\mathbf{Z})^\times$. Moreover H decomposes into two disjoint union as $H=(H\cap aH)\cup(H\cap -aH)$, which implies that the mean value $m(H)=\dfrac{n-1}{4}$ for any half system H.

Remark 1. From this proposition and the fact $\mu_{H_1}(a)\equiv\mu_{H_2}(a) \mod 2$, we see these values don't depend on the choice of the half systems. Hence one may expect the values $\mu_{H_1}(a)$ and $\mu_{H_2}(a)$ does not differ so much. But it is not true in general. We note here that the exact values $\mu_{H_1}(a)$ and $\mu_{H_2}(a)$ actually depend on the choice of the half systems H_1 and H_2. To explain this fact, we shall give here two special examples of half systems as follows.

Example 1. Let $n = p$ be a prime and g be a primitive root mod p. n_1 denotes $(p-1)/2$ as above. Then it is well known that $(\mathbf{Z}/p\mathbf{Z})^\times = \langle \overline{g} \rangle$ and $\overline{g}^{n_1} = \overline{-1}$. Since $F(p) = \{\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{2n_1-1}\} = (\mathbf{Z}/p\mathbf{Z})^\times$, we can take a half system H_1 by putting

$$H_1 = \{\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{n_1-1}\}.$$

In the case $0 \leq k \leq n_1$, we see

$$g^k H_1 = \{\overline{g}^k, \overline{g}^{k+1}, \overline{g}^2, \ldots, \overline{g}^{n_1+k-1}\},$$

and

$$g^k H_1 \cap -H_1 = \{-\overline{1}, -\overline{g}, \ldots, -\overline{g}^{k-1}\}.$$

Hence we have $\mu_{H_1}(g^k) = k$ for this case.
In the case $n_1 < k \leq 2n_1 - 1$, we shall put $k' = k - n_1$. Then we see

$$g^k H_1 = \{\overline{g}^{n_1}\overline{g}^{k'}, \overline{g}^{n_1}\overline{g}^{k'+1}, \ldots, \overline{g}^{n_1}\overline{g}^{n_1+k'-1}\}.$$

Since $\overline{g}^{n_1} = \overline{-1}$, we have

$$g^k H_1 \cap -H_1 = \{-\overline{g}^{k'}, -\overline{g}^{k'+1}, \ldots, -\overline{g}^{n_1-1}\}.$$

Hence we have $\mu_{H_1}(g^k) = n_1 - k' = 2n_1 - k$ for this case.
Thus the exact values of $\mu_{H_1}(g^k)$ is

$$\{\mu_{H_1}(g^k) \mid 0 \leq k \leq p-2 = 2n_1 - 1\} = \{0, 1, 1, 2, 2, \ldots, n_1 - 1, n_1 - 1, n_1\}.$$

Hence we can calculate $m(H_1)$ directly by

$$m(H_1) = \frac{\sum \mu_{H_1}(g^k)}{\phi(p)} = \frac{\sum_{k=0}^{n_1} k + \sum_{k'=1}^{n_1-1} k'}{2n_1}$$

$$= \frac{n_1^2}{2n_1} = \frac{n_1}{2} = \frac{p-1}{4}.$$

In this case the variance $v(H_1)$ of the distribution of $\{\mu_{H_1}(a)\}$ is given by

$$v(H_1) = \frac{\sum_{k=0}^{n_1} \mu_{H_1}(g^k)^2 + \sum_{k'=1}^{n_1-1} \mu_{H_1}(g^{k'})^2}{2n_1} - m(H_1)^2$$

$$= \frac{\sum_{k=0}^{n_1} k^2 + \sum_{k'=1}^{n_1-1} k'^2}{2n_1} - \frac{n_1^2}{4}$$

$$= \frac{n_1(n_1+1)(2n_1+1) + (n_1-1)n_1(2n_1-1)}{12n_1} - \frac{n_1^2}{4} = \frac{n_1^2+2}{12}.$$

Example 2. Assume $n = p$ is a prime congruent to 3 mod 4. Then we can take a half system $H_2 = \langle \overline{g}^2 \rangle$. Then H_2 is a subgroup of index 2 of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times$. We know $(\mathbf{Z}/n\mathbf{Z})^\times = H_2 \cup -H_2$ is the cosset decomposition mod H_2. For any a with $(a,p) = 1$, we have

$$\mu_{H_2}(a) = \begin{cases} 0 & \text{when } \left(\frac{a}{p}\right) = 1, \\ n_1 & \text{when } \left(\frac{a}{p}\right) = -1. \end{cases}$$

Thus we can calculate $m(H_2)$ directly by

$$m(H_2) = \frac{\sum_a \mu_{H_2}(a)}{2n_1} = \frac{n_1(0+n_1)}{2n_1} = \frac{n_1}{2} = \frac{p-1}{4}.$$

In this case, the variance $v(H_2)$ of the distribution $\{\mu_{H_2}(a) \mid \overline{a} \in (\mathbf{Z}/n\mathbf{Z})^\times\}$ is given by

$$\begin{aligned} v(H_2) &= \frac{\sum_a (\mu_{H_2}(a) - m(H_2))^2}{2n_1} \\ &= 2n_1 \times \frac{(n_1/2)^2}{2n_1} = \frac{n_1^2}{4}. \end{aligned}$$

2. Schering's generalization of Gauss's lemma

We shall begin to study the action $(\mathbf{Z}/n\mathbf{Z})^\times$ on $F(n,d)$ more precisely. Put $m = \phi(d)$. Then, from the definition of $F(n,d)$, $F(n,d)$ can be expressed as

$$F(n,d) = \{(n/d)\overline{x_1}, (n/d)\overline{x_2}, \ldots, (n/d)\overline{x_m}\},$$

where x_i satifies $1 \leq x_i \leq d$ and $(x_i, d) = 1$. Here we denote $(x_i \mod d)$ by $\overline{x_i}$. Since n is odd, the divisor d is also odd. Hence $m = \phi(d)$ is always even. Put $m = 2m_1$. Then we can express the set $H(n,d) = H \cap F(n,d)$ as follows

$$H(n,d) = \{(n/d)\overline{a_1}, (n/d)\overline{a_2}, \ldots, (n/d)\overline{a_{m_1}}\}.$$

Here $\{\overline{a_1}, \overline{a_2}, \ldots, \overline{a_{m_1}}\}$ is a half system mod d. Take any a such that $(a,n) = 1$. Then we have

$$aF(n,d) = F(n,d) = H(n,d) \cup -H(n,d).$$

Hence, for each $1 \leq i \leq m_1$, there exists exactly one j $(1 \leq j \leq m_1)$ which satisfies

$$a\overline{a_i} = \overline{a_j} \text{ or } -\overline{a_j}.$$

Therefore, we get the following congruence

$$(aa_1)(aa_2)\cdots(aa_{m_1}) \equiv (-1)^{\mu_{H(n,d)}(a)} a_1 a_2 \cdots a_{m_1} \mod d.$$

Since $(a_1 a_2 \cdots a_{m_1}, d) = 1$, we have verified the following proposition.

Proposition 3 (Generalized Euler's criterion).
For any a such that $(a, n) = 1$, we have a generalization of Euler's criterion

$$(-1)^{\mu_{H(n,d)}(a)} \equiv a^{\phi(d)/2} \mod d.$$

Remark 2. From this Euler's criterion, we have shown the parity of $\mu_{H(n,d)}(a)$ does not depend on the choice of the half system H.

Remark 3. We note that the special case when n is a prime p and $d = 1$ in Proposition 3 is the exactly the following case:

$$a^{(p-1)/2} \equiv (-1)^{\mu_{H(p,p)}(a)} = \left(\frac{a}{p}\right) \mod p,$$

which is usual Euler's criterion for Legendre symbol $\left(\frac{a}{p}\right)$. We shall denote the usual Gauss's half system by $H_0 = \{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\}$. In the following, we shall simply write $\mu_{H_0(p,p)}(a)$ by $\mu_p(a)$.

Using this generalized Euler's criterion, we shall show the following generalized Gauss's lemma, which was firstly proved by Schering [12] (1882).

Gauss's lemma. *Let n be odd positive integer. For any a with $(a, n) = 1$, the Jacobi symbol $\left(\frac{a}{n}\right)$ satisfies*

$$\left(\frac{a}{n}\right) = (-1)^{\mu_H(a)},$$

for any n and any half system mod n H.

We shall show this lemma by proving following two lemmas.

Lemma 1. *Suppose $(pq)|d$, where $p \neq q$ are distinct prime divisors of d. Then*

$$\mu_{H(n,d)}(a) \equiv 0 \mod 2.$$

Lemma 2. *Suppose $p^e|n$ and $p^{e+1} \not| n$. Put $d = p^e$. Then we have*

$$\mu_{H(n,p^e)}(a) \equiv \mu_{H(n,p^{e-1})}(a) \equiv \cdots \equiv \mu_{H(n,p)}(a) \equiv \mu_p(a) \mod 2.$$

Proofs of Lemma 1 and Lemma 2.
We shall prove Lemma 1 as follows. From the assumption $(pq)|d$, d decomposes into $d = p^e \cdot q^f \cdot d_1$ with p, q are distinct prime divisors and $(pq, d_1) = 1$. There exists an isomoriphsm of reduced residue class groups:

$$(\mathbf{Z}/d\mathbf{Z})^\times \cong (\mathbf{Z}/p^e\mathbf{Z})^\times \times (\mathbf{Z}/q^f\mathbf{Z})^\times \times (\mathbf{Z}/d_1\mathbf{Z})^\times,$$

where the residue class

$$(a \mod d) \in (\mathbf{Z}/n\mathbf{Z})^\times$$

corresponds to

$$(a \mod p^e, a \mod q^f, a \mod d_1).$$

Moreover we have $\phi(d) = \phi(p^e)\phi(q^f)\phi(d_1) = (p^{e-1}(p-1))(q^{f-1}(q-1))\phi(d_1)$. Since $p - 1 \equiv q - 1 \equiv 0 \mod 2$, we have

$$\begin{aligned} a^{\phi(d)/2} &\equiv (a^{\phi(p^e)})^{\phi(d_1)(\phi(q^f)/2)} \equiv 1 \mod p^e, \\ a^{\phi(d)/2} &\equiv (a^{\phi(q^f)})^{\phi(d_1)(\phi(p^e)/2)} \equiv 1 \mod q^f. \\ a^{\phi(d)/2} &\equiv (a^{\phi(d_1)})^{\phi(p^e))(\phi(q^f)/2)} \equiv 1 \mod d_1. \end{aligned}$$

Thus $a^{\phi(d)/2} \equiv 1 \mod d$. From Proposition 3, we have $(-1)^{\mu_{H(n,d)}(a)} \equiv 1 \mod d$. Since $d \geq 3$, we can conclude $(-1)^{\mu_{H(n,d)}(a)} = 1$ for this case, that is, $\mu_{H(n,d)}(a) \equiv 0 \mod 2$, which completes the proof of Lemma 1.

Now, we shall prove Lemma 2. Let $p^e||n$ as above. In the case $d|p^e$, the primitive root $g \mod p^e$ is also the primitive root mod $d = p^c$. Hence we can take a half system $H(n, d)$ of the following form

$$H(n,d) = \{(n/d)\overline{1}, (n/d)\overline{g}, (n/d)\overline{g}^2, \ldots, (n/d)\overline{g}^{\phi(d)/2-1}\},$$

where $g^{\phi(d)/2} \equiv -1 \mod d$.
Take any a with $(a, n) = 1$. Then a can be expressed $(a \equiv g^r \mod p^e)$. We note that, for any $1 \leq c \leq e$, $(g \mod p^c)$ is a generator of the cyclic group $(\mathbf{Z}/p^c\mathbf{Z})^\times$. r_1 denotes the residue of $(r \mod \phi(p^c))$, where $\phi(p^c) = p^{c-1}(p-1)$ is always even. Hence we have shown:

$$a \equiv g^r \equiv g^{r_1} \mod p^c,$$

and

$$r_1 \equiv r \mod 2.$$

In the same way as Example 1, we have

$$\mu_{H(n,d)}(a) = \begin{cases} r_1 & \text{for } 0 \leq r_1 \leq \frac{\phi(d)}{2}, \\ \phi(d) - r_1 & \text{for } \frac{\phi(d)}{2} < r_1 < \phi(d). \end{cases}$$

Hence we have

$$\mu_{H(n,p^c)}(a) \equiv r_1 \mod 2.$$

Therefore we can conclude, for any $1 \leq c \leq e$,

$$\mu_{H(n,p^c)}(a) \equiv r \mod 2.$$

Since, $\mu_{H(n,p)}(a) = \mu_p(a)$, we have

$$\mu_{H(n,p^e)}(a) \equiv \mu_{H(n,p^{e-1})}(a) \equiv \cdots \equiv \mu_{H(p,p)}(a) \equiv \mu_p(a) \mod 2.$$

Hence we have shown:

$$\sum_{c=1}^{e} \mu_{H(n,p^c)}(a) \equiv e\mu_p(a) \mod 2,$$

which completes the proof of Lemma 2.

Let n be decomposed into primes of the form $n = p_1^{e_1} p_1^{e_2} \cdots p_k^{e_k}$. Combining the above two lemmas, we have

$$\begin{aligned} \mu_H(a) &= \textstyle\sum_{d|n} \mu_{H(n,d)}(a) \\ &\equiv \textstyle\sum_{1 \leq i \leq k, 1 \leq c_i \leq e_i} \mu_{H(n,p_i{}^{c_i})}(a) \mod 2 \\ &\equiv \textstyle\sum_{i=1}^{k} e_i \mu_{p_i}(a) \mod 2. \end{aligned}$$

Thus we have shown

$$(-1)^{\mu_{H(n)(a)}} = \prod_{i=1}^{k} (-1)^{e_i \mu_{p_i}(a)} = \prod_{i=1}^{k} ((-1)^{\mu_{p_i}(a)})^{e_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i} = \left(\frac{a}{n}\right),$$

which completes the proof of generalized Gauss's lemma.

3. Takagi's proof of quadratic reciprocity laws for Jacobi symbols

In this section, we shall give a visual proof of the quadratic reciprocity laws of Jacobi symbols. The proof is not new but an explicit visual version of Takagi's proof [13] based on Schering's generalized Gauss's lemma.

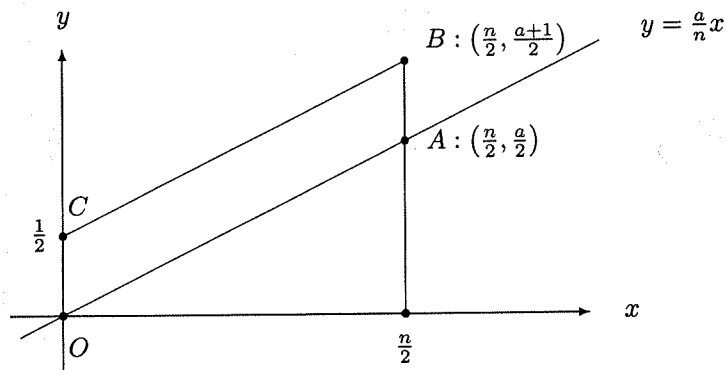
Let n an odd positive integer and a be an integer coprime to n. Let $H_0 = \{1, 2, \ldots, n_1 = \frac{n-1}{2}\}$ be a Gauss's half system mod n as in section 2. Then the generalized Gauss's lemma mod n for half system H_0 states that

$$\left(\frac{a}{n}\right) = (-1)^{\mu_{H_0}(a)},$$

where $\mu_{H_0}(a)$ is the number of x $(1 \leq x \leq n_1 = (n-1)/2)$ such that

$$\left[\frac{ax}{n}\right] + \frac{1}{2} < \frac{ax}{n} < \left[\frac{ax}{n}\right] + 1.$$

Let $N(n, a)$ denote the number of integer points (x, y) lying in the following parallelogram $OABC$.



We note that

$$\left[\frac{ax}{n}\right] + \frac{1}{2} < \frac{ax}{n} < \left[\frac{ax}{n}\right] + 1 \Longleftrightarrow \frac{ax}{n} < \left[\frac{ax}{n}\right] + 1 < \frac{ax}{n} + \frac{1}{2}.$$

Hence we know $\mu_{H_0}(a) = N(n, a)$ and Schering's generalized Gauss's lemma can be written as follows:

Visual version of Gauss's lemma.
With the above notation, Jacobi symbol $\left(\frac{a}{n}\right)$ *can be expressed by the number of integer points in the above parallelogram* $OABC$*, that is*

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

The special cases $a = -1$ and $a = 2$ are called the first supplemental law and the second supplemental law, respectively. From the following parallelograms $OABC$, we see

$$N(n,-1) = \#\{(x,0) \in OABC\} = n_1 = \frac{n-1}{2},$$

and

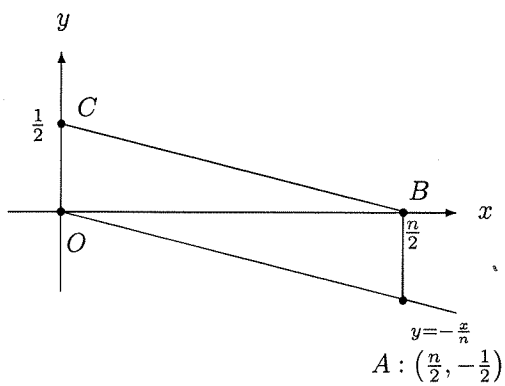
$$N(n,2) = \#\{(x,1) \in OABC\} = \left[\frac{n}{2}\right] - \left[\frac{n}{4}\right],$$

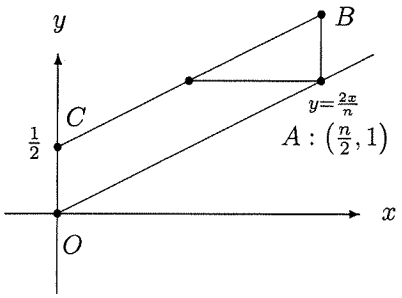
and obtain the first supplemental law;

$$\left(\frac{-1}{n}\right) = \begin{cases} 1 & \text{for } n \equiv 1 \mod 4, \\ -1 & \text{for } n \equiv -1 \mod 4, \end{cases}$$

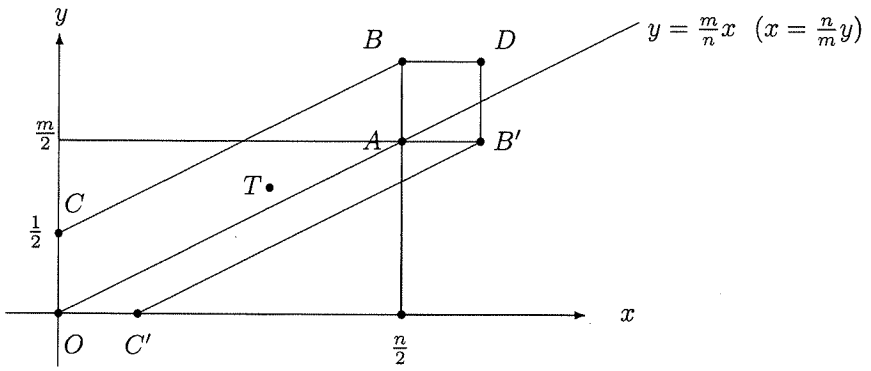
and the second supplemental law;

$$\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{for } n \equiv 1 \text{ or } -1 \mod 8, \\ -1 & \text{for } n \equiv 3 \text{ or } -3 \mod 8. \end{cases}$$





Now we shall show a visual version of the quadratic reciprocity law, which is nothing but the modified proof given by Takagi replacing p, q by n, m. Let m, n be two distinct odd positive coprime integers. Then the number of integer points lying in the following parallelograms $OABC$ and $OAB'C'$ are $N(n,m)$ and $N(m,n)$, respectively.



From the visual version of Gauss's lemma as above, we know that

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{N(n,m)+N(m,n)}.$$

Let N be the number of integer points in the hexagon $OC'B'DBC$. Since there is no integer point lying in the square $AB'DB$, we know that

$$N(n,m) + N(m,n) = N.$$

One sees that the hexagon $OC'B'DBC$ is symmetric with respect to the center $T = \left(\frac{n+1}{4}, \frac{m+1}{4}\right)$. Hence we know that the number N is even except for the center T.
We have the fact:

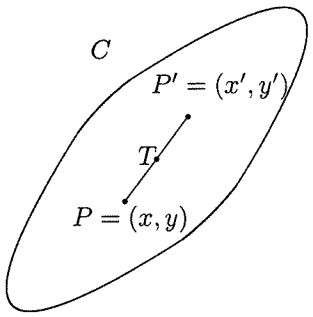
T is an integer point $\iff$ both n and $m \equiv 3 \mod 4$.

Thus $N(n,m) + N(m,n)$ is odd, if and only if both n and m are congruent to 3 mod 4, which completes the proof the following quadratic reciprocity law of Jacobi symbols:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\cdot\frac{m-1}{2}}.$$

4. Concluding Remarks

In his paper [8], T. Kubota introduced a new geometrical method for constructing class field theory. One of his aim was to establish the Artin's reciprocity law directly and then construct class field theory through the Artin's reciprocity law. At a first glance, his construction seems very complicated. But if one restrict Kubota's geometrical proof to quadratic residues, one can get a very simple proof of quadratic reciprocity laws. We note that the reader who interested in the proof can find this simple proof in his ealier paper [7]. The second author has heard from Kubota that his another aim was to find a way of construction of class field theory as easy to be understood by the students of elementary schools and junior high schools. We feel Kubota's proof for quadratic reciprocity laws in [7] has still difficult points to be understood by these students. On the contraly, we have generalized the proof of Legendre symbols to Jacobi symbols. Hence we have avoided the notion of primes. Thus, if one adopts the definition of Jacobi symbols by the number of integer points in the above parallelogram, then the key ingredient of our proof is the parity of the number of integer points in the following point-symmetric region C.



We assume the co-ordinates (a, b) of the center T of the point-symmetric region C satisfies $2a, 2b \in \mathbf{Z}$. Then the symmetric points $P = (x, y)$ and $P' = (x', y')$ satisfies $x' = 2a - x, y' = 2b - y$. Thus we know

$$\begin{aligned} & (x, y) \text{ is an integer point} \\ \Longleftrightarrow \quad & (x'y') \text{ is an integer point.} \end{aligned}$$

Thus the number of the integer points in this point-symmetric region is odd if and only if the center T of the region C is an integer point.

We hope our visual modification of Takagi's proof would be of some interest to those young students.

References

[1] P. Bachman, Grundlehren der Neueren Zahlentheorie, Walter de Gruyter, Berlin, 1931.

[2] C. F. Gauss, Disquisitiones Arithmeticae, English Edition, Springer–Verlag, New York, 1986.

[3] C. F. Gauss, Theorematis arithmetici demonstratio nova, *Comment. Soc. regiae sci. Göttingen*, **16**, (1808), 69; Werke II, 1-8.

[4] C. F. Gauss, Werke II, Verlag, Hildesheim, 1973.

[5] G. H. Hardy and E. M. Wright, An Introduction to The Theory of Numbers, 5th edition, Oxford University Press, Oxford, 1979.

[6] C. G. J. Jacobi, Über die Kleistheilung und ihre Anwendung auf die Zahlentheorie, *J. Reine Angew Math.*, **30**, (1837), 127-136; Werke VI, 254-274.

[7] T. Kubota, Geometry of numbers and class field theory, *Sūrikaisekiken-kōkyūroku*, **411**, (1981), 121-141 (in Japanese).

[8] T. Kubota, Geometry of numbers and class field theory, *Japan. J. math. (N.S.)*, **13**, (1987), 235-275.

[9] T. Kubota, A foundation of class field theory applying properties of spatial figures, *Sūgaku Expositions*, **8**, (1995), 1-16.

[10] A. Kuroki, Quadratic reciprocity laws, Master thesis (2009) Tokushima University (in Japanese).

[11] F. Lemmermeyer, Reciprocity Laws, Springer–Verlag, Berlin, 2000.

[12] E. Schering, Zur Theorie der quadratischen Reste, *Acta Math.*, **1**, (1882), 153-170; Werke II, 69-86.

[13] T. Takagi, A simple proof of the law of quadratic reciprocity for quadratic residues, *Proc. Phys.-Math. Soc. Japan* Ser **2**, (1903), 74-78.

[14] T. Takagi, Lectures on Elementary Number Theory, 2nd edition, Kyōritsu-shuppan, Tokyo, 1971 (in Japanese).